CSC 4222/6222 – Exam #2 **Name: ____________________________________**
Spring 2020

The exam is open book and open notes. It is **NOT open partner**. You must **justify your answers and/or show your work**, without this, you will not receive any credit. State any assumptions needed. Once finished, submit your exam to the dropbox folder labeled Exam 2. The deadline to submit is 12:30 PM – NO late submissions accepted. Please ensure that the document submitted is legible. If possible, use one of the free scanner apps to convert your work to a pdf – this will be better than taking pictures of each page.

If you are unable to print out the exam and do your work on these pages, make sure to clearly label the problem numbers. It is fine to solve the exam on plain paper and submit.

In accordance with both the letter and spirit of the University Policy on Academic Honesty, I have neither given nor received assistance on this examination.

SIGNATURE: ____

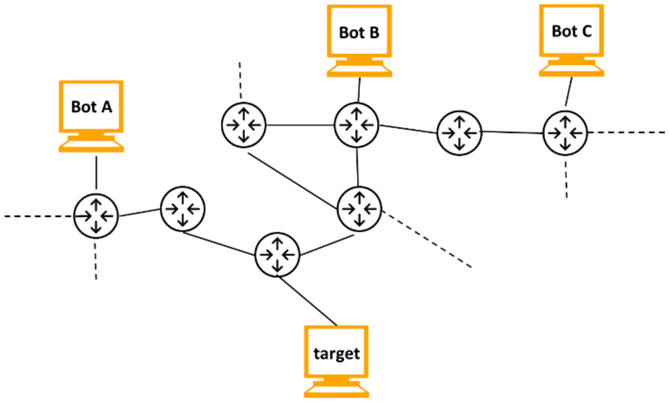
1. [15 points] Assume you are developing your own quote of the day application, where a client reaches out to a server to receive a new quote. Note that this is not handling critical information and a request can be sent again if the request or response gets lost, so we are not worried about data transfer reliability

a) If the size of the Ethernet packet is 1200 bytes, how many bytes make up the application layer message?

b) Grad students or bonus for undergrads: What additional steps should you take to ensure that data is not manipulated along the way and to keep the quote information confidential?

2. [15 points] Suppose an IDS has a 75% accuracy rate. After analyzing the detailed performance, we can see that over a certain time period, the alarm was sounded a total of 3500 times. Assume we know that there were 150 true positive events and 2350 false positive events. Determine how many total entries were logged for this period and also determine how many of these events were of valid activity.

3. [10 points] Suppose routers in the network shown below have been configured to implement the IP Traceback scheme, where each router tags itself with 30% probability. In the scenario shown, the bottom node is a target for a DDoS attack. You can assume the routing algorithms have set up routing tables for the shortest paths.

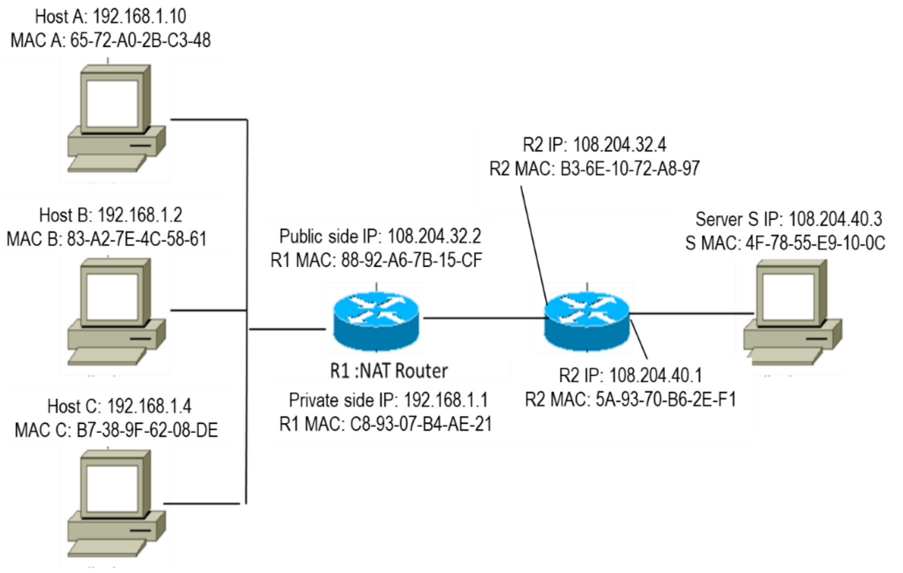


a) What will be the probability that the victim can determine the gateway or next hop router of Node C? Briefly explain your findings and implications.

b) Grad students or UG students for bonus: If Node C is using a spoofed IP address, will the IP Traceback be useful in any way? Briefly explain why or why not.

4. [10 points] Consider a user Sarah that wants to view the current data from the WHO website. After completing a DNS query, Sarah needs to establish a TCP connection to the WHO server. Assume Sarah's end selects 24680 as her starting sequence number and the server selects 35791 as the initial sequence number. What will be the sequence number and acknowledgement numbers be for the first packet sent after the handshaking is completed? Draw a diagram to justify your answer.

5. [15 points] Refer to the diagram below. Hosts A, B and C belong to a private network and are behind a NAT router. Assume both hosts A and B are initiating an HTTP request with Host S (recall that the server listens for incoming SSH requests at port 80). Afterwards, Server S sends back a response to both hosts A and B. Fill in the table below for the requested details. Assume Host A selects Port 56784 and Host B selects Port 23456. State any other assumptions you need to make.



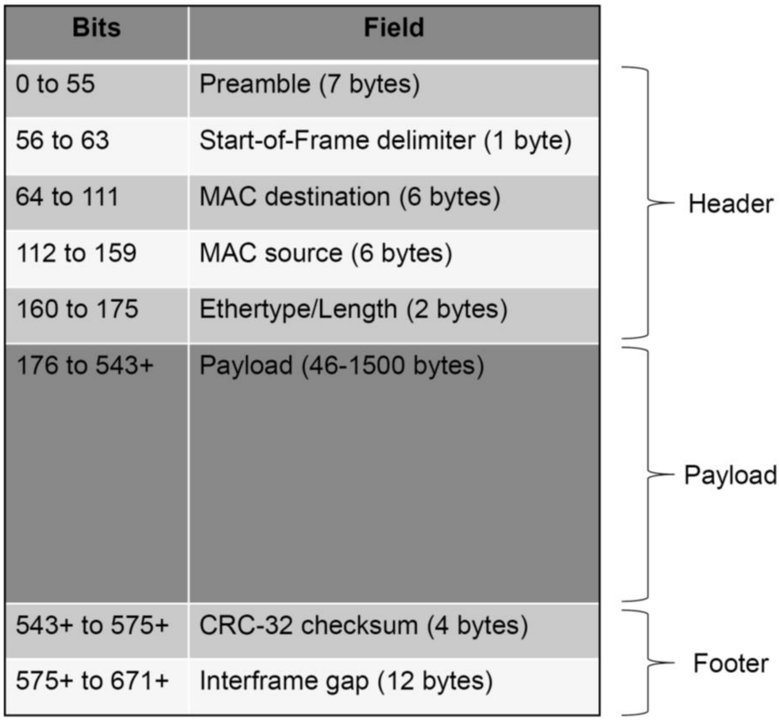
	Source IP	Destination IP	Source MAC	Destination MAC
From R2 to S (for request from A)				
From R2 to R1 (for response to B)				
From R1 to A (for response to A)				
From B to R1 (for request from B)				

6. [15 points] Consider the set of policies below. If you were in charge of security for your company, provide a set of rules and their configuration to match the policies. Would your firewall be stateless? Explain why or why not.

- Internal hosts are allowed to request TCP connections to any external server
- Internal hosts are not allowed to act as a server for any outside connection
- External servers are able to provide TCP connections to the requests from internal hosts and continue communicating within this connection
- Internal hosts are not allowed to connect with any external server for an application running on top of UDP

7. [10 points] If an attacker has managed to poison one DNS cache, can this cause other DNS caches to become infected as well? Briefly explain why or why not?

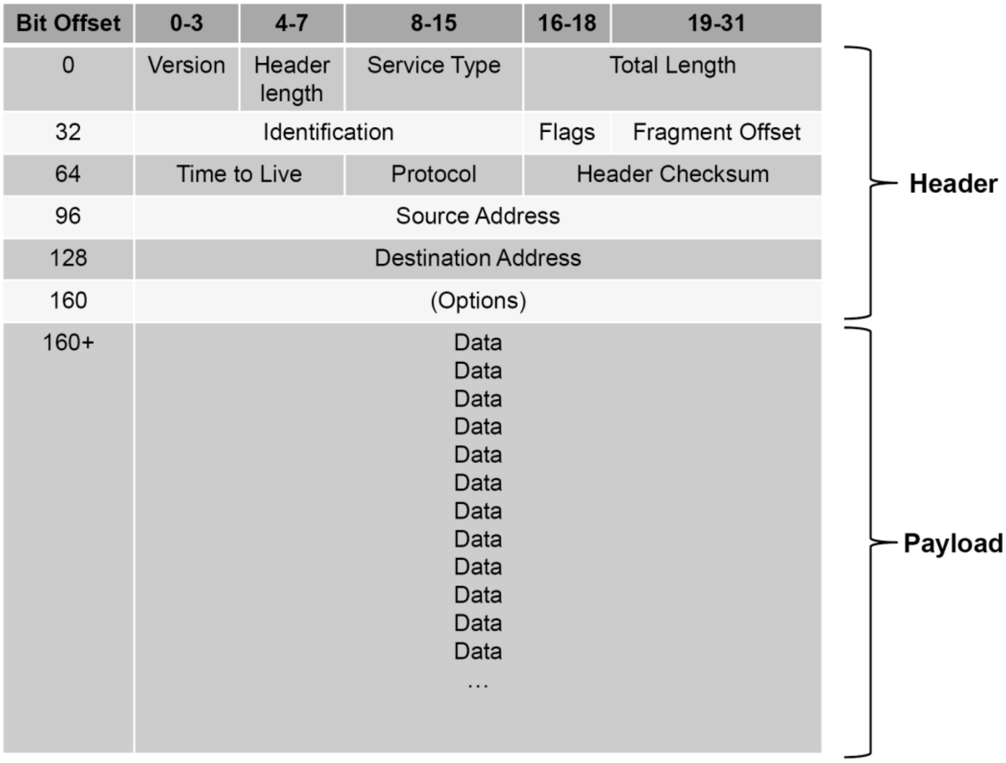
8. [10 points] When an attacker is performing an ARP spoofing attack they are trying to poison the ARP tables. Why would an attacker consider sending the spoofed information over and over again, even if no requests have been made on the LAN?



Bits	Field
0 to 55	Preamble (7 bytes)
56 to 63	Start-of-Frame delimiter (1 byte)
64 to 111	MAC destination (6 bytes)
112 to 159	MAC source (6 bytes)
160 to 175	Ethertype/Length (2 bytes)
176 to 543+	Payload (46-1500 bytes)
543+ to 575+	CRC-32 checksum (4 bytes)
575+ to 671+	Interframe gap (12 bytes)

Header
Payload
Footer

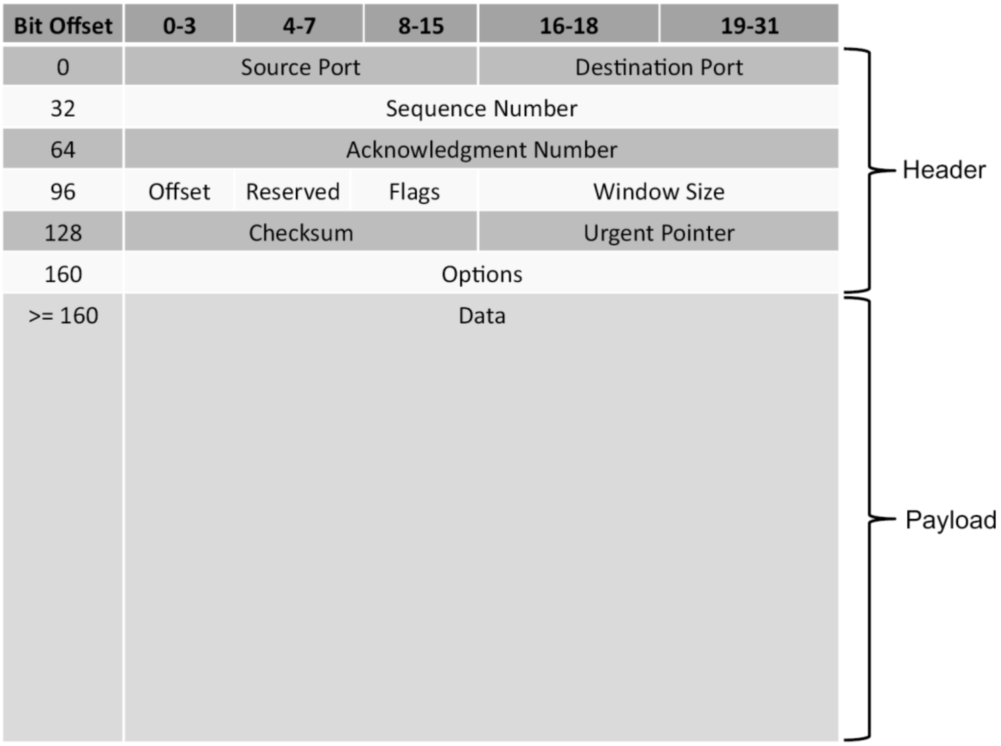
Figure 5.7: The format of an Ethernet frame.



Bit Offset	0-3	4-7	8-15	16-18	19-31
0	Version	Header length	Service Type	Total Length	
32	Identification			Flags	Fragment Offset
64	Time to Live		Protocol	Header Checksum	
96	Source Address				
128	Destination Address				
160	(Options)				
160+	Data Data Data Data Data Data Data Data Data Data Data Data …				

Header
Payload

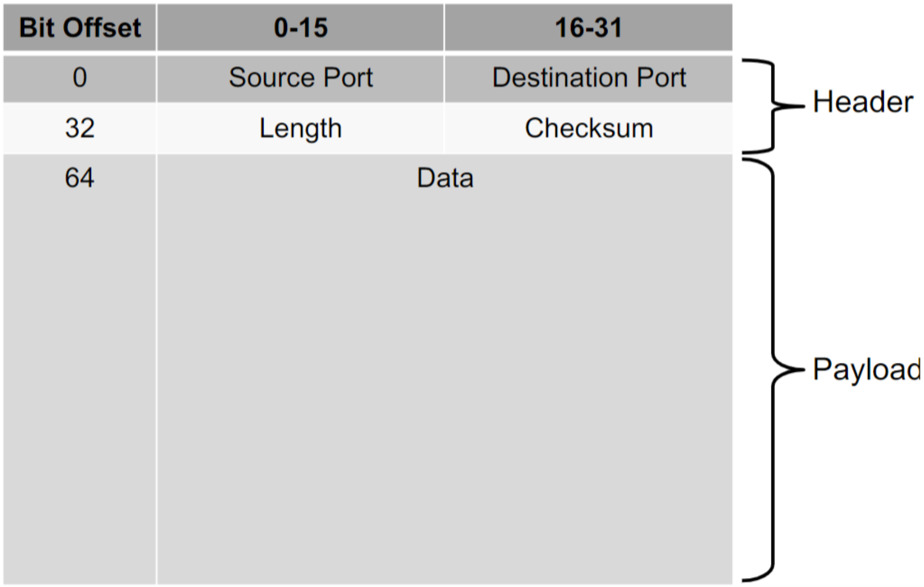
Figure 5.10: Format of an IPv4 packet.



Bit Offset	0-3	4-7	8-15	16-18	19-31
0	Source Port			Destination Port	
32	Sequence Number				
64	Acknowledgment Number				
96	Offset	Reserved	Flags	Window Size	
128	Checksum			Urgent Pointer	
160	Options				
>= 160	Data				

Header
Payload

Figure 5.14: Format of a TCP packet.



Bit Offset	0-15	16-31
0	Source Port	Destination Port
32	Length	Checksum
64	Data	

Header
Payload

Figure 16: Format of a UDP packet.