NEERAJ®

M.C.S.-218

Data Communication And Computer Networks

Chapter Wise Reference Book
Including Many Solved Sample Papers

Based on

I.G.N.O.U.

& Various Central, State & Other Open Universities

By: *Anand Prakash Srivastava*

NEERAJ PUBLICATIONS
(Publishers of Educational Books)

Mob.: 8510009872, 8510009878 E-mail: info@neerajbooks.com
Website: www.neerajbooks.com

MRP ₹ 380/-

Content

DATA COMMUNICATION AND COMPUTER NETWORKS

Question Paper—June-2024 (Solved) 1-5
Question Paper—December-2023 (Solved) 1-8
Question Paper—June-2023 (Solved) 1-6

S.No.	*Chapterwise Reference Book*	*Page*

BLOCK-1: INTRODUCTION TO DATA COMMUNICATION

1. Introduction to Internet 1
2. Data Transmission Basics and Transmission Media 17
3. Data Encoding and Multiplexing 32
4. Multiplexing and Switching 43

BLOCK-2: MEDIA ACCESS CONTROL AND DATA LINK LAYER

5. Data Link Layer Fundamentals 58
6. Retransmission Strategies 73

S.No.	Chapterwise Reference Book	Page
7.	Contention-based Media Access Protocols	83
8.	Warless LAN and Datalink Layer Switching	92

BLOCK-3: NETWORK LAYER

9.	Introduction to Layer Functionality and Design Issues	106
10.	Routing Algorithms	119
11.	Congestion Control Algorithms	136
12.	Emerging Networking Technologies	145

BLOCK-4: TRANSPORT LAYER AND APPLICATION LAYER SERVICES

13.	Transport Service and Mechanism	161
14.	TCP/UDP	171
15.	Network Security-I	186
16.	Network Security-II	203

■■

Sample Preview of the Solved Sample Question Papers

Published by:

NEERAJ PUBLICATIONS

www.neerajbooks.com

QUESTION PAPER

June – 2024

(Solved)

DATA COMMUNICATION AND COMPUTER NETWORKS

M.C.S.-218

***Time*: 3 Hours]** **[*Maximum Marks* : 100**

***Note*:** *(i) Question No. 1 is compulsory. (ii) Attempt any three questions from the rest.*

Q. 1. ***(a)*** **Differentiate between Analog and Digital signals. Draw the diagrams for both.**

Ans. Ref.: See Chapter-2, Page No. 18-19, 'Analog and Digital Data Transmission' and Page No. 23-24, Q. No. 4.

(b) **Define vulnerable period. Give an expression of throughput in pure ALOHA. Also differentiate pure ALOHA with slotted ALOHA.**

Ans. The vulnerable period in the context of networking and communication refers to the time window during which a data frame is susceptible to collisions. It is a critical concept in protocols that manage access to the network medium, such as CSMA/CD (Carrier Sense Multiple Access with Collision Detection) and CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).

Also Add: Ref.: See Chapter-7, Page No. 83-85, 'Pure Aloha', 'Slotted Aloha'.

(c) **Define bridge. In which scenario bridge should be used? What are the characteristics of it?**

Ans. Ref.: See Chapter-8, Page No. 97-97, 'Switching at Data Link Layer' and Page No. 104, Q. No. 6.

(d) **Describe transmission and propagation delays. Explain the working of a fibre-optic cable.**

Ans. Ref.: See Chapter-2, Page No. 23, Q. No. 3

Also Add: The working of a fibre optic cable involves transmitting data in the form of light pulses through a thin strand of glass or plastic. Here's a detailed explanation of how fibre optic cables work:

Structure of Fiber Optic Cable

1. Core:

- The core is the central part of the fibre optic cable through which light travels. It is made of a very pure glass or plastic material.
- Light signals (usually infrared light) are transmitted through the core, bouncing off the walls of the core due to a principle called total internal reflection.

2. Cladding:

- Surrounding the core is the cladding, which is a layer of glass or plastic with a lower refractive index than the core.
- The cladding ensures that light signals remain within the core through reflection. When light encounters the core-cladding boundary at an angle greater than the critical angle, it reflects back into the core rather than escaping.

3. Buffer Coating:

- The core and cladding are typically coated with a buffer layer made of a protective material such as acrylate polymer.
- The buffer coating provides mechanical protection to the delicate fibers and serves as a cushion against physical damage.

4. Strength Members:

- Fiber optic cables often include additional strength members, such as aramid yarn (e.g., Kevlar) or fiberglass, to provide tensile strength and protect against stretching and bending.

5. Outer Jacket:

- The outermost layer of the fibre optic cable is the outer jacket, made of durable materials like PVC (polyvinyl chloride) or LSZH (low smoke zero halogen).
- The jacket protects the entire cable from environmental factors such as moisture, chemicals, and physical abrasion.

Working Principle of Fiber Optic Cable

1. Transmitter:

- At one end of the fibre optic cable, data is converted into light signals by a transmitter.
- The transmitter typically uses a light-emitting diode (LED) or a laser diode to generate light pulses.

2. Propagation through the Core:

- Light pulses generated by the transmitter travel through the core of the fiber optic cable.
- As the light travels down the core, it repeatedly undergoes total internal reflection at the core-cladding boundary, ensuring minimal loss of signal strength.

3. Receiver:

- At the other end of the fibre optic cable, a receiver detects the light pulses.

QUESTION PAPER

December – 2023

(Solved)

DATA COMMUNICATION AND COMPUTER NETWORKS

M.C.S.-218

***Time*: 3 Hours]** **[*Maximum Marks* : 100**

***Note*:** *(i) Question No. 1 is compulsory. (ii) Attempt any three questions from the rest.*

Q. 1. ***(a)*** **Define Network Topology. Compare Star and Bus topologies.**

Ans. Ref.: See Chapter-1, Page No. 5, 'Network Topology'.

Also Add: Here's a comparison of Star and Bus topologies:

Feature	Star Topology	Bus Topology
Structure	Centralized, all nodes connected to a central hub/device	Linear, all nodes connected to a single backbone
Topology Type	Point-to-point	Multi-point
Reliability	More reliable; failure in one node doesn't affect others	Less reliable; failure in backbone affects all nodes
Scalability	Easier to scale by adding more nodes directly to hub	Limited scalability due to potential signal degradation
Installation	Easy to install and reconfigure	Easy to install; requires less cabling
Performance	Better performance with fewer collisions	Performance degrades with more nodes or heavy traffic
Cost	Higher cost due to hub device and cabling	Lower cost due to simpler structure and less cabling

(b) **Define Hamming Code. Write the bit stream generated by Hamming code for 001100.**

Ans. Hamming Code is a type of error-correcting code that adds extra parity bits to data to detect and correct errors during transmission. It ensures data integrity by adding redundancy.

For a given data word, Hamming Code calculates parity bits that cover certain combinations of bits (parity bits cover specific positions in the data word). Here's how it works:

1. Identify Parity Bits Positions: Determine the positions of parity bits. In Hamming Code, these are typically powers of 2 (1, 2, 4, 8, etc.).

2. Insert Data Bits: Insert the original data bits into the remaining positions, leaving placeholders for the parity bits.

3. Calculate Parity Bits: Calculate the values of the parity bits based on the positions they cover (e.g., parity bit at position 1 covers bits 1, 3, 5, 7, ...).

4. Construct the Hamming Code Word: Combine the data bits with the calculated parity bits to form the Hamming Code word.

Let's apply this to the bit stream "001100":

1. Identify Parity Bit Positions:

Parity bit at position 1**:** covers bits 1, 3, 5, 7, ...

Parity bit at position 2**:** covers bits 2, 3, 6, 7, ...

Parity bit at position 4**:** covers bits 4, 5, 6, 7, ...

2. Insert Data Bits: Place the data bits (001100) into positions 3, 5, 6, and 7, leaving positions 1, 2, and 4 for parity bits.

3. Calculate Parity Bits:

Parity bit at position 1**:** XOR of bits at positions 1, 3, 5, 7 ($1 \oplus 0 \oplus 0 \oplus 0 = 1$)

Parity bit at position 2**:** XOR of bits at positions 2, 3, 6, 7 ($0 \oplus 0 \oplus 0 \oplus 0 = 0$)

Parity bit at position 4**:** XOR of bits at positions 4, 5, 6, 7 ($1 \oplus 0 \oplus 0 \oplus 0 = 1$)

Sample Preview of The Chapter

Published by:

NEERAJ PUBLICATIONS

www.neerajbooks.com

DATA COMMUNICATION AND COMPUTER NETWORKS

Introduction to Internet

1

INTRODUCTION

The age of computers, or more specifically, the age of digital data, is now. Computers are used by any business, no matter how big or small, domestic or international, with one or more locations, to perform a variety of transactions. They are also used to exchange information across sites spread over various geographically remote locations. The computer Internet is a method for exchanging data among geographically dispersed computers. A network is made up of entities that are linked together to exchange information. The computer network is what happens when things are replaced by computing devices. In a matter of seconds, digital information may be accessed instantly from one end of the earth to the other. The sharing of digital information over computer networks has significantly enhanced efficiency across all organisations, regardless of their industry. A computer network consists of two or more independent computers linked together to exchange data, resources, communications, etc., regardless of where they are physically located.

CHAPTER AT A GLANCE

WHAT IS THE INTERNET?

The largest computer network having a global reach is the Internet. It is a network within a network. There are thousands of different sorts of organisational networks on the Internet, including domestic and international, academic and commercial, and governmental ones. These networks all exchange different kinds of data and information. 'Net' is a common way we refer to the Internet in everyday speech. It allows billions of individuals from all over the world to share knowledge by connecting them via computers or mobile devices. ARPANET was the first all-purpose computer network in existence. The Bob Taylor is credited for founding the Internet. He started the project in 1 966 to make it possible to access computers from a distance. As a result, the first remote computer access occurred in 1969. This marked the beginning of the digital information and computer world as we know it today.

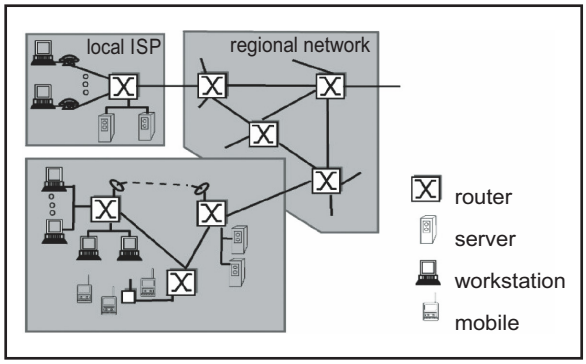

Fig. 1: Overview of the Internet

The public Internet is a global computer network that connects millions of computing units that are dispersed around the globe. Computers, laptops, smartphones, and web TVs are examples of computing devices.

ISP and Internet Backbone

ISP: The movement of traffic on the Internet is the responsibility of ISPs (Internet Service Providers). The Internet is extremely large in terms of traffic, the number of end systems, the number of intermediary devices, the interconnecting networks, and the geographic dispersion of these. As a result, there are many ISPs that run the Internet.These ISPs are categorised into three groups—tier-1, tier-2, and tier-3—in order to effectively manage and control Internet services. This hierarchical concept is known as the "3-tier model". Depending on the kind of Internet services they offer, ISPs fall under the tier-1, tier-2, or tier-3 categories.

As soon as we have an Internet connection, any of us can act as an access ISP. All we have to do to enable other users or clients to connect to us is purchase the necessary gear or software (such as a router, modem, firewall, etc.). It's as easy to add additional tiers and branches to the Internet as it is to add a new Lego piece to an existing Lego structure.

Interconnection of ISPs

Through this three-tier architecture of ISPs, as depicted in Figure, end systems or hosts located at the Internet's edge are connected to the rest of the Internet.

Internet Backbone: Internet backbone, a core network, handles high-speed traffic and connects other networks for global data transfer. Internet backbone is mostly tier-1 ISP networks. It links all tier-1 ISPs and transmits most Internet traffic. The internet backbone consists of several routers, switches, and other intermediary devices linked by high-speed optical fiber cables. Companies may create their own backbone infrastructure for office connection. The PC connects to a tier -3 ISP's access network, which links to the main Internet backbone (tier -2 or tier -1) to access the global network.

Taxonomy of Network

- A Local location Network (LAN) is a network that is constrained to a certain location, such as a building or campus. In an organization or institution, personal computers form a local area network to share resources and information, such as printers and scanners.
- The Metropolitan Area Network (MAN) covers a city and has a range of 100 kilometres. Man may be wired or wireless. Examples of MAN include city-based cable TV and broadband networks (wired and wireless).
- A Wide region Network (WAN) spans a broad geographical region, including cities, states, and even nations. A WAN connects millions of computers over a vast area. The Internet is the biggest ever-established Wide Area Network.

Standard Internet Protocols

Any effective communication must adhere to a certain set of rules, known as the protol. A protocol enables communication between computers. A protocol outlines the many types of data that can be transferred, the commands used to send and receive data, and the procedures for confirming when data has been received.

Some protocols must be followed in spoken language interactions between people in order to communicate, share, or exchange any information. Every spoken language has a set of guidelines that must be adhered to when communicating. Use a language that both the sender and the recipient understand in order to improve communication. This is the first and most important guideline in human communication. If two people can talk and understand one another in a similar language, such as Hindi, English, or any other, they can communicate with one another. Similar to this, a hardware device can communicate with other hardware that supports the same protocols, regardless of the device's type or manufacturer. Similar to how an email sent from an iPhone can be received on an Android device thanks to a shared mail protocol.

Various protocols are created for networking applications on the Internet. IEEE 802.11 protocol, which is used in wireless communication, is similar to the Ethernet protocol used in wired networks. A collection of common protocols used for data transmission over the Internet is known as an Internet protocol suite.

Standard Internet protocols may be classified into four major categories:

1. **Application layer:** Hyper Text Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP).
2. **Transport layer:** Transmission Control Protocol (TCP), UserDatagram Protocol (UDP).
3. **Network layer:** Internet Protocol (IP) version 4 and version 6
4. **Data link layer:** Ethernet, IEEE 802.11 (Wi-Fi).

Application layer protocols, including HTTP for accessing webpages and SMTP for sending emails, are made to make it easier for Internet users to use a variety of Internet resources. You can employ a variety of application layer protocols. The method data is transmitted, received, and accurately confirmed receipt is defined by the transport layer. There are two methods of data transmission offered by the transport layer: dependable data delivery and faulty data delivery. TCP offers trustworthy data delivery, which means that it can be verified that sent data is received correctly and undamaged, whereas UDP offers unreliable data delivery, which means that data is sent but no attempt is made to verify reception. Data routing on the Internet is handled by network layer protocols.

Public Network & Private Network (Intranet)

Anyone may connect to a public network because it is an open network. The best example of a public network is the internet. With the exception of the security, addressing, and authentication methods in place, there is no technological distinction between a private and public network in terms of hardware and infrastructure. the absence In a public network, there are usually no limits or access control rules that must be followed in order to connect and use the network's

resources. Public networks are the least secure since the fewest security mechanisms are in place there; as a result, one must be extremely cautious when connecting to a public network.

Access to a private network is limited, and it is monitored and governed by a central authority. Schools, universities, and other organizations' networks are instances of private networks. In a private network, the network administrator can impose restrictions on who can access the Internet, what can be accessed, and how much can be accessed. Intranet is another name for private network. Intranet refers to a computer network used exclusively within an organisation for the exchange of information and the provision of computing services.

While private domain IP addresses should be assigned to the systems in a private network, public domain IP addresses are utilised in public networks. NAT (network address translator), which translates private IP addresses to public IP addresses before entering the public network, is necessary in private networks. Public domain IP addresses can only be used on a single system in a public network, however private domain IP addresses used in a private network or intranet can be reused in other private networks. One needs a public IP address to connect to the Internet's public network, which can be acquired from your ISP.

Accessing the Internet

Any of the three available technologies, namely wireless network, cable network, and telephone network, can be used to access the Internet.

Telephone Network

The public switched telephone network, or PSTN for short, is a global telephone system used for voice communications. Installing a new infrastructure for data in addition to the current PSTN is not an easy or worthwhile solution; instead, the infrastructure already in place for voice communication is used for data transmission as well. Therefore, the telephone network system is a necessary and integral component of the transmission of computer data. Dial-up configuration is used for the very first data connection over telephone lines. Dedicated lines were created as a further improvement.

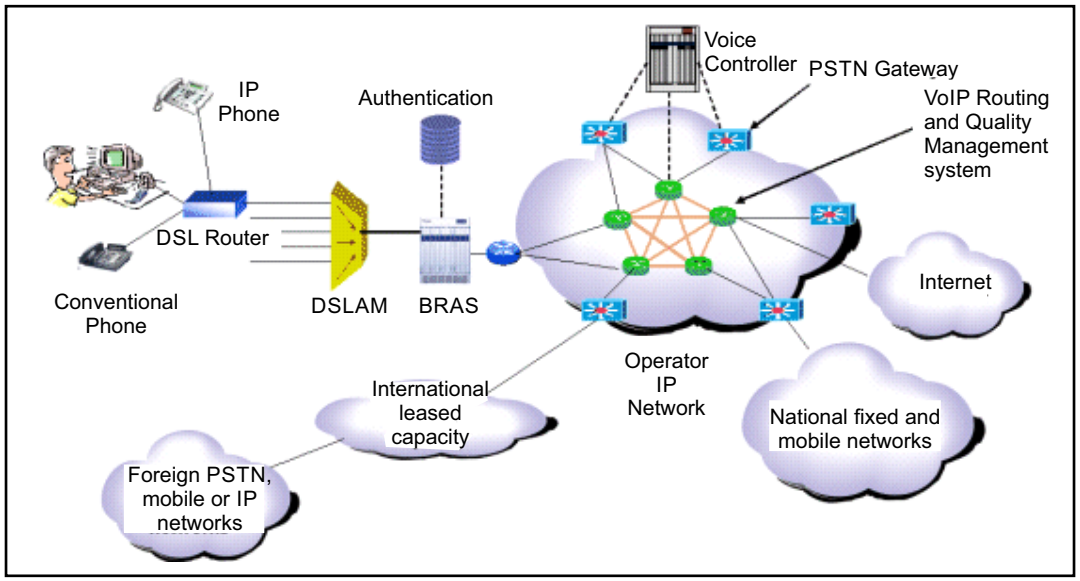

Fig. 2: PSTN Network

Dial-Up Lines: Installing a modem on both the sender side and the receiver side is necessary when setting up a data connection over existing analog telephone lines. The dial-up arrangement used to establish a data connection over the phone line is the same one used to establish a voice conversation. A temporary link between the transmitter and the recipient must be established before to transferring the computer data. The modem on the sender side dials the modem on the receiver side's phone number to establish the connection. Data transfer is possible once the link has been made. Either party to the communication can close the connection after the data transmission is finished. No other connections between end devices can be made throughout the communication, however at some point, voice or data communication may be feasible. Over the dialup connection, the data transmission speed is incredibly slow. The fastest speed possible with a dial-up connection is 56 kbps.

The following are some benefits of dial-up connections: Low price and accessibility.

The following are some drawbacks of dial-up connections: Low data transmission speed, requires a phone line, making it impossible to use it for both speech and data communication over the telephone, connection must be created every time, and Route busy: no other connections could be made between communicating end devices.

Dedicated Lines: Dedicated lines eliminate the need to dial the other end's phone number in order to create a connection. The data connection is created separately from the voice connection via a dedicated line. It is an always-on connection type, therefore a connection does not need to be formed every time it is used. As opposed to dial-up lines, dedicated lines offer a higher quality connection for data transmission. Analog lines and digital lines are the two subcategories of dedicated lines. In the current environment, digital lines are frequently utilized to link end customers to the global Internet. Compared to analog lines, dedicated digital lines transmit data far more quickly. ISDN and DSL are two types of dedicated digital lines.

Integrated Services Digital Network (ISDN): When compared to dial-up lines, data transmission over the Integrated Services Digital Network (ISDN) is much faster.

Digital Subscribe Line (DSL)

Using the current telephone lines, DSL is utilized to send information quickly.

Cable Network

Cables are utilized as the network's transmission medium in cable networks. Access to the Internet through cable is made possible by the existing cable infrastructure for television. Additionally known as broadband Internet access. In the cable network, Internet access is provided by a cable modem device. The cable network uses coaxial cable for connectivity. Dial-up and DSL connections cannot match the up to 1 Gbps speed offered by cable Internet.

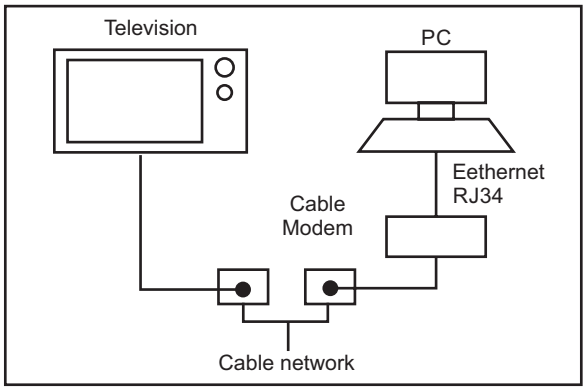

Fig. 3: Cable Network

The cable network of television infrastructure is used from the Internet service provider to the end user to provide last-mile access, or cable Internet. In the current environment, fiber optic networks, wireless networks, and mobile networks are stifling cable Internet access.

The benefits of using cable Internet access include high-speed data transfer, quick installation and use, and the fact that it doesn't utilize telephone lines to operate.

Internet connectivity has a number of drawbacks, including the fact that it is more expensive than dial-up and DSL connections and less secure overall. Additionally, not all cable television networks offer this option.

Wireless Network

It is substantially less expensive to establish and operate wireless networks. Installation of a wired network is not necessary for wireless network architecture. To create a wireless network, you need an access point, router, and wireless modem. To construct a wireless network, a variety of wireless technologies are available. Some of the wireless technologies frequently used to set up a wireless network include Bluetooth, InfraRed, Wi-Fi, and others. One of the most commonly utilized technologies for wireless networks is Wi-Fi (wireless Fidelity). A Wi-Fi capable modem typically has a range of about 90 meters. The maximum possible connection speed is 1544 Kbps.

Internet Services

One can access information on the Internet by using Internet services. Communication services, information retrieval services, web services, and world wide web are the four main categories into which these Internet services can be divided.

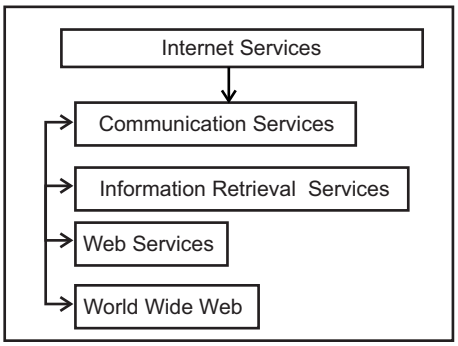

Fig. 4: Internet Services

Communication Services: Communication services allow Internet information sharing.

One popular communication method is email.

Electronic mail is a method of exchanging communications electronically. Other communication services include Telnet, which establishes and exchanges communications between distant computers. Internet