Solution to End Semester Exam

1. Explain the following types of Routing. **1 marks each**

   (a) Multipath Routing

   When a router computes and keeps more than one path to a destination. Some packets are sent on one path, while other packets are sent on other paths.

   Please note that just the first line is not enough as an answer, since that is too obvious from the name itself. That both paths are used simultaneously is the crucial part of the answer.

   (b) **Loose** Source Routing

   When the source determines a partial path. The packet must go through the routers specified by the source, though it may go through additionl routers as well.

   You need to explain both "source routing" and "loose."

   (c) Type-of-Service Routing

   When the router has multiple routing tables built by considering different cost metrics. Each cost metric is chosen in a way that it would help achieve a particular type of service.

   Note that simply saying that routing based on type of service, would not be enough, as it is too obvious from the question itself.

   (d) Inter-domain Routing

   Routing across different autonomous systems. Different AS have different protocols and cost metrics for their own internal routing, and hence a global routing cannot be on the basis of a unique cost metric.

   (e) Hot-potato or Deflection Routing

   Routing in which the packet is sent on the link with smallest queue.

2. Consider a TCP connection which implements Slow Start, Congestion Avoidance, and Delayed Ack. A data packet takes one millisecond to transmit. One way delay in reaching the destination is 50 ms (not counting the transmission time at source). Transmission of ACK takes

negligible time, but takes 50 ms delay to reach back the source. The timer for waiting for the second data packet before sending an in-sequence ACK is 2 ms.

Show when each data packet will be transmitted, assuming that the first one begins transmission at t = 0 ms. Show all data packets till there are four data packets in transit.

Hint: More than 4 packets will be transmitted. **4 marks**

Packet No.	Start time	Rcv time	Ack Sent	Ack Recv
1	**0**	**51**	**53**	**103**
2	**103**	**154**		
3	**104**	**155**	**155**	**205**
4	**205**	**256**		
5	**206**	**257**	**257**	**307**
6	**207**	**258**	**260**	**310**
7	**307**			
8	**308**			
9	**309**			
10	**310**			

Note that you need to only provide the first two columns. The others are for explanation. Delayed acks means that you either send an ack when you receive the second packet, or after 2 ms (as per the data given in the question). For every ack received by sender, the send window will go up by one packet. So, when you see ack for 1, your window becomes 2. When you see an ack for 3 (no ack for 2), your window becomes 3 (and not 4), and you send packets 4, 5, and 6. When you see ack for 5, your window becomes 4, and you can send packets 7, 8, and 9 (since 6 is already outstanding). But as you finish sending 9, ack for 6 is received and you still don't have 4 outstanding packets. And the window will become 5. So you can send packets 10 and 11. Only 10 needs to be shown in the answer, since that will ensure that there are 4 packets in transit.

3. What all processing happens to a message in PGP. Preferably use a figure. **4 marks**

   (a) **Getting a hash value of message and encrypting it with private key of sender and attaching this to the message.**

   (b) **Compression**

   (c) **Encrypting the compressed message with a session key.**

(d) **Encrypting the session key with public key of receiver and attaching that to the encrypted/compressed message.**

(e) **Base64 encoding to convert the resultant message to printable characters.**

Note: Three encryption steps are must for one mark each. One mark for either compression or base64.

4. When I type in a URL in the browser, and start wireshark at the same time. What all packets am I likely to see. Assume that the webpage is very small, and will fit into one response HTTP packet. **4 marks**

   Will see the following packets:

   (a) **ARP request for Router's IP address and ARP response**

   (b) **DNS request for the domain name mentioned in the URL and a DNS response.**

   (c) **TCP 3-way handshake with the IP address of the server in URL.**

   (d) **TCP/HTTP request and response packets.**

   (e) **TCP close connection packets.**

   One mark each for ARP, DNS and HTTP. One mark for either connection setup or connection release.

5. In the following questions, the answer may need some explanation. **3 marks each**

   (a) Earlier Ethernet (10Base5) used an encoding scheme called "Differential Manchester" which ensured that there was a transition in every bit. Design an encoding scheme which will ensure that there is at least one transition in every 4 bits.

   Expected 4B/5B as the answer.

   Would be ok with 2B/3B, etc. But would not accept a trivial mechanism which says that I will have a transition after every 4 bits, or if in 4B/5B, you have just mapped abcd to abcd1 for every 4-bit value, since then you have not understood the concept.

   (b) Consider a 1 Gbps network connecting two nodes with a round-trip time of 100 milli-seconds. Assume 20 percent of the network capacity is used by various headers, gaps between successive packets and other overheads.

What is the maximum rate at which data can be transmitted from one node to the other assuming no Window Scale option and a WS option with a large value. Assume there is no packet loss.

Without WS, one can do only 64KB per RTT as the maximum window can be 16-bit or 64KB. Since RTT is 100 ms, the max data rate can be 640 KB per second, or 5.120 Mbps.

With WS, one can consume the entire bandwidth, which is 80Hence, 800 Mbps, or 100 MB per second.

(c) In Public-key cryptography, if host A is sending a message to host B, how should the message be encrypted so that it provides integrity, privacy, authentication and non-repudiation.

Take M + Hash (M). Encrypt Hash(M) with Pvt key of Sender. Encrypt M + Signature (M) with Public key of Receiver.

Of course, there can be other solutions as well.

(d) What is the difference between a multi-port repeater (or a hub) and a switch.
Difference between a switch and a router.
Difference between an amplifier and a repeater.

Repeater will forward a packet to all ports, including a collision signal. Switch will forward a packet to only the port on which the destination is there, and will not forward collision signal to any port.

Switch operates at MAC or Data Link layer. Router operates at Network layer.

Amplifier does not interpret signal and hence amplifies noise as well. Repeater regenerates signal thereby removing all noise.

(e) Explain ASK, FSK, and PSK.

Amplitude Shift Keying encodes bits 0 and 1 by using different amplitudes of the wave.

Frequency Shift Keying encodes bits 0 and 1 by using different frequencies in the signal.

Phase Shift Keying encodes bits 0 and 1 by using different initial phases of the sine wave signal.

(f) What are the following timers used for in DHCP.

i. Lease renewal

ii. Lease rebinding

iii. Lease expiry

Lease renewal is the time after which the node tries to contact the SAME DHCP server who had given the original lease for its extension.

Lease rebinding is the time after which the node tries to contact ALL DHCP servers in the LAN for its extension.

Lease expiry is the time after which the node has to stop using the IP address leased to it.

Note that explaining expiry in terms of stopping to use IP address is critical. Just saying lease expiry means that lease has expired is not enough.

(g) We can't keep adding repeaters to extend Ethernet, there is a limit of 4 repeaters between any two nodes. Why such a limit.

But we can extend the Ethernet if we connect two segments with a switch. Why is the above limit not applicable to a switch.

We can't have the entire Internet based on connecting networks by switches (at least not with today's technology). What could be a limiting factor (or what do routers do that switches do not).

As the length of the network increases, the minimum packet size will also increase to ensure that collisions can be detected.

A switch divides the network into multiple collision domains, and we don't need to worry about collisions in one domain to be detectable in another domain.

Switching requires that the destination MAC address be searched in switching table by comparing all 48 bits of destination MAC address with all stored MAC addresses. Since MAC addresses are not hierarchical, this comparison is very expensive, and in today's technology, it is not possible to store billions of MAC addresses and search in them within the transmission time of a packet.

(h) In Random Early Drop variant where there is no drop but just warning to the source about a possible congestion building up, how/when are the two unused bits in IP header of ToS field used.

When a router determines that the indication of congestion needs to be informed to the source, it sets one of the two bits in ToS byte meant for this purpose. The destination of this packet will copy that bit to the other bit in the ToS byte, and the source will see that bit.

6. In the following questions, the answer is at most a few lines. **2 marks each**

(a) The minimum Ethernet packet size (assume 10Base5) is 64 bytes. If a transmitter is noticing collision for the 4th time, what is the maximum backoff (in time) it will face for the next attempted transmission of the same packet.

Maximum backoff will be $2^4 - 1$ **= 15 time units. Each time unit is time to send the smallest Ethernet packet, which is 64 bytes or 512 bits. Time for sending such a packet is 51.2 microseconds. Hence maximum backoff is** $51.2 * 15$ **microseconds.**

(b) Why is error checking done at multiple layers.

Error checking is done at lower layers because an early detection of error will save resources used in unnecessarily transmitting this packet.

Error checking is done at higher layers, since error can be introduced at multiple layers, and the checking must be done at the highest layer where an error can possibly be introduced.

(c) If a TCP source receives Selective ACK for a packet, it cannot delete that packet from its buffers, and must wait for the good old cumulative ACK. What purpose does SACK option serve?

The source can make an intelligent guess about whether the losses are due to congestion or random loss. The source can use this information in more efficient retransmission, that is, not retransmitting SACked packets initially.

(d) Why can we use NRZ encoding to store bits on a disk, but not to code bits on a wire to send to another node.

On a disk, the same clock is being used to store and retrieve. Hence there is no issue of clock synchronization.

(e) In TCP, we monitor the round-trip time of only one packet at a time. (Assuming that we are not using RTTM Option.) Suppose the packet which was being monitored got lost and had to be retransmitted. When it is finally acknowledged, will we consider RTT as the time from 1st transmission or the 2nd transmission. Why?

Neither. If we use first send-time, and it was really in response to the second packet, we would have increased the RTT estimate substantially. On the other hand, if we use second send-time, and it was really in response to the first packet, we would have decreased the RTT estimate substantially.

(f) Is a `bind()` call necessary for server software. Why?
How about client software.

Bind call is necessary for server and not for client. Server identity needs to be known to all clients, which means that its port number must be known to clients. Clients' identity is not needed before the connection, and it will anyway be provided during the connection establishment.

(g) What does Cyclic Redundancy Checksum (CRC) cover in a TCP packet.

Checksum in TCP covers the entire TCP packet, including header and data, and it also includes a pseudo-header which includes IP source/destination addresses, Protocol field, and TCP segment length.

(h) Assume an MTU of 600 bytes for an outgoing link at a router. There is an incoming IP packet of 1200 bytes (including IP header of 20 bytes). What will be the sizes of various fragments of this packet.

596, 596, 48

(i) What is the total number of valid IP addresses that can be assigned to nodes in the Internet. Assume that all networks can have as many nodes as the number of addresses in that network. Assume there are no private addresses.
$2^{31} + 2^{30} + 2^{29}$

This is approximate. If you have subtracted special cases, that is ok. But if you have just given 2^{32} that is not ok.

(j) A router acting as a firewall is called a filtering router as it filters (allows or drops) incoming/outgoing packets based on some information in the packet. Name five fields that a filtering router can look at for firewall purposes.

Src IP, Dst IP, Src port, Dst port, Protocol.

(k) How can ARP be used to detect if there is another machine on my subnet that is using the IP address assigned to my machine.

Send an ARP request with your own IP address. If you receive an ARP reply with a MAC address, then someone else is using it.

(l) How does Token Bus handle a single node going down and breaking the virtual ring.

Previous node of the crashed node will send the Token but will not hear any activity. After a couple of times, it will assume that its successor is down, and will send a message asking who follows the crashed node. The next node will reply. The previous node will make that node as its next node, send the token to it, and the next node will set its previous node to this one.

If you have talked about voluntary leaving of node, that is also ok.

(m) Explain the process of removing an orphaned packet in Token Ring. (That is, the source goes down after transmission of packet.)

Each ring has a special node called Monitor, and each packet has a bit called Monitor bit. When a node transmits a packet, it sets the monitor bit to 0. When the packet passes through the monitor, the monitor will set the bit to 1. If the source does not remove the packet and the packet reaches the monitor again, the monitor will recognise this condition by noticing that the Monitor bit is 1, and will remove the packet.

(n) What all system calls are called by a server of a connection-oriented application. Please use only Socket programming system calls in C.

socket, bind, listen, accept, close/shutdown.

Any four (but only one of close and shutdown). Read/write won't count.

7. In the following questions, the answer is very short. **1 mark each**

   (a) Ethernet has a 8-byte preamble, whose purpose is to ensure that the receiver hardware is ready and its clock is synchronized to the sender's clock. If the receiver's hardware will take some time to get ready during which an unknown number of bits have been received (and lost), how will it know when the 8-byte preamble is over.

   The 8th byte is special - 10101011. Two consecutive is an indication of end of preamble.

   (b) A 160-bit address in IPv6 would have enabled it to have the same addressing size as ATM and OSI's Network layer protocols, making it easier to inter-operate. Why did we not accept that size.

   64-bit architecture can handle multiples of 64 bits data much more efficiently, and hence 128 bits.

   (c) In 1970s, General Motors was interested in developing a protocol stack for factory automation in which all machines on the assembly line would be connected by a LAN. The research led to MAP (Manufacturing Automation Protocol). For its MAC layer, GM chose Token Bus, instead of Ethernet, which was the dominant standrd of the time.

   Can you guess why Token Bus was chosen ove Ethernet?

   To have a guarantee of upper limit within which a packet will be allowed to be transmitted. No node will starve indefinitely.

   (d) In WiFi MAC, we used CSMA/CA (RTS/CTS messages with the time of transmission mentioned). Under what condition would the CA part be reduntant. (CD part may still remain a problem.)

   If there is no hidden node. That is, if all nodes are within each other's listening range.

   (e) In TCP, a source can retransmit a packet even before the retrasmission time expires. Under what condition?

   If a source receives 3 duplicate acks.

(f) In order to avoid reflection attack, we want to ensure that a random number used in one direction can not be used in another direction. Give one way to do so.

Odd numbers in one direction. Even in the other.

(g) The network utility, *ping*, operates as follows: You send a packet and the destination replies. From the replies, you can know which packets were received and which were not and you can also estimate the round trip times of packets which were replied to.

What type of message is used in this utility.

ICMP Echo request/reply.

(h) To be able to detect collision in a CSMA/CD network, a minimum packet size is specified. When we moved from a 10Mbps Ethernet to a 100Mbps Ethernet, the minimum packet size should have become 10 times, keeping all other parameters constant. But it didn't happen this way. The minimum packet size remained the same. What changed?

Maximum distance became one tenth.

(i) There is a folklore regarding "Net 10." The erstwhile ARPAnet was assigned IP addresses of the type, **10.0.x.y**. As ARPAnet stopped functioning, the IP address range became available for Private IP addresses. What class of network was ARPAnet.

class A

(j) There is a transient routing loop (which can happen because the routing table updates are not synchronized and information that each router has is different). A packet is going around in this loop. For how long will the packet keep moving in this loop.

Till TTL field becomes 0.

(k) What is the drawback of TCP when it comes to supporting a transaction oriented application.

Delay of 1 RTT due to 3-way handshake.

(l) In a sliding window protocol, a receiver is allowed to store at most two out-of-sequence packets. That is, if the receiver is expecting a packet with sequence number x, the receiver can buffer packets numbered $x+1$ and $x+2$. If the sequence number is **4** bits, what is the maximum send-window size.

13

Sequence number space is 16. Max rcv window is 3. So max send window is 16 -3.

(m) Two nodes are communicating using TCP. The receiver crashes and reboots within a few seconds. The sender does not get ACKs and has retransmitted packets while the receiver was rebooting. How will the source eventually realize that it has only a half-open connection.

When it retransmits again after the other side has rebooted, it will receive a RESET message.

(n) I want to know the IP addresses of all the routers that the packet will pass through. Record Route Option was defined just for this purpose. But it does not work. What is the limitation.

The IP options can only be 40 bytes at most, which is not enough to store IP addresses of all intermediate routers.

(o) What functionality (other than error checking) is implemented at multiple layers of network protocols.

Fragmentation and reassembly.

(p) What is coding violation.

In situations like 4B5B or 8B6T, certain signal values have no corresponding bit values. Using those signal values is coding violation.

(q) Why can we not have a protocol purely based on negative ACKs. Why do we must have some form of positive ACKS in a protocol for reliability.

Negative ACKs cannot recover if the last packet is lost.

(r) When a router sends an ICMP error message to a source, how does the source know which connection did the dropped packet belong to.

ICMP message has a payload which are several initial bytes of the dropped packet.

(s) Why is it that a fragmented IP packet is not re-assembled by the next router.

Since different fragments may take different paths.