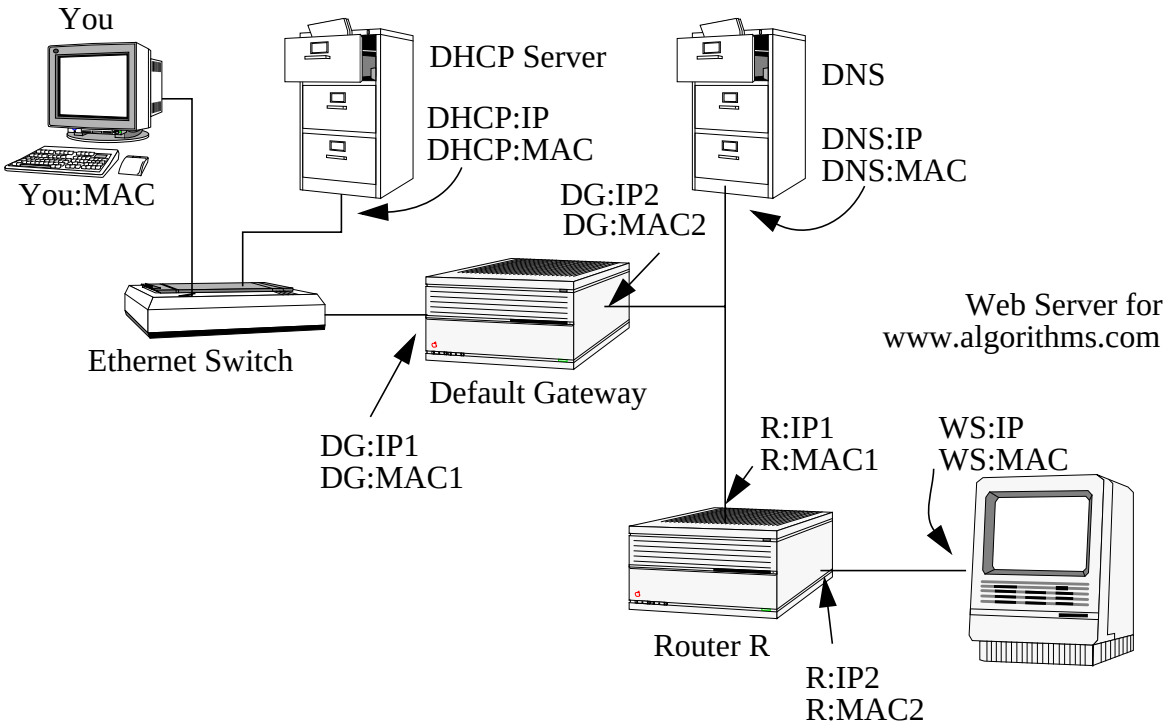
Final Exam: 24:370 2005

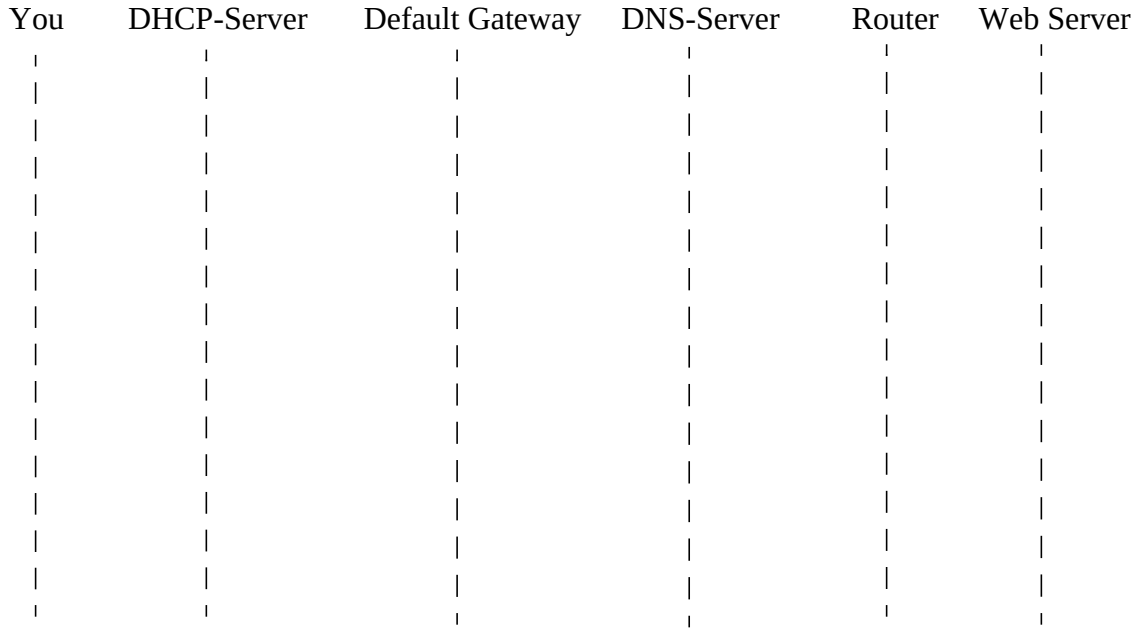
Question 1) Message Sequence Charts (MSC): Ultimately you would like to establish a TCP connection to a web server that houses a collection of your favorite algorithms. www.algorithms.com Value (25) (Network reproduced at back of test)

a) You arrive at work and turn your computer on (ARP tables are empty). The computer is DHCP enabled and knows the IP address of the DHCP Server, Default Gateway (router), and the IP address of the DNS Server. The network resembles the following:

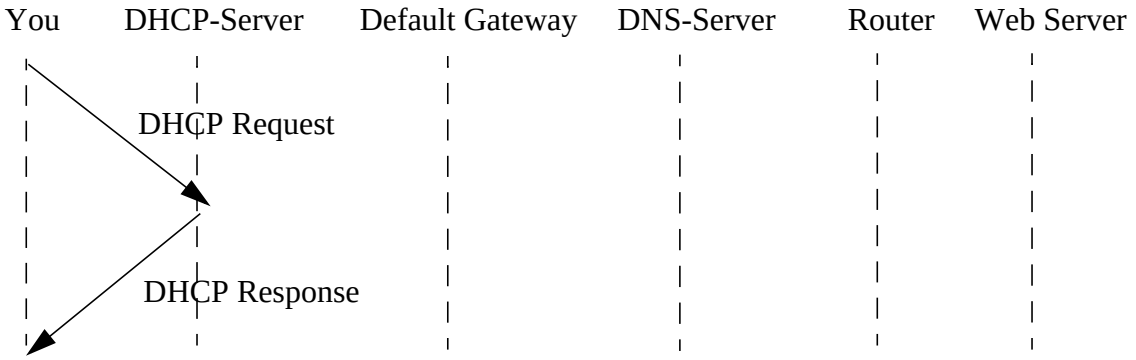


How does your machine acquire its IP address?

Sketch the MSC for acquiring your IP address, ie. You:IP. Assume the DHCP is simple a request response over udp. Remember the ARP tables on your machine are empty .



b)A more likely scenario for acquiring your IP address would be to broadcast the DHCP message and have any DHCP server on the network respond. In this manner the IP address of the DHCP Server does not have to be known in advance by the requesting client.
Assume the DHCP is simple a request response over udp. .



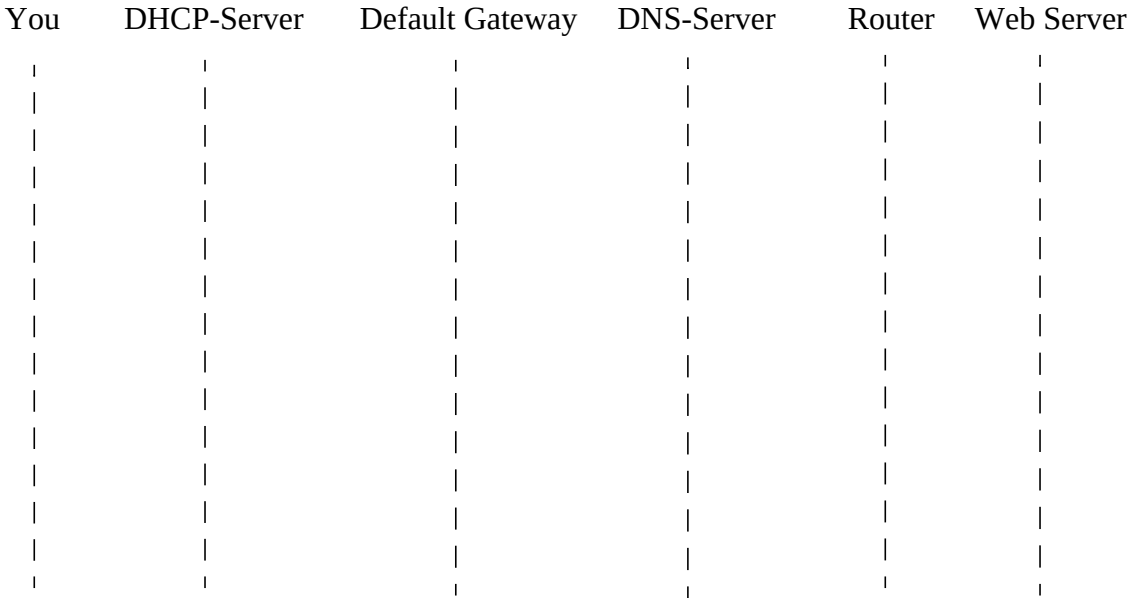
For the DHCP Request, what is the destination MAC address on the ethernet frame?
The MAC of the DHCP Server, or a broadcast? (Circle one)

For the DHCP Request, what is the destination IP address in the IP packet?
The IP address of the DHCP Server or an IP adress for a broadcast on this network.
(Circle one)

For the DHCP Response, what is the destination MAC address on the ethernet frame?
The MAC of the your machine, or a broadcast? (Circle one)

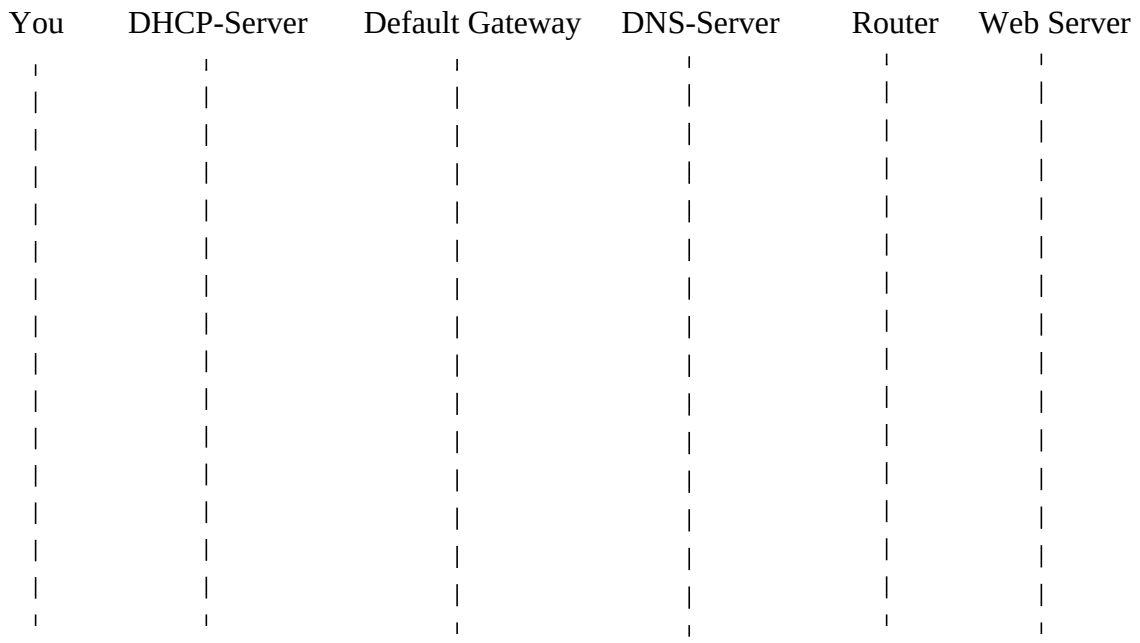
For the DHCP Response, what is the destination IP address in the IP packet?
The IP address of your machine or an IP adress for a broadcast on this network.
(Circle one)

c)Assume now that you now want to contact the www.algorithms.com. How does your machine acquire the IP address of the web server? Assume DNS is running over UDP.



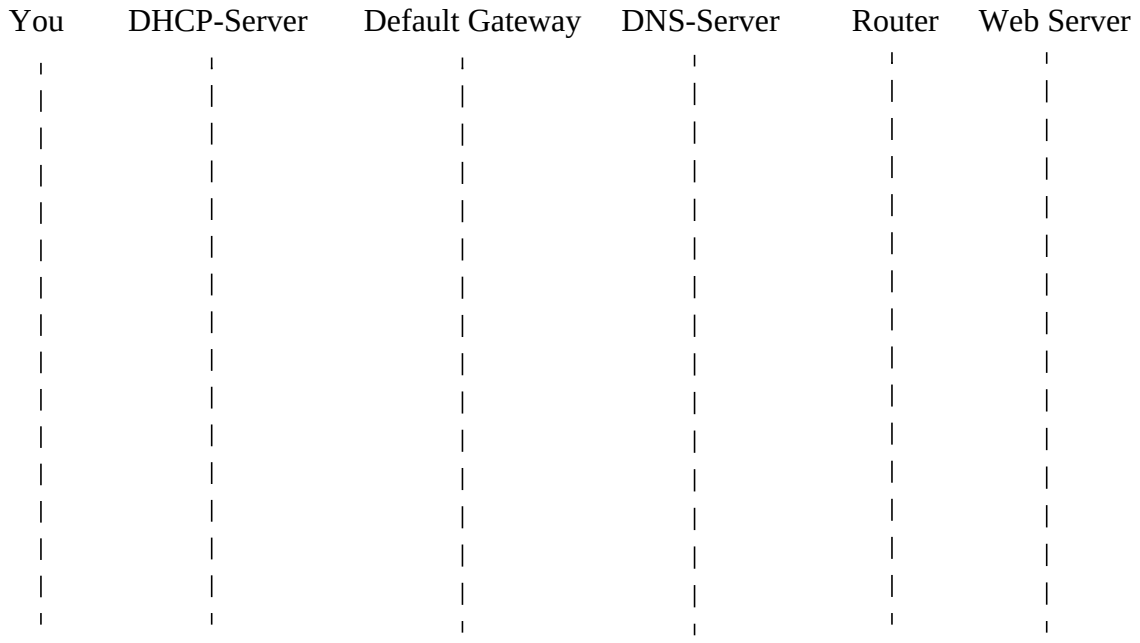
If the DNS server were listening on port 53. What would be the port numbers the client selected for the query?

d) Assume now that you want to initiate a TCP session with web server hosting www.algorithms.com. Sketch the MSC for the three way hand shake in TCP connection establishment.



If the web server were listening on port 80. What would be the port numbers the client selected for the TCP connection?

e) Assume now that you want to terminate the TCP session with web server hosting www.algorithms.com. Sketch the MSC for the four way hand shake in TCP connection tear down.



Final Exam: 24:370 2005

Question 2) MAC and IP addresses. Value (6)
a) MAC addresses are local or global? (Circle one)

b) IP addresses are local or global? (Circle one)

c) For an IP packet traversing from your machine to www.algorithms.com fill in the following table.

Network Leg		Source	Destination
You to Ethernet Switch	IP address		
	MAC address		
Ethernet Switch to Default Gateway	IP address		
	MAC address		
Default Gateway to Router R	IP address		
	MAC address		
Router R to Web Server	IP address		
	MAC address		

d) Assume that the Default Gateway provided Network Address Translation. i.e. The IP address assigned by the DHCP Server was non routable on the Internet. Again for an IP packet traversing from your machine to www.algorithms.com fill in the following table.

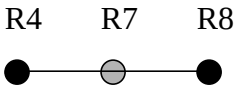
Network Leg		Source	Destination
You to Ethernet Switch	IP address		
	MAC address		
Ethernet Switch to Default Gateway	IP address		
	MAC address		
Default Gateway to Router R	IP address		
	MAC address		
Router R to Web Server	IP address		
	MAC address		

Final Exam: 24:370 2005

Question 3) Internet Routing: OSPF or connecting the dots Value (14)

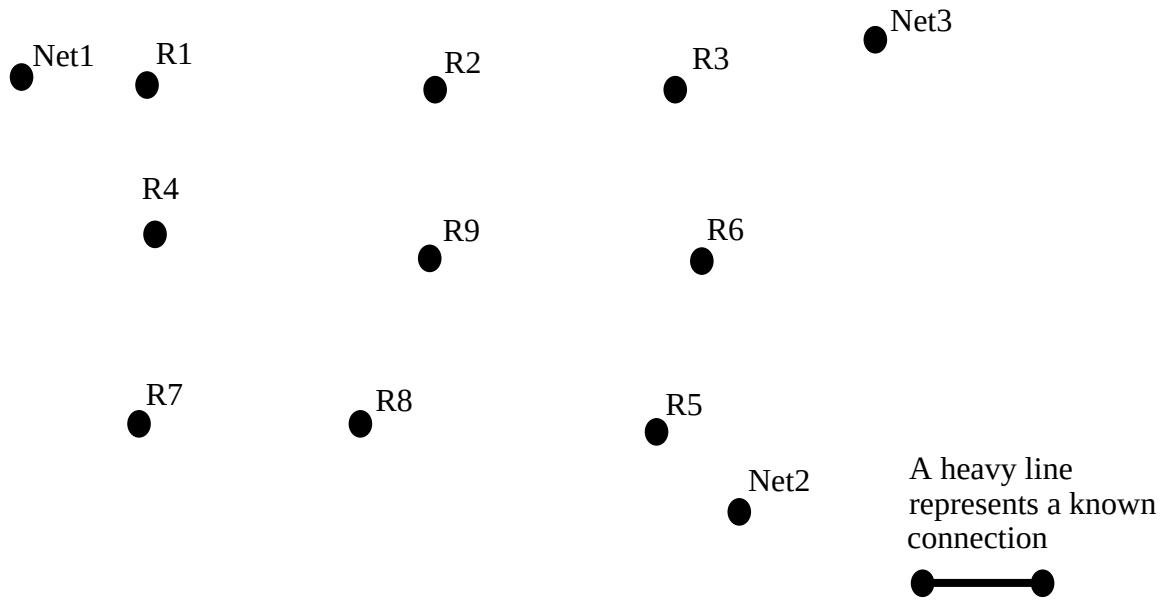
Given: Phase I Neighbour Identification Information, Ri is a router Neti is a network lan.
R1 neighbours R2 R4 R9 Net1
R2 neighbours R1 R3 R9
R3 neighbours R2 R6 Net3
R4 neighbours R1 R7 R9
R5 neighbours R6 R8 R9 Net2
R6 neighbours R3 R5 R9
R7 neighbours R4 R8
R8 neighbours R5 R7 R9
R9 neighbours R1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

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

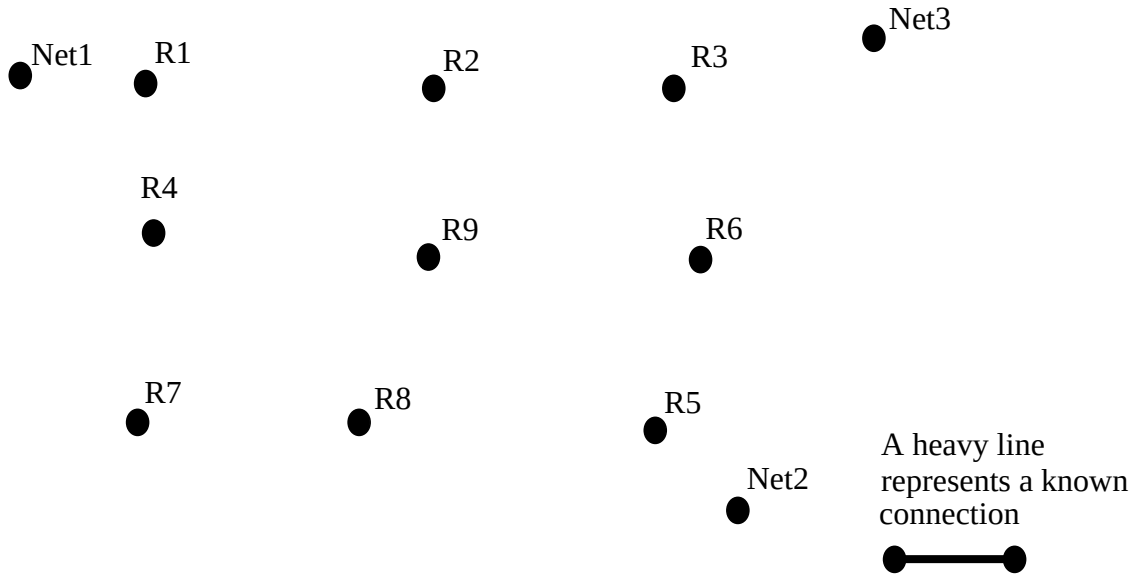


Final Exam: 24:370 2005

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.

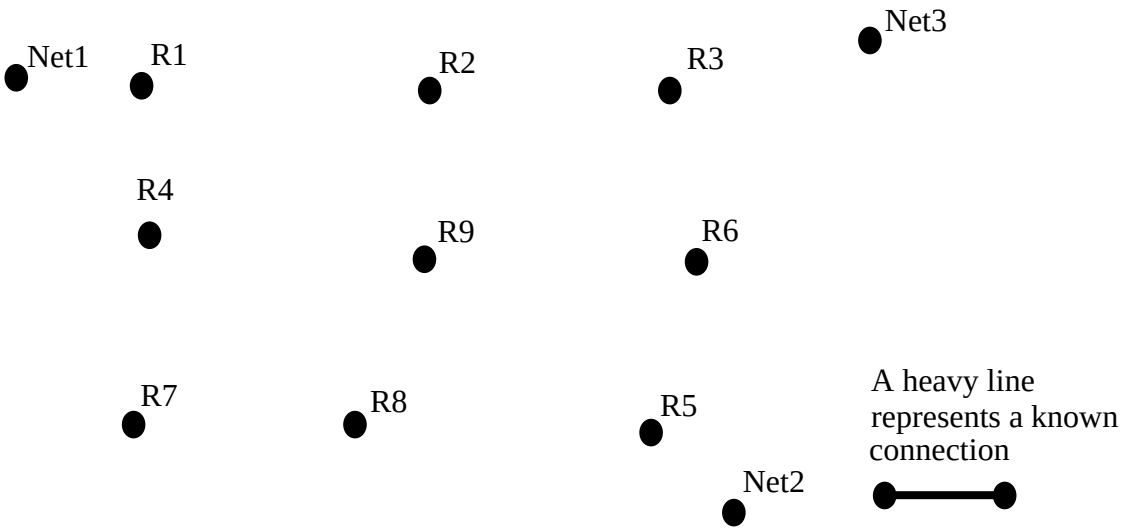


Phase II: Second exchange of router connectivity with second nearest neighbours. Draw the connectivity graph from R1's perspective.



Final Exam: 24:370 2005

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



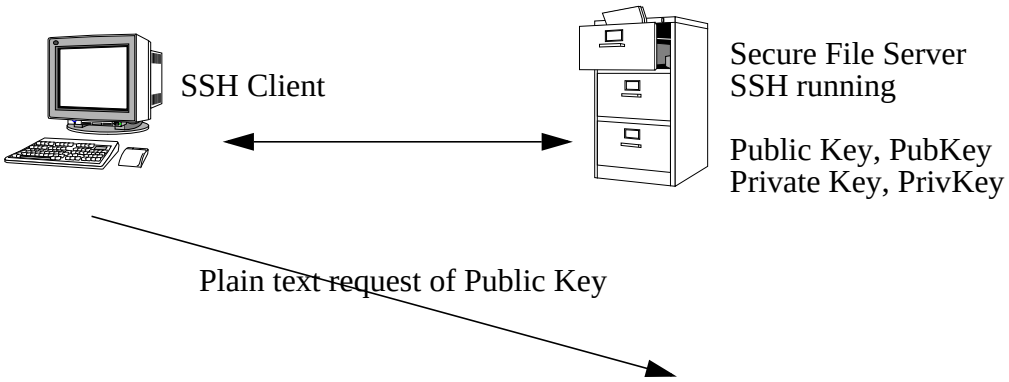
From the graph of the network developed, what is the routing table for R1? Assume all edges equal weight.

What does the network look like from R9's perspective?

If R9 crashes, after OSPF stabalizes what is new route from Net1 to Net2?

Final Exam: 24:370 2005

Question 4) SSL, provides a secure connection for a shell tool or secure file transfer. The basic idea is to combine a key exchange machanism with a secret key encryption algorithm. Sketch a message sequence chart that illustrates the high level exchange of messages that facilitates the secure connections. Assume RSA for the public key, DES for the private key. Value(5)



SSL operates above what level in the protocol stack?

What is an advantage of SSl over IPSec with respect to operating system requirements?

Final Exam: 24:370 2005

Question 5) You want to use a CRC as a hash function for a fingerprint. Albeit not the most secure it is simple.
Value (5).

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

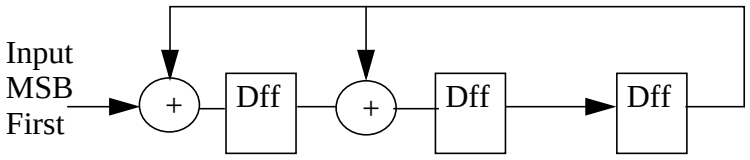
a) CRC Hash Generation: Divide D(x) by the CRC polynomial, the remainder is the hash. What is the hash R(x)?

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.

$$
\begin{array}{r}
 & x^2 + x \\
\hline
x^2 + 1 \;\big|\; x^4 + x^3 + x^2 + 1 \\
 \quad x^4 \qquad\quad x^2 \\
\hline
 \qquad x^3 + \qquad 1 \\
 \qquad x^3 + \quad x \\
\hline
 \qquad\qquad x + 1 \text{ (Remainder)}
\end{array}
$$

$$
\frac{x^4 + x^3 + x^2 + 1}{x^2 + 1} = x^2 + x + R(x+1)
$$

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.

b) This hash R(x) is the fingerprint for D(x). Assume that a shared secret key was generated using Diffie Hellman key exchange and has the value 1010. Sketch a system that allows a person to send D(x) and authenticate D(x), i.e. provide some degree of security against tampering.

Final Exam: 24:370 2005

Question 6) Short snappers Value (8)

a) How can a hash function that takes 512 bits in and generates a 128 bit hash be used to hash a file that may be 1 MB in size?

b)What is meant by hidden nodes on an 802.11 netork?

c) How are collisions avoided on an 802.11 network if two nodes can not hear each other? That is how are RTS/CTS frames used to affect collision avoidance?

d) What is $2^{126} \bmod 127$, $3^{126} \bmod 127$, and $99^{126} \bmod 127$? Why?

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

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

g) A telephone network is circuit switched. True or False?

h) A TCP checksum is a strong integrity check. True or False?

Final Exam: 24:370 2005

Question 7) TCP throughput (Show your work) Value (18)

a) A machine is connected to a 100Mbps network to another machine that is 100 msec away. Assume the machine is running a TCP stack that allocated a 15 KByte buffer. If the recieving machine has an advertized window of 15KByte, what is the average throughput in the steady state? What is the bandwidth utilization?

Assume now that the sending machine is running a TCP stack that allocated a 30 KByte buffer. If the recieving machine has an advertized window of 15 KByte, what is the average throughput in the steady state? What is the bandwidth utilization?

If the recieving machine now advertizes its window to be 30 KByte, what is the average throughput in the steady state? What is the bandwidth utilization?

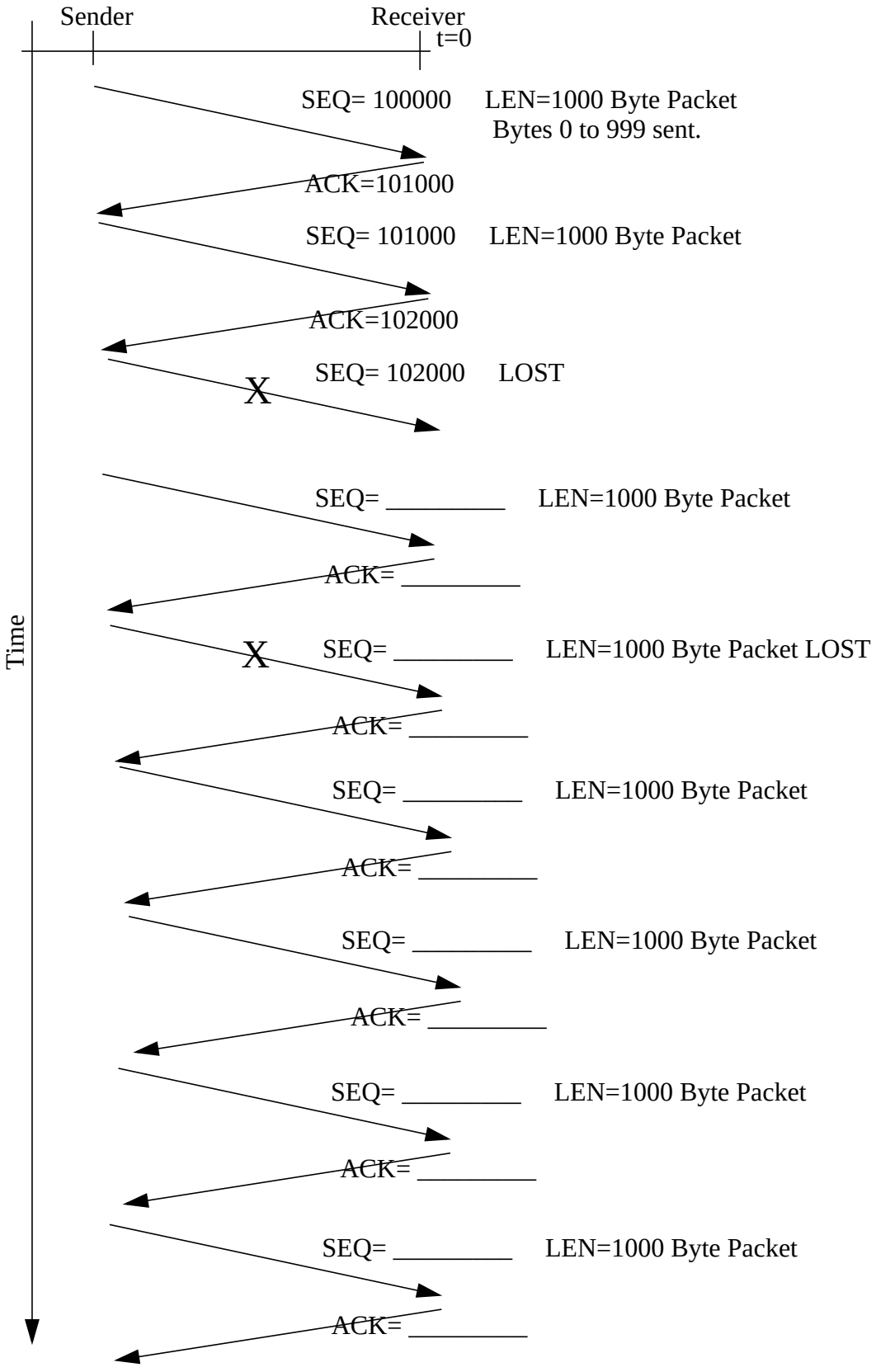
You are unhappy with the performance and decide to upgrade the network to GigE. That is, GigaBit Ethernet, 1000 Mbps. Assuming a sender buffer of 30KBytes and an advertized window of 30KBytes, what is the average throughput in the steady state? What is the bandwidth utilization?

You now hack both kernels and their TCP stacks and all interveining routers to support a 3KByte IP packet. Assuming a sender buffer of 30KBytes and an advertized window of 30KBytes, what is the average throughput in the steady state? What is the bandwidth utilization?

For the situation of standard IP packets and a 100 Mbps network, what is the optimal buffer size at the sender and reciever to obtain maximal throughput.

Final Exam: 24:370 2005

Question 8) Fast Retransmission. Assume sender window >32K. Timeout = 10 RTT. Maximum number of Duplicate ACKs is 3. Value(5)



Final Exam: 24:370 2005

Hints:
Primes are generated using a pseudo primailty test relying on Fermat's little theorem which states $a^{p-1} \bmod p = 1$ when p is prime.

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

Network of Question 1 for Reference