Carnegie Mellon
Computer Science Department.
15-441 Fall 2011
Midterm

Name: ______________________________

Andrew ID: ______________________________

INSTRUCTIONS:

There are **??** pages (numbered at the bottom). Make sure you have all of them.

Please write your name on this cover and at the top of each page in this booklet **except the last.**

If you find a question ambiguous, be sure to write down any assumptions you make.

It is better to partially answer a question than to not attempt it at all.

Be clear and concise. Limit your answers to the space provided.

A	B	C	D	E	F	Total
/ 15	/ 24	/ 9	/ 14	/ 17	/ 1	/ 80

A True and False / Multiple Choice

1. In an Ethernet network, what happens when a sender has a packet to transmit but some other sender is already transmitting?
    A. The packet is discarded.
    B. The sender waits a random time, then sends.
    C. The sender waits for the beginning of the next slot, then sends.
    D. The sender waits for the current transmission to finish, then sends.

> **Solution:** The sender waits for the beginning of the next slot, then sends.
>
> 2pts for correct

2. Ethernet interface addresses:
    A. are assigned at manufacturing time.
    B. are assigned manually or by DNS.
    C. are generated randomly and checked for uniqueness by broadcasting a message.
    D. share the same high order bits, which determine the network or subnet in an internetwork.

> **Solution:** ...are assigned at manufacturing time.
>
> 2pts for correct

3. Which of the following is/are true about different unicast routing protocols:
    A. Each iteration of a distance vector protocol (neighbor exchange) and each iteration of a link state protocol (LSP flood) creates the same number of total messages across the entire network.
    B. The use of split-horizon and poison-reverse in a distance-vector protocol like RIP always prevents the count-to-infinity problem when a network partition occurs.
    C. BGP always uses the shortest path (in terms of router hops) between two nodes.
    D. Link-state protocols do not suffer from the count-to-infinity problem.

> **Solution:** Total: **4 pts**
>
> - (D) is the correct answer
> - (A) LSP flood requires node * edges, DV requires 2 * edges
> - (B) Split horizon and poison reverse fix single hop loops, but multiple hop loops can still remain.
> - (C) BGP uses the shortest number of AS path hops, not router hops.
>
>   +1 per correct line..

4. Which of the following is true? (circle True or False)

(True / False) One reason why we use IP address on links instead of Ethernet addresses is that Ethernet addresses may not be unique.

(True / False) Every router has exactly one IP address

(True / False) All lower layers in a protocol stack must have some form of demultiplexing field to identify the higher layer protocol carried in the message payload

(True / False) It is possible to have entries in the forwarding table that overlap, meaning that some addresses may match more than one entry

(True / False) The goal of ARP is to enable each host on a network to build up a table of mappings between IP addresses and human-readable names.

(True / False) Because IP provides best effort delivery, reliability issues such as in-order delivery are the responsibilities of an upper layer protocol.

(True / False) Shannon's Law predicts that the capacity of communication link is equal to channel bandwidth (in Hz).

Solution:

F – MAC addresses are unique.

F – Routers may have more than 1 IP. If routers only had one IP address, they wouldn't connect any networks

T – For IP, is the protocol field. For transport-layer protocols TCP and UDP, it is the port number

T – If address matches multiple entries, take the longest prefix match

F – ARP's purpose is to build a mapping between IP addresses and link layer addresses

T – IP provides minimal functionality to support a diverse set of networks. Thus, reliability issues need to be dealt with by upper layer protocols like TCP.

F – Capacity is not equivalent directly to bandwidth (SNR is also considered in Shannon's Law)

+1 per correct line...7pts

B Short Answer

5. A forwarding table for a router in a network using CIDR is given below.

Address prefix	Next hop
192.128.64.32/8	A
192.160.128.89/16	B
192.0.0.0/2	C
0.0.0.0/0	D

   (a) If the router receives a packet with destination 192.207.128.89, what will the next hop be?

   Solution: A

   (b) If the router recieves a packet with destination 192.160.64.32, what will the next hop be?

   Solution: B

   3pts total, 1pt for getting one part right

6. Assume that you are sending 1000 bit packets over a 100Mbps network with a *round trip time* of 40μs. What is the latency for a single packet from the start of transmission to the completion of reception?

   Solution: 20μs network latency + 1000b / 100Mbps message duration = 30μs

   3pts, -1pt for calc error

7. After finishing 441, you create a new networking startup that is housed in an abandoned Pittsburgh steel mill. You want a gigabit (1000Mbps) network. The size of your factory building necessitates that your cables be as long as 500 meters. The maximum backoff and retry attempts for your network is set to 8. To save money, you decide to twist your own ethernet cables using steel instead of copper. For purposes of this question, assume that electromagnetic waves propagate through your steel wires at a speed of $1 * 10^8$ m/s. What should the minimum packet size be for this network?

   Solution: (5 points)

   2*(1000*10^6 bps)*(500m)/1*10^8mps = 10000bits

   4pts, -1 per calc error, -2 for factor of 2 error

8. In project 1, you used the socket API to write your Liso webserver. For this question, there is a single client communicating with a single server using TCP. The client sends a very small amount of data using the send() function, and the server receives the data with a recv() call. Each of the following scenarios shows a different order in which the socket calls are called on both the client and the server. For each scenario, answer the following: Will the server get the data sent by the client? (Yes or No). If not, explain why not.

   Assume that there is no latency between the client and the server. Time is proceeding down the page.

   (a) time ↓

Client	**Server**
	socket()
socket()	
	bind()
connect()	
	listen()
send()	
	accept()
close()	
	recv()
	close()

   Solution: No. `connect()` will fail, since it is called before the server calls `listen()`.
   2pts, 1 for answer, 1 for reason

   (b) time ↓

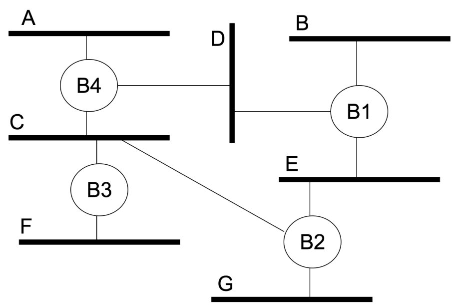
Client	**Server**
	socket()
socket()	
	bind()
	listen()
	accept()
	recv()
connect()	
send()	
close()	
	close()

   Solution: No - the server is attempting to accept() and read() before the client has connected.
   2pts, 1 for answer, 1 for reason

9. The Hamming distance is the number of bit positions in which two code words differ. What is the minimum Hamming distance between two valid code words using single-bit parity? Show an example of two minimally distant code words using 8 bits + parity.

> **Solution:**
>
> 2, e.g. 000000001 and 000000010
>
> 3pts, -2 per part wrong

10. The figure below describes an extended LAN. The LAN's are labeled A-G and the bridges are labeled B1-B4. Bridge Bi has an ID of i which is used as the tie breaker. (Choose the lowest i to break a tie.) Before answering the following questions, compute the spanning tree of the extended LAN. (You might want to make a sketch in the space below.)



(a) Which bridge represents the root of the spanning tree?

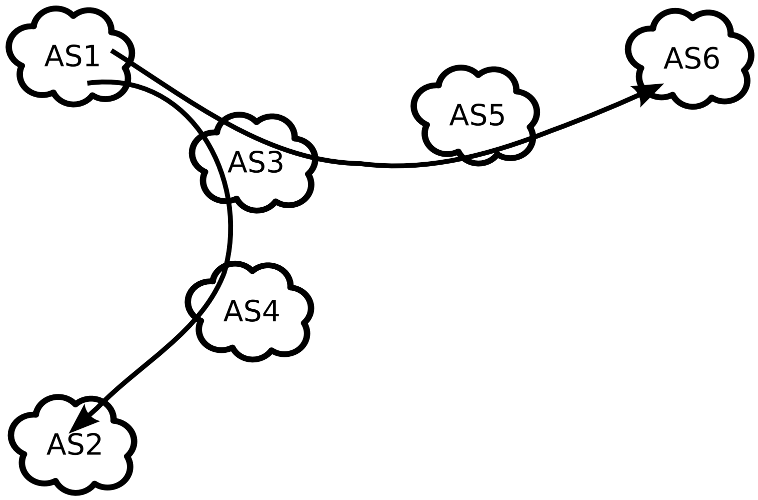
> **Solution:** B1
>
> 1pt

(b) Mark each network port of each bridge as follows: Use "X" to mark a port that is part of the spanning tree. Use "O" to mark a port that is not part of the spanning tree. (In the lecture slide terminology, "X" marks ports in the *forwarding state* and "O" marks ports in the *blocked state*).

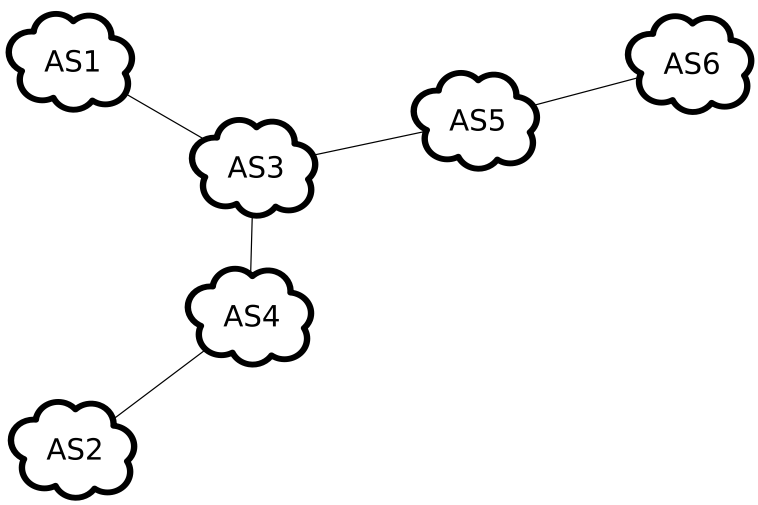
> **Solution:** Mark every port with "X" except B4 to C.
>
> 2pts

11. Assume in the network there is only customer-provider relationship and that AS 3 is the only tier-1 ISP. In addition, the following are two valid paths:

- Path 1: $1 \to 3 \to 4 \to 2$
- Path 2: $1 \to 3 \to 5 \to 6$

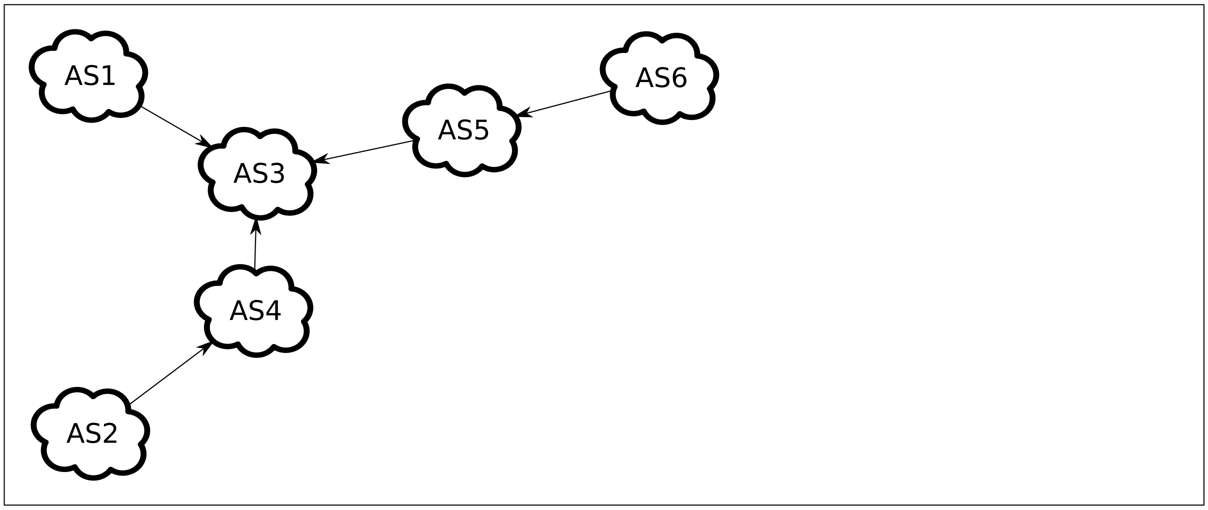


Please mark the edges in the figure below to indicate the customer-provider relationship (customer $\to$ provider).



Solution: 4pts total, -2 per wrong arrow

See figure below. The arrow between AS3 and AS5 can be either way.


AS1
AS6
AS5
AS3
AS4
AS2

C Crypto

This problem is about Public Key Infrastructure (PKI). In PKI systems there are **Certificate Authorities**, **hosts**, and **clients**. For this problem we will consider a Certificate Authority CA, a client C trying to communicate securely with a host H, and a malicious host H' attempting to eavesdrop. Assume that C already has the public key of CA in a database of trusted CA's and that CA has signed a public key providing a certificate to H for identification to clients.

12. Assume C wants to communicate securely with server H in the described PKI system. However, H' has been placed between them transparently. Is it possible for H' to pretend to be H at this point in time? Assume H' forges a public key certificate, linked to a private key that H' controls (thus, H' can decrypt communication from C to H), identifying it as H and presents the forged certificate to C.

> **Solution:** No, because the client does not trust H' as a CA.
>
> 3pts

13. Assume C has contacted H directly and is communicating securely using HTTPS via TLS. H is currently streaming a large file to C. What form of cryptography will be used to encrypt the transmission of this stream? Why this form?

> **Solution:** Symmetric key cryptography methods are used for stream encryption between two TLS endpoints. This is because public key (asymmetric) algorithms are slow in practice today; symmetric key ciphers can run at orders of magnitude higher speeds in terms of time and throughput.
>
> 3pts

14. In the previous part to this question you described how TLS encrypts bytes between clients and hosts, but there is still a problem of key distribution. What form of cryptography is used to exchange session keys in TLS?

> **Solution:** Asymmetric (public key) cryptography is used to setup keys for symmetric key session ciphers in TLS. This forms a hybrid cryptographic system.
>
> 3pts

D DNS

For answering the following question, consider the following name servers and mappings they contain:

local name server 128.2.184.224

Name	Value	Type	Class	TTL
com	a.gtld-servers.net nstld.verisign-grs.com	SOA	IN	1 day
a.gtld-servers.net	192.5.6.30	A	IN	1 day

a.gtld-servers.net name server

Name	Value	Type	Class	Additional Info	TTL
google.com	ns1.google.com	NS	IN	216.239.32.10	1 day

google.com name server

Name	Value	Type	Class	TTL
www.google.com	72.14.204.105	A	IN	10 minutes

15. Suppose a client queries the local name server for the IP address of www.google.com. The local name server recursively resolves the request and cache the results. Write down the requests and responses the local nameserver will perform and the answer it eventually sends back to client. Number steps sequentially in the table below.

    We have started from the initial client request to the local name server and the first request the local name server performs in servicing the query.

Request / Response	Source	Destination	Name	Value	Additional Info
Request 1	client	local name server	www.google.com		
Request 2	local name server	a.gtld-servers.net	google.com		
Response 2					

Solution:

Request / Response	Source	Destination	Name	Value	Additional Info
Request 1	client	local name server	www.google.com		
Request 2	local name server	a.gtld-servers.net	google.com		
Response 2	a.gtld-servers.net	local name server	google.com	ns1.google.com	216.239.32.10
Request 3	local name server	ns1.google.com	www.google.com		
Response 3	ns1.google.com	local name server	www.google.com	72.14.204.105	
Response 1	local name server	client	www.google.com	72.14.204.105	

2pts per line correct

16. 11 minutes later the same client queries the local name server for www.google.com. List out the requests and the responses from the point of view of the local name server and the response it eventually sends back to client.

    Start with the request of the client to the local name server and number request/response pairs as in the previous part of this question.

Request / Response	Source	Destination	Name	Value	Additional Info

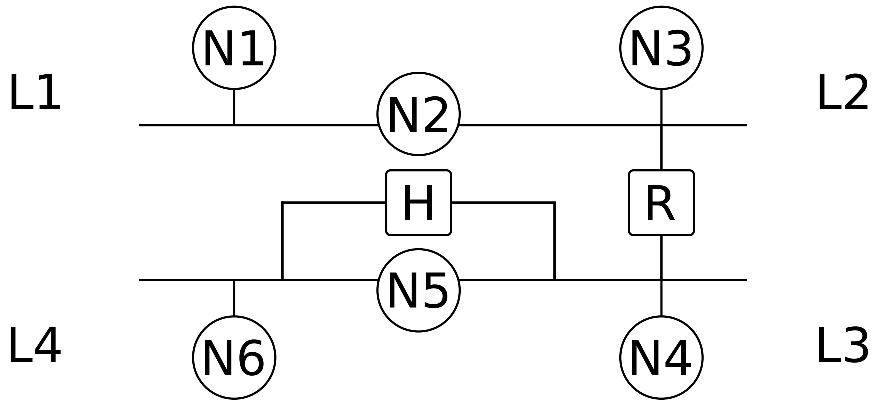
Solution:

Request / Response	Source	Destination	Name	Value	Additional Info
Request 1	client	local-name server	www.google.com		
Request 2	local-name server	ns1.google.com	www.google.com		
Response 2	ns1.google.com	local-name server	www.google.com	72.14.204.105	
Response 1	local-name server	client	www.google.com	72.14.204.105	

3pts per line correct

E Bridging and Switching

A small company has the network topology shown below. In this topology there are four Ethernet segments (L1, L2, L3, and L4) interconnected with a hub H and router R. Nodes N1, N2, N3, N4, N5, and N6 are endsystems. Endsystems do not forward packets.



17. In this problem, use the following notation: the MAC address of node N1 is n1 (lower case), its IP address is N1 (UPPER CASE). If a node has multiple IP or MAC addresses, use the index of the segment to differentiate between them. For example, host N2 has two different IP addresses, N2[L1] and N2[L2], since it is on two LANs. The first line in the table provides an example entry for a packet from N1 to N2 on link L1.

    Suppose host N6 transmits a packet to N3. In the following table, give the MAC and IP source and destination addresses of the packet as it is observed traveling on the different links.

Location	Link	MAC Source	MAC Destination	IP Source	IP Destination
N1 to N2	L1	n1	n2[L1]	N1	N2[L1]
N6 to N3	L4				
N6 to N3	L3				
N6 to N3	L2				

Solution:

Location	MAC Source	MAC Destination	IP Source	IP Destination
N1 to N2 on L1	n1	n2[L1]	N1	N2[L1]
N6 to N3 on L4	n6	r[L3]	N6	N3
N6 to N3 on L3	n6	r[L3]	N6	N3
N6 to N3 on L2	r[L2]	n3	N6	N3

2pts per line

18. If we move N6 to L2, do we need to reconfigure N6? If so, how?

Solution:

need a new IP address

2pts

19. If we move N6 to L3, do we need to reconfigure N6? If so, how?

> **Solution:**
>
> no
>
> 1pts

20. N3 is transmitting a large number of broadcast packets on L2.

    (a) Will this affect the performance of N6's file transfer to N5? Explain.

    > **Solution:**
    > no effect
    >
    > 2pt

    (b) If it has an impact on the transfer, what can we replace node H with to reduce the impact? Note that you should select a replacement device that addresses the problem *AND* that requires the minimum amount of reconfiguration in the network.

    > **Solution:** no change
    >
    > 0pt

21. N4 is transmitting a large volume of data to N3.

    (a) Will this affect the performance of N6's file transfer to N5? Explain.

    > **Solution:** yes...
    >
    > 2pt

    (b) If it has an impact on the transfer, what can we replace node H with to reduce the impact? Note that you should select a replacement device that addresses the problem *AND* that requires the minimum amount of reconfiguration in the network.

    > **Solution:** bridge
    >
    > 1pt

22. N4 is transmitting a large number of broadcast packets on L3.

    (a) Will this affect the performance of N6's file transfer to N5? Explain.

    > **Solution:** yes
    >
    > 2pt

    (b) If it has an impact on the transfer, what can we replace node H with to reduce the impact? Note that you should select a replacement device that addresses the problem *AND* that requires the minimum amount of reconfiguration in the network.

    > **Solution:** router
    >
    > 1pt

The End – Phew!

F 1 Free Point for Tearing Off Page: Anonymous Feeback

List one thing you liked about the *class* and would like to see more of or see continued (any topic—lectures, homework, projects, bboards, topics covered or not covered, etc.):

List one thing you would like to have changed or have improved about the class: