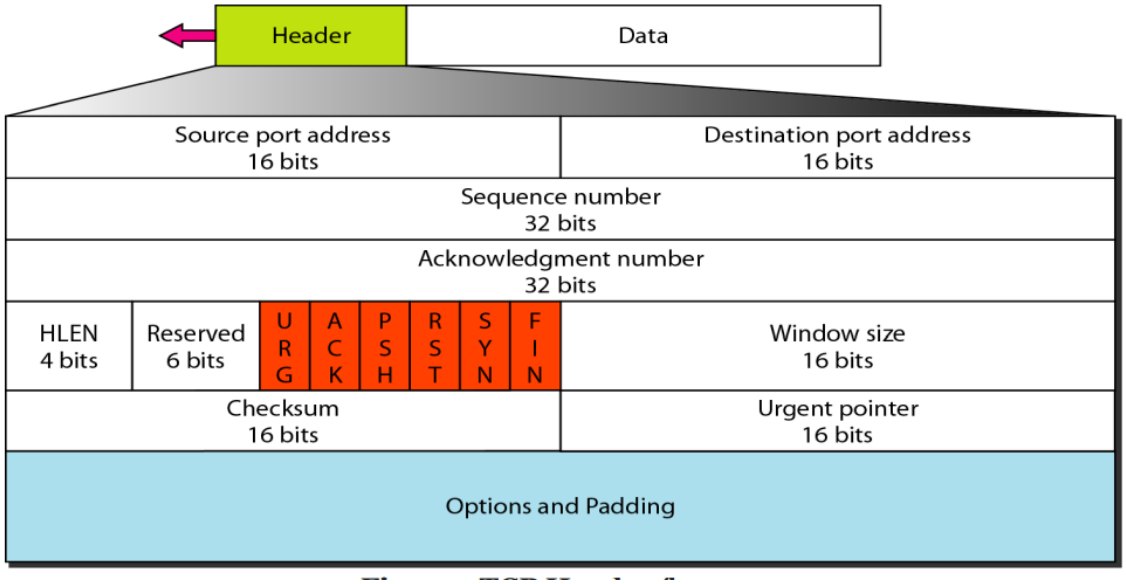
CST 303 COMPUTER NETWORKS

QUESTION BANK

MODULE 5

1. Draw TCP header format



2. Explain TCP Congestion control? /List different strategies used by TCP to control congestion./ Why TCP congestion control is termed as AIMD (Additive Increase Multiplicative Decrease).

Congestion policy in TCP –

Slow Start Phase: starts slowly increment is exponential to threshold

Congestion Avoidance Phase: After reaching the threshold increment is by 1

Congestion Detection Phase: Sender goes back to Slow start phase or Congestion avoidance phase.

Slow Start Phase : exponential increment – In this phase after every RTT the congestion window size increments exponentially.

Initially cwnd = 1

After 1 RTT, cwnd = 2^(1) = 2

2 RTT, cwnd = 2^(2) = 4

3 RTT, cwnd = 2^(3) = 8

Congestion Avoidance Phase : additive increment – This phase starts after the threshold value also denoted as ssthresh. The size of cwnd(congestion window) increases additive. After each RTT cwnd = cwnd + 1.

Initially cwnd = i

After 1 RTT, cwnd = i+1

2 RTT, cwnd = i+2

3 RTT, cwnd = i+3

Congestion Detection Phase : multiplicative decrement – If congestion occurs, the congestion window size is decreased. The only way a sender can guess that congestion has occurred is the need to retransmit a segment. Retransmission is needed to recover a missing packet that is assumed to have been dropped by a router due to congestion. Retransmission can occur in one of two cases: when the RTO timer times out or when three duplicate ACKs are received.

Case 1 : Retransmission due to Timeout – In this case congestion possibility is high.

(a) ssthresh is reduced to half of the current window size.

(b) set cwnd = 1

(c) start with slow start phase again.

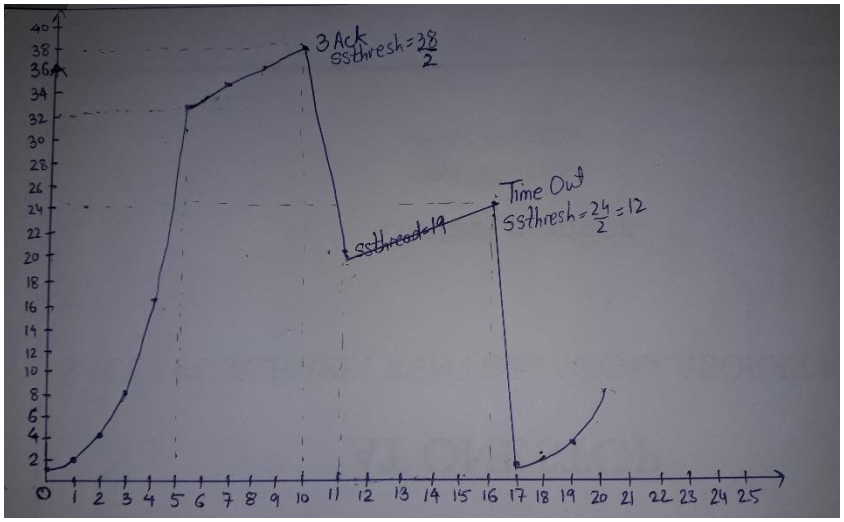
Case 2 : Retransmission due to 3 Acknowledgement Duplicates – In this case congestion possibility is less.

(a) ssthresh value reduces to half of the current window size.

(b) set cwnd= ssthresh

(c) start with congestion avoidance phase

Example – Assume a TCP protocol experiencing the behavior of slow start. At 5th transmission round with a threshold (ssthresh) value of 32 goes into congestion avoidance phase and continues till 10th transmission. At 10th transmission round, 3 duplicate ACKs are received by the receiver and enter into additive increase mode. Timeout occurs at 16th transmission round. Plot the transmission round (time) vs congestion window size of TCP segments.



3. Differentiate between TCP and UDP

UDP	TCP
Message oriented protocol	Byte oriented protocol
Connection Less	Connection Oriented
Preserve message boundaries	Does not Preserve message boundaries
Unreliable	Reliable
No congestion and flow control	Have congestion and flow control
Each message follows different route so no sequencing	Each message follows same route so have in sequence data delivery
Port no 17	Port no 6

4. What is socket? Which are various primitives used in client server communication.

Sockets allow communication between two different processes on the same or different machines. A socket is bound to a port number so that the TCP layer can identify the application that data is destined to be sent to. An endpoint is a combination of an IP address and a port number.

socket() creates a new socket of a certain socket type, identified by an integer number, and allocates system resources to it.

bind() is typically used on the server side, and associates a socket with a socket address structure, i.e. a specified local port number and IP address.

listen() is used on the server side, and causes a bound TCP socket to enter listening state.

connect() is used on the client side, and assigns a free local port number to a socket. In case of a TCP socket, it causes an attempt to establish a new TCP connection.

accept() is used on the server side. It accepts a received incoming attempt to create a new TCP connection from the remote client, and creates a new socket associated with the socket address pair of this connection.

send() and recv(), or write() and read(), or sendto() and recvfrom(), are used for sending and receiving data to/from a remote socket.

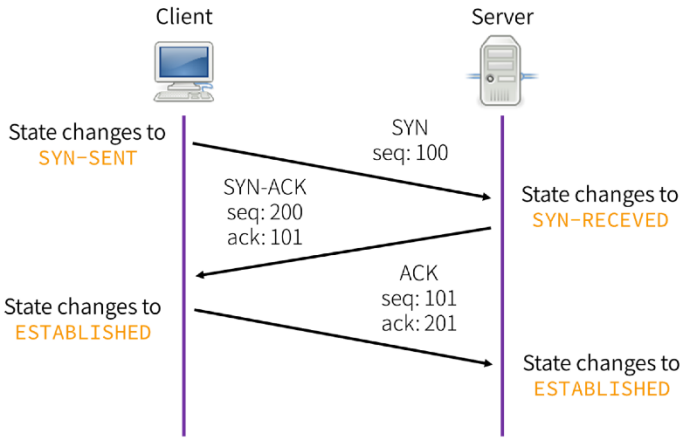
close() causes the system to release resources allocated to a socket. In case of TCP, the connection is terminated.

gethostbyname() and gethostbyaddr() are used to resolve host names and addresses. IPv4 only.

5. Draw and Explain 3-way handshake process of TCP.

TCP connections are established via an exchange known as the three-way handshake. If A is the client and B is the LISTENing server, then the handshake proceeds as follows:

- A sends B a packet with the SYN bit set (a SYN packet)
- B responds with a SYN packet of its own; the ACK bit is now also set
- A responds to B's SYN with its own ACK



Normally, the three-way handshake is triggered by an application's request to connect; data can be sent only after the handshake completes. This means a one-RTT delay before any data can be sent.

6. "TCP header having a checksum field is redundant as IP header already has a checksum".Do you think the statement is right? Yes/No. Validate your claim with relevant examples.

It is not right; TCP header checksum field is not redundant with IP header checksum.

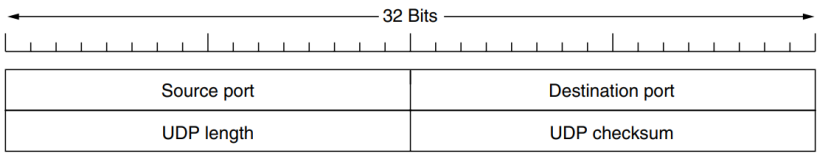
Reasons:

- IP checksum is only performed for the ipv4 header (first 20 bytes) not for the payload.
- This makes a lot of difference. From this fact arises the need for TCP and UDP to perform complete checksum to verify the data integrity.
- IP does not always run over ethernet
- IP does not checksum the data
- TCP packets can be reassembled incorrectly from IP packets and fragments that each have perfect checksums
- Even if reassembled correctly, software or other errors could be introduced in the layers between IP and TCP
- Every time a new header is introduced there is more to checksum, and the new layer can't see the header bits of the layer below.

7. Explain UDP header? The following is a DUMP of a UDP header in hexadecimal format. 06 32 00 0D 00 1C E2 17.

a. What is source port number?
b. What is destination port number?
c. What is length of user datagram?

The UDP header consists of four fields each of 2 bytes in length:



a. The source port number is the first four hexadecimal digits (0632) or 1586
b. The destination port number is the second four hexadecimal digits (000D) or 13.

c. The third four hexadecimal digits (001C) define the length of the whole UDP packet as 28 bytes.

8. State which transport layer protocol is used by following application layer protocol. HTTP,FTP,DHCP,DNS,SMTP,TELNET

Application Layer Protocol	Transport layer Protocol TCP/UDP
HTTP	TCP
SMTP	TCP
DNS	UDP
TELNET	TCP
DHCP	UDP
FTP	TCP

9. Compare IMAP and POP3.

Both are Mail Access Protocols works in association with SMTP for the final mail delivery

	POP3	IMAP
Name	Post Office Protocol	Internet Messaging Access Protocol
Method	Always download new emails to local storage	Only message summary are downloaded until the message is selected
Email inbox	All mails are downloaded into Inbox folder	Preserves a main folder "imap.hyperoffice.com"
Access	Can only be accessed by one computer	Email can be manipulated to multiple devices
Storage	Emails are deleted from server once it is successfully downloaded by user	Emails are kept in server storage until the user decides to delete it
Port number used	110	143

10. What is the use of MIME? Explain MIME header in detail.

Multipurpose Internet Mail Extensions (MIME) is an Internet standard that extends the format of email to support:

- Text in character sets other than ASCII
- Non-text attachments: audio, video, images, application programs etc.
- Message bodies with multiple parts
- Header information in non-ASCII character sets

MIME headers appear at the beginning of a MIME message as well as within the separate body parts. Some MIME headers can be used both as message headers and in MIME body parts. Some additional headers are defined for use only in body parts. The following headers are defined in MIME:

- MIME-Version is a required header indicating that this message is to use the rules of MIME. "MIME-Version: 1.0" is the only currently defined MIME-Version header allowed.
- Content-Type headers are used to specify the media type and subtype of data in the body of a message
- Content-Transfer-Encoding headers can have two different meanings. If the value is "base64" or "quoted printable", then the header indicates the encoding used for this body part. If the value is "7bit", "8bit", or "binary", then the header indicates that there is no encoding
- Content-ID headers are world-unique values that identify body parts
- Content-Description headers are optional and are often used to add descriptive text to non-textual body parts.
- Content-Disposition headers provide information about how to present a message or a body part.

11. What is DNS? Explain its working with the example. / Describe the name-address resolution techniques used in DNS / DNS Query resolution.

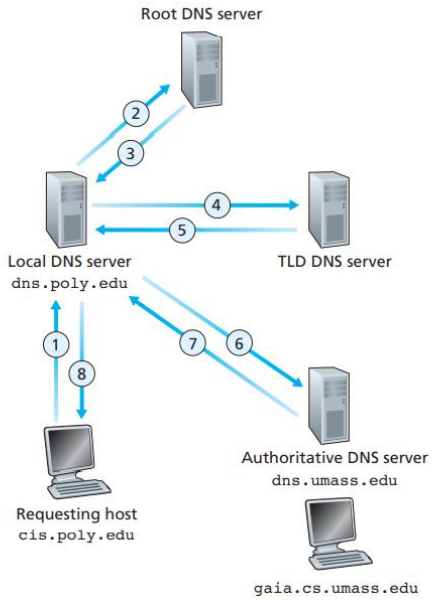
DNS: Domain Name Servers (DNS) are the Internet's equivalent of a phone book. They maintain a directory of domain names and translate them to Internet Protocol (IP) addresses. This is necessary because, although domain names are easy for people to remember, computers or machines, access websites based on IP addresses.

Two types of name resolution:

Recursive Resolution –

Here, the client requires the Local Server to give either the requested mapping or an error message. A DNS Query is generated by the application program to the resolver to fetch the destination IP Address. The Query is then forward to the local DNS Server. If it knows the IP Address, it sends a response to the resolver. Assuming, it does not know the IP Address, it sends the query to the root name server.

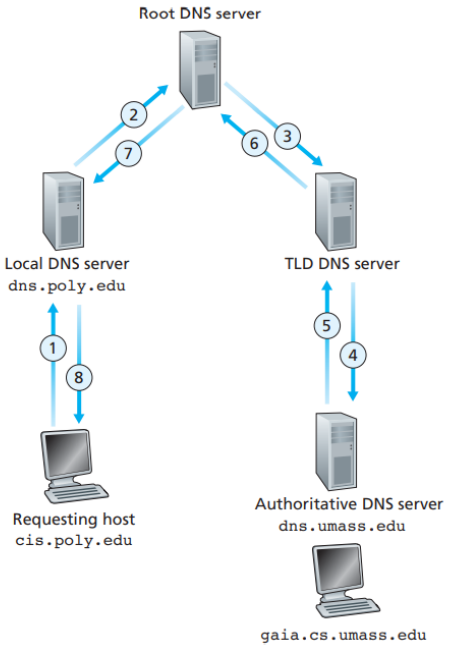
The root name server contains information about at least one server of Top Level Domain. The query is then sent to the respective Top-Level Domain server. If it contains the mapping, the response is sent back to the root server and then to the host's local server. If it doesn't contain the mapping, it should contain the IP Address of the destination's local DNS Server. The local DNS server knows the destination host's IP Address. The information is then sent back to the top-level domain server, then to the root server and then to the host's Local DNS Server, and finally to the host.



Iterative Resolution –

The main difference between iterative and recursive resolution is that here each server that does not know the mapping sends the IP Address of the next server to the one requested it. Here, the client allows the server to return the best answer it can give as a match or as a referral. A DNS Query is generated by the application program to the resolver to fetch the destination IP Address. The Query is then forward to the local DNS Server. Assuming, it does not know the IP Address, it sends the query to the root name server.

The root name server returns the IP Address of the Top-Level Domain Server to the Local Server. The Top-Level Domain server is contacted by the Local Server and it returns either the IP of the destination host or its local DNS Server. If it returns the server's address, then by contacting the destination's Local DNS Server, we get the IP Address of the destination host. The response/mapping is then passed from the host's local DNS server to the resolver and then finally to the host.



12. Discuss FTP (File Transfer Protocol) in detail.

During FTP Connection 2 transmission channels are open

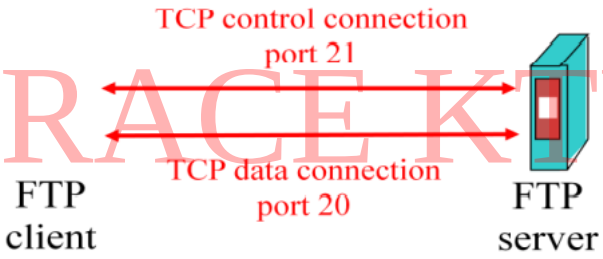
1. Control Channel (For command)

2. Data Channel (For data)

Control uses port no 21 and Data connection uses Port no 20. FTP client contacts FTP server at port 21, TCP is transport protocol. client authorized over control connection. client browses remote directory by sending commands over control connection. when server receives file transfer command, server opens 2 nd TCP connection (for file) to client . After transferring one file, server closes data connection. Server opens another TCP data connection to transfer another file. Control connection: “out of band” .FTP server maintains “state”: current directory, earlier authentication.

Sample commands: sent as ASCII text over control channel

- USER username
- PASS password
- LIST return list of file in current directory
- RETR filename retrieves (gets) file
- STOR filename stores (puts) file onto remote host



13. What is SNMP? List three components of SNMP. List different messages of SNMP.

Simple Network Management Protocol (SNMP) –

SNMP is an application layer protocol that uses UDP port number 161/162.SNMP is used to monitor the network, detect network faults, and sometimes even used to configure remote devices.

SNMP components –

There are 3 components of SNMP:

1. SNMP Manager –

It is a centralized system used to monitor network. It is also known as Network Management Station (NMS)

2. SNMP agent –

It is a software management software module installed on a managed device. Managed devices can be network devices like PC, routers, switches, servers, etc.

3. Management Information Base –

MIB consists of information on resources that are to be managed. This information is organized hierarchically. It consists of objects instances which are essentially variables.

SNMP messages –

GetRequest –

SNMP manager sends this message to request data from the SNMP agent. It is simply used to retrieve data from SNMP agents. In response to this, the SNMP agent responds with the requested value through a response message.

GetNextRequest –

This message can be sent to discover what data is available on an SNMP agent. The SNMP manager can request data continuously until no more data is left. In this way, the SNMP manager can take knowledge of all the available data on SNMP agents.

GetBulkRequest –

This message is used to retrieve large data at once by the SNMP manager from the SNMP agent. It is introduced in SNMPv2c.

SetRequest –

It is used by the SNMP manager to set the value of an object instance on the SNMP agent.

Response –

It is a message sent from the agent upon a request from the manager. When sent in response to Get messages, it will contain the data requested. When sent in response to the Set message, it will contain the newly set value as confirmation that the value has been set.

Trap –

These are the message sent by the agent without being requested by the manager. It is sent when a fault has occurred.

InformRequest –

It was introduced in SNMPv2c, used to identify if the trap message has been received by the manager or not. The agents can be configured to set trap continuously until it receives an Inform message. It is the same as a trap but adds an acknowledgement that the trap doesn’t provide.