Data communication and computer Network

Data communication is the physical transfer of data over a physical or radiator media.

Basic parts of a data communication system

- Source - Generate information to send.
- Transmitter - Convert the information for sending over the medium.
- Communication medium - The medium which is used to transmit.
- Receiver - Convert to information which was in medium compatible.
- Destination – The ultimate receiver.

Protocols

Protocols are digital rules that are used to send message among computers. This process has two parts.

1. Synchronization (SYN)
2. Acknowledgement (ACK)

Signals

Information can be transmitted over a medium by changing a physical property. There are two types of signals.

1. Analog (Continuous) signals.
2. Digital (Discreet) signals.

Analog signals

A continuous signal that changes its amplitude continuously with time.

Digital signals

A discreet signal that keep the amplitude at a constant level.

Communication Method

1. Manual Communication Methods
   Cave drawing, Messenger Birds, Arrows, etc.
2. Modern Communication Methods
   - Telephone- Transmit and receive voice over a pair of copper wires as electricity.
   - Radio/TV - Uses radio/magnetic waves to transmit audio/video signals.
   - Satellite - Uses microwave to connect between earth station.
   - Integrated Services Digital Network – Used to provide higher data rates through a telephone network for business application before ADSL.
   - Asymmetric Digital Subscriber Line (ADSL/DSL) - Uses the telephone line to transmit high speed data.
   - Code division multiple access (CDMA) - Multiple digital signals are sent over a same frequency at the same time.
   - General Packet Radio Service (GPRS) - It adds packet capability (Data) to GSM.
   - Global system for mobile communication (GSM) - It uses a subscriber identity module (SIM).

Modulation Techniques

This is the process of encoding source data into a carrier signal.

Properties of signal

1. Amplitude (A) - The strength of a wave at a given time.
2. Frequency - Is the rate at which a signal pattern repeats.
3. Wavelength - Distance between repeating units of a wave.
4. Phase - Is a definition of the position.

Two type of modulation techniques.

1. Analog signal modulation.
2. Digital signal modulation.

Analog Signal Modulation

1. Amplitude modulation (AM) - The carrier signals amplitude is changed according to variation of original signal.
2. Frequency Modulation (FM) - The carrier signals frequency is changed according to variation of modulating signal.
3. Phase Modulation (PM) - The carrier signals phase is changed according to modulating signal.

Digital Signal Modulation

1. Amplitude shift keying (ASK) - Two different amplitudes are used to represent 0 and 1.
2. Frequency shift keying (FSK) - Two or more frequencies are used to represent 0 and 1.
3. Phase shift keying (PSK) - Carrier wave is systematically shifted 0 or 180^{O} degrees at each symbol period.

Analog to Digital Modulation

Pulse code modulation (PCM) - Commonly used to convert analog signal to digital signal. PCM has following 3 phases.

1. Sampling
2. Quantizing
3. Encoding

Sampling - The voice send over the telephone falls within the limits 0.3 kHz-3.4 kHz it is generally taken as 0.4 kHz.

Quantizing - Each sample is calculated into a specific level so that it can be encoded.

Encoding - The quantized sample is then encoded using 8 bits.

Multiplexing

Multiplexing is the technique used to send multiple signal over the same medium at same time. 3 types

1. Frequency division multiplexing (FDM)
2. Time division multiplexing (TDM)
3. Code division multiplexing (CDM)

Frequency division multiplexing (FDM) - Used to divide the total bandwidth available in a communication medium into a series of non-overlapping frequency.

Time division multiplexing - Time sharing among source signals using around robin technique to send the signal over a single medium. Most used in digital telephone.

Code division multiplexing - Form of spread spectrum which narrow band signal is spread over a wider frequency band. Popularly known as CDMA.

Transmission mediums

1. Guided media (wired) - Use a physical medium
2. Radiator/Unguided media (wireless)

Guided Media

1. Twisted pair cable - Consist two insulated copper wires. Twisting reduce interference. Used for building communication and telephone networks.
    a. Unshielded twisted pair
    b. Shielded twisted pair
2. Coaxial Cable - A center conductor is shielded and out of the shield there is a braided outer conductor.
3. Fiber Optic - Transmit data based on total internal reflection.

Unguided Media

Data transmitted over air.

1. Radio transmission - Can work with or without line off sight.
2. Satellite transmission - Used to link ground station.
3. Terrestrial Microwave - Uses radio frequency to establish connection. (1GHz- 170GHz)
4. Intrawave - signals are sent from an infrared LED and received by a photo diode.

Transmission Impairments

Transmission lines get distorted due to transmission impairments. There are 3 types of impairment.

1. Attenuation
2. Distortion
3. Noise

Attenuation

- The signal becomes weaker over distance.
- Affects intelligibility of the received signal.

Distortion

- Signals changes its form or shape.
- The shape of the composite signal is therefore not the same.

Noise

Insertion of unwanted signals into the transmission signal.

- Thermal Noise - Caused by the thermal. Always present in electronic circuit and also called white noise.
- Intermodulation noise - When multiplexing different signals could mix and produce new signal.
- Crosstalk - Unwanted coupling between signals.
- Impulse noise - That may cause by lightning or electrical load variations.

Computer Networks

Two or more computing devices connected via a form of communication technology is a computer network.

Advantages

- Can share resources.
- Can establish communication facilities.
- Remote information access.
- Centralized Control.
- Expensive to establish and manage.
- If central device fail whole network is fail.
- Special skills and training required to maintain.

Connection Types

- Point-To-Point - Provides a dedicated link between two devices.
- Multipoint - Single link shared among several devices.

Classification of networks

Based on geographical distance.

- ✓ Local Area Network - Connects a set of devices in a small geographical area.
- ✓ Metropolitan Area Network - Extended over an entire city.
- ✓ Wide Area Network - Large geographical area.

Network Topologies

- ❖ Star
    - Better performance
    - Easy to maintain
    - Centralized management
    - Centralized device failed whole network is down
    - Central device is expensive.
    - Nodes are limited by central device.
- ❖ Bus
    - Less cables
    - Less expensive
    - Suitable for small networks
    - If main cable fails whole network is fail
    - Difficult to detect problem
    - Less security
- ❖ Ring
    - Data is sent only one node at a time
    - Less collusion
    - No need central device
    - Each data passes through all nodes
    - If one node fails the whole network is affected
    - Highly depends on wire
- ❖ Tree
    - Expansion is easy
    - Network divisions can be controlled easily
    - If one damaged it doesn't affect to network
    - Depends on main bus cable
    - Maintenance is difficult
    - Troubleshooting is difficult
- ❖ Mesh
    - Data can be transmitted simultaneously
    - If one cable fail it doesn't affect to network
    - High security
    - Cost is high
    - Setup and maintenance is difficult
    - Adding a computer is hard

VPN

VPN is technique used for sending data securely over internet through a tunnel.

Network Modules

1. Peer to peer – Each computer acts as both client and server.
2. Client Server Network – Provide a service is known as a server. And requester is known as a client. Server is a powerful machine that share resources with clients.

Network Commands

Ping- Check the connectivity to a device or computer.
Hostname – Shows the host name of the computer.
IPconfig – Display current network setting.
NSLookup – Looks the IP address of a domain.

ISO-OSI 7 Layer Remembering Song

All **P**eoples **S**eems **T**o **N**eed **D**ata **P**rocessing

ISO-OSI 7 Layer Architecture

Open system international model defines a 7 layers to a networking framework to implement protocols and devices.

1. Application – 7th layer provides application services for file transfer and other network software.
2. Presentation – Translating application layer data into network layer compatible data.
3. Session – Establish, manage, and terminate connection between applications.
4. Transport – Provides transparent transfer of data between systems or hosts.
5. Network – Provides switching and routing technologies. Create logical path to send data.
6. Data link – Data packets are encoded and decoded into bits.
    - Media Access Control Layer (MAC)
    - Logical link control layer (LLC)
7. Physical – Physical devices on the network.

Datagrams in 7 layers

Upper Layer Data	Application Presentation Session
Segments	Transport
Packets	Network
Frame	Data link
Bits	Physical

Addresses

3 types on addresses related to computer networks.

1. Port Address – An Interface on a computer which identifies the type of service.
2. Logical Address – The IP is an identifier for a device on the TCP/IP network.
3. Physical Address – The hardware address that uniquely identify each node of a network.

Networking Devices

- Repeater – Used to regenerate or replicate a signal. Operates in physical layer.
- Hub – Used for connecting segments or nodes. Operates in physical layer.
- Bridge – A device that connects two LAN's or two segments of same LAN. Operate in data link layer.
- Switch – Filters and forwards packets between LAN segments. Operate in data link layer.
- Router – Forwards data packets between different networks. Used to connect LAN to WAN. Operate in network layer.
- Gateway – Serves as an entrance to another network. Operates in transport and application layer.

TCP/IP Models

TCP/IP is a collection of communication protocols used to connect hosts in the internet.

TCP/IP vs OSI

<table>
<tr><td>Application</td><td rowspan="3"></td><td rowspan="3">Application</td></tr>
<tr><td>Presentation</td></tr>
<tr><td>Session</td></tr>
<tr><td>Transport</td><td></td><td>Transport</td></tr>
<tr><td>Network</td><td></td><td>Internet/Network</td></tr>
<tr><td>Data link</td><td rowspan="2"></td><td rowspan="2">Network Access</td></tr>
<tr><td>Physical</td></tr>
</table>

OSI Model Internet Model

Application layer

Defines TCP/IP protocols and how host program interface with the transport layer services to use the network.

Transport Layer

Provide communication sessions management between host computers.

Internet layer

Packages data into IP datagrams.

Network access Layer

Specifies details how data is physically sent through the network.

- A protocol is a set of rules agreed by both ends.

IEEE 802.3/Ethernet

- Station sends a link before start to transmission (Carrier Signal – CS)
- Multiple pc's access media at different time (Multiple Access - MA)
- Station monitors the medium to see if transmission is successful (Collusion Detection – CD)
- If collusion detected station stops transmission.
- Retransmit if the medium is free.

IEEE 802.5 token ring (Physical Layer)

A token ring network is a local area network (LAN) topology where nodes/stations are arranged in a ring topology.

Internet Protocol (Network Layer)

- IP format of packets are called datagrams.
- Most networks combined IP with transmission control protocol.(IP/TCP)

Transmission Control Protocol – TCP (Transport Layer)

- TCP enable to establish a connection and exchange streams of data.
- TCP guarantees the delivery of data.
- Connection is established between client and server.
- Error control and flow control can be done.
- Data transfer is reliable.

User Datagrams Protocol – UDP (Transport Layer)

- Connection less.
- Data will go through the network and reach the server.
- The server doesn't send any acknowledgement.
- Primarily used for broadcasting messages over a network.

Internet control message protocol (ICMP) (Network Layer)

ICMP is an extension to the internet protocol and it supports packets containing error control information messages.

Address Resolution Protocol (ARP) (Network Layer)

ARP is used to convert IP address into a physical address and is known as MAC address.

Application Layer Protocol

Dynamic Host Configuration Protocol (DHCP)

DHCP protocol used to assign dynamic IP addresses to a device on a network.

Domain Name Server (DNS)

An internet service that translate domain name into IP address.

TELNET

The telnet protocol is used for remote login.

File Transfer Protocol (FTP)

Protocol used for exchanging files over the internet. FTP uses TCP/IP protocol to enable data transfer.

Trivial File Transfer Protocol (TFTP)

TFTP is a file transfer protocol which is simple in nature and uses UDP than TCP and user authentication is not required.

Simple Mail Transfer Protocol (SMTP)

A protocol used to send email between servers.

Post Office Protocol v3 (POP3)

Protocol used to retrieve email from server.

Simple Network Management Protocol

A set of protocols for managing complex networks

Hyper Text Transfer Protocol (HTTP)

HTTP is protocol used by WWW. HTTP defines how messages are forwarded and transmitted. HTTP doesn't remember previous commands. S-HHTP is another version of HTTP and is used to send data securely.

Client-Server Architecture

1. Web server – Web servers are computers that deliver web pages and it has an IP address and possibly a domain name. Any computer can be turned into web server by installing server software.
2. Mail server – An email server acts as a virtual post office service and internal space is required to store emails.
3. Proxy server – A proxy server acts as an intermediary for requests from clients and checks if it can fulfill the requests itself.
    a. Improve performance by providing faster service.
    b. Filter requests for restricted websites.
4. Application server – Application server handles all application operations between users.
5. DNS server – DNS is an internet service that translate domain into IP addresses.

Leased Lines

A permanent telephone line between two points to connect geographically distance offices.

IP Addresses

- IP addresses are used to identify a computer on the network.
- Worldwide IP addresses are assigned by Internet Assigned Number Authority (IANA).
- Asia Pacific Network Information Center (APNIC) decide IP address range for Sri Lanka.
- Two versions of IP
    - IPv4 – Uses 32 binary bits separated into 4 groups each having 8 bits and the 8 bits known as an octet.

      Eg: 192.168.100.1
    - IPv6 – Uses 128 binary bits and expressed by 8 groups of hexadecimal numbers separated by columns.

      Eg: 2001:cdba:0000:0000:0000:3132:4365:fedc
- IPv6 was introduced because of the limitation of capacity in IPv4

Network ID and Host ID

The IP address consist of two sections.

1. Network ID – Defines the network within internet.
2. Host ID – Identifies the computer within the network.

IP address classes

Class	First Octet Range	Max Hosts
A	1 – 126	16 Million
B	128 – 191	64 Thousand
C	192 – 223	254
D	224 – 239	N/A
E	240 - 254	N/A

- Class D IP addresses are used for multicasting purpose.
- Class E IP addresses was set aside for experimental use and reserved for future use by IANA.

Private IP addresses

Used to identify a computer in a private network. These can be repeated within private networks.

Class	IP range
A	10.0.0.0 – 10.255.255.255
B	172.016.0.0 – 172.31.255.255
C	192.168.0.0 – 192.168.255.255

IP sub-netting

Sub-netting enables the host part of the IP address to be divided to create smaller network called subnet.
Depending on the number of subnets require the network part borrows bits from host part of the IP.

- The number of subnets that is created is calculated from the following expression.

2^n-2 (“n” is the number of bits borrowed from the host side.)

Subnet Mask

The subnet mask is the network address plus the bits reserved for identifying the sub network.