**17IT3503 – Computer Networks**

**Unit-2 Important Questions**

**One Mark Questions**

Define Application architecture

Mention the different types of Application architecture

Define a Cookie

Outline the general formats of HTTP request and response message for a web page

Define Data connection

What are FTP commands .Explain

What is SMTP?

How Does SMTP Work?

Define DNS caching

What are the services provided by the DNS in addition to translating host names to IP addresses?

What is Checksum?

UDP Segment Structure?

What is MTU?

TCP Segment Structure?

Define Congestion

What is end-to-end congestion control?

Define Congestion window

What is fairness?

**Essay Questions**

Describe the Application layer protocols

Define Proxy Server. Explain the benefit of Proxy server with the help of an example

Give the Overview of HTTP

Explain the scenario how FTP moves files between local and remote file systems

Explain the scenario how FTP moves files between local and remote file systems

Explain the diff b/w control connection and a data connection

Explain the basic operation of SMTP by taking an example scenario

Explain the working of a Distributed, Hierarchical database

Describe the services provided by DNS

Many applications are better suited for UDP for the following reasons. Explain

Evaluate the UDP Checksum for the data word “Network”

Explain a case study for sequence and Acknowledgement numbers

Evaluate the TCP checksum for any 16 bit integer data

Explain the cause and cost of congestion with 2 senders, a router with infinite buffers scenario

Explain the Approaches toward Congestion Control

Explain Congestion control algorithm with a neat diagram

Does TCP Ensure Fairness, if so How?

**Placement Questions from Unit-2**

**Topic 1: Principles of Network Applications**

1. What is a client/ server network?

A client/ server network is a network where one computer behaves as a server to the other computers. The server is usually more powerful than the clients and serves the clients.

2. How are networks classified based on their connections?

Answer: Networks are classified into two categories based on their connection types. They are mentioned below:

Peer-to-peer networks (P2P): When two or more computers are connected together to share resources without the use of a central server is termed as a peer-to-peer network. Computers in this type of network act as both server and client. It is generally used in small companies as they are not expensive.

Server-based networks: In this type of network, a central server is located to store the data, applications, etc of the clients. The server computer provides the security and network administration to the network.

3. Describe the key elements of the protocol?

Answer: Below are the 3 key elements of the protocol:

Syntax: It is the format of the data. That means in which order the data is displayed.

Semantics: Describes the meaning of the bits in each section.

Timing: At what time the data is to be sent and how fast it is to be sent.

**Topic 2: The Web and HTTP**

1. What is HTTP and what port does it use?

Answer: HTTP is HyperText Transfer Protocol and it is responsible for web content. Many web pages are using HTTP to transmit the web content and allow the display and navigation of HyperText. It is the primary protocol and port used here is TCP port 80.

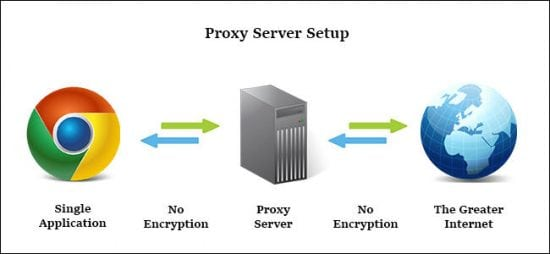
2. What is HTTPs and what port does it use?

Answer: HTTPs is a Secure HTTP. HTTPs is used for secure communication over a computer network. HTTPs provides authentication of websites that prevents unwanted attacks.

In bi-directional communication, the HTTPs protocol encrypts the communication so that the tampering of the data gets avoided. With the help of an SSL certificate, it verifies if the requested server connection is a valid connection or not. HTTPs use TCP with port 443.

3. What is a Proxy Server and how do they protect the computer network?

Answer: For data transmission, IP addresses are required and even DNS uses IP addresses to route to the correct website. It means without the knowledge of correct and actual IP addresses it is not possible to identify the physical location of the network. Proxy servers prevent external users who are unauthorized to access such IP addresses of the internal network. It makes the computer network virtually invisible to external users.



4. Define Round Trip Time?

Answer: The time taken for a signal to reach the destination and travel back to the sender with the acknowledgment is termed as Round Trip Time (RTT). It is also called Round Trip Delay (RTD).

5. Define Pipelining?

Answer: In Networking, when a task is in progress another task gets started before the previous task is finished. This is termed as Pipelining.

**Topic 3:File Transfer Protocol(FTP)**

1. What is File Transfer Protocol (FTP)?

FTP (File Transfer Protocol) is a standard network protocol used to copy a file from one host to another over a TCP/IP-based network, such as the Internet. FTP is built on a client-server architecture and utilizes separate control and data connections between the client and server applications, which solves the problem of different end host configurations (i.e., Operating System, file names). File Transfer Protocol is used with user-based password authentication or with anonymous user access.

2. Explain security concerns of FTP?

The original FTP specification has many security concerns. In May 1999, the following flaws were addressed:

? Bounce Attacks

? Spoof Attacks

? Brute Force Attacks

? Sniffing

? Username Protection

? Port Stealing

3. Explain Anonymous FTP?

A host that provides an FTP service may additionally provide anonymous FTP access. Users typically log into the service with an anonymous account when prompted for user name. Although users are commonly asked to send their email address in lieu of a password, no verification is actually performed on the supplied data, examples of anonymous FTP servers can be found here.

4. Explain Remote FTP or FTP mail?

Where FTP access is restricted, a remote FTP or FTP mail service can be used to circumvent the problem. An email containing the FTP commands to be performed is sent to a remote FTP server, which is a mail server that parses the incoming email, executes the FTP commands, and sends back an email with any downloaded files as an attachment. Obviously this is less flexible than an FTP client, as it is not possible to view directories interactively or to modify commands, and there can also be problems with large file attachments in the response not getting through mail servers. As most internet users these days have ready access to FTP, this procedure is no longer in everyday use.

**Topic 4: Electronic Mail in the Internet (SMTP)**

1. What Is SMTP?

Answer: Logging into your email account to retrieve email seems fairly simple. However, there is technology working behind the scenes, such as simple mail transfer protocol (SMTP) and internet networks to ensure you can send and receive email. Think about SMTP as a mail carrier, sorting and delivering messages to mail servers. These messages are then delivered directly to your email inbox.

2. Explain How SMTP Evolved?

Answer: Electronic messaging was created decades before the internet revolution. In the 1960s people were exploring how to communicate using mainframe computers. The U.S. Government was the first to create a server to transmit email. In the 1970s, the mailbox protocol was developed, which was an early version of SMTP. The modern version of this technology was developed in 1982.

3. Explain How Does SMTP Work?

Answer: SMPT is responsible for transmitting email across Internet networks (IPs). This technology is used specifically for sending outgoing email. Clients typically use applications such as Internet Message Access Protocol (IMAP) or Post Office Protocol (POP) to access to their email box. For example, if you send an email it goes to a mail server using SMTP. The mail client will then deliver it to the user's mailbox.

4. Explain The SMTP Basic Functions?

Answer: SMTP is responsible for a little more than just deliver messages to servers. It performs several functions that streamline the delivery process.

•It evaluates the configuration and grants permission to the computer who is trying to send a message.

•It can also track if the message was sent successfully. If it isn't, an error message is sent to the sender.

•Extended SMTP is a little more advanced than older versions. It helps cut back on email spam.

**Topic 5: DNS-The Internet Directory Service**

1. What Is DNS?

Answer: Domain Name System is a service that can be installed on any windows server operating system to resolve the Name to IP Address and vice-versa. TCP/IP networks, such as the Internet, use DNS to locate computers and services through user-friendly names.

(Address) Maps a host name to an IP address. When a computer has multiple adapter cards and IP addresses, it should have multiple address records.

CNAME (Canonical Name) sets an alias for a host name. For example, using this record, zeta.tvpress.com can have an alias as www.tvpress.com.

MX (Mail Exchange) specifies a mail exchange server for the domain, which allows mail to be delivered to the correct mail servers in the domain.

NS (Name Server) specifies a name server for the domain, which allows DNS lookups within various zones. Each primary and secondary name server should be declared through this record.

PTR (Pointer) creates a pointer that maps an IP address to a host name for reverse lookups.

SOA (Start of Authority) declares the host that is the most authoritative for the zone and, as such, is the best source of DNS information for the zone. Each zone file must have an SOA record (which is created automatically when you add a zone).

2. What is the port no of dns?

53

3. What is a Forward Lookup?

Resolving Host Names to IP Addresses.

4. What is Reverse Lookup?

It’s a file contains host names to IP mapping information.>What is a Resource Record?

It is a record provides the information about the resources available in the N/W infrastructure.

5. What are the diff. DNS Roles?

Standard Primary, Standard Secondary, & AD Integrated.

6. What is a Zone?

Zone is a sub tree of DNS database.

7. What is primary, Secondary, stub & AD Integrated Zone?

Primary Zone: - zone which is saved as normal text file with filename (.dns) in DBS folder. Maintains a read, write copy of zone database.

Secondary Zone: - maintains a read only copy of zone database on another DNS server. Provides fault tolerance and load balancing by acting as backup server to primary server.

Stub zone: - contains a copy of name server and SOA records used for reducing the DNS search orders. Provides fault tolerance and load balancing

**Topic 6: Connectionless Transport: UDP**

1. Write Udp/sock\_dgram Applications?

Answer: To implement the udp service we must create socket by socket system call which takes argument as SOCK\_DGRAM which is used for to pass the data in the form of datagrams

2. How to Get Ip Header of a Udp Message?

Answer: Actually ip header is not in an udp message. It a comes at network link layer while udp message generate at Transport layer

3. How To Be Sure That a Udp Message Is Received?

Answer : In IP Header Protocol field is available, it tells which protocol it is using as a transport layer, if this field is having 6(in decimal)it indicates TCP,17(in decimal)it indicates UDP. ate at transport layer.

4. What is the UDP packet format?

Answer: The UDP packet format contains four fields:

Source Port and Destination Port fields (16 bits each): Endpoints of the connection.

Length field (16 bits): length of the header and data.

Checksum field (16 bits): It allows packet integrity checking (optional).

5. Is UDP better than TCP?

Answer: Both protocols are used for different purposes. If the user wants error-free and guarantees to deliver data, TCP is the choice. If the user wants fast transmission of data and little loss of data is not a problem, UDP is the choice.

6. Explain User Datagram Protocol, UDP.

Answer: UDP is a connection-less protocol. In simple terms, if one data packet is lost during transmission, it will not send that packet again.

This protocol is suitable where minor data loss is not a major issue.

**Topic 7: Connection-Oriented Transport-TCP**

1. What is the sequence of a TCP connection?

TCP connection flow. The following sequence shows the flow of a TCP connection: The server creates the listener socket that is waiting for remote clients to connect. The client issues the connect () socket function to start the TCP handshake (SYN, SYN/ACK, ACK).

2. How is a connection established and terminated in TCP?

TCP Connection Establish and Terminate. To establish a connection, TCP uses a three-way handshake. Before a client attempts to connect with a server, the server must first bind to and listen at a port to open it up for connections: this is called a passive open. ... SYN-ACK: In response, the server replies with a SYN-ACK.

3. What is 3 way handshaking in TCP?

THREE-WAY HANDSHAKE or a TCP 3-way handshake is a process which is used in a TCP/IP network to make a connection between the server and client. It is a three-step process that requires both the client and server to exchange synchronization and acknowledgment packets before the real data communication process starts.

4. What are the 3 steps in a TCP handshake?

To establish a connection, the three-way (or 3-step) handshake occurs:

• SYN: The active open is performed by the client sending a SYN to the server. ...

• SYN-ACK: In response, the server replies with a SYN-ACK. ...

• ACK: Finally, the client sends an ACK back to the server.

5. How does TCP guarantee delivery?

TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent. ... Sequence numbers are used to coordinate which data has been transmitted and received. TCP will arrange for retransmission if it determines that data has been lost.

6. What is TCP packet format?

TCP packet. The TCP packet format consists of these fields: Source Port and Destination Port fields (16 bits each) identify the end points of the connection. Sequence Number field (32 bits) specifies the number assigned to the first byte of data in the current message.

**Topic 8: Principles of Congestion control**

1. What are the principles of congestion control?

Network-assisted congestion control:With network-assisted congestion control, network-layer components (i.e., routers) provide explicit feedback to the sender regarding the congestion state in the network. This feedback may be as simple as a single bit indicating congestion at a link.

2. What is congestion control in transport layer?

The well-known and widely used close-loop control mechanism is TCP congestion control, which is implemented at transport layer. ... This algorithm controls the number of packets entering the network, and allows multiple TCP connections to share the bandwidth of a link.

3. What is choke packet how is it used for congestion control?

A choke packet is used in network maintenance and quality management to inform a specific node or transmitter that its transmitted traffic is creating congestion over the network. This forces the node or transmitter to reduce its output rate. Choke packets are used for congestion and flow control over a network.

4. What is it goal of congestion control?

Congestion control is a network layer issue, and is thus concerned with what happens when there is more data in the network than can be sent with reasonable packet delays, no lost packets, etc. Flow control is a local, congestion control is global.

5. Why does congestion occur in networks?

Congestion occurs when bandwidth is insufficient and network data traffic exceeds capacity. Data packet loss from congestion is partially countered by aggressive network protocol retransmission, which maintains a network congestion state after reducing the initial data load.

**Topic 9: TCP Congestion Control**

1. Which algorithm is used for congestion control?

Transmission Control Protocol (TCP) uses a network congestion-avoidance algorithm that includes various aspects of an additive increase/multiplicative decrease (AIMD) scheme, along with other schemes including slow start and congestion window, to achieve congestion avoidance

2. What is TCP CWND?

Congestion Window (cwnd) is a TCP state variable that limits the amount of data the TCP can send into the network before receiving an ACK. ... Together, the two variables are used to regulate data flow in TCP connections, minimize congestion, and improve network performance

3. What is threshold in TCP congestion control?

This phase continues until the congestion window size reaches the slow start threshold. Threshold. = Maximum number of TCP segments that receiver window can accommodate / 2. = (Receiver window size / Maximum Segment Size) / 2.

4. What is congestion window in TCP?

Congestion Window (cwnd) is a TCP state variable that limits the amount of data the TCP can send into the network before receiving an ACK. The Receiver Window (rwnd) is a variable that advertises the amount of data that the destination side can receive

5. What is fast retransmission in TCP?

Fast retransmit is a modification to the congestion avoidance algorithm. As in Jacobson's fast retransmit algorithm, when the sender receives 3rd duplicate ACK, it assumes that the packet is lost and retransmit that packet without waiting for a retransmission timer to expire.

6. What do you mean by slow start in TCP congestion?

Slow start prevents a network from becoming congested by regulating the amount of data that's sent over it. It negotiates the connection between a sender and receiver by defining the amount of data that can be transmitted with each packet, and slowly increases the amount of data until the network's capacity is reached

7. Why does TCP wait for 3 duplicates?

Since TCP does not know whether a duplicate ACK is caused by a lost segment or just a reordering of segments, it waits for a small number of duplicate ACKs to be received. ... If three or more duplicate ACKs are received in a row, it is a strong indication that a segment has been lost.