

CS 5565 Final Exam

This is a closed-book, closed-internet, closed-cellphone and closed-computer exam. However, you may refer to your 2 sheets of prepared notes. Your exam should have 11 pages with 6 questions totaling 100 points. You have 120 minutes. Please write your answers in the space provided on the exam paper. If you unstaple your exam, please put your initials on all pages. You may use the back of pages if necessary, but please indicate if you do so we know where to look for your solution. You may ask us for additional pages of scratch paper. You must submit all sheets you use with your exam. However, we will not grade what you scribble on your scratch paper unless you indicate you want us to do so. Answers will be graded on correctness and clarity. You will lose points if your solution is more complicated than necessary.

Name (printed) _____

I accept the letter and the spirit of the Virginia Tech graduate honor code – I have not given or received aid on this exam.

(signed) _____

#	Problem	Points	Score
1	Error Correction and Detection	12	
2	Understanding IP Addressing	24	
3	Accountable Internet Protocol	20	
4	Routing Algorithms	20	
5	Link Layer	12	
6	Optimizing RPC	12	
	Total	100	

1 Error Correction and Detection (12 pts)

a) (8 pts) Hamming Codes

Consider the following (7,3) code¹, which maps 3 data bits to 8 code words A-H, listed below. The right half of the table lists the Hamming distance for each pair of code words.

	A	B	C	D	E	F	G	H	
A 0000000	: 0	4	4	4	4	4	4	4	A
B 0001111	: 4	0	4	4	4	4	4	4	B
C 0110011	: 4	4	0	4	4	4	4	4	C
D 0111100	: 4	4	4	0	4	4	4	4	D
E 1010101	: 4	4	4	4	0	4	4	4	E
F 1011010	: 4	4	4	4	4	0	4	4	F
G 1100110	: 4	4	4	4	4	4	0	4	G
H 1101001	: 4	4	4	4	4	4	4	0	H
	A	B	C	D	E	F	G	H	

- i. (4 pts) How many bit errors can this code detect?
- ii. (4 pts) How many bit errors can this code correct?

b) (4 pts) Layering and Error Detection

Currently, error detection is commonly performed at the link-layer (via CRC-32) and the transport layer (via TCP/UDP Internet checksum). Is this redundant? Discuss the consequences of removing this feature from either layer!

- i. (2 pts) If error detection were implemented at layer 2 only:
- ii. (2 pts) If error detection were implemented at layer 4 only:

¹ Created with Richard Tarvo's Hamming Code tool at <http://www.ee.unb.ca/cgi-bin/tarvo/hamming.pl?X=+Generate+&L=7&D=4&T=000>

2 Understanding IP Addressing (24 pts)

a) (3 pts) On Gateways and Netmasks

You're being asked to set up a machine for your research lab, which uses static IP addresses. The network administrator gives you the following information:

IP Address: 128.173.237.141
Default Gateway: 128.173.236.1
Netmask: 255.255.255.0

Can this information be correct? Justify your answer!

b) (3 pts) Static DHCP

Your network admin tells you that they are using "static DHCP," in which your laptop will be provided with the same IP address every time it sends out a DHCP Discover request.

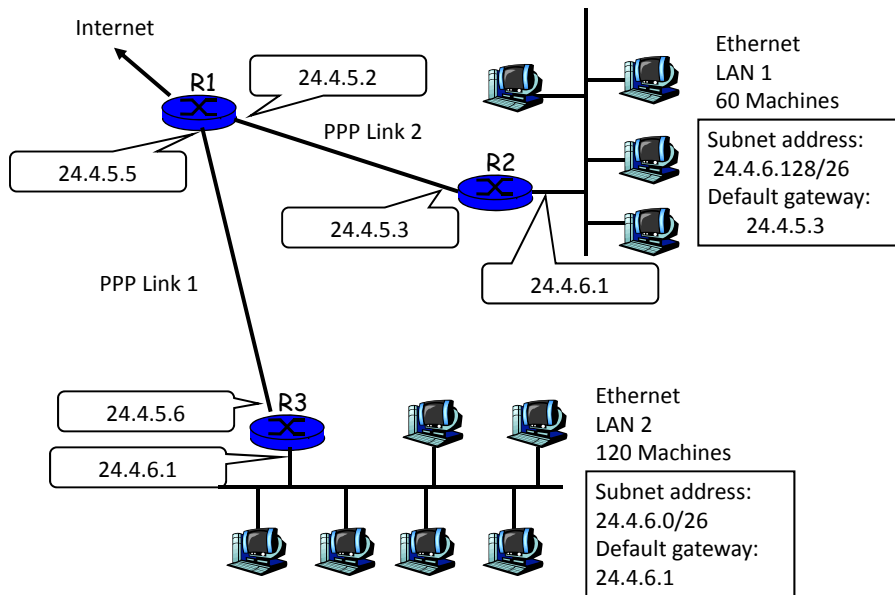
What information will the network administrator need from you?

c) (4 pts) Prefixes vs. Subnets

Explain the difference between a prefix and subnet!

d) (6 pts) On Subnets

You are being brought in as a consultant to debug the configuration of a company's network. The network consists of three IP routers connected by two PPP links to a border router connecting to the company's ISP. Each IP router serves a LAN of 60 and 120 machines, respectively. The current configuration is shown below; the rectangles on the right denote information that is distributed via DHCP in each LAN.



Identify 3 mistakes in this setup!

- i. (2 pts) Mistake 1:

- ii. (2 pts) Mistake 2:

- iii. (2 pts) Mistake 3:

e) (4 pts) IPv6

Suppose you ported your project 2 to be compatible with IPv6.
Discuss which changes you would have to make!

f) (4 pts) IPv6 Adoption

IPv6 adoption is lagging because IPv6 is said to have a “chicken-and-egg” problem. Explain what this problem is!

3 Accountable Internet Protocol (20 pts)

a) (2x3 pts) Lack of Accountability

The paper by Anderson et al laments a “lack of accountability” at the current network layer. Name two attacks that can arise from this shortcoming!

b) (4 pts) Preventing Spoofing

If the Internet used AIP, what would happen if a malicious host attempted to disguise as another host by using that hosts’s EID address?

c) (6 pts) Routing Scalability

AIP has been criticized because CIDR-like aggregation cannot be used.

- i. (2 pts) Explain why not:

- ii. (2 pts) Explain what potential negative impact results from this:

- iii. (2 pts) Can the use of multiple AD: prefixes ameliorate the problem?

d) (4 pts) Forwarding Performance

Would AIP, as proposed, work well with the hybrid hardware/software approach proposed by Casado et al in the "Rethinking Packet Forwarding Hardware?"

Justify your answer!

scratch space

4 Routing Algorithms (20 pts)

a) (6 pts) *Count To Infinity*

The “poisoned reverse” technique can reduce the count to infinity problem, but not eliminate it in all cases. Give a concrete topology, and a concrete link cost changes, for which count to infinity would occur even if poisoned reverse is being used!

b) (4 pts) *Route Oscillations*

- i. (2 pts) What are route oscillations and how can they arise?

- ii. (2 pts) In lecture, we had discussed oscillations in the context of link-state algorithms.
Can oscillation also occur when a distance vector algorithm is used?
Justify your answer!

c) (4 pts) Trade-offs

In project 2B, you needed to decide on suitable time intervals in which to a) check for cost changes and b) poll your neighbors to identify whether a link is up or not. For each of these two parameters, describe the trade-off involved in choosing an appropriate value.

- i. (2 pts) The trade-off involving the Link Cost Change Polling Interval:

- ii. (2 pts) The trade-off involving Neighbor Polling Interval:

d) (6 pts) Broadcasting

Reverse path forwarding is a multicast or broadcast forwarding algorithm that forwards packets if and only if they arrived on the interface that leads to the shortest path to the source.

- i. (3 pts) If a network has $|V|$ vertices and $|E|$ edges, how many packets are being sent for each packet being broadcast?

- ii. (3 pts) By contrast, how many packets would be sent if a spanning tree based algorithm were used?

5 Link Layer (12 pts)

a) (8 pts) Self-configuration

Most layer 2 switches deployed today include firmware that allows users to patch them together in an arbitrary topology, even one including redundant links. A spanning-tree algorithm sets forwarding policies that prevent loops. However, the resulting forwarding may not be optimal. An alternative would be to implement a traditional link-state or distance vector routing algorithm in each switch's firmware.

Discuss the merits of this idea! Assume that no changes to the Ethernet frame format, and no changes to the NIC controllers in end hosts are allowed!

b) (4 pts) Switch Poisoning

What is switch poisoning, and how might an attacker benefit from it?

6 Optimizing RPC (12 pts)

RPC, including the simple implementation you created in project 2A, suffers from the same performance limitations as other stop-and-wait protocols. As we discussed in lecture, sliding window protocols provide better performance because they use pipelining. In this problem, discuss how to adapt your RPC implementation to allow for pipelining.

(8 pts) Can you accomplish this goal without changing the semantics of the program that is using your RPC middleware layer? If so, what changes, if any, would be required to your language binding? State your assumptions if necessary!

(4 pts) Provide a concrete example from project 2B in which your approach would result in performance improvements!