**LAN & Networking**

**Sample Question Paper**

Note: Q.No. 1 is compulsory, attempt one question from each unit.

Q. 1. a). What are the uses of Computer network? 2.5 X10

b) What is the Principal difference between connectionless and connection oriented communication?

c). What is the difference between congestion control and flow control?

d). What is the need of using layered protocols.

e) Explain Data link layer.

f) Explain Token Ring.

g) What is CSMA ?

h) What is STP and UTP?

i) What is VLAN?

j)What is DNS?

Unit-1

Q. 2. Explain with a neat sketch, the functions of the protocols used in each layer of the OSI model and illustrate how communication is taking place between two end systems. 12.5

Q 3. a) What is Internet? Explain evolution of Internet. 6.5

b) Explain TCP/IP model. 6

Unit-2

Q4. What is a transmission medium? Explain its types in detail. 12.5

Q 5. a) Explain Radiowaves, Infrared and Microwave. 6.5

b) Explain framing in detail. 6

Unit-3

Q6. a) What is ALOHA?Explain CSMA protocols in detail. 6.5

b) Explain Virtual LAN in detail. 6

Q 7. Differentiate between IPV 4 & IPV 6 12.5

Unit-4

Q. 8. Write short notes on:

a) HTTP 4

b)Telnet 4

c) Broadband 4.5

Q. 9. Write short notes on:

a) ISDN 4

b) Cryptography 4

c) ISP 4.5

**Answers**

Ans. 1 a) Business Applications

Home Applications

Mobile Users

Social Issues

b) Connection-oriented communication includes the steps of setting up a call from one computer to another, transmitting/receiving data, and then releasing the call, just like a voice phone call. However, the network connecting the computers is a packet switched network, unlike the phone system's circuit switched network. Connection-oriented communication is done in one of two ways over a packet switched network: with and without virtual circuits.Connectionless communication is just packet switching where no call establishment and release occur. A message is broken into packets, and each packet is transferred separately. Moreover, the packets can travel different route to the destination since there is no connection. Connectionless service is typically provided by the UDP (User Datagram Protocol), which we will examine later. The packets transferred using UDP are also called datagrams.

c) Flow control is controlled by the receiving side. It ensures that the sender only sends what the receiver can handle. Think of a situation where someone with a fast fiber connection might be sending to someone on dialup or something similar. The sender would have the ability to send packets very quickly, but that would be useless to the receiver on dialup, so they would need a way to throttle what the sending side can send. Flow control deals with the mechanisms available to ensure that this communication goes smoothly.

Congestion control is a method of ensuring that everyone across a network has a "fair" amount of access to network resources, at any given time. In a mixed-network environment, everyone needs to be able to assume the same general level of performance. A common scenario to help understand this is an office LAN. You have a number of LAN segments in an office all doing their thing within the LAN, but then they may all need to go out over a WAN link that is slower than the constituent LAN segments. Picture having 100mb connections within the LAN that ultimately go out through a 5mb WAN link. Some kind of congestion control would need to be in place there to ensure there are no issues across the greater network.

d) Layered protocols are specifically encountered in networking technology. The two main reasons for this are abstraction and specialization. A protocol creates a neutral standard from which rival companies can create compatible programs. The field requires so many protocols that they need to be organized and directed to those specialists whose work each protocol impacts. Using layered protocols, a software house can create a network program knowing that if it follows the guidelines of one layer, the services of lower layers will be provided by other companies. This enables them to specialize. Abstraction is the state of assuming lower services will be provided by another protocol.

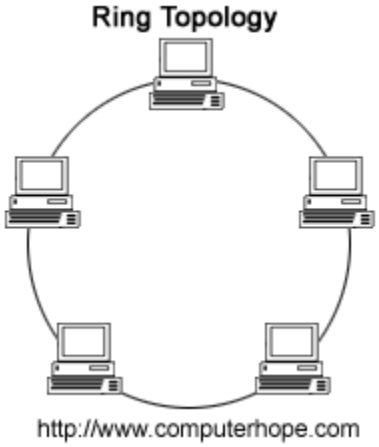
e) The Data-Link layer is the protocol layer in a program that handles the moving of data in and out across a physical link in a network. The Data-Link layer is layer 2 in the Open Systems Interconnect (OSI) model for a set of telecommunication protocols.

The Data-Link layer contains two sublayers that are described in the IEEE-802 LAN standards:

- Media Access Control (MAC)
- Logical Link Control (LLC)

The Data-Link layer ensures that an initial connection has been set up, divides output data into data frames, and handles the acknowledgements from a receiver that the data arrived successfully. It also ensures that incoming data has been received successfully by analyzing bit patterns at special places in the frames.

f) Token ring or 802.5 is a network where all computers on the network are connected in a circle fashion. The term token is used to describe a segment of information that is sent through that circle; when a computer on the network is able to decode that token, the information is received on that computer. The token ring is used byARCNET, token bus and FDDI. Today, 802.5 and Token ring is also considered inactive.




g) Carrier Sense Multiple Access (CSMA) is a probabilistic Media Access Control (MAC) protocol in which a node verifies the absence of other trafficbefore transmitting on a shared transmission medium, such as an electrical bus, or a band of the electromagnetic spectrum.

"Carrier Sense" describes the fact that a transmitter uses feedback from a receiver that detects a carrier wave before trying to send. That is, it tries to detect the presence of an encoded signal from another station before attempting to transmit. If a carrier is sensed, the station waits for the transmission in progress to finish before initiating its own transmission.

"Multiple Access" describes the fact that multiple stations send and receive on the medium. Transmissions by one node are generally received by all other stations using the medium.

h) Unshielded Twisted Pair (UTP) : UTP is the copper media, inherited from telephony, which is being used for increasingly higher data rates, and is rapidly becoming the de facto standard for horizontal wiring, the connection between, and including, the outlet and the termination in the communication closet. A Twisted Pair is a pair of copper wires, with diameters of 0.4-0.8 mm, twisted together and wrapped with

a plastic coating. The twisting increases the electrical noise immunity, and reduces the bit error rate (BER) of the data transmission. A UTP cable contains from 2 to 4200 twisted pairs.

UTP is a very flexible, low cost media, and can be used for either voice or data communications. Its greatest disadvantage is the limited bandwidth, which restricts long distance transmission with low error rates.

Shielded Twisted Pair (STP) : STP is heavier and more difficult to manufacture, but it can greatly improve the signaling rate in a given transmission scheme Twisting provides cancellation of magnetically induced fields and currents on a pair of conductors. Magnetic fields arise around other heavy current-carrying conductors and around large electric motors. Various grades of copper cables are available, with Grade 5 being the best and most expensive.

Grade 5 copper, appropriate for use in 100-Mbps applications, has more twists per inch than lower grades. More twists per inch means more linear feet of copper wire used to make up a cable run, and more copper means more money.

Shielding provides a means to reflect or absorb electric fields that are present around cables. Shielding comes in a variety of forms from copperbraiding or copper meshes to aluminized.

i) In simple terms, a VLAN is a set of workstations within a LAN that can communicate with each other as though they were on a single, isolated LAN.
What does it mean to say that they "communicate with each other as though they were on a single, isolated LAN"?
Among other things, it means thatbroadcast packets sent by one of the workstations will reach all the others in the VLAN broadcasts sent by one of the workstations in the VLAN will not reach any workstations that are not in the VLAN broadcasts sent by workstations that are not in the VLAN will never reach workstations that are in the VLANthe workstations can all communicate with each other without needing to go through a gateway. For example, IP connections would be established by ARPing for the destination IP and sending packets directly to the destination workstation—there would be no need to send packets to the IP gateway to be forwarded on the workstations can communicate with each other using non-routable protocols.
j) The DNS translates Internet domain and host names toIP addresses. DNS automatically converts the names we type in our Web browser address bar to the IP addresses of Web servers hosting those sites.

DNS implements a distributed database to store this name and address information for all public hosts on the Internet. DNS assumes IP addresses do not change (are statically assigned rather than dynamically assigned).

The DNS database resides on a hierarchy of special database servers. When clients like Web browsers issue requests involving Internet host names, a piece of software called the *DNS resolver* (usually built into the network operating system) first contacts a DNS server to determine the server's IP address. If the DNS server does not contain the needed mapping, it will in turn forward the request to a different DNS server at the next higher level in the hierarchy. After potentially several forwarding and delegation messages are sent

within the DNS hierarchy, the IP address for the given host eventually arrives at the resolver, that in turn completes the request over Internet Protocol.

**Ans.2.** The OSI, or *Open System Interconnection*, model defines a networking framework to implement protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, and proceeding to the bottom layer, over the channel to the next station and back up the hierarchy.

There's really nothing to the OSI model. In fact, it's not even tangible. The OSI model doesn't do any functions in the networking process, It is a *conceptual framework* so we can better understand complex interactions that are happening. The OSI model takes the task of internetworking and divides that up into what is referred to as a vertical stack that consists of the following layers:

Physical (Layer 1)

This layer conveys the bit stream - electrical impulse, light or radio signal -- through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards and physical aspects. Fast Ethernet, RS232, and ATM are protocols with physical layer components.

Data Link (Layer 2)

At this layer, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control and frame synchronization. The data link layer is divided into two sub layers: The Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. The MAC sub layer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronization, flow control and error checking.

- *Layer 2 Data Link examples include PPP, FDDI, ATM, IEEE 802.5/ 802.2, IEEE 802.3/802.2, HDLC, Frame Relay,*

Network (Layer 3)

This layer provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing,internetworking, error handling, congestion control and packet sequencing.

- *Layer 3 Network examples include AppleTalk DDP, IP, IPX.*

Transport (Layer 4)

This layer provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer.

- *Layer 4 Transport examples include SPX, TCP, UDP.*

Session (Layer 5)

This layer establishes, manages and terminates connections between applications. The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. It deals with session and connection coordination.

- *Layer 5 Session examples include NFS, NetBios names, RPC, SQL.*

Presentation (Layer 6)

This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the syntax layer.

- *Layer 6 Presentation examples include encryption, ASCII, EBCDIC, TIFF, GIF, PICT, JPEG, MPEG, MIDI.*

Application (Layer 7)

This layer supports application and end-user processes. Communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. Everything at this layer is application-specific. This layer provides application services for file transfers, e-mail, and other network software services. Telnet and FTP are applications that exist entirely in the application level. Tiered application architectures are part of this layer.

- *Layer 7 Application examples include WWW browsers, NFS, SNMP, Telnet, HTTP, FTP*

**Ans.3a)** The Internet is a global system of interconnected computer networks that use the standard Internet protocol suite(TCP/IP) to link several billion devices worldwide. It is a *network of networks* that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic, wireless, and optical networking technologies. The Internet carries an extensive range of information resources and services, such as the inter-linked hypertext documents and applications of the World Wide Web (WWW), theinfrastructure to support email, and peer-to-peer networks for file sharing and telephony. The origins of the Internet date back to research commissioned by the United States government in the 1960s to build robust, fault-tolerant communication via computer networks. While this work, together with work in the United Kingdom and France, led to important precursor networks, they were not the Internet. There is no consensus on the exact date when the modern Internet came into being, but sometime in the early to mid-1980s is considered reasonable. From that point, the network experienced decades of sustained exponential growth as generations of institutional, personal, and mobile computers were connected to it.

The funding of a new U.S. backbone by the National Science Foundation in the 1980s, as well as private funding for other commercial backbones, led to worldwide participation in the development of new networking technologies, and the merger of many networks. Though the Internet has been widely used by academia since the1980s, the commercialization of what was by the 1990s an international network resulted in its popularization and incorporation into virtually every aspect of modern human life. As of

June 2012, more than 2.4 billion people—over a third of the world's human population—have used the services of the Internet; approximately 100 times more people than were using it in 1995.[1][2] Internet use grew rapidly in the West from the mid-1990s to early 2000s and from the late 1990s to present in thedeveloping world. In 1994 only 3% of American classrooms had access to the Internet while by 2002 92% did.[3]

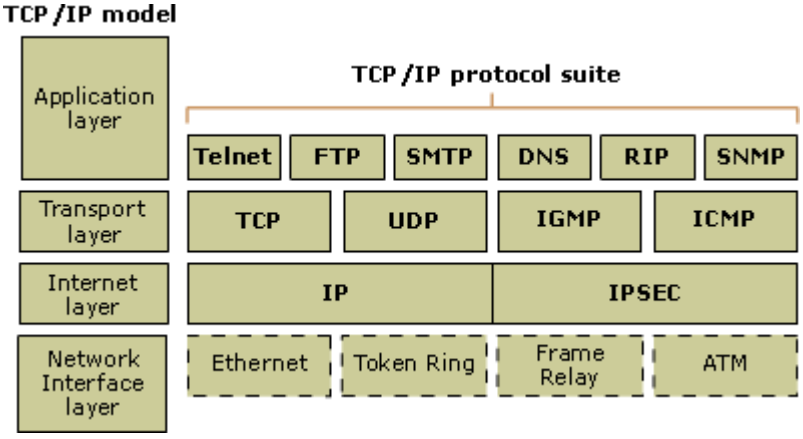
Most traditional communications media including telephone, music, film, and television are being reshaped or redefined by the Internet, giving birth to new services such as voice over Internet Protocol (VoIP) and Internet Protocol television (IPTV). Newspaper, book, and other print publishing are adapting to website technology, or are reshaped into blogging and web feeds. The Internet has enabled and accelerated new forms of human interactions through instant messaging, Internet forums, and social networking. Online shopping has boomed both for major retail outlets and small artisans and traders. Business-to-business and financial serviceson the Internet affect supply chains across entire industries.

The Internet has no centralized governance in either technological implementation or policies for access and usage; each constituent network sets its own policies. Only the overreaching definitions of the two principal name spaces in the Internet, the Internet Protocol address space and the Domain Name System, are directed by a maintainer organization, the Internet Corporation for Assigned Names and Numbers (ICANN). The technical underpinning and standardization of the core protocols (IPv4 and IPv6) is an activity of the Internet Engineering Task Force (IETF), a non-profit organization of loosely affiliated international participants that anyone may associate with by contributing technical expertise.

**3 b)** The TCP/IP model

TCP/IP is based on a four-layer reference model. All protocols that belong to the TCP/IP protocol suite are located in the top three layers of this model.

As shown in the following illustration, each layer of the TCP/IP model corresponds to one or more layers of the seven-layer Open Systems Interconnection (OSI) reference model proposed by the International Standards Organization (ISO).




The types of services performed and protocols used at each layer within the TCP/IP model are described in more detail in the following table.

| Layer | Description | Protocols |
|---|---|---|
| Application | Defines TCP/IP application protocols and how host programs interface with transport layer services to use the network. | HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP, X Windows, other application protocols |
| Transport | Provides communication session management between host computers. Defines the level of service and status of the connection used when transporting data. | TCP, UDP, RTP |
| Internet | Packages data into IP datagrams, which contain source and destination address information that is used to forward the datagrams between hosts and across networks. Performs routing of IP datagrams. | IP, ICMP, ARP, RARP |
| Network interface | Specifies details of how data is physically sent through the network, including how bits are electrically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted-pair copper wire. | Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232, v.35 |

**Note**

- The OSI reference model is not specific to TCP/IP. It was developed by the ISO in the late 1970s as a framework for describing all functions required of an open interconnected network. It is a widely known and accepted reference model in the data communications field and is used here only for comparison purposes.

**Ans. 4** In a data transmission system, the transmission medium is the physical path between transmitter and receiver.

*Magnetic Media*

One of the most convenient way to transfer data from one computer to another, even before the birth of networking, was to save it on some storage media and transfer physical from one station to another. Though it may seem odd in today's world of high speed Internet, but when the size of data to transfer is huge, Magnetic media comes into play.

For an example, say a Bank has Gigs of bytes of their customers' data which stores a backup copy of it at some geographically far place for security and uncertain reasons like war or tsunami. If the Bank needs to

store its copy of data which is Hundreds of GBs, transfer through Internet is not feasible way. Even WAN links may not support such high speed or if they do cost will be too high to afford.

In these kinds of cases, data backup is stored onto magnetic tapes or magnetic discs and then shifted physically at remote places.

*Twisted Pair Cable*

A twisted pair cable is made of two plastic insulated copper wires twisted together to form a single media. Out of these two wires only one carries actual signal and another is used for ground reference. The twists between wires is helpful in reducing noise (electro-magnetic interference) and crosstalk.

here are two types of twisted pair cables available:

- Shielded Twisted Pair (STP) Cable
- Unshielded Twisted Pair (UTP) Cable

STP cables comes with twisted wire pair covered in metal foil. This makes it more indifferent to noise and crosstalk.

UTP has seven categories, each suitable for specific use. In computer networks, Cat-5, Cat-5e and Cat-6 cables are mostly used. UTP cables are connected by RJ45 connectors.

*Coaxial Cable*

Coaxial cables has two wires of copper. The core wire lies in center and is made of solid conductor. Core is enclosed in an insulating sheath. Over the sheath the second wire is wrapped around and that too in turn encased by insulator sheath. This all is covered by plastic cover.

Because of its structure coax cables are capable of carrying high frequency signals than that of twisted pair cables. The wrapped structure provides it a good shield against noise and cross talk. Coaxial cables provide high bandwidth rates of up to 450 mbps.

There are three categories of Coax cables namely, RG-59 (Cable TV), RG-58 (Thin Ethernet) and RG-11 (Thick Ethernet. RG stands for Radio Government.

Cables are connected using BNC connector and BNC-T. BNC terminator is used to terminate the wire at the far ends.

*Power Lines*

Power Line communication is Layer-1 (Physical Layer) technology which uses power cables to transmit data signals. Send in PLC modulates data and sent over the cables. The receiver on the other end de-modulates the data and interprets.

Because power lines are widely deployed, PLC can make all powered devices controlled and monitored. PLC works in half-duplex.

Two types of PLC exists:

- Narrow band PLC
- Broad band PLC

Narrow band PLC provides lower data rates up to 100s of kbps, as they work at lower frequencies (3-5000 kHz). But can be spread over several kilometers.

Broadband PLC provides higher data rates up to 100s of Mbps and works at higher frequencies (1.8 – 250 MHz). But cannot be much extended as Narrowband PLC.

*Fiber Optics*

Fiber Optic works on the properties of light. When light ray hits at critical angle it tends to refracts at 90 degree. This property has been used in fiber optic. The core of fiber optic cable is made of high quality glass or plastic. From one end of it light is emitted, it travels through it and at the other end light detector detects light stream and converts it to electric data form.

Fiber Optic provides the highest mode of speed. It comes in two modes, one is single mode fiber and second is multimode fiber. Single mode fiber can carries single ray of light whereas multimode is capable of carrying multiple beams of light.

**Ans. 5 a)** The electromagnetic (EM) spectrum is the range of all types of EM radiation. Radiation is energy that travels and spreads out as it goes – the visible light that comes from a lamp in your house and the radio waves that come from a radio station are two types of electromagnetic radiation. The other types of EM radiation that make up the electromagnetic spectrum are microwaves, infrared light,ultraviolet light, X-rays and gamma-rays.

You know more about the electromagnetic spectrum than you may think. The image below shows where you might encounter each portion of the EM spectrum in your day-to-day life.

Radio: Your radio captures radio waves emitted by radio stations, bringing your favorite tunes. Radio waves are also emitted by stars and gases in space.

Microwave: Microwave radiation will cook your popcorn in just a few minutes, but is also used by astronomers to learn about the structure of nearby galaxies.

Infrared: Night vision goggles pick up the infrared light emitted by our skin and objects with heat. In space, infrared light helps us map the dust between stars.

**5 b)** The data link layer is the protocol layer that transfers data between adjacent network nodes in a wide area network or between nodes on the same local area network segment.[1] The data link layer provides the functional and procedural means to transfer data between network entities and might provide the means to detect and possibly correct errors that may occur in the physical layer. Examples of data link protocols are Ethernet for local area networks (multi-node), the Point-to-Point Protocol (PPP), HDLC and ADCCP for point-to-point (dual-node) connections.

The data link layer is concerned with local delivery of frames between devices on the same LAN. Data-link frames, as these protocol data units are called, do not cross the boundaries of a local network. Inter-network

routing and global addressing are higher layer functions, allowing data-link protocols to focus on local delivery, addressing, and media arbitration. In this way, the data link layer is analogous to a neighborhood traffic cop; it endeavors to arbitrate between parties contending for access to a medium, without concern for their ultimate destination.

When devices attempt to use a medium simultaneously, frame collisions occur. Data-link protocols specify how devices detect and recover from such collisions, and may provide mechanisms to reduce or prevent them.

- Character count - Has general format of:

Count <Count Characters> Count <Count Characters> ...

to send the ASCII message "ABCDEFGHI" in three separate transmissions: 3ABC4DEFG3HI

The problem is that the message is transmitted in binary as (in hexadecimal): 034142430434454647034849 4A
An error of any type in the *Count* field (e.g. a single bit error changes $2_{10} = 00000010_2$ to $130_{10}=10000010_2$) can cause the receiver to lose count without hope of recovery.

- Character stuffing
- Special start/end characters can be used (e.g. STX to start and ETX to end a frame) but these characters cannot then occur in the message itself, only for framing.
- Character stuffing uses the special start/end characters for framing and allows those characters in the message also. The method is for the sender to *stuff* an extra special character whenever the start or end character occurs naturally so that within the message the special character always occurs in pairs. The receiver recognizes the single special character as start/end and removes from the message the first special character from pairs received.

Using the special character of <DEL> and <STX> and <ETX> for start/end framing, the message:

AB<DEL>C<STX><ETX>DE

would be sent as (stuffed characters are underlined):

<STX>AB<DEL><DEL>C<DEL><STX><DEL><ETX>DE<ETX>...<STX>

- If the receiver loses track it can wait for the next <STX> to locate the next frame. <DEL><STX> would be recognized as data since a <DEL> in data is stuffed as <DEL><DEL>. One problem is the dependency on use of the 8-bit ASCII code.

*How would the following data be sent using character stuffing?*

- *ABC*
- *<DEL><STX>A<DEL><ETX>*

- Bit stuffing - Similar to character stuffing except a special bit pattern used to flag framing (e.g. 111111 marks the start of a frame). If that pattern naturally occurs (e.g. the data contains 6 1's, 111111) the sender stuffs in a 0 after natural 5 1's (11111 becomes 111110). To the receiver all 111111 are framing and all 111110 should have the 0 removed to become 11111. As with character stuffing, on a framing error the receiver can wait for the next framing bits to locate the next frame.

**Ans. 6. a)** ALOHA: ALOHA is a system for coordinating and arbitrating access to a shared communication Networks channel. It was developed in the 1970s by Norman Abramson and his colleagues at the University of Hawaii. The original system used for ground based radio broadcasting, but the system has been implemented in satellite communication systems. shared communication system like ALOHA requires a method of handling collisions that occur when two or more systems attempt to transmit on the channel at the same time. In the ALOHA system, a node transmits whenever data is available to send. If another node transmits at the same time, a collision occurs, and the frames that were transmitted are lost. However, a node can listen to broadcasts on the medium, even its own, and determine whether the frames were transmitted.

Aloha means "Hello". Aloha is a multiple access protocol at the datalink layer and proposes how multiple terminals access the medium without interference or collision. In 1972 Roberts developed a protocol that would increase the capacity of aloha two fold. The Slotted Aloha protocol involves dividing the time interval into discrete slots and each slot interval corresponds to the time period of one frame. This method requires synchronization between the sending nodes to prevent collisions.

There are two different versior.s/types of ALOHA:

(i) PureALOHA
(ii) Slotted ALOHA

In pure ALOHA, the stations transmit frames whenever they have data to send.

• When two or more stations transmit simultaneously, there is collision and the frames are destroyed.

• In pure ALOHA, whenever any station transmits a frame, it expects the acknowledgement from the receiver.

• If acknowledgement is not received within specified time, the station assumes that the frame (or acknowledgement) has been destroyed.

• If the frame is destroyed because of collision the station waits for a random amount of time and sends it again. This waiting time must be random otherwise same frames will collide again and again.

• Therefore pure ALOHA dictates that when time-out period passes, each station must wait for a random amount of time before resending its frame. This randomness will help avoid more collisions.

Slotted ALOHA was invented to improve the efficiency of pure ALOHA as chances of collision in pure ALOHA are very high.

• In slotted ALOHA, the time of the shared channel is divided into discrete intervals called slots.

• The stations can send a frame only at the beginning of the slot and only one frame is sent in each slot.

Carrier Sense Multiple Access (CSMA) is a probabilistic Media Access Control (MAC) protocol in which a node verifies the absence of other trafficbefore transmitting on a shared transmission medium, such as an electrical bus, or a band of the electromagnetic spectrum.

"Carrier Sense" describes the fact that a transmitter uses feedback from a receiver that detects a carrier wave before trying to send. That is, it tries to detect the presence of an encoded signal from another station before attempting to transmit. If a carrier is sensed, the station waits for the transmission in progress to finish before initiating its own transmission.

"Multiple Access" describes the fact that multiple stations send and receive on the medium. Transmissions by one node are generally received by all other stations using the medium.

Types of CSMA

- 1-persistent CSMA

When the sender (station) is ready to transmit data, it checks if the physical medium is busy. If so, it senses the medium continually until it becomes idle, and then it transmits a piece of data (a frame). In case of a collision, the sender waits for a random period of time and attempts to transmit again.

- p-persistent CSMA

When the sender is ready to send data, it checks continually if the medium is busy. If the medium becomes idle, the sender transmits a frame with aprobability *p*. If the station chooses not to transmit (the probability of this event is *1-p*), the sender waits until the next available time slot and transmits again with the same probability *p*. This process repeats until the frame is sent or some other sender stops transmitting. In the latter case the sender monitors the channel, and when idle, transmits with a probability *p*, and so on.

- o-persistent CSMA

Each station is assigned a transmission order by a supervisor station. When medium goes idle, stations wait for their time slot in accordance with their assigned transmission order. The station assigned to transmit first transmits immediately. The station assigned to transmit second waits one time slot (but by that time the first station has already started transmitting). Stations monitor the medium for transmissions from other stations and update their assigned order with each detected transmission (i.e. they move one position closer to the front of the queue).

**6 b)**VLAN's allow a network manager to logically segment a LAN into different broadcast domains. Since this is a logical segmentation and not a physical one, workstations do not have to be physically located together. Users on different floors of the same building, or even in different buildings can now belong to the same LAN.

VLAN's offer a number of advantages over traditional LAN's. They are:

1) Performance

In networks where traffic consists of a high percentage of broadcasts and multicasts, VLAN's can reduce the need to send such traffic to unnecessary destinations. For example, in a broadcast domain consisting of 10 users, if the broadcast traffic is intended only for 5 of the users, then placing those 5 users on a separate VLAN can reduce traffic [ Passmore et al (3Com report)].

Compared to switches, routers require more processing of incoming traffic. As the volume of traffic passing through the routers increases, so does the latency in the routers, which results in reduced performance. The use of VLAN's reduces the number of routers needed, since VLAN's create broadcast domains using switches instead of routers.

2) Formation of Virtual Workgroups

Nowadays, it is common to find cross-functional product development teams with members from different departments such as marketing, sales, accounting, and research. These workgroups are usually formed for a short period of time. During this period, communication between members of the workgroup will be high. To contain broadcasts and multicasts within the workgroup, a VLAN can be set up for them. With VLAN's it is easier to place members of a workgroup together. Without VLAN's, the only way this would be possible is to physically move all the members of the workgroup closer together.

However, virtual workgroups do not come without problems. Consider the situation where one user of the workgroup is on the fourth floor of a building, and the other workgroup members are on the second floor. Resources such as a printer would be located on the second floor, which would be inconvenient for the lone fourth floor user.

Another problem with setting up virtual workgroups is the implementation of centralized server farms, which are essentially collections of servers and major resources for operating a network at a central location. The advantages here are numerous, since it is more efficient and cost-effective to provide better security, uninterrupted power supply, consolidated backup, and a proper operating environment in a single area than if the major resources were scattered in a building. Centralized server farms can cause problems when setting up virtual workgroups if servers cannot be placed on more than one VLAN. In such a case, the server would be placed on a single VLAN and all other VLAN's trying to access the server would have to go through a router; this can reduce performance [Netreference Inc. article].

3) Simplified Administration

Seventy percent of network costs are a result of adds, moves, and changes of users in the network. Every time a user is moved in a LAN, recabling, new station addressing, and reconfiguration of hubs and routers becomes necessary. Some of these tasks can be simplified with the use of VLAN's. If a user is moved within a VLAN, reconfiguration of routers is unnecessary. In addition, depending on the type of VLAN,

other administrative work can be reduced or eliminated. However the full power of VLAN's will only really be felt when good management tools are created which can allow network managers to drag and drop users into different VLAN's or to set up aliases.

Despite this saving, VLAN's add a layer of administrative complexity, since it now becomes necessary to manage virtual workgroups .

VLAN's can be used to create broadcast domains which eliminate the need for expensive routers.

5) Security

Periodically, sensitive data may be broadcast on a network. In such cases, placing only those users who can have access to that data on a VLAN can reduce the chances of an outsider gaining access to the data. VLAN's can also be used to control broadcast domains, set up firewalls, restrict access, and inform the network manager of an intrusion.

**Ans. 7.** Address Length

The most obvious difference is the increase in length of addresses, from 32 bits in IPv4 to 128 bits in IPv6. This increases the total address space size from $2^{32}$ (about 4.3 billion) to $2^{128}$ (about 340 trillion, trillion, trillion). It also doubles the size of the Packet Header, which adds 20 bytes of additional overhead on every packet.

External Data Representation

The next most obvious difference is IPv6's use of "coloned-hex" (e.g. 2001:470:20::2) for external data representation, instead of IPv4's "dotted-decimal" (e.g. 123.34.56.78).

Both IPv4 and IPv6 addresses are represented *internally* (in memory, or on the wire) as strings of bits (32 of them for IPv4, 128 of them for IPv6).

IPv4 addresses are represented *externally* with 4 fields of 8 bits each, using up to 3 decimal digits in each field (values 0 to 255). Fields are separated by dots ("."). Leading zeros can be suppressed in each field.

IPv6 addresses are represented *externally* with up to 8 fields of 16 bits each, using up to 4 hexadecimal digits in each field (values 0 to ffff). Fields are separated by colons (":"). Leading zeros can be suppressed in each field. At most one string of all-zero fields can be replaced by "::". In effect, everything to the left of the "::" is left justified in the 128 bits, everything to the right of it is right justified in the 128 bits. The extreme cases of this notation are the "unspecified address" (128 bits of 0), represented by "::", and the loopback address (127 bits of 0 followed by a single 1 bit), represented by "::1".

## Packet Header

Packet Headers are affixed to the beginning of all IP packets. You can think of them as being like "shipping labels" pasted on a package. A Packet Header contains a "from" address (where the packet is being sent from) called the *source address*; and a "to" address (where the packet is going) called the *destination address*. In the case of packets, these addresses are not "street" addresses, but IP addresses. On IPv4 packets, there is an IPv4 Packet Header. On IPv6 packets, there is an IPv6 Packet Header. These have the same purpose, but are fairly different due to improvements in the IPv6 protocol.

The IPv4 Packet Header is 20 bytes long (plus the length of the options field, if any). All but one bit of the first 20 bytes has long since been accounted for. There is no official Header Extension mechanism (although IPsec uses something similar). Some fields are used only in fragmented packets, but take up room on all packets.

## Address Resolution

IP "address resolution" involves mapping IP addresses to Link Layer addresses (e.g. MAC addresses). This must be done to get packets to the desired node over Ethernet.

IPv4 uses ARP, specified in RFC 826, "An Ethernet Address Resolution Protocol", November 1982. This protocol lives in the Link Layer. There is no way to secure it, so it is a favorite target of hackers, and there are many potent hacking attacks against it.

IPv6 uses Neighbor Discovery Address Resolution to map an IPv6 addresses onto a MAC address (or any Link Layer Address). This protocol lives in the Internet Layer, and you can protect it with IPsec AH and/or ESP if you desire (tunnel mode or transport mode). There is a secure version of Neighbor Discovery that provides an even better way to secure Address Resolution. This is specified in RFC 3971, "SEcure Neighbor Discovery (SEND)", March 2005. Unfortunately, Microsoft has not implemented this in any version of Windows, so it is not really usable in most networks. It is supported in both FreeBSD and Linux. SEND is fairly complicated to deploy, as it needs a working PKI (or equivalent) to create the necessary digital certificates.

## Transmission Modes

IPv4 Supports unicast (one-to-one), multicast (one-to-many subscribed), and broadcast (one-to-all) transmission modes. There are four IPv4 unicast scopes: node-local (loopback, 127.0.0.1), link-local (APIPA, 169.254.0.0/16), site-local (RFC 1918 private addresses) and global (all other IPv4 addresses not otherwise reserved).

IPv6 supports unicast (one-to-one), multicast (one-to-many subscribed) and anycast (one-to-closest-of-many) transmission modes. There is no broadcast mode in IPv6. There are four scopes for unicast addresses: interface-local (loopback), link-local (fe80::/64), site-local (ULA, fc00::/7) and global (2000::/3). The original site-local (fec0::/64) was deprecated.

Multicast Addresses

IPv4 uses "Class D" addresses (224.0.0.0 to 239.255.255.255) for multicast. This is a total of 268 million multicast addresses. Support for multicast is optional in IPv4 routers, so many do not support it. It usually works only within "walled gardens" where one entity owns and manages all of the routers.

IPv6 has strong support for multicast in all scopes. It uses the block ff00::/8. There are $2^{112}$ possible IPv6 multicast "groups". This is a total of 5.19E+33 multicast addresses. There are six multicast scopes: *interface-local* (loopback), *link-local*, *site-local*, *admin-local*, *organization-local* and *global*.
Multicast is used extensively in IPv6 mechanisms, such as Router Discovery and Stateless Address Autoconfiguration, so support is mandatory. The Multicast Listener Discovery Protocol (MLDv1 and MLDv2) are actually subsets of the ICMPv6 protocol. IPv6 multicast scales very well, potentially to the entire world.

IPsec

IPsec is short for Internet Protocol Security. It was originally created as a part of IPv6, but has been retrofitted (badly) into IPv4. It works OK in a private internet with no NAT, but it does not cross NAT very well. It uses something like a digital signature to detect changes to IP addresses or ports (in the header), which is exactly what NAT does. So, IPsec correctly identifies NAT as an attack. It is possible to use NAT traversal, such as STUN, to make IPsec work even through NAT, but that introduces more problems than IPsec solves in the first place. Because of this, IPsec is not widely used in IPv4.

IPsec works great in IPv6 because there is no NAT to break it.

IP Subnetting and CIDR

Because of the scarcity of IPv4 addresses, IPv4 had to use variable length masks and CIDR. This means that the split between the address prefix (or "network address") and the address suffix (or "interface identifier") can come at any point in the 32 bits (from bit 8 down to bit 30). This makes subnetting very complex in IPv4.

There is no scarcity of IPv6 addresses. Virtually all IPv6 subnets split the address prefix and address suffix at bit 64 (64 bit prefix and 64 bit suffix, or interface identifier). There is no subnetting required in the bottom 64 bits. There are some subnetting issues with managing the Subnet IDs if your IPv6 allocation is greater than one /64 block (e.g. a typical company allocation of a /48).

**Ans. 8. a)** The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermediainformation systems.[1] HTTP is the foundation of data communication for the World Wide Web.

Hypertext is structured text that uses logical links (hyperlinks) between nodes containing text. HTTP is the protocol to exchange or transfer hypertext.

The standards development of HTTP was coordinated by the Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C), culminating in the publication of a series of Requests for Comments (RFCs), most notablyRFC 2616 (June 1999), which defines HTTP/1.1, the version of HTTP in common use.

HTTP functions as a request-response protocol in the client-server computing model. A web browser, for example, may be the*client* and an application running on a computer hosting a web site may be the *server*. The client submits an HTTP *request*message to the server. The server, which provides *resources* such as HTML files and other content, or performs other functions on behalf of the client, returns a *response* message to the client. The response contains completion status information about the request and may also contain requested content in its message body.

A web browser is an example of a *user agent* (UA). Other types of user agent include the indexing software used by search providers (web crawlers), voice browsers, mobile apps and other software that accesses, consumes or displays web content.

HTTP is designed to permit intermediate network elements to improve or enable communications between clients and servers. High-traffic websites often benefit from web cache servers that deliver content on behalf of upstream servers to improve response time. Web browsers cache previously accessed web resources and reuse them when possible to reduce network traffic. HTTP proxy servers at private network boundaries can facilitate communication for clients without a globally routable address, by relaying messages with external servers.

**b)** Telnet is a network protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communication facility using a virtualterminal connection. User data is interspersed in-band with Telnet control information in an 8-bit byte oriented data connection over the Transmission Control Protocol (TCP).

Telnet was developed in 1969 beginning with RFC 15, extended in RFC 854, and standardized as Internet Engineering Task Force (IETF) Internet Standard STD 8, one of the first Internet standards.

Historically, Telnet provided access to a command-line interface (usually, of an operating system) on a remote host. Most network equipment and operating systemswith a TCP/IP stack support a Telnet service for remote configuration (including systems based on Windows NT). However, because of serious security issues when using Telnet over an open network such as the Internet, its use for this purpose has waned significantly[*citation needed*] in favor of SSH.

The term *telnet* may also refer to the software that implements the client part of the protocol. Telnet client applications are available for virtually all computer platforms. *Telnet* is also used as a verb. *To telnet* means to establish a connection with the Telnet protocol, either with command line client or with a programmatic interface. For example, a common directive might be: "*To change your password, telnet to the server, log in and run the passwd command.*" Most often, a user will be*telnetting* to a Unix-like server system or a network device (such as a router) and obtaining a login prompt to a command line text interface or a character-based full-screen manager.

Telnet is a client-server protocol, based on a reliable connection-oriented transport. Typically, this protocol is used to establish a connection to Transmission Control Protocol (TCP) port number 23, where a Telnet server application (telnetd) is listening. Telnet, however, predates TCP/IP and was originally run over Network Control Program (NCP) protocols.

**c)** The term *broadband* refers to the wide bandwidth characteristics of a transmission medium and its ability to transport multiple signals and traffic types simultaneously. The medium can be coax, optical fiber, twisted pair, DSL local telephone networks orwireless. In contrast, baseband describes a communication system in which information is transported across a single channel.[1]

Different criteria for "broad" have been applied in different contexts and at different times. Its origin is in physics, acoustics and radio systems engineering, where it had been used with a meaning similar to wideband.[2][3] Later, with the advent of digital telecommunications, the term was mainly used for transmission over multiple channels. Whereas a passband signal is also modulated so that it occupies higher frequencies (compared to a *baseband* signal which is bound to lowest end of spectrum, see line coding), it is still occupying a single channel. The key difference is that what is typically considered a *broadband signal* in this sense is a signal that occupies multiple (non-masking, orthogonal) passbands thus allowing for much higher throughput over a single medium, but with additional complexity in the transmitter/receiver circuitry. Finally, the term became popularized through the 1990s as a marketing term for Internet access that was faster than dialup access, the original Internet access technology, which was limited to 56 kbps. This meaning is only distantly related to its original technical meaning.

Broadband refers to a communication bandwidth of at least 256 kbit/s. Each channel is 4 MHz wide and it uses an extensive range of frequencies to effortlessly relay and receive data between networks.[4] In telecommunications, a broadband signaling method is one that handles a wide band of frequencies. *Broadband* is arelative term, understood according to its context. The wider (or broader) the bandwidth of a channel, the greater the information-carrying capacity, given the same channel quality.

In radio, for example, a very narrow-band will carry Morse code; a broader band will carry speech; a still broader band will carry music without losing the high audio frequencies required for realistic sound

reproduction. This broad band is often divided into channels or *frequency bins* using passband techniques to allowfrequency-division multiplexing, instead of sending a higher-quality signal.

A television antenna may be described as "broadband" because it is capable of receiving a wide range of channels; while a single-frequency or Lo-VHF antenna is "narrowband" since it receives only 1 to 5 channels. The US federal standard FS-1037C defines "broadband" as a synonym for wideband.[5]

In data communications a 56k modem will transmit a data rate of 56 kilobits per second (kbit/s) over a 4 kilohertz wide telephone line (narrowband or voiceband). The various forms of digital subscriber line (DSL) services are *broadband* in the sense that digital information is sent over multiple channels. Each channel is at higher frequency than the baseband voice channel, so it can support plain old telephone service on a single pair of wires at the same time.

Ans. 9 a) Integrated Services for Digital Network (ISDN) is a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network. It was first defined in 1988 in the CCITT red book.[1] Prior to ISDN, the telephone system was viewed as a way to transport voice, with some special services available for data. The key feature of ISDN is that it integrates speech and data on the same lines, adding features that were not available in the classic telephone system. There are several kinds of access interfaces to ISDN defined as Basic Rate Interface (BRI), Primary Rate Interface (PRI), Narrowband ISDN (N-ISDN), and Broadband ISDN (B-ISDN).

ISDN is a circuit-switched telephone network system, which also provides access to packet switched networks, designed to allow digital transmission of voice and dataover ordinary telephone copper wires, resulting in potentially better voice quality than an analog phone can provide. It offers circuit-switched connections (for either voice or data), and packet-switched connections (for data), in increments of 64 kilobit/s. A major market application for ISDN in some countries is Internet access, where ISDN typically provides a maximum of 128 kbit/s in both upstream and downstream directions. Channel bonding can achieve a greater data rate; typically the ISDN B-channels of three or four BRIs (six to eight 64 kbit/s channels) are bonded.

ISDN should not be mistaken for its use with a specific protocol, such as Q.931 where as ISDN is employed as the network, data-link and physical layers in the context of the OSI model. In a broad sense ISDN can be considered a suite of digital services existing on layers 1, 2, and 3 of the OSI model. ISDN is designed to provide access to voice and data services simultaneously.

However, common use reduced ISDN to be limited to Q.931 and related protocols, which are a set of protocols for establishing and breaking circuit switched connections, and for advanced calling features for the user. They were introduced in 1986.[2]

In a videoconference, ISDN provides simultaneous voice, video, and text transmission between individual desktop videoconferencing systems and group (room) videoconferencing systems.

b) Cryptography is the practice and study of techniques for secure communication in the presence of third parties (called adversaries).[2] More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries[3] and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation.[4] Modern cryptography intersects the disciplines of mathematics, computer science, andelectrical engineering. Applications of cryptography include ATM cards, computer passwords, andelectronic commerce.

Cryptography prior to the modern age was effectively synonymous with *encryption*, the conversion of information from a readable state to apparent nonsense. The originator of an encrypted message shared the decoding technique needed to recover the original information only with intended recipients, thereby precluding unwanted persons to do the same. Since World War I and the advent of the computer, the methods used to carry out cryptology have become increasingly complex and its application more widespread.

Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. It is theoretically possible to break such a system but it is infeasible to do so by any known practical means. These schemes are therefore termed computationally secure; theoretical advances, e.g., improvements in integer factorization algorithms, and faster computing technology require these solutions to be continually adapted. There exist information-theoretically secure schemes that provably cannot be broken even with unlimited computing power—an example is the one-time pad—but these schemes are more difficult to implement than the best theoretically breakable but computationally secure mechanisms.

c) An Internet service provider (ISP) is an organization that provides services for accessing, using, or participating in the Internet. Internet service providers may be organized in various forms, such as commercial, community-owned, non-profit, or otherwise privately owned.

Internet services typically provided by ISPs include Internet access, Internet transit, domain name registration, web hosting, colocation.

For a monthly fee, the service provider usually provides a software package, username, password and access phone number. Equipped with a modem, you can then log on to the Internet and browse the World Wide Web and USENET, and send and receive e-mail. For broadband access you typically receive the broadband modem hardware or pay a monthly fee for this equipment that is added to your ISP account billing.

In addition to serving individuals, ISPs also serve large companies, providing a direct connection from the company's networks to the Internet. ISPs themselves are connected to one another through Network Access Points (NAPs). ISPs may also be called IAPs (Internet Access Providers).