**FORMULAS**

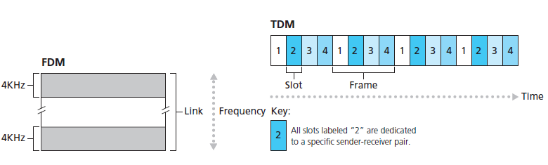
**DEFINITIONS – CHAPTER 1**

Access Technologies  
 Home Access: DSL, Cable, Fiber To The Home, Dial-Up, Satellite (Unguided),

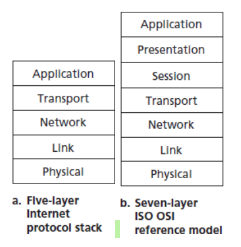
Hybrid Fiber Coaxial

Enterprise: Ethernet, Wireless LAN (802.11)

Wide Area (Unguided): 3G, LTE

Circuit Switching – Dedicated physical path between hosts

Circuit Switching Vs Packet Switching 
Circuit Switching 
Physical path betw•een 
source and destinaim 
All packets use same 
path 
Reserve entire 
bandwidth in advance 
Bandwidtl Wastage 
No store and forward 
transmission 
Packet Switching 
No physical path 
Packets travel 
independently 
Does not reserve 
NO Bandwidth 
wastage 
Supports store and 
forward transmission Packet Switching – Logical path between hosts; no physical hardware dedicated



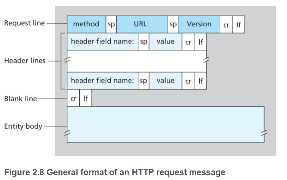
**DEFINITIONS – CHAPTER 2**

HTTP (80) – HyperText Transfer Protocol; SMTP (25, 465, 587) – Simple Mail Transfer Protocol

POP3 (110; 995) – Post Office Protocol v3; IMAP (143, 993)– Internet Mail Access Protocol

DNS (53)– Domain Name System; DASH (80) – Dynamic Adaptive Streaming over HTTP

CDN – Content Distribution Network

**METHODS**

* GET – Retrieve items
* POST – Submit data
* PUT – Upload data
* PATCH – Update data
* DELETE – Remove data
* HEAD – Retrieve just headers

**HTTP COMMON REQUEST HEADER FIELDS**

- If-Modified-Since: Retrieve the requested only if it has changed since the date provided; Commonly used by CDNs

- Set-Cookie: Provide the cookie value for the site

- Content-Type: Accepted content types

- Accept-Language: What languages content will be accepted in  
- User-Agent: Identify the client operating system and browser

- Date-Modified: Server information about the file modification time.

- Content-Length: Tells the browser when to stop expecting data from the server (Length of body)

**round-trip time (RTT):** the time it takes for a small packet to travel from client to server and then back to the client. The RTT includes packet-propagation delays, packet-queuing delays in intermediate routers and switches, and packet-processing delays

**HTTP RESPONSE STATUS CODES**

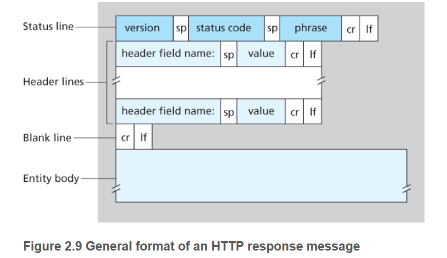
200 OK: Request succeeded and the information is returned in the response.

301 Moved Permanently: Requested object has been permanently moved; the new URL is specified in Location: header of the response message. The client software will automatically retrieve the new URL.

400 Bad Request: This is a generic error code indicating that the request could not be understood by the server.

404 Not Found: The requested document does not exist on this server.

505 HTTP Version Not Supported: The requested HTTP protocol version is not supported by the server.

**SMTP –** Encoded in 7-bit ASCII character set

**POP3 –**

Download and Delete: When message is retrieved from the server, it is deleted from the server.

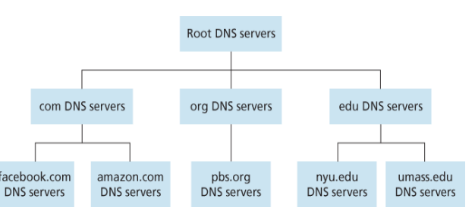
Download and Keep: Message is retrieved from server and must be explicitly deleted.

**IMAP –** IMAP associates messages with folders; Allows user to obtain parts of message (e.g. sent time, sender, headers, etc.)  
**DNS – Record Types (Name, Value, Type, TTL[time-to-live])**

A – Name = Hostname; Value = IP

NS – Name = domain; Value = Authoritative DNS IP

CNAME – Name = Hostname (A Record); Value = Canonical Hostname

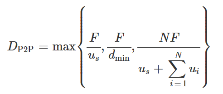
MX – Name = Hostname (A Record); Value = Canonical Name of Mail Server

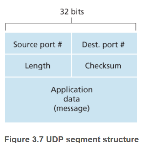
13 Root Organizations / Servers

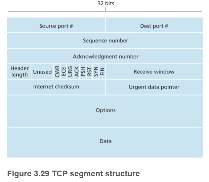
TLD – Top Level Domain Servers (.com, .net, .nyc)

Authoritative DNS - (nyu.edu, nyc.gov)

**P2P**

**Rarest First**: The idea is to determine, from among the chunks she does not have, the chunks that are the rarest among her neighbors (that is, the chunks that have the fewest repeated copies among her neighbors) and then request those rarest chunks first.  
Every 10 seconds, she recalculates the rates and possibly modifies the set of four peers. In BitTorrent lingo, these four peers are said to be **unchoked**. Importantly, every 30 seconds, she also picks one additional neighbor at random and sends it chunks. Let’s call the randomly chosen peer Bob. In BitTorrent lingo, Bob is said to be **optimistically unchoked.**   
In **DASH**, the video is encoded into several different versions, with each version having a different bit rate and, correspondingly, a different quality level. The client dynamically requests chunks of video segments of a few seconds in length. When the amount of available bandwidth is high, the client naturally selects chunks from a high-rate version; and when the available bandwidth is low, it naturally selects from a low-rate version. The client selects different chunks one at a time with HTTP GET request messages   
**CDN – Enter Deep** – Deploy CDN in Access ISPs around the world  
**CDN – Bring Home** – Deploy CDN in large clusters (smaller number) in IXPs  
https://cl.ly/00fdd5cd458f

UDP – 2 Tuple (Source Port, Destination Port)  
Header – 8 bytes  
Connectionless – No state and no handshake   
No processing on network layer of data; passes directly to application  
Examples: DNS, Video, VOIP

Checksum – See binary addition with rollover  
  
  
TCP – 4 Tuple (Source IP, Source Port, Destination IP, Destination Port)

Header – Receiver window (Depends on the buffer size); Seq Number; Ack Number (expected next seq number)  
Total header size: 20bytes

RDT (Reliable Data Transfer) contains:

Sequence Number – Identify the amount of data successfully transmitted up to this point (to determine or not the data is retransmitted)

Ack – expected next seq number. If segment A has seq 1000, contains 1000bytes, the ack would be 2000

Timer – Amount of time is passed since the oldest packet was sent but not acked

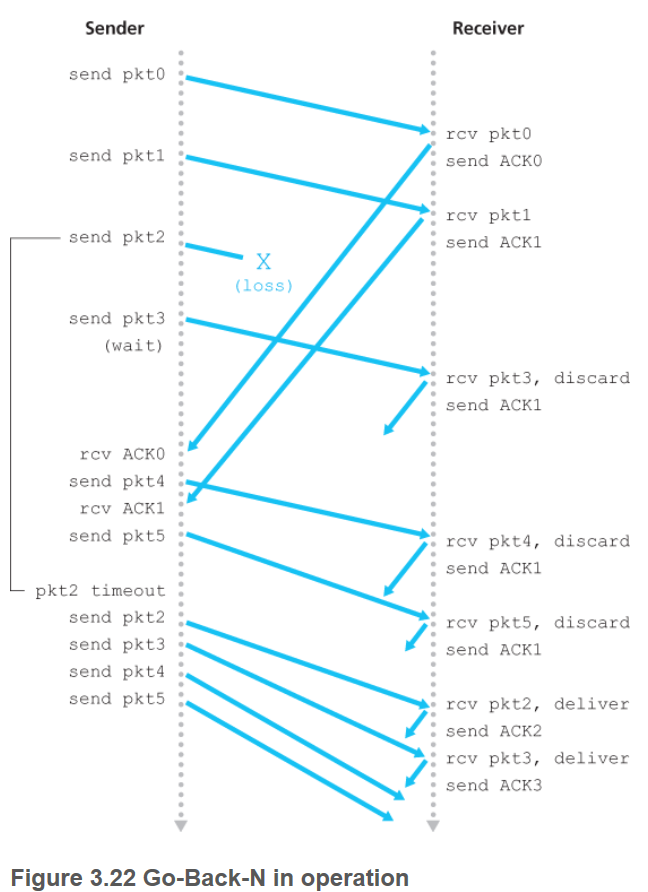
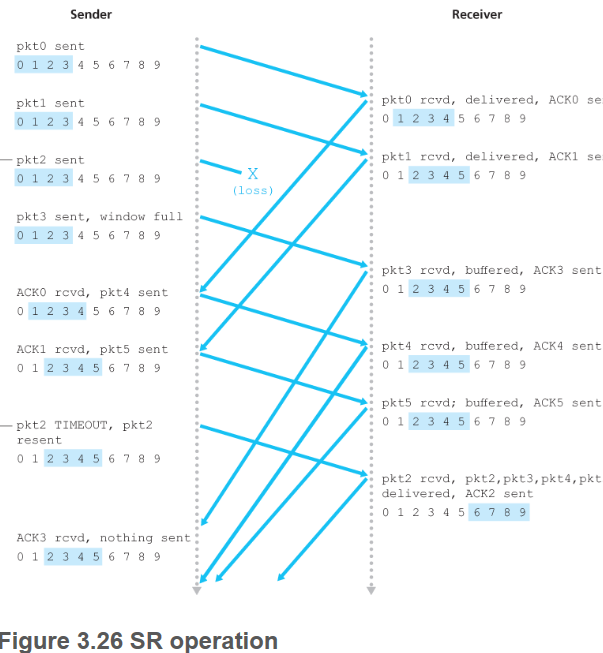
MSS – Maximum Segment Size – Maximum size of the data in each segment

Typically, the MTU is 1500, MSS is 1460, TCP header is 20bytes, and IP header is 20bytes

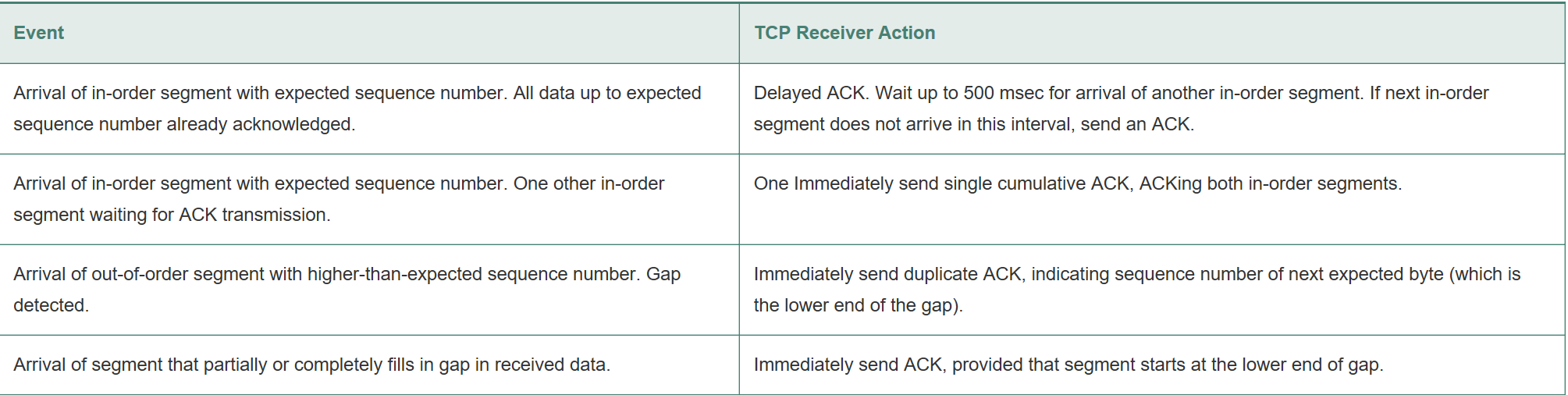
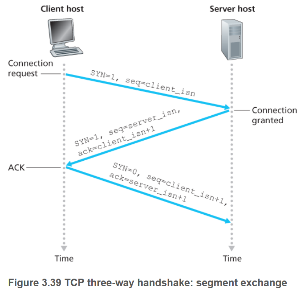
3way handshake – SYN, SYNACK, ACK

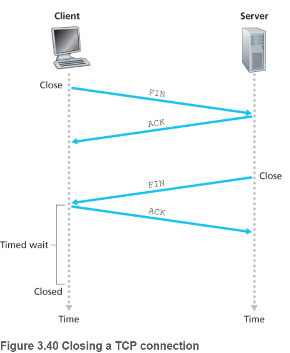
Go-Back-N: Sender can send multiple packets up to *N* without receiving ACK

Selectively Repeat: Sender retransmits only packets that were lost / transmitted out-of-order

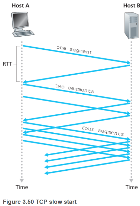
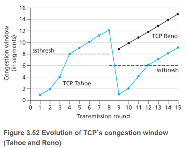
**Fast Retransmit**





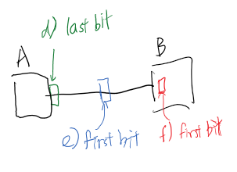
Congestion Window (cwnd): constraint on the rate

a sender can send traffic into network.

cwnd normally starts at 1 MSS and increases by 1 MSS each time a transmitted segment is ACKd

ssthresh = cwnd/2

**R20.** Suppose end system A wants to send a large file to end system B. At a very high level, describe how end system A creates packets from the file. When one of these packets arrives to a router, what information in the packet does the router use to determine the link onto which the packet is forwarded? Why is packet switching in the Internet analogous to driving from one city to another and asking directions along the way?  
End system A breaks the large file into chunks. It adds header to each chunk, thereby generating multiple packets from the file. The header in each packet includes the IP address of the destination (end system B). The packet switch uses the destination IP address in the packet to determine the outgoing link. Asking which road to take is analogous to a packet asking which outgoing link it should be forwarded on, given the packet’s destination address.  
**P6**. This elementary problem begins to explore propagation delay and transmission delay, two central concepts in data networking. Consider two hosts, A and B, connected by a single link of rate R bps. Suppose that the two hosts are separated by m meters, and suppose the propagation speed along the link is s meters/sec. Host A is to send a packet of size L bits to Host B.

1. Express the propagation delay, , in terms of m and s.
2. Determine the transmission time of the packet, , in terms of L and R.
3. Ignoring processing and queuing delays, obtain an expression for the end-to-end delay.
4. Suppose Host A begins to transmit the packet at time . At time , where is the last bit of the packet?
5. Suppose is greater than . At time , where is the first bit of the packet?
6. Suppose is less than . At time , where is the first bit of the packet?
7. Suppose , , and . Find the distance so that equals .

**R4**. For a P2P file-sharing application, do you agree with the statement, "There is no notion of client and server sides of a communication session"? Why or why not?

No. In a P2P file-sharing application, the peer that is receiving a file is typically the client and the peer that is sending the file is typically the server.

**R10**. What is meant by a handshaking protocol?

A protocol uses handshaking if the two communicating entities first exchange control packets before sending data to each other. SMTP uses handshaking at the application layer whereas HTTP does not.

**R11**. Why do HTTP, SMTP, and POP3 run on top of TCP rather than on UDP?

The applications associated with those protocols require that all application data be received in the correct order and without gaps. TCP provides this service whereas UDP does not.

**R12**. Consider an e-commerce site that wants to keep a purchase record for each of its customers. Describe how this can be done with cookies.

When the user first visits the site, the server creates a unique identification number, creates an entry in its back-end database, and returns this identification number as a cookie number. This cookie number is stored on the user’s host and is managed by the browser. During each subsequent visit (and purchase), the browser sends the cookie number back to the site. Thus the site knows when this user (more precisely, this browser) is visiting the site.

**R18**. From a user’s perspective, what is the difference between the download-and-delete mode and the download-and-keep mode in POP3?

With download and delete, after a user retrieves its messages from a POP server, the messages are deleted. This poses a problem for the nomadic user, who may want to access the messages from many different machines (office PC, home PC, etc.). In the download and keep configuration, messages are not deleted after the user retrieves the messages. This can also be inconvenient, as each time the user retrieves the stored messages from a new machine, all of non-deleted messages will be transferred to the new machine (including very old messages).

**R21**. In BitTorrent, suppose Alice provides chunks to Bob throughout a 30-second interval. Will Bob necessarily return the favor and provide chunks to Alice in this same interval? Why or why not?

It is not necessary that Bob will also provide chunks to Alice. Alice has to be in the top 4 neighbors of Bob for Bob to send out chunks to her; this might not occur even if Alice provides chunks to Bob throughout a 30-second interval.

**R25**. Besides network-related considerations such as delay, loss, and bandwidth performance, there are other important factors that go into designing a CDN server selection strategy. What are they?

Other than network-related factors, there are some important factors to consider, such as load-balancing (clients should not be directed to overload clusters), diurnal effects, variations across DNS servers within a network, limited availability of rarely accessed video, and the need to alleviate hot-spots that may arise due to popular video content.

**P1**. True or false?

a. A user requests a Web page that consists of some text and three images. For this page, the client will send one request message and receive four response messages. False

b. Two distinct Web pages (for example, www.mit.edu/research.html and www.mit.edu/students.html) can be sent over the same persistent connection. True

c. With non-persistent connections between browser and origin server, it is possible for a single TCP segment to carry two distinct HTTP request messages. False

d. The Date: header in the HTTP response message indicates when the object in the response was last modified. False

e. HTTP response messages never have an empty message body. False

**P4**. Consider the following string of ASCII characters that were captured by Wireshark when the browser sent an HTTP GET message (i.e., this is the actual content of an HTTP GET message). The characters <cr><lf> are carriage return and line-feed characters (that is, the italized character string <cr> in the text below represents the single carriage-return character that was contained at that point in the HTTP header). Answer the following questions, indicating where in the HTTP GET message below you find the answer.

GET /cs453/index.html HTTP/1.1<cr><lf>Host: gai

a.cs.umass.edu<cr><lf>User-Agent: Mozilla/5.0 (

Windows;U; Windows NT 5.1; en-US; rv:1.7.2) Gec

ko/20040804 Netscape/7.2 (ax) <cr><lf>Accept:ex

t/xml, application/xml, application/xhtml+xml, text

/html;q=0.9, text/plain;q=0.8, image/png,\*/\*;q=0.5

<cr><lf>Accept-Language: en-us, en;q=0.5<cr><lf>Accept-

Encoding: zip, deflate<cr><lf>Accept-Charset: ISO

-8859-1, utf-8;q=0.7,\*;q=0.7<cr><lf>Keep-Alive: 300<cr>

<lf>Connection:keep-alive<cr><lf><cr><lf>

a. What is the URL of the document requested by the browser?

The document request was http://gaia.cs.umass.edu/cs453/index.html. The Host : field indicates the server's name and /cs453/index.html indicates the file name.

b. What version of HTTP is the browser running?

The browser is running HTTP version 1.1, as indicated just before the first <cr><lf> pair.

c. Does the browser request a non-persistent or a persistent connection?

The browser is requesting a persistent connection, as indicated by the Connection: keep-alive.

d. What is the IP address of the host on which the browser is running?

This is a trick question. This information is not contained in an HTTP message anywhere. So there is no way to tell this from looking at the exchange of HTTP messages alone. One would need information from the IP datagrams (that carried the TCP segment that carried the HTTP GET request) to answer this question.

e. What type of browser initiates this message? Why is the browser type needed in an HTTP request message?

Mozilla/5.0. The browser type information is needed by the server to send different versions of the same object to different types of browsers.

**P6**. Obtain the HTTP/1.1 specification (RFC 2616). Answer the following questions:

a. Explain the mechanism used for signaling between the client and server to indicate that a persistent connection is being closed. Can the client, the server, or both signal the close of a connection?

Persistent connections are discussed in section 8 of RFC 2616 (the real goal of this question was to get you to retrieve and read an RFC). Sections 8.1.2 and 8.1.2.1 of the RFC indicate that either the client or the server can indicate to the other that it is going to close the persistent connection. It does so by including the connection-token "close" in the Connection-header field of the http request/reply.

b. What encryption services are provided by HTTP?

HTTP does not provide any encryption services

c. Can a client open three or more simultaneous connections with a given server? Computer Networking

(From RFC 2616) "Clients that use persistent connections should limit the number of simultaneous connections that they maintain to a given server. A single-user client SHOULD NOT maintain more than 2 connections with any server or proxy."

d. Either a server or a client may close a transport connection between them if either one detects the connection has been idle for some time. Is it possible that one side starts closing a connection while the other side is transmitting data via this connection? Explain.

Yes. (From RFC 2616) "A client might have started to send a new request at the same

time that the server has decided to close the "idle" connection. From the server's point

of view, the connection is being closed while it was idle, but from the client's point of

view, a request is in progress."

**R3**. Consider a TCP connection between Host A and Host B. Suppose that the TCP segments traveling from Host A to Host B have source port number x and destination port number y. What are the source and destination port numbers for the segments traveling from Host B to Host A?

Source port number y and destination port number x.

**R4**. Describe why an application developer might choose to run an application over UDP rather than TCP.

An application developer may not want its application to use TCP’s congestion control, which can throttle the application’s sending rate at times of congestion. Often, designers of IP telephony and IP videoconference applications choose to run their applications over UDP because they want to avoid TCP’s congestion control. Also, some applications do not need the reliable data transfer provided by TCP.

**R5**. Why is it that voice and video traffic is often sent over TCP rather than UDP in today’s Internet? (Hint: The answer we are looking for has nothing to do with TCP’s congestion-control mechanism.)

Since most firewalls are configured to block UDP traffic, using TCP for video and voice traffic lets the traffic though the firewalls.

**R7**. Suppose a process in Host C has a UDP socket with port number 6789. Suppose both Host A and Host B each send a UDP segment to Host C with destination port number 6789. Will both of these segments be directed to the same socket at Host C? If so, how will the process at Host C know that these two segments originated from two different hosts?

Yes, both segments will be directed to the same socket. For each received segment, at the socket interface, the operating system will provide the process with the IP addresses to determine the origins of the individual segments.

**R8.** Suppose that a Web server runs in Host C on port 80. Suppose this Web server uses persistent connections, and is currently receiving requests from two different Hosts, A and B. Are all of the requests being sent through the same socket at Host C? If they are being passed through different sockets, do both of the sockets have port 80? Discuss and explain.

For each persistent connection, the Web server creates a separate “connection socket”. Each connection socket is identified with a four-tuple: (source IP address, source port number, destination IP address, destination port number). When host C receives and IP datagram, it examines these four fields in the datagram/segment to determine to which socket it should pass the payload of the TCP segment. Thus, the requests from A and B pass through different sockets. The identifier for both of these sockets has 80 for the destination port; however, the identifiers for these sockets have different values for source IP addresses. Unlike UDP, when the transport layer passes a TCP segment’s payload to the application process, it does not specify the source IP address, as this is implicitly specified by the socket identifier.

**R10**. In our rdt protocols, why did we need to introduce timers?

To handle losses in the channel. If the ACK for a transmitted packet is not received within the duration of the timer for the packet, the packet (or its ACK or NACK) is assumed to have been lost. Hence, the packet is retransmitted.

**R14**. True or false?

a. Host A is sending Host B a large file over a TCP connection. Assume Host B has no data to send Host A. Host B will not send acknowledgments to Host A because Host B cannot piggyback the acknowledgments on data. **False**

b. The size of the TCP rwnd never changes throughout the duration of the connection. **False**

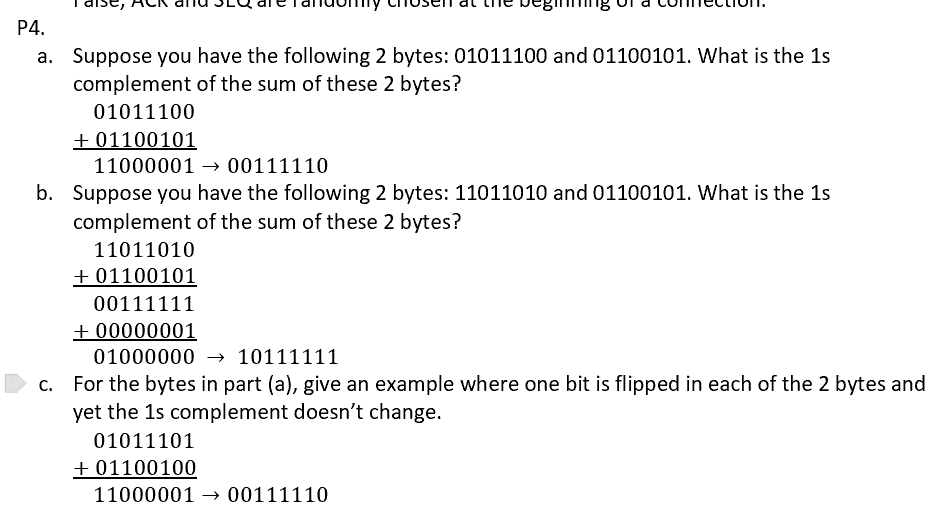
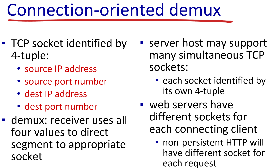
c. Suppose Host A is sending Host B a large file over a TCP connection. The number of unacknowledged bytes that A sends cannot exceed the size of the receive buffer. **True**

d. Suppose Host A is sending a large file to Host B over a TCP connection. If the sequence number for a segment of this connection is m, then the sequence number for the subsequent segment will necessarily be . **False**

e. The TCP segment has a field in its header for rwnd. **True**

f. Suppose that the last SampleRTT in a TCP connection is equal to 1 sec. The current value of TimeoutInterval for the connection will necessarily be ≥ 1 sec. **False**

g. Suppose Host A sends one segment with sequence number 38 and 4 bytes of data over a TCP connection to Host B. In this same segment the acknowledgment number is necessarily 42. **False**



|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Quiz 1  Store-and-forward transmission provides aid in which of the following switching approach?  A. Circuit switching  B. Packet Switching  C. Both (a) and (b) are correct  D. Neither of the options is correct  In which of the approach for moving the data through a network, the resources needed for the link between two end systems are 'reserved' for the duration of the communication session?  A. Circuit switching  B. Packet Switching  C. Both (a) and (b) are correct  D. Neither of the options is correct  Which of the tool is used for sniffing the packet over the internet?  A. Minesweeper  B. Skype  C. Wireshark  D. Adobe reader  The term defined for the time or duration wasted during idle dedicated circuits in circuit switching is referred to as:  A. Silent period  B. Unassigned slot  C. Dead circuit  D. Wasted frame  Which of the following layer is NOT part of the TCP/IP model?  A. Session layer  B. Application layer  C. Network layer  D. Transport layer  A compromised network device which can be controlled and leveraged by cyber attackers for spam distribution or distributed Denial-of-service?  A. Botnet  B. Virus  C. Worms  D. Command-and-control server  Which of the following type of delay can be referred to in the scenario where a link experiences heavy traffic and the next packets in line to enter the link have to experience a wait before being transmitted.  A. Queuing Delay  B. Transmission delay  C. Propagation delay  D. Instantaneous delay  Which of the following is used to overcome the stateless design of HTTP protocol and ensure stateful session?  A. Saved logins  B. Cookie  C. Browser History  D. Digital certificate  Wireless LAN access/WiFi is based on which IEEE specification?  A. IEEE 802.3  B. IEEE 802.5  C. IEEE 802.11  D. IEEE 802.2  Match the following   |  |  | | --- | --- | | A. Frame | 1. Application layer - B | | B. Message | 2. Transport layer - D | | C. Datagram | 3. Network layer - C | | D. Segment | 4. Link Layer - A | | Quiz 2  Full form of HTTP protocol:  A. Hypertext Transfer Protocol  B. Hyperlinked Transfer protocol  C. Heavy data transfer protocol  D. none of the option  DNS caching is an important feature of DNS in order to \_\_\_\_\_\_\_\_\_  A. Improve the delay performance  B. Reduce the number of DNS queries  C. Both of the options a and b are correct  D. None of these  SMTP or simple mail transfer protocol by default runs on which protocol and service:  A. port 25, UDP  B. port 161, TCP  C. port 25, TCP  D. port 80, UDP  Which of the term is used to denote the time taken by a network packet to travel from client to server and then back to a client?  A. Throughput  B. Transmission Delay  C. Round-trip time  D. Propagation Delay  In a network application, the software interface which is responsible for the process of sending and receiving messages is known as:  A. HTTP  B. UDP  C. Socket  D. TCP  For major video streaming companies like Youtube, Netflix, etc., the major problem of maintaining a single data center represents a single point of failure. To deal with this issue, which of the technology is used:  A. Peer to peer networks  B. Content Distribution Networks  C. DNS servers  D. POP3 servers  In a peer-to-peer communication, it is important for clients to have a connectivity with a common server in order to communicate with each other?  True  False  Which of the following are the classes of DNS servers architecture:  1. Root DNS  2. Top-Level domain DNS  3. Authoritative DNS  A. Option 1 and 2 only  B. Option 1 and 3 only  C. All of the options (1,2 and 3)  D. Only option 1  Which of the following options represents the correct fields present in a four-tuple DNS Resource record?  A. No. of hosts connected, Value, Type, TTL  B. Name, record Expiry date, Type, TTL  C. Value, TTL, Name, renewal date  D. Name, Value, Type, TTL |
| We are sending a 30 Mb file from a source host to a destination host. Suppose the message sent consists of the entire file. All links in the path between source and destination have a transmission rate of 10 Mbps. Assume that the propagation speed of each link is 2 \* 108 meters/sec, and the distance between source and destination is 10,000 km.  Initially, suppose there is only one link between source and destination. What is transmission delay?  Referring to the above question, what is the end-to-end delay (transmission delay plus propagation delay)?  Referring to the above question, how many bits will the source have transmitted when the first bit arrives at the destination?  Now, suppose there are two links between source and destination, with one router connecting the two links. Each link is 5,000 km long. Suppose processing delay is negligible and there is no congestion, so that the message is transmitted onto the second link as soon as the router receives the entire message. What is the end-to-end delay?  Now, suppose there is only one link between source and destination, and there are 10 TDM channels in the link. The file is sent over one of the channels. What is the end-to-end delay?  Now, suppose there is only one link between source and destination, and there are 10 FDM channels in the link. The file is sent over one of the channels. What is the end-to-end delay?  See above. | |