BSc (Hons) in Computer Science via GDSE

Module Code ITS1140

Introduction to Network Programming

Assignment 01

THEEKSHANA DILSHAN PREMARATHNA

2301671055

67

SUBMISSION DATE(14/01/2023)

Part - 1

1. Basics of Networking:

a. What is a network : A computer network is a system that connects two or more computing devices for transmitting and sharing information.

   Its significance : exchanging data and sharing resources.

2. Understanding Protocols:

a. What is a network protocol ? : protocol is a set of rules that control how devices communicate with each other.

b. examples of commonly used protocols and their purposes

- Transmission Control Protocol (TCP)
  - Purpose: Provides reliable, connection-oriented communication. It ensures that data is delivered without errors and in the correct order. TCP is used for applications where data integrity is crucial, such as file transfers, email, and web browsing.
- Internet Protocol (IP)
  - Purpose: Responsible for addressing and routing packets of data to ensure they reach the correct destination on a network. IP is a fundamental protocol in the Internet protocol suite and is used for the transmission of data across different networks.
- Hypertext Transfer Protocol (HTTP)
  - Purpose: Facilitates the transfer of web pages and other resources on the World Wide Web. HTTP is the foundation of any data exchange on the Web and is used for retrieving and transmitting hypertext.
- Hypertext Transfer Protocol Secure (HTTPS)

    - Purpose: Similar to HTTP but adds a layer of security using SSL/TLS protocols to encrypt data during transmission. It is commonly used for secure communication over the Internet, such as online banking and e-commerce.
- File Transfer Protocol (FTP)
    - Purpose: Used for transferring files between a client and a server on a network. FTP is commonly used for uploading and downloading files from servers, and it supports authentication for secure file transfers.
- Simple Mail Transfer Protocol (SMTP)
    - Purpose: Manages the sending of emails between servers. SMTP is essential for the transmission of emails, enabling communication between email clients and servers.
- Post Office Protocol version 3 (POP3) and Internet Message Access Protocol (IMAP)
    - Purpose: Both are email retrieval protocols. POP3 allows the download of emails to a local device, while IMAP allows users to access and manage emails directly on a server, enabling synchronization across multiple devices.
- Domain Name System (DNS)
    - Purpose: Translates human-readable domain names into IP addresses, allowing users to access resources on the Internet using easily memorable names. DNS is crucial for the functioning of the Internet by providing a distributed naming system.

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

a. LAN means Local Area Network. WAN means Wide Area Network.
    ➔ LAN connects users and applications in close geographical proximity (same building).
    ➔ WAN connects users and applications in geographically dispersed locations (across the globe).

b. example for LAN - Small Office Environment.
   example for WAN - Offices are located in different cities or countries.

   ➔ LANs are good for private IoT networks, bot networks, and small business networks. WANs are good for disaster recovery, applications with global users, and large corporate networks.

4. Network Devices

a. The Internet is formed by networks throughout the world interconnecting and passing on data to each other. A router is a small device that sits between your modem and computer. Most routers are about the same size and shape as a modem. The purpose of the router is to take the information from the modem and deliver it to your computer.
   A router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet. Routers make the Internet work by forwarding data using a unified addressing system. They can send information to anywhere in the world as long as that location has an IP address.

b. A hub is a networking device that connects multiple PCs to a single network, whereas a Switch connects multiple devices on a single computer network. A hub operates on the OSI physical layer, whereas a switch operates on the OSI data link layer.

5. Network Security

a. A firewall is essential software or firmware in network security that is used to prevent unauthorized access to a network. It is used to inspect the incoming and outgoing

traffic with the help of a set of rules to identify and block threats by implementing it in software or hardware form.

b. A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely.

6. Addressing in Networks

a. An IP address definition is a numeric label assigned to devices that use the internet to communicate. Computers that communicate over the internet or via local networks share information to a specific location using IP addresses.

b. The Internet's DNS system works much like a phone book by managing the mapping between names and numbers. DNS servers translate requests for names into IP addresses, controlling which server an end user will reach when they type a domain name into their web browser. These requests are called queries.

7. Network Infrastructure

a. A gateway is a network node used in telecommunications that connects two networks with different transmission protocols together. Gateways serve as an entry and exit point for a network as all data must pass through or communicate with the gateway prior to being routed.

b. Latency refers to the amount of time a data packet takes to travel from one point to another, AKA the delay between the time data is sent and received, measured in milliseconds (ms). Whereas bandwidth refers to the volume of data sent, latency refers to the speed at which it's transmitted.

8. Data Transmission

a. In networking, a packet is a small segment of a larger message. Data sent over computer networks*, such as the Internet, is divided into packets. These packets are then recombined by the computer or device that receives them.
b. The main difference between TCP (transmission control protocol) and UDP (user datagram protocol) is that TCP is a connection-based protocol and UDP is connectionless. While TCP is more reliable, it transfers data more slowly. UDP is less reliable but works more quickly.

9. Network Configuration

a. DHCP (Dynamic Host Configuration Protocol) is a network management protocol used to dynamically assign an IP address to any device, or node, on a network so it can communicate using IP.
b. Both MAC addresses and IP addresses serve the same purpose, which is to identify a device on a network. While the MAC address identifies the physical address of a device on the same local network, the IP address identifies the device globally or through its internet address.

10. Emerging Technologies

a. IPv6 is the latest version of the Internet Protocol, designed to succeed IPv4. It was introduced due to the exhaustion of IPv4 addresses. IPv6 provides a vastly expanded address space (128-bit) compared to IPv4 (32-bit), addressing the growing number of connected devices on the Internet.

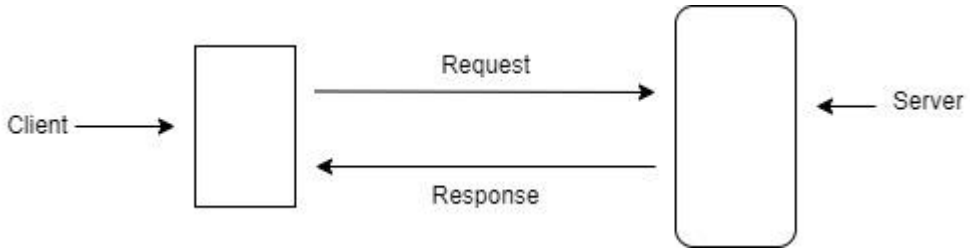
b. IPv6 offers these improvements over IPv4: More efficient routing without fragmenting packets. Built-in Quality of Service (QoS) that distinguishes delay-sensitive packets. Elimination of NAT to extend address space from 32 to 128 bits.

10. Miscellaneous

a. A proxy server is a system or router that provides a gateway between users and the internet. Therefore, it helps prevent cyber attackers from entering a private network. It is a server, referred to as an "intermediary" because it goes between end-users and the web pages they visit online.
b. An internet service provider (ISP) is a company that provides access to the internet. ISPs can provide this access through multiple means, including dial-up, DSL, cable, wireless and fiber-optic connections. A variety of companies serve as ISPs, including cable providers, mobile carriers, and telephone companies.

Part - 2

1. client-server architecture, architecture of a computer network in which many clients (remote processors) request and receive service from a centralized server (host computer). Client computers provide an interface to allow a computer user to request services of the server and to display the results the server returns.



2. Java socket programming is a way to create a connection between two programs running on different computers.This can be used to create a variety of network applications, such as web servers, file sharing applications, and chat applications.

3. **Advantages of Java Sockets**

    - Platform Independence
    - Simple and Flexible API
    - Wide Protocol Support
    - Robustness and Reliability
    - Scalability

    Disadvantages of Java Sockets

    - Low-Level Programming
    - Lack of Built-in Security
    - Limited Functionality
    - Performance Overhead
    - Asynchronous Operations