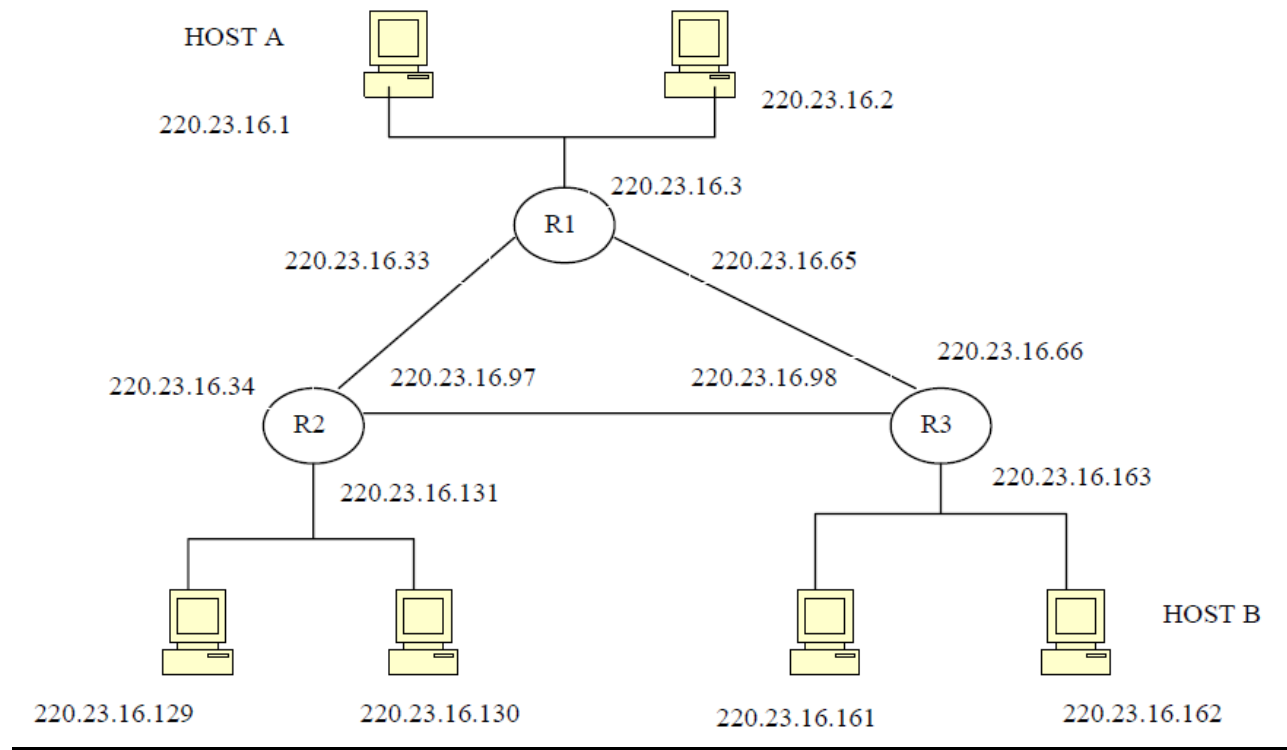


Final Exam
Computer Networks Fall 2015
Prof. Cheng-Fu Chou

Question 1: CIDR (10%)

You are given a pool of **220.23.16.0/24** IP addresses to assign to hosts and routers in the system drawn below:



- a) (3%) How many separate networks are in the system?

There are 6 networks.

- b) (7%) Partition the given address space and assign addresses to the networks. To answer this question properly you should write down the addresses of all of the networks in the CIDR **A.B.C.D/x** format.

220.23.16.0/(27~30)

220.23.16.32/(27~30)

220.23.16.64/(27~30)

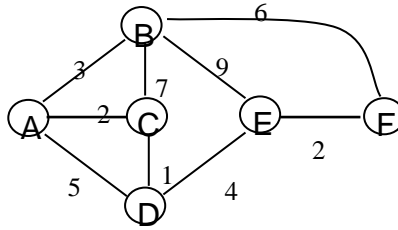
220.23.16.96/(27~30)

220.23.16.128/(27~30)

220.23.16.160/(27~30)

Question 2: Routing Algorithms (30%)

- a) (10%) Consider the network shown below. Show the operation of Dijkstra's (Link State) algorithm for computing the least cost path from A to all destinations.



Step	N'	D(B) p(B)	D(C) p(C)	D(D) p(D)	D(E) p(E)	D(F) p(F)
0	A	3,A	2,A	5,A	∞	∞
1	AC	3,A		3,C	∞	∞
2	ACB			3,C	12,B	9,B
3	ACBD				7,D	9,B
4	ACBDE					9,B (9,E)
5	ACBDEF					

or

Step	N'	D(B) p(B)	D(C) p(C)	D(D) p(D)	D(E) p(E)	D(F) p(F)
0	A	3,A	2,A	5,A	∞	∞
1	AC	3,A		3,C	∞	∞
2	ACD	3,A			7,D	∞
3	ACDB				7,D	9,B
4	ACDBE					9,B (9,E)
5	ACDBEF					

- b) (20%) Consider the three-node topology: the link costs are $c(x,y)=6$, $c(y,z)=2$, and $c(z,x)=50$. We focus here only on y's and z's distance table entries to destination x. Please explain the details of how the DV algorithm could reach a quiescent (or stable) state when the following cases happen.

- a. (5%) When $c(x,y)$ decreases from 6 to 1.

First, Y detects link-cost change, updates its DV, and informs its neighbors. Then, Z receives the update from Y, updates its table, computes new least cost to X, and sends its neighbors its DV. Finally, Y receives Z's update, and updates its distance table. Y's least costs do not change, so it does not send a message to Z again.

- b. (5%) When $c(x,y)$ increases from 6 to 55.

First, Y detects link-cost change, computes new least cost to X via Z (6 to 10), and sends its neighbors its DV. Then, Z receives the update from Y, updates its table, computes new least cost to X via Y (8 to 12), and sends its neighbors its DV. After several iterations, Y and Z's least cost to X eventually converge to 52 and 50.

- c. (10%) How the poisoned reverse solves the above looping problem.
“Poisoned reverse” means that if Z routes through Y to get to X, Z tells Y its (Z’s) distance to X is infinite. This solves the looping problem since Y won’t route to X via Z (That is, $Y \rightarrow Z \rightarrow Y \rightarrow Z \dots$ will not occur).

Question 3: Network Address Translation (10%)

- a) (6%) Briefly describe how NAT works.
Every (IP address, port #) of a message leaving the internal network is mapped by the NAT gateway to a (NAT IP address, new port #) pair which is stored by the NAT gateway node. When a message from outside arrives at the NAT gateway node for that port # the NAT gateway node checks its table and sends the message on to the proper (IP address, port #) in the internal network.
- b) (2%) What problem was NAT introduced to solve?
Local networks running out of IP addresses.
- c) (2%) Give one reason why NAT is controversial. (In class, we discussed a few. Just give one of them).
1. Routers should only process up to level 3 but NAT routers process higher up (they need to be aware of applications).
 2. NAT violates the end-to-end argument.
 3. NAT translation can cause problems when designing applications.

Question 4: Multiple Access Protocols (12%)

- a) (2%) List one advantage and one disadvantage of using channel-partitioning MAC protocols.
Advantage: shares channel efficiently at high loads
Disadvantage: inefficient at low loads
- b) (2%) List one advantage and one disadvantage of using random-access MAC protocols.
Advantage: efficient usage of channel at low loads
Disadvantage: inefficient at high loads (due to collision overhead)
- c) (4%) The standard Ethernet CSMA/CD protocol uses *exponential backoff*. First, describe the Ethernet *exponential backoff* algorithm (your explanation must include why it is called *exponential*). Next, explain the reason(s) for using exponential backoff.

After a collision choose K at random from $\{0, 1, 2, \dots, 2^{\min(m,10)} - 1\}$ and wait $K * 512$ bit times before sensing channel again. m is the number of collisions encountered while trying to broadcast this particular frame. It is called exponential backoff due to the $2^m - 1$ term.

The reason for using exponential backoff is that if there have been a lot of collisions so far this implies that there are many nodes trying to access the link at the same time.

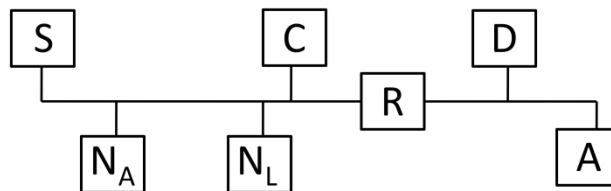
Increasing the possible range of waiting times from which the link(s) choose makes it more likely that no two nodes will choose the same waiting time.

- d) (4%) The 802.11 wireless LAN protocols use CSMA/CA instead of CSMA/CD. Explain why 802.11 **does not** use CSMA/CD.

Due to the hidden terminal problem. When using wireless LAN it is not always possible to do collision detection.

Question 5: Your Web Browser in action (15%)

In the topology shown below, machine A is a desktop client, D is a local DHCP server, R is A's gateway router, S is a Web server, and C is a Web cache. N_L is C's local nameserver, while N_A is the nameserver authoritative for S. Client A is configured to use Web cache C for all requests (assume that the Web cache resolves the name for any Web server and that the client is configured with the IP address of the cache). All wires/links are Ethernet segments.



Assume the following:

- All the machines were just booted and their associated caches (ARP, DNS, Web, persistent connections) are all empty
- `http://S/index.html` fits in a single packet
- Persistent HTTP connections are used among A, C, and S (i.e. you should assume that once

any connection between these hosts is established it is never closed)

- Web caches respond to TCP requests that look like packet two in table 1 below (e.g., GET http://foo/bar/). They reply with the normal web cache contents.

a) (8%) The user on machine A, requests the web page http://S/index.html. The table below shows a number of messages sent/received in servicing this request (this is not necessarily a complete list of all packets). In addition, there are a few bogus packets that are never sent/received. The packets are not listed in temporal order.

ID	SRC	DST	SRC Port	DST Port	Protocol	Contents
1	C	DNS root		DNS	UDP	Query for S
2	A	C		Web cache	TCP	GET http://S/index.html
3	N _L	DNS root		DNS	UDP	Query for S
4	C	S		HTTP	TCP	SYN
5	C	S		HTTP	TCP	GET index.html
6	S	A	HTTP		TCP	index.html
7	A	Broadcast			ARP	Who is R
8	C	A	Web cache		TCP	index.html
9	N _L	C	DNS		UDP	Address for S
10	S	C	HTTP		TCP	index.html
11	A	Broadcast		DHCP	UDP	DHCP Request from A
12	N _L	N _A		DNS	UDP	Query for S

List the proper order of packets (in terms of their IDs) that are sent on the network:

11, 7, 2, 3, 12, 9, 4, 5, 10, 8

b) (7%) Assume that the client A has no local Web or DNS cache and that cache C has no DNS cache. However, all other cacheable things are cached. On a subsequent request for http://S/index.html, which of your items from your list in (5a) would be eliminated? (Use the ID column to name the messages.)

11, 7, 3, 12, 9, 4, 5, 10

Question 6: Multiple choice (8%)

6a. Which best describes the Ethernet protocol? (Circle ONE)

- A. Talk only if you hear no one else talking, but stop as soon as you hear anybody else.
- B. Pass a ticket around and only talk if you are holding the ticket.

- C. Raise your hand and wait till a moderator gives you permission to talk.
- D. Every person is scheduled a time to talk.

A

6b. Which of the following is/are true about a communications channel that uses time-division multiplexing?

(Circle ALL that are correct)

- A. There may be times when the channel is idle, even if a sender has data to send on the channel.
- B. The channel requires the sender's and receiver's clocks to be closely synchronized.
- C. Data in the channel could experience variable delays due to queuing.
- D. In times of high utilization, a sender could be completely denied access to the channel.

A, B

6c. Which of the following is/are true about increase/decrease policies for fairness and efficiency in congestion control? (Circle ALL that are correct)

- A. Additive increase reduces fairness.
- B. Additive increase improves efficiency.
- C. Multiplicative increase improves fairness.
- D. Multiplicative decrease improves fairness.

B, D

6d. Which of the following is/are true about web caches? (Circle ALL that are correct)

- A. A web cache, or proxy server, is a network entity that satisfies HTTP requests from clients.
- B. A web cache is both a client and a server at the same time.
- C. HTTP does not explicitly support caching or cache consistency.
- D. All HTTP objects are cacheable.

A, B

Question 7: Pipelined protocols (homework review) (10%)

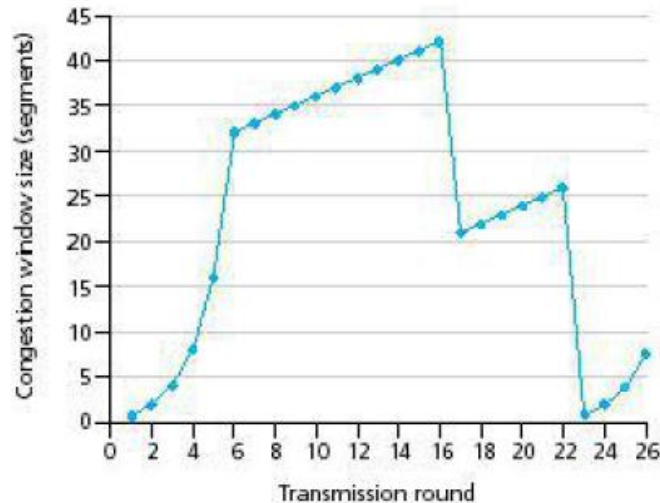
Consider the Go-Back-N (GBN) protocol with a sender window size of 4 and a sequence number range of 1024. Suppose that at time t , the next in-order packet that the receiver is expecting has a sequence number of k . Assume that the medium does not reorder messages. Answer the following question:

What are the possible sets of sequence numbers inside the sender's window at time t ? Please list all possible sets and justify your answer.

Here we have a window size of $N = 4$. Suppose the receiver has received packet $k - 1$, and has ACKed that and all other preceding packets. If all of these ACK's have been received by sender,

then sender's window is $[k, k + N - 1]$. Suppose next that none of the ACKs have been received at the sender. In this second case, the sender's window contains $k - 1$ and the N packets up to and including $k - 1$. The sender's window is thus $[k - N, k - 1]$. By these arguments, the sender's window is of size 4 and begins somewhere in the range $[k - 4, k]$.

Question 8: TCP congestion control (homework review) (20%)



Assuming TCP Reno is the protocol experiencing the behavior shown above, answer the following questions. In all cases, you should provide a short discussion justifying your answer.

- a) (4%) After the 16th transmission round, is segment loss detected by a triple duplicate ACK or by a timeout? How about 22nd transmission round?

1. Triple duplicate ACK. Because the congestion window size only becomes half the value after 16th round.
2. Timeout. Because the congestion window size has dropped to 1 after 22th round.

- b) (4%) What is the value of *ssthresh* at the 24th transmission round?

13.

The threshold is set to half the value of the congestion window when packet loss is detected. When loss is detected during 22nd transmission round, the congestion windows size is 26. Hence the threshold is 13 during the 24th transmission round.

- c) (4%) Assuming a packet loss is detected after the 26th round by the receipt of a triple duplicate ACK, what will be the values of the congestion window size and of *ssthresh*?

4, 4.

The congestion window and threshold will be set to half the current value of the congestion window (8) when the loss occurred. Thus the new values of the threshold and window will be 4.

- d) (4%) Suppose TCP Tahoe is used (instead of TCP Reno), and assume that triple duplicate ACKs are received at the 16th round. What are the *ssthresh* and the congestion window size at the 20th round?

21, 8.

Threshold is set to $42/2 = 21$. The congestion window size is first reset to 1, and then grows to 8 in 20th round.

- e) (4%) Again suppose TCP Tahoe is used, and there is a timeout event at 22nd round. How many packets have been sent out from 17th round till 22nd round, inclusive?

17th round, 1 packet;

18th round, 2 packets;

19th round, 4 packets;

20th round, 8 packets;

21st round, 16 packets;

22nd round, 21 packets.

So, the total number is 52.