Indian Institute of Technology, Kharagpur
End-Autumn Semester 2018-19

Date of Examination: 27-11-2018 Session: FN (9-12 pm) Duration: 3 hrs
Subject No.: IT30037 Subject: INTRODUCTION TO INTERNET
Department/Center/School: Computer Science and Engineering
Specific charts, graph paper, log book etc., required: NO
Special instructions (if any): NO

1. **(0.5+0.5+1+0.5+2+0.5+1+0.5+2.5 = 9M)**

(a) What is meant by vulnerable period in ALOHA protocols?
It is the time interval in which no user is allowed for transmission, except the intended ready user.

(b) Vulnerable period of pure ALOHA (in terms of frame time)
2 X Frame time

(c) Vulnerable period of slotted ALOHA (in terms of frame time)
1 X Frame time

(d) Ten thousand airline reservation stations are competing for the use of single slotted ALOHA channel. The average station makes 18 requests per hour. A slot is 125 micro-seconds. What is the approximate total channel load?
Total channel load = $\frac{10000\times18\times125}{3600\times1000000} = \frac{1}{160}$

(e) Steps executed by a ready station in case of non-persistent CSMA protocol:
First, it will sense the channel,
Step (i): if the channel is free, it will send the frame.
Step (ii): If the channel is busy, it will wait for random time interval and sense the channel.
Based on the status of the channel it will execute either step (i) or step (ii).

(f) Assume the ethernet LAN is configured with CSMA/CD using bus topology. If the stations are using frames of size 500 bits and the datarate offered by a cable is 50 mbps (megabits per second). The signal speed inside the cable is 2,50,000 km/sec. The stations are connected uniformly with a spacing of 10 mts between the adjacent ones. What will be the maximum number stations that can be connected?
Frame transmission time = $\frac{500}{50\times1000000} = 10\ micro\ sec$
For detection collissions in CSMA/CD, the minimum frame trasmission time = $2 \times$ *cable propagation delay*.
Cable propagation delay = 5 micro sec.
Length of the cable = $\frac{250000\times1000\times5}{1000000} = 1250\ mts$
Number stations can be connected = $\frac{1250}{10} + 1 = 126$

(g) Name two collission free protocols:
(i) Bit-map protocol and (ii) Binary countdown

(h) Clearly discuss collission and collission-free protocols in view of delay and channel efficiency under light and heavy load conditions.
Collission protocols offer less delay and less overhead during light load condition and more delay and poor channel utilization during heavy load condition due to repeated collissions.
Collission-free protocols offer more delay and overhead during light load condition and less delay and high channel efficiency during high load conditions.

(i) What is the use of binary exponential back-off algorithm?
In case of CSMA/CD execution in IEEE 802.3 LAN, for resolving the collissions, after each collission the number of delay slots will be increased exponentially (doubled) after each collission (2^n delay slots after n successive collissions.

(j) Answer the following:

i. Why CSMA/CD protocol is not appropriate for wireless LANs?
In wireless LANs collissions are not heard (observed) by the transmitting station, and hence CSMA/CD protocols are not appropriate. In addition to this there will be hidden and exposed station problems present in wireless LANs in presence of CSMA/CD protocol.

ii. With appropriate diagrams, explain hidden-station and exposed-station problems in view of wireless LANs.
Hidden station problem: Suppose station A is sending message to B using wireless transmission. Station C is out of range of A's transmission, and hence C is not able to hear (sense) A's transmission. But, if the receiver of A's transmission B is within the transmission range of C's transmission. During A's transmission to B, C can transmit as per CSMA/CD principle. But, C's transmission overlap (collission) with A's transmission at the receiver B, and hence the message reception at B is garbled. This problem is known as hidden station problem. Hence C is hidden station to A's transmission.
Exposed station problem: Suppose A is tranmitting to B, and C want to communicate to D, where the receivers B and D are out of range of C and A, respectively. If C is within the transmission range of A, then C is not allowed to transmit during A's transmission as per CSMA/CD, even though there won't be any overlap transmissions at their intended receivers B and D. This is because, C is exposed to A's transmission before it is attempting to transmit. This problem is known as exposed station problem.

iii. Clearly explain how hidden and exposed station problems are addressed in wireless LANs.
The above mentioned hidden and exposed station problems can be resolved by using 2-way hand-shake messages between the transmitter (sender) and receiver (destination). When A want to communicate to B, first A will send a control message RTS (request to send) to B, which contains the size of data it want to send. Up on receiving RTS, B will send an acknowledgement CTS (clear to send) back to A, indicating the amount of data it is willing to receive from A. The stations, which receive only CTS (hidden stations) will not attempt to transmit until B's reception is completed. The stations which receive only RTS, but not CTS (exposed stations) can be allowed for transmission. Thus by using RTS and CTS, hidden and exposed station problems can be resolved.

2. (a) Answer the following in view of classful addressing: **(2+5+1+1+2.5 = 11.5M)**

i. How many classes exist?
Five (5)

ii. Name the classes which support unicasting:
A, B and C

iii. Total number of network addresses supported:
$2^7 + 2^{14} + 2^{21} = 2113664$

iv. Number of addresses reserved:
$2^{28} = 268435456$

(b) A large number of consecutive IP addresses are available starting at 54.128.128.0. Suppose that five organizations, A, B, C, D and E, request 1000, 3000, 500, 16000 and 8000 addresses, respectively, and in that order. For each of these, give the first IP address assigned, the last IP address assigned, and the mask in the w.x.y.z/s notation.

Org	# addr	1st IP addr	Last IP addr	Network mask (\n)
A	**1000**	**54.128.128.0**	**54.128.131.255**	**255.255.252.0 (\22)**
B	**3000**	**54.128.144.0**	**54.128.159.255**	**255.255.240.0 (\20)**
C	**500**	**54.128.132.0**	**54.128.133.255**	**255.255.252.0 (\22)**
D	**16000**	**54.128.192.0**	**54.128.255.255**	**255.255.192.0 (\18)**
E	**8000**	**54.128.160.0**	**54.128.191.255**	**255.255.224.0 (\19)**

(c) Provide expansion to NAT. What is the role of NAT?
NAT: Network Address Translator. It is used to provide internet access to a large group of users with very few public IP addresses, using mapping between private and public addresses. It exploits destination's public IP, port number and source port number to map multiple private addresses to few public addresses.

(d) Show the original IPv6 (unabbreviated) address for the following compact notation: 0:234::3:BC
0000:0234:0000:0000:0000:0000:0003:00BC

(e) Briefly answer the following in view of priority field in IPv6 header:

i. How many distince priorities are supported?
16 (0-15)

ii. What is congestion-controlled traffic?
The data that can be discarded during congestion and sending control information to their respective sources to inform them about dropping their packets. With this sources can slow down their data rates and hence congestion may be controlled. For this data, 0-7 priorities are assigned.

iii. Provide two examples of data, which fall under congestion-controlled traffic.
Background data, unattended data traffic, attended bulk data traffic, interactive traffic and control traffic

iv. What is noncongestion-controlled traffic? Provide an example.
The data where retransmission is not feasible, in this case, at the time of congestion, the packets are not usually discarded. Hence their priorities will be given as 8-15. Low priority (8,9,...) (high fedility audio/video) will be given for data having enough redundancy and high priority (low fedility audio/video, priorities 15, 14,..) will be

given for packets having less redundancy and contains key details of the application.
Realtime audio/video applications.

v. How priorities are assigned for noncongestion-controlled traffic?
Low priority (8,9,...) (high fedility audio/video) will be given for data having enough redundancy and high priority (low fedility audio/video, priorities 15, 14,..) will be given for packets having less redundancy and contains key details of the application.

3. **(1+0.5+0.5+0.5+1+1+1+0.5+1 = 7M)**

(a) What is the expansion of ARP? What is the role of ARP in network layer?
ARP: Address Resolution Protocol
ARP is used to find (Map) the physical address (MAC address) from the IP address of the router/host.

(b) What is proxy ARP?
In case of normal ARP, only the genuine host/router responds to ARP request by specifying its physical address. But, in case of proxy ARP, a router of a sub-network will responds to ARP request (on behalf of all the hosts of the subnet) corresponds to any of the hosts present in the subnet, instead of the genuine target host.

(c) Why RARP is replaced by BOOTP or DHCP?
In case of RARP, each network on the internet needs RARP server to map the Physical address to IP address. Whereas for BOOTP or DHCP, the above constraint is not there.

(d) How DHCP differ from BOOTP?
DHCP maintains both static and dynamic binding of physical addresses to their respective IP addresses. But, BOOTP maintains only static/permanant bindings of Physical to IP addresses.

(e) Name the error reporting messages supported by ICMP.
(i) Destination unreachable, (ii) Source quench, (iii) Time exceeded, (iv) Parameter problem and (v) Redirection.

(f) With appropriate diagrams show how ICMP error reporting messages are created using the IP datagrams which will be discarded due to errors.
The discrded packet's IP address and first 8 bytes of data are considered as ICMP packet's body. ICMP header is attached prior to its body to indicate what is the type of error and other related information. To send the ICMP packet to the desired source, it will be send through IP by encapsulating the ICMP packet within IP packet.

(g) Name the query messages supported by ICMP.
(i) Echo request and reply, (ii) Time stamp request and reply, (iii) Address-mask request and reply and (iv) Router solicitation and advertisement.

(h) Mention two important debugging tools use ICMP query messages.
(i) Ping and (ii) Traceroute

(i) Provide the expansion of IGMP. Mention different message types used by IGMP.
IGMP: Intenet Group management Protocol

IGMP Message types: (i) General query, (ii) Special query, (iii) Membership report and (iv) Leave report.

4. (a) Show the forwarding process of the following packets at the router R1 with the following destination addresses: (a) 112.59.163.200 (b) 112.59.198.49 (c) 155.79.128.197 and (d) 155.74.234.45 **(4+1+4+1 = 10M)**

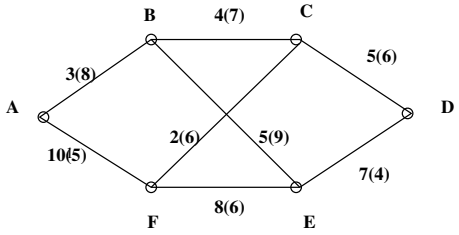
Router Table of R1			
Mask	Network Address	Next Hop	Interface
255.255.192.0	112.59.192.0	——-	m0
255.255.0.0	112.59.128.0	———	m1
255.254.0.0	155.72.0.0	———	m2
255.248.0.0	155.76.0.0	———	m3
Any	Any	189.72.146.55	m1

Forwarding process of Router R1					
Dest address	Mask	obtained n/w address	Network Address	Next Hop	Interface
112.59.163.200	255.255.192.0	112.59.128.0	112.59.192.0	189.72.146.55	m1
112.59.163.200	255.255.0.0	112.59.0.0	112.59.128.0		
112.59.163.200	255.254.0.0	112.58.0.0	155.72.0.0		
112.59.163.200	255.248.0.0	112.56.0.0	155.76.0.0		
112.59.198.49	255.255.192.0	112.59.192.0	112.59.192.0	——	m0
112.59.198.49	255.255.0.0	112.59.0.0	112.59.128.0		
112.59.198.49	255.254.0.0	112.58.0.0	155.72.0.0		
112.59.198.49	255.248.0.0	112.56.0.0	155.76.0.0		
155.79.128.197	255.254.0.0	155.78.0.0	155.72.0.0	189.72.146.55	m1
155.79.128.197	255.248.0.0	155.72.0.0	155.76.0.0		
155.74.234.45	255.254.0.0	155.74.0.0	155.72.0.0	189.72.146.55	m1
155.74.234.45	255.248.0.0	155.72.0.0	155.76.0.0		

(b) In view of router table entries, briefly discuss the salient points regarding address aggregation.
(i) Router table size will be reduced with address aggregation. Ex: National ISP, Regional ISP and Local ISP are the hierarchy from top to bottom. The network addresses under regional and local ISPs are invisible outside the National ISP. All the networks within national ISP are viewed as single IP (network address) indicated by National ISP's IP address. (ii) In presence of address aggregation, the masks present in router table should have the decreasig order of their size.

(c) Consider the subnet shown in figure. The link delays at time t1 are marked on the figure (outside the brackets). The link delays at time t2 (t2 > t1) are marked on the figure (within the brackets). Using distance vector routing determine the following: (i) Delay vectors sent to Node C by the neighbouring nodes at time t1 (ii) Node C's routing table at time t1 (iii) Delay vectors sent to Node C by the neighbouring nodes at time t2 (iv) Node C's routing table at time t2.

(d) In the context of multicast routing protocols highlight the distince features of (i) source-based tree and (ii) group-shared tree.



	Router Table of C at time t1								Router Table of C at time t2							
Dest	B	D	F	CB	CD	CF	C	NH	B	D	F	CB	CD	CF	C	NH
A	3	12	9	7	17	11	7	B	8	15	5	15	21	11	11	F
B	-	9	6	4	14	8	4	B	-	13	13	7	19	19	7	B
C	4	5	2	-	-	-	-	-	7	6	6	-	-	-	-	-
D	9	-	7	13	5	9	5	D	13	-	10	20	6	16	6	D
E	5	7	8	9	12	10	9	B	9	4	6	16	10	12	10	D
F	6	7	-	10	12	2	2	F	13	10	-	20	16	6	6	F

Source-based tree: Each source (router) has to maintain one shortest path tree (SPT) for each group. Therefore, if there are N groups, each router has to maintain N shortest path trees. Whereas in case of unicasting each router will maintain only one SPT, and it is nothing but the entires of its router table.
Group-shared tree: In stead of each router maintaining N SPTs, only one designated router known to be core router maintains N SPTs correspond to all groups. Each router will forward the multicast packet to core router for for futher routing.

5. (a) With a neat diagram (marked with five rows, where each row indicates 4 bytes) clearly mention all the fields present in TCP basic header. **(2+2+2+1.5 = 7.5M)**
Source port address (16), destination port address (16)
Sequence number (32)
Acknowledgement number (32)
HLEN (4), Reserved (6), URG/ACK/PSH/RST/SYN/FIN (6), Window size (16)
Checksum (16), Urgent pointer (16)
Options and Padding

   (b) Provide a diagram to illustrate the connection establishment using 3-way handshaking with TCP. Assume the sequence numbers at client and server are 1000 and 5000, respectively. Clearly indicate the necessary values (seq no, ack no, flags) at appropriate fields within the segments.
From client to server: Seq = 1000, SYN = 1
From server to client: Seq = 5000, ack = 1001, ACK = SYN = 1
From client to server: Seq = 1000, ack = 5001, ACK = 1

   (c) Show the TCP connection termination process with suitable diagram in view of half-close scenario. At the time of closing from client side, the sequence and acknowledgement numbers in the last segment are 12000 and 5000, respectively. Whereas the sequence number of last segment from server side before its closing is 21000. Clearly indicate the necessary values (seq no, ack no, flags) at appropriate fields within the segments.

Client to server: Seq = 12000, Ack = 5000, ACK = FIN = 1
Server to client: Seq = 4999, Ack = 12001, ACK = 1
Data transmission from server to client and client to server connection was closed
Server to client: Seq = 21000, Ack = 12001, ACK = FIN = 1
Client to server: Seq = 12000, Ack = 21001, ACK = 1

(d) Answer the following in view of congestion control:

i. Name two important network performance measures affect with congestion.
Delay and Throughput

ii. Name any two open-loop congestion control policies
Retransmission policy, window policy, acknowledgement policy, discarding policy and admission policy

iii. Name the two closed-loop congestion control mechanisms
Back pressure, choke packet, implicit signalling, explicit signalling and congestion window

6. Match the following: **[0.25 × 20 = 5M]**

(1) Class-A	(e)	(a) Server can send data to client
(2) Number of group addresses in IPv4	(l)	(b) Data transmission within a LAN
(3) Limited contention	(p)	(c) Message oriented
(4) Class-B address	(j)	(d) Queues
(5) Flow Label	(s)	(e) 16000000 hosts
(6) Strict source route	(m)	(f) Flow control
(7) Classless addressing	(k)	(g) Full duplex connection
(8) BOOTP	(n)	(h) OSPF
(9) Ping	(q)	(i) 3-duplicate acks
(10) Direct delivery	(b)	(j) 178.29.67.123
(11) Path vector routing	(t)	(k) p.q.r.s/t
(12) link state packet transmission	(r,h,o)	(l) 256 millions
(13) Distance vector routing	(o)	(m) Optional header of IPv4
(14) Congestion window	(f)	(n) Physical to logical address mapping
(15) UDP	(c,d)	(o) Intradomain routing
(16) Half-close	(a)	(p) Adaptive tree walk protocol
(17) Fast retransmission	(i)	(q) Statistics of RTT
(18) TCP	(g)	(r) Flooding
(19) UDP implementation	(d,c)	(s) IPv6
(20) Shortest path tree	(h)	(t) Interdomain routing