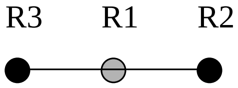
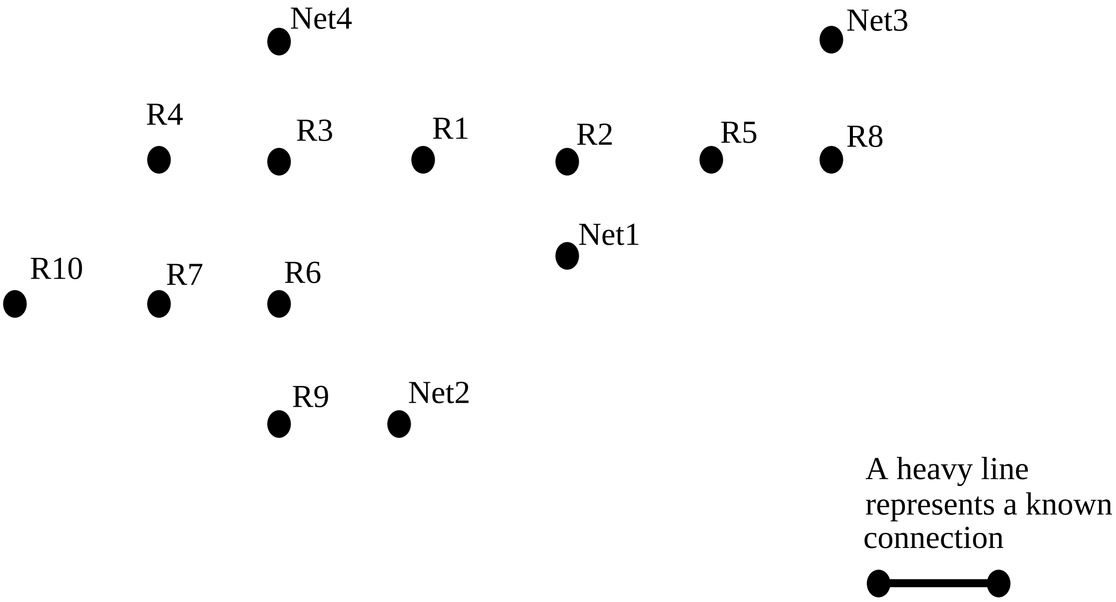
1) Internet Routing: OSPF or connecting the dots Value (15)

Given: Phase I Neighbour Identification Information, Ri is a router Neti is a network lan.
R1 neighbours R2 R3
R2 neighbours R1 R5 Net1
R3 neighbours R1 R4 R6 Net4
R4 neighbours R3 R5
R5 neighbours R1 R2 R4 R6 R8
R6 neighbours R3 R7 R9
R7 neighbours R6 R8 R9 R10
R8 neighbours R5 R7 R10 Net3
R9 neighbours R6 R7 Net2
R10 neighbours R7 R8

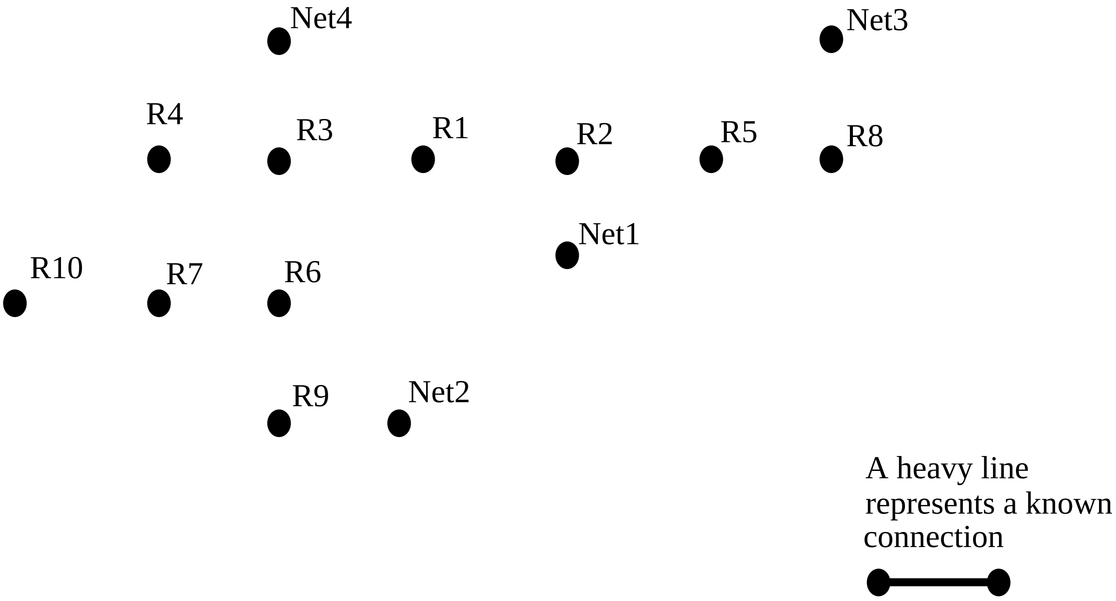
Phase I: For each router Ri draw its neighbours.
e.g.



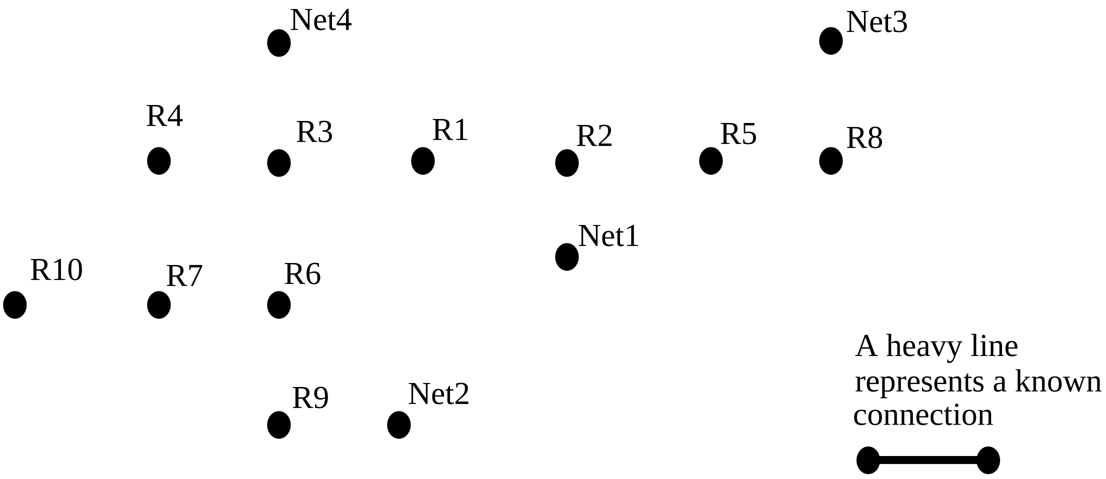
Phase II: First exchange of router connectivity with neighbours. Draw the connectivity graph from R1's perspective. That is, after the initial exchange of connectivity information with immediate neighbours what does the graph look like from R1? Draw heavy lines between nodes as the graph of the network develops.



Phase II: Second exchange of router connectivity with second nearest neighbours. Draw the connectivity graph from R1's perspective.



Phase II: Continued exchange of router connectivity. Draw the connectivity graph from R1’s perspective.



From the graph of the network developed, what is the routing table for R1? Assume all edges equal weight.

What does the routing network look like from R9’s perspective?

What is the routing table for R9?

2)Diffie Hellboy key exchange and ElGamal public key crypto. (15)
Part i) Diffie Hellboy (DH) key exchange.
You want to send Alice a secret 7 bit BES (Bob's encryption standard) key 1010101.
For this you are going to use DH, and decide together on the numbers g and n. (g=2, n =127).

You pick x=12 your secret number, Alice picks y=5 as her secret number.

You calculate 2^{12} mod 127 =X, Alice calculate 2^{5} mod 127 =Y. What are X and Y?

Exchange X and Y.

Alice calculates k = X^{5} mod 127. What is k?

You calculate k' = Y^{12} mod 127. What is k'?

How would you use k to securely encode and send the BES key?

How would Alice decrypt the BES key?

If Eve intercepted g, n, and X, what would she need to do the break the security of DH.

2 Part ii) ElGamal is a public key system closely related to DH key exchange.
You want to send Alice the message m="43". Go through the same DH key exchange process up but not including the X,Y exchange.

Alice posts Y as her public key.

You create a cipher text c by multiplying the message by Y exponentiated by x all mod 127.

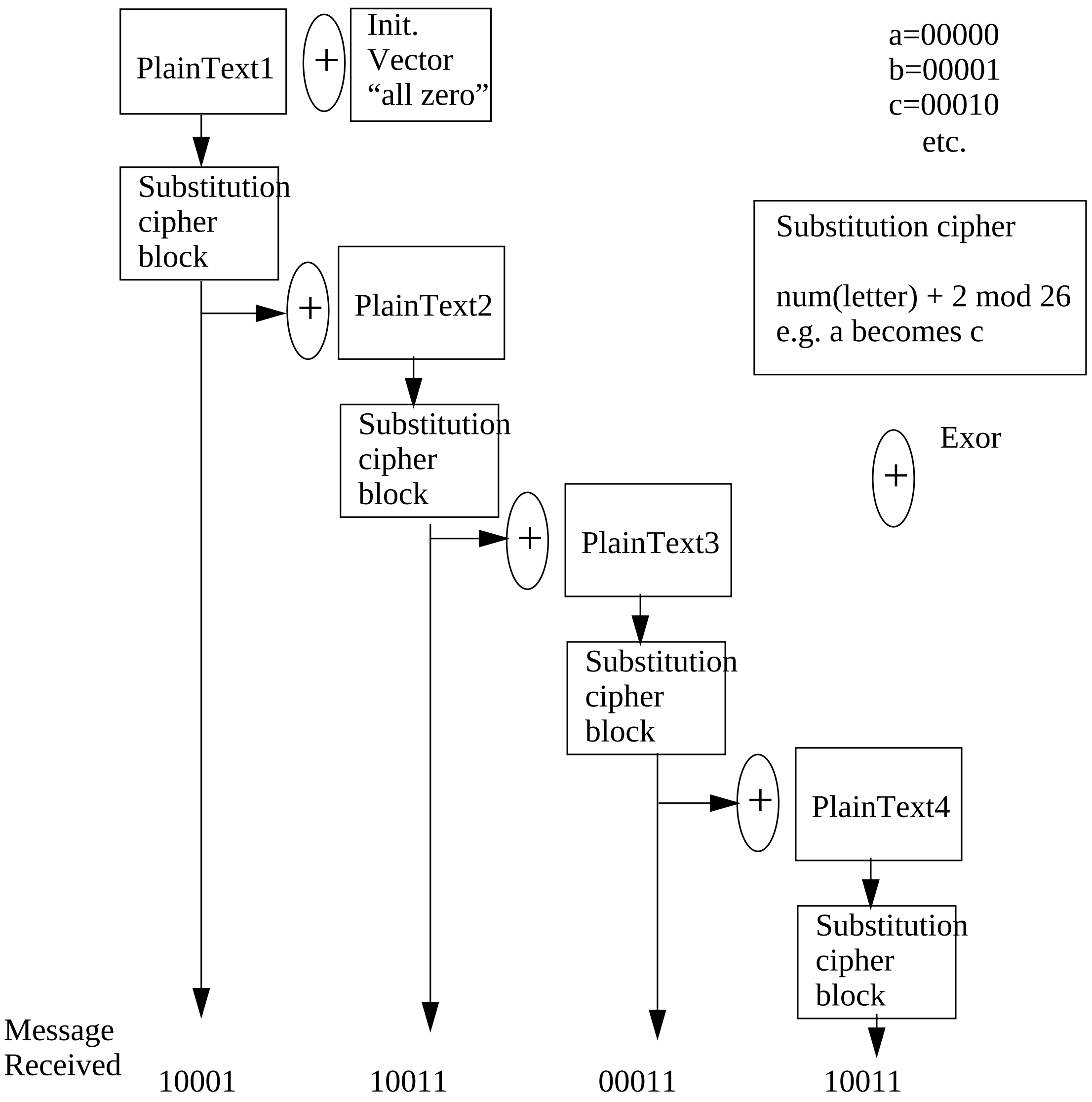
That is, $c = m\ Y^x$ mod 127 and send it to Alice along with X. What is c?

Alice decrypts the cipher m' = $c\ X^{-y}$ mod 127. Expand out m' and illustrate mathematically (symbolically) why m'=m.

What is the largest message (number of bits) that can be sent in the example above.

Bonus: In this example what is -y, or rather how would you calculate $c\ X^{-y}$ mod 127? This is a bonus worth 5, because I don't know the answer.

3) Substitution ciphers and block chaining. Value 15.
Given the following encryption system.



What is the original message? (I never checked it, so it might not be a real word)

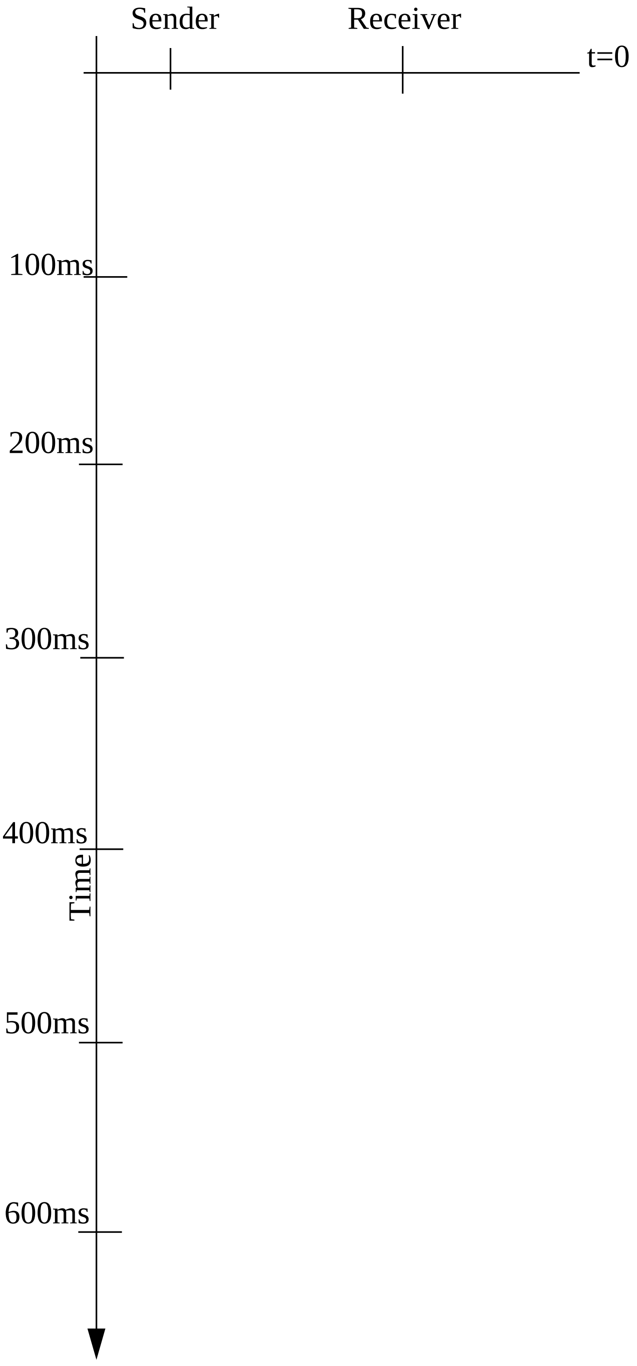
What is the point of block chaining?

How can the above scheme be used as a 5 bit hash on any number of characters?

How can it be used as a keyed hash?

4) Transmission Control Protocol: Value 15.
Part i) Slow Start: Congestion Threshold set at 16K Bytes. Advertised window set at 16K Bytes. MSS set at 1K Bytes. Congestion window initially set at 1K Bytes. RTT 100ms.

The transmission starts with the sender sending 1 1KB packet (8000 bits) on a 100Mbps network.
Sketch the Transmission Sequence Chart: Indicate the sender window size. (Error free mode)



Questions:

a)How long does it take for the sender's window to become 16K?

b)What is the throughput in Mbps after slow start, i.e. in steady state?

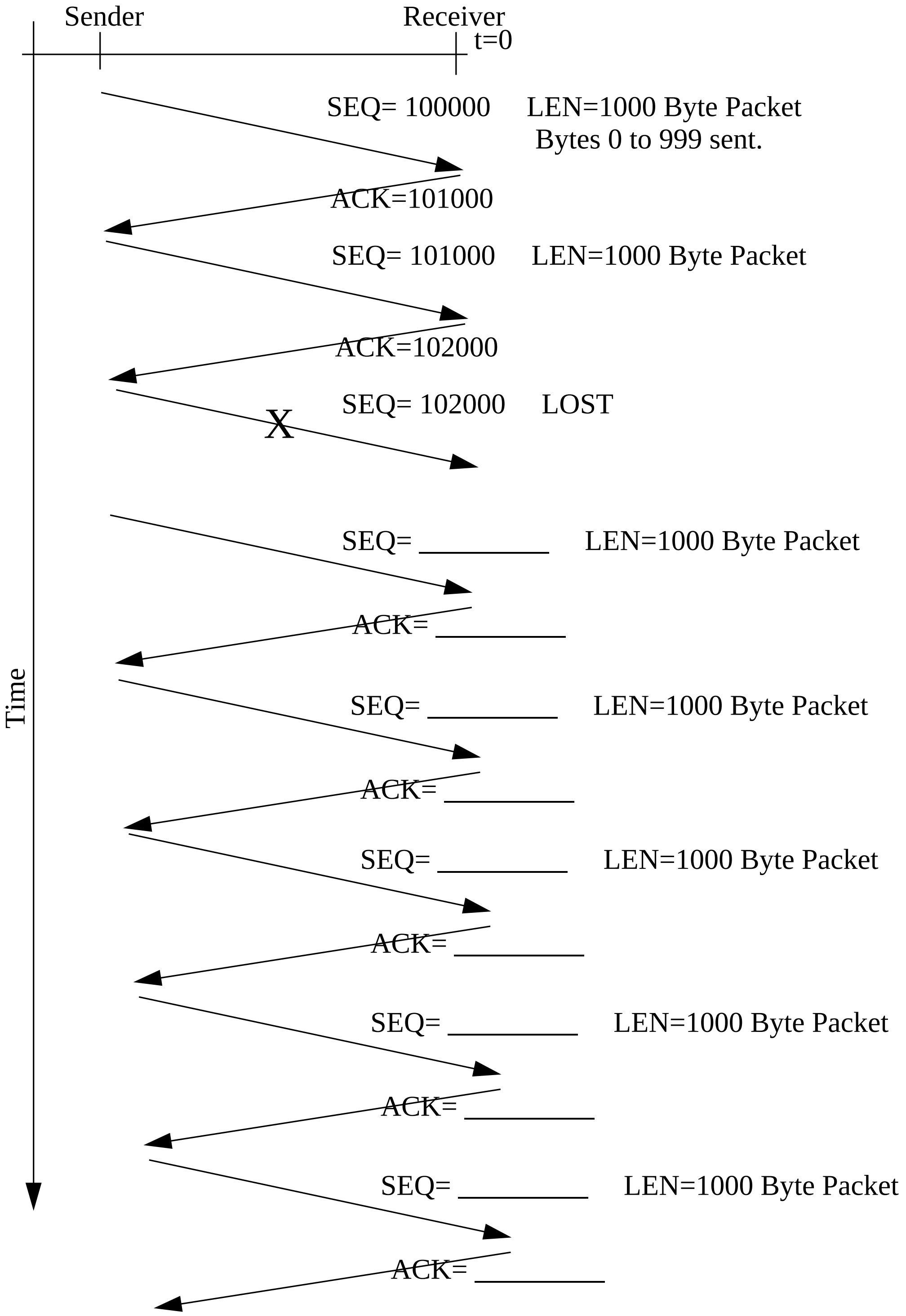
c)What is the efficiency?

d)What happens if the receiver's advertised window is 32K.

e)How long does it take for the sender's window to equal 32K?

f)What is the throughput after steady state in this case?

4 Part ii) Fast Retransmission. Assume sender window >32K. Timeout = 10 RTT. Maximum number of Duplicate ACKs is 3.


Sender
Receiver
t=0
SEQ= 100000 LEN=1000 Byte Packet
Bytes 0 to 999 sent.
ACK=101000
SEQ= 101000 LEN=1000 Byte Packet
ACK=102000
SEQ= 102000 LOST
X
SEQ= __________ LEN=1000 Byte Packet
ACK= __________
SEQ= __________ LEN=1000 Byte Packet
ACK= __________
SEQ= __________ LEN=1000 Byte Packet
ACK= __________
SEQ= __________ LEN=1000 Byte Packet
ACK= __________
SEQ= __________ LEN=1000 Byte Packet
ACK= __________
Time

5) CRC Fun with polynomial division. Value 20.

Sender side: Consider a frame of data consisting of Data = 1 0 0 1 0 1 1, or D(x)=x^6+x^3+x+1

The CRC polynomial is P(x) = $x^3 + x + 1$. Degree of the CRC is 3.

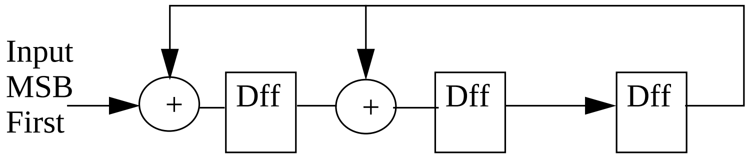
For the data calculate: D’(x) = x^3D(x), this is ordinary polynomial multiplication.
What is D’(x)?

CRC Remainder Generation: Divide D’(x) by the CRC polynomial.

Methods to use:
1) Either use long division of polynomials in GF(2). Multiplication is ordinary multiplication, 1x1=1, 1x0 = 0, addition and subtraction are the exor operation, 1+1 =0, 1+0 =1, 1-1 = 0, 0-1=1.
e.g.

$$
\begin{array}{rl}
 & \phantom{x^4 + x^3 + {}} x^2 + x \\ \cline{2-2}
x^2 + 1 \,\big| & x^4 + x^3 + x^2 + 1 \\
 & x^4 \phantom{{} + x^3 + {}} x^2 \\ \cline{2-2}
 & \phantom{x^4 + {}} x^3 + \phantom{x^2 + {}} 1 \\
 & \phantom{x^4 + {}} x^3 + \phantom{{}x^2} x \\ \cline{2-2}
 & \phantom{x^4 + x^3 + x^2 + {}} x + 1 \text{ (Remainder)}
\end{array}
\qquad
\frac{x^4 + x^3 + x^2 + 1}{x^2 + 1} = x^2 + x \;\; + R(x + 1)
$$

or 2) CRC Circuit analysis.



Initial conditions: the Dffs all set to zero.

Dff = D type FF

Operation after clocking in all the data D’(x), the CRC remainder R(x) is in the Dffs.

Add R(x) to D’(x) to obtain D”(x). What is D”(x)?

Send D”(x) to the receiver.

Receiver Side: After receiving D”(x), check it for errors using the CRC.

That is, Divide D”(x) by P(x) (the CRC polynomial). Either method described above can be used.

What is the CRC signature or remainder?

If the D(x) were corrupted during transit such that the original data x^6+x^3+x+1 were changed to x^6+x^3+x. What is the CRC that the receiver would calculate?

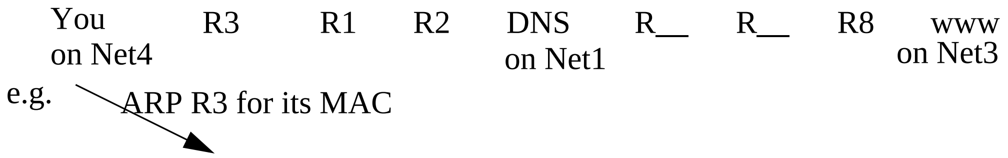
If the corrupted frame was associated with a wired Ethernet MAC, what would happen.

If the corrupted frame was associated with a wireless 802.11 MAC, what would happen?

6) Packet Sequence Events: Use the network of Question1. Value 10.
You are the lone host on Net4, the DNS server is on Net1, www.beerafterexamtastesgreat.com is on Net3.

Draw the packet sequence chart for initially contacting www.beerafterexamtastesgreat.com from your browser. (Include TCP connection handshake SYN and ACK flag settings)

The Network Routing Tables and ARP tables are up to date. Host ARP tables are not. That is routers know next router hop and the next router’s MAC address.



You on Net4 | R3 | R1 | R2 | DNS on Net1 | R__ | R__ | R8 | www on Net3

e.g. ARP R3 for its MAC

7) Confidence Boosters: Value 5

a) The IP header checksum, checks the IP header only.   True or False?

b) The TCP checksum, checks the TCP header plus the data payload.   True or False?

c) An IP network is packet switched. True or False?

d) This test was pretty hard. True or False?

e) All the answers in this section are True. True or False?

Appendix: Helpful hints

a mod b + c mod b = (a+c) mod b
a mod b x c mod b = (ac) mod b