BLACK N WHITE
Learn Today Lead Tomorrow

BCA 4TH SEMSESTER

COMPUTER NETWORKING/ DCA2201

SET.:- 1

1.)Define Network edge. Explain OSI reference model.

Answer.:- The network edge refers to area where a device or local network interfaces with the internet . The edge is close to the devices it is communicating with and is the entry point to point network . the network edge is a crucial security boundary that network administrators .

OSI is stand for Open System Interconnection . The reference model is a covered by seven layers of architecture and also developed by a hugely structured method . There are seven layer in OSI model :-

i.) Physical Layer :- It is used to transmitting vital bits from one nodes to another nodes

ii.) Data Link Layer :- It is used to manage the access to and uses of the transmitted data .

iii.) Network Layer :- It is mainly responsible for delivering routing services from source point to destination across the Internet .

iv.) Transport Layer :- It is the orderly and reliable delivery of data between the end systems after accepting the data of session layer.

v.) Session Layer :- It is also answerable for the orderly recovery from failures by implementing check pointing mechanisms .

vi.) Presentation Layer :- This is responsible for rectifying those differences by resorting the syntax .

vii.) Application Layer :- This is used to provides services for user and software task .

2.)(A) Differentiate between Byte-oriented protocols and Bit-oriented protocols. Explain different error detecting codes.

Answer.:- There are two different types of data transmission protocols used in computer networking: byte-oriented protocols and bit-oriented protocols. Byte-oriented protocols: A form of data transmission protocol used in computer networking is called a "byte-oriented protocol." These protocols use bytes, which are typically made up of 8 bits, to convey data. Data that is structured into larger units, such as characters or text strings, can be handled via byte-oriented protocols. Example: The Transmission Control Protocol (TCP), a popular protocol for dependable data transmission over the Internet, is one illustration of a byte-oriented system. To ensure that data is transferred precisely and dependably, TCP divides data into segments that are transmitted in units of bytes and offers features like flow control and mistake recovery. Bit-oriented protocols: Data transmission protocols used in computer networking fall under the category of bit-oriented protocols. Instead than sending data in bigger units like bytes, these protocols send data in units of individual bits. Bit-oriented protocols are frequently employed in communication systems that need exact synchronization and timing since they are made to handle data that is grouped into smaller pieces, such binary

integers. Example: The High-Level Data Link Control (HDLC) protocol, which is frequently used in communication systems, including telephone networks, for data transmission, is an illustration of a bit-oriented protocol. A bit-oriented protocol called HDLC has the ability to both detect and rectify errors. To guarantee the precision and dependability of data transmission in computer networks, various error detection codes are employed. These codes are used to find and fix faults that could happen when data is being transmitted. These are some examples of frequently used error detection codes:

- ⇨ Parity Check: Parity check is a straightforward error-detection routine that increases each byte or data unit by one bit. Depending on how many 1s there are in the byte or data unit, the additional bit is either set to 0 or 1. The extra bit is set to 0 if the number of ones is even, and to 1 if the number of ones is odd.
- ⇨ CRC (Cyclic Redundancy Check): CRC is a more complex error-detecting code that creates a checksum for the data using a polynomial division algorithm. To make sure that the data was not corrupted during transmission, the checksum is then sent together with the data and validated at the receiving end.
- ⇨ Hamming Code: The error-correcting code known as Hamming uses several parity bits to find and fix faults. In order to check for errors and rectify them if they do exist, the code adds extra bits to the data. In computer networks, error detecting codes are crucial for guaranteeing the accuracy and dependability of data transmission. Several codes may be employed depending on the unique requirements and properties of the data being transferred.

3.)(A)Write a short note on shortest path algorithm and flooding. Differentiate between multicasts and broadcast routing.

Answer:- Shortest path algorithm: Finding the shortest path between two nodes in a graph is done using the shortest path algorithm, which is a fundamental procedure in graph theory. In computer networks, routing protocols, and GPS navigation systems, this technique is frequently employed. Dijkstra's approach, which begins at the source node and iteratively explores surrounding nodes until it reaches the destination node, is the most well-known shortest path algorithm. It records the shortest path from the source node to each node along the way.

- **Flooding:** In computer networks, flooding is a straightforward but ineffective routing strategy. In flooding, a packet is transmitted from the source node to every node in its immediate vicinity, which then sends the packet to every node in its immediate vicinity, and so on, until it reaches the destination node. Flooding is useful in circumstances when the network topology is ambiguous or dynamic, but it can clog the network and waste resources. There are two alternative ways to send data packets over a network—multicast and broadcast routing.
- **Multicasts Routing:** On the other hand, multicast routing includes transmitting a packet from a single source node to a particular collection of nodes. Only the group's nodes will really get the packet. When numerous nodes need to receive the same data but not every node in the network does, multicast routing might be helpful. Instead of transmitting a different stream to each individual node, in video streaming, a single video stream can be multicast to all of the nodes that are watching it. As multicast routing uses less network traffic and bandwidth than broadcast routing, it is more effective.
- **Broadcast Routing:** Sending a packet from a single source node to every node in the network is known as broadcast

routing. To put it another way, every node in the network receives the packet. Typical applications of broadcast routing include network discovery and routing table updates. Even if they are not the intended recipients of the data, every node that gets the broadcast packet must process it. This can clog up the network and waste resources. In conclusion, the primary distinction between multicast and broadcast routing is that multicast transmits data packets to a certain set of nodes while broadcast sends packets to every node in the network. By transmitting data solely to nodes that are a part of the particular group, multicast is more bandwidth-efficient than broadcast at lowering network traffic.

SET.:- 2

4.)(A) Describe process to process delivery. Explain TCP connection establishment and connection release.

Answer.:- Data transfer from one application process to another running on different hosts inside a network is known as process-to-process delivery. The transport layer of the OSI model's process-to-process delivery is in charge of guaranteeing dependable and effective communication between the processes.

➔ The following steps are commonly involved in the process-to-process delivery process:

- The source host's application process starts a data transfer and sends the information to a transport layer protocol like TCP or UDP. 2.
- The data is given a header by the transport layer protocol that contains details like the source and destination ports, sequence numbers, and acknowledgement numbers.
- The data is subsequently sent from the transport layer protocol to the network layer, which adds a network header with the IP addresses of the source and destination, and delivers the information to the data link layer.
- The data is sent across the physical network by the data link layer after it adds a data link header, such as an Ethernet or Wi-Fi header.

In computer networks, **TCP (Transmission Control Protocol)** is a dependable and connection oriented transport layer protocol. By establishing a connection between two hosts before to a data transfer and releasing the connection after the transfer is over, TCP offers a dependable data transmission service.

➔ This is a description of the TCP connection establishment and release process:

⇨ TCP Connection Establishment:

- The procedure starts when the client sends the server a SYN (Synchronize) packet to indicate that it wants to connect. A client-generated random sequence number can be found in the SYN packet.
- The SYN-ACK (Synchronize-Acknowledge) packet is the server's response to receiving the SYN packet. The SYN-ACK packet includes a server-generated random sequence number and an acknowledgement number that is equal to the client's sequence number plus one.
- The client sends an ACK (Acknowledge) packet to the server after receiving the SYNACK message. The acknowledgement number in the ACK packet is equal to the sequence number of the server plus one.

⇨ **TCP Connection Release:**

- Sending a FIN (Finish) packet to the other host to indicate that it has no more data to deliver is the first step in closing a TCP connection.
- The opposite host replies by sending an ACK packet to confirm receipt of the FIN packet.
- The second host sends a FIN packet to the first host after it has done delivering data as well.
- The first host replies by sending an ACK packet to confirm receipt of the FIN packet.
- Both hosts are now free to start new connections as the connection has been ended.

In conclusion, a handshake mechanism between the two hosts is involved in the setup and release of TCP connections. A SYN-ACK handshake between the client and server and a FIN-ACK handshake between the hosts make up the setup and release processes, respectively. These handshakes are used to assist guarantee dependable and effective data flow between the hosts.

5.)(A) Describe SMTP. Explain HTTP request and response messages.

Answer.:- Email messages are transferred between servers using the SMTP (Simple Mail Transmission Protocol) protocol. SMTP is in charge of sending email messages between clients and servers or between servers and operates on the application layer of the OSI model. The following stages are commonly involved with SMTP:

- The email client of the sender connects to the SMTP server on port 25 or port 587.
- The email message is subsequently transferred to the server by the client via a series of commands. The commands allow you to provide the email content, as well as the sender and recipient addresses.
- The email message is subsequently forwarded by the SMTP server to the correct recipient server.
- The email message is subsequently sent to the recipient's email client by the recipient server.

On the World Wide Web, the HTTP (Hypertext Transfer Protocol) protocol is used to transport data from a client to a server. The OSI model's application layer, where HTTP functions, is in charge of managing web requests and responses.

The client sends HTTP requests to the web server in order to request resources from it. The following elements are typically present in HTTP requests:

- Request line: The first line of a request message that specifies the resource being sought, the HTTP method, and the version of the protocol. GET /index.html HTTP/1.1, for instance.
- Headers: Extra metadata included in the request message that includes details about the client, such as the user agent and the anticipated format of the response Headers include Accept, Content-Type, and User-Agent, for instance.
- Body: Optional information included in the request message, such as file uploads or form submissions. POST or PUT requests are the only ones that use this component.

The server responds to a client's request by sending an HTTP response. The following elements are typically present in HTTP responses:

- Status line: The HTTP version, status code, and status message are all contained on the status line, which is the first line of the response message. For illustration, "HTTP/1.1 200 OK."
- Headers: Extra metadata sent in the response message that tells us more about the server, including the content's length and type. Content-Type, Content-Length, and Last Modified are a few header examples.
- Body: The information that is sent as part of the response, such as a JSON object or an HTML page. HEAD request responses do not contain this element. Body: Optional information included in the request message, such as file uploads or form submissions. POST or PUT requests are the only ones that use this component.

Several HTTP methods are available for HTTP requests and responses, including:

- **GET:** A request method for data from a particular resource.
- **POST:** Used to submit an entity to the designated resource, frequently leading to a server state change or unintended consequences.
- **PUT:** A method for updating a resource-specific entity.
- **DELETE:** This command is used to remove a given entity from a resource.
- **HEAD:** This command is used to get the response headers for a given resource.

6.)(A) Describe Virtual Private Networks. Write short notes on web security.

Answer.:- In order to establish a private and secure connection across a public network, like the internet, use a virtual private network (VPN). To access resources on a private network as if they were directly connected, a VPN often entails building a virtual tunnel between a user's device and a remote server.

VPNs have a number of advantages, including:

- Security: VPNs utilize encryption to safeguard data sent over public networks, assisting in the prevention of data theft and eavesdropping.
- Privacy: By hiding a user's IP address and encrypting their internet traffic, VPNs can help to safeguard a user's identity and location.
- Access: VPNs enable users to gain remote access to private network resources, such as business networks.

Web Security: Protecting websites, web applications, and web services from cyberattacks, data breaches, and illegal access is the practice of web security. Web security is now a

vital component of information security due to the rise in internet users and reliance on online services.

Common web security risks include the following:

- In a cross-site scripting (XSS) attack, malicious code is injected into a web page that is being viewed by other users. This may lead to the theft of private data or the hijacking of user accounts.
- SQL Injection: This kind of attack entails injecting SQL code into the input fields of a web application. As a result, the attacker may be able to access sensitive information or change the database.
- Cross-Site Request Forgery (CSRF) is an attack type where a user is tricked into using a web application without their knowledge or consent. This may result in unauthorized user data alteration or other security lapses.
- A sort of assault known as a distributed denial of service (DDoS) occurs when an attacker overwhelms an online application with traffic, rendering it inaccessible to users. The targeted organization may suffer substantial downtime and financial loss as a result of this.

Organizations should put into practice a variety of security measures, such as:

- To prevent unwanted access, data must be transformed into an unreadable format through the process of encryption. Websites should implement encryption techniques like HTTPS to guarantee secure data transmission.
- Access control is the process of limiting unauthorized users' access to sensitive data or functionality. Strong authentication and authorization procedures should be implemented by organizations to guarantee that only authorized users have access to their data.
- Frequent testing and auditing is the process of checking for vulnerabilities in web applications on a regular basis. To find

and address vulnerabilities, organizations should do frequent security audits and penetration tests.

- Users' Education: This refers to the process of informing users about dangers to and best practices for web security. Businesses should offer training and awareness campaigns to inform their staff and clients about web security risks and how to protect themselves.

In conclusion, web security is an essential component of information security that entails safeguarding websites, web applications, and web services against a variety of dangers. To ensure that their online applications are safe from cyberattacks and secure, organizations should use a variety of security measures and best practices.