Cover Page
ECE 461 Lab4 Report

Name: Wei Lin (#999595193)
Name: Shenglin Meng (#1000695517)

Exercise 1B

1.Include the NAT table of Router2 and provide an explanation of the columns of the table.

Data:

Pro	Inside global	Inside local	Outside local	Outside global
---	200.0.0.1	10.0.1.1	---	---
---	200.0.0.2	10.0.1.2	---	---
---	200.0.0.3	10.0.1.3	---	---

Ans:

-- Pro: It refers to a protocol used for a specific NAT entry.
-- Inside global: An IP address that represent inside IP address to outside
-- Inside local: It refers to the IP address assigned to a private network host , and it is unknown to the public network.
-- Outside local: It represents the outside host as an IP address in the inside network
-- Outside global: It refers to an IP address allocated from a globally routable address on a host of outside network.

2. For each of the ping commands above, provide an explanation why the command succeeds or fails.

Ans:

On PC3 :

1. Ping 10.0.1.3
The command was executed successfully, because PC3 and Router 3 are in the same private network.
2.Ping 128.143.136.1
The command was executed successfully, because PC3 is mapped to a global IP address of 200.0.0.2 in the NAT table of router 2. Therefore, PC3 can communicate with public network.

On Router 3:

3.Ping 10.0.1.2
This command was executed successfully , because PC3 and Router 3 are in the same private network.
4.Ping 128.143.136.1
This command failed because the IP address of Router 3 is not mapped to a NAT table entry and it does not have a global IP.

On PC4:

5.Ping 10.0.1.2

This command failed because PC4 does not have destination address of 10.0.1.2 in its routing table and there is no default gateway. NAT breaks end-to-end connectivity and PC4 is in the public network, so the private network address 10.0.1.2 is not reachable for PC4.
6.Ping 200.0.0.2
This command was executed successfully because the public IP address 200.0.0.2 is mapped to private IP address 10.0.1.2 in the NAT table of router 2.

3.Include the IP source address and IP destination address from the IP header data of an ICMP request and the corresponding ICMP reply packet before and after it passes through Router2.

Data:

ICMP request before pass through router 2:

No.	Time	Source	Destination	Protocol	Info
5	15.085977	10.0.1.2	128.143.136.1	ICMP	Echo (ping) request

ICMP request after pass through router 2:

No.	Time	Source	Destination	Protocol	Info
2	9.135260	200.0.0.2	128.143.136.1	ICMP	Echo (ping) request

ICMP reply before pass through router 2:

No.	Time	Source	Destination	Protocol	Info
3	9.135299	128.143.136.1	200.0.0.2	ICMP	Echo (ping) reply

ICMP reply after pass through router 2:

No.	Time	Source	Destination	Protocol	Info
6	15.086530	128.143.136.1	10.0.1.2	ICMP	Echo (ping) reply

Exercise 1C

1.For each of the telnet and ping commands above, provide an explanation why a command succeeds or fails.

Ans:

Telnet/Ping:

On PC 1:

1.Telnet/Ping 10.0.1.3
The command was executed successfully , because PC1 and Router 1 are in the same private network.

2. Telnet/Ping 128.143.136.1
The command was successfully executed, because all hosts in the same private network, including PC1 and router 3, are mapped a public IP address 128.143.136.22 in the NAT table of PC2 by IP masquerading.

On Router 1:
3. Telnet/Ping 10.0.1.2
The command was executed successfully , because PC1 and Router1 are in the same private network.
4. Telnet/Ping 128.143.136.1
The command was successfully executed, because all hosts in the same private network, including PC1 and router 3, are mapped a public IP address 128.143.136.22 in the NAT table of PC2 by IP masquerading.

On PC 4:
5. Telnet/Ping 10.0.1.12
The command failed because PC4 does not have destination address of 10.0.1.2 in its routing table and there is no default gateway. NAT breaks end-to-end connectivity and PC4 is in the public network, so the private network address 10.0.1.2 is not reachable for PC4.k.

2.For each successful telnet session, include the IP header data of an outgoing and an incoming packet header (with respect to the private network).

Ans:

On PC 1:

Telnet 10.0.1.3
Incoming traffic
eth0:

No. Time Source Destination Protocol Info
5 16.667568 10.0.1.2 10.0.1.3 TCP 37988 > 23 [SYN] Seq=0 Len=0 MSS=1460 TSV=1078562 TSER=0

No. Time Source Destination Protocol Info
6 16.668823 10.0.1.3 10.0.1.2 TCP 23 > 37988 [SYN, ACK] Seq=0 Ack=1 Win=4128 Len=0 MSS=1460

Telnet 128.143.136.1
Incoming traffic
eth0:
No. Time Source Destination Protocol Info
5 10.907132 10.0.1.2 128.143.136.1 TCP 35498 > 23 [SYN] Seq=0 Len=0 MSS=1460 TSV=1119622 TSER=0
eth1:
No. Time Source Destination Protocol Info
4 0.000148 128.143.136.1 128.143.136.22 TCP 23 > 35498 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 TSV=1111332 TSER=1119622

Outgoing traffic
eth1:
No. Time Source Destination Protocol Info
3 0.000082 128.143.136.22 128.143.136.1 TCP 35498 > 23 [SYN] Seq=0 Len=0 MSS=1460 TSV=1119622 TSER=0
eth0:
No. Time Source Destination Protocol Info
6 10.911699 128.143.136.1 10.0.1.2 TCP 23 > 35498 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 TSV=1111332 TSER=1119622

On Router 1:

Telnet 10.0.1.2
Incoming traffic:
eth0:
No. Time Source Destination Protocol Info
3 17.398385 10.0.1.3 10.0.1.2 TCP 62363 > 23 [SYN] Seq=0 Len=0 MSS=1460

No. Time Source Destination Protocol Info
6 17.400430 10.0.1.2 10.0.1.3 TCP 23 > 62363 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460

Telnet 128.143.136.1
Incoming traffic:
eth0:
No. Time Source Destination Protocol Info

3 6.849376 10.0.1.3 128.143.136.1 TCP 29001 > 23 [SYN] Seq=0 Len=0 MSS=536

eth1:

No. Time Source Destination Protocol Info

2 0.000070 128.143.136.1 128.143.136.22 TCP 23 > 29001 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460

Outgoing traffic:

eth1:

No. Time Source Destination Protocol Info

1 0.000000 128.143.136.22 128.143.136.1 TCP 29001 > 23 [SYN] Seq=0 Len=0 MSS=536

eth0:

No. Time Source Destination Protocol Info

4 6.849500 128.143.136.1 10.0.1.3 TCP 23 > 29001 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460

3.For each successful ping command, include the IP header data of an outgoing ICMP Request message and an incoming ICMP reply message (with respect to the private network).

On PC 1:

Ping 10.0.1.3

Incoming traffic

eth0:

No. Time Source Destination Protocol Info

3 0.000489 10.0.1.2 10.0.1.3 ICMP Echo (ping) request

No. Time Source Destination Protocol Info

6 0.996465 10.0.1.3 10.0.1.2 ICMP Echo (ping) reply

Ping 128.143.136.1

Incoming traffic

eth0:

No. Time Source Destination Protocol Info

5 15.363811 10.0.1.2 128.143.136.1 ICMP Echo (ping) request

eth1:

No.	Time	Source	Destination	Protocol	Info
4	0.000149	128.143.136.1	128.143.136.22	ICMP	Echo (ping) reply

Outgoing traffic

eth1:

No.	Time	Source	Destination	Protocol	Info
3	0.000082	128.143.136.22	128.143.136.1	ICMP	Echo (ping) request

eth0:

No.	Time	Source	Destination	Protocol	Info
6	15.370912	128.143.136.1	10.0.1.2	ICMP	Echo (ping) reply

On Router 1:

Ping 10.0.1.2

Incoming traffic

eth0:

No.	Time	Source	Destination	Protocol	Info
3	19.060380	10.0.1.3	10.0.1.2	ICMP	Echo (ping) request

No.	Time	Source	Destination	Protocol	Info
4	19.060446	10.0.1.2	10.0.1.3	ICMP	Echo (ping) reply

Ping 128.143.136.1

Incoming traffic

eth0:

No.	Time	Source	Destination	Protocol	Info
3	18.577451	10.0.1.3	128.143.136.1	ICMP	Echo (ping) request

eth1:

No.	Time	Source	Destination	Protocol	Info
4	0.000145	128.143.136.1	128.143.136.22	ICMP	Echo (ping) reply

Outgoing traffic

eth1:

No.	Time	Source	Destination	Protocol	Info
3	0.000082	128.143.136.22	128.143.136.1	ICMP	Echo (ping) reques**t**

eth0:

No. Time Source Destination Protocol Info
6 18.585989 128.143.136.1 10.0.1.3 ICMP Echo (ping) reply

4.How does PC know that a packet coming from the public network is destined to a host in the private network?

Ans: The PC will check on the NAT table for the packet received on the public network. If the packet matches the prerouting chain , then it means the packet is destined to a host in a private network.

5. Explain the steps performed by the kernel during IP address translation.

Ans: When PC recived a packet on the public network, it will check for the NAT table to see if the packet matches the prerouting and postrouting rules(prerouting for incoming packet, postrouting for outgoing packet.) and if it matches , then the packet header will be modified based on the rules and send to next hop/destination.

Exercise 1D

1. Use the captured data to explain the outcome of the FTP experiment. In particular, if the file was successfully downloaded, explain how the problem of sending the IP address as part of the data payload of the IP packet is solved.

Ans:

ftp -d 128.143.136.22, PC4 want to gets a file from PC2:

In this case, the file transfer is successful and no NAT is involved, since both PC4 and PC2 has public IP address.

FTP headers show that a file with size 66 bytes is transferred successfully:

No. Time Source Destination Protocol Info
22 8.748778 128.143.136.1 128.143.136.22 FTP Request: PORT 128,143,136,1,131,148

No. Time Source Destination Protocol Info
23 8.748890 128.143.136.22 128.143.136.1 FTP Response: 200 PORT command successful. Consider using PASV.

No. Time Source Destination Protocol Info
24 8.754406 128.143.136.1 128.143.136.22 FTP Request: RETR labdata

No. Time Source Destination Protocol Info
28 8.754860 128.143.136.22 128.143.136.1 FTP Response: 150 Opening BINARY mode data connection for labdata (66 bytes).

No. Time Source Destination Protocol Info
29 8.754912 128.143.136.22 128.143.136.1 FTP-DATA FTP Data: 66 bytes

No. Time Source Destination Protocol Info
36 13.019469 128.143.136.1 128.143.136.22 FTP Request: QUI

ftp -d 128.143.136.22, PC3 want to get a file from PC2:

In this case, NAT is involved in file transfer, since PC3 is in a private network while PC2 is in the public network. The router is configured in passive FTP mode, therefore, the file transfer will be successful.

In passive FTP mode, the host in the private network will always initiate the both command channel and data channel, so the server will not be blocked by NAT router. The hosts in the private network, in this case, PC3, will put its private IP address and active port number into the PORT packet during the connection establishment. When the packet go through the router, the private IP address in the PORT packet will be translated to the public IP address in the NAT table.

The data below shows the PORT packet with the private IP address of PC3 and header with information about passive FTP mode :

No. Time Source Destination Protocol Info
27 21.910963 10.0.1.2 128.143.136.22 FTP Request: PORT 10,0,1,2,215,153
...
File Transfer Protocol (FTP)
PORT 10,0,1,2,215,153\r\n
Request command: PORT
Request arg: 10,0,1,2,215,153
Active IP address: 10.0.1.2 (10.0.1.2)
Active port: 55193

No. Time Source Destination Protocol Info

28 21.912365 128.143.136.22 10.0.1.2 FTP **Response: 200 PORT command successful. Consider using PASV.**

...

The data shows that PC3 successfully receives the file:

No. Time Source Destination Protocol Info
30 21.912783 10.0.1.2 128.143.136.22 FTP Request: RETR labdata

...

No. Time Source Destination Protocol Info
34 21.914704 128.143.136.22 10.0.1.2 FTP-DATA FTP Data: 66 bytes

...

No. Time Source Destination Protocol Info
37 21.915221 128.143.136.22 10.0.1.2 FTP Response: 150 Opening BINARY mode data connection for labdata (66 bytes).

...

No. Time Source Destination Protocol Info
40 21.916565 128.143.136.22 10.0.1.2 FTP Response: 226 File send OK.

2. How can NAT be used to spoof a host address? How can you prevent this?

Ans: The NAT can be used to spoof a host address since it first compares the IP address to the translation table when there is an incoming packet, and if it matches the destination entry on the table then it will be forwarded to the corresponding destination. This process makes NAT vulnerable to spoof because one can easily intercept the data from user's ISP and modify the content and have them sent to the user.

Eg. : Source Destination (NAT 100.1.1.1)
1.0.0.0 64.0.0.0
64.0.0.0 100.1.1.1

The method to prevent NAT spoofing is to fashion the packet with a second layer (MAC address) of the NAT gateway but the layer 3 address (IP) of the internal system and send it. Therefore it can effectively prevent the packet gets filtered out by the upstream router, and will go directly to the NAT gateway.

Exercise 2C

1. What type of DHCP message can be observed?

Ans: There are totally four types of DHCP messages observed.

1. DHCPOFFER from 10.0.1.21
2. DHCPREQUEST on eth0 to 255.255.255.255 on port 67
3. DHCPDISCOVER on eth0 to 255.255.255.255 on port 67
4. DHCPACK from 10.0.1.21

Data:

No. Time Source Destination Protocol Info
1 0.000000 0.0.0.0 255.255.255.255 DHCP DHCP Discover - Transaction ID 0xbec0265d

…

No. Time Source Destination Protocol Info
3 0.594865 10.0.1.21 10.0.1.10 DHCP DHCP Offer - Transaction ID 0xbec0265d

…

No. Time Source Destination Protocol Info
4 0.595172 0.0.0.0 255.255.255.255 DHCP DHCP Request - Transaction ID 0xbec0265d

…

No. Time Source Destination Protocol Info
5 0.598512 10.0.1.21 10.0.1.10 DHCP DHCP ACK - Transaction ID 0xbec0265d

2. How long does a DHCP client wait until it attempts to renew its lease?

Data:

DHCPREQUEST on eth0 to 10.0.1.21 port 67
DHCPACK from 10.0.1.21
bound to 10.0.1.10 -- renewal in 54 seconds.

Ans: As the data above shows , the DHCP client waits 54 seconds until it attempts to renew its lease.

3. The expected outcome is that PC4 receives an IP address, but that PC3 is not successful. Why is the negative outcome for PC3 expected?

Ans: PC3 is not successfully receiving IP address, because Router 1 hasn't been set up as a relay agent.

4.Compare the IP addresses assigned to PC1 and PC4. Is there a specific order in which IP addresses are assigned by the DHCP server

Ans: Yes , there is a specific order for each IP address assigned by DHCP server. The DHCP server assigns address to hosts in the same subnet in decreasing order. PC1 firstly sends a DHCP discover, so PC1 receives a DHCP offer with IP address 10.0.1.10. Then, PC4 sends DHCP discover and receives a DHCP offer with IP address 10.0.1.9.

Data from the dhcpd.lease:

```
lease 10.0.1.10 {
  starts 3 2007/08/08 10:30:17;
  ends 3 2007/08/08 10:32:17;
  tstp 3 2007/08/08 10:32:17;
  binding state active;
  next binding state free;
  hardware ethernet 00:04:5a:7a:c8:25;
}
lease 10.0.1.9 {
  starts 3 2007/08/08 10:31:02;
  ends 3 2007/08/08 10:33:02;
  binding state active;
  next binding state free;
  hardware ethernet 00:04:5a:81:35:94;
}
```

5.Use a figure to explain the packets that were exchanged by the DHCP client and the DHCP server as part of the process of acquiring an IP address.

Data:

```
No.     Time       Source              Destination         Protocol Info
      1 0.000000   0.0.0.0             255.255.255.255     DHCP     DHCP Discover - Transaction
ID 0xbec0265d
...
No.     Time       Source              Destination         Protocol Info
      3 0.594865   10.0.1.21           10.0.1.10           DHCP     DHCP Offer    - Transaction ID
0xbec0265d
...
No.     Time       Source              Destination         Protocol Info
```

4 0.595172 0.0.0.0 255.255.255.255 DHCP DHCP Request - Transaction ID 0xbec0265d

...

No. Time Source Destination Protocol Info

5 0.598512 10.0.1.21 10.0.1.10 DHCP DHCP ACK - Transaction ID 0xbec0265d

Ans: The steps of DHCP client acquiring an IP address is :

1. A DHCP discover packet is sent broadcast to find a DHCP server.
2. A DHCP server picks up the broadcast request then replies to the client a DHCP offer packet with the IP address acquired.
3. The client receives the DHCP offer packet and then sends another DHCP request packet to the same server to request a spot for the IP address.
4. DHCP server acknowledges the DHCP request packet.

Figure:

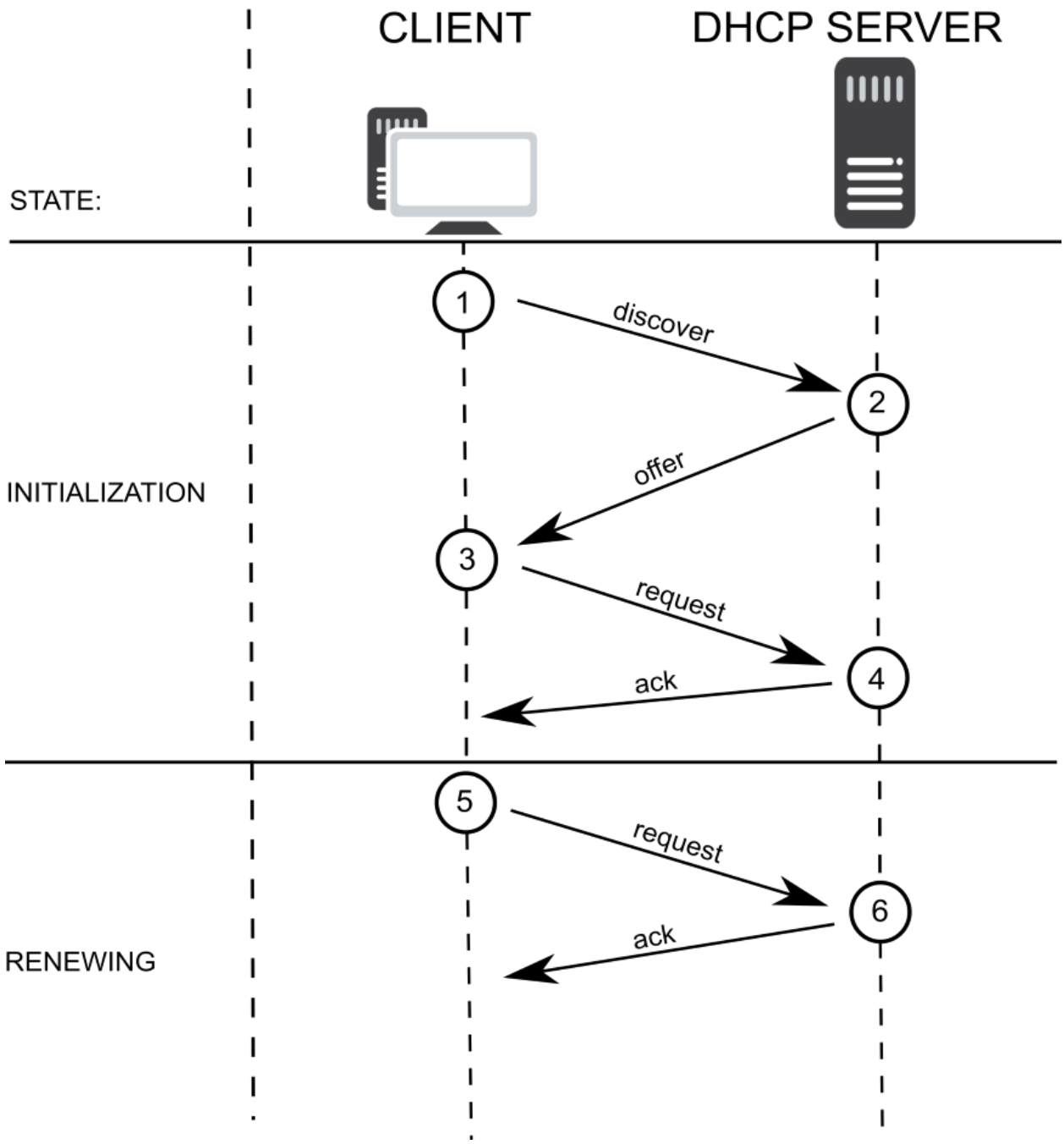

Figure 1.

6. Explain the entries in the lease file. How is the content of the lease file used when a DHCP server cannot contact the DHCP server?

Ans:

The interface means the ethernet interface of the client with assigned IP address. The fixed-address means the IP address assigned by the DHCP server. The option subnet-mask means the subnet mask of the assigned IP address. option dhcp-lease-time means the lease time of the IP address. option routers means the default gateway. option dhcp-message-type specifies the type of DHCP message. option dhcp-server-identifier refers to the address of DHCP server. renew, rebind, expire indicates the starting time and end time of the lease.

If the DHCP client fails to communicate with DHCP server, the lease file is used to determine the expired time. If the IP address of the client is released after lease expiration, the lease file will be written to keep track of the state.

Data:

```
lease {
  interface "eth0";
  fixed-address 10.0.1.10;
  option subnet-mask 255.255.255.0;
  option dhcp-lease-time 120;
  option routers 10.0.1.21;
  option dhcp-message-type 5;
  option dhcp-server-identifier 10.0.1.21;
  renew 3 2007/8/8 09:33:23;
  rebind 3 2007/8/8 09:34:14;
  expire 3 2007/8/8 09:34:29;
}
```

7. In most client-server application, the port number of a server is a well-known number (e.g., an FTP server uses port number 21, the telnet server uses port number 23, etc.), while the client uses a currently available (ephemeral) port number. DHCP is different. Here, both the client and the server use a well-known port: UDP port 67 for the DHCP server, and UDP port 68 for the DHCP client. Refer to RFC 2131 and provide an explanation for this protocol design choice.

Ans: The reason why both client and server use a well-known number is because it allows the client which does not have an IP address yet communicate with server. Furthermore, the DHCP server can broadcast to an UDP port to communicate with a client without IP address.

8. Another protocol that can be used to assign IP addresses is the Reverse ARP (RARP) protocol. Compare the services provided by RARP and DHCP

Ans: For RARP, the client have to set up a predefined table of MAC to IP address mapping , which is a one to one setting. When a network client broadcasts for an IP address , the RARP server will try to find the matching IP address , and send it back to the client once found. However for DHCP , it does not only delivers the IP address for a client after asked but also many other information like broadcast address , default router etc. Also, in DHCP you can define a range of IP address for clients that will be used for, which is a one to many setting. Therefore by using DHCP, a IP address can serve many clients within the lease time.

Exercise 2D

1. Does the DHCP relay server modify DHCP packets or the IP header? If so, what are the modifications?

Data:

On PC2:

No. Time Source Destination Protocol Info
1 0.000000 10.0.3.1 10.0.2.21 DHCP DHCP Discover - Transaction ID 0xa4b4bd5b

No. Time Source Destination Protocol Info
3 0.262518 10.0.2.21 10.0.3.1 DHCP DHCP Offer - Transaction ID 0xa4b4bd5b

On PC3:

No. Time Source Destination Protocol Info
1 0.000000 0.0.0.0 255.255.255.255 DHCP DHCP Discover - Transaction ID 0xa4b4bd5b

No. Time Source Destination Protocol Info
3 0.264742 10.0.3.1 10.0.3.10 DHCP DHCP Offer - Transaction ID 0xa4b4bd5b

Ans: As the data above shows, the DHCP relay agent modifies the IP header by replacing the source IP address of the packet to its own IP address, and the dest address to the IP address of DHCP server.

2. How does the relay agent redirect the replies from the DHCP server? Does it broadcast them or unicast them to the DHCP client?

Ans: The DHCP server will reply to the relay agent with unicast, and the relay agent will broadcast the replies to the client because the client does not have an IP address,.

3. Is there a difference in the response of the DHCP server as compared to the DHCP configuration of PC1? If so, explain the difference.

Ans: Yes, there is a difference between response of the DHCP and the configuration, DHCP configuration of PC1 directly exchanges data with the client, while the DHCP server first sends the packet to relay agent, then relay agent sends the packet to client, hence its an indirect method of transmission.

4. How does the DHCP server (PC2) know on which network PC3 is located, when it receives the DHCP request?

Ans: DHCP server(PC2) can know the subnet where PC3 is located based on the IP address of the DHCP relay agent that sends the discover packet.

5. What is the destination IP address of the first DHCP packet that the DHCP server sends to PC3?

Data:

No. Time Source Destination Protocol Info
3 0.262518 10.0.2.21 10.0.3.1 DHCP DHCP Offer - Transaction ID 0xa4b4bd5b

Ans: As the data shown above, the destination IP address is 10.0.3.1

Lab Report

1. Include the ethereal data of the first three DHCP packets that are exchanged between PC3 and PC2.

Data:

ON PC2:

No. Time Source Destination Protocol Info
1 0.000000 10.0.3.1 10.0.2.21 DHCP DHCP Discover - Transaction ID 0xa4b4bd5b

No. Time Source Destination Protocol Info

3 0.262518 10.0.2.21 10.0.3.1 DHCP DHCP Offer - Transaction ID 0xa4b4bd5b

No. Time Source Destination Protocol Info
4 0.265290 10.0.3.1 10.0.2.21 DHCP DHCP Request - Transaction ID 0xa4b4bd5b

On PC3:

No. Time Source Destination Protocol Info
1 0.000000 0.0.0.0 255.255.255.255 DHCP DHCP Discover - Transaction ID 0xa4b4bd5b

No. Time Source Destination Protocol Info
3 0.264742 10.0.3.1 10.0.3.10 DHCP DHCP Offer - Transaction ID 0xa4b4bd5b

No. Time Source Destination Protocol Info
4 0.264986 0.0.0.0 255.255.255.255 DHCP DHCP Request - Transaction ID 0xa4b4bd5b

2.What happens if a network has multiple DHCP servers?

Ans: If a network has multiple DHCP servers , then all the servers will send DHCP offers , but the client will only accept one offer from the servers.

Exercise 3

1. Include the ethereal data from the first ICMP Request and ICMP Reply messages.

Data:

PC1:

No.	Time	Source	Destination	Protocol Info
1	0.000000	10.0.1.10	10.0.3.23	ICMP Echo (ping)request
No.	Time	Source	Destination	Protocol Info
2	0.000318	10.0.3.23	10.0.1.10	ICMP Echo (ping)reply

PC2 :

No.	Time	Source	Destination	Protocol Info
1	0.000000	10.0.2.10	10.0.3.23	ICMP Echo (ping)request
No.	Time	Source	Destination	Protocol Info
2	0.000247	10.0.3.23	10.0.2.10	ICMP Echo (ping)reply

2. Include the routing table and the output of the ifconfig command from all PCs.

Data:

PC1 routing table:

Kernel IP routing table

Destination	Gateway	Genmask	Flags	MSS	Window	irtt	Iface
10.0.1.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
127.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0	lo
0.0.0.0	10.0.1.1	0.0.0.0	UG	0	0	0	eth0

PC1 ifconfig output:

```
eth0      Link encap:Ethernet  HWaddr 00:04:5A:7A:C8:25
          inet addr:10.0.1.10  Bcast:10.0.1.255  Mask:255.255.255.0
          inet6 addr: fe80::204:5aff:fe7a:c825/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:72 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:104 dropped:0 overruns:0 carrier:208
          collisions:0 txqueuelen:1000
          RX bytes:14451 (14.1 KiB)  TX bytes:0 (0.0 b)
          Interrupt:16 Base address:0xd800

eth1      Link encap:Ethernet  HWaddr 00:04:5A:80:76:DF
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:3 dropped:0 overruns:0 carrier:6
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
```

```
          Interrupt:20 Base address:0xdc00

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:72 errors:0 dropped:0 overruns:0 frame:0
          TX packets:72 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:5448 (5.3 KiB)  TX bytes:5448 (5.3 KiB)

sit0      Link encap:IPv6-in-IPv4
          NOARP  MTU:1480  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
```

PC2 routing table:

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
10.0.1.0        0.0.0.0         255.255.255.0   U         0 0          0 eth0
10.0.2.0        0.0.0.0         255.255.255.0   U         0 0          0 eth1
127.0.0.0       0.0.0.0         255.0.0.0       U         0 0          0 lo
0.0.0.0         10.0.2.1        0.0.0.0         UG        0 0          0 eth1
```

PC2 ifconfig output:

```
eth0      Link encap:Ethernet  HWaddr 00:04:5A:7A:C8:CA
          inet addr:10.0.1.1  Bcast:10.0.1.255  Mask:255.255.255.0
          inet6 addr: fe80::204:5aff:fe7a:c8ca/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:139 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:140 dropped:0 overruns:0 carrier:280
          collisions:0 txqueuelen:1000
          RX bytes:37988 (37.0 KiB)  TX bytes:0 (0.0 b)
          Interrupt:16 Base address:0xd800

eth1      Link encap:Ethernet  HWaddr 00:04:5A:7A:C5:B5
          inet addr:10.0.2.10  Bcast:10.0.2.255  Mask:255.255.255.0
```

inet6 addr: fe80::204:5aff:fe7a:c5b5/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:48 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:93 dropped:0 overruns:0 carrier:186
collisions:0 txqueuelen:1000
RX bytes:6783 (6.6 KiB) TX bytes:0 (0.0 b)
Interrupt:20 Base address:0xdc00

lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:118 errors:0 dropped:0 overruns:0 frame:0
TX packets:118 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:9796 (9.5 KiB) TX bytes:9796 (9.5 KiB)

sit0 Link encap:IPv6-in-IPv4
NOARP MTU:1480 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)

PC3 routing table:

Kernel IP routing table

Destination	Gateway	Genmask	Flags	MSS	Window	irtt	Iface
10.0.3.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
127.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0	lo
0.0.0.0	10.0.3.1	0.0.0.0	UG	0	0	0	eth0

PC3 ifconfig output:

eth0 Link encap:Ethernet HWaddr 00:04:5A:7A:C6:64
inet addr:10.0.3.23 Bcast:10.0.3.255 Mask:255.255.255.0
inet6 addr: fe80::204:5aff:fe7a:c664/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:42 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:71 dropped:0 overruns:0 carrier:142
collisions:0 txqueuelen:1000
RX bytes:6230 (6.0 KiB) TX bytes:0 (0.0 b)

```
          Interrupt:16 Base address:0xd800

eth1      Link encap:Ethernet  HWaddr 00:04:5A:7A:C6:67
          inet6 addr: fe80::204:5aff:fe7a:c667/64 Scope:Link
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:3 dropped:0 overruns:0 carrier:6
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:20 Base address:0xdc00

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:24 errors:0 dropped:0 overruns:0 frame:0
          TX packets:24 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1588 (1.5 KiB)  TX bytes:1588 (1.5 KiB)

sit0      Link encap:IPv6-in-IPv4
          NOARP  MTU:1480  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
```

3. Include the NAT table form PC2.

Data:

```
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
MASQUERADE  all  --  10.0.1.0/24         anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Reference

1.Flowmon , Martin Skoda, *DHCP Monitoring with Flowmon* , 18 March .2016 . [Online] Available:
https://www.flowmon.com/en/blog/dhcp-monitoring-in-flowmon-8-0