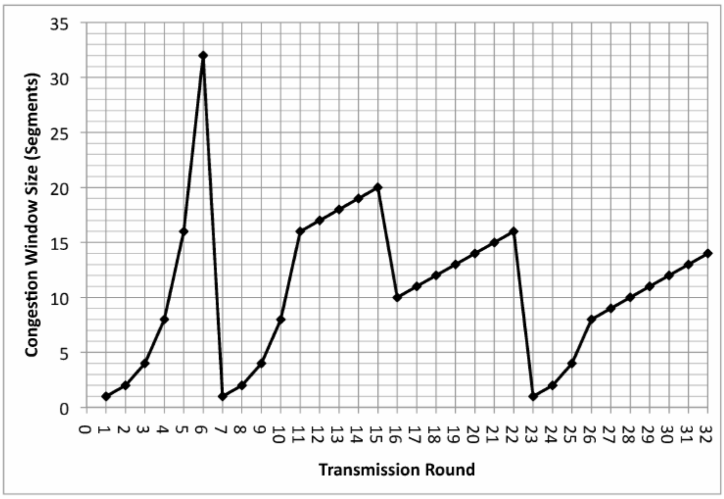
Department of Computer Science & Engineering
Indian Institute of Technology, Guwahati
End-semester Examination

Subject : CS341 Computer Networks **Full Marks :** 70
Date of Examination : 24/11/2022 *Attempt all questions* **Time** : 3 hours

1. The Transmission Control Protocol uses a method called congestion control to regulate the traffic entering the network. The behaviour of TCP congestion control can be represented as a graph in which the x-axis indicates the time, and the y-axis indicates congestion window size. Please use the graph shown below to the answer the following questions. Note that the graph does not explicitly show timeouts, but you should be able to figure out when timeouts happened based on the events shown. 12 marks



(a) **Slow Start:** give two reasons why slow start is used, and explain why it does a better job than congestion avoidance for that function. 2 marks

(b) **Slow Start:** identify the intervals of time when TCP slow start is operating. For each interval, identify which of the above reasons apply and do not apply and explain why. 2 marks

(c) **Congestion Avoidance:** identify the intervals of time when TCP congestion avoidance is operating. Why should congestion avoidance be used instead of slow start during these intervals? Please clearly identify one specific reason. 2 marks

(d) **Fast Retransmission:** identify the intervals of time when TCP fast retransmission is used. Please explain what fast retransmission does and how it is triggered. 2 marks

(e) **Fast Recovery:** identify the intervals of time when TCP fast recovery is operating. What does fast recovery do and explain why is it beneficial. 2 marks

(f) **Lack of fast recovery:** identify the interval(s) of time when fast recovery could have happened, but did not. Identify one specific example of a circumstance that may prevent fast recovery from happening. 2 marks

Ans:

a) Slow start is used because:

i) When a flow starts, it has no idea of the current network situation. In case network is not congested, slow start very quickly ramps up to achieve the optimum throughput

ii) In case the network is already congested, slow start inserts very few packets.

iii) It helps to achieve fairness among competing TCP flows and helps new flows to acquire fair share of the network bandwidth

As congestion avoidance increases cwnd linearly, if initialized by 1 MSS, it takes lot more time to ramp up to the optimum throughput.

b)1-6 (reason i as the flow just started), 7-11 (reason ii as the flow experienced congestion), 23-26 (reason ii as the flow experienced congestion)

c) 11-15, 16-22, 26-32. As the throughput has reached to the point where last congestion was experienced, TCP should be careful while injecting more packets. So, instead of exponential increase, linear increment of cwnd is preferable.

d) 16 (cwnd is reduced and then retransmition happens)

In case of Fast Retransmission, 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. After retransmission, the sender continues normal data transmission. That means TCP does not wait for the other end to acknowledge the retranmission.

e) 16-22

Fast Recovery is a packet loss recovery technique. When there is a packet loss detected, the TCP sender does 4 things: Reduces the cwnd by 50%, Reduces the ssthresh value by 50% of cwnd, Retransmit the lost packet, Enters the Fast Recovery phase. The first recovery phase comprises of two parts: The half window of silence, Maintain the inflight=cwnd until a new ACK arrives at the sender side.

f) 5-7. In case the duplicate ACKs are lost, sender will experience timeout and go to slow start

2. Assuming TCP receives a large amount of data from an application, it starts slow start phase with 1 KB segment size. The RTT for the destination is 1 sec, and the retransmission timeout is set to 1 RTT. Assume that the edge router has a token bucket to limit the burstiness of traffics. The token bucket has the maximum token capacity of 10 KB, token filling rate is 2 KB/s, and the outgoing link capacity is 10 KB/s. 5 marks

- **(a) Show the token bucket residue and the number of outgoing packets from the edge router for 1st to 7th RTT.** 3 marks
- **(b) What is the maximum throughput the host will achieve within 7th RTT? What is the average throughput the host will achieve within 7th RTT?** 2 marks

Ans:

a)

During RTT	TCP cwnd	Bucket residue (at the beginning of current RTT)	# outgoing packets
1	1	10 (initial amount)	1
2	2	10 (1 consumed and 2 new inflow in previous RTT, but cannot exceed the capacity 10)	2
3	4	10 (2 consumed and 2 new inflow in previous RTT)	4
4	8	8 (4 consumed and 2 new inflow in previous RTT)	8
5	16	2 (8 consumed and 2 new inflow in previous RTT)	2 (14 packets dropped by edge router)
6	1 (timeout)	2 (2 consumed and 2 new inflow in previous RTT)	1
7	2	3 (1 consumed and 2 new inflow in previous RTT)	2

Alternatively, if it is assumed that the bucket is empty initially, the solution will be:

During RTT	TCP cwnd	Bucket residue (at the beginning of current RTT)	# outgoing packets
1	1	0 (initial amount)	0
2	1 (timeout)	2 (2 new inflow in previous RTT)	1
3	2	3 (1 consumed and 2 new inflow in previous RTT)	2
4	4	3 (2 consumed and 2 new inflow in previous RTT)	3 (1 packet dropped by edge router)
5	1 (timeout)	2 (3 consumed and 2 new inflow in previous RTT)	1
6	2	3 (1 consumed and 2 new inflow in previous RTT)	2
7	4	3 (2 consumed and 2 new inflow in previous RTT)	3 (1 packet dropped by edge router)

b) In this case, among all the assumptions about the initial condition of the token bucket, only the first assumption needs to be considered as it gives the maximum achievable throughput. No other assumptions will be considered.
Maximum throughput is 8 KBps. Average throughput: 20/7 = 2.85 KBps.

3. Consider the configuration of a token bucket and a leaky bucket for network traffic shaping. 5 marks

(a) Give the expression for *S*, the maximum output burst length of the token bucket assuming input at the required rate is available. 1 mark

(b) Give the expression for *S'*, the maximum output burst length of the leaky bucket. 1 mark

(c) Assume that the token bucket is full of tokens and the leaky bucket is empty and a burst of input of length *S* arrives at *M* bytes / second. What should be the value of time of burst (*K)* so that there is no overflow (and therefore data loss) at the leaky bucket? 2 marks

(d) After this burst of length *S* at *M* bytes / second, how much time must elapse (*z*) before another burst of length *S* at *M* bytes / second can arrive? 1 mark

Given the following values: *M* = 25 MB/sec, *C* = 250KB, *r* = 2 MB / sec, *N* = 10 MB /sec., calculate *K* and *z*

Ans:

Following information are given. (though not explicitly, as they are implied)
Leaky bucket capacity, token bucket capacity are same as C = 250 KB = 0.25 MB
Token filling rate r = 2 MB/s
Incoming data rate M for token bucket= 25 MB/s
Outgoing rate of leaky bucket N = 10 MB/s
A token bucket and a leaky bucket is installed in series (output of the token bucket goes to the input of the leaky bucket) to shape the input traffic.

a. Burst length S = C/(M-r) sec
b. No burst traffic from leaky bucket output
c. Incoming burst for leaky bucket is the burst output form token bucket which is M = 25 MB/s. Therefore, leaky bucket filling rate is 25-10 (outgoing rate of leaky bucket) = 15 MB/s. Therefore, allowed the burst length K = 0.25/15 = 0.0166 sec
d. To allow the same burst length, the leaky bucket must be empty first.

   Time to become leaky bucket empty: z= 0.25/10 = 0.025 sec

4. Assume that an organization has been assigned the 196.35.1.0/24 network address. The organization decides to create subnets (each will support at least 20 hosts). 6 marks

- **a) Specify the length of subnet address that will allow creation of at least 20 hosts in each subnet.** 1 mark
- **b) What is the maximum number of hosts that can be supported on one subnet?** 1 mark
- **c) What is the maximum number of subnets?** 1 mark
- **d) Write the subnet address in dotted decimal notation.** 2 marks
- **e) What is the broadcast address of subnet 196.35.1.192?** 1 mark

Ans:

a) To accommodate 20 hosts, we need at least 5 bit host-ID in each subnets.
Therefore, the subnet length is 8-5 = 3.

b) 2^5 -2 = 32-2 = 30 (1st addr to denote the subnet and last one to denote broadcast addr)

c) Though possible number of subnets are 2^3 = 8, but the first one and the last one are not used to avoid ambiguity. The destination address 196.35.1.0 will simultaneously indicate the network 196.35.1.0/24 as well as the subnet 196.35.1.0/27. The destination address 196.35.1.255 will simultaneously indicate the broadcast address of network 196.35.1.0/24 as well as the subnet 196.35.1.224/27.

d) The six subnet addresses are (excluding the striked ones): ~~196.35.1.0/27~~, 196.35.1.32/27, 196.35.1.64/27, 196.35.1.96/27, 196.35.1.128/27, 196.35.1.160/27, 196.35.1.192/27, ~~196.35.1.224/27~~

e) 196.35.1.223

5. Suppose a router has built up the routing table as shown in the table below. 5 marks

Subnet	Subnet mask	Interface
128.96.39.0	255.255.255.128	a
128.96.39.128	255.255.255.128	b
128.96.40.0	255.255.255.128	c
192.4.153.0	255.255.255.192	d
Default		e

Indicate the router does when it receives IP packets with the following destination address.

- **a) 128.96.39.10** 1 mark
- **b) 128. 96.40.12** 1 mark
- **c) 128.96.40.151** 1 mark
- **d) 192.4.153.17** 1 mark
- **e) 192.4.153.90** 1 mark

Ans: Apply each subnet mask one by one on the destination address. If the prefix matches with the corresponding subnet column, then use that corresponding outgoing interface. (In the given table there is always a unique match.)

(a) Applying the subnet mask 255.255.255.128, we get 128.96.39.0. Use interface ‘a’ as the next hop.

(b) Applying subnet mask 255.255.255.128, we get 128.96.40.0. Use interface ‘c’ as the next hop.

(c) All subnet masks give 128.96.40.128 as the prefix. Since there is no match, use the default entry. Next hop is to interface ‘e’.

(d) Next hop is interface ‘d’.

(e) None of the subnet number entries match, hence use default router to interface ‘e’.

6. 6 marks

(a) Is there any ARP reply against gratuitous ARP? Explain in details including its usage (if any) 2 marks

(b) Why is the hardware MAC address present in both the Ethernet header and the ARP packet (request and reply)? 2 marks

(c) Having ARP table entries time out after 10-15 minutes is an attempt at a reasonable compromise. Describe the problems that can occur if the timeout value is too small or too large. 2 marks

Ans:

a) There is no reply against Gratuitous ARP. A GARP is an ARP broadcast in which the source and destination MAC addresses are the same. It is used primarily by a host to inform the network about its IP address. They can help detect IP conflicts. When a machine receives an ARP request containing a source IP that matches its own, then it knows there is an IP conflict. They assist in the updating of other machines' ARP table. Clustering solutions utilize this when they move an IP from one NIC to another, or from one machine to another. Other machines maintain an ARP table that contains the MAC associated with an IP. When the cluster needs to move the IP to a different NIC, be it on the same machine or a different one, it reconfigures the NICs appropriately then broadcasts a gratuitous ARP reply to inform the neighboring machines about the change in MAC for the IP. Machines receiving the ARP packet then update their ARP tables with the new MAC. They inform switches of the MAC address of the machine on a given switch port, so that the switch knows that it should transmit packets sent to that MAC address on that switch port. Every time an IP interface or link goes up, the driver for that interface will typically send a gratuitous ARP to preload the ARP tables of all other local hosts. Thus, a gratuitous ARP will tell us that that host just has had a link up event, such as a link bounce, a machine just being rebooted or the user/sysadmin on that host just configuring the interface up. If we see multiple gratuitous ARPs from the same host frequently, it can be an indication of bad Ethernet hardware/cabling resulting in frequent link bounces.

b) The MAC of ethernet header is for frame delivery whereas the MAC addresses of the ARP messages are used to create/update ARP entries. The Ethernet header is processed by the data link driver and removed from the packet. When the ARP protocol gets the packet, it needs to know the hardware and protocol addresses in order to update the table. That is why the hardware MAC address is present in both the Ethernet header and the ARP packet.

c) If the timeout value is too small, we clutter the network with unnecessary re-requests, and halt transmission until the re-request is answered. When a host’s Ethernet address changes, eg because of a card replacement, then that host is unreachable to others that still have the old Ethernet address in their ARP cache. 10-15 minutes is a plausible minimal amount of time required to shut down a host, swap its Ethernet card, and reboot. If the timeout value is too large, it may result in the cache keeping the old data link interface addresses even if the network interface has failed and has been replaced. This would result in wrong addresses being used while transmission and this transmission would receive no acknowledgment, so the transmission will be repeated.

7. Consider a network of N nodes and L links. A node wishes to flood a packet to the entire network. Each node forwards the packet to all its neighbors except the incoming node after it receives the packet for the first time, and will not forward after it sees the packet for twice or more. Prove that the total number of transmissions M involved in flooding the packet satisfies. 3 marks

(a) $M \geq L$. 1 mark

(b) $M < 2L$. 2 marks

Give adequate justification.

Ans:

a) For each node, all the links the node is attached to are used at least one. One link for incoming, and rest other links for outgoing. Clearly, M>=L

b) In the worst scenario, the network is a complete graph with L = n(n-1)/2. The 1st node floods the packet to all (n-1) links. Receiving the packet, all remaining n-1 nodes simultaneously forwards the packet to (n-2) links except the incoming link. As a result, the number of transmission becomes (n-1)(n-2). By this time, all nodes have received 2 copies of the packet so no more forwarding. Clearly, (n-1)(n-2) < n(n-1) < 2L

8. 5 marks

(a) Why is it important for protocols using the service of Ethernet to have a length field in their header, indicating how long the payload is? 1 mark

(b) Suppose we want to transmit the message 1011 0010 0100 1011 and protect it from errors using the RC8 polynomial $x^8 + x^2 + x + 1$.
i) Determine the message that should be transmitted. 2 mark
ii) Suppose the leftmost bit of the message is inverted due to noise on the transmission link. What is the result of the receiver's CRC calculation? How does the receiver know that an error has occurred? 2 mark

Ans:

a) As Ehternet frame uses padding (if required), the entire payload may not be upper layer data. Accordingly, upper layers need to mention the correct length in the length field

b) Take the message 1011 0010 0100 1011, append 8 zeros, and divide by
10000 0111 (x8 + x2 + x1 + 1)

i) The remainder is 1001 0011. We transmit the original message with this remainder appended, resulting in 1011 0010 0100 0011 1001 0011.

ii) Inverting the first bit gives 0011 0010 0100 1011 1001 0011. Dividing by 1 0000 0111 (x8 + x2 + x1 + 1) gives a remainder of 1011 0110.

9. There are two popular technologies for Local Area Network (LAN) design, namely IEEE 802.3 Ethernet and IEEE 802.11 WiFi. Use your knowledge of these technologies to answer the following questions. 7 marks

(a) What Data link Layer service model is provided by each of these LAN technologies? How are they similar? How are they different? 1+1+1 = 3 marks

(b) List three similarities about LLC frames in Ethernet and WiFi. 1 mark

(c) Which of these two LAN technologies has the higher bit error rate, and why? 1 mark

(d) Which LAN technology provides better support for mobile users, and how? 1 mark

(e) List and explain any two other features of WiFi technology that are not available (or even possible) in Ethernet LANs. 1 mark

Ans:

a)

- connection-less DLL service model for both
- Ethernet is unacknowledged
- WiFi is acknowledged

b)

- uses 48-bit MAC addresses for source and destination
- uses CRC-32 checksum for error detection in trailer of frame
- supports variable size frames (length field)
- transmits on a shared broadcast channel using a CSMA protocol

c)

WiFi: unguided transmission over ‘‘air interface’’, which is subject to a lot of ambient interference and noise
- usually half-duplex, with multi-path fading, and limited RF power

d)

WiFi: wireless RF signals propagate omni-directionally; allows roaming
- devices automatically associate with ‘‘best’’ AP signal strength
- multiple APs can be configured as an extended service set (ESSID)
- example: AirUC (or AirUC-secure)

e)

```
- can adapt data rate based on signal quality (1,2,5.5,11 Mbps)
- ad hoc mode to support mobile computing without Internet access
- RTS/CTS protocol for handling hidden node problem
- MAC-layer retransmission of unacknowledged frames
- three types of frames: Management, Control, Data
- backwards compatibility with earlier IEEE 802.11 standards
- polling mode to support power-saving operation
```

10. Consider 12 stations (hosts) attached to a 10 Mbps Ethernet. The throughput of the Ethernet is the total rate at which data is delivered to all the hosts. Assume all frames are addressed to individual stations, not to group or broadcast addresses. What is the maximum possible throughput if. . . 6 marks

(a) .....all hosts are connected to a single hub (repeater)? 2 marks

(b). . . each host is connected via a half-duplex interface to a single Ethernet switch? 2 marks

(c) . . . each host is connected via a full-duplex interface to a single Ethernet switch? 2 marks

Ans:

Assuming no time lost for contention resolve and no packet collision. All nodes are having packets to send all the time.

a) Only one node can transmit at a time. However, it can transmit with 10Mbps.

b) Communication happens between two parties. One of them transmits while the other can only receive because of half-duplex nature. Maximum 6 nodes can transmit simultaneously. Each are connected to switch by 10 Mbps ethernet cable. Therefore, throughput is 60 Mbps

c) Because of full-duplex nature, all nodes can simultaneously transmit and receive. Each are connected to switch by 10 Mbps ethernet cable. As a result, max throughput will be 120 Mbps.

11. Describe into detail the multiple access scheme used in the DCF function of IEEE 802.11 presenting in particular: 8 marks

a) How the hidden terminal problem is avoided; 1 mark

b) What the exposed terminal problem is; 1 mark

c) given a graph G(N,V) representing network topology and a transmission (i,j), indicate which transmissions are blocked by the virtual carrier sense and which could be possible without collisions; 1+2=3 marks

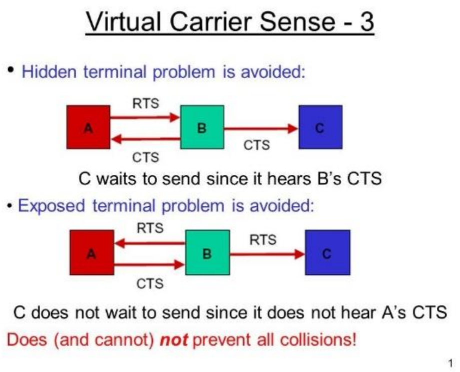
d) why physical carrier sense is used in addition to the virtual carrier sense; 1 mark

e) Describe the use of the address fields in the MAC frame. 2 marks

Ans:

a) Multiple Access with Collision Avoidance (MACA) can be used to avoid the Hidden Terminal Problem. MACA protocol uses RTS and CTS to avoid hidden terminal problem. In hidden terminal problem two nodes try to contact same node at a same time which can create collision. To combat this if two nodes send RTS to same node then the node which receives CTS will send the data not the other one which will avoid the collision.

b) Exposed Terminal Problem arises when a transmitting station is prevented from sending frames due to interference with another transmitting station.



Virtual Carrier Sense - 3

- Hidden terminal problem is avoided:

C waits to send since it hears B's CTS

- Exposed terminal problem is avoided:

C does not wait to send since it does not hear A's CTS

Does (and cannot) ***not*** prevent all collisions!

1

c) In the graph G(N,V), suppose n1 wants to transmit a data packet to n2. Let the 1-hop neighbor of n1 is denoted by nbr(n1) and the 1-hop neighbor of n2 is denoted by nbr(n2).
In that case, the transmissions of node set N' given by (nbr(n1) U nbr(n2)) are blocked by NAV. Among these nodes, N'' = (nbr(n1) – nbr(n2)) denotes set of nodes which are 1 hop neighbors of n1, but not in 1 hop distance of n2. The nodes of N'' could have transmitted to any node outside of nbr(n1), but is blocked by NAV. Similarly, N''' = (nbr(n2) – nbr(n1)) could have received data from any node outside nbr(n2), but is blocked by NAV.

d) There are four address fields in the 802.11 MAC frame. The number and meaning of the 48-bit address fields depend on context. The transmitter address and receiver address are the MAC addresses of stations joined to the BSS that are transmitting and receiving frames over the wireless LAN. The service set ID (SSID) identifies the wireless LAN over which a frame is transmitted. For an IBSS, the SSID is a random number generated at the time the network is formed. For a wireless LAN that is part of a larger configuration the SSID identifies the BSS over which the frame is transmitted; specifically, the SSID is the MAC-level address of the AP for this BSS. Finally, the source address and destination address are the MAC addresses of stations, wireless or otherwise, that are the ultimate source and destination of this frame. The source address may be identical to the transmitter address and the destination address may be identical to the receiver address.

12. In an 802.11 wireless network, station A sends one non-fragmented data frame station B. What would be the value of the Duration field (in microseconds) that needs be set for the NAV period in each of the following frames: RTS, CTS, Data, and ACK? 1 + 1 + 1 + 1 = 4 marks

Assumptions:

(a) The transmission time for RTS, CTS, and ACK is 8 µs each.

(b) The transmission time for the data frame is 50 µs.

(c) The SIFS duration is set to 1 µs.

(d) Propagation time may be ignored.

(e) Each frame needs to set the duration of NAV for the rest of time the medium needs to be reserved to complete the transaction.

Ans:

In RTS: SIFS + T(CTS) + SIFS + T(DATA) + SIFS + T(ACK) = 1+8+1+50+1+8 = 69
In CTS: SIFS + T(DATA) + SIFS + T(ACK) = 1+50+1+8 = 60
In DATA: SIFS + T(ACK) = 1+8 = 9
In ACK: 0

13. 3 marks

(a) Given the following three 8 chip spreading codes (CDMA), calculate the bits sent by senders A, B and C with the combined transmitted chips (-1, -1, 3, 1, 1, -3, 1, 1). Ensure that in your answer, you include all the steps of your calculation. 2 marks

A_k = (+1,+1,-1,-1,+1,+1,-1,-1); B_k = (+1,-1,+1,-1,+1,-1,+1,-1); C_k = (+1,-1,-1,+1,-1,+1,+1,-1)

(b) A new device, D starts transmitting data, with spreading code D_k =(+1,-1,-1,+1,+1,-1,-1,+1). If A and D want to send a single data bit whose value is 0, whilst B and C send 1 valued single data bits, what would be the value of the combined transmitted chips received by the Base Station? 1 mark

Ans:

a) Though third symbol of A_k is unintentionally incorrectly printed without sign, from the orthogonal property of the codes, it can be easily derived as -1 without any ambiguity. The combined chip is **(-1, -1, 3, -1, 1, -3, 1, 1).** But due to a transmission error in the fourth symbol of the combined chip, the transmitted chip is **(-1, -1, 3, 1, 1, -3, 1, 1).** As the chip combination (A'_k, B_k, C'_k) yields the closest chip sequence **(-1, -1, 3, -1, 1, -3, 1, 1)** to the received erroneous chip sequence is **(-1, -1, 3, 1, 1, -3, 1, 1)** with only one symbol error, the chip combination (A'_k, B_k, C'_k) is the answer which implies 0,1, and 0 sent by A, B, and C.

Partial marks will be given if one has correctly pointed out any of the errors and correctly narrated the same.

b)

A'= (-1,	-1,	+1,	+1,	-1,	-1,	+1,	+1)
B= (+1,	-1,	+1,	-1,	+1,	-1,	+1,	-1)
C= (+1,	-1,	-1,	+1,	-1,	+1,	+1,	-1)
D'= (-1,	+1,	+1,	-1,	-1,	+1,	+1,	-1)
BS =(0,	-2,	2,	0,	-2,	0,	4,	-2)

---END---