Laboratory Practical Report

of

Data Communication and Networks

(ICT ED 456)

Submitted To

TRIBHUVAN UNIVERSITY

In Partial Fulfillment of the Requirements of the course

B.Ed. ICTE 5th Semester

Submitted By

Sanam Tamang

Symbol No.: 76214020

T.U. Regd. No.: 9-2-214-54-2019

Under the guidance of

Mr. Giriraj Dahal

Lecturer

Sukuna Multiple Campus

SUKUNA MULTIPLE CAMPUS

Sundarharaincha-12, Morang, Nepal

2080

CERTIFICATE

This is to certify that the Laboratory Practical Report

of

Data Communication and Networks

(ICT ED 456)

In Partial Fulfillment of the Requirements of the course

B.Ed. ICTE 5th Semester

Submitted By

Sanam Tamang

Symbol No.: 76214020

T.U. Regd. No.: 9-2-214-54-2019

is a bonafide record of experiments carried out by him/her under the guidance of

_____

Mr. Giriraj Dahal

Lecturer

Sukuna Multiple Campus

Sundarharaincha-12, Morang

(Internal Examiner)

Submitted for the Final Examination on: 2080/02/07

_____

Lecturer

(External Examiner)

Contents

1. How internet works?

The internet is a global network of computers that allows for the transmission and exchange of information between users. It functions through a combination of hardware, software, and protocols. Here's a simplified explanation of how the internet works:

1. Devices and Connections:

   The internet involves various devices, such as computers, servers, routers, and mobile devices. These devices are connected to each other through physical cables (fiber-optic, copper, or wireless connections) or satellite links.

2. IP Addresses:

   Every device connected to the internet is assigned a unique identifier called an IP (Internet Protocol) address. IP addresses are numerical values that enable devices to locate and communicate with each other. There are two main versions of IP addresses in use today: IPv4 (32-bit) and IPv6 (128-bit).

3. Protocols:

   The internet relies on protocols, which are a set of rules and conventions that govern how data is transmitted and received. The most fundamental protocol of the internet is the Internet Protocol (IP), which establishes how data packets are addressed and delivered between devices.

4. Data Packet Transmission:

   When you send or receive data over the internet, it is broken down into smaller units called data packets. Each data packet contains the source and destination IP addresses, along with a portion of the original data. These packets travel independently across the internet and may take different routes to reach their destination.

5. Routing:

   Routers are key components of the internet infrastructure. They receive data packets and determine the most efficient path for them to travel based on the destination IP address. Routers use routing tables and algorithms to make these decisions, forwarding the packets along the appropriate links.

6. Transmission Control Protocol (TCP)/Internet Protocol (IP):

   TCP/IP is a set of protocols that govern the exchange of data over the internet. TCP breaks down the data into packets, numbers and sequences them, and ensures they are reassembled correctly at the destination. IP handles the addressing and routing of these packets.

7. Domain Name System (DNS):

   The DNS translates human-readable domain names (e.g., www.example.com) into IP addresses. When you type a URL into your web browser, the DNS server resolves the domain name to the corresponding IP address, allowing your device to establish a connection.

8. Client-Server Model:

   The internet follows a client-server model. Clients (such as your computer or smartphone) request data or services from servers (computers that store and serve data). Clients send requests to specific servers using their IP addresses, and servers respond by sending back the requested information.

9. Internet Service Providers (ISPs):

   ISPs are companies that provide access to the internet. They connect individual users or organizations to the internet infrastructure through various technologies like DSL, cable, fiber-optic, or wireless connections.

2. Describe OSI reference in brief.

The OSI (Open Systems Interconnection) reference model is a conceptual framework that standardizes and describes the functions of a communication system. It provides a structured approach to understanding and implementing network protocols and communication protocols. The OSI model consists of seven layers, each serving a specific purpose:

1. Physical Layer:

   The physical layer deals with the transmission of raw data bits over the physical medium, such as cables or wireless signals. It defines characteristics like voltage levels, cable specifications, and connector types.

2. Data Link Layer:

   The data link layer is responsible for reliable point-to-point data transfer between two directly connected nodes. It handles issues such as framing, error detection, and flow control. Ethernet switches and Wi-Fi access points operate at this layer.

3. Network Layer:

   The network layer enables the transfer of data packets from the source to the destination across different networks. It handles tasks like logical addressing, routing, and fragmentation of packets. The IP (Internet Protocol) operates at this layer.

4. Transport Layer:

   The transport layer ensures reliable and efficient data delivery between end systems. It provides mechanisms for segmentation, reassembly, flow control, and error recovery. The Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are protocols that operate at this layer.

5. Session Layer:

   The session layer establishes, manages, and terminates communication sessions between applications. It allows synchronization, checkpointing, and recovery of data exchanges. This layer facilitates establishing connections and managing data transfer between two applications.

6. Presentation Layer:

   The presentation layer handles the formatting, encryption, and compression of data to be sent across the network. It ensures that data from the application layer of one system can be properly interpreted by the application layer of another system.

7. Application Layer:

   The application layer is the closest to the end-user and provides services directly to user applications. It includes protocols like HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), and SMTP (Simple Mail Transfer Protocol) that enable functions such as web browsing, file transfer, and email.

3. Define Multiplexing. Describe any two of them.

Multiplexing is a technique used in telecommunications and computer networks to combine multiple data streams into a single transmission channel, thereby maximizing the utilization of available resources.

Here are two common types of multiplexing:

1. Time Division Multiplexing (TDM):

Time Division Multiplexing divides the available transmission time of a communication channel into discrete time slots and assigns each slot to different data streams. In this technique, each data stream is allocated a fixed time slot in a repetitive cycle. The data from each stream is transmitted sequentially during its assigned time slot, and the cycle repeats continuously.

TDM is often used in digital communication systems, such as telephone networks. It allows multiple voice or data signals to be transmitted over a single physical channel by dividing the channel's capacity into time slots. The advantage of TDM is that it provides fair and predictable access to the channel for each data stream.

2. Frequency Division Multiplexing (FDM):

Frequency Division Multiplexing combines multiple data streams by allocating different frequency ranges for each stream. Each data stream is modulated onto a separate carrier signal at a specific frequency within the allocated frequency band. The modulated carrier signals are then combined and transmitted simultaneously over the same physical medium.

FDM is commonly used in analog communication systems, such as traditional broadcast radio and television. It allows multiple audio or video signals to be transmitted over a single channel by assigning different frequency ranges to each signal. FDM requires bandpass filters at the receiving end to separate and extract the individual signals from the combined transmission.

The key advantage of FDM is its ability to support simultaneous transmission of multiple signals without interference. However, it requires careful frequency planning and sufficient frequency bandwidth to accommodate all the desired signals.

Both TDM and FDM are multiplexing techniques that enable efficient sharing of communication channels, optimizing the utilization of resources and increasing overall data throughput.

4. Define protocol? Describe any 5 of them.

A protocol is a set of rules and guidelines that govern the communication and interaction between devices, systems, or applications. Protocols define the format, timing, sequencing, and error handling of messages exchanged during communication. They ensure that data is transmitted reliably, efficiently, and consistently across a network or between different components of a system.

Here are descriptions of five commonly used protocols:

1. Transmission Control Protocol (TCP):

TCP is a connection-oriented protocol used for reliable and ordered data transmission over IP networks. It breaks data into packets, assigns sequence numbers to them, and ensures they are reassembled correctly at the receiving end. TCP provides features like error detection, congestion control, and flow control, making it suitable for applications that require data integrity, such as web browsing, file transfer, and email.

2. Internet Protocol (IP):

IP is the fundamental protocol of the internet and is responsible for addressing and routing data packets across networks. It defines how data is encapsulated into packets, assigns unique IP addresses to devices, and determines the best path for packet delivery. IP is a connectionless protocol, meaning it does not establish a dedicated connection before transmitting data. It works in conjunction with other protocols, such as TCP or UDP, to provide end-to-end communication.

3. Hypertext Transfer Protocol (HTTP):

HTTP is the protocol used for transferring hypertext (text with embedded links) and related resources on the World Wide Web. It defines how web browsers request web pages from web servers and how servers respond with the requested content. HTTP operates in a client-server model, where a client (web browser) sends a request to a server, and the server sends back a response with the requested data. HTTP has evolved over time, with the current version being HTTP/2.

4. File Transfer Protocol (FTP):

FTP is a protocol used for transferring files between a client and a server on a network. It provides a set of commands and responses that allow users to upload, download, rename, delete, and manipulate files on remote servers. FTP can operate in either active or passive mode, depending on how the data connection is established. It has been widely used for file sharing and remote file management.

5. Simple Mail Transfer Protocol (SMTP):

SMTP is a protocol used for sending and receiving email messages over a network. It defines the format and rules for the exchange of email between mail servers. SMTP is a reliable, text-based protocol that uses a series of commands and responses to facilitate the transfer of email messages. It works in conjunction with other protocols like POP (Post Office Protocol) or IMAP (Internet Message Access Protocol), which are used for retrieving email from a mail server.

These are just a few examples of protocols that are crucial for various aspects of communication and data exchange over networks. Different protocols serve different purposes and are designed to meet specific requirements of the applications or systems they support.