BSc (Hons) in Computer Science via GDSE

Assignment - 01

INTRODUCTION TO NETWORK PROGRAMMING

H.M Yehani Harshika Pamunuwa

2301671057

GDSE 67

SUBMITTION DATE(14/01/2024)

Part - 1

01. Basics of Networking:

a. A computer network is a collection of two or more computer systems that are linked together to share resources and information (such as computers, printers, and servers).A network connection between these devices can be established using cable or wireless media.

Global Connectivity

Communication

help to provide Data security and management

Increase in Reliability – If one machine fails, another can take its place.

02. Understanding Protocols:

a. A protocol is a set of rules and guidelines for communicating data

I. Internet Protocol (IP) - Manages the addressing and routing of data packets in a network.
II. Hypertext Transfer Protocol (HTTP) - Facilitates the transfer of web pages and related files on the internet.
III. File Transfer Protocol (FTP) - Used for transferring files between computers on a network.
IV. Simple Mail Transfer Protocol (SMTP) - Manages email transmission.

b.

TCP (Transmission Control Protocol)

- TCP is Connection-oriented protocol.

- TCP provides Reliable, ordered, error-checked delivery.

- Has a larger header size compared to UDP.

- TCP Implements flow control mechanisms

UDP (User Datagram Protocol).

- UDP is Connectionless protocol.

- UDP is Unreliable, no ordering, no error checking.

- UDP has a smaller header size

- No inherent flow control for UDP.

3. Local Area Network (LAN) and Wide Area Network (WAN):

a. A Local Area Network (LAN) is a network that is limited to a small geographic area.(such as a single building or a campus).

A Wide Area Network (WAN), covers a larger geographical area.

LAN(Local Area Network)

- Limited to a small geographic area, like a building or campus.

- Typically higher speeds and greater bandwidth, as the devices are in close proximity.

- Often owned, set up, and controlled by a single organization or entity.

- Generally more cost-effective to set up and maintain.

WAN(Wide Area Network)

- covers larger areas, possibly covering cities, countries, or continents.
- Speeds may vary and are generally lower than LAN due to the longer distances and dependence on external infrastructure.
- Involves multiple organizations, and the infrastructure may be owned and operated by different entities.
- Can be more expensive due to the need for long-distance communication infrastructure.

b.

LAN(Local Area Network)

Office or Business Environment:

LANs are suitable for connecting computers and devices within an office or business setting, facilitating efficient file sharing, communication, and resource utilization.

Educational Institutions:

Schools and universities often use LANs to connect computers and other devices within their campus, providing seamless access to shared resources.

WAN(Wide Area Network):

Multinational Corporations:

WANs are essential for large corporations with offices spread across different cities or countries, enabling them to connect and communicate globally.

4. Network Devices:

a. A router is a networking device that forwards data packets between computer networks.

- Routers perform the traffic directing functions between networks and on the global Internet.

- Routers check where data needs to go based on its destination IP address and decide the best way to send it there.

- Routers connect multiple networks together, enabling data communication between devices on different subnets or even different networks.

- Routers can implement security features such as firewalls and access control lists (ACLs) to control and monitor traffic entering and leaving the network.

b. A switch is a network device that operates at the data link layer (Layer 2) of the OSI model.

Its primary function is to connect devices within the same local area network (LAN) and efficiently manage the traffic between them.

- Switch Minimizes collisions by providing a better communication path for each connected device.

- Switch Learns the MAC addresses of connected devices and uses this information to forward data only to the intended recipient but Hub Broadcasts data to all connected devices, regardless of the intended recipient.

- Switch is a full duplex transmission mode. but Hub is a half duplex transmission mode.

- Switch can be used as a repeater but Hub cannot be used as a repeater.

5. Network Security:

a. A firewall is a network security device that maintains the security of incoming and outgoing network traffic

- Protection from unauthorized access: Firewalls can be set up to restrict incoming traffic from particular IP addresses or networks, preventing hackers or other malicious actors from easily accessing a network or system.

- Prevention of malware and other threats

- Control of network access: Firewalls control access to specific network resources by limiting entry to designated individuals or groups for particular servers or applications.

- By using firewalls to split up a bigger network into smaller subnets, the attack surface is reduced and the security level is raised.

b. A Virtual Private Network (VPN) contributes to securing network communications by creating a secure and encrypted connection over the internet, allowing users to transmit data between their devices and the VPN server in a private and protected manner.

- VPNs employ encryption protocols to secure data between a user's device and the VPN server, safeguarding sensitive information from unauthorized access or interception.
- The encrypted tunnel created by a VPN ensures that the data exchanged between the user and the VPN server remains confidential.
- VPNs use authentication to verify user and device identity, ensuring secure network connections.

6. Addressing in Networks:

a. An IP address is a unique identifier associated with a computer or network, which allows users to send and receive data.

- An IP address uniquely identifies a device on a network.
- IP addresses are used for routing data packets between devices on a network.

b. A Domain Name System (DNS) turns domain names into machine-readable IP addresses, whichallow browsers to get to websites and other internet resources. This translation is essential because computers communicate using IP addresses, and associating a domain name with its corresponding IP address allows users to access

websites and services using easy-to-remember names instead of numerical IP addresses.

7. Network Infrastructure:

a. A gateway is a piece of networking hardware or software used in telecommunications networks that allows data to flow from one discrete network to another.

A gateway in a network serves as an entry and exit point for data traffic between different networks.

b.

Bandwidth - Bandwidth refers to the maximum rate at which data can be transferred over a network or internet connection.

It is typically measured in bits per second (bps), kilobits per second (kbps), megabits per second (Mbps), or gigabits per second (Gbps).

Higher bandwidth allows for the transmission of more data in a given amount of time, leading to faster data transfer and better network performance.

Latency - Latency, often called ping, is the time it takes for data to travel from the source to the destination in a network.

It is typically measured in milliseconds (ms).

8. Data Transmission:

a. A packet is a unit of data transmitted over a network.

for it facilitate data transmission,

Dividing Data: Large files or messages are broken down into smaller packets for efficient transmission.

Routing: Each packet can take a different route to reach the destination, optimizing network resources and avoiding congestion.

Reassembly: At the destination, the packets are reassembled into the original data, ensuring integrity and completeness.

Error Handling: Control information in packets allows for error detection and correction

b. TCP (Transmission Control Protocol):

Reliability: TCP is connection-oriented and provides reliable, error-checked communication. It ensures that data is delivered in the correct order without loss.

Use Cases: Ideal for applications where data integrity is critical, such as file transfers, web browsing, email, and any scenario where ensuring the accurate delivery of data is essential.

UDP (User Datagram Protocol):

Reliability: UDP is connectionless and does not guarantee reliable delivery. It does not check for errors or guarantee the order of data delivery.

Use Cases: Suitable for real-time applications where low latency is more critical than perfect data delivery, such as online gaming, video streaming, and VoIP. It is also used in scenarios where some data loss is acceptable.

9. Network Configuration:

a. It is the critical feature on which the users of an enterprise network communicate. DHCP helps enterprises to smoothly manage the allocation of IP addresses to the end-user clients' devices such as desktops, laptops, cellphones, etc.

b. A MAC address is a 12-digit hexadecimal number assigned to each device connected to the network.

A MAC address uniquely identifies devices on a network, facilitating proper communication by enabling switches to forward data only to the intended recipients and allowing to Address Resolution Protocol (ARP) to map IP addresses to specific devices within the local network.

10. Emerging Technologies:

a. IPv6 (Internet Protocol version 6) is the sixth revision to the Internet Protocol and the successor to IPv4. It functions similarly to IPv4 in that it provides the unique IP addresses necessary for Internet-enabled devices to communicate. However, it does have one significant difference: it utilizes a 128-bit IP address.

b.

• More efficient routing without fragmenting packets

• Built-in Quality of Service (QoS) that distinguishes delay-sensitive packets

• Enhancing security features

• Support for Future Internet Growth: As the number of internet-connected devices continues to rise, IPv6 provides the necessary infrastructure to accommodate this growth.

• Elimination of NAT to extend address space from 32 to 128 bits

• Stateless address auto-configuration for easier network administration

• Improved header structure with less processing overhead

• improving routing efficiency

11. Miscellaneous:

a. The proxy server is a computer on the internet that accepts the incoming requests from the client and forwards those requests to the destination server. It works as a gateway between the end-user and the internet. It has its own IP address. It separates the client system and web server from the global network.

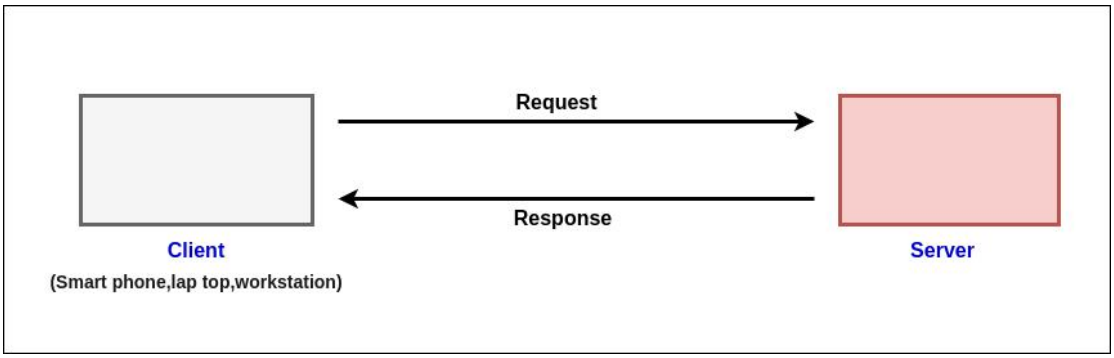
b. An ISP is a company or organization that provides internet access to customers. Without ISPs, the internet as we know it would not be accessible to the masses. thus by the ISP,

- Providing Internet Access: ISPs offer various types of internet connections, such as broadband, DSL, cable, and fiber optics, allowing users to connect to the global network.

- Infrastructure Maintenance: ISPs build and maintain the necessary infrastructure, including networks and data centers, to ensure reliable and high-speed internet access for their customers.
- IP Address Allocation: ISPs allocate IP addresses to their customers, enabling devices to be uniquely identified on the internet. They manage and distribute these addresses to ensure proper functioning of the internet protocol.
- Providing Additional Services: Many ISPs offer additional services, such as email hosting, domain registration, and virtual private networks (VPNs), to enhance the overall internet experience for their users.
- Customer Support: ISPs provide customer support services to address technical issues, billing inquiries, and other concerns that users may encounter while using their internet services.

Part - 2

01.



The client-server architecture refers to a system that hosts, delivers, and manages most of the resources and services that the client requests.

Client -The client is the end-user device or application that requests services or resources from the server.

Client Initiates communication by sending requests to the server.(ex : Web browsers, mobile apps, database clients)

Server -The server is a dedicated computing system or software that provides services or resources in response to client requests.

Server Listens for incoming requests, processes them, and sends back the appropriate responses.(Ex : Web servers, database servers, application servers)

Communication Channel - The communication channel is the medium through which data is exchanged between clients and servers.

Communication Channel Facilitates the transmission of requests and responses.(Ex : Networks (Internet, local area networks), protocols (TCP/IP, HTTP))

02.Socket programming involves using sockets (communication endpoints) to enable communication between processes, either on the same computer or across a network.

- Allows processes on the same or different machines to communicate.
- Essential for building networked applications.
- Supports various protocols (TCP, UDP) for different communication needs.
- Facilitates real-time data exchange between applications.
- Enables the development of Scalable and distributed systems.

03.

Advantages of Socket Programming:

- Flexible & powerful
- Very sufficient
- Updated Information can be used to send only between devices
- Low network traffic if efficient use
- Efficiency

Disadvantages of Socket Programming:

- Increased complexity cost and high-Security restrictions.
- Socket-based communications allow only to send packets of raw data between applications.
- Communication can be established with the machine requested not with another machine.
- Both ends should have the ability to intercept the data.