COMP3331 Lab7

Ruofei HUANG

April 28, 2019

1 Exercise 1

1.1 Question 1

Subnet Table:

Subnet	Number	Netmask
Subnet 1	10.1.1.0	255.255.255.0
Subnet 2	10.1.2.0	255.255.255.0
Subnet 3	10.1.0.0	255.255.0.0

Interface Table:

Interface	Ip Address
H1	10.1.1.2
H2	10.1.1.3
H3	10.1.2.2
H4	10.1.2.3
R1a	10.1.1.1
R1b	10.1.0.2
R1c	10.1.2.1
NAT-i	10.1.0.1

1.2 Question 2

Since the IPv6 will use 128-bit of address, it can count more than all the sand on earth. Hence, it's impossible to run out of the address space in forseeable future. The NAT machnism is dealing with the address is not enough in IPv4. So if every device can be directly addressed by IPv6 in public network, there's no need to setup an NAT device in subnet.

1.3 Question 3

It's tedious to remember the IPv6 address and difficult to type into address bar without any error.

1.4 Question 4

HTTP as an example:
There's some IP address and port number inside UDP segment. If NAT leave it as what it is, orthers may not find the correct address because it's belong to subnet and need to translate. In this case, if NAT doesn't do the support, all the application base on this protocal wont work.

2 Exercise 2

2.1 Question 1

192.168.1.100

2.2 Question 2

Source 192.168.1.100:4335
Destination 64.233.169.104:80

2.3 Question 3

At 7.158797

2.4 Question 4

At 7.108986
Source: 192.168.1100:4335
Destination: 64.233.169.104:80

2.5 Question 5

Source: 64.233.169.104:80
Destination: 192.168.1100:4335
At 7.108986

2.6 Question 6

At 6.069168

2.7 Question 7

Source 71.192.34.104:4335
Destination: 64.233.169.104:80
The destination ip and port are same as Question 2.

2.8 Question 8

The reponse in frame and next request in frame are changed

2.9 Question 9

The checksum is changed, because the checksum is include the source ip and destination, so it will be changed (becasue source ip is changed).

2.10 Question 10

At 6.117570

2.11 Question 11

Source: 64.233.169.104:80
Destination: 71.192.34.104:4335
The destination port and ip is different.

2.12 Question 12

TCP SYN at 6.035475
The server to client TCP SYN/ACK at 6.067775

2.13 Question 13

Segment Name	Source IP	Destination IP	
TCP SYN	71.192.34.104	64.233.169.104	The source of TCP SYN
TCP SYN/ACK	64.233.169.104	71.192.34.104	

and the destination of TCP SYN/ACK are different. The destination of TCP SYN and Source of TCP SYN/ACK are same.

2.14 Question 14

Source	Destination
192.168.1100:4335	71.192.34.104:4335

Maybe there's a line for:

Source	Destination
71.192.34.104:4335	192.168.1100:4335

2.15 Question 15

Browser will check an online backlist by url. So if the URL is in the blacklist, the browser block the request.

3 Exercise 3

3.1 Question 1

Source: 00:06:25:da:af:73

3.2 Question 2

Destination: 00:d0:59:a9:3d:68 No, it's not, this MAC address is belong to the switch in this subnet.

3.3 Question 3

0x00000800

3.4 Question 4

0x37= 3*16+ 7 = 55, The "G" is number 55 bytes of the Ethernet frame. So, it's 55 bytes away from the very start of the ethernet frame.
No preamble bytes. 14 bytes.
There are 41 bytes remains.

3.5 Question 5

The source is 00:06:25:da:af:73. Both answer are no. The address is belong to the switch of this subnet.

4 Exercise 4

4.1 Question 1

No	Source	Destination
1	00:d0:59:a9:3d:68	ff:ff:ff:ff:ff:ff
2	00:06:25:da:af:73	00:d0:59:a9:3d:68

The address of ff:ff:ff:ff:ff:ff means broadcast, not the actural address.

4.2 Question 2

0x00000806

4.3 Question 3

(48+48+16+16+16+8+8)/8 = 20 bytes

4.4 Question 4

0x002

4.5 Question 5

Yes

4.6 Question 6

It's in the target IP. it's from 0x26 to 0x2A bytes, which is 38 to 42 bytes in IPv4

4.7 Question 7

Same as question 3? 20 bytes.

4.8 Question 10

The heximal contain the source and destination is: 0000 00 01 08 00 06 04 00 02 00 06 25 da af 73 c0 a8 0010 01 01 00 d0 59 a9 3d 68 c0 a8 01 69 The hex of sourcce and destination are:

Source	00:06:25:da:af:73
Destination	00:d0:59:a9:3d:68