LAN & Networking

Sample Question Paper

Note: Attempt five Questions in all, Q.No. 1 is compulsory.

Q. 1. a). What is the use of Application layer in OSI Model. 2.5 X10

b) Explain Internet.

c). Differentiate between ALOHA and CSMA.

d). Explain Gigabit Ethernet.

e) Differentiate between hub and switch.

f) Explain Cryptography.

g) What is p-CSMA ?

h) What is encryption and decryption?

i) What is ISDN?

j)What is DNS?

Q. 2. Explain TCP/IP Model in detail. 12.5

Q 3. a) Differentiate between Twisted pair, coaxial cable and fiber optics. 6.5

b) Explain CSMA/ CD protocol in detail. 6

Q4. What is Ethernet ? Explain all 3 types of Ethernet in detail . 12.5

Q. 5. Write short notes on:

a) DSL 4

b)HTTP 4

c) SMTP, POP 4.5

Answers

Ans 1. a) In the Internet model, the **application layer** is an abstraction layer reserved for communications protocols and methods designed for process-to-process communications across an Internet Protocol (IP) computer network. Application layer protocols use the underlying transport layer protocols to establish process-to-process connections via ports.[1]

In the OSI model, the definition of its application layer is narrower in scope. The OSI model defines the application layer as being the user interface – responsible for displaying the information received to the user. The OSI application layer is responsible for displaying data and images to the user in a human-recognizable format and to interface with the presentation layer below it.

OSI separates functionality above the transport layer at two additional levels, the session layer and the presentation layer, specifying strict modular separation of functionality at these layers. It also provides protocol implementations for each layer.

b) 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.

c) **Aloha Protocol**

As mentioned earlier, Aloha is a simple communication protocol where each source in the network transmits data whenever it has a frame to be transmitted. If the frame is transmitted successfully, the next frame will be transmitted. If the transmission is failed, the source will send the same frame again. Aloha works well with wireless broadcast systems or half-duplex two-way links. But when the network becomes more complex, such as an Ethernet with multiple sources and destinations that uses a common data path, problems occur due to colliding of data frames. When the communication volume increases, the collision problem becomes worse. This can reduce the efficiency of a network since colliding frames will cause loss of data in both the frames. Slotted Aloha is an improvement to the original Aloha protocol, where discrete time slots were introduced to increase the maximum throughput while reducing collisions. This is achieved by allowing sources to transmit only at the beginning of a timeslot.

CSMA Protocol

CSMA protocol is a probabilistic MAC protocol in which a node verifies that the channel is free before transmitting on a shared channel such as an electrical bus. Before transmitting, the transmitter tries to detect whether there is a signal from another station in the channel. If a signal is detected, the transmitter waits until the ongoing transmission is finished before it starts to transmit again. This is the “Carrier Sense” part of the protocol. “Multiple Access” defines that multiple stations send and receive signals on the channel and a

transmission by a single node is generally received by all the other stations using the channel. Carrier Sense Multiple Access with Collision Detection (CSMA/CD) and Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) are two modifications of the CSMA protocol. CSMA/CD improves performance of CSMA by stopping a transmission as soon as a collision is detected and CSMA/CA improves the performance of CSMA by delaying the transmission by a random interval if the channel is sensed busy.

Difference between CSMA and ALOHA

Main difference between Aloha and CSMA is that Aloha protocol does not try to detect whether the channel is free before transmitting but the CSMA protocol verifies that the channel is free before transmitting data. Thus CSMA protocol avoids clashes before they happen while Aloha protocol detects that a channel is busy only after a clash happens. Due to this, CSMA is more suitable for networks such as Ethernet where multiple sources and destinations use the same channel.

d) **Gigabit Ethernet** is part of the family of Ethernet computer networking and communication standards. The Gigabit Ethernet standard supports a theoretical maximum data rate of 1 gigabit per second (Gbps) (1000 Mbps).

When first developed, some thought achieving gigabit speeds with Ethernet would require using fiber optic or other special cables. However, today's Gigabit Ethernet works using twisted pair copper cable (specifically, the *CAT5e* and CAT6 cabling standards) similar to older 100 Mbps Fast Ethernet (that works over CAT5 cables).

Newer home broadband routers now support Gigabit Ethernet along with other mainstream computer network equipment. Gigabit Ethernet also provides backward compatibility to older 100 Mbps and 10 Mbps legacy Ethernet devices: Connections to these devices function normally but perform at the lower speed.

Also Known As: 1000 Mbps Ethernet

e) A **Hub** is a networking device that allows one to connect multiple PCs to a single network. Hubs may be based on Ethernet, Firewire, or USB connections. A**switch** is a control unit that turns the flow of electricity on or of in a circuit. It may also be used to route information patterns in streaming electronic data sent over networks. In the context of a network, a switch is a computer networking device that connects network segments. A switch is used to connect various network segments. A network switch is a small hardwaredevice that joins multiple computers together within one local area network (LAN).

A Hub connects multiple Ethernet devices together, making them act as a single segment.

f) The art of protecting information by transforming it (*encrypting* it) into an unreadable format, called cipher text. Only those who possess a secret *key* can decipher (or *decrypt*) the message intoplain text. Encrypted messages can sometimes be broken by cryptanalysis, also called *codebreaking*, although modern cryptography techniques are virtually unbreakable.

As the Internet and other forms of electronic communication become more prevalent, electronic security is becoming increasingly important. Cryptography is used to protect e-mail messages, credit card information, and corporate data. One of the most popular cryptography systems used on the Internet is *Pretty Good Privacy*because it's effective and free.

Cryptography systems can be broadly classified into symmetric-key systems that use a single key that both the sender and recipient have, and *public-key*systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses.

g) This is a sort of trade-off between 1 and non-persistent CSMA access modes. 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 a probability *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 starts transmitting. In the latter case the sender monitors the channel, and when idle, transmits with a probability *p*, and so on. p-persistent CSMA is used in CSMA/CA systems including Wi-Fi and other packet radio systems.

h) Encryption is the conversion of data into a form, called a ciphertext, that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood.

The use of encryption/decryption is as old as the art of communication. In wartime, a cipher, often incorrectly called a code, can be employed to keep the enemy from obtaining the contents of transmissions. (Technically, a code is a means of representing a signal without the intent of keeping it secret; examples are Morse code and ASCII.) Simple ciphers include the substitution of letters for numbers, the rotation of letters in the alphabet, and the "scrambling" of voice signals by inverting the sideband frequencies. More complex ciphers work according to sophisticated computer algorithms that rearrange the data bits in digital signals.

In order to easily recover the contents of an encrypted signal, the correct decryption key is required. The key is an algorithm that undoes the work of the encryption algorithm. Alternatively, a computer can be used in an attempt to break the cipher. The more complex the encryption algorithm, the more difficult it becomes to eavesdrop on the communications without access to the key.

i) ISDN (Integrated Services Digital Network) is a set of CCITT/ITU standards for digital transmission over ordinary telephone copper wire as well as over other media. Home and business users who install an ISDN adapter (in place of a telephone modem) receive Web pages at up to 128 Kbps compared with the maximum 56 Kbps rate of a modem connection. ISDN requires adapters at both ends of the transmission so your access provider also needs an ISDN adapter. ISDN is generally available from your phone company in most urban areas in the United States and Europe. In many areas where DSL and cable modem service are now offered, ISDN is no longer as popular an option as it was formerly.

There are two levels of service: the Basic Rate Interface (BRI), intended for the home and small enterprise, and the Primary Rate Interface (PRI), for larger users. Both rates include a number of B-channels and a D-channels. Each B-channel carries data, voice, and other services. Each D-channel carries control and signaling information.

The Basic Rate Interface consists of two 64 Kbps B-channels and one 16 Kbps D- channel. Thus, a Basic Rate user can have up to 128 Kbps service. The Primary Rate consists of 23 B-channels and one 64 Kpbs D-channel in the United States or 30 B-channels and 1 D-channel in Europe.

j) The **Domain Name System** (**DNS**) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates easily memorized domain names to the numerical IP addressesneeded for the purpose of locating computer services and devices worldwide. The Domain Name System is an essential component of the functionality of the Internet.

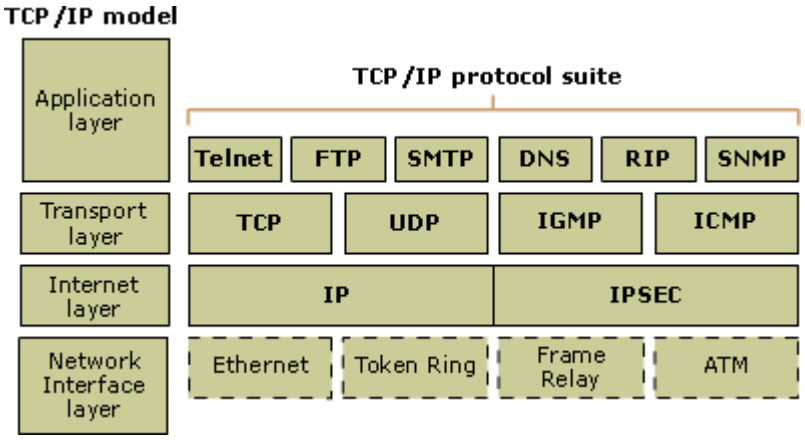
An often-used analogy to explain the Domain Name System is that it serves as the phone book for the Internet by translating human-friendly computer hostnames into IP addresses. For example, the domain name www.example.comtranslates to the addresses 93.184.216.119 (IPv4) and 2606:2800:220:6d:26bf:1447:1097:aa7 (IPv6). Unlike a phone book, the DNS can be quickly updated, allowing a service's location on the network to change without affecting the end users, who continue to use the same host name. Users take advantage of this when they use meaningful Uniform Resource Locators (URLs), and e-mail addresses without having to know how the computer actually locates the services.

The Domain Name System distributes the responsibility of assigning domain names and mapping those names to IP addresses by designating authoritative name servers for each domain. Authoritative name servers are assigned to be responsible for their supported domains, and may delegate authority over subdomains to other name servers. This mechanism provides distributed and fault tolerant service and was designed to avoid the need for a single central database.

Ans. 2. 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 3. a) Coaxial Cables

First invented in the 1880s, "coax" was best known as the kind of cable that connected television sets to home antennas. Coaxial cable is also a standard for 10 Mbps Ethernet cables. When 10 Mbps Ethernet was most popular, during the 1980s and early 1990s, networks typically utilized one of two kinds of coax cable - *thinnet* (10BASE2 standard) or *thicknet*(10BASE5). These cables consist of an inner copper wire of varying thickness surrounded by insulation and other shielding. Their stiffness caused network administrators difficulty in installing and maintaining thinnet and thicknet.

Twisted Pair Cables

Twisted pair eventually emerged during the 1990s as the leading cabling standard for Ethernet, starting with 10 Mbps (10BASE-T, also known as Category 3 or Cat3), later followed by improved versions for 100 Mbps (100BASE-TX, Cat5 and Cat5e) and successively higher speeds up to 10 Gbps (10GBASE-T). Ethernet twisted pair cables contain up to 8 wires wound together in pairs to minimize electromagnetic interference.

Two primary types of twisted pair cable industry standards are defined – Unshielded Twisted Pair (UTP) and Shielded Twisted Pair (STP). Modern Ethernet cables use UTP wiring due to its lower cost, while STP cabling can be found in some other types of networks such as *FDDI*.

Fiber Optics

Instead of insulated metal wires transmitting electrical signals, fiber optic network cables work using strands of glass and pulses of light. These network cables are bendable despite being made of glass. They have proven especially useful in wide area network (WANs) installations where long distance underground or outdoor cable runs are required and also in office buildings where a high volume of communication traffic is common.
Two primary types of fiber optic cable industry standards are defined – single-mode (100BaseBX standard) and multimode (100BaseSX standard). Long-distance telecommunications networks more commonly use single-mode for its relatively higherbandwidth capacity, while local networks typically use multimode instead due to its lower cost.

3 b) CSMA/CD (**Carrier Sense Multiple Access/Collision Detection**) is the protocol used in Ethernet networks to ensure that only one network node is transmitting on the network wire at any one time.

- CSMA/CD is a type of **contention protocol**.
- CSMA/CD is a set of rules determining how network devices respond when two devices attempt to use a data channel simultaneously (called a collision). Standard Ethernet networks use CSMS/CD to physically monitor the traffic on the line at participating stations. If no transmission is taking place at the time, the particular station can transmit. If two stations attempt to transmit simultaneously, this causes a collision, which is detected by all participating stations. After a random time interval, the stations that collided attempt to transmit again. If another collision occurs, the time intervals from which the random waiting time is selected are increased step by step. This is known as exponential back off.

Carrier Sense à means that every Ethernet device listens to the Ethernet wire before it attempts to transmit. If the Ethernet device senses that another device is transmitting, it will wait to transmit.
Multiple Access à means that more than one Ethernet device can be sensing (listening and waiting to transmit) at a time.
Collision Detection à means that when multiple Ethernet devices accidentally transmit at the same time, they are able to detect this error.

How collisions occur under CSMA/CD

Imagine a very simple Ethernet network with only two nodes. Each node, independently, decides to send an Ethernet frame to the other node. Both nodes listen to the Ethernet wire and sense that no carrier is present. Both nodes transmit simultaneously, causing a collision. Both nodes detect the collision and each node waits a random amount of time before transmitting again. Collisions are normal on an Ethernet network. A small amount of collisions are expected in the protocol design. If too many nodes are transmitting on an Ethernet network the number of collisions can rise to an unacceptable level. This can reduce the amount of available bandwidth on an Ethernet network because so much bandwidth is lost in retransmission. Ethernet switches greatly reduce the already minor difficulties experienced with the CSMA/CD protocol.

Ans. 4 Anyone who has plugged their computer into a broadband Internet connection such as cable or DSL has used an Ethernet cable. Ethernet cables are the standard cables commonly used to connect a modem to a router, and, likewise, to connect a router to a computer's network interface card (NIC). These thick, flexible cables are all practically indistinguishable to the untrained eye, but not all Ethernet cables are the same.

Ethernet cables have been evolving since the beginning of the Ethernet standard in 1985. Many different categories of Ethernet cable have been developed, and each category has different specifications as far as shielding from electromagnetic interference, data transmission speed, and the possible bandwidth frequency range required to achieve that speed. It is understandable that some confusion can arise when looking at all the available options for Ethernet cabling. Luckily, the category of cable is usually clearly printed on the cable's sheath, so there can be no doubt as to the type of cable being used. There are also certain types of cables recognized as common industry standards. This guide will describe a few of the most common categories of Ethernet cable that are used in modern networks.

Category 3

Category 3 Ethernet cable, also known as Cat 3 or station wire, is one of the oldest forms of Ethernet cable still in use today. It is an unshielded twisted pair (UTP) cable that is capable of carrying 10 megabits per second (Mbps) of data or voice transmissions. Its maximum possible bandwidth is 16 MHz. Cat 3 cable reached the peak of its popularity in the early 1990s, as it was then the industry standard for computer networks. With the debut of the faster Category 5 cable, however, Cat 3 fell out of favor. It still can be seen in use in two-line telephone systems and older 10BASE-T Ethernet installations.

Category 5

Category 5 (Cat 5) Ethernet cable is the successor to the earlier Category 3. Like Cat 3, it is a UTP cable, but it is able to carry data at a higher transfer rate. Cat 5 cables introduced the 10/100Mbps speed to the Ethernet,

which means that the cables can support either 10 Mbps or 100 Mbps speeds. A 100 Mbps speed is also known as Fast Ethernet, and Cat 5 cables were the first Fast Ethernet-capable cables to be introduced. They also can be used for telephone signals and video, in addition to Ethernet data. This category has been superseded by the newer Category 5e cables.

Category 5e

The Category 5 e standard is an enhanced version of Cat 5 cable, which is optimized to reduce crosstalk, or the unwanted transmission of signals between data channels. This category works for 10/100 Mbps and 1000 Mbps (Gigabit) Ethernet, and it has become the most widely used category of Ethernet cable available on the market. While Cat 5 is common in existing installations, Cat 5e has completely replaced it in new installations. While both Cat 5 and Cat 5e cables contain four twisted pairs of wires, Cat 5 only utilizes two of these pairs for Fast Ethernet, while Cat 5e uses all four, enabling Gigabit Ethernet speeds. Bandwidth is also increased with Cat 5e cables, which can support a maximum bandwidth of 100 MHz. Cat 5e cables are backward compatible with Cat 5 cables, and can be used in any modern network installation.

Category 6

One of the major differences between Category 5e and the newer Category 6 is in transmission performance. While Cat 5e cables can handle Gigabit Ethernet speeds, Cat 6 cables are certified to handle Gigabit Ethernet with a bandwidth of up to 250 MHz. Cat 6 cables have several improvements, including better insulation and thinner wires, that provide a higher signal-to-noise ratio, and are better suited for environments in which there may be higher electromagnetic interference. Some Cat 6 cables are available in shielded twisted pair (STP) forms or UTP forms. However, for most applications, Cat 5e cable is adequate for gigabit Ethernet, and it is much less expensive than Cat 6 cable. Cat 6 cable is also backwards compatible with Cat 5 and 5e cables.

Category 6a

Category 6 a cable, or augmented Category 6 cable, improves upon the basic Cat 6 cable by allowing 10,000 Mbps data transmission rates and effectively doubling the maximum bandwidth to 500 MHz. Category 6a cables are usually available in STP form, and, as a result, must have specialized connectors that ground the cable.

Category 7

Category 7 cable, also known as Class F, is a fully shielded cable that supports speeds of up to 10 Gbps (10,000 Mbps) and bandwidths of up to 600 Mhz. Cat 7 cables consist of a screened, shielded twisted pair (SSTP) of wires, and the layers of insulation and shielding contained within them are even more extensive than that of Cat 6 cables. Because of this shielding, they are thicker, more bulky, and more difficult to bend. Additionally, each of the shielding layers must be grounded, or else performance may be reduced to the point that there will be no improvement over Cat 6, and performance may be worse than Cat 5. For this reason, it’s very important to understand the type of connectors at the ends of a Cat 7 cable.

The following table summarizes the most common types of Ethernet cables, including their maximum data transmission speeds and maximum bandwidths.

Ans. 5. a) Digital subscriber line (**DSL**, originally **digital subscriber loop**) is a family of technologies that provide Internet access by transmitting digital data over the wires of a local telephone network. In telecommunications marketing, the term DSL is widely understood to mean asymmetric digital subscriber line (ADSL), the most commonly installed DSL technology. DSL service is delivered simultaneously with wired telephone service on the same telephone line. This is possible because DSL uses higher frequency bands for data. On the customer premises, a DSL filter on each non-DSL outlet blocks any high frequency interference, to enable simultaneous use of the voice and DSL services.

The bit rate of consumer DSL services typically ranges from 256 kbit/s to over 100 Mbit/s in the direction to the customer (downstream), depending on DSL technology, line conditions, and service-level implementation. Bit rates of 1 Gbit/s have been reached in trials.[1] In ADSL, the data throughput in the upstreamdirection, (the direction to the service provider) is lower, hence the designation of *asymmetric* service. In symmetric digital subscriber line (SDSL) services, the downstream and upstream data rates are equal.

A 2007 book described DSL as "the most globally prolific broadband access technology, yet it is only available to around 60–75 percent of the population in many developed countries.

b) 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.

c)**Simple Mail Transfer Protocol** (**SMTP**) is an Internet standard for electronic mail (e-mail) transmission. First defined by RFC 821 in 1982, it was last updated in 2008 with the Extended SMTP additions by RFC 5321 - which is the protocol in widespread use today.

SMTP by default uses TCP port 25. The protocol for mail submission is the same, but uses port 587. SMTP connections secured by SSL, known as SMTPS, default to port 465.

While electronic mail servers and other mail transfer agents use SMTP to send and receive mail messages, user-level client mail applications typically use SMTP only for sending messages to a mail server for relaying. For receiving messages, client applications usually use either the POP3 or the IMAP.

While proprietary systems (such as Microsoft Exchange and Lotus Notes/Domino) and webmail systems (such asHotmail, Gmail and Yahoo! Mail) use their own non-standard protocols to access mail box accounts on their own mail servers, all use SMTP when sending or receiving email from outside their own systems.

In computing, the **Post Office Protocol** (**POP**) is an application-layer Internet standard protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection.[1] POP has been developed through several versions, with version 3 (**POP3**) being the current standard.

Virtually all modern e-mail clients and servers support POP3, and it along with IMAP (Internet Message Access Protocol) are the two most prevalent Internet standard protocols for e-mail retrieval,[2] with many webmail service providers such as Google Mail, Microsoft Mail and Yahoo! Mail also providing support for either IMAP or POP3 to allow mail to be downloaded.

POP supports simple download-and-delete requirements for access to remote mailboxes (termed maildrop in the POPRFC's).[3] Although most POP clients have an option to leave mail on server after download, e-mail clients using POP generally connect, retrieve all messages, store them on the user's PC as new messages, delete them from the server, and then disconnect. Other protocols, notably IMAP, (Internet Message Access Protocol) provide more complete and complex remote access to typical mailbox operations. Many e-mail clients support POP as well as IMAP to retrieve messages; however, fewer Internet Service Providers (ISPs)