FIRST TERM EXAMINATION [FEB.–2016]
SIXTH SEMESTER [B. TECH]
COMPUTER NETWORKS [ETCS–306]

Time: 1.30 Hrs. **Max Marks: 30**

Note: *Attempt Q. no. 1 and any two more questions.*

Q.1. (a) What are the two broad classifications under which Networks can be divided? **(2)**

Ans. All computer networks fit in one of the two dimensions namely:

(*a*) Transmission Technology, this focuses on the basic underlying physical network, for e.g. whether the nodes share a communication media or each pair of node has a separate dedicated link. There are various topologies like mesh topology, ring topology, star topology and bus topology etc.

(*b*) Scale, it focuses on the scale of network how large is your network.

Q.1. (*b*) Explain the signficance of protocols in communication? **(2)**

Ans. Protocols are **rules and procedures for communicating**. When several computers are networked, the rules and technical procedures governing their communication and interaction are called protocols.

Protocols should specify rules governing the transmission. The protocol steps must be carried out in a consistent order that is the same on every computer in the network. In general, much of the following should be addressed:

1. Data formats for data exchange. Digital message bitstrings are exchanged. Address formats for data exchange. Addresses are used to identify both the sender and the intended receiver(s).

2. Address mapping: Sometimes protocols need to map addresses of one scheme on addresses of another scheme.

3. Routing: When systems are not directly connected, intermediary systems along the *route* to the intended receiver(s) need to forward messages on behalf of the sender.

4. Detection of transmission errors: Is necessary on networks which cannot guarantee error-free operation.

5. Acknowledgements: Of correct reception of packets is required for connection-oriented communication.

6. Loss of information-timeouts and retries: Packets may be lost on the network or suffer from long delays.

7. Flow control is needed when the sender transmits faster than the receiver or intermediate network equipment can process the transmissions.

Q. 1. (*c*) Differentiate between UTP and STP cable.

Ans: Difference between STP and UTP.

Shielded Twisted pair	Un-shielded Twisted pair
1. STP has a metal foil covering.	1. UTP does not have a metal foil covering.
2. STP gives better resistance to electromagnetic interference as compared to UTP.	2. UTP does not provide better resistance to electromagnetic interference as compared to STP.
3. STP is little expensive the UTP.	3. UTP is less expensive than STP.
4. Grounding is possible.	4. Grounding is not possible
5. Possibility of cross talk is less as it resist to EMI.	5. Possibility of cross talk is more as it provide less resistance to EMI.
6. Distance travelled is large and can be used is MAN.	6. Distance travelled is less and used in LAN.

dotnotes.xyz

Q. 1. (*d*) Explain the principle of ISDN?

Ans. ISDN, which stands for Integrated Services Digital Network, is a system of digital phone connections which has been available for over a decade. This system allows voice and data to be transmitted simultaneously across the world using end-to-end digital connectivity. There are two basic types of ISDN service: **Basic Rate Interface (BRI)** and **Primary Rate Interface (PRI)**. BRI consists of two 64 kb/s B channels and one 16 kb/s D channel for a total of 144 kb/s. This basic service is intended to meet the needs of most individual users.

PRI is intended for users with greater capacity requirements. Typically the channel structure is 23 B channels plus one 64 kb/s D channel for a total of 1536 kb/s.

Some advantages of ISDN

Speed: ISDN allows multiple digital channels to be operated simultaneously through the same regular phone wiring used for analog lines. The change comes about when the telephone company's switches can support digital connections.

Multiple Devices: ISDN allows multiple devices to share a single line. It is possible to combine many different digital data sources and have the information routed to the proper destination. Since the line is digital, it is easier to keep the noise and interference out while combining these signals.

Signaling: Instead of the phone company sending a ring voltage signal to ring the bell in your phone ("In-Band signal"), it sends a digital packet on a separate channel ("Out-of-Band signal").

Q. 1. (*e*) What is bit stuffing? Why is it used?

Ans. Bit Stuffing: The practice of adding bits to a stream of data. Bit stuffing is required by many network and communications protocols for the following reasons:

- To prevent *data* being interpreted as *control* information. For example, many frame-based protocols, such as X.25, signal the beginning and end of a frame with six consecutive 1 bits. Therefore, if the actual data being transmitted has six 1 bits in a row, a zero is inserted after the first 5 so that the dat is not interpreted as a frame delimiter. Of course, on the receiving end, the stuffed bits must be discarded.
- For protocols that require a fixed-size frame, bits are sometimes inserted to make the frame size equal to this set size.
- For protocols that required a continuous stream of data, zero bits are sometimes inserted to ensure that the stream is not broken.

In a example of bit stuffing, a standard HDLC packet begins and ends with 01111110. To make sure this sequence doesn't appear again before the end of the packet a 0 is inserted after every five consecutive 1s.

Q. 2. (*a*) Describe the goals of multiplexing. Differentiate between synchronous and statistical TDM.

Ans. Networks use multiplexing for two reasons:

- To make it possible for any network device to talk to any other network device without having to dedicate a connection for each pair. This requires shared media.
- To make a scarce or expensive resource stretch further —*e.g.*, to send many signals down each cable or fiber strand running between major metropolitan areas, across one satellite uplink.

Difference Between Synchronous TDM and Statistical TDM

Parameter	Synchronous TDM	Statistical TDM
Working	In Synchronous TDM data flow of each input connection is divided into units and each input occupies one output time slot.	In Statistical TDM slots are allotted dynamically. *i.e.* input line is given slots in output frame if and only if it has data to send.
No. of Slots	In Synchronous TDM No. of slots in each frame are equal to No. of input lines.	In Statistical TDM, No. of slots in each frame are less than the No. of input lines.
Buffers	Buffering is not done, frame is sent after a particular interval of time whether someone has data to send or not.	Buffering is done and only those inputs are given slots in output frame whose buffer contains data to send.
Addressing	Slots in Synchronous TDM carry data only and there is no need of addressing. Synchronization and pre assigned relationships between input and outputs that serve as an address.	Slots in Statistical TDM contain both data and address of the destination.
Synchro-nization	Synchronization bits are used at the beginning of each frame.	No synchronization bits are used.
Capacity	Max. Bandwidth utilization if all inputs have data to send.	The capacity of link is normally is less than the sum of the capacity of each channel.
Data	In Synchronous TDM de-multiplexer at receiving end decomposes each frame, discards framing bits and extracts data unit in turn. This extracted data unit from frame is then passed to destination device.	In Statistical TDM de-multiplexer at receiving end decomposes each frame by checking local address of each data unit. This extracted data unit from frame is then passed to destination device.

Q. 2. (*b*) Name the four basic network topologies, and cite an advantage of each type. (4)

Ans. Types of Network Topology.

Network' Topology is the schematic description of a network arrangement, connecting various nodes through lines of connection.

Bus Topology

Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called **Linear Bus topology**.

Advantages of Bus Topology

1. It is cost effective.
2. Cable required is least compared to other network topology.
3. Used in small networks.
4. It is easy to understand.

Ring Topology

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.

dotnotes.xyz

Advantages of Ring Topology

1. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
2. Cheap to install and expand.

Star Topology

In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.

Advantages of Star Topology

1. Fast performance with few nodes and low network traffic.
2. Hub can be upgraded easily.
3. Easy to troubleshoot.

Mesh Topology

It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has n(n-2)/2 physical channels to link n devices.

Advantages of Mesh Topology

1. Each connection can carry its own data load.
2. It is robust.
3. Fault is diagnosed easily.
4. Provides security and privacy.

Q.2. (c) Differenciate between Internet and Intranet. (2)

Ans.

Internet	Intranet
(*i*) It is the Network of Computer which is open for all.	(*i*) In this the network is designed for specific group of uses.
(*ii*) Internet Can't be accessed from Intranet.	(*ii*) Intranet can be accessed by Internet But with same restrictions.
(*iii*) Unlimited Number of User.	(*iii*) Limited number of user.
(*iv*) Visitor traffic is unlimited	(*iv*) Limited visitor traffic.

Q.3. (a) Briefly explain the sliding window protocol with help of an example (4

Ans. Sliding Window

• In sliding window method, multiple frames are sent by sender at a time befor needing an acknowledgment.

Sliding window refers to an imaginary boxes that hold the frames on both send and receiver side.

• It provides the upper limit on the number of frames that can be transmitt before requiring an acknowledgment.

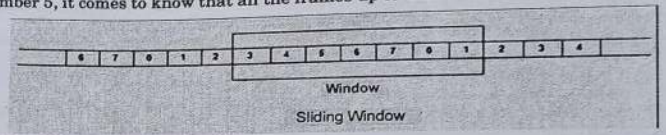
• Frames may be acknowledged by receiver at any point even when window is n full on receiver side.

• Frames may be transmitted by source even when window is not yet full on sender si

• The windows have a specific size in which the frames are numbered modulo- which means they are numbered from 0 to n-1. For *e.g.* if $n = 8$, the frames are number 0, 1, 2, 3, 4, 5, 6, 7, 0, 1, 2, 3, 4, 5, 6, 7, 0, 1, ...

• The size of window is n-1. For *e.g.* In this case it is 7. Therefore, a maximum n-l frames may be sent before an acknowledgment.

• When the receiver sends an ACK, it includes the number of next frame it expects to receive. For example in order to acknowledge the group of frames ending in frame 4, the receiver sends an ACK containing the number 5. When sender sees an ACK with number 5, it comes to know that all the frames up to number 4 have been received.



Sliding Window on Sender Side

At the beginning of a transmission, the sender's window contains n-l frames.

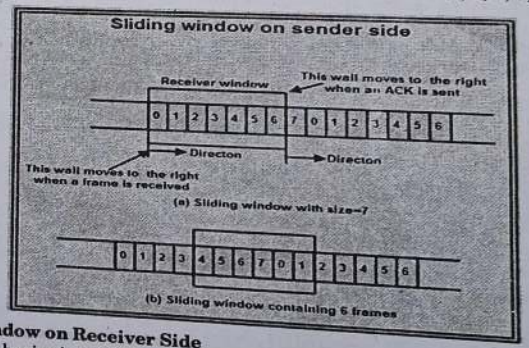
• As the frames are sent by source, the left boundary of the window moves inward, shrinking the size of window. This means if window size is w, if four frames are sent by source after the last acknowledgment, then the number of frames left in window is w-4.

• When the receiver sends an ACK, the source's window expand i.e. (right boundary moves outward) to allow in a number of new frames equal to the number of frames acknowledged by that ACK.

• For example, let the window size is 7 (in fig. (a), if frames 0 through 3 have been sent and no acknowledgment has been received, then the sender's window contains three frames - 4, 5, 6.

• Now, if an ACK numbered 3 is received by source, it means three frames (0, 1, 2) have been received by receiver and are undamaged.

• The sender's window will now expand to include the next three frames in its buffer. At this point the sender's window will contain six frames (4, 5, 6, 7, 0, 1).



Sliding Window on Receiver Side

• At the beginning of transmission, the receiver's window contains n-1 spaces for frame but not the frames.

• As the new frames come in, the size of window shrinks.

• Therefore the receiver window represents not the number of frames received but the number of frames that may still be received without an acknowledgment ACK must be sent.

• Given a window of size w, if three frames are received without an ACK being returned, the number of spaces in a window is w-3.

• As soon as acknowledgment is sent, window expands to include the number of frames equal to the number of frames acknowledged.

dotnotes.xyz

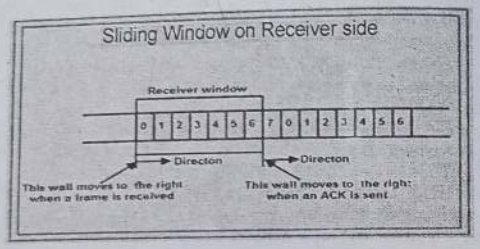
• For example, let the size of receiver's window is 7 as shown in diagram. It means window contains spaces for 7 frames.

• With the arrival of the first frame, the receiving window shrinks, moving the boundary from space 0 to 1. Now, window has shrunk by one, so the receiver may accept six more frame before it is required to send an ACK.

• If frames 0 through 3 have arrived but have DOC been acknowledged, the window will contain three frame spaces.

• As receiver sends an ACK, the window of the receiver expands to include as many new placeholders as newly acknowledged frames.

• The window expands to include a number of new frame spaces equal to the number of the most recently acknowledged frame minus the number of previously acknowledged frame. For *e.g.*, If window size is 7 and if prior ACK was for frame 2 & the current ACK is for frame 5 the window expands by three (5-2).



Therefore, the sliding window of sender shrinks from left when frames of data are sending. The sliding window of the sender expands to right when acknowledgments are received.

• The sliding window of the receiver shrinks from left when frames of data are received. The sliding window of the receiver expands to the right when acknowledgement is sent.

Q.3. (*b*) The codeword is received as 1100100101011. Check whether there are errors in the received code, if the divisor is 10101. **(4)**

Ans. To check codeword for errors, the received codeword is divided by the given divisor, that is, 10101 as shown below.

```
        111110001
10101 ) 1100100101011
        10101
        011000
         10101
          11010
          10101
           11111
           10101
            10100
            10101
             00011
             00000
              00110
              00000
               01101
               00000
                11011
                10101
                 1110 ←— Remainder (CRC)
```

Since the remainder obtained (CRC) is non-zero, the received codeword contains errors.

Q.3. (*c*) How is a hub related to a repeator? **(2)**

Ans. HUBS: It is a simplest connectivity device that is used to extend a network.All the networks requere a central junction called as hub there are 3 types of hub passive, active and intelligent.

Repeater: It is normally used for the expansion of the n/w length.

It generates a physical signal. It receives a weak signal. Amplified it and then retransmits it.

Q.4. (*a*) A seven bit hamming code is received as 110101. State whether the received is correct or wrong. If wrong, locate the error and correct it. **(4)**

Ans. For example: Suppose a 7-bit hamming codé is received as 1110101 and parity used is assumed to be even hence we can detect and correct the code as

Step 1: Received 7 bit hamming code is applied to hamming code format as

D7	*D6*	*D5*	*D4*	*D3*	*D2*	*P1*
1	0	1	0	1	0	1

Step 2: Checkbits for P4 bit

i.e. P4 D5 D6 D7

0	1	1	1	= odd parity hence error

So, P4 = 1

Step 3: Check bits for P2 bit

i.e. P2 D3 D6 D7

0	1	1	1	= odd parity hence error

So, P2 = 1

Step 4: Check bits for P1 bit

i.e. P1 D3 D5 D7

0	1	1	1	= even parity hence no error

So, P1 = 0

Hence the error word is E =

P4	*P2*	*P1*
1	1	0

Step 5: Decimal equivalent of 110 is 6 hence 6th bit is incorrect so invert it and the correct code word will be,

D7	*D6*	*D5*	*D4*	*D3*	*D2*	*D1*
1	0	1	0	1	0	1

Hence by using this method we can detect a s well as correct the error in the transmitted coded word. But it can locate a single bit error and fails detecting the burst error.

Q.4.(b) Compare and contrast a circuit switched network and a packet switched network. **(4)**

Ans. Refer Q1(b) of First Term Exam 2018 (Page No.: 1-2018)

Q.1.(b) Discuss the automatic repeat request (ARQ) method. **(2)**

Ans. Refer Q9 of End Term Exam 2017 (Page No.: 32-2017)

dotnotes.xyz

SECOND TERM EXAMINATION [APRIL–2016]
SIXTH SEMESTER [B. TECH]
COMPUTER NETWORKS [ETCS–306]

Time: 1½ Hrs. **Max Marks: 30**

Note: *Question No. 1 is compulsory and attempt any two from rest.*

Q.1. (a) In classless addressing, we know the first address and the number of addresses in the block. Can we find the prefix length? If yes show the process. (2)

Ans. Yes: We know the number of addresses in the block which is equivalent to the number of digits in the suffix raised to the power of two. If there are 64 addresses in the block, that is 2^6, therefore there are 6 bits in the suffix, and the prefix is 32-6 bits, or 26 bits

$$n = 32 - \log N = 23 - \log 64 = 26 \text{ bits}$$

Q.1. (b) Can the header length field in IPV4 packet be less than 5? When is it exactly 5? (2)

Ans. The value of header length in an IP packet cannot be less than 5. It is between 5 and 15. The header length is 20-60 bytes. The length of the datagram header is a 4 byte word. So its value must be divided by 4 to give the length in unit less.

So 20/4 = 5, so minimum value is 5 and maximum value is 15.

Q.1. (c) Explain how TCP, which uses the services provided by the unreliable IP, can provide reliable communication.

Ans. The primary difference between TCP & UDP lies in the way they implement data transfer TCP include support guaranteed delivery, in which recipient automatically acknowledges the sender when message is received. In addition the sender waits and retransmits the data if implement guaranteed message delivery. A UDP datagram can get lost during transmission and the protocol will not be able to detect and report this.Few mechanisms help to provide the reliability of TCP such as

- Checksum-All TCP segment carry a checksum, which is used by the receiver to detect errors with either the TCP header or data.
- Duplicate and detection-It is possible for packets to be duplicated in packet switched network; therefore TCP keeps track of bytes received in order to discard duplicate copies of data that has already been received.
- Retransmissions-In order to guarantee delivery of data, TCP must implement retransmission schemes for data that may be lost or damaged. The use of positive acknowledgments by the receiver to the sender confirms successful reception of data. The lack of positive acknowledgments, coupled with a timeout period calls for retransmission.
- Sequencing -In packet switched networks, it is possible for packets to be delivered out of order. It is TCP's job to properly sequence segments it receives so it can deliver the byte stream data to anapplication in order.
- Timers-TCP maintain various static and dynamic timers on data sent. The sending TCP waits for the receiver to reply with an acknowledgment within a bounded length of time. If the timer expires before receiving an acknowledgment, the sender can retransmit the segment.

Q.1. (d) The following is a dump of UDP header in hexsadecimal format: 0045DF0000580000. (2)

(i) What is the source port number?

(ii) What is the destination port number?

(iii) What is the length of the data?

(iv) Is the packet directed from the client to the server or vice versa?

Ans. (i) First four hexadecimal digits are 0045 which gives the decimal value 69.

[(0045) = 0000 0000 0100 0101 = 2 ^ 6 + 2 ^ 2 + 2 ^ 0 = 64 + 4 + 1 = 69

Ans. (ii) Second four hexadecimal digits are DF00 or 57088

[(DF00)=1101 1111 0000 0000 = 2 ^ 15 + 2 ^ 14 + 2 ^ 12 + 2 ^ 11 + 2 ^ 10 + 2 ^ 9 + 2 ^ 8 = 32768 + 16384 + 4096 + 2048 + 1024 + 512 + 256 = 57088

Ans. (iii) Length of the whole packet minus the length of the header, or 88 – 8 = 80 bytes.

Length of whole packet is calculated as

[(0058) = 0000 0000 0101 1000 = 2 ^ 6 + 2 ^ 4 + 2 ^ 3 = 64 + 16 + 8 = 88

Ans. (iv) Since the destination port number is 57088 (not well-known port), the packet is from the client to the server.

Q. 1. (e) What is SDH technology? Differentiate between PDH and SDH?

Ans. SDH: SDH supports various topologies such as point to point, ring, star, linear bus etc. It uses TDM and octet multiplexing.

In **SDH**, digital multiplexer's inputs are of same bit rate and are derived from common clock, hence are in phase. Hence it is synchronous.

Word (group of bits) Interleaving is used in SDH to combine digital signals.

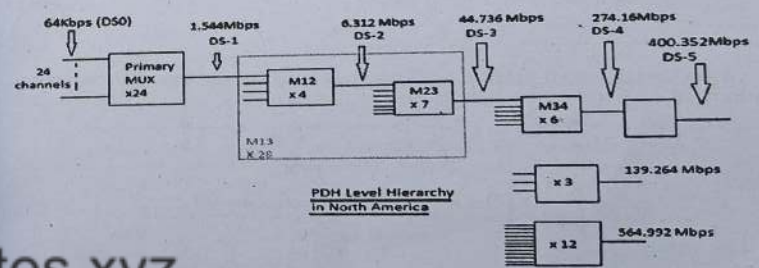
As per CCITT, any of PDH rates upto 140 Mbps can be integrated with SDH rates up to 155.52 Mbps.

Following are the merits or advantages of SDH:

- A more simplified multiplexing and demultiplexing technique.
- Synchronous networking and SDH supports multipoint networking.
- Capability of transporting existing PDH signals.
- Easy growth to higher bit rates which enhances the administration and maintenance process.
- It is capable of transporting broadband signals.
- It is multivendor and supports different operators.
- It provides network transport services on LAN such as video conferencing, and interactive multimedia.
- Optical fibre bandwidth can be increased without limit in SDH.
- Switching protection to traffic is offered by rings.
- SDH allows quick recovery from failure.

PDH: In **PDH**, digital multiplexer's inputs (bit streams) are of same bit rate and are derived from different clocks from different oscillators. Each will differ within tolerance of few clock periods. Hence it is called plesiochronous.

Bit Interleaving is used in PDH to combine digital signals.

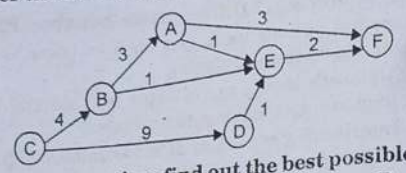


dotnotes.xyz

Following are the limitations of PDH:

- In PDH, different frame is used for transmission and in data layer. Hence multiplexing and de-multiplexing is very complex.
- Accessing lower tributary requires the whole system to be de-multiplexed.
- The maximum capacity for PDH is 566 Mbps, which is limited in bandwidth.
- Tolerance is allowed in bit rates.
- PDH allows only Point-to-Point configuration.
- PDH does not support Hub.
- Every manufacturer has its own standards; PDH also has different multiplexing hierarchies making it difficult to integrate interconnecting networks together.

Q.2. (*a*) Consider the network shown in the figure.



Using distance vector routing, find out the best possible path A → D. **(4)**

Ans. We have to find out the shortest distance from A to D using distance vector Routing.

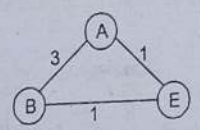
In distance vector routing every node maintains a distance vector to all other nodes which represents the cost to reach the neighbouring nodes.

Every node of the graph or vector share its vector with its neighbouring nodes and then the vectors get updated if any other path which is shortest is found through their neighbouring nodes.

Initially the table can be like.

From	To *A*	*B*	*C*	*D*	*E*	*F*
A	0	3	∞	∞	1	3
B	3	0	4	∞	1	6
C	∞	4	0	9	∞	∞
D	∞	∞	9	0	1	2
E	1	1	∞	1	0	2
F	3	∞	∞	∞	2	0

This table consists of the distance link entries. Any link that is down is marked as ∞. Considering Node A:

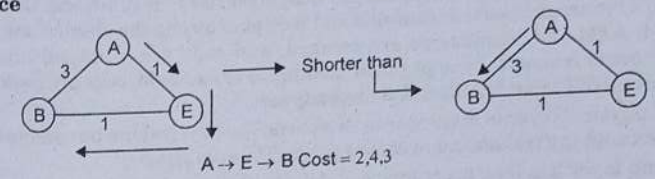


A has 2 neighbours *B* and *E*, so it will use vectors of B and E to find out the shortest paths to all other nodes. The table updates to

From	To *A*	*B*	*C*	*D*	*E*	*F*
A	0	3	∞	∞	1	3
B		2	6	2		
C						
D						
E						
F						

(similarly the complete table is updated)

Since



A → B cost 2

Similarly B has shortest path to C (cost = 4)

∴ A → C becomes A → B → C Cost = 2 + 4 = 6.

Cost = 2 + 4 = 6

and for *D*

$A \to E \to D$ Cost = 2 < ∞

∴ $A \to D$ cost = 2

No other updations can be made in vector of A. This update vector of A is shared with B and E. The final table is obtained when no updation can be made in case of each and every node.

The table results in

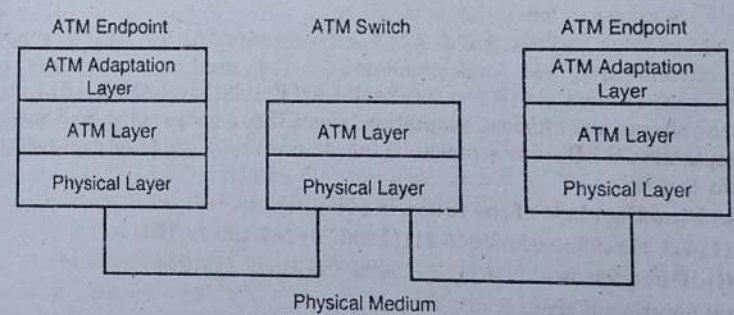
From	To *A*	*B*	*C*	*D*	*E*	*F*
A	0	2	4	2	1	3
B	3	0	4	5	1	6
C	7	4	0	9	5	10
D	2	2	9	0	1	2
E	1	1	5	1	0	2
F	3	3	7	3	2	0

Therefore the distance from *A* to *D* is 2

$$A \xrightarrow{1} E \xrightarrow{1}$$

Q.2. (*b*) Name the ATM layers and explain their functions **(4)**

Ans. ATM: Asynchronous Transfer Mode (ATM) is a standard switching technique designed to unify telecommunication and computer networks. It uses asynchronous time-division multiplexing,[1][2] and it encodes data into small, fixed-sized cells. This differs from approaches such as the Internet Protocol or Ethernet that use variable sized packets or frames. ATM provides data link layer services that run over a wide range of OSI physical Layer links.



dotnotes.xyz

The ATM Physical Layer: The ATM physical layer has four functions: Cells are converted into a bitstream, the transmission and receipt of bits on the physical medium are controlled, ATM cell boundaries are tracked, and cells are packaged into the appropriate types of frames for the physical medium. For example, cells are packaged differently for SONET than for DS-3/E-3 media types.

The ATM physical layer is divided into two parts: the physical medium-dependent (PMD) sublayer and the transmission convergence (TC) sublayer.

The TC sub layer has four functions: cell delineation, header error control (HEC) sequence generation and verification, cell-rate decoupling, and transmission frame adaptation. The cell delineation function maintains ATM cell boundaries, allowing devices to locate cells within a stream of bits. HEC sequence generation and verification generates and checks the header error control code to ensure valid data. Cell-rate decoupling maintains synchronization and inserts or suppresses idle (unassigned) ATM cells to adapt the rate of valid ATM cells to the payload capacity of the transmission system. Transmission frame adaptation packages ATM cells into frames acceptable to the particular physical layer implementation.

ATM Adaptation Layers: AAL1: AAL1, a connection-oriented service, is suitable for handling constant bit rate sources (CBR), such as voice and videoconferencing. ATM transports CBR traffic using circuit-emulation services. Circuit-emulation service also accommodates the attachment of equipment currently using leased lines to an ATM backbone network. AAL1 requires timing synchronization between the source and the destination. For this reason, AAL1 depends on a medium, such as SONET, that supports clocking.

ATM Adaptation Layers: AAL2: Another traffic type has timing requirements like CBR but tends to be bursty in nature. This is called variable bit rate (VBR) traffic. This typically includes services characterized as packetized voice or video that do not have a constant data transmission speed but that do have requirements similar to constant bit rate services. AAL2 is suitable for VBR traffic. The AAL2 process uses 44 bytes of the cell payload for user data and reserves 4 bytes of the payload to support the AAL2 processes.

VBR traffic is characterized as either real-time (VBR-RT) or as non-real-time (VBR-NRT). AAL2 supports both types of VBR traffic.

ATM Adaptation Layers: AAL3/4: AAL3/4 supports both connection-oriented and connectionless data. It was designed for network service providers and is closely aligned with Switched Multimegabit Data Service (SMDS). AAL3/4 is used to transmit SMDS packets over an ATM network.

An AAL 3/4 SAR PDU header consists of Type, Sequence Number, and Multiplexing Identifier fields. Type fields identify whether a cell is the beginning, continuation, or end of a message. Sequence number fields identify the order in which cells should be reassembled. The Multiplexing Identifier field determines which cells from different traffic sources are interleaved on the same virtual circuit connection (VCC) so that the correct cells are reassembled at the destination.

ATM Adaptation Layers: AAL5: AAL5 is the primary AAL for data and supports both connection-oriented and connectionless data. It is used to transfer most non-SMDS data, such as classical IP over ATM and LAN Emulation (LANE). AAL5 also is known as the simple and efficient adaptation layer (SEAL) because the SAR sublayer simply accepts the CS-PDU and segments it into 48-octet SAR-PDUs without reserving any bytes in each cell.

Q.2. (c) Find the class of the following IP address. (2)

(i) 01111011 11110000 01101010 11111000 (ii) 147.120.12.194

Ans. (i) IP address is 01111011 11110000 01101010 1111000

Decimal notation of given binary form is

124. 240. 106. 248

This IP address falls in the range of class- A *i.e* (0-127). So, this IP address belongs to class A.

(ii) IP address is 147.120.12.194

This IP address falls in the range of class-B *i.e.* (128-191)

So, this IP address belongs to class B.

Q.3. (a) An organization is granted the block 130.56. 10.0. The administrator wants to create 1024 subnets (6)

(1) Find the number of addresses in each subnet

(2) Find the first and last address of the first subnet.

(3) Find the subnet mask.

(4) Find the first and lest address of the last subnet.

Ans. $1024 = 2^n$ where $n = 10$. The address is a Clas B address so the default mask is /16 and so if we require 10 bits for the subnets then the required subnet mask is /16 + 10 = /26. (Could be specified as 0xffffffc0, or 255. 255. 255. 192 in dotted decimal format) therefore, the subnet mask will be 255.255.255.192.

(1) The remaining bits must be used for the addresses in each subnet i.e. we shall have 32–26 = 6 bits for the address component or $2^6 = 64$ bits. We lose two addresses per subnet as they are not actually allocatable Each subnet mask will be able to maintain 62 valid addresses.

(2) The first and last allocatable addresses in subnet 1 are

130.56.0.1 to 130.56.0.62

Working

The first address for the block is found by ANDing the address 130.56.0.0 with the subnet mask 26 giving 10000010 00111000 00000000 00000000 (130.56.0.0).

But this is not an allocatable address, so the next one is 10000010 00111000 00000000 00000001 (130.56.0.1)

Finally, we note that the broadcast address is the last one of the 64 addresses so the last allocatable one is the one before that broadcast address so it must be

10000010 00111000 00000000 00111110 (130.56.0.62)

(3) The subnet mask will be 126. i.e.

10000010 00111000 00000000 00000000.

(4) First address in the 1024 subnet = 130.56.255.193 Last address in 1024 subnet = 130.56.255.254

Q. 3. (b) Explain the process of connection establishment in TCP. (4)

Ans. The TCP three-way handshake in Transmission Control Protocol (also called the three message handshake) is the method used to establish TCP socket connections and tear down TCP socket connections over the network. TCP's three way handshaking technique is referred to as the 3-way handshake or as "SYN-SYN-ACK" (or more accurately SYN, SYN-ACK, ACK). The TCP handshaking mechanism is designed so that two computers attempting to communicate can negotiate the parameters of thenetwork TCP socket connection before beginning communication. This three way handshaking process is also designed so that both ends can initiate and negotiate separate TCP socket connections at the same time. Being able to negotiate multiple TCP socket connections in both directions at the same time allows a single *physical network interface (such as ethernet) to be multiplexed.*

3-Way Handshake Description

Host A(client) sends a TCP SYNchronize packet to Host B(server)

Host B receives A's SYN

dotnotes.xyz

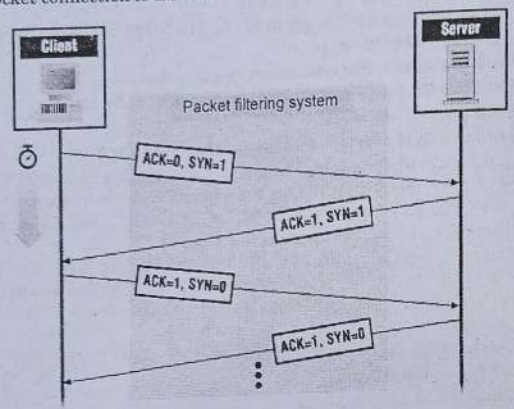
Host B sends a SYNchronize-ACKnowledgement

Host A receives B's SYN-ACK

Host A sends ACKnowledge

Host B receives ACK

TCP socket connection is ESTABLISHED.



Q. 4. (*a*) Draw IP datagram and explain the each field of the datagram. A packet has arrived in which the off set is 300 and payload size is 100 bytes. What is the number of the first byte and the last byte? (5)

Ans. Working of IP: fragmentation: When a router receives a packet, it examines the destination address and determines the outgoing interface to use. The interface has an MTU. If the packet size is bigger than the MTU, the router may fragment the packet.

0	4	8	16	19	31
Version	IHL	Type of Service	Total Length		
Identification			Flags	Fragment Offset	
Time to Live		Protocol	Header Checksum		
Source IP Address					
Destination IP Address					
Options				Padding	

Fig. IP Frame Format

The router divides the packet into segments. The max size of each segment is the MTU minus the IP header size (20 bytes minimum; 60 bytes maximum). The router puts each segment into its own packet, each fragment packet having following changes:

- The *total length* field is the segment size.
- The *more fragments* (MF) flag is set for all segments except the last one, which is set to 0.
- The *fragment offset* field is set, based on the offset of the segment in the original data payload. This is measured in units of eight-byte blocks.

- The *header checksum* field is recomputed.

Reassembly: A receiver knows that a packet is a fragment if at least one of the following conditions is true:

- The "more fragments" flag is set. (This is true for all fragments except the last.)
- The "fragment offset" field is nonzero. (This is true for all fragments except the first.)

The receiver identifies matching fragments using the identification field. The receiver will reassemble the data from fragments with the same identification field using both the fragment offset and the more fragments flag. When the receiver receives the last fragment (which has the "more fragments" flag set to 0), it can calculate the length of the original data payload, by multiplying the last fragment's offset by eight, and adding the last fragment's data size. In the example above, this calculation was $495 \times 8 + 540 = 4500$ bytes.

When the receiver has all the fragments, it can put them in the correct order, by using their offsets. It can then pass their data up the stack for further processing.]

To find the number of the first byte: We multiply the offset value by 8. This means that the first byte number is 800.

Since payload is 100 bytes. So last byte number is 879

Q.4. (*b*) Write a short note on leaky bucket algorithm. (3)

Ans . Leaky Bucket Algorithm: Consider a Bucket with a small hole at the bottom, whatever may be the rate of water pouring into the bucket, the rate at which water comes out from that small hole is constant. This scenario is depicted in figure (a). Once the bucket is full, any additional water entering it spills over the sides and is lost (*i.e.* it doesn't appear in the output stream through the hole underneath).

The same idea of leaky bucket can be applied to packets, as shown in Fig.*b*. Conceptually each network interface contains a leaky bucket. And the following steps are performed:

- When the host has to send a packet, the packet is thrown into the bucket.
- The bucket leaks at a constant rate, meaning the network interface transmits packets at a constant rate.
- Bursty traffic is converted to a uniform traffic by the leaky bucket.
- In practice the bucket is a finite queue that outputs at a finite rate.

This arrangement can be simulated in the operating system or can be built into the hardware. Implementation of this algorithm is easy and consists of a finite queue. Whenever a packet arrives, if there is room in the queue it is queued up and if there is no room then the packet is discarded.

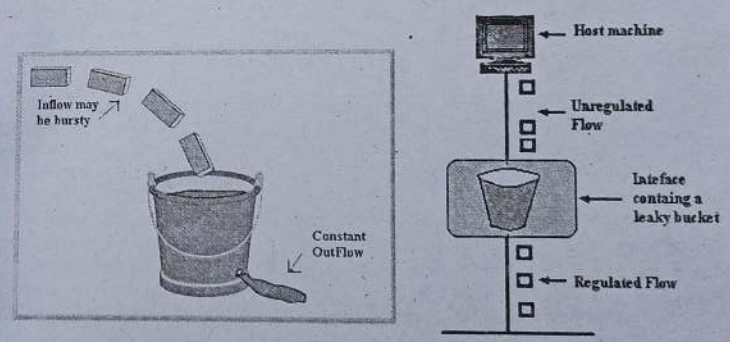


Fig. (a) Leaky bucket (b) Leaky bucket implementation

dotnotes.xyz

Q.4. (c) Explain the role of NAV in CSMA/CA. **(2)**

Ans. NAV allows stations to indicate the amount of time required for transmission of required frames immediately following the current frame.

This is important to reserve the medium as busy for these mandatory frames. The importance of NAV virtual carrier sense is to ensure medium reservation for frames critical to operation of the 802.11 protocol. Typically these are control frames, but not always. They include 802.11 acknowledgements, subsequent data and acknowledgement frames as part of a fragment burst, and data and acknowledgement frames following an RTS/CTS exchange.

The NAV is carried in the 802.11 MAC header Duration field which is part of the MPDU payload, and is encoded at a variable data rate as discussed previously. Therefore, not all stations within the area may be able to decode the MPDU due to insufficient SNR. However, all stations within the area should still be able to decode the PLCP header used for CCA. Since the critical frames that the NAV protects use shorter inter-frame spacing values (SIFS for example), those frames should still gain access to the medium before any other station attempts to transmit and stations will detect a busy medium through CCA carrier sense. However, the added protection through NAV reservation is lost.

Stations that are able to decode the 802.11 header extract the Duration field value and use it mark the medium as busy for the amount of time specified (in microseconds). Therefore, the transmitter should follow the strict rules defined in the 802.11 specification for calculation of the NAV value to be sent within frames.

END TERM EXAMINATION [MAY-JUNE–2016]
SIXTH SEMESTER [B. TECH]
COMPUTER NETWORKS [ETCS–306]

Time: 3 Hrs. **Max Marks: 75**

Note: *Attempt any five questions including Q.No. 1 which is compulsory.*

Q.1. Attempt All.

Q.1. (a) Differentiate between circuit switching, packet switching and message switching. **(5)**

Ans. Circuit-Switching, Message-Switching and Packet-Switching

Circuit switching network establishes a fixed bandwidth circuit (channel) between nodes before the users may communicate, as if the nodes were physically connected with an electrical circuit. The bit delay is constant during the connection, as opposed to packet switching, where packet queues may cause varying delay.

Each circuit cannot be used by other callers until the circuit is released and a new connection is set up. Even if no communication is taking place in a dedicated circuit then, that channel still remains unavailable to other users. Channels that are available for new calls to be set up are said to be idle. Telephone network is example of circuit switching system.

Virtual circuit switching is a packet switching technology that may emulate circuit switching, in the sense that the connection is established before any packets are transferred, and that packets are delivered in order.

Message switching was the precursor of packet switching, where messages were routed in their entirety, one hop at a time. It was first introduced in 1961. Nowadays, message switching systems are mostly implemented over packet-switched or circuit-switched data networks. E-mail is example of a message switching system.

Packet switching is a communications paradigm in which packets (discrete blocks of data) are routed between nodes over data links shared with other traffic. The term "packets" refers to the fact that the data stream from your computer is broken up into packets of about 200 bytes (on average), which are then sent out onto the network. Each packet contains a "header" with information necessary for routing the packet from source to destination. Each packet in a data stream is independent.

The main advantage of packet-switching is that it permits "statistical multiplexing" on the communications lines. The packets from many different sources can share a line, allowing for very efficient use of the fixed capacity. With current technology, packets are generally accepted onto the network on a first-come, first-served basis. If the network becomes overloaded, packets are delayed or discarded ("dropped").

Q.1. (b) Differentiate between adaptive and non-adaptive routing algorithms. **(5)**

Ans.1. Adaptive Routing Algorithm: These algorithms change their routing decisions to reflect changes in the topology and in traffic as well. These get their routing information from adjacent routers or from all routers. The optimization parameters are the distance, number of hops and estimated transit time. This can be further classified as follows:

(a) Centralized: In this type some central node in the network gets entire information about the network topology, about the traffic and about other nodes. This then transmits this information to the respective routers. The advantage of this is that only one node is required to keep the information. The disadvantage is that if the central node goes down the entire network is down, i.e. single point of failure.

dotnotes.xyz

(6) Isolated: In this method the node decides the routing without seeking information from other nodes. The sending node does not know about the status of a particular link. The disadvantage is that the packet may be send through a congested route resulting in a delay. Some examples of this type of algorithm for routing are:

• **Hot Potato:** When a packet comes to a node, it tries to get rid of it as fast as it can, by putting it on the shortest output queue-without regard to where that link leads. A variation of this algorithm is to combine static routing with the hot potato algorithm. When a packet arrives, the routing algorithm takes into account both the static weights of the links and the queue lengths.

• **Backward Learning:** In this method the routing tables at each node gets modified by information from the incoming packets. One way to implement backward learning is to include the identity of the source node in each packet, together with a hop counter that is incremented on each hop. When a node receives a packet in a particular line, it notes down the number of hops it has taken to reach it from the source node. If the previous value of hop count stored in the node is better than the current one then nothing is done but if the current value is better then the value is updated for future use. The problem with this is that when the best route goes down then it cannot recall the second best route te a particular node. Hence all the nodes have to forget the stored informations periodically and start all over again.

(c) Distributed: In this the node receives information from its neighbouring nodes and then takes the decision about which way to send the packet. The disadvantage is that if in between the the interval it receives information and sends the paket something changes then the packet may be delayed.

2. Non-Adaptive Routing Algorithm: These algorithms do not base their routing decisions on measurements and estimates of the current traffic and topology. Instead the route to be taken in going from one node to the other is computed in advance, off-line, and downloaded to the routers when the network is booted. This is also known as static routing. This can be further classified as:

(a) Flooding: Flooding adapts the technique in which every incoming packet is sent on every outgoing line except the one on which it arrived. One problem with this method is that packets may go in a loop. As a result of this a node may receive several copies of a particular packet which is undesirable. Some techniques adapted to overcome these problems are as follows:

• **Sequence Numbers:** Every packet is given a sequence number. When a node receives the packet it sees its source address and sequence number. If the node finds that it has sent the same packet earlier then it will not transmit the packet and will just discard it.

• **Hop Count:** Every packet has a hop count associated with it. This is decremented(or incremented) by one by each node which sees it. When the hop count becomes zero(or a maximum possible value) the packet is dropped.

• **Spanning Tree:** The packet is sent only on those links that lead to the destination by constructing a spanning tree routed at the source. This avoids loops in transmission but is possible only when all the intermediate nodes have knowledge of the network topology!

Blooding is not practical for general kinds of applications. But in cases where high degree of robustness is desired such as in military applications, flooding is of great help.

(6) **Random Walk:** In this method a packet is sent by the node to one of its neighbours randomly. This algorithm is highly robust. When the network is highly

interconnected, this algorithm has the property of making excellent use of alternative routes. It is usually implemented by sending the packet onto the least queued link.

Q.1. (c) Explain parity bit error detection method in detail. **(5)**

Ans. Parity Checking of Error Detection

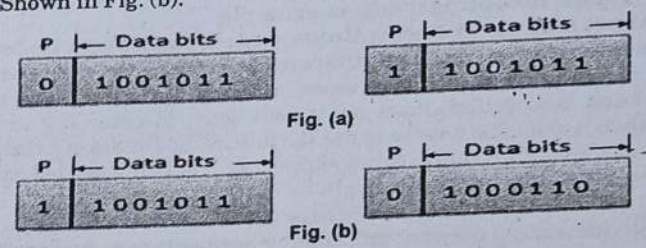
Even parity — Even parity means the number of 1's in the given word including the parity bit should be even (2, 4, 6,....).

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.

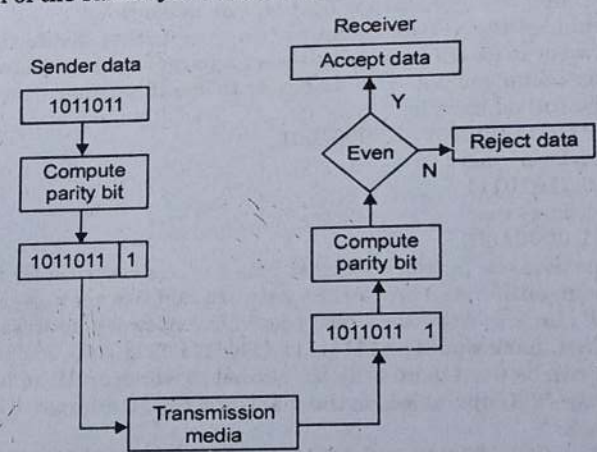
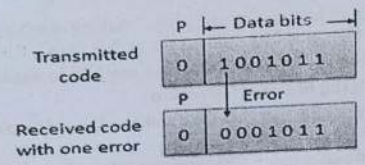


Fig. Even-parity checking scheme

dotnotes.xyz



Q. 1. (*d*) Differentiate between narrow band ISDN, broadband ISDN **(5)**

Ans. The narrowband ISDN is based on the use of a 64 kbps channel as the basic unit of switching and has a circuit switching orientation. The major technical contribution of the narrowband ISDN effort has been frame relay. The B-ISDN supports very high data rates (100s of Mbps) and has a packet switching orientation. The major technical contribution of the B-ISDN effort has been asynchronous transfer mode, also known as cell relay.

Q. 1. (*e*) Explain subneting using an example. **(5)**

Ans. A **subnet** is a logical grouping of connected network devices. Nodes on a subnet tend to be located in close physical proximity to each other on a LAN. The pourpose of subnetting is not to provide extra addresses, but to keep network data separated to prevent congestion. Subnetting allows you to not waste addresses. If your network has only 10 hosts then it would be unwise to use the full 255 addresses of a class C network. It would be much more efficient to use an address with only the needed amount of host bits so that the remaining addresses might be used in other networks.

The major reasons for subnetting the network:

1. To divide a large network into smaller segments to reduce traffic and speed up the sections of your network.
2. To connect networks across geographical areas.

Subnet Mask

A mask used to determine what subnet an IP address belongs to. An IP address has two components, the network address and the host address. For example, consider the IP address 150.215.017.009. Assuming this is part of a Class B network, the first two numbers (150.215) represent the Class B network address, and the second two numbers (017.009) identify a particular host on this network.

Subnetting enables the network administrator to further divide the host part of the address into two or more subnets. In this case, a part of the host address is reserved to identify the particular subnet. This is easier to see if we show the IP address in binary format. The full address is:

10010110.11010111.00010001.00001001

The Class B network part is:

10010110.11010111

and the host address is:

00010001.00001001

The subnet mask is the network address plus the bits reserved for identifying the subnetwork. (By convention, the bits for the network address are all set to 1, though it would also work if the bits were set exactly as in the network address.) In this case, therefore, the subnet mask would be 11111111.11111111.11110000.00000000. It's called a *mask* because it can be used to identify the subnet to which an IP address belongs by performing abitwise AND operation on the mask and the IP address. The result is the subnetwork address:

Subnet Mask	255.255.240.000	11111111.11111111.11110000.00000000
IP Address	150.215.017.009	10010110.11010111.00010001.00001001

Subnet Address	150.215.016.000	10010110.11010111.00010000.00000000

The subnet address, therefore, is 150.215.016.000.

Q.2. (a) Compute the CRC for a 10-bit sequence 1010011110 and a divisor of 1011. **(6)**

Ans. Given Sequence: 1010011110 We append 000 and divided by 1011

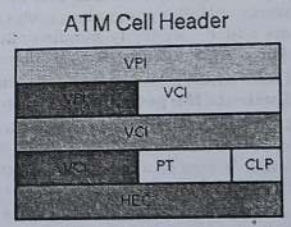
Code:

```
1011)1010 011 1100 000   (1001001110
     1011
     ----
      1011
      1011
      ----
        1100
        1011
        ----
         1110
         1011
         ----
          1010
          1011
          ----
           010 —Remainder
```

So,CRC encoded sequence is 10100111100010

Q.2. (b) Give the header format of ATM Cell. Also explain the semantics of each filed in the header. **(6.5)**

Ans. The ATM cell is the basic unit of information transfer in the B-ISDN ATM communication. The cell is comprised of 53 bytes. Five of the bytes make up the header field and the remaining 48 bytes form the user information field. The following is the structure of the Network Node Interface (NNI) ATM Cell Header:



Generic Flow Control

The Generic Flow Control (GFC) field is a 4-bit field that was originally added to support the connection of ATM networks to shared access networks such as a Distributed Queue Dual Bus (DQDB) ring. The GFC field was designed to give the User-Network Interface (UNI) 4 bits in which to negotiate multiplexing and flow control among the cells of various ATM connections. However, the use and exact values of the GFC field have not been standardized, and the field is always set to 0000.

Payload Type (PT) / Cell Loss Priority (CLP) / Header Error Control (HEC): When user information is present or the ATM cell has suffered traffic congestion then the PT field will yield this information.

dotnotes.xyz

The CLP bit is used to tell the system whether the corresponding byte is to be discarded during network congestion . ATM cells with CLP=0 have a priority in regard to cell loss than ATM cells with CLP=1. Therefore, during resource congestions, CLP=1 cells are dropped before any CLP=0 cell is dropped.

HEC is a CRC byte for the cell header field and is used for sensing and correcting cell errors and in delineating the cell header.

Virtual Path Identifier / Virtual Channel Identifier (VPI/VCI): The role of the VPI/VCI fields is to indicate Virtual Path or Virtual Channel identification numbers, so that the cells belonging to the same connection can be distinguished. A unique and separate VPI/VCI identifier is assigned in advance to indicate which type of cell is following, unassigned cells, physical layer OAM cells, metasignalling channel or a generic broadcast signaling channel.

(*ii*) How is a virtual connection established and how is QoS negotiated for that connection? This is done through the process called signaling. Signaling performs call setup and call clearing, and many other functions related to the network.

There are two sets of standards for ATM signaling:

UNI signaling

NNI signaling

UNI signaling is performed between an end station and a private ATM switch, or between a private ATM switch and the public ATM network. The UNI signaling is simpler because it doesn't involve routing. The standards are produced by the ATM Forum and are called UNI 3.1 (1994) and UNI 4.0 (1996). (UNI 4.0 is an addition to UNI 3.1, UNI 3.1 is derived from the Public Net- work Signaling protocol Q.2931 brought by the ITU-T, which is further derived from Q931 used in ISDN and Frame Relay).

NNI signaling is performed between the switches of a public ATM network. Since a public net- work generally involves several (or many) switches the routing becomes very important compo- nent of the NNI signaling. NNI signaling has two major standards: IISP (Integrated Interswitch Signaling Protocol) and PNNI (Private Network-to-Network Interface). IISP is a simple signaling protocol which uses static routing and is designed for small private ATM networks. PNNI is a signaling protocol that uses very elaborate dynamic routing algorithms which can easily handle small to large ATM networks which can have hundreds, thousands and even tens of thousands of ATM switches.

Q.3. Explain channel allocation problem and its solution algorithm in detail. Provide an example to illustrate the problem and its solution. **(12.5)**

Ans. In any broadcast network, the key issue is how to determine who gets to use the channel when there is competition for it. The protocols used to determine who goes next on a multi-access channel belong to a sub-layer of the data link layer called the MAC (Medium Access Control) sub-layer.

The Channel Allocation Problem is how to allocate a single broadcast channel among competing users.

Static channel Allocation: The most typical way of allocating a single channel among multiple competing users is Frequency Division Multiplexing (FDM). If the number of users are N, the banduidth is divided into N equal-sized portions. Each user is assigned one portion. If the number of users are small and constant, FDM is a simple and efficient allocation mechanism.

A telephone trunk can be a simple example of this type. However, when the number of senders is not small and constant or the traffic is heavy. FDM presents some problems. If the spectrum is divided into N regions the number of users currently interested in communicating is less than *N* a large piece of valuable spectrum will be wasted.

And due to this problem. If more than N users want to communicate, some of them will be denied permission for lack of bandwidth.The main reason for lack of bandwidth is that some of the users who have been assigned a frequency band hardly ever transmit or receive anything. So. dividing a single channel into static sub channels is quiet inefficient.The poor performance of static FDM can easily be seen from a simple queuing theory calculation. If the mean time delay is *T*, for a channel of capacity C bps, with an arrival rate of lambda frames/sec, each frame having a length drawn from an exponential probability density function with mean *i/i/^* bits/frame. With these parameters the arrival rate is lambda frames/sec and the service rate is ^C frames/sec.

From queuing theory. T = i (^C-lambda) For example, if *C* is 100 Mbps, The mean frame length, is 10,000 bits. and the frame arrival rate, lambda, is 5000 frames/sec, then T = 200 sec.

Dynamic Channel Allocation : Unlike the static channel,dynamic channel allocation is efficient and is used in areas where the traffic is nonuniform and heavy. Five main assumptions must be considered in dynamic channel allocation.

1. Station Model: Stations are also called terminals. The number of independent stations are N, with independent constant arrival rates lambda, and probability of a frame being generated in a time interval of (delta t) is (delta t x lambda). Once a frame has been generated the station does nothing until the frame has successfully been transmitted.

2. Single Channel Assumption: From hardware point of view, all stations are equal. A single channel is available for communication on which all stations can transmit on it and all can receive from it.

3. Collision Assumption: If two frames are transmitted simultaneously, they will collide resulting in a false signal. Each station has the ability to detect collision and it must be kept in mind that collided frame must be retransmitted later.

4. Time Management:

Continuous Time: Frame transmission can begin at any instant as there is no master clock diving time into discrete intervals.

Slotted Time: Frame transmission start at the beginning of the time slots. A slot may contain 0,1. or more frame corresponding to an idle, successful or collision transmission respectively.

5. Sensing of Channel:

Carrier Sense: A channel can be sensed by station before trying to use it. If a station senses the channel as busy, no station will attempt to use it, unitl it gols idle.

No Carrier Sense: Station connot sense the channel before trying to use it. First the transmit and the came to where the channels is busy or idle

Q. 4. (*a*) Discuss the various issues in designing data link layer in detail. **(6)**

Ans. The data link layer has a number of specific functions to carry out. These functionsinclude providing a well-defined service interface to the network layer, determining how the bits of the physical layer are grouped into frames, dealing with transmission errors and regulating the flow or frames so that slow receivers are not swaped by fast senders. In the following sections we will examine each of these issues in turn.

There are the following issues:

(*a*) Services Provided to the Network Layer

(*b*) Framing

dotnotes.xyz

The CLP bit is used to tell the system whether the corresponding byte is to be discarded during network congestion . ATM cells with CLP=0 have a priority in regard to cell loss than ATM cells with CLP=1. Therefore, during resource congestions, CLP=1 cells are dropped before any CLP=0 cell is dropped.

HEC is a CRC byte for the cell header field and is used for sensing and correcting cell errors and in delineating the cell header.

Virtual Path Identifier / Virtual Channel Identifier (VPI/VCI): The role of the VPI/VCI fields is to indicate Virtual Path or Virtual Channel identification numbers, so that the cells belonging to the same connection can be distinguished. A unique and separate VPI/VCI identifier is assigned in advance to indicate which type of cell is following, unassigned cells, physical layer OAM cells, metasignalling channel or a generic broadcast signaling channel.

(*ii*) How is a virtual connection established and how is QoS negotiated for that connection? This is done through the process called signaling. Signaling performs call setup and call clearing, and many other functions related to the network.

There are two sets of standards for ATM signaling:

UNI signaling

NNI signaling

UNI signaling is performed between an end station and a private ATM switch, or between a private ATM switch and the public ATM network. The UNI signaling is simpler because it doesn't involve routing. The standards are produced by the ATM Forum and are called UNI 3.1 (1994) and UNI 4.0 (1996). (UNI 4.0 is an addition to UNI 3.1, UNI 3.1 is derived from the Public Net- work Signaling protocol Q.2931 brought by the ITU-T, which is further derived from Q931 used in ISDN and Frame Relay).

NNI signaling is performed between the switches of a public ATM network. Since a public net- work generally involves several (or many) switches the routing becomes very important compo- nent of the NNI signaling. NNI signaling has two major standards: IISP (Integrated Interswitch Signaling Protocol) and PNNI (Private Network-to-Network Interface). IISP is a simple signaling protocol which uses static routing and is designed for small private ATM networks. PNNI is a signaling protocol that uses very elaborate dynamic routing algorithms which can easily handle small to large ATM networks which can have hundreds, thousands and even tens of thousands of ATM switches.

Q.3. Explain channel allocation problem and its solution algorithm in detail. Provide an example to illustrate the problem and its solution. **(12.5)**

Ans. In any broadcast network, the key issue is how to determine who gets to use the channel when there is competition for it. The protocols used to determine who goes next on a multi-access channel belong to a sub-layer of the data link layer called the MAC (Medium Access Control) sub-layer.

The Channel Allocation Problem is how to allocate a single broadcast channel among competing users.

Static channel Allocation: The most typical way of allocating a single channel among multiple competing users is Frequency Division Multiplexing (FDM). If the number of users are N, the banduidth is divided into N equal-sized portions. Each user is assigned one portion. If the number of users are small and constant, FDM is a simple and efficient allocation mechanism.

A telephone trunk can be a simple example of this type. However, when the number of senders is not small and constant or the traffic is heavy. FDM presents some problems. If the spectrum is divided into N regions the number of users currently interested in communicating is less than *N* a large piece of valuable spectrum will be wasted.

And due to this problem. If more than N users want to communicate, some of them will be denied permission for lack of bandwidth.The main reason for lack of bandwidth is that some of the users who have been assigned a frequency band hardly ever transmit or receive anything. So. dividing a single channel into static sub channels is quiet inefficient.The poor performance of static FDM can easily be seen from a simple queuing theory calculation. If the mean time delay is T, for a channel of capacity C bps, with an arrival rate of lambda frames/sec, each frame having a length drawn from an exponential probability density function with mean *i/i/^* bits/frame. With these parameters the arrival rate is lambda frames/sec and the service rate is ^C frames/sec.

From queuing theory. T = i (^C-lambda) For example, if C is 100 Mbps, The mean frame length, is 10,000 bits. and the frame arrival rate, lambda, is 5000 frames/sec, then T = 200 sec.

Dynamic Channel Allocation : Unlike the static channel,dynamic channel allocation is efficient and is used in areas where the traffic is nonuniform and heavy. Five main assumptions must be considered in dynamic channel allocation.

1. Station Model: Stations are also called terminals. The number of independent stations are N, with independent constant arrival rates lambda, and probability of a framé being generated in a time interval of (delta t) is (delta t x lambda). Once a frame has been generated the station does nothing until the frame has successfully been transmitted.

2. Single Channel Assumption: From hardware point of view, all stations are equal. A single channel is available for communication on which all stations can transmit on it and all can receive from it.

3. Collision Assumption: If two frames are transmitted simultaneously, they will collide resulting in a false signal. Each station has the ability to detect collision and it must be kept in mind that collided frame must be retransmitted later.

4. Time Management:

Continuous Time: Frame transmission can begin at any instant as there is no master clock diving time into discrete intervals.

Slotted Time: Frame transmission start at the beginning of the time slots. A slot may contain 0,1. or more frame corresponding to an idle, successful or collision transmission respectively.

5. Sensing of Channel:

Carrier Sense: A channel can be sensed by station before trying to use it. If a station senses the channel as busy, no station will attempt to use it, unitl it gols idle.

No Carrier Sense: Station connot sense the channel before trying to use it. First the transmit and the came to where the channels is busy or idle

Q. 4. (*a*) Discuss the various issues in designing data link layer in detail. **(6)**

Ans. The data link layer has a number of specific functions to carry out. These functionsinclude providing a well-defined service interface to the network layer, determining how the bits of the physical layer are grouped into frames, dealing with transmission errors and regulating the flow or frames so that slow receivers are not swaped by fast senders. In the following sections we will examine each of these issues in turn.

There are the following issues:

(*a*) Services Provided to the Network Layer

(*b*) Framing

drnotes.xyz

(c) Error Control

(d) Flow Control

Q.4. (b) Explain sliding window protocol in detail and using an example. (6.5)

Ans. Refer Q. 3. (a) First-Term Examomation 2016.

Q.5. Explain the following cables in detail. (4)

Q. 5. (a) Baseband Coaxial Cable.

Ans. A baseband coaxial cable, commonly called an Ethernet cable, is a 50-ohm cable that transmits an unmodulated digital signal. Transmission in baseband cables is bidirectional, meaning a signal inserted at any point propagates in both directions. Baseband cables are commonly used in local area networks. Broadband coaxial cables are 75-ohm cables that transmit modulated, analog signals. Broadband cables are unidirectional, but can compensate for this by dividing into different channels.

Baseband cables are not capable of transmitting more than one signal at a time, and the transmissions are restricted to data and voice. Additionally, baseband cables exceeding 0.62 mile in length experience a steady drop in transmission rates unless an amplifier is used. However, advantages of using baseband cable are the associated low cost and the ease of use. Another benefit of using baseband cable is the absence of a modem because the cable's signals are already digital.

A baseband coaxial cable transmits a single signal at a time at very high speed. A baseband cable is mainly used for **LANs**. Baseband coaxial cable supports frequency range of a-4kHz and are used for digital signaling. Baseband coaxial cables are 50 ohm cables used for 'digital transmission'. For 1Km cables the bandwidth is 1-2 Gbps. Longer cables can be used with low data rates or periodic amplifiers. (4)

Q.5.(b) Broadband coaxial cable

Ans. Refer Q4(b) of First Term Exam 2017 (Page No.: 12-2018) (4.5)

Q.5. (c) Fiber cable

Ans. Working of fiber optics: Light travels down a fiber-optic cable by bouncing repeatedly off the walls. Each tiny photon (particle of light) bounces down the pipe like a bobsleigh going down an ice run. Now you might expect a beam of light, traveling in a clear glass pipe, simply to leak out of the edges. But if light hits glass at a shallow angle (less than 42 degrees), it reflects back in again—as though the glass were really a mirror. This phenomenon is called total internal reflection. It's one of the things that keeps light inside the pipe.

The other thing that keeps light in the pipe is the structure of the cable, which is made up of two separate parts. The main part of the cable—in the middle—is called the core and that's the bit the light travels through. Wrapped around the outside of the core is another layer of glass called the cladding. The cladding's job is to keep the signal inside the core. It can do this because it is made of a different type of glass to the core. (More technically, the cladding has a higher refractive index than the core. Light travels slower in the cladding than in the core. Any light that tries to leak into *the* cladding tends to bend back inside the core.

Advantages of fiber optics:

1. Extremely high bandwidth - No other cable-based data transmission medium offers the bandwidth that fiber does.

2. Easy to accomodate increasing bandwidth - Using many of the recent generations of fiber optic cabling, new equipment can be added to the inert fiber cable that can provide vastly expanded capacity over the originally laid fiber. DWDM, (Dense Wavelength Division Multiplexing, lends fiber optic cabling the ability to turn

various wavelengths of light traveling down the fiber on and off at will. These two characteristics of fiber cable enable dynamic network bandwidth provisioning to provide for data traffic spikes and lulls.

3. Resistance to electromagnetic interference - Fiber has a very low rate of bit (error (10 EXP-13), as a result of fiber being so resistant to electromagnetic interference Fiber-optic transmission are virtually noise free.

4. Early detection of cable damage and secure transmissions - Fiber provides an extremely secure transmission medium, as there is no way to detect the data being transmitted by "listening in" to the electromagnetic energy "leaking" through the cable as is possible with traditional, electron-based transmissions. By constantly monitoring an optical network and by carefully measuring the time it takes light to reflect down the fiber, splices in the cable can be easily detected.

Disadvantages of Fiber Optics:

1. Installation costs, while dropping, are still high - Despite the fact that fiber installation costs are dropping by as much as 60% a year, installing fiber optic cabling is still relatively costly. As installation costs decrease, fiber is expanding beyond its original realm and major application in the carrier backbone and is moving into local loop, and through technologies such as FTTx (Fiber To The Home, Premises, etc), and PONs (Passive Optical networks), enabling subscriber and end user broadband access.

2. Special test equipment is often required - The test equipment typically and traditionally used for conventional electron-based networking is of no use in a fiber optic network. Equipment such as an OTDR (Optical Time Domain Reflectometer) is required, and expensive, specialized optical test equipment such as optical probes are needed at most fiber endpoints and connection nexuses in order to properly provide testing of optical fiber.

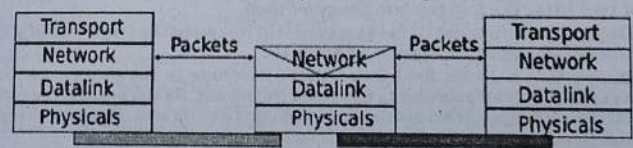
3. Susceptibility to physical damage - Fiber is a small and compact cable, and it is highly susceptible to becoming cut or damaged during installation or construction activities. Because railroads often provide rights-of-way for fiber optic installation, railroad car derailments pose a significant cable damage threat, and these events can disrupt service to large groups of people, as fiber optic cables can provide tremendous data transmission capabilities. Because of this, when fiber optic cabling is chosen as the transmission medium, it is necessary to address restoration, backup and survivability.

4. Wildlife damage to fiber optic cables - Many birds, for example, find the Kevlar reinforcing material of fiber cable jackets particularly appealing as nesting material, so they peck at the fiber cable jackets to utilize bits of that material.

Q.6. Explain the network layer in the internet and the network layer in ATM networks in detail. Differentiate in between these two: (12.5)

Ans. The network layer in the internet

The main objective of the network layer is to allow endsystems, connected to different networks, to exchange information through intermediate systems called ***router***. The unit of information in the network layer is called a ***packet***.



dotnotes.xyz

Network Layer Functions

Some of the specific jobs normally performed by the network layer include:

• **Logical Addressing:** Every device that communicates over a network has associated with it a logical address, sometimes called a layer three address. For example, on the Internet, the Internet Protocol (IP) is the network layer protocol and every machine has an IP address.

• **Routing:** Moving data across a series of interconnected networks is probably the defining function of the network layer.

• **Datagram Encapsulation:** The network layer normally encapsulates messages received from higher layers by placing them into *datagrams* (also called packets) with a network layer header.

• **Fragmentation and Reassembly:** The network layer must send messages down to the data link layer for transmission. Some data link layer technologies have limits on the length of any message that can be sent.

• **Error Handling and Diagnostics:** Special protocols are used at the network layer to allow devices that are logically connected, or that are trying to route traffic, to exchange information about the status of hosts on the network or the devices themselves.

Packet Structure

Version Number (4 bits)	Header Length (4 bits)	Type of Service (8 bits)	Total Length (16 bits)	
ID (16 bits)			Flags (3bits)	Flag Offset (13 bits)
Time to Live (8 bits)		Protocol (8 bits)	Header checksum (16 bits)	
Source (32 bits)				
Destination (32 bits)				
Options				

• **Version Number :** The current version is Version 4 (0100).

• **Header Length :** Header will always be a multiple of 4bytes and so we can have a maximum length of the field as 15, so the maximum size of the header is 60 bytes (20 bytes are mandatory).

• **Type of Service (ToS) :** The structure is :

First three bits : They specify the precedences i.e. the priority of the packets.

Next three bits :

• D bit - D stands for delay.

• T bit - T stands for throughput.

• R bit - R stands for reliability.

Last two bits: The last two bits are never used.

ID Field : The source and ID field together will represent the fragments of a unique packet. So each fragment will have a different ID.

• **Offset :** It is a 13 bit field that represents where in the packet, the current fragment starts. Each bit represents 8 bytes of the packet. So the packet size can be at most 64 kB. Every fragment except the last one must have its size in bytes as a multiple of 8 in order to ensure compliance with this structure.

• **Flags :** It has three bits -

• M bit : If M is one, then there are more fragments on the way and if M is 0, then it is the last fragment.

• DF bit : If this bit is sent to 1, then we should not fragment such a packet.

• Reserved bit : This bit is not used.

• **Total Length :** It includes the IP header and everything that comes after it.

• **Time To Live (TTL) :** Using this field, we can set the time within which the packet should be delivered or else destroyed.

• **Protocol :** This specifies the module to which we should hand over the packet (UDP or TCP). It is the next encapsulated protocol.

ATM networks:

The *asynchronous transfer mode* (ATM) protocol architecture is designed to support the transfer of data with a range of guarantees for quality of service. The user data is divided into small, fixed-length packets, called cells, and transported over virtual connections. ATM operates over high data rate physical circuits, and the simple structure of ATM cells allows switching to be performed in hardware, which improves the speed and efficiency of ATM switches.

Figure 1 shows the reference model for ATM. The first thing to notice is that, as well as layers, the model has planes. The functions for transferring user data are located in the user plane; the functions associated with the control of connections are located in the control plane; and the co-ordination functions associated with the layers and planes are located in the management planes.

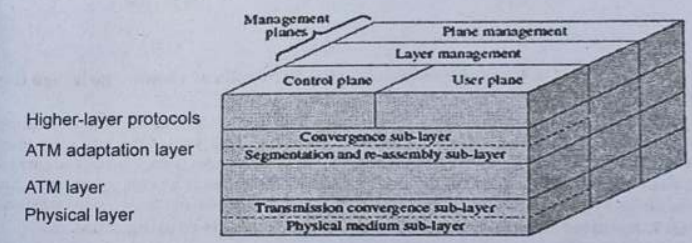


Fig. 1: ATM reference model

The three-dimensional representation of the ATM protocol architecture is intended to portray the relationship between the different types of protocol. The horizontal layers indicate the encapsulation of protocols through levels of abstraction as one layer is built on top of another, whereas the vertical planes indicate the functions that require co-ordination of the actions taken by different layers. An advantage of dividing the functions into control and user planes is that it introduces a degree of independence in the definition of the functions: the protocols for transferring user data (user plane) are separated from the protocols for controlling connections (control plane).

The protocols in the ATM layer provide communication between ATM switches while the protocols in the ATM adaptation layer (AAL) operate end-to-end between users. This is illustrated in the example ATM network in Fig.b.

dotnotes.xyz

Two types of interface are identified in Fig. 1. One between the users and the network (user-network interface), and the other between the nodes (switches) within the network (network-node interface).

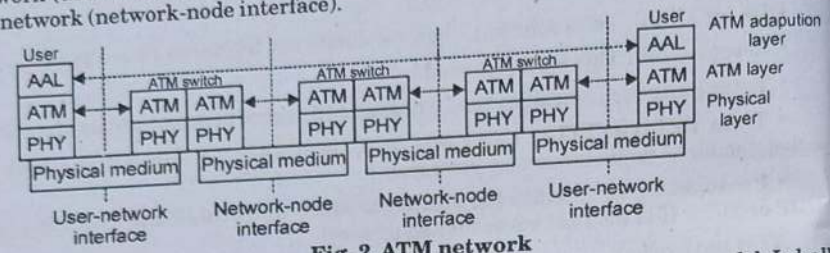


Fig. 2. ATM network

Before describing the functions of the three layers in the ATM reference model, I shall briefly describe the format of ATM cells. Fig. 3 shows the two basic types of cell.

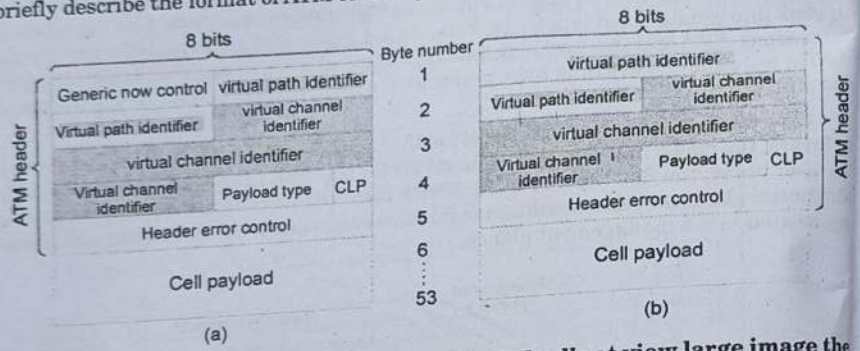


Fig. 3 (a) ATM cells at the user-network-node (b) ATM cells at view large image the interface

Each ATM cell consists of 53 bytes: the header is five bytes long and the remaining 48 bytes (the cell payload) carry information from higher layers. The only difference between the two types of ATM cell is that the cells at the user-network interface carry a data field for the flow control of data from users. This means that only eight bits are available for virtual path identifiers, rather than 12 bits at the network-node interface.

Q. 7. A router has the following (CIDR) entries in its routing table.

Address/Mask	Next Hop
135.46.56.0/22	Interface 0
135.46.60.0/22	Interface 1
135.53.40.0/22	Router 1
Default	Router 2

For each of the following IP addresses, what does the router do if a packet with that address arrives? (12.5

(a) 135.46.63.10
(b) 135.46.57.14
(c) 135.46.52.2
(d) 192.53.40.7
(e) 192.53.56.7

Ans.

A route has the following (CIDR) entries in its routing table:

Address/ mask	Next hop
135.46.56.0/22	Interface 0
135.46.60.0/22	Interface 1
192.53.40.0/23	Router 1
Default	Router 2

For each of the following IP address,

(a) 135.46.63.10		10000111 00101110 00111111 00001010
135.46.63.10		11111111 11111111 11111100 00000000
255.255.252.0	AND	AND
135.46.60.0		10000111 00101110 00111100 0000000

It matches entry with 135.46.60.0/22, and no other matches found, so it's forwarded to interface 1.

(b) 135.46.57.14		10000111 00101110 00111001 00001110
135.46.57.14		11111111 11111111 11111100 00000000
255.255.252.0	AND	AND
135.46.60.0		10000111 00101110 00111100 00000000

It matches entry with 135.46.56.0/22, and no other matches found, so its forwarded to interface 0.

(c) 135.46.52.2		10000111 00101110 00110100 00000010
135.46.52.2		11111111 11111111 11111100 00000000
255.255.252.0	AND	AND
135.46.52.0		10000111 00101110 00110100 00000000

It doesn't matches any entry, so it's forwarded to the one defined in default entry, namely, Router 2.

(d) 192.53.40.7		11000000 00110101 00101000 00000111
192.53.40.7		11111111 11111111 11111110 00000000
255.255.254.0	AND	AND
192.53.40.0		11000000 00110101 00101000 00000000

It matches entry with 192.53.40.0/23, and no other matches found, so it's forwarded to Router 1.

(e) 192.53.56.7		11000000 00110101 00111000 00000111
192.53.56.7		11111111 11111111 11111110 00000000
255.255.254.0	AND	AND
192.53.56.0		11000000 00110101 00111000 00000000

dotnotes.xyz

It doesn't matches any entry, so it's forwarded to the one defined in default entry, namely, Router 2.

Q.8. Write short notes on any two of the following: **(12.5)**

Q.8. (a) Domain Name Registration and Registrars

Ans. Domains Name Registration: A domain name regisby is a databas of all domain name registered in a top-level domain. A registy operator, also called a Network Information Center (NIC) is a part of the Domain Name System (DNS) of the Internet that keeps the database of domain names.

Domain Name Registrars: Name for websites have to be registered online meaning that there are websites which at are also compaines that have been approved by a responsible organization called ICANN (Internet Corporation for Assigned Names & Numbers) ICANN accredits domain name regisbars. A register is a company which is also a website where domain name are registered.

Q. 8. (b) Satellite networks.

Ans. Data networking is one of the hottest applications for today's advanced satellite services. There are two main markets:

- Commercial-mostly consisting of Corporate & Government users
- Consumer-mostly consisting of services to homes and small businesses

Both markets are growing rapidly and both rely on the use of small satellite dishes at the receive site, often less than one meter in diameter, called "very small aperture terminals" or VSAT's.

Satellites have served the commercial data market since the 1980s when large numbers of VSATs were deployed for "point of sale" transactions at retail business locations. Satellites have more recently begun to serve the consumer market. Analysts estimate that today there are about two million commercial VSATs and another one million for consumer services deployed around the world. Most of these are used for Internet Protocol (IP) broadband services.

The rapid growth of satellite broadband is primarily due to the improved price and performance of today's satellite-based solutions. Experienced operators like Telesat can now seamlessly integrate any number of satellite VSAT sites into a commercial customer's existing network with high quality standards backed by strong service level agreements. This enables remote users to have a high quality experience for a host of IP applications.

Other key reasons for the rapid growth of VSAT networking:

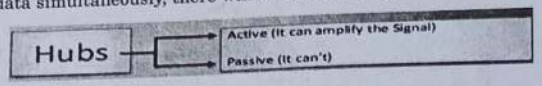
- Satellites offer global, regional and/or local reach
- Satellites offer an increasing range of solutions, from traditional SCPC (single channel per carrier) services to IP-based VoIP and data networking
- Satellites offer direct, last mile connectivity to regions with little existing infrastructure, at a fraction of the cost of installing and maintaining terrestrial solutions
- Satellite networks can be implemented quickly, sometimes within hours, when a disaster strikes, providing "instant infrastructure"

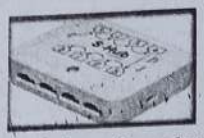
Q.8. (c) Network devices.

Ans. Repeater

A repeater is a device similar to the Hub, but has additional features. It also works in the Physical layer. The repeaters are used in places where amplification of input signal is necessary. But, the kind of amplification done by the repeater is different from the regular amplification by amplifiers.

Hence, the repeater regenerates the faded signal. In addition, it has all the features of a Hub. One common problem between the repeaters and the Hubs are that only one transmission can take place on the network at a particular time. If multiple devices transmit data simultaneously, there will be data collision.





- **Hubs:** There are two types of hubs: active and passive.
- Passive hubs simply connect all ports together electrically and are usually not powered.
- Active hubs use electronics to amplify and clean up the signal before it is broadcast to the other ports.
- Hubs are devices used to link several computers together.
- They repeat any signal that comes in on one port and copy it to the other ports (a process that is also called broadcasting).
- It works in physical Layer of OSI Model.
- **Bridges**

> They join similar topologies and are used to divide network segments.

> It can filter traffic on the basis of MAC address.

> If it is aware of the destination address, it is able to forward packets; otherwise a bridge will forward the packets to all segments. They are more intelligent than repeaters but are unable to move data across multiple networks simultaneously.

> Unlike repeaters, bridges *can* filter out noise.

> Works in Data link Layer of OSI Model.

> Multiple collision Domain but single Broadcast Domain.

> The main disadvantage to bridges is that they can't connect dissimilar network types or perform intelligent path selection. For that function, you would need a router.

- **Switches:**

> A network switch is a computer networking device that connects network segments.

> Populates MAC address table on the basis of source MAC address of a Frame.

> Network switches are capable of inspecting data frames as they are received, determining the source and destination device of that frame, and forwarding it appropriately.

> Data Link Layer or Layer 2 Device.

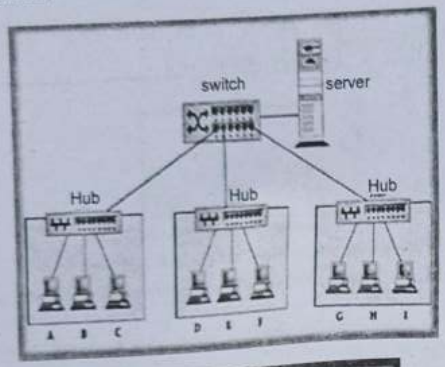
> Multiple collision Domain but single Broadcast Domain.

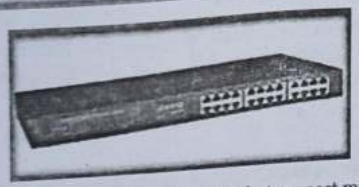
> A vital difference between a **hub** and a **switch** is that all the nodes connected to a hub share the bandwidth among themselves, while a device connected to a switch port has the **full bandwidth** all to itself.

dotnotes.xyz

For example, if 10 nodes are communicating using a hub on a 10-Mbps network, then each node may only get a portion of the 10 Mbps if other nodes on the hub want to communicate as well.

But with a switch, each node could possibly communicate at the full 10 Mbps.





Router: Routers are highly intelligent devices that connect multiple network types and determine the best path for sending data.

Routers are normally used to connect one LAN to another.

These devices examine incoming packets to determine the destination address of the data. It then examines its internal routing table to choose the best path for the packet through the network, and switches them to the proper outgoing port.

However, they are slower than bridges because they are more intelligent devices; as such, they analyze every packet, causing packet-forwarding delays. Because of this intelligence, they are also more expensive.

Routers are OSI network layer 3 devices.

Typically, when a WAN is set up, there will be at least two routers used.

FIRST TERM EXAMINATION [FEB. 2017]
SIXTH SEMESTER [B.TECH]
COMPUTER NETWORK [ETCS–306]

Time : 1.30 Hrs. **M.M. : 30**

Note: *Q.No. 1 is compulsory and attempt any two more questions from the remaining-*

Q.1. (a) Explain the difference between an Internet draft and a proposed standard. **(2)**

Ans. Internet draft: Internet Draft is a series of working documents published by the IETF. Typically, they are drafts for RFCs, but may be other works in progress not intended for publication as RFCs. During the development of a specification, draft versions of the document are made available for informal review and comment by placing them in the IETF's Internet-Drafts directory. This makes an evolving working document readily available to a wide audience, facilitating the process of review and revision. Internet-Drafts have no formal status, and are subject to change or removal at any time; therefore they should not be cited or quoted in any formal document.

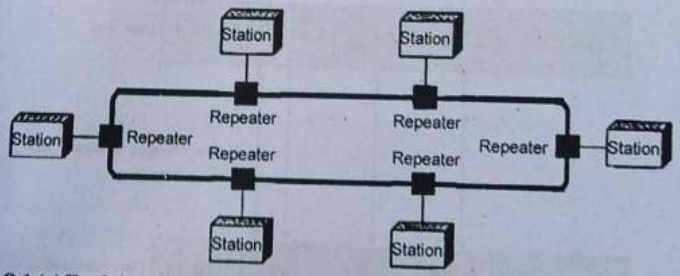
Proposed Standard: The entry-level maturity for the standards track is "Proposed Standard". A specific action by the IESG is required to move a specification onto the standards track at the "Proposed Standard" level.

A Proposed Standard specification is generally stable, has resolved known design choices, is believed to be well-understood, has received significant community review, and appears to enjoy enough community interest to be considered valuable.

Usually, neither implementation nor operational experience is required for the designation of a specification as a Proposed Standard. However, such experience is highly desirable, and will usually represent a strong argument in favour of a Proposed Standard designation.

Q.1.(b) In the ring topology what happens if one of the station is unplugged? **(2)**

Ans. In a ring topology, unplugging one station interrupts the ring. However, most ring networks use a mechanism that bypasses the station; the ring can continue its operation.



Q.1.(c) Explain why collision is an issue in random access protocols but not n controlled access protocols. **(2)**

Ans. In random access methods, there is no access control (as there is in controlled ccess methods) and there is no predefined channel (as in channelization). Each station an transmit when it desires. This liberty may create collision.

dotnotes.xyz

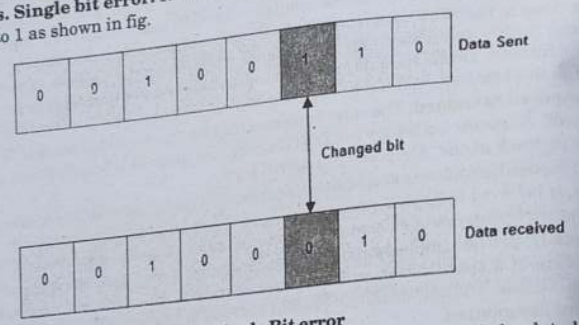
In controlled access methods, the stations consult one another to find which station has the right to send. A station cannot send unless it has been authorized by other stations.

In random access methods, there is no access control (as there is in controlled access methods) and there is no predefined channels (as in channelization). Each station can transmit when it desires.

In a random access method, the whole available bandwidth belongs to the station that wins the contention; the other stations needs to wait. In a channelization method the available bandwidth is divided between the stations. If a station does not have data to send, the allocated channel remains idle.

Q.1.(d) How does a single bit error differ from a burst error? (2

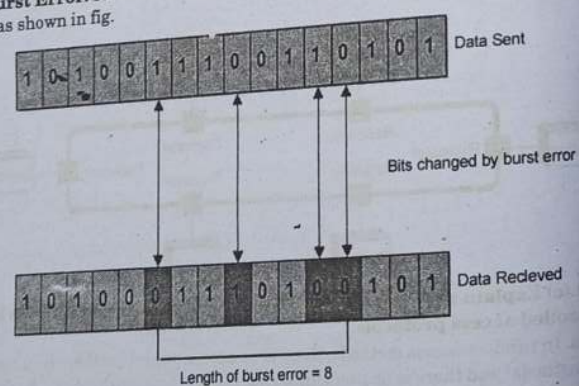
Ans. Single bit error: It means only one bit of data unit is changed from 1 to 0 or from 0 to 1 as shown in fig.



Single Bit error

Single bit error can happen in parallel transmission where all the data bits are transmitted using separate wires. Single bit errors are the least likely type of error in serial transmission.

Burst Error: It means two or more bits in data unit are changed from 1 to 0 from 0 to 1 as shown in fig.



Burst error

In burst error, it is not necessary that only consecutive bits are changed. The length of burst error is measured from first changed bit to last changed bit. As shown in fig. length of burst error is 8, although some bits are unchanged in between. Burst error is most likely to occur in a serial transmission.

Q.1.(e) Describe the need for switching. (2)

Ans. Switching is process to forward packets coming in from one port to a port leading towards the destination. When data comes on a port it is called ingress, and when data leaves a port or goes out it is called egress. A communication system may include number of switches and nodes. At broad level, switching can be divided into two major categories:

- **Connectionless:** The data is forwarded on behalf of forwarding tables. No previous handshaking is required and acknowledgements are optional.
- **Connection Oriented:** Before switching data to be forwarded to destination, there is a need to pre-establish circuit along the path between both endpoints. Data is then forwarded on that circuit. After the transfer is completed, circuits can be kept for future use or can be turned down immediately.

Q.2.(a) Discuss the functions of all layers of OSI model. (4)

Ans. 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:

dotnotes.xyz

— What physical medium options can be used

— How many volts/db should be used to represent a given signal state, using a giv physical medium

Data Link Layer: The data link layer provides error-free transfer of data fram from one node to another over the physical layer, allowing layers above it to assum virtually error-free transmission over the link. To do this, the data link layer provide

- Link establishment and termination: establishes and terminates the logical lin between two nodes.
- Frame traffic control: tells the transmitting node to "back-off" when no fram buffers are available.
- Frame sequencing: transmits/receives frames sequentially.
- Frame acknowledgment: provides/expects frame acknowledgments. Detects an recovers from errors that occur in the physical layer by retransmitting non-acknowledge 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: The network layer controls the operation of the subnet, decidin which physical path the data should take based on network conditions, priority of servic and other factors. It provides:

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

Communications Subnet: The network layer software must build headers so th the network layer software residing in the subnet intermediate systems can recogni 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 da transmission and intermediate switching technologies used to connect systems. establishes, maintains and terminates connections across the intervenin communications facility (one or several intermediate systems in the communicati subnet).

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

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

dotnotes.xyz

- Remote file acces
- Remote printer access
- Inter-process communication
- Network managment
- Directory services
- Electronic messaging (such as mail)

Q.2. (b) What is transmission medium? Discuss various propagation modes in the fiber optics. **(4)**

Ans. The path through which data is transmitted from one place to another in called channel. It is also known as communication mdedia or transmission media. These are different types of transmittion media

(i) Guided media

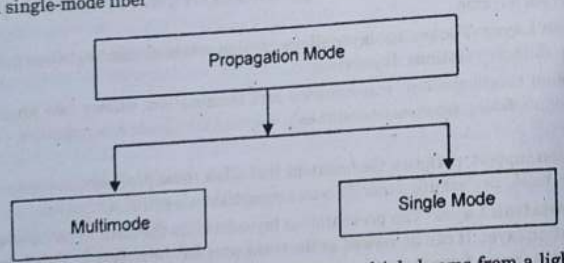
(ii) Unguided media

Guided media

In guided media communication device are directly connected with each other by using some physical media like wires. It also called bounded media.

Unguided Media: In unguided media communication devices communicates with each other through air or space using broadcast radio signals microwave signals and infrared signals unguided media is used where it is impossible to install cable data can be transfer all over the world using media it is also called unguided media.

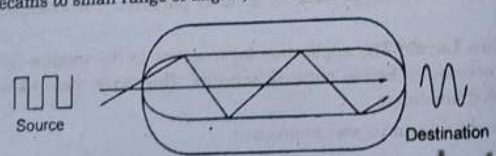
Propagation Mode: There are two different modes for propagating light along optical channels: multimode and single mode. There are two basic types of fiber: multimode fiber and single-mode fiber



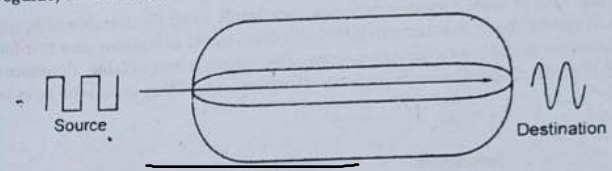
Multimode: Multimode is so named because multiple beams from a light sourc move through the core in different paths. Multimode cable is made of glass fibers, with common diameters in the 50-100 micron range for the light carry component (the mos common size is 62.5).

Multimode fiber gives you high bandwidth at high speeds over medium distance Light waves are dispersed into numerous paths, or modes, as they travel through th cable's core typically 850 or 1300 nm. Typical multimode fiber core diameters are 50 62.5, and 100 micrometers.

Single Mode: Single mode uses step-index fiber and a highly focused source of ligh that limits becams to small range of angles, all close to the horizontal.



Single Mode cable is a single stand of glass fiber with a diameter of 8.3 to 10 microns that has one mode of transmission. Single Mode Fiber with a relatively narrow diameter, through which only one mode will propagate typically 1310 or 1550 nm. Carries higher bandwidth than multimode fiber, but requires a light source with a narrow spectral width. Single-mode fiber is also called as mono-mode optical fiber, single-mode optical waveguide, unimode fiber.



Q.2.(c) Compare the throughput of a pure ALOHA network with a slotted ALOHA network. **(2)**

Ans. Throughput of pure A LOHA channel

Let G be the average number of frames generated by the system during one frame transmission time. Then it can be proved that the average no of successful transmissions for pure ALOHA is $S = G \times e^{-2G}$. The maximum throughput S_{max} is 0.184, for G = 1/2. i.e. if one - half a frame is generated during one one frame transmission time, then 18.4 percent of these frames reach their destination successfully. This is an expected result because : the vulnerable time is 2 times the frame transmission time. Therefore, if a station generates only one frame in this vulnerable time, the frame will reach its destination successfully.

The throughput for pure ALOHA is $S = G \times e^{-2G}$

The maximum throughput $S_{max} = 0.184$ when $G = (1/2)$

Throughput of slotted ALOHA channel

The average number of successful transmissions for slotted ALOHA is $S = G \times e^{-G}$. The maximum throughput S_{max} is 0.368, when G = 1. In other words, if a frame is generated during one frame transmission time, then 36.8 percent of these frames reach their destination successfully. This result can be expected because the vulnerable time is equal to the frame transmission time. Therefore, if a station generates only one frame in this vulnerable-time, the frame will reach its destination successfully

The throughput for slotted ALOHA is $S = G \times e^{-G}$

The maximum throughput $S_{max} = 0.368$ when G = 1

Q.3.(a) Why channel allocation is a difficult task? Explain the random access method that tries to avoid collision. **(5)**

Ans. Refer Q.3 End term june – 2016.

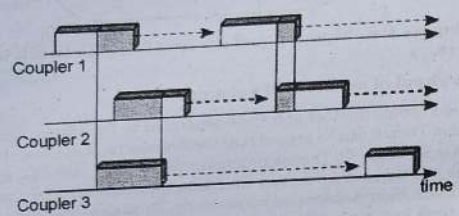
Random Access, which is to issue a completely random time, relies on the Aloha method.

In this method, when a coupler has information to transmit, it sends it without worry about other users. If there is a collision, that is to say superposition of two signals or more users, the signals become indecipherable and are lost. They are subsequently

dotnotes.xyz

transmitted, as shown in Figure, in which the couplers 1, 2 and 3 collide. The coupler 1 transmits its field first because he shot the smallest timer. Then, the module 2 emits and its signals collide with the coupler 1. Both derive a random time of retransmission. The coupler 3 is listening while the couplers 1 and 2 are silent, so that the frame of the coupler 3 passes successfully. Technical aloha is the origin of all the random access methods.

The flow rate of such a system becomes very small when the number of couplers increases. It can be shown mathematically that if the number of stations goes to infinity the flow becomes zero. From a certain moment, the system is more stable. To reduce the likelihood of conflict between users, various improvements of this technique have been proposed.



Operating Principle of Pure Aloha

Slotted aloha, aloha or sliced

Improved technical aloha was to cut the time into time slots, or slots, and to authorize the issuance of frames that slice first, the transmission time of a frame requiring exactly a slice of time. In this way, there is no collision if a single frame transmitted at the beginning of slice. However, if several frames start transmitting in the beginning of slice, the frames emissions are superimposed along the slot. In the latter case, there has retransmission after a random time.

This method improves the throughput during the start-up period but remains unstable. In addition, there is an additional cost from a complication of the devices, since all emissions must be synchronized.

Q.3.(b) A bit stream 10011101 is transmitted using the standard CRC method. The generator polynomial is $x^3 + 1$. Show the actual bit string being transmitted. Suppose a bit is inverted during transmission. Show how this error is detected at the receivers end. **(5)**

Ans. Our generator $G(x) = x^3 + 1$ encoded as 1001. Because the generator polynomial is of the degree three we append three zeros to the lower end of the frame to be transmitted. Hence after appending the 3 zeros the bit stream is 10011101000. On dividing the message by generator after appending three zeros to the frame we get a remainder of 100. We do modulo 2 subtraction thereafter of the remainder from the bit stream with the three zeros appended. The actual frame transmitted is 10011101100. See below.


```
          1 0 0 0 1 1 0 0
1001 | 1 0 0 1 1 1 0 1 0 0 0
       1 0 0 1
         0 0 0 1
         0 0 0 0
           0 0 1 1
           0 0 0 0
             0 1 1 0
             0 0 0 0
               1 1 0 1
               1 0 0 1
                1 0 0 0
                1 0 0 1
                 0 0 1 0
                 0 0 0 0
                  0 1 0 0
                  0 0 0 0
                    1 0 0 (remainder)
```

Actual frame transmitted: 10011101000–100=10011101100 (modulo 2 subtraction)

Now suppose the third bit from the left is garbled and the frame is received as 10111101100. Hence on dividing this by the polynomial generator we get a remainder of 100 which shows that an error has occured. Had the received frame been error free we would have got a remainder of zero. See below.

```
          1 0 1 0 1 0 0 0
1001 | 1 0 1 1 1 1 0 1 0 0 0
       1 0 0 1
         0 1 0 1
         0 0 0 0
           1 0 1 1
           1 0 0 1
             0 1 0 0
             0 0 0 0
               1 0 0 1
               1 0 0 1
                 0 0 0 1
                 0 0 0 0
                  0 0 1 0
                  0 0 0 0
                    0 1 0 0
                    0 0 0 0
                      1 0 0 (remainder indicating error)
```

dotnotes.xyz

Q.4.(a) What are various design issues involved in the data link layer? Explain sliding window protocol. (4)

Ans. The data link layer has a number of specific functions to carry out. These functions include providing a well-defined service interface to the network layer, determining how the bits of the physical layer are grouped into frames, dealing with transmission errors and regulating the flow or frames so that slow receivers are not swapped by fast senders.

There are the following issues.

(a) Services Provided to the Netowrk Layer

(b) Framing

(c) Error Control

(d) Flow Control

Refer Q.3.(a) of First Term Examination 2016.

Q.4.(b). State and explain various frame types in HDLC. (3)

Ans. There are three types of HDLC frames :

- Information transfer frame (I-Frame)
- Supervisory frame (S-Frame)
- Unnumbered frame (U-Frame)

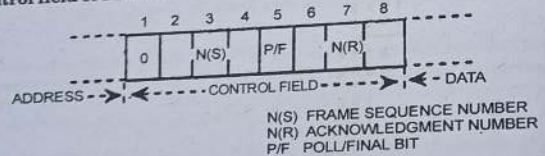
Information Transfer Frame (I-FRAME)

I-Frame is used for transporting user data. It also carries acknowledgement of the received frames. The control field of the I-Frame is as shown in Fig.. The first bit is 0 which identifies the frame as an I-Frame. The next three bits are the sequence number N(S) of the frame.

The fifth is Poll/Final (P/F) bit.

The last three bits are the sequence number N(R) of the acknowledgement (RR) which is piggy backed on the I-Frame.

Control field of I-frame

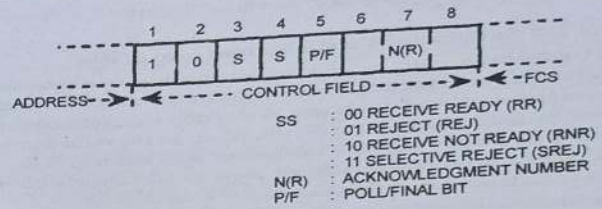


Supervisory Frame (S-FRAME)

S-Frame does not have data field and is used to carry only acknowledgements, requests for retransmission, etc. It is identified by the first two bits of the control field. These two bits are 10 in an S-Frame. The next two bits (SS) are used to indicate four supervisory states. Receive Ready (RR), Receive Not Ready (RNR), Reject (REJ) and Selective Reject (SREJ).

The fifth bit is Poll/Final bit. The last three bits are the sequence number associated with the supervisory states RR, RNR, REJ and SREJ indicated in the SS-Bits of the control field. Note that an acknowledgement (RR) can be sent either on a supervisory frame or piggybacked on an I-Frame as mentioned earlier. On the other hand RNR, REJ and SREJ are sent only through a supervisory frame.

Control field of S-frame

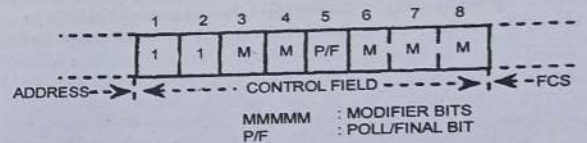


Unnumbered Frame (U-Frame)

The U-Frames do not have data field as S-Frames. They are used for link establishment, termination, mode setting and other control functions. Controls field of an unnumbered frame is shown.

The first two bits of the control field are 11 which identify an unnumbered frame. The fifth bit is Poll/Final bit. The rest five bits are called modifier bits. They specify the control function.

Cntrol Field of a U-Frame



Q.4.(c) If the 7-bit Hamming code word is received by a receiver is 1011011. Assuming the even parity state, find whether the received code word is correct or wrong. If wrong, locate the error and correct the code word. (3)

Ans.

d7	d6	d5	p4	d3	p2	p1
1	0	1	1	0	1	1

P4 = d5 d6 d7

= 1 => 1 0 1 p4 is 1

P2 = p2 d3 d6 d7

dotnotes.xyz

= 0 = >0 0 1 p2 = 0

P1 = p1 d3 p5 d7

= 1=> 011

P1 = 1.

P4 p2 p1 = 101 = 5

Error at 5th bit.

Corrected answer after changing the 5th bit will be : 1001011

Q.4.(d) List the characteristics of broad band coaxial cable.

Ans. Coaxial cables are the guided media that carnes the signal of higher frequency range compared to twisted pair cable. Coaxial cables are also called *coax*. (short form). Two types of coaxial cables are widely used: 50 ohm cable and 75 ohm cable. 50 ohm cable is used for digital transmission and 75 ohm cable is used for analog transmission. Due to the shield provided, this cable has excellent noise immunity. It has a large bandwidth and low losses. Co axial cables are easy to install. They are often installed either in a device to device daisy chain (Ethernet) or a star (ARC net).

A coaxial cable consists of many small cables in a protective cover. The cover shields the cable from physical dangers as well as from electromagnetic interference. Within the cover, the various cables are shielded from interference with one another. Coaxial cables are used in communication networks that require many simultaneous communication links. Each coaxial cable can provide more than 5000 links. It has a data rate of 10 Mbps which can be increased with the increase in diameter of the inner conductor. The specified maximum number of nodes on a thin net segment is 30 nodes and on a thick net it is 100 nodes.

Since broadband is used for large area, it requires amplifiers which are unidirectional. In dual band systems two identical cables run together, one used for outgoing data, one for incoming data. Different bandwidths are given for inbound and outbound cables. Eg: for 300MHz, 5-30MHz for inbound and 40-300MHz for outbound. There are two systems that use the bus LANs namelv 10 BASE 5 and 10 BASE 2

END TERM EXAMINATION [MAY-JUNE 2017]
SIXTH SEMESTER [B.TECH]
COMPUTER NETWORK [ETCS–306]

M.M. : 75

Time : 3 Hrs.

Note: *Q. No. 1 is compulsory. Attempt any five . Questions from the rest.*

Q.1. (a) How flow control is different from congesition control? **(3)**

Ans. Flow control means preventing the source from sending data that the sink will end up dropping because it runs out of buffer space. This is fairly easy with a sliding window protocol—just make sure the source's window is no larger than the free space in the sink's buffer. TCP does this by letting the sink advertise its free buffer space in the window field of the acks.

Congestion control means preventing (or trying to prevent) the source from sending data that will end up getting dropped by a router because its queue is full. This is more complicated, because packets from different sources travelling different paths can converge on the same queue.

Q.1.(b) Difference between bit rate and baud rate? Explain with example. **(3)**

Ans. Data rate *is* the capacity of a channel in bits per second. Bit rates measure the number of data bits (that is 0?s and l?s) transmitted in one second in a communication channel. A figure of 2400 bits per second means 2400 zeros or ones can be transmitted in one second, hence the abbreviation "bps." Individual characters (for example letters or numbers) that are also referred to as bytes are composed of several bits.

Baud rate represents the number of times the line condition (i.e., frequency, amplitude or phase) changes each second. Data rate = n bits × baud rate, where n is equal to the number of bits one signal represents. A baud rate is the number of times a signal in a communications channel changes state or varies. For example, a 2400 baud rate means that the channel can change states up to 2400 times per second. The term "change state" means that it can change from 0 to 1 or from 1 to 0 up to X (in this case, 2400) times per second. It also refers to the actual state of the connection, such as voltage, frequency, or phase level.

Q.1.(c) What is difference between Classfull addressing and Classless IP addressing? **(4)**

Ans. Classfull Addressing:

All IP addresses have a network and host portion. In classful addressing, the network portion ends on one of the separating dots in the address (on an octet boundary). Classful addressing divides an IP address into the Network and Host portions along octet boundaries.In the classful addressing system all the IP addresses that are available are divided into the five classes A,B,C,D and E, in which class A,B and C address are frequently used because class D is for Multicast and is rarely used and class E is reserved and is not currently used.

dotnotes.xyz

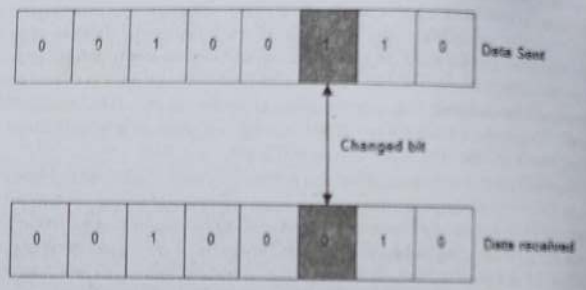
In controlled access methods, the stations consult one another to find which sta has the right to send. A station cannot send unless it has been authorized by ot stations.

In random access methods, there is no access control (as there is in contro access methods) and there is no predefined channels (as in channelization). Each sta can transmit when it desires.

In a random access method, the whole available bandwidth belongs to the sta that wins the contention; the other stations needs to wait. In a channelization meth the available bandwidth is divided between the stations. If a station does not ha data to send, the allocated channel remains idle.

Q.1.(d) How does a single bit error differ from a burst error?

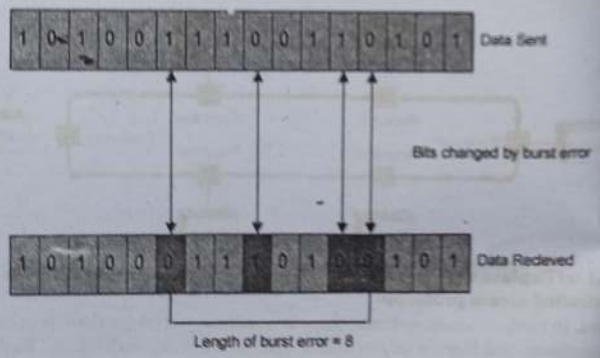
Ans. Single bit error: It means only one bit of data unit is changed from 1 to 0 from 0 to 1 as shown in fig.



Single Bit error

Single bit error can happen in parallel transmission where all the data bits transmitted using separate wires. Single bit errors are the least likely type of erro serial transmission.

Burst Error: It means two or more bits in data unit are changed from 1 to 0 fr 0 to 1 as shown in fig.



Burst error

In burst error, it is not necessary that only consecutive bits are changed. The length of burst error is measured from first changed bit to last changed bit. As shown in fig. length of burst error is 8, although some bits are unchanged in between. Burst error is most likely to occur in a serial transmission.

Q.1.(e) Describe the need for switching. **(2)**

Ans. Switching is process to forward packets coming in from one port to a port leading towards the destination. When data comes on a port it is called ingress, and when data leaves a port or goes out it is called egress. A communication system may include number of switches and nodes. At broad level, switching can be divided into two major categories:

- **Connectionless:** The data is forwarded on behalf of forwarding tables. No previous handshaking is required and acknowledgements are optional.
- **Connection Oriented:** Before switching data to be forwarded to destination, there is a need to pre-establish circuit along the path between both endpoints. Data is then forwarded on that circuit. After the transfer is completed, circuits can be kept for future use or can be turned down immediately.

Q.2.(a) Discuss the functions of all layers of OSI model. **(4)**

Ans. 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:

dotnotes.xyz

— What physical medium options can be used

— How many volts/db should be used to represent a given signal state, using a giv physical medium

Data Link Layer: The data link layer provides error-free transfer of data fram from one node to another over the physical layer, allowing layers above it to assum virtually error-free transmission over the link. To do this, the data link layer provide

• Link establishment and termination: establishes and terminates the logical lin between two nodes.

• Frame traffic control: tells the transmitting node to "back-off" when no fram buffers are available.

• Frame sequencing: transmits/receives frames sequentially.

• Frame acknowledgment: provides/expects frame acknowledgments. Detects an recovers from errors that occur in the physical layer by retransmitting non-acknowledge 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: The network layer controls the operation of the subnet, decidin which physical path the data should take based on network conditions, priority of servic and other factors. It provides:

• Routing: routes frames among networks.

• Subnet traffic control: routers (network layer intermediate systems) can instru a sending station to "throttle back" its frame transmission when the router's buffer fil up.

• Frame fragmentation: if it determines that a downstream router's maximu transmission unit (MTU) size is less than the frame size, a router can fragment a fram for transmission and re-assembly at the destination station.

• Logical-physical" address mapping: translates logical addresses, or names, in physical addresses.

• Subnet usage accounting: has accounting functions to keep track, of fram forwarded by subnet intermediate systems, to produce billing information.

Communications Subnet: The network layer software must build headers so th the network layer software residing in the subnet intermediate systems can recogni 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 dat transmission and intermediate switching technologies used to connect systems. establishes, maintains and terminates connections across the interveni communications facility (one or several intermediate systems in the communicati subnet).

In the network layer and the layers below, peer protocols exist between a node an its immediate neighbour, but the neighbor may be a node through which data is route not the destination station. The source and destination stations may be separated b 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.

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

dotnotes.xyz

- Remote file acces
- Remote printer access
- Inter-process communication
- Network managment
- Directory services
- Electronic messaging (such as mail)

Q.2. (b) What is transmission medium? Discuss various propagation modes in the fiber optics. **(4)**

Ans. The path through which data is transmitted from one place to another in called channel. It is also known as communication mdedia or transmission media. These are different types of transmittion media

(i) Guided media

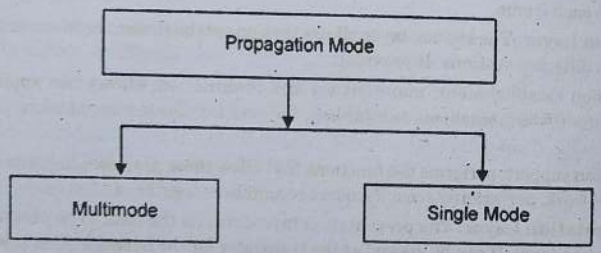
(ii) Unguided media

Guided media

In guided media communication device are directly connected with each other by using some physical media like wires. It also called bounded media.

Unguided Media: In unguided media communication devices communicates with each other through air or space using broadcast radio signals microwave signals and infrared signals unguided media is used where it is impossible to install cable data can be transfer all over the world using media it is also called unguided media.

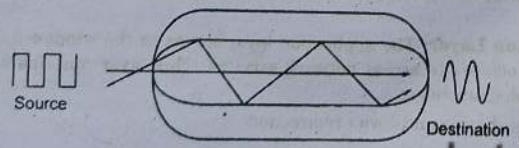
Propagation Mode: There are two different modes for propagating light along optical channels: multimode and single mode. There are two basic types of fiber: multimode fiber and single-mode fiber



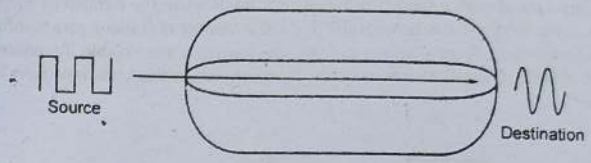
Multimode: Multimode is so named because multiple beams from a light source move through the core in different paths. Multimode cable is made of glass fibers, with common diameters in the 50-100 micron range for the light carry component (the most common size is 62.5).

Multimode fiber gives you high bandwidth at high speeds over medium distances. Light waves are dispersed into numerous paths, or modes, as they travel through the cable's core typically 850 or 1300 nm. Typical multimode fiber core diameters are 50, 62.5, and 100 micrometers.

Single Mode: Single mode uses step-index fiber and a highly focused source of fight that limits becams to small range of angles, all close to the horizontal.



Single Mode cable is a single stand of glass fiber with a diameter of 8.3 to 10 microns that has one mode of transmission. Single Mode Fiber with a relatively narrow diameter, through which only one mode will propagate typically 1310 or 1550 nm. Carries higher bandwidth than multimode fiber, but requires a light source with a narrow spectral width. Single-mode fiber is also called as mono-mode optical fiber, single-mode optical waveguide, unimode fiber.



Q.2.(c) Compare the throughput of a pure ALOHA network with a slotted ALOHA network. **(2)**

Ans. Throughput of pure A LOHA channel

Let G be the average number of frames generated by the system during one frame transmission time. Then it can be proved that the average no of successful transmissions for pure ALOHA is $S = G \times e^{-2G}$. The maximum throughput S_{max} is 0.184, for G = l/2. i.e. if one - half a frame is generated during one one frame transmission time, then 18.4 percent of these frames reach their destination successfully. This is an expected result because : the vulnerable time is 2 times the frame transmission time. Therefore, if a station generates only one frame in this vulnerable time, the frame will reach its destination successfully.

The throughput for pure ALOHA is $S = G \times e^{-2G}$

The maximum throughput $S_{max} = 0.184$ when G = (l/2)

Throughput of slotted ALOHA channel

The average number of successful transmissions for slotted ALOHA is $S = G \times e^{-G}$. The maximum throughput S_{max} is 0.368, when G = 1. In other words, if a frame is generated during one frame transmission time, then 36.8 percent of these frames reach their destination successfully. This result can be expected because the vulnerable time is equal to the frame transmission time. Therefore, if a station generates only one frame in this vulnerable-time, the frame will reach its destination successfully

The throughput for slotted ALOHA is $S = G \times e^{-G}$

The maximum throughput $S_{max} = 0.368$ when G = 1

Q.3.(a) Why channel allocation is a difficult task? Explain the random access method that tries to avoid collision. **(5)**

Ans. Refer Q.3 End term june – 2016.

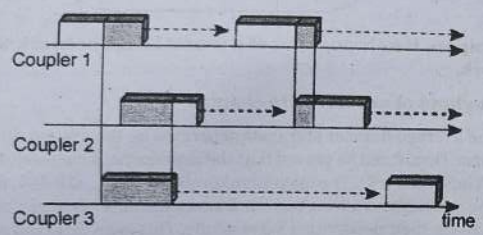
Random Access, which is to issue a completely random time, relies on the Aloha method.

In this method, when a coupler has information to transmit, it sends it without worry about other users. If there is a collision, that is to say superposition of two signals or more users, the signals become indecipherable and are lost. They are subsequently

dotnotes.xyz

transmitted, as shown in Figure, in which the couplers 1, 2 and 3 collide. The coupler transmits its field first because he shot the smallest timer. Then, the module 2 emits and its signals collide with the coupler 1. Both derive a random time of retransmission. The coupler 3 is listening while the couplers 1 and 2 are silent, so that the frame of the coupler 3 passes successfully. Technical aloha is the origin of all the random access methods.

The flow rate of such a system becomes very small when the number of couplers increases. It can be shown mathematically that if the number of stations goes to infinity the flow becomes zero. From a certain moment, the system is more stable. To reduce the likelihood of conflict between users, various improvements of this technique have been proposed.



Operating Principle of Pure Aloha

Slotted aloha, aloha or sliced

Improved technical aloha was to cut the time into time slots, or slots, and to authorize the issuance of frames that slice first, the transmission time of a frame requiring exactly a slice of time. In this way, there is no collision if a single frame transmitted at the beginning of slice. However, if several frames start transmitting in the beginning of slice, the frames emissions are superimposed along the slot. In the latter case, there has retransmission after a random time.

This method improves the throughput during the start-up period but remains unstable. In addition, there is an additional cost from a complication of the devices since all emissions must be synchronized.

Q.3.(b) A bit stream 10011101 is transmitted using the standard CRC method. The generator polynomial is $x^3 + 1$. Show the actual bit string being transmitted. Suppose a bit is inverted during transmission. Show how this error is detected at the receivers end. (5)

Ans. Our generator $G(x) = x^3 + 1$ encoded as 1001. Because the generator polynomial is of the degree three we append three zeros to the lower end of the frame to be transmitted. Hence after appending the 3 zeros the bit stream is 10011101000. On dividing the message by generator after appending three zeros to the frame we get a remainder of 100. We do modulo 2 subtraction thereafter of the remainder from the bit stream with the three zeros appended. The actual frame transmitted is 10011101100. See below.


```
          1 0 0 0 1 1 0 0
1001 | 1 0 0 1 1 1 0 1 0 0 0
       1 0 0 1
         0 0 0 1
         0 0 0 0
           0 0 1 1
           0 0 0 0
             0 1 1 0
             0 0 0 0
               1 1 0 1
               1 0 0 1
                 1 0 0 0
                 1 0 0 1
                   0 0 1 0
                   0 0 0 0
                     0 1 0 0
                     0 0 0 0
                       1 0 0 (remainder)
```

Actual frame transmitted: 10011101000–100=10011101100 (modulo 2 subtraction)

Now suppose the third bit from the left is garbled and the frame is received as 10111101100. Hence on dividing this by the polynomial generator we get a remainder of 100 which shows that an error has occured. Had the received frame been error free we would have got a remainder of zero. See below.

```
          1 0 1 0 1 0 0 0
1001 | 1 0 1 1 1 1 0 1 0 0 0
       1 0 0 1
         0 1 0 1
         0 0 0 0
           1 0 1 1
           1 0 0 1
             0 1 0 0
             0 0 0 0
               1 0 0 1
               1 0 0 1
                 0 0 0 1
                 0 0 0 0
                   0 0 1 0
                   0 0 0 0
                     0 1 0 0
                     0 0 0 0
                       1 0 0 (remainder indicating error)
```

dotnotes.xyz

Q.4.(a) What are various design issues involved in the data link layer? Explain sliding window protocol. (4)

Ans. The data link layer has a number of specific functions to carry out. These functions include providing a well-defined service interface to the network layer, determining how the bits of the physical layer are grouped into frames, dealing with transmission errors and regulating the flow or frames so that slow receivers are not swapped by fast senders.

There are the following issues.

(a) Services Provided to the Netowrk Layer

(b) Framing

(c) Error Control

(d) Flow Control

Refer Q.3.(a) of First Term Examination 2016.

Q.4.(b). State and explain various frame types in HDLC. (3)

Ans. There are three types of HDLC frames :

- Information transfer frame (I-Frame)
- Supervisory frame (S-Frame)
- Unnumbered frame (U-Frame)

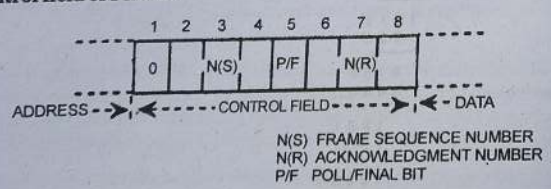
Information Transfer Frame (I-FRAME)

I-Frame is used for transporting user data. It also carries acknowledgement of the received frames. The control field of the I-Frame is as shown in Fig.. The first bit is 0 which identifies the frame as an I-Frame. The next three bits are the sequence number N(S) of the frame.

The fifth is Poll/Final (P/F) bit.

The last three bits are the sequence number N(R) of the acknowledgement (RR) which is piggy backed on the I-Frame.

Control field of I-frame

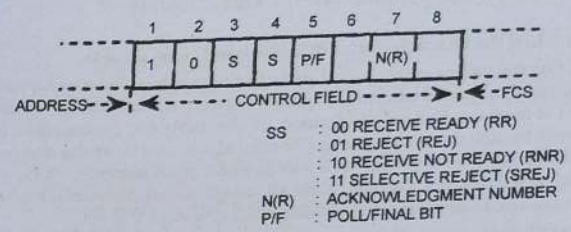


Supervisory Frame (S-FRAME)

S-Frame does not have data field and is used to carry only acknowledgements, requests for retransmission, etc. It is identified by the first two bits of the control field. These two bits are 10 in an S-Frame. The next two bits (SS) are used to indicate four supervisory states. Receive Ready (RR), Receive Not Ready (RNR), Reject (REJ) and Selective Reject (SREJ).

The fifth bit is Poll/Final bit. The last three bits are the sequence number associated with the supervisory states RR, RNR, REJ and SREJ indicated in the SS-Bits of the control field. Note that an acknowledgement (RR) can be sent either on a supervisory frame or piggybacked on an I-Frame as mentioned earlier. On the other hand RNR, REJ and SREJ are sent only through a supervisory frame.

Control field of S-frame

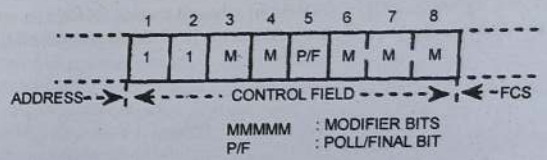


Unnumbered Frame (U-Frame)

The U-Frames do not have data field as S-Frames. They are used for link establishment, termination, mode setting and other control functions. Controls field of an unnumbered frame is shown.

The first two bits of the control field are 11 which identify an unnumbered frame. The fifth bit is Poll/Final bit. The rest five bits are called modifier bits. They specify the control function.

Cntrol Field of a U-Frame



Q.4.(c) If the 7-bit Hamming code word is received by a receiver is 1011011. Assuming the even parity state, find whether the received code word is correct or wrong. If wrong, locate the error and correct the code word. (3)

Ans.

d7	d6	d5	p4	d3	p2	p1
1	0	1	1	0	1	1

P4 = d5 d6 d7

= 1 => 1 0 1 p4 is 1

P2 = p2 d3 d6 d7

dotnotes.xyz

= 0 = >0 0 1 p2 = 0

P1 = p1 d3 p5 d7

= 1=> 011

P1 = 1.

P4 p2 p1 = 101 = 5

Error at 5th bit.

Corrected answer after changing the 5th bit will be : 1001011

Q.4.(d) List the characteristics of broad band coaxial cable.

Ans. Coaxial cables are the guided media that carnes the signal of higher frequency range compared to twisted pair cable. Coaxial cables are also called *coax*. (short form). Two types of coaxial cables are widely used: 50 ohm cable and 75 ohm cable. 50 ohm cable is used for digital transmission and 75 ohm cable is used for analog transmission. Due to the shield provided, this cable has excellent noise immunity. It has a large bandwidth and low losses. Co axial cables are easy to install. They are often installed either in a device to device daisy chain (Ethernet) or a star (ARC net).

A coaxial cable consists of many small cables in a protective cover. The cover shields the cable from physical dangers as well as from electromagnetic interference. Within the cover, the various cables are shielded from interference with one another. Coaxial cables are used in communication networks that require many simultaneous communication links. Each coaxial cable can provide more than 5000 links. It has a data rate of 10 Mbps which can be increased with the increase in diameter of the inner conductor. The specified maximum number of nodes on a thin net segment is 30 nodes and on a thick net it is 100 nodes.

Since broadband is used for large area, it requires amplifiers which are unidirectional. In dual band systems two identical cables run together, one used for outgoing data, one for incoming data. Different bandwidths are given for inbound and outbound cables. Eg: for 300MHz, 5-30MHz for inbound and 40-300MHz for outbound. There are two systems that use the bus LANs namelv 10 BASE 5 and 10 BASE 2

END TERM EXAMINATION [MAY-JUNE 2017]
SIXTH SEMESTER [B.TECH]
COMPUTER NETWORK [ETCS–306]

M.M. : 75

Time : 3 Hrs.

Note: *Q. No. 1 is compulsory. Attempt any five . Questions from the rest.*

Q.1. (a) How flow control is different from congesition control? (3)

Ans. Flow control means preventing the source from sending data that the sink will end up dropping because it runs out of buffer space. This is fairly easy with a sliding window protocol—just make sure the source's window is no larger than the free space in the sink's buffer. TCP does this by letting the sink advertise its free buffer space in the window field of the acks.

Congestion control means preventing (or trying to prevent) the source from sending data that will end up getting dropped by a router because its queue is full. This is more complicated, because packets from different sources travelling different paths can converge on the same queue.

Q.1.(b) Difference between bit rate and baud rate? Explain with example. (3)

Ans. Data rate *is* the capacity of a channel in bits per second. Bit rates measure the number of data bits (that is 0?s and 1?s) transmitted in one second in a communication channel. A figure of 2400 bits per second means 2400 zeros or ones can be transmitted in one second, hence the abbreviation "bps." Individual characters (for example letters or numbers) that are also referred to as bytes are composed of several bits.

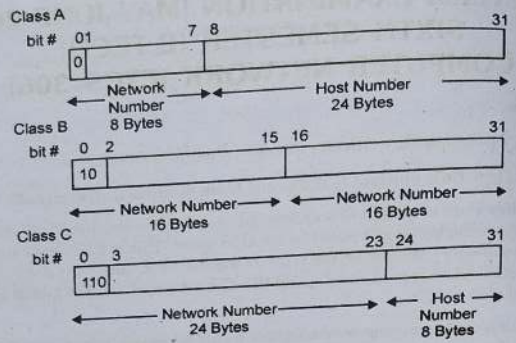
Baud rate represents the number of times the line condition (i.e., frequency, amplitude or phase) changes each second. Data rate = n bits x baud rate, where n is equal to the number of bits one signal represents. A baud rate is the number of times a signal in a communications channel changes state or varies. For example, a 2400 baud rate means that the channel can change states up to 2400 times per second. The term "change state" means that it can change from 0 to 1 or from 1 to 0 up to X (in this case, 2400) times per second. It also refers to the actual state of the connection, such as voltage, frequency, or phase level.

Q.1.(c) What is difference between Classfull addressing and Classless IP addressing? (4)

Ans. Classfull Addressing:

All IP addresses have a network and host portion. In classful addressing, the network portion ends on one of the separating dots in the address (on an octet boundary). Classful addressing divides an IP address into the Network and Host portions along octet boundaries.In the classful addressing system all the IP addresses that are available are divided into the five classes A,B,C,D and E, in which class A,B and C address are frequently used because class D is for Multicast and is rarely used and class E is reserved and is not currently used.

dotnotes.xyz



Each of the IP address belongs to a particular class that's why they are classf addresses.Earlier this addressing system did not have any name,but when classle addressing system came into existence then it is named as Classful addressi system.The main disadvantage of classful addressing is that it limited the flexibili and number of addresses that can be assigned to any device.One of the maj disadvantage of classful addressing is that it does not send subnet information but will send the complete network address.

Classless Addressing:

Classless addressing uses a variable number of bits for the network and hos portions of the address.

Classless addressing treats the IP address as a 32 bit stream of ones and zeroe where the boundary between network and host portions can fall anywhere between b 0 and bit 31.Classless addressing system is also known as CIDR(Classless Inte Domain Routing).Classless addressing is a way to allocate and specify the Interne addresses used in inter-domain routing more flexibly than with the original system Internet Protocol (IP) address classes. CIDR (Classless Internet Domain Routing defines arbitrarily-sized subnets solely by base address and number of significant bit in the address.

Q.1.(d) What is major advantages of STP over UTP? (2.

Ans. Shielded twisted pair cable have a conducting shielded made of metallic f encasing the twisted wire pairs, which blocks the electromagnetic interference allowin it to carry data at faster rate of speed rather than unshielded twisted pair howev they have several disadvantages STP cables work by attracting interference to th shield them running it off into a grounded cable. It the cable is improperly ground then the noise conceding capabilities are severely compromised additionally, STP cab are bigger than UTP cable, and are more expensive. Finally they are more fragile th UTP cables, as the shielded must be kept intact in order for them to work properly t best use for STP cable are in industrial setting with high amounts of electromagnet

interference, such as a factory with large electronic equipment, where they can be properly installed and maintained.

1. 'STP' is shielded while 'UTP' is not.
2. STPs are for heavy duty use while UTPs are not.
3. STPs allow maximum bandwidth while UTPs do not.

Q.1.(e) Differentiate between Intranet, internet and Internet? **(2.5)**

Ans. Many networks exist in the world, often with different hardware and software.- People connected to one network often want to communicate with people attached to a different one. This desire requires connecting together different, and frequently incompatible networks, sometimes by using machines called gateways to make the connection and provide the necessary translation, both in terms of hardware and software. A collection of interconnected networks is called an internetwork or just internet.

It is simply any network made up of multiple smaller networks using the same internetworking protocols. An internet (little "i") isn't necessarily connected to the Internet (big "I"), nor does it necessarily use TCP/IP as its internet working protocol. There are isolated corporate internets.

The Internet, with a capital "I," refers to the network that began its life as the AKPAnet and continues today as, roughly, the confederation of all TCP/IP networks directly or indirectly connected to commercial U.S. backbones. Seen up close, it's actually quite a few different networks-commercial TCP/IP backbones, corporate and U.S. government TCP/IP networks, and TCP/IP networks in other countries-interconnected by high-speed digital circuits.

It means a specific worldwide internet that is widely used to connect universities, government offices, companies, and of late, private individuals.

An internetwork is formed when distinct networks are connected together. In our view, connecting a LAN and a WAN or connecting two LANs forms an internetwork, but there is little agreement in the industry over terminology in this area.

Intranet: This is a network that is not available to the world outside of the Intranet. If the Intranet network is connected to the Internet, the Intranet will reside behind a firewall and, if it allows access from the Internet, will be an Extranet. The firewall helps to control access between the Intranet and Internet to permit access to the Intranet only to people who are members of the same company or organisation.

In its simplest form, an Intranet can be set up on a networked PG without any PC on the network having access via the Intranet network to the Internet.

For example, consider an office with a few PCs and a few printers all networked together. The network would not be connected to the outside world. On one of the drives of one of the PCs there would be a directory of web pages that comprise the Intranet. Other PCs on the network could access this Intranet by pointing their browser (Netscape or Internet Explorer) to this directory - for example

U:\inet\index.htm

From then onwards they would navigate around the Intranet in the same way as they would get around the Internet.

dotnotes.xyz

Q.1.(f) Difference between baseband transmission and broad band transmission? **(2.5)**

Ans. A baseband coaxial cable, commonly called an Ethernet cable, is a 50-ohm cable that transmits'an unmodulated digital signal. Transmission in baseband cables is bidirectional, meaning a signal inserted at any point propagates in both directions. Baseband cables are commonly used in local area networks. Broadband coaxial cables are 75-ohm cables that transmit modulated, analog signals. Broadband cables are unidirectional, but can compensate for this by dividing into different channels.

Baseband cables are not capable of transmitting more than one signal at a time, and the transmissions are restricted to data and voice. Additionally, baseband cables exceeding 0.62 mile in length experience a steady drop in transmission rates unless an amplifier is used. However, advantages of using baseband cable are the associated low cost and the ease of use. Another benefit of using baseband cable is the absence of a modem because the cable's signals are already digital.

A baseband coaxial cable transmits a single signal at a time at very high speed. A baseband cable is mainly used for **LANs.** Baseband coaxial cable supports frequency range of a-4kHz and are used for digital signaling. Baseband coaxial cables are 50 ohm cables used for 'digital transmission'. For IKm cables the bandwidth is 1-2 Gbps. Longer cables can be used with low data rates or periodic amplifiers.

The role of coaxial cable in broad band networks. The convergence of voice, video and data over a single infrastructure is the trend in broadband communications networks worldwide. Hybrid fiber/coaxial cable (hfc) networks offer broadband signal capability combined with rugged performance and economy.

Q.1.(g). What do you mean by Network Topology? Discuss the problems and benefits of any three topologies? **(4.5)**

Ans. 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:

1. Hierarchical topology
2. Bus topology
3. Star topology
4. Ring topology
5. Mesh topology
6. Hybrid topology

1. BUS Topology

Features of Bus Topology

1. It transmits data only in one direction.
2. Every device is connected to a single cable

Advantages of Bus Topology

1. It is cost effective.
2. Cable required is least compared to other network topology.
3. Used in small networks.

Disadvantages of Bus Topology

1. Cables fails then whole network fails.

2. If network traffic is heavy or nodes are more the performance of the network decreases.
3. It is slower than the ring topology.

RING Topology

Features of Ring Topology.

1.The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called **Dual Ring Topology**.

2. Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.

Advantages of Ring Topology

1.Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.

2. Cheap to install and expand

Disadvantages of Ring Topology

1.Troubleshooting is difficult in ring topology.

2.Adding or deleting the computers disturbs the network activity.

3.Failure of one computer disturbs the whole network.

STAR Topology

Features of Star Topology

1.Every node has its own dedicated connection to the hub.

2.Hub acts as a repeater for data flow.

3.Can be used with twisted pair, Optical Fibre or coaxial cable.

Advantages of Star Topology

1.Fast performance with few nodes and low network traffic..

2. Easy to troubleshoot.

3. Easy to setup and modify.

Disadvantages of Star Topology

1. Cost of installation is high.

2. Expensive to use.

3. If the hub fails then the whole network is stopped because all the nodes depend on the hub.

Q.1.(h) What is routing? Differentiate between distance vector routing and link state routing? **(3)**

Ans. Routing is the process of forwarding of a packet in a network so that it reaches its intended destination. The main goals of routing are:

1. Correctness: The routing should be done properly and correctly so that the packets may reach their proper destination.

2. Simplicity: The routing should be done in a simple manner so that the overhead is as low as possible. With increasing complexity of the routing algorithms the overhead also increases.

dotnotes.xyz

3. Robustness: Once a major network becomes operative, it may be expected to run continuously for years without any failures. The algorithms designed for routing should be robust enough to handle hardware and software failures and should be able to cope with changes in the topology and traffic without requiring all jobs in all hosts to be aborted and the network rebooted every time some router goes down.

4. **Stability:** The routing algorithms should be stable under all possible circumstances.

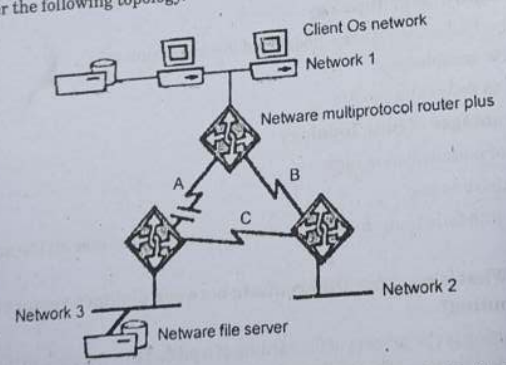
Compare the following routing techniques.

- Link state routing
- Distance vector routing

Distance vector routing is so named because it involves two factors: the *distance*, or metric, of a destination, and the *vector*, or direction to take to get there. Routing information is only exchanged between directly connected neighbours. This means a router knows from which neighbour a route was learned, but it does not know where that neighbour learned the route; a router can't see beyond its own neighbours. This aspect of distance vector routing is sometimes referred to as "routing by rumor." Measures like split horizon and poison reverse are employed to avoid routing loops.

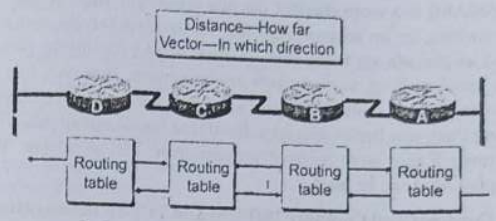
Link-state routing, in contrast, requires that all routers know about the paths reachable by all other routers in the network. Link-state information is flooded throughout the link-state domain (an area in OSPF or IS-IS) to ensure air routers posses a synchronized copy of the area's link-state database. From this common database, each router constructs its own relative shortest-path tree, with itself as the root, for all known routes.

Consider the following topology.



Both distance vector and link-state routing protocols are suitable for deployment on this network, but each will go about propagating routes in a different manner.

Distance Vector: If we were to run a distance vector routing protocol like RIP or EIGRP on this topology, here's how Rl would see the network, assuming each link has metric of 1 (locally connected routes have been omitted):



Routers pass periodic copies of their routing table to neighbouring routers and accumulate distance vectors.

To maintain the state of all links in the network, distance vector protocols typically consume less overhead at the expense of limited visibility. Because routers have only a limited view of the network, tools like split horizon and poison reverse are needed to prevent routing loops.

Link-State: Now, let's look at the topology running a link-state routing protocol (in a single area). Because each router records the state of all links in the area, each router can construct a shortest-path tree from itself to all known destinations.

Although maintaining link-state information for the entire area typically requires more overhead than does processing advertisements only from direct neighbours, but provide more robust operation and scalability.

Q.2.(a). Calculate the throughput of the pure and slotted ALOHA channel. Which Channel gives better throughput and why? (6)

Ans. Refer Q.2. (c) of First Term Examination 2017.

Slotted aloha gives better performance. The number of collisions that can possibly take place in slotted aloha is reduced by a huge margin. And hence, the performance become much better compared to Pure Aloha. Collisions may only take place with nodes that are ready to speak at the same time. But nevertheless, this is a substantial reduction.

Q.2.(b). Define Stop and Wait ARQ protocol. Explain the reason for moving from stop and wait ARQ protocol to the GO-Back-N ARQ protocol? (6.5)

Ans. Stop and Wait transmission is the simplest reliability technique and is adequate for a very simple communications protocol. A stop and wait protocol transmits a Protocol Data Unit (PDU) of information and then waits for a response. The receiver receives each PDU and sends an Acknowledgement (ACK) PDU if a data PDU is received correctly, and a Negative Acknowledgement (NACK) PDU if the data was not received. In practice, the receiver may not be able to reliably identify whether a PDU has been received, and the transmitter will usually also need to implement a timer to recover from the condition where the receiver does not respond.

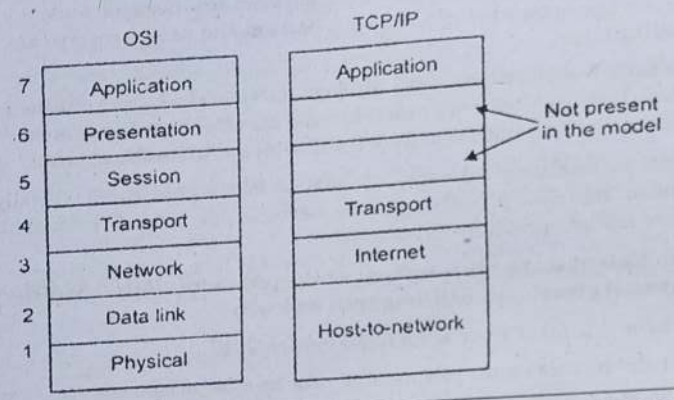
Under normal transmission the sender will receive an ACK for the data and then commence transmission of the next data block. For a long delay link, the sender may have to wait an appreciable time for this response. While it is waiting the sender is said to be in the "idle" state and is unable to send further data.

dotnotes.xyz

Go-Back-N ARQ is a more efficient use of a connection than Stop-and-wait ARQ, since unlike waiting for an acknowledgement for each packet, the connection is still being utilized as packets are being sent. In other words, during the time that would otherwise be spent waiting, more packets are being sent. However, this method also results in sending frames multiple times-if any frame was lost or damaged, or the ACK acknowledging them was lost or damaged, the if that frame and all following frames in the window (even if they were received without error) will be re-sent. To avoid this, Selective Repeat ARQ can be used.

Q.3.(a). Contrast and Compare ISO-OSI and TCP/IP networking models? (6.5)

Ans. OSI (Open system Interconnection) TCP/IP (Transmission Control Protocol/ Internet Protocol/Internet Protocol).



OSI (Open System Interconnection)	TCP/IP (Transmission Control Protocool/Internet Protocol)
1. OSI provides layer functioning and also defines functions of all the layers.	1. TCP/IP model is more based on protocols and protocols are not with flexible other layers.
2. In OSI model the transport layer guarantees the delivery of packets packets.	2. In TCP/IP model the transport layer does not guarantees delivery of
3. Follows horizontal approach	3. Follows vertical approach.
4. OSI model has a separate presentation layer	4. TCP/IP does not have a separate presentation layer
5. OSI is a general model. other application.	5. TCP/IP model cannot be used in any
6. Network layer of OSI model provide both connection oriented and connection less service.	6. The Network layer in TCP/IP model provides connectionless service.

7. OSI model has a problem of fitting the protocols in the model	7. TCP/IP model does not fit any protocol
8. Protocols are hidden in OSI model and are easily replaced as the technology changes.	8. In TCP/IP replacing protocol is not easy.
9. OSI model defines services, interfaces and protocols very clearly and makes clear distination between them.	9. In TCP/IP it is not clearly separated its services, interfaces and protocols.
10. It has 7 layers	10. It has 4 layers

Q.3.(b) What is the need for adaptive routing algorithm? Explain in detail? (6)

Ans. Adaptive routing is driven purely by the current state information available for the network. The term adaptive refers to the network's ability to adapt to conditions and find a route optimal to the present conditions. Unlike time-dependent routing, alternative routes are evaluated on a real-time basis and as such have no dependence on the time of day. Adaptive routing is computation intensive at the switches since the state information must be examined frequently but it is also more responsive to local network conditions.

Time-dependent routing is not considered adaptive because routing alternatives remain fixed during a constant time period, such as one hour.

1. Centralized: In this type some central node in the network gets entire information about the network topology, about the traffic and about other nodes. This then transmits this information to the respective routers. The advantage of this is that only one node is required to keep the information. The disadvantage is that if the central node goes down the entire network is down, i.e. single point of failure.

2. Isolated: In this method the node decides the routing without seeking information from other nodes. The sending node does not know about the status of a particular link. The disadvantage is that the packet may be send through a congested route resulting in a delay. Some examples of this type of algorithm for routing are:

- **Hot Potato:** When a packet comes to a node, it tries to get rid of it as fast as it can, by putting it on the shortest output queue without regard to where that link leads. A variation of this algorithm is to combine static routing-with the hot potato algorithm. When a packet arrives, the routing algorithm takes into account both the static weights of the links and the queue lengths.

- **Backward Learning:** In this method the routing tables at each node gets modified by information from the incoming packets. One way to implement backward learning is to include the identity of the source node in each packet, together with a hop counter that is incremented on each hop. When a node receives a packet in a particular line, it notes down the number of hops it has taken to reach it from the source node. If the previous value of hop count stored in the node is better than the current one then nothing is done but if the current value is better then the value is updated for future use. The problem with this is that when the best route goes down then it cannot'recall the

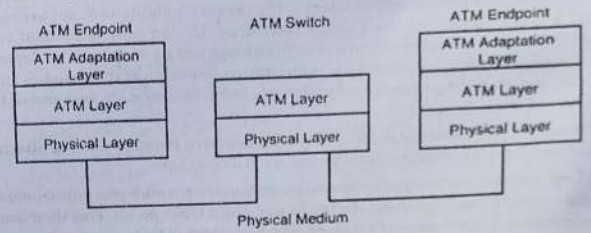
dotnotes.xyz

second best route to a particular node. Hence all the nodes have to forget the stored information periodically and start all over again.

3. Distributed: In this the node receives information from its neighbouring nodes and then takes the decision about which way to send the packet. The disadvantage is that if in between the the interval it receives information and sends the packet something changes then the packet may be delayed.

Q.4.(a) Explain ATM reference model? Why does ATM use small fixed length cell? What is ATM signaling? **(6.5)**

Ans. ATM: Asynchronous Transfer Mode (ATM) is a standard switching technique designed to unify telecommunication and computer networks. It uses asynchronous time-division multiplexing,[1][2] and it encodes data into small, fixed-sized cells. This differs from approaches such as the Internet Protocol or Ethernet that use variable sized packets or frames. ATM provides data link layer services that run over a wide range of OSI physical Layer links.



The ATM reference model is composed of the following ATM layers:

- Physical layer
- ATM layer ATM adaptation layer (AAL)

- Physical layer - Analogous to the physical layer of the OSI reference model, the ATM physical layer manages the medium-dependent transmission. The ATM reference model is composed of the following ATM layers.

- ATM layer - Combined with the ATM adaptation layer, the ATM layer is roughly analogous to the data link layer of the OSI reference model. The ATM layer is responsible for the simultaneous sharing of virtual circuits over a physical link (cell multiplexing) and passing cells through the ATM network (cell relay). To do this, it uses the VPI and VCI information in the header of each ATM cell.

- ATM adaptation layer (AAL) - Combined with the ATM layer, the AAL is roughly analogous to the data link layer of the OSI model. The AAL is responsible for isolating higher-layer protocols from the details of the ATM processes. The adaptation layer prepares user data for conversion into cells and segments the data into 48-byte cell payloads.

Finally, the higher layers residing above the AAL accept user data, arrange it into packets, and hand it to the AAL.

The ATM Physical Layer: The ATM physical layer has four functions: Cells are converted into a bitstream, the transmission and receipt of bits on the physical medium are controlled, ATM cell boundaries are tracked, and cells are packaged into the appropriate types of frames for the physical medium. For example, cells are packaged differently for SONET than for DS-3/E-3 media types.

The ATM physical layer is divided into two parts: the physical medium-dependent (PMD) sublayer and the transmission convergence (TC) sublayer.

The PMD sublayer provides two key functions. First, it synchronizes transmission and reception by sending and receiving a continuous flow of bits with associated timing information. Second, it specifies the physical media for the physical medium used, including connector types and cable. The TC sub layer has four functions: cell delineation, header error control (HEC) sequence generation and verification, cell-rate decoupling, and transmission frame adaptation.

ATM Adaptation Layers: AAL1: AAL1, a connection-oriented service, is suitable for handling constant bit rate sources (CBR), such as voice and videoconferencing. ATM transports CBR traffic using circuit-emulation services. Circuit-emulation service also accommodates the attachment of equipment currently using leased lines to an ATM backbone network. AAL1 requires timing synchronization between the source and the destination. For this reason, AAL1 depends on a medium, such as SONET, that supports clocking.

ATM Adaptation Layers: AAL2: Another traffic type has timing requirements like CBR but tends to be bursty in nature. This is called variable bit rate (VBR) traffic. This typically includes services characterized as packetized voice or video that do not have a constant data transmission speed but that do have requirements similar to constant bit rate services. AAL2 is suitable for VBR traffic. The AAL2 process uses 44 bytes of the cell payload for user data and reserves 4 bytes of the payload to support the AAL2 processes.

VBR traffic is characterized as either real-time (VBR-RT) or as non-real-time (VBR-NRT). AAL2 supports both types of VBR traffic.

ATM Adaptation Layers: AAL3/4: AAL3/4 supports both connection-oriented and connectionless data. It was designed for network service providers and is closely aligned with Switched Multimegabit Data Service (SMDS). AAL3/4 is used to transmit SMDS packets over an ATM network.

An AAL 3/4 SAR PDU header consists of Type, Sequence Number, and Multiplexing Identifier fields. Type fields identify whether a cell is the beginning, continuation, or end of a message. Sequence number fields identify the order in which cells should be reassembled. The Multiplexing Identifier field determines which cells from different traffic sources are interleaved on the same virtual circuit connection (VCC) so that the correct cells are reassembled at the destination.

ATM Adaptation Layers: AAL5: AAL5 is the primary AAL for data and supports both connection-oriented and connectionless data. It is used to transfer most non-SMDS data, such as classical IP over ATM and LAN Emulation (LANE). AAL5 also is known as the simple and efficient adaptation layer (SEAL) because the SAR sublayer simply accepts the CS-PDU and segments it into 48-octet SAR-PDUs without reserving any bytes in each cell.

dotnotes.xyz

1. Allows better statistical multiplexing of information on a given medium than the use of larger packets of variable length.

2. With longer varible-length packets, high-speed switching would be more complex.

3. The limited amount of information in the header allows ATM cells to be processed at a very high rate from 150 Mbps to several Gbps. .

4. Provides speed, flexibility and compatibility with any different applications and physical media.

5. The reduced size of the internal buffers guarantees a minimal delay and delay jitter. This is why ATM can handle both constant rate traffic (audio, video) and variable rate traffic (data) easily.

6. To limit the queuing delays in internal buffers.

ATM Signalling Protocol:

Protocol consists of two parts

→ User-Network Interface (UNI)

- defines how hosts talk to switches

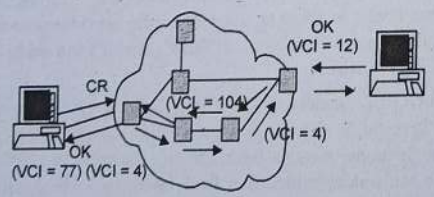
→ Network-Network Interface (NNI)

- defines how switches talk to other switches
- Cell formats slightly different

ATM Signalling Operation:-

- Connection requests proceed hop-by-hop through the switches of the network en route to destination
- Switches perform Call Admission Control (CAC) based on traffic descriptor, QOS requirements, and available resources at that switch
- If connection is acceptable, then request is forwarded on, otherwise "reject" is returned
- If destination accepts connection, then "accept" is returned

Example of ATM Signalling:



CR : Connection Request
OK : Connection Accept

Q.4.(b). Write short notes on ISDN? **(4)**

Ans. ISDN, which stands for Integrated Services Digital Network, is a system of digital phone connections which has been available for over a decade. This system allows voice and data to be transmitted simultaneously across the world using end-to-end digital connectivity. There are two basic types of ISDN service: **Basic Rate Interface (BRI)** and **Primary Rate Interface (PRI)**. BRI consists of two 64 kb/s B channels and one 16 kb/s D channel for a total of 144 kb/s. This basic service is intended to meet the needs of most individual users.

PRI is intended for users with greater capacity requirements. Typically the channel structure is 23 B channels plus one 64 kb/s D channel for a total of 1536 kb/s.

Some advantages of ISDN

Speed: ISDN allows multiple digital channels to be operated simultaneously through the same regular phone wiring used for analog lines. The change comes about when the telephone company's switches can support digital connections.

Multiple Devices: ISDN allows multiple devices to share a single line. It is possible to combine many different digital data sources and have the information routed to the proper destination. Since the line is digital, it is easier to keep the noise and interference out while combining these signals.

Signaling: Instead of the phone company sending a ring voltage signal to ring the bell in your phone ("In-Band signal"), it sends a digital packet on a separate channel ("Out-of-Band signal").

Q.4.(c) What is Tunneling? **(2)**

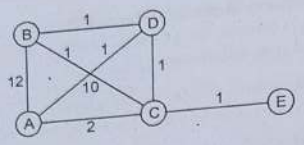
Ans. Tunneling: also known as "port forwarding," is the transmission of data intended for use only within a private, usually corporate network through a public network in such a way that the routing nodes in the public network are unaware that the transmission is part of a private network. Tunneling is generally done by encapsulating the private network data and protocol information within the public network transmission units so that the private network protocol information appears to the public network as data. Tunneling allows the use of the Internet, which is a public network, to convey data on behalf of a private network.

One approach to tunneling is the Point-to-Point Tunneling Protocol (PPTP) developed by Microsoft and several other companies. The PPTP keeps proprietary data reasonably secure, even though part of the path(s) between or among end users exists in public communication channels. The PPTP makes it possible for authorized users to gain access to a private network - called'a virtual private network (VPN) -through an Internet service provider (ISP) or online service. Another commonly used tunneling protocol is generic routing encapsulation (GRE), developed by Cisco Systems. There are numerous, less common tunneling protocols.

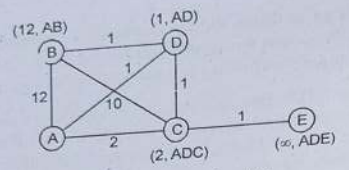
Tunneling, and the use of a VPN, is not intended as a substitute for encryption/ decryption. In cases where a high level of security is necessary, the strongest possible encryption should be used within the VPN itself, and tunneling should serve only as a convenience.

Q.5.(a) Given the network topology below use the Dijkstra's algorithm to compute the shortest path from A to all other nodes. Make sure to show the results of the computations at each step. **(6.5)**

dotnotes.xyz

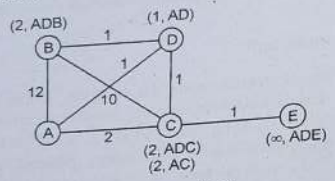


Ans.



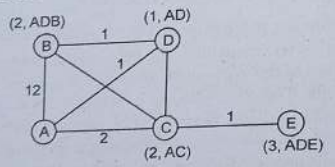
smallest is (1, AD) so we will consider the edge AD.

Now we are at Node D



Smallest is 2 so can take any node ADB or ADC.

Let us consider C Node.



Q.5.(b). What is collision? How does CSMA/CD detect and correct collision? (6)

Ans. In computer networking, a condition that occurs when two or more computers on a network try to transmit signals at the same time. Handling collisions is one of the main functions of a networking access method.

How Collision Works: When a station begins transmitting a signal and detects a collision, the station stops transmitting and issues a jam signal to tell the other stations that a collision has occurred. Both stations then stop transmitting and wait a random interval of time before retransmitting their signals. The amount of time the station

wait before retransmitting increases with the number of collisions occurring on the network.

CSMA is a network access method used on shared network topologies such as Ethernet to control access to the network. Devices attached to the network cable listen (carrier sense) before transmitting. If the channel is in use, devices wait before transmitting. MA (multiple access) indicates that many devices can connect to and share the same network. All devices have equal access to use the network when it is clear. Even though devices attempt to sense whether the network is in use, there is a good chance that two stations will attempt to access it at the same time. On large networks, the transmission time between one end of the cable and another is enough that one station may access the cable even though another has already just accessed it. Method for avoiding these collisions is as below:

"CSMA/CD (carrier sense multiple access/collision detection) CD (collision detection) defines what happens when two devices sense a clear channel, then attempt to transmit at the same time. A collision occurs, and both devices stop transmission, wait for a random amount of time, then retransmit. This is the technique used to access the 802-3 Ethernet network channel. This method handles collisions as they occur, but if the bus is constantly busy, collisions can occur so often that performance drops drastically. It is estimated that network traffic must be less than 40 percent of the bus capacity for the network to operate efficiently. If distances are long, time lags occur that may result in inappropriate carrier sensing, and hence collisions.

Q.6.(a). Draw and explain packet format of Transmission control protocol? Explain various steps that are followed in releasing a TCP connection? (8)

Ans. Refer Q.4.(a) Second Term 2016.

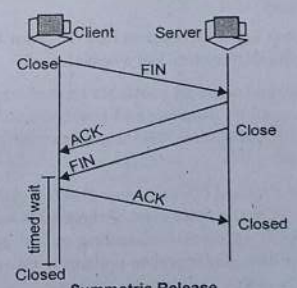
The basic steps followed by TCP to establish the connection are as follows :

Release can be asymmetric(one sided, where data may loss) or symmetric (both sides agreed) Steps for symmetric Release:

- Step 1: Client end system sends TCP FIN control segment to server
- Step 2: Server receives FIN, replies with ACK. Closes connection, sends FIN.
- Step 3: Client receives FIN, replies with ACK.

Enters "timed wait" - will respond with ACK to received FINs

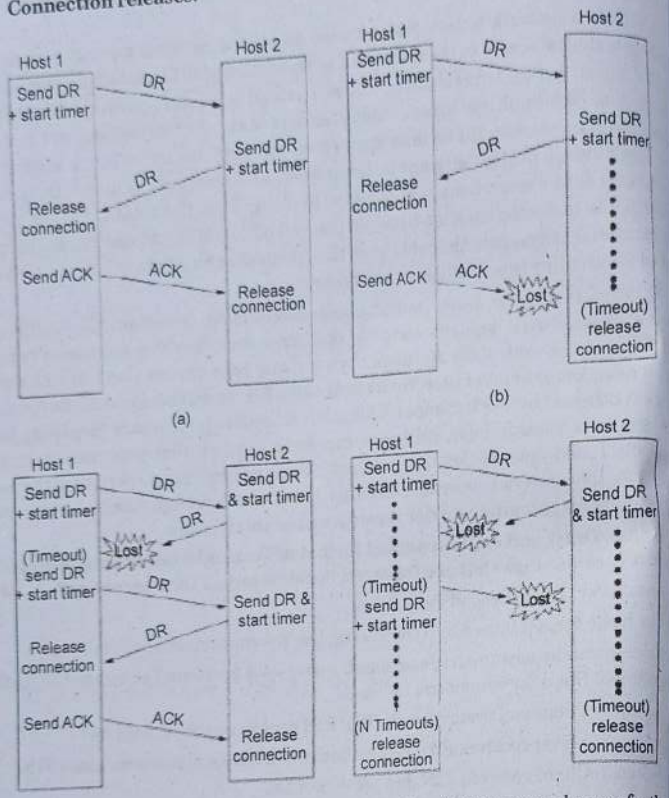
- Step 4: server, receives ACK. Connection closed.



Symmetric Release

dotnotes.xyz

Connection releases:



Four protocol scenarios for releasing a connection. (a) The normal case of a thre way handshake. (b) final ACK lost. (c) Response lost. (d) Response lost and subseque DRs (Disconnection Requests) lost.

Q.6.(b). Why transport layer protocols like TCP an UDP are called end-t end protocols. What is the difference between them? (4.

Ans. I assume end-to-end transport protocols typically mean protocols which a handling the full interconnectivity from one end-point to another end-point. From y computer to Any Web server for instance. The transport protocols are residing in La 4 in the OSI network model.

The Transport Control Protocol (TCP) running on top of the Internet Protocol (I often therfore called TCP/IP, is the most used of the end-to-end transport protocols offers reliable transport with automatic resending of lost packets. Another is U Datagram Protocol (UDP) which also is end-to-end but without reliability, no resend of lost data packets.

Difference :

TCP	UDP
Connection-oriented	Connectionless
Reliable packet delivery	Unreliable packet delivery
Has flow control mechanism	No flow control mechanism
Not preferred for real time applications	Preferred for real time applications
Has considerable overhead	Lightweight protocol with less overhead
Application: FTP, HTTP etc	Application: DNS, DNS

Q.7.(a) Explain the Leaky bucket algorithm to control cogestion. Explain how the drawbacks of this are overcome in token bucket algorithms? (6.5)

Ans. Leaky Bucket Algorithm: Consider a Bucket with a small hole at the bottom, whatever may be the rate of water pouring into the bucket, the rate at which water comes out from that small hole is constant. This scenario is depicted in figure (a). Once the bucket is full, any additional water entering it spills over the sides and is lost (*i.e.* it doesn't appear in the output stream through the hole underneath).

The same idea of leaky bucket can be applied to packets, as shown in Fig.*b*. Conceptually each network interface contains a leaky bucket. And the following steps are performed:

- When the host has to send a packet, the packet is thrown into the bucket.
- The bucket leaks at a constant rate, meaning the network interface transmits packets at a constant rate.
- Bursty traffic is converted to a uniform traffic by the leaky bucket.
- In practice the bucket is a finite queue that outputs at a finite rate.

This arrangement can be simulated in the operating system or can be built into the hardware. Implementation of this algorithm is easy and consists of a finite queue. Whenever a packet arrives, if there is room in the queue it is queued up and if there is no room then the packet is discarded.

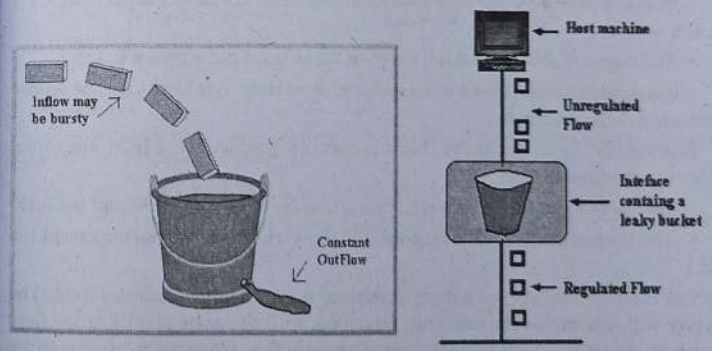


Fig. (a) Leaky bucket (b) Leaky bucket implementation

dotnotes.xyz

Q.7.(b) What is the maximum number of subnets in each case? **(6)**

(i) Class A: mask 255.255.192.0

(ii) Class B: mask 255.255.192.0

(iii) Class C: mask 255.255.192

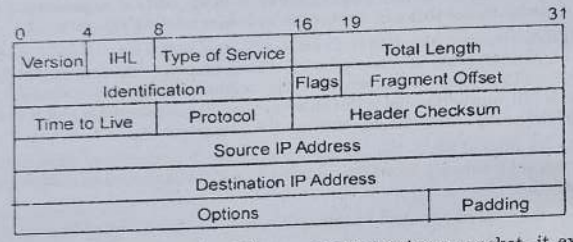
(iv) Class C: mask 255.255.255.240

Ans. (a) 1024 (b) 4

(c) 4 (d) 16

Q.8.(a) Difference between IPV4 and IPV6? Draw and explain the IPv4 protocol packet format? **(8.5)**

Ans.



Working of Ip: fragmentationrWhen a router receives a packet, it examines the destination address and determines the outgoing interface to use. The interface has an MTU, If the packet size is bigger than the MTU, the router may fragment the packet.

The router divides the packet into segments. The max size of each segment is the MTU minus the IP header size (20 bytes minimum; 60 bytes maximum). The router puts each segment into its own packet, each fragment packet having following changes:

- The *total length* field is the segment size.
- The *more fragments* (MF) flag is set for all segments except the last one, which is set to 0. —•
- The *fragment offset* field is set, based on the offset of the segment in the original data payload. This is measured in units of eight-byte blocks. « The *header checksum* field is recomputed.

Reassembly: A receiver knows that a packet is a fragment if at least one of the following conditions is true:

- The "more fragments" flag is set. (This *is* true for all fragments except the last.)
- The "fragment offset" field is nonzero. (This is true for all fragments except the first.)

The receiver identifies matching fragments using the identification field. The receiver will reassemble the data from fragments with the same identification field using both the fragment offset and the more fragments flag. When the receiver receives the last fragment (which has the "more fragments" flag set to 0), it can calculate the length of the original data payload, by multiplying the last fragment's offset by eight and adding the last fragment's data size. In the example above, this calculation was 495*8 + 540 = 4500 bytes.

When the receiver has all the fragments, it can put them in the correct order, by using their offsets. It can then pass their data up the stack for further processing.

The following table lists the important differences between IPv4 and IPv6.

IPv4	IPv6
IPv4 addresses are 32 bit length.	**IPv6, addresses** are 128 bit length.
IPv4 addresses are **binary numbers** represented in decimals.	**IPv6 addresses are binary numbers** represented in **hexadecimals.**
IPSec support is only optional.	Inbuilt IPSec support.
Fragmentation is done by sender and forwarding routers.	**Fragmentation** is done only by sender.
No packet flow identification.	Packet flow identification is available within the **IPv6 header** using the **Flow Label** field.
Checksum field is available in **IPv4 header**	No checksum field in **IPv6 header.**
Options fields are available in **IPv4 header.**	No option fields, but **IPv6 Extension headers** are available.
Address Resolution Protocol (ARP) is available to map IPv4 addresses to MAC addresses.	**Address Resolution Protocol (ARP)** is replaced with a function of **Neighbor Discovery Protocol (NDP).**
Internet Group Management Protocol (IGMP) is used to manage multicast group membership.	IGMP is replaced with Multicast Listener Discovery (MLD) messages.
Broadcast messages are available.	**Broadcast message** are not available. Instead a link-local scope "All nodes" **multicast IPv6 address** (FF02::1) is used for broadcast similar functionality.
Manual configuration (Static) of **IPv4 addresses** or DHCP (Dynamic configuration) is required to configure IPv4 addresses.	Auto-configuration of addresses is available.

Q.8. (b) Explain the maximum bit rate for a channel having bandwidth 3100Hz and S/N ratio of 20 dB.

Ans. S/N = 20 dB

i.e. 20 dB = 10log (S/N)

S/N = 100

$C = BW*\log_2 (1+S/N)$

$= 3100*\log_2 (1+100)$

$C = 3100\log_{10} (101)/\log_{10}2)]$

= 20, 643 BITS/SEC.

dotnotes.xyz

Q.9. (b) Compare various frame retransmission techniques used for error correction in data link layer.

Ans. Automatic Repeat Request (ARQ): Automatic Repeat request (ARQ) is an error control method for data transmission that makes use of error-detection codes, acknowledgment and/or negative acknowledgment messages, and timeouts to achieve reliable data transmission. An *acknowledgment* is a message sent by the receiver to indicate that it has correctly received a data frame.

Usually, when the transmitter does not receive the acknowledgment before the timeout occurs (*i.e.*, within a reasonable amount of time after sending the data frame), it retransmits the frame until it is either correctly received or the error persists beyond a predetermined number of retransmissions.

Three types of ARQ protocols are Stop-and-wait ARQ, Go-Back-N ARQ, and Selective Repeat ARQ.

ARQ is appropriate if the communication channel has varying or unknown capacity, such as is the case on the Internet. However, ARQ requires the availability of a back channel, results in possibly increased latency due to retransmissions, and requires the maintenance of buffers and timers for retransmissions, which in the case of network congestion can put a strain on the server and overall network capacity.

For example, ARQ is used on shortwave radio data links in the form of ARQ-E, or combined with multiplexing as ARQ-M.

Error-correcting code: An error-correcting code (ECC) or forward error correction (FEC) code is a process of adding redundant data, or *parity data*, to a message, such that it can be recovered by a receiver even when a number of errors (up to the capability of the code being used) were introduced, either during the process of transmission, or on storage. Since the receiver does not have to ask the sender for retransmission of the data, a backchannel is not required in forward error correction, and it is therefore suitable for simplex communication such as broadcasting. Error-correcting codes are frequently used in lower-layer communication, as well as for reliable storage in media such as CDs, DVDs, hard disks, and RAM.

Error-correcting codes are usually distinguished between convolutional codes and block codes:

- Convolutional codes are processed on a bit-by-bit basis. They are particularly suitable for implementation in hardware, and the Viterbi decoder allows optimal decoding.
- Block codes are processed on a block-by-block basis. Early examples of block codes are repetition codes, Hamming codes and multidimensional parity-check codes. They were followed by a number of efficient codes, Reed–Solomon codes being the most notable due to their current widespread use. Turbo codes and low-density parity-check codes (LDPC) are relatively new constructions that can provide almost optimal efficiency.

Hybrid schemes: Hybrid ARQ is a combination of ARQ and forward error correction. There are two basic approaches:

- Messages are always transmitted with FEC parity data (and error-detection redundancy). A receiver decodes a message using the parity information, and requests retransmission using ARQ only if the parity data was not sufficient for successful decoding (identified through a failed integrity check).
- Messages are transmitted without parity data (only with error-detection information). If a receiver detects an error, it requests FEC information from the transmitter using ARQ, and uses it to reconstruct the original message.

The latter approach is particularly attractive on an erasure channel when using a rateless erasure code.

FIRST TERM EXAMINATION [FEB. 2018]
SIXTH SEMESTER [B.TECH]
COMPUTER NETWORK [ETCS–306]

Time : 1½ hrs. **M.M. : 30**

Note: Attempt Q. No. 1 which is compulsory and any two other questions from remaining questions.

Q. 1. (a) In the sliding window protocol, can the sender receive an ACK for a packet that falls outside its current window? If yes, specify the scenario under which this occurs as well. **(2)**

Ans. Outside can mean to either side of the window. The sender will not receive an ACK for a packet that is to the right of the window since the sender never sent such a packet. The sender can potentially receive an ACK (duplicate) for packets outside of the window to the left. This can happen when for example the original ACK got delayed and the sender retransmitted the packet on timeout.

Q.1. (b) What is the difference between circuit switching and packet switching and Message Switching. **(2)**

Ans. Circuit-Switching, Message-Switching and Packet-Switching

Circuit switching network establishes a fixed bandwidth circuit (channel) between nodes before the users may communicate, as if the nodes were physically connected with an electrical circuit. The bit delay is constant during the connection, as opposed to packet switching, where packet queues may cause varying delay.

Each circuit cannot be used by other callers until the circuit is released and a new connection is set up. Even if no communication is taking place in a dedicated circuit then, that channel still remains unavailable to other users. Channels that are available for new calls to be set up are said to be idle. Telephone network is example of circuit switching system.

Virtual circuit switching is a packet switching technology that may emulate circuit switching, in the sense that the connection is established before any packets are transferred, and that packets are delivered in order.

Message switching was the precursor of packet switching, where messages were routed in their entirety, one hop at a time. It was first introduced in 1961. Nowadays, message switching systems are mostly implemented over packet-switched or circuit-switched data networks. E-mail is example of a message switching system.

Packet switching is a communications paradigm in which packets (discrete blocks of data) are routed between nodes over data links shared with other traffic. The term "packets" refers to the fact that the data stream from your computer is broken up into packets of about 200 bytes (on average), which are then sent out onto the network. Each packet contains a "header" with information necessary for routing the packet from source to destination. Each packet in a data stream is independent.

The main advantage of packet-switching is that it permits "statistical multiplexing" on the communications lines. The packets from many different sources can share a line, allowing for very efficient use of the fixed capacity. With current technology, packets are generally accepted onto the network on a first-come, first-served basis. If the network becomes overloaded, packets are delayed or discarded ("dropped").

Q.1. (c) Give two advantages of using optical fibre cable compared to coaxial cable. **(2)**

Ans. The computers and other electronic devices transmit the data from one to another device in the form of signals and using a transmission media. The transmission

dotnotes.xyz

media can be fundamentally categorised into two types guided and unguided. Unguid
media is a wireless communication which carries electromagnetic waves by making u
of air as medium and without requiring a physical conductor. Guided media need
physical medium to transmit signals such as wires. Guided media is classified in th
ways twisted pair cable, coaxial cable and fibre-optic cable. The article explains you th
difference between optical fibre and coaxial cable.

Unguided media is a wireless communication which carries electromagnetic wa
by making use of air as medium and without requiring a physical conductor. Guid
media need a physical medium to transmit signals such as wires. Guided media
classified in three ways twisted pair cable, coaxial cable and fibre-optic cable. The art
explains you the difference between optical fibre and coaxial cable.

Essentially, the optical fibre is a guided media which transmits the signals fro
one device to another in the form of light (optical form). Whereas coaxial cable transm
the signals in electrical form.

Key Differences Between Optical Fibre and Coaxial Cable

1. Optical fibre carries the signals in optical form while coaxial cable carries
signal in the form of electricity.
2. Fibre optics cable is made of glass fibre and plastic. In contrast, the coax ca
is made up of metal wire (copper), plastic and metal mesh braid.
3. The optical fibre is more efficient than coaxial cable as it has higher noise immu
4. Optical cable is costlier than coaxial cable.
5. The effect of bending of the cable is negative in case of an optical fibre. As agai
the coaxial cable is unaffected by the bending.
6. The optical fibre provides high bandwidth and data rates. On the contrary
bandwidth and data rates provided by the coaxial cable are moderately high but le
than optical cable.
7. Coaxial cable can be easily installed whereas installation of optical cable req
extra effort and care.
8. The optical fibre is lightweight and has a small diameter. Conversely, a co
cable is heavier and has a large diameter.

OR

The advantage of using optical fiber cable compared to coaxial cable are :

Thinner: Optical fibers can be drawn to smaller diameters than copper wire

Higher carrying capacity: Because optical fibers are thinner than copper w
more fibers can be bundled into a given-diameter cable than copper wires. This al
more phone lines to go over the same cable or more channels to come through the c
into your cable TV box.

Less signal degradation: The loss of signal in optical fiber is less than in copper

Light signals: Unlike electrical signals in copper wires, light signals from one f
do not interfere with those of other fibers in the same cable. This means clearer p
coverations of TV reception.

**Q.1. (d) In stop and wait ARQ, what happens if a negative acknowledge
is lost in transit?**

Ans. Stop-and-wait ARQ is a form of stop-and-wait flow control extended to in
retransmission of data in case of lost or damaged frames. For retransmission to w
four features are added to the basic flow control mechanism:

The sending device keeps a copy of the last frame transmitted until it receiv
acknowledgment for that frame.

For identification purposes, both data frames and ACK frames are numbered alternately 0 and 1. A data 1 frame is acknowledged by an ACK 1 frame, indicating that the receiver has gotten data 1 and is now expecting data 0. This numbering allows for identification of data frames in case of duplicate transmission

Lost Acknowledgment In this case, the data frame has made it to the receiver and been found to be either acceptable or not acceptable. But the ACK or NAK frame returned by the receiver is lost in transit. The sending device waits until its timer goes off, and then retransmits the data frame. The receiver checks the number of the new data frame. If the lost frame was a NAK, the receiver accepts the new copy and returns the appropriate ACK (assuming the copy arrives undamaged). If the lost frame was an ACK, the receiver recognizes the new copy as a duplicate, acknowledges its receipt, then discards it and waits for the next frame (see Figure)

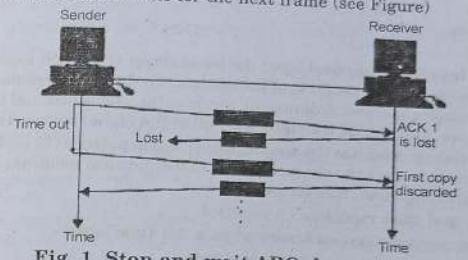


Fig. 1. Stop-and-wait ARQ, lost ACK frame

If an error is discovered in a data frame, indicating that it has been corrupted in transit, a NAK frame is returned. NAK frames, which are not numbered, tell the sender to retransmit the last frame sent. NAK frames are not numbered because it tells the sender to retransmit the last frame send. Stop-and-wait ARQ requires that the sender wait until it receives an acknowledgment for the last frame transmitted before it transmits the next one. When the sending device receives a NAK, it resends the frame transmitted after the last acknowledgment, regardless of number.

Q.1. (e) A binary signal is sent over a 3 kHz channel whose signal-to-noise ratio is 20dB. Calculate the maximum achievable data rate. (2)

Ans. 3KHZ channel

$$\text{SNR} = 20 \text{ dB}$$
$$\text{Data rate} = ?$$
$$\text{Data rate} = \text{Band width} \times \log_2 (1 + \text{SNR})$$
$$= 3 \times 10^3 \times \log_2 (1 + 20)$$
$$\text{Data rate} = 3 \times 10^3 \times \log_2 (21)$$
$$\text{Data rate} = 3 \times 10^3 \times 4.39$$
$$\text{Data rate} = 3000 \times 4.39$$
$$= 13{,}170 \text{ bPs.}$$

Q.2. (a) For 'n' devices in a network, what is the number of cable links required for a mesh, ring, bus and star topology ? (2)

Ans. Number of cable links required for a mesh is $n(n-1)/2$

Number of cable links required for a ring topology is $(n-1)$

dotnotes.xyz

Number of cable links required for a star topology is (n)

Q.2. (b) How do the layers of the TCP/IP protocol suite correlate to the layers of the OSI model?

Ans. 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: 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 neighbour 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

dotnotes.xyz

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

Q.2. (c) Briefly discuss the role of following devices in context of networking.

(i) Repeater **(ii) Gateway** (8)

Ans. (i) Repeater: 1. In digital communication systems, a repeater is a device that receives a digital signal on an electromagnetic or optical transmission medium and regenerates the signal along the next leg of the medium. In electromagnetic media

repeaters overcome the attenuation caused by free-space electromagnetic-field divergence or cable loss. A series of repeaters make possible the extension of a signal over a distance.

Repeaters remove the unwanted noise in an incoming signal. Unlike an analog signal, the original digital signal, even if weak or distorted, can be clearly perceived and restored. With analog transmission, signals are restrengthened with amplifiers which unfortunately also amplify noise as well as information.

Because digital signals depend on the presence or absence of voltage, they tend to dissipate more quickly than analog signals and need more frequent repeating. Whereas analog signal amplifiers are spaced at 18,000 meter intervals, digital signal repeaters are typically placed at 2,000 to 6,000 meter intervals.

2. In a wireless communications system, a repeater consists of a radio receiver, an amplifier, a transmitter, an isolator, and two antennas. The transmitter produces a signal on a frequency that differs from the received signal. This so-called frequency offset is necessary to prevent the strong transmitted signal from disabling the receiver. The isolator provides additional protection in this respect. A repeater, when strategically located on top of a high building or a mountain, can greatly enhance the performance of a wireless network by allowing communications over distances much greater than would be possible without it.

3. In satellite wireless, a repeater (more frequently called a transponder) receives uplink signals and retransmits them, often on different frequencies, to destination locations.

4. In a cellular telephone system, a repeater is one of a group of transceivers in a geographic area that collectively serve a system user.

5. In a fiber optic network, a repeater consists of a photocell, an amplifier, and a light-emitting diode (LED) or infrared-emitting diode (IRED) for each light or IR signal that requires amplification. Fiber optic repeaters operate at power levels much lower than wireless repeaters, and are also much simpler and cheaper. However, their design requires careful attention to ensure that internal circuit noise is minimized.

6. Repeaters are commonly used by commercial and amateur radio operators to extend signals in the radio frequency range from one receiver to another. These consist of drop repeaters, similar to the cells in cellular radio, and hub repeaters, which receive and retransmit signals from and to a number of directions.

7. A bus repeater links one computer bus to a bus in another computer chassis, essentially chaining one computer to another.

(ii) Gateway: A gateway is a network node that connects two networks using different protocols together. While a bridge is used to join two similar types of networks, a gateway is used to join two dissimilar networks.

A gateway device provides communication to a remote network or an autonomous system that is out of bounds for the host network nodes. Gateways serve as the entry and exit point of a network; all data routed inward or outward must first pass through and communicate with the gateway in order to use routing paths. Generally, a router is configured to work as a gateway device in computer networks.

A network gateway joins two networks so the devices on one network can communicate with the devices on another network. Without gateways, you couldn't be able to access the internet, communicate and send data back and forth. A gateway can be implemented completely in software, hardware, or a combination of both. Because a network gateway by definition appears at the edge of a network, related capabilities such as firewalls and proxy servers tend to be integrated with it.

Types of Gateways for Homes and Small Businesses

Whichever type of network gateway you use in your home or small business, the

dotnotes.xyz

function is the same. It connects your local area network (LAN) and all the devices on it to the internet and from there to wherever the devices want to go. Types of network gateways in use include:

• On home networks and in small businesses, a broadband router typically serves as the network gateway. It connects the devices in your home or small business with the internet. A gateway is the most important feature of a router. Routers are the most common type of gateways.

• In some cases, such as in a residence that uses dial-up internet access, the gateway is a router at the internet service provider's location. This has become increasingly less common as dial-up access declines in popularity.

• Some small businesses configure a computer to serve as the gateway to the internet, rather than use a router. This method requires two network adapters - one connected to the local network and one connected to the internet.

Gateways as Protocol Converters: Gateways are network protocol converters. Often the two networks that a gateway joins use different base protocols. The gateway facilitates compatibility between the two protocols. Depending on the types of protocols they support, network gateways can operate at any level of the OSI model.

Q.3. (a) An 8 bit byte binary value 10101111 is to be encoded using an even parity Hamming code. What is the binary value after encoding ? (5)

Ans. The given 8 bit byte with a binary value of 10101111 yields a parity value of 101001001111.

This is how you solve it:

1. Mark all bit positions that are powers of two as parity bits. (positions 1, 2, 4, 8, 16, 32, 64,etc.)
2. All other bit positions are for the data to be encoded. (positions 3, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15, 17 etc).
   – – 1 – 0 1 0 – 1 1 1 1
3. Each parity bit calculates the parity for some of the bits in the code word. The position of the parity bit determines the sequence of bits that it alternately checks and skips.
   Position 1: check 1 bit, skip 1 bit, check 1 bit, skip 1 bit, etc.
   (1, 3, 5, 7, 9, 11, 13, 15, ...)
   Position 2: Check 2 bits, skip 2 bits, check 2 bits, skip 2 bits, etc.
   (2, 3, 6, 7, 10, 11, 14, 15, ...)
   Position 4: Check 4 bits, skip 4 bits, check 4 bits, skip 4 bits, etc.
   (4, 5, 6, 7, 12, 13, 14, 15, 20, 21, 22, 23, ...)
   Position 8: Check 8 bits, skip 8 bits, check 8 bits, skip 8 bits, etc.
   (8 – 15, 24 – 31. 40 – 47, ...)
   Position 16: Check 16 bits, skip 16 bits, check 16 bits, skip 16 bits, etc.
   (16 – 31, 48 – 63, 80 – 95, ...)
   Position 32: Check 32 bits, skip 32 bits, check 32 bits, skip 32 bits,
   (32 – 63, 96 – 127, 160 – 191, ...) etc.
4. Set a parity bit to 1 if the total number of ones in the positions it checks is odd. Set a parity bit to 0 if the total number of ones in the positions it checks is even.

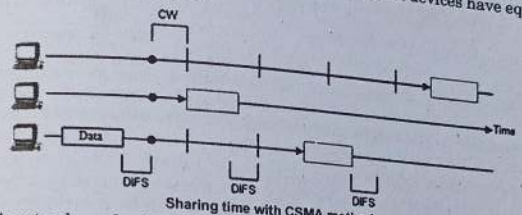
Doing the calculations: Position 1 yields a value of 3, which is odd and therefore a 1. Positions 2, 4 and 8 equal 4, 2 and 4 respectively. So they each get a value of 0. Filling them in gets you:

Q.3. (b) How throughput is improved in slotted ALOHA over pure ALOHA? (5)

Ans. Refer Q.2. (c) of First Term Examination 2017.

Q.3. (c) What is CSMA?How p-persistent CSMA is different from non persistent ? (2)

Ans. Carrier Sensed Multiple Access (CSMA) : CSMA is a network access method used on shared network topologies such as Ethernet to control access to the network. Devices attached to the network cable listen (carrier sense) before transmitting. If the channel is in use, devices wait before transmitting. MA (Multiple Access) indicates that many devices can connect to and share the same network. All devices have equal access to use the network when it is clear.



Sharing time with CSMA method.

CSMA protocol was developed to overcome the problem found in ALOHA i.e. to minimize the chances of collision, so as to improve the performance. CSMA protocol is based on the principle of 'carrier sense'. The station senses the carrier or channel before transmitting a frame. It means the station checks the state of channel, whether it is idle or busy.

Even though devices attempt to sense whether the network is in use, there is a good chance that two stations will attempt to access it at the same time. On large networks, the transmission time between one end of the cable and another is enough that one station may access the cable even though another has already just accessed it.

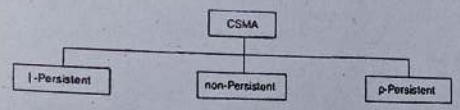
The chances of collision still exist because of propagation delay. The frame transmitted by one station takes some time to reach other stations. In the meantime, other stations may sense the channel to be idle and transmit their frames. This results in the collision.

There Are Three Different Type of CSMA Protocols

(*i*) I-persistent CSMA

(*ii*) Non- Persistent CSMA

(*iii*) *p*-persistent CSMA



Types of CSMA

(*i*) I-persistent CSMA

• In this method, station that wants to transmit data continuously senses the channel to check whether the channel is idle or busy.

• If the channel is busy, the station waits until it becomes idle.

• When the station detects an idle-channel, it immediately transmits the frame with probability 1. Hence it is called I-persistent CSMA.

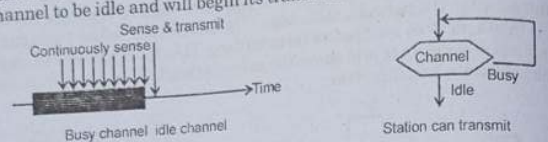
• This method has the highest chance of collision because two or more stations may find channel to be idle at the same time and transmit their frames.

• When the collision occurs, the stations wait a random amount of time and start allover again.

dotnotes.xyz

Drawback of I-persistent

• The propagation delay time greatly affects this protocol. Let us suppose, just after the station 1 begins its transmission, station 2 also became ready to send its data and senses the channel. If the station 1 signal has not yet reached station 2, station 2 will sense the channel to be idle and will begin its transmission. This will result in collision.



I-persistent CSMA

Even if propagation delay time is zero, collision will still occur. If two stations became ready in the middle of third station's transmission, both stations will wait until the transmission of first station ends and then both will begin their transmission exactly simultaneously. This will also result in collision.

(ii) Non-persistent CSMA

• In this scheme, if a station wants to transmit a frame and it finds that the channel is busy (some other station is transmitting) then it will wait for fixed interval of time.

• After this time, it again checks the status of the channel and if the channel is free it will transmit.

• A station that has a frame to send senses the channel.

• If the channel is idle, it sends immediately.

• If the channel is busy, it waits a random amount of time and then senses the channel again.

• In non-persistent CSMA the station does not continuously sense the channel for the purpose of capturing it when it detects the end of previous transmission.

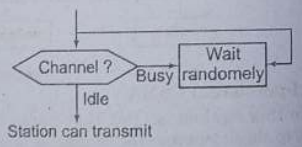
Advantage of non-persistent

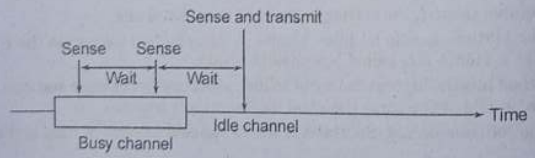
• It reduces the chance of collision because the stations wait a random amount of time. It is unlikely that two or more stations will wait for same amount of time and will retransmit at the same time.

Disadvantage of non-persistent

• It reduces the efficiency of network because the channel remains idle when there may be stations with frames to send. This is due to the fact that the stations wait a random amount of time after the collision.

Non-Persistent





(iii) p-persistent CSMA

• This method is used when channel has time slots such that the time slot duration is equal to or greater than the maximum propagation delay time.

o Whenever a station becomes ready to send, it senses the channel.

o If channel is busy, station waits until next slot.

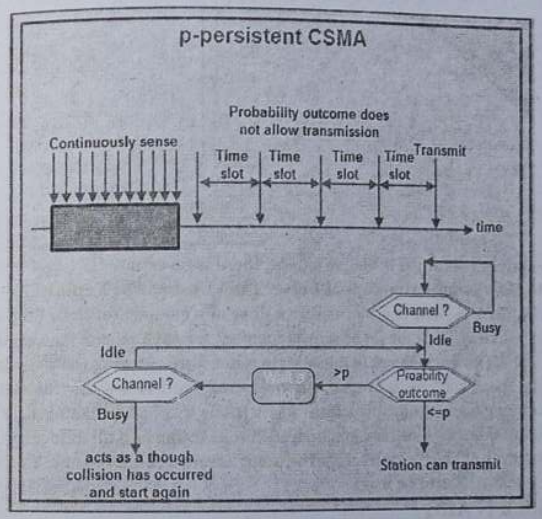
o If channel is idle, it transmits with a probability p.

o With the probability $q = l - p$, the station then waits for the beginning of the next time slot.

o If the next slot is also idle, it either transmits or waits again with probabilities p and q.

o This process is repeated till either frame has been transmitted or another station has begun transmitting.

o In case of the transmission by another station, the station acts as though a collision has occurred and it waits a random amount of time and starts again.



Advantage of *p*-persistent

o It reduces the chance of collision and improves the efficiency of the network.

Q.4. (a) For a generator polynomial of $x^3 + x^2 + 1$, what is the CRC value if the message is 10011010?express answer as bit sequence with no spaces. (5)

Ans. Generated polynomial $x^3 + x^2 + 1$ binary representation 1101

Given message, 10011010

CRC calculation:

dotnotes.xyz

```
          11111
1101)10011010
     1101↓
      1001
      1101↓
       1000
       1101↓
        1011
        1101↓
         1100
         1101
         [001] ← remainder
```

CRC generated

At receiver side, data received is 10011011.

```
          11111
1101)10011011
     1101↓
      1001
      1101↓
       1000
       1101↓
        1011
        1101↓
         1101
         1101
         0000
```

The remainder obtained is 000, it means, there is no error.

Q.4. (b) How is selective repeat better than Go-backN. Explain ? (5)

Ans. Go-Back-N ARQ is a more efficient use of a connection than Stop-and-wait ARQ, since unlike waiting for an acknowledgement for each packet, the connection is still being utilized as packets are being sent. In other words, during the time that would otherwise be spent waiting, more packets are being sent. However, this method also results in sending frames multiple times - if any frame was lost or damaged, or the ACK acknowledging them was lost or damaged, then that frame and all following frames in the window (even if they were received without error) will be re-sent. To avoid this, Selective Repeat ARQ can be used.

Go-Back-N ARQ

1. Retransmission begins with the last unacknowledged frame even if subsequent frames have arrived correctly .duplicate frames are discarded.
2. Go-back-*n* ARQ -- Receiver must get Frames in correct order

Selective Repeat ARQ

3. Only the unacknowledged frame is retransmitted.
4. It may be (slightly) more efficient than Go-back-n ARQ, but also much more complicated.
5. Selective repeat ARQ -- correctly-received out-of-order Frames are stored at Receiver until they can be re-assembled into correct order

END TERM EXAMINATION [MAY-JUNE 2018]
SIXTH SEMESTER [B.TECH]
COMPUTER NETWORK [ETCS–306]

Time : 3 hrs. **M.M. : 75**

Note: Attempt five question in all including Q. No. 1 which is compulsory select one question from each unit.

Q 1 Attempt the following questions:-

Q.1. (a) What are two reasons for using layered protocols ? What is the one possible disadvantages of using layered protocols ? (5)

Ans. A layered protocol architecture provides a conceptual framework for dividing the complex task of exchanging information between remote hosts into simpler tasks.

- Each protocol layer has a narrowly defined responsibility.
- A protocol layer provides a standard interface to the next higher protocol layer.
- Consequently, it hides the details of the underlying physical network infrastructure.
- Benefit: The same user-level (application) program can be used over very diverse communication networks.
- Example: The same WWW browser can be used when you are connected to the internet via a LAN or a dial-up line.

Some of the disadvantages of using layered protocols are the redundancy and overall lower performance.

Re implementing everything from remote and wired to connectionless and association situated application correspondence, with each ringer and shriek of BGP, MPLS, multicast steering and so on would be a gigantic endeavor and potentially unmanageable in this solid across the board convention. I could envision specialty utilize situations where most extreme execution is imperative most importantly where an exceptionally basic framework might be wanted.

Q.1. (b) Compare and contrast CSMA/CD with CSMA/CA. (5)

Ans. CSMA/CD (Carrier Sense multiple Access Collision Detection): This multiple access method is used in wired networks since it is possible to detect collision and then proceed with so used in LANs and WANs.

This is used by IEEE 802.3 standard Ethernet networks in which each node monitors the traffic in the line and if no traffic is available then a particular node can transmit. But at the same time if two are trying to transmit then it is known as a collision. This situation is sensed by all the nodes in the given network. After that the stations which had the collision will try to send data again after some random time interval which are vary for each node. If again a collision takes place the random time taken is increased and waits again. This is the procedure used in CSMA/CD networks and the method does not have any deterministic capability.

CSMA/CA (Carrier Sense multiple Access Collision Avoidance): This is the multiple access scheme used in layer 2 access method in which the following method is used when nodes are trying to transmit simultaneously in a shared network. Here the node which wishes to transmit first has to listen to the medium for a pre determined period to assess the channel state. If the channel is idle then the node is capable of transmitting. Else the channel is said to be busy and node has to wait until the channel comes to idle mode.

dotnotes.xyz

This is implemented in IEEE 802.11 wireless LANs and other wireless networks and this is preferred since the wireless networks cannot detect collision while transmitting like wired networks. So the implementation of CSMA/CA will improve the packet dropping in wireless networks.

CSMA/CD Vs CSMA/CA

1. CSMA/CD is used in wired LANs and CSMA/CA used in wireless LANs and other types of wireless networks.

2. CSMA/CD is standardized in IEEE 802.3 and CSMA/CA is standardized in IEEE 802.11.

3. CSMA/CD will not take steps to prevent transmission collision until it is taken place whilst CSMA/CA will take actions not to take place any collision since the latter has no means of knowing whether a collision has taken place.

Q.1. (c) What is the relationship between SONET and SDH ? (5)

Ans. Synchronous Optic Network (SONET) and Synchronous Digital Hierarchy (SDH) are standards used in fiber optic networks that power large telephone and Internet networks. SONET networks are deployed in North America; SDH networks are deployed everywhere else. The data communications industry uses the concept of "backbone" to refer to a large network capable of carrying heavy loads of traffic. SONET and SDH fiber optic networks, although expensive, are ideal backbone networks, offering high speeds and reliability.

SONET adheres to standards T1.105 and T1.106 developed by ANSI or the American National Standards Institute. SDH is an ITU or International Telecommunications Union standard developed to allow it to work with SONET line rates. It is a flexible standard that connects to several interfaces and bandwidths and has bandwidth on-demand capability.

Q.1. (d) What is the difference between open-loop congestion control and closed -loop congestion control? (5)

Ans. Open Loop Congestion Control

Open loop congestion control policies are applied to prevent congestion before it happens. The congestion control is handled either by the source or the destination.

Policies adopted by open loop congestion control -

1. Retransmission Policy: It is the policy in which retransmission of the packets are taken care. If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted. This transmission may increase the congestion in the network.

To prevent congestion, retransmission timers must be designed to prevent congestion and also able to optimize efficiency.

2. Window Policy: The type of window at the sender side may also affect the congestion. Several packets in the Go-back-n window are resent, although some packets may be received successfully at the receiver side. This duplication may increase the congestion in the network and making it worse.

Therefore, Selective repeat window should be adopted as it sends the specific packet that may have been lost.

3. Discarding Policy: A good discarding policy adopted by the routers is that the routers may prevent congestion and at the same time partially discards the corrupted or less sensitive package and also able to maintain the quality of a message.

In case of audio file transmission, routers can discard less sensitive packets to prevent congestion and also maintain the quality of the audio file.

4. Acknowledgment Policy: Since acknowledgement are also the part of the load in network, the acknowledgment policy imposed by the receiver may also affect congestion.

Several approaches can be used to prevent congestion related to acknowledgment.

The receiver should send acknowledgement for N packets rather than sending acknowledgement for a single packet. The receiver should send a acknowledgment only if it has to sent a packet or a timer expires.

5. Admission Policy: In admission policy a mechanism should be used to prevent congestion. Switches in a flow should first check the resource requirement of a network flow before transmitting it further. If there is a chance of a congestion or there is a congestion in the network, router should deny establishing a virtual network connection to prevent further congestion.

All the above policies are adopted to prevent congestion before it happens in the network.

Closed Loop Congestion Control

Closed loop congestion control technique is used to treat or alleviate congestion after it happens. Several techniques are used by different protocols; some of them are:

1. Backpressure: Backpressure is a technique in which a congested node stop receiving packet from upstream node. This may cause the upstream node or nodes to become congested and rejects receiving data from above nodes. Backpressure is a node-to-node congestion control technique that propagate in the opposite direction of data flow. The backpressure technique can be applied only to virtual circuit where each node has information of its above upstream node.

In above diagram the 3rd node is congested and stops receiving packets as a result 2nd node may be get congested due to slowing down of the output data flow. Similarly 1st node may get congested and informs the source to slow down.

2. Choke Packet Technique: Choke packet technique is applicable to both virtual networks as well as datagram subnets. A choke packet is a packet sent by a node to the source to inform it of congestion. Each router monitor its resources and the utilization at each of its output lines. whenever the resource utilization exceeds the threshold value which is set by the administrator, the router directly sends a choke packet to the source giving it a feedback to reduce the traffic. The intermediate nodes through which the packets has traveled are not warned about congestion.

3. Implicit Signaling: In implicit signaling, there is no communication between the congested nodes and the source. The source guesses that there is congestion in a network. For example when sender sends several packets and there is no acknowledgment for a while, one assumption is that there is a congestion.

4. Explicit Signaling: In explicit signaling, if a node experiences congestion it can explicitly sends a packet to the source or destination to inform about congestion. The difference between choke packet and explicit signaling is that the signal is included in the packets that carry data rather than creating different packet as in case of choke packet technique.

Explicit signaling can occur in either forward or backward direction.

- **Forward Signaling:** In forward signaling signal is sent in the direction of the congestion. The destination is warned about congestion. The reciever in this case adopt policies to prevent further congestion.
- **Backward Signaling:** In backward signaling signal is sent in the opposite direction of the congestion. The source is warned about congestion and it needs to slow down.

Q.1. (e) Are both UDP and IP unreliable to the same degree ? Why or why not ? (5)

Ans. UDP is layer 4 protocol and IP is layer 3 of TCP/IP model. You cannot compare them because they server different purposes. And anyways, protocols are not unreliable,

dotnotes.xyz

it's the medium through which data transmission occurs, that is unreliable. So, UDP transmits its data over this unreliable medium and forgets about it. On the other hand, TCP also transmits data over unreliable medium, but it makes sure data reaches other side by making use of Acknowledgements.

IP encapsulates the data sent by above layer (TCP, UDP, etc.), chunks it (if required), adds its own header and sends it to Layer 2. So, if data sent by IP is not received by destination and you are using TCP, you will have to send it again. But, if you are using UDP, you just send it once.

When IP sends a packet, it receives a confirmation for each packet and, if needed, rebroadcast the packet. This makes it reliable. UDP does not get confirmation. It broadcast each packet only once and assumes that it get to you. This makes it less reliable then IP because it does not check for problems or rebroadcast.

Q.2. (a) What are the advantages of fiber optics over copper as a transmission medium? Is there any downside of using fiber optics over copper ? (6.25)

Ans. Advantages of Fiber Optic Transmission—

Optical fibers have largely replaced copper wire communications in core networks in the developed world, because of its advantages over electrical transmission. Here are the main advantages of fiber optic transmission.

Extremely High Bandwidth: No other cable-based data transmission medium offers the bandwidth that fiber does. The volume of data that fiber optic cables transmit per unit time is far great than copper cables. Longer Distance: in fiber optic transmission, optical cables are capable of providing low power loss, which enables signals can be transmitted to a longer distance than copper cables. Resistance to Electromagnetic Interference: in practical cable deployment, it's inevitable to meet environments like power substations, heating, ventilating and other industrial sources of interference. However, fiber has a very low rate of bit error (10 EXP-13), as a result of fiber being so resistant to electromagnetic interference. Fiber optic transmission is virtually noise free. Low Security Risk: the growth of the fiber optic communication market is mainly driven by increasing awareness about data security concerns and use of the alternative raw material. Data or signals are transmitted via light in fiber optic transmission. Therefore there is no way to detect the data being transmitted by "listening in" to the electromagnetic energy "leaking" through the cable, which ensures the absolute security of information. Small Size: fiber optic cable has a very small diameter. For instance, the cable diameter of a single OM3 multimode fiber is about 2mm, which is smaller than that of coaxial copper cable. Small size saves more space in fiber optic transmission.

Light Weight: fiber optic cables are made of glass or plastic, and they are thinner than copper cables. These make them lighter and easy to install. Easy to Accommodate: Increasing Bandwidth: with the use of fiber optic cable, new equipment can be added to existing cable infrastructure. Because optical cable can provide vastly expanded capacity over the originally laid cable. And WDM (wavelength division multiplexing) technology, including CWDM and DWDM, enables fiber cables the ability to accommodate more bandwidth.

Disadvantages of Fiber Optic Transmission

Though fiber optic transmission brings lots of convenience, its disadvantages also cannot be ignored.

Fragility: Usually optical fiber cables are made of glass, which lends to they are more fragile than electrical wires. In addition, glass can be affected by various chemicals including hydrogen gas (a problem in underwater cables), making them need more care when deployed under ground. Difficult to Install: it's not easy to splice fiber optic cable. And if you bend them too much, they will break. And fiber cable is highly susceptible to becoming cut or damaged during installation or construction activities. All these make

it difficult to install. Attenuation & Dispersion: as transmission distance getting longer, light will be attenuated and dispersed, which requires extra optical components like EDFA to be added. Cost Is Higher Than Copper Cable: despite the fact that fiber optic installation costs are dropping by as much as 60% a year, installing fiber optic cabling is still relatively higher than copper cables. Because copper cable installation does not need extra care like fiber cables. However, optical fiber is still moving into the local loop, and through technologies such as FTTx (fiber to the home, premises, etc.) and PONs (passive optical networks), enabling subscriber and end user broadband access.

Special Equipment Is Often Required: to ensure the quality of fiber optic transmission, some special equipment is needed. For example, equipment such as OTDR (optical time-domain reflectometry) is required and expensive, specialized optical test equipment such as optical probes and power meter are needed at most fiber endpoints to properly provide testing of optical fiber.

Q.2. (b) What is the remainder obtained by dividing x^7+x^5+1 by the generator polynomial x^3+1 ? (6.25)

Ans.

$$M(x) = x^7+x^5+1$$
$$G(x) = x^3+1$$

Since degree of $G(x)$ is $r = 3$, append 3 zero bits to the lower end of $M(x)$.

Frame = 10100001

Generator = 1001

Message after 3 zero bits are appended: 10100001000

```
1001)10100001000
     1001
      0110
      0000
       1100
       1001
        1010
        1001
         0111
         0000
          1110
          1001
           1110
           1001
            1110
            1001
             111
```

The remainder obtained by dividing x^7+x^5+1 by generator polynemial x^3+1 is 111.

Q.3. (a) What are the disadvantages of of using small, fixed length cells in ATM? (6.25)

Ans. ATM is not contention-based or shared like FDDI, ethernet or token ring. A full 155 Mbps is continuously available to every endstation. ATM transmits fixed-length 53 bytes cells. It consists of a header field (5 bytes) and information field of 48 bytes. The header field contains routing info and the information field carries the service data. Small fixed length cells facilitate efficient multiplexing and a traffic prioritization scheme ensures delay-sensitive traffic receives special consideration. Multiplexing

dotnotes.xyz

techniques allow more than one service to share a particular ATM link at any given time. Services are organized into virtual channels(VC) and virtual paths(VP). A VC identifies the service and a VP identifies a collection of VC's. ATM can be switched at both the VP and VC level.

ATM uses cell switches, not bridges or routers. Switching is done by connecting one port to another directly. All this is done in hardware which makes it more efficient and faster. Bridges and routers also introduce latency/delays. This is because bridges and routers normally process large/variable length packets. These large packets introduce noticeable application delay to a user.

In Ehternet or FDDI rings, media is shared. As more stations are added, available bandwidth to each station decreases. When this happens, we normally segment the network into smaller peices by adding bridges and routers. However, these now increases latency since packets must cross more devices between endstations. Additionally, adding more routers/bridges means adding more subnets and additional complexity. So traditonal networks scales poorly. As we add more bandwidth by adding more devices like bridges and routers, we suffer from higher latency, worse performance end to end and added complexity to a network.

ATM is scalable and inherently exhibits low latentcy. ATM networks are not contention-based. There are built on point-to-point connections between endstations and switches. Each connection runs at a full guaranteed 155Mbps even through a switch. Stations are added by plugging in to an unused port or additional port modules. Also good ATM switches can tie switches/modules together to act like a bigger switch. Also switch-to-switch rates normally can run faster than 155 Mbps.

Price of ATM technology is dropping rapidly. Price of an ATM adapter card is about the cost of an Ethernet NIC card in 1983.

There are several advantages to the use of small, fixed-size cells. First, the use of small cells may reduce queuing delay for a high-priority cell, since it waits less if it arrives slightly behind a lower-priority cell that has gained access to a resource (such as the transmitter). Second, it appears that fixed-size cells can be switched more efficiently which is important for the very high data rates of ATM.

Q.3. (b) Compare and contrast HDLC with PPP. Which one is byte-oriented;which one is bit oriented ? **(6.25)**

Ans. The major difference between HDLC and PPP is that HDLC is the bit oriented protocol, while PPP is the character-oriented protocol. The HDLC and PPP are the crucial data link layer protocols used in WAN (wide area network) where the HDLC can also be implemented with PPP for the efficient results.

HDLC describes the encapsulation technique employed on the data in the synchronous serial data link. On the other hand, the PPP protocol deals with the encapsulation of the data transported in the point-to-point links and it could be synchronous or asynchronous.

Content: HDLC Vs PPP

1. Comparison Chart
2. Definition
3. Key Differences
4. Conclusion

Comparison Chart

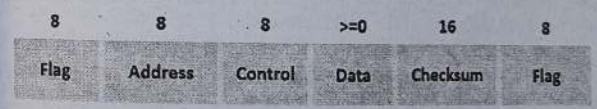
Basis for comparison	HDLC	PPP
Expands to	High-level Data Link Layer Protocol	Point-to-Point Protocol
Type of protocols	Bit-oriented protocol	Byte oriented protocol
Used in	Only synchronous media	Synchronous as well as asynchronous media
Authentication	No provision of authentication	Provides authentication
Dynamic addressing	Does not offer dynamic addressing.	Dynamic addressing is used.
Implemented in	Point-to-point and multipoint configurations.	Only point-to-point configurations.
Compatibility with other protocols	Can not be operated with non-Cisco devices.	Interoperable with non-Cisco devices also.

Definition of HDLC:

HDLC (High-level Data Link Control) is a WAN protocol intended to perform the encapsulation of the data in the data link layer. The encapsulation of the data means to change the format of the of the data. SDLC is the predecessor of the HDLC which stands for the **Synchronous Data Link Control protocol**. Both SDLC and HDLC protocol are developed by IBM and submitted to the ANSI and ISO for the acceptance as the international standards.

The HDLC protocol follows the bit-oriented concept and uses bit stuffing for achieving data transparency. Here bit oriented approach signifies that the single bit is used to present the control information. The frame structure of HDLC contains the address, control, data, checksum and flag fields. The default encapsulation protocol in the Cisco devices is the HDLC. The Cisco proprietary HDLC only works when the devices in both of the ends of the link are of cisco. Standard HDLC can have different devices in the ends.

Frame format for the bit-oriented protocols



Frame format for HDLC protocol

- **Address field** – It is used to describe the terminal.
- **Control field** – The bits in the control field is intended for the sequence number and acknowledgements.
- **Data field** – This field is used to hold the information.
- **Checksum field** -In this field, the bits are reserved for the performing the cyclic redundancy code.

HDLC Commands and Requests

The HDLC uses a group of commands and responses for its working. There are three types of frames information, supervisory and unnumbered.

dotnotes.xyz

- **Information transfer format (I-Frame)** - It transports the numbered fra in a sequential manner, which contain the information field.
- **Supervisory format (S-Frame)** - The supervisory frames conduct managerial functions such as acknowledgement, information transfer status, poll and error recovery. The commands and requests included in this are RECEIVE READ RECEIVE NOT READY, REJECT, etcetera.
- **Unnumbered format (U-Frame)** - It basically extends the data link co functions. There several commands and requests fall under this category such as RES TEST, FRAME REJECT, REQUEST DISCONNECT, etcetera.

Definition of PPP: PPP (Point-to-Point Protocol) is also a WAN protocol, but are several enhancements made in the PPP protocol after HDLC. Priorly, the protocol is not proprietary, which means that it can be used with two different by devices without committing changes over the format of the data. All of the collaboratively treated as single, independent IP network which is having its own format, hardware addressing method, and data link protocol. A point-to-point conn is obtained without assigning multiple IP addresses to the tangible wires, and needs the IP network number.

There are several features of PPP, which are discussed below.

- To clearly identify the start and end of the frame, the framing method is us the asynchronous data. It is also beneficial in the detection of the errors.
- A link control protocol is used for enabling the network lines, testing terminate them when no longer used. This link control protocol is basically he handling the synchronous and asynchronous circuits, and byte and bit-oriented erro
- It can select the NCP (Network Control Protocol) for each supported netwo

Frame format for the PPP

Bytes	1	1	1	1 or 2	Variable	2 or 4	1
	Flag	Address	Control	Protocol	Payload	Checksum	Flag

Frame format for PPP protocol

The PPP frame contains two flag fields, a protocol filed to determine the packet residing in the payload, and a payload field which can variate. However, of the fields are the same as the HDLC protocol.

Working of the PPP protocol

- The User first calls the internet service provider's router to establish the connection; the request goes through the modem.
- After the generation of the reply by the router's modem, the physical con is established.
- User device sends a set of LCP packets in the payload field of one or mo frames sequence wise.
- The PPP parameters are chosen according to the packets and their resp
- After selecting PPP parameters, the NCP packets are delivered configuration of the network layer.
- Then the IP addresses are dynamically assigned with the help of the NC newly attached devices for the duration of its login by the provider.
- Now the device is an internet host and is able to send and receive the IP
- At, the NCP ends the network layer connection and spares the IP addr

Key Differences Between HDLC and PPP

1. The HDLC is a bit-oriented protocol while PPP is byte-oriented as well as bit ented because it can be sent over the dial-up modem lines and also true bit-oriented HDLC.
2. Only synchronous media can be used in HDLC. In contrast, PPP can work with chronous and asynchronous media.
3. No link authentication is provided in HDLC, whereas it is provided in PPP.
4. PPP can dynamically assign and frees up the IP address according to the use. As ainst, this not the case in HDLC.
5. Interoperability between the non-cisco devices in HDLC is not achievable. wever, this limitation of HDLC is eliminated from the PPP protocol.

Q.4. (a) Compare and contrast the Go-Back-N ARQ protocol with selective-peat ARQ.

Ans. Refer to Q.no. 4(b) First Term Examation 2018. **(6.25)**

Q.4. (b) Explain why collision is an issue in a random access protocol but t in controlled access or channeliazing protocols. **(6.25)**

Ans. In random access or contention methods, no station is superior to another ation and none is assigned the control over another. No station permits, or does not rmit, another station to send. In a random access method, each station has the right the medium without being controlled by any other station. There is no scheduled time a station to transmit. Transmission is random among the stations. That is why these thods are called random access. Also, no rules specify which station should send next. tations compete with one another to access the medium. That is why these methods e also called contention methods. Protocols in this category : ALOHA, CSMA, CSMA/ D, CSMA/CA.

Channelization is a multiple-access method in which the available bandwidth of a nk is shared in time, frequency, or through code, between different stations. Protocols this category: FDMA, TDMA, and CDMA

In random access methods, there is no access control (as there is in controlled access thods) and there is no predefined channel (as in channelization). Each station can ansmit when it desires. This liberty may create collision.

In random access method, there is no control over which station holds the link, any ation can randomly use the link, which may even cause collision. In controlled access rotocol, there is a primary station that controls the link, and decides which station s the link at a given time, thus reducing chances of collision

In a random access method, the whole available bandwidth belongs to the station hat wins the contention; the other stations need to wait. In a channelization method, he available bandwidth is divided between the stations. If a station does not have data send, the allocated channel remains idle.

In controlled access protocol, the whole available bandwidth belongs to the primary ation (the sation with control to the link). In channelization protocol, available andwidth is divided between stations. If a station does not have data to send the llocated channel remains idle. We do not need a multiple access method in this case. The local loop provides a dedicated point-to-point connection to the telephone office.

Q.5. (a) Explain the similarities and differences between bridge and router in detail. **(6.25)**

dotnotes.xyz

Ans. The basic difference between Bridge and Router is that Bridge is a network device mainly operating at the data link layer of the OSI model with filtering and forwarding capabilities.

While Router is an internetworking device operating at the network layer of the OSI model. A router is attached to the two or more networks and forwards packets from one network to another.

Difference Between Bridge and Router

The basic difference between Bridge and Router is that Bridge is a network device mainly operating at the data link layer of the OSI model with filtering and forwarding capabilities.

While Router is an internetworking device operating at the network layer of the OSI model. A router is attached to the two or more networks and forwards packets from one network to another.

Content: Bridge Vs Router

1. Comparison Chart
2. Definition
3. Key Differences
4. Conclusion

Comparison Chart

Basis for comparison	Bridge	Router
Operates on	Data link layer	Network layer
Store and Forward	Frame	Packet
Transparency station	Bridges are protocol independent and transparent to the end stations.	Routers do not provide transparency.
Reads	MAC address of the device	IP address of the device
Works on	Single broadcast domain	More than one broadcast domain

Definition of Bridge: A bridge is a networking device for connecting two segments of a network and transmitting data between them. Bridge operate in both the physical and the data link layers of OSI model. There is a compulsion of using identical protocols for the segments to communicate. The primary use of a bridge is to send, filter, or flood any arriving frame depending on the MAC address of that specific frame.

The frames can be transferred between two originally separate LANs by a bridge. However, bridges incorporate logic that permits them to retain the traffic for each segment separately. When a frame enters in a bridge interface, it checks the destination MAC address and forwards the late copy to the segment to which the address belongs. Bridges are also apparent to the end stations.

Bridges are hardware based, and it uses specialized hardware called ASIC (Application specific integrated circuit) chip to maintain MAC address table and to make filtering decision. Bridged network fragments collision domains, but do not fragment broadcast domains, instead forward all broadcasts.

Types of bridges:

• Simple Bridges are the predecessor of its other types and the least expensive type of bridge. A simple bridge connects two segments and contains a table that lists the addresses of all the stations included in each of them. What makes it primitive is that these addresses must be entered manually.

• Multiport Bridge is employed when we want to link more than two LANs, and each table is containing the physical addresses of stations approachable through the particular port.

• Transparent Bridge performs its bridging functions and creates its own table of station addresses.

Definition of Router: A router can be defined as a Network layer mechanism, be it software or hardware, using metrics to decide the best path to use for transmission of network traffic.

A router is a device that routes or forward data from one network to other based on their IP address. When Data packet is received from the router, the router inspects the data's IP address and determines if the packet is meant for its own network then it receives the data, or if the data is for another network, then it transfers the data to the other network. It means that routers only forward the data if destination computer is the intended user.

Routers have access to network layer addresses and contain software that enables them to determine which of the several possible paths between those addresses is the best for the particular transmission.

Routers break up broadcast and collision domains. It means broadcasts are not forwarded through the router, by default. It also provides connections for the virtual LANs (VLANs).

Key Differences Between Bridge and Router

1. Bridge functions at Data link layer while router operates at the Network layer of the OSI model.
2. The bridge can relay frame from one segment to another whereas Router store and forward packets.
3. Routers are not transparent to the end stations. In contrast, Bridges are transparent to the end stations and does not rely on the protocol.
4. In a bridge, frames are forwarded on the basis of the MAC address of the frame. As against, Router checks logical address (i.e., IP address) of the packets.
5. The router can work on more than broadcast domain while Bridge can work on a single broadcast domain.

Q.5. (b) What is quality of services and what are general techniques to improve quality of service ? (6.25)

Ans. QoS is an overall performance measure of the computer network.

Important flow characteristics of the QoS are given below:

1. Reliability: If a packet gets lost or acknowledgement is not received (at sender), the re-transmission of data will be needed. This decreases the reliability.

The importance of the reliability can differ according to the application.

For example:

E- mail and file transfer need to have a reliable transmission as compared to that of an audio conferencing.

2. Delay: Delay of a message from source to destination is a very important characteristic. However, delay can be tolerated differently by the different applications.

For example:

The time delay cannot be tolerated in audio conferencing (needs a minimum time delay), while the time delay in the e-mail or file transfer has less importance.

dotnotes.xyz

3. Jitter: The jitter is the variation in the packet delay.

If the difference between delays is large, then it is called as high jitter. On the contrary, if the difference between delays is small, it is known as low jitter.

Example:

Case1: If 3 packets are sent at times 0, 1, 2 and received at 10, 11, 12. Here, the delay is same for all packets and it is acceptable for the telephonic conversation.

Case2: If 3 packets 0, 1, 2 are sent and received at 31, 34, 39, so the delay is different for all packets. In this case, the time delay is not acceptable for the telephonic conversation.

4. Bandwidth: Different applications need the different bandwidth.

For example:

Video conferencing needs more bandwidth in comparison to that of sending an e-mail.

Integrated Services and Differentiated Service

These two models are designed to provide Quality of Service (QoS) in the network.

1. Integrated Services(IntServ)

Integrated service is flow-based QoS model and designed for IP.

In integrated services, user needs to create a flow in the network, from source to destination and needs to inform all routers (every router in the system implements IntServ) of the resource requirement.

Following are the steps to understand how integrated services works.

(i) Resource Reservation Protocol (RSVP): An IP is connectionless, datagram, packet-switching protocol. To implement a flow-based model, a signaling protocol is used to run over IP, which provides the signaling mechanism to make reservation (every applications need assurance to make reservation), this protocol is called as RSVP.

(ii) Flow Specification: While making reservation, resource needs to define the flow specification. The flow specification has two parts:

(a) Resource specification: It defines the resources that the flow needs to reserve. For example: Buffer, bandwidth, etc.

(b) Traffic specification: It difines the traffic categorization of the flow.

(iii) Admit or deny

After receiving the flow specification from an application, the router decides to admit or deny the service and the decision can be taken based on the previous commitments of the router and current availability of the resource.

Classification of services: The two classes of services to define Integrated Services are:

(a) Guaranteed Service Class: This service guarantees that the packets arrive within a specific delivery time and not discarded, if the traffic flow maintains the traffic specification boundary.

This type of service is designed for real time traffic, which needs a guaranty of minimum end to end delay.

For example: Audio conferencing.

(b) Controlled Load Service Class: This type of service is designed for the applications, which can accept some delays, but are sensitive to overload network and to the possibility to lose packets.

For example: E-mail or file transfer.

Problems with Integrated Services.

The two problems with the Integrated services are:

(i) **Scalability**

In Integrated Services, it is necessary for each router to keep information of each flow. But, this is not always possible due to growing network.

(ii) Service- Type Limitation

The integrated services model provides only two types of services, guaranteed and control-load.

2. Differentiated Services (DS or Diffserv):

- DS is a computer networking model, which is designed to achieve the scalability in managing the network traffic.
- DS is a class based QoS model specially designed for IP.
- DS was designed by IETF (Internet Engineering Task Force) to handle the problems of Integrated Services.

The solutions to handle the problems of Integrated Services are explained below:

(i) Scalability: The main processing unit can be moved from central place to the edge of the network to achieve the scalability. The router does not need to store the information about the flows and the applications (or the hosts) define the type of services they want every time while sending the packets.

(ii) Service Type Limitation: The routers, route the packets on the basis of class of services define in the packet and not by the flow. This method is applied by defining the classes based on the requirement of the applications.

Q.6. (a) An organization is granted the block 211.17.180.0/24. The administrator wants to create 32 subnets. **(6)**

(i) Find the subnet mask

(ii) Find the no. of addresses in each subnet.

(iii) Find the first and last addresses in subnet 1

(iv) Find the first and last addresses in subnet 32.

Ans. 211.17.180.0

Class C Address

(a) Subnet Mask 255-255-255-10

11111111 . 011111111 . 011111111 . 00000000

(b) No. of address

$$= 2^{32-n}$$

Here $n = 24$

$\therefore$ $2^{32-24} = 2^8 = 256$ (is the no. of addresses)

(c) 11111111 . 011111111 . 011111111 . 011111 000

0	0	0	0	0
0	0	0	0	1
0	0	0	1	0
0	0	0	1	1

dotnotes.xyz

Subnet

1.	First address.	Last address
	211.17.180.0/24	211.17.18.255/24 subnet

(d) 211.17.180.0/24 32 subnets

Q.6. (b) Explain distance vector and link state routing protocols. What are the merits and demerits of the both protocols ? (6.5)

Ans. Refer Q.1. (h) of End Term Exam. 2017. (P. No.- 13-2017.)

Q.7. (a)In case where reliability is not of primary importance,UDP would make a good transport protocol. Give examples of specific cases. (6)

Ans. The User Datagram Protocol (UDP) is a connectionless, unreliable transport protocol. It performs very limited error checking. If UDP is so powerless, why would a process want to use it? UDP is a very simple protocol using a minimum overhead. If a process wants to send a small message and does not care much about reliability, it can use UDP. Sending a small message by using UDP takes much less interaction between the sender and receiver than using TCP. Example Reliability is not of primary importance in applications such as echo, daytime, Users, TFTP (trivial file transfer protocol) and SNMP (simple network management protocol).

So here is the solution to the problem. Part1) Reliability is the not at all the primitive concern in many applications like Bootstrap Protocol, Simple Network Management Protocol , Trivial File Transfer Protocol .But in case of custom made software reliability plays very important role in client-server applications are help in building up the reliability and provide a low over head service. Part2) Both UDP and IP are connectionless and unreliable protocols. The difference b/w them is that in case of UDP it calculates the check sum for the entire datagram but the scenario is different in case of IP it only calculates the checksum of the IP header. Part3) There is no need of Port addresses to be unique universally and is used with the IP address .

Q.7. (b) Explain the IPV4 protocol with header format . Compare it with IPV6. (6.5)

Ans. Refer Q.8. (a) of End Term Examation 2017.

Q.8. (a) What are the different elements of transport layer protocols ? (6)

Ans. Elements of transport protocols (etp)

- Transport <> Data Link.
- Addressing.
- Establishing a connection.
- Releasing a connection.
- Flow control and buffering.
- Multiplexing.
- Crash recovery.

In detail-

The transport service is implemented by a transport protocol.

1. Addressing in TCP and UDP

A typical host has many application processes running on it. These processes generate data that is sent to either TCP or UDP, which in turn passes it to IP for transmission. This multiplexed stream of datagrams is sent out by the IP layer to various destinations.

Similarly, a device's IP layer receives datagrams, these datagrams need to be de-multiplexed, so they end up at the correct process on the device that receives them.

2. Multiplexing and De-multiplexing Using Ports:

The question is: How do we de-multiplex a sequence of IP datagrams that need to go to different application processes on the same host? Let's consider a particular host bearing the IP address 24.156.79.20. How does the IP layer know which packet goes to which process on the same host?

The first part of the answer lies in the Protocol field included in the header of each IP datagram. This field carries a code that identifies the protocol that sent the data. Since most end-user applications use TCP or UDP at the transport layer, the Protocol field in a received datagram tells IP to pass data to either TCP or UDP as appropriate.

But both TCP and UDP are used by many applications at once. This means TCP or UDP must figure out which process to send the data to. To make this possible, an additional addressing element is necessary. This transport layer address is called a port.

A port can also be called a TSAP (Transport Service Access Point). An IP address can also be called a NSAP (Network Service Access Point). Key Concept: TCP/IP transport layer addressing is accompanied using TCP and UDP ports. Each port number within a particular IP device identifies a particular application process.

3. Source Port and Destination Port Numbers:

In both UDP and TCP messages, two addressing fields appear, for a Source Port and a Destination Port. These are analogous to the fields for source address and destination address at the IP level, but at a higher level of detail. While the source address and destination address at the IP level identify the source machine and the destination machine; The Source Port and a Destination Port identify the originating process on the source machine, and the destination process on the destination machine.

TCP and UDP port numbers are 16-bits in length.

Summary of Port Numbers for Datagram Transmission and Reception: So, to summarize, here's the basics of how transport-layer addressing (port addressing) works in TCP and UDP:

(a) Sending Datagrams: An application specifies the source and destination port it wishes to use for the communication. These are encoded into the TCP or UDP header, depending on which transport layer protocol the application is using. When TCP or UDP passes data to IP, IP indicates the protocol type (TCP or UDP) in the Protocol field of the IP datagram. The source and destination port numbers are encapsulated as part of the TCP or UDP message, Within the IP datagram's data area.

(b) Receiving Datagrams: The IP software receives the datagram, inspects the Protocol field and decides to which protocol the datagram belongs (TCP or UDP). TCP or UDP receives the datagram and passes its contents to the appropriate process based on the destination port number.

FLOW CONTROL and BUFFERING

1. Buffering

(a) Sender:

i. In case of an unreliable network service the sending transport entity must buffer all TPDU's as it might need to retransmit them.

ii. In case of a reliable network service the sender may/may not buffer outgoing TPDU's.

(b) Receiver:

i. If all TPDU's are of same size, there will be a pool of identically sized buffers (one TPDU per buffer).

dotnotes.xyz

ii. If there is a wide variation in the TPDU sizes, variable sized buffer are used.

iii. Another option is to dedicate a single large buffer per connection.

2. Dynamic Buffer Management

In cases where traffic patterns change, the sender and receiver need to dynamically adjust their buffer allocations.

Working:

(a) Sender requests receiver to allocate certain number of buffers to it.

(b) The receiver depending on its load allocates as many buffers as possible.

(c) When the sender sends a TPDU it decrements its allocation.

(d) When the sender finishes its allocated quota it stops sending.

(e) The receiver piggybacks acknowledgement and further buffer allocations on the reverse traffic. There might be a case where there are sufficient buffers at the sender and receiver but the subnet is congested. Therefore, along with buffering, flow control should also concentrate on the carrying capacity of the subnet.

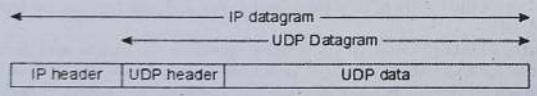
3.Multiplexing

(a) Upward Multiplexing: If only one network address is available on a host all the transport connections on that machine use that single address. When a TPDU comes in, upward multiplexing is used to decide which process to give it to.

(b) Downward Multiplexing: Assume that a subnet uses virtual circuits internally and a maximum data rate is imposed on each one. If a user needs more bandwidth than what a single virtual circuit can provide, downward multiplexing can be used to open multiple network connection and distribute the traffic among them.

Q.8. (b) Discuss the header panel of UDP. **(6.5)**

Ans. UDP header: UDP is a simple, datagram-oriented, transport layer protocol: each output operation by a process produces exactly one UDP datagram, which causes one IP datagram to be sent. The encapsulation of a UDP datagram as an IP datagram looks like this:

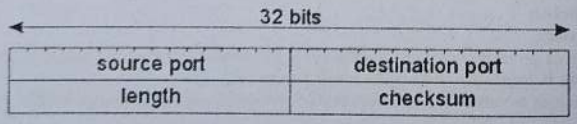


UDP encapsulation

UDP Header Format

Each UDP message is called a user datagram. Conceptually, a user datagram consists of two parts: a UDP Header and a UDP data area. The header is divided in four 16-bit fields as shown:

UDP header format



Source and Destination Port: The port numbers identify the sending process and the receiving process. TCP and UDP use the destination port number to demultiplex incoming data from IP. Since IP has already demultiplexed the incoming IP datagram to either TCP or UDP (based on the protocol value in the IP header), this means the TCP

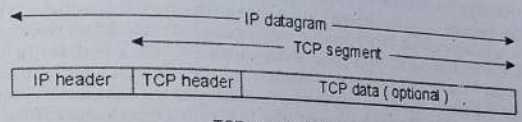
port numbers are looked at by TCP, and the UDP port numbers by UDP. The TCP port numbers are independent of the UDP port numbers.

Length: The length in bytes of the UDP header and the encapsulated data. The minimum value for this field is 8.

Checksum: This is computed as the 16-bit one's complement of the one's complement sum of a pseudo header of information from the IP header, the UDP header, and the data, padded as needed with zero bytes at the end to make a multiple of two bytes. If the checksum is set to zero, then checksuming is disabled. The designers chose to make the checksum optional to allow implementations to operate with little computational overhead. If the computed checksum is zero, then this field must be set to 0xFFFF.

Q.9. Discuss the header format of TCP. **(12.5)**

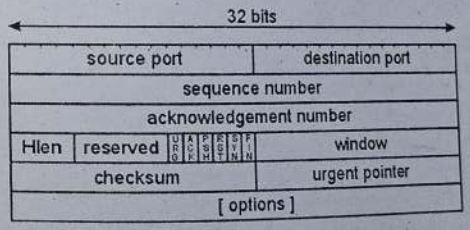
Ans. TCP Header: TCP is the primary transport protocol used to provide reliable, full-duplex connections. The most common use of TCP is to exchange TCP data encapsulated in an IP datagram. Although IP is implemented on both hosts and routers, TCP is typically implemented on hosts only to provide reliable end-to-end data delivery. The unit of transfer between the TCP software on two machines is called a TCP segment. Segments are exchanged to establish connections, transfer data, send acknowledgements, advertize window sizes and close connections.



TCP encapsulation

Each TCP segment, encapsulated in an IP datagram, has a TCP header - 20 bytes long, unless options are present. Let's look at the standard header format in more detail. We will come back to the practical use of this format using a simple case study, after handling the process of connecting and disconnecting two TCP applications as well as the data flow control mechanisms in TCP.

TCP header format



Source and Destination Port Number: Identification of the sending and receiving application. Along with the source and destination IP addresses in the IP - header identify the connection as a socket.

dotnotes.xyz

Sequence Number: The sequence number of the first data byte in this segment. If the SYN bit is set, the sequence number is the initial sequence number and the first data byte is initial sequence number + 1.

Acknowledgement Number

If the ACK bit is set, this field contains the value of the next sequence number the sender of the segment is expecting to receive. Once a connection is established this is always sent.

Hlen: The number of 32-bit words in the TCP header. This indicates where the data begins. The length of the TCP header is always a multiple of 32 bits.

Flags: There are six flags in the TCP header. One or more can be turned on at the same time.

URG	The URGENT POINTER field contains valid data
ACK	The ackowledgement number is valid
PSH	The receiver should pass this data to the application as soon as possible
RST	Reset the connection
SYN	Synchronize sequence numbers to initiate a connection.
FIN	The sender is finished sending data.

Window: This is the number of bytes, starting with the one specified by the acknowledgment number field, that the receiver is willing to accept. This is a 16-bit field, limiting the window to 65535 bytes.

Checksum: This covers both the header and the data. It is calculated by prepending a pseudo-header to the TCP segment, this consists of three 32 bit words which contain the source and destination IP addresses, a byte set to 0, a byte set to 6 (the protocol number for TCP in an IP datagram header) and the segment length (in words). The 16-bit one's complement sum of the header is calculated (i.e., the entire pseudo-header is considered a sequence of 16-bit words). The 16-bit one's complement of this sum is stored in the checksum field. This is a mandatory field that must be calculated and stored by the sender, and then verified by the receiver.

Urgent Pointer: The urgent pointer is valid only if the URG flag is set. This pointer is a positive offset that must be added to the sequence number field of the segment to yield the sequence number of the last byte of urgent data. TCP's urgent mode is a way for the sender to transmit emergency data to the other end. This feature is rarely used.

dotnotes.xyz

FIRST TERM EXAMINATION [FEB. 2019]
SIXTH SEMESTER [B.TECH]
COMPUTER NETWORK [ETCS–306]

ime : 1.5 hrs. M.M. : 30

ote: *Attempt Q.No. 1 which is compulsory and any two more questions from the remaining.*

Q.1. (a) What is the difference between Message switching and Packet witching? (2)

Ans. Refer Q.No. 1(b), First Term Examination 2018.

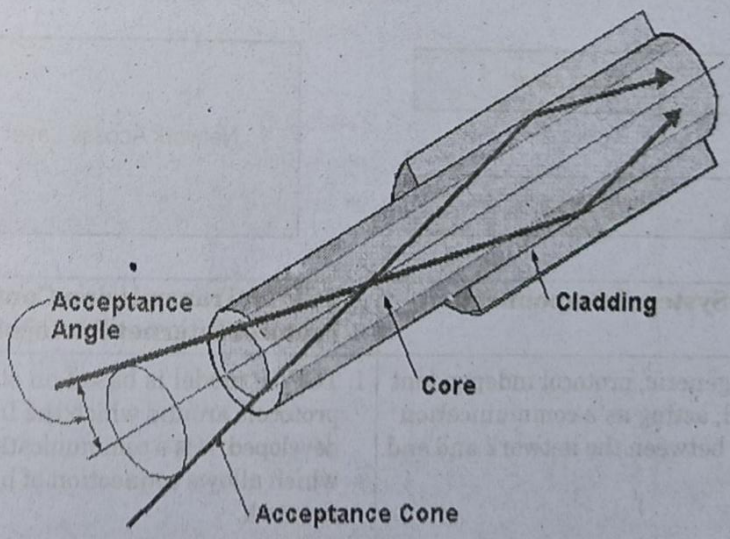
Q.1. (b) We need to send 256 kbps over a noiseless channel with a bandwidth 20 kHz. How many signal levels do we need? (2)

Ans. Nyquist bit rate for noiseless channel:

$$\text{Bitrate} = 2 * \text{Bandwidth} * \log_2(\lambda)$$
$$265 \text{ kbps} = 2 * (20 \text{ KHz}) * \log_2(\lambda)$$
$$265000 = 2 * (20.000) * \log_2(\lambda)$$
$$\Rightarrow \quad \log_2(\lambda) = 6.628$$
$$\Rightarrow \quad \lambda = 26.625 = 987 \text{ levels.}$$

Q.1. (c) Justify the purpose of cladding in an optical fiber? Discuss its density elative to the core. (2)

Ans. An optical fiber has two layers, the inner layer and the outer layer. The inner yer is called core. The data pass through a core. This core is made of dense of glass or astic. The outer layer of a fiber is called cladding. It is also made of glass or plastic. s glass or plastic is less dense. Cladding is used in optical fiber for prevent any fraction while passing data. The function of cladding is to occur full internal reflection optical fiber. That is why a cladding's density is lower then core.



Q.1. (d) Give the relationship between propagation time and propagation eed? (2)

Ans. Propagation speed is the amount of time it takes for one particular signal to t from one point to another. Transmission Rate is the total amount of data that can be nt from one place to another in a given period of time.

dotnotes.xyz

Q.1. (e) Compare the probability of successful transmission of data packet and maximum efficiency of slotted ALOHA over pure ALOHA?

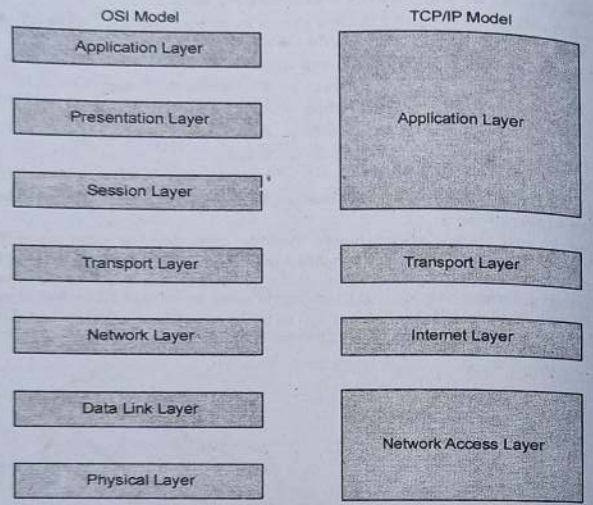
Ans. Refer Q.1. (e) End Term Examination 2019. (2)

Q.2. (a) For 'n' devices in a network, what is the number of Input-Output ports required for each device in a mesh, ring, bus and star topology?'

Ans. Refer Q.2. (a) First Term Examination 2018. (2)

Q.2. (b) Compare the OSI reference model and TCP/IP model while discussing layered architecture. (5)

Ans. Diagrammatic Comparison between OSI Reference Model and TCP/IP Reference Model



OSI(Open System Interconnection)	TCP/IP(Transmission Control Protocol/Internet Protocol)
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
2 In OSI model the transport layer guarantees the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3. Follows vertical approach.	3. Follows horizontal approach.

4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.
5. Transport Layer is Connection Oriented	5. Transport Layer is both Connection Oriented and Connection less.
6. Network Layer is both Connection Oriented and Connection less.	6. Network Layer is Connection less.
7. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	7. TCP/IP model is, in a way implementation of the OSI model.
8. Network layer of OSI model provides both connection oriented and connectionless service.	8. The Network layer in TCP/IP model provides connectionless service.
9. OSI model has a problem of fitting the protocols into the model.	9. TCP/IP model does not fit any protocol.
10. Protocols are hidden in OSI model and are easily replaced as the technology changes.	10. In TCP/IP replacing protocol is not easy.
11. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	11. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
12. It has 7 layers	12. It has 4 layers

Q.2. (c) Differentiate between Hidden Station and Exposed Station problem in wireless LAN protocol. (3)

Ans. A significant difference between wired and wireless LANs is the fact that, in general a fully connected topology between the WLAN nodes cannot b assumed. This problem gives rise to 'hidden' and 'exposed' station problems.

Hidden Terminal:

- The transmission range of A reaches B but not C. Similarly, the range of C reaches B but not A. Also the range of B reaches both A and C.
- Now, the node A starts to send something to B and C doesn't receive this transmission.
- Now C also wants to send data to B and senses the carrier. As it senses it to be free, it also starts sending to B.
- Hidden terminal problem occurs when two nodes that are outside each other's range performs simultaneous transmission to a node that is within the range of each of them resulting in a collision.
- That means the data from both parties A and C will be lost during the collision.
- Hidden nodes mean increased probability of collision at receiver end.
- One solution to avoid this is to have the channel sensing range much greater than the receiving range. Another solution is to use the Multiple Access with Collision Avoidance (MACA).

dotnotes.xyz

Exposed Terminal:

- Imagine a situation wherein the B node is currently sending some data to node A.
- Now the other node C which is right now free want to send data to some node D which is outside the range of A and B.
- Now before starting transmission it senses the carrier and realizes that the carrier is busy (due to interference of B's signal).
- Hence, the C node postpones the transmission to D until it detects the medium to be idle.
- However such a wait was un-necessary as A was outside the interference range of C.
- Also a collision at B will be a weak enough to be unable to penetrate into C.
- Exposed terminal problem occurs when the node is within the range of a node that is transmitting and it cannot be transmitted to any node.
- Exposed node means denied channel access unnecessarily which ultimately results in under-utilization of bandwidth resources.
- It also results in wastage of time-resource.

Q.3. (a) 8-bit messages are transmitted using a Hamming Code. How many check bits are needed to ensure that the receiver can detect and correct single bit error? Show the bit pattern transmitted for the message 10011101. Assume that even parity is used in the Hamming Code. (5)

Ans. A byte of data is 10011101 create the code word, leaving spaces for parity bits.

_ _ 1 _ 0 0 1 _ 1 1 0 1

- Position 1 checks bits 1, 3, 5, 7,9, 11

0 _ 1 _ 0 0 1 _ 1 1 0 1

- Odd parity so set position 1 to 1

1 _ 1 _ 0 0 1 _ 1 1 0 1

- Position 2 checks bits 2, 3, 6,7, 10, 11.

1 0 1 _ 0 0 1 _ 1 1 0 1

- Odd parity so set position 2 to 1

1 1 1 _ 0 0 1 _ 1 1 0 1

- Position 4 checks bits 4,5,6,7,12

1 1 1 0 0 0 1 _ 1 1 0 1

Even parity, so set position 4 to 0.

1 1 1 0 0 0 1 _ 1 1 0 1

- Position 8 checks bits 8,9,10,11,12

1 1 1 0 0 0 1 0 0 0 0 1

Odd parity, so set position 8 to 1.

1 1 1 0 0 0 1 1 1 1 0 1

∴ Code word : 1 1 1 0 0 0 1 1 1 1 0 1

Q.3. (b) A group of N stations share 100 Kbps slotted ALOHA channel. Each station output a 500 bits frame on an average of 5000 ms even if previous one has not been sent. What is the required value of N? (5)

Ans. Maximum through put of pure ALOHA = 184% = 0.184

Since N station shares a rate of 100 kbps.

Hence usable channel rate =

$$0.184 \times 100 = 184 \text{ Kbps}$$

Each station outputs 500 bit frame per 5000 ms hence bits per sec. outputted by each station.

$$= \frac{500\,bits}{5\,\text{sec}} = 100 bits/\text{sec}.$$

Therefore N station give an output of 100 bps on a channel having a rate of 18.4 KbPs. hence

$$N \doteq (18.4 \times 10^3)/100$$
$$= 184 \text{ Stations.}$$

Q.4. (a) For a generator polynomial of $x^3 + 1$, what is the CRC value if the message is $x^7 + x^5 + 1$? Express answer as a bit sequence with no spaces. (5)

Ans. Refer Q.2. (b) End Term Examination 2018

Q.4. (b) How is selective repeat better than Go-Back N, Explain with help of an example? (5)

Ans. Refer Q.4. (b) First Term Examination 2018.

dotnotes.xyz

END TERM EXAMINATION [MAY. 2019]
SIXTH SEMESTER [B.TECH]
COMPUTER NETWORKS [ETCS–306]

Time : 3 hrs.

Note: *Attempt any five questions including Q.no. 1 which is compulsory.* **M.M. : 75**

Q.1. Attempt any five of the following :

Q.1. (a) Differentiate between Intranet, internet and Internet? (5)

Ans. Many networks exist in the world, often with different hardware and software. People connected to one network often want to communicate with people attached to a different one. This desire requires connecting together different, and frequently incompatible networks, sometimes by using machines called gateways to make the connection and provide the necessary translation, both in terms of hardware and software. A collection of interconnected networks is called an internetwork or just internet.

It is simply any network made up of multiple smaller networks using the same internetworking protocols. An internet (little "i") isn't necessarily connected to the Internet (big "I"), nor does it necessarily use TCP/IP as its internet working protocol. There are isolated corporate internets.

The Internet, with a capital "I," refers to the network that began its life as the AKPAnet and continues today as, roughly, the confederation of all TCP/IP networks directly or indirectly connected to commercial U.S. backbones. Seen up close, it's actually quite a few different networks-commercial TCP/IP backbones, corporate and U.S. government TCP/IP networks, and TCP/IP networks in other countries-interconnected by high-speed digital circuits.

It means a specific worldwide internet that is widely used to connect universities, government offices, companies, and of late, private individuals.

An internetwork is formed when distinct networks are connected together. In our view, connecting a LAN and a WAN or connecting two LANs forms an internetwork, but there is little agreement in the industry over terminology in this area.

Intranet: This is a network that is not available to the world outside of the Intranet. If the Intranet network is connected to the Internet, the Intranet will reside behind a firewall and, if it allows access from the Internet, will be an Extranet. The firewall helps to control access between the Intranet and Internet to permit access to the Intranet only to people who are members of the same company or organisation.

In its simplest form, an Intranet can be set up on a networked PG without any PC on the network having access via the Intranet network to the Internet.

For example, consider an office with a few PCs and a few printers all networked together. The network would not be connected to the outside world. On one of the drives of one of the PCs there would be a directory of web pages that comprise the Intranet. Other PCs on the network could access this Intranet by pointing their browser (Netscape or Internet Explorer) to this directory - for example

U:\inet\index.htm

From then onwards they would navigate around the Intranet in the same way as they would get around the Internet.

Q.1. (b) Differentiate between PAN, LAN, MAN and WAN. 2019–7

Ans. Local Area Network (LAN): LAN stands for local area network. It covers, as (5)
the name suggests, a local area. This usually includes a local office and they're also very common in homes.

Wide Area Network (WAN): WAN, in contrast to a LAN, refers to a wide area network. The name is exactly what it sounds like: a network that covers an area wider than a LAN. Beyond that, the definition is less clear. Distances can range from a network connecting multiple buildings on a corporate or college campus to satellite links connecting offices in different countries. The most popular WAN is the one you're using to read this article: the internet. It's actually a collection of other networks, including other LANs and WANs

Personal Area Network (PAN): PAN stands for personal area network, and again, it's exactly what it sounds like: a network covering a very small area, usually a small room. The best known wireless PAN network technology is Bluetooth, and the most popular wired PAN is USB. You might not think of your wireless headset, your printer or your smartphones as components in a network, but they are definitely talking with each other. Many peripheral devices are actually computers in their own right. Wi-Fi also serves as a PAN technology, since Wi-Fi is also used over a small area.

Metropolitan Area Network (MAN): A metropolitan area network (MAN) connects nodes located in the same metro area. One of the most common ways for organizations to build this kind of network is to use microwave transmission technology. You might have seen a microwave antenna on a TV news van, extended high in the air, beaming video and sound back to the main TV studio. It's also possible to wire buildings together using fiber-optic cable, but as with WANs, most organizations that use wires will lease them from another carrier. Laying cable themselves is quite expensive.

Q.1. (c) Differentiate between Adaptive and non-adaptive routing? (5)

Ans. 1. Adaptive Routing Algorithm: These algorithms change their routing decisions to reflect changes in the topology and in traffic as well. These get their routing information from adjacent routers or from all routers. The optimization parameters are the distance, number of hops and estimated transit time. This can be further classified as follows:

(a) **Centralized:** In this type some central node in the network gets entire information about the network topology, about the traffic and about other nodes. This then transmits this information to the respective routers. The advantage of this is that only one node is required to keep the information. The disadvantage is that if the central node goes down the entire network is down, i.e. single point of failure.

(b) **Isolated:** In this method the node decides the routing without seeking information from other nodes. The sending node does not know about the status of a particular link. The disadvantage is that the packet may be send through a congested route resulting in a delay. Some examples of this type of algorithm for routing are:

- **Hot Potato:** When a packet comes to a node, it tries to get rid of it as fast as it can, by putting it on the shortest output queue-without regard to where that link leads. A variation of this algorithm is to combine static routing with the hot potato algorithm. When a packet arrives, the routing algorithm takes into account both the static weights of the links and the queue lengths.
- **Backward Learning:** In this method the routing tables at each node gets modified by information from the incoming packets. One way to implement backward learning is

dotnotes.xyz

to include the identity of the source node in each packet, together with a hop counter that is incremented on each hop. When a node receives a packet in a particular line, it notes down the number of hops it has taken to reach it from the source node. If the previous value of hop count stored in the node is better than the current one then nothing is done but if the current value is better then the value is updated for future use. The problem with this is that when the best route goes down then it cannot recall the second best route to a particular node. Hence all the nodes have to forget the stored informations periodically and start all over again.

(c) Distributed: In this the node receives information from its neighbouring nodes and then takes the decision about which way to send the packet. The disadvantage is that if in between the the interval it receives information and sends the paket something changes then the packet may be delayed.

2. Non-Adaptive Routing Algorithm: These algorithms do not base their routing decisions on measurements and estimates of the current traffic and topology. Instead the route to be taken in going from one node to the other is computed in advance, off-line, and downloaded to the routers when the network is booted. This is also known as static routing. This can be further classified as:

(a) Flooding: Flooding adapts the technique in which every incoming packet is sent on every outgoing line except the one on which it arrived. One problem with this method is that packets may go in a loop. As a result of this a node may receive several copies of a particular packet which is undesirable. Some techniques adapted to overcome these problems are as follows:

- **Sequence Numbers:** Every packet is given a sequence number. When a node receives the packet it sees its source address and sequence number. If the node finds that it has sent the same packet earlier then it will not transmit the packet and will just discard it.
- **Hop Count:** Every packet has a hop count associated with it. This is decremented(or incremented) by one by each node which sees it. When the hop count becomes zero(or a maximum possible value) the packet is dropped.
- **Spanning Tree:** The packet is sent only on those links that lead to the destination by constructing a spanning tree routed at the source. This avoids loops in transmission but is possible only when all the intermediate nodes have knowledge of the network topology.

Blooding is not practical for general kinds of applications. But in cases where high degree of robustness is desired such as in military applications, flooding is of great help.

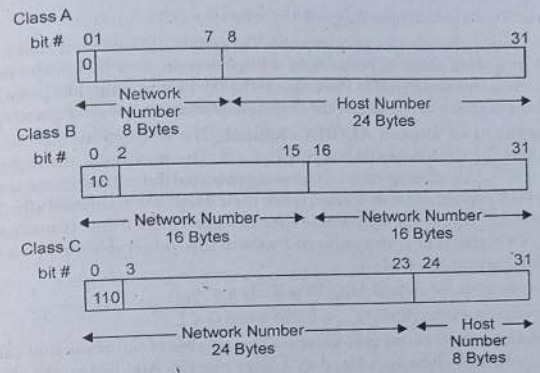
(b) Random Walk: In this method a packet is sent by the node to one of its neighbours randomly. This algorithm is highly robust. When the network is highly interconnected, this algorithm has the property of making excellent use of alternative routes. It is usually implemented by sending the packet onto the least queued link.

Q.1. (d) What is difference between Classful IP addressing and Classless IP addressing? What are maximum number of subnet in CLASS A with mask 255.255.192.0. (5)

Ans. Classfull Addressing:

All IP addresses have a network and host portion. In classful addressing, the network portion ends on one of the separating dots in the address (on an octet boundary). Classful addressing divides an IP address into the Network and Host portions along octet boundaries.In the classful addressing system all the IP addresses that are

available are divided into the five classes A,B,C,D and E, in which class A,B and C address are frequently used because class D is for Multicast and is rarely used and class E is reserved and is not currently used.



Each of the IP address belongs to a particular class that's why they are classful addresses.Earlier this addressing system did not have any name,but when classless addressing system came into existence then it is named as Classful addressing system.The main disadvantage of classful addressing is that it limited the flexibility and number of addresses that can be assigned to any device.One of the major disadvantage of classful addressing is that it does not send subnet information but it will send the complete network address.

Classless Addressing:

Classless addressing uses a variable number of bits for the network and host portions of the address.

Classless addressing treats the IP address as a 32 bit stream of ones and zeroes, where the boundary between network and host portions can fall anywhere between bit 0 and bit 31.Classless addressing system is also known as CIDR(Classless Inter-Domain Routing).Classless addressing is a way to allocate and specify the Internet addresses used in inter-domain routing more flexibly than with the original system of Internet Protocol (IP) address classes. CIDR (Classless Internet Domain Routing), defines arbitrarily-sized subnets solely by base address and number of significant bits in the address.

Q.1. (e) Calculate the throughput of slotted ALOHA and PURE ALOHA? (5)

Ans. Throughput of pure A LOHA channel: Let G be the average number of frames generated by the system during one frame transmission time. Then it can be proved that the average no of successful transmissions for pure ALOHA is $S = G \times e^{-2G}$. The maximum throughput S_{max} is 0.184, for G = 1/2. i.e. if one - half a frame is generated during one one frame transmission time, then 18.4 percent of these frames reach their

dotnotes.xyz

destination successfully. This is an expected result because : the vulnerable time is 2 times the frame transmission time. Therefore, if a station generates only one frame in this vulnerable time, the frame will reach its destination successfully.

The throughput for pure ALOHA is $S = G \times e^{-2G}$

The maximum throughput $S_{max} = 0.184$ when $G = (1/2)$

Slotted aloha gives better performance. The number of collisions that can possibly take place in slotted aloha is reduced by a huge margin. And hence, the performance become much better compared to Pure Aloha. Collisions may only take place with nodes that are ready to speak at the same time. But nevertheless, this is a substantial reduction.

Throughput of slotted ALOHA channel: The average number of successful transmissions for slotted ALOHA is $S = G \times e^{-G}$. The maximum throughput S_{max} is 0.368, when G = 1. In other words, if a frame is generated during one frame transmission time, then 36.8 percent of these frames reach their destination successfully. This result can be expected because the vulnerable time is equal to the frame transmission time. Therefore, if a station generates only one frame in this vulnerable-time, the frame will reach its destination successfully.

The throughput for slotted ALOHA is $S = G \times e^{-G}$

The maximum throughput $S_{max} = 0.368$ when $G = 1$

Slotted aloha gives better performance. The number of collisions that can possibly take place in slotted aloha is reduced by a huge margin. And hence, the performance become much better compared to Pure Aloha. Collisions may only take place with nodes that are ready to speak at the same time. But nevertheless, this is a substantial reduction.

Q.1. (f) Define the terms bit rate, baud rate and bit interval in terms of data transmission. (5)

Ans. Bit rate and **Baud rate**, these two terms are often used in data communication. Bit rate is simply the **number of bits** (i.e., 0's and 1's) transmitted in per unit time. While Baud rate is the **number of signal units** transmitted per unit time that is needed to represent those bits.

The crucial difference between bit rate and baud rate that one change of state can transfer one bit, or slightly more or less than one bit that relies on the modulation technique used. Hence, the given equation defines the relation between the two:

Bit rate = baud rate × the number of bit per baud

If we talk about computer efficiency, the bit rate is the more important where we want to know how long it takes to process each piece of information. But when we are more concerned about how that data is moved from one place to another we emphasize on the baud rate. The fewer signals required, the more efficient the system and the less bandwidth needed to transmit more bits.

Q.1. (g) Differentiate between FDM, TDM and WDM. (5)

Ans. FDM: Bandwidth is the total capacity of a channel to transmit data. In FDM, the complete bandwidth is divided among the users. Therefore, each user gets its own bandwidth or a frequency range. In other words, all users can use the channel at the same time but they have their own bandwidths or frequency ranges to transmit data. On the sending end, all the signals are combined to a single signal using a multiplexer. Afterward, the signal travels through the channel. On the receiving end, there is a demultiplexer. It separates the composite signal back to separate signals. One drawback of this multiplexing technique is that, since all signals transmit at the same time, there is a possibility of crosstalk. In brief, FDM divides bandwidth and provide frequencies for the users. It does not divide time among users.

TDM: In TDM, the users can get complete channel bandwidth to send signals but for a fixed time slot. It scales the time among the users. Assume that there are three users as u1, u2 and u3 and the fixed time slot is t0. First, u1 will get the entire frequency bandwidth for t0 time. When u1 transmit data, the other users cannot transmit data. After that time slot is over, u2 can transmit data for a t0 time. When u2 transmit data, the other users cannot transmit data. Then, u3 transmits data for t0 time.

In brief, TDM divides time not the bandwidth among users. They can only transmit signals within the available time slot. As only, one signal transmits at a time, the crosstalk in TDM is minimum.

WDM: Fiber Optic communication use WDM. The concept of WDM relates to Physics. When a white light beam goes through a prism, it separates into individual colored light beams by the prism. Each light beam has different wavelengths. This scenario works vice versa as well. The individual color beams combine back to generate a white light beam.

FDM vs TDM vs WDM		
FDM is a transmission technique in which multiple data signals are combined for simultaneous transmission via a shared communication medium.	TDM is a transmission technique that allows multiple users to send signals over a common channel by allocating fixed time slot for each user.	WDM is a transmission technique that modulates numerous data streams, optical carrier signals of varying wavelengths into a single light beams through a single optical fiber.
Functionality		
FDM divides the bandwidth into smaller frequency ranges and transmitter transmit data simultaneously through a common channel within their frequency range.	TDM allocates a fixed time slot for each user to send signals through a common channel. User gets the entire bandwidth within that time slot.	WDM combines multiple light beams from several channels and combine them to a single light beam and sends through a fiber optic strand similar to FDM.
Stands for		
FDM stands for Frequency Division Multiplexing.	TDM stands for Time Division Multiplexing.	WDM stands for Wave Length Multiplexing.
Type of Signals		
FDM uses analog signals.	TDM uses digital and analog signals.	WDM uses optical signals.

Q.2. (a) Compare and contrast all the network topologies. (6.5)

Ans. 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:

dotnotes.xyz

1. Hierarchical topology 2. Bus topology 3. Star topology
4. Ring topology 5. Mesh topology 6. Hybrid topology

1. BUS Topology

Features of Bus Topology

1. It transmits data only in one direction.
2. Every device is connected to a single cable

Advantages of Bus Topology

1. It is cost effective.
2. Cable required is least compared to other network topology.
3. Used in small networks.

Disadvantages of Bus Topology

1. Cables fails then whole network fails.
2. If network traffic is heavy or nodes are more the performance of the network decreases.
3. It is slower than the ring topology.

RING Topology

Features of Ring Topology.

1. The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called **Dual Ring Topology**.
2. Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.

Advantages of Ring Topology

1. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
2. Cheap to install and expand

Disadvantages of Ring Topology

1. Troubleshooting is difficult in ring topology.
2. Adding or deleting the computers disturbs the network activity.
3. Failure of one computer disturbs the whole network.

STAR Topology

Features of Star Topology

1. Every node has its own dedicated connection to the hub.
2. Hub acts as a repeater for data flow.
3. Can be used with twisted pair, Optical Fibre or coaxial cable.

Advantages of Star Topology

1. Fast performance with few nodes and low network traffic.
2. Easy to troubleshoot.
3. Easy to setup and modify.

Disadvantages of Star Topology

1. Cost of installation is high.
2. Expensive to use.
3. If the hub fails then the whole network is stopped because all the nodes depend on the hub.

Q.2. (b) What is packet switching technique? Why is circuit switching better for telephone network? (6)

Ans. Refer to Q.1. (b) First Term Examination 2018.

Q.3. (a) An organization is granted the block 16.0.0.0/8. The administrator wants to create 500 fixed length subnets. Find the following: (6)

(i) Subnet Mask

(ii) Number of addresses in brief subnet.

(iii) The first and last address in first subnet.

Ans. (*i*) 255.255.128.0

(*ii*) $2^{15} - 2 = 32766$

(*iii*) First valid address - 16.0.0.1

Last valid address - 16.0.127.254

Q.3. (b) Give advantage of IEEE 802.3 standards? Explain Traditional Ethernet, Fast Ethernet, Gigabit Ethernet for High speed LAN. (6.5)

Ans. Traditionally, Ethernet is used over 'thick' coaxial cable (Normally yellow in colour) called 10Base5 (the '10' denotes 10Mbps, base means that the signal is baseband i.e. takes the whole bandwidth of the cable (so that only one device can transmit at one time on the same cable), and the '5' denotes 500m maximum length). The minimum length between stations is 2.5m.

The cable is run in one long length forming a 'Bus Topology'. Stations attach to it by way of inline N-type connections or a transceiver which is literally screwed into the cable (by way of a 'Vampire Tap') providing a 15-pin AUI (Attachment Unit Interface) connection (also known as a DIX connector or a DB-15 connector) for a drop lead connection (maximum of 50m length) to the station. The segments are terminated with 50 ohm resistors and the shield should be grounded at one end only.

Fast Ethernet uses the same frame formats and CSMA/CD technology as normal 10Mbps Ethernet. The difference is that the maximum delay for the signal across the segment is now 5.12 microseconds instead of 51.2 microseconds. This comes from the fact that the bit time (time to transmit one bit) is 0.01 microseconds and that the slot time for a frame is 512 bit times. The Inter-Packet Gap (IPG) for 802.3u is 0.96 microseconds as opposed to 9.6 microseconds for 10Mbps Ethernet.

Fast Ethernet is the most popular of the newer standards and is an extension to 10BaseT, using CSMA/CD. The '100' denotes 100Mbps data speed and it uses the same two pairs as 10BaseT (1 and 2 for transmit, 3 and 6 for receive) and must only be used on Category 5 UTP cable installations with provision for it to be used on Type 1 STP. The Copper physical layer being based on the **Twisted Pair-Physical Medium Dependent (TP-PMD)** developed by ANSI X3T9.5 committee. The actual data throughput increases by between 3 to 4 times that of 10BaseT.

dotnotes.xyz

Although the functional principles of Gigabit Ethernet are the same as Ethernet and Fast Ethernet i.e. CSMA/CD and the Framing format, the physical outworking is very different. One difference is the slot time. The standard Ethernet slot time required in CSMA/CD half-duplex mode is not long enough for running over 100m of copper, so **Carrier Extension** is used to guarantee a 512-bit slot time.

Q.4.(a) Given the network topology below, use the Dijkstra's algorithm to compute the shortest path from 1 to all other nodes. Make sure to show the results of the computation at each step. **(8.5)**

Ans.

1	2	3	4	5	6	7	8	9
0	∞	∞	∞	∞	∞	∞	∞	∞
	3	10	∞	∞	∞	∞	∞	∞
		10	10	6	∞	∞	∞	∞
		8	10	–	∞	∞	13	∞
			10	–	16	∞	13	∞
			–	–	16	14	12	13
			–	–	16	14	–	13
			–	–	16	14	–	–
			–	–	16	–	–	–
			–	–	–	–	–	–

Shortest path:

Shortest	Path	Weight
1 to 2	1 – 2	3
1 to 3	1 – 2 – 5 – 3	8
1 to 4	1 – 2 – 4	10
1 to 5	1 – 2 – 5	6
1 to 6	1 – 2 – 5 – 3 – 6	16
1 to 7	1 – 2 – 4 – 7	14
1 to 8	1 – 2 – 4 – 8	12
1 to 9	1 – 2 – 4 – 9	13

Q.4. (b) Explain leaky bucket algorithm. What kind of problems are address using leaky bucket algorithm? **(4)**

Ans. Leaky Bucket Algorithm: Consider a Bucket with a small hole at the bottom, whatever may be the rate of water pouring into the bucket, the rate at which water comes out from that small hole is constant. This scenario is depicted in figure (a). Once the bucket is full, any additional water entering it spills over the sides and is lost (*i.e.* it doesn't appear in the output stream through the hole underneath).

The same idea of leaky bucket can be applied to packets, as shown in Fig.*b*. Conceptually each network interface contains a leaky bucket. And the following steps are performed:

- When the host has to send a packet, the packet is thrown into the bucket.

- The bucket leaks at a constant rate, meaning the network interface transmits packets at a constant rate.
- Bursty traffic is converted to a uniform traffic by the leaky bucket.
- In practice the bucket is a finite queue that outputs at a finite rate.

This arrangement can be simulated in the operating system or can be built into the hardware. Implementation of this algorithm is easy and consists of a finite queue. Whenever a packet arrives, if there is room in the queue it is queued up and if there is no room then the packet is discarded.

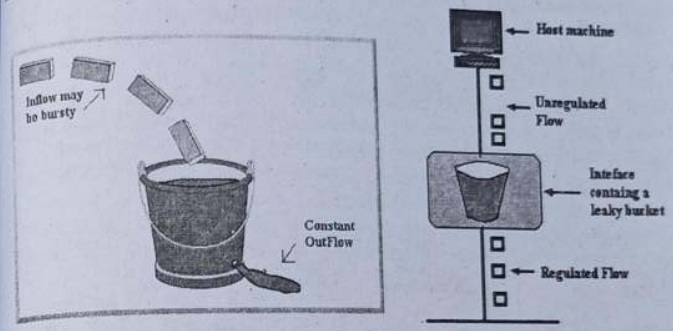


Fig. (a) Leaky bucket (b) Leaky bucket implementation

Q.5. (a) Draw and explain packet format of Transmission control protocol. Explain various steps that are followed in releasing a TCP connection? **(8.5)**

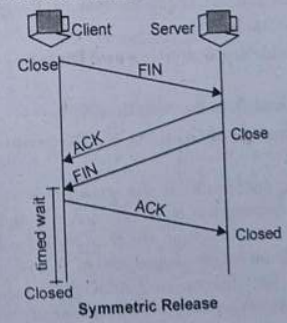
Ans. The basic steps followed by TCP to establish the connection are as follows :

Release can be asymmetric(one sided, where data may loss) or symmetric (both sides agreed) Steps for symmetric Release:

- Step 1: Client end system sends TCP FIN control segment to server
- Step 2: Server receives FIN, replies with ACK. Closes connection, sends FIN.
- Step 3: Client receives FIN, replies with ACK.

Enters "timed wait" - will respond with ACK to received FINs

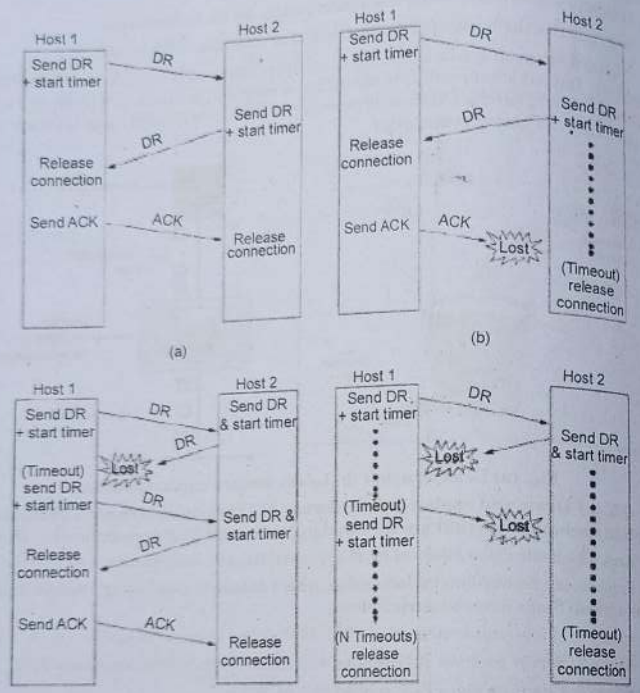
- Step 4: server, receives ACK. Connection closed.



Symmetric Release

dotnotes.xyz

Connection releases:



Four protocol scenarios for releasing a connection. (a) The normal case of a three-way handshake. (b) final ACK lost. (c) Response lost. (d) Response lost and subsequent DRs (Disconnection Requests) lost.

Q.5. (b) Compare Link State routing and Distance Vector Routing using suitable diagram. (4)

Ans. Refer to Q.1.(h) End Term Examination 2017.

Q.6.(a) Explain advantage of GO-Back-N ARQ protocol over stop-and-wait ARQ? (6)

Ans. Stop and Wait transmission is the simplest reliability technique and is adequate for a very simple communications protocol. A stop and wait protocol transmits a Protocol Data Unit (PDU) of information and then waits for a response. The receiver receives each PDU and sends an Acknowledgement (ACK) PDU if a data PDU is received correctly, and a Negative Acknowledgement (NACK) PDU if the data was not received. In practice, the receiver may not be able to reliably identify whether a PDU has been

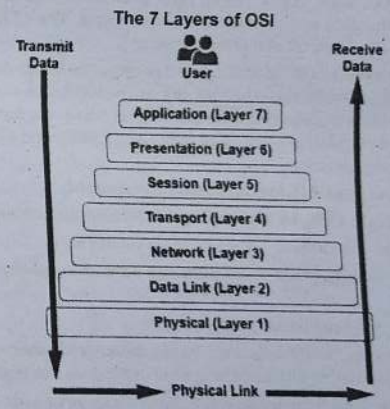
received, and the transmitter will usually also need to implement a timer to recover from the condition where the receiver does not respond.

Under normal transmission the sender will receive an ACK for the data and then commence transmission of the next data block. For a long delay link, the sender may have to wait an appreciable time for this response. While it is waiting the sender is said to be in the "idle" state and is unable to send further data.

Go-Back-N ARQ is a more efficient use of a connection than Stop-and-wait ARQ, since unlike waiting for an acknowledgement for each packet, the connection is still being utilized as packets are being sent. In other words, during the time that would otherwise be spent waiting, more packets are being sent. However, this method also results in sending frames multiple times-if any frame was lost or damaged, or the ACK acknowledging them was lost or damaged, the if that frame and all following frames in the window (even if they were received without error) will be re-sent. To avoid this, Selective Repeat ARQ can be used.

Q.6. (b) Explain OSI reference model in detail? Explain which layer is responsible for data and flow control? (6.5)

Ans. In the OSI model, control is passed from one layer to the next, starting at the application layer (Layer 7) in one station, and proceeding to the bottom layer, over the channel to the next station and back up the hierarchy. The OSI model takes the task of inter-networking and divides that up into what is referred to as a *vertical stack* that consists of the following 7 layers.



Application (Layer 7): OSI Model, Layer 7, supports application and end-user processes. Communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. Everything at this layer is application-specific. This layer provides application services for file transfers, e-mail, and other network software services. Telnet and FTP are applications that exist entirely in the application level. Tiered application architectures are part of this layer.

dotnotes.xyz

Presentation (Layer 6): This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the syntax layer.

Session (Layer 5): This layer establishes, manages and terminates connections between applications. The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. It deals with session and connection coordination.

Transport (Layer 4): OSI Model, Layer 4, provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer.

Network (Layer 3): Layer 3 provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing.

Data Link (Layer 2): At OSI Model, Layer 2, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control and frame synchronization. The data link layer is divided into two sub layers: The Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. The MAC sub layer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronization, flow control and error checking.

Physical (Layer 1): OSI Model, Layer 1 conveys the bit stream - electrical impulse, light or radio signal — through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards and physical aspects. Fast Ethernet, RS232, and ATM are protocols with physical layer components.

Layer 4 is responsible for data and flow control.

Q.7. (a) Explain CSMA/CD and CSMA/CA random access protocols? (6)

Ans. Refer to Q.1. (b) End Term Examination 2018.

Q.7. (b) List various error correction and detection mechanisms used by Data link Layer? (6.5)

Ans. Error control can be done in two ways

• **Error detection** " Error detection involves checking whether any error has occurred or not. The number of error bits and the type of error does not matter.

• **Error correction** " Error correction involves ascertaining the exact number of bits that has been corrupted and the location of the corrupted bits.

For both error detection and error correction, the sender needs to send some additional bits along with the data bits. The receiver performs necessary checks based upon the additional redundant bits. If it finds that the data is free from errors, it removes the redundant bits before passing the message to the upper layers.

Error Detection Techniques: There are three main techniques for detecting errors in frames: Parity Check, Checksum and Cyclic Redundancy Check (CRC).

Parity Check: The parity check is done by adding an extra bit, called parity bit to the data to make a number of 1s either even in case of even parity or odd in case of odd parity.

While creating a frame, the sender counts the number of 1s in it and adds the parity bit in the following way

• In case of even parity: If a number of 1s is even then parity bit value is 0. If the number of 1s is odd then parity bit value is 1.

• In case of odd parity: If a number of 1s is odd then parity bit value is 0. If a number of 1s is even then parity bit value is 1.

On receiving a frame, the receiver counts the number of 1s in it. In case of even parity check, if the count of 1s is even, the frame is accepted, otherwise, it is rejected. A similar rule is adopted for odd parity check.

The parity check is suitable for single bit error detection only.

Checksum: In this error detection scheme, the following procedure is applied

• Data is divided into fixed sized frames or segments.

• The sender adds the segments using 1's complement arithmetic to get the sum. It then complements the sum to get the checksum and sends it along with the data frames.

• The receiver adds the incoming segments along with the checksum using 1's complement arithmetic to get the sum and then complements it.

• If the result is zero, the received frames are accepted; otherwise, they are discarded.

Cyclic Redundancy Check (CRC): Cyclic Redundancy Check (CRC) involves binary division of the data bits being sent by a predetermined divisor agreed upon by the communicating system. The divisor is generated using polynomials.

• Here, the sender performs binary division of the data segment by the divisor. It then appends the remainder called CRC bits to the end of the data segment. This makes the resulting data unit exactly divisible by the divisor.

• The receiver divides the incoming data unit by the divisor. If there is no remainder, the data unit is assumed to be correct and is accepted. Otherwise, it is understood that the data is corrupted and is therefore rejected.

Error Correction Techniques: Error correction techniques find out the exact number of bits that have been corrupted and as well as their locations. There are two principle ways

• **Backward Error Correction (Retransmission–** If the receiver detects an error in the incoming frame, it requests the sender to retransmit the frame. It is a relatively simple technique. But it can be efficiently used only where retransmitting is not expensive as in fiber optics and the time for retransmission is low relative to the requirements of the application.

• **Forward Error Correction–** If the receiver detects some error in the incoming frame, it executes error-correcting code that generates the actual frame. This saves bandwidth required for retransmission. It is inevitable in real-time systems. However, if there are too many errors, the frames need to be retransmitted.

dotnotes.xyz

The four main error correction codes are

- Hamming Codes
- Binary Convolution Code
- Reed – Solomon Code
- Low-Density Parity-Check Code

Q.8.(a) How does ATM differ from Frame Relay? List and define the ATM service classes in detail? (7.5)

Ans. Asynchronous Transfer Mode (ATM): ATM is a network switching technology that uses a cell based methodology to quantize data. ATM data communication consists of fixed size cells of 53 bytes. An ATM cell contains a 5 byte header and 48 bytes of ATM payload. This smaller size, fixed-length cells are good for transmitting voice, image and video data as the delay is minimized.

ATM is a connection oriented protocol and therefore a virtual circuit should be established between sending and receiving points. It establishes a fixed route between two points when the data transfer starts.

Another important aspect of ATM is its asynchronous operation in time division multiplexing. Therefore cells are transmitted only when data is available to be sent unlike in conventional time division multiplexing where synchronization bytes are transferred if there data is not available to be sent.

ATM is designed to be convenient for hardware implementation and therefore processing and switching have become faster. Bit rates on ATM networks can go up to 10 Gbps. ATM is a core protocol used over the SONET/SDH backbone of the ISDN.

ATM provides a good quality of service in networks where different types of information such as data, voice, and are supported. With ATM, each of these information types can pass through a single network connection.

Frame Relay: Frame relay is a packet switching technology for connecting network points in Wide Area Networks (WAN). It is a connection oriented data service and establishes a virtual circuit between two end points. Data transfer is done in packets of data known as frames. These frames are variable in packet size and more efficient due to flexible transfers. Frame Relay was originally introduced for ISDN interfaces though it is currently used over a variety of other network interfaces as well.

In frame relay, connections are called as 'Ports'. All the points which need to connect to the frame relay network needs to have a port. Every port has a unique Address. A frame is made of two parts which can be called as 'actual data' and the 'frame relay header'. Frame architecture is same as defined for LAP-D (Link Access Procedures on the D channel) which has a variable length for information field. These frames are sent over Virtual Connections.

Frame relay can create multiple redundant connections among various routers, without having multiple physical links. Since frame relay is not specific for media, and provides means to buffer speed variations, it has the possibility to create a good interconnect medium between different types of network points with different speeds.

The ATM Forum has defined four ATM Layer service classes, each with scalable Quality of Service (QoS) levels:

Class A: Class A, or Constant Bit Rate (CBR), traffic is characterized by a continuous stream of bits at a steady rate, such as TDM multiplexer traffic. Class A traffic is low-bandwidth traffic that is highly sensitive to delay and intolerant to cell loss.

Class B and C: Class B and C traffic, defined as Variable Bit Rate (VBR), has a bursty nature and can be characterized by voice or video applications that use compression. Class B traffic is real-time VBR, (RT-VBR), where end-to-end delay is critical, such as interactive video conferencing. Class C is non-real time (VBR-NRT) traffic, where delay is not so critical, such as video playback, training tapes and video mail messages.

Class D: Class D traffic is split into two classes: Available Bit Rate (ABR) and Unspecified Bit Rate (UBR). These classes are for bursty LAN traffic and data that is more tolerant of delays and cell loss. UBR is a "best effort" service that does not specify bit rate or traffic parameters and has no quality of service guarantees. Originally devised as a way to make use of excess bandwidth, UBR is subject to increased cell loss and the discard of whole packets. ABR, like UBR, is also a best effort service, but differs in that it is a managed service, based on minimum cell rate (MCR) and with a low cell loss.

Q.8. (b) What is SHD technology? Differentiate between PDH and SDH? (5)

Ans. SDH: SDH supports various topologies such as point to point, ring, star, linear bus etc. It uses TDM and octet multiplexing.

In **SDH**, digital multiplexer's inputs are of same bit rate and are derived from common clock, hence are in phase. Hence it is synchronous.

Word (group of bits) Interleaving is used in SDH to combine digital signals.

As per CCITT, any of PDH rates upto 140 Mbps can be integrated with SDH rates up to 155.52 Mbps.

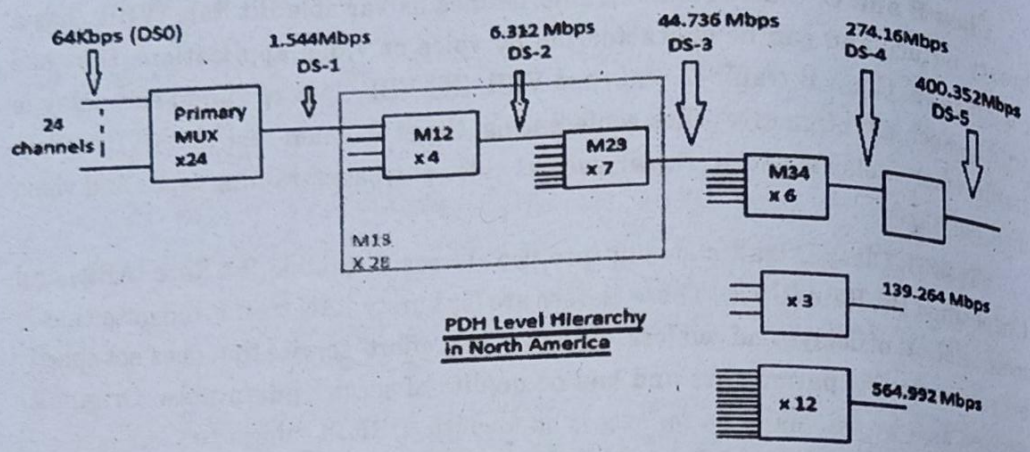
Following are the merits or advantages of SDH:

- A more simplified multiplexing and demultiplexing technique.
- Synchronous networking and SDH supports multipoint networking.
- Capability of transporting existing PDH signals.
- Easy growth to higher bit rates which enhances the administration and maintenance process.
- It is capable of transporting broadband signals.
- It is multivendor and supports different operators.
- It provides network transport services on LAN such as video conferencing, and interactive multimedia.
- Optical fibre bandwidth can be increased without limit in SDH.
- Switching protection to traffic is offered by rings.
- SDH allows quick recovery from failure.

PDH: In **PDH**, digital multiplexer's inputs (bit streams) are of same bit rate and are derived from different clocks from different oscillators. Each will differ within tolerance of few clock periods. Hence it is called plesiochronous.

Bit Interleaving is used in PDH to combine digital signals.

dotnotes.xyz



PDH Level Hierarchy in North America

Following are the limitations of PDH:

- In PDH, different frame is used for transmission and in data layer. Hence multiplexing and de-multiplexing is very complex.
- Accessing lower tributary requires the whole system to be de-multiplexed.
- The maximum capacity for PDH is 566 Mbps, which is limited in bandwidth.
- Tolerance is allowed in bit rates.
- PDH allows only Point-to-Point configuration.
- PDH does not support Hub.
- Every manufacturer has its own standards; PDH also has different multiplexing hierarchies making it difficult to integrate interconnecting networks together.

dotnotes.xyz