ECE358 Final W2018

1.

A) 7
B) 8
C) 12
D) 10
E) 11
F) 3
G) 4
H) 1
I) 14
J) 6

2.

a) Sequence number: 207
   Source port number: 302
   Destination port number: 80
b) Ack number: 207
   Source port number: 80
   Destination port number: 302
c) Ack number: 127

3.

1) Part 1
   a. 3 duplicate ACKs
   b. False. At event B, the network is experiencing some congestion. There may be some packet delay or loss. Since the loss event was 3 duplicate ACKs rather than a timeout, the congestion is likely temporary and not extreme.
   c. Timeout
   d. False. At event D, the network is likely to have more severe congestion and increased packet loss/delay. A timeout is more likely to be due to more severe congestion, but could also have occurred due to other factors such as a checksum error, so we cannot say for certain that the network is fully congested and cannot deliver any packets to the receiver.
2) The slope labeled by A increases exponentially as it is in the slow start phase. In the slow start phase, we want to increase the window quickly as we are less likely to reach congestion in this phase and want to increase throughput quickly.
3) Part 3
   a. At point B, the window size is 8k bytes, which is 8MSS's. Since we double the MSS each RTT and at time 0 we are at 1MSS, we must be at 3RTT. 300ms has progressed by point B.
   b. At point C, the window size is 4k bytes. At point D, the window size is 16k bytes. Since the window size is increasing by 1MSS every RTT, 12RTTs = 1200ms have elapsed.
   c. At point E, we have that ssthresh=8k. Hence it takes 3MSS to reach 8k bytes. Then we switch to congestion avoidance, where it takes 2MSS to reach point F (window size 10k). Hence 500ms have elapsed.
4) Since the sender shares its network with other clients, point D might be higher than point B because there was less traffic from other clients at the time, allowing the sender to increase its window size by more (thus creating more traffic) before a loss event, than at point B, where there was more traffic from other clients creating congestion.

4.

a) Ethernet dest: MAC2
   IP dest: 3.0.0.1
b) Ethernet source: MAC 3
   Ethernet dest: MAC 4
   IP source: 2.2.3.2
   IP dest: 3.0.0.1
c) Ethernet source: MAC 5
   Ethernet dest: MAC 6
   IPv4 source: 1.2.3.7
   IPv4 dest: 1.2.4.4
   IPv6 source (inside IPv4 payload): 2.2.3.2
   IPv6 dest (inside IPv4 payload): 3.0.0.1
d) Ethernet source: MAC 12
   Ethernet dest: MAC 11
   IP source: 10.0.0.2
   IP dest: 2.2.3.2

5.

step	added to N'	D_t	D_u	p_v	D_w	D_y	D_z	arc added
	x	∞	∞	3	6	6	8	
1	v	7	6	3	6	6	8	(x,v)
2	u	7	6		6	6	8	(v,u)
3	w	7			6	6	8	(x,w)
4	y	7				6	8	(x,y)
5	t	7					8	(v,t)
6	z						8	(x,z)

6. Multiple possible solutions

Subnet	# Hosts	Block size (# bits)	Network ID	Prefix length	Broadcast address
A	13	16 (4 bits)	192.168.10.160 [1010/]	28	192.168.10.175
B	120	128 (7 bits)	192.168.10.0 [0/]	25	192.168.10.127
C	6	8 (3 bits)	192.168.10.152 [10011/]	29	192.168.10.159
D	2	4 (2 bits)	192.168.10.128 [100000/]	30	192.168.10.131
E	60	64 (2 bits)	192.168.10.192 [110000/]	xxx	xxxxxxxxxxxxxx
F	14	16 (4 bits)	192.168.10.176 [1011/]	xxx	xxxxxxxxxxxxxx
G	5	8 (3 bits)	192.168.10.144 [10010/]	xxx	xxxxxxxxxxxxxx
H	2	4 (2 bits)	192.168.10.132 [100001/]	xxx	xxxxxxxxxxxxxx
I	2	4 (2 bits)	192.168.10.136 [100010/]	xxx	xxxxxxxxxxxxxx

7.

i) Forwarded on links: 1,3,4,5,6; since switch table is empty, it does not know interface for MAC E, so flood

MAC address	Link
MAC B	2

ii) Forwarded on links: 2; since switch knows which interface corresponds to MAC B

MAC address	Link
MAC B	2
MAC E	5

iii) Forwarded on links: 2; since switch knows interface for MAC B

MAC address	Link
MAC B	2
MAC E	5
MAC A	1

iv) Forwarded on links: 1; since switch knows interface for MAC A

MAC address	Link
MAC B	2
MAC E	5
MAC A	1

8.

a) Let p(A) be the probability that node A succeeds in a slot.
   Then we have that
   p(A) = p(A transmits)p(B does not)p(C does not)p(D does not) = p(1-p)^3
   = 0.0384
   Then we have that
   p(A succeeds for first time in slot 5) = p(A)(1-p(A))^4 = 0.03264
b) p(A) = p(B) = p(C) = p(D)
   p(some node succeeds) = 4p(A) = 0.1536
c) p(no node succeeds) = 1 - p(some node succeeds)
   p(first success in slot 3) = p(some node succeeds) p(no node succeeds)^2
   = 0.11
d) efficiency = p(some node succeeds) = 0.1536

9.

a) Switches are link layer devices while routers are network layer devices. Switches have a switch table that map MAC addresses to network interfaces. Routers have forwarding tables that determine where to forward based on destination IP. Overall, they both store and forward packets at their respective layer.
b) ARP (address resolution protocol) is used to determine the MAC address of the next hop. Each NIC has an ARP table that is filled over time. Whenever a new mapping between an IP@ and a MAC@ is learned it is kept in the ARP table for a certain TTL (typically 20 minutes)

   Example: A wants to send datagram to B. B's MAC address not in A's ARP table, so A uses ARP to find B's MAC address. A broadcasts ARP query in a frame, containing B's IP address. The frame has a type field indicating that it is an ARP frame (there is no payload in that frame), with destination MAC address = FF-FF-FF-FF-FF-FF. All nodes on LAN receive the ARP query. B replies to A in an ARP frame where destination MAC address = A's MAC address, source MAC address = B's MAC address. A receives B's reply, adds B entry into its local ARP table.
c) Inter-AS routing routes traffic between AS's. Inter-AS routing uses BGP, which is a policy-based routing protocol. This is because admins want control over how its traffic is routed and who routes through its network. Intra-AS routing routes packets within the AS. The two common non-proprietary IGPs are OSPF and RIP. Intra-AS routing is more focused on performance rather than policy, as there is a single admin so policy is less of an issue.
d) Ignore this question
e) Flow control allows the receiver to prevent the sender from overflowing its buffers, preventing packet loss due to receiver buffer overflow.
f) Congestion control helps prevent congestion in the network, which can cause packet loss and delays due to packets being dropped in router buffers.