Computer Neworking

New Syllabus

Bachelor in Computer Applications
Course Title: Computer Networking
Code No: CACS303
Semester: V

Full Marks: 60
Pass Marks: 24
Time: 3 hours

Candidates are required to give their answer in their own words as far as practicable.

Group 'A'

Attempt all the questions. $10 \times 1 = 10$

1. Circle (O) the correct answer in the following questions

i. Set of rules that governs data communication is called _____
   a) Protocol b) standards c) RFCs d) servers

ii. Which of this is not a guided media?
   a) Coaxial cable b) twisted pair cable
   c) optical fiber d) wireless LAN

iii. The identifier that is used for data transfer in virtual circuit network is calle _____
   a) Global address b) virtual circuit identifier
   c) Network identifier d) IP identifier

iv. In classless addressing, there are no classes but addresses are still granted i _____
   a) IPs b) blocks c) codes d) sizes

v. In classful addressing, a large part of available addresses is _____
   a) Organized b) blocked c) wasted d) communicate

vi. Which is not an application layer protocol?
   a) HTTP b) SMTP c) FTP d) TCP

vii. Which mode of IPSec should you use to assure the security an confidentiality of data within the same LAN?
   a) AH transport mode b) ESP transport mode
   c) ESP tunnel mode d) AH tunnel mode

viii. The entire hostname has a maximum of _____
   a) 255 characters b) 127 characters
   c) 63 characters d) 31 characters

ix. What protocol is not used in the operation of a VPN?
   a) PPTP b) IPSec c) YMUM d) L2TP

x. The DHCP server can provide the _____ of the IP addresses.
   a) Dynamic allocation b) automatic allocation
   c) Static allocation d) all of the mentioned

Answer-Key

i. (a)	ii. (c)	iii. (b)	iv. (b)	v. (c)	vi. (d)	vii. (b)	viii. (a)	ix. (c)	x. (d)

Group B

Attempt any SIX questions. [6×5=30]

2. Is 192.16.144.64/27 a host, network or broadcast address? In which layer of OSI model do HUB, Switch and Router operate on? [4+1]

Ans: IP address: 192.16.144.64/27

Subnet Mask: 11111111 11111111 11111111 11100000 = 255.255.255.224

Total Subnets = $2^3 = 8$

Valid Subnets (4^{th} octet) =Total subnet mask - Current subnet mask

= 256 – 224= 32

Networks ID are: 192.16.144.0, 192.16.144.32, 192.16.144.64, 192.16.144.96, 192.16.144.128, 192.16.144.160, 192.16.144.192, 192.16:144.224

Therefore, 192.16.144.64/27 is a network address.

The layers of OSI model where HUB, Switch and Router operate are First Layer (Physical Layer), Second Layer (Data Link Layer) and Third Layer (Network Layer) respectively.

3. Describe the working procedure of Token bus and Token ring. [2.5+2.5]

Ans: **Token Bus**

The IEEE 802.4 Committee has defined token bus standards as broadband computer networks, as opposed to Ethernet's baseband transmission technique. **Physically, the token bus is a linear or tree-shape cable to which the stations are attached. The topology of the computer network can include groups of workstations connected by long trunk cables. Logically, the stations are organized into a ring.** These workstations branch from hubs in a star configuration, so the network has both a bus and star topology. Token bus topology is well suited to groups of users that are separated by some distance. IEEE 802.4 token bus networks are constructed with 75-ohm coaxial cable using a bus topology. The broadband characteristics of the 802.4 standard support transmission over several different channels simultaneously.

Token Passing Mechanism in Token Bus

In token bus network station must have possession of a token before it can transmit on the computer network. When the logical ring is initialized, the highest numbered station may send the first frame. The token and frames of data are passed from one station to another following the numeric sequence of the station addresses. Thus, the token follows a logical ring rather than a physical ring. The last station in numeric order passes the token back to the first station. The token does not follow the physical ordering of workstation attachment to the cable. Station 1 might be at one end of the cable and station 2 might be at the other, with station 3 in the middle. In such a case, there is no collision as only one station possesses a token at any given time. In token bus, each station receives each frame; the station whose address is specified in the frame processes it and the other stations discard the frame. This is depicted in the following diagram:

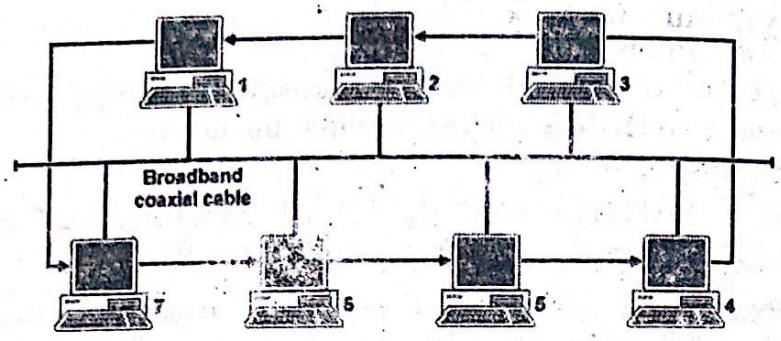


Figure: Token bus network

Token Ring

Token ring is the IEEE 802.5 standard for a token-passing ring in communication networks. A ring consists of a collection of ring interfaces connected by point-to-point lines i.e., ring interface of one station is connected to the ring interfaces of its left station as well as right station. Internally, signals travel around the communication network from one station to the next in a ring.

These point-to-point links can be created with twisted pair, coaxial cable or fiber optics. Each bit arriving at an interface is copied into a 1-bit buffer. In this buffer the bit is checked and may be modified and is then copied out to the ring again. This copying of bit in the buffer introduces a 1-bit delay at each interface.

Token Ring is a LAN protocol defined in the IEEE 802.5 where all stations are connected in a ring and each station can directly hear transmissions only from its immediate neighbor. Permission to transmit is granted by a message (token) that circulates around the ring. A token is a special bit pattern (3 bytes long). There is only one token in the network.

Token Passing Mechanism in Token Ring

If a station has a frame to transmit when it receives a token, it sends the frame and then passes the token to the next station; otherwise it simply passes the token to the next station. Passing the token means receiving the token from the preceding station and transmitting to the successor station. The data flow is unidirectional in the direction of the token passing. In order that tokens are not circulated infinitely, they are removed from the network once their purpose is completed. This is shown in the following diagram –

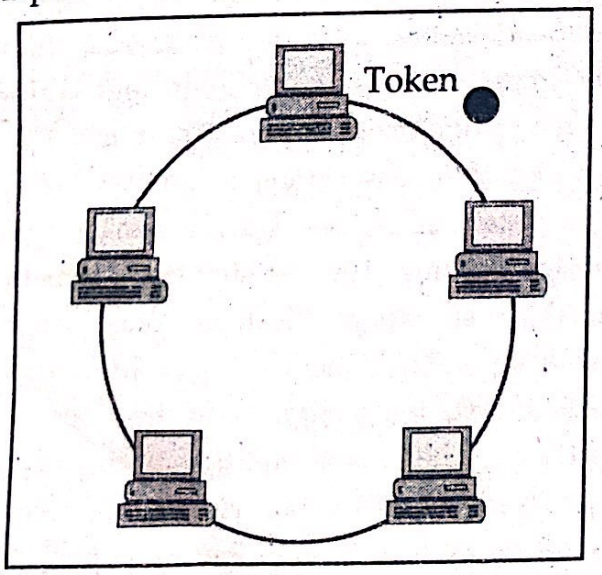


Figure: Token ring network

4. **Why do you think network traffic analysis is carried out? How does IPv6 overcome the disadvantages of IPv4?** [2+3]

Ans: Unlimited information exchange is one of the most significant results of today's advancing computing and information technologies. The world becomes smaller, as people get more connected every day. This evolution has brought many benefits to our society when it comes to information dissemination, international cooperation, business opportunities and more. Unfortunately, these advantages bring with them serious security threats. Information can be disseminated through unsecure avenues because anyone with basic knowledge of computers and internet computing can easily share information online. The various technological innovations have also given birth to a new generation of hackers, whose main objective is to steal and trade valuable information either for money or political purposes. This is why many companies have started to secure their firewalls, update their anti-malware software, and invest in a network security solution. Network traffic analysis helps in warding off different cyber-attacks like:

- Uses Behavioral Patterns to Spot Suspicious Activities
- Helps Pinpoint Invisible Threats
- Minimizes Damage and Profit-loss

IPv6 overcomes the disadvantages of IPv4 as follows:

- **More Efficient Routing:** IPv6 reduces the size of routing tables and makes routing more efficient and hierarchical. IPv6 allows ISPs to aggregate the prefixes of their customers' networks into a single prefix and announce this one prefix to the IPv6 Internet. In addition, in IPv6 networks, fragmentation is handled by the source device, rather than the router, using a protocol for discovery of the path's maximum transmission unit (MTU).
- **More Efficient Packet Processing:** IPv6's simplified packet header makes packet processing more efficient. Compared with IPv4, IPv6 contains no IP-level checksum, so the checksum does not need to be recalculated at every router hop. Getting rid of the IP-level checksum was possible because most link-layer technologies already contain checksum and error-control capabilities. In addition, most transport layers, which handle end-to-end connectivity, have a checksum that enables error detection.
- **Directed Data Flows:** IPv6 supports multicast rather than broadcast. Multicast allows bandwidth-intensive packet flows (like multimedia streams) to be sent to multiple destinations simultaneously, saving network bandwidth. Disinterested hosts no longer must process broadcast packets. In addition, the IPv6 header has a new field, named Flow Label that can identify packets belonging to the same flow.
- **Simplified Network Configuration**: Address auto-configuration (address assignment) is built in to IPv6. A router will send the prefix of the local link in its router advertisements. A host can generate its own IP address by appending its link-layer (MAC) address, converted into Extended Universal Identifier (EUI) 64-bit format, to the 64 bits of the local link prefix.

- **Support for New Services:** By eliminating Network Address Translation (NAT), true end-to-end connectivity at the IP layer is restored, enabling new and valuable services. Peer-to-peer networks are easier to create and maintain, and services such as VoIP and Quality of Service (QoS) become more robust.
- **Security:** IPSec, which provides confidentiality, authentication and data integrity, is baked into in IPv6. Because of their potential to carry malware, IPv4 ICMP packets are often blocked by corporate firewalls, but ICMPv6, the implementation of the Internet Control Message Protocol for IPv6, may be permitted because IPSec can be applied to the ICMPv6 packets.

5. Find Hamming Code for data 01100111. [5]

Ans: Total number of data bits 'm' = 8

Number of redundant bits r: $2^r >= m + r + 1$

$2^r \geq 8 + r + 1$

$2^4 \geq 8 + 4 + 1 = 13$ (Satisfied)

Therefore, the value of r is 4 that satisfy the above relation and $r_8r_4r_2r_1$ are redundant bits.

Total number of bits = m +r = 8 + 4 = 12;

0	1	1	0	r_8	0	1	1	r_4	1	r_2	r_1
12	11	10	9	8	7	6	5	4	3	2	1

r_1: Checking even parity on bits 1,3,5,7,9,11

r_1:1

r_2: Checking even parity on bits 2, 3, 6, 7, 10, 11

r_2:0

r_4: Checking even parity on bits 4, 5, 6, 7, 12

r_4:1

r_8: Checking even parity on bits 8, 9, 10, 11, 12

r_8:0

Substituting the value of redundant bits, we get,

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

Therefore, Hamming Code for data 01100111 is **011000111101.**

6. Differentiate between TCP and UDP.

Ans: Difference between TCP and UDP are shown in table below:

Characteristics / Description	UDP	TCP
General	Simple, High Speed, Low Functionality	Full-featured, Reliable Data Transfer
Connection Setup	Connectionless	Connection Oriented
Data Interface to Application	Message Based Data is Sent	Stream Based data is sent
Reliability	Unreliable (No ACK)	Reliability (ACK available)
Retransmission	Not Performed	Data is Lost → Retransmission
Flow Control	None	Sliding Window → Flow Control
Overhead	Very Low	Low, Higher than UDP
Transmission Speed	Very High	High, Lower than UDP

Application that uses Protocol	DNS, DHCP, SNMP, (Multimedia Application)	FTP, Telnet, SMTP, DNS, HTTP, etc.

7. Explain DNS with reference to its hierarchy and records.

Ans: DNS is a global system for translating IP addresses to human-readable domain names. When a user tries to access a web address like "example.com", their web browser or application performs a DNS Query against a DNS server, supplying the hostname. The DNS server takes the hostname and resolves it into a numeric IP address, which then web browser can connect to.

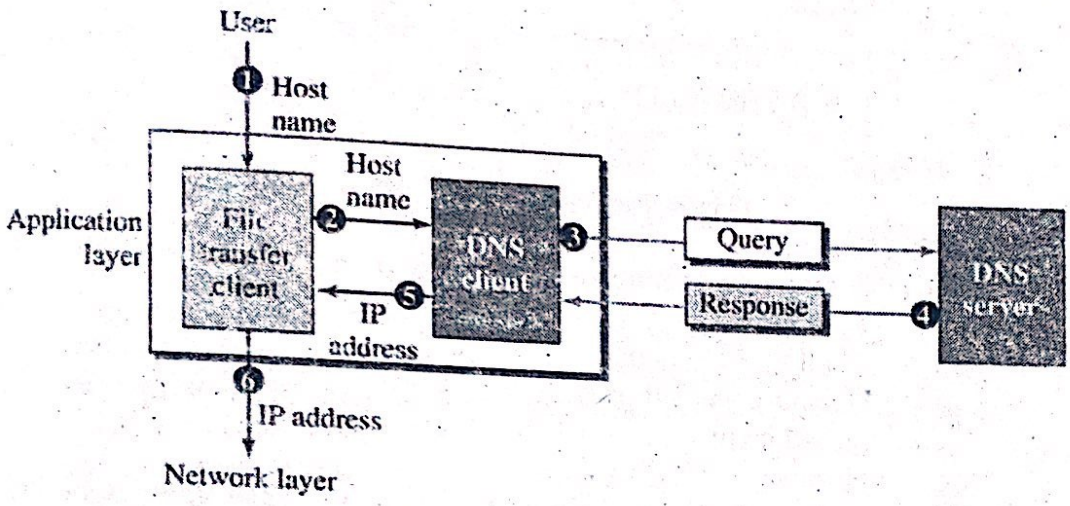


Figure: Purpose of DNS

Let's discuss the concepts and ideas behind the DNS. Above figure shows how TCP/IP uses a DNS client and a DNS server to map a name to an address. A user wants to use a file transfer client to access the corresponding file transfer server running on a remote host. The user knows only the file transfer server name. Such as *example.com*. However, the TCP/IP suite needs the IP address of the file transfer server to make the connection.

The following six steps map the host name to an IP address:

i. The user passes the host name to the file transfer client.
ii. The file transfer client passes the host name to the DNS client.
iii. Each computer, after being booted, knows the address of one DNS server. The DNS client sends a message to a DNS server with a query that gives the file transfer server name using the known IP address of the DNS server.
iv. The DNS server responds with the IP address of the desired file transfer server.
v. The DNS server passes the IP address to the file transfer client.
vi. The file transfer client now uses the received IP address to access the file transfer server.

Figure below shows an example of how DNS client/server program can support an e-mail program to find the IP address of an e-mail recipient. A user of an e-mail program may know the e-mail address of the recipient; however, the IP protocol needs the IP address. The DNS client program sends a request to a DNS server to map the e-mail address to the corresponding IP address.

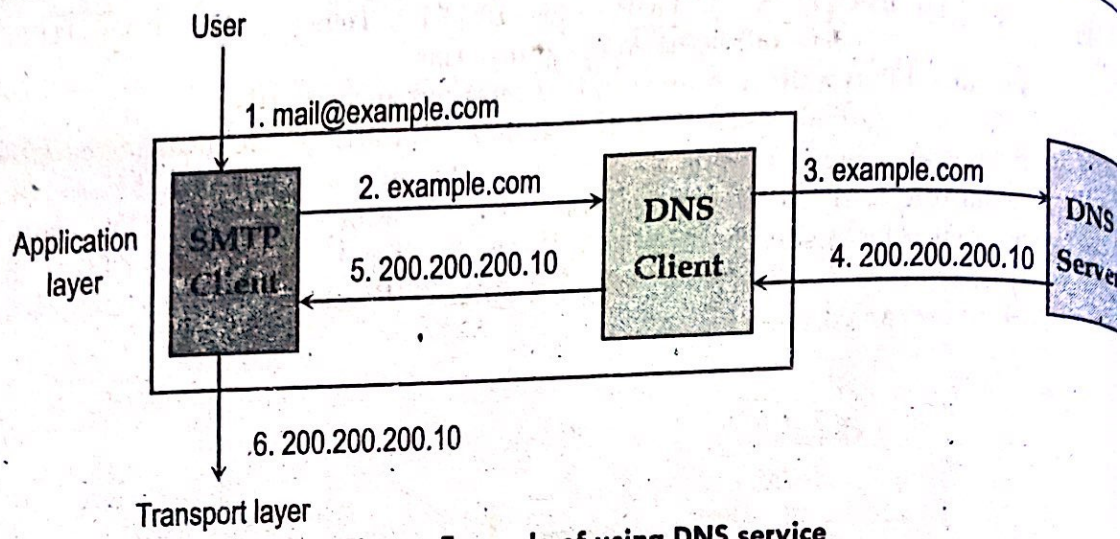


Figure: Example of using DNS service

DNS Hierarchy

The DNS hierarchy is comprised of the following elements:

i) Root Level
ii) Top Level Domains
iii) Second Level Domains
iv) Sub-Domain
v) Host-

For example, in the figure below, .edu is the top-level domain, berkeley i the second level domain, and .cs is the sub-domain of berkeley. Eos is th host name. A DNS server would store the IP address of the host where it name resides in the tree.

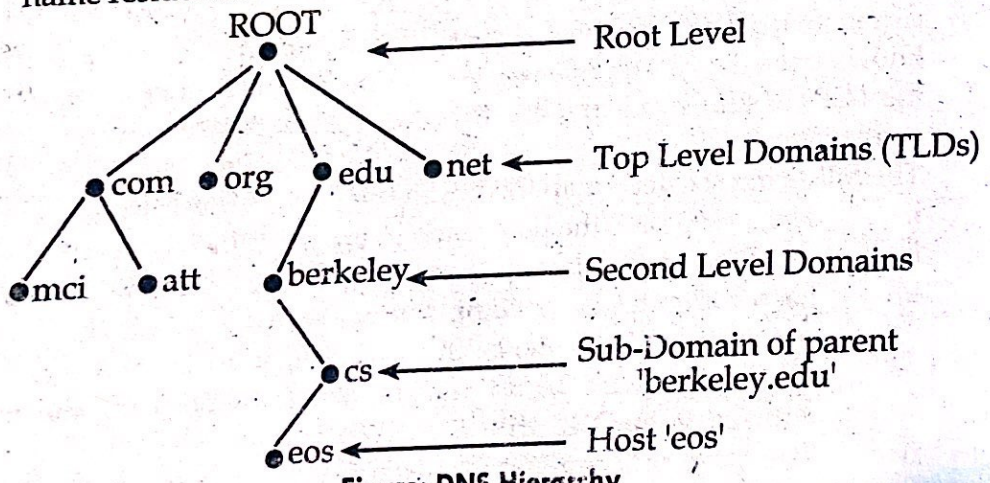


Figure: DNS Hierarchy

Types of DNS Records

Two types of records are used in DNS i.e. question records and resource records.

Question Record

A question record is used by the client to get information from a server. This contains the domain name. The list below describes question record fields.

- **Query name:** This is a variable-length field containing a domain name.
- **Query type:** This is a 16-bit field defining the type of query. Table below shows some of the types commonly used.

Type	Description
A	**Address.** A 32-bit IPv4 address
PTR	**Pointer.** It is used to convert an IP address to a domain name.
NS	**Name Server.** It identifies the authoritative servers for a zone
CNAME	**Canonical name.** It defines an alias for the official name of a host
SOA	**Start of Authority.** It marks the beginning of a zone
MX	**Mail exchange.** It redirects mail to a mail server
AAAA	**Address.** An IPv6 address
WKS	**Well-known services.** It defines the network services that a host provides.
AXFR	A request for the transfer of the entire zone.
ANY	A request for all records

- **Query class:** This is a 16-bit field defining the specific protocol using DNS.

Resource Record

Each domain name (each node on the tree) is associated with a record called the resource record. The server database consists of resource records. Resource records are also what is returned by the server to the client.

8. **Write short notes on (Any Two):** **[2.5+2.5]**

a. Multiplexing

Ans: Multiplexing is a technique used to combine and send the multiple data streams over a single medium. The process of combining the data streams is known as multiplexing and hardware used for multiplexing is known as a multiplexer. Multiplexing is achieved by using a device called **Multiplexer (MUX)** that combines n input lines to generate a single output line. Multiplexing follows many-to-one, i.e., n input lines and one output line. Demultiplexing is achieved by using a device called **Demultiplexer (DEMUX)** available at the receiving end. DEMUX separates a signal into its component signals (one input and n outputs). Therefore, we can say that demultiplexing follows the one-to-many approach.

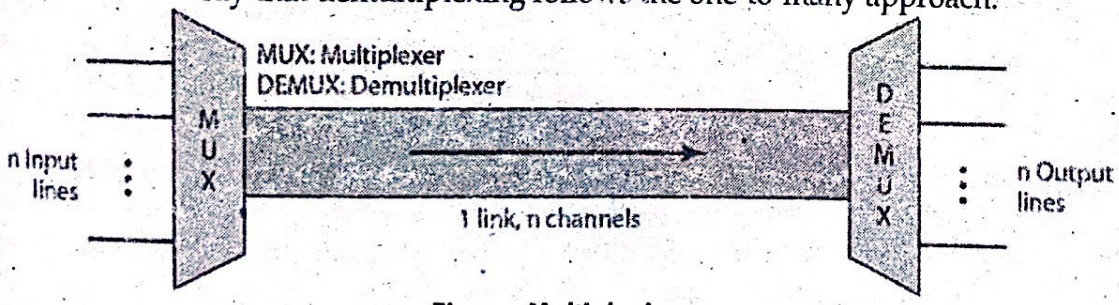


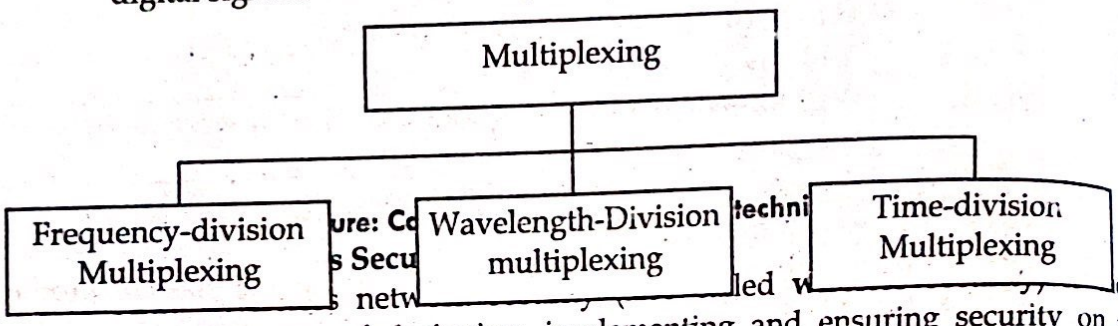
Figure: Multiplexing

Above figure depicts the multiplexing function in its simplest form. There are **n** inputs to a multiplexer. The multiplexer is connected by a single data link to a demultiplexer. The link is able to carry **n** separate channels of data. The multiplexer combines (multiplexes) data from the n input lines and transmits over a higher-capacity data link. The demultiplexer accepts the multiplexed data stream, separates (demultiplexes) the data according to channel, and delivers data to the appropriate output lines.

Advantages of Multiplexing:

- More than one signal can be sent over a single medium.
- The bandwidth of medium can be utilized effectively.

There are three basic multiplexing techniques: *frequency-division multiplexing, wavelength-division multiplexing, and time-division multiplexing.* The first two are techniques designed for analog signals, the third, for digital signals.



process of designing, implementing and ensuring security on a wireless computer network. It is a subset of network security that adds protection for a wireless computer network.

Wireless network security primarily protects a wireless network from unauthorized and malicious access attempts. Typically, wireless network security is delivered through wireless devices (usually a wireless router/switch) that encrypts and secures all wireless communication by default. Even if the wireless network security is compromised, the hacker is not able to view the content of the traffic/packet in transit. Moreover, wireless intrusion detection and prevention systems also enable protection of a wireless network by alerting the wireless network administrator in case of a security breach.

The wireless security protocols are:

i. **Wired Equivalent Policy (WEP):** WEP was developed for wireless networks and approved as a Wi-Fi security standard in September 1999. WEP was supposed to offer the same security level as wired networks, however there are a lot of well-known security issues in WEP, which is also easy to break and hard to configure. Despite all the work that has been done to improve the WEP system it still is a highly vulnerable solution. Systems that rely on this protocol should be either upgraded or replaced in case security upgrade is not possible. WEP was officially abandoned by the Wi-Fi Alliance in 2004.

ii. **Wi-Fi Protected Access (WPA):** This wireless security protocol precedes the WEP. Hence, it is designed to deal with the flaws that are found with the WEP protocol. Most modern WPA applications use a pre-shared key (PSK), most often referred to as WPA Personal, and the Temporal Key Integrity Protocol (TKIP) for encryption. WPA Enterprise uses an authentication server for keys and certificates generation.

iii. **Wi-Fi Protected Access 2 (WPA2):** The WPA2, a successor to WPA, comes with enhanced features and encryption abilities.

For instance, the WPA2 uses Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) instead of (TKIP). This replacement feature is known to be efficient in encrypting data. Hence, WPA2 is considered the best wireless security protocol. At this time the main vulnerability to a WPA2 system is when the attacker already has access to a secured Wi-Fi network and can gain access to certain keys to perform an attack on other devices on the network.

iv. **Wi-Fi Protected Access 3 (WPA3):** This one is a recent wireless protocol. It is enhanced in terms of encryption abilities and keeping hackers at bay from both private and public networks. WPA3 will protect against dictionary attacks by implementing a new key exchange protocol. WPA3's expanded encryption for public networks also keeps Wi-Fi users safe from a vulnerability they may not realize exists in the first place. In fact, if anything it might make Wi-Fi users feel too secure.

c. **ICMP**

Ans: Since IP does not have an inbuilt mechanism for sending error and control messages. It depends on Internet Control Message Protocol (ICMP) to provide an error control. ICMP is a protocol used primarily for sending error messages, performing diagnostics, and controlling the flow of data. An example of an error message and of flow control is an ICMP source-quench packet sent by a router to a source host to tell the host to slow down because the router is overloaded. Performing Diagnostics with ICMP: As stated earlier, the ICMP protocol is used for performing diagnostics. An example of using ICMP as a diagnostic tool is with the Ping utility. Ping stands for Packet Internet Groper.

ICMP messages are divided into two broad categories:

- Error-reporting messages
- Query messages.

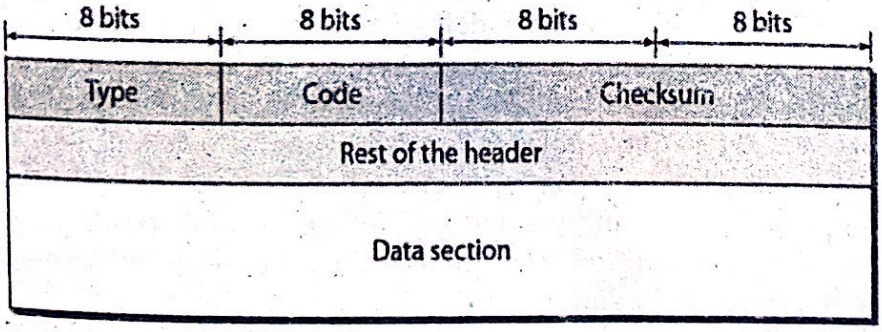


Figure: ICMP message.

The format of an ICMP message is shown above. The 8-bit type code identifies the types of message. Each ICMP message contains three fields that define its purpose and provide a checksum. They are TYPE, CODE, and CHECKSUM fields. The TYPE field identifies the ICMP message, the CODE field provides further information about the associated TYPE field, and the CHECKSUM provides a method for determining the integrity of the message.

Although over twenty ICMP messages have been defined, only a few are used. Table below lists key ICMP messages and the purpose of each.

Table: Examples of ICMP messages with the message number and purpose.

Number	Type	Purpose
0	Echo Reply	Used by the ping problem
3	Destination Unreachable	Datagram could not be delivered
5	Redirect	Host must change a route
8	Echo	Used by the ping program
11	Time Exceeded	TTL expired or fragments timed out
12	Parameter Problem	IP header is incorrect
30	Traceroute	Used by the traceroute program

As the above table illustrates, ICMP contains two message types: messages used to report errors and messages used to obtain information. For example, the *Time Exceeded* and *Destination Unreachable* messages each report an error when a datagram cannot be delivered successfully. A destination address is unreachable if no route exists to the address; a datagram times out if either the TTL count in the header expires or fragments of the datagram do not arrive before the reassembly timer expires. In contrast, the *Echo Request* and *Echo Reply* messages do not correspond to an error. Instead, they are used by the ping application to test connectivity — when it receives an *echo request* message, ICMP software on a host or router sends an *echo reply* that carries the same data as the request. Thus, a ping application sends a request to a remote host, waits for a reply, and either declares that the host is reachable, or after a suitable timeout, declares that the host is unreachable.

Group C

Attempt any TWO questions. [2×10=20]

9. Why do we need layered protocol architecture? What are the Functions of 7 layers of OSI reference model? [3+7]

Ans: A layered architecture facilitates development in complex environments by grouping specific related functions into separate well-defined layers with clear interfaces. This methodology reduces complexity by breaking the problem space into smaller and simpler components and standardizes interfaces facilitating multi-vendor development and modular component based engineering. Layered architectures in conjunction with open standards define a common vocabulary necessary for understanding and cooperation in multi-vendor environments and positively results in increased competition and innovation. The need of layered protocol architecture can be summarized as follow:

- To Separate Specific Functions in Each Layer.
- Each Layer Should Define a Unique Function.
- To make their Implementation Transparent to Other Components.
- Allows Independent Design and Testing of Each Component.
- Modularization Eases Maintenance and Updating of System.

Functions of 7 layers of OSI model are as follows:

a) Physical Layer:

- Physical characteristics of interfaces and media

- Representation of bits
- Data Rate or Transmission rate
- Synchronization of bits
- Line Configuration
- Physical Topology
- Transmission Mode

b) **Data Link Layer:**
- Enable Node to Node (hop to hop) communication
- Responsible for transmitting frames from one node to next.
- Framing
- Physical addressing
- Flow Control
- Error control
- Access Control [E.g. CSMA/CD]

c) **Network Layer:**
- Enables Host to Host Communication
- Responsible for Delivery of Packets
- Logical Addressing
- Routing

d) **Transport Layer:**
- Enables Process to Process Communication.
- Port Addressing
- Segmentation and Reassembly.
- Connection Control
- Flow Control
- Error Control

e) **Session Layer:**
- Control of Dialogues between Applications.
- Whose Turn is to Transmit?
- Dialogue Discipline => Half Duplex/ Full Duplex

f) **Presentation Layer:**
- Data Formats and Coding.
- Data Compression
- Encryption

g) **Application Layer:**
- Responsible for Providing Service to End Users.
- Mail Transfer Service.
- File Transfer Service.

10. **Highlight on the importance of routing algorithm. Explain Distance Vector Routing algorithm and compare it with link state routing. [3+3+4]**

Ans: In order to transfer the packets from source to the destination, the network layer must determine the best route through which packets can be transmitted. Whether the network layer provides datagram service or virtual circuit service, the main job of the network layer is to provide the best route. The routing protocol provides this job. The routing protocol is a routing algorithm that provides the best path from the source to the destination. The best path is the path that has the "least-cost path" from source to the destination. Routing is the process of forwarding the packets

from source to the destination but the best route to send the packets is determined by the routing algorithm. A routing algorithm is a set of step-by-step operations used to direct Internet traffic efficiently. When a packet of data leaves its source, there are many different paths it can take to its destination. The routing algorithm is used to determine mathematically the best path to take.

Distance Vector Routing Algorithm: It is a dynamic routing algorithm. A distance-vector routing protocol requires that a router inform its neighbors of topology changes periodically. The term distance vector refers to the fact that the protocol manipulates vectors (arrays) of distances to other nodes in the network. It makes use of Bellman Ford Algorithm for making routing tables. Problems of this algorithm are:

- Count to infinity problem which can be solved by splitting horizon
- Good news spread fast and bad news spread slowly.
- Persistent looping problem i.e. loop will be there forever.

Distance Vector Routing Algorithm Working:

Step 1) Initialization

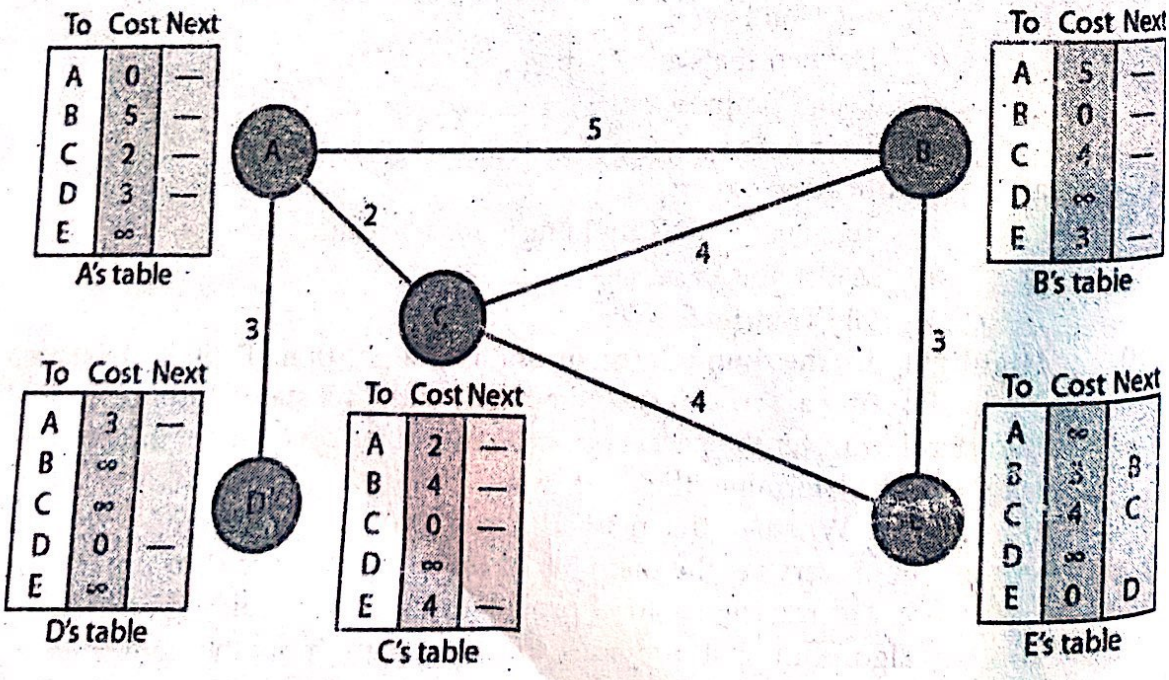
- At the beginning, each node knows the cost of itself and its immediate neighbor. [Node directly connected to it.]
- The distance of any entry that is not a neighbor is marked as infinite (unreachable).

Step 2) Sharing

- Idea is to share the information between neighbors.
- The node C does not know the distance about D, but C's neighbor node A and node B does.
- If node A and B share it routing table with C, node C can also know how to reach node D.

Step 3) Updating in distance vector routing

- When node C get routing tables from A and B, it will compare the distance of both nodes to go to D, whose ever distance is less, node C will update the entry in routing table according to it.

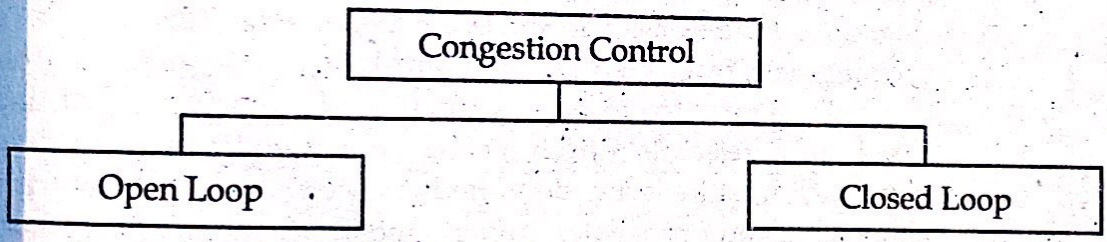


Comparison between Distance Vector Routing and Link State Routing

	Distance Vector Routing	Link State Routing
1.	Bandwidth required is less due to local sharing, small packets and no flooding.	Bandwidth required is more due to flooding and sending of large link state packets.
2.	Based on local knowledge since it updates table based on information from neighbors.	Based on global knowledge i.e. it has knowledge about entire network
3.	Makes use of Bellman Ford algorithm	Make use of Dijkstra's algorithm
4.	Traffic is less	Traffic is more
5.	Converges slowly i.e. good news spread fast and bad news spread slowly.	Converges faster
6.	Count to infinity problem	No count to infinity problem
7.	Persistent looping problem i.e. loop will there forever.	No persistent loops, only transient loops.
8.	Practical implementation is RIP and IGRP	Practical implementation is OSPF and ISIS

11. Explain various congestion control approaches. **[10]**

Ans: Congestion control refers to the techniques used to control or prevent congestion. Congestion control techniques can be broadly classified into two categories:



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 –

a) **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.

b) **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.

c) **Acknowledgment Policy:** Since acknowledgement is 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 receiv
should send acknowledgement for N packets rather than sendir
acknowledgement for a single packet. The receiver should send
acknowledgment only if it has to send a packet or a timer expires.

d) **Discarding Policy:** A good discarding policy adopted by t
routers is that the routers may prevent congestion and at the san
time partially discards the corrupted or less sensitive package ar
also able to maintain the quality of a message. In case of audio fi
transmission, routers can discard less sensitive packets to preve
congestion and also maintain the quality of the audio file.

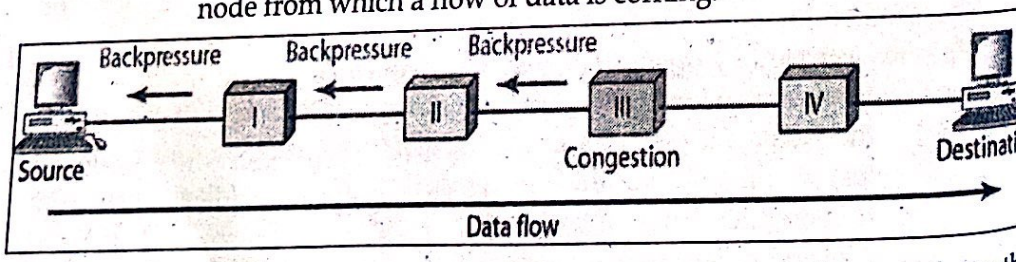
e) **Admission Policy:** In admission policy a mechanism should
used to prevent congestion. Switches in a flow should first che
the resource requirement of a network flow before transmitting
further. If there is a chance of congestion or there is congestion
the network, router should deny establishing a virtual netwo
connection to prevent further congestion.

All the above policies are adopted to prevent congestion before it happe
in the network.

Closed Loop Congestion Control

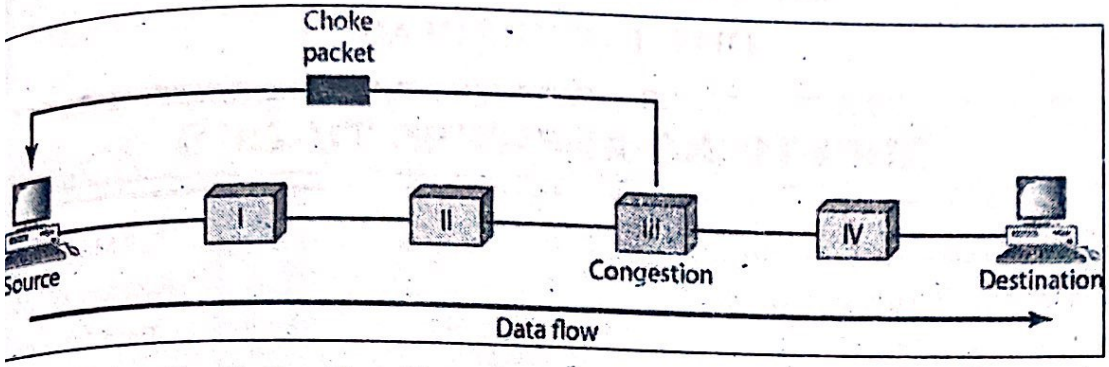
Closed loop congestion control technique is used to treat or allevia
congestion after it happens. Several techniques are used by differe
protocols; some of them are:

a) **Back-pressure:** The technique of backpressure refers to
congestion control mechanism in which a congested nod- sto
receiving data from the immediate upstream node or nodes. Th
may cause the upstream node or nodes to become congested, ar
they, in turn, reject data from their upstream nodes or nodes. Ar
so on. Backpressure is a node-to-node congestion control that sta
with a node and propagates, in the opposite direction of data flo
to the source. The backpressure technique can be applied only
virtual circuit networks, in which each node knows the upstrea
node from which a flow of data is corning.



b) **Choke Packet:** A choke packet is a packet sent by a node to t
source to inform it of congestion. Note the difference between t
backpressure and choke packet methods. In backpressure, t
warning is from one node to its upstream node, although t
warning may eventually reach the source station. In the chok
packet method, the warning is from the router, which ha
encountered congestion, to the source station directly. Th
intermediate nodes through which the packet has traveled are no
warned. We have seen an example of this type of control in ICMP
When a router in the Internet is overwhelmed datagrams, it may
discard some of them; but it informs the source. Host, using

source quench ICMP message. The warning message goes directly to the source station; the intermediate routers, and does not take any action.



c) **Implicit Signaling:** In implicit signaling, there is no communication between the congested node or nodes and the source. The source guesses that there is congestion somewhere in the network from other symptoms. For example, when a source sends several packets and there is no acknowledgment for a while, one assumption is that the network is congested. The delay in receiving an acknowledgment is interpreted as congestion in the network; the source should slow down.

d) **Explicit Signaling:** The node that experiences congestion can explicitly send a signal to the source or destination. The explicit signaling method, however, is different from the choke packet method. In the choke packet method, a separate packet is used for this purpose; in the explicit signaling method, the signal is included in the packets that carry data. Explicit signaling, as we will see in Frame Relay congestion control, can occur in either the forward or the backward direction.

- **Backward Signaling**: A bit can be set in a packet moving in the direction opposite to the congestion. This bit can warn the source that there is congestion and that it needs to slow down to avoid the discarding of packets.
- **Forward Signaling**: A bit can be set in a packet moving in the direction of the congestion. This bit can warn the destination that there is congestion. The receiver in this case can use policies, such as slowing down the acknowledgments, to alleviate the congestion.

TRIBHUVAN UNIVERSITY

Faculty of Humanities & Social Sciences

OFFICE OF THE DEAN

QUESTIONS-ANSWERS TU-2020

Bachelor in Computer Applications — Full Marks: 6
Course Title: Computer Networking — Pass Marks: 2
Code No: CACS303 — Time: 3 hour
Semester: V

Candidates are required to give their answer in their own words as far a practicable.

Group B

Attempt any six questions. **[6×5=30]**

2. Define protocols. Explain WWW and HTTP protocol. **[1+2+2]**

Ans: In information technology, a protocol is the special set of rules that end points in a telecommunication connection use when they communicate. In brief **a protocol is defined as a set of rules that governs communication.** Protocols exist at several levels in a telecommunication connection. For example, there are protocols for the data interchange at the hardware device level and protocols for data interchange at the application program level. Some examples of network protocols are hyper-text transfer protocol (HTTP), file transfer protocol (FTP), transmission control protocol/ internet protocol (TCP/IP), secure sockets layer etc.

WWW

The World Wide Web (WWW), or the Web, is a repository of information spread all over the world and linked together. The WWW has a unique combination of flexibility, portability, and user-friendly features that distinguish it from other services provided by the Internet. The WWW project was initiated by CERN (European Laboratory for Particle Physics) to create a system to handle distributed resources necessary for scientific research.

Today it is a distributed client-server service, in which a client using a browser can access a service using a server. However, the service provided is distributed over many locations called websites, as shown in figure 6.12. Each website holds one or more documents, referred to as web pages. Each web page, however can contain some links to other web pages in the same or other websites. The pages can be retrieved and viewed by using **browsers.**

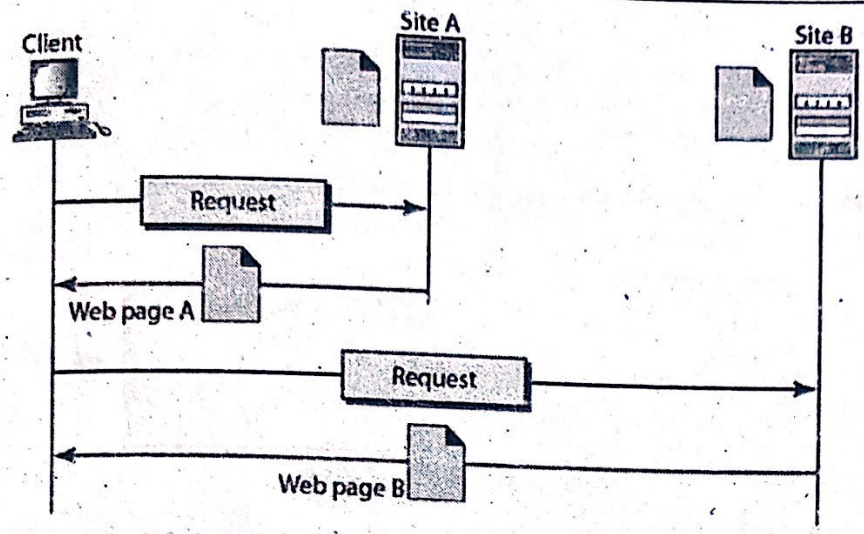


Figure: Architecture of WWW

Let us go through the scenario shown in above figure. The client needs to see some information that it knows belongs to site A. It sends a request through its browser, a program that is designed to fetch Web documents. The request, among other information, includes the address of the site and the Web page, called the URL. The server at site A finds the document and sends it to the client. When the user views the document, s/he finds some references to other documents, including a Web page at site B. The reference has the URL for the new site. The user is also interested in seeing this document. The client sends another request to the new site, and the new page is retrieved.

The above example shows the idea of **hypertext** and **hypermedia**. Hypertext means creating documents that refer to other documents. In a hypertext document, a part of text can be defined as a link to another document. When a hypertext is viewed with a browser, the link can be clicked to retrieve the other document. Hypermedia is a term applied to document that contains links to other textual document or documents containing graphics, video, or audio.

HTTP

The Hypertext Transfer Protocol (HTTP) is a protocol used mainly to access data on the World Wide Web. The protocol transfers data in the form of plain text, hypertext, audio, video, and so on. It is called the Hypertext Transfer Protocol because its efficiency allows its use in a hypertext environment where there are rapid jumps from one document to another.

The HTTP controls the transactions between a web client and a web server. The HTTP protocol transparently makes use of DNS and other Internet protocols to form connections between the web client and the web server, so the user is aware of only the web site's domain name and the name of the document itself. HTTP uses the services of TCP on well-known port 80.

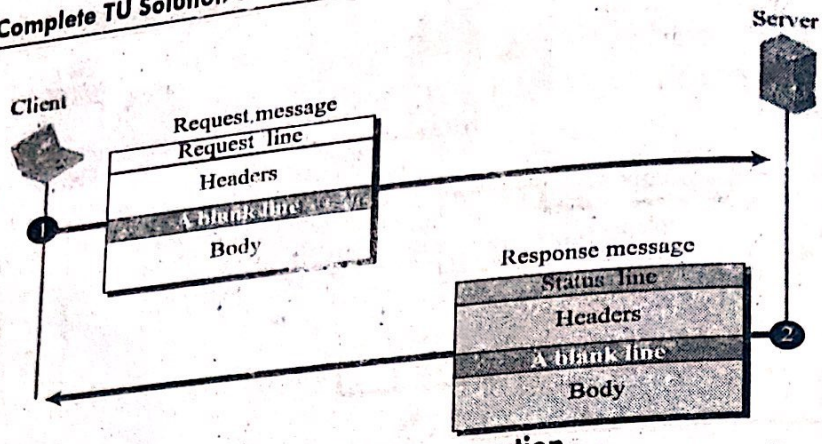


Figure: HTTP transaction

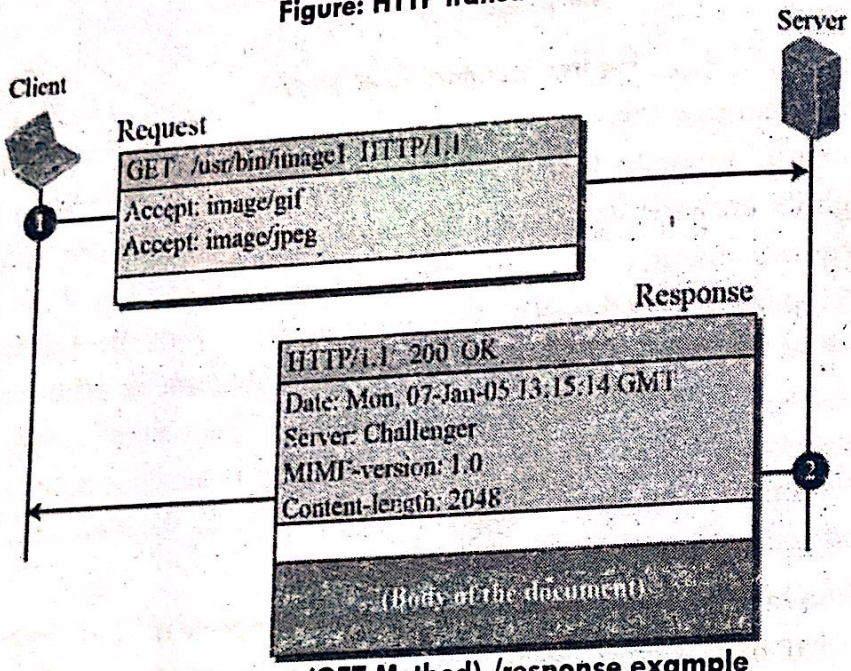


Figure: Request (GET Method) /response example

The above example retrieves a document. We use the GET method to retrieve an image with the path /usr/bin/image1. The request line shows the method (GET), the URL, and the HTTP version (1.1). The header has two lines that show that the client can accept images in the GIF or JPEG format. The request does not have a body. The response message contains the status line and four lines of header. The header lines define the date, server, MIME version, and length of the document. The body of the document follows the header.

3. Define transmission impairment. Explain the causes of impairments. [1+4]

Ans: When signal travels through the medium, which are not perfect? The imperfection cause signal impairment. This means that the signal at the beginning of the medium is not the same as the signal at the end of the medium. Three causes of impairment are attenuation, distortion and noise.

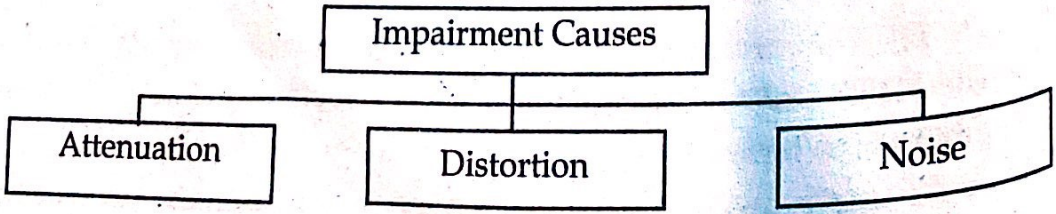


Figure: Causes of impairment

Attenuation

Attenuation means a loss of energy. For the receiver to interpret the data accurately, the signal must be sufficiently strong. When the signal passes through the medium, it tends to get weaker. As it covers distance, it loses strength. To compensate for this loss, amplifiers are used to amplify the signal. Figure below shows the effect of attenuation and amplification.

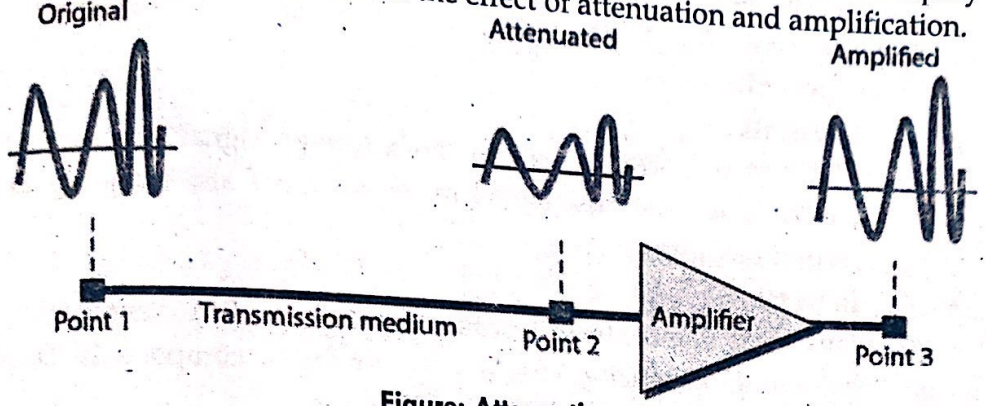


Figure: Attenuation

Distortion

Distortion means that the signal changes its form or shape. Signals are sent over media with pre-defined speed and frequency. If the signal speed and frequency do not match, there are possibilities that signal reaches destination in arbitrary fashion. In digital media, this is very critical that some bits reach earlier than the previously sent ones. In other words, signal components at the receiver have phase different from what they had at the sender. The shape of the composite signal is therefore not the same. Figure below shows the effect of distortion on a composite signal.

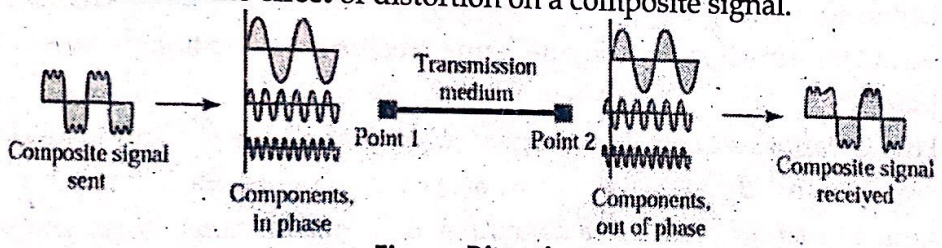


Figure: Distortion

Noise

Random disturbance or fluctuation in analog or digital signal is said to be Noise in signal, which may distort the actual information being carried. Several types of noise, such as thermal noise, intermodulation, crosstalk and impulse noise, may corrupt the signal.

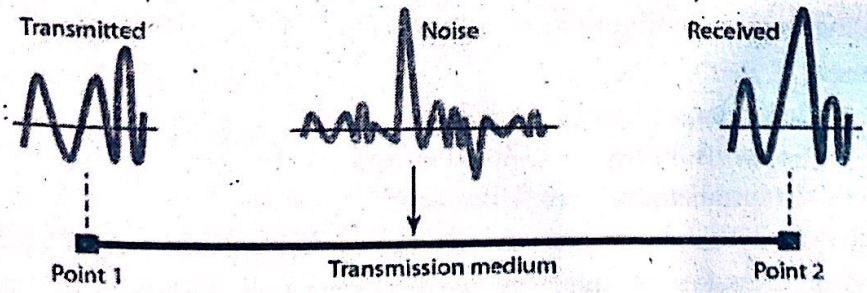


Figure: Noise

- **Thermal Noise**
  Heat agitates the electronic conductors of a medium which may introduce noise in the media. Up to a certain level, thermal noise is unavoidable.

- **Intermodulation**
  When multiple frequencies share a medium, their interference can cause noise in the medium. Intermodulation noise occurs if two different frequencies are sharing a medium and one of them has excessive strength or the component itself is not functioning properly, then the resultant frequency may not be delivered as expected.
- **Crosstalk**
  This sort of noise happens when a foreign signal enters into the media. This is because signal in one medium affects the signal of second medium.
- **Impulse**
  This noise is introduced because of irregular disturbances such as lightening, electricity, short-circuit, or faulty components. Digital data is mostly affected by this sort of noise.

3. Define HDLC. Explain the HDLC frame formats. [1+4]

Ans: High-level Data Link Control (HDLC) is a bit-oriented protocol for communication over point-to-point and multipoint links. HDLC is a synchronous Data Link layer bit-oriented protocol developed by the International Organization for Standardization (ISO). The current standard for HDLC is ISO 13239. HDLC was developed from the Synchronous Data Link Control (SDLC) standard proposed in the 1970s. HDLC provides both connection-oriented and connectionless service. HDLC uses synchronous serial transmission to provide error free communication between two points.

HDLC defines a Layer 2 framing structure that allows for flow control and error control through the use of acknowledgments. Each frame has the same format, whether it is a data frame or a control frame. When you want to transmit frames over synchronous or asynchronous links, you must remember that those links have no mechanism to mark the beginnings or ends of frames. HDLC uses a frame delimiter, or flag, to mark the beginning and the end of each frame.

To provide the flexibility necessary to support all the options possible in the modes and configurations just described, HDLC defines three types of frames:

1. Information frames (I-frames),
2. Supervisory frames (S-frames), and
3. Unnumbered frames (U-frames).

Each type of frame serves as an envelope for the transmission of a different type of message. **I-frames** are used to data-link user data and control information relating to user data (piggybacking). **S-frames** are used only to transport control information. **U-frames** are reserved for system management. Information carried by U-frames is intended for managing the link itself.

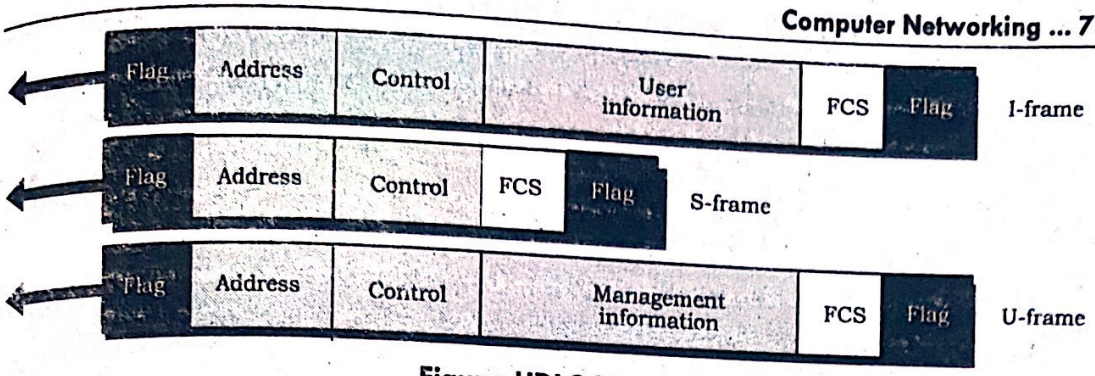


Figure: HDLC frames

Let us now discuss the fields and their use in different frame types.

- **Flag field.** This field contains synchronization pattern 01111110, which identifies both the beginning and the end of a frame.
- **Address field.** This field contains the address of the secondary station. If a primary station created the frame, it contains a to address. If a secondary station creates the frame, it contains a from address. The address field can be one byte or several bytes long, depending on the needs of the network.
- **Control field.** The control field is one or two bytes used for flow and error control. The interpretations of bits are discussed later.

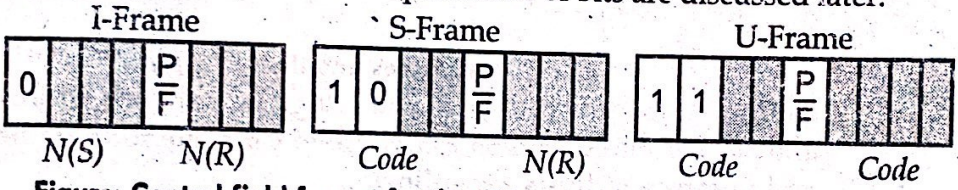


Figure: Control field format for the different frame types

- **Information field.** The information field contains the user's data from the network layer or management information. Its length can vary from one network to another.
- **FCS field.** The frame check sequence (FCS) is the HDLC error detection field. It can contain either a 2- or 4-byte CRC.

4. **Define IP Address. Specify IPv4 address classes with their address ranges.** **[1+4]**

Ans: An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.

IPv4 addresses are 32-bit numbers that are typically displayed in dotted decimal notation. A 32-bit address contains two primary parts: the network prefix and the host number. All hosts within a single network share the same network address. Each host also has an address that uniquely identifies it.

IPv4 classfull addresses

To provide flexibility in the number of addresses distributed to networks of different sizes, 4-octet (32-bit) IP addresses are divided into five different categories or classes: **Class A, Class B, Class C, Class D** and **Class E**. Each address class specifies a different number of bits for its network prefix and host number as shown in following diagram:

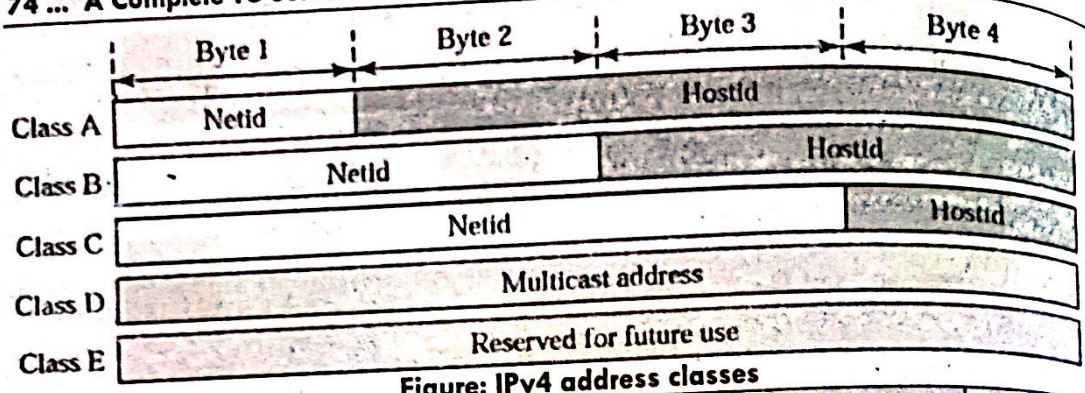


Figure: IPv4 address classes

Class	Leading bit	First Octet IP Range		IP Range		Remark
		Binary	Decimal Dotted	Start	End	
A	0	00000000 - 01111111	0 – 127	0.0.0.0	127.255.255.255	0 and 127 are reserved.
B	10	10000000 – 10111111	128 – 191	128.0.0.0	191.255.255.255	
C	110	11000000 - 11011111	192 – 223	192.0.0.0	223.255.255.255	
D	1110	11100000 – 11101111	224 – 239	224.0.0.0	239.255.255.255	Multicast address
E	1111	11110000 – 11111111	240 - 255	240.0.0.0	255.255.255.255	Reserved for future use

Figure: IPv4 classes and their IP ranges

5. Define Subnetting. Suppose you are given network address: 192.168.10.0 and subnet mask: 255.255.255.240 then calculate total number of subnets and numbers of hosts per subnet. [1+2+2]

Ans: Subnetting is the strategy used to partition a single physical network into more than one smaller logical sub-networks (subnets). Subnets are designed by accepting bits from the IP address's host part and using these bits to assign a number of smaller sub-networks inside the original network. Subnetting allows an organization to add sub-networks without the need to acquire a new network number via the Internet service provider (ISP). Subnetting helps to reduce the network traffic and conceals network complexity. Subnetting is essential when a single network number has to be allocated over numerous segments of a local area network (LAN).

IP address: 192.168.10.0

New Subnet Mask: 255.255.255.240 = 11111111 11111111 11111111 11110000

Total Subnets = $2^4 = 16$

Total hosts = $2^4 = 16$

Usable hosts = 16 -2 = 14

Valid Subnets (4th octet) = 256 – 240= 16

Starting Address (Network ID)	Usable Host IP Range		Ending Address (Broadcast ID)
	First host	Last host	
192.168.10.0	192.168.10.1	192.168.10.14	192.168.10.15
192.168.10.16	192.168.10.17	192.168.10.30	192.168.10.31
192.168.10.32	192.168.10.33	192.168.10.46	192.168.10.47
192.168.10.48	192.168.10.49	192.168.10.62	192.168.10.63
192.168.10.64	192.168.10.65	192.168.10.78	192.168.10.79
192.168.10.80	192.168.10.81	192.168.10.94	192.168.10.95
192.168.10.96	192.168.10.97	192.168.10.110	192.168.10.111

192.168.10.112	192.168.10.113	192.168.10.126	192.168.10.127
192.168.10.128	192.168.10.129	192.168.10.142	192.168.10.143
192.168.10.144	192.168.10.145	192.168.10.158	192.168.10.159
192.168.10.160	192.168.10.161	192.168.10.174	192.168.10.175
192.168.10.176	192.168.10.177	192.168.10.190	192.168.10.191
192.168.10.192	192.168.10.193	192.168.10.206	192.168.10.207
192.168.10.208	192.168.10.209	192.168.10.222	192.168.10.223
192.168.10.224	192.168.10.225	192.168.10.238	192.168.10.239
192.168.10.240	192.168.10.241	192.168.10.254	192.168.10.255

6. Draw a user Datagram format. Explain UDP operations. **[2+3]**

Ans: A UDP datagram header contains four fields of two bytes each as shown in figure below.

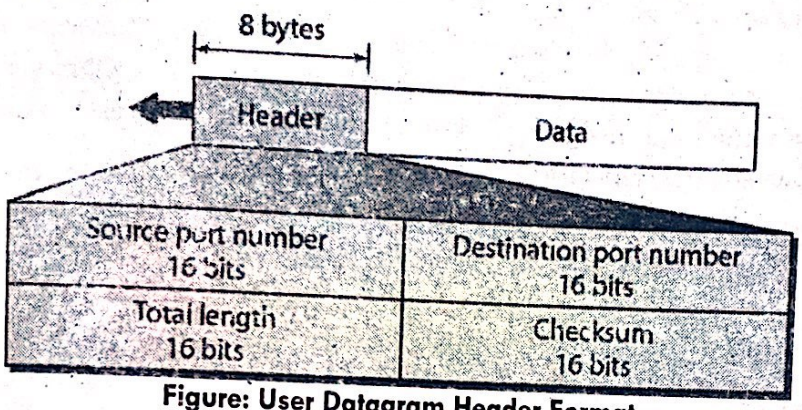


Figure: User Datagram Header Format

- **Source Port:** Source Port is 2 Byte long fields used to identify port number of sources.
- **Destination Port:** It is 2 Byte long fields, used to identify the port of destined packet.
- **Length:** Length is the length of UDP including header and the data. It is 16-bits field.
- **Checksum:** Checksum is 2 Bytes long field. It is the 16-bit one's complement of the one's complement sum of the UDP header, pseudo header of information from the IP header and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets.

UDP operations

UDP (User Datagram Protocol) is an alternative communications protocol to Transmission Control Protocol (TCP) used primarily for establishing low-latency and loss-tolerating connections between applications on the internet.

UDP uses a simple transmission model but does not employ handshaking dialogs for reliability, ordering and data integrity. The protocol assumes that error-checking and correction is not required, thus avoiding processing at the network interface level. UDP is widely used in video conferencing and real-time computer games. The protocol permits individual packets to be dropped and UDP packets to be received in a different order than that in which they were sent, allowing for better performance. UDP network traffic is organized in the form of datagrams, which comprise one message units. The first eight bytes of a datagram contain header information, while the remaining bytes contain message data.

As it is a connectionless protocol, it is not at all reliable protocols when compared to the TCP. It will never offer any sequencing of the data. Hence, the data will arrive at the destination device in the various orders from which it is sent. This will occur in the large networks like the internet, where datagrams take various paths to a destination and also experience the delay in the different router. The UDP is generally the IP with the transport layer port addressing. Sometimes this UDP is also known as the wrapper protocol.

7. **Write short notes on (Any Two):** [2.5+2.5]

(a) DNS

Ans: DNS is a global system for translating IP addresses to human-readable domain names. When a user tries to access a web address like "example.com", their web browser or application performs a DNS Query against a DNS server, supplying the hostname. The DNS server takes the hostname and resolves it into a numeric IP address, which then web browser can connect to.

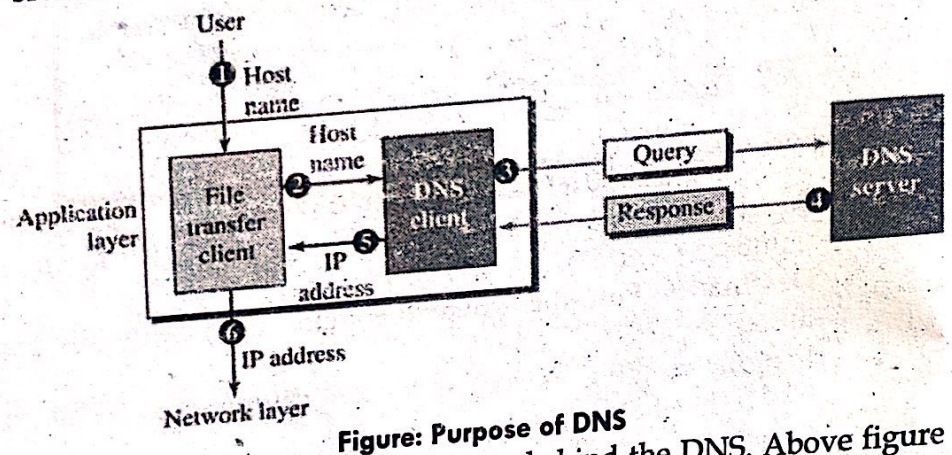


Figure: Purpose of DNS

Let's discuss the concepts and ideas behind the DNS. Above figure shows how TCP/IP uses a DNS client and a DNS server to map a name to an address. A user wants to use a file transfer client to access the corresponding file transfer server running on a remote host. The user knows only the file transfer server name. Such as example.com. However, the TCP/IP suite needs the IP address of the file transfer server to make the connection.

The following six steps map the host name to an IP address:

1. The user passes the host name to the file transfer client.
2. The file transfer client passes the host name to the DNS client.
3. Each computer, after being booted, knows the address of one DNS server. The DNS client sends a message to a DNS server with a query that gives the file transfer server name using the known IP address of the DNS server.
4. The DNS server responds with the IP address of the desired file transfer server.
5. The DNS server passes the IP address to the file transfer client.
6. The file transfer client now uses the received IP address to access the file transfer server.

Note that the purpose of accessing the Internet is to make a connection between the file transfer client and server, but before this can happen,

another connection needs to be made between the DNS client and DNS server. In other words, we need at least two connections in this case. The first is for mapping the name to an IP address; the second is for transferring files.

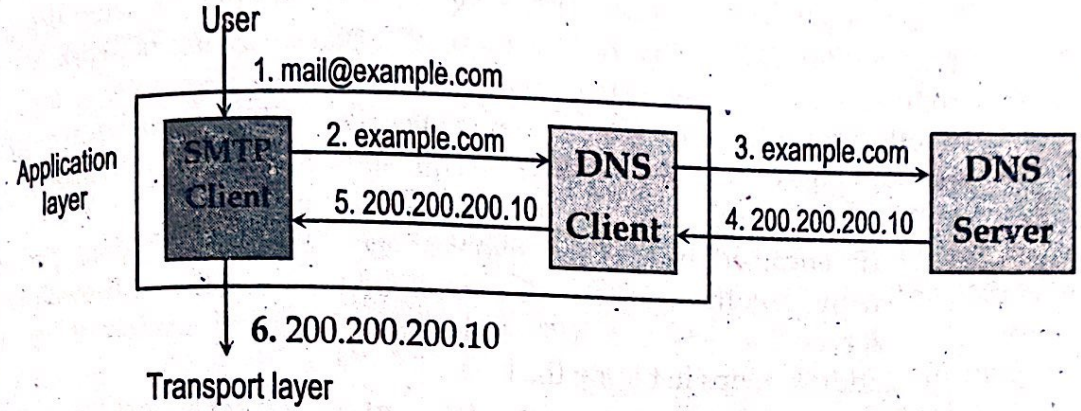


Figure: Example of using DNS service

Above figure shows an example of how DNS client/server program can support an e-mail program to find the IP address of an e-mail recipient. A user of an e-mail program may know the e-mail address of the recipient; however, the IP protocol needs the IP address. The DNS client program sends a request to a DNS server to map the e-mail address to the corresponding IP address.

(b) Public Key Cryptography

Ans: Public Key Cryptography use one key to encrypt data and a different key to decrypt data. One key is public and the other is private. In a public-key encryption system, any person can encrypt a message using the public key of the receiver, and the receiver is the only one that can decrypt it using his private key. Parties exchange secure messages without needing a pre-shared key, as shown in figure below. Asymmetric algorithms are more complex. These algorithms are resource intensive and slower to execute.

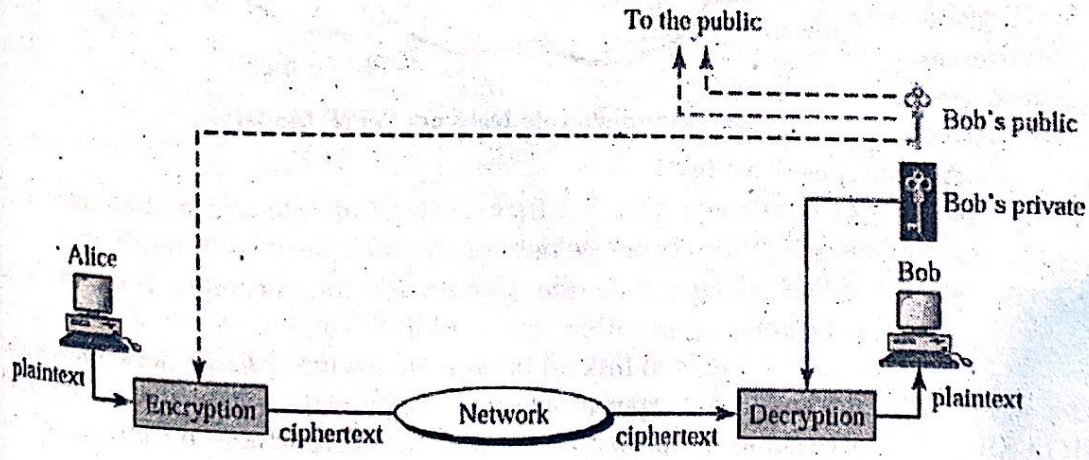


Figure: Public-key cryptography

We have the same situation as the symmetric-key algorithm, with a few exceptions. First, there are two keys instead of one: **public key** and **private key**. To send a secured message to Bob, Alice first encrypts the message using Bob's public key. To decrypt the message, bob uses his own Private Key. Some algorithm based on public-key cryptography are RSA, DSA, Diffie-Hellman etc.

(c) VPN

Ans: A Virtual Private Network (VPN) provides a secure connection between sender and a receiver over a public non-secure network such as th Internet. A secure connection is generally associated with privat networks. (*A private network is a network that is owned, or at least controlled b leased lines, by an organization.*) A VPN can transform the characteristics of public non-secure network into those of a private secure network. VPN reduce remote access costs by using public network resources. Compare to other solutions, including private networks, a VPN is inexpensive. VP has two types: *Remote Access VPN and Site-to-site VPN.*

VPN technology must do the following activities:

- **IP encapsulation:** This involves enclosing TCP/IP data packe within another packet with an IP address of either a firewall or server that acts as a VPN end-point. This encapsulation of host address helps in hiding the host.
- **Encryption:** It is done on the data part of the packet. Just like in SS the encryption can be done either in transport mode which encryp its data at the time of generation or tunnel mode which encrypts an decrypts data during transmission encrypting both data and header
- **Authentication:** It involves creating an encryption domain whic includes authenticating computers and data packets by user f public encryption.

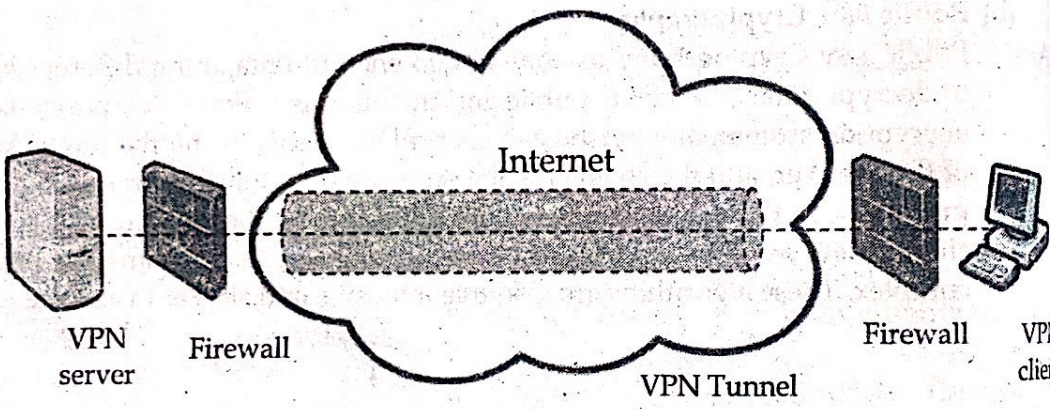


Figure: Virtual Private Network (VPN) Model

Advantages of VPNs

- VPNs are inexpensive; they provide remote and mobile user wi access to the corporate network at the price of a local call.
- VPNs also provide the framework for corporate **intranets** an **extranets**. Corporations can exploit the global nature of the Intern and use VPNs to link all branch offices into private networks calle intranets. A corporation can make certain sections of its intran accessible to its vendors and strategic partners by means of th extranet.
- VPN tunnels permit non-routable protocols to be delivered specific LAN segments in the corporate intranet. In this way, VPN enable legacy applications to use the intranet.
- VPNs have also contributed significantly to the increased use private IP addresses. Since applications are tunneled rather tha routed across the WAN, companies can assign their own addresse as long as these addresses are not advertised to the outside world.

Group C

Attempt any TWO questions. [2×10=20]

8. Critically analyze the OSI reference model. [10]

Ans: Neither the OSI model and its protocols nor the TCP/IP model and its protocols are perfect. The criticism of the OSI model and its protocols can be summarized as:

(a) Bad timing

The competing TCP/IP protocols were already in widespread use by research universities by the time the OSI protocols appeared. While the billion-dollar wave of investment had not yet hit, the academic market was large enough that many vendors had begun cautiously offering TCP/IP products. When OSI came around, they did not want to support a second protocol stack until they were forced to, so there were no initial offerings. With every company waiting for every other company to go first, no company went first and OSI never happened.

(b) Bad Technology

The second reason that OSI never caught on is that both the model and the protocols are flawed. The choice of seven layers was more political than technical, and two of the layers (session and presentation) are nearly empty, whereas two other ones (data link and network) are overfull. The OSI model, along with its associated service definitions and protocols, is extraordinarily complex. They are also difficult to implement and inefficient in operation. In addition to being incomprehensible, another problem with OSI is that some functions, such as addressing, flow control, and error control, reappear again and again in each layer.

(c) Bad Implementations

Given the enormous complexity of the model and the protocols, it will come as no surprise that the initial implementations were huge, unwieldy, and slow. It did not take long for people to associate "OSI" with "poor quality". Although the products improved in the course of time, the image stuck. In contrast, one of the first implementations of TCP/IP was part of Berkeley UNIX and was quite good. People began using it quickly, which led to a large user community, which led to improvements, which led to an even larger community. Here the spiral was upward instead of downward.

(d) Bad Politics

On account of the initial implementation, many people, especially in academia, thought of TCP/IP as part of UNIX, and UNIX in the 1980s in academia was not unlike parenthood and apple pie. OSI, on the other hand, was widely thought to be the creature of the European telecommunication ministries. The very idea of a bunch of government bureaucrats trying to shove a technically inferior standard down the throats of the poor researchers and programmers down in the trenches actually developing computer networks did not aid OSI's cause.

The TCP/IP model and protocols have their problems too. **First,** the model does not clearly distinguish the concepts of services, interfaces, and protocols. Good software engineering practice requires differentiating between the specification and the implementation, something that OSI does very carefully, but TCP/IP does not. Consequently, the TCP/IP model is not much of a guide for designing new networks using new technologies.

Second, the TCP/IP model is not at all general and is poorly suited to describing any protocol stack other than TCP/IP. Trying to use the TCP/IP model to describe Bluetooth, for example, is completely impossible.

Third, the link layer is not really a layer at all in the normal sense of the term as used in the context of layered protocols. It is an interface (between the network and data link layers). The distinction between an interface and layer is crucial and one should not be sloppy about it.

Fourth, the TCP/IP model does not distinguish between the physical and data link layers. These are completely different. The physical layer has to do with the transmission characteristics of copper wire, fiber optics, and wireless communication. The data link layer's job is to delimit the start and end of frames and get them from one side to the other with the desired degree of reliability. A proper model should include both as separate layers. The TCP/IP model does not do this.

Finally, although the IP and TCP protocols were carefully thought out and well implemented, many of the other protocols were ad hoc, generally produced by a couple of graduate students hacking away until they got tired. The protocol implementations were then distributed free, which resulted in their becoming widely used, deeply entrenched, and thus hard to replace. Some of them are a bit of an embarrassment now.

9. **Explain the random-access protocols under the multiple access taxonomy.** [10]

Ans:

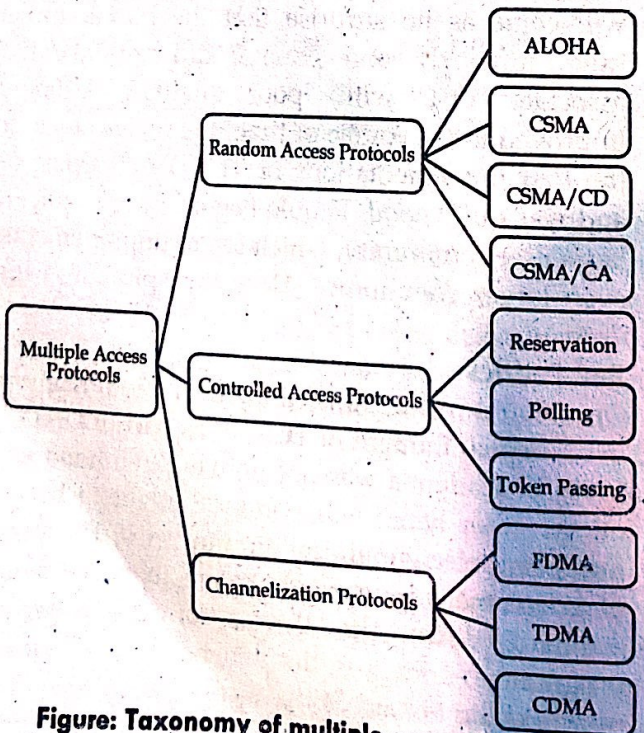


Figure: Taxonomy of multiple-access Protocols

Random Access Protocol

In random access or contention methods, no station is superior to another station and none is assigned the control over another. No station permits, or does not permit, another station to send. At each instance, a station that has data to send uses a procedure defined by the protocol to make a decision on whether or not to send. Any station can send data depending on medium's state (idle or busy). It has two features:

- There is no fixed time for sending data
- There is no fixed sequence of stations sending data

The random-access protocols are further subdivided as:

(a) **ALOHA**

The Aloha protocol was designed as part of a project at the University of Hawaii. It provided data transmission between computers on several of the Hawaiian Islands involving packet radio networks. Aloha is a multiple access protocol at the data link layer and proposes how multiple terminals access the medium without interference or collision. There are two different versions of ALOHA:

- **Pure ALOHA:**

Pure Aloha is an un-slotted, decentralized, and simple to implement protocol. In pure ALOHA, the stations simply transmit frames whenever they want data to send. It does not check whether channel is busy or not before transmitting. In case, two or more stations transmit simultaneously, collision occurs and frames are destroyed. Whenever any station transmits a frame, it expects the acknowledgement from the receiver. If it is not received within specified time, the station assumes that the frame or acknowledgement has been destroyed. Then, the station waits for a random amount of time and sends the frame again. This randomness helps in avoiding more collisions. This scheme works well in small networks where the load is not much. But in largely loaded networks, this scheme fails poorly. This led to the development of Slotted Aloha.

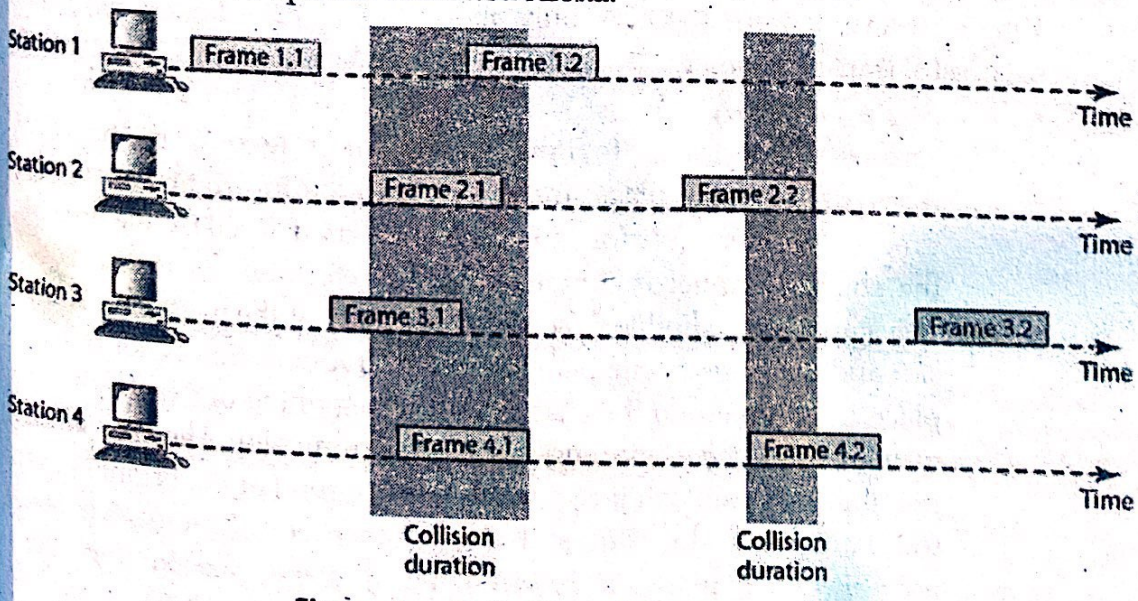


Figure: Frames in Pure ALOHA Network

To assure pure aloha: Its throughput and rate of transmission of frame to be predicted. For that to make some assumption:

i) All the frames should be the same length.

ii) Stations cannot generate frame while transmitting or trying to transmit frame.

iii) The population of stations attempts to transmit (both new frames and old frames that collided) according to a Poisson distribution.

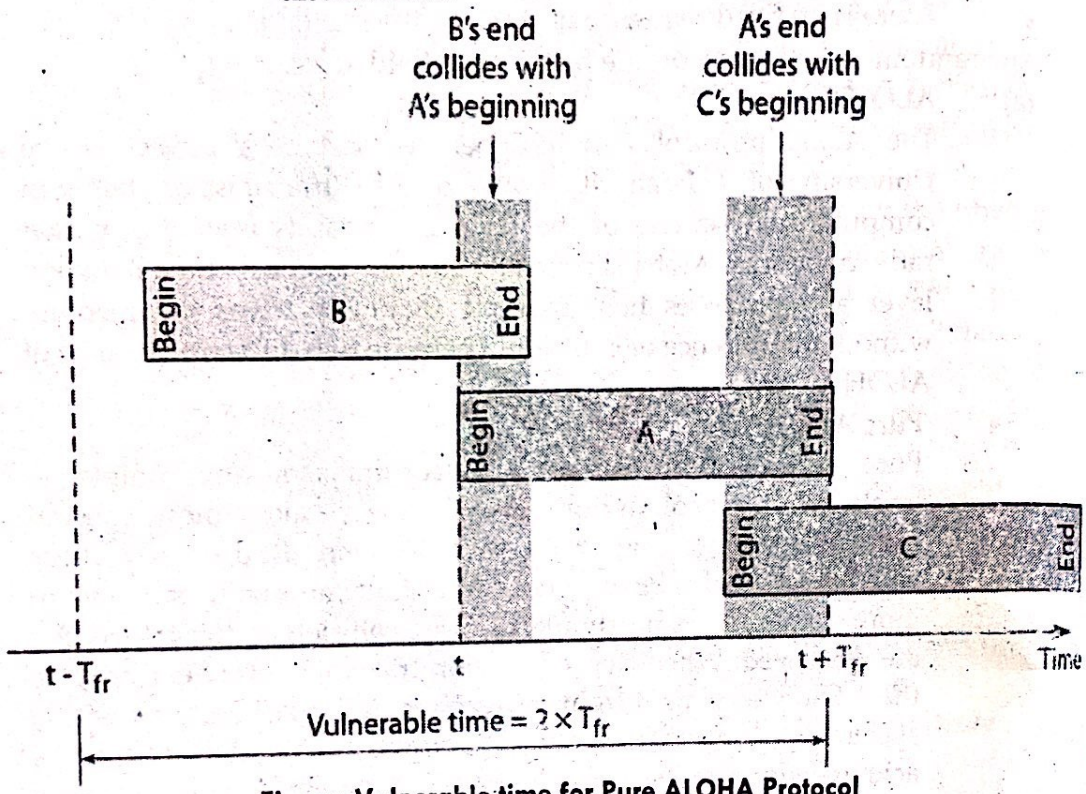


Figure: Vulnerable time for Pure ALOHA Protocol

Pure ALOHA vulnerable Time = 2 × Frame Transmission Time (T_{fr})

Throughput for pure ALOHA (Spure) = $G \times e^{-2G}$

Where G is number of stations wants to transmit in T_{fr} slot.

Maximum throughput $(Spure)_{max}$ = 0.184 for G=0.5

Which means, in Pure ALOHA, only about 18.4% of the time is used for successful transmissions.

- **Slotted ALOHA**

  This is quite similar to Pure Aloha, differing only in the way transmissions take place. Instead of transmitting right at demand time, the sender waits for some time. In slotted ALOHA, the time of the shared channel is divided into discrete intervals called Slots. The stations are eligible to send a frame only at the beginning of the slot and only one frame per slot is sent. If any station is not able to place the frame onto the channel at the beginning of the slot, it has to wait until the beginning of the next time slot. There is still a possibility of collision if two stations try to send at the beginning of the same time slot. But still the number of collisions that can possibly take place is reduced by a large margin and the performance becomes much well compared to Pure Aloha.

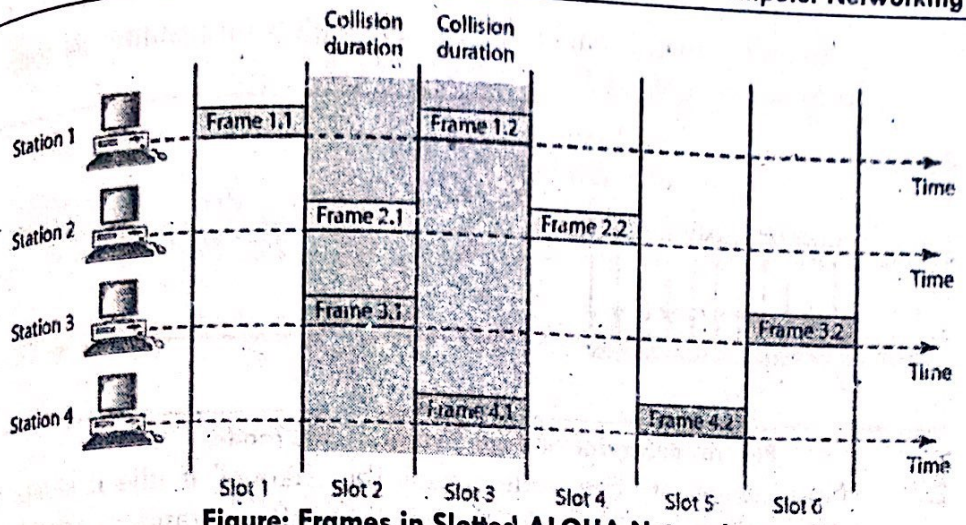


Figure: Frames in Slotted ALOHA Network

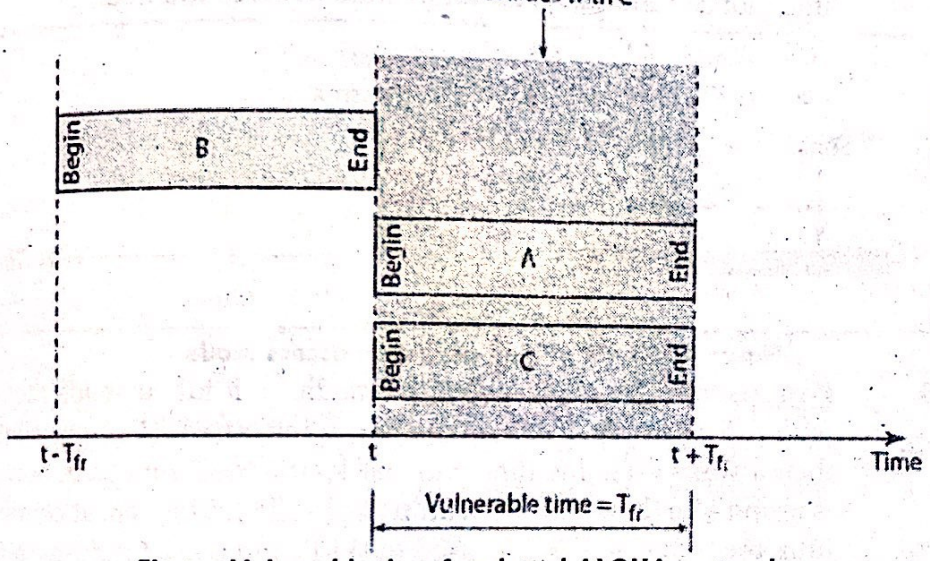


Figure: Vulnerable time for slotted ALOHA protocol

Slotted ALOHA vulnerable Time = Frame Transmission Time (T_0)

Throughput for Slotted ALOHA (Sslotted) = $G \times e^{-2G}$

Where G is number of stations wants to transmit in T_{fr} slot.

Maximum throughput $(Sslotted)_{max}$ = 0.368 for G=1

Which means, in slotted ALOHA, about 36.8% of the time is used for successful transmissions.

(b) **Carrier Sense Multiple Access (CSMA)**

Carrier Sense Multiple Access (CSMA) ensures fewer collisions as the station is required to first sense the medium (for idle or busy) before transmitting data. If it is idle then it sends data, otherwise it waits till the channel becomes idle. However, there is still chance of collision in CSMA due to propagation delay. For example, if station A wants to send data, it will first sense the medium. If it finds the channel idle, it will start sending data. However, by the time the first bit of data is transmitted (delayed due to propagation delay) from station A, if station B requests to send data and senses the medium it will also find it idle and will also send data. This will result in collision of data from station A and B.

CSMA access modes:

1. 1-persistent: The node senses the channel, if idle it sends the data, otherwise it continuously keeps on checking the medium for being

idle and transmits unconditionally (with 1 probability) as soon as the channel gets idle.

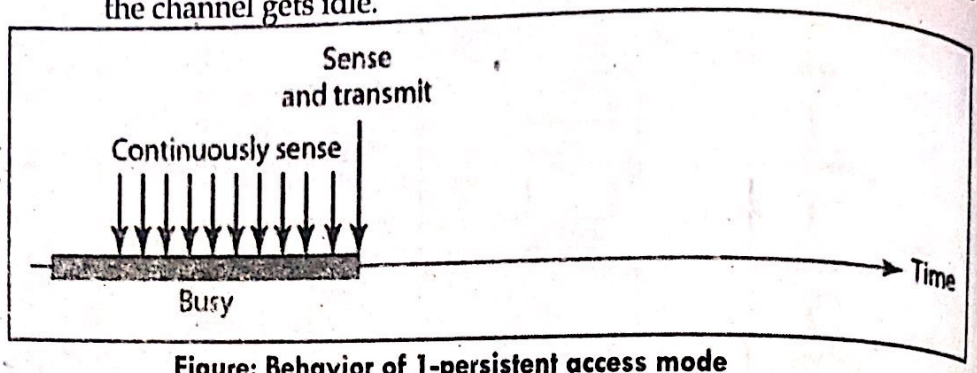


Figure: Behavior of 1-persistent access mode

2. Non-Persistent: The node senses the channel, if idle it sends the data, otherwise it checks the medium after a random amount of time (not continuously) and transmits when found idle.

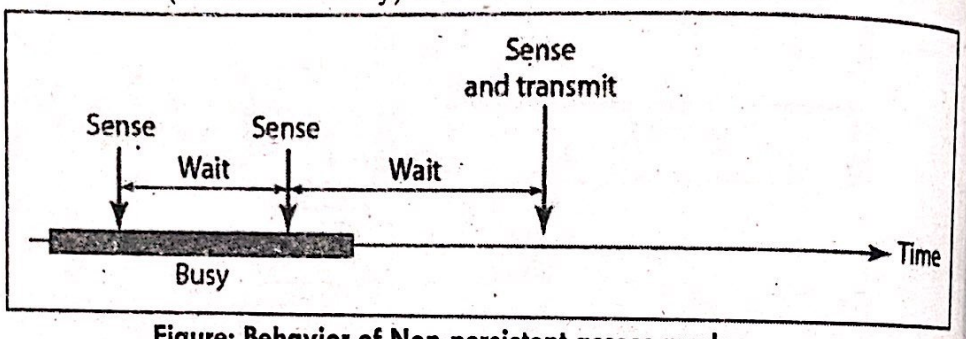


Figure: Behavior of Non-persistent access mode

3. **P-persistent:** The node senses the medium, if idle it sends the data with p probability. If the data is not transmitted ((1-p) probability) then it waits for some time and checks the medium again, now if it is found idle then it sends with p probability. This repeat continues until the frame is sent. It is used in Wi-Fi and packet radio systems.

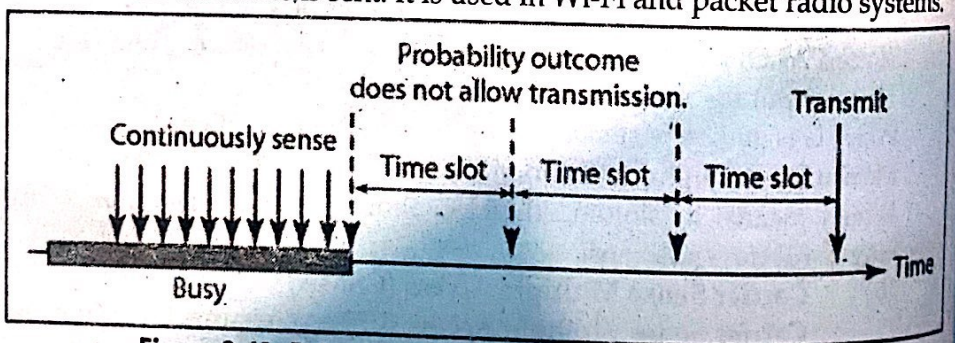


Figure 3.41: Behavior of p-persistent access mode

4. **O-persistent:** Superiority of nodes is decided beforehand and transmission occurs in that order. If the medium is idle, node waits for its time slot to send data.

(c) **Carrier Sense Multiple Access with Collision Detection (CSMA/CD)**

The CSMA method does not tells us what to do in case there is a collision. Carrier sense multiple access with collision detection (CSMA/CD) adds on to the CSMA algorithm to deal with collision. In CSMA/CD, the size of a frame must be large enough so that collision can be detected by sender while sending the frame. So, the frame transmission delay must be at least two times the maximum propagation delay.

To better understand CSMA/CD, let us look at the first bits transmitted by the two stations involved in the collision. Although each station continues to send bits in the frame until it detects the collision, we show what happens as the first bits collide. In figure below, stations A and C are involved in the collision.

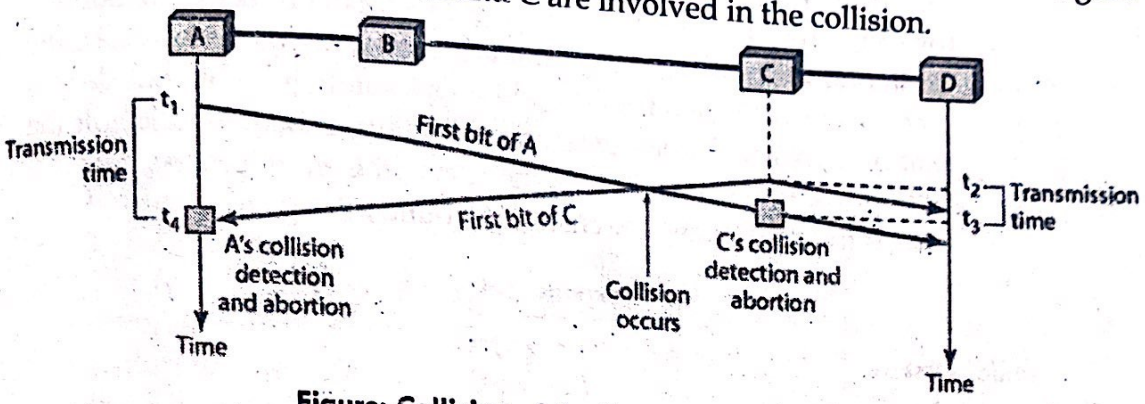


Figure: Collision of the first bit in CSMA/CD

At time t_1, station A has executed its persistence procedure and starts sending the bits of its frame. At time t_2, station C has not yet sensed the first bit sent by A. Station C executes its persistence procedure and starts sending the bits in its frame, which propagate both to the left and to the right. The collision occurs sometime after time t_2. Station C detects a collision at time t_3 when it receives the first bit of A's frame. Station C immediately (or after a short time, but we assume immediately) aborts transmission. Station A detects collision at time t_4 when it receives the first bit of C's frame; it also immediately aborts transmission. Looking at the figure, we see that A transmits for the duration $t_4 - t_1$; C transmits for the duration $t_3 - t_2$.

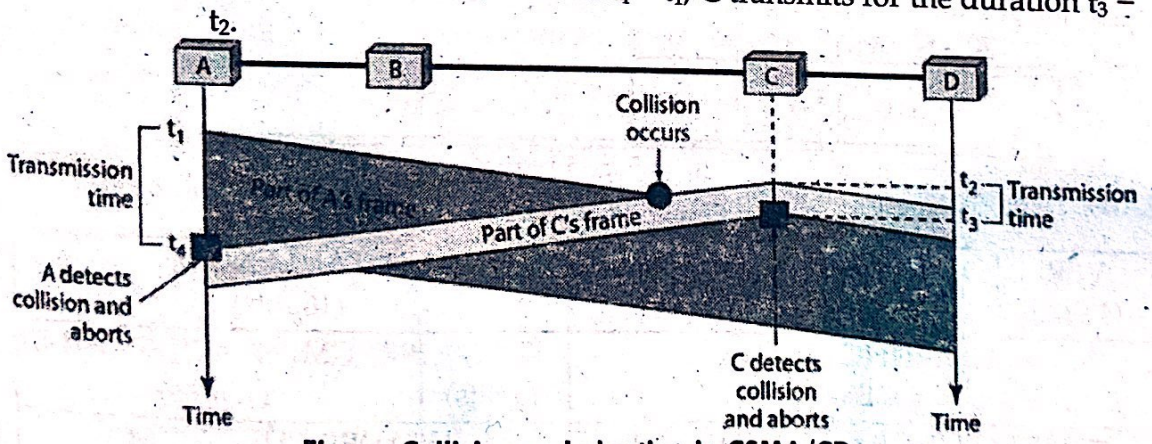


Figure: Collision and abortion in CSMA/CD

(d) Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

Carrier sense multiple access with collision avoidance (CSMA/CA) was invented for wireless networks. The process of collisions detection involves sender receiving acknowledgement signals. If there is just one signal (its own) then the data is successfully sent but if there are two signals (its own and the one with which it has collided) then it means a collision has occurred. To distinguish between these two cases, collision must have a lot of impact on received signal. However, it is not so in wired networks, so CSMA/CA is used in this case.

CSMA/CA avoids collision by:

a) **Interframe space:** Station waits for medium to become idle and if found idle it does not immediately send data (to avoid collision due to propagation delay) rather it waits for a period of time called Interframe space or IFS. After this time, it again checks the medium for being idle. The IFS duration depends on the priority of station.

b) **Contention Window:** It is the amount of time divided into slots. If the sender is ready to send data, it chooses a random number of slots as wait time which doubles every time medium is not found idle. If the medium is found busy it does not restart the entire process, rather it restarts the timer when the channel is found idle again.

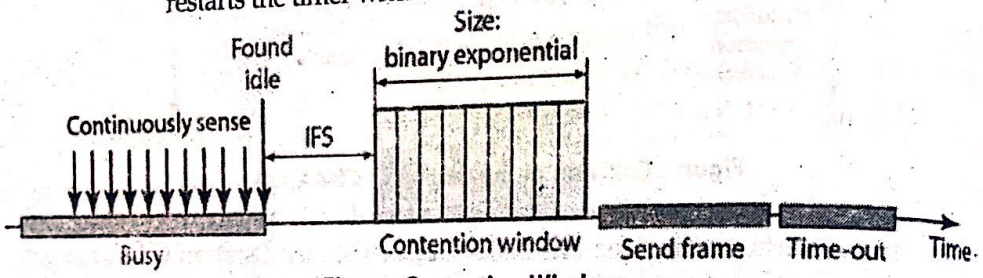


Figure: Contention Window

c) **Acknowledgement:** Sender re-transmits the data if acknowledgement is not received before time-out.

10. Explain the IPv4 header format in detail. [10]

Ans: Packets in the network (internet) layer are called datagrams. A datagram is a variable-length packet consisting of two parts: **header** and **data**. The header is 20 to 60 bytes in length and contains information essential to routing and delivery. It is customary in TCP/IP to show the header in 4-byte sections. The following figure shows the IP datagram format.

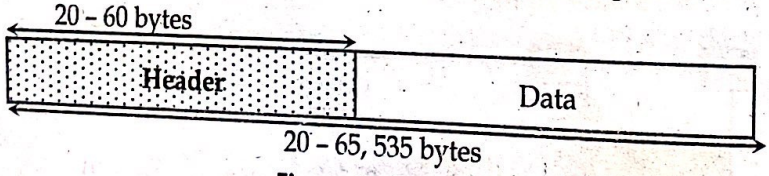


Figure: IP datagram

VER (4 Bits)	HLEN (4 Bits)	TYPE OF SERVICE	TOTAL LENGTH (16 Bits)
IDENTIFICATION (16 Bits)		FLAGS (3 Bits)	FRAGMENTATION OFFSET (13 Bits)
TIME TO LIVE (8 Bits)	PROTOCOL (8 Bits)		HEADER CHECKSUM (16 Bits)
SOURCE IP ADDRESS (32 Bits)			
DESTINATION IP ADDRESS (32 Bits)			
OPTIONS + PADDING (0 to 40 bytes)			
DATA (16 Bits)			

Figure: IPv4 header format

Version Number (VER)

These 4 bits specify the IP protocol version of the datagram. By looking at the version number, the router can determine how to interpret the remainder of the IP datagram. Different versions of IP use different datagram formats.

Header Length (HLEN)

Because an IPv4 datagram can contain a variable number of options (which are included in the IPv4 datagram header), these 4 bits are needed to determine where in the IP datagram the data actually begins. Most IP datagrams do not contain options, so the typical IP datagram has a 20-byte header.

Type of Service

The type of service (TOS) bits was included in the IPv4 header to allow different types of IP datagrams (for example, datagrams particularly requiring low delay, high throughput, or reliability) to be distinguished from each other. For example, it might be useful to distinguish real-time datagrams from non-real-time traffic (for example, FTP). The specific level of service to be provided is a policy issue determined by the router's administrator.

Total Length

This is the total length of the IP datagram (header plus data), measured in bytes. Since this filed is 16 bits long, the theoretical maximum size of the IP datagram is 65,535 bytes. However, datagrams are rarely larger than 1,500 bytes.

Length of data = total length - header length

Identification

If IP packet is fragmented during the transmission, all the fragments contain same identification number to identify original IP packet they belong to.

Flags

As required by the network resources, if IP Packet is too large to handle, these flags tells if they can be fragmented or not. The first bit is reserved (not used). The second bit is called the do not fragment bit. If its value is 1, the machine must not fragment the datagram. If it cannot pass the datagram through any available physical network, it discards the datagram and sends an ICMP error message to the source host. If its value is 0, the datagram can be fragmented if necessary. The third bit is called the more fragment bit. If its value is 1, it means the datagram is not the last fragment. If its value is 0, it means this is the last or only fragment.

Fragment Offset

This offset tells the exact position of the fragment in the original IP Packet.

Time-to-live

To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross. At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded.

Protocol

This field is used only when an IP datagram reaches its final destination. The value of this field indicates the specific transport-layer protocol to which the data portion of this IP datagram should be passed. For example,

a value of 6 indicates that the data portion is passed to TCP, while a value of 17 indicates that the data is passed to UDP.

Header Checksum

This field is used to keep checksum value of entire header which is then used to check if the packet is received error-free.

Source Address

This 32-bit field define the address of the Sender (or source) of the packet.

Destination Address

This 32-bit field define the address of the Receiver (or destination) of the packet.

Options

This is optional field, which is used if the value of IHL is greater than 5. These options may contain values for options such as Security, Record Route, Time Stamp, etc.

Data (Payload)

Finally, we come to the last and most important field. In most circumstances, the data field of the IP datagram contains the transport-layer segment (TCP or UDP) to be delivered to the destination. However, the data field can carry other types of data, such as ICMP messages.

❑❑❑

MODEL QUESTIONS SETS FOR PRACTICE

MODEL SET 1

Course Title: Computer Networking
Course No: CACS303
Nature of the Course: Theory + Lab
Semester: V

Full Marks: 60
Pass Marks: 24
Time: 3

Candidates are required to give their answer in their own words as far as practicable.

Group- A

Attempt all the questions **[10x1=10]**

1. Circle (O) the correct answer in the following questions:

i. Computer Network is _____
   a) Collection of hardware components and computers
   b) Interconnected by communication channels
   c) Sharing of resources and information
   d) all of the above

ii. Which transmission media provides the highest transmission speed in a network?
   a) Coaxial cable
   b) twisted pair cable
   c) optical fiber
   d) electrical cable

iii. Which of the following is the multiple access protocol for channel access control?
   a) CSMA/CD
   b) CSMA/CA
   c) Both CSMA/CD & CSMA/CA
   d) HDLC

iv. You have an IP address of 172.16.13.5 with a 255.255.255.128 subnet mask. What is your class of address, subnet address, and broadcast address?
   a) Class A, Subnet 172.16.13.0, Broadcast address 172.16.13.127
   b) Class B, Subnet 172.16.13.0, Broadcast address 172.16.13.127
   c) Class B, Subnet 172.16.13.0, Broadcast address 172.16.13.255
   d) Class B, Subnet 172.16.0.0, Broadcast address 172.16.255.255

v. Which of the following is false with respect to TCP?
   a) Connection-oriented
   b) Process-to-process
   c) Transport layer protocol
   d) Unreliable

vi. Which is not an application layer protocol?
   a) HTTP
   b) SMTP
   c) FTP
   d) TCP

vii. In cryptography, what is cipher?
   a) algorithm for performing encryption and decryption
   b) Encrypted message
   c) Both algorithm for performing encryption and decryption and encrypted message
   d) Decrypted message

viii. Communication channel is shared by all the machines on the network in _____
   a) Broadcast network
   b) unicast network
   c) Multicast network
   d) any-cast network

ix. Bluetooth is an example of _____
a) Local area network b) wide area network
c) Persona area network d) virtual private network

x. A single channel is share by multiple signals by _____.
a) Analog modulation b) digital modulation
c) Phase modulation d) multiplexing

Group B

Attempt any SIX questions. [6×5=30]

2. What do you mean by Internet Protocol Stack?
3. Explain the principle of congestion control.
4. What do you mean by IP datagram fragmentation?
5. Explain Give a detail note on slotted ALOHA protocols.
6. Explain about GBN Sliding window protocol.
7. Explain the term checksum in reference to error detection codes.
8. Write short notes on (ANY TWO): [2.5+2.5]
   a) Bluetooth Standards
   b) Analog vs. Digital Signals
   c) IPSec

Group C

Attempt any TWO questions. [2×10=20]

9. What is the significance of layered architecture? Explain the OSI layered architecture with neat sketch.
10. With an example explain the Dynamic routing algorithm used in computer networks.
11. Define DNS. Explain the DNS records and DNS messages.

MODEL SET 2

Candidates are required to give their answer in their own words as far as practicable.

Group- A

Attempt all the questions [10 x1=10]

1. **Circle (O) the correct answer in the following questions:**

i. The structure or format of data is called _____
a) Syntax b) Semantics c) Struct d) Formatting

ii. The physical layer provides _____
a) Mechanical specifications of electrical connectors and cables
b) Electrical specification of transmission line signal level
c) Specification for IR over optical fiber
d) all of the mentioned

iii. Which of the following tasks is not done by data link layer?
a) framing b) error control
c) flow control d) channel coding

iv. CRC stands for _____
a) cyclic redundancy check b) code repeat check
c) code redundancy check d) cyclic repeat check

v. The network layer is concerned with _____ of data.

a) bits b) frames c) packets d) bytes

vi. Which is not a function of network layer?
a) routing b) inter-networking
c) congestion control d) error control

vii. A _____ is a TCP name for a transport service access point.
a) port b) pipe c) node d) protocol

viii. In an asymmetric-key cipher, the receiver uses own _____ key to decipher.
a) private b) public
c) all of the above d) none of the above

ix. Virtual terminal protocol is an example of the _____
a) transport layer b) presentation layer
c) application layer d) none of the above

x. In a network with 26 computers, which topology would require the most extensive cabling?
a) mesh b) bus c) ring d) star

Group B

Attempt any SIX questions. **[6×5=30]**

2. Describe in details about light wave transmission.
3. Explain the working principle of SMTP.
4. Define data link layer and its services.
5. Explain point-to-point protocol (PPP).
6. Explain the multicasting routine and its applications.
7. What are the responsibilities of Presentation layer and Session layer of OSI Model?
8. Write short notes on (ANY TWO): [2.5+2.5]
   a. Packet Switching
   b. DHCP
   c. Firewalls

Group C

Attempt any TWO questions. **[2×10=20]**

9. Explain the principles of application layer protocols. What do you mean by file transfer?
10. Draw TCP packet header format. Explain 3-way handshaking of Transmission Control Protocol.
11. Define protocol and standard. Explain TCP/IP model with a neat diagram.

MODEL SET 3

Candidates are required to give their answer in their own words as far as practicable.

Group- A **[10 x1=10]**

Attempt all the questions

1. Circle (O) the correct answer in the following questions:

i. In a P2P network, who controls the devices?
a) first computer b) last computer
c) no device controls d) all devices control

ii. A computer network consists of _____ number of computers or servers or system.
a) 2 b) 3 c) more than 2 d) all of the above

iii. The two sub-layers of a data link layer are _____.
a) LLC b) MAC
c) both LLC and MAC d) data layer

iv. The technique of temporarily delaying outgoing acknowledgements so that they can be hooked onto the next outgoing data frame is called _____
a) piggybacking b) cyclic redundancy check
c) fletcher's checksum d) parity check

v. A 4 bytes IP address consists of _____
a) Only network address b) only host address
c) Network address & host address d) network address & MAC address

vi. For carrying digital data over long distance using either analog signal or digital signal at approximately spaced points, we must have
a) Amplifiers b) repeater
c) switch d) either amplifier or repeater

vii. IPSec is designed to provide security at the _____
a) Transport layer b) network layer
c) Application layer d) session layer

viii. The packet of information at the application layer is called _____
a) Message b) segment c) packet d) frame

ix. When displaying a web page, the application layer uses the _____
a) FTP protocol b) HTTP protocol
c) SMTP protocol d) TCP protocol

x. Cryptanalysis is used _____
a) To find some insecurities in a cryptographic scheme
b) to increase the speed
c) To encrypt the data
d) To make new ciphers

Group B

Attempt any SIX questions. [6×5=30]

2. What is circuit-switching? How is it different from packet-switching?
3. Discuss different fields of UDP. How is it different from TCP?
4. What is static routing? How is it different from dynamic routing?
5. What is random access protocol? Discuss FDMA in detail.
6. Differentiate between thicknet and thinnet cable.
7. Perform encryption and decryption using the RSA algorithm for p=5, q=7, e=7 and m=2.
8. Write short notes on (ANY TWO): [2.5+2.5]
   a. SNMP
   b. ARP
   c. Framing

Group C

Attempt any TWO questions. [2×10=20]

9. Why do we need layered protocol architecture? Discuss each layer of TCP/IP architecture along with function of each layer. Compare TCP/IP with OSI mode.
10. Assume a Class B network. Divide this network in 16 different sub-networks. What is new subnet mask?

11. Define multiplexing. What are the benefits of using multiplexing? Discuss Go-Back-N and Selective Repeat protocol in detail.

MODEL SET 4

Candidates are required to give their answer in their own words as far as practicable.

Group- A

Attempt all the questions **[10 x1=10]**

1. **Circle (O) the correct answer in the following questions:**

i. When collection of various computers seems a single coherent system to its client, then it is called _____
   a) Computer network b) distributed system
   c) Networking system d) mail system

ii. Who developed standards for the OSI reference model?
   a) ANSI – American National Standards Institute
   b) ISO – International Standards Organization
   c) IEEE – Institute of Electrical and Electronics Engineers
   d) ACM – Association for Computing Machinery

iii. An Ethernet jack is _____
   a) RJ11 b) RJ14 c) RJ45 d) None

iv. The size of an IP address in IPv6 is _____.
   a) 4 bytes b) 128 bits c) 8 bytes d) 100 bits

v. Which of the following is false with respect to UDP?
   a) connection-oriented b) low overhead
   c) Transport layer protocol d) Unreliable

vi. Two broad categories of congestion control are
   a) open-loop and closed-loop b) open-control and closed-control
   c) active control and passive control d) active loop and passive loop

vii. The communication protocol used by internet is_____
   a) HTTP b) WWW c) TCP/IP d) FTP

viii. Web site is a collection of _____
   a) HTML Documents b) Graphic files
   c) Audio and video files d) all of the above

ix. The shortest frame in HDLC protocol is usually the _____.
   a) Information frame b) management frame
   c) Supervisory frame d) none of the above

x. Digital signature does not provide _____
   a) Nonrepudiation b) privacy
   c) Authentication d) all of the above

Group B

Attempt any SIX questions. **[6×5=30]**

2. What is transmission media? Explain about any three transmission medias in detail.
3. Is 192.16.10.64/26 a host, network or broadcast address? Also write subnet mask and usable hosts of the following network.
4. Explain how a TCP connection can be gracefully terminated?

5. What methods are used so that IPV6 and IPV4 networks are interoperable?
6. Find Hamming Code for data 11010111.
7. Describe how SMTP protocol is used in e-mail applications.
8. Write short notes on (Any Two):
   a. NAT
   b. Virtual LAN
   c. Single bit parity

Group C

Attempt any TWO questions. [2×10=20]

9. Explain the reason behind layering the network architecture? Write the functions of all layers of TCP/IP model.
10. Explain the signature generation and signature verification in digital signature process.
11. Suppose we want to transmit the message 1011 0010 0111 and protect it from errors using the CRC polynomial $x^4 + x^2 + 1$. Use polynomial long division to determine the message that should be transmitted. Suppose the leftmost bit of the message is inverted due to noise on the transmission link. What is the result of the receiver's CRC calculation? How does the receiver known that an error has occurred?

MODEL SET 5

Candidates are required to give their answer in their own words as far as practicable.

Group- A

Attempt all the questions [10 x1=10]

1. **Circle (O) the correct answer in the following questions:**

i. A list of protocols used by a system, one protocol per layer, is called _____
   a) Protocol architecture b) protocol stack
   c) Protocol suite d) protocol system

ii. Which one of the following is an architecture paradigm?
   a) peer-to-peer b) client-server
   c) http d) both peer-to-peer and client-server

iii. The first network was called _____.
   a) CNNET b) NSFNET c) ARPANET d) ASAPNET

iv. The physical layer provides _____.
   a) Mechanical specifications of electrical connectors and cables
   b) Electrical specification of transmission line signal level
   c) Specification for IR over optical fiber
   d) all of the mentioned

v. When two or more bits in a data unit has been changed during the transmission, the error is called _____
   a) Random error b) burst error c) inverted error d) double error

vi. The network layer protocol for internet is _____
   a) Ethernet b) internet protocol c) FTP d) HTTP

vii. ICMP is primarily used for _____
   a) error and diagnostic functions b) addressing
   c) Forwarding d) routing

viii. Transmission control protocol _____
a) is a connection-oriented protocol
b) Uses a three way handshake to establish a connection
c) Receives data from applications as a single stream
d) all of the mentioned

ix. For separate channels in TDM, it is necessary to use
a) Time slots
b) bandpass filters
c) Differentiation
d) none of the above

x. VPN technology uses two simultaneous techniques to guarantee privacy for an organization: _____
a) SSL; tunneling
b) IPSec; SSL
c) IPSec; tunneling
d) none of the above

Group B

Attempt any SIX questions. **[6×5=30]**

2. What do you mean by Internet Protocol Stack?
3. Define mobile network. Discuss the evolution of mobile network generation from 1G to 5G.
4. Explain POP3 and IMAP4.
5. Explain IPv4 addressing.
6. Explain on ALOHA and Slotted ALOHA protocols.
7. Draw and explain three-way handshake process of TCP.
8. Write short notes on (ANY TWO):
   a) OSPF
   b) Transmission Impairment
   c) Congestion Control

Group C

Attempt any TWO questions. **[2×10=20]**

9. What are the seven layers of OSI model? Explain the structure of TCP Header format.
10. What do you mean by cryptography? Explain the encryption and decryption in cryptosystem.
11. Consider 8 bit 10101010 is transmitted using Hamming distance. Show the actual bits transmitted without any error. If the 6th bit from LSB is inverted during transmission. Show how the error is detected and corrected at the receiver's end. Also, obtain the original data after correction.

MODEL SET 6

Candidates are required to give their answer in their own words as far as practicable.

Group- A

Attempt all the questions **[10 x1=10]**

1. **Circle (O) the correct answer in the following questions:**

i. Individual pieces of information within a network protocol mean _____
a) Syntax b) Semantics c) Struct d) Formatting

ii. A mobile station only communicates with one base station, in a _____
a) back off b) soft handoff c) hard handoff d) low handoff

iii. In which one of the following, the slow and fast hopping is used?
a) GSM b) GPRS c) FHSS d) none of the above

iv. Which of the following computer networks is built on the top of another network?
a) Overlay network b) prime network
c) Chief network d) prior network

v. The datalink layer is concerned with _____ of data.
a) Bits b) frames c) packets d) bytes

vi. Function of network layer.
a) Routing b) inter-networking
c) congestion control d) all of the mentioned

vii. What is the measure (unit) used to represent signaling rate per second?
a) Baud b) Hz
c) Bps d) none of the above

viii. What is the main advantages of UDP?
a) more overload b) reliable
c) low overhead d) fast

ix. Which one of the following protocol deliver/store mail to receiver server?
a) SMTP b) POP c) IMAP d) HTTP

x. In the _____ mode, the IPSec header is added between the IP header and the rest of the packet.
a) Tunnel b) transport c) transition d) none of the above

Group B

Attempt any SIX questions. [6×5=30]

2. Explain peer-to-peer network model.
3. Your friend cannot communicate with you without protocol, why?
4. Explain how slotted ALOHA improves the performance of system over pure ALOHA.
5. Differentiate between broadband and base band services.
6. Compare and contrast the IPv4 and the IPv6 header files. Do they have any fields in common?
7. What is meant by "domain name"? How is a domain name translated to an equivalent IP address? Explain
8. Write short notes on (ANY TWO):
   a) ICMP
   b) Throughput vs. Good put
   c) Sliding window

Group C

Attempt any TWO questions. [2×10=20]

9. Define public key cryptography. In RSA system, how private key is generated from given public key? Explain with an example.
10. Explain the various field of the TCP header and the working of the TCP protocol.
11. Explain how does CRC detect the error with multiple bits? Given message is $M(x) = x^7 + x^4 + x^3 + x^2 + 1$ and the generator $G(x) = x^3 + 1$. Show the actual bit string transmitted, suppose the third bit from the left is inverted during the transmission. Show how the error is detected at the receiver's end.

MODEL SET 7

Candidates are required to give their answer in their own words as far as practicable.

Group- A

Attempt all the questions [10 x1=10]

1. **Circle (O) the correct answer in the following questions:**

i. In the layer hierarchy as the data packet moves from the upper to the lower layers, headers are __
   a) Added b) removed c) rearranged d) modified

ii. Which of this is not a network edge device?
   a) PC b) smartphone c) servers d) switch

iii. The device operation at Data Link layer is
   a) Repeater b) router c) bridge d) none of the above

iv. Which of the following routing algorithms can be used for network layer design?
   a) Shortest path algorithm b) distance vector routing
   c) Link state routing d) all of the above

v. Application layer offers _____ service.
   a) End to end
   b) Process to process
   c) both end to end and process to process
   d) None of the above

vi. Which of the following is true with respect to TCP?
   a) Connection-oriented b) Process-to-process
   c) Transport layer protocol d) all of the above

vii. Pick the odd one out.
   a) File transfer b) file download
   c) Interactive games d) e-mail

viii. Which of the following is a fundamental principle of wireless communication?
   a) Electromagnetic waves b) microwaves
   c) Both a) and b) d) none of the above

ix. In cryptography, what is cipher?
   a) Encrypted message
   b) Algorithm for performing encryption and decryption
   c) Both algorithm for performing encryption and decryption and encrypted message
   d) Decrypted message

x. A proxy firewall filters at _____
   a) Physical layer b) data link layer
   c) Network layer d) application layer

Group B

Attempt any SIX questions. [6×5=30]

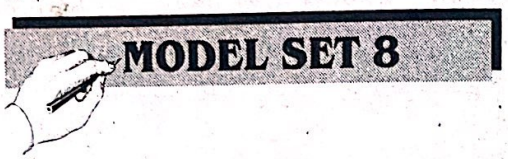
2. Explain client server system. How is it different from peer-to-peer system?
3. Explain the final delivery of email to the end user using POP3.
4. Assume a class A network and divide it into four subnets. What is the value of new subnet mask?

5. Discuss CRC as an error detection mechanism.
6. What is congestion control? Why do we need it?
7. Differentiate between circuit switching, packet switching and message switching.
8. Write short notes on (ANY TWO): [2.5+2.5]
   a) IEEE 802.3
   b) Nyquist bit Rate
   c) IPSec tunnel modes

Group C

Attempt any TWO questions. [2×10=20]

9. Define Protocol. Why do we need layered protocol architecture? Discuss each layer of TCP/IP protocol architecture in detail
10. Define transmission media. Differentiate between guided and unguided transmission media. Discuss each guided transmission media in detail.
11. What is routing? Discuss link state routing algorithm in detail.



Candidates are required to give their answer in their own words as far as practicable.

Group- A

Attempt all the questions [10 x1=10]

1. Circle (O) the correct answer in the following questions:

i. Which transmission media is easy to install inside a city to create a network quickly?
   a) Cable media
   b) fiber optic
   c) Radio frequency devices
   d) all of the above

ii. Which one of the following is an architecture paradigm?
   a) peer-to-peer
   b) client-server
   c) Http
   d) both peer-to-peer and client-server

iii. Which is the network that can cover an entire city?
   a) LAN
   b) MAN
   c) WAN
   d) all of the above

iv. Which is the layer that converts raw bits to frames and frames to raw bits in the OSI model?
   a) Application layer
   b) transport layer
   c) Network layer
   d) data link layer

v. When two or more bits in a data unit has been changed during the transmission, the error is called _____
   a) Random error
   b) burst error
   c) inverted error
   d) double error

vi. In reality, Internet Protocol recognizes only
   a) An IP address
   b) a location of the host
   c) a postal mail address
   d) none of the above

vii. FTP is used for _____
a) Uploading files only b) downloading files only
c) Both (A) and (B) d) none of the above

viii. Which of the network allow different speed links?
a) Message-switched networks b) packet-switched networks
c) circuit-switched networks d) none of the mentioned

ix. Three security goals are _____.
a) Confidentiality, cryptography, and nonrepudiation
b) Confidentiality, encryption, and decryption
c) Confidentiality, integrity, and availability
d) None of the above

x. In _____ cryptography, the same key is used in both directions.
a) symmetric-key b) asymmetric-key
c) public-key d) none of the above

Group B

Attempt any SIX questions. **[6×5=30]**

2. Discuss FTP in detail.
3. What is Subnetting? Assume a class C network and divide it into four subnets. What is the value of new subnet mask?
4. How does the system correct error after error detection?
5. What is transmission media? Discuss wireless transmission media in detail.
6. Suppose you have got 50 PCs to set up in a LAN, which cable, device, protocol, you prefer and why justify with reason.
7. What are sliding window protocol? Explain one -bit sliding window protocol with an appropriate diagram.
8. Write short notes on (ANY TWO): [2.5+2.5]
   a) Single bit parity
   b) Leaky bucket
   c) Cable Network

Group C

Attempt any TWO questions. **[2×10=20]**

9. Discuss the relationship between transport layer and network layer. Discuss TCP as a transport layer protocol along with its segment structure.
10. Design a general model for network security. Explain.
11. Why do we need routing algorithm? Discuss distance vector routing algorithm in detail.

❑❑❑