Tulsiramji Gaikwad-Patil College of Engineering and Technology
Wardha Road, Nagpur-441 108
NAAC Accredited

Department of Computer Science & Engineering

Subject: Computer Network

Semester: VI

Q.1 a] Explain in detail about layers in OSI reference model.

The Open Systems Interconnect (OSI) model has seven layers. This article describes and explains them, beginning with the 'lowest' in the hierarchy (the physical) and proceeding to the 'highest' (the application). The layers are stacked this way:

- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical

PHYSICAL LAYER

The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers. It provides:

- Data encoding: modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization. It determines:
    - What signal state represents a binary 1
    - How the receiving station knows when a "bit-time" starts
    - How the receiving station delimits a frame
- Physical medium attachment, accommodating various possibilities in the medium:
    - Will an external transceiver (MAU) be used to connect to the medium?
    - How many pins do the connectors have and what is each pin used for?
- Transmission technique: determines whether the encoded bits will be transmitted by baseband (digital) or broadband (analog) signaling.
- Physical medium transmission: transmits bits as electrical or optical signals appropriate for the physical medium, and determines:
    - What physical medium options can be used
    - How many volts/db should be used to represent a given signal state, using a given physical medium

DATA LINK LAYER

The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link. To do this, the data link layer provides:

- Link establishment and termination: establishes and terminates the logical link between two nodes.
- Frame traffic control: tells the transmitting node to "back-off" when no frame buffers are available.
- Frame sequencing: transmits/receives frames sequentially.
- Frame acknowledgment: provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting non-acknowledged frames and handling duplicate frame receipt.
- Frame delimiting: creates and recognizes frame boundaries.
- Frame error checking: checks received frames for integrity.
- Media access management: determines when the node "has the right" to use the physical medium.

NETWORK LAYER

Tulsiramji Gaikwad-Patil College of Engineering and Technology
Wardha Road, Nagpur-441 108
NAAC Accredited

Department of Computer Science & Engineering

The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors. It provides:

- Routing: routes frames among networks.
- Subnet traffic control: routers (network layer intermediate systems) can instruct a sending station to "throttle back" its frame transmission when the router's buffer fills up.
- Frame fragmentation: if it determines that a downstream router's maximum transmission unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and re-assembly at the destination station.
- Logical-physical address mapping: translates logical addresses, or names, into physical addresses.
- Subnet usage accounting: has accounting functions to keep track of frames forwarded by subnet intermediate systems, to produce billing information.

Communications Subnet

The network layer software must build headers so that the network layer software residing in the subnet intermediate systems can recognize them and use them to route data to the destination address.

This layer relieves the upper layers of the need to know anything about the data transmission and intermediate switching technologies used to connect systems. It establishes, maintains and terminates connections across the intervening communications facility (one or several intermediate systems in the communication subnet).

In the network layer and the layers below, peer protocols exist between a node and its immediate neighbor, but the neighbor may be a node through which data is routed, not the destination station. The source and destination stations may be separated by many intermediate systems.

TRANSPORT LAYER

The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.

The size and complexity of a transport protocol depends on the type of service it can get from the network layer. For a reliable network layer with virtual circuit capability, a minimal transport layer is required. If the network layer is unreliable and/or only supports datagrams, the transport protocol should include extensive error detection and recovery.

The transport layer provides:

- Message segmentation: accepts a message from the (session) layer above it, splits the message into smaller units (if not already small enough), and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message.
- Message acknowledgment: provides reliable end-to-end message delivery with acknowledgments.
- Message traffic control: tells the transmitting station to "back-off" when no message buffers are available.
- Session multiplexing: multiplexes several message streams, or sessions onto one logical link and keeps track of which messages belong to which sessions (see session layer).

Typically, the transport layer can accept relatively large messages, but there are strict message size limits imposed by the network (or lower) layer. Consequently, the transport layer must break up the messages into smaller units, or frames, prepending a header to each frame.

The transport layer header information must then include control information, such as message start and message end flags, to enable the transport layer on the other end to recognize message boundaries. In addition, if the lower layers do not maintain sequence, the transport header must contain sequence information to enable the transport layer on the receiving end

to get the pieces back together in the right order before handing the received message up to the layer above.

End-to-end layers

Unlike the lower "subnet" layers whose protocol is between immediately adjacent nodes, the transport layer and the layers above are true "source to destination" or end-to-end layers, and are not concerned with the details of the underlying communications facility. Transport layer software (and software above it) on the source station carries on a conversation with similar software on the destination station by using message headers and control messages.

SESSION LAYER

The session layer allows session establishment between processes running on different stations. It provides:

- Session establishment, maintenance and termination: allows two application processes on different machines to establish, use and terminate a connection, called a session.
- Session support: performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging, and so on.

PRESENTATION LAYER

The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station.

The presentation layer provides:

- Character code translation: for example, ASCII to EBCDIC.
- Data conversion: bit order, CR-CR/LF, integer-floating point, and so on.
- Data compression: reduces the number of bits that need to be transmitted on the network.
- Data encryption: encrypt data for security purposes. For example, password encryption.

APPLICATION LAYER

The application layer serves as the window for users and application processes to access network services. This layer contains a variety of commonly needed functions:

- Resource sharing and device redirection
- Remote file access
- Remote printer access
- Inter-process communication
- Network management
- Directory services
- Electronic messaging (such as mail)
- Network virtual terminals

b) Write the difference between service and protocols. Also list and explain the different service primitives.

Services and protocols

An important aspect to understand before studying computer networks is the difference between a *service* and a *protocol*.

Tulsiramji Gaikwad-Patil College of Engineering and Technology
Wardha Road, Nagpur-441 108
NAAC Accredited

Department of Computer Science & Engineering

In order to understand the difference between the two, it is useful to start with real world examples. The traditional Post provides a service where a postman delivers letters to recipients. The Post defines precisely which types of letters (size, weight, etc) can be delivered by using the Standard Mail service. Furthermore, the format of the envelope is specified (position of the sender and recipient addresses, position of the stamp). Someone who wants to send a letter must either place the letter at a Post Office or inside one of the dedicated mailboxes. The letter will then be collected and delivered to its final recipient. Note that for the regular service the Post usually does not guarantee the delivery of each particular letter, some letters may be lost, and some letters are delivered to the wrong mailbox. If a letter is important, then the sender can use the registered service to ensure that the letter will be delivered to its recipient. Some Post services also provide an acknowledged service or an express mail service that is faster than the regular service.

In computer networks, the notion of service is more formally defined in [X200] . It can be better understood by considering a computer network, whatever its size or complexity, as a black box that provides a service to *users* , as shown in the figure below. These users could be human users or processes running on a computer system.

The four types of primitives

Four types of primitives are defined :

- *X.request*. This type of primitive corresponds to a request issued by a user to a service provider
- *X.indication*. This type of primitive is generated by the network provider and delivered to a user (often related to an earlier and remote *X.request* primitive)
- *X.response*. This type of primitive is generated by a user to answer to an earlier *X.indication* primitive
- *X.confirm*. This type of primitive is delivered by the service provide to confirm to a user that a previous *X.request* primitive has been successfully processed.

- **Explain the design issues of OSI model layer**

The following are the design issues for the layers:

- **Reliability:** It is a design issue of making a network that operates correctly even when it is made up of unreliable components.
- **Addressing:** There are multiple processes running on one machine. Every layer needs a mechanism to identify senders and receivers.
- **Error Control**: It is an important issue because physical communication circuits are not perfect. Many error detecting and error correcting codes are available. Both sending and receiving ends must agree to use any one code.
- **Flow Control:** If there is a fast sender at one end sending data to a slow receiver, then there must be flow control mechanism to control the loss of data by slow receivers. There are several mechanisms used for flow control such as increasing buffer size at receivers, slow down the fast sender, and so on. Some process will not be in position to accept arbitrarily long messages. This property leads to mechanisms for disassembling, transmitting and the reassembling messages.
- **Multiplexing and De-multiplexing:** If the data has to be transmitted on transmission media separately, it is inconvenient or expensive to setup separate connection for each pair of communicating processes. So, multiplexing is needed in the physical layer at sender end and de-multiplexing is need at the receiver end.
- **Scalability**: When network gets large, new problem arises. Thus scalability is important so that network can continue to work well when it gets large.
- **Routing:** When there are multiple paths between source and destination, only one route must be chosen. This decision is made on the basis of several routing algorithms, which chooses optimized route to the destination.

- **Confidentiality and Integrity:** Network security is the most important factor. Mechanisms that provide confidentiality defend against threats like eavesdropping. Mechanisms for integrity prevent faulty changes to messages.

Q.2 a] State and explain the significance of studying topology. Explain any four topologies with their advantages and disadvantages.

Network topology refers to the arrangement of computers connected in a network through some physical medium such as cable, optical fiber etc. Topology generally determines the shape of the network. The various types of network topologies are as follows:

- Hierarchical topology
- Bus topology
- Star topology
- Ring topology
- Mesh topology
- Hybrid topology

1) Hierarchical Topology

The hierarchical topology is also known as tree topology, which is divided into different levels connected with the help of twisted pair, coaxial cable or fiber optics

This type of topology is arranged in the form of a tree structure in which top level contains parent node (root node), which is connected with the child nodes in the second level of hierarchy with point-to-point link. The second level nodes are connected to the third level nodes, which in turn are connected to the fourth level nodes and so on. Except the top-level nodes, each level node has a parent node.

The number of point-to-point links in the hierarchical type of topology is generally one less than the total number of nodes in the structure. The hierarchical topology is symmetrical, having a fixed branching factor, f, associated with each node. The branching factor is the number of point-to-point links between the levels of hierarchy. **Figure 1 shows the arrangement of computers in hierarchical topology**.

Advantages of hierarchical topology are:

- The hierarchical topology is generally supported by most hardware and software.
- In the hierarchical topology, data is received by all the nodes efficiently because of point-to-point link.

The following are the disadvantages of hierarchical topology:

- In the hierarchical topology, when the root node fails, the whole network crashes.
- The hierarchical topology is difficult to configure.

2) Linear Bus Topology

In the linear bus topology, all the nodes are connected to the single backbone or bus with some medium such as twisted pair, coaxial cable etc.

When a node wants to communicate with the other nodes in the network, it simply sends a message to the common bus. All the nodes in the network then receive the message but the node for which it was actually sent only processes it. The other nodes discard the message. **Figure 2 shows the arrangement of computers in the linear bus topology**.

Advantages of linear bus topology are:

- The linear bus topology usually requires less cabling.
- The linear bus topology is relatively simple to configure and install.
- In the linear bus topology, the failure of one computer does not affect the other computers in the network.

Tulsiramji Gaikwad-Patil College of Engineering and Technology
Wardha Road, Nagpur-441 108
NAAC Accredited

Department of Computer Science & Engineering

The following are the disadvantages of linear bus topology:

- In the linear bus topology, the failure of the backbone cable results in the breakdown of entire network.
- Addition of computers in the linear bus topology results in the performance degradation of the network.
- The bus topology is difficult to reconstruct in case of faults.

3) Star Topology

In the star topology, all the nodes are connected to a common device known as hub. Nodes are connected with the help of twisted pair, coaxial cable or optical fiber.

When a node wants to send a message to the other nodes, it first sends the message to the hub, which in turn forwards the message to the intended node. Each node in the network is connected with a point-to-point link to the centralized hub. The task of hub is to detect the faulty node present in the network. On the other hand, it also manages the overall data transmission in the network. Figure 3 shows the arrangement of computers in the star topology.

Advantages of star topology are:

- This topology allows easy error detection and correction.
- In the star topology, the failure of one computer does not affect the other computers in the network.
- Star topology is easy to install.

The following are the disadvantages of star topology:

- In the star topology, the hub failure leads to the overall network crash.
- The star topology requires more amount of cable for connecting the nodes.
- It is expensive due to the cost of the hub.

4) Ring Topology

In the ring topology, the nodes are connected in the form of a ring with the help of twisted pair cable.

Each node is connected directly to the other two nodes in the network. The node, which wants to send a message, first passes the message to its consecutive node in the network. Data is transmitted in the clockwise direction from one node to another.

Figure 4 shows the arrangement of computers in the ring topology. Each node incorporates a repeater, which passes the message to next node when the message is intended for another node.

Advantages of ring topology are:

- Each node has an equal access to other nodes in the network.
- Addition of new nodes does not degrade the performance of the network.
- Ring topology is easy to configure and install.

The following are the disadvantages of ring topology:

- It is relatively expensive to construct the ring topology.
- The failure of one node in the ring topology affects the other nodes in the ring.

b]Explain the difference between connection oriented and connection less protocols

Connection-Oriented and Connectionless Protocols

A number of characteristics can be used to describe communications protocols. The most important is the distinction between *connection-oriented transport* services (COTS) and *connectionless transport* services (CLTS).

Connection-Oriented Protocols

Tulsiramji Gaikwad-Patil College of Engineering and Technology
Wardha Road, Nagpur-441 108
NAAC Accredited

Department of Computer Science & Engineering

TCP is an example of a connection-oriented protocol. It requires a logical connection to be established between the two processes before data is exchanged. The connection must be maintained during the entire time that communication is taking place, then released afterwards. The process is much like a telephone call, where a virtual circuit is established--the caller must know the person's telephone number and the phone must be answered--before the message can be delivered.

TCP/IP is also a connection-oriented transport with orderly release. With orderly release, any data remaining in the buffer is sent before the connection is terminated. The release is accomplished in a three-way handshake between client and server processes. The connection-oriented protocols in the OSI protocol suite, on the other hand, do not support orderly release. Applications perform any handshake necessary for ensuring orderly release.

Examples of services that use connection-oriented transport services are telnet, rlogin, and ftp.

Connectionless Protocols

Connectionless protocols, in contrast, allow data to be exchanged without setting up a link between processes. Each unit of data, with all the necessary information to route it to the intended destination, is transferred independent of other data packets and can travel over different paths to reach the final destination. Some data packets might be lost in transmission or might arrive out of sequence to other data packets.

UDP is a connectionless protocol. It is known as a datagram protocol because it is analogous to sending a letter where you don't acknowledge receipt.

Examples of applications that use connectionless transport services are broadcasting and tftp. Early implementations of NFS used UDP, whereas newer implementations prefer to use TCP.

Q.3 a] Explain the different error detection and correction techniques

What is Error?

Error is a condition when the output information does not match with the input information. During transmission, digital signals suffer from noise that can introduce errors in the binary bits travelling from one system to other. That means a 0 bit may change to 1 or a 1 bit may change to 0.

Error-Detecting codes

Whenever a message is transmitted, it may get scrambled by noise or data may get corrupted. To avoid this, we use error-detecting codes which are additional data added to a given digital message to help us detect if an error occurred during transmission of the message. A simple example of error-detecting code is **parity check**.

Error-Correcting codes

Along with error-detecting code, we can also pass some data to figure out the original message from the corrupt message that we received. This type of code is called an error-correcting code. Error-correcting codes also deploy the same strategy as error-detecting codes but additionally, such codes also detect the exact location of the corrupt bit.

In error-correcting codes, parity check has a simple way to detect errors along with a sophisticated mechanism to determine the corrupt bit location. Once the corrupt bit is located, its value is reverted (from 0 to 1 or 1 to 0) to get the original message.

How to Detect and Correct Errors?

To detect and correct the errors, additional bits are added to the data bits at the time of transmission.

- The additional bits are called **parity bits**. They allow detection or correction of the errors.
- The data bits along with the parity bits form a **code word**.

Parity Checking of Error Detection

It is the simplest technique for detecting and correcting errors. The MSB of an 8-bits word is used as the parity bit and the remaining 7 bits are used as data or message bits. The parity of 8-bits transmitted word can be either even parity or odd parity.

Tulsiramji Gaikwad-Patil College of Engineering and Technology
Wardha Road, Nagpur-441 108
NAAC Accredited

Department of Computer Science & Engineering

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

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

Use of Parity Bit

The parity bit can be set to 0 and 1 depending on the type of the parity required.

- For even parity, this bit is set to 1 or 0 such that the no. of "1 bits" in the entire word is even. Shown in fig. (a).
- For odd parity, this bit is set to 1 or 0 such that the no. of "1 bits" in the entire word is odd. Shown in fig. (b).

How Does Error Detection Take Place?

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

b]What is framing? Explain the different types of framing with example?

A point-to-point connection between two computers or devices consists of a wire in which data is transmitted as a stream of bits. However, these bits must be *framed* into discernible blocks of information. Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. Ethernet, token ring, frame relay, and other data link layer technologies have their own frame structures. Frames have headers that contain information such as error-checking codes.

There are three different types of framing, each of which provides a way for the sender to tell the receiver where the block of data begins and ends:

- **Byte-oriented framing** Computer data is normally stored as alphanumeric characters that are encoded with a combination of 8 bits (1 byte). This type of framing differentiates one byte from another. It is an older style of framing that was used in the terminal/mainframe environment. Examples of byte-oriented framing include IBM's BISYNC protocol.
- **Bit-oriented framing** This type of framing allows the sender to transmit a long string of bits at one time. IBM's SDLC (Synchronous Data Link Control) and HDLC (High-level Data Link Control) are examples of bit-oriented protocols. Most LANs use bit-oriented framing. There is usually a maximum frame size. For example, Ethernet has a maximum frame size of 1,526 bytes. The beginning and end of a frame is signaled with a special bit sequence (01111110 for HDLC). If no data is being transmitted, this same sequence is continuously transmitted so the end systems remain synchronized.

. Clock-based framing In a clock-based system, a series of repetitive pulses are used to maintain a constant bit rate and keep the digital bits aligned in the data stream. SONET (Synchronous Optical Network) is a synchronous system in which all the clocks in the network are synchronized back to a master clock reference. SONET frames are then positioned within the clocked stream.

The advantage of using frames is that data is broken up into recoverable chunks that can easily be checked for corruption. A glitch in the line during the transmission will corrupt some frames. Only the lost frames and not the entire set of data needs to be retransmitted. Detecting and correcting errors is discussed under "Error Detection and Correction."

Q.4 a] Explain HDLC. What are the three frames of HDLC, explain with example

Tulsiramji Gaikwad-Patil College of Engineering and Technology
Wardha Road, Nagpur-441 108
NAAC Accredited

Department of Computer Science & Engineering

High-Level Data Link Control (HDLC) is a bit-oriented code-transparent synchronous data link layer protocol developed by the International Organization for Standardization (ISO).

HDLC provides both connection-oriented and connectionless service.

HDLC can be used for point-to-multipoint connections, but is now used almost exclusively to connect one device to another, using *Asynchronous Balanced Mode* (ABM). The original master-slave modes Normal Response Mode (NRM) and Asynchronous Response Mode (ARM) are rarely used.

- Information frames, or **I-frames**, transport user data from the network layer. In addition they can also include flow and error control information piggybacked on data.
- Supervisory Frames, or **S-frames**, are used for flow and error control whenever piggybacking is impossible or inappropriate, such as when a station does not have data to send. S-frames **do not** have information fields.
- Unnumbered frames, or **U-frames**, are used for various miscellaneous purposes, including link management. Some U-frames contain an information field, depending on the type

I -Frame[control]

- Information frames, or **I-frames**, transport user data from the network layer. In addition they also include flow and error control information piggybacked on data. The sub-fields in the control field define these functions.

The least significant bit (first transmitted) defines the frame type. 0 means an I-frame. Except for the interpretation of the P/F field, there is no difference between a command I frame and a response I frame; when P/F is 0, the two forms are exactly equivalent.

S-Frames (control)

Supervisory Frames, or 'S-frames', are used for flow and error control whenever piggybacking is impossible or inappropriate, such as when a station does not have data to send. S-frames **do not** have information fields.

The S-frame control field includes a leading "10" indicating that it is an S-frame. This is followed by a 2-bit type, a poll/final bit, and a sequence number. If 7-bit sequence numbers are used, there is also a 4-bit padding field.

The first 2 bits mean it is an S-frame. All S frames include a P/F bit and a receive sequence number as described above. Except for the interpretation of the P/F field, there is no difference between a command S frame and a response S frame; when P/F is 0, the two forms are exactly equivalent.

1|0 |S|S|P/F|N(R)| The 2-bit type field encodes the type of S frame.

Receive Ready (RR)

- Bit Value = 00 (0x00 to match above table type field bit order[2])
- Indicate that the sender is ready to receive more data (cancels the effect of a previous RNR).
- Send this packet if you need to send a packet but have no I frame to send.
- A primary station can send this with the P-bit set to solicit data from a secondary station.
- A secondary terminal can use this with the F-bit set to respond to a poll if it has no data to send.

Receive Not Ready (RNR)

- Bit value = 10 (0x04 to match above table type field bit order[3])
- Acknowledge some packets and request no more be sent until further notice.
- Can be used like RR with P bit set to solicit the status of a secondary station
- Can be used like RR with F bit set to respond to a poll if the station is busy.

Reject (REJ)

- Bit value = 01 (0x08 to match above table type field bit order[4])
- Requests immediate retransmission starting with N(R).
- Sent in response to an observed sequence number gap. After seeing I1/I2/I3/I5, send REJ4.
- Optional to generate; a working implementation can use only RR.

Tulsiramji Gaikwad-Patil College of Engineering and Technology
Wardha Road, Nagpur-441 108
NAAC Accredited

Department of Computer Science & Engineering

Selective Reject (SREJ)

- Bit value = 11 (0x0c to match above table type field bit order)
- Requests retransmission of only the frame N(R).
- Not supported by all HDLC variants.
- Optional to generate; a working implementation can use only RR, or only RR and REJ.

U-Frames

Unnumbered frames, or **U-frames**, are used for link management, and can also be used to transfer user data. They exchange session management and control information between connected devices, and some U-frames contain an information field, used for system management information or user data. The first 2 bits (11) mean it is a U-frame. The 5 type bits (2 before P/F bit and 3 bit after P/F bit) can create 32 different types of U-frame

- Mode settings (SNRM, SNRME, SARM, SARME, SABM, SABME, UA, DM, RIM, SIM, RD, DISC)
- Information Transfer (UP, UI)
- Recovery (FRMR, RSET)
    - Invalid Control Field
    - Data Field Too Long
    - Data field not allowed with received Frame Type
    - Invalid Receive Count
- Miscellaneous (XID, TEST)

b] Explain the selective repeat ARQ protocol.

Selective Repeat Automatic Repeat Request (ARQ) Protocol

Go-Back-N ARQ simplifies the process at the receiver site. The receiver keeps track of only one variable, and there is no need to buffer out-of-order frames; they are simply discarded. However, this protocol is very inefficient for a noisy link.

In a noisy link a frame has a higher probability of damage, which means the resending of multiple frames. This resending uses up the bandwidth and slows down the transmission. For noisy links, there is another mechanism that does not resend N frames when just one frame is damaged; only the damaged frame is resent. This mechanism is called Selective Repeat ARQ. It is more efficient for noisy links, but the processing at the receiver is more complex.

The Selective Repeat Protocol also uses two windows: a send window and a receive window. However, there are differences between the windows in this protocol and the ones in Go-Back-N. First, the size of the send window is much smaller; it is $2^m - 1$.

The send window maximum size can be $2^m - 1$. The smaller window size means less efficiency in filling the pipe, but the fact that there are fewer duplicate frames can compensate for this.

The Selective Repeat Protocol allows as many frames as the size of the receive window to arrive out of order and be kept until there is a set of in-order frames to be delivered to the network layer. Because the sizes of the send window and receive window are the same, all the frames in the send frame can arrive out of order and be stored until they can be delivered. We need, however, to mention that the receiver never delivers packets out of order to the network layer.

The above figure shows the receive window in this protocol. Those slots inside the window that are colored define frames that have arrived out of order and are waiting for their neighbors to arrive before delivery to the network layer.

Design:

The design in this case is to some extent similar to the one we described for the Go Back-N, but more complicated, as shown in the following figure.

Tulsiramji Gaikwad-Patil College of Engineering and Technology
Wardha Road, Nagpur-441 108
NAAC Accredited

Department of Computer Science & Engineering

Window Sizes:

We can now show why the size of the sender and receiver windows must be at most one half of 2m. For an example, we choose m = 2, which means the size of the window is $2^m/2$, or 2. The following figure compares a window size of 2 with a window size of 3.

If the size of the window is 2 and all acknowledgments are lost, the timer for frame 0 expires and frame 0 is resent. However, the window of the receiver is now expecting frame 2, not frame 0, so this duplicate frame is correctly discarded.

When the size of the window is 3 and all acknowledgments are lost, the sender sends a duplicate of frame 0. However, this time, the window of the receiver expects to receive frame 0 (0 is part of the window), so it accepts frame 0, not as a duplicate, but as the first frame in the next cycle. This is clearly an error.

Q 5.a] Write a short note on following Multiple Access Protocols.
i) Pure ALOHA
ii) Slotted ALOHA

- **CSMA – CD**

ALOHA Class of Multiple Access Protocols

•

ALOHA

, also called pure ALOHA: Whenever a user has a frame to send, i
t simply transmits the
frame. If collision occurs, it waits for a random period of ti
me and re-sends it again
–
Sender can always find out if its frame was destroyed by listening to channel. For a LAN,
feedback is immediate, while for a satellite there is a long delay of 270 ms before sender knows–If listening while transmitting is not possible, ACKs are needed, e.g. in packet radio, collision from simultaneous transmissions of multiple transmittersis detected by base station, who sendsout ACK or NAK accordingly (via reverse channel)

•

Performance
:
throughput
S
(frames/s) which defines average number of frames successfully transmitted per unit time, and average delay
D
(s) experienced by a frame

•

Assuming average frame length τ f(s) and fixed channel rate, frame transmission can be modelled by Poisson distribution with mean arrival rate λ(frames/s)Normalised channel traffic or average number of old and new frames submitted per frame time
G=λτ f (unit in Erlang)
The throughput is then given by
S=G×Prob(no collision)

Slotted ALOHA

After the pure ALOHA in 1970, Roberts introduced an another method to improve the capacity of the Pure ALOHA which is called Slotted ALOHA. He proposed to divide the time into discrete intervals called time slots. Each time slot corresponds to the length of the frame. In contrast to the Pure ALOHA, Slotted ALOHA does not allow to transmit the data whenever the station has the data to be send. The Slotted ALOHA makes the station to wait till the next time slot begins and allow each data frame to be transmitted in the new time slot.

CSMA/CD

Tulsiramji Gaikwad-Patil College of Engineering and Technology
Wardha Road, Nagpur-441 108
NAAC Accredited

Department of Computer Science & Engineering

Short for **Carrier Sense Multiple Access/Collision Detection**, **CSMA/CD** is a Media Access Control (MAC) protocol. It defines how network devices respond when two devices attempt to use a data channel simultaneously and encounter a data collision. The CSMA/CD rules define how long the device should wait if a collision occurs. The medium is often used by multiple data nodes, so each data node receives transmissions from each of the other nodes on the medium.

There are several CSMA access modes: 1-persistent, P-persistent, and O-persistent. 1-persistent is used in CSMA/CD systems, like Ethernet. This mode waits for the medium to be idle, then transmits data. P-persistent is used in **CSMA/CA** systems, like Wi-Fi. This mode waits for the medium to be idle, then transmits data with a probability p. If the data node does not transmit the data (a probability of 1-p), the sender waits for the medium to be idle again and transmit the data with the same probability p. O-persistent is used by CobraNet, LonWorks, and the controller area network. This mode assigns a transmission order to each data node. When the medium becomes idle, the data node next in line can transmit data. The data node next in line waits for the medium to be idle again and then transmits its data. After each data node transmits data, the transmission order is updated to reflect what data nodes have already transmitted, moving each data node through the queue.

6. a) Write a short note on following controlled Access Protocols.

- **Token Ring**
- **Polling**

Controlled access:

In controlled access, the stations consult one another to find which station has the right to send. A station cannot send unless it has been authorized by other stations. The three popular controlled-access methods are as follows.

1. Token Passing:

In the token-passing method, the stations in a network are organized in a logical ring. In other words, for each station, there is a predecessor and a successor. The predecessor is the station which is logically before the station in the ring; the successor is the station which is after the station in the ring. The current station is the one that is accessing the channel now. The right to this access has been passed from the predecessor to the current station. The right will be passed to the successor when the current station has no more data to send.

In this method, a special packet called a token circulates through the ring. The possession of the token gives the station the right to access the channel and send its data. When a station has some data to send, it waits until it receives the token from its predecessor. It then holds the token and sends its data. When the station has no more data to send, it releases the token, passing it to the next logical station in the ring. The station cannot send data until it receives the token again in the next round.

Token management is needed for this access method. Stations must be limited in the time they can have possession of the token. The token must be monitored to ensure it has not been lost or destroyed. For example, if a station that is holding the token fails, the token will disappear from the network. Another function of token management is to assign priorities to the stations and to the types of data being transmitted. And finally, token management is needed to make low-priority stations release the token to high priority stations.

Logical Ring:

In a token-passing network, stations do not have to be physically connected in a ring; the ring can be a logical one. The following figure show four different physical topologies that can create a logical ring.

• In the physical ring topology, when a station sends the token to its successor, the token cannot be seen by other stations; the successor is the next one in line. This means that the token does not have to have the address of the next successor. The problem with this topology is that if one of the links-the medium between two adjacent stations fails, the whole system fails.

Tulsiramji Gaikwad-Patil College of Engineering and Technology
Wardha Road, Nagpur-441 108
NAAC Accredited

Department of Computer Science & Engineering

• The dual ring topology uses a second (auxiliary) ring which operates in the reverse direction compared with the main ring. The second ring is for emergencies only. If one of the links in the main ring fails, the system automatically combines the two rings to form a temporary ring. After the failed link is restored, the auxiliary ring becomes idle again.

2. Polling:

Polling works with topologies in which one device is designated as a primary station and the other devices are secondary stations. All data exchanges must be made through the primary device even when the ultimate destination is a secondary device.

Random access Protocols

Aloha Protocols

Carrier Sense Multiple Access Protocol

Carrier Sense Multiple Access with Collision Detection

The primary device controls the link; the secondary devices follow its instructions. It is up to the primary device to determine which device is allowed to use the channel at a given time. The primary device, therefore, is always the initiator of a session. Consider the following figure.

If the primary wants to receive data, it asks the secondaries if they have anything to send, this is called poll function. If the primary wants to send data, it tells the secondary to get ready to receive; this is called select function.

Select:

The select function is used whenever the primary device has something to send. If it has something to send, the primary device sends it. It has to know whether the target device is prepared to receive or not. So the primary must alert the secondary to the upcoming transmission and wait for an acknowledgment of the secondary's ready status. Before sending data, the primary creates and transmits a select (SEL) frame, one field of which includes the address of the intended secondary.

Poll:

The poll function is used by the primary device to solicit transmissions from the secondary devices. When the primary is ready to receive data, it must ask (poll) each device in turn if it has anything to send. When the first secondary is approached, it responds either with a NAK frame if it has nothing to send or with data (in the form of a data frame) if it does. If the response is negative (a NAK frame), then the primary polls the next secondary in the same manner until it finds one with data to send. When the response is positive (a data frame), the primary reads the frame and returns an acknowledgment (ACK frame), verifying its receipt.

b] Write down the difference between FDMA, TDMA, CDMA .

Frequency division multiple access (FDMA):

It is a technology by which the total bandwidth available to the system is divided into frequencies. This division is done between non overlapping frequencies that are then assigned to each communicating pair (2 phones)

FDMA is used mainly for analog transmission. Its not that this technology is not capable of carrying digital information, but just that it is not considered to be an efficient method for digital transmission. Because just imagine if the frequencies to handle the customers gets over? What if more capacity is required? The only option would be to drill down the existing frequencies to a much narrower amount which will not be very competent. In FDMA all users share the satellite simultaneously but each user transmits at single frequency.

Tulsiramji Gaikwad-Patil College of Engineering and Technology
Wardha Road, Nagpur-441 108
NAAC Accredited

Department of Computer Science & Engineering

To understand this technology better, just imagine how FM radio works. All the radios have their own frequency bands and they send their signals at the carefully allocated unique frequencies within the available bands.

Code division multiple access (CDMA):
Unlike FDMA, CDMA separates calls by code. Every bit of a conversation is been tagged with a specific and unique code. The system gets a call, it allocates a unique code to that particular conversation, now the data is split into small parts and is tagged with the unique code given to the conversation of which they are part of. Now, this data in small pieces is sent over a number of the discrete frequencies available for use at any time in the specified range. The system then at the end reassembles the conversation from the coded bits and deliver it☺ Does it make sense?
Just think about how you recollect your luggage at the end of the flight journey. When you check in, a tag with a code is given to you which is also given to your luggage☺ And at the destination, you collects your luggage on the basis of that☺ I know you will say that you recognize your bag, but then I have a habit of always matching the codes of my bag and the one on the tag given to me and that is how I become sure of not picking up the wrong luggage☺

Time division multiple access (TDMA):
Unlike FDMA and CDMA, In TDMA the division of calls happens on time basis. The system first digitizes the calls, and then combines those conversations into a unified digital stream on a single radio channel. Now it divides each cellular channel into three time slots that means three calls get put on a single frequency and then, a time slot is assigned to each call during the conversation, a regular space in a digital stream. The users transmit in rapid succession, one after the other, each using its own time slot. This allows multiple stations to share the same transmission medium (e.g. radio frequency channel) while using only a part of its channel capacity.
This technology enables three different users to use one frequency at the same time.
Here there is no need for three separate frequencies like in FDMA. As in FDMA, instead of monopolizing a single radio channel for a single call, TDMA efficiently carries three calls at the same time☺
BTW, this technology is the one used in our GSM system

Q7.a) Explain the significance of optimal Routing Number in Hierarchical Routing .

Hierarchical routing is the procedure of arranging routers in a hierarchical manner. A good example would be to consider a corporate [internet]. Most corporate intranets consist of a high speed backbone network. Connected to this backbone are routers which are in turn connected to a particular workgroup. These workgroups occupy a unique LAN. The reason this is a good arrangement is because even though there might be dozens of different workgroups, the span (maximum hop count to get from one host to any other host on the network) is 2. Even if the workgroups divided their LAN network into smaller partitions, the span could only increase to 4 in this particular example.

Considering alternative solutions with every router connected to every other router, or if every router was connected to 2 routers, shows the convenience of hierarchical routing. It decreases the complexity of network topology, increases routing efficiency, and causes much less congestion because of fewer routing advertisements. With hierarchical routing, only core routers connected to the backbone are aware of all routes. Routers that lie within a LAN only know about routes in the LAN. Unrecognized destinations are passed to the default route.

Hierarchical routing was mainly devised, among other things, to reduce memory requirements of simulations over very large topologies. A topology is broken down into several layers of hierarchy, thus downsizing the routing table. The table size is reduced from , for flat routing, to about log n

for hierarchical routing. However some overhead costs results as number of hierarchy levels are increased. Optimum results were found for 3 levels of hierarchy and the current ns implementation supports upto a maximum of 3 levels of hierarchical routing.

To be able to use hierarchical routing for the simulations, we need to define the hierarchy of the topology as well as provide the nodes with hierarchical addressing. In flat routing, every node knows about every other node in the topology, thus resulting in routing table size to the order of . For hierarchical routing, each node knows only about those nodes in its level. For all other destinations outside its level it forwards the packets to the border router of its level. Thus the routing table size gets downsized to the order of about log n

Hierarchical routing requires some additional features and mechanisms for the simualtion. For example, a new node object called HierNode is been defined for hier rtg. Therefore the user must specify hierarchical routing requirements before creating topology. This is done as shown below:

First, the address format ( ) or the address space used for node and port address, needs to be set in the hierarchical mode. It may be done in one of the two ways:

```
set ns [new Simulator]
\$ns set-address-format hierarchical
```

This sets the node address space to a 3 level hierarchy assigning 8 bits in each level.

b) What is the cause for count to infinity problems in distance vector routing algorithm.

Distance vector routing:

- Distance Vector Routing is one of the dynamic routing algorithm.
- It is suitable for packet switched network.
- In distance vector routing, each router maintains a routing table.
- It contains one entry for each router in the subnet.
- This entry has two parts:

  a. The first part shows the preferred outgoing line to be used to reach the destination.

  b. Second part gives an estimate of the time or distance to the destination.

- In distance vector routing, a node tells its neighbor about its distance to every other node in the network.

Count to infinity problem:

- One of the important issue in Distance Vector Routing is County of Infinity Problem.
- Counting to infinity is just another name for a routing loop.
- In distance vector routing, routing loops usually occur when an interface goes down.
- It can also occur when two routers send updates to each other at the same time.

Example:

Ø Imagine a network with a graph as shown above in figure 4.8.

Ø As you see in this graph, there is only one link between A and the other parts of the network.

Ø Now imagine that the link between A and B is cut.

Ø At this time, B corrects its table.

Ø After a specific amount of time, routers exchange their tables, and so B receives C's routing table.

Ø Since C doesn't know what has happened to the link between A and B, it says that it has a link to A with the weight of 2 (1 for C to B, and 1 for B to A -- it doesn't know B has no link to A).

Tulsiramji Gaikwad-Patil College of Engineering and Technology
Wardha Road, Nagpur-441 108
NAAC Accredited

Department of Computer Science & Engineering

Ø B receives this table and thinks there is a separate link between C and A, so it corrects its table and changes infinity to 3 (1 for B to C, and 2 for C to A, as C said).

Ø Once again, routers exchange their tables.

Ø When C receives B's routing table, it sees that B has changed the weight of its link to A from 1 to 3, so C updates its table and changes the weight of the link to A to 4 (1 for C to B, and 3 for B to A, as B said).

Ø This process loops until all nodes find out that the weight of link to A is infinity.

Ø This situation is shown in the table below 4.2.

Ø In this way, Distance Vector Algorithms have a slow convergence rate.

Ø One way to solve this problem is for routers to send information only to the neighbors that are not exclusive links to the destination.

Ø For example, in this case, C shouldn't send any information to B about A, because B is the only way to A.

Disadvantage

a) The primary drawback of this algorithm is its vulnerability to the 'Count-to-Infinity' problem. Many partial solutions have been proposed but none works under all circumstances.

b) Another drawback of this scheme is that it does not take into account link bandwidth.

c.Yet another problem with this algorithm is that it takes longer time for convergence as network size grows.

C] Explain shortest path algorithm for routing

Shortest path algorithm finds the shortest paths between routers/node in a graph. The widely used shortest path algorithm is Dijkstra's shortest path algorithm. It can also be used for finding the shortest paths from a single node to a single destination node by stopping the algorithm once the shortest path to the destination node has been determined.

Definitions:

- **G(V, E)**: weighted directed graph, with set of vertices **V** and set of directed edges **E**,
- **w(u, v)**: cost of directed edge from node **u** to node **v** (costs are non-negative).

Links that do not satisfy constraints on the shortest path are removed from the graph

- **s**: the source node
- **t**: the destination node
- ***k***: the number of shortest paths to find
- $\mathbf{P_u}$: a path from **s** to **u**
- **B** is a heap data structure containing paths
- **P**: set of shortest paths from **s** to **t**
- $\mathbf{count_u}$: number of shortest paths found to node **u**

Algorithm:

P =empty, $\mathbf{count_u}$ = 0, for all u in V
insert path $\mathbf{P_s}$ = {s} into **B** with cost **0**
while **B** is not empty and $\mathbf{count_u}$ < **K**:
– let $\mathbf{P_u}$ be the shortest cost path in **B** with cost **C**
– **B** = **B** − $\{\mathbf{P_u}\}$, $\mathbf{count_u}$ = $\mathbf{count_u}$ + 1
– if **u** = **t** then **P** = **P** ∪ $\mathbf{P_u}$
– if $\mathbf{count_u} \leq \mathbf{K}$ then

- for each vertex **v** adjacent to **u**:

Tulsiramji Gaikwad-Patil College of Engineering and Technology
Wardha Road, Nagpur-441 108
NAAC Accredited

Department of Computer Science & Engineering

– if **v** is not in P_u then
– let P_v be a new path with cost **C** + **w(u, v)** formed by concatenating edge **(u, v)** to path P_u
– insert P_v into **B**

return **P**

8. Explain following Routing protocols.

i) Flooding

- **Distance Vector Routing**
- **Link Stat Routing**

1.Flooding

There are generally two types of flooding available, uncontrolled flooding and controlled flooding.

Uncontrolled flooding is the fatal law of flooding. All nodes have neighbors and route packets indefinitely. More than two neighbours creates a broadcast storm.

Controlled flooding has its own two algorithms to make it reliable, SNCF (Sequence Number Controlled Flooding) and RPF (Reverse Path Forwarding). In SNCF, the node attaches its own address and sequence number to the packet, since every node has a memory of addresses and sequence numbers. If it receives a packet in memory, it drops it immediately while in RPF, the node will only send the packet forward. If it is received from the next node, it sends it back to the sender.

Algorithms

There are several variants of flooding algorithms. Most work roughly as follows:

- Each node acts as both a transmitter and a receiver.
- Each node tries to forward every message to every one of its neighbors except the source node.

This results in every message eventually being delivered to all reachable parts of the network.

Algorithms may need to be more complex than this, since, in some case, precautions have to be taken to avoid wasted duplicate deliveries and infinite loops, and to allow messages to eventually expire from the system.

Selective flooding

A variant of flooding called **selective flooding** partially addresses these issues by only sending packets to routers in the same direction. In selective flooding the routers don't send every incoming packet on every line but only on those lines which are going approximately in the right direction.

Advantages

- If a packet can be delivered, it will (probably multiple times).
- Since flooding naturally utilizes every path through the network, it will also use the shortest path.
- This algorithm is very simple to implement.[*citation needed*]

- **Disadvantages**

- Flooding can be costly in terms of wasted bandwidth. While a message may only have one destination it has to be sent to every host. In the case of a ping flood or a denial of service attack, it can be harmful to the reliability of a computer network.
- Messages can become duplicated in the network further increasing the load on the networks bandwidth as well as requiring an increase in processing complexity to disregard duplicate messages.
- Duplicate packets may circulate forever, unless certain precautions are taken:
    - Use a hop count or a time to live (TTL) count and include it with each packet. This value should take into account the number of nodes that a packet may have to pass through on the way to its destination.
    - Have each node keep track of every packet seen and only forward each packet once.
    - Enforce a network topology without loops.

Tulsiramji Gaikwad-Patil College of Engineering and Technology
Wardha Road, Nagpur-441 108
NAAC Accredited

Department of Computer Science & Engineering

Distance Vector Routing Protocols

Distance Vector routing protocols base their decisions on the best path to a given destination based on the distance. Distance is usually measured in hops, though the distance metric could be delay, packets lost, or something similar. If the distance metric is hop, then each time a packet goes through a router, a hop is considered to have traversed. The route with the least number of hops to a given network is concluded to be the best route towards that network.

The vector shows the direction to that specific network. Distance vector protocols send their entire routing table to directly connected neighbors. Examples of distance vector protocols include **RIP - Routing Information Protocol** and **IGRP - Interior Gateway Routing Protocol**.

If you're interested in finding out more information on RIP, check out my articles on how to configure Routing Information Protocol RIPv1 and RIPv2.

Link State Routing Protocols

Link state protocols are also called shortest-path-first protocols. Link state routing protocols have a complete picture of the network topology. Hence they know more about the whole network than any distance vector protocol.

Three separate tables are created on each link state routing enabled router. One table is used to hold details about directly connected neighbors, one is used to hold the topology of the entire internetwork and the last one is used to hold the actual routing table.

Link state protocols send information about directly connected links to all the routers in the network. Examples of Link state routing protocols include **OSPF - Open Shortest Path First** and **IS-IS - Intermediate System to Intermediate System.**

There are also routing protocols that are considered to be hybrid in the sense that they use aspects of both distance vector and link state protocols. **EIGRP - Enhanced Interior Gateway Routing Protocol** is one of those hybrid routing protocols.

9.Explain following congestion control algorithms.

i) Choke packets

- **Leaky Bucket**
- **Token Bucket**

Open loop: try to prevent congestion occurring by good design

- Closed-loop: monitor the system to detect congestion, pass this information to where action can be taken, and adjust system operation to correct the problem (detect,feedback and correct).

Leaky Bucket

- Imagine a bucket with a small hole in the bottom.
- No matter the rate at which water enters the bucket, the outflow is at a constant rate, when there is any water in the bucket and zero when the bucket is empty.
- Also, once the bucket is full, any additional water entering it spills over the sides and is lost.
- The same idea can be applied to packets, as shown in Fig. (b).
- Conceptually, each host is connected to the network by an interface containing a leaky bucket, that is, a finite internal queue.
- If a packet arrives at the queue when it is full, the packet is discarded. In other words, if one or more processes within the host try to send a packet when the maximum number is already queued, the new packet is unceremoniously discarded.

The Token Bucket Algorithm

- For many applications, it is better to allow the output to speed up somewhat when large bursts arrive, so a more flexible algorithm is needed, preferably one that never loses data.
- One such algorithm is the token bucket algorithm.
- Tokens arrive at the constant rate in the token bucket.
- If the bucket is full, tokens are discarded.

- A packet from the buffer can be taken out only if a token in the token bucket can be drawn.
- The token bucket algorithm provides a different kind of traffic shaping than that of the leaky bucket algorithm. The leaky bucket algorithm does not allow idle hosts to save up permission to send large bursts later.
- The token bucket algorithm does allow saving, up to the maximum size of the bucket, n. This property means that bursts of up to n packets can be sent at once, allowing some burstiness in the output stream and giving the faster response to sudden bursts of input.

Q 10]

a]Explain IPV4 and IPV6 header formats.

There are a number of unfamiliar fields within the IPv6 header but each of them replicates some of the functionality of the IPv4 header fields. Table 1 takes a look at each of these fields and what they are used for:

Version

The version field is 4 bits long and contains the IP version to be expected in the following contents; since this article is talking about IPv6, this value is always going to be 6 (0110).

Traffic Class

The traffic class field is 8 bits long and operates the same as the IPv4 Type of Service field; this includes support for the marking of traffic based on a differentiated services code point (DSCP).

Flow Label

The flow label field is 20 bits long and is new to IPv6 and enables the ability to track specific traffic flows at the network layer.

Payload Length

The payload length field is 16 bits long and operates the same as the IPv4 length field; this field includes the length of the data portion of the IPv6 packet.

Next Header

The next header field is 8 bits long and operates similarly to the IPv4 protocol field. The next header field indicates what to expect after the basic IPv6 header; this includes options like a TCP or UDP header and packet.

Hop Limit

The hop limit field is 8 bits long and operates similarly to the IPv4 Time to Live field. This field is used to specify the maximum number of routers that the packet is allowed to travel through before being discarded.

Source Address

The source address field is 128 bits long and operates the same as the IPv4 source address field, with the exception of the length differences.

Destination Address

The destination address field is 128 bits long and operates the same as the IPv4 destination address field, with the exception of the length differences.

b) Explain ARP and RARP protocols

ARP --Address Resolution Protocol

What is it for: Arp translates IP numbers into hardware addresses.

How ARP works: Send a packet from the querrying host with an Ethernet broadcast address asking the target host with the given IP address to respond. All hosts on the physical network receive this packet, and the one with the given IP number responds. Then the original querring host knows the physical address of the target host. Does not use IP; uses's physical frames.

Common ARP improvements: Keep a cache of recently received translations. Remember that these addresses are quite small, and the space needed to store them is also small. Store both the physical and IP addresses of all ARP broadcasting

hosts. Then every host who receives a broadcast ARP request can know the address translation of the sender. This is especially imporant for the receiver of the broadcast.

How to Write ARP Software: There are two parts. The first part uses the cache to map IP -> physical addresses. The second part fills the cache with mapping upon request from the first part.

Security: Can you fool ARP software. Yes, by poluting the network with your own answers.

Interesting question: To send machine A some data, you broadcast seeking machine A. Would it not be easier just to broadcast the data. That would for sure reduce the total number of packets sent, at the cost of changing many unicasts to broadcasts. What if someone answers an ARP request for you, and lies about who they are? Who answers an ARP for a machine

RARP -- Reverse Address Resolution Protocol

What is it for: Diskless clients don't have a place to store there IP number. Rarp translates machines addresses into IP numbers.

How RARP works: The client broadcasts a RARP packet with an ethernet broadcast address, and it's own physical address in the data portion. The server responds by telling the client it's IP address. Note there is no name sent. Also note there is no security. Does not use IP; uses's physical frames.

Common RARP improvements: Don't let an RARP client retry indefinitlly. That just causes wasted broadcasts. Have a backup RARP server or two, on random time delays.

11. a) Why does UDP exists? Explain UDP segment format.

The User Datagram Protocol (UDP)

The User Datagram Protocol (UDP) is a transport layer protocol defined for use with the IP network layer protocol. It is defined by RFC 768 written by John Postel. It provides a best-effort datagram service to an End System (IP host).

The service provided by UDP is an unreliable service that provides no guarantees for delivery and no protection from duplication (e.g. if this arises due to software errors within an Intermediate System (IS)). The simplicity of UDP reduces the overhead from using the protocol and the services may be adequate in many cases.

UDP provides a minimal, unreliable, best-effort, message-passing transport to applications and upper-layer protocols. Compared to other transport protocols, UDP and its UDP-Lite variant are unique in that they do not establish end-to-end connections between communicating end systems. UDP communication consequently does not incur connection establishment and teardown overheads and there is minimal associated end system state. Because of these characteristics, UDP can offer a very efficient communication transport to some applications, but has no inherent congestion control or reliability. A second unique characteristic of UDP is that it provides no inherent On many platforms, applications can send UDP datagrams at the line rate of the link interface, which is often much greater than the available path capacity, and doing so would contribute to congestion along the path, applications therefore need to be designed responsibly

One increasingly popular use of UDP is as a tunneling protocol, where a tunnel endpoint encapsulates the packets of another protocol inside UDP datagrams and transmits them to another tunnel endpoint, which decapsulates the UDP datagrams and forwards the original packets contained in the payload. Tunnels establish virtual links that appear to directly connect locations that are distant in the physical Internet topology, and can be used to create virtual (private) networks. Using UDP as a tunneling protocol is attractive when the payload protocol is not supported by middleboxes that may exist along the path, because many middleboxes support UDP transmissions.

UDP does not provide any communications security. Applications that need to protect their communications against eavesdropping, tampering, or message forgery therefore need to separately provide security services using additional protocol mechanisms.

Protocol Header

A computer may send UDP packets without first establishing a connection to the recipient. A UDP datagram is carried in a single IP packet and is hence limited to a maximum payload of 65,507 bytes for IPv4 and 65,527 bytes for IPv6. The transmission of large IP packets usually requires IP fragmentation. Fragmentation decreases communication reliability and efficiency and should therefore be avoided.

Tulsiramji Gaikwad-Patil College of Engineering and Technology
Wardha Road, Nagpur-441 108
NAAC Accredited

Department of Computer Science & Engineering

To transmit a UDP datagram, a computer completes the appropriate fields in the UDP header (PCI) and forwards the data together with the header for transmission by the IP network layer.

The UDP protocol header consists of 8 bytes of Protocol Control Information (PCI)

The UDP header consists of four fields each of 2 bytes in length:

Source Port (UDP packets from a client use this as a service access point (SAP) to indicate the session on the local client that originated the packet. UDP packets from a server carry the server SAP in this field)

Destination Port (UDP packets from a client use this as a service access point (SAP) to indicate the service required from the remote server. UDP packets from a server carry the client SAP in this field)

UDP length (The number of bytes comprising the combined UDP header information and payload data)

UDP Checksum (A checksum to verify that the end to end data has not been corrupted by routers or bridges in the network or by the processing in an end system. The algorithm to compute the checksum is the Standard Internet Checksum algorithm. This allows the receiver to verify that it was the intended destination of the packet, because it covers the IP addresses, port numbers and protocol number, and it verifies that the packet is not truncated or padded, because it covers the size field. Therefore, this protects an application against receiving corrupted payload data in place of, or in addition to, the data that was sent. In the cases where this check is not required, the value of 0x0000 is placed in this field, in which case the data is not checked by the receiver.

Like for other transport protocols, the UDP header and data are not processed by Intermediate Systems (IS) in the network, and are delivered to the final destination in the same form as originally transmitted.

At the final destination, the UDP protocol layer receives packets from the IP network layer. These are checked using the checksum (when >0, this checks correct end-to-end operation of the network service) and all invalid PDUs are discarded. UDP does not make any provision for error reporting if the packets are not delivered. Valid data are passed to the appropriate session layer protocol identified by the source and destination port numbers (i.e. the session service access points).

UDP and UDP-Lite also may be used for multicast and broadcast, allowing senders to transmit to multiple receivers.

b) Why does maximum packet lifetime, T, have to large enough to ensure that not only the

packet but also its acknowledgements have vanished.

c) How the crash recovery is handled by transport layer. What are the difficulties in crash

recovery process.

The transport layer

As the transport layer is built on top of the network layer, it is important to know the key features of the network layer service. There are two types of network layer services : connectionless and connection-oriented. The connectionless network layer service is the most widespread. Its main characteristics are :

the connectionless network layer service can only transfer SDUs of limited size [1]

the connectionless network layer service may discard SDUs

the connectionless network layer service may corrupt SDUs

the connectionless network layer service may delay, reorder or even duplicate SDUs

The transport layer in the reference model

These imperfections of the connectionless network layer service will become much clearer once we have explained the network layer in the next chapter. At this point, let us simply assume that these imperfections occur without trying to understand why they occur.

Some transport protocols can be used on top of a connection-oriented network service, such as class 0 of the ISO Transport Protocol (TP0) defined in [X224] , but they have not been widely used. We do not discuss in further detail such utilisation of a connection-oriented network service in this book.

Tulsiramji Gaikwad-Patil College of Engineering and Technology
Wardha Road, Nagpur-441 108
NAAC Accredited

Department of Computer Science & Engineering

This chapter is organised as follows. We will first explain how it is possible to provide a reliable transport service on top of an unreliable connectionless network service. For this, we explain the main mechanisms found in such protocols. Then, we will study in detail the two transport protocols that are the most commonly used in the Internet. We begin with the User Datagram Protocol (UDP) which provides a simple connectionless transport service. Then, we will describe in detail the Transmission Control Protocol (TCP), including its congestion control mechanism.

Crash recovery

Transactions (or units of work) against a database can be interrupted unexpectedly. If a failure occurs before all of the changes that are part of the unit of work are completed, committed, and written to disk, the database is left in an inconsistent and unusable state. Crash recovery is the process by which the database is moved back to a consistent and usable state. This is done by rolling back incomplete transactions and completing committed transactions that were still in memory when the crash occurred .

1. Rolling back units of work (crash recovery)

If the database or the database manager fails, the database can be left in an inconsistent state. The contents of the database might include changes made by transactions that were incomplete at the time of failure. The database might also be missing changes that were made by transactions that completed before the failure but which were not yet flushed to disk. A crash recovery operation must be performed in order to roll back the partially completed transactions and to write to disk the changes of completed transactions that were previously made only in memory.

12. a) Explain the task perform by transport layer with respect to following.

i) Addressing

ii) Connection Establishment

iii) Connection Release

Transport layer:

In the Open Systems Interconnection (OSI) communications model, the Transport layer ensures the reliable arrival of messages and provides error checking mechanisms and data flow controls. The Transport layer provides services for both "connection-mode" transmissions and for "connectionless-mode" transmissions. For connection-mode transmissions, a transmission may be sent or arrive in the form of packets that need to be reconstructed into a complete message at the other end.

The transport level provides end-to-end communication between processes executing on different machines. Although the services provided by a transport protocol are similar to those provided by a data link layer protocol, there are several important differences between the transport and lower layers:

Addressing becomes a significant issue. That is, now the user must deal with it; before it was buried in lower levels. How does a user open a connection to ``the mail server process on wpi"?

Two solutions:

Use well known addresses that rarely if ever change, allowing programs to ``wire in" addresses. For what types of service does this work? While this works for services that are well established (e.g., mail, or telnet), it doesn't allow a user to easily experiment with new services.

Use a name server. Servers register services with the name server, which clients contact to find the transport address of a given service.

In both cases, we need a mechanism for mapping high-level service names into low-level encodings that can be used within packet headers of the network protocols. In its general form, the problem is quite complex.

One simplification is to break the problem into two parts: have transport addresses be a combination of machine address and local process on that machine.

Storage capacity of the subnet. Assumptions valid at the data link layer do not necessarily hold at the transport Layer. Specifically, the subnet may buffer messages for a potentially long time, and an ``old" packet may arrive at a destination at unexpected times.

Tulsiramji Gaikwad-Patil College of Engineering and Technology
Wardha Road, Nagpur-441 108
NAAC Accredited

Department of Computer Science & Engineering

We need a dynamic flow control mechanism. The data link layer solution of preallocating buffers is inappropriate because a machine may have hundreds of connections sharing a single physical link. In addition, appropriate settings for the flow control parameters depend on the communicating end points (e.g., Cray supercomputers vs. PCs), not on the protocol used.

Don't send data unless there is room. Also, the network layer/data link layer solution of simply not acknowledging frames for which the receiver has no space is unacceptable. Why? In the data link case, the line is not being used for anything else; thus retransmissions are inexpensive. At the transport level, end-to-end retransmissions are needed, which wastes resources by sending the same packet over the same links multiple times. If the receiver has no buffer space, the sender should be prevented from sending data.

Deal with congestion control. In connectionless internets, transport protocols must exercise congestion control. When the network becomes congested, they must reduce rate at which they insert packets into the subnet, because the subnet has no way to prevent itself from becoming overloaded.

Connection establishment.

Transport level protocols go through three phases: establishing, using, and terminating a connection.

For datagram-oriented protocols, opening a connection simply allocates and initializes data structures in the operating system kernel.

Connection oriented protocols often exchanges messages that negotiate options with the remote peer at the time a connection is opened. Establishing a connection may be tricky because of the possibility of old or duplicate packets.

Finally, although not as difficult as establishing a connection, terminating a connection presents subtleties too. For instance, both ends of the connection must be sure that all the data in their queues have been delivered to the remote application.

b) Explain the fields in TCP header in detail.

A TCP segment consists of a TCP header, TCP options and the data that the segment transports. Following table represents a TCP header and it's fields. The fields of TCP header are source port and destination port of a application, 32 bit sequence number, 32 bit acknowledgement number, TCP header length, 6 reserved bits, 6 flags (URG, ACK, PSH, RST, SYS, FIN), 16 bit window size, 16 bit TCP checksum, 16 bit urgent pointer, Options if any and padding if needed. Minimum header length is 20 bytes long i.e 5 32 bit words. The TCP maximum header size can be up to 15, 32 bit words. i.e. 60 byte long.

bits	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31												
0	16-bit source port			16-bit destination port									
32	32-bit sequence number												
64	32-bit acknowledgement number												
96	Header Length 4-bits			Reserved 6-bits		URG	ACK	PSH	RST	SYN	FIN	16-bit	window size
128	16-bit TCP checksum			16-bit urgent pointer									
160	Options Padding												

Source and Destination Ports:

Both source and destination ports are 16-bit fields identify protocol ports of the sending and receiving applications. The source and destination port numbers plus source and destination IP addresses in the IP header combine to uniquely identify each TCP connection referred as a socket.

Sequence Number:

Sequence number is a 32-bit wide field identifies the first byte of data in the data area of the TCP segment. We can identify every byte in a data stream by a sequence number.

Tulsiramji Gaikwad-Patil College of Engineering and Technology
Wardha Road, Nagpur-441 108
NAAC Accredited

Department of Computer Science & Engineering

Acknowledgement Number:

Acknowledge number is also a 32-bit wide field which identifies the next byte of data that the connection expects to receive from the data stream.

Header Length:

Header length is a field which consists of 4 bit to specifies the length of the TCP header in 32-bit words. Receiving TCP module can calculate the start of the data area by examining the header length field.

Flags:

URG – URG flag tells the receiving TCP module as it is urgent data

ACK – ACK tells the receiving TCP module that the acknowledge number field contains a valid acknowledgement number

PSH – PSH flag tells the receiving TCP module to immediately send data to the destination application

RST – RST flag asks the receiving TCP module to reset the TCP connection

SYN – SYN flag tells the receiving TCP module to synchronize sequence number

FIN – FIN flag tells the receiving TCP module that the sender has finished sending data

Window size field is a 16-bit wide which tells the receiving TCP module the number of bytes that the sending end id willing to accept. The value in this field specifies the width of the sliding window.

Checksum:

TCP checksum is a 16-bit wide filed includes the TCP data in it's calculations. This field helps the receiving TCP module to detect data corruption. That is, TCP requires the sending TCP module to calculate and include checksums in this field and receiving TCP module to verify checksums when they receive data. The data corruption is detected in this way..

c) Write a short note on Domain Name System.

The domain name system (DNS) is the way that internet domain names are located and translated into internet protocol (IP) addresses. The domain name system maps the name people use to locate a website to the IP address that a computer uses to locate a website. For example, if someone types TechTarget.com into a web browser, a server behind the scenes will map that name to the IP address 206.19.49.149.

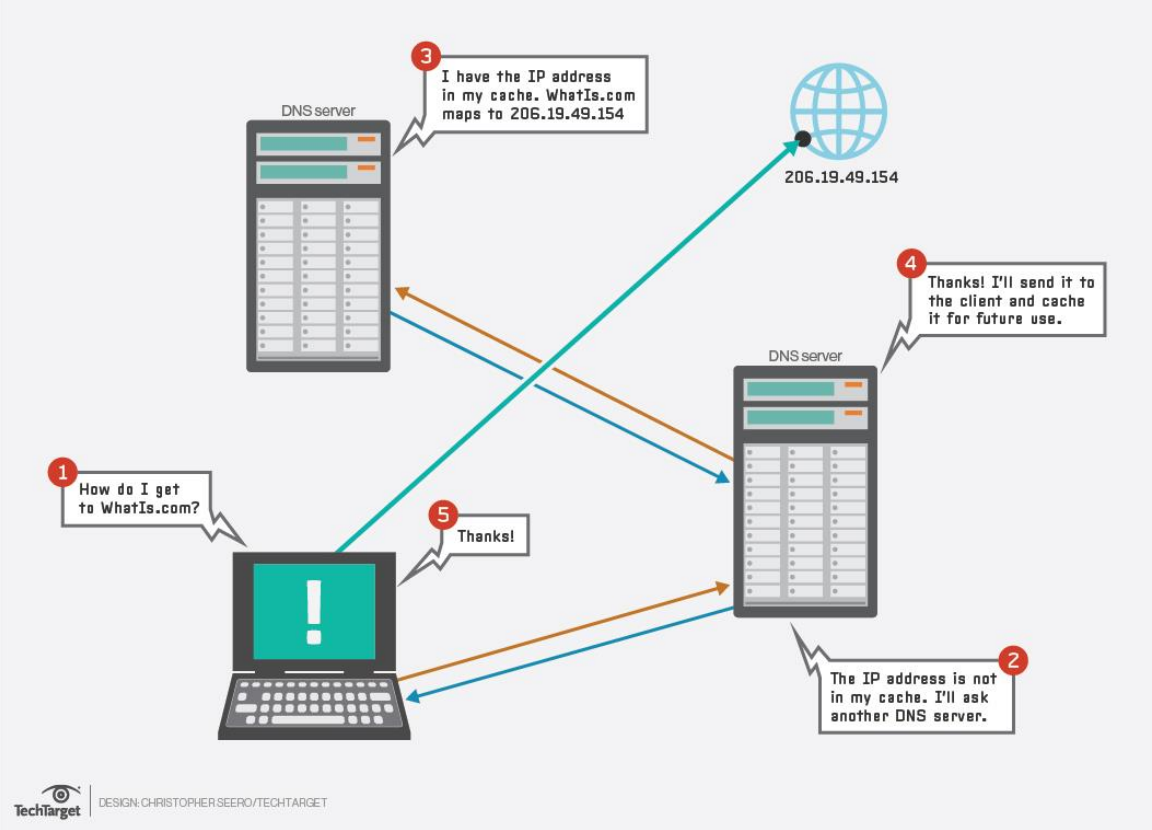
Web browsing and most other internet activity rely on DNS to quickly provide the information necessary to connect users to remote hosts. DNS mapping is distributed throughout the internet in a hierarchy of authority. Access providers and enterprises, as well as governments, universities and other organizations, typically have their own assigned ranges of IP addresses and an assigned domain name; they also typically run DNS servers to manage the mapping of those names to those addresses. Most URLs are built around the domain name of the web server that takes client requests. For example, the URL for this page is

How does DNS work?

DNS servers answer questions from both inside and outside their own domains. When a server receives a request from outside the domain for information about a name or address inside the domain, it provides the authoritative answer. When a server receives a request from inside its own domain for information about a name or address outside that domain, it passes the request out to another server -- usually one managed by its internet service provider. If that server does not know the answer or the authoritative source for the answer, it will reach out to the DNS servers for the top-level domain -- e.g., for all of .com or .edu. Then, it will pass the request down to the authoritative server for the specific domain -- e.g., techtarget.com or stkate.edu; the answer flows back along the same path.

Tulsiramji Gaikwad-Patil College of Engineering and Technology
Wardha Road, Nagpur-441 108
NAAC Accredited

Department of Computer Science & Engineering



Tulsiramji Gaikwad-Patil College of Engineering and Technology
Wardha Road, Nagpur-441 108
NAAC Accredited

Department of Computer Science & Engineering