Ans1.

a)

Simple Parity Check : A Parity bit is added to the data; 1 is added if the block contains odd number of 1s, 0 is added if the block contains even number of 1s. Useful for detecting only 1-bit errors.

2D Parity Check : Similar to simple parity check, but parity is calculated for every row of data instead. Calculated parities are then sent along with the data. Can detect 2-bit or bigger errors.

Checksum : Data is divided into k segments of m bits each. All the segments are then added, the sum is then subjected to 1s compliment. This value is sent along with the data to the receiver. The receiver then sums all the received segments and adds the sum to the received checksum, if the value is 0 then no error had occurred, else we can say errors have occurred.

b)

Slotted Aloha is more efficient than Pure Aloha because of the slotted nature of the protocol. In Pure Aloha, senders are allowed to send data at their wish i.e. whenever they want to. Although even in Slotted Aloha senders can send data whenever they wish to, there are slots; a sender can begin to send data only when a slot starts and not in the middle of slots.

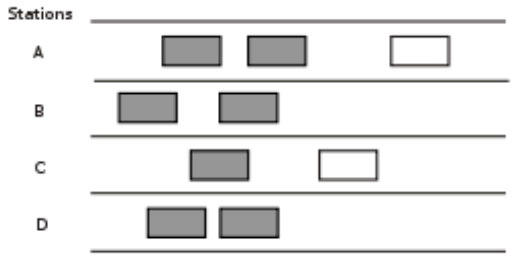

Figure 1: Pure Aloha

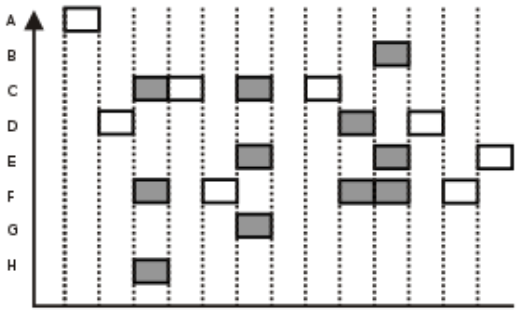

Figure 2: Slotted Aloha

Having slots makes it impossible for a scenario like Figure 1 to happen, no other sender can start sending data in middle of a slot, hence it cannot disturb the transmission. While in Pure Aloha, senders are allowed to start sending anytime they wish to, which results in a lot of collisions where a sender started sending in middle of someone else's transmission. Hence that's why probabilistically Pure Aloha has more chances of causing a collision.

Ans2.

a) IPv4 Address Squatting

b) Jim will broadcast an ARP request to the entire network to check if the IP addressed offered is used by any other computer[1].

c) After that Jim will send a DHCPDECLINE response back to the HDCP server, declining the DHCPOFFER[1].

Ans3.

a) No, the topology will not work. It will eventually crash because of the topology consists of a loop. Switches broadcast the messages sent to them, and with a loop introduced between the switches a broadcast loop gets created which keeps on getting amplified as more data is sent through switches. Eventually as the switches run out of resources to manage all the data, they crash.

b) It can be prevented by using Spanning Tree Protocol(STP). STP runs on switches and scans for loops, and then builds a loop-free topology by shutting down certain ports. Running STP on our switches will prevent our switches from crashing eventually because no loops would be formed then.

c) Yes, it's possible to use both the links for forwarding traffic by aggregating them by creating an EtherChannel. EtherChannel is a port aggregation technology that allows us to aggregate two or more ports on a device to be aggregated and used as a single ethernet port. By aggregating the ports, we can use both the links for forwarding traffic.

Ans4.

Broadcast Domain: Broadcast Domain is the scenario where a device sends out a broadcast message, i.e. all the devices present in its broadcast domain will have to listen to it. This has potential to create problems like congestion creating slowdowns in the entire network.

Collision Domain: Collision Domain is the scenario where a device sends out a message to all the devices which exist in its collision domain, without talking in account if they needed that message or not. This has potential to create problems like collisions, for example in a case when two devices start talking at the same time, which leads them to wait and resend their messages one at a time.

Hub: Hubs only join networks, don't create them so they operate in a single collision and broadcast domain. Hubs do not break both collision and broadcast domains, thus they face potential problems caused by both the domains.

Switch: Every port on a switch is on a different collision domain, hence they do not face the potential issue of having a collision. But switches do not break down broadcast domain, which means they still face potential issues of a broadcast domain.

Router: A router breaks down both collision and broadcast domains. A router can connect multiple networks together, a broadcast message from a network will not reach any other network.

Repeater: Repeater are layer 1 devices, which simply repeat the information they're receiving; hence they do not break either collision or broadcast domain.

Ans5.

From X

	X	Y	Z	U	V	W	T
X	0	6	8	..	3	6	..
Y		6	8	..	3	6	13
Z		6	8	..	3	6	13
V		6	8	6	3	6	7
W		6	8	6	3	6	7
U		6	8	6	3	6	7
T		6	8	6	3	6	7

Hence, Minimum distance from

X -> U is 6
X -> V is 3
X -> W is 6
X -> T is 7
X -> Y is 6
X -> Z is 8

a) from T

	T	U	V	W	X	Y	Z
T	0	2	4	..	..	7	..
U		2	4	5	..	7	..
V		2	4	5	7	7	..
W		2	4	5	7	7	..
Y		2	4	5	7	7	19
X		2	4	5	7	7	15
Z		2	4	5	7	7	15

Hence, Minimum distance from

T -> U is 2
T -> V is 4
T -> W is 5
T -> X is 7
T -> Y is 7
T -> Z is 15

b) from U

	U	T	V	W	X	Y	Z
U	0	2	3	3	..	..	..
T		2	3	3	..	9	..
V		2	3	3	6	9	..
W		2	3	3	6	9	..
X		2	3	3	6	9	14
Y		2	3	3	6	9	14
Z		2	3	3	6	9	14

Hence, Minimum distance from

U-> T is 2
U -> V is 3
U -> W is 3
U -> X is 6
U -> Y is 9
U -> Z is 14

Ans6.

a) B sends frame to E.

Frame is forwarded to A,B,C,D,E and the switch learns the mac-address of B. Before this transaction the switch table on the switch is empty so switch does not know what interface B is connected to.

b) E replied with a frame to B

Frame is forwarded to B because switch has learned the mac and the interface of B. Switch will now learn the mac-address of E and add it to the switch table.

c) A sends a frame to B

Frame is forwarded to B because switch already knows the mac-address and interface of B. Switch will learn the mac-address of A and add it to the switch table.

d) B replied with a frame to A

Frame will be forwarded to A because switch learned about it in the last step.

Ans7.

The minimum packet size at the data link layer has to be 64 bytes, that means it can carry 46 bytes of payload at the minimum.

As for why, the minimum packet size is needed to have a more efficient network overall by helping detect collisions reliably by all the devices. The minimum packet size is selected such that the data being can be read back by the sender to detect if it's garbled or not and respond with a JAM message informing everyone on the network to ignore the message. The minimum size is 64 bytes because when it was decided, ethernet 10M was the latest incarnation, and thee 10M data rate with a probabilistic average RTT was used to calculate the 64 byte value.

Ans8.

Initial packet from 192.168.1.2, will have the source IP of itself and the destination IP of the destination while having the source MAC address of itself and the destination incoming MAC address of its gateway.

Source IP	Destination IP	Source MAC	Destination MAC
192.168.1.2	10.0.0.3	DC:85:ED:9E:DC:44	5F:1D:5B:BC:6D:DE

After reaching the first router, the router will change the source outgoing MAC address in the header to its own MAC address and the destination incoming MAC address of the router the packet will be hoping to next. IP fields will go unchanged.

Source IP	Destination IP	Source MAC	Destination MAC
192.168.1.2	10.0.0.3	5A:1F:5B:55:AC:5F	5A:FF:AB:BB:AC:CD

After the second router, the second router will do the same as previous router, i.e. change the source MAC to it's outgoing MAC address and the destination MAC to the next routers incoming MAC.

Source IP	Destination IP	Source MAC	Destination MAC
192.168.1.2	10.0.0.3	FF:85:34:FF:CA:AA	AA:BB:CC:DD:EE:FF

After the third router, the router again will change the source MAC to its outgoing MAC and the destination MAC to next routers incoming MAC.

Source IP	Destination IP	Source MAC	Destination MAC
192.168.1.2	10.0.0.3	FF:15:AD:BB:CA:CD	FF:15:AD:BB:CA:C1

After the final router, also the gateway for our destination IP, will change the source MAC to its own outgoing interfaces MAC address and the destination MAC address to the destination PC a.k.a 192.168.0.3's receiving interfaces MAC address.

Source IP	Destination IP	Source MAC	Destination MAC
192.168.1.2	10.0.0.3	5F:1A:5A:BC:FD:DD	AB:50:CC:AA:EF:DD

Ans9.

Assuming we already know the destination IP and the port number.

The initial packet what will be formed will have the source IP of the source computer inside the NAT but destination IP of the destination's NAT'ed router. Destination Port number would also be of a port number that is mapped on the destinations NAT router.

Source IP	Destination IP	Source Port	Destination Port
192.168.1.2	192.10.124.1	693	421

At the source networks router, the NAT router will change the source IP from the computers IP to its own outgoing IP address, and will change the source port to a random port number that will be mapped to the original port number of the computer.

Source IP	Destination IP	Source Port	Destination Port
129.10.123.1	192.10.124.1	893	421

At third router and forth router everything will stay the same

Source IP	Destination IP	Source Port	Destination Port
129.10.123.1	192.10.124.1	893	421

At the final router, destination port will be mapped and changed to the real port number and the destination IP will also be mapped and changed to the destination computers NAT'ed IP.

Source IP	Destination IP	Source Port	Destination Port
129.10.123.1	10.10.0.3	893	674

Ans10.

Jamming signal is required in case of a collision on an ethernet network. When a collision is detected by a device, the device sends out a Jam signal.

Collisions on an ethernet shared medium network occur when multiple devices start to communicate or send a message at the same time resulting in the receiver receiving garbled data. Once the two senders detect the collision is happening, they send out a jam signal indicating the receivers that a collision occurred, and they should reject the data they've received so far.

After sending the jam signal, the stations must wait for a short period of time before attempting to start sending again. The time is randomized on the stations so the chances of a collision occurring again are minimal.

The jam signal should start with a 64-bit pattern of repeating 1s and 0s followed by a 32-bit portion that provides a dummy checksum value for the other transmitting device.

References:

[1]. RFIC 1541, Pg 15. tools.ietf.org/html/rfc1541