

## 網路系統總整與實作 Lab #3

### Dynamic Routing and Network Address Translation

0716236 劉耀文

#### Part 1 BGP and Zebra configuration

##### 1. Take routing tables screenshot before/after on [r1-r4] (10%)

```
ywliu722@SDN-NFV: ~/NSCap/Lab/Lab3
檔案(F) 編輯(E) 檢視(V) 搜尋(S) 終端機(T) 求助(H)
ywliu722@SDN-NFV:~/NSCap/Lab/Lab3$ sudo python topology.py
[sudo] password for ywliu722:
mininet> r1 route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
10.0.1.0 0.0.0.0 255.255.255.0 U 0 0 0 r1-eth0
192.168.1.0 0.0.0.0 255.255.255.192 U 0 0 0 r1-eth1
192.168.1.64 0.0.0.0 255.255.255.192 U 0 0 0 r1-eth2
mininet> r2 route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
10.0.0.0 0.0.0.0 255.255.255.0 U 0 0 0 r2-eth0
10.0.1.0 0.0.0.0 255.255.255.0 U 0 0 0 r2-eth1
mininet> r3 route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
10.0.0.0 0.0.0.0 255.255.255.0 U 0 0 0 r3-eth0
10.0.2.0 0.0.0.0 255.255.255.0 U 0 0 0 r3-eth1
mininet> r4 route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
10.0.2.0 0.0.0.0 255.255.255.0 U 0 0 0 r4-eth0
140.114.0.0 0.0.0.0 255.255.255.0 U 0 0 0 r4-eth1
mininet>
```

➔ 一開始尚未載入 BGP 的 routing table，除了有連接到的子網之外沒有其他項目。

```
ywliu722@SDN-NFV: ~/NSCap/Lab/Lab3
檔案(F) 編輯(E) 檢視(V) 搜尋(S) 終端機(T) 求助(H)
mininet> r1 route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
10.0.1.0 0.0.0.0 255.255.255.0 U 0 0 0 r1-eth0
140.114.0.0 10.0.1.1 255.255.0.0 UG 20 0 0 r1-eth0
192.168.1.0 0.0.0.0 255.255.255.192 U 0 0 0 r1-eth1
192.168.1.64 0.0.0.0 255.255.255.192 U 0 0 0 r1-eth2
mininet> r2 route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
10.0.0.0 0.0.0.0 255.255.255.0 U 0 0 0 r2-eth0
10.0.1.0 0.0.0.0 255.255.255.0 U 0 0 0 r2-eth1
140.113.0.0 10.0.1.2 255.255.0.0 UG 20 0 0 r2-eth1
140.114.0.0 10.0.0.2 255.255.0.0 UG 20 0 0 r2-eth0
mininet> r3 route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
10.0.0.0 0.0.0.0 255.255.255.0 U 0 0 0 r3-eth0
10.0.2.0 0.0.0.0 255.255.255.0 U 0 0 0 r3-eth1
140.113.0.0 10.0.0.1 255.255.0.0 UG 20 0 0 r3-eth0
140.114.0.0 10.0.2.3 255.255.0.0 UG 20 0 0 r3-eth1
mininet> r4 route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
10.0.2.0 0.0.0.0 255.255.255.0 U 0 0 0 r4-eth0
140.113.0.0 10.0.2.1 255.255.0.0 UG 20 0 0 r4-eth0
140.114.0.0 0.0.0.0 255.255.255.0 U 0 0 0 r4-eth1
mininet>
```

➔ 逐一載入 zebra 以及 BGP 設定檔並完成路由探索之後的結果，由於在 r2 以及 r3 的 BGP 設定檔中並沒有設定所屬子網域 IP，故只會增加 r1 以及 r4 連接之子網域 IP。

## 2. Telnet zebra and bgpd daemons of [r1-r4] and take screenshots of routes in zebra and bgpd daemons. (10%)

```

root@SDN-NFV: ~/NSCap/Lab/Lab3
root@SDN-NFV:~/NSCap/Lab/Lab3# telnet 127.0.0.1 2601
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.

Hello, this is Quagga (version 1.2.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

User Access Verification

Password:
Password:
zebra> show ip route bgp
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, P - PIM, A - Babel, N - NHRP,
       > - selected route, * - FIB route
B>* 140.114.0.0/16 [20/0] via 10.0.1.1, r1-eth0, 00:07:14
zebra>

```

```

root@SDN-NFV: ~/NSCap/Lab/Lab3
root@SDN-NFV:~/NSCap/Lab/Lab3# telnet 127.0.0.1 2601
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.

Hello, this is Quagga (version 1.2.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

User Access Verification

Password:
zebra> show ip route bgp
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, P - PIM, A - Babel, N - NHRP,
       > - selected route, * - FIB route
B>* 140.113.0.0/16 [20/0] via 10.0.1.2, r2-eth1, 00:07:59
B>* 140.114.0.0/16 [20/0] via 10.0.0.2, r2-eth0, 00:07:54
zebra>

```

```

root@SDN-NFV: ~/NSCap/Lab/Lab3
root@SDN-NFV:~/NSCap/Lab/Lab3# telnet 127.0.0.1 2601
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.

Hello, this is Quagga (version 1.2.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

User Access Verification

Password:
zebra> show ip route bgp
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, P - PIM, A - Babel, N - NHRP,
       > - selected route, * - FIB route
B>* 140.113.0.0/16 [20/0] via 10.0.0.1, r3-eth0, 00:07:40
B>* 140.114.0.0/16 [20/0] via 10.0.2.3, r3-eth1, 00:07:45
zebra>

```

```

root@SDN-NFV: ~/NSCap/Lab/Lab3
root@SDN-NFV:~/NSCap/Lab/Lab3# telnet 127.0.0.1 2601
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.

Hello, this is Quagga (version 1.2.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

User Access Verification

Password:
zebra> show ip route bgp
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, P - PIM, A - Babel, N - NHRP,
       > - selected route, * - FIB route
B>* 140.113.0.0/16 [20/0] via 10.0.2.1, r4-eth0, 00:08:01
zebra>

```

➔ Zebra daemon 顯示除了自己所在子網之外的 routing table entries。左上 r1、右上 r2、左下 r3、右下 r4。

```

root@SDN-NFV: ~/NSCap/Lab/Lab3
Connected to 127.0.0.1.
Escape character is '^]'.

Hello, this is Quagga (version 1.2.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

User Access Verification

Password:
r1> show ip bgp summary
BGP router identifier 10.0.1.2, local AS number 65000
RIB entries 3, using 336 bytes of memory
Peers 1, using 9088 bytes of memory

Neighbor      V      AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
10.0.1.1      4 65001   186    189     0  0  0 00:09:10    1
Total number of neighbors 1
Total num. Established sessions 1
Total num. of routes received 1
r1>

```

```

root@SDN-NFV: ~/NSCap/Lab/Lab3
Escape character is '^]'.

Hello, this is Quagga (version 1.2.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

User Access Verification

Password:
r2> show ip bgp summary
BGP router identifier 10.0.0.1, local AS number 65000
RIB entries 3, using 336 bytes of memory
Peers 2, using 18 KiB of memory

Neighbor      V      AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
10.0.0.2      4 65002   192    195     0  0  0 00:09:30    1
10.0.1.2      4 65000   193    194     0  0  0 00:09:30    1
Total number of neighbors 2
Total num. Established sessions 2
Total num. of routes received 2
r2>

```

```

root@SDN-NFV: ~/NSCap/Lab/Lab3
Escape character is '^]'.

Hello, this is Quagga (version 1.2.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

User Access Verification

Password:
r3> show ip bgp summary
BGP router identifier 10.0.2.1, local AS number 65002
RIB entries 3, using 336 bytes of memory
Peers 2, using 18 KiB of memory

Neighbor      V      AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
10.0.0.1      4 65001   190    191     0  0  0 00:09:21    1
10.0.2.3      4 65003   189    192     0  0  0 00:09:21    1
Total number of neighbors 2
Total num. Established sessions 2
Total num. of routes received 2
r3>

```

```

root@SDN-NFV: ~/NSCap/Lab/Lab3
Connected to 127.0.0.1.
Escape character is '^]'.

Hello, this is Quagga (version 1.2.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

User Access Verification

Password:
r4> show ip bgp summary
BGP router identifier 10.0.2.3, local AS number 65003
RIB entries 3, using 336 bytes of memory
Peers 1, using 9088 bytes of memory

Neighbor      V      AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
10.0.2.1      4 65002   198    199     0  0  0 00:09:43    1
Total number of neighbors 1
Total num. Established sessions 1
Total num. of routes received 1
r4>

```



➔ BGPd daemon 顯示了此 router 連接之其他 router 以及其所在之 AS。左上 r1、右上 r2、左下 r3、右下 r4。

### 3. Capture BGP packets from wireshark and take screenshot to verify your answer for the following questions (20%)

#### 3-1 Show BGP packets (OPEN, UPDATE, KEEP ALIVE) exchanged by r2 and r3

+r2-eth0						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
bgp						
No.	Time	Source	Destination	Protocol	Length	Info
20	76.351170619	10.0.0.2	10.0.0.1	BGP	125	OPEN Message
22	76.351421829	10.0.0.1	10.0.0.2	BGP	144	OPEN Message, KEEPALIVE Message
24	76.351592167	10.0.0.2	10.0.0.1	BGP	104	KEEPALIVE Message, KEEPALIVE Message
26	76.351664730	10.0.0.1	10.0.0.2	BGP	85	KEEPALIVE Message
28	77.352752648	10.0.0.2	10.0.0.1	BGP	89	UPDATE Message
30	77.352828788	10.0.0.1	10.0.0.2	BGP	140	UPDATE Message, UPDATE Message
32	79.352220072	10.0.0.1	10.0.0.2	BGP	85	KEEPALIVE Message
34	79.352447825	10.0.0.2	10.0.0.1	BGP	85	KEEPALIVE Message
36	82.353143500	10.0.0.1	10.0.0.2	BGP	85	KEEPALIVE Message
38	82.353203332	10.0.0.2	10.0.0.1	BGP	85	KEEPALIVE Message
40	85.353324009	10.0.0.1	10.0.0.2	BGP	85	KEEPALIVE Message
42	85.353386655	10.0.0.2	10.0.0.1	BGP	85	KEEPALIVE Message
44	88.354152154	10.0.0.1	10.0.0.2	BGP	85	KEEPALIVE Message

+r3-eth0						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
bgp						
No.	Time	Source	Destination	Protocol	Length	Info
18	45.625329023	10.0.0.2	10.0.0.1	BGP	125	OPEN Message
20	45.625581850	10.0.0.1	10.0.0.2	BGP	144	OPEN Message, KEEPALIVE Message
22	45.625750237	10.0.0.2	10.0.0.1	BGP	104	KEEPALIVE Message, KEEPALIVE Message
24	45.625824520	10.0.0.1	10.0.0.2	BGP	85	KEEPALIVE Message
26	46.626908085	10.0.0.2	10.0.0.1	BGP	89	UPDATE Message
28	46.626988682	10.0.0.1	10.0.0.2	BGP	140	UPDATE Message, UPDATE Message
30	48.626386932	10.0.0.1	10.0.0.2	BGP	85	KEEPALIVE Message
32	48.626602901	10.0.0.2	10.0.0.1	BGP	85	KEEPALIVE Message
34	51.627305082	10.0.0.1	10.0.0.2	BGP	85	KEEPALIVE Message
36	51.627361484	10.0.0.2	10.0.0.1	BGP	85	KEEPALIVE Message
38	54.627485799	10.0.0.1	10.0.0.2	BGP	85	KEEPALIVE Message
40	54.627544732	10.0.0.2	10.0.0.1	BGP	85	KEEPALIVE Message
42	57.628318989	10.0.0.1	10.0.0.2	BGP	85	KEEPALIVE Message

+r3-eth1						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
bgp						
No.	Time	Source	Destination	Protocol	Length	Info
20	63.715509706	10.0.2.3	10.0.2.1	BGP	125	OPEN Message
22	63.715714827	10.0.2.1	10.0.2.3	BGP	144	OPEN Message, KEEPALIVE Message
24	63.715793021	10.0.2.3	10.0.2.1	BGP	104	KEEPALIVE Message, KEEPALIVE Message
26	63.715846404	10.0.2.1	10.0.2.3	BGP	85	KEEPALIVE Message
28	64.717217663	10.0.2.3	10.0.2.1	BGP	143	UPDATE Message, UPDATE Message
30	64.717354432	10.0.2.1	10.0.2.3	BGP	144	UPDATE Message, UPDATE Message
32	66.716404282	10.0.2.1	10.0.2.3	BGP	85	KEEPALIVE Message
33	66.716422007	10.0.2.3	10.0.2.1	BGP	85	KEEPALIVE Message
36	69.719754547	10.0.2.1	10.0.2.3	BGP	85	KEEPALIVE Message
38	69.720085382	10.0.2.3	10.0.2.1	BGP	85	KEEPALIVE Message
40	72.721005659	10.0.2.1	10.0.2.3	BGP	85	KEEPALIVE Message
42	72.721195902	10.0.2.3	10.0.2.1	BGP	85	KEEPALIVE Message
44	75.722685522	10.0.2.1	10.0.2.3	BGP	85	KEEPALIVE Message

➔ r2-eth0 以及 r3-eth0 可以列出 r2 以及 r3 兩個 router 之間的交換訊息封包、r3-eth1 可以列出 r3 以及 r4 兩個 router 之間的交換訊息封包。

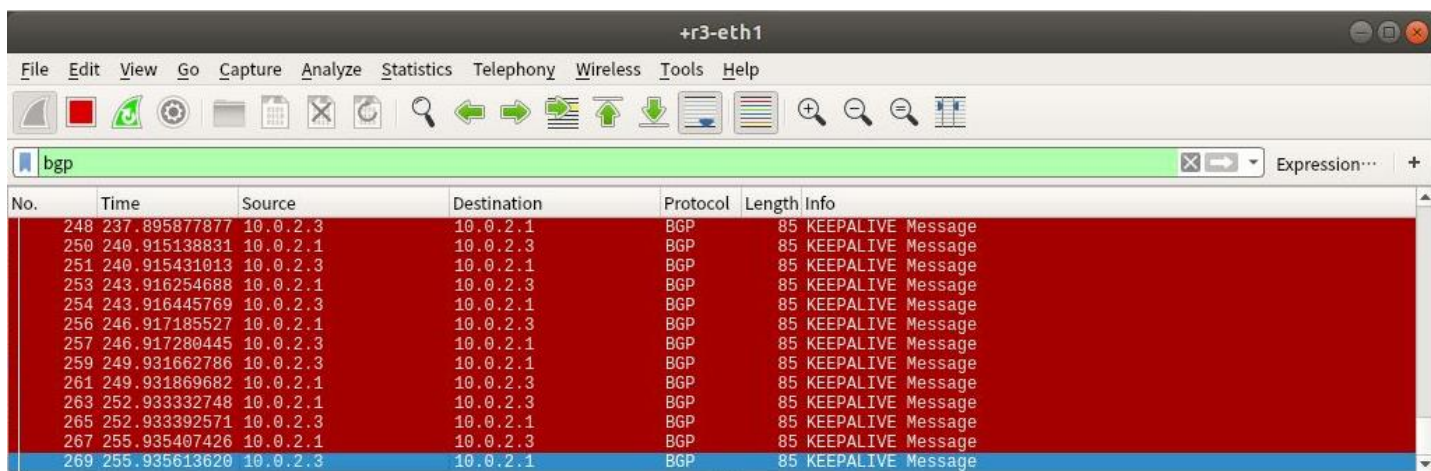
### 3-2 What will happen to the routing table if you set r4-eth0 down?

```
ywliu722@SDN-NFV: ~/NSCap/Lab/Lab3
檔案(F) 編輯(E) 檢視(V) 搜尋(S) 終端機(T) 求助(H)

mininet> r4 ip link set r4-eth0 down
mininet> r1 route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
10.0.2.0 0.0.0.0 255.255.255.0 U 0 0 0 r4-eth0
140.113.0.0 10.0.2.1 255.255.0.0 UG 20 0 0 r4-eth0
140.114.0.0 0.0.0.0 255.255.255.0 U 0 0 0 r4-eth1
mininet> r2 route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
10.0.1.0 0.0.0.0 255.255.255.192 U 0 0 0 r1-eth0
192.168.1.0 0.0.0.0 255.255.255.192 U 0 0 0 r1-eth1
192.168.1.64 0.0.0.0 255.255.255.192 U 0 0 0 r1-eth2
mininet> r3 route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
10.0.0.0 0.0.0.0 255.255.255.0 U 0 0 0 r2-eth0
10.0.1.0 0.0.0.0 255.255.255.0 U 0 0 0 r2-eth1
140.113.0.0 10.0.1.2 255.255.0.0 UG 20 0 0 r2-eth1
mininet> r4 route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
10.0.0.0 0.0.0.0 255.255.255.0 U 0 0 0 r3-eth0
10.0.2.0 0.0.0.0 255.255.255.0 U 0 0 0 r3-eth1
140.113.0.0 10.0.0.1 255.255.0.0 UG 20 0 0 r3-eth0
mininet>
```

→ 此圖為執行指令後的 routing table。將 r4 的 eth0 介面關閉後，r4 便無法和外部交換 BGP keep alive 封包，故其他 router 會認為 r4 已經關閉，便將 r4 所在之子網域從 routing table 移除。

### 3-3 How does r3 know r4 is unreachable? Explain how



No.	Time	Source	Destination	Protocol	Length	Info
248	237.895877877	10.0.2.3	10.0.2.1	BGP	85	KEEPALIVE Message
250	240.915138831	10.0.2.1	10.0.2.3	BGP	85	KEEPALIVE Message
251	240.915431013	10.0.2.3	10.0.2.1	BGP	85	KEEPALIVE Message
253	243.916254688	10.0.2.1	10.0.2.3	BGP	85	KEEPALIVE Message
254	243.916445769	10.0.2.3	10.0.2.1	BGP	85	KEEPALIVE Message
256	246.917185527	10.0.2.1	10.0.2.3	BGP	85	KEEPALIVE Message
257	246.917280445	10.0.2.3	10.0.2.1	BGP	85	KEEPALIVE Message
259	249.931662786	10.0.2.3	10.0.2.1	BGP	85	KEEPALIVE Message
261	249.931869682	10.0.2.1	10.0.2.3	BGP	85	KEEPALIVE Message
263	252.933332748	10.0.2.1	10.0.2.3	BGP	85	KEEPALIVE Message
265	252.933392571	10.0.2.3	10.0.2.1	BGP	85	KEEPALIVE Message
267	255.935407426	10.0.2.1	10.0.2.3	BGP	85	KEEPALIVE Message
269	255.935613620	10.0.2.3	10.0.2.1	BGP	85	KEEPALIVE Message

→ 此圖為 r3-eth1 所經過之 BGP 封包。如上題所述，r4 的 eth0 介面關閉後 r3 的 eth1 便無法與之聯繫，BGP keep alive 封包的持續傳輸也隨之停止，r3 也因此得知 r4 目前為 unreachable 的狀態。



### 3-4 How does r2 know r4 is unreachable? Explain how

The image shows a Wireshark packet capture on the interface r3-eth0. The packet list displays a series of BGP messages. The packet details pane for Frame 282 (a BGP UPDATE message) is expanded, showing the following structure:

- Marker: ffffffffffffffffffffffffffffffffff
- Length: 26
- Type: UPDATE Message (2)
- Withdrawn Routes Length: 3
- Withdrawn Routes
  - 140.114.0.0/16
- Total Path Attribute Length: 0

➔ 此圖為 r3-eth0 所經過之 BGP 封包。由於 r3 已經得知 r4 為 unreachable 的狀態，所以會傳送 BGP update 封包(withdraw routes)給所有連接的 router(目前只剩下 r2)，告訴所有 router 之前存在的 r4 現在已經離線，所以要更新會經過該點的路由或是 r4 所在的子網域路由，因此 r2 便能知道 r4 目前為 unreachable 狀態。

## Part 2 Source NAT and Destination NAT

### 1. Take screenshot of curl result (10%)

```
ywliu722@SDN-NFV: ~/NSCap/Lab/Lab3
檔案(F) 編輯(E) 檢視(V) 搜尋(S) 終端機(T) 求助(H)

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

mininet> h3 python -m SimpleHTTPServer &
mininet> h4 curl 140.113.0.40:80
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 3.2 Final//EN"><html>
<title>Directory listing for /</title>
<body>
<h2>Directory listing for /</h2>
<hr>
<ul>
<li><a href="/configs/">configs</a>
<li><a href="/dhcpd.conf">dhcpd.conf</a>
<li><a href="/example/">example</a>
<li><a href="/src/">src</a>
<li><a href="/topology.py">topology.py</a>
</ul>
<hr>
</body>
</html>
mininet>
```

➔ 此為 h4 透過 curl 這個程式來聯繫位於 h3 上的 HTTP server 所得到之回傳訊息。由於我們有在 iptables 設定 DNAT，故外部的 h4 可以與子網域內的 h3 聯繫。

### 2. Check reachability and take screenshot (10%)

```
ywliu722@SDN-NFV: ~/NSCap/Lab/Lab3
檔案(F) 編輯(E) 檢視(V) 搜尋(S) 終端機(T) 求助(H)

</ul>
<hr>
</body>
</html>
mininet> h1 ping h4 -c 1
PING 140.114.0.1 (140.114.0.1) 56(84) bytes of data:
64 bytes from 140.114.0.1: icmp_seq=1 ttl=60 time=0.362 ms

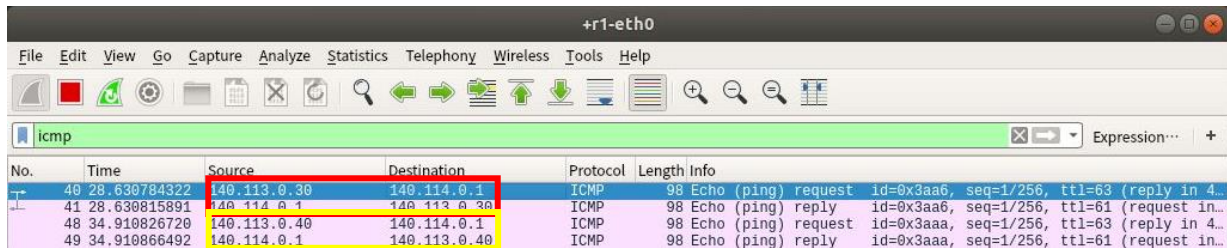
--- 140.114.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.362/0.362/0.362/0.000 ms
mininet> h2 ping h4 -c 1
PING 140.114.0.1 (140.114.0.1) 56(84) bytes of data:
64 bytes from 140.114.0.1: icmp_seq=1 ttl=60 time=0.308 ms

--- 140.114.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.308/0.308/0.308/0.000 ms
mininet> h3 ping h4 -c 1
Serving HTTP on 0.0.0.0 port 8000 ...
140.114.0.1 - - [20/Mar/2021 23:36:44] "GET / HTTP/1.1" 200 -
PING 140.114.0.1 (140.114.0.1) 56(84) bytes of data:
64 bytes from 140.114.0.1: icmp_seq=1 ttl=60 time=0.293 ms

--- 140.114.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.293/0.293/0.293/0.000 ms
mininet>
```

➔ 此圖為 h1、h2、h3 對 h4 執行 ping 指令的結果。由於我們有在 iptables 設定 SNAT，故可以將封包於傳出 r1 之前改變 source IP，r1 在收到來自 h4 的回應封包之後，也可以透過 SNAT 所轉換的結果將封包回傳給對應的 host，所以 h1、h2、h3 之間是可以連通的(h1 有先透過 DHCP 取得 IP(from Lab2)，故也可以和 h4 連通)。

3. Run wireshark on r1 to take screenshot of input/output packet (10%)  
Explain the difference of packet headers



Wireshark capture on r1-eth0 showing ICMP traffic. The filter is 'icmp'. The table below shows the captured packets with source and destination IP addresses highlighted in red and yellow.

No.	Time	Source	Destination	Protocol	Length	Info
40	28.630784322	140.113.0.30	140.114.0.1	ICMP	98	Echo (ping) request id=0x3aa6, seq=1/256, ttl=63 (reply in 4...)
41	28.630815891	140.114.0.1	140.113.0.30	ICMP	98	Echo (ping) reply id=0x3aa6, seq=1/256, ttl=61 (request in...)
48	34.910826720	140.113.0.40	140.114.0.1	ICMP	98	Echo (ping) request id=0x3aaa, seq=1/256, ttl=63 (reply in 4...)
49	34.910866492	140.114.0.1	140.113.0.40	ICMP	98	Echo (ping) reply id=0x3aaa, seq=1/256, ttl=61 (request in...)



Wireshark capture on r1-eth1 showing ICMP traffic. The filter is 'icmp'. The table below shows the captured packets with source and destination IP addresses highlighted in red.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.8	140.114.0.1	ICMP	98	Echo (ping) request id=0x3aa6, seq=1/256, ttl=64 (reply in 2)
2	0.000052741	140.114.0.1	192.168.1.8	ICMP	98	Echo (ping) reply id=0x3aa6, seq=1/256, ttl=60 (request in...)



Wireshark capture on r1-eth2 showing ICMP traffic. The filter is 'icmp'. The table below shows the captured packets with source and destination IP addresses highlighted in yellow.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.65	140.114.0.1	ICMP	98	Echo (ping) request id=0x3aaa, seq=1/256, ttl=64 (reply in 2)
2	0.000056259	140.114.0.1	192.168.1.65	ICMP	98	Echo (ping) reply id=0x3aaa, seq=1/256, ttl=60 (request in...)

➔ 根據 SNAT 的設定，192.168.0.0/26 的 IP 會轉換為 140.113.0.30、192.168.0.64/26 的 IP 會轉換為 140.113.0.40，可以從上圖觀察出 r1 在 eth1 以及 eth2 接收到的封包，會根據所在之子網對 source IP 進行轉換，使外部網路所看到之 source IP 皆來自 140.113.0.0/16，而非子網內的 192.168.0.0/24，收到回應封包後也會根據 SNAT 轉換規則將 destination IP 改為子網內的 IP。