Q1

a) 1. Parity checking:

parity checking is divided into two kinds which are single bit parity and two-dimensional bit parity.

Single bit parity checks every bit of the message one by one while two-dimensional bit parity put them in a two-dimensional panel and check every columns and rows instead.

2. Internet checksum:

Internet checksum is used to detect errors in transmitted packets, and it is only used in transport layer.

In internet checksum, the sender computes the checksum through the information in the package and then put the checksum in the package. The receiver then computes the checksum through the information it receives and check whether it equals the checksum it receives from the sender. If they are different, the error is detected.

3. Cyclic redundancy check (CRC):

CRC treats the data bits as a binary number D and then choose a r+1 bit pattern G. Then, r bits of CRC bits are added to the end of D to make <D, R> exactly divisible by G in modulo 2. The receiver knows the generator G, it then divided the message it receives with G to see whether the result is 0. If it's not 0, the error is detected.

b) Because there is a greater possibility for frame collision to happen when using pure ALOHA.

The best channel used for useful transmission for slotted ALOHA is 37% while it is only 18% while using pure ALOHA.

Q2

a. Yes, it will crash.

b. EtherChannel can be configured to prevent this problem. Two channels can be grouped to work as one. Static (on mode), PAgP (Port Aggregation Protocol) and LACP (Link Aggregation Control Protocol) can be used to create EtherChannel.

c. Yes. STP can be used to set the priority (root bridge).

Q3

Broadcast domain: the collection of all devices in the network that can receive the same broadcast message.

Collision domain: the collection of all devices in the network that are connected to the same wire.

Repeater: repeater can separate VLAN but it can't separate broadcast domain or collision domain.

Hub: the devices that are connected through hub are actually connected through the same wire, so they are in the same broadcast domain and the same collision domain.

Switch: switch can separate collision domain but not broadcast domain.

Router: router can separate both collision domain and broadcast domain.

Q4

x:

Step	N'	D(z),p(z)	D(y),p(y)	D(w),p(w)	D(v),p(v)	D(u),p(u)	D(t),p(t)
0	x	8,x	6,x	6,x	3,x	∞	∞
1	xv	8,x	6,x	6,x		6,v	7,v
2	xvy	8,x		6,x		6,v	7,v
3	xvyw	8,x				6,v	7,v
4	xvywu	8,x					7,v
5	xvywut	8,x					
6	xvywutz						

t:

Step	N'	D(z),p(z)	D(y),p(y)	D(x),p(x)	D(w),p(w)	D(v),p(v)	D(u),p(u)
0	t	∞	7,t	∞	∞	4,t	2,t
1	tu	∞	7,t	∞	5,u	4,t	
2	tuv	∞	7,t	7,v	5,u		
3	tuvw	∞	7,t	7,v			
4	tuvwx	15,x	7,t				
5	tuvwxy	15,x					
6	tuvwxyz						

u:

Step	N'	D(z),p(z)	D(y),p(y)	D(x),p(x)	D(w),p(w)	D(v),p(v)	D(t),p(t)
0	u	∞	∞	∞	3,u	3,u	2,u
1	ut	∞	9,t	∞	3,u	3,u	
2	utv	∞	9,t	6,v	3,u		
3	utvw	∞	9,t	6,v			
4	utvwx	14,x	9,t				
5	utvwxy	14,x					
6	utvwxyz						

Q5

(a)

MAC address	interface	TTL
B	Interface of B	Time for frame (a) arrives

There is no record of B initially, so the switch records the information about B and will delete it in a period of time no frame with source address of B arrives in this period of time. The frame will be transmitted to A, C, D, E, F because the switch doesn't know where E is, which is called "flood".

(b)

MAC address	interface	TTL
B	Interface of B	Time for frame (a) arrives
E	Interface of E	Time for frame (b) arrives

The same happens to device E as it was in (a) to device B. The frame will be transmitted directly to B because the switch knows where B is.

(c)

MAC address	interface	TTL
B	Interface of B	Time for frame (a) arrives
E	Interface of E	Time for frame (b) arrives
A	Interface of A	Time for frame (c) arrives

The same happens to device A as it was in (a) to device B. The frame will be transmitted directly to B because the switch knows where B is.

(d)

MAC address	interface	TTL
B	Interface of B	Time for frame (a) arrives
E	Interface of E	Time for frame (b) arrives
A	Interface of A	Time for frame (c) arrives

The frame will be transmitted directly to A because the switch knows where A is.

Q6

The minimum packet size is 14+46+4 = 64 bytes. 14 is the Ethernet header, 4 is the Ethernet CRC. 46 is the minimum size of the Ethernet payload. The 64 bytes of the minimum size is fixed because it equals to the slot time. A collision could happens at any time before the end of the slot time, so if the packet is smaller than the slot time, the collision may not be detected by the sender which will leads to a cut down of throughput.

Q7

First, device 192.168.1.2 find out that the destination is not in its LAN, it then sends the packet to its default gateway which is 192.168.1.1. If it doesn't know the MAC address of the gateway, it will first broadcast an ARP packet in its LAN like this:

Source IP	Destination IP	Source MAC	Destination MAC
192.168.1.2	192.168.1.1	DC:85:ED:9E:DC:44	FF:FF:FF:FF:FF:FF

The router will then repeat it with the packet:

Source IP	Destination IP	Source MAC	Destination MAC
192.168.1.1	192.168.1.2	5F:1D:BC:6D:DE	DC:85:ED:9E:DC:44

Then 192.168.1.2 will send a packet like this:

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

If it knows the MAC address of the gateway, it will send the third packet directly.

The first router will then find out that the destination IP is in which router and then determine which is the next router. The packet will be like this:

Source IP	Destination IP	Source MAC	Destination MAC
192.168.1.2	10.0.0.3	5A:1F:58:55:AC:5F	5A:FF:AB:BB:AC:CD

The second router will then do the similar thing as the first one and send the packet like this:

Source IP	Destination IP	Source MAC	Destination MAC
192.168.1.2	10.0.0.3	5A:FF:34:FA:CC:AA	AA:BB:CC:DD:EE:FF

The third router is the same:

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

When the fourth router receives the packet, if the destination device is not in its ARP list, it will first broadcast an ARP packet like this:

Source IP	Destination IP	Source MAC	Destination MAC
10.0.0.1	10.0.0.3	5F:1A:5A:BC:FD:DD	FF:FF:FF:FF:FF:FF

The 10.0.0.3 will reply:

Source IP	Destination IP	Source MAC	Destination MAC
10.0.0.3	10.0.0.1	AB:50:CC:AA:EF:DD	5F:1A:5A:BC:FD:DD

The fourth router will then send the packet:

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

If 10.0.0.3 is in the ARP list of the fourth router, it will directly send the last packet.
The routing then ends.

Q8

First, device 192.168.1.2 find out that the destination is not in its LAN, it then sends the packet to its default gateway which is 192.168.1.1. If it doesn't know the MAC address of the gateway, it will first broadcast an ARP packet in its LAN like this:

Source IP	Destination IP	Source MAC	Destination MAC
192.168.1.2	192.168.1.1	DC:85:ED:9E:DC:44	FF:FF:FF:FF:FF:FF

The router will then repeat it with the packet:

Source IP	Destination IP	Source MAC	Destination MAC
192.168.1.1	192.168.1.2	5F:1D:BC:6D:DE	DC:85:ED:9E:DC:44

Then 192.168.1.2 will send a packet like this, the IP address and port number of the destination ISP is changed by the NAT router at the destination LAN:

Source IP	Destination IP	Source MAC	Destination MAC
192.168.1.2,3001	129.10.124.1,5002	DC:85:ED:9E:DC:44	5F:1D:BC:6D:DE

If it knows the MAC address of the gateway, it will send the third packet directly.
The first router will then find out that the destination IP is in which router and then determine which is the next router. The IP address and port number will be changed by NAT. The packet will be like this:

Source IP	Destination IP	Source MAC	Destination MAC
129.19.123.1,5001	129.10.124.1,5002	5A:1F:58:55:AC:5F	5A:FF:AB:BB:AC:CD

The second router will then do the similar thing as the first one and send the packet like this:

Source IP	Destination IP	Source MAC	Destination MAC
129.19.123.1,5001	129.10.124.1,5002	5A:FF:34:FA:CC:AA	AA:BB:CC:DD:EE:FF

The third router is the same:

Source IP	Destination IP	Source MAC	Destination MAC
129.19.123.1,5001	129.10.124.1,5002	FF:15:AD:BB:CA:CD	FF:15:AD:BB:CA:C1

When the fourth router receives the packet, if the destination device is not in its ARP list, it will first broadcast an ARP packet like this:

Source IP	Destination IP	Source MAC	Destination MAC
10.0.0.1	10.0.0.3	5F:1A:5A:BC:FD:DD	FF:FF:FF:FF:FF:FF

The 10.0.0.3 will reply:

Source IP	Destination IP	Source MAC	Destination MAC
10.0.0.3	10.0.0.1	AB:50:CC:AA:EF:DD	5F:1A:5A:BC:FD:DD

The fourth router will then send the packet:

Source IP	Destination IP	Source MAC	Destination MAC
129.19.123.1,5001	10.0.0.3	5F:1A:5A:BC:FD:DD	AB:50:CC:AA:EF:DD

If 10.0.0.3 is in the ARP list of the fourth router, it will directly send the last packet.
The routing then ends.

There are several benefits of using NAT:
1. It can ensure the security of the network in some degree. The outside networks won't know the topology of the LAN.
2. It can save IP addresses. The devices in the same LAN can use the same outside IP address.

Q9
In CSMA/CD, the node will keep on monitor the channel before sending data. Once the channel is idle, it will send the data immediately. If the collision happens while data is being sent, the collision may not be detected by the other nodes which may cause the data loss, so a jamming signal should be sent to strengthen the collision to ensure the other nodes in the network can detect the collision and stop sending data.