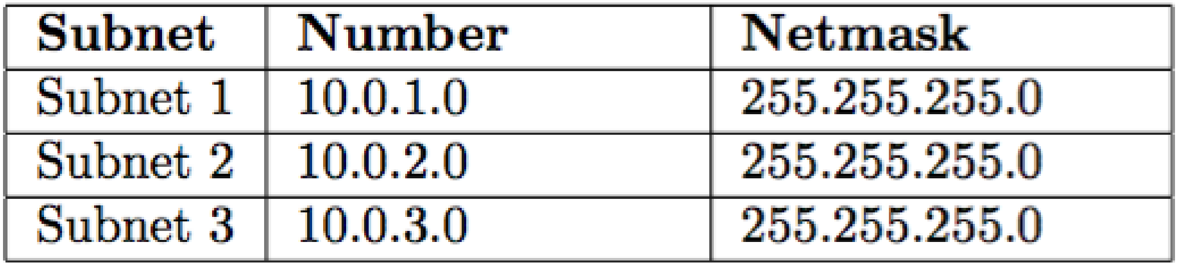
Lab Exercise 7: Solutions

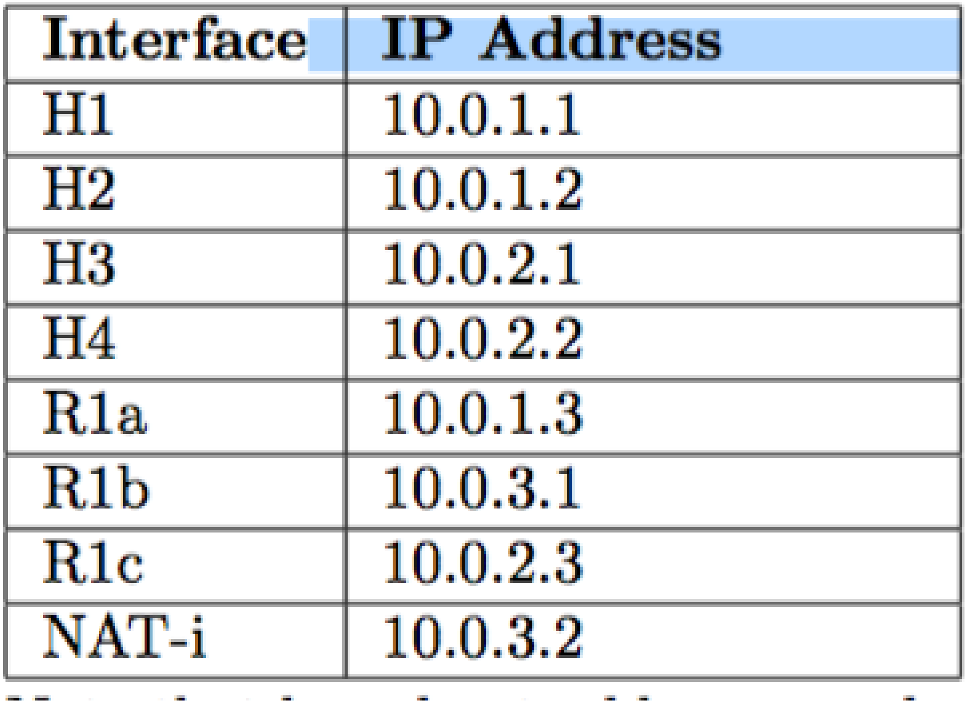
Exercise 1: IP Addressing and NAT (2 marks)

Question 1. **(1 mark)**

There are many solutions. Here is one:



Subnet	Number	Netmask
Subnet 1	10.0.1.0	255.255.255.0
Subnet 2	10.0.2.0	255.255.255.0
Subnet 3	10.0.3.0	255.255.255.0



Interface	IP Address
H1	10.0.1.1
H2	10.0.1.2
H3	10.0.2.1
H4	10.0.2.2
R1a	10.0.1.3
R1b	10.0.3.1
R1c	10.0.2.3
NAT-i	10.0.3.2

Note that the broadcast address (10.255.255.255) and the subnet address (10.0.0.0) are not assigned to interfaces.

Question 2.

IPv6 would allow Elliot to obtain IP addresses for all network connected devices in his home network from his ISP. This because with IPv6 we have almost infinite # of IP addresses. Thus, there would not be need of a private network and the NAT device.

Question 3.

A NAT box provides a measure of security by hiding the private network from the public Internet and also not permitting unsolicited inbound connections. This may be a reason to continue to use the NAT box.

Question 4. **(1 mark)**

FTP would not work through this NAT box because it requires that the server open a connection back to the client. (Passive mode FTP would work—it has the client open the connection instead). Any protocol that embeds IP or TCP-layer information in the application stream is likely to be broken by a basic NAT box.

Exercise 2: Understanding NAT using Wireshark (4 marks)

Question 1.

IP address of the client is 192.168.1.100

Question 2. (**0.5 mark**)

Source IP: 192.168.1.100, Source Port: 4335, Destination IP: 64.233.169.104, Destination Port: 80

Question 3. (**0.5 mark**)

7.158798 seconds.

Source IP: 64.233.169.104, Source Port: 80, Destination IP: 192.168.1.100, Destination Port: 4335

Question 4.

7.075657 seconds.

Source IP: 192.168.1.100, Source Port: 4335, Destination IP: 64.233.169.104, Destination Port: 80

Question 5.

Source IP: 64.233.169.104, Source Port: 80, Destination IP: 192.168.1.100, Destination Port: 4335. The ACK is transmitted at 7.108986.

Question 6.

6.069169 seconds.

Question 7. (**0.5 mark**)

Source IP: 71.192.34.104, Source Port: 4335, Destination IP: 64.233.169.104, Destination Port: 80

Only the source IP address has changed.

Question 8.

No, the HTTP Get message is unmodified.

Question 9. (**0.5 mark**)

Version: Not Changed. Header Length: Not Changed, Flags: Not Changed. Checksum: Changed. Since the IP source address has changed, and the checksum includes the value of the source IP address, the checksum has to be recomputed by the NAT router.

Question 10.

6.117570 seconds.

Question 11. (**0.5 mark**)

Source IP: 64.233.169.104, Source Port: 80, Destination IP: 71.192.34.104, Destination Port: 4335

Only the destination IP address has changed.

Question 12.

6.035475 seconds, and 6.067775 seconds, respectively.

Question 13. **(1 mark)**

For the SYN: Source IP: 71.192.34.104, Source Port: 4335, Destination IP: 64.233.169.104, Destination Port: 80.

For the SYN/ACK: Source IP : 64.233.169.104, Source Port: 80, Destination IP: 71.192.34.104, Destination Port: 4335.

For the SYN, the source IP address has changed, For the SYN/ACK, the destination IP address has changed. The port numbers are unchanged.

Question 14. (**0.5 mark**)

The NAT translation table would be as follows:

WAN side	**LAN side**
71.192.34.104, 4335	192.168.1.100, 4335

Question 15.

Safe Browsing is a blacklist service provided by Google. Google maintains a lit of URLs that contain malicious content such as malware or phishing sites. Web browsers can check the URLs being visited against these lists to ensure that the sites being visited are not malicious. Google provides a public API for the service. You can find further details at Safe Browsing API .

Exercise 3: Using Wireshark to understand Ethernet (2 marks)

Question 1.

The source Ethernet address is 00:d0:59:a9:3d:68.

Question 2. (**0.5 mark**)

The destination address is 00:06:25:da:af:73. The source host sending the GET request and the web server (the intended recipient of the GET message) do not belong to the same subnet and are in fact separated by several routers in between. So the destination address here is the MAC address of the router connected to the LAN segment of which the source host is a part of (i.e. the first hop router).

Question 3.

The 16 bit hexadecimal value for the Frame type is 0x0800 indicating the IP protocol.

Question 4. (1 **mark**)

“G” appears 54 bytes after the start of the frame. The reason for this is that the first 14 bytes represent the Ethernet frame header. The next 20 bytes represent the 20 byte IP header and the 20 bytes following that consist of the TCP headers. Note that the HTTP GET request is encapsulated in a TCP segment, which in turn is encapsulated in an IP datagram, which finally is encapsulated in an Ethernet frame. The preamble bytes are not captured by Wireshark.

Question 5. (**0.5 mark**)

The source Ethernet address for this frame is 00:06:25:da:af:73. This is neither the Ethernet address of gaia.cs.umass.edu nor the source host. This refers to the Ethernet address of the first-hop router from the source host. This address corresponds to the answer of Question 2 above.

Question 6.

The destination address of the frame is 00:d0:59:a9:3d:68 which is indeed the Ethernet address of the source host that sent the earlier GET HTTP request

Question 7.

In this case “O” starts 67 bytes from the start of the Ethernet frame. This includes 14 bytes of the Ethernet frame header, 20 bytes of IP header, 20 bytes of TCP header and 13 bytes for the “HTTP /1.1 200 “ part of the HTTP response status line.

Exercise 4: Using Wireshark to understand ARP (2 marks)

Question 1. (**0.5 marks**)

The source address is 00:d0:59:a9:3d:68 and the destination address is ff:ff:ff:ff:ff:ff, which is the broadcast address.

Question 2.

The frame type field has a value of 0x0806 indicating ARP.

Question 3.

The *opcode* field begins 20 bytes from the start of the Ethernet frame. The first 14 bytes are for the Ethernet frame header and the next 6 bytes include other ARP fields.

Question 4.

The *opcode* is 0x0001, which stands for an ARP Request.

Question 5.

Yes it does. The sender IP address is 192.168.1.105.

Question 6. (**0.5 marks**)

The IP address of the machine whose Ethernet address is being queried is included as the target IP address. The target Ethernet address is left blank (i.e. all 0's).

Question 7. (**0.5 marks**)

As in the ARP request, the *opcode* in the response message is located 20 bytes from the beginning of the frame.

Question 8.

The value is 0x0002, which stands for an ARP Reply.

Question 9.

The answer i.e. the Ethernet address of the IP address queried in the ARP Request appears in the Sender MAC address field. Notice that the IP address that was queried appears in the Sender IP address field whereas the sender MAC and IP address contain the Ethernet and IP address of the host machine that sent out the ARP query.

Question 10. (**0.5 marks**)

The source address is 00:06:25:da:af:73 and the destination address is the 00:d0:59:a9:3d:68, which is the Ethernet address of the host computer that sent out the earlier ARP request.