ACADEMIC PROGRAMME: BACHELOR OF SCIENCE IN COMPUTER SCIENCE
COURSE CODE AND TITLE: BSCS 302 – DATA COMMUNICATION AND NETWORKS
LECTURER'S NAME: PETER SIELE
LECTURER'S CONTACTS: Phone No.: 0711707689 **Email**: peter.siele@gretsauniversity.ac.ke

Open Systems Interconnection Reference Model in Summary

Layer No.	Layer Name	Description
7	Application	Consists of standard communication services and applications that everyone can use.
6	Presentation	Ensures that information is delivered to the receiving system in a form that the system can understand.
5	Session	Manages the connections and terminations between cooperating systems.
4	Transport	Manages the transfer of data. Also assures that the received data are identical to the transmitted data.
3	Network	Manages data addressing and delivery between networks.
2	Data link	Handles the transfer of data across the network media.
1	Physical	Defines the characteristics of the network hardware.

TCP/IP PROTOCOL SUITE

"TCP/IP" is commonly used to refer the set of network protocols that compose the **Internet Protocol suite**. Many texts use the term "Internet" to describe both the protocol suite and the global wide area network.

Protocol Layers and the Open Systems Interconnection Model

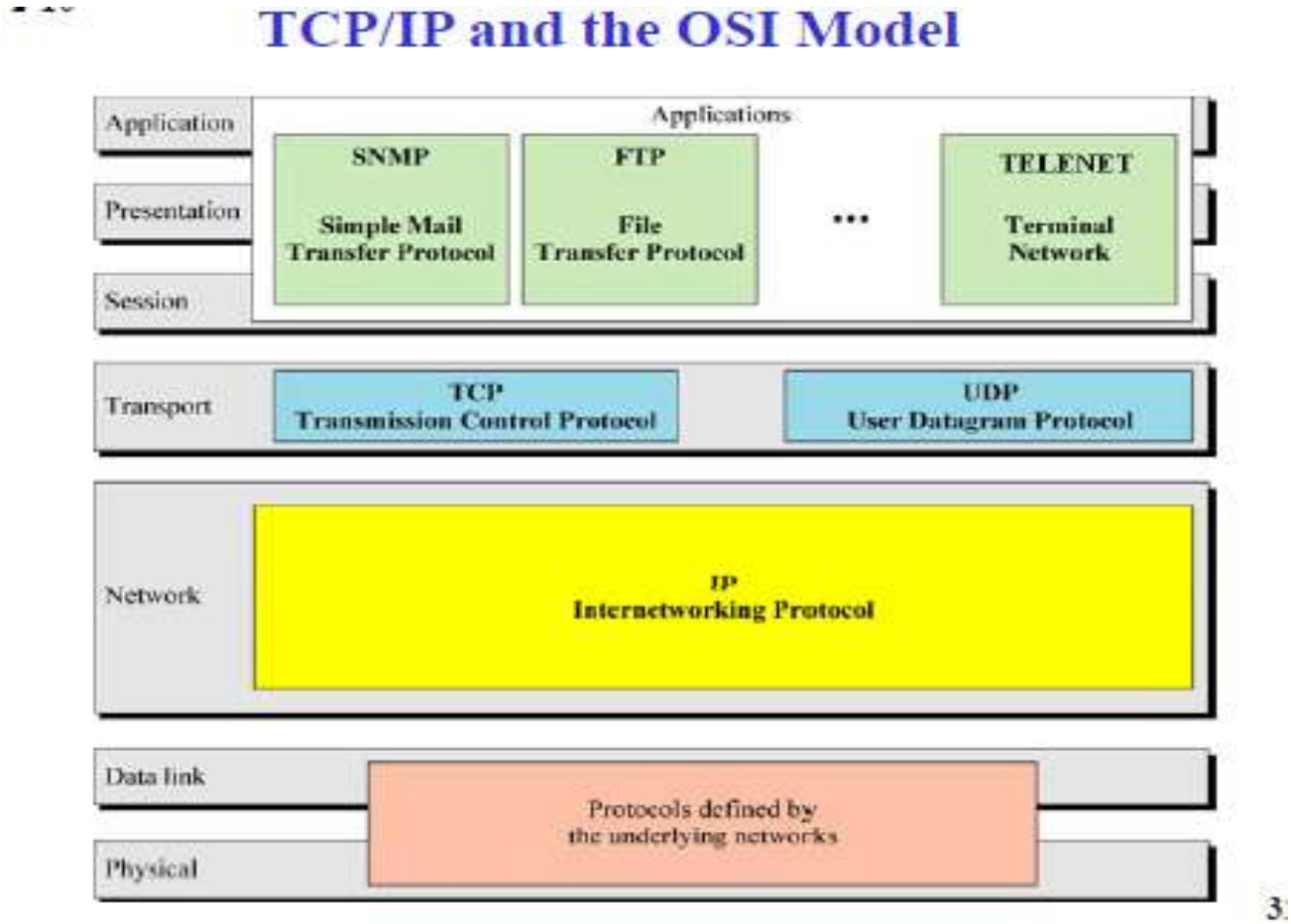
Most network protocol suites are structured as a series of layers, sometimes collectively referred to as a **protocol stack**. Each layer exists on both the sending and receiving systems. A specific layer on one system sends or receives exactly the same object that another system's **peer process** sends or receives.

TCP/IP Protocol Architecture Model

The table shows the TCP/IP protocol layers and the OSI model equivalents including examples of the protocols that are available at each level of the TCP/IP protocol stack

TCP/IP Protocol Stack

OSI Ref. Layer No.	OSI Layer Equivalent	TCP/IP Layer	TCP/IP Protocol Examples
5,6,7	Application, session, presentation	**Application**	NFS, DNS, LDAP, telnet, RIP, RDISC, SNMP, and others
4	Transport	**Transport**	TCP, UDP, SCTP
3	Network	**Internet**	IPv4, IPv6, ARP, ICMP
2	Data link	**Data link**	PPP, IEEE 802.2
1	Physical	**Physical network**	Ethernet (IEEE 802.3), Token Ring, RS-232, , and others



IEEE 802 Standards

IEEE 802 is a standard that specifies the functions of the physical and data link layers of major LAN and MAN protocols.

• Data link layer is divided into two sublayers:

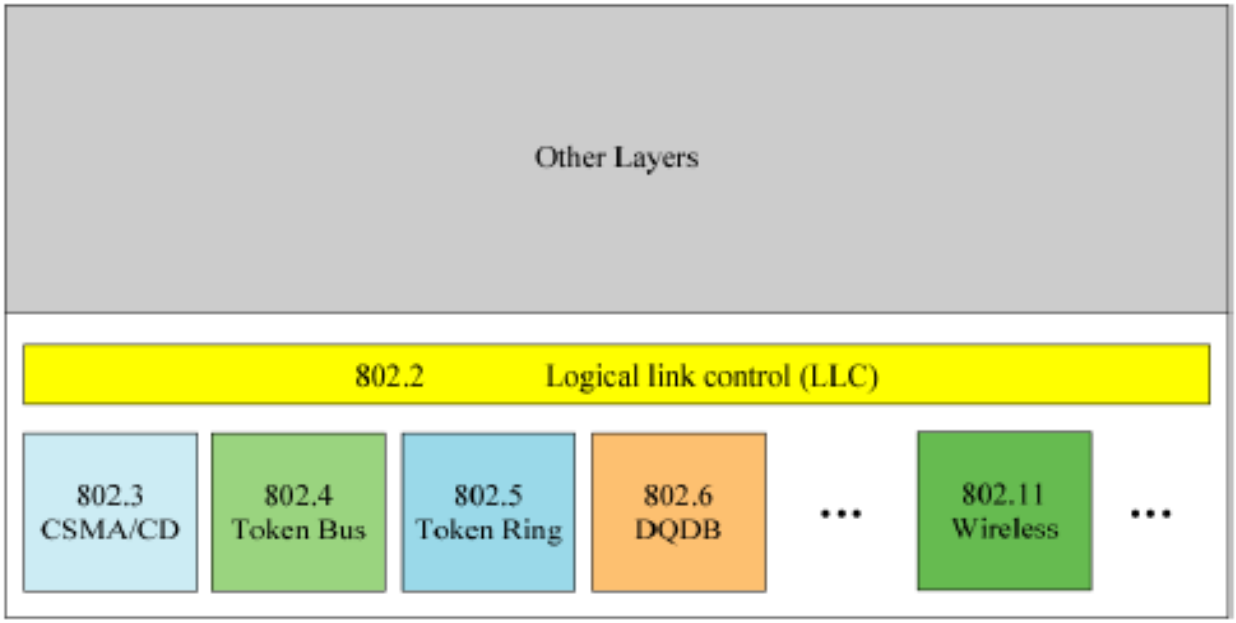
– Logical link control (LLC): same for all IEEE LANs

– Media access control (MAC): different for different types of LANs

• Physical Sublayers

– Totally depend on the implementation and type of the physical media used

IEEE Standards for LANs



Project 802

Physical Network Layer

The physical layer of TCP/IP describes hardware standards such as IEEE 802.3, the specification for Ethernet network media, and RS-232, the specification for standard pin connectors.

Data-Link Layer

The **data-link layer** identifies the network protocol type of the packet, in this instance TCP/IP. The data-link layer also provides error control and "framing." Examples of data-link layer protocols are Ethernet IEEE 802.2 framing and Point-to-Point Protocol (PPP) framing.

Internet Layer

The Internet layer, accepts and delivers packets for the network. This layer includes the powerful Internet Protocol (IP), the Address Resolution Protocol (ARP), and the Internet Control Message Protocol (ICMP).

IP Protocol

IP is responsible for the following:

- **IP addressing** – The IP addressing conventions are part of the IP protocol. This involves IPv4 and IPv6 addressing schemes.
- **Host-to-host communications** – IP determines the path a packet must take, based on the receiving system's IP address.
- **Packet formatting** – IP assembles packets into units that are known as **datagrams**. Datagrams are fully described in Internet Layer: Where Packets Are Prepared for Delivery.
- **Fragmentation** – If a packet is too large for transmission over the network media, IP on the sending system breaks the packet into smaller fragments. IP on the receiving system then reconstructs the fragments into the original packet.

ARP Protocol(Address Resolution Protocol)

ARP is used to translate protocol addresses to hardware interface addresses. ARP assists IP in directing datagrams to the appropriate receiving system.

While the RARP (Reverse Address Resolution Protocol) protocol is used to translate hardware interface addresses to protocol addresses.

ICMP Protocol

The Internet Control Message Protocol (ICMP) detects and reports network error conditions. ICMP reports on the following:

- **Dropped packets** – Packets that arrive too fast to be processed
- **Connectivity failure** – A destination system cannot be reached
- **Redirection** – Redirecting a sending system to use another router

Transport Layer

The TCP/IP **transport layer** ensures that packets arrive in sequence and without error(**end-to-end communication)**.

Transport layer protocols at this level are:

- Transmission Control Protocol (TCP),
- User Datagram Protocol (UDP),
- Stream Control Transmission Protocol (SCTP).

TCP and SCTP provide reliable, end-to-end service. UDP provides unreliable datagram service.

- May use a *connection-oriented protocol* such as TCP to ensure destination received segments
- TCP performs some tasks of OSI session layer, e.g. creating full-duplex connection between two application layers
- May use a *connectionless protocol* such as UDP to send segments without assurance of delivery
- UDP is used for fast delivery of single shot packets without flow and error control.

Stream Control Transmission Protocol (SCTP).

Features of SCTP include:

- Reliable transmission of both ordered and unordered data streams.
- Multihoming support in which one or both endpoints of a connection can consist of more than one IP address, enabling transparent fail-over between redundant network paths.
- Delivery of chunks within independent streams eliminates unnecessary head-of-line blocking, as opposed to TCP byte-stream delivery.
- Explicit partial reliability.
- Path selection and monitoring to select a primary data transmission path and test the connectivity of the transmission path.
- Validation and acknowledgment mechanisms protect against flooding attacks and provide notification of duplicated or missing data chunks.

Connection Oriented Services/network

There is a sequence of operation to be followed by the users of connection oriented service. These are:

1. Connection is established.
2. Information is sent.
3. Connection is released.

In connection oriented service we have to establish a connection before starting the communication.

Connection Less Services/network

It is similar to the postal services, as it carries the full address where the message (letter) is to be carried. Each message is routed independently from source to destination. The order of message sent can be different from the order received.

In connectionless the data is transferred in one direction from source to destination without checking that destination is still there or not or if it prepared to accept the message.

TCP Protocol

TCP enables applications to communicate with each other as though they were connected by a physical circuit. This transmission consists of the following:

- Starting point, which opens the connection
- Entire transmission in byte order
- Ending point, which closes the connection.

TCP attaches a header onto the transmitted data. This header contains many parameters that help processes on the sending system connect to peer processes on the receiving system.

UDP Protocol

UDP provides datagram delivery service. UDP does not verify connections between receiving and sending hosts. Because UDP eliminates the processes of establishing and verifying connections, applications that send small amounts of data use UDP.

IP Datagrams

- IP provides connectionless, unreliable delivery of IP datagrams.
- Connectionless: each datagram is independent of all others.
- Unreliable: there is no guarantee that datagrams are delivered correctly or at all.

Excercise

TCP or UDP ?

- Internet commerce ?
- Video server?
- File transfer?
- Email ?
- Chat groups?
- Robotic surgery controlled remotely over a network?
- Video Conferencing

Application Layer

The **application layer** defines standard Internet services and network applications that anyone can use.

Standard TCP/IP Services

- **FTP and Anonymous FTP** – The File Transfer Protocol (FTP) transfers files to and from a remote network,
- **Telnet** – The Telnet protocol enables terminals and terminal-oriented processes to communicate on a network that runs TCP/IP.

Internet Protocol (IP)

IP (short for Internet Protocol) specifies the technical format of packets and the addressing scheme for computers to communicate over a network. Most networks combine IP with a higher-level protocol called Transmission Control Protocol (TCP), which establishes a virtual connection between a destination and a source.

TCP/IP, on the other hand, establishes a connection between two hosts so that they can send messages back and forth for a period of time.

IP Addresses

- IP addresses are logical addresses (not physical)
- 32 bits.
- Includes a network ID and a host ID.
- Every host must have a unique IP address.
- IP addresses are assigned by a central authority.

IP addresses

- **Internet Protocol version 4** (**IPv4**) is the fourth version of the Internet Protocol (IP).
- IPv4 is a connectionless protocol for use on packet-switched networks, in that it does not guarantee delivery, nor does it assure proper sequencing or avoidance of duplicate delivery.
- IPv4 uses 32-bit (four-byte) addresses, which limits the address space. This limitation motivated the development of IPv6
- **Internet Protocol version 6 (**IPv6) is an evolutionary upgrade to the Internet Protocol.
- IPv6 is being deployed to fulfill the need for more Internet addresses.
- IPv6 provides Flexible options and extensions

An IP address is binary numbers but can be stored as text for human readers. For example, a 32-bit numeric address (IPv4) is written in decimal as four numbers separated by periods. Each number can be zero to 255. For example, **1.160.10.240** could be an IP address.

IPv6 addresses are 128-bit IP address written in hexadecimal and separated by colons. An example IPv6 address could be written like this: **2ffe:1600:4646:3:300:f8ff:fe31:54cff**

IPV4	IPV6
IPv4 has 32-bit address length	IPv6 has 128-bit address length
It Supports Manual and DHCP address configuration	It supports Auto and renumbering address configuration
In IPv4 end to end connection integrity is Unachievable	In IPv6 end to end connection integrity is Achievable
It can generate 4.29×109 address space	Address space of IPv6 is quite large it can produce 3.4×1038 address space
Security feature is dependent on application	IPSEC is inbuilt security feature in the IPv6 protocol
Address representation of IPv4 in decimal	Address Representation of IPv6 is in hexadecimal
Fragmentation performed by Sender and forwarding routers	In IPv6 fragmentation performed only by sender

In IPv4 Encryption and Authentication facility not provided	In IPv6 Encryption and Authentication are provided

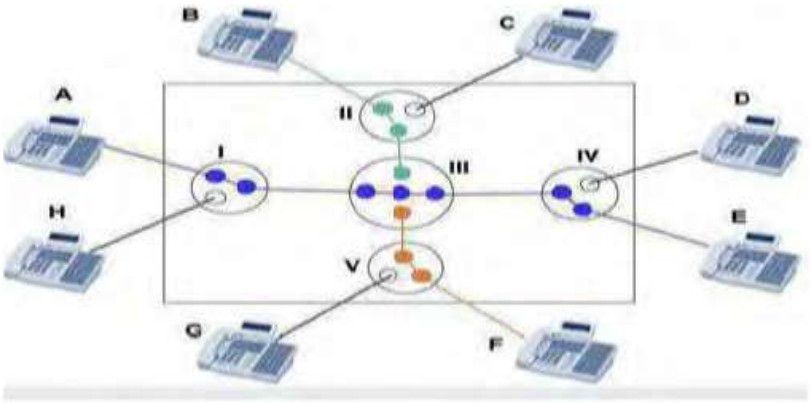
SWITCHING

Switching is defined as the process where connecting devices (Switches) interlinked are capable of creating temporary connections between two or more devices linked to the switch. In switched network, some of these nodes are connected to the end systems computers or telephones others are used only for routing purpose.

For example: - whenever a telephone called is placed, there are numerous junctions in the communication path that perform this movement of data from one network onto another network.

The main types of switching include:

1. **circuit switching -** A type of communications in which a dedicated channel (or circuit) is established for the duration of a transmission. The most ubiquitous circuit switching network is the telephone system, which links together wire segments to create a single unbroken line for each telephone call.



The above figure shows that device A is connected to device E through the switches I, III & IV. Other devices can connect to each other's by moving the levers of the switches.

2. **Packet switching:** The other common communications method is **packet switching**, which divides messages into packets and sends each packet individually. The **Internet** is based on a packet-switching protocol, **TCP/IP**.