Name : Sumit Kumar Yadav

Roll No. : 18CS30042

Answer 1:

TCP uses selective repeat for flow control because, when packets are lost due to congestion, the protocols do not require the sender to retransmit every unacknowledged packet sent by the sender. The sender just retransmits the oldest unacknowledged packet.

Answer 2:

“SYN Flood” attack on TCP connections is a form of denial-of-service attack in which an attacker rapidly initiates a connection to a server without finalizing the connection. The server has to spend resources and waiting for half-opened connections, which can consume enough resources to make the system unresponsive to legitimate traffic.

Also, we can say that a vulnerability with implementing the three-way handshake is that the listening process must remember its sequence number as soon it responds withits own SYNsegment. This means that a malicious sender can tie up resources ona host by sending a stream of SYNsegments and never following through to complete the connection and it crippled many web servers in the 1990s.

One way to resisting this attack is to use SYN cookies. Instead of remembering the sequence number, a host chooses acryptographically generated sequence number and puts it on the outgoing segment, and forgets it.

Answer 3:

No, it is not safe to use this 16-bit sequence number field for a sliding window based flow control algorithm. This is because, in our case when we calculate BDP we get,

BDP = Bandwidth*Delay= 100 Mb

Therefore for each segment is of 1 byte, total no. of segments= BDP/1 byte= 10000000(approx). But our sequence no. range is only 65536(2^16). Therefore, it is unsafe to use 16 bit sequence numbers since we’ll run out of unique sequence numbers very soon

Answer 4:

Silly Window Syndrome of TCP is a problem that arises due to poor implementation of TCP. It degrades the TCP performance and makes the data transmission extremely inefficient. The problem is called so because:

(i) It causes the sender window size to shrink to a silly value.

(ii) The window size shrinks to such an extent where the data being transmitted is smaller than TCP Header.

It occurs mainly due to these following reason:

a. sender window transmitting one byte of data repeatedly.

b.receiver window accepting one byte of data repeatedly.

Clark's solution for the problem,

(i)receiver should not send a window update for 1 byte.

(ii)receiver should wait until it has a decent amount of space available.

(iii)receiver should then advertise that window size to the sender.

Answer 5:

Roll number: 18CS30042

Therefore, alpha=(1+8+3+19+3+4+2)mod(5)/10+1/2

Alpha=40mod5/10+1/2

Alpha=0+1/2

Finally, **Alpha=1/2**

And beta=alpha/2

Beta=1/4

SRTT1=550ms

RTTVAR1=412.5ms

RTO1=1sec

SRTT2=1025 ms

RTTVAR2=459.375ms

RTO2=1sec

Answer 6:

(a) False, Ordinary implementations of TCP does not uses Selective Acknowledgement (SACK) to request for missing segments. Also, One can include the SACK option in the Option parameter of the TCP Header. This allows the sender only specific segments to the receiver.

(b) True, The Maximum Segment Size(MSS) for a TCP connection is often set to about 1500 bytes in practice.

(c) False, During the Slow Start phase, the CWnd parameter in TCP Tahoe increases at an exponential rate not in extremely slow rate.

(d) True, The receiver waits for data on which to piggyback an acknowledgement, and the sender waits on the acknowledgement to send more data, thus causing a temporary deadlock.

(e) False, The URG flag has higher priority than PSH flag, because it is used to send the data on a priority basis to the application layer. When URG is set to 1, the “urgent” data is send directly to application layer while bypassing the buffer. This confirms the higher priority of URG flag