Date: / /

1. NETWORKING ARCHITECTURE

LAYERING & PROTOCOLS & OSI & INTERNET

OSI LAYERS – OSI Means Open System Interconnection.

OSI reference model describes how the information moves from one computer to another computer through a network.

The model was developed by the INTERNATIONAL ORGANIZATION FOR STANDARDIZATION in 1984.

This model is used for understanding and designing a network architecture that is flexible, robust and inter-operable. It consists of seven layers, where each layer defines a part of the process of the moving information accross the network.

LAYER 7	Application Layer
LAYER 6	Presentation Layer
LAYER 5	Session Layer
LAYER 4	Transport Layer
LAYER 3	Network Layer
LAYER 2	Data Link Layer
LAYER 1	Physical Layer

1. PHYSICAL LAYER – It is responsible for electrical, mechanical and procedural checks. The main functionality of the physical layer is to transmit the individual bits from one node to another node.

Date: / /

Devices working at physical layer are Hub, Repeater, Cables, Modem etc.

2. DATA LINK LAYER - It is devicded into two sub layers -

A. LLC - LOGICAL LINK CONTROL
It talks about WAN protocols.
eg. - PPP, HDLC, Frame-relay.

B. MAC - MEDIA ACCESS CONTROL
It talks about physical address. It is a 48 bit address.

It is also responsible for error detection.
Devices working on Data Link Layer are Switch, Bridge, NIC.

3. NETWORK LAYER - It is responsible for providing best path for data to reach the destination point. Logical addressing works on this layer. Router is a network layer device.

4. TRANSPORT LAYER - It specifies the process to delivery of the entire message. It is responsible for flow control and error control. It is responsible for end to end connectivity. Following steps are performed at the transport layer -

A. Identifying service

Date: / /

B. Multiplexing and de-multiplexing
C. Segmentation
D. Sequencing and re-assembling

5. SESSION LAYER - Session layer is the network dialog controller. It is responsible for establishing, maintaing and terminating session.
RPC - Remote Procedure Call
SQL - Structured Query Language
NES - Network File System

6. PRESENTATION LAYER - It is responsible for converting data into standard format. It is also responsible for data encryption, data decryption and comprehension.
eg.- ASCII, EBCDIC, JPEG, MPEG, BMP, MIDI, WAV, MP3.
Following tasks are perform at presentation layer -
Encoding - Decoding
Encryption - Decryption
Comprehension - Decomprehension

7. APPLICATION LAYER - It is also known as Desktop Layer. It is responsible for providing user interfaces and application services for file transfers, email and other network software services.
Identification of series is done using port numbers. Ports are entry and exit points to the layer.

Date: / /

Total No. of Ports → 0 - 65535
Reserved Ports → 0 - 1023
Open Client Ports → 1024 - 65535

Example of network services -

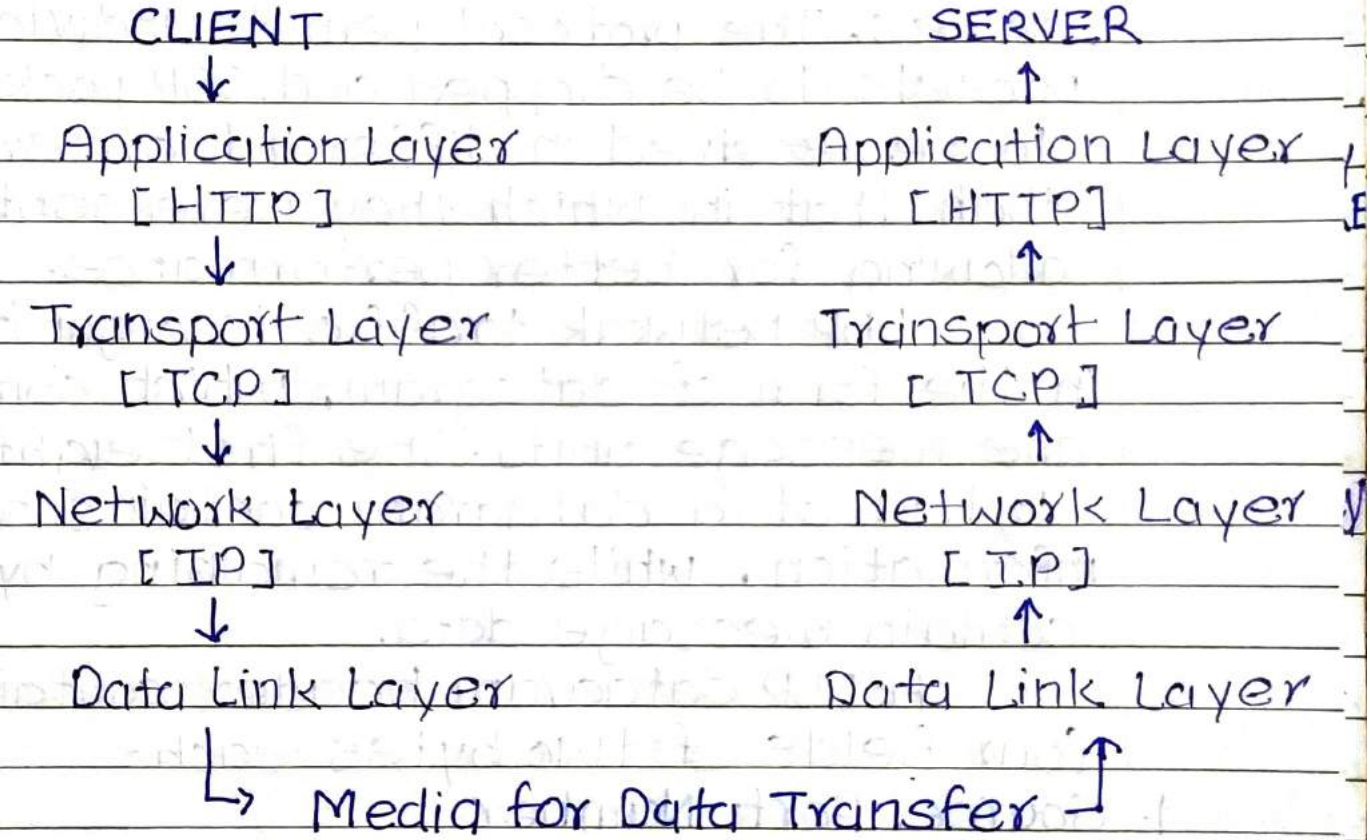
SERVICE	PORT NO.
HTTP	80
FTP	21
SMTP	25
TELNET	23
TFTP	69

PROTOCOL - A protocol is a set of rules that allow electronic devices to communicate with each other.
It is responsible for how to format, transmit and receive data from one computer to another computer.

TYPES OF PROTOCOL - There are various types of protocol -
TCP - Transmission Control Protocol
IP - Internet Protocol
UDP - User Datagram Protocol
SMTP - Simple Mail Transfer Protocol
POP - Post Office Protocol
IMAP - Internet Message Access Protocol
HTTP - Hyper Text Transfer Protocol
FTP - File Transfer Protocol

Date: / /

TCP/IP - TCP/IP stands for TRANSMISSION CONTROL PROTOCOL / INTERNET PROTOCOL. TCP/IP is a set of layered protocols used for communication over the Internet. The communication model of this suite is CLIENT/SERVER model. A computer that sends a request is the client, and a computer to which the request is sent is the server.



TCP/IP has four layers -

1. Application Layer
2. Transport Layer
3. Network Layer
4. Data Link Layer

TCP/IP is widely used in many communication networks other than the Internet.

Date: / /

UDP [USER DATAGRAM PROTOCOL] - UDP uses a simple transmission model but does not employ handshaking dialogs for reliability, ordering and data integrity. The protocol assumes that error-checking and correction is not required, thus avoiding processing at the network interface level.

UDP is widely used in video conferencing and real time computer games. The protocol permits individual packets to be dropped and UDP packets to be received in different order than that in which they were sent, allowing for better performance.

UDP network traffic is organized in the form of datagram, which comprise one message units. The first eight bytes of a datagram contains header information, while the remaining bytes contain message data.

A UDP datagram header contains four fields of two bytes each-

1. Source Port Number
2. Destination Port Number
3. Datagram Size
4. Checksum

SMTP [SIMPE MAIL TRANSFER PROTOCOL] - SMTP is a set of communication guidelines that allow software to transmit on email over the Internet

Date: / /

It provides a mail exchange between users on the same or different computers and it also supports -

1. It can send a single message to one or more recipients.
2. Sending message can include text, voice, video, graphics etc.
3. It can also send the messages on networks outside the internet.

The main purpose of SMTP is used to setup communication rules between server. The servers have a way of identifying themselves and announcing what kind of communication they are trying to perform. They also have a way of handling the errors such as incorrect email address.

For example, if the recipient email address is wrong, then receiving server reply with an error message of some kind.

POP [POST OFFICE PROTOCOL] - POP is the primarily protocol behind email communication. POP works through a supporting software, client that integrates POP for contacting to the remote email server that downloads email message to the recepient's computer machine.

POP uses the TCP/IP protocol stack for network connection and works with SMTP for end-to-end email communication, where POP pulls message and SMTP pushes them to the server.

Date: / /

IMAP [INTERNET MESSAGE ACCESS PROTOCOL]

IMAP was originally designed as remote mailbox protocol in 1986 by Mark Crispin. This was during the popular use of POP. IMAP and POP are still both supported by the majority of modern email servers and clients. However, IMAP is a remote file server, while POP istores and forwards. In other words, with IMAP all emails remains on the server untill the clients deletes them.

IMAP also permits multiple clients to access and control same mailbox. When a user requests an email, it is routed through a central server. This keeps a storage document for the email files.

Port 143 : It is a non-encrypted IMAP port

Port 993 : This port is used when IMAP client wants to connect through IMAP securely.

HTTP [HYPER TEXT TRANSFER PROTOCOL]

HTTP is the most fundamental protocol used for transferring text, graphics, image, video and other multimedia files on the World Wide Web. HTTP is an application layer protocol and was outlined for the first time by Tim Berners-Lee, who is also known as the father of WWW.

Date: / /

HTTP is a request-response protocol. Here is how it functions -

- Client submits request to HTTP.
- TCP connection is established with the server
- After necessary processing, server sends back status request as well as message. The message may have the requested content or an error message.

An HTTP request is called METHOD. Some of the most popular methods are, GET, PUT, POST, CONNECT etc.

The version of HTTP that is completely secure is HTTPS, where S stands for SECURE

FTP [FILE TRANSFER PROTOCOL] - FTP is a client/server protocol used for transferring files to or from a host computer. FTP may be authenticated with usernames & password

Anonymous FTP allows users to access files, programs and other data from the Internet without the need for a user ID or password.

COMPUTER NETWORK ARCHITECTURE

Computer network architecture defined as the physical and logical design of the software, hardware, protocols and media of the transmission of data. Simply we can say that how computers are organized and how tasks are allocated to the computer.

Date: / /

The two types of network architecture are used –

1. Peer - to - Peer Network
2. Client / Server Network

1. PEER-TO-PEER NETWORK - Peer - to - Peer network in which all the computers are linked together with equal privilege and responsibilities for processing the data.

Peer - to - Peer network is useful for small environments, usually upto 10 computers also this network has no dedicated server.

ADVANTAGES OF PEER-TO-PEER NETWORK –

1. It is less costly as it does not contain any dedicated server.
2. If one computer stops working but other computer will not stop working.
3. It is easy to setup and maintain as each computer manage itself.

DISADVANTAGES OF PEER-TO-PEER NETWORK

1. In the case of Peer-to-Peer network, it does not contain the centralized system. Therefore it can not back up the data as the data is different in different locations.
2. It has a security issue as the device manage itself.

Date: / /

2. CLIENT/SERVER NETWORK - Client/server is a network model designed for the end users called clients, to access the resources such as songs, videos etc. from a central computer known as server.

The server performs all major operations such as security and network management also it is responsible for managing all the resources such as files, directories, ~~pr~~ etc.

All the clients communicate with each other through a server.

For example - If CLIENT-1 wants to send some data to CLIENT-2, then it first sends the request to server for the permission. The server sends the response ~~for~~ to CLIENT-1 to initiate its communication with the CLIENT-2.

ADVANTAGES OF CLIENT/SERVER NETWORK -

1. A client/server network contains the centralized system, therefore we can backup the data easily.
2. A client/server network has a dedicated server that improves the overall performance of the whole system.
3. Security is better in Client/Server network as a single server administers the shared resources.
4. It also increase the speed of the sharing resources.

Date: / /

DISADVANTAGES OF CLIENT/SERVER NETWORK

1. Client/server network is expensive as it requires the server with large memory.
2. A server has a Network Operating System (NOS) to provide the resources to clients, but the cost of NOS is very high.
3. It requires a dedicated network admin to manage all the resources.

NETWORK TOPOLOGY

Network topology refers to the physical or logical layout of a network. It defines the way, different nodes are placed and interconnected with each other.

Alternately, network topology may describe how the data is transferred between these nodes.

There are two types of network topologies: physical and logical.

Physical topology emphasizes the physical layout of the interconnected devices and nodes, while the logical topology focuses on the pattern of data transfer between network nodes.

Some of the factors that affect choice of network topology are -

1. COST - Installation cost is very important factor in overall cost of setting up an infrastructure. So cable lengths, distance

Date: / /

between nodes, location of servers etc. have to be considered when designing a network.

2. FLEXIBILITY - Topology of a network should be flexible enough to allow re-configuration of office set-up, addition of new nodes and relocation of existing nodes.

3. RELIABILITY - Network should be designed in such a way that it has minimum down time. Failure of one node or a segment of cabling should not render the whole network useless.

4. SCALABILITY - Network topology should be scalable, i.e- it can accommodate load of new devices and nodes without perceptible drop in performance.

5. EASE OF INSTALLATION - Network should be easy to install in terms of hardware, software and technical personnel requirement.

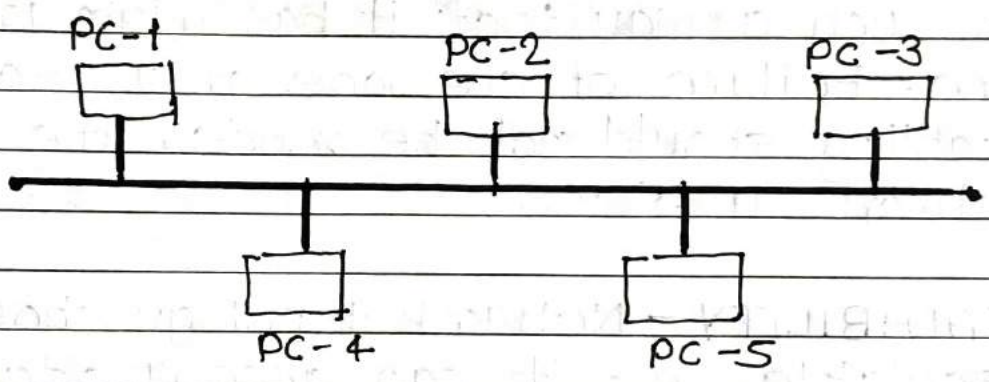
6. EASE OF MAINTENANCE - Troubleshooting and maintenance of network should be easy.

The physical and logical network topolgy of a network do not necessarily have to be identical. However both physical and logical network topologies can be categorized into five basic models.-

Date: / /

1. BUS TOPOLOGY – Data network with bus topology has a linear transmission cable, usually co-axial to which many network devices and workstations are attatched along the length.

The data travels in both directions along the bus. When the destination terminal sees the data, it copies to the local disk.



ADVANTAGES OF BUS TOPOLOGY –

1. Easy to install and maintain
2. Can be extended easily
3. Very reliable because of single transmission line.

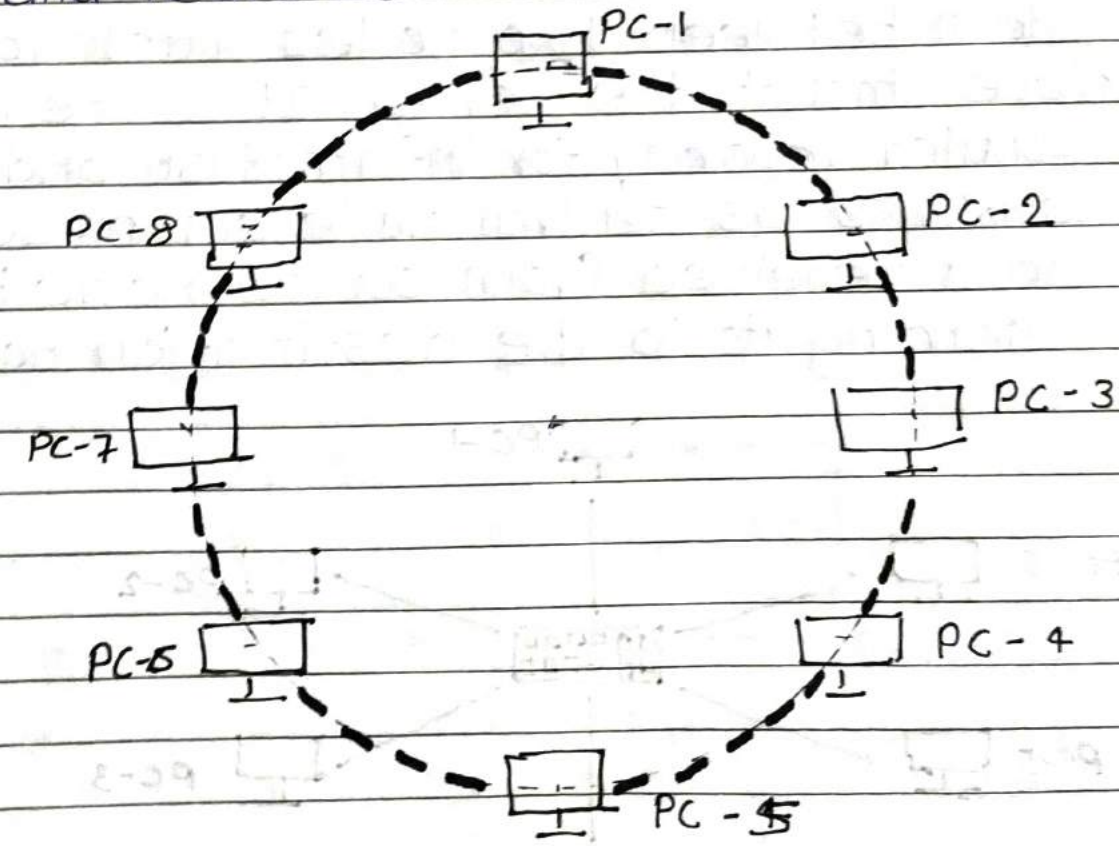
DISADVANTAGES OF BUS TOPOLOGY –

1. Troubleshooting is difficult as there is no point of control.
2. One faulty node can bring the whole network down.
3. Dumb terminals can not be connected to the bus.
4. Data is 'half-duplex', which means it can not be sent in two opposite direction at the same time.

Date: / /

2. RING TOPOLOGY – In Ring topology, each terminal is connected to exactly two nodes, giving the network a circular shape. Data travels only in one pre-determined direction.

When a terminal has to send data, it transmits it to the neighboring node which transmits it to the next one. Before further transmission data may be amplified. In this way, data traverses the network and reaches the destination node, which removes it from the network. If the data reaches the sender, it removes the data and resends it later.



ADVANTAGES OF RING TOPOLOGY –

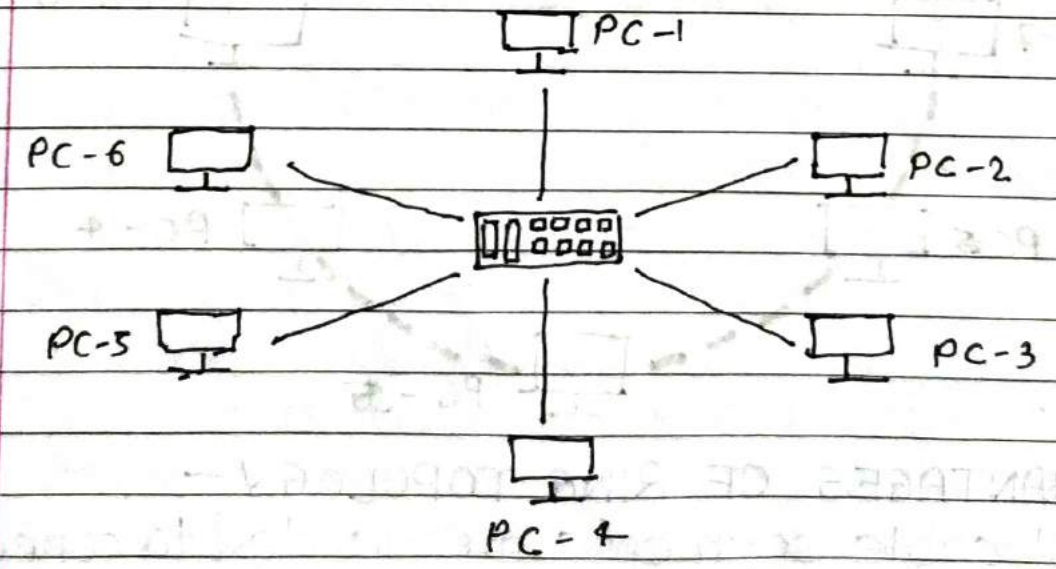
1. Small cable segments are needed to connect nodes.
2. Ideal for optical fibres as data travels only in one direction.
3. Very high transmission speeds possible.

Date: / /

DISADVANTAGES OF RING TOPOLOGY –

1. Failure of single node brings down the whole network.
2. Troubleshooting is difficult as many nodes may have to be inspected before faulty one is identified.
3. Difficult to remove one or more nodes while keeping the rest of the network intact.

3. STAR TOPOLOGY – In star topology, server is connected to each other node individually. Server is also called the central node. Any exchange of data between two nodes must take place through the server. It is the most popular topology for information and voice networks as central node can process data received from source node before sending it to the destination node.



Date: / /

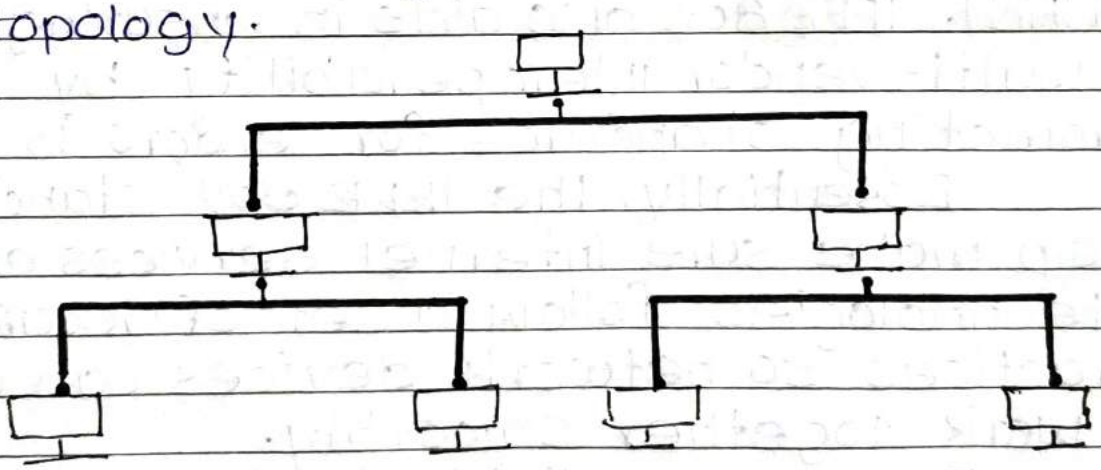
ADVANTAGES OF STAR TOPOLOGY -

1. Failure of one node does not affect the network
2. Troubleshooting is easy as faulty node can be detected from the central node immediately
3. Simple access protocols required as on of the communicating node is always the central node.

DISADVANTAGES OF STAR TOPOLOGY -

1. Long cable may be required to connect each node to the server.
2. Failure of single node brings down the whole network.

4. TREE TOPOLOGY - Tree topology has a group of star networks connected to a linear bus backbone cable. It incorporates feature of both star and bus topologies. Tree topology is also called hierarichal topology.



ADVANTAGES OF TREE TOPOLOGY -

1. Existing network can be easily expanded.
2. Well suited for temporary networks.

Date: / /

3. Point-to-Point wiring for individual segments means easier installation & maintenance.

DISADVANTAGES OF TREE TOPOLOGY –

1. Technical expertise required to configure and wire free topology.
2. Failure of backbone cable brings down entire network.
3. Insecure network.
4. Maintenance is difficult for large network.

IEEE 802 STANDARDS

IEEE 802 is a collection of networking standards that cover the physical and data-link layer specifications for technologies such as Ethernet and Wireless. These specifications apply to Local Area Network (LAN) and Metropolitan Area Network (MAN). IEEE 802 also aids in ensuring multi-vendor interoperability by promoting standards for vendors to follow.

Essentially, the IEEE 802 standards help make sure internet services and technologies follow a set of recommended practices so network devices can all work together smoothly.

IEEE 802 is divided into 22 parts that cover the physical and data-link aspects of networking. The family of standards is developed by the

Date: / /

IEEE 802 LAN/MAN STANDARDS COMMITTEE also called the LMSC. IEEE stands for INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS.

The set of standard started in 1979 with a "local network for computer interconnection" standard, which was approved a year leter. The LMSC has made more than 70 standards for IEEE 802.

The better known specification include 802.3 Ethernet, 802.11 Wifi and 802.15 Bluetooth/Zigbee. However, some of these standards have been labeled as disbanded or hibernating and are either superseded by newer standards or are being reworked. Using an open process, the LMSC advocates for these standards globally.

WHY IEEE 802 STANDARDS ARE IMPORTANT