CSC358 - Problem Set 1

Arslan Qamar, 100 269 7897

January 20 , 2018

Solutions

1. This is an example of two-dimensional parity check.
1 1 1 0 — 1
1 0 1 1 — 1
1 0 0 0 — 1
- - - - - -
1 1 0 1 — 1

Below, the 0 at row 1 column 2 has been detected because it doesn't match the parity for row and column. Since it is detected, taking the bit at row 1 column 2 to invert it back to 0 in order to correct the error.
1 0 1 0 — 1
1 0 1 1 — 1
1 0 0 0 — 1
- - - - - -
1 1 0 1 — 1

Now, use the same example of two-dimensional parity check. Notice, in row 1, column 2 and column 3 values been inverted which show a double-bit error has been detected. The parity bits on column 2 and column 3 don't match the parity in the columns. However, row parity bits match the row 1, and one cannot find the intersection of row and column to find the inverted bits so it can't be corrected.
1 0 0 0 — 1
1 0 1 1 — 1
1 0 0 0 — 1
- - - - - -
1 1 0 1 — 1

2. (a) E will not perform an ARP query to find B's MAC address since they are not in the same subnet. E is aware that B is not in subnet 3 due to B's IP address. Depending on the situtation, E might have to find the R1's MAC address through the ARP request.
When sending Ethernet frame containing the IP datagram destined to B from E, the source and destination IP are E's and F's IP address respectively. The source MAC address is E's MAC address and destination MAC address is R1's MAC address.
   (b) When A will broadcast an ARP request message, Switch S1 will floods/forward the broadcast to all interfaces connected to it except from A (where broadcast came from). The router R1 will receive the ARP request message. However, it won't forward the message to Subnet 3.
Once B will receive the ARP request message, it will add A's MAC address and it will send back to Host A an ARP response message but it won't send ARP query message asking for A's MAC address. Because A's MAC address can be found from switch S1.
As the question says that S1 already has entries for host B, so it won't add in the forwarding table.

3. (a) The minimum RTT for the link would be:
$RTT = \frac{distance}{speedoflight}$
$= \frac{385000km*1000m}{3*10^8 \frac{m}{s}} = 1.283$
since it is round trip delay time, multiply by 2

$RTT = 1.283s * 2$
RTT = 2.566 s

(b) RTT as the delay which is 2.566 s
Bandwidth product 1-Gbps can be written like 125 MBps (mega-Byte per second) because 8 bits makes 1 Byte..
= delay * bandwidth product
$= 2.566s * 125MBps$
$= 320.75MB$
$\therefore$ the bandwidth delay product is 320.75 MB.

(c) The significance of the bandwidth-delay product is the data that can be sent before a receiver sees any of it.

(d) Calculate the transmission delay,
transmission delay = $\frac{messagesize}{bandwidthrate}$
$= \frac{25MB}{125MBps}$ (1-Gbps is equals to 125-MBps)
transmission delay = 0.2 s
=0.2 s + 2.566 s = 2.766 s (add the RTT time)
$\therefore$ The minimum amount of time that would elapse between when the request for the data goes out and transfer is finished is 2.766 s.

4. (a) latency = propagation delay + transmission delay
100 Mbps can be written like that $= 100Mbps * \frac{1000000bits}{1Mb} = 1000000000bits/s$
transmission delay $= \frac{12000bits}{1000000000bits/s} = 0.00012s(120\mu s)$
latency $= 10\mu s + 120\mu s = 130\mu s$
since from first bit sent to last bit received, $130 * 2 = 260\mu s$
$\therefore$ the latency would be $260\mu s$

(b) Each link will take $130\mu s$ including the propagation delay, so 3 switches and 4 links would take,
$= 4 * 130 = 520\mu s$

(c) By cut through switching, (100-Mbps is equivalent to $= 100Mbps * \frac{1000000bits}{Mb} = 100000000bits/s$)
$= \frac{200bits}{100000000bits/s} = 0.000002s(2\mu s)$
After propagation delay of $10\mu s$, then to send the remaining packet from (a) $120\mu s$ with a addition of propagation delay of $10\mu s$ again,
so altogether $2 + 10 + 120 + 10 = 142\mu s$

5. The following is the answer.

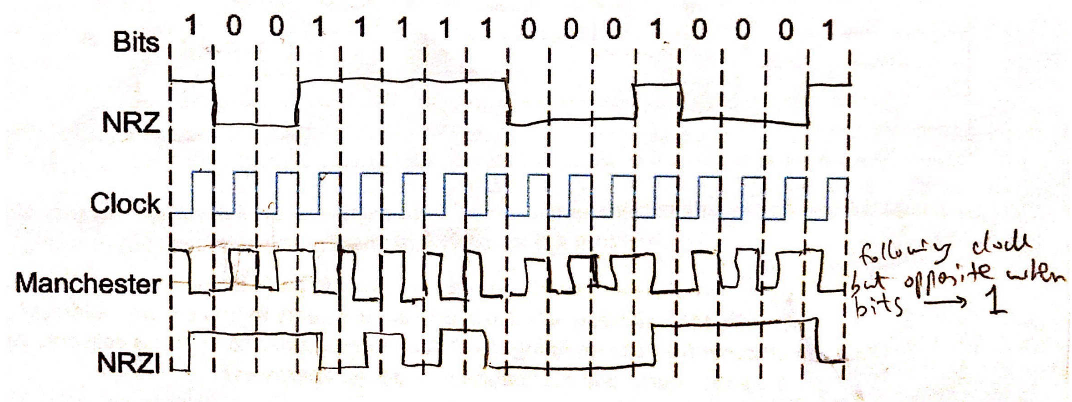

Figure 1: NRZ, Manchestor and NRZI encodings

6. (a) The transmit message is 1110 0011, append 000 to it so it becomes 1110 0011 000.
Divide by 1001 ($x^3 + 1$). The remainder would be 100
The transmit message would be 11100011100

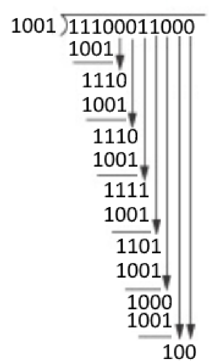

Figure 2: showing the long division

(b) Now, the message has been changed to 0110 0011 000.
To check the received signal take message 0110 0011 100 (100 is remainder from last part) which divide by 1001, if we get non-zero value then the receiver know that an error has occurred. Since, the remainder was 10 we know that an error has occurred.

7. The table below shows the data gram forwarding for every node.

For Node A

Destination	Node to Forward
A	-
B	C
C	C
D	C
E	C
F	C

For Node B

Destination	Node to Forward
A	E
B	-
C	E
D	E
E	E
F	E

For Node C

Destination	Node to Forward
A	A
B	E
C	-
D	E
E	E
F	F

For Node D

Destination	Node to Forward
A	E
B	E
C	E
D	-
E	E
F	E

For Node E

Destination	Node to Forward
A	C
B	B
C	C
D	D
E	-
F	C

For Node F

Destination	Node to Forward
A	C
B	C
C	C
D	C
E	C
F	C

Figure 3: data gram forwarding table for each node

8. There are many possible alterations in which ports are not selected by the spanning tree algorithm. The arrow shows which port won't be selected.

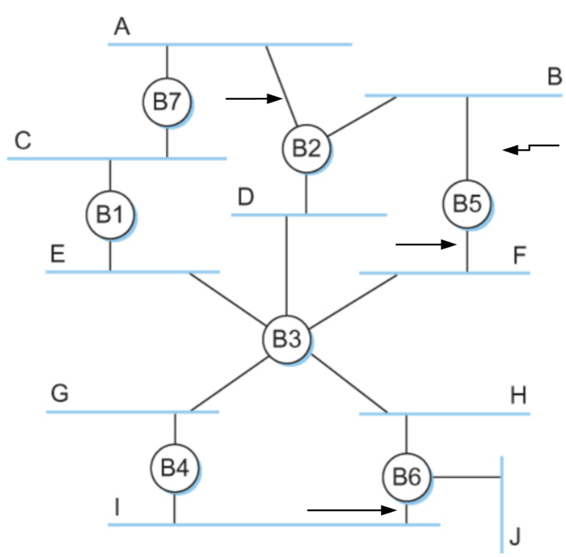

Figure 4: ports that are not selected by spanning tree algorithm

9. (a) Bridges B1, B2, B3 will learn the location of host X. Host Y would be able to see the packet because every bridge will send packet since they don't know where host W is located.

   (b) Bridges B1, B2 and B3 will learn the location of host Z. Host Y would not be able to see the packet since from part (a) the location of host X is already determined. And X is in B1's and B2's forwarding table.

   (c) Bridge B1 and B2 will be knowing the location of Y. Host Z will not be able to see the packet since it's not part of path and location of X is determined because X is in B1's and B2's forwarding table.

(d) Bridge B2 and B3 will learn the location of W. Host Z would be able to see the packet Basically, B3 have to flood since there is not entry of Y in forwarding table. .

10. (a) A-75 hosts needs $2^7 = 128$ and subnet mask would be 255.255.255.128
B-35 hosts needs $2^6 = 64$ and subnet mask would be 255.255.255.192
C-20 hosts needs $2^5 = 32$ and subnet mask would be 255.255.255.224

D-18 hosts needs $2^5 = 32$ and subnet mask would be 255.255.255.224 (this is right since we can't have more than 255)

(b) The limit for host is only 148 and if D grows to 32 hosts, the organization needs 14 more hosts. The possible solution is to break the each departments into more than 1 subnets specially department A. Or use the iPV6 technology.

11. (a) Assume for all parts, the router does the longest prefix match.
For destination 128.96.171.92, the subnet mask will be 255.255.254.0 and 128.96.170.0 as a subnet number, so deliver packets directly over interface 0.

(b) For destination 128.96.167.151, 255.255.254.0 would be the subnet mask and subnet number is 128.96.166.0, so forward packets to R2.

(c) For destination 128.96.163.151, subnet mask won't be applied, so use (default) and forward packets to R4.

(d) For destination 128.96.169.192, the subnet mask will be 255.255.254.0 and 128.96.168.0 as a subnet number, so deliver packets directly over interface 1.

(e) For destination 128.96.165.121, 255.255.252.0 would be the subnet mask and subnet number is 128.96.164.0, so forward packets to R3.

12. When two hosts on the same Ethernet shares the same hardware address, the information can be sent to the wrong host. The first host would receive the information intended for the second host and vice verse. Because Ethernet is considering the two host as one host. Even if deliver correct, the host can think that information don't belong to them. There are types of other complications that can also take place. This behavior is a problem because it compromises the information security for each host.