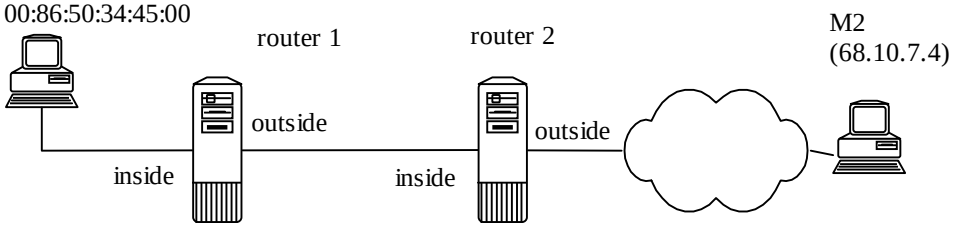
Instructions:

- Open book, open notes
- Laptops are allowed
- Allow 75 minutes for exam
- Calculators are allowed

NAME: _____ **SCORE:** _____

1. (15 pts) Given the figure below fill in the table below. An IP packet with 2500 bytes of user data needs to be sent across an Ethernet network from machine M1 to machine M2 and therefore needs to be fragmented. Show the fragments for the network segment **between the two routers** (fill in the table [all parts of the table that are blank], for the data field indicate the length of the data). Assume the first fragment is as large as possible for an Ethernet network.

M1
IP = 129.186.5.4
Enet = 00:86:50:34:45:00

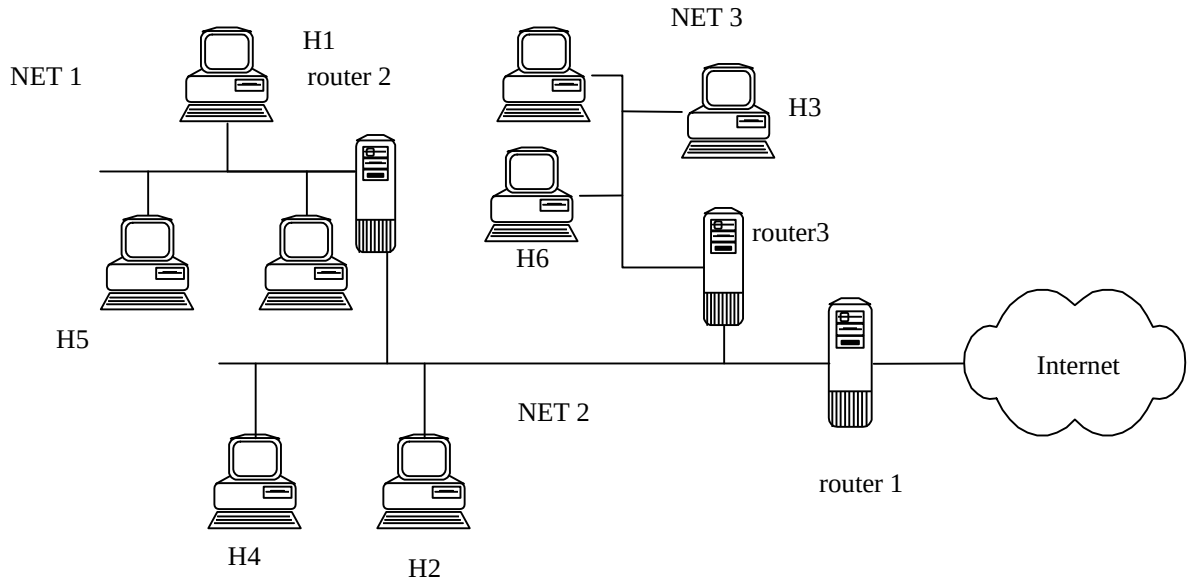


Router 1
outside
IP = 192.34.25.10
Enet = 00:80:08:45:22:FF
inside
IP = 129.186.5.254
Enet = 00:80:08:34:12:45

Router 2
outside
IP = 12.123.34.45
Enet = 00:88:88:38:12:EC
inside
IP = 192.34.25.15
Enet = 00:7C:23:33:19:AA

Layer	Field Name	Original	Fragment 1	Fragment 2
Ethernet	Destination	N/A		
	source	N/A		
	Type field	N/A		
IP	Ver/IHL	4 5		
	Type	0		
	Len			
	ID	2774		
	Flags	0 0 0		
	Offset	0		
	TTL	200		
	Protocol	17		
	Checksum	Computed	Computed	Computed
	Source IP			
	Destination IP			
Data		2500 bytes		

2. (20 pts) Using the figure below answer the following questions



Assume the following addresses:

Name	IP	Name	IP
H1	129.186.5.4	Router 2	129.186.5.254 (for the network 129.186.5.0)
H2	129.186.4.10	Router 2	129.186.4.100 (for the main network)
H3	129.186.10.20	Router 1	129.186.4.254 (for the main network)
H4	129.186.4.25	Router 1	10.0.0.5 (for the internet side)
H5	129.186.5.34	Router 3	129.186.4.253 (for NET 2)
		Router 3	129.186.10.254 (the NET 3)

Assume DNS is not used

Assume H2 sent a message to H1, H3, H4, H5, H6 and a machine on the Internet (207.14.19.47). How many entries would be in H2's ARP table due to these messages?

For this part assume all ARP caches are cleared before machine H3 sends a single ICMP ECHO request to machine H1. Fill in the table below showing the number of each type of packets that are transmitted on each network because H3 sends an ICMP ECHO request to machine H1 which then replies with an ICMP ECHO reply

Network	Number of ARP Packets	Number of ICMP packets
Network 1		
Network 2		
Network 3		

3. (10 pts) Describe ARP cache poisoning and what damage an attacker could cause by poisoning the ARP cache.

4. (15 pts) Which category or categories in the taxonomy does each of the following mitigate?

   a) VLAN

   b) WPA/WEP

5. (10 pts) Describe why the network architecture is divided into layers.

6. (30 pts) Describe each of the following and what impact it will have on security:

   a. Rogue or fake wireless access point

   Impact:

   b. Rogue DHCP server

   Impact:

   c. Network Sniffing

   Impact:

   d. Denial of service

   Impact:

   e. IP Address Spoofing

   Impact:

   f. MAC Address Spoofing

   Impact: