ASSIGNMENT 1

Switch used in lab: Cisco 24 port

What are computer networks?

Computer networks is the group of computers connected with each other through transmission media so that various devices can interact with each other.

Features of Computer Networks.

1. Fault Tolerance : Fault Tolerance means the ability to continue working despite failures and ensure no loss of services.
2. Scalability : Scalability means the ability to grow based on the needs and have good performance after growth.
3. Quality of Service (QoS) : Quality of Service (QoS) refers to the ability to set priorities and manage data traffic and reduce data loss, delay, etc.
4. Security : Security is the ability to prevent unauthorized access, misuse, or forgery. Also it is the ability to provide confidentiality, integrity and availability.

LAN, MAN, WAN

1. LAN stands for local area network. It is a group of network devices that allow communication between various connected devices. LAN has a short propagation delay than MAN as well as WAN. It covers smaller areas such as colleges, schools, hospitals, and so on.

2. MAN stands for metropolitan area network. It covers a larger area than LAN such as small towns, cities, etc.

3. WAN stands for wide area network. It covers a large area than LAN as well as a MAN such as country/continent etc. PSTN or satellite medium is used for wide area networks.

List of Networking Devices

Network devices, also known as networking hardware, are physical devices that allow hardware on a computer network to communicate and interact with one another.

1. Repeater – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy it bit by bit and regenerate it. It is a 2-port device.

2. Hub – A hub is a basically multi-port repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different

stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, the collision domain of all hosts connected through Hub remains one. Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

3. Bridge – A bridge operates at the data link layer. A bridge is a repeater, which adds on the functionality of filtering content by reading the MAC addresses of the source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

4. Switch – A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only. In other words, the switch divides the collision domain of hosts, but the broadcast domain remains the same.

5. Routers – A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets. The router divides the broadcast domains of hosts connected through it.

6. Gateway – A gateway, as the name suggests, is a passage to connect two networks that may work upon different networking models. They work as messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switches or routers.

8. NIC – NIC or network interface card is a network adapter that is used to connect the computer to the network. It is installed in the computer to establish a LAN. It has a unique id that is written on the chip, and it has a connector to connect the cable to it. The cable acts as an interface between the computer and the router or modem. NIC card is a layer 2 device which means that it works on both the physical and data link layers of the network model.

Wireshark

Wireshark is a software tool used to monitor the network traffic through a network interface. It is the most widely used network monitoring tool today.

Public and Private IP

Private IP address of a system is the IP address that is used to communicate within the same network. Using private IP data or information can be sent or received within the same network.

Public IP address of a system is the IP address that is used to communicate outside the network. A public IP address is basically assigned by the ISP (Internet Service Provider).

Ping : Ping is a method of determining latency or the amount of time it takes for data to travel

Types of Topologies

1. Star :

   ● Star topology is a network topology in which all the nodes are connected to a single device known as a central device.

   ● Star topology requires more cable compared to other topologies. Therefore, it is more robust as a failure in one cable will only disconnect a specific computer connected to this cable.

   ● If the central device is damaged, then the whole network fails.

   ● Star topology is very easy to install, manage and troubleshoot. It is commonly used in office and home networks.

2. Ring :
   - Ring topology is a network topology in which nodes are exactly connected to two or more nodes and thus, forming a single continuous path for the transmission.
   - It does not need any central server to control the connectivity among the nodes.
   - If the single node is damaged, then the whole network fails.
   - Ring topology is very rarely used as it is expensive, difficult to install and manage.
   - Examples of Ring topology are SONET network, SDH network, etc.
3. Bus :
   - Bus topology is a network topology in which all the nodes are connected to a single cable known as a central cable or bus.
   - It acts as a shared communication medium, i.e., if any device wants to send the data to other devices, then it will send the data over the bus which in turn sends the data to all the attached devices.
   - Bus topology is useful for a small number of devices.
   - As if the bus is damaged then the whole network fails.

4. Mesh :
    - Mesh topology is a network topology in which all the nodes are individually connected to other nodes.
    - It does not need any central switch or hub to control the connectivity among the nodes.
    - Mesh topology is categorized into two parts: Fully connected mesh topology: In this topology, all the nodes are connected to each other. Partially connected mesh topology: In this topology, all the nodes are not connected to each other.
    - It is robust as a failure in one cable will only disconnect the specified computer connected to this cable.
    - Mesh topology is rarely used as installation and configuration are difficult when connectivity gets more.
    - Cabling cost is high as it requires bulk wiring.

ASSIGNMENT 02

Types of Transmission Media:

1. Guided Media: It is also referred to as Wired or Bounded transmission media.

(i) Twisted Pair Cable : It consists of 2 separately insulated conductor wires wound about each other.

- Unshielded Twisted Pair (UTP)**:** UTP consists of two insulated copper wires twisted around one another. This type of cable has the ability to block interference and does not depend on a physical shield for this purpose.
- Shielded Twisted Pair (STP): This type of cable consists of a special jacket (a copper braid covering or a foil shield) to block external interference.

(ii) Coaxial Cable : It has an outer plastic covering containing an insulation layer made of PVC or Teflon and 2 parallel conductors each having a separate insulated protection cover.

(iii) Optical Fiber Cable : It uses the concept of refraction of light through a core made up of glass or plastic. The core is surrounded by a less dense glass or plastic covering called the cladding

2. Unguided Media: It is also referred to as Wireless or Unbounded transmission media. No physical medium is required for the transmission of electromagnetic signals.

(i) Radio waves : These are easy to generate and can penetrate through buildings. The sending and receiving antennas need not be aligned. Frequency Range:3KHz – 1GHz.

(ii) Microwaves : It is a line of sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Frequency Range:1GHz – 300GHz.

(iii) Infrared : Infrared waves are used for very short distance communication. They cannot penetrate through obstacles. This prevents interference between systems. Frequency Range:300GHz – 400THz.

ASSIGNMENT 3

Error Type difference between CRC and Hamming

Hamming Code | Error detection Correction Encodding Decodding 7 bit in hindi/Urdu

Lec-29: Cyclic Redundancy Check(CRC) for Error Detection and Correction | Computer N...

Hamming Code : Hamming code is a set of error-correction codes that can be used to detect and correct the errors.

Redundant bits are extra binary bits that are generated and added to the information-carrying bits of data transfer to ensure that no bits were lost during the data transfer. The number of redundant bits can be calculated using the following formula:

$2^r \geq m + r + 1$

where, r = redundant bit, m = data bit

A **parity bit** is a bit appended to a data of binary bits to ensure that the total number of 1's in the data is even or odd. Parity bits are used for error detection.

ASSIGNMENT 4

Sliding Window Protocol:

The sliding window is a technique for sending multiple frames at a time. It controls the data packets between the two devices where reliable and gradual delivery of data frames is needed. It is also used in TCP (Transmission Control Protocol).

In this technique, each frame has sent from the sequence number. The sequence numbers are used to find the missing data in the receiver end. The purpose of the sliding window technique is to avoid duplicate data, so it uses the sequence number.

Go-Back-N ARQ :

Go-Back-N ARQ protocol is also known as Go-Back-N Automatic Repeat Request. It is a data link layer protocol that uses a sliding window method. In this, if any frame is corrupted or lost, all subsequent frames have to be sent again.

If the receiver receives a corrupted frame, it cancels it. The receiver does not accept a corrupted frame. When the timer expires, the sender sends the correct frame again.

Selective Repeat ARQ :

Selective Repeat ARQ is also known as the Selective Repeat Automatic Repeat Request. It is a data link layer protocol that uses a sliding window method. The Go-back-N ARQ protocol works well if it has fewer errors. But if there is a lot of error in the frame, lots of bandwidth loss in sending the frames again. So, we use the Selective Repeat ARQ protocol. In this protocol, the size of the sender window is always equal to the size of the receiver window.

If the receiver receives a corrupt frame, it does not directly discard it. It sends a negative acknowledgement to the sender. The sender sends that frame again as soon as on the receiving negative acknowledgment. There is no waiting for any time-out to send that frame

Types of Network Architecture:

1. Peer-To-Peer network

    - Peer-To-Peer network is a 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 up to 10 computers.
    - Peer-To-Peer network has no dedicated server.
    - Special permissions are assigned to each computer for sharing the resources, but this can lead to a problem if the computer with the resource is down.

2. Client/Server Network

    - Client/Server network is a network model designed for the end users called clients, to access the resources such as songs, video, etc. from a central computer known as Server.
    - The central controller is known as a server while all other computers in the network are called clients. A server performs all the major operations such as security and network management.
    - A server is responsible for managing all the resources such as files, directories, printer, etc. All the clients communicate with each other through a server.

ASSIGNMENT 05

Classless Inter Domain Routing (CIDR)

Classful addressing the no of Hosts within a network always remains the same depending upon the class of the Network.
Class A network contains 224 Hosts,
Class B network contains 216 Hosts,
Class C network contains 28 Hosts
In order to reduce the wastage of IP addresses a new concept of Classless Inter-Domain Routing is introduced.

Subnetting vs Supernetting

S.NO	Subnetting	Supernetting
1.	Subnetting is the procedure to divide the network into sub-networks.	While supernetting is the procedure of combine the small networks.
2.	In subnetting, Network addresses's bits are increased.	While in supernetting, Host addresses's bits are increased.
3.	In subnetting, The mask bits are moved towards right.	While In supernetting, The mask bits are moved towards left.
4.	Subnetting is implemented via Variable-length subnet masking.	While supernetting is implemented via Classless interdomain routing.
5.	In subnetting, Address depletion is reduced or removed.	While It is used for simplify routing process.

Network Address Translation (NAT)

To access the Internet, one public IP address is needed, but we can use a private IP address in our private network. The idea of NAT is to allow multiple devices to access the Internet through a single public address. To achieve this, the translation of a private IP address to a public IP address is required. Network Address Translation (NAT) is a process in which one or more local

IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts.

Subnetting with examples of IPv4-32bit Ipv6-128bit, Supernetting, classes of IPV4 decimal/binary

ASSIGNMENT 06

Distance Vector routing algorithm(Bellman Ford algo):

The Distance vector algorithm is a dynamic algorithm. Historically known as the old ARPANET routing algorithm. Each router maintains a distance table known as Vector. Distance vector routing algorithm simplifies the routing process by assuming the cost of every link is one unit. Therefore, the efficiency of transmission can be measured by the number of links to reach the destination. In Distance vector routing, the cost is based on hop count.

Hop count - number of routers you have to pass to get to your destination

Information kept by DV router -

- Each router has an ID
- Associated with each link connected to a router, there is a link cost (static or dynamic).
- Intermediate hops

Link State Routing Algorithm:

- It is a dynamic routing algorithm in which each router shares knowledge of its neighbors with every other router in the network.
- A router sends its information about its neighbors only to all the routers through flooding.
- Information sharing takes place only whenever there is a change.
- It makes use of Dijkstra's Algorithm for making routing tables.
- Problems – Heavy traffic due to flooding of packets.
  – Flooding can result in infinite looping which can be solved by using the Time to live (TTL) field.

ASSIGNMENT 07

Packet tracer with tools, for wired/ Wireless N/W setup, examples of RIP/OSPF/BGP

Routing Information Protocol (RIP) is a dynamic routing protocol that uses hop count as a routing metric to find the best path between the source and the destination network. It is a distance-vector routing protocol that has an AD value of 120 and works on the Network layer of the OSI model. RIP uses port number 520.

ASSIGNMENT 08

Types of Sockets:

1. Datagram Sockets: Datagram sockets allow processes to use the User Datagram Protocol (UDP). It is a two-way flow of communication or messages. It can receive messages in a different order from the sending way and also can receive duplicate messages. These sockets are preserved with their boundaries.

2. Stream Sockets: Stream socket allows processes to use the Transfer Control Protocol (TCP) for communication. A stream socket provides a sequenced, constant or reliable, and two-way (bidirectional) flow of data. After the establishment of connection, data can be read and written to these sockets in a byte stream.

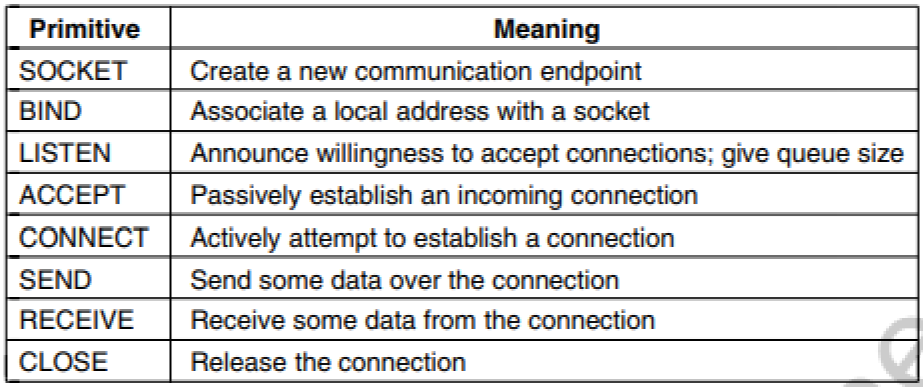
3. Raw Sockets: Raw Socket provide user access to the Internet Control Message Protocol (ICMP). Raw sockets are not used for most applications. These sockets are the same as the datagram oriented, their characteristics are dependent on the interfaces. They provided support in developing new communication protocols or for access to more facilities of an existing protocol. Only the super-users can access the Raw Sockets.

4. Sequenced Packet Sockets: Sequenced Packet Sockets are similar to the stream socket, with the exception that record boundaries are preserved in-stream sockets. The given interface in this section is of Network System (NS) that has an abstraction of Sockets and is ordered in all the applications.

TCP

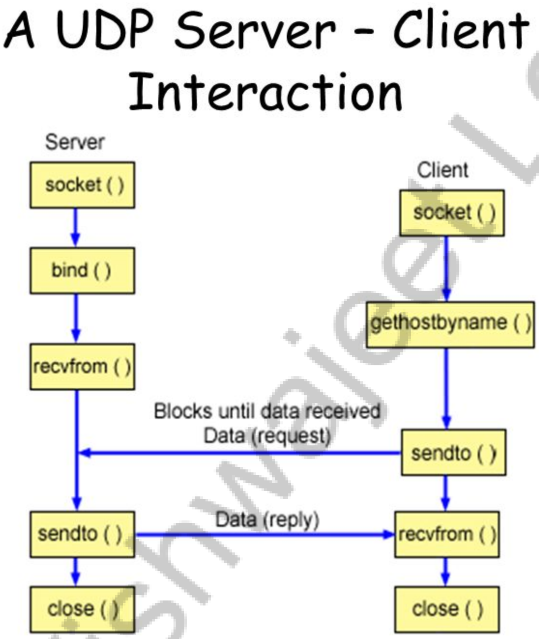
TCP (Transmission Control Protocol) is one of the main protocols of the Internet protocol suite. It lies between the Application and Network Layers which are used in providing reliable delivery services. It is a connection-oriented protocol for communications that helps in the exchange of messages between the different devices over a network.

Socket primitives/functions



Primitive	Meaning
SOCKET	Create a new communication endpoint
BIND	Associate a local address with a socket
LISTEN	Announce willingness to accept connections; give queue size
ACCEPT	Passively establish an incoming connection
CONNECT	Actively attempt to establish a connection
SEND	Send some data over the connection
RECEIVE	Receive some data from the connection
CLOSE	Release the connection

Figure 6-5. The socket primitives for TCP.



Ports: A port is used to differentiate among different applications using the same network interface. It is an additional qualifier used by the system software to get data to the correct application. Physically, a port is a 16-bit integer. Some ports are reserved for particular applications; they are labeled as well-known ports.

UDP protocol, datagram socket, UDP port number

It is an unreliable and connectionless protocol. So, there is no need to establish a connection prior to data transfer. The UDP helps to establish low-latency and loss-tolerating connections establish over the network. The UDP enables process-to-process communication.

For real-time services we need UDP. Since high performance is needed, UDP permits packets to be dropped instead of processing delayed packets. There is no error checking in UDP, so it also saves bandwidth. User Datagram Protocol (UDP) is more efficient in terms of both latency and bandwidth.

In UDP, the client does not form a connection with the server like in TCP and instead just sends a datagram. Similarly, the server need not accept a connection and just waits for datagrams to arrive. Datagrams upon arrival contain the address of the sender which the server uses to send data to the correct client.

UDP port number: fields are each 16 bits long, therefore the range for port numbers is defined from 0 to 65535; port number 0 is reserved. Port numbers help to distinguish different user requests or processes.

Domain names root/ Local, DNS code, DNS servers

DNS (Imp) :

1. DNS is an acronym that stands for Domain Name System. DNS was introduced by Paul Mockapetris and Jon Postel in 1983.

2. It is a naming system for all the resources over the internet which includes physical nodes and applications. It is used to locate resources easily over a network.

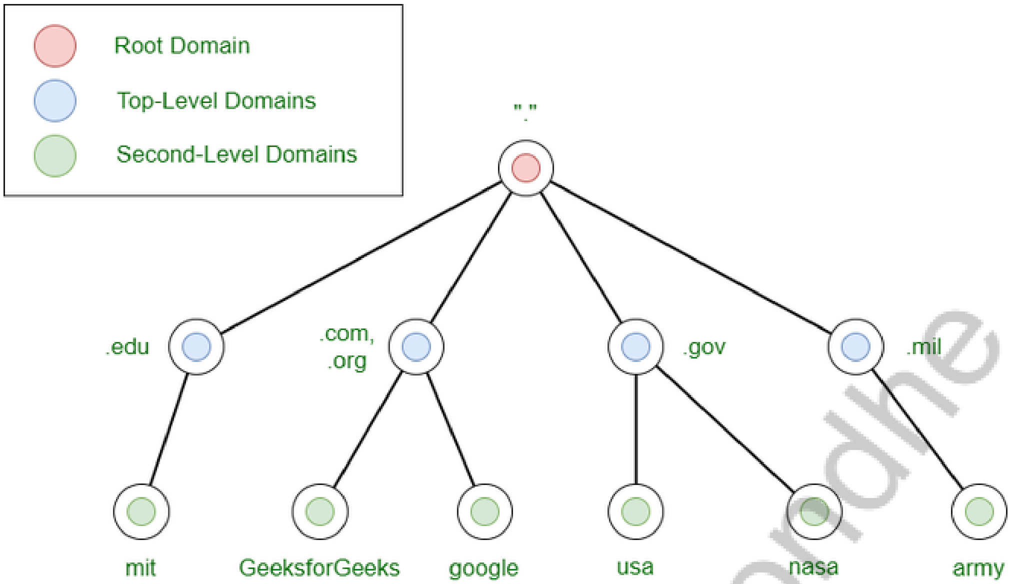
3. DNS is an internet which maps the domain names to their associated IP addresses.

4. Without DNS, users must know the IP address of the web page that you wanted to access.

Working of DNS (Imp): If you want to visit the website of "shaurya", then the user will type "https://www.shaurya.com" into the address bar of the web browser. Once the domain name is entered, then the domain name system will translate the domain name into the IP address which can be easily interpreted by the computer. Using the IP address, the computer can locate the web page requested by the user.

DNS Forwarder : A forwarder is used with a DNS server when it receives DNS queries that cannot be resolved quickly. So it forwards those requests to external DNS servers for resolution. A DNS server which is configured as a forwarder will behave differently than the DNS server which is not configured as a forwarder.

Domain Hierarchy :



TLD (Top-Level Domain) is the rightmost part of a domain name. The TLD for geeksforgeeks.com is ".com". TLDs are divided into two categories: gTLDs (generic top-level domains) and ccTLDs (country code top-level domains). Historically, the purpose of a common top-level domain (gTLD) was to inform users of the purpose of the domain name; For example, a.com would be for business purposes, .org for organization, .edu for education, and .gov for the government. And a country code top-level domain (ccTLD) was used for geographic purposes, such as .ca for Canadian sites, .co.uk for UK sites, and so on. As a result of the high demand, many new gTLDs have emerged, including.online,.club,.website,.biz, and many others.

SLD(Second-Level Domain): The .org component of geeksforgeeks.org is the top-level domain, while geeksforgeeks is the second-level domain. Second-level domains can only contain a-z 0-9 and hyphens and are limited to 63 characters and TLDs when registering a domain name (may not start or end with hyphens or contain consecutive hyphens).

Subdomain: A period is used to separate a subdomain from a second-level domain. For example, the admin part is a subdomain named admin.geeksforgeeks.org. A subdomain name, like a second-level domain, is restricted to 63 characters and can only contain the letters a-z, 0-9, and hyphens (cannot begin or end with hyphens or consecutive hyphens).

DHCP installation, configuration, software installation on remote machine, Applications of

DHCP: DHCP is the Dynamic Host Configuration Protocol. It is an application layer protocol used to auto- Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to dynamically assign an IP address to any device, or node, on a network so they can communicate using IP (Internet Protocol). DHCP automates and centrally manages these configurations. There is no need to manually assign IP addresses to new devices. Therefore, there is no requirement for any user configuration to connect to a DHCP based network. DHCP can be implemented on local networks as well as large enterprise networks. DHCP is the default protocol used by the most routers and networking equipment.

It uses port 67 by default.

Benefits of DHCP:

There are following benefits of DHCP:

- Centralized administration of IP configuration: DHCP IP configuration information can be stored in a single location and enables that administrator to centrally manage all IP address configuration information.

- Dynamic host configuration: DHCP automates the host configuration process and eliminates the need to manually configure individual host. When TCP/IP (Transmission control protocol/Internet protocol) is first deployed or when IP infrastructure changes are required.

- Seamless IP host configuration: The use of DHCP ensures that DHCP clients get accurate and timely IP configuration IP configuration parameter such as IP address, subnet mask, default gateway, IP address of DND server and so on without user intervention.

- Flexibility and scalability: Using DHCP gives the administrator increased flexibility, allowing the administrator to move easily change IP configuration when the infrastructure changes.

HTTP and HTTPS diff, request and reply msg, HTTP port number

HTTP :

HTTP is the HyperText Transfer Protocol which defines the set of rules and standards on how the information can be transmitted on the World Wide Web (WWW). It helps the web browsers and web servers for communication. It is a ‘stateless protocol’ where each command is independent with respect to the previous command. HTTP is an application layer protocol built upon the TCP. It uses port 80 by default.

HTTPS:

HTTPS is the HyperText Transfer Protocol Secure or Secure HTTP. It is an advanced and secured version of HTTP. On top of HTTP, SSL/TLS protocol is used to provide security. It enables secure transactions by encrypting the communication and also helps identify network servers securely. It uses port 443 by default.

SSL and TLS, SSL certificate

SSL (Secure Socket Layer) and TLS (Transport Layer Security) are popular cryptographic protocols that are used to imbue web communications with integrity, security, and resilience against unauthorized tampering. PKI uses the TLS protocol to establish secure connections between clients and servers over the internet, ensuring that the information relayed is encrypted and unable to be read by an external third party.

Note: SSL was the predecessor of TLS, and the world began moving away from SSL once TLS was introduced in 1999, thanks to the improved security features of the latter. TLS is currently in its third iteration, and is called TLS 1.3. However, SSL continues to be used as a metonym for both protocols in general (for example, the word 'SSL certificate' is widely used, but SSL has been completely deprecated and no modern systems support SSL anymore).

Connections that are secured by TLS will indicate their secure status by displaying HTTPS (Hypertext Transfer Protocol Secure) in the address bar of web browsers, as opposed to just HTTP. While TLS is primarily used to secure client-server connection, it is also used to protect emails, VoIP calls, and other connections.

SSL Certificate : Digital certificates are digital documents that are 'signed' by trusted authorities, and act as documents of ownership of a public key. By extension, they serve to validate the legitimacy of a server or a client. Certificates are key to making websites easily recognizable to users as a trusted, secure page. Webpages with valid SSL/TLS certificates installed on them will have 'https' preceding the name of the website in the search bar

IPsec

The IP security (IPSec) is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted and authenticated packets. The protocols needed for secure key exchange and key management are defined in it.

What are the cyber or network attacks

A network attack is an attempt to gain unauthorized access to an organization's network, with the objective of stealing data or perform other malicious activity.

1. Unauthorized access
2. Distributed Denial of Service (DDoS) attacks
3. Man in the middle attacks
4. Insider threats

How antivirus will work

Antivirus applications come with a directory of already checked-viruses and match the codes and patterns in files and web pages to unique bits and patterns that make up the code of a virus. If they match, the file is quarantined, means that it is moved to a new and safe location so that it does not infect any other files on the system.

How firewall will work

A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.Firewall match the network traffic against the rule set defined in its table. Once the rule is matched, associate action is applied to the network traffic.

Protocols used in what's app/Instagram/Facebook/Twitter

->XMPP(extesible message and presence protocol)

Difference between 4g & 5g

Bluetooth/Infrared/ZigBee

Cell phone network/Processors

Cellular Network is formed of some cells, cell covers a geographical region, has a base station analogous to 802.11 AP which helps mobile users attach to network and there is an air-interface of physical and link layer protocol between mobile and base station. All these base stations are connected to Mobile Switching Center which connects cells to wide area net, manages call setup and handles mobility.

Service providers

Internet Service Provider which is a term used to refer to a company that provides internet access to people who pay the company or subscribe to the company for the same.

ARPANET/ IANA/ ISP

ARPANET was first network which consisted of distributed control. It was first to implement TCP/IP protocols. It was basically beginning of Internet with use of these technologies.

The Internet Assigned Numbers Authority (IANA) assigns an IPV4 (Version 4) address as a unique identifier to each device on the Internet.

Manchester/ subnetting in binary calculations/ IP classes -2,3

MAC address 48 bit

MAC address is a unique identifier that is assigned to a NIC (Network Interface Controller/ Card). It consists of a 48 bit or 64-bit address, which is associated with the network adapter. MAC addresses can be in hexadecimal format. The full form of MAC address is Media Access Control address.

MAC address is a unique number which is used to track a device in a network. MAC address provides a secure way to find senders or receivers in the network and helps prevent unwanted network access.

ISO-OSI model with layers and devices

OSI (Open System Interconnections) (Imp) : It is a network architecture model based on the ISO standards. It is called the OSI model as it deals with connecting the systems that are open for communication with other systems. The OSI model has seven layers. The principles used to arrive at the seven layers can be summarized briefly as below:

1. Create a new layer if a different abstraction is needed.

2. Each layer should have a well-defined function.

3. The function of each layer is chosen based on internationally standardized protocols.

Seven Layers :

1. Physical Layer

- It is the lowest layer of the OSI reference model.
- It is used for the transmission of an unstructured raw bit stream over a physical medium.
- Physical layer transmits the data either in the form of electrical/optical or mechanical form.
- The physical layer is mainly used for the physical connection between the devices, and such physical connection can be made by using twisted-pair cable, fibre-optic or wireless transmission media.

2. Data Link Layer

- It is used for transferring the data from one node to another node.

- It receives the data from the network layer and converts the data into data frames and then attaches the physical address to these frames which are sent to the physical layer.

- It enables the error-free transfer of data from one node to another node.

Functions of Data-link layer:

- Frame synchronization: Data-link layer converts the data into frames, and it ensures that the destination must recognize the starting and ending of each frame.

- Flow control: Data-link layer controls the data flow within the network.

- Error control: It detects and corrects the error occurred during the transmission from source to destination.

- Addressing: Data-link layers attach the physical address with the data frames so that the individual machines can be easily identified.

- Link management: Data-link layer manages the initiation, maintenance and termination of the link between the source and destination for the effective exchange of data.

3. Network Layer

- Network layer converts the logical address into the physical address.

- The routing concept means it determines the best route for the packet to travel from source to the destination.

Functions of network layer :

- Routing: The network layer determines the best route from source to destination. This function is known as routing.

- Logical addressing: The network layer defines the addressing scheme to identify each device uniquely.

- Packetizing: The network layer receives the data from the upper layer and converts the data into packets. This process is known as packetizing.

- Internetworking: The network layer provides the logical connection between the different types of networks for forming a bigger network.

- Fragmentation: It is a process of dividing the packets into fragments..

4. Transport Layer

- It delivers the message through the network and provides error checking so that no error occurs during the transfer of data.

It provides two kinds of services:

- Connection-oriented transmission: In this transmission, the receiver sends the acknowledgement to the sender after the packet has been received.
- Connectionless transmission: In this transmission, the receiver does not send the acknowledgement to the sender.

5. Session Layer

- The main responsibility of the session layer is beginning, maintaining and ending the communication between the devices.

- Session layer also reports the error coming from the upper layers.

- Session layer establishes and maintains the session between the two users.

6. Presentation Layer

- The presentation layer is also known as a Translation layer as it translates the data from one format to another format.

- At the sender side, this layer translates the data format used by the application layer to the common format and at the receiver side, this layer translates the common format into a format used by the application layer.

Functions of presentation layer:

- Character code translation
- Data conversion
- Data compression
- Data encryption

7. Application Layer

- Application layer enables the user to access the network.

- It is the topmost layer of the OSI reference model.

- Application layer protocols are file transfer protocol, simple mail transfer protocol, domain name system, etc.

- The most widely used application protocol is HTTP (Hypertext transfer protocol). A user sends the request for the web page using HTTP

TCP/IP model

TCP/IP Reference Model : It is a compressed version of the OSI model with only 4 layers. It was developed by the US Department of Defence (DoD) in the 1860s. The name of this model is based on 2 standard protocols used i.e. TCP (Transmission Control Protocol) and IP (Internet Protocol).

1. Link : Decides which links such as serial lines or classic Ethernet must be used to meet the needs of the connectionless internet layer. Ex - Sonet, Ethernet

2. Internet : The internet layer is the most important layer which holds the whole architecture together. It delivers the IP packets where they are supposed to be delivered. Ex - IP, ICMP.

3. Transport : Its functionality is almost the same as the OSI transport layer. It enables peer entities on the network to carry on a conversation. Ex - TCP, UDP (User Datagram Protocol)

4. Application : It contains all the higher-level protocols. Ex - HTTP, SMTP, RTP, DNS.

Design Issues

Design issues with data link layer are :

1. Services provided to the network layer –
   The data link layer act as a service interface to the network layer. The principle service is transferring data from network layer on sending machine to the network layer on destination machine. This transfer also takes place via DLL (Data link-layer).
2. Frame synchronization –
   The source machine sends data in the form of blocks called frames to the destination machine. The starting and ending of each frame should be identified so that the frame can be recognized by the destination machine.
3. Flow control –
   Flow control is done to prevent the flow of data frame at the receiver end. The source machine must not send data frames at a rate faster than the capacity of destination machine to accept them.
4. Error control –
   Error control is done to prevent duplication of frames. The errors introduced during transmission from source to destination machines must be detected and corrected at the destination machine.

Network layer design issues:

1. Store and Forward packet switching:

The host sends the packet to the nearest router. This packet is stored there until it has fully arrived once the link is fully processed by verifying the checksum then it is forwarded to the next router till it reaches the destination. This mechanism is called "Store and Forward packet switching."

2. Services provided to Transport Layer:

Through the network/transport layer interface, the network layer transfers it's services to the transport layer. These services are described below.

But before providing these services to the transfer layer following goals must be kept in mind :-

- Offering services must not depend on router technology.
- The transport layer needs to be protected from the type, number and topology of the available router.
- The network addresses for the transport layer should use uniform numbering pattern also at LAN and WAN connections.

3. Implementation of Connectionless Service:

Packet are termed as "datagrams" and corresponding subnet as "datagram subnets". When the message size that has to be transmitted is 4 times the size of the packet, then the network layer divides into 4 packets and transmits each packet to router via. a few protocol. Each data packet has destination address and is routed independently irrespective of the packets.

4. Implementation of Connection Oriented service:

To use a connection-oriented service, first we establishes a connection, use it and then release it. In connection-oriented services, the data packets are delivered to the receiver in the same order in which they have been sent by the sender.

Design Issues in Physical Layer :

- The physical layer is basically concerned with transmitting raw bits over a communication channel.
- Mainly the design issues here deal with electrical, mechanical, timing interfaces, and the physical transmission medium, which lies below the physical layer.
- Design issue has to do with making sure that when 1 bit send from one side, it is received 1 bit by other side also not as a 0 bit.

Port opening command

netstat –lntu : (List Open Ports)

This will print all *listening* sockets (-l) along with the port *number* (-n), with TCP ports (-t) and UDP ports (-u)

ss –lntu : (List Listening Sockets)

netstat -na | grep :4000 (opens 4000 port assuming it's not open already)

Ports of DNS/FTP/HTTP

DNS = 53

FTP = port 21 for the command port and port 20 for the data port.

HTTP = 80

Network security architecture

1. Physical Network Security:
   This is the most basic level that includes protecting the data and network through unauthorized personnel from acquiring control over the confidentiality of the network. These include external peripherals and routers that might be used for cable connections. The same can be achieved by using devices like biometric systems.

2. Technical Network Security:
   It primarily focuses on protecting the data stored in the network or data involved in transitions through the network. This type serves two purposes. One is protected from unauthorized users, and the other is protection from malicious activities.

3. Administrative Network Security:
   This level of network security protects user behavior like how the permission has been granted and how the authorization process takes place. This also ensures the level of sophistication the network might need for protecting it through all the attacks. This level also suggests necessary amendments that have to be done to the infrastructure.

Authentication /Authorization -6

Authentication (AuthN) is a process that verifies that someone or something is who they say they are. Authorization is the security process that determines a user or service's level of access.

Wired/Wireless technologies

(a) Wired Network: Wired refers to any physical medium made up of cables. Copper wire, twisted pair, or fiber optic cables are all options. A wired network employs wires to link devices to the Internet or another network, such as laptops or desktop PCs.

(b) Wireless Network: “Wireless” means without wire, media that is made up of electromagnetic waves (EM Waves) or infrared waves. Antennas or sensors will be present on all wireless devices. Cellular phones, wireless sensors, TV remotes, satellite disc receivers, and laptops with WLAN cards are all examples of wireless devices. For data or voice communication, a wireless network uses radiofrequency waves rather than wires.

Virtual machine

A Virtual Machine (VM) is a compute resource that uses software instead of a physical computer to run programs and deploy apps. Each virtual machine runs its own operating system and functions separately from the other VMs, even when they are all running on the same host.

Advantages:
There are no protection problems because each virtual machine is completely isolated from all other virtual machines.

1. Virtual machine can provide an instruction set architecture that differs from real computers.
2. Easy maintenance, availability and convenient recovery.

Disadvantages:

1. When multiple virtual machines are simultaneously running on a host computer, one virtual machine can be affected by other running virtual machines, depending on the workload.
2. Virtual machines are not as efficient as a real one when accessing the hardware.

What is system/application software

System software is a type of computer program that is designed to run a computer's hardware and application programs. If we think of the computer system as a layered model, the system software is the interface between the hardware and user applications. The operating system is the best-known example of system software. The OS manages all the other programs in a computer.

What is device driver software

A device driver is a special kind of software program that controls a specific hardware device attached to a computer. Device drivers are essential for a computer to work properly. These programs may be compact, but they provide the all-important means for a computer to interact with hardware, for everything from mouse, keyboard and display (user input/output) to working with networks, storage and graphics.

Explain TELNET, DHCP, and SNMP protocol

TELNET : Stands for Teletype Network. It is a type of protocol that enables one computer to connect to local computer. It is a used as a standard TCP/IP protocol for virtual terminal service which is given by ISO. During telnet operation whatever that is being performed on the remote computer will be displayed by local computer. Telnet operates on client/server principle. Local computer uses telnet client program and the remote computers uses telnet server program.

Explain IDS

An Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for the harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system.

Explain public and private key

Private Key: In the Private key, the same key (secret key) is used for encryption and decryption. In this key is symmetric because the only key is copied or shared by another party to decrypt the cipher text. It is faster than public-key cryptography.

Public Key: In a Public key, two keys are used one key is used for encryption and another key is used for decryption. One key (public key) is used to encrypt the plain text to convert it into cipher text and another key (private key) is used by the receiver to decrypt the cipher text to read the message.

Explain Socket programming.

Socket programming is a way of connecting two nodes on a network to communicate with each other. One socket(node) listens on a particular port at an IP, while the other socket reaches out to the other to form a connection. The server forms the listener socket while the client reaches out to the server.