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 across 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 devided 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

Excimple of network services -

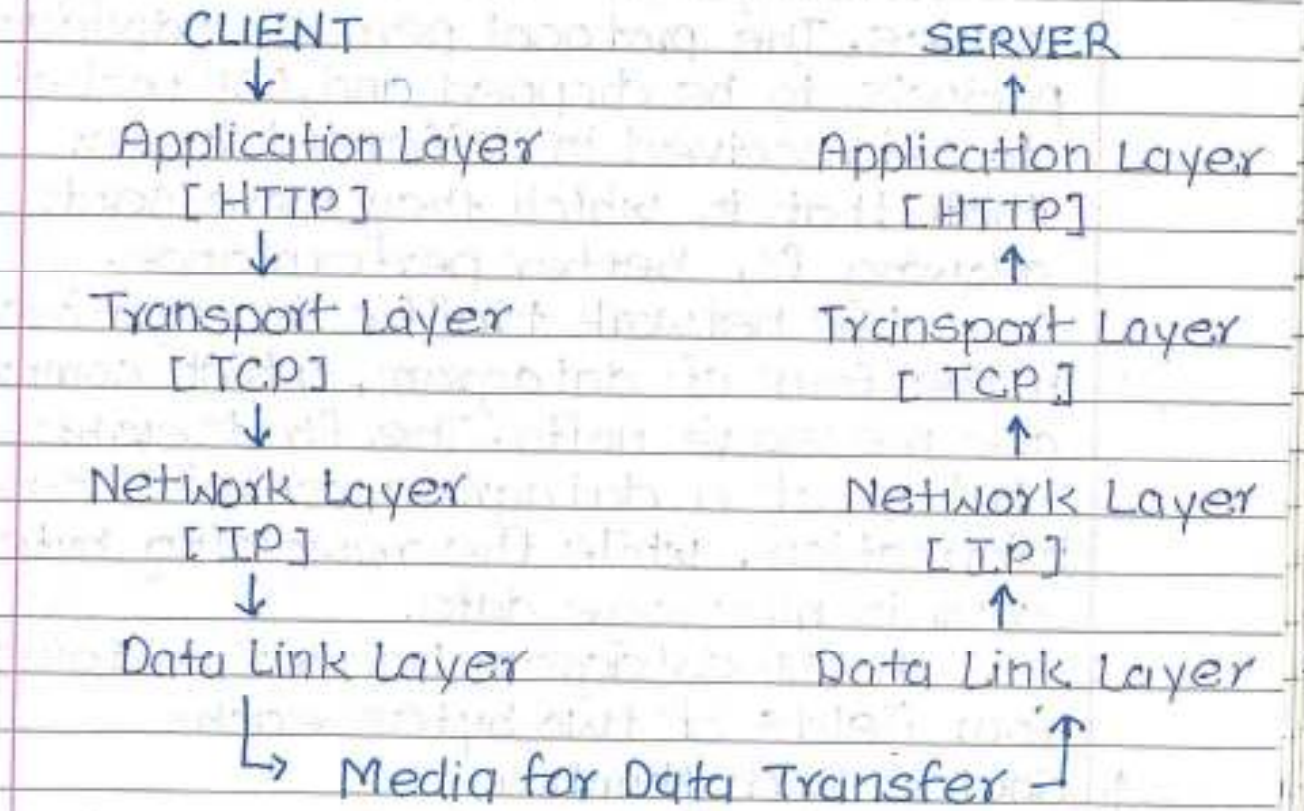
SERVICE	PORT NO.
HTTP	80
FTP	21
SMTP	25
TELNET	23
TFTP	69

PROTOCOL - A protocal 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

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 papular 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 until 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 to 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.

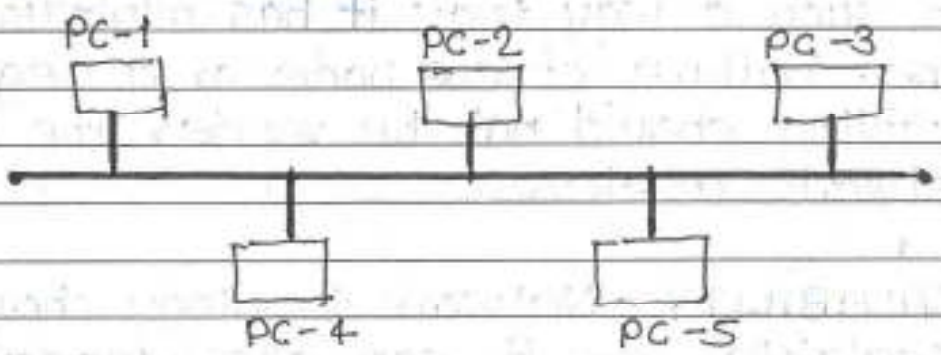
6. EASE OF MAINTENANCE - Troubleshooting and maintenance of network should be easy.

The physical and logical network topology 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.

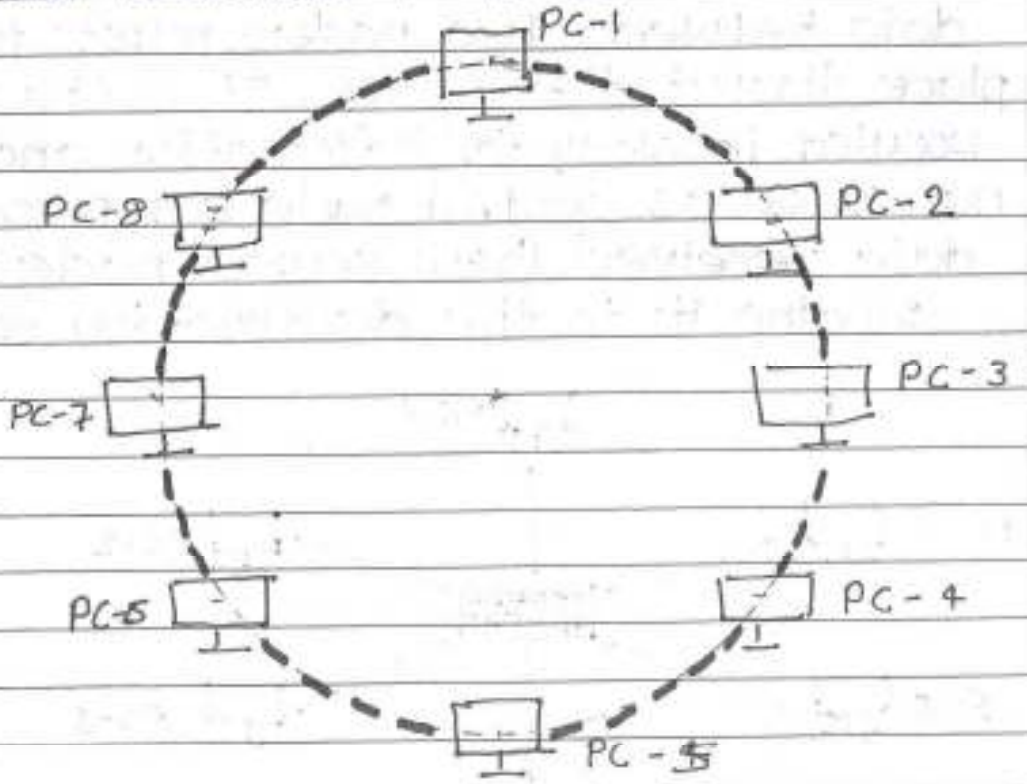
DISADVANTAGES OF BUS TOPOLOGY –

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 -

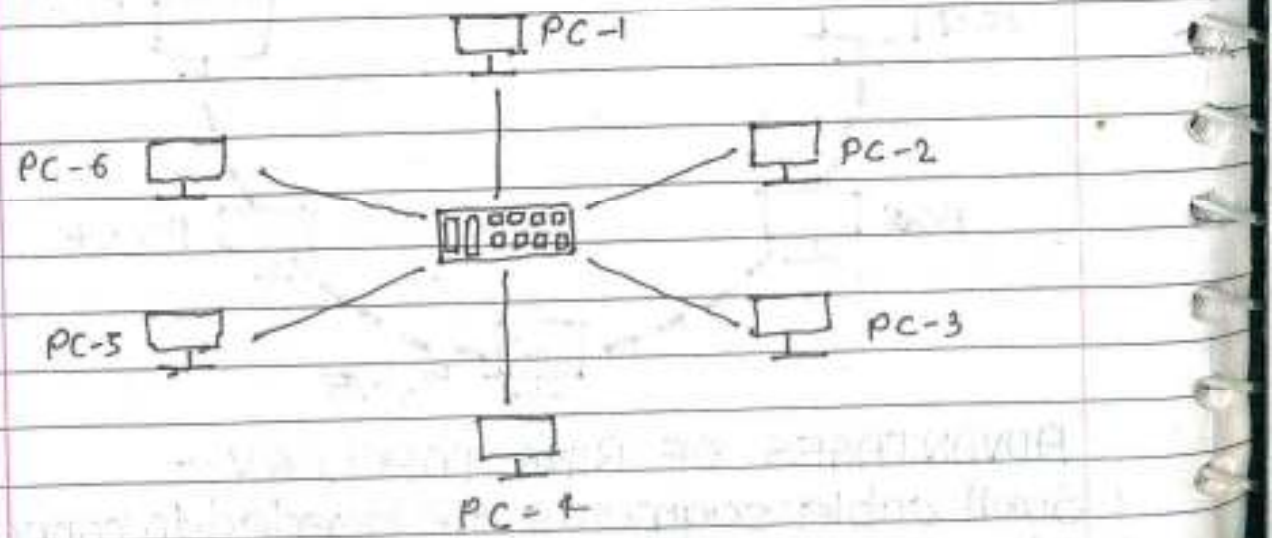
1. Small cable sagments are needed to connect nodes.
2. Ideal for optical fibres as data travels only in one direction

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: / /

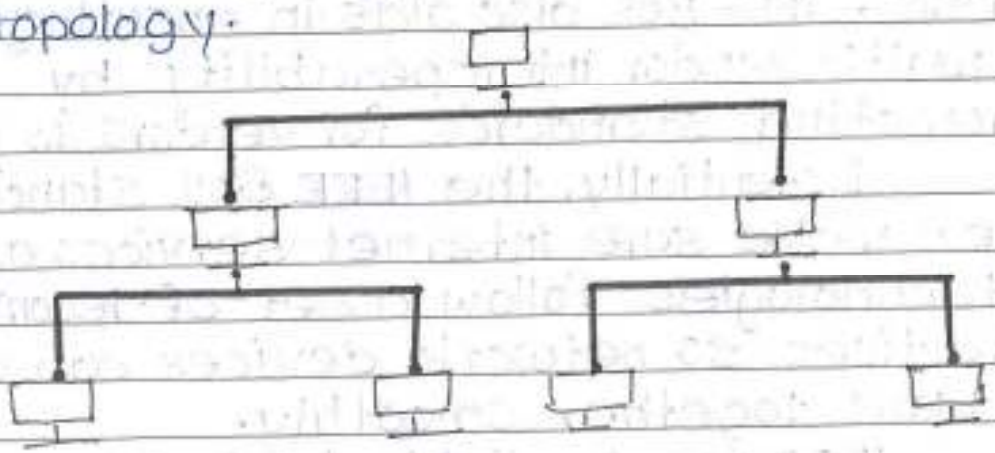
ADVANTAGES OF STAR TOPOLOGY -

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 hierarchal 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 tree 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

LMSC was formed in 1980 in order to standardize network protocols and provide a path to compatible devices across numerous industries.

Without these standards, equipment suppliers would manufacture program hardware that would only connect to certain computers. It would be much more difficult to connect to systems not

Date: / /

Standardizing protocols help ensure that multiple type of device can connect to multiple networks types. It also help make sure that network management isn't the challange it could be if it wasn't in place

IEEE 802 will also coordinate with other international standards, such as ISO, to help maintain international standards.

In addition, the "802" in IEEE 802 does not stand for anything with ~~ether~~ high significance. 802 was just the next numbered project.

NETWORK ADAPTER

A network adapter is the component of a computer's internal hardware that is used for communicating over a network with another computer. It enables a computer to connect with another computer, server or any networking device over an Local Area Network (LAN) connection. A network adapter can be used over a wired or wireless networks.

A network adapter is usually the component within a computer for interacting or connecting with a network. Typically it is built on a

Date: / /

printed circuit boards with jumpers that connect it with the computer's motherboard.

A network adapter for wired networks has an RJ-45 port that uses twisted or untwisted pair cable for network connectivity. Wireless adapter connects with the network through a built-in or externally connected antenna. Both network adapters support popular LAN protocols, including TCP/IP.

SWITCHING TECHNIQUES

In large networks, there may be more than one paths for transmitting data from sender to receiver. Selecting a path that data must take, out of the available options is called switching. There are two popular switching techniques - circuit switching and packet switching.

CIRCUIT SWITCHING - When a dedicated path is established for data transmission between sender and receiver, it is called circuit switching. When any network node wants to send data, be it audio, video, text or any other type of information, a call ~~request~~ request signal is sent to the receiver and acknowledged back to ensure.

Date: / /

availability of dedicated path. This dedicated path is then used to send data. ARPANET used circuit switching for communication over the network.

ADVANTAGES OF CIRCUIT SWITCHING -
Circuit switching provides these advantages over other switching techniques.

1. One path is set up, the only delay is in data transmission speed.
2. No problem of congestion or garbled message.

DISADVANTAGES OF CIRCUIT SWITCHING
Circuit switching has its disadvantages too -

1. Long set up time is required.
2. A request token must travel to the receiver and the acknowledged before any transmission can happen.
3. Line may be held up for a long time.

PACKET SWITCHING - The major problem with circuit switching is that it needs a dedicated line for transmission. In packet switching, data is broken down into small packets with each packet having source and destination addresses travelling from one router to the next router.

Date: / /

NETWORKING TERMINOLOGIES

1. CHANNEL - Physical medium like cables over which information is exchanged is called channel. Transmission channel may be analog or digital. As the name suggests, analog channel transmit data using analog signal while digital channel transmit data using digital signals.

2. PATH - Path over which data is sent or received is called data channel. The data channel may be a tangible medium like copper wire cables or broadcast medium like radio waves.

3. DATA TRANSFER RATE - The speed of data transferred or received over transmission channel, measured per unit time is called data transfer rate. The smallest unit of measurement is bits per second (bps). 1 bps means 1 bit (0 or 1) of data is transferred in 1 second.

Here are some commonly used data transfer rates -

1 bps = 1 Byte per second = 8 bits / sec
1 kbps = 1 kilobits / sec. = 1024 bits / sec.
1 mbps = 1 Megabit / sec. = 1024 kbps
1 Gbps = 1 Gigabit / sec = 1024 Mbps

Date: / /

4. BANDWIDTH - Data transfer rates can be supported by a network is called its bandwidth. It is measured in bits per second (bps). Modern day network provides bandwidth in Kbps, Mbps and Gbps.
Some of the factors affecting a network's bandwidth include -
A. Network device used
B. Protocols used
C. Number of users connected
D. Network overheads like collision, error etc.

5. THROUGHPUT - Throughput is the actual speed with which data gets transferred over the network. Besides transmitting the actual data, network bandwidth is used for transmitting error messages, acknowledgement frame etc.
Throughput is better measurement of network speed, efficiency, and capacity utilization rather then bandwidth.

6. PROTOCOL - Protocol is a set of rule and regulations used by devices to communicate over the network. Just like humans computers also need rules to

Date: / /

ensure successful communication. If two people start speaking at the same time or in different languages or when no interpreter is present, no meaningful exchange of information can occur.

Similarly, devices connected on the network need to follow rules defining situations like when and how to transmit data, when to receive data, how to give error free message, etc.

Some common protocols used over the Internet are -

A. Transmission Control Protocol
B. Internet Protocol
C. Point-to-Point Protocol
D. File Transfer Protocol
E. HyperText Transfer Protocol
F. Internet Message Access Protocol

TRANSMISSION MEDIA

For any networking to be effective, raw stream of data is to be transmitted from one device to another device over same medium. Various transmission media can be used for transfer of data.

These transmission media may be of two types -

A. Guided Transmission Media
B. Unguided Transmission Media

Date: / /

1. GUIDED TRANSMISSION MEDIA

In guided transmission media, data travels through cabling system that has a fixed path. For example- copper wire, fibreoptic.

2. UNGUIDED TRANSMISSION MEDIA

In unguided transmission media, transmitted data travels through free space in form of electromagnetic signal. For example- laser, radio waves etc.

Each transmission media has its own advantages and disadvantages in terms of bandwidth, speed, delay, cost per bit, ease of installation and maintenance etc.

TWISTED PAIR CABLE - Copper wire are the most common wires used for transmitting signals because of good performance at low costs. They are most commonly used in telephone lines. However, if two or more wires are lying together, they can interfere with each other's signals. To reduce this electromagnetic interference, pair of copper wires are twisted together in helical shape like a DNA molecule. Such twisted copper wires are called twisted pair. To reduce interference between

Date: / /

nearly twisted pairs, the twist rates are different for each pair.

Upto 25 twisted pair are put together in a protective covering to form twisted pair cables that are the backbone to telephone systems and Ethernet network.

ADVANTAGES OF TWISTED PAIR CABLE -

Twisted pair cable are the oldest and most popular cables all over the world. This is due to the many advantages that they offer -

1. Trained personnel easily available due to shallow learning curve.
2. Can be used for both analog and digital transmissions.
3. Least expensive for short distance.
4. Entire network does not go down if a part of network is damaged.

DISADVANTAGES OF TWISTED PAIR CABLE -

1. Signal can not travel long distances without repeaters.
2. High error rate for distances greater than 100 m.
3. Very thin and hence breaks easily.
4. Not suitable for broadband connections.

SHIELDED TWISTED PAIR CABLE - To cover the

Date: / /

pair cables to pick up noise signals, wires are shielded in the following three ways:

1. Each twisted pair is shielded
2. Set of multiple twisted pairs in the cable is shielded.
3. Each twisted pair and then all the pairs are shielded.

Such twisted pair are called Shielded Twisted Pair (STP) cables. The wires that are not shielded but simply bundled together in a protective sheath are called Unshielded Twisted Pair (UTP) cables. These cables can have maximum length of 100 meters.

Shielding makes the cable bulky so UTP are more popular than STP. UTP cables are used as the last mile network connection in homes & offices.

CO-AXIAL CABLE - Co-axial cables are copper cables with better shielding than twisted pair cables, so that transmitted signals may travel longer distances at higher speed. A co-axial cable consists of these layers starting from the innermost -

1. Stiff copper wire as core.
2. Insulating material surrounding the core.
3. Closely woven braided mesh of conducting material surrounding the insulator.

Date: / /

4. Protective plastic sheath encasing the wire.

Co-axial cables are widely used for cable TV connections and LANs

ADVANTAGES OF CO-AXIAL CABLES -

1. Excellent noise immunity.
2. Signals can travel longer distances at higher speed.
3. Can be used for both analog and digital signal.
4. Inexpensive as compared to fibre optic cables.
5. Easy to install and maintain.

DISADVANTAGES OF CO-AXIAL CABLE →

1. Expensive as compared to twisted pair cables.
2. Not compatible with twisted pair cables.

OPTICAL FIBRE - Thin glass or plastic threads used to transmit data using light waves are called optical fibre. Light Emitting Diodes (LEDs) or Laser Diodes (LDs) emit light waves at the source which is read by a detector at the other end. Optical fibre cable has a bundle of such threads or fibres bundled together in a protective covering. Each fibre is made up of these three layers, starting with the innermost layer -

1. Core made of high quality silica glass or plastic
2. Cladding made of high quality silica glass or plastic with a lower refractive index than the core

Date: / /

3. Protective outer covering called buffer.

Both core and cladding are made of similar material. However as refractive index of the cladding is lower, any stray light wave trying to escape the core is reflected back due to total internal reflection.

Optical fibre is rapidly replacing copper wires in telephone lines, internet communication and even cable TV connections because transmitted data can travel very long distances without weakening. Single mode fibre optics can have maximum segment length of 2 KMs and bandwidth of upto 100 Mbps. Multi-mode fibre optics cable can have maximum segment length of 100 KMs and bandwidth upto 2 Gbps.

ADVANTAGE OF OPTICAL FIBRE-

Optical fibre is fast replacing copper wires because of these advantages that it offers -

1. High bandwidth.
2. Immune to electromagnetic interference
3. Suitable for industry and noisy areas.
4. Signals carrying data can travel long distances without weakening.

Date: / /

DISADVANTAGES OF OPTICAL FIBRE -

Despite long segment lengths and high bandwidth, using optical fibre may not be viable option for every one due to these disadvantages -

1. Optical fibre cables are expensive.
2. Sophisticated technology required for manufacturing, installing and maintaining optical fibre cables.
3. Light waves are unidirectional, so two frequencies are required for full-duplex transmission.

INFRARED - Low frequency infrared waves are used for very short distance communication like TV remote, wireless speakers, automatic doors, hand held device, etc. Infrared signal cannot penetrate walls but they can propagate within a room. However due to short distance, it is considered to be one of the most secure transmission modes.

RADIO WAVE - Transmission of data using radio frequencies is called 'radio-wave transmission'. We all are familier with radio channels that broadcast entertainment programs. Radio stations transmit radio-waves using transmitters, which are received by the receiver installed in our devices.

Both transmitters and receivers uses

Date: / /

antennas to radiate or capture radio signals. These radio frequencies can also be used for direct voice communication within the allocated range. This range is usually 10 miles

ADVANTAGES OF RADIO WAVES -

1. Inexpensive mode of information exchange
2. No lands need to be acquired for laying cables
3. Installation and maintenance of devices is cheap.

DISADVANTAGES OF RADIO WAVES -

1. Insecure communication medium.
2. Prone to weather changes like rain, thunderstorms etc.

NETWORK DEVICES

Hardware devices that are used to connect computers, printers, fax machines and other electronic devices to a network are called network devices. These devices transfer data in a fast, secure and correct way over same or different networks. Network devices may be inter-network or intra-network. Some devices are installed on the device, like NIC card or RJ-45 connector. Whereas some

Date: / /

are part of the network, like router, switch etc.

1. MODEM – Modem is a device that enables a computer to send or receive data over telephone or cable lines. The data stored on the computer is digital, whereas a telephone line or cable wire can transmit only analog data.

The main function of the modem is to convert digital signal into analog and vice versa. Modem is a combination of two devices - modulator and demodulator. The modulator converts digital data into analog data when the data is being sent by the computer. The demodulator converts analog signal into digital data. When it is being received by the computer.

Modem can be categorized in several ways like in which it can transmit data, type of connection to the transmission line, transmission mode etc.

Depending on direction of data transmission modem can be of these types –

A. SIMPLEX – A simplex modem can transfer data in only one direction, from digital device to network (modulator) or network to digital device (demodulator).

Date: / /

B. HALF DUPLEX - A half duplex modem has the capacity to transfer data in the both directions but only one at a time.

C. FULL DUPLEX - A full duplex modem can transmit data in the both directions simultaneously.

2. RJ45 CONNECTOR - RJ45 is the acronym for registered jack - 45.
RJ-45 connector is an 8-pin jack used by devices to physically connect to Ethernet based Local Area Networks (LANs) Ethernet is a technology that defines protocols for establishing a LAN. The cable used for Ethernet LANs are twisted pair ones and have RJ45 connector pins at both ends. These pins go into the corresponding socket on devices and connect to the devices of the network.

3. ETHERNET CARD - Ethernet card is also known as Network Interface Card. (NIC), is a hardware component used by computers to connect to Ethernet LAN and communicate with other devices on the LAN. The earliest Ethernet cards were external to the system and needed to be installed manually. In modern computer

Date: / /

systems, it is an internal hardware component. The NIC has RJ45 socket where network cable is physically plugged-in.

Ethernet cards speeds may vary depending upon the protocols it supports. Old Ethernet cards had maximum speed of 10Mbps. However, modern cards support fast Ethernets up to a speed of 100Mbps. Some cards even have capacity of 1Gbps.

4. ROUTER - A router is a network layer hardware device that transmits data from one LAN to another. If both networks supports the same set of protocols. So a router is typically connected to at least two LANs and the Internet Service Provider (ISP). It receives its data in the form of packets, which are data frames with their destination address added. Router also strengthens the signals before transmitting them. That's why it is also called repeater.

5. ROUTING TABLE - A router reads its routing table to decide the best available route the packet can take to reach its destination quickly and accurately. The routing table may be of these two types -

Date: / /

A. STATIC ROUTING TABLE - In a static routing table the routes are fed manually. So, it is suitable only for very small networks that have maximum two or three routers

B. DYNAMIC ROUTING TABLE - In a dynamic routing table, the router communicates with other routers through protocols to determine which routers are free This is suited for larger networks where manual feeding may not be feasible due to large number of routers.

6. SWITCH - Switch is a network device that connects other devices to Ethernet networks through twisted pair cables. It uses packet switching technique to receive, store and forwards data packets on the network. The switch maintains a list of network addresses of all the devices connected to it.

On receiving a packet, it checks the destination address and transmit the packet to the correct port. Before forwarding, the packets are checked for collision and other network errors. The data is transmitted in full-duplex mode.

Date: / /

Data transmission speed in switches can be double that of other network devices like hubs used for networking. This is because switch shares its maximum speed with all the devices connected to it. This helps in maintaining network speed even during high traffic. In fact, higher data speeds are achieved on network through use of multiple switches.

Monday 27/09/2021

7. GATEWAY - Gateway is a network device used to connect two or more dissimilar networks. In networking parlance network that use different protocols are dissimilar networks. A gateway usually is a different computer with multiple NIC connected to different networks. A gateway can also be configured completely using software. As networks connect to a different network through gateways, these gateways are usually hosts or end points of the network. Gateways uses packet switching technique to transmit data from one network to another. In this way it is similiar to a router, the only difference being router can transmit data only over networks that use same protocols.

8. Wi-Fi CARD - Wi-Fi is the acronym for Wireless fidelity. Wi-Fi technology is used to achieve wireless connection to any

Date: / /

network. Wi-Fi card is a card used to connect any device to the local network wirelessly. The physical area of the network which provides internet access through Wi-Fi is called Wi-Fi Hotspot. The hotspot can be setup at home, office or any public place. Hotspots are themselves are connected to the network through wires.

Modern devices come with their in-built wireless network adapter.

TYPES OF NETWORKS

Networks can be categorized depending on size, complexity, level of security, or geographical range. We will discuss some of the most popular topologies based on geographical spread.

1. LAN – LAN or Local Area Network is a wired network spread over a single site like an office, building or manufacturing unit. LAN is set up to when team members need to share software and hardware resources with each other but not with the outside world. Typical software resource include official documents, user manuals, employee handbook etc. Hardware resources that can be easily shared

Date: / /

over the network include printers, fax machine modems, memory space etc. This decreases infrastructure costs for the organization.

A LAN may be set up using wired or wireless connection. A LAN that is completely wireless is called Wireless LAN or WLAN.

2. MAN - MAN is the acronym for Metropolitan Area Network. It is a network spread over a city, college campus, or a small region. MAN is larger than a LAN and typically spread over several kilometers. Objective of MAN is to share hardware and software resources, thereby decreasing infrastructure costs. MAN can be built by connecting several LANs.

The most common example of MAN is cable TV network.

3. WAN - WAN or Wide Area Network spread over a country or many countries. WAN is typically a network of many LANs, MANs and WANs. Network is set up using wired or wireless connections, depending on availability and reliability

The most common example of WAN is the Internet.

TELNET - Telnet is a network protocol used to virtually access a computer and

Date: / /

to provide a two way collaborative and text based communication channel between two machines.

It follows a user command, TCP/IP for creating remote sessions. On the web HyperText Transfer Protocol (HTTP) and File Transfer Protocol (FTP) simply enable users to request specific files from remote computers, while through Telnet users can log on as a regular user with the privileges they are granted to the specific applications and data on that computer.

Telnet is most likely to be used by program developers and anyone who has a need to use specif application or data located at a remote machine.

HOW TELNET WORKS - Telnet is a type of client server protocol that can be used to open a command line on a remote computer, typically a server. Users can utilize this tool to ping a port and find out whether it is open. Telnet works with what is called a virtual terminal connection emulator or an abstract instance of a connection to a computer using standard protocols to act like a physical terminal connected to a mach

Date: / /

machine. FTP may also be used along with Telnet for users working to send data.

Users connect remotely to a machine using Telnet, sometimes referred as Telnetting into the system. They are prompt to enter their username and password combination to access the remote computer, which enables the running of command line as if logged into the computer in-person. Despite the physical location of users, their IP address will match the computer logged into rather than the one physically used to connect.

USES OF TELNET - Telnet can be used for a variety of activities on a server, including editing files, running various programs and checking email.

Some servers enables remote connections using telnet to access public data to play simple games or look up weather reports. Many of these features exist for nostalgic fun or because they still have compatibility with older systems that need access to specific data.

Users are also able to connect to any software that utilizes text-based, unencrypted protocols via Telnet from web servers to ports. Users can open a command prompt on the remote machine, type the word telnet and the remote machine's

Date: / /

name or IP address, and the telnet connection will ping the port to see if it is open or not. An open port will show a blank screen, while an error message that says the port is connecting means that it is closed.

SECURITY - Telnet is not a secure protocol and is un-encrypted By monitoring a user's connection, anyone can access a person's username, password and other private information that is typed over the Telnet session in plaintext. With this information access can be gained to the user's device.

SSH & OTHER PROTOCOLS - Some modern systems enable only command-line connections using Secure-Shell (SSH), an encrypted tool similar to telnet or through a Virtual Private Network (VPN). Because of security concern, many professional organizations require use of SSH, PuTTy or other options instead of Telnet. SSH is the most commonly used alternative, largely because it encrypts all the traffic that passes over the communication channel.

Date: / /

Also, unlike newer protocols, Telnet doesn't support Graphical User Interfaces (GUIs), making it uncompatible with many modern programs, from spreadsheets and web browsers to word processors and simulation software. Because those program run complex graphical interfaces, large amounts of data, especially visual data would be lost through a Telnet session connection.

WHAT IS DNS ?

The domain name system (DNS) is the phonebook of the internet. Human access information online through domain names like google.com. Web browsers interact through Internet Protocol (IP). DNS translates domain names to IP addresses so browsers can load internet resources.

Each device connected to the internet has a unique IP address which other machine use to find the device. DNS servers eliminate the need for humans to memorize IP addresses such as 192.168.1.1 (in IPv4) or more complex newer alphanumeric IP addresses such as ~~2400:cb00:2048~~ 2400:cb00:2048:1::c629:d7a2 (in IPv6).

HOW DOES DNS WORK - The process of DNS resolution involves converting

Date: / /

a hostname such as (example.com) into a computer friendly IP address (such as 192.168.1.1). An IP address is given to each device on the Internet, and that address is necessary to find the appropriate internet device - like a street address is used to find a particular home. When a user wants to load a webpage, a translation must occur between what a user types into their web browser (example.com) and the machine friendly address necessary to locate the example.com webpage.

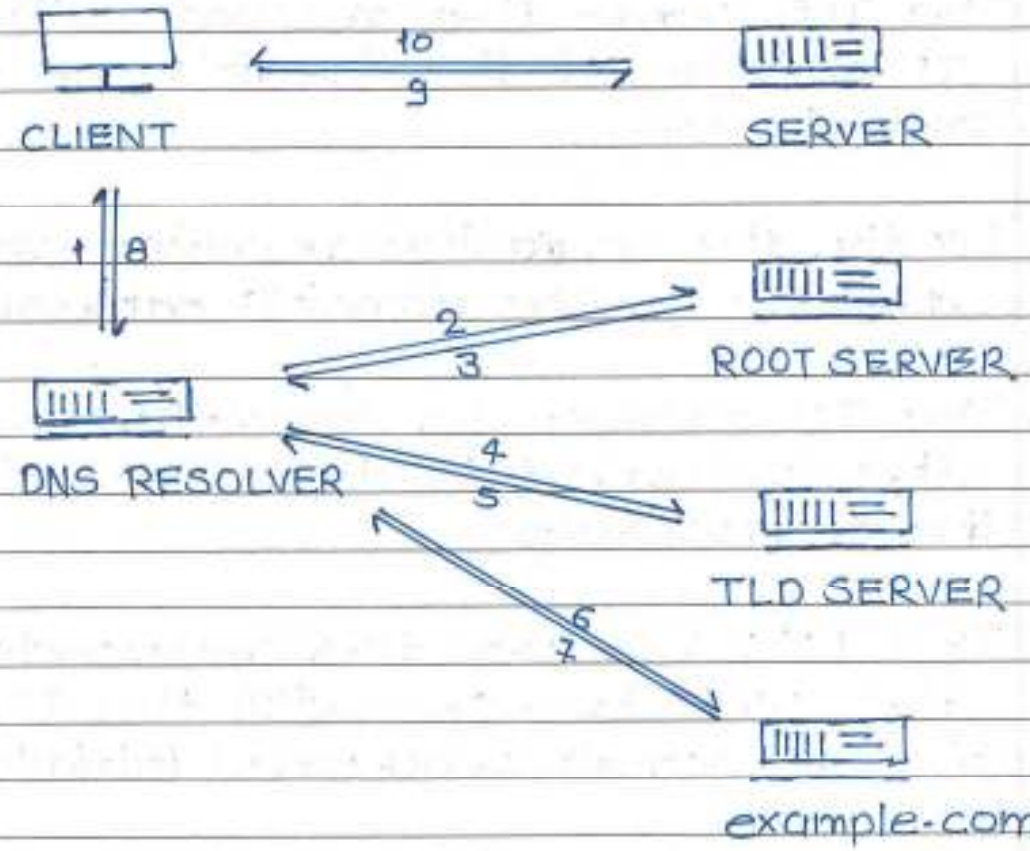
WHAT ARE THE STEPS IN A DNS LOOKUP-

For most situations, DNS is concerned with a domain name being translated into the appropriate IP address. To learn how this process works, it helps to follow the path of a DNS lookup as it travels from a web browser, through the DNS lookup process, and back again.

Often DNS lookup information will be cached either locally inside the querying computer or remotely in the DNS infrastructure. There are typically 8 steps in a DNS lookup. When DNS information is cached, steps are skipped from the DNS lookup process which

Date: / /

makes it quicker. The example below outlines all 8 steps when nothing is cached:



1. A user types 'example.com' into a web browser and the query travels into the Internet and received by a DNS resolver.

2. The resolver then queries a DNS root nameserver (.).

3. The root server then responds to the resolver with the address of a Top Level Domain (TLD) DNS server (such as .com or .net) which stores the information for its domain. When

Date: / /

4. The resolver then makes a request to the .com TLD.

5. The TLD server then responds with the IP address of the domain's nameserver - example.com.

6. Lastly, the recursive resolver sends a query to the domain's nameserver

7. The IP address for example.com is then returned to the resolver from the nameserver.

8. The DNS resolver then responds to the web browser with the IP address of the domain requested initially.

Once 8 steps of the DNS lookup have returned the IP address for example.com, the browser is able to make the request for the webpage.

9. The browser makes a HTTP request to the IP address.

10. The server at that IP returns the webpage to be rendered in the browser.

Date: / /

NETWORK SECURITY

A network is defined as two or more computing devices connected together for sharing resources efficiently. Further, connecting two or more networks together is known as internetworking. Thus, the Internet is just an internetwork - a collection of interconnected networks.

For setting up its internal network, an organization has various options. It can use a wired network or a wireless network to connect all workstations. Nowdays, organizations are mostly using combination of both wired and wireless network.

WIRED AND WIRELESS NETWORK - In a wired network, devices are connected to each other using cables. Typically, wired networks are based on Ethernet protocols where devices are connected using the Unshielded Twisted Pair (UTP) cables to the different switches. These switches are further connected to the network router for accessing the Internet.

In wireless network, the device is connected to an access point through radio transmissions. The access points are further connected through cables to switch/ router for external network access.

Wireless networks have gained

Date: / /

popularity due to the mobility offered by them. Mobile devices need not to be tied to a cable and can roam freely within the wireless network range. This ensures efficient information sharing and boosts productivity.

VULNERABILITIES & ATTACKS - The common vulnerability that exists in both wired and wireless networks is an "un-authorized access" to a network. An attacker can connect his device to a network though unsecure hub/switch port. In this regards wireless network are considered less secure than wired network, because wireless network can be easily accessed without any physical connection. After accessing, an attacker can exploit this vulnerability to launch attacks such as -

1. Sniffing the packet data to steal valuable information.
2. Denial of service to legitimate users on a network by flooding the network medium with spurious packets.
3. Spoofing physical identities (MAC) of legitimate hosts and then stealing data or further launching a "man-in-the-middle' attack.

Date: / /

GOALS OF NETWORK SECURITY -

There exists large number of vulnerabilities in the network. Thus during transmission, data is highly vulnerable to attacks. An attacker can target the communication channel, obtain the data and read the same or re-insert a false message to achieve his nefarious aims.

Network security is not only concerned about the security of the computer at each end of the communication chain; however, it aims to ensure that the entire network is secure.

Network security entails protecting the usability, reliability, integrity, and safety of network and data. Effective network security defeats a variety of threats from entering or spreading on a network.

The primary goal of network security are confidentially, integrity and availability. These three pillars of network security are often represented as CIA triangle.

1. CONFIDENTIALITY - The function of confidentiality is to protect precious business data from unauthorized access. Confidentiality part of network security makes sure that the data is available only to the intended and authorized persons only.

2. INTEGRITY - This goals means maintaining

Date: / /

and assuring the accuracy and consistency of data. The function of integrity is to make sure that data is reliable and is not changed by unauthorized person.

3. AVAILABILITY - The function of availability in network security is to make sure that the data, network resources/ services are continuously available to the legitimate users, whenever they require it.

→ SECURITY MECHANISMS AT NETWORKING LAYERS

Several security mechanisms have been developed in such a way that can be developed at a specific layer of the OSI network layer model.

1. SECURITY AT APPLICATION LAYER

Security measures at this layer are application specific. Different types of application would need separate security measures. In order to ensure application layer security, the applications needs to be modified.

2. SECURITY AT TRANSPORT LAYER

Security measures at this layer can be used to protect data in a single communication session between two hosts. The most common use for transport

Date: / /

layer security protocols is protecting the HTTP and FTP session traffic. The Transport Layer Security (TLS) and Secure Socket Layer (SSL) are the most common protocol used for this purpose

3. SECURITY AT NETWORK LAYER

Security measures at this layer can be applied to all applications; thus they are not application-specific. All network communications between two hosts or networks can be protected at this layer without modifying any application. In some environments, network layer security protocol such as Internet Protocol Security (IPsec) provides a much better solution than transport or application layer controls because of the difficulties in adding controls to individual applications. However, security protocols at this layer provides less communication flexibility that may be required by some applications.

Incidentally, a security mechanism designed to operate at a higher layer cannot provide protection for data at lower layers, because the lower layers perform functions of which the higher layers are not aware. Hence, it may be necessary to deploy multiple security mechanism for enhancing the network security.

Date: / /

VOICE OVER IP

VoIP is the acronym for Voice Over Internet Protocol. It means telephone services over Internet. Traditionally Internet had been used for exchanging messages but due to advancement in technology, its service quality has increased manifold. It is now possible to deliver voice communication over IP networks by converting voice data into packets. VoIP is a set of protocols and systems developed to provide this service seamlessly.

Here are some of the protocols used for VoIP -

1. H.323
2. Session Initiation Protocol (SIP)
3. Session Description Protocol (SDP)
4. Media Gateway Control Protocol (MGCP)
5. Real-time Transport Protocol (RTP)
6. Skype Protocol

We will discuss two of the most fundamental protocols - H.323 & SIP here.

1. H.323 - H.323 is a VoIP standard for defining the components, protocols and procedures to provide real-time multimedia sessions including audio, video and data transmissions over packet

Date: / /

switched networks. Some of the services facilitated by H.323 include -

1. IP telephony
2. Video telephony
3. Simultaneous audio, video and data communications.

2. SIP - SIP is an acronym for Session Initiation Protocol. SIP is a protocol to establish, modify and terminate multimedia sessions like IP telephony. All systems that need multimedia sessions are registered and provide SIP address, much like IP address. Using this address, caller can check callee's availability and invite it for a VoIP session accordingly.

SIP facilitates multiparty multimedia sessions like video confrencing involving three or more people. In a short span of time SIP has become integral to VoIP and largely replaced H.323.

INTRODUCTION TO VPN

A VPN (Virtual Private Network) is a service that creates a safe, encrypted online connection. Internet users may use a VPN to give themselves more privacy and anonymity online or circumvent geographic-based blocking and censorship. VPNs essentially extend a

Date: / /

private network across a public network, which should allow a user to securely send and receive data ~~across~~ the internet.

Typically, a VPN is used over a less secure network, such as the public internet. Internet service providers (ISP) normally have a rather large amount of insight into a customer's activities. In addition, some unsecured Wi-Fi access points (APs) may be convenient avenue for attackers to gain access to a user's personal data. An internet user could use a VPN to avoid these encroachments on privacy.

VPNs can be used to hide a user's history, IP addresses, and geographical location, Web security or devices being used. Anyone on the same network will not be able to see what a VPN user is doing. This makes VPNs a go-to tool for online privacy.

A VPN uses tunneling protocols to encrypt data at the sending end and decrypts it at the receiving end. The originating network addresses are also encrypted to provide better security for online activities.

Date: / /

VPN apps are often used to protect data transmissions on mobile devices. They can also be used to visit websites that are restricted by location. However, secure access through a mobile VPN should not be confused with private browsing. Private browsing does not involve encryption, it is simply optional browser setting that prevents identifiable data from being collected.

VPN PROTOCOLS - VPN protocols ensure an appropriate level of security to the connected systems when the underlying network infrastructure alone cannot provide it. There are several different protocols used to secure and encrypt users and corporate data. They include the following

1. IP Security (IPsec)
2. Secure Socket Layer (SSL) and Transport Layer Security (TLS)
3. Point-to-point Tunneling Protocol (PPTP)
4. Layer-2 Tunneling Protocol (L2TP)
5. OpenVPN

BENIFITS AND CHALLENGES OF USING A VPN

BENIFITS OF USING A VPN INCLUDE THE FOLLOWING-

1. Secure connections with encrypted data.
2. Bypassing geo-blocked content.

Date: / /

3. The ability to hide a user's IP address and browsing history.
4. Making it more difficult for advertisers to target individual ads.

CHALLANGES OF USING A VPN. INCLUDE THE FOLLOWING -

1. Not all devices may support a VPN
2. Paid VPNs are more trusted, secure options
3. A VPN may slowdown internet speeds
4. VPN do not protect against every threat

INTRODUCTION TO DHCP

Dynamic Host Configuration Protocol (DHCP) is a client-server protocol that automatically assigns an Internet Protocol (IP) address to a device as well as other related configurations.

Every computer on a network must have an IP address to communicate with other devices. An IP address is an identifier for a computer or device on a network.

There are two ways an IP address is assigned to a computer - static and dynamic. A static IP is where a user assigns an IP address manually to a computer. However, this process is tedious and error-prone as it requires

Date: / /

manual intervention every time a device joins the network. Dynamic IP assignment resolves the issue.

A dynamic IP is where a computer receives an IP from a DHCP server. Moreover a DHCP server also assigns a device a subnet mask, default gateway and the Domain Name System (DNS) server in addition.

HOW DOES DHCP WORK - In a network, each device will have a DHCP client installed. Additionally, there is a DHCP server which is responsible for the automatic assignment of addresses as requested by the DHCP client.

The assignment between the DHCP client and server follows four steps -

1. SERVER DISCOVERY - Once a device joins a network and requires an IP address, it broadcasts a message to the network asking for it. The DHCP server will process the request and all other devices in the network will ignore this message.

2. DHCP OFFER - The DHCP server looks for an available IP address from its pool of addresses and offers one to the requesting device.

Date: / /

3. DHCP REQUEST - The device responds to the DHCP server by confirming the provided IP address.

4. ACKNOWLEDGMENT - The DHCP server provides the IP address, subnet mask, default gateway and the DNS server details to the device.

BENIFITS OF DHCP - DHCP offers several benifits over static IP configuration -

1. RELIABLE IP ADDRESS MANAGEMENT
DHCP minimizes configuration errors caused by manual IP address configuration, such as typographical errors or address conflicts caused by the assignment of an IP address to more than one computer at the same time.

2. REDUCED MANUAL INTERVENTION -
DHCP lets network administrators centralize and automate the IP address configuration process. DHCP lets efficient management of IP addresses. For example- if a device leaves the network or moves to different location, the assigned IP address is removed and assigned to another device.

Date: / /

NETWORK INTEGRITY

Network integrity automatically detects and validates rogue wi-fi networks and spoofed carrier networks. Whenever these type of suspicious networks are detected, Network integrity protects the user devices by either disconnecting from the network or establishing a policy-driven Smart VPN tunnel.

Network integrity gives insight into whether users are connecting to an evil twin or suspicious network. Attackers setup evil twin hotspots, including the primary network name of a nearby business, such as a coffee shop that provides free wi-fi access to its customers. By imitating a legitimate hotspot and tricking users into connecting to it, an attacker can then steal account names and passwords and redirect victims to malware sites or phishing sites.

Network integrity prevents from various network attacks and attacks on browsers when users -

1. Connect to suspicious network
2. Connect to network with previous detections
3. Connect to evil twin networks