**CHAPTER 1**

#1: Two companies are considering pooling their resources to form a joint venture. The CEO

of the first company meets with his legal team, and the legal team consults a number of middle managers in the proposed product area. Meanwhile, the CEO of the first company sends an e-mail to the CEO of the second company to offer a couple of suggestions concerning the joint venture. Does this scenario follow either the TCP/IP protocol suite or the OSI model? Explain your answer.

Ans: This follows TCP/IP protocol suite and does not follow the OSI model as all the physical communications are happening through the lowest layer and Upper layers do not communicate directly.

#2: List the TCP! IP protocol suite layer that performs each of the following functions:

a. data compression

b. multiplexing

c. routing

d. definition of a signal's electrical characteristics

e. e-mail

f. error detection

g. end-to-end flow control

Ans: TCP/IP answers are:

a. Application

b. Network access, transport

c. Network

d. Network access

e. Application

f. Network access, transport

g. Transport

#3: For each function in the previous exercise, list the OSI layer that performs that function.

Ans: OSI answers are:

a. Presentation

b. Physical, transport

c. Network

d. Physical

e. Application

f. Data link, transport

g. Transport

#4: You have been asked to create a new network architecture model. Will it be layered, or will its components take some other form? Show your model's layers or its new form, and describe the functions performed by each of its components.

If am asked to design and create a new network architecture model, then it will be a layered architecture and I will use OSI model for this.

Application Layer – This layer is used by Network applications that is the ones that use internet like Google Chrome, Mozilla Firefox, Outlook and Skype. These are the applications that are running in the PC and uses application layer protocols like HTTP or HTTPs to do web surfing, FTP for File transfers, SMTP for emails and Telnet for virtual terminals. Not only Web browsers but other network applications are dependent on application layer protocols to function.

Presentation Layer: This layer receives the data from application layer in the form of characters and numbers and converts the data to machine understandable binary format by translating and data compressing. To maintain the integrity data is encrypted before transmission. At the receiver level it is decrypted.

Session Layer: This layer in my model will help in setting up and managing connections, enabling, sending and receiving of data followed by termination of session and connection. Upon authentication a connection is established and then authorization is checked. On requesting a website in the web browser, it opens a separate session and downloads text and data files and are received in the form of data packets. This layer will also help in managing the session.

Web browser performs all the function of the above three layers.

Transport Layer: This layer will control the reliability of communication through segmentation, flow control and error control. Data received is divided into small data units called segments where each segment contains port and sequence number. Under flow control transport layer controls the amount of data to be transmitter. This layer recovers the missing data using automatic repeat request. Two types of services are available: Connection oriented and connectionless.

Network Layer: Data segments are transmitted to the network layer. This will work for the transmission of the received segments from one computer to another located in different networks. Routers reside in this layer. There are three functions performed by this layer that is logical addressing, routing and path determination. Data units are called packets which is comprised of sender and receivers IP addresses to assure each data packet reaches the correct destination.

Data Link Layer: Data packet is received. Logical addressing is done at network layer whereas physical addressing happens at data link layer to form a Frame. Error detection is also handled in this layer.

Physical Layer: this layer converts the binary sequence into signals and transmit over local media. Finally, data is moved to application layer. Application layer protocol makes the senders message visible in the application at the receiver’s end.

**CHAPTER 2**

#1: What is the difference between data and signals?

Data are the entities that convey meaning and signals are the electric or electromagnetic encoding of data.

#2: A signal starts at point X. As it travels to point Y, it loses 8 dB. At point Y, the signal is boosted by 10 dB. As the signal travels to point Z, it loses 7 dB. What is the dB strength of the signal atpoint Z?

-8 dB + 10 dB + (-7 dB) = -5dB

-5 dB

#3: What is the decibel loss of a signal that loses half its power during the course of transmission?

dB = 10 log10 (P2 / P1)

dB = 10 log10 (5/10)

dB = 10 log10 (0.5)

dB = 10 (-0.3)

dB = -3 dB

log10

-3db

#4: Can modems and codecs be used interchangeably? Defend your position. (The modem converts digital data to analog signals and back to digital data; the codec converts analog data to digital signals and back to analog data.}

**Codec** is Coder-Decoder. Codec is the device which converts analog data to digital data and back. At the transmit end it converts analog data into digital coded form and at the receiver it converts the digital coded data to its original analog form.  
For example, analog audio tones.

**modem** is modulator-demodulator. Modem is the device which modulates baseband information at transmit end and demodulates modulated signal at the receive end.

No, they cannot. Modems input digital data and produce analog signals, while codecs input analog data and produce digital signals.

**CHAPTER 3**

#1 What are the advantages and disadvantages of shielded twisted pair?

Shielded twisted Pair is a copper telephone wiring used in business installations. It is like unshielded twisted pair but in addition has a shielding around the cable to protect it from external interference.

**Advantages:**

1. It provides protection from interference and reduces chances of crosstalk.
2. Easily terminated with modular connector**.**
3. Better electrical characteristics.

**Disadvantages:**

1. Cost is high.
2. Not much improvement in the length of segment despite being thick and heavy.
3. Picks unwanted signals if shields of the cable not grounded properly.
4. Diameter and weight of the cable is increased due to shielding and becomes difficult to install in narrow cable ducts due to the thickness of the cable.

#2 What is meant by right-of-way?

Right of way is "**the legal right**, established by usage or grant, to pass along a specific route through grounds or property belonging to another", or "a path or thoroughfare subject to such a right". For eg. A footpath is a right of way that can only be used by pedestrians.

With regards to conducted media, **Right-of-way** is the legal capability of a business or a person to install a wire or cable across someone else's property. If a business wants to install a conducted medium between two buildings, and the business does not own the property in between the buildings, the business must receive the right-of-way from the owner of the in-between property.

#3: The local cable TV company is considering removing all the coaxial cable and replacing it with fiber-optic cable. List the advantages and disadvantages of this plan.

Fiber-optic cables have both advantages and disadvantages. The advantages over a coaxial cable is

1. Greater Bandwidth – Fiber optic cables provides more bandwidth for carrying more data.
2. Faster speeds – Faster than Cat5 or Cat 6 copper cables.
3. Longer Distances – Can carry signals farther than 328-foot limitation of copper cables.
4. Thinner and sturdier construction – Thinner and lighter in weight.
5. Better reliability – Immune to weather changes, also it does not carry electric current so no interruption during data transmission by electromagnetic interference.

Disadvantages:

1. The optical fibers are difficult to splice, and there is loss of the light in the fiber due to scattering.
2. Not as robust as the wires and are expensive to install.
3. The fiber optic cable is a small and compact cable, and it is highly susceptible to becoming cut or damaged during installation or construction activities.
4. The fibers can be broken or have transmission losses when wrapped around curves.

#4 You are sitting at your desk at work, using your laptop computer. The boss calls an emergency meeting for you and several coworkers and asks everyone to bring his or her laptop computer. When you get to the meeting room, the boss wants to download an important file from his laptop to all your coworkers' laptops. List three possible media solutions that will support this download, along with their advantages and disadvantages.

The three possible media solution that supports this download are:

Infrared, Bluetooth and WLAN (Wireless Local Area Network)

Advantages of Infrared:

1. Reliable.
2. Covers a wide range of area without any faults.
3. The devices used for the implementation of infrared wireless technology is cheaper.
4. Consumes much less power and are more compact.

Disadvantages of Infrared:

1. Not all devices are compatible of receiving the signal produced by it.
2. Devices need to be in stable position during the transmission.
3. Speed at which the data is transmitted is slower than wired transmission.
4. Signal can be blocked by any foreign material that is in front of the transmission.

Advantages of Bluetooth:

1. Avoids interference from other wireless devices.
2. Lower power consumption.
3. It has range better than infrared communication.
4. Bluetooth devices are available at very cheap cost.
5. No line of sight.

Disadvantages of Bluetooth:

1. It can loose connection in certain conditions.
2. Low bandwidth as compared to Wi-Fi
3. Security is a very key aspect as it can be hacked.
4. Allows only short-range communication between devices.

Advantages of WLAN:

1. Mobility.
2. High data rate, as coverage area is small.
3. Fast, easy and flexible.
4. Cost is average, lower than the cost of wired LAN.
5. Signal is not blocked by any other objects.

Disadvantages of WLAN:

1. This communication is prone to interference and noise.
2. It has limited coverage area.
3. Communication is not very secure and unauthorized access is common.

**CHAPTER 4**

**#1** What are the four components of an interface?

electrical, mechanical, functional, and procedural

* + Electrical component: deals with voltages, line capacitance, and other electrical characteristics
  + Mechanical component: deals with items such as the connector or plug description
  + Functional component: describes the function of each pin or circuit that is used in a particular interface
  + Procedural component: describes how the particular circuits are used to perform an operation

**#2** What is the difference between half-duplex and full-duplex communications?

* A *full-duplex* connection transmits data in both directions and at the same time
* A *half-duplex* connection transmits data in both directions but in only one direction at a time.

**#3** If I have a device that has a Universal Serial Bus 3.0 interface, but my computer only has a Universal Serial Bus 2.0 connector, is my device going to work? Explain why or why not.

Yes, device will work but the USB 3.0 interface will come down to the slower interface speed of USB 2.0.

**#4** How does the isochronous connection compare to the asynchronous and synchronous connections? Compare the applications and efficiencies of all three

Synchronous: Each basic unit of data in a synchronous data stream must be transferred in sync with a clock signal. Clock signal provides the control signals for the data. During the synchronous data transfer, due to the error detection mechanism data can be resent if an error is detected.

Eg.: GSM audio, TWI (clock pulse)

Asynchronous: In the data transfer, data can be sent at random intervals and the data rate need not be constant. These transfers use a start bit to signal the beginning of the data transmission and stop bit to signal the end of data transmission. Data can be resent with the help of error detection mechanism if any error detected.

Eg.: RS-232, RS-422, RS-485.

Isochronous: An isochronous data transfer system combines the features of an asynchronous and synchronous data transfer system. It sends blocks of data over a Synchronous transmission system. To transmit data each data source is given a fixed interval of time in that it can transfer data at whatever intervals. If the data requires more time than allotted to transmit it sends the remaining data in next turn or if the data requires less time than given time, then it stays idle for some time and then sends it over. There is no error detection mechanism so not possible to resend the data upon error due to strict timing conditions.

This is commonly used for streaming video or voice, where data must be delivered within certain time constraints.

Eg.: USB, Firewire.

These three can be explained with an example:

Synchronous: If having food is data transfer and you don’t know how to cook and totally depend on other person to cook for you then transfer of this data is synchronous to the other person who cooks.

Asynchronous: In the same example, this time you know cooking and the data transfer is not dependent and is asynchronous.

Isochronous: this time you know how to cook, and you also live with the other person who cooks so either you cook or the other person depending on need. Data transfer is isochronous.

**CHAPTER 5**

#1: Compared to the other multiplexing techniques, state two advantages and two disadvantages of each of the following:

a. frequency division multiplexing

b. synchronous time division multiplexing

c. statistical time division multiplexing

d. wavelength division multiplexing

1. Frequency division multiplexing

Advantages:

1. It does not need synchronization between its transmitter and receiver.
2. Simple and Popular with radio, TV, cable TV
3. Due to slow narrow band fading only one channel gets affected.
4. It is used for analog signals and all the receivers, such as cellular phones, do not need to be at the same location
5. Many signals (channels) can be transmitted simultaneously.

Disadvantages:

1. It suffers problem of crosstalk that is noise problems with analog signals.
2. Potentially wastes bandwidth
3. Limited by frequency ranges
4. synchronous time division multiplexing

Advantages:

1. Digital signals
2. Relatively straight-forward
3. Commonly used with T-1, SONET.

Disadvantages:

1. Potentially wastes bandwidth
2. statistical time division multiplexing

Advantages:

1. More efficient use of bandwidth
2. Frame can contain control and error information
3. Packets can be of varying size

Disadvantages:

1. More complex than synchronous time division multiplexing
2. wavelength division multiplexing

Advantages:

1. Full duplex transmission is possible.
2. Very high capacities over fiber
3. It provides higher bandwidth.
4. Signals can have varying speeds
5. High security and scalable

Disadvantages:

1. Signals cannot be very close.
2. Cost of system increases with addition of optical components.
3. Complexity

#2: The telephone company has a fiber-optic line with time division multiplexing that runs from the United States to England and lies on the ocean floor. This fiber-optic line has reached capacity. What alternatives can the telephone company consider to increase capacity?

Alternative could be wavelength division multiplexing to increase the capacity.

#3: Is the form of DSL that a company uses different from the form of DSL to which a home user subscribes? Explain.

Yes. The one that company uses is quite fast and is mostly of type symmetric.

#4: Can you compress a set of bank statements using JPEG compression? Explain.

It can be compressed but not preferred as it is a lossy compression and you might lose data. It is mostly used to compress multimedia data like audio, video and images.

**CHAPTER 6**

#1: Which type of noise is the most difficult to remove from an analog signal? Why?

Impulse is a type of noise that is most difficult to remove from an analog signal, because it is noncontinuous and appears as an analog waveform, which makes it difficult to separate from the analog waveform of the data.

#2: Which type of noise is the most difficult to remove from a digital signal? Why?

Jitter is a type of noise which is most difficult to remove from a digital signal, regeneration of the signal, which reduces other forms of noise, can increase the amount of jitter.

#3: In a Stop-and-wait error-control system, Station A sends packet 0, and it is lost. What happens next?

Then Station B responds with a NAK

#4: In a Stop-and-wait error-control system, Station A sends packet 0, it arrives without error, and an ACK is returned, but the ACK is lost. What happens next?

After a timeout, Station A will retransmit packet 0.

#5: In a sliding window error-control system in which each packet is numbered, Station A sends packets 4, 5, 6, and 7. Station B receives them and wants to acknowledge all of them. What does Station B send back to Station A?

An ACK with the number of the next packet is expected.

#6: In a sliding window error-control system, Station A sends a packet with bytes 501- 700, followed immediately by a packet with bytes 701- 900. Create a diagram of this error-control scenario, and show the response(s) that Station B will send if both packets arrive, but there is a checksum error in the second packet.

Receiver waits for 500 ms for the second packet to arrive. Since it doesn’t arrive , the receiver returns an ACK with value 701.

#7: In a sliding window error-control system, Station A sends three packets with bytes ~100, 101- 200, and 201- 300, respectively. The second packet with bytes 101-200 is held up somewhere in the network long enough that the third packet arrives before the second one. Create a diagram of this error-control scenario, and show the response(s) that Station B will send. Now assume that five seconds after Station B responds, the second packet shows up. What does Station B do now?

Receiver sends an ACK with value 101 and buffers packet 201-300. When packet with bytes 101-200 arrives, it is inserted into stream. If packet with bytes 201-300 shows up, it is tossed.

#8: Is Stop-and-wait error control a half-duplex protocol or a full-duplex protocol? Explain your response.

It is Half-duplex because communication is happening but not simultaneously. It is one direction at a time.

**CHAPTER 7**

#1: Which of the Ethernet standards (10 Mbps, 100 Mbps, 1000 Mbps, 10 Gbps) allow for twisted pair media? What are the corresponding IEEE standard names?

All, but 10 Gbps Ethernet can run over twisted pair. The corresponding IEEE standard names are:

10 Mbps – **10BaseT**

100 Mbps – **100BaseTX**

1000 Mbps – **1000BaseT**

#2: What is the difference between the physical representation of a star-wired bus LAN and its logical representation?

The physical representation looks more like a star, but the logical representation is of a ring.

A star-wired bus physically looks like a star but acts logically like a bus.

#3: Are hubs and switches interchangeable? Explain.

Switches can be a substitute of Hub, but hub cannot be because Hubs are considered Layer 1 (Physical) devices whereas switches are put into Layer 2 (Data Link). This is where hubs and switches differ Hubs broadcast the traffic whereas switches isolate the traffic resulting in a less traffic.

#4: Give an example of a situation in which a virtual LAN might be a useful tool in a business environment. What about in an educational environment?

If you want a certain group of users to work together on a project, you might want to place them on a virtual LAN; likewise, for school.

#5: What does it mean when a switch or device is cut through? What is the main disadvantage of a cut through switch? Is there a way to solve the disadvantage of a cut-through switch without losing its advantages? Defend your answer.

Cut-through switching is a switching method used in packet-switching systems where the switch forwards packets or frames to its destination immediately after the destination address has been processed without waiting for the entire data to be received.

A disadvantage is that errors are propagated. There’s not a way if you want to keep it truly cut-through

#6: Your company's switch between its two networks has just died. You have a router lying on your desk that is not currently being used. Will the router work in place of the broken switch? Explain.

No, the router mainly operates on IP addresses hence cannot work if the switch is broken whereas switches operate on NIC addresses.

#7: You work for a small advertising company with approximately 100 employees. Scattered around the company are a number of separate computer workstations that perform word processing, graphics design, spreadsheet operations, and market analysis. Your boss has asked you to consider installing some form of local area network to support computer operations. What type of local area network might you suggest? What type of wiring would you suggest? What would be the topology? What kind of support equipment (switches, servers) might you need? Where would that support equipment be located?

I would suggest 100Base-T Ethernet which is runs over Category 5e or above cable. It runs on both twisted pair and fiber optic cable whereas I would suggest twisted pair cable with TCP/IP protocol as each network segment can have a maximum cabling distance of 100 meters. I would prefer star wired bus topology because it is simple to interconnect the networks and easy to add components. Information is passed through a ring like representation. I would use CSMA/CD for medium access control. I would spread switches across the company that would create a star network for interconnect workstations. As several separate computer workstations are spread across the company and employees are working on word process, graphics design, spreadsheet, and market analyses. Finally, the servers are in the centralized server room.

#8: Find the IEEE (or other) Web site and report on the latest advances in the 802 standards. Do any additional standards exist for >10-Gbps Ethernet or wireless LANs? Are there any new proposals for systems not mentioned in this chapter? Explain what you find.

IEEE stands for The **Institute of Electrical and Electronics Engineers** is a professional association for electronic engineering and electrical engineering. **IEEE 802** is a family of IEEE standards dealing with Local area networks and metropolitan area networks.

The IEEE 802 standards does not have the transmission speed rate for wireless LAN for more than 10-Gbps. However, the IEEE 802.3 ethernet standards does have the data transfer rate of more than 10-Gpbs for Ethernet which are: IEEE 802.3bj

IEE 802.3bq.

The few advances of IEEE are:

**IEEE 802.11ac** in Dec 2013 - Changes compared to 802.11n include wider channels in the 5 GHz band, more spatial streams, higher-order modulation.  
**IEEE 802.11ad** in Dec 2012 - is an amendment that defines a new physical layer for 802.11 networks to operate in the 60 GHz millimeter wave spectrum.  
**IEEE 802.11af** in Feb 2014 - also referred to as "White-Fi" and "Super Wi-Fi".  
**IEEE 802.11aj** in Apr 2018   
**IEEE 802.11ah** in Dec 2016  
**IEEE 802.11ax** in Sep 2019 - is the successor to 802.11ac, and will increase the efficiency of WLAN networks. Currently in development, this project has the goal of providing 4x the throughput of 802.11ac at the user layer.

**CHAPTER 8**

#1: At what frequency ranges do the IEEE 802.11 b/a/g/n/ac standards transmit? What is important about these different frequencies? (and include 802.11ac & 802.11ax)

2.4GHz, 5GHz, 2.4GHz, 2.4/5GHz, 5GHz. The 5 GHz frequencies don’t travel as far.

**IEEE 802.11b**: This standard provides 11 Mbps transmission in the **2.4 GHz** operating frequency and bandwidth of 22MHz.

**IEEE802.11a**: Networks using 802.11a operate at radio frequency of **5GHz** or **3.7GHz** and a bandwidth of 20MHz.

**IEEE 802.11g:** This standard operates at **2.4GHz** frequency and bandwidth of 20MHz.

**IEEE 802.11n:** This standard operates at **2.4GHz** frequency and involves increasing the channel bandwidth from 20MHz to 40MHz.

**IEEE 802.11ac:** This standard operating frequency is **5GHz**, and bandwidth of 20, 40, 80, 160MHz sectors.

**IEEE 802.11ax:** This operates in both the **2.4Ghz** and **5Ghz** ranges, thus creating more available channels

Wi-Fi generations 1–6 refer to the 802.11b, 802.11a, 802.11g, 802.11n, 802.11ac, and 802.11ax protocols, in that order. The only difference in these different frequencies being the 5 GHz frequencies don’t travel as far.

#2: In a client/server system, a client transmits a request to a server, the server performs a processing operation, and the server returns a result. List all the possible problems that can occur with transmission in this scenario.

The possible problems that can occur with transmission in this scenario are:

1. Request gets lost, and client waits.
2. Request gets temporarily lost, client sends another, then 2 requests arrive at the server.
3. Results from server are lost.
4. Results from server temporarily lost, then client sends request again, getting 2 sets of results.
5. Client crashes before the results come back from the server.
6. Server crashes before the request arrives or after results start their way back.

#3: In what ways are UNIX and Linux similar? In what ways are they different?

Unix is a complete operating system and proprietary whereas Linux is Unix like Operating System kernel and opensource. They both have text-based interfaces, robust and powerful.

Outside the box

#4: An office complex is four stories high. Each floor is roughly 75 meters (yards) by 75 meters. The company wants to create a wireless LAN for the entire complex. Which wireless LAN technology would you recommend? Where would you place the access points? Where would you place the wired backbone?

I would recommend the IEEE 802.11n standard wireless LAN technology because it utilizes multiple wireless antennas in tandem to transmit and receive data [3-4]. The antenna technology used with the IEEE802.11n standard is known as Multiple Input, Multiple Output (MIMO). The MIMO increases both the range and throughput of a wireless network. The IEEE802.11n indoor/outdoor ranges are 75m, and 250m respectively. The access points would be the center of every floor. Would prefer ground floor to place the wired backbone as ethernet can transfer data up to 100 meters distance and here each floor is roughly 75 meters.

**CHAPTER 9**

#1: What are the main differences *between* a local area network and a wide area network?

 Local Area Network (**LAN**) is a computer network, which is limited to a small office, single building, multiple buildings inside a campus etc. Typically, a Local Area Network (LAN) is a private network owned and maintained by a single organization.

A Wide Area Network (**WAN**) spans over multiple geographic locations, which is composed of multiple LANs. It is nearly impossible for a small to medium organization (except Network Service Providers) to pull network cables between their two offices in two different countries located 1000s of kilometers away. Network Service Providers (also called as ISPs) provide the connectivity solutions for Wide Area Networks (WAN).

Local area network: smaller, different protocols, different functions.

#2: What are the main characteristics of a circuit switched network? What are its advantages and disadvantages?

The main characteristics of a circuit-switched network is that it is a dedicated network as in it is dedicated for only that user and always uses the same path. It is a fixed circuit.

The advantages are that there is no routing decision as the path is dedicated to only you.

The disadvantages are the cost, especially if you are not transmitting continuously.

#3: What are the main advantages and disadvantages of:

a. Centralized routing

b. Distributed routing

c. Adaptive routing

Centralized Routing:

Advantages:

Fast and simple. only one computer develops the routing table others simply use it hence resources saved.

Disadvantages:

1. vulnerability of the computer developing the routing tables
2. does not reflect changing network conditions such as computers that are overloaded by many messages
3. when routing tables are changed, network capacity is “wasted” to transmit the routing tables to all computers.
4. Distributed routing

Advantages:

Each node maintains its own routing table. Each node shares information with other nodes so that individual routing tables can be created.

distributed routing does away with much of the data traffic on a network that a centralized routing scheme can generate.

Disadvantages:

One disadvantage of distributed routing is related to the problems that arise if the routing tables need to be updated. When all the routing information is in one place (that is, in a single table), it is simple to make updates. When routing information is scattered throughout a network, getting the appropriate routing

information to each node is a complex problem. Another consequence of storing routing information at multiple locations is that at any given point in time, there may be one or more routing tables that contain old or incorrect information.

1. Adaptive routing

Advantages:

* 1. can improve performance, as seen by the network user.
  2. aid in congestion control because an adaptive routing strategy tends to balance loads.

Disadvantages:

1. The routing decision is more complex; therefore, the processing burden on network nodes increases.
2. An adaptive strategy may react too quickly, causing congestion-producing oscillation, or too slowly, being irrelevant.

#4: Which type of network application requires more elaborate software: connection oriented or connectionless? Explain.

The type of network application which requires more elaborate software is connection oriented as it must create a dialog that establishes, maintains, and deletes the connection.

It requires software for communication whereas connectionless does not require software.

Connection oriented requires a logical connection between a sender and a receiver as there is no loss of information.

**CHAPTER 10**

#1: List the main responsibilities of the Internet Protocol.

The main responsibility of the Internet Protocol is to transfer data packets across the Internet

#2: List the main responsibilities of the Transmission Control Protocol.

The main responsibility of the Transmission Control Protocol to create an error-free end-to-end connection over the Internet

#3: Explain the relationship of the port number to an IP address.

An IP address identifies a computer’s connection to the Internet, while a port address identifies an application on that computer.

#4: How does the Domain Name System translate a URL into a 32-bit binary address?

Domain Name System (DNS) uses a distributed database system of URL address to translate a URL into 32-bit binary address.

#5: Why is ARP necessary if every workstation connected to the Internet has a unique IP address?

ARP is necessary even if every workstation connected to the internet has a unique IP address because once a packet arrives at the destination local area network (such as a CSMA/CD LAN), the LAN protocol does not look at IP addresses but uses the MAC layer addresses to deliver the frame.

#6: If three users on one local area network all request a Web page at the same time, how does NAT know which results go to which workstation?

The NAT software records each outgoing request so that when the Web pages come back, it knows which Web page goes to which workstation.

#7: What are the advantages and disadvantages of using dynamic IP address assignments?

Advantages: A company can purchase fewer IP addresses since each machine will not be statically assigned a fixed address but dynamically assigned an address when it accesses the Internet.

Disadvantages: The software is more elaborate; say if 10 IP addresses are purchased and the 11th user tries to access the Internet?

#8: Two banks want to establish an electronic link between themselves, over which they can transmit money transfers. Can they use a virtual private network and a tunneling protocol, or is a better technique available? Defend your answer

A VPN would be a preferred solution, if a high level of security is implemented. Even a leased telephone service with encryption will work.

**CHAPTER 11**

#1: You want to start your own local telephone company. Do you have to install your own telephone lines to each house and business? Explain.

No. We need not install telephone lines to each house and business because according to the Telecommunications Act of 1996 we can lease equipment and lines from existing local telephone companies (ILECs).

#2: If you install a 56-kbps modem in your computer and dial in to a remote network that has only 33,600-bps modems, is your modem useless? Defend your answer.

No, the 56k modem will fall back to the appropriate speed.

#3: What are the basic functions of a cable modem?

Functions of a cable modem:

1. Provides high-speed access to the Internet.
2. Provides cable television.
3. Splits the signal between computer and television

#4: Describe a business or school application that would benefit from unified communications.

Help desks, telemarketing, information centers, online database service.

**CHAPTER 12**

#1: How do hackers exploit operating system vulnerabilities?

Hackers exploit operating system vulnerabilities ﻿﻿﻿﻿﻿by launching a virus that attacks something about the operating system.

#2: How does a denial-of-service attack work?

Denial-of-service attack bombards a selected site with an overwhelming number of messages.

#3: How is steganography used to hide secret messages?

It takes little bit of secret messages and hides it within another document or file. This is how steganography hides secret messages.

#4: What are the three basic types of firewalls?

Packet filter, Stateful inspection and Proxy server are the three different types of firewalls.

#5: What are the advantages of having a security policy in place?

Everyone, employees, management, external users know the score.

#6: You have forgotten your password, so you call the help desk and ask the representative to retrieve your password. After a few moments, the help desk representative your forgotten password. What has just happened, and what is its significance?

Passwords are usually stored in the computer in an undecipherable form. Apparently in this system they were not, which means anyone might be able to find the password file and dump its contents.

#7: You want to write a song and apply a digital signature to it, so that you can later prove that it is your song. How do you apply the signature; and later, how would you use it to prove that the song is yours?

You first convert the song to a digital form, take the hash of the form, and then apply a private key to the hash. Then you save the encrypted hash. If someone claims ownership in future, you can decrypt the hash and rehash the song, comparing the hashes.

#8: Can a firewall filter out requests to a particular IP address, a port address, or both? What is the difference?

Both. The IP address would be the address of a device connected to the Internet, while a port address would be the address of an application on a machine. You might want to restrict all access to a particular machine or just restrict access to particular applications on a machine.

**CHAPTER 13**

#1: Describe each phase of the Systems Development Life Cycle

Planning: determining which projects to examine; Analysis: learning about the current system and recommending a business solution; Design: creating the computer-based solution; Implementation: installing the system; Maintenance

#2: List the three most important skills a network administrator should possess.

Technical skills, people skills, training skills

#3: What is meant by the statistical term "availability"?

Probability a device will be available in a given time frame

#4: What basic diagnostic tools are used to support a computer network?

Diagnostic tools that test and debug the network hardware and diagnostic tools that analyze the data transmitted over the network.