ECE 461 Lab 7 Lab Report

Xiaoyang Guo 999578513

Mingqi Hou 999767676

Xiaolong Zhang 997969104

Exercise 1(B)

1. **Include the NAT table of Router 2 and give explanation to the columns of the table.**

NAT table of Router 2

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	---	---

- Pro: The protocol used for the particular NAT entry.
- Inside global: A legitimate IP address that represents one or more inside local IP addresses to the outside world.
- Inside local: The IP address assigned to a host in the private network, which is unknown to the public network.
- Outside local: The IP address of an outside host as it appears to the inside network.
- Outside global: The IP address assigned to a host on the outside network by the owner of the host. The address is allocated from a globally routable address or network space.

2. **For each preceding *ping* commands, provide an explanation of why a command succeeds or fails.**

Commands are issued on PC 3:

- ping 10.0.1.3
  Command succeeds as Router3 and PC3 are in the same private network.
- ping 128.143.136.1
  Command succeeds as PC 3 is mapped in the NAT table. PC 3 has a global IP address of 200.0.0.2/24.

Commands are issued on Router 3:

- ping 10.0.1.2
  Command succeeds because Router 3 is in the same network with Router3.
- ping 128.143.136.1
  Command fails because the IP address of Router 3 is not mapped in the NAT table.

Commands are issued on PC4:

- ping 10.0.1.2
  Command fails as PC4 can not private address in a public network.

- ping 200.0.0.2

Command succeeds because the public address 200.0.0.2 is mapped in NAT table, which converted into 10.0.1.2 by Router2.

3. **Include the IP source address and the IP destination address from the IP header data of an ICMP Echo Request and the corresponding ICMP Echo Reply packet before and after it passed through Router2.**

packets before passing through Router 2

No.	Time	Source	Destination	Protocol	Info
13	52.480365	10.0.1.2	128.143.136.1	ICMP	Echo (ping) request
No.	Time	Source	Destination	Protocol	Info
14	52.485878	128.143.136.1	10.0.1.2	ICMP	Echo (ping) reply

packets after passing through Router 2

No.	Time	Source	Destination	Protocol	Info
9	36.190806	200.0.0.2	128.143.136.1	ICMP	Echo (ping) request
No.	Time	Source	Destination	Protocol	Info
10	36.190830	128.143.136.1	200.0.0.2	ICMP	Echo (ping) reply

Exercise 1(C)

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

Commands are issued on PC 1:

- ping 10.0.1.3 / telnet 10.0.1.3
  Command succeeds because PC 1 and Router 1 are in the same private network.
- ping 128.143.136.1 / telnet 128.143.136.1
  Command succeeds as all hosts in this private network are mapped to the same public IP address in the NAT table. Due to IP masquerading, all hosts in this private network are able to exchange traffic with hosts in public network.

Commands are issued on Router 1:

- ping 10.0.1.2 / telnet 10.0.1.2
  Command succeeds because PC 1 and Router 1 are in the same private network.
- ping 128.143.136.1 / telnet 128.143.136.1
  Command succeeds as all hosts in this private network are mapped to the same public IP address in the NAT table. Due to IP masquerading, all hosts in this private network are able to exchange traffic with hosts in public network.

Command is issued on PC 4:

- ping 10.0.1.2 / telnet 10.0.1.2
  Command fails as PC4 can not private address in a public network.

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

Ethereal data captured on PC1

- Outgoing Packet for command telnet 10.0.1.3

No. Time Source Destination Protocol Info
11 23.050695 10.0.1.2 10.0.1.3 TCP 54853 > telnet [ACK] Seq=1 Ack=1 Win=5840 Len=0
...
Internet Protocol, Src: 10.0.1.2 (10.0.1.2), Dst: 10.0.1.3 (10.0.1.3)
...

- Incoming Packet for command telnet 10.0.1.3

No. Time Source Destination Protocol Info
12 23.151035 10.0.1.3 10.0.1.2 TELNET Telnet Data ...
...
Internet Protocol, Src: 10.0.1.3 (10.0.1.3), Dst: 10.0.1.2 (10.0.1.2)
...

- Outgoing Packet for command telnet 128.143.136.1

No. Time Source Destination Protocol Info
27 1.011532 128.143.136.22 128.143.136.1 TELNET Telnet Data ...
...
Internet Protocol, Src: 128.143.136.22 (128.143.136.22), Dst: 128.143.136.1 (128.143.136.1)
...

- Incoming Packet for command telnet 128.143.136.1

No. Time Source Destination Protocol Info
31 1.013721 128.143.136.1 128.143.136.22 TELNET Telnet Data ...
...
Internet Protocol, Src: 128.143.136.1 (128.143.136.1), Dst: 128.143.136.22 (128.143.136.22)
…

Ethereal data captured on Router1

- Outgoing Packet Header for command telnet 10.0.1.2

No. Time Source Destination Protocol Info
55 24.998970 10.0.1.3 10.0.1.2 TELNET Telnet Data ...
...
Internet Protocol, Src: 10.0.1.3 (10.0.1.3), Dst: 10.0.1.2 (10.0.1.2)
...

- Incoming Packet for command telnet 10.0.1.2

No. Time Source Destination Protocol Info
56 25.000109 10.0.1.2 10.0.1.3 TCP telnet > 42875 [ACK] Seq=86 Ack=82 Win=5840 Len=0
...

Internet Protocol, Src: 10.0.1.2 (10.0.1.2), Dst: 10.0.1.3 (10.0.1.3)
...

- Outgoing Packet for command telnet 128.143.136.1

No. Time Source Destination Protocol Info
27 1.010012 128.143.136.22 128.143.136.1 TELNET Telnet Data ...
...
Internet Protocol, Src: 128.143.136.22 (128.143.136.22), Dst: 128.143.136.1 (128.143.136.1)
...

- Incoming Packet for command telnet 128.143.136.1

No. Time Source Destination Protocol Info
28 6.911825 128.143.136.1 128.143.136.22 TELNET Telnet Data ...
...
Internet Protocol, Src: 128.143.136.1 (128.143.136.1), Dst: 128.143.136.22 (128.143.136.22)
...

3. For each successful *ping* command, include the IP header of an outgoing ICMP Echo request message and an incoming ICMP Echo reply message.

Ethereal data captured on PC1

- Packets for command ping 10.0.1.3

No. Time Source Destination Protocol Info
14 18.235784 10.0.1.2 10.0.1.3 ICMP Echo (ping) request
...
Internet Protocol, Src: 10.0.1.2 (10.0.1.2), Dst: 10.0.1.3 (10.0.1.3)
...
No. Time Source Destination Protocol Info
15 18.320152 10.0.1.3 10.0.1.2 ICMP Echo (ping) reply
...
Internet Protocol, Src: 10.0.1.3 (10.0.1.3), Dst: 10.0.1.2 (10.0.1.2)
...

- Packets for command ping 128.143.136.1

No. Time Source Destination Protocol Info
7 8.999952 10.0.1.2 128.143.136.1 ICMP Echo (ping) request
...
Internet Protocol, Src: 10.0.1.2 (10.0.1.2), Dst: 128.143.136.1 (128.143.136.1)
...
No. Time Source Destination Protocol Info
8 1.000023 128.143.136.1 128.143.136.22 ICMP Echo (ping) reply
...
Internet Protocol, Src: 128.143.136.1 (128.143.136.1), Dst: 128.143.136.22 (128.143.136.22)
...

Ethereal data captured on Router1

- Packets for command ping 10.0.1.2

```
No.  Time       Source        Destination   Protocol Info
11   4.800460   10.0.1.3      10.0.1.2      ICMP Echo (ping) request
...
Internet Protocol, Src: 10.0.1.3 (10.0.1.3), Dst: 10.0.1.2 (10.0.1.2)
...
No.  Time       Source        Destination   Protocol Info
12   4.825520   10.0.1.2      10.0.1.3      ICMP Echo (ping) reply
...
Internet Protocol, Src: 10.0.1.2 (10.0.1.2), Dst: 10.0.1.3 (10.0.1.3)
...
```

- Packets for command ping 128.143.136.1

```
No.  Time       Source        Destination    Protocol Info
15   8.399925   10.0.1.3      128.143.136.1  ICMP Echo (ping) request
...
Internet Protocol, Src: 10.0.1.3 (10.0.1.3), Dst: 128.143.136.1 (128.143.136.1)
...
No.  Time       Source        Destination     Protocol Info
21   0.000109   128.143.136.1 128.143.136.22  ICMP Echo (ping) reply
...
Internet Protocol, Src: 128.143.136.1 (128.143.136.1), Dst: 128.143.136.22 (128.143.136.22)
...
```

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

When packets from the public network are received, the PC consults with its NAT table. If the packet matches the rules in the PREROUTING chain, it indicates that the packet is destined to a host in the private network.

5. **Explain the steps performed by the Linux kernel during IP address translation.**
   1) A packet arrives. The IP address is searched in NAT to determine if the packet matches any rules of the PREROUTING / POSTROUTING chains.
      a) For incoming datagrams,the PREROUTING chain is applied.
      b) For outgoing datagrams, the POSTROUTING chain is applied.
   2) If a match is found, the packet is modified according to the corresponding chain and sent to next hop / destination.

Exercise 1(D)

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 the IP packet is solved.

For the first case, NAT was not involved, both PC4 and PC2 have IP addresses that from the internet, thus no address translation is required for IP addresses in the data payload of the IP packet. As a result, FTP would work.

For the second case, NAT was involved in order for PC3 to establish a FTP session with PC4. This configuration was still using active FTP, since packets were being sent with the private IP address in the payload of the packet. Downloading files using this configuration was also successful.

On the private network, the host would put its private IP address on the PORT packet. Once that packet goes through the router into the public network, the IP address in the PORT packet was changed to match the translated public address.

Exercise 2(C)

Step 3

1. **What type of DHCP message can be observed ?**

4 types of DHCP messages can be observed.

- DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 7
- DHCPOFFER from 10.0.1.21
- DHCPREQUEST on eth0 to 255.255.255.255 port 67
- DHCPACK from 10.0.1.21

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

DHCP client waits 27 seconds until it attempts to renew its lease. This is should in dhclient.leases file

```
bound to 10.0.1.10 -- renewal in 27 seconds.
```

Step 4

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

Because PC3 can only receives traffic from Router 1 which hasn't been set as a DHCP relay agent.

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

No, a new IP address is assigned each time independently.

Lab Report

1. **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.**

The following is the selected data captured by *ethereal*

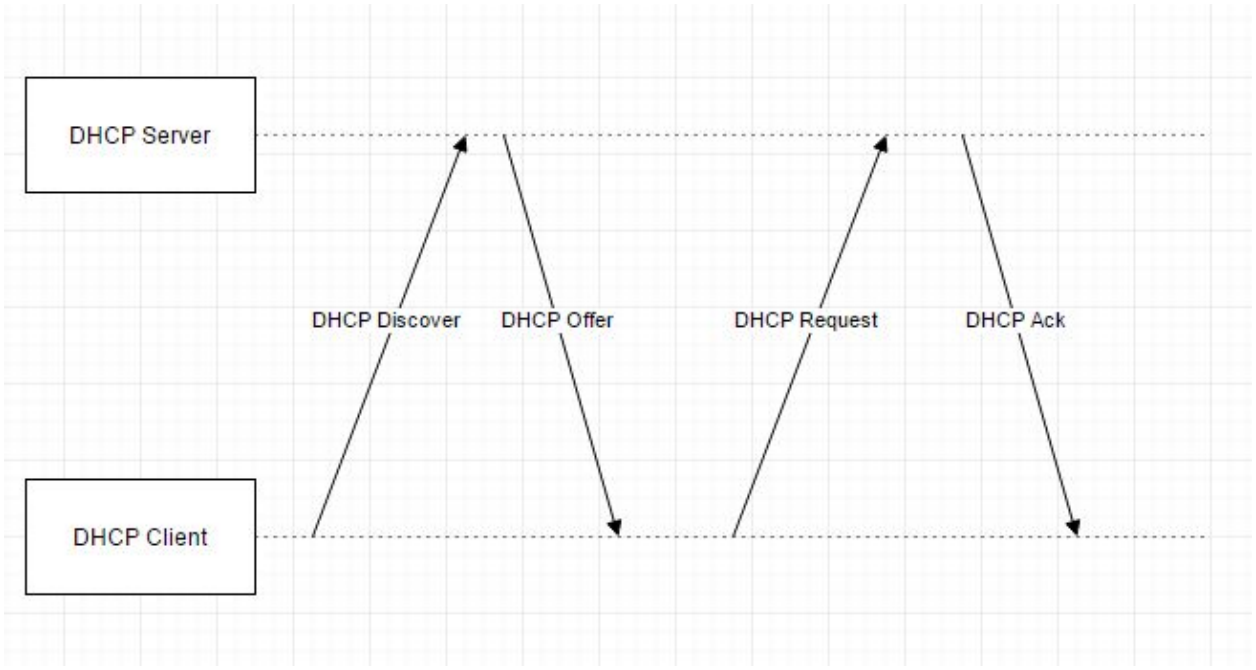
```
No.  Time       Source       Destination      Protocol Info
1    0.000000   0.0.0.0      255.255.255.255  DHCP     DHCP Discover
-
                                             Transaction ID
0x24616941
No.  Time       Source       Destination      Protocol Info
2    0.000290   10.0.1.21    10.0.1.9         DHCP     DHCP Offer -
                                             Transaction ID
0x24616941
```

```
No.  Time       Source       Destination      Protocol Info
3    0.000609   0.0.0.0      255.255.255.255  DHCP     DHCP Request
-
                                              Transaction ID
0x24616941

No.  Time       Source       Destination      Protocol Info
4    0.014603   10.0.1.21    10.0.1.9         DHCP     DHCP ACK -
                                              Transaction ID
0x24616941
```

The following steps take place when a DHCP client acquires an IP address.

1. DHCP client broadcasts a DHCPDISCOVER packet to find the DHCP server.
2. DHCP server receives the broadcast and replies an DHCPOFFER packet, whic contains the offered IP address
3. DHCP client receives DHCPOFFER packet and replies an DHCPREQUEST packet to request the placement of the offered IP address.
4. DHCP server acknowledges the request by replying DHCPACK packet.



2. Explain the entries in the lease file dhcpd.leases. How is the content of the lease file used when a DHCP client cannot contact the DHCP server.

The following is a selection of data stored in file dhcpd.leases

```
lease 10.0.3.10 {
  starts 5 2016/11/25 01:22:38;
  ends 5 2016/11/25 01:23:38;
```

```
  binding state active;
  next binding state free;
  hardware ethernet 00:04:5a:7a:c6:64;
}
```

The file indicates the starting and end time of a particular lease. The MAC address indicates the owner of the IP address.

When the DHCP client fails to contact the DHCP server, the lease file is used to determine the expiration time. If the IP address of the client is released after lease expiration, the dhcpd.leases file will be written to keep track of this.

3. **In most client-server applications, the port number of a server is a well-known number, while the client uses a currently available 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.**

By using well known ports for DHCP clients and servers, DHCP protocol enables the client to communicate with server without an IP address. DHCP server can reach the client, which doesn't have an IP address. by broadcasting to a certain UDP port.

Exercise 2 (D)

Step 3

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

The relay agent modifies the IP header of the DHCP packets. The relay agent substitutes the packet source IP address with its own address and the packet destination IP address with its DHCP server address.

The following is the selected data captured by *ethereal* on PC3

No.	Time	Source	Destination	Protocol	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x1542ec2b
No.	Time	Source	Destination	Protocol	Info
2	0.035885	10.0.3.1	10.0.3.10	DHCP	DHCP Offer - Transaction ID 0x1542ec2b

The following is the selected data captured by *ethereal* on PC2

No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.0.3.1	10.0.2.21	DHCP	DHCP Discover - Transaction ID 0x1542ec2b

No. Time Source Destination Protocol Info
2 0.033678 10.0.2.21 10.0.3.1 DHCP DHCP Offer -
Transaction ID 0x1542ec2b

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

After the DHCP server unicasts the reply to the relay agent, the relay agent will broadcast the replies back the to client as the client does not yet have its own 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.**

Instead of directly communicating with the client, the DHCP server sends the packets to the relay agent, which will be forward those packets to the client.

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

DHCP server (PC2) determines the subnet PC3 belongs to based on IP address of the DHCP relay that forwards the DHCP discover packet.

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

The destination IP address is 10.0.3.1.

The following is the selected data captured by ethereal

No. Time Source Destination Protocol Info
2 0.033678 10.0.2.21 10.0.3.1 DHCP DHCP Offer -
Transaction ID 0x1542ec2b

Lab Report

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

Ethereal data captured on PC3

No. Time Source Destination Protocol Info
1 0.000000 0.0.0.0 255.255.255.255 DHCP DHCP Discover -
Transaction ID 0x1542ec2b
No. Time Source Destination Protocol Info
2 0.035885 10.0.3.1 10.0.3.10 DHCP DHCP Offer -
Transaction ID 0x1542ec2b
No. Time Source Destination Protocol Info
3 0.036122 0.0.0.0 255.255.255.255 DHCP DHCP Request -
Transaction ID 0x1542ec2b

Ethereal data captured on PC2

No.	Time	Source	Destination	Protocol Info
1	0.000000	10.0.3.1	10.0.2.21	DHCP DHCP Discover - Transaction ID 0x1542ec2b
No.	Time	Source	Destination	Protocol Info
2	0.033678	10.0.2.21	10.0.3.1	DHCP DHCP Offer - Transaction ID 0x1542ec2b
No.	Time	Source	Destination	Protocol Info
3	0.036403	10.0.3.1	10.0.2.21	DHCP DHCP Request - Transaction ID 0x1542ec2b

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

Multiple DHCP servers may send DHCP offers, but the client will only accept one offer.

Exercise 3

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

***Ethereal* data from 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    0.000398  10.0.3.23  10.0.1.10     ICMP Echo (ping) reply
```

***Ethereal* data from 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    0.000275  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.**

Routing table of PC1

```
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
```

ifconfig output of PC1

```
eth0      Link encap:Ethernet  HWaddr 00:04:5A:7B:4D:1D
          inet6 addr: fe80::204:5aff:fe7b:4d1d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:25 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:47 dropped:0 overruns:0 carrier:94
          collisions:0 txqueuelen:1000
          RX bytes:9006 (8.7 KiB)  TX bytes:0 (0.0 b)
          Interrupt:16 Base address:0xd800

eth1      Link encap:Ethernet  HWaddr 00:04:5A:7A:C7:A2
          inet6 addr: fe80::204:5aff:fe7a:c7a2/64 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:40 errors:0 dropped:0 overruns:0 frame:0
          TX packets:40 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2824 (2.7 KiB)  TX bytes:2824 (2.7 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)
```

Routing table of PC2

```
Kernel IP routing table
Destination  Gateway   Genmask        Flags MSS Window irtt Iface
10.0.1.0     10.0.1.1  255.255.255.0   UG    0    0     0    eth0
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
```

ifconfig output of PC2

```
eth0      Link encap:Ethernet  HWaddr 00:04:5A:7A:C8:94
          inet addr:10.0.1.21  Bcast:10.0.1.255  Mask:255.255.255.0
          inet6 addr: fe80::204:5aff:fe7a:c894/64 Scope:Link
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:22 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:33 dropped:0 overruns:0 carrier:66
          collisions:0 txqueuelen:1000
          RX bytes:7642 (7.4 KiB)  TX bytes:0 (0.0 b)
          Interrupt:16 Base address:0xd800

eth1      Link encap:Ethernet  HWaddr 00:04:5A:80:2A:D0
          inet addr:10.0.2.21  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::204:5aff:fe80:2ad0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:129 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:45 dropped:0 overruns:0 carrier:90
```

collisions:0 txqueuelen:1000
RX bytes:40383 (39.4 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:36 errors:0 dropped:0 overruns:0 frame:0
TX packets:36 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:2560 (2.5 KiB) TX bytes:2560 (2.5 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)

Routing table of PC3

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

ifconfig output of PC3

eth0 Link encap:Ethernet HWaddr 00:04:5A:7B:21:D7
inet addr:10.0.3.23 Bcast:10.0.3.255 Mask:255.255.255.0
inet6 addr: fe80::204:5aff:fe7b:21d7/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:117 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:28 dropped:0 overruns:0 carrier:56
collisions:0 txqueuelen:1000
RX bytes:36954 (36.0 KiB) TX bytes:0 (0.0 b)
Interrupt:16 Base address:0xd800

eth1 Link encap:Ethernet HWaddr 00:04:5A:7A:C8:97
inet6 addr: fe80::204:5aff:fe7a:c897/64 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:28 errors:0 dropped:0 overruns:0 frame:0
TX packets:28 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:1912 (1.8 KiB) TX bytes:1912 (1.8 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)

Routing table of PC4

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

ifconfig output of PC4

eth0 Link encap:Ethernet HWaddr 00:04:5A:80:93:F3
inet6 addr: fe80::204:5aff:fe80:93f3/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:33 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:39 dropped:0 overruns:0 carrier:78
collisions:0 txqueuelen:1000
RX bytes:15466 (15.1 KiB) TX bytes:0 (0.0 b)
Interrupt:16 Base address:0xd800

eth1 Link encap:Ethernet HWaddr 00:02:44:BF:31:A6
UP BROADCAST MULTICAST MTU:1500 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:1000

RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
Interrupt:20 Base address:0xcb00

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 from PC2

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