# GUJARAT TECHNOLOGICAL UNIVERSITY (GTU)

**Subject Name :** Mobile Computing and Networks

**Subject Code :** 4351602

**Teaching and Examination Scheme :**

| Teaching Scheme (In Hours) | | | Total Credits (CI+T/2+P/2) | Examination Marks | | | | Total Marks |
|---|---|---|---|---|---|---|---|---|
| | | | | Theory Marks | | Practical Marks | | |
| CI | T | P | C | CA | ESE | CA | ESE | |
| 3 | 0 | 2 | 4 | 30 | 70 | 25 | 25 | 150 |

**Legends :** L-Lecture; T – Tutorial/Teacher Guided Theory Practice; P -Practical; C – Credit, CA - Continuous Assessment; ESE -End Semester Examination.

**Detailed Cource Content :**

| Unit | Unit Outcomes (UOs) (4 to 6 UOs at Application and above level) | Topics and Sub-topics |
|---|---|---|
| **Unit–I Networking Essential** | 1a. Differentiate different models of Network Computing.<br>1b. Explain OSI Model and TCP/IP of each layer.<br>1c. Describe Data traffic and Congestion Management. | 1.1 Models of Network Computing<br>– Centralized Computing<br>– Distributed Computing<br>– Collaborative Computing<br>1.2 Client Server Network and Peer to Peer Network<br>1.3 Need of layered mechanism<br>1.4 OSI Model<br>– Responsibilities of each layer<br>1.5 TCP/IP Protocol Suite<br>– Comparison of TCP/IP with OSI model<br>– List of Protocols at each layer of TCP/IP and a brief description of each protocol<br>1.6 Data Traffic<br>– Traffic descriptor<br>– Traffic profiles<br>1.7 Congestion<br>– Network Performance<br>1.8 Congestion Control<br>– Open-Loop Congestion Control<br>– Closed-Loop Congestion Control |

| | | |
|---|---|---|
| **Unit–II Protocol and Addressing Scheme** | 2a. Explain different protocols of the OSI layer.<br>2b. Explain IPv4 and IPv6 addressing scheme.<br>2c. Describe Subnetting and Supernetting of IPv4. | 2.1 ARP,RARP (Introduction)<br>2.2 Routing<br>– Types of routing<br>– Routing table<br>2.3 SMTP, POP, IMAP (Introduction)<br>2.4 Introduction to WWW and HTTP/S<br>2.5 Data link layer protocols<br>– Simplest, stop and wait, stop and wait ARQ<br>2.6 IPv4 addressing scheme<br>– Classful and classless notations<br>– Ipv4 datagram header<br>– Subnetting and Supernetting<br>– Network address translation<br>– Advantages, Disadvantages<br>2.7 IPV6 Addressing<br>– Need for IPv6 migration<br>– IPv6 advantages |
| **Unit–III Introduction to Mobile Computing** | 3a. Explain Architecture for Mobile Computing.<br>3b. Explain Ad Hoc Networks.<br>3c. Describe Middleware and Gateway.<br>3d. List out Application of Mobile Computing. | 3.1 Evolution of Mobile Computing<br>3.2 Architecture for Mobile Computing<br>3.3 Networks (Brief)<br>– Wireless Networks<br>– Ad-hoc networks<br>– Bearer<br>3.4 Middleware and Gateways (Brief)<br>– Communication middleware<br>– Transaction processing Communication middleware<br>– Behavior management middleware<br>– Communication Gateways<br>3.5 Application and Services<br>3.6 Security and Standards |
| **Unit–IV Mobile Network and Transport Layer** | 4a. Explain Packet Delivery, handover management and Location management.<br>4b. Differentiate Indirect TCP, snooping TCP and Mobile TCP.<br>4c. Explain TCP over 3.0 G mobile. | 4.1 Mobile IP<br>– Goals, assumptions and requirements<br>– Entities and terminology<br>4.2 Packet Delivery, handover management and Location management<br>4.3 Registration, Tunneling and encapsulation<br>4.4 Dynamic host configuration (Introduction)<br>4.5 Indirect TCP, snooping TCP and Mobile TCP<br>4.6 TCP over 3.0 G mobile |

| Unit–V Technologies in Trends | 5a. Explain Architecture of WLAN<br>5b. Explain Bluetooth<br>5c. Differentiate 4G, 5G and 6G Mobile Network. | 5.1 WLAN<br>– Introduction of WLAN<br>– Architecture of WLAN<br>– Types of WLAN<br>5.2 WPAN<br>– Introduction of WPAN<br>– Applications in WPAN - Bluetooth, architecture and Bluetooth protocol stack<br>5.3 Mobile Networks<br>– 4G, 5G, 6G (Introduction, features) |
|---|---|---|

**Note :** The UOs need to be formulated at the 'Application Level' and above of Revised Bloom's Taxonomy' to accelerate the attainment of the COs and the competency.

**Suggested Specification Table for Question Paper Design :**

| Unit No. | Unit Title | Teaching Hours | Distribution of Theory Marks | | | |
|---|---|---|---|---|---|---|
| | | | R Level | U Level | A Level | Total Marks |
| 1 | Networking Essential | 8 | 2 | 6 | 2 | 10 |
| 2 | Protocol and Addressing Scheme | 10 | 4 | 8 | 6 | 18 |
| 3 | Introduction to Mobile Computing | 4 | 8 | 8 | 4 | 16 |
| 4 | Mobile Network and Transport Layer | 10 | 6 | 10 | 0 | 16 |
| 5 | Technologies in Trends | 6 | 2 | 8 | 0 | 10 |
| | **Total** | **42** | **18** | **40** | **12** | **70** |

**Legends :** R – Remember, U – Understand, A – Apply and above (Revised Bloom's taxonomy)

**Note :** This specification table provides general guidelines to assist students for their learning and to teachers to teach and question paper designers/setters to formulate test items/questions assess the attainment of the UOs. The actual distribution of marks at different taxonomy levels (of R, U and A) in the question paper may vary from above table.

■ ✣ ■

# Index ...



■ ✳ ■

**TO THE READERS**


Authors and publisher would welcome suggestions towards future edition of this book or the pointing out of any misprint or obscurity. Please write to The Technical Editor, ATUL PRAKASHAN, Under Farnandis Bridge, Gandhi Road, Ahmedabad-1.

# UNIT–I

# NETWORKING ESSENTIAL

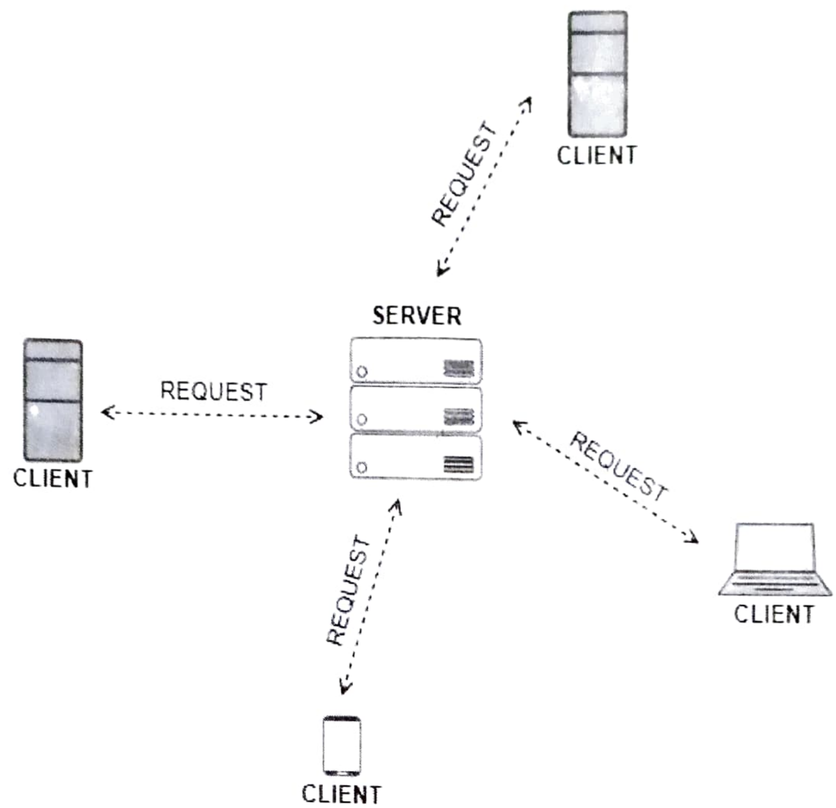
Networking essentials are the fundamental concepts, technologies, and practices that form the foundation of computer networking. Understanding these essentials is crucial for building, maintaining, and troubleshooting computer networks.

## 1.1 MODELS OF NETWORK COMPUTING

There are several models of network computing that have been developed over the years. Here are some of the commonly known models:

### 1. Centralized Computing

Centralized computing refers to a model where all the computing resources, such as servers, storage, and software applications, are located and managed in a central location or data center. In this model, all the processing and data storage tasks are performed on a central server, and users access these resources remotely through network connections. The central server is responsible for executing tasks and delivering results to the users. It provides a controlled and secure environment where resources can be efficiently managed and shared among multiple users.




**CENTRALIZED COMPUTING**

**Applications of centralized computing:**

**(1) Business Enterprises:** Many businesses use centralized computing to manage their operations and data. They set up centralized servers and data centers to store and process their critical information, such as customer data, financial records, and inventory details. Centralized computing allows for efficient data management, backup, and security measures. It also enables employees to access and share information from various locations, improving collaboration and productivity.

**(2) Educational Institutions:** Educational institutions, such as schools and universities, often adopt centralized computing models. They use central servers and systems to manage student records, course materials, and administrative tasks. Centralized computing allows for easy access to educational resources, secure storage of sensitive student information, and efficient communication among students, teachers, and administrators.

**(3) Government Organizations:** Government agencies and departments utilize centralized computing to streamline their operations and provide services to citizens. They establish centralized data centers and networks to store and process large amounts of data related to public records, taxation, healthcare, and more. Centralized computing enables secure data management, efficient processing of citizen requests, and integration of different government systems for effective governance.

**(4) Banking and Financial Institutions:** Banks and financial institutions rely on centralized computing for their core banking systems. Centralized servers and data centers are used to process transactions, store customer account information, and ensure the security of financial data.

**Advantages of centralized computing:**

(1) **Efficient Resource Management:** Centralized computing allows for the efficient management of computing resources, such as servers, storage, and software applications. With a central server or data center, resources can be allocated, monitored, and utilized effectively, ensuring optimal performance and utilization.

(2) **Simplified Administration:** In a centralized computing model, the administration and maintenance of resources are centralized, making it easier to manage. IT administrators can implement consistent policies, updates, and security measures across the entire system from a central point, reducing complexity and ensuring uniformity.

(3) **Enhanced Data Security:** Centralized computing provides a higher level of data security. Data can be stored and protected in a controlled and secure environment, such as a data center with physical security measures and advanced security protocols. This reduces the risk of unauthorized access, data loss, or data breaches.

(4) **Improved Collaboration:** Centralized computing enables better collaboration among users. With shared resources and centralized data storage, individuals and teams can access and share information easily, fostering collaboration and teamwork. This is particularly beneficial for projects that require simultaneous access to data and real-time collaboration.

(5) **Cost Savings:** Centralized computing can result in cost savings for organizations. By consolidating resources into a central server or data center, businesses can optimize hardware and software utilization, reduce the need for individual hardware and software licenses, and streamline maintenance and support costs.

(6) **Centralized Backup and Recovery:** With centralized computing, backups and disaster recovery processes can be centralized as well. Data can be regularly backed up and stored in a central location, ensuring easier recovery in case of data loss or system failures. This simplifies backup processes and improves data availability.

**Disadvantages of centralized computing:**

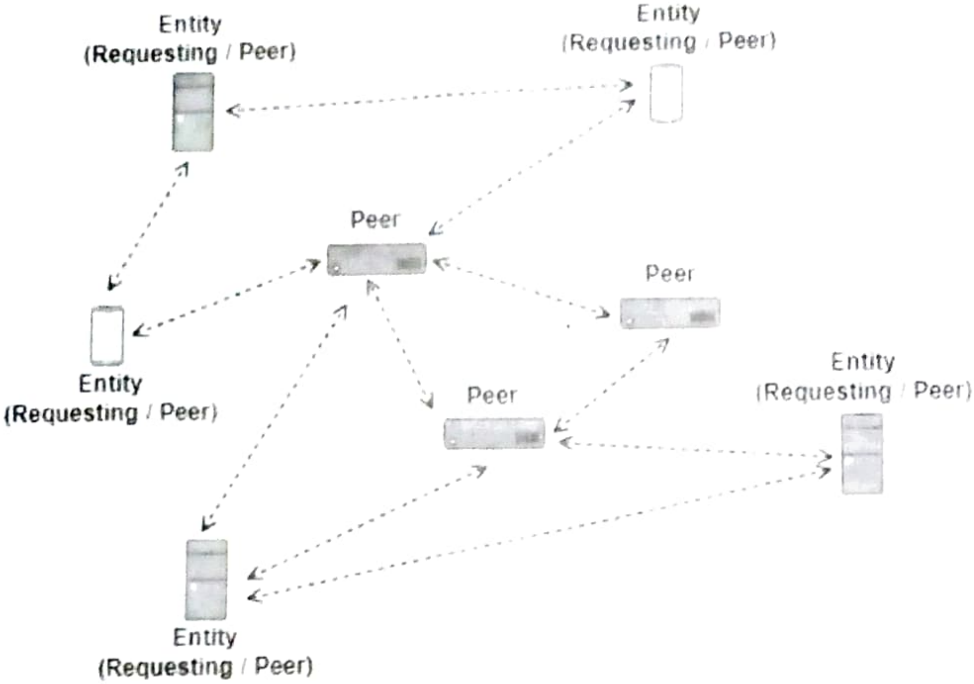
(1) **Single point of failure:** If the central system experiences a hardware or software failure, the entire system may become inaccessible.

(2) **Limited scalability:** Adding more clients or increasing computing demands may require significant upgrades to the central system, which can be costly and time-consuming.

(3) **Network dependency:** Centralized computing heavily relies on network connectivity, and any disruptions or latency issues can affect the performance of the entire system.

## 2. Distributed Computing

Distributed computing is a model where computing tasks and data processing are distributed across multiple interconnected computers or nodes. In this model, each node contributes its processing power and resources to work on a specific part of a task or process data simultaneously. The nodes communicate and coordinate with each other to achieve a common goal. Distributed computing enables parallel processing, allowing large and complex tasks to be completed faster and more efficiently. It also offers fault tolerance, as the failure of one node does not necessarily result in the failure of the entire system.




DISTRIBUTED COMPUTING

**Applications of Distributedcomputing:**

**(1) Scientific Research:** In scientific research, distributed computing is often used to tackle complex calculations and simulations. Projects like protein folding, climate modeling, and drug discovery require substantial computational power. By distributing the tasks across a network of computers, scientists can harness the combined processing power of many machines, allowing them to process large volumes of data and perform calculations much faster.

**(2) Internet Services:** Many internet services rely on distributed computing to handle high volumes of requests from users. Search engines, social media platforms, and e-commerce websites employ distributed computing to distribute user requests across multiple servers. This allows for faster response times, better handling of traffic spikes, and improved scalability to accommodate a large number of users simultaneously.

**(3) Content Delivery Networks (CDNs):** CDNs are widely used to deliver web content efficiently. They distribute content across multiple servers located in different geographical regions. When a user requests a webpage or media file, the content is delivered from the nearest server in the CDN, reducing latency and improving the user experience. By distributing the content, CDNs can handle high traffic loads and ensure faster content delivery.

**(4) Blockchain Technology:** Blockchain, the underlying technology of cryptocurrencies like Bitcoin, relies on distributed computing. A blockchain is a decentralized and distributed ledger that records transactions across multiple nodes in a network. Each node contributes to the verification and validation of transactions, ensuring the security and integrity of the blockchain.

**(5) Grid Computing:** Grid computing refers to the coordinated use of distributed computing resources across multiple organizations or institutions. It is commonly used in scientific collaborations, such as in physics and astronomy, where large-scale data analysis and processing are required. By sharing computational resources across multiple sites, grid computing enables scientists to tackle complex problems that require significant computing power.

(6) **Distributed File Sharing:** Peer-to-peer file sharing systems, like BitTorrent, utilize distributed computing. In such systems, files are divided into smaller pieces, and each participating user contributes their resources to upload and download these pieces. This distribution of tasks allows for faster file transfers and reduces the burden on individual servers.

**Advantages of Distributed Computing:**

(1) **Faster Processing:** With distributed computing, tasks can be divided and processed simultaneously across multiple computers. This results in faster execution of complex calculations and data processing.

(2) **Increased Reliability:** Distributed computing improves reliability by distributing tasks and data across multiple computers. If one computer fails or experiences issues, the system can continue functioning as other computers can pick up the workload.

(3) **Better Scalability:** Distributed computing allows for easy scalability by adding more computers to the network. This ensures that the system can handle increasing workloads and accommodate growing demands without sacrificing performance.

(4) **Cost Efficiency:** By utilizing existing resources across multiple computers, distributed computing can be more cost-effective compared to investing in high-end individual machines. It allows organizations to make the most of their existing infrastructure.

(5) **Enhanced Fault Tolerance:** Since tasks are distributed among multiple computers, if one computer fails or experiences issues, the impact on the overall system is minimized. This fault tolerance ensures uninterrupted operation and reduces the risk of system failures.

**Disadvantages of distributed computing include:**

(1) **Complexity:** Designing and managing distributed systems can be challenging due to the need for synchronization, load balancing, and communication between nodes.

(2) **Network overhead:** Distributed systems require efficient communication and data transfer between nodes, which can introduce network overhead and latency.

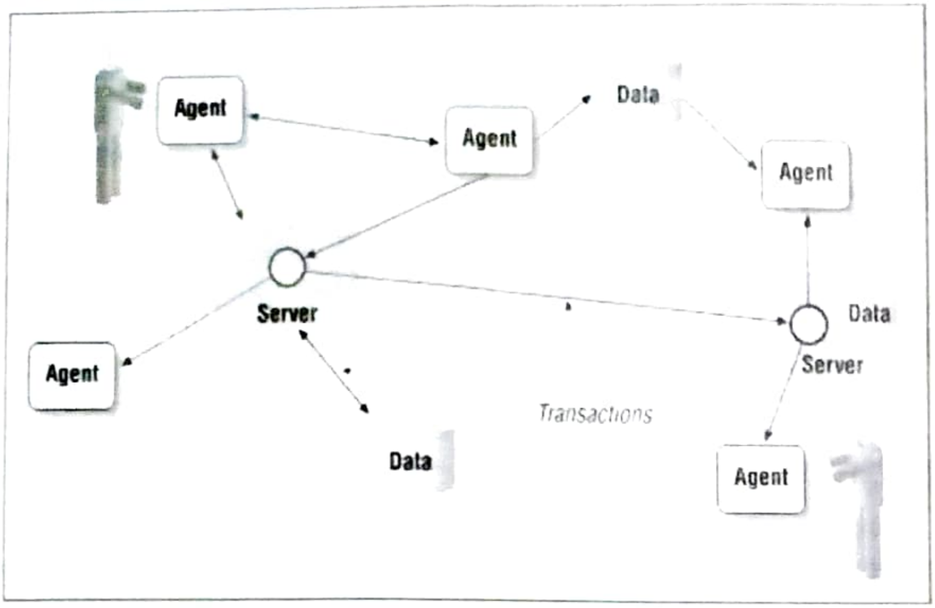
(3) **Data consistency:** Ensuring data consistency across multiple nodes can be complex, especially when dealing with concurrent updates or distributed transactions.

## 3. Collaborative Computing

Collaborative computing, also known as collaborative network computing, involves a group of interconnected computers or devices working together to solve a problem or achieve a common objective. Unlike centralized or distributed computing, where the focus is on resource sharing or parallel processing, collaborative computing emphasizes collaboration and cooperation among users and devices. It enables individuals or groups to share information, exchange ideas, and work together in real-time, regardless of their physical location. Collaborative computing can involve various tools and technologies, such as instant messaging, video conferencing, document sharing, and real-time collaboration platforms, to facilitate communication and collaboration among users.

**Applications of Collaborative computing:**

(1) **Online Collaboration Tools:** Collaborative computing finds extensive application in online collaboration tools such as project management platforms, shared document editing, and video conferencing software. These tools allow individuals and teams to work together in real-time, regardless of their physical location. They can collaborate on documents, share ideas, communicate through video calls, and track project progress, fostering effective teamwork and productivity.




COLLABORATIVE COMPUTING

(2) **Virtual Meetings and Remote Work:** Collaborative computing enables virtual meetings and remote work scenarios. Through video conferencing, screen sharing, and instant messaging tools, individuals and teams can collaborate and communicate seamlessly, regardless of their physical proximity. This facilitates remote work setups, where employees can collaborate and contribute to projects from different locations, increasing flexibility and efficiency.

(3) **Online Learning and Education:** Collaborative computing plays a significant role in online learning and education. Virtual classrooms, learning management systems, and online discussion forums enable students and teachers to interact and collaborate remotely. Students can participate in group projects, share resources, and engage in collaborative learning activities, fostering an interactive and inclusive educational environment.

(4) **Social Networking and Social Media:** Social networking platforms and social media rely on collaborative computing. Users can connect, share content, and engage in discussions, creating a collaborative and interactive online community. Features like comment threads, likes, and shares facilitate collaboration and knowledge exchange among users.

**Advantages of Collaborative computing:**

(1) **Enhanced Collaboration:** Collaborative computing enables individuals and teams to work together more effectively. It fosters communication, knowledge sharing, and real-time collaboration, allowing for seamless teamwork regardless of physical location. This leads to improved productivity and outcomes.

(2) **Increased Efficiency:** By providing a platform for real-time collaboration, collaborative computing streamlines work processes and reduces time wasted on email exchanges and version control issues. Multiple people can work on the same document simultaneously, making edits and updates instantly visible to others, which saves time and effort.

(3) **Improved Decision Making:** Collaborative computing allows for collective decision making by enabling individuals to share their ideas, insights, and perspectives. It facilitates brainstorming sessions, discussions, and collaborative problem-solving, leading to better-informed decisions and innovative solutions.

(4) **Flexibility and Remote Work:** Collaborative computing supports remote work and flexible work arrangements.

(5) **Knowledge Sharing and Learning:** Collaborative computing facilitates knowledge sharing among team members. It provides a platform to exchange information, share resources, and learn from one another.

(6) **Improved Accountability and Transparency:** Collaborative computing platforms often provide features like task assignment, progress tracking, and document versioning.

(7) **Seamless Communication:** Collaborative computing tools offer various communication features like chat, video conferencing, and notifications. These features enable seamless communication, quick information sharing, and efficient feedback loops, enhancing team coordination and reducing communication barriers.

**Disadvantages of Collaborative computing:**

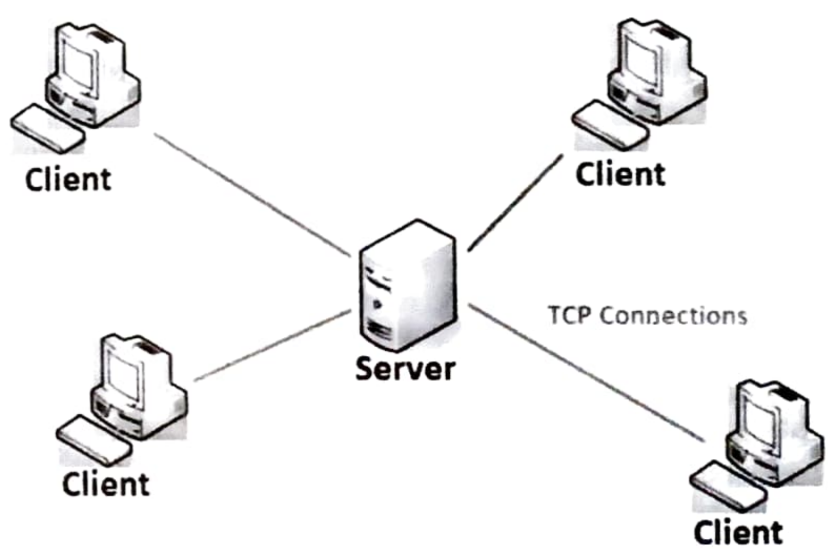
(1) **Dependency on Technology:** Collaborative computing heavily relies on technology and software platforms. If there are technical issues, such as system downtime, connectivity problems, or software compatibility issues, it can hinder collaboration and disrupt work processes. This dependency on technology increases the risk of interruptions and requires users to have a certain level of technical proficiency.

(2) **Security Risks:** Collaborative computing involves sharing and accessing sensitive information and data. There is a risk of data breaches, unauthorized access, or accidental exposure of confidential information if proper security measures are not in place. It is essential to implement robust security protocols, access controls, and encryption methods to mitigate these risks.

## 1.2 CLIENT SERVER AND PEER TO PEER NETWORK

### 1. Client Server Network:

In a client-server network, there are two main components: the client and the server. The client refers to a device or computer that requests and consumes resources or services from the server. Examples of clients can be laptops, smartphones, or desktop computers. The server, on the other hand, is a powerful computer or device that provides resources, services, or data to the clients.




CLIENT SERVER

In a client-server network, clients send requests to the server for specific resources or services, such as accessing files, retrieving data from a database, or requesting a web page. The server processes these requests and provides the requested resources or services back to the clients. The server is responsible for managing and storing the resources, ensuring security, and coordinating communication between the clients.

An analogy to understand client-server network is visiting a restaurant. The customers (clients) sit at their tables and make requests to the waitstaff (server) for food and drinks. The waitstaff takes the orders, delivers them to the kitchen, and brings the prepared food back to the customers.

**Advantages of Client Server:**

**(1) Resource Sharing:** The client-server model facilitates efficient sharing of resources. Common resources such as files, printers, and databases can be stored and managed on the server, making them accessible to multiple clients. This enables easier collaboration, data consistency, and eliminates the need for duplicate resources on individual client devices.

**(2) Centralized Data Storage and Backup:** With the client-server model, data can be stored centrally on the server, ensuring reliable data storage and backup. This reduces the risk of data loss due to device failures or other local issues. Regular backups can be performed on the server, protecting critical data and facilitating disaster recovery.

**(3) Easy Software Updates and Maintenance:** Software updates and maintenance can be easily implemented in a client-server model. Updates can be performed on the server, ensuring that all clients accessing the resources benefit from the latest features, bug fixes, and security patches. This eliminates the need to update software individually on each client device.

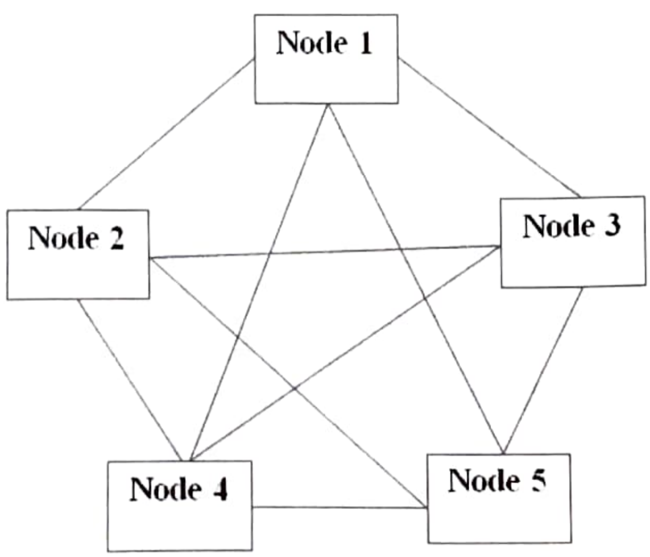
**(4) Enhanced Security:** The client-server model offers enhanced security compared to other network models. With a centralized server, security measures, such as firewalls, intrusion detection systems, and encryption, can be implemented at a single point, making it easier to protect sensitive data and control access. This reduces the risk of unauthorized access and data breaches.

**2. Peer-To-Peer (P2P) Network:**

Peer-to-Peer (P2P) network is a way for computers or devices to connect directly with each other to share files, resources, or information without the need for a central server.

Eg.Imagine you and your friends are sitting in a circle and want to share snacks. Instead of having a big table in the center where all the snacks are placed and everyone has to go there to get what they want, you pass the snacks directly to the person sitting next to you. That's how a P2P network works!

In a P2P network, each computer or device is called a "peer," and they can all communicate and share things with each other directly. This means that if one computer has a file or data that another computer needs, they can exchange it directly without relying on a central authority to coordinate the process.




PEER-TO-PEER

P2P networks are commonly used for file sharing, like when people share music or videos with each other online. They are also used in various applications, such as online gaming and communication tools, where direct connections between peers can be faster and more efficient than going through a central server.

**Applications of Peer-to-Peer:**

(1) Sharing files like music and movies directly between computers or devices without a central server.

(2) Communicating and calling others without relying on a middleman.

(3) Playing games with others online for faster and smoother gameplay.

(4) Distributing web content and software updates efficiently.

(5) Combining the power of many devices for tasks like scientific research.

(6) Creating decentralized and secure cryptocurrencies like Bitcoin.

(7) Enabling smart devices to interact and share data without a central server.

(8) Collaborating on documents or projects with others.

(9) Backing up and synchronizing data across multiple devices.

**Advantages of Peer-to-Peer:**

**(1) Decentralization:** P2P networks don't rely on a central server, which means there's no single point of failure. Everyone can connect directly, making the system more resilient.

**(2) Faster Sharing:** Files and data can be shared directly between devices, leading to faster transfer speeds compared to going through a central server.

**(3) Privacy and Security:** Since data is shared directly between peers, there's less risk of data being intercepted or manipulated by a central entity.

**(4) Less Network Congestion:** P2P networks distribute data across multiple devices, reducing the strain on any individual network connection.

**(5) Content Availability:** Popular files or data are widely available in a P2P network, reducing the chances of slow downloads or unavailability.

## 1.3 NEED OF LAYERED MECHANISM

The need for a layered mechanism in computer networks is to make communication more organized and efficient. Imagine a building with multiple floors, and each floor serves a specific purpose. Similarly, in computer networks, we use layers to divide the communication process into smaller, manageable tasks.

Each layer in the network has its own job and communicates with the layers above and below it. This layering helps to:

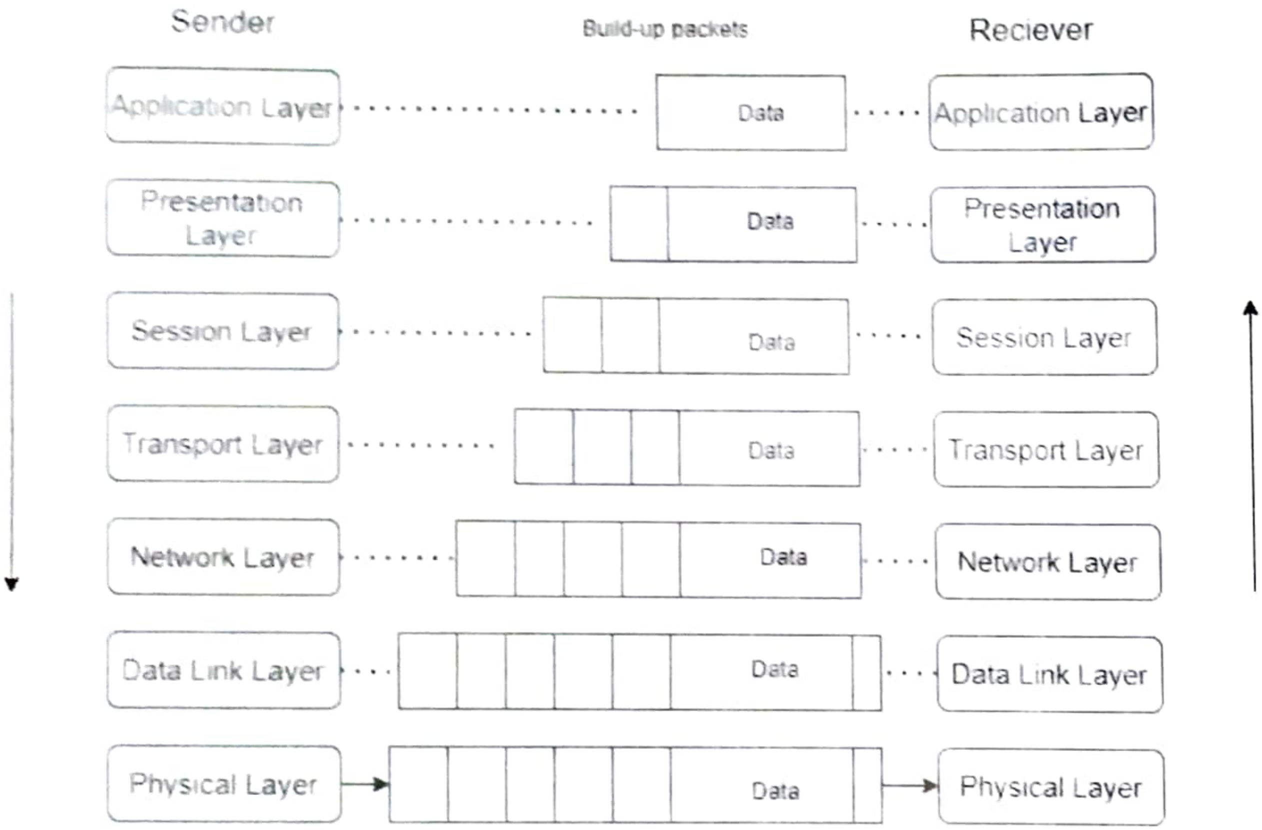
1. **Simplify Complexity:** Breaking down the communication process into layers makes it easier to understand and manage. Each layer focuses on its specific task, so we don't have to worry about all the details at once.

2. **Modularity:** Layers can be updated or replaced independently without affecting the rest of the network. It's like replacing one floor in a building without needing to change the others.

3. **Interoperability:** Different devices and technologies can work together if they follow the same layered approach. Just like people from different backgrounds can communicate better if they all speak a common language.

4. **Troubleshooting:** When an issue arises, the layered approach helps pinpoint the problem to a specific layer. This speeds up the process of finding and fixing the cause.
5. **Standardization:** Layered protocols allow for standardization, ensuring that different manufacturers and developers can build compatible network components and software.
6. **Efficiency:** By dividing tasks among layers, the network can work more efficiently. Each layer focuses on its specific job, leading to smoother and faster communication.

## 1.4 OSI MODEL




**OSI MODEL**

The OSI (Open Systems Interconnection) reference model is a conceptual framework that helps us understand how computer networks communicate with each other. It divides the communication process into seven distinct layers, each responsible for specific tasks. Let's explain each layer in simple words and its functionalities:

1. **Physical Layer (Layer 1):**
   a. **Functionality:** This is the actual physical connection of devices through wires, cables, or wireless signals.
   b. **Responsibilities:** It handles the transmission of raw bits over the network medium, like converting digital data into electrical signals for transmission and vice versa.
2. **Data Link Layer (Layer 2):**
   a. **Functionality:** This layer focuses on reliable data transfer between directly connected devices (e.g., switches and network interface cards).

b. **Responsibilities:** It frames data into packets, detects and corrects errors, and manages access to the shared communication medium to avoid data collisions.

3. **Network Layer (Layer 3):**

   a. **Functionality:** The network layer is responsible for routing data packets across different networks to reach their destination.

   b. **Responsibilities:** It determines the best path for data transmission, handles logical addressing (e.g., IP addresses), and forwards data between different subnets.

4. **Transport Layer (Layer 4):**

   a. **Functionality:** This layer ensures the reliable delivery of data between applications on the source and destination devices.

   b. **Responsibilities:** It segments data from the application layer into smaller packets, establishes and terminates connections (if needed), and manages flow control and error recovery.

5. **Session Layer (Layer 5):**

   a. **Functionality:** The session layer establishes, manages, and terminates communication sessions between applications on different devices.

   b. **Responsibilities:** It enables synchronization between applications, maintains sessions in case of interruptions, and allows for checkpointing and recovery.

6. **Presentation Layer (Layer 6):**

   a. **Functionality:** This layer focuses on data representation, ensuring that data from the application layer is in a compatible format for transmission.

   b. **Responsibilities:** It handles data encryption, compression, and formatting, ensuring that different systems can understand each other's data.

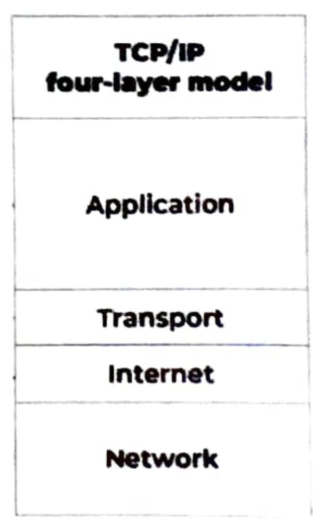
7. **Application Layer (Layer 7):**

   a. **Functionality:** The application layer is the closest to the end-users and provides network services directly to applications (e.g., web browsers, email clients).

   b. **Responsibilities:** It enables specific network applications, like file transfer, email, and web browsing, by providing a user interface and translating user requests into data that the lower layers can understand.

## 1.5 TCP/IP PROTOCOL SUIT

The TCP/IP model is another conceptual framework used in computer networks, and it is the foundation of the modern internet. It consists of four layers, each responsible for different aspects of network communication. Let's explain each layer in simple words along with its functionalities:



TCP/IP MODEL

1. **Application Layer:**

   a. **Functionality:** The application layer is the closest to the user and provides network services directly to applications (e.g., web browsers, email clients).

   b. **Responsibilities:** It enables specific network applications, like web browsing (HTTP), email (SMTP), and file transfer (FTP). This layer handles user interactions and translates user requests into data that the lower layers can understand.

2. **Transport Layer:**

   a. **Functionality:** The transport layer ensures reliable data delivery between applications on the source and destination devices.

   b. **Responsibilities:** It takes data from the application layer and breaks it into smaller chunks called segments. The transport layer also establishes and terminates connections, manages flow control to prevent data overload, and handles error recovery to ensure that data reaches its destination accurately.

3. **Internet Layer:**

   a. **Functionality:** The internet layer is responsible for routing data packets across different networks to reach their destination.

   b. **Responsibilities:** It takes the segments from the transport layer and encapsulates them into packets. This layer uses logical addressing (IP addresses) to determine the best path for data transmission and forwards the packets between different networks, ensuring they reach the correct destination.

4. **Link Layer (or Network Access Layer):**

   a. **Functionality:** The link layer is the lowest layer and deals with the actual physical connection of devices to the network medium.

   b. **Responsibilities:** It takes the packets from the internet layer and encapsulates them into frames for transmission over the physical medium, such as Ethernet or Wi-Fi. The link layer handles error detection and correction, as well as access to the shared communication medium to avoid data collisions.

### 1.5.1 COMPARISON OF TCP/IP WITH OSI MODEL

| PARAMETERS | TCP/IP | OSI MODEL |
|---|---|---|
| Name | Transmission Control Protocol/ Internet Protocol | Open System Interconnection |
| Layers | 4 a. Network Access<br>b. Internet<br>c. Transport<br>d. Application | 7 a. Physical<br>b. Data Link<br>c. Network<br>d. Transport<br>e. Session<br>f. Presentation<br>g. Application |
| Approach | Horizontal | Vertical |
| Model Type | Derived From OSI | Reference Model |
| Protocol Dependent/Independent | Dependent | Independent |
| Flexibility and Modularity | More Flexible and practical. | Less Flexible as compared to TCP/IP |
| Adoption and Implementation | Widely Used | Not widely Used |
| Delivery | No Guaranteed Delivery | Guaranteed Delivery |
| Replacement/Changes | Cannot be done easily. | Can be done easily. |
| Usage | More Used. | Less Used. |

### 1.5.2 LIST OF PROTOCOLS USED AT EACH LAYER IN TCO/IP AND A BRIEF DESCRIPTION ABOUT EACH PROTOCOL

1. **Application Layer**

   a. **HTTP (Hypertext Transfer Protocol):** The protocol used for web communication, allowing the retrieval and display of hypertext documents.

   b. **FTP (File Transfer Protocol):** Used for file transfers between hosts over a network.

   c. **SMTP (Simple Mail Transfer Protocol):** Responsible for sending and receiving email messages.

   d. **DNS (Domain Name System):** Translates domain names into IP addresses, enabling human-readable web addresses.

   e. **SNMP (Simple Network Management Protocol):** Facilitates network management and monitoring of network devices.

   f. **DHCP (Dynamic Host Configuration Protocol):** Automatically assigns IP addresses and network configuration to devices on a network.

   g. **Telnet:** Enables remote terminal access to network devices.

2. **Transport Layer**

   a. **TCP (Transmission Control Protocol):** Provides reliable, connection-oriented communication by ensuring the ordered delivery of data packets, congestion control, and error recovery.

   b. **UDP (User Datagram Protocol):** Offers connectionless, unreliable communication with minimal overhead, suitable for applications where real-time data delivery is important.

3. **Internet Layer**

   a. **IP (Internet Protocol):** The primary protocol responsible for logical addressing and routing of data packets across different networks.

   b. **ICMP (Internet Control Message Protocol):** Supports network troubleshooting, error reporting, and diagnostic messages.

   c. **ARP (Address Resolution Protocol):** Resolves IP addresses to MAC addresses within a local network.

4. **Network Access Layer**

   a. **Ethernet:** A widely used protocol for local area networks (LANs) that defines the physical and data link layer specifications.

   b. **Wi-Fi (IEEE 802.11):** Enables wireless communication and connectivity between devices in a local area network.

   c. **PPP (Point-to-Point Protocol):** Establishes a direct connection between two network nodes, often used for dial-up internet connections.

   d. **SLIP (Serial Line Internet Protocol):** Similar to PPP, SLIP is a protocol for point-to-point serial communication.

## 1.6 DATA TRAFFIC

Data traffic refers to the flow of data packets across a network. It represents the volume of data being transmitted and received by devices on a network. Data traffic can occur within a local network (LAN) or across wide area networks (WANs), including the internet.

### 1.6.1 TRAFFIC DESCRIPTOR

Traffic descriptors in networking are like labels that tell us about the characteristics of data flowing through a network. They help us understand and manage the traffic by describing its important attributes. It's like having tags on different vehicles to know their speed, size, and direction on a busy road.

The main traffic descriptors include:

1. **Rate:** This describes how much data is sent or received per unit of time. It tells us how fast the traffic is moving through the network.
2. **Burstiness:** Burstiness tells us whether the traffic comes in short, rapid bursts or flows more evenly over time. It helps in understanding how the data packets are being sent.
3. **Peak Rate:** The peak rate shows the maximum data rate that the traffic can reach, especially during short bursts.
4. **Committed Information Rate (CIR):** CIR is the minimum guaranteed rate at which the network will transmit data. It's like the minimum speed guaranteed for a specific type of traffic.
5. **Excess Information Rate (EIR):** EIR represents the extra or additional data rate that can be transmitted beyond the CIR. It's like having a higher speed limit than the minimum guaranteed speed.

### 1.6.2 TRAFFIC PROFILES

Traffic profiles in networking are like unique patterns or characteristics that describe how data flows through a network over time. It's similar to looking at the different shapes and sizes of waves in the ocean.

Each network can have its own traffic profile, which helps us understand the behavior of data traffic in that specific network. These profiles give us insights into things like:

1. **Peak Hours:** When the network experiences the highest amount of data traffic. It's like rush hour on a busy road.
2. **Quiet Periods:** Times when the network has very little traffic. It's like a road with very few cars during the night.
3. **Regular Patterns:** Consistent traffic flows that happen regularly, like data flowing smoothly during work hours.
4. **Sudden Surges:** Unexpected spikes in data traffic, which can happen during special events or sudden bursts of user activity.
5. **Variations in Traffic Type:** Different types of data traffic, such as web browsing, video streaming, file transfers, or online gaming.

## 1.7 CONGESTION

Congestion in networking is like a traffic jam on a busy road. It occurs when there is too much data trying to travel through a network, and the network resources (like bandwidth) become overwhelmed, causing a slowdown or even a complete halt in data flow.

Eg.Imagine many cars trying to drive on a narrow road at the same time. When there are too many cars, they start to slow down, and the traffic becomes congested. Similarly, in a network, when too many data packets are trying to travel through limited network resources, like routers and switches, they can get stuck or delayed, causing communication problems.

Congestion can lead to various issues, such as slow internet speeds, dropped connections, and delays in data delivery. Network administrators use different techniques to manage congestion and ensure smooth data flow, such as prioritizing critical data, expanding network capacity, and using congestion control algorithms.

### 1.7.1 NETWORK PERFORMANCE

Network performance in congestion refers to how well a computer network is functioning when it experiences traffic jams or overcrowding, just like a road during rush hour.

When a network becomes congested due to too much data traffic, its performance can suffer. This can lead to:

1. **Slow Speeds:** Data takes longer to travel from one place to another, like slower cars in a traffic jam.
2. **Delays:** Messages or data packets may get delayed, causing a wait time before they reach their destination.
3. **Packet Loss:** Some data packets may get lost or dropped due to the congestion, leading to incomplete or missing information.
4. **Unreliable Connections:** Congestion can cause temporary disruptions in connections, leading to intermittent or unstable network access.

## 1.8 CONGESTION CONTROL

Congestion control in networking is like managing traffic on a busy road to prevent gridlock and ensure smooth movement of vehicles.

Eg.Imagine a road with many cars trying to drive at the same time. If there are too many cars and the road is narrow, they will get stuck, and traffic will slow down or come to a standstill. Congestion control in networking is about avoiding such traffic jams in the data flow.

Congestion control can be classified into two main approaches: open-loop congestion control and closed-loop congestion control. Let's explore each of them:

### 1.8.1 OPEN LOOP

Open-loop congestion control in networking is like trying to prevent traffic jams on a road without knowing how many cars are on the road or how fast they are moving.

Eg.Imagine you're driving on a busy road, but there's no information about the current traffic conditions or any signals guiding the flow of cars. Open-loop congestion control in networking works similarly. It doesn't actively monitor or adjust data flow based on the network's current conditions.

In this approach, the network sends data packets without considering how congested the network might be. There are no mechanisms in place to check if the network is overloaded or if data is getting stuck. This lack of feedback means that open-loop congestion control cannot adapt to changing network conditions, and it might lead to network congestion and performance issues.

Open-loop congestion control is not as efficient as closed-loop congestion control, which actively monitors network conditions and adjusts data flow accordingly. Closed-loop congestion control is more like having traffic lights and traffic updates to manage the flow of cars on the road, preventing traffic jams and ensuring a smoother driving experience.

### 1.8.2 CLOSED LOOP

Closed-loop congestion control in networking is like having a traffic management system that actively monitors and adjusts the flow of data to prevent network congestion and ensure smooth data transmission.

Eg.Imagine a road with traffic lights that change based on the number of cars on the road. When there are more cars, the traffic lights adjust to keep traffic moving smoothly. Closed-loop congestion control works similarly in a network.

In this approach, the network continuously checks its own traffic conditions. If it detects congestion, like too many data packets or slow data movement, it takes immediate action to alleviate the problem. It can slow down data transmission, prioritize important data, or find alternative paths for data to reach its destination efficiently.

By actively monitoring and adapting to changing network conditions, closed-loop congestion control helps prevent slowdowns, data losses, and disruptions. It ensures that the network runs efficiently and provides a better experience for users, much like a well-managed road with traffic lights keeps traffic flowing smoothly.

## QUESTION BANK

- **Multiple Choice Questions (MCQs):**

1. What is centralized computing?
   (a) A model where computing resources are distributed across various locations.
   (b) A model where computing resources are located in a central data center.
   (c) A model where computing resources are stored on individual user devices.
   (d) A model where computing resources are managed by multiple independent servers.
2. In centralized computing, where are computing resources typically located?
   (a) On individual user devices
   (b) In a central data center
   (c) Distributed across various remote locations
   (d) On cloud servers managed by different providers
3. Which of the following is a suitable scenario for centralized computing?
   (a) Real-time online gaming
   (b) Collaborative document editing
   (c) Peer-to-peer file sharing
   (d) Autonomous vehicle control
4. Which network model is most efficient when there is a heavy traffic load?
   (a) Centralized Model
   (b) Distributed Model
   (c) Collaborative Model
   (d) None of the above

5. Which service is provided by network layer in OSI model?
   (a) Fragmentation
   (b) Bit by bit Transmission
   (c) Forwarding and Routing
   (d) Session Tracking
6. __________ in networking are like labels that tell us about the characteristics of data flowing through a network.
   (a) Open Loop Congestion Control
   (b) Closed Loop Congestion Control
   (c) Traffic Profiles
   (d) Traffic Descriptors
7. __________ in networking are like unique patterns or characteristics that describe how data flows through a network over time.
   (a) Open Loop Congestion Control
   (b) Closed Loop Congestion Control.
   (c) Traffic Profiles
   (d) Traffic Descriptors
8. When a network becomes congested due to too much data traffic, its performance can suffer. This can lead to:
   (a) Slow Speeds
   (d) Unreliable Connections.
   (b) Delays
   (e) All of the above
   (c) Packet Loss

**ANSWERS**

1. (b) A model where computing resources are located in a central data center
2. (b) In a central data center
3. (b) Collaborative document editing
4. (a) Centralized Model
5. (c) Forwarding and Routing
6. (d) Traffic Descriptors
7. (c) Traffic Profiles
8. (e) All of the above

## Short Questions:

1. List types of models in network computing.
2. OSI stands for __________.

3. What is the functionality of Transport Layer in OSI model.
4. Which protocols works at network layer.
5 Why Layered mechanism is required mobile computing.
6. Define Data traffic.
7. Define Congestion.
8. Enlist applications of Client Server Model.
9. Differentiate open loop and closed loop congestion control.

## ■ Long Questions:

1. Explain Models of Network computing with its application and advantages.
2. Briefly explain OSI model with all its layers and functionalities of each layer.
3. Explain Protocols working at each layer in OSI models with its functionalities.
5. Explain client server and peer to peer network models.
6. Differentiate OSI model with TCP/IP model.
7. Explain TCP/IP model with all its layers and functionalities of each layer.
8. What is congestion control? Why it is required?
9. Explain types of congestion control.

■ * ■