COMPUTER SCIENCE & INFORMATION TECHNOLOGY

Computer Networks

Comprehensive Theory
with Solved Examples *and* Practice Questions

MADE EASY Publications

www.madeeasypublications.org

MADE EASY Publications Pvt. Ltd.

Corporate Office: 44-A/4, Kalu Sarai (Near Hauz Khas Metro Station), New Delhi-110016 | **Ph. :** 9021300500

Email : infomep@madeeasy.in | **Web :** www.madeeasypublications.org

Computer Networks

EDITIONS

First Edition : 2015
Second Edition : 2016
Third Edition : 2017
Fourth Edition : 2018
Fifth Edition : 2019
Sixth Edition : 2020
Seventh Edition : 2021
Eighth Edition : 2022

Ninth Edition : 2023

CONTENTS

Computer Networks

CHAPTER 4

CHAPTER 5

Computer Networks

Goal of the Subject

The main goal of networking is "Resource sharing", and it is to make all programs, data and equipment available to anyone on the network without the regard to the physical location of the resource and the user.

A second goal is to provide high reliability by having alternative sources of supply. For example, all files could be replicated on two or three machines, so if one of them is unavailable, the other copies could be available.

Another goal is saving money. Small computers have a much better price/performance ratio than larger ones. This goal leads to networks with many computers located in the same building. Such a network is called a LAN (Local Area Network).

Another closely related goal is to increase the systems performance as the work load increases by just adding more processors. With central mainframes, when the system is full, it must be replaced by a larger one, usually at great expense and with even greater disruption to the users.

Computer networks provide a powerful communication medium. A file that was updated/ modified on a network can be seen by the other users on the network immediately.

Computer Networks

INTRODUCTION

Although Computer network is a vast subject on its own, in this book we tried to keep it around the GATE syllabus. Each topic required for GATE is crisply covered with illustrative examples and each chapter is provided with Student Assignment at the end of each chapter so that the students get the thorough revision of the topics that he/she had studied. This subject is carefully divided into eight chapters as described below.

1. **Networking Fundamentals and Physical layer:** In this chapter we discuss transmission medium, noise that cause bit errors, types of transmission media, concept of protocol layering. Finally we discuss the IP addressing, Subnetting and Network address translation.
2. **Data Link layer:** In this chapter we discuss Delays in computer networks, Protocol layering, Circuit-switched and Packet switching. Data link layer functions, farming methods, error correction and detection methods, Sliding window protocols for flow control the Static and dynamic channel allocation methods. Then we finally discuss Networking devices like Repeaters, Hubs, Bridges, Switches, Routers and Gateways.
3. **Network Layer:** In this chapter we discuss the classification of routing algorithms, Distance vector and Link state routing protocols. We also cover congestion control algorithms at network layer, Internet protocol, and finally we cover the network layer protocols namely ARP, RARP, ICMP and IPv4 & NAT.
4. **Transport Layer Protocols:** In this chapter we discuss the TCP protocol as connected oriented service and reliable service provider, TCP congestion control, TCP timers and finally we discuss UDP.
5. **Application Layer and Protocols:** In this chapter we discuss the various protocols used at application layer: DNS, HTTP, SMTP, Telnet, UDP, FTP etc.

■■■■

CHAPTER

1

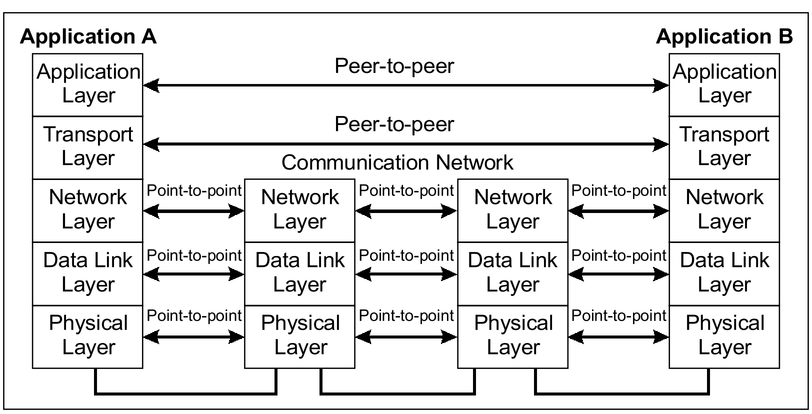
Networking Fundamentals and Physical Layer

1.1 Introduction

1.1.1 Protocol Layering

There are several advantages of protocol layering.

1. Protocol layering enables us to divide a complex task into several smaller simpler tasks. This is referred to as modularity.
2. It allows to separate the services from the implementation.
3. Intermediate systems need only some layers but not all layers. Protocol layering helps us in designing the system or devices with required number of layers implemented in it.



1.1.2 OSI layer vs TCP/IP layer

OSI (Open System Interconnection)	TCP (Transmission Control Protocol/ Internet Protocol)
• OSI provide layer function and also defines functions of all layers	• TCP/IP model the transport layer does not guarantees delivery of packets
• IN OSI model the transport layer guarantees the delivery of packets	• Follows vertical approach
• Follows horizontal approach	• TCP/IP does not have a separate presentation layer
• OSI model has a separate presentation layer	• TCP/IP model cannot be used in any other application
• OSI is a general model	• The network layer in TCP/IP model provides connectionless services
• Network layer of OSI model provide both connection oriented and connectionless service	• TCP/IP model does not fit any protocol
• Protocols are hidden in OSI model and are easily replaced as the technology changes	• In TCP/IP replacing protocol is not easy
• OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them	• In TCP/IP it is not clearly separated its services, interfaces and protocols.
• It has 7 layer	• It has 5 layers

The Open Systems Interconnection (OSI) model is a standard "reference model" created by the International Organization for Standardization (ISO) to describe how the different software and hardware components involved in a network communication should divide labor and interact with one another.

It defines a seven-layer set of functional elements, ranging from the physical interconnections at Layer 1 (also known as the physical layer, or PHY interface) all the way up to Layer 7, the application layer.

The Transmission Control Protocol (TCP) and the Internet Protocol (IP) are two of the network standards that define the Internet.

IP defines how computers can get data to each other over a routed, interconnected set of networks. TCP defines how applications can create reliable channels of communication across such a network. Basically, IP defines addressing and routing, while TCP defines how to have a conversation across the link without garbling or losing data. TCP/IP grew out of research by the U.S. Dept. of Defense and is based on a loose rather than a strict approach to layering. Many other key Internet protocols, such as the Hypertext Transfer Protocol (HTTP), the basic protocol of the Web, and the Simple Mail Transfer Protocol (SMTP), the core e-mail transfer protocol, are built on top of TCP. The User Datagram Protocol (UDP), a companion to TCP, sacrifices the guarantees of reliability that TCP makes in return for faster communications.

TCP/IP doesn't map cleanly to the OSI model, since it was developed before the OSI model and was designed to solve a specific set of problems, not to be a general description for all network communications.

ISO/OSI Layer	TCP/IP Model	Sample Protocols	Devices
7. Application	Application	**SOAP, XML**	**XML Appliances**
6. Presentation		HTTP, HTTPS FTP TELNET SMTP, NTP	Content Service Switch Layer 4-7 Switches
5. Session			
4. Transport			
3. Network	Transport	TCP, UDP	Router, Layer-3 Switch
2. Data Link	Network	IP, ICMP, IGMP, IPX	Switches, Bridges
1. Physical	Link	Network Interface: Ethernet, Token Ring, FDDI	Hubs, Repeaters

Two layers in the OSI model, session and presentation, are missing from the TCP/IP protocol suite. These two layers were not added to the TCP/IP protocol suite after the publication of the OSI model. The application layer in the suite is usually considered to be the combination of three layers in the OSI model. The OSI model did not replace the TCP/IP protocol suite because it was completed when TCP/IP was fully in place and because some layers in the OSI model were never fully defined.

1.1.3 Similarities between OSI Model and TCP/IP Model

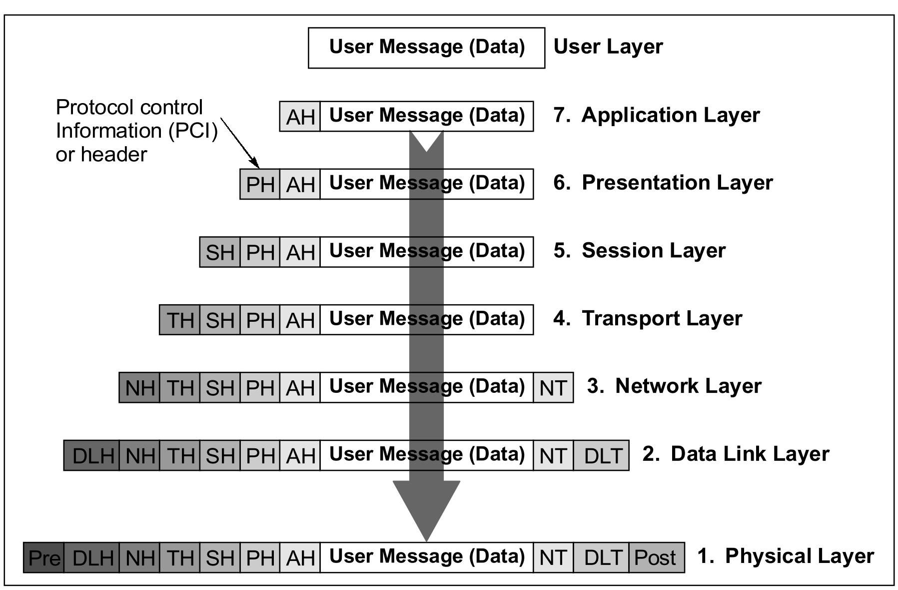
1. Both of them use a layered architecture to explain data communication process in computer networks.
2. Each layer performs well-defined functions in both models.
3. Similar types of protocols are used in both models.
4. OSI and TCP/IP reference models are open in nature.
5. Both models give a good explanation on how various types of network hardware and software interact during a data communication process.
6. Data hiding principle is well maintained on each layer in the two models. The core level functional details of each layer are not revealed to other layers.
7. Transport layer defines end-end data communication process and error-correction techniques in both the models.
8. OSI and TCP/IP reference models process data in the form of packets to perform routing.

1.1.4 Encapsulation and Decapsulation

Messages generated by application are encapsulated by every layer before passing on to the layer below it. Information that is encapsulated where is from layer-to-layer. This encapsulated information is also called as 'header'.

The TCP header information includes the port address, Ack information, checksum and other useful information. The network layer header includes source and destination IP address, header checksum, fragmentation information and other useful information.

Data link layer includes the MAC address information, error control, error detection, error correction and other useful information.



OSI Layer and Message passing

1.1.5 Data Flow

Communication between two devices can be simplex, half-duplex, or full-duplex.

(a) **Simplex:** In simplex *mode*, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive.

Example: Keyboards and Traditional Monitors.

(b) **Half-Duplex:** In half-duplex, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa.

Example: Walkie-talkies and Citizen band (CB) Radio.

(c) **Full-Duplex:** In full-duplex, both stations can transmit and receive simultaneously.

Example: Telephone networks.

The simplex mode can use the entire capacity of the channel to send data in one direction. The half-duplex mode is used in cases where there is no need for communication in both direction at the same time; the entire capacity of the channel can be utilized for each direction.

The full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel, however, must be divided between the two directions.

1.1.6 Network Topologies

(a) **Mesh Topology:** In mesh topology, every device has a dedicated point-to-point link to every other device. The term *dedicated* means that the link carries traffic only between the two devices it connects. Node 1 must be connected to $n-1$ nodes, node 2 must be connected to $n-1$ nodes, and finally node n must be connected to $n-1$ nodes. Hence in total we need $n(n-1)$ physical links. Every node must have $n-1$ input/output (I/O) ports.

(b) **Star Topology:** In a start topology, each device has a dedicated point-to-point link only to a central controller, usually called a **hub**. The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices. In a star, each device needs only one link and one I/O port to connect it to any number of others.

(c) **Bus Topology:** A bus topology is multipoint. One long cable acts as **backbone** to link all the devices in a network. A drop line is a connection running between the device and the main cable.

(d) **Ring Topology:** In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater. Each device is linked to only its immediate neighbours.

1.2 Circuit-Switched vs Packet Switched Network

Circuit Switching

A **circuit-switched network** consists of a set of switches connected by physical links. A circuit-switched network is made of a set of switches connected by physical links, in which each link is divided into n channels.

Circuit switching takes place at the physical layer. Before starting communication, the stations must make a reservation for the resources to be used during the communication. These resources, such as channels (bandwidth in FDM and time slots in TDM), switch buffers, switch processing time, and switch input/output ports, must remain dedicated during the entire duration of data transfer until the **teardown phase**.

Data transferred between the two stations are not packetized (physical layer transfer of the signal). The data are a continuous flow sent by the source station and received by the destination station, although there may be periods of silence.

There is no addressing involved during data transfer. The switches route the data based on their occupied band (FDM) or time slot (TDM). Of course, there is end-to-end addressing used during the setup phase, as we will see shortly.

In circuit switching, the resources need to be reserved during the setup phase; the resources remain dedicated for the entire duration of data transfer until the teardown phase.

Three phase:

(a) **Setup phase:** Before the two parties (or multiple parties in a conference call) can communicate, a dedicated circuit (combination of channel in links) needs to be established.

(b) **Data-transfer phase:** After the establishment of the dedicated circuit (channels), the two parties can transfer data.

(c) **Teardown phase:** When one of the parties needs to disconnect, a signal is sent to each switch to release the resources.

Packet Switching

1. Refers to protocols in which messages are divided into packets before they are sent. Each packet is then transmitted individually and can even follow different routes to its destination.
2. Once all the packets forming a message arrive at the destination, they are recompiled into the original message.
3. Most modern Wide Area Network (WAN) protocols, including TCP/IP, X.25, and Frame Relay, are based on packet-switching technologies.
4. In contrast, normal telephone service is based on a circuit-switching technology, in which a dedicated line is allocated for transmission between two parties.
5. Circuit-switching is ideal when data must be transmitted quickly and must arrive in the same order in which it's sent.
6. This is the case with most real-time data, such as live audio and video. Packet switching is more efficient and robust for data that can withstand some delays in transmission, such as e-mail messages and Web pages.
7. A new technology, ATM, attempts to combine the best of both worlds — the guaranteed delivery of circuit-switched networks and the robustness and efficiency of packet-switching networks.

1.3 Physical Layer

Source (as shown in the following figure) is where the data is originated. Typically it is a computer, but it can be any other electronic equipment such as telephone handset, video camera, etc., which can generate data for transmission to some destination.

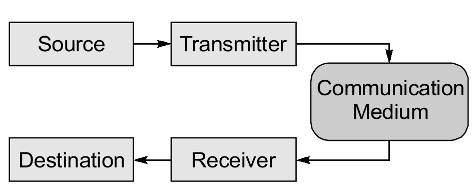


Figure: *Simplified model of a data communication system*

Transmitter

As data cannot be sent in its native form, it is necessary to convert it into signal. This is performed with the help of a transmitter such as modem.

Communication Medium

The signal can be sent to the receiver through a communication medium, which could be a simple twisted-pair of wire, a coaxial cable, optical fiber or wireless communication system. It may be noted that the signal that comes out of the communication medium is different from that was sent by the transmitter (received data may not be same as it was send).

The receiver receives the signal and converts it back to data before forwarding to the destination. Destination is where the data is absorbed. Again, it can be a computer system, a telephone handset, a television set and so on.

Data

Data refers to information that conveys some meaning based on some mutually agreed up rules or conventions between a sender and a receiver and today it comes in a variety of forms such as text, graphics, audio, video and animation.

Data can be of two types; analog and digital. Analog data take on continuous values on some interval. Digital data take on discrete values.

1.4 Signal

It is electrical, electronic or optical representation of data, which can be sent over a communication medium.

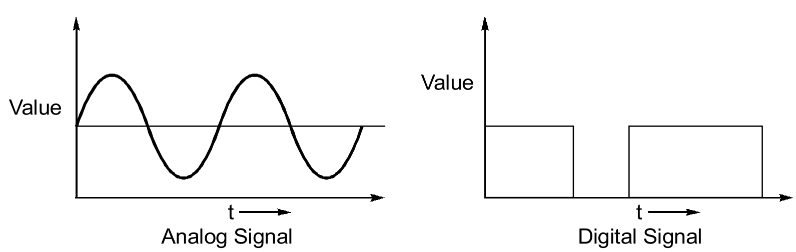


Figure: *Analog signal and Digital signal*

Digital signal can have only a limited number of defined values, usually two values 0 and 1. Analog signals are continuous with the wave forms as shown in the figure.

1.4.1 Signal Characteristics

A signal can be represented as a function of time, i.e. it varies with time. However, it can be also expressed as a function of frequency, i.e. a signal can be considered as a composition of different frequency components. Thus, a signal has both time-domain and frequency domain representation.

Bandwidth

The range of frequencies over which most of the signal energy of a signal is contained is known as **bandwidth** or effective bandwidth of the signal. The term 'most' is somewhat arbitrary. Usually, it is defined. The frequency spectrum and spectrum of a signal is shown in figure.

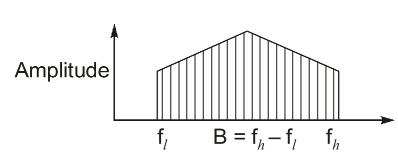


Figure:
Frequency spectrum and bandwidth of a signal

Bandwidth (B) = $F_h - f_l$

1.4.2 Digital Signal

Most digital signals are aperiodic and thus, period or frequency is not appropriate. Two new terms, bit interval (instead of period) and *bit rate* (instead of frequency) are used to describe digital signals. The bit interval is the time required to send one single bit. The bit rate is the number of bit interval per second. This mean that the bit rate is the number of bits sent in one second, usually expressed in bits per second (bps) as shown in figure.

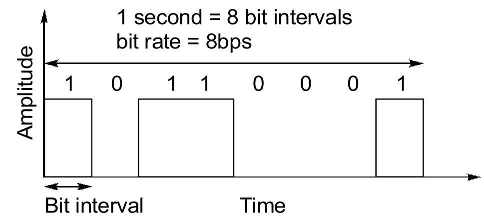


Figure: *Bit Rate and Bit Interval*

A digital signal can be considered as a signal with an infinite number of frequencies and transmission of digital requires a low-pass channel as shown in figure. On the other hand, transmission of analog signal requires band-pass channel shown in figure.

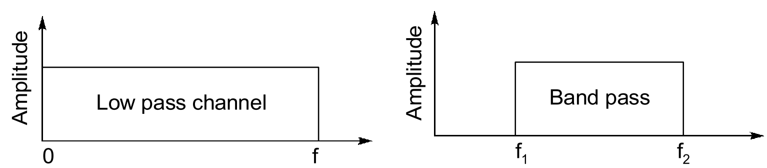


Figure: *Low pass channel required for transmission of digital and Analog signal*

Digital transmission has several advantages over analog transmission. That is why there is a shift towards digital transmission despite large analog base. Some of the advantages of digital transmission are highlighted below:

- Analog circuits require amplifiers, and each amplifier adds distortion and noise to the signal. In contrast, digital amplifiers regenerate an exact signal, eliminating cumulative errors. An incoming (analog) signal is sampled, its value is determined, and the node then generates a new signal from the bit value; the incoming signal is discarded. With analog circuits, intermediate nodes amplify the incoming signal, noise and all.
- Voice, data, video, etc. can all by carried by digital circuits. What about carrying digital signals over analog circuit? The modem example shows the difficulties in carrying digital over analog. A simple encoding method is to use constant voltage levels for a "1'' and a "0". Can lead to long periods where the voltage does not change.
- Easier to multiplex large channel capacities with digital.
- Easy to apply encryption to digital data.
- Better integration if all signals are in one form. Can integrate voice, video and digital data.

Base-band and Broadband Signals

Base-band is defined as one that uses digital signaling, which is inserted in the transmission channel as voltage pulses. In baseband LANs, the entire frequency spectrum of the medium is utilized and transmission is bi-directional. Baseband systems used for small distance communication.

Broadband systems are those, which use analog signaling to transmit information using a carrier of high frequency.

Since broadband systems use analog signaling, frequency division multiplexing is possible, where the frequency spectrum of the cable is divided into several sections of bandwidth. These separate channels can support different types of signals of various frequency ranges to travel at the same instance.

Broadband is a unidirectional medium where the signal inserted into the media propagates in only one direction. Two data paths are required, which are connected at a point in the network called *headend*. All the stations transmit towards the headend on one path and the signals received at the headend are propagated through the second path.

Example-1.27 Assume host A having an IP address of 125.32.16.5 with a subnet mask of 255.255.255.128. Also, assume another host B, having an IP address of 125.32.16.120 with a subnet mask of 255.255.255.192.

Which of the following is correct?

(a) 'A' assumes 'B' to be on the same network.
(b) 'B' assumes 'A' to be on the same network.
(c) Both 'A' and 'B' assume each other to be on the same network.
(d) Neither of the two assume themselves to be on the same network.

Solution: (a)

IP address of 'A' = 125.32.16.5
Subnet mask of 'A' = 255.255.255.128
Subnet ID of A according to 'A' = 125.32.16.0
IP address of 'B' = 125.32.16.120
Subnet ID of B according to 'A' = 125.32.16.0

Hence 'A' assumes 'B' to be on the same network

IP address of 'B' = 125.32.16.120
Subnet mask of 'B' = 255.255.255.192
Subnet ID of B according to 'B' = 125.32.16.64
Subnet ID of A according to 'B' = 125.32.16.0

Hence 'B' assumes 'A' to be on different network.

Summary

- A data communications system must transmit data to the correct destination in an accurate and timely manner.
- The five components that make up a data communications system are the message, sender, receiver, medium and protocol. Text, numbers, images, audio, and video are different forms of information. Data flow between two devices can occur in one of three ways: simplex, half-duplex, or full-duplex.
- **Base-band** is defined as one that uses digital signaling, which is inserted in the transmission channel as voltage pulses.
- **Broadband** systems are those, which use analog signaling to transmit information using a carrier of high frequency.
- Co-axial cable has superior frequency characteristics compared to twisted-pair and can be used for both analog and digital signaling.
- The term broadband refers to analog transmission over coaxial cable.
- Fibre optics has very high data rate, and low error rate.
- Unguided transmission is used when running a physical cable (either fiber or copper) between two end points is not possible.
- The baud rate or signaling rate is defined as the number of distinct symbols transmitted per second, irrespective of the form of encoding.
- The bit rate or information rate is the actual equivalent number of bits transmitted per second.

- The **bit rate** represents the number of bits sent per second, whereas the **baud rate** defines the number of signal elements per second in the signal. Depending on the encoding technique used, baud rate may be more than or less than the data rate.
- In the standard Manchester coding there is a transition at the middle of each bit period. A binary **1** corresponds to a **low-to-high transition** and a binary **0** to a **high-to-low transition** in the middle.
- In Differential Manchester, inversion in the middle of each bit is used for synchronization.
- IP defines how computers can get data to each other over a routed, interconnected set of networks. TCP defines how applications can create reliable channels of communication across such a network.

Student's Assignment

Q.1 For a class B network an appropriate mask with 200 subnets each with 220 systems is
(a) 255.255.255.254
(b) 255.255.255.0
(c) 255.255.255.220
(d) 255.255.200.220

Q.2 Consider the following statements regarding OSI model
(*i*) It divides the network communication into smaller and simpler components, aiding component development, design and troubleshooting.
(*ii*) It allows multiple-vendor development through standardization of network components.
(*iii*) It prevents the changes in one layer from affecting the other layers, allowing for quicker development.
(*iv*) It usually do not correspond exactly to the protocol stack running on an actual system.
Which of the above are true?
(a) (*i*) and (*iv*) only
(b) (*ii*) and (*iii*) only
(c) (*i*), (*ii*) and (*iv*) only
(d) All of these

Q.3 An organization is granted the block 190.76.0.0/16. The administrator wants to create 1024 subnets using 10 bits. The first and last addresses in subnet 1024 respectively are
(a) 190.76.255.0/26 and 190.76.255.255/26
(b) 190.76.255.1/16 and 190.76.255.255/16
(c) 190.76.255.192/26 and 190.76.255.255/26
(d) 190.76.255.192/16 and 190.76.255.255/16

Q.4 What is the netmask of gateway interface in a sub-C network where only 14 hosts exist and IP address of one of the hosts in 193.146.129.76?
(a) 255.255.129.76
(b) 255.255.129.240
(c) 255.255.255.240
(d) 255.255.255.255

Q.5 The number of bits in IPv6 address is
(a) 64
(b) 128
(c) 256
(d) None of these

Q.6 In Hexadecimal colon notation, a 128-bit long IPv6 address is divided into ________ sections, each comprising ________ hexadecimal digits.
(a) 4, 2
(b) 8, 4
(c) 16, 2
(d) 4, 8

Q.7 Given the following IP address and network mask, what is the broadcast address?
IP : 160.168.30.100
Net Mask : 255.255.240.0
(a) 160.168.31.255
(b) 160.168.30.255
(c) 160.168.240.255
(d) 160.168.255.255

Q.8 The Router connecting company's network to the Internet applies the mask 255.255.252.0 to the destination address of incoming IP packets. Find the corresponding subnetwork for the destination IP address of packet 159.133.7.220.
(a) 159.133.7.0
(b) 159.133.0.0
(c) 159.133.4.0
(d) 159.133.6.0

Q.9 Let X and Y be the number of 0's in the binary notation of network ID and Direct Broadcast Address (DBA) respectively for the IP address 200.25.80.67 (classfull address). The value of $X \log_2 Y$ is _______.

Q.10 For a class C network if IP address of a computer is 200.99.39.112 and subnet mask is 255.255.255.224 the decimal value of last octet of last host of sixth subnet is _______.

Q.11 Match **List-I** and **List-II** and select the correct answer using the codes given below the lists:

List-I (Packets)

A.

Data	Source IP	Destination IP
Data	250.255.255.255	50.50.50.50

B.

Data	Source IP	Destination IP
Data	24.50.48.30	255.255.255.255

C.

Data	Source IP	Destination IP
Data	24.66.50.77	24.50.30.20

List-II

1. Unicast packet within network
2. This packet never exists
3. Limited broadcasting

Codes:

	A	B	C
(a)	1	2	3
(b)	2	3	1
(c)	3	1	2
(d)	2	1	3

Q.12 Consider a class C network has an IP address of one of the computers is 202.23.65.119. Which of the following can be host on network?

(a) 202.23.65.0 (b) 202.23.0.0
(c) 0.0.0.119 (d) None of these

Q.13 An organization is granted the block 190.76.0.0/16. The administrator wants to create 1024 subnets using 10 bits. What is the first and last addresses in last subnet which can assign to host?

(a) 90.76.255.0/26 and 190.76.255.255/26
(b) 190.76.255.1/16 and 190.76.255.255/16
(c) 190.76.255.193/26 and 190.76.255.254/26
(d) 190.76.255.192/16 and 190.76.255.255/16

Q.14 Consider the following IP address:

(*i*) 210.15.16.62 (*ii*) 210.15.16.94
(*iii*) 210.15.16.127 (*iv*) 210.15.16.191

Which of following IP address may represents last host of any subnet if subnet mask is 255.255.255.224?

(a) (*i*) and (*ii*) (b) (*i*) and (*iii*)
(c) (*ii*) and (*iv*) (d) (*iii*) and (*iv*)

Q.15 A router uses the following routing table:

Network Address	Mask	Interface
205.32.0.0	/25	R0
205.32.16.0	/26	R1
205.32.32.0	/24	R2
205.32.16.32	/27	R3

Find the next hop (where router will send the packet), if the router has IP address "205.32.16.63".

(a) R0 (b) R1
(c) R2 (d) R3

Q.16 An organization is granted the block 172.89.0.0/16. The administrator wants to create 1024 subnets using 10 bits. The first and last addresses of any host in subnet 1024 respectively are

(a) 172.89.255.0/26 and 172.89.255.255/26
(b) 172.89.255.1/26 and 172.89.255.245/26
(c) 172.89.0.1/26 and 164.76.255.255/26
(d) 172.89.0.1/26 and 172.89.255.245/26

Q.17 If the broadcast address of the subnet is given as 173.140.31.255, which of the following mask cannot suit the above address?

(a) 255.255.240.0 (b) 255.255.248.0
(c) 255.255.192.0 (d) Both (b) and (c)

Q.18 Match **List-I** with **List-II** and select the correct answer using the codes given below the lists:

List-I

A. Passive scanning
B. Active scanning
C. Association

List-II

1. Assigning a one or two word SSID to the access point.

2. Creating a virtual wire between itself and AP by the wireless station.
3. Scanning channels and listening for beacon frames.
4. Broadcasting a probe frame that will be received by all APs within the wireless Host's range.

Codes:

	A	B	C
(a)	3	2	1
(b)	3	4	2
(c)	4	2	1
(d)	4	3	1

Q.19 In a block of addresses, we know the IP address of one of the host is 128.44.82.16 / 25. Which of the following represent first address and last addresses that can be assign to host in the block?
(a) 128.44.82.0 and 128.44.82.126
(b) 128.44.82.1 and 128.44.82.127
(c) 128.44.82.1 and 128.44.82.126
(d) 128.44.82.0 and 128.44.82.127

Q.20 In the network 143.128.67.235 / 20, if x represent the decimal value of 3rd octet and y represent the decimal value of 4th octet of last IP address assigned to any host, then value of $x \times y$ is ________.

Q.21 Consider a IP address 201.24.58.69 in classful address, if the number of 1's in directed broadcast address is a and number of 1's in network ID, of the given IP address is b, value of $a + b$ ________.

Q.22 Consider a class B network with 100 subnets each with 160 system. What is the subnet mask of this network?
(a) 255.255.255.190
(b) 255.255.255.0
(c) 255.255.254.0
(d) 250.255.254.128

Q.23 An organization is granted the block 178.52.0.0/16, the administrator wants to create 510 subnets, what is the first and last IP address respectively in the last subnet that can be assign to the host?
(a) 178.52.255.120/25, 178.52.254.254/25
(b) 178.52.255.129/16, 178.52.255.129/16
(c) 178.52.255.128/26, 178.52.255.254/25
(d) 178.52.255.129/25, 178.52.255.254/25

Q.24 Consider the following IP addresses and which of the following IP address may represents last host of any subnet, given subnet mask is 255.255.255.224?
(i) 196.24.63.127
(ii) 196.24.63.94
(iii) 196.24.63.62
(a) (i) and (ii)
(b) (ii) and (iii)
(c) (i) and (iii)
(d) Only (i)

Answer Key:

1. (b)	**2.** (d)	**3.** (c)	**4.** (c)	**5.** (b)
6. (b)	**7.** (a)	**8.** (c)	**9.** (96)	**10.** (222)
11. (b)	**12.** (c)	**13.** (c)	**14.** (a)	**15.** (d)
16. (d)	**17.** (c)	**18.** (b)	**19.** (c)	**20.** (20066)
21. (28)	**22.** (c)	**23.** (d)	**24.** (b)	

Student's Assignments Explanations

1. **(b)**
Given:
Number of subnets = 200 ($2^7 < 200 < 2^8$)
Number of systems per subnet = 220
Default mask for class B = 255.255.0.0
(i.e., 16 bits for NID and 16 Bits for HID)

Check whether $\boxed{200 \times 220 < 2^{16}}$

Now, $\dfrac{16 \text{ bits}}{\text{NID}} = \dfrac{16 \text{ bits}}{\dfrac{8 \text{ bits}}{\text{SID}} \quad \dfrac{8 \text{ bits}}{\text{HID}}}$

We can use 255 . 255 . 255 . 0

2. **(d)**
(*i*) OSI model reduces complexity by breaking network communication into smaller and simpler components. It provides a teaching tool to help network administrators understand the communication process used between networking components.

(*ii*) OSI model defines the process for connecting two layers together, promoting interoperability between vendors. It allows vendors to compartmentalize their design efforts to fit a modular design, which eases implementations and simplifies troubleshooting.

(*iii*) OSI model ensures interoperable technology.

(*iv*) The data link layer protocols often include physical layer specifications. The network and transport layer protocols work together to provide a cumulative end-to-end communication service.

∴ All are true.

3. (c)

Number of subnets = 1024
Bits required for subnet = 10
Network mask = 255.255.255.192
Number of hosts / subnet = $2^6 - 2$
Ranges are:
190.76.0.0/26 to 190.76.0.63/26 ——— 1st subnet
190.76.0.64/26 to 190.76.0.127/26 ——— 2nd subnet
190.76.0.128/26 to 190.76.0.191/26 ——— 3rd subnet
190.76.0.192/26 to 190.76.0.255/26 ——— 4th subnet
190.76.1.0/26 to 190.76.1.63/26 ——— 5th subnet
⋮
190.76.255.128/26 to 190.76.255.191/26 ——— 1023th subnet
190.76.255.192/26 to 190.76.255.255/26 ——— 1024th subnet

4. (c)

Only 14 hosts exists in the network. Therefore only 4 bits are sufficient for host bits.
The remaining 4 bits (MSB bits) of the last octet are part of Network ID.
Therefore the mask would be - 255.255.255.240

5. (b)

IPv6 uses 128 bit address, where as IPv4 uses 32 bit address.

6. (b)

An IPv6 address is represented as eight groups of 4 hexadecimal digits, each group representing 16 bits (2 octets). The groups are separated by colons (:).
∴ Option (b) is correct

7. (a)

In the Broadcast Address, All the host bits need to be 1.
Network ID is the result obtained after bitwise AND operation of IP and Net Mask.

```
        160.168.30.100
        255.255.240.0
        -------------
i.e.    160.168.16.00
```

By expanding 3rd octet we observe

16: 0001 (Network bits) 0000 (Host bits)

∴ Broadcast address is 160.168.31.255 obtained by placing 1's in host bits.

8. (c)

```
IP Address : 159.133.7.220
      Mask:  255.255.252.0
             -------------
             159.133.4.0
```

Boolean AND operation
The subnetwork is 159.133.4.0.

9. (96)

The IP address 200.25.80.67 belongs to class C network. Therefore network ID is 200.25.80.0 and DBA is 200.25.80.255.
The binary representation contains:
11001000.00011001.01010000.00000000
⇒ 24 0's in network ID
11001000.00011001.01010000.11111111
⇒ 16 0's in network IP
∴ $24 \log_2 16 = 24 \times 4 = 96$

10. (222)

Since the subnet mask is 255.255.255.224 that means the first 3 bits of subnet are reserved for subnet id and rest 5 are host id bits.

Hence, sixth subnet, last octet will be $[11011110]_2 = [222]_{10}$.

11. (b)
Packet A: The source IP contain direct broad cast address and we never use direct broadcast address in source IP. It is always used in destination IP. Hence packet A never exists.
Packet B: If destination IP address contain all 1's then it broadcasts within same network (Limited Broadcasting).
Packet C: It is a unicast packet within the same network as network ID 24.0.0.0 is same for both source and destination IP.

12. (c)
IP address of computer (Host) = 202.23.65.119
To find number of host = [Wild Card Mask of the Class] XOR [Host IP] = [Wild Card Mask of Class] XOR [Host IP]

i.e.	202	. 23	. 65	. 119
	0	. 0	. 0	. 255
	0	. 0	. 0	. 119

13. (c)
Block size = 190.76.255.1/16
Number of subnets to be created = 10
Subnet Id = 190.76.255.192
Now, the remaining 8 bits of 4th octet will be used for addressing.
Hence, the first address will be 190.76.255.193/26
and the last address will be 190.76.255.254/26.

14. (a)
Subnet mask is 255.255.255.224
(*i*) $62 \Rightarrow \underleftrightarrow{001}\ \underleftrightarrow{11110} \Rightarrow$ Last host
(*ii*) $94 \Rightarrow \underleftrightarrow{010}\ \underleftrightarrow{11110} \Rightarrow$ Last host
(*iii*) $127 \Rightarrow \underleftrightarrow{011}\ \underleftrightarrow{11111} \Rightarrow$ Direct broadcast address
(*iv*) $191 \Rightarrow \underleftrightarrow{101}\ \underleftrightarrow{11111} \Rightarrow$ Direct broadcast address

15. (d)
Routing in classless addressing follows "Longest Mask Matching". This states that the routing table is sorted from the longest mask to the shortest mask.
So here firstly starts with /27
To find N/W address = 205.32.16.63 AND 255.205.255.224 = 205.32.16.32 {Matched with R3}
So interface chosen is R3.

16. (d)
Number of subnets = 1024
Bits required for subnet = 10
Subnet mask = 255.255.255.192
[i.e. take bits from host portion]
Number of hosts = $2^6 - 2$
Ranges are:
172.89.0.0/26 **to** 172.89.0.63/26 —— 1st subnet
172.89.0.64/26 **to** 172.89.0.127/26 —— 2nd subnet
⋮
172.89.255.192/26 **to** 172.89.255.255/26 —— 16th subnet
So first host address will be 172.89.0.1/26 and last host address will be 172.89.255.245/26.

17. (c)
Broadcast address = 173.140.31.255
173 is class B
31.255 = 00011111.11111111
(A) 240.0 ⇒ 11110000.00000000 ⇒ 12 bits are host
(B) 248.0 ⇒ 11111000.00000000 ⇒ 11 bits are host
(C) 192.0 ⇒ 11000000.00000000 ⇒ 14 bits are host
14 bits of host remains all 14 bits should be 1's in broadcast address, this condition is violating. So 255.255.128.0 cannot suit for given address.

18. (b)
- Passive scanning is a process of scanning channels and listening for beacon frames.
- A wireless host can perform active scanning by broadcasting a probe frame that will be received by all APs within the wireless host range.