UNIT I INTRODUCTION AND APPLICATION LAYER

Data Communication - Networks - Network Types - Protocol Layering - TCP/IP Protocol suite - OSI Model - Introduction to Sockets - Application Layer protocols: HTTP - FTP - Email protocols (SMTP - POP3 - IMAP - MIME) - DNS - SNMP

PART-A

1 **Compare LAN and WAN.**

LAN	WAN
Scope of Local Area Network is restricted to a small/ singlebuilding	F bwbqnScope of Wide Area Network spans over large geographical areacountry/ Continent
LAN is owned by some organization.	A part of network asserts is owned or not owned.
Data rate of LAN 10-.10-100mbps.	Data rate of WAN is Gigabyte.

2 **Define Full Duplex and simplex transmission system.**

With Full duplex transmission, two stations can simultaneously send and receive data from each other. This mode is known as two-way simultaneous. The signals are transmitted in only one direction. One is the sender and another is the receiver.

3 **Define networks.** ***(Nov 12)***

A computer network is a group of computer systems and other computing hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users. Networks are commonly categorized based on their characteristics.

4 **Why do we need a Domain Name System? What role does the DNS Resolver play in the DNS system?** ***(Nov 12)***

Domain Name System can map a name to an address and conversely an address to name. The Domain Name System converts domain names into IP numbers. IP numbers uniquely identify hosts on the Internet

5 **What are the four fundamental characteristics that the datacommunication system depends on?**

The four fundamental characteristics are: Delivery, Accuracy,

Timeliness and Jitter.

6 **What are the five components of data communications system?**

The five components are Message, Sender, Receiver, TransmissionMedium and Protocol.

7 **Define link and state the types of connection.**

A link is the communication pathway that transfers data from onedevice to another. The two possible types of connections are pointto point and multipoint

8 **Define point to point and Multipoint.**

Point to point: A point to point connection provides a dedicatedlink between two devices.
Multipoint: A multipoint connection is one in which more than two specific devices share a single link.

9 **What is Network topology? List its types.**

Network topology is the interconnected pattern of network elements. A network topology may be physical, mapping hardware configuration, or logical, mapping the path that the data must take in order to travel around the network. The types are Bus topology, Star topology, Mesh topology and Ring Topology.

10 **What are the four main properties of HTTP?**

- Global Uniform Resource Identifier.
- Request-response exchange.
- Statelessness.
- Resource metadata.

11 **What is a protocol? What are the key elements of a protocol?** ***(Nov 15)***

Protocol is the set of rules governing the exchange of data between two entities. It defines what is communicated, how it is communicated, when it is communicated. The Key elements of a Protocol are as follows,

- Syntax – It refers to the structure or format of data meaning theorder in which they are presented.
- Semantics – It refers to the meaning of each section of bit. Howto do interpretation.
- Timing – When data should be sent and how fast they can be

sent.

12 **Define File Transfer Protocol.** ***(Nov 21)***

The File Transfer Protocol is a standard communication protocol used for the transfer of computer files from a server to a client on a computer network. FTP is built on a client–server model architecture using separate control and data connections between
the client and the server.

13 **What is WWW and SMTP?** ***(Nov 10,15) (May 15)***

World Wide Web is an internet application that allows user to view pages and move from one web page to another.

It helps to store and share data across varied distances. The TCP/IP protocol that supports electronic mail on the Internet is called Simple Mail Transfer (SMTP). It is a system for sending
messages to other computer users based on e-mail addresses.

14 **List the two types of DNS message.** ***(May 16)***

There are two types of DNS messages – Query and Response

- **Query message** – consists of the header and question records.
- **Response message** – consists of header, question record,authoritative record and additional record.

15 What is a layered Network Architecture?

A layer is created when a different level of abstraction occurs at protocol. Each layer should perform a well-defined function. Function of each layer should be chosen using internationality standardized protocols. Boundaries between should be chosen to minimize information flow across the interfaces.

16 Compare OSI and TCP/IP models.

OSI Model	TCP / IP Model
It distinguishes between Service, Interface, Protocol	It does not distinguish between Service, Interface, Protocol
Protocols are well hidden	Protocols are not just hidden
Dejure standard Fit Model	Defacto standard Fit Model
In transport layer onlyconnection-oriented services are available	In Transport layer choice is for connection oriented and connectionless
Contains 7 layers	Contains 5 layers

17 How do layers of the internet model correlate to the layers of the OSI model?

OSI	TCP/IP
Physical Layer	Physical Layer
Data Link Layer	Network Access Layer
Network Layer	IP Layer
Transport Layer	TCP Layer
Session Layer	Application Layer
Presentation Layer	
Application layer	

18 **Describe why HTTP is defined as a stateless protocol.** Maintaining state across request–Response connectionssignificantly increases the initial interactions in a connection, since the identity of each party needs to be established and any saved state much be retrieved. HTTP is therefore stateless to ensure that internet is scalable since state is not contained in a HTTP request /
response pair by default.

19 **What are the four groups of HTTP Headers? What are the twomethods of HTTP?** ***(May 15) (Nov 15)***

The four groups of HTTP headers are

- General headers
- Entity Headers
- Request Headers
- Response Headers.

Two methods of HTTP are Get Method( ) Post Method( )

20 **Justify the need for layer five in the OSI model.** ***(Nov 21)***

Layer 5 of the OSI Model: Session Layer is the layer of the ISO Open Systems Interconnection (OSI) model that controls the dialogues (connections) between computers. It establishes, manages, and terminates the connections between the local and remote application.

21 **What are the functions of Application Layer?** ***(Apr 11)***

It enables the user (human/software) to access the network. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management and other types of distributed information services. Services provided by the application layer are Network Virtual terminal, File transfer, access and management. Mail services, Directory services.

22 **Define anonymous FTP.** ***(May / June 2021)***

An anonymous FTP is where users are given access to adistributed file where they do not need to sign in with a specific username and password.

23 **What are the transmission modes of FTP?**

Stream mode: Default mode and data is delivered from FTP toTCP as a continuous stream of data.

Block mode: Data is delivered from FTP to TCP in terms of blocks.Each data block follows the three-byte header.

Compressed mode: File is compressed before transmitting if size is big. Run length encoding method is used for compression.

24 **Why is an application such as POP needed for electronic messaging?** ***(May 12)***

Workstations interact with the SMTP host, which receives the mail on behalf of every host in the organization, to retrieve messages by using a client-server protocol such as Post Office Protocol. Although POP3 is used to download messages from the server, the SMTP client still needed on the desktop to forward messages from the workstation user to its SMTP mail server.

25 **What is the difference between IMAP and POP?** ***(May / June 2021)***

POP	IMAP
POP allows downloadingmessages from your Inbox to your local computer	IMAP allows the user to see allthe folders on the mail server.
The mail can only be accessed from a single device at a time.	Messages can be accessed across multiple devices
To read the mail it has to be downloaded on the localsystem	The mail content can be readpartially before downloading.
The user cannot organize mailsin the mailbox of the mail server.	The user can organize theemails directly on the mail server.

26 What is the use of MIME Extension?

Multipurpose Internet Mail Extensions (MIME) is a supplementary protocol that allows non-ASCII data to be sent through SMTP. MIME transforms non-ASCII data at the sender site to NVT ASCII data and deliverers it to the client SMTP to be sent through the Internet. MIME converts binary files, executed files into text files. Then only it can be transmitted using SMTP

27 **How are the subgroups of the OSI model layers segregated by their functions? *(May / June 2021)***

The lower 4 layers (transport, network, data link and physical) are concerned with the flow of data from end to end through the network and hence are called as network support layers. The upper four layers of the OSI model (application, presentation and session) are orientated more toward services to the applications
and hence are called user support layers.

28 **Identify the Port number of Hyper Text Transfer Protocol andTelnet. *(Nov 21)***

By default, these two protocols are on their standard port number of 80 for HTTP and 443 for HTTPS. For telnet port number is 23.

29 **Discuss the three main division of the domain name space. *(May 12)***

Domain name space is divided into three different sections:generic domains, country domains & inverse domain.

- Generic domain: Define registered hosts according to their generic behavior, uses generic suffixes.
- Country domain: Uses two characters to identify a country asthe last suffix.

  Inverse domain: Finds the domain name given the IP address.

30 **List the two types of DNS message.** ***(May 16)***

There are two types of DNS messages,

- Query
- Response

Query message – consists of the header and question records. **Response message** –consists of header, question record,authoritative record and additional record.

31 **Define SNMP.** ***(May 12)***

Simple Network Management Protocol (**SNMP**) is an "Internet- standard protocol for managing devices on IP networks". Devices that typically support SNMP include routers, switches, servers, workstations, printers, & modem. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

PART-B

1 **Explain different types of networks in detail with neat diagram** ***(Nov/Dec 2021)***

Local Area Network

A local area network (LAN) is usually privately owned and links the devices in a single office, building, or campus. LAN size is limited to a few kilometres. LANs are designed to allow resources to be shared between personal computers or workstations.

In addition to size, LANs are distinguished from other types of networks by their transmission media and topology. In general, a given LAN will use only one type of transmission medium. The most common LAN topologies are bus, ring, and star. Wireless LANs are the newest evolution in LAN technology.

Wide Area Network

A wide area network (WAN), provides long-distance transmission of data, image, audio and video information over large geographic areas that may comprise a country, a continent, or even the whole world. The switched WAN connects the end systems, which usually comprise a router (internetworking connecting device) that connects to another LAN or WAN.

Metropolitan Area Networks

A metropolitan area network (MAN) is a network with a size between a LAN and a WAN which is illustrated in Fig 1.12. It normally covers the area inside a town or a city. It is designed for customers who need a high-speed connectivity, normally to the Internet, and have endpoints spread over a city or part of city. A good example of a MAN is the part of the telephone company network that can provide a high-speed DSL line to the customers

2 **Discuss in detail about the layers in OSI model.** ***(Nov10,11,12,15,19) (May 12) (May / June 2021)***

- Starting from bottom, first the **physical layer** handles the transmission of raw bits over a communications link. The physical layer is also concerned with representation of bits, data rate, synchronization of bits, line configuration and transmission mode.
- The **data link layer** then collects a stream of bits into a larger aggregate called a frame. This means that frames, not raw bits, are actually delivered to hosts. Other responsibilities of the data link layer include framing, error control, flow control and physical addressing.
- The **network layer** handles routing among nodes within a packet-switched network. At this layer, the unit of data exchanged among nodes is typically called a packet rather than a frame. The network layer is responsible for the delivery of individual packets from the source host to the

destination host.

- The **transport layer** then implements process-to-process channel. Here, the unit of data exchanged is commonly called a message rather than a packet or a frame. The transport layer is responsible for the delivery of a message from one process to another. Like the data link layer, the transport layer is responsible for flow Control and error control. However, flow control at this layer is performed end to end rather than across a single link.
- The **session layer** is used to tie together the potentially different transport streams that are part of a single application. The session layer is the network *dialog controller*. It establishes, maintains, and synchronizes the interaction among communicating systems.
- The **presentation layer** is concerned with the format of data exchanged between peers, for example, whether an integer is 16, 32, or 64 bits long and whether the most significant bit is transmitted first or last. The presentation layer is also responsible for translation, compression, and encryption.
- The top (seventh) layer is **application layer**. The application layer is responsible for providing services to the user.

3 **Explain in detail about the TCP/IP protocol suite with neat diagram**

The Internet architecture, which is also sometimes called the TCP/IP architecture because of its two main protocols. It is a four layer model which shown in Fig 1.17. At the physical and data link layers, TCP/IP does not define any specific protocol. It supports all the standard and proprietary protocols. At the network layer (or, more accurately, the internetwork layer), *TCP/IP* supports the Internetworking Protocol. IP, in turn, uses four supporting protocols: ARP, RARP, ICMP, and IGMP. Transport Layer was represented in *TCP/IP* by two protocols: TCP and UDP. IP is a host-to-host protocol, meaning that it can deliver a packet from one physical device to another. UDP and TCP are transport level protocols responsible for delivery of a message from a process (running program) to another process.

Application Layer
Transport Layer
Network Layer
Physical & Data link Layer

4 **Discuss how the Simple Mail Transfer Protocol (SMTP) is useful inelectronic mail. (*May 12,15) (Nov 13,15) (Nov 19) (May/June 2021) (Nov 21)***

Message Format

The message header is a series of <CRLF> terminated lines. (<CRLF> stands for carriage-return + line-feed, which are a pair of ASCII control characters often used to indicate the end of a line of text). The header is separated from the message body by a blank line.

For example,

- To : header identifies the message recipient
- Subject : header says something about the purpose of the message
- Date : when the message was transmitted
- From : what user sent the message
- Received : each mail server that handled this message

Message Transfer

SMTP protocol used to transfer messages from one host to another. This is shown in Fig 2.4. First, users interact with a *mail reader* when they compose, then there is a *mail daemon* (or process) running on each host. It is possible that the sendmail program on a sender's machine establishes an SMTP/TCP connection

to the sendmail program on the recipient's machine. In many cases the mail traverses one or more *mail gateways* on its route from the sender's host to the receiver's host.

Mail Gateways

Independent of how many mail gateways are in the path, an independent SMTP connection is used between each host to move the message closer to the recipient. Each SMTP session involves a dialog between the two mail daemons, with one acting as the client and the other acting as the server. Multiple messages might be transferred between the two hosts during a single session. Since RFC 822 defines messages using ASCII as the base representation, SMTP is also ASCII based. This means it is possible for a human at a keyboard to pretend to be an SMTP client program.

Mail Reader

The final step is for the user to actually retrieve her messages from the mailbox, read them, reply to them, and possibly save a copy for future reference. The user performs all these actions by interacting with a mail reader. In many cases, this reader is just a program running on the same machine as the user's mailbox resides, in which case it simply reads and writes the file that implements the mailbox.

6 **Explain the role of a DNS on a computer network, including its involvement in the process of a user accessing a web page.** ***(May13) (Nov 15, 19) (Nov 21)***

We have been using addresses to identify hosts. The addresses are not exactly user friendly. For this reason that a unique *name* is also typically assigned to each host in a network. A naming service can be developed to map user-friendly names into router-friendly addresses. Name services are sometimes called *middleware* because they fill a gap between applications and the underlying network.

Host names differ from host addresses in two important ways.

- First, they are usually of variable length and mnemonic, thereby making them easier for humans to remember.
- Second, names typically contain no information that helps the network locate the host.

Some basic terminologies are:

- First a *Namespace* defines the set of possible names.
- Second, the naming system maintains a collection of *bindings* of names to values.
- Finally, a *resolution mechanism* is a procedure that, when invoked with a name, returns the corresponding value.
- A *name server* is a specific implementation of a resolution mechanism that is available on a network and that can be queried by sending it a message.

Name Servers

Name Resolution

7 **Explain about HTTP. Give their uses, state strengths and weaknesses.** ***(Nov 10,13)***

The Hypertext Transfer Protocol (HTTP) is a protocol used mainly to access data on the World Wide Web. HTTP functions as a combination of FTP and SMTP. It is similar to FTP because it transfers files and uses the services of TCP. It is much simpler than FTP because it uses only one TCP connection. HTTP is like SMTP because the data transferred between the client and the server look like SMTP messages. Unlike SMTP, the HTTP messages are not destined to be read by humans; they are read and interpreted by the HTTP server and HTTP client (browser). SMTP messages are stored and forwarded, but HTTP messages are delivered immediately

Strength

It offers lower CPU and memory usage due to less simultaneous connections.

➡It enables HTTP pipelining of requests/responses.

➡It offers reduced network congestion as there are fewer TCP connections.

➡Handshaking is done at the initial connection establishment stage.

Weekness

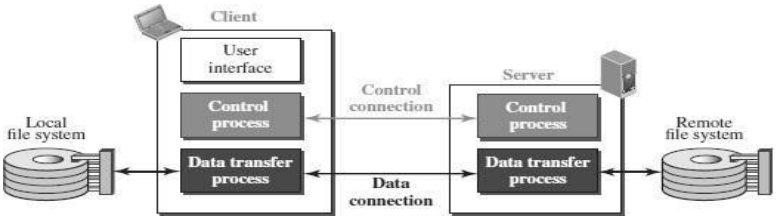
Lack of encryption

Man-in-the-middle attacks

Unsecured connections.

8 **Explain about FTP.** ***(Nov 12, 13, 19), May 13)***

FTP Mechanism



- Fig 2.2 shows the basic model of the FTP.
- The FTP client has three components:
  - user interface, control process, and data transfer process.
- The server has two components:
  - server control process and server data transfer process.

9 **Explain in detail about SNMP.**

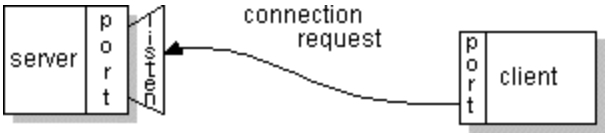
A network is a complex system, both in terms of the number of nodes and protocols that can be running on any one node. All the state of the nodes such as address translation tables, routing tables, TCP connection state, and so on need to be maintained for network management. Simple Network Management Protocol (SNMP) is a specialized request/reply protocol that allows us to read, and possibly write various pieces of state information on different network nodes. It supports two kinds of messages: GET and SET. GET is used to retrieve a piece of state from some node, and the SET is used to store a new piece of state in some node.

10 **Explain in detail about sockets with an example.**

Socket

A *socket* is one endpoint of a two-way communication link between two programs running on the network. A socket is bound to a port number so that the TCP layer can identify the application that data is destined to be sent to.

Normally, a server runs on a specific computer and has a socket that is bound to a specific port number. The server just waits, listening to the socket for a client to make a connection request.



UNIT II TRANSPORT LAYER

Introduction - Transport-Layer Protocols: UDP - TCP: Connection Management - Flow control - Congestion Control - Congestion avoidance (DECbit, RED) - SCTP - Quality of Service

PART-A

1 **Give any two Transport layer service.** ***(Dec 12)***

Multiplexing: Transport layer performs multiplexing/de- multiplexing function. Multiple applications employ same transport protocol, but use different port number. According to lower layer n/w protocol, it does upward multiplexing or downward multiplexing.

Reliability: Error Control and Flow Control.

2 **How IANA has divided port numbers?**

IANA (Internet Assigned Number Authority) has divided portnumbers into three ranges: 1) Well Known ports

2) Registered ports 3) Dynamic Ports.

List few well known ports for UDP.

Port	Protocol	Description
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram received
11	Users	Active Users
13	Daytime	Returns Date and Time

4 **How congestion occurs in a network?** ***(May / June 2021)***

The routers / switches in a network have a limited buffer size to store the received packets. If the packets arrive at a faster rate than what the receiver can store, then the packets are dropped leading to congestion.

5 **What is a Port?** ***(Nov 21)***

In computer networking, a port is a communication endpoint. At the software level, within an operating system, a port is a logical construct that identifies a specific process or a type of network service.

6 **Give the datagram format of UDP?**

The basic idea of UDP is for a source process to send a message toa port and for the destination process to receive the message from a port.

Source PortAddress 16 bits	Destination PortAddress 16 bits
Total Length 16 bits	Checksum 16 bits

7 **What is the main difference between TCP & UDP?**

TCP	UDP
It provides connection- oriented service	Provides connectionless service.
Connection Establishment delay will be there	No connection establishment and no delay
Provides reliable service	Provides unreliable, but fast service
It is used by FTP, SMTP	It is used by DNS, SNMP, audio,video and multimedia applications.

8 **Name the techniques and policies that can prevent (avoid)congestion.**

Techniques to avoid congestion:

- DEC (Digital Equipment Corporation) bit.
- Random Early Detection (RED).
- Source based congestion avoidance.

The congestion may be avoided by two policies:

- BECN - Backward Explicit Congestion Notification
- FECN - Forward Explicit Congestion Notification.

9 **List out various congestion control techniques.**

AIMD (Additive Increase Multiplicative Decrease), Slow start, Fastretransmit, Fast Recovery

10 **What are the advantages of using UDP over TCP?** ***(Nov 10)***

UDP is very useful for audio or video delivery which does not needacknowledgement. It is useful in the transmission of multimedia
data. Connection Establishment delay will occur in TCP.

11 **What is the use of UDP's Pseudo header?**

The pseudo header consists of three field from the IP header protocol number, source IP address and destination IP address plus the UDP length field (which is included twice in checksum calculation). The pseudo header is used to check whether the message is delivered between 2 endpoints.

12 **What are the four aspects related to the reliable delivery of data?**

(May 12)

The four aspects are

(i) Error control,

(ii) Sequence control

(iii) Loss control

(iv) Duplication control.

13 **Outline Stop and Wait ARQ mechanism. (Nov 19)**

In the stop-and-wait ARQ mechanism, sender sends one frame at a time; it is a special case of the general sliding window protocol with transmit and receive window sizes equal to one in both cases.

14 **What do you mean by slow start in TCP congestion?** ***(May 16)***

TCP slow start is an algorithm which balances the speed of a network connection. Slow start gradually increases the amount ofdata transmitted until it finds the network's maximum carrying capacity.

15 **Differentiate congestion control and flow control.** ***(Nov 13,15)***

Congestion Control	Flow Control
Congestion control means preventing the source from sending data that will end up getting dropped by a router because its queue is full.	Flow control means preventing the source from sending data that the receiver will end up dropping because it runs out of buffer space.
This is more complicated, because packets from different sources travelling different paths can converge on the same queue.	This is fairly easy with a slidingwindow protocol

16 **List the different phases used in TCP Connection.** ***(May 16)***

The different phases used in TCP connection are Connectionestablishment Phase, Data transfer and Connection Termination Phase

17 **List the advantages of Connection oriented services overconnectionless services.** ***(May 17)***

Connection Oriented:

Advantages:

1. Buffers can be reserved in advance
2. Sequencing can be guaranteed.Short headers.

18 **How do fast retransmit mechanism of TCP works?** ***(May 17)***

Fast Retransmit is an enhancement to TCP that reduces the time sender waits before retransmitting a lost segment. A TCP sender uses a timer to recognize lost segments. If an acknowledgement not received for a particular segment within a specified time (function of the estimated round-trip delay time), the sender will assume the segment was lost in the network, and will retransmit thesegment.

19 **Define SCTP** ***(Nov 21)***

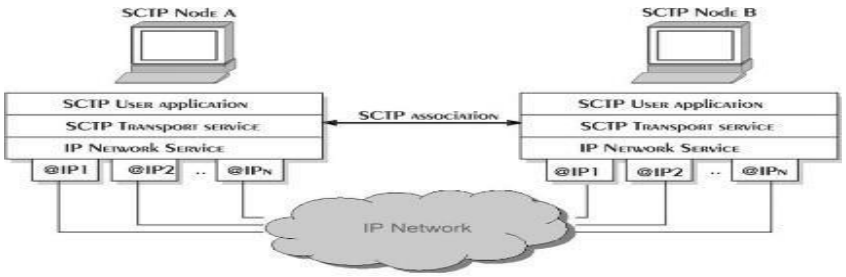
SCTP (Stream Control Transmission Protocol) is a reliable, message-oriented transport layer protocol. It combines the best features of UDP and TCP. It is mostly designed for internet applications.

20 **What is the use of SCTP Multiple stream service?**

SCTP allows multi stream service in each connection, which is called association in SCTP terminology. If one of the streams is blocked, the other streams can still deliver their data. The idea is similar to multiple lanes on a highway. The figure shows the idea of multi stream delivery.

21 **Define Multihoming Concept of SCTP**

Multihoming is the ability of an SCTP association to support multiple IP paths to its peer endpoint. The benefit of multihoming associations is that it makes the association more fault-tolerant against physical network failures and other issues on the interfaces.



22 **What happens in a three-way handshaking between any 2 devices? *(May/June 2021)***

The three-way handshake involves the exchange of three messages between the client and the server.

The client sends a segment to the server stating the initial sequence number it plans to use (Flags = SYN, Sequence Num = x).

The server responds with a single segment that both acknowledges the client's sequence number (Flags = ACK, ACK = x +1) and states its own beginning sequence number, (Flags = SYN, Sequence Num = y). Both the SYN and ACK bits are set in the Flags field of this secondmessage.

23 **What are the two categories of QoS attributes?**

User Oriented and Network Oriented. User related attributes are

SCR – Sustainable Cell RatePCR – Peak Cell Rate

MCR- Minimum Cell Rate

CVDT – Cell Variation Delay Tolerance.

The network related attributes are, Cell loss ratio (CLR), Cell transfer delay (CTD), Cell delay variation (CDV), Cell error ratio (CER).

UNIT-II / PART-B

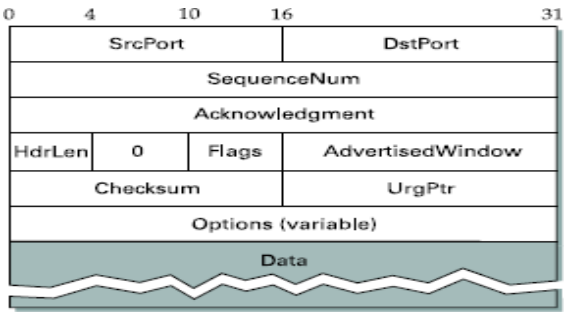
1 **Write short notes on *(May 12) (Nov 19) (Nov 21)***

i) TCP segment format (ii) Silly window syndrome

(Or)

Discuss the silly window syndrome and explain how to avoid it.

ii)

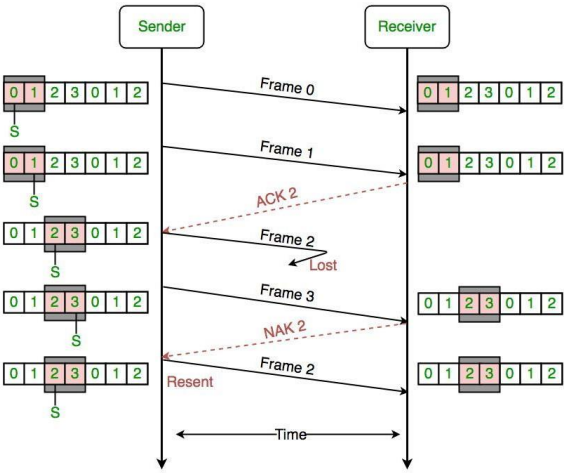


Silly Window Syndrome is a problem that arises due to poor implementation of TCP. It degrades the TCP performance and makes the data transmission extremely inefficient. The problem is called so

because:

i) It causes the sender window size to shrink to a silly value.
ii) The window size shrinks to such an extent that the data being transmitted is smaller than TCP Header.

2 **With neat architecture, Explain TCP and its sliding window algorithm for flow control.** ***(Nov 15)***



3 **Describe with examples the three mechanisms by which congestion control is achieved in TCP.** ***(Nov 13,15)(May 15,16)(Nov19)***

1. Additive Increase/Multiplicative Decrease

TCP maintains a new state variable for each connection, called Congestion Window, which is used by the source to limit how much data it is allowed to have in transit at a given time. TCP is modified such that the maximum number of bytes of unacknowledged data allowed is now the minimum of the congestion window and the advertised window

2. Slow Start

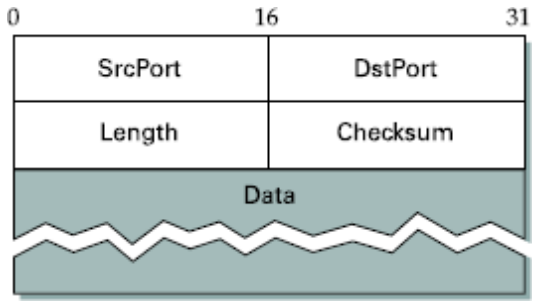
The additive increase mechanism is the right approach to use when the source is operating close to the available capacity of the network, but it takes too long to ramp up a connection when it is starting from scratch. TCP, therefore, provides a second mechanism, ironically called *slow start*, that is used to increase the congestion window rapidly from a cold start. Slow start effectively increases the congestion window exponentially, rather than linearly. Specifically, the source starts out by setting Congestion Window to one packet.

4 **Discuss congestion avoidance algorithm like DEC bit method and random early detection in transport layer with an example.*(May12,17)***

The first mechanism was developed for use on the Digital Network Architecture (DNA), a connectionless network with a connection-oriented transport protocol. The idea here is to more evenly split the responsibility for congestion control between the routers and the end nodes. Each router monitors the load it is experiencing and explicitly notifies the end nodes when congestion is about to occur. This notification is implemented by setting a binary congestion bit in the packets that flow through the router; hence the name DECbit. The destination host then copies this congestion bit into the ACK it sends back to the source. Finally, the source adjusts its sending rate so as to avoid congestion. A router sets this bit in a

packet if its average queue length is greater than or equal to 1 at the time the packet arrives.

5 **Define UDP. Discuss the operations of UDP. Explain UDP checksum with one example.** ***(Nov 21)***



UNIT III NETWORK LAYER

Switching: Packet Switching - Internet protocol - IPV4 - IP Addressing - Subnetting - IPV6, ARP, RARP, ICMP, DHCP

UNIT-III / PART-A

1 **What is packet switching?** ***(Nov 12)***

In a packet-switched network, it's not necessary to dedicate transmission capacity along a path through the network. Rather,data are sent out in a sequence of small chunks, called packets.

2 **What is subnetting?** ***(Nov 11,15)***

The whole network can't manage by single server, so that the entire network divided into small network in order to manage the network easily. Subnetting provides an elegantly simple way to reduce the total number of network numbers that are assigned. The idea is to take a single IP network number and allocate the IP address with that network to several physical networks, which are now referred to as subnets.

3 **What is subnet mask?**

A subnet mask is a number that defines a range of IP addresses available within a network. A single subnet mask limitsthe number of valid IPs for a specific network. Multiple subnet masks can organize a single network into smaller networks (called subnetworks or subnets).

4 **Define CIDR?**

CIDR, which stands for Classless Inter-Domain Routing, is an IP addressing scheme that improves the allocation of IP addresses. Itreplaces the old system based on classes A, B, and C. This helped to extend the life of IPv4 as well as slow the growth of routing tables.

5 **How many network addresses and host addresses are supportedby class A, class B networks?**

Class A: Number of networks = 127 Number of hosts = 2^{24} -1

Class B: Number of networks = 2^{14} -1

Number of hosts = 2^{16} – 1 = 65,535

6 **List out the functions of IP.**

IP services are unreliable, best-effort, connectionless packet delivery system. Unreliable – delivery is not guaranteed, Connectionless – each pocket is treated independent from others,
Best-effort delivery – it makes an earnest attempt to deliver
packets. It defines basic unit of data transfer through TCP/IP.

7 **What do you mean by ICMP?**

ICMP is an error reporting mechanism. It does not specify the action to be taken for each possible error. The source must relatethe error to an individual application program and take other actions to correct the problem.

8 **To whom ICMP reports error message will be sent?**

ICMP allows routers to send error messages to other router or hosts. ICMP is an error reporting mechanism. It does not specify the action to be taken for each possible error. It is informing the source that the error has occurred and the source has to take
actions to rectify the errors.

9 **When ICMP redirect message is used?** ***(May 17)***

An ICMP redirect is an error message sent by a router to the sender of an IP packet Redirects are used when a router believes a packet is being routed sub optimally and it would like to informthe sending host that it should forward the subsequent packets to that same destination through a different gateway.

10 **State the rules of non-boundary-level masking*? (May 12*)**

- The bytes in the IP address that corresponds to 255 in the maskwill be repeated in the sub network address.
- The bytes in the IP address that corresponds to 0 in the maskwill change to 0 in the sub network address.
- For other bytes, use the bit-wise AND operator.Example-

IP address	45	123	21	8
Mask	255	192	0	0
Subnet	45	64	0	0
123	0 1 1 1 1 0 1 1			
192	1 1 0 0 0 0 0 0			
64	0 1 0 0 0 0 0 0			

11 **How many network addresses and host addresses are supportedby class A, class B networks?**

Class A: Number of networks = 127 Number of hosts = 2^{24} -1Class B: Number of networks = 2^{14} -1
Number of hosts = 2^{16} – 1 = 65,535

12 **What is the network address in a class A subnet with the IP addresses of one of the hosts as 25.34.12.56 and mask255.255.0.0?** ***(May 14)***

IP Address - 25.34.12.56 , Mask - 255.255.0.0 , Network Address - 25.34.0.0

13 **What is IP address?**

An Internet Address is made of four bytes (32 bits) that define a host's connection to a network. There are currently 5 different field lengths patterns, each define a class of addresses. These aredesigned to

cover the needs of different types of organizations, class A, B, C, D, E.

14 **Explain IPV6 protocol. Why IPV6 is preferred over IPV4?** ***(May / June 2021)***

IPv6 (Internet Protocol version 6) is a set of basics of IPv6 are similar to those of IPv4. The most obvious improvement in IPv6 over IPv4 is that IP addresses are lengthened from 32 bits to 128 bits. This extension anticipates considerable future growth of the Internet and provides relief for what was perceived as an impending shortage of network addresses.

15 **What is DHCP?** ***(Nov 19)***

DHCP (Dynamic Host Configuration Protocol) is a protocol that provides quick, automatic, and central management for the distribution of IP addresses within a network. DHCP is also used to configure the subnet mask, default gateway, and DNSserver information on the device.

16 **Explain IPV4 protocol.**

IPv4 (Internet Protocol Version 4) is the fourth revision of the Internet Protocol (IP) used to identify devices on a network through an addressing system. The Internet Protocol is designed for use in interconnected systems of packet-switched computer communication networks. IPv4 is the most widely deployed Internet protocol used to connect devices to the Internet.IPv4 uses a 32-bitaddress scheme

17 **Present an outline of IPv6 addressing.** ***(Nov 19)***

An IPv6 address is 128 bits in length and consists of eight, 16-bit fields, with each field bounded by a colon. Each field must containa hexadecimal number, in contrast to the dotted-decimal notation of IPv4 addresses. In the below figure, the x's represent
hexadecimal numbers.

18 **What are the differences between IPV4 and IPV6?** ***(Nov 21)***

IPV4	IPV6
A 32-bit numeric address in IPv4 is written in decimal as four numbers separated by periods. Each number can be zero to 255. For eg, **1.160.10.240** could be an IPaddress.	IPv6 addresses are 128-bit IPaddress written in hexadecimaland separated by colons. An example IPv6 address could bewritten like this: **3ffe:1900:4545:3:200:f8ff:fe21:67cf**

19 **Identify the class of the following IP Address:** ***(May / June 2021)***

11000001 10000011 00011011 11111111 = Class C

252.5.15.111 = Class D

20 **Why is IPV4 to IPV6 transition required?** ***(May 17)***

IPv4 and IPv6 networks are not directly interoperable, transitiontechnologies are designed to permit hosts on either network type to communicate with any other host.

21 **Compare ARP and RARP.**

ARP	RARP
Address Resolution Protocol.	Reverse Address Resolution Protocol.
Retrieves the physical address of the receiver.	Retrieves the logical address fora computer from the server.

22 **What is the need of ARP? (Nov/Dec 2015)**

ARP is used to find the physical address of the node when its Internet address is known. Any time a host/router needs to find the physical address of another host on its network, it formats anARP query packet that includes the IP address and broadcasts it. All hosts in the network process the ARP packet but only the required station sends back physical address.

23 **Define RARP.**

Allows a host to discover its internet address when it knows only its physical address (a diskless computer). The host wishing to retrieve its internet address broadcasts an RARP query packet that contains its physical address to every host on its physical network.

A server on the network recognizes the RARP packet and returns

the host's internet address.

24 How many network addresses and host addresses are supportedby class A, class B networks?

- Class A: Number of networks = 127

  Number of hosts = 224 -1
- Class B: Number of networks = 214 -1

  Number of hosts = 216 – 1 = 65,535

25 List the difference between Packet Switching and CircuitSwitching. (Apr/May 2011, Nov/Dec 2011, May/June 2014)

Issue	Packet switching	Circuit Switching
Circuit setup	Not Required	Required
Transmission path	No Transmission path	Dedicated path
Delay	Packet transmission delay	Call setup delay
Addressing	Each packet containsthe full source and destination address	Only data is sent
Bandwidth	Dynamic Bandwidth	Fixed Bandwidth
Routing	Each packet is routed independently	Entire data is sent through the same path
Congestion control	Difficult	Easy if enough buffers can be located in advance for each VC set up
Complexity	In the transport layer	In the network layer
Suited for	Connection-oriented and connectionless service	Connection-oriented service

UNIT-III / PART- B

1 **Explain Packet Switching in detail.**

In this switching type, no specific path is used for data transfer. Instead, the data is chopped up into small pieces called packets and sent over the network. The packets can be routed, combined or fragmented, as required to get them to their eventual destination. On the receiving end, the process is reversed—the data is read from the packets and re-assembled into the form of the original data.

Datagrams

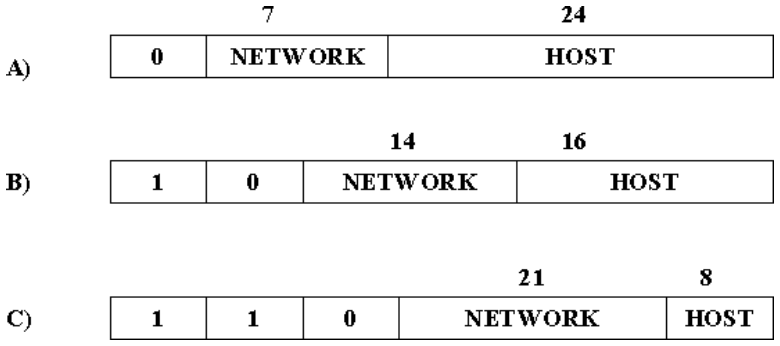
The idea behind datagram is every packet contains enough information to enable any switch to decide how to get it to its destination. That is, every packet contains the complete destination address. To decide how to forward a packet, a switch consults a forwarding table (sometimes called a routing table).

2 **i) Discuss the IP addressing methods. (May/June2014)**

Class A

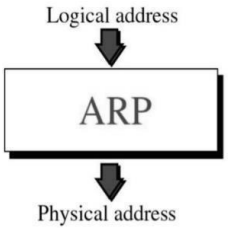
Class B

Class C



ii) Write short notes on ARP. (May/June2014) or Explain in detailARP. (Nov/Dec 2015)

ARP is a network layer protocol used to **convert a IP address (Network/Logical address) into a MAC Address (Hardware /Physical address).** The computer programs/applications use logical address (IP address) to send/receive messages, however the actual communication happens overthe physical address (MAC address)



3 **Explain in detail about DHCP. (Nov/Dec 2015)**

- The dynamic host configuration protocol is used to simplify the installation andmaintenance of networked computers.
- DHCP is derived from an earlier protocol called BOOTP.
- Ethernet addresses are configured into network by manufacturer and they areunique.

- IP addresses must be unique on a given internetwork but also must reflect thestructure of the internetwork

4 What is the need for ICMP? Mention ICMP MESSAGES and their purpose. (May/June 2013)

IP is always configured with a companion protocol, known as the Internet Control Message Protocol (ICMP), that defines a collection of error messages that are sent back to the source host whenever a router or host is unable to process an IP datagram successfully. For example, ICMP defines error messages indicating that the destination host is unreachable, the reassembly process failed, the TTL had reached 0, the IP header checksum failed, and so on. ICMP messages are divided into two broad categories:

- Error-reporting messages and
- Query messages.

5 Explain about IPV6? Compare IPV4 and IPV6 *(May 16)(Nov 21)*

To overcome the deficiencies of IPv4, IPv6 (Internetworking Protocol, version 6), also known as IPng (Internetworking Protocol, next generation), was proposed and is now a standard. In IPv6, the Internet protocol was extensively modified to accommodate the unforeseen growth of the Internet.

Prefix	Use
00...0 (128 bits)	Unspecified
00...1 (128 bits)	Loopback
1111 1111	Multicast addresses
1111 1110 10	Link local unicast
1111 1110 11	Site local unicast
Everything else	Global unicast

- IPv6 has longer addresses than IPv4. They are 128 bits long, providing an effectively unlimited supply of Internet addresses.
- The second major improvement of IPv6 is the simplification of the header. It contains only seven fields.
- The third major improvement is better support for options. This change was essential with the new header because fields that previously were required are now optional (because they are not used so often).
- IPv6 is not compatible with IPv4, but it is compatible with the other auxiliary Internet protocols, including TCP, UDP, ICMP, IGMP, OSPF, BGP, and DNS.
- Support for more security. The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.

UNIT IV ROUTING

Routing and protocols: Unicast routing - Distance Vector Routing - RIP - Link State Routing - OSPF - Path-vector routing - BGP - Multicast Routing: DVMRP - PIM.

UNIT IV - PART A

1 **Define routing.** ***(Nov12,15)***

It is the process of building up the tables that allow the collect output for a packet to be determined It is a lot harder to create the forwarding tables in large, complex networks with dynamically changing topologies and multiple paths between destinations. Routing is a process that takes place in the background so that, when a data packet turns up, we will have the right information in the forwarding table to be able to forward, or switch, the packet.

2 **Write on the packet cost referred in distance vector and link staterouting.** ***(May 2012)***

In distance vector routing, cost refer to hop count while in case oflink state routing, cost is a weighted value based on a variety of factors such as security levels, traffic or the state of the link.

3 **What is source routing?** ***(Nov 13)***

Rotation, stripping off and using pointers are the different types of source routing approach.

4 **What is the function of a router? (*Nov 10)(Nov 21*)**

Routers relay packets among multiple interconnected networks. They route packets from one network to any of a number of potential destination networks on internet. A router operates at the physical data link and network layer of the OSI model.

5 **Write the difference between Distance vector routing and Link state routing.**

Distance Vector Routing	**Link state routing**
Basic idea is each node sends its knowledge about the entire network to its neighbors.	Basic idea is every node sends its knowledge about its neighbors to the entire network
It is dynamic routing	It is dynamic routing
RIP uses Distance vector routing	OSPF uses link state routing

6 **What does a router do when it receives a packet with a destination address that it does not have an entry for, in itsrouting table?**

Default Router: If IP Software is not able to find the destination, from routing table then it sends the datagram to default router. It is useful when a site has small set of local address connected to it and connected to the rest of the Internet.

7 **What is piggybacking?** ***(Nov 19)***

The technique of temporarily delaying outgoing acknowledgmentso that they can be hooked onto the next outgoing data frame is
widely known as piggybacking.

8 **Explain Multicast routing?**

Multicast IP Routing protocols are used to distribute data forexample, audio/video streaming broadcasts) to multiple recipients. Using multicast, a source can send a single copy of datato a single multicast address, which is then distributed to an entire group of recipients.

9 **What is RIP?**

RIP (Routing Information Protocol) is a widely-used protocol for managing router information within a self-contained network such as a corporate local area network or an interconnected group of such LANs. Using RIP, a gateway host (with a router) sends its entire routing table (which lists all the other hosts it knows about)to its closest neighbor host every 30 seconds.

10 **Explain about OSPF.**

OSPF (Open Shortest Path First) is a router protocol used within larger autonomous system networks in preference to the RoutingInformation Protocol (RIP), an older routing protocol that is installed in many of today's corporate networks.

11 **What is PIM?**

Protocol-Independent Multicast (**PIM**) is a familyof multicast routing protocols for Internet Protocol (IP) networks that provide one-to-many and many-to-many distribution of data over a LAN, WAN or the Internet. It is termed *protocol- independent* because PIM does not include its own topology discovery mechanism, but instead uses routing information supplied by other routing protocols. PIM Source-Specific Multicast, Bidirectional PIMPIM Dense Mode, PIM Sparse Mode

12 **What is DVMRP?**

The Distance Vector Multicast Routing Protocol (DVMRP), is a routing protocol used to share information between routers to facilitate the transportation of IP multicast packets among networks. The protocol is based on the RIP protocol. The router generates a routing table with the multicast group of which it hasknowledge with corresponding distances. When a multicast packet is received by a router, it is forwarded by the router's interfaces specified in the routing table.

13 **What are the metrics used by routing protocols? (Apr/May 2015)** Path length, bandwidth, load, hop count, path cost, delay, Maximum Transmission Unit (MTU), reliability and communications cost.

14 **Define Unicasting, Broadcasting and Multicasting. (Nov/Dec 2011)**

Unicasting: Transmitting data from a single sender to a singlereceiver.
Broadcasting: Transmitting data from a single source to all theother nodes in the network
Multicasting: Transmitting data from a single source to a group ofdestination nodes.

15 **Explain BGP.**

BGP stands for Border Gateway Protocol. It can be defined as a standardized exterior gateway protocol which is developed to interchange routing information and reachability information between various autonomous systems (AS) on the Internet. It isclassified as a path vector protocol as well as a distance-vector routing protocol.

16 **What is a path vector routing protocol?**

A path-vector routing protocol is a network routing protocol which maintains the path information that gets updated dynamically. Updates that have looped through the network and returned to the same node are easily detected and discarded.

17 **What is count to infinity problem in distance vector routing?**

1. One of the important issues in Distance Vector Routing isCounty of Infinity Problem.
2. Counting to infinity is just another name for a routing loop.
3. In distance vector routing, routing loops usually occur when aninterface goes down.
4. It can also occur when two routers send updates to each other at the same time.

18 **What techniques are used to overcome the count to infinity issuein distance vector routing?**

Split horizon technique and split horizon with poison reverse technique are used to overcome count to infinity issue in distancevector routing.

19 **What are the contents of a link spate packet (LSP)?**

LSP contains the following information:

1. The ID of the node that created the LSP
2. A list of directly connected neighbors of that node, with the cost of the link to each one
3. A sequence number
4. A time to live for this packet

20 **What is the main difference between BGP and Distance vectorrouting.**

BGP differs from Distance Vector and Link State routings as it advertises complete paths as an enumerated list of ASs to reach aparticular network.

UNIT IV - PARTB

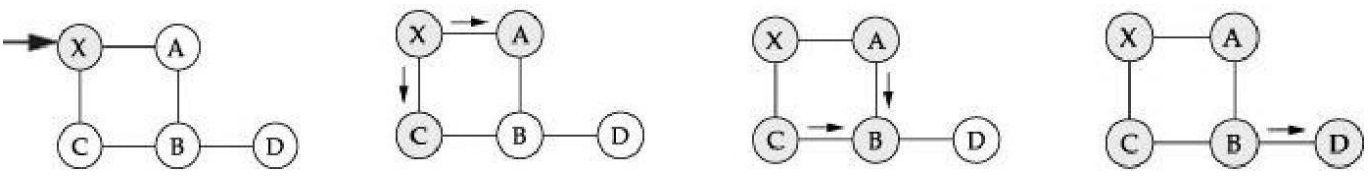
1 Explain what is Distance Vector Routing and Demonstrate how distance table gives routing table ***(Nov 21)***

- Distance vector routing is *distributed*, i.e., algorithm is run on all nodes.
- Each node *knows* the distance (cost) to each of its directly connected neighbors.
- Nodes construct a *vector* (Destination, Cost, NextHop) and distributes to its neighbors.
- Nodes compute routing table of *minimum* distance to every other node via NextHop using information obtained from its neighbors.

2 Discuss about Link-state routing and routers. ***(Nov 12) (May 15)***

- Each node knows state of link to its neighbors and cost.
- Nodes create an update packet called link-state packet (LSP) that contains:
- ID of the node
- List of neighbors for that node and associated cost
- 64-bit Sequence number
- Time to live
- Link-State routing protocols rely on two mechanisms:
- Reliable flooding of link-state information to all other nodes
- Route calculation from the accumulated link-state knowledge

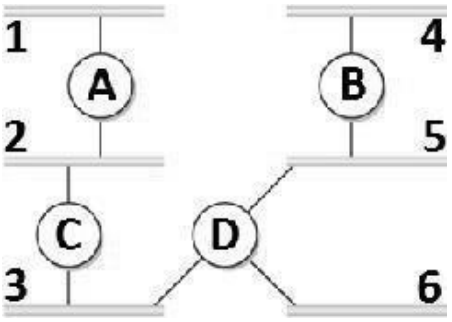
Example:



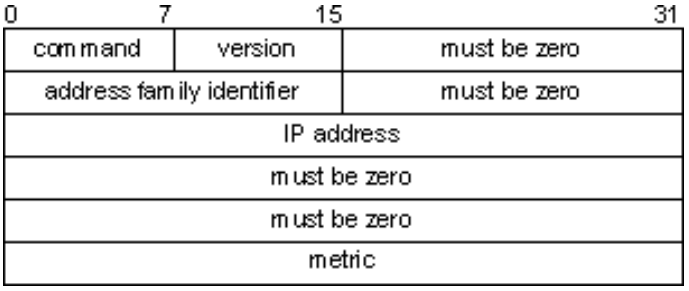
4 Explain the Routing Information protocol/Distance vector routing in detail.***(Nov 13,15) (May 15,16)(Nov 19)***

- RIP is an intra-domain routing protocol based on distance-vector algorithm.

Example



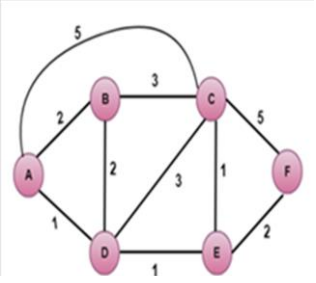
- Routers *advertise* the cost of reaching networks. Cost of reaching each link is 1 hop. For example, router *C* advertises to *A* that it can reach network 2, *3* at cost 0 (directly connected), networks *5*, *6* at cost 1 and network *4* at cost 2.
- Each router *updates* cost and next hop for each network number.
- Infinity is defined as 16, i.e., any route cannot have more than 15 hops. Therefore RIP can be implemented on small-sized networks only.
- Advertisements are sent every 30 seconds or in case of triggered update.



5 What are the different routing algorithms? List out their pros and cons. ***(May / June 2021)***

1. Distance Vector Routing Algorithm – Routing Information Protocol
2. Link State Routing Algorithm – Open Shortest Path First Protocol
3. Path-Vector Routing Algorithm - Border Gateway Protocol

6 Explain Link state routing with D ijkstra's algorithm for the following graph.



Step	N	D(B),P(B)	D(C),P(C)	D(D),P(D)	D(E),P(E)	D(F),P(F)
1	A	2,A	5,A	1,A	∞	∞
2	AD	2,A	4,D		2,D	∞
3	ADE	2,A	3,E			4,E
4	ADEB		3,E			4,E
5	ADEBC					4,E
6	ADEBCF					

Step 1:
The first step is an initialization step. The currently known least cost path from A to its directly attached neighbors, B, C, D are 2,5,1 respectively. The cost from A to B is set to 2, from A to D is set to 1 and from A to C is set to 5. The cost from A to E and F are set to infinity as they are not directly linked to A.

Step 2:
In the above table, we observe that vertex D contains the least cost path in step 1. Therefore, it is added in N. Now, we need to determine a least-cost path through D vertex.

UNIT V DATA LINK AND PHYSICAL LAYERS

Data Link Layer - Framing - Flow control - Error control - Data-Link Layer Protocols - HDLC - PPP - Media Access Control - Ethernet Basics - CSMA/CD - Virtual LAN - Wireless LAN (802.11) - Physical Layer: Data and Signals - Performance - Transmission media- Switching - Circuit Switching.

UNIT V - PART A

1 **List out the functions of data link layer *(May / June 2021)***

Data link layer deals with node-to-node delivery of data. The services provided by the data link layer include: framing, flowcontrol, error control and access control.

2 **What do you mean by framing? (Nov/Dec2013 and Nov/Dec 2014)**

The data link layer divides the stream of bits received from the network layer into manageable data units called frames. The waysto address the framing problem are

- Byte-Oriented Protocols (PPP)
- Bit-Oriented Protocols (HDLC)
- Clock-Based Framing (SONET)

3 **What are the two types of errors occurred during datatransmission? (May/June 2012)**

Single bit error and burst error

4 **Compare error detection and correction. (Nov/Dec 2012)**

Error Detection	Error Correction
Only the occurrence of an erroris checked	The exact number of bits thatare corrupted and location of error in the message areknown.

5 **Define bit stuffing. (Apr/May 2011)**

HDLC denotes both the beginning and the end of a frame with the distinguished bit sequence 01111110. This sequence might appear anywhere in the body of the frame, it can be avoided by bit stuffing. On the sending side, any time five consecutive 1's has been transmitted from the body of the message (i.e., excluding when the sender is trying to transmit the distinguished 01111110 sequence), the sender inserts a 0 before transmitting the next bit.

6 **What do you mean by Flow Control? (Nov/Dec 2011)**

Flow control is a technique for assuring that a transmitting entity does not overwhelm a receiving entity with data. It is a feedback mechanism by which the receiver is able to regulate the sender. Such a mechanism is used to keep the sender from overrunning the receiver, i.e., from transmitting more data than the receiver is able to process

7 **Why is flow control and error control duplicated in differentlayers?**

Like the data link layer, the transport layer is responsible for flow and error control. Flow control and error control at data link layer is node-to-node level. But at transport layer, flow control and error control is performed end-end rather than across a single link.

8 **Differentiate between lost frame and damaged frame?**

Lost Frame	Damaged Frame
Lost frame is the frame thatfails to arrive at the other side.	The damaged frame is arecognizable frame does arrive, but some of the bits are in error

9 **What is the difference between stop and wait and slidingwindow protocol? (Nov/Dec 2012)**

Stop and Wait Protocol	Sliding Window Protocol
In stop and wait protocol,we can send one frame at a time	In sliding window protocol, we cansend multiple frames at a time.
Shows poor performance than Sliding Window Protocol, comparatively	As sliding window doesn't waste network bandwidth compared with stop-n-wait, both in normal and in congested condition, sliding window show better performance than stop-n-wait.

10 **Why sliding window flow control is considered to be moreefficient than stop and wait flow control?**

In sliding window flow control, the transmission link is treated asa pipeline that may be filled with frames in transit. But with stop- and-wait flow control only one frame may be in the pipe at a time.

11 **Define Piggybacking?**

The technique of temporarily delaying outgoing acknowledgmentso that they can be hooked onto the next outgoing data frame is widely known as piggybacking.

12 **Find the hamming distance between the two pair of code words:A = 01011; B = 11110** ***(May / June 2021)***

Hamming distance is the numbers of bits by which two codes differ. Here hamming distance = 3

13 **Define hidden node problem.** ***(May 16)***

In wireless networking, the hidden node problem or hidden terminal problem occurs when a node is visible from a wireless access point (AP), but not from other nodes communicating with that AP. This leads to difficulties in media access control sub layer.

14 **What is the access method used by wireless LAN?** ***(May 14)***

The access method used by wireless LAN is Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

15 **What is meant by Exponential back of algorithm?**

After first collision, each station waits either 0 or 1 slot time before trying again. If two stations collide and each one picks samerandom number 0/1. After second collision, each one picks 0, 1, 2 or 3 slot at random and waits. If collision occurs again, then next time the number of slots to wait is chosen at random from 0 to $[2^3 - 1]$. This algorithm is called binary exponential "back off algorithm".

16 **What is High Level data link control?** ***(Nov 21)***

High-Level Data Link Control is a bit-oriented code-transparent synchronous data link layer protocol developed by the International Organization for Standardization. The standard for HDLC is ISO/IEC 13239:2002. HDLC provides both connection- oriented and connectionless service.

17 **Give the format of Ethernet address.**

Preamble	Destaddr	Src addr	Type	Body	CRC
64	48	48	16		32

18 **Outline the use of cyclic redundancy check.** ***(Nov 19)***

A cyclic redundancy check (CRC) is an error-detecting codecommonly used in digital networks and storage devices to detect accidental changes to raw data.

19 **What is CSMA/CD?** ***(Nov 11)***

Carrier Sense Multiple Access with Collision Detection is one of the methods of medium access. It is used to sense whether a medium is busy before transmission. If the medium is busy, it refrains from transmitting the data or else proceeds with the transmission. Also has the ability to check whether a transmission has collided with another.

20 **Examine how Network Interface Card works.** ***(Nov 21)***

A Network Interface Card provides a computer with a dedicated, full-time connection to a network. It implements the physical layer circuitry necessary for communicating with a data link layer standard, such as Ethernet or Wi-Fi.

21 **List the rules for CSMA/CD.**

1. If the medium is idle, transmit; otherwise go to step 2.
2. If the medium is busy, continue to listen until the channel is idle,and then transmit immediately.
3. If a collision detected during transmission, transmit a brief jamming signal to all station to indicate collision has occurred andthen cease transmission.

22 **Mention some of the physical properties of Ethernet.** ***(May 11)***

The Ethernet is a multiple-access network, meaning that a set of nodes send and receive frames over a shared link. An Ethernet islike a bus that has multiple stations plugged into it.

23 **Write the parameters used to measure network performance.** ***(May 2016)***

The parameters used to measure network performance are Latency, Throughput, Delay and Bandwidth.

24 **Outline the need for switching.** ***(Nov 19)***

Switched communication networks are those in which data transferred from source to destination is routed between various intermediate nodes. Switching is the technique by which nodes control or switch data to transmit it between specific points on a network. There are three common switching techniques:

Circuit Switching, message switching and packet switching.

25 **List the types of Transmission media.** ***(Nov 21)***

Transmission Media is broadly classified into the following types: Guided Media: It is also referred to as Wired or Bounded transmission media. Common types are: (i) Twisted Pair Cable (ii) Coaxial Cable (iii) Optical Fiber Cable

Unguided Media: Wireless Transmission. Common Types are:

(i) Satellite (ii) Infrared (iii) Broadcast (iv)Wi-Fi

26 **Define Bandwidth**

Bandwidth refers to the number of bits per second that a channel,a link, or even a network can transmit.

27 **What is Throughput?**

It is a measure of how data can actually be sent through network.

28 **What is meant by the contention period of Ethernet?**

When several stations on an Ethernet have data to send, there arecontention periods during which collisions happen and no data issuccessfully transmitted.

29 **What does IEEE 10 Base 5 standard signify?**

- 10 represents data rate 10 Mbps.
- 5 refers to segment length 5* 100 m that can run withoutrepeaters
- Base represents Base band communication.

30 **What do you mean by CSMA protocol? (Apr/May 2015)**

Carrier sense multiple access (CSMA) is a media access control (MAC) protocol in which a node verifies the absence of other traffic before transmitting on a shared transmission medium.

Carrier sense means that a transmitter attempts to determine whether another transmission is in progress before initiating a transmission. If a carrier is sensed, the node waits for the transmission in progress to end before initiating its own transmission. In other words, CSMA is based on the principle "sense before transmit". Multiple access means that multiple nodes may send and receive on the medium. Transmissions by one node are generally received by all other nodes connected to the medium.

UNIT-V / PART-B

1 Given a remainder of 111, a data unit of 10110011 and a divisor of 1001, is there an error in the data unit. Justify your answer with necessary principles. ***(May 14)***

Ans:

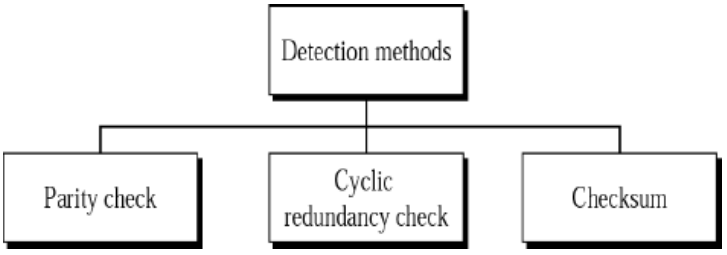
While using CRC technique, the reminder should be zero for errorless data transfer. Here it has 111 as reminder. So definitely the data at receiver end has error.

2 Explain the various error detection techniques with example. (Nov 10,12), (May 12,16)

Types of errors

SINGLE-BIT ERROR

BURST ERROR



3. Discuss in detail about the HDLC protocol (Bit Oriented Protocol). ***(May 16) (Nov 19)***
    1. Normal response mode (NRM)
    2. Asynchronous balanced mode (ABM)

HDLC FRAMES:

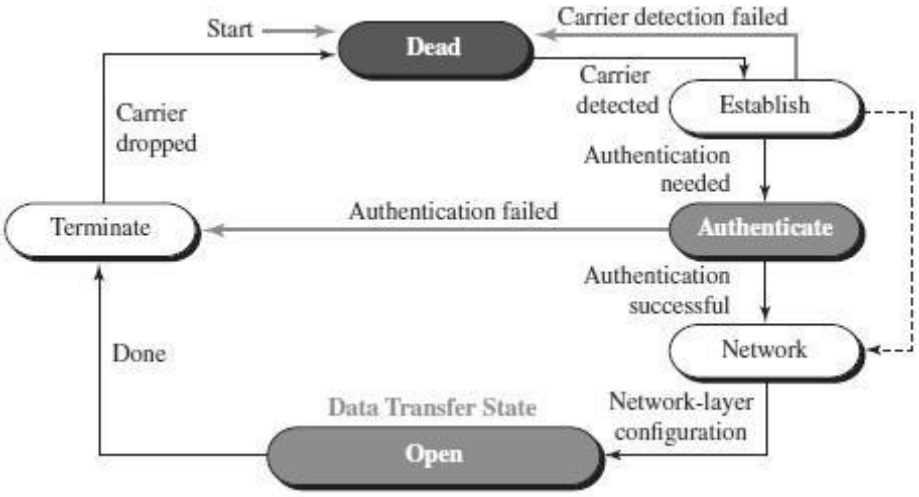
HDLC defines three types of frames:

3. Information frames (I-frames) - used to carry user data
4. Supervisory frames (S-frames) - used to carry control information
5. Unnumbered frames (U-frames) – reserved for system management

4. Discuss in detail about the PPP protocol (Byte Oriented Protocol).
    - Point-to-Point Protocol (PPP) was devised by IETF (Internet EngineeringTask Force) in 1990 as a Serial Line Internet Protocol (SLIP).
    - PPP is a data link layer communications protocol used to establish a direct connection between two nodes.
    - It connects two routers directly without any host or any other networkingdevice in between.

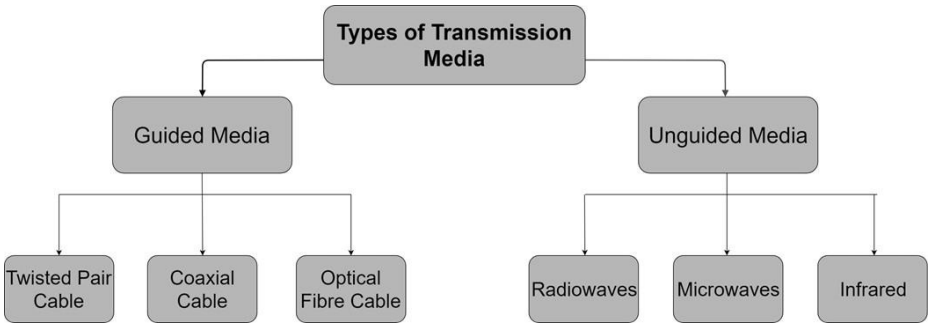
PPP Frame

Transition Phases in PPP



5. Explain Transmission media and its types in detail. ***(May / June 2021)***

- Transmission media is a communication channel that carries the information from the sender to the receiver.
- Data is transmitted through the electromagnetic signals.
- The main functionality of the transmission media is to carry the information in the form of bits (Either as Electrical signals or Light pulses).
- It is a physical path between transmitter and receiver in data communication.


Types of Transmission Media
Guided Media
Unguided Media
Twisted Pair Cable
Coaxial Cable
Optical Fibre Cable
Radiowaves
Microwaves
Infrared