**Computer Networks**

End Semester Examination - **SOLUTIONS**

**All questions of a Serial Number need to be done together in one place. Any assumption needs to be carefully stated. Do Question 8 in a separate sheet and attach it to the main answer script.**

**Answer all Questions**

Time: 3 hrs. Max. Marks: TBD

**Question 1: The following questions have only ONE correct answer. Choose the most appropriate option. [10 x 1 = 10]**

1. One of the header fields in an IP datagram is the Time to Live (TTL) field. Which of the following statements best explains the need for this field?
2. It can be used to prioritize packets
3. It can be used to reduce delays
4. It can be used to optimize throughput
5. It can be used to prevent packet looping

**Answer: (D)**

Time to Live can be thought as an upper bound on the time that an IP datagram can exist in the network. The purpose of the TTL field is to avoid a situation in which an undeliverable datagram keeps circulating.

1. Which one of the following is not a client server application?
2. Internet chat
3. Web browsing
4. E-mail
5. Ping

**Answer: (D)**

Ping is not a client server application. Ping is a computer network administration utility used to test the reachability of a host on an Internet Protocol (IP). In ping, there is no server that provides a service.

1. In the IPv4 addressing format, the number of networks allowed under Class C addresses is
2. 214
3. 27
4. 221
5. 224

**Answer: (C)**

In class C, 8 bits are reserved for Host ID and 24 bits are reserved for Network ID. Out of these 24 Network ID bits, the leading 3 bits are fixed as 110; remaining 21 bits can be used for different networks.

1. Which of the following transport layer protocols is used to support electronic mail?
2. SMTP
3. IP
4. TCP
5. UDP

**Answer: (C)**

E-mail uses SMTP as *application* layer protocol. SMTP uses TCP as ***transport*** layer protocol.

1. Which one of the following protocols is NOT used to resolve one form of address to another one?
2. DNS
3. ARP
4. DHCP
5. RARP

**Answer: (C)**

DHCP is used to assign IP dynamically. All others are used to convert one address to other.

1. In one of the pairs of protocols given below, both the protocols can use multiple TCP connections between the same client and the server. Which one is that?
2. HTTP, FTP
3. HTTP, Telnet
4. FTP, SMTP
5. HTTP, SMTP

**Answer: (A)**

HTTP may use different TCP connection for different objects of a webpage if non-persistent connections are used. FTP uses two TCP connections, one for data and another control. Telnet and FTP can only use ONE connection at a time.

1. Which one of the following uses UDP as the transport protocol?
2. HTTP
3. Telnet
4. DNS
5. SMTP

**Answer: (C)**

DNS primarily uses User Datagram Protocol (UDP) on port number 53 to serve requests. DNS queries consist of a single UDP request from the client followed by a single UDP reply from the server.

1. What is the maximum size of data that the application layer can pass on to the TCP layer below?
2. Any size
3. 216 bytes-size of TCP header
4. 216 bytes
5. 1500 bytes

**Answer: (A)**

The default TCP Maximum Segment Size is 536. Where a host wishes to set the maximum segment size to a value other than the default, the maximum segment size is specified as a TCP option, initially in the TCP SYN packet during the TCP handshake. Because the maximum segment size parameter is controlled by a TCP option, a host can change the value in any later segment.

1. The address resolution protocol (ARP) is used for:
	1. Finding the IP address from the DNS
	2. Finding the IP address of the default gateway
	3. Finding the IP address that corresponds to a MAC address
	4. Finding the MAC address that corresponds to an IP address

**Answer: (D)**

Address Resolution Protocol (ARP) is a request and reply protocol used to find MAC address from IP address.

1. Packets of the same session may be routed through different paths in:
2. TCP, but not UDP
3. TCP and UDP
4. UDP, but not TCP
5. Neither TCP nor UDP

**Answer: (B)**

Packet is the Network layer Protocol Data Unit (PDU). TCP and UDP are Transport layer protocols. Packets of same session may be routed through different routes. Most networks don’t use static routing, but use some form of adaptive routing where the paths used to route two packets for same session may be different due to congestion on some link, or some other reason.

**Question 2: Answer the following questions. [10 x 2 = 20]**

1. Suppose computers A and B have IP addresses 10.105.1.113 and 10.105.1.91 respectively and they both use the same netmask N. Which of the values of N given below should NOT be used if A and B should belong to the same network?
	1. 255.255.255.0
	2. 255.255.255.128
	3. 255.255.255.192
	4. 255.255.255.224

**Answer: (D)**

The last octets of IP addresses of A and B are 113 (01110001) and 91 (01011011). The netmask in option (D) has first three bits set in last octet. If netmask has first 3 bits set, then these bits must be same in A and B, but that is not the case. In simple words, we can say option (D) is not a valid netmask because doing binary ‘&’ of it with addresses of A and B doesn’t give the same network address. It must be same address as A and B are on same network.

1. Consider different activities related to email.

m1: Send an email from a mail client to a mail server

m2: Download an email from mailbox server to a mail client

m3: Checking email in a web browser

From the list below, choose one application level protocol used for each of the activities m1, m2, and m3 mentioned above:

1. HTTP
2. SMTP
3. POP
4. IMAP
5. FTP

**Answer: m1 – SMTP; m2 – POP; m3 – HTTP**

Simple Mail Transfer Protocol (SMTP) is typically used by user clients for sending mails. Post Office Protocol (POP) is used by clients for receiving mails. Checking mails in web browser is a simple HTTP process.

1. For each of the use-cases below, indicate the transport layer protocol used:
	1. Real time multimedia
	2. File transfer
	3. DNS
	4. Email

**Answer: (A) UDP, (B) TCP, (C) UDP and (D) TCP**

TCP is connection oriented and UDP is connectionless, this makes TCP more reliable than UDP. But UDP is stateless (less overhead), that makes UDP is suitable for purposes where error checking and correction is less important than timely delivery.

For real time multimedia, timely delivery is more important than correctness –> UDP

For file transfer, correctness is necessary –> TCP

DNS, timely delivery is more important –> UDP

Email again same as file transfer –> TCP

1. An Internet Service Provider (ISP) has the following chunk of CIDR-based IP addresses available with it: 245.248.128.0/20. The ISP wants to give half of this chunk of addresses to Organization A, and a quarter to Organization B, while retaining the remaining with itself. Which of the following is a valid allocation of address to A and B?

(A) 245.248.136.0/21 and 245.248.128.0/22

(B) 245.248.128.0/21 and 245.248.128.0/22

(C) 245.248.132.0/22 and 245.248.132.0/21

(D) 245.248.136.0/24 and 245.248.132.0/21

**Answer: (A)**

Since routing prefix is 20, the ISP has 2(32-20) or 212 addresses. Out of these 212 addresses, half (or 211) addresses have to be given to organization A and quarter (210) addresses have to be given to organization B. So routing prefix for organization A will be 21. For B, it will be 22. If we see all options given in question, only options (A) and (B) are left as only these options have same number of routing prefixes. Now we need to choose from option (A) and (B).

To assign addresses to organization A, ISP needs to take first 20 bits from 245.248.128.0 and fix the 21st bit as 0 or 1. Similarly, ISP needs to fix 21st and 22nd bits for organization B. If we take a closer look at the options (A) and (B), we can see the 21st and 22nd bits for organization B are considered as 0 in both options. So, 21st bit of organization A must be 1. Now take the first 20 bits from 245.248.128.0 and 21st bit as 1, we get addresses for organization A as 245.248.136.0/21.

1. Identify the correct order in which the following actions take place in an interaction between a web browser and a web server.

1. The web browser requests a webpage using HTTP.

2. The web browser establishes a TCP connection with the web server.

3. The web server sends the requested webpage using HTTP.

4. The web browser resolves the domain name using DNS.

**Answer: 4, 2, 1, 3**

The web browser first need to figure out IP address of site from URL using DNS, then establishes a TCP connection, typically at port 80. Once the TCP connection is established, the browser sends a HTTP request using GET. Finally web server responds with HTTP response.

1. Consider the following three statements about link state and distance vector routing protocols, for a large network with 500 network nodes and 4000 links.

[S1] The computational overhead in link state protocols is higher than in distance vector protocols.

[S2] A distance vector protocol (with split horizon) avoids persistent routing loops, but not a link state protocol.

[S3] After a topology change, a link state protocol will converge faster than a distance vector protocol.

Which one of the following is correct about S1, S2, and S3?

(A) S1, S2, and S3 are all true.

(B) S1, S2, and S3 are all false.

(C) S1 and S2 are true, but S3 is false.

(D) S1 and S3 are true, but S2 is false.

**Answer: (D)**

[S1] is clearly true as in Link State all nodes compute shortest path for whole network graph.

[S3] is also true as Distance Vector protocol has count to infinity problem and converges slower.

[S2] is false. In distance vector protocol, split horizon with poison reverse reduces the chance of forming loops and uses a maximum number of hops to counter the ‘count-to-infinity’ problem. These measures avoid the formation of routing loops in some, but not all, cases.

1. In Ethernet when Manchester encoding is used, is there a relation between the bit rate and the baud rate (Yes/No)?

If yes, suppose that the bit rate is **x** times the baud rate. What is the value of **x**?

**Answer: Yes, 0.5**

In Manchester encoding, the bitrate is half of the baud rate.

1. Indicate the OSI model layer in column B, which corresponds to each of the protocols mentioned in column A below:

*Column A* *Column B*

(P) SMTP (1) Application layer

(Q) BGP (2) Transport layer

(R) TCP (3) Data link layer

(S) PPP (4) Network layer

(5) Physical layer

**Answer: P – 1, Q – 4, R – 2, S – 3**

SMTP is an application layer protocol used for e-mail transmission.

TCP is a core transport layer protocol.

BGP is a network layer protocol backing the core routing decisions on the Internet

PPP is a data link layer protocol commonly used in establishing a direct connection between two networking nodes.

1. *Fill in the blank:* In a token ring network, the transmission speed is 107 bps and the propagation speed is 200 metres/µs. A 1-bit delay in this network is equivalent to \_\_\_\_\_\_\_\_\_\_ metres of cable.

**Answer: 20**

Transmission delay for 1 bit is t = 1/107 = 0.1 µs.

200 meters can be traveled in 1 µs. Therefore, in 0.1 µs, 20 meters can be traveled.

1. In a network of LANs connected by bridges, packets are sent from one LAN to another through intermediate bridges. Since more than one path may exist between two LANs, packets may have to be routed through multiple bridges. Why is the spanning tree algorithm used for bridge-routing?
	1. For shortest path routing between LANs
	2. For avoiding loops in the routing paths
	3. For fault tolerance
	4. For minimizing collisions

**Answer: (B)**

The main idea for using Spanning Trees is to avoid loops.

**Question 3: Answer the following questions.**

1. Determine the maximum length of the cable (in km) for transmitting data at a rate of 500 Mbps in an Ethernet LAN with frames of size 10,000 bits. Assume the signal speed in the cable to be 2,00,000 km/s. [2]

**Answer: 2 km**

Data should be transmitted at the rate of 500 Mbps.

Transmission Time = 2\*Propagation Time

=> 10000/(500\*1000000) = 2\*length/200000

=> length = 2 km (max)

1. Consider a token ring network with a length of 2 km having 10 stations including a monitoring station. The propagation speed of the signal is 2 x 108 m/s and the token transmission time is ignored. If each station is allowed to hold the token for 2 µsec, determine the minimum time for which the monitoring station should wait (in µsec) before assuming that the token is lost. [3]

**Answer: 28 micro secs.**

Length = 2 km

Propagation Speed v = 2\*108 m/s

Token Holding Time = 2 micro sec

Waiting time = length/speed + (#stations - 1)\*(token holding time) = 28 micro sec.

1. Consider a selective repeat sliding window protocol that uses a frame size of 1 KB to send data on a 1.5 Mbps link with a one-way latency of 50 msec. To achieve a link utilization of 60%, what is the minimum number of bits required to represent the sequence number field? [3]

**Answer: 5 bits**

Transmission delay = Frame Size/bandwidth = (1\*8\*10^3)/(1.5 \* 106) = 5.33 ms

Propagation delay = 50 ms

Efficiency = window size/(1+2a) = 0.6

a = Propagation delay/Transmission delay

So, window size = 11.856 (approx.)

Min. sequence number = 2\*window size = 23.712

Bits required in min. sequence number = log2(23.712) = 4.56

Ceiling(4.56) = 5

1. The message 11001001 is to be transmitted using the CRC polynomial x3 + 1 to protect it from errors. What is the message that should be transmitted? [2]

**Answer: 11001001011**

The polynomial x3+1 corresponds to divisor is 1001.

After dividing the given message 11001001 by 1001, we get the remainder as 011 which is the CRC. The transmitted data is, message + CRC which is 11001001 011.

**Question 4: Answer the following questions.**

1. Consider a LAN with four nodes S1, S2, S3 and S4. Time is divided into fixed-size slots, and a node can begin its transmission only at the beginning of a slot. A collision is said to have occurred if more than one node transmit in the same slot. The probabilities of generation of a frame in a time slot by S1, S2, S3 and S4 are 0.1, 0.2, 0.3 and 0.4, respectively. What is the probability of sending a frame in the first slot without any collision by any of these four stations? [3]

**Answer: 0.44**

The probability of sending a frame in the first slot without any collision by any of these four stations is sum of following 4 probabilities:

Probability that S1 sends a frame and no one else does +

Probability that S2 sends a frame and no one else does +

Probability that S3 sends a frame and no one else does +

Probability that S4 sends a frame and no one else does

= 0.1 \* (1 - 0.2) \* (1 - 0.3) \*(1 - 0.4) +

 (1 -0.1) \* 0.2 \* (1 - 0.3) \*(1 - 0.4) +

 (1 -0.1) \* (1 - 0.2) \* 0.3 \*(1 - 0.4) +

 (1 -0.1) \* (1 - 0.2) \* (1 - 0.3) \* 0.4

= 0.4404

1. Suppose that the stop-and-wait protocol is used on a link with a bit rate of 64 kilobits per second and 20 milliseconds propagation delay. Assume that the transmission time for the acknowledgment and the processing time at nodes are negligible. What should be the minimum frame size in bytes to achieve a link utilization of at least 50%? [3]

**Answer: 320**

Transmission or Link speed = 64 kb per sec

Propagation Delay = 20 millisec.

Since stop and wait is used, a packet is sent only when previous one is acknowledged.

Let x be size of packet, transmission time = x / 64 millisec.

Since utilization is at least 50%, minimum possible total time for one packet is twice of transmission delay, which means:

x/64 \* 2 = x/32

x/32 > x/64 + 2\*20

x/64 > 40

x > 2560 bits = 320 bytes

1. A sender uses the Stop-and-Wait ARQ protocol for reliable transmission of frames. Frames are of size 1000 bytes and the transmission rate at the sender is 80 Kbps (1Kbps = 1000 bits/second). Size of an acknowledgement is 100 bytes and the transmission rate at the receiver is 8 Kbps. The one-way propagation delay is 100 milliseconds. Assuming no frame is lost, calculate the sender throughput in bytes/second. [4]

**Answer: 2500**

Total time = Transmission-Time + 2\* Propagation-Delay + Ack-Time.

Trans. time = (1000\*8)/80\*1000 = 0.1 sec

2\*Prop-Delay = 2\*100ms = 0.2 sec

Ack-time = 100\*8/8\*1000 = 0.1 sec.

Total Time = 0.1 + 0.2 + 0.1 = 0.4 sec.

Throughput = ((L/B)/Total time) \* B,

L = data packet to be sent and

B = BW of sender.

Throughput = L/Total Time

 = 1000/0.4

 = 2500 bytes/sec.

**Question 5: Answer the following questions.**

1. Consider a network with five nodes, N1 to N5, as shown below:



1

The network uses a Distance Vector Routing protocol. Once the routes have stabilized, the distance vectors at different nodes are as following:

N1: (0, 1, 7, 8, 4)

N2: (1, 0, 6, 7, 3)

N3: (7, 6, 0, 2, 6)

N4: (8, 7, 2, 0, 4)

N5: (4, 3, 6, 4, 0)

Each distance vector is the distance of the best known path at that instance to nodes, N1 to N5, where the distance to itself is 0. Also, all links are symmetric and the cost is identical in both directions. In each round, all nodes exchange their distance vectors with their respective neighbors. Then all nodes update their distance vectors. In between two rounds, any change in cost of a link will cause the two incident nodes to change only that entry in their distance vectors.

* 1. The cost of link N2-N3 reduces to 2 in (both directions). After the next round of updates, what will be the new distance vector at node N3? [2]

**Answer: (3, 2, 0, 2, 5)**

In the next round, every node will send and receive distance vectors to and from neighbors, and update its distance vector.

N3 will receive (1, 0, 2, 7, 3) from N2 and it will update distances to N1 and N5 as 3 and 5 respectively.

* 1. After the update in the previous question, the link N1-N2 goes down. N2 will reflect this change immediately in its distance vector as cost, ∞. After the next round of update, what will be the cost to N1 in the distance vector of N3? [2]

**Answer: 10**

In the next round, N3 will receive distance from N2 to N1 as infinite. It will receive distance from N4 to N1 as 8. So it will update distance to N1 as 8 + 2.

1. Assume that source S and destination D are connected through two intermediate routers labeled R. Determine how many times each packet has to visit the network layer and the data link layer during a transmission from S to D. [3]

**Answer: Network layer – 4 times, data link layer – 2 times**

A router is a network layer device – so every packet goes through to the network layer of every intermediate router just once, before being forwarded. No. of times network layer is visited = 1 (n/w layer of S) + 2 (n/w layer of 2 Rs) + 1 (n/w layer of D) = 4 times.

In contrast, a packet moves through the data link layer twice for each intermediate router, once while being received, and once more while being forwarded. No. of times datalink layer is visited = 1 (d/l layer of S) + 2\*2 (d/l layers of 2 Rs) + 1 (d/l layer of D) = 6 times.

1. In an IPv4 datagram, the M bit is 0, the value of HLEN is 10, the value of total length is 400 and the fragment offset value is 300. State: [3]
2. The position of the datagram (first, last, or middle)
3. The sequence number of the first byte of the payload
4. The sequence number of the last byte of the payload

**Answer: (A) last position; (B) 2400; (C) 2759**

M = 0 indicates that this packet is the last packet among all fragments of original packet. It is given that HLEN field is 10. Header length is number of 32 bit words. So header length = 10 \* 4 = 40.

Also, given that total length = 400. Total length indicates total length of the packet including header. So, packet length excluding header = 400 - 40 = 360. Last byte address = 2400 + 360 - 1 = 2759 (Because numbering starts from 0).

**Question 6: Answer the following questions.**

1. An IP datagram of size 1000 bytes arrives at a router. The router has to forward this packet on a link whose MTU (maximum transmission unit) is 100 bytes. Assume that the size of the IP header is 20 bytes. Compute the number of fragments that the IP datagram will be divided into for transmission. [3]

**Answer: 13**

MTU = 100 bytes

Size of IP header = 20 bytes

So, size of data that can be transmitted in one fragment = 100 – 20 = 80 bytes

Size of data to be transmitted = Size of datagram – size of header = 1000 – 20 = 980 bytes

Now, we have a datagram of size 1000 bytes.

So, we need ceiling(980/80) = 13 fragments.

Thus, there will be 13 fragments of the datagram.

1. A computer on a 10Mbps network is regulated by a token bucket. The token bucket is filled at a rate of 2Mbps. It is initially filled to capacity with 16Megabits. What is the maximum duration for which the computer can transmit at the full 10Mbps? [3]

**Answer: 2 seconds**

New tokens are added at the rate of r bytes/sec which is 2Mbps in the given question.

Capacity of the token bucket (b) = 16 Mbits

Maximum possible transmission rate (M) = 10Mbps

So the maximum burst time = b/(M-r) = 16/(10-2) = 2 seconds

In the above formula, r is subtracted from M to calculate the maximum burst time. The reason for this subtraction is, new tokens are added at the rate of r while transmission happens at maximum transmission rate M.

1. The address of a class B host is to be split into subnets with a 6-bit subnet numbers. What is the maximum number of subnets and the maximum number of hosts in each subnet? [2]

**Answer: 62 subnets and 1022 hosts**

Maximum number of subnets = 26 – 2 = 62.

Note that 2 is subtracted from 26. The RFC 950 specification reserves the subnet values consisting of all zeros (see above) and all ones (broadcast), reducing the number of available subnets by two.

Maximum number of hosts is 210 – 2 = 1022.

2 is subtracted for the number of hosts also. The address with all bits as 1 is reserved as broadcast address and address with all host id bits as 0 is used as network address of subnet.

In general, the number of addresses usable for addressing specific hosts in each network is always 2N – 2 where N is the number of bits for host id.

1. How is a peer-to-peer network different from a client-server setup? State the average complexity of finding a record using a finger table, as implemented by the Chord protocol. [1+1]

**Answer:** A peer-to-peer network is different in the following ways:

(1) No central control for routing

(2) No central data repository

**O(log n)**

**Question 7: Answer the following questions:**

1. Consider an instance of TCP’s Additive Increase Multiplicative decrease (AIMD) algorithm where the window size at the start of the slow start phase is 2 MSS (max. segment size) and the threshold at the start of the first transmission is 8 MSS. Assume that a timeout occurs during the fifth transmission. Find the congestion window size at the end of the tenth transmission. [3]

**Answer: 7 MSS**

Since Slow Start is used, window size is increased by the number of segments successfully sent. This happens until either threshold value is reached or time out occurs. In both of the above situations AIMD is used to avoid congestion. If threshold is reached, window size will be increased linearly. If there is timeout, window size will be reduced to half.

Window size for 1st transmission = 2 MSS

Window size for 2nd transmission = 4 MSS

Window size for 3rd transmission = 8 MSS

Threshold reached, increase linearly (according to AIMD)

Window size for 4th transmission = 9 MSS

Window size for 5th transmission = 10 MSS

Time out occurs, resend 5th with window size starts with as slow start.

Window size for 6th transmission = 2 MSS

Window size for 7th transmission = 4 MSS

Threshold reached, now increase linearly (according to AIMD)

Additive Increase: 5 MSS (since 8 MSS isn’t permissible anymore)

Window size for 8th transmission = 5 MSS

Window size for 9th transmission = 6 MSS

Window size for 10th transmission = 7 MSS

1. How does NAT work (Answer in max. 3 sentences, with a neat diagram)? State two problems of NAT. [2+1]

**Answer:** While leaving – IP, port are put in table, checksum is calculated and inserted into the packets. While coming back – IP, port, checksum of IP and port checksum.

Two problems out of:

1. Internet from connection-less to connection-oriented
2. NAT violates the most fundamental rule of protocol layering
3. Processes on the Internet are not required to use TCP or UDP
4. Some applications insert IP address in their body, e.g. FTP – NAT doesn’t know about it.
5. Consider a telnet connection to an interactive editor that reacts on every keystroke. What would be the worst-case overhead of sending one character assuming TCP connection (consider only TCP and IP headers)? Briefly describe the algorithm which solves this problem. [2+2]

**Answer:** When a character arrives at the sending TCP entity, TCP creates a 21-byte TCP segment, which it gives to IP to send as a 41-byte IP datagram. At the receiving side, TCP immediately sends a 40-byte acknowledgement. Later, when the editor has read the byte, TCP sends a window update, moving the window 1 byte to the right. This packet is also 40 bytes. Finally, when the editor has processed the character, it echoes the character as a 41-byte packet. In all, 162 bytes of bandwidth are used and four segments are sent for each character typed.

*Solution: Nagle’s algorithm:*

When data come into the sender one byte at a time, just send the first byte and buffer all the rest until the outstanding byte is acknowledged. Then send all the buffered characters in one TCP segment and start buffering again until they are all acknowledged. The algorithm additionally allows a new packet to be sent if enough data have trickled in to fill half the window or a maximum segment.

**Question 8: Answer the following questions.**

1. What are the different types of *admission control* used in a network? What is the most common way of identifying a flow in the network? How does *TSpec* deal with the possibility of a sender not conforming to the set rules? [1.5+1+2.5]

**Answer:** (1) Based on spare resources; (2) Parameter based; (3) Measurement based.

Common way of identifying flow: 5-tuple information

1. Policing: Packets that do not conform to *TSpec* are treated as best effort and could be dropped.
2. Shaping: Buffer packets to conform to *TSpec* by buffering; done in internal nodes and not at the edge.
3. State two problems of the *IntServ* scheme? How does *DiffServ* remove them? What happens in *Assured Forwarding*? [1+1+1]

**Answer:** Problems with *IntServ* (any 2 must be written):

1. Suited for long lived flows – video conferencing, most web flows are short lived
2. All intermediate network elements/routers must support IntServ
3. Authorization, authentication, and accounting of reservations difficult

*DiffServ* approach (any 2 depending upon points stated above):

1. (Solves point #1) Classify traffic into forwarding classes (and loss priority) – individual flows do not matter
2. (Solves point #2) Admission control is done at edge of the network
3. (Solves point #3) No resource reservation setup

*Assured Forwarding*: Four forwarding classes are defined, and 3 drop priorities are defined within each forwarding class. Drop priorities are used to select which packets to drop during congestion.

1. State the use of the following flags in the TCP header: [1+1]
2. URG
3. PSH

**Answer**: Use of flags:

1. URG – on pushing Ctrl-C to break-off remote computation, the sending application sets URG flag.
2. PSH – Used to force data out.