網路系統總整與實作 Final Project

Virtual Customer Premise Equipment

0716236 劉耀文

1. Show the configuration commands you made on each node to provide Internet connectivity for hosts and briefly explain the purpose of the commands (10%)
   a) BRG1
      ■ GRE over UDP (statically)
      (1) docker exec -it BRG1 dhclient BRG1-eth1
         ➔ 從 edge router 上的 DHCP server 取得 IP 以及 default gateway(edge router)

      (2) sudo modprobe fou
         ➔ 將 fou 所需的 Linux kernel module 載入(每次開機都須執行一次)

      (3) docker exec -it BRG1 ip fou add port 11111 ipproto 47
         ➔ 將 port 11111 指定爲 fou receiving port 並將接收之封包以 GRE 封包做處理

      (4) docker exec -it BRG1 ip link add GRE type gretap remote 140.113.0.2 local \
      172.27.140.236 key 11111 encap fou encap-sport 11111 encap-dport 33333
         ➔ 建立與 BRGr 的 gretap tunnel，其中 key 選項是爲了和 BRG2 所建立的通道做區別而設定，因對 BRGr 而言 BRG1 以及 BRG2 的 IP address 相同(通過 edge 上的 NAT)，若無此設定選項將無法同時於兩個 router 間(edge NAT side / BRGr)建立兩條通道。

      (5) docker exec -it BRG1 ip link set GRE up
         ➔ 將建立好的 GRETAP 介面啓動。

      (6) docker exec -it BRG1 ip link add br0 type bridge
         ➔ 建立一個 bridge 裝置，以連接 BRG1-eth0(與 h1 連接之介面)以及 GRETAP 介面。

      (7) docker exec -it BRG1 brctl addif br0 BRG1-eth0
      docker exec -it BRG1 brctl addif br0 GRE
         ➔ 將 BRG1-eth0 以及 GRETAP 介面和 bridge 連接。

      (8) docker exec -it BRG1 ip link set br0 up
         ➔ 將 br0 啓動來讓封包可以從 GRETAP 以及 BRG1-eth0 通過。

b) BRGr

■ GRE over UDP (dynamically)

(1) docker exec -it BRGr ip addr add 140.113.0.2/16 dev BRGr-eth1

➔ 設定 WAN port 的 IP address。

(2) docker exec -it BRGr ip route add 140.114.0.0/16 via 140.113.0.1
docker exec -it BRGr ip route add default dev BRGr-eth0

➔ 設定 static routing rules 來讓封包到達正確位置，若 destination IP 爲 140.114.0.0 網段(GRE 封裝後要送給 hosts 的封包)則將封包往 WAN port 送，其他皆往 GWr 送。

(3) sudo docker cp ./0716236 BRGr:/

➔ 將事先在 VM 上編譯好的 Auto Creation Program 執行檔複製到 BRGr。

(4) docker exec -it BRGr ./0716236

➔ 在 BRGr 上執行 Auto Creation Program，並以 udp 作爲初始 filter expression，來過濾 fou 封包，並分析對應之 IP/port 來自動建立另一方向之 tunnel。

c) Edge Router

■ DHCP for BRG1, BRG2

(1) sudo docker cp /var/lib/dhcp/dhcpd.leases edge:/var/lib/dhcp/dhcpd.leases

➔ 因 container 內並沒有 DHCP server 用來記錄租借 IP 的檔案，故需要先將此檔案從 VM 上複製一份至 container 當中。

(2) sudo docker cp ./dhcpd.conf edge:/

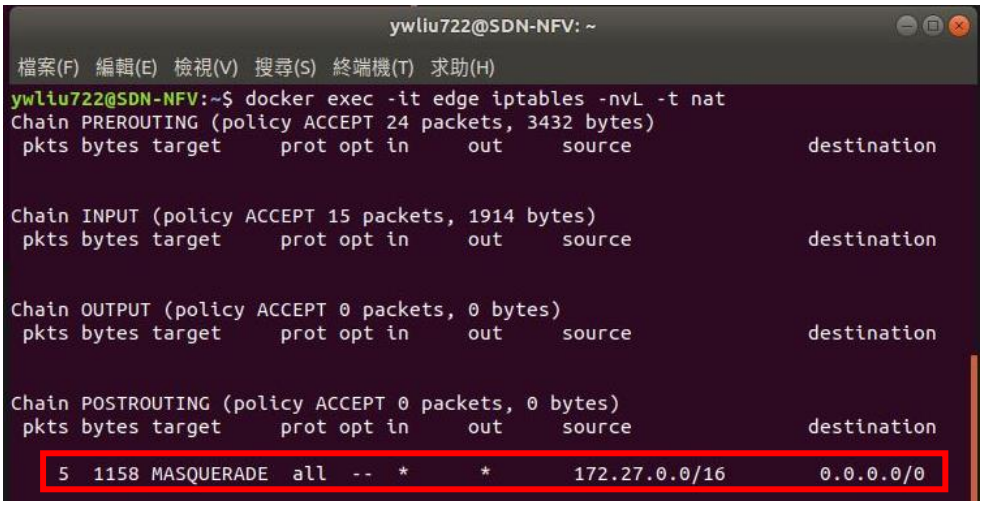
➔ 將事先編輯好的 dhcpd.conf 從 VM 複製至 container 當中。

(3) docker exec -it edge /usr/sbin/dhcpd 4 -pf /run/dhcp-server-dhcpd.pid \
-cf ./dhcpd.conf edge-eth1

➔ 將 DHCP server 建立於 edge-eth1 介面上，讓 BRG1 以及 BRG2 能夠以此獲得 IP 位置，並以 dhcpd.conf 作爲 DHCP server 的設定檔。/usr/sbin/dhcpd 爲建立 DHCP server 的 demon；4 代表 IPv4；-pf /run/dhcp-server-dhcpd.pid 代表將 DHCP server 的 PID 存放在此位置。

■ NAT rules for BRG1 (show NAT tables to justify your answer)

(1) docker exec -it edge iptables -t nat -A POSTROUTING -s 172.27.0.0/16 -j \
MASQUERADE



➔ 將來自 172.27.0.0/16 網段的所有封包做 NAT translate，轉換之目標 IP 則是由 iptables 從介面當中選擇適合之目標 IP，以將封包送往 GWr。

d) GWr

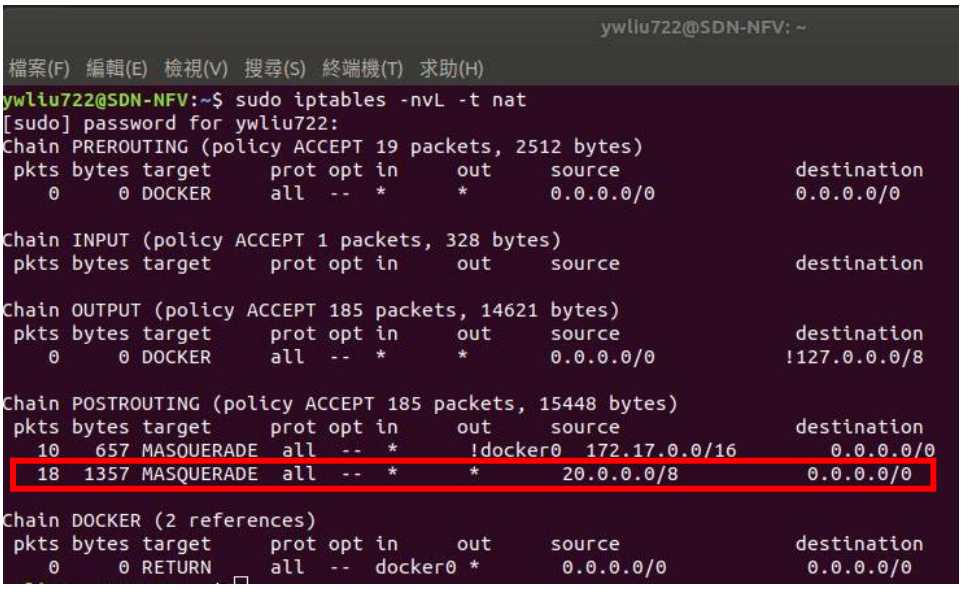
■ DHCP for hosts

(1) sudo /usr/sbin/dhcpd 4 -pf /run/dhcp-server-dhcpd.pid -cf ./dhcpd_outer.conf \
veth

➔ 將 DHCP server 建立於 veth 介面上，讓 BRG1 以及 BRG2 能夠以此獲得 IP 位置，並以 dhcpd_outer.conf 作爲 DHCP server 的設定檔。/usr/sbin/dhcpd 爲建立 DHCP server 的 demon；4 代表 IPv4；-pf /run/dhcp-server-dhcpd.pid 代表將 DHCP server 的 PID 存放在此位置。

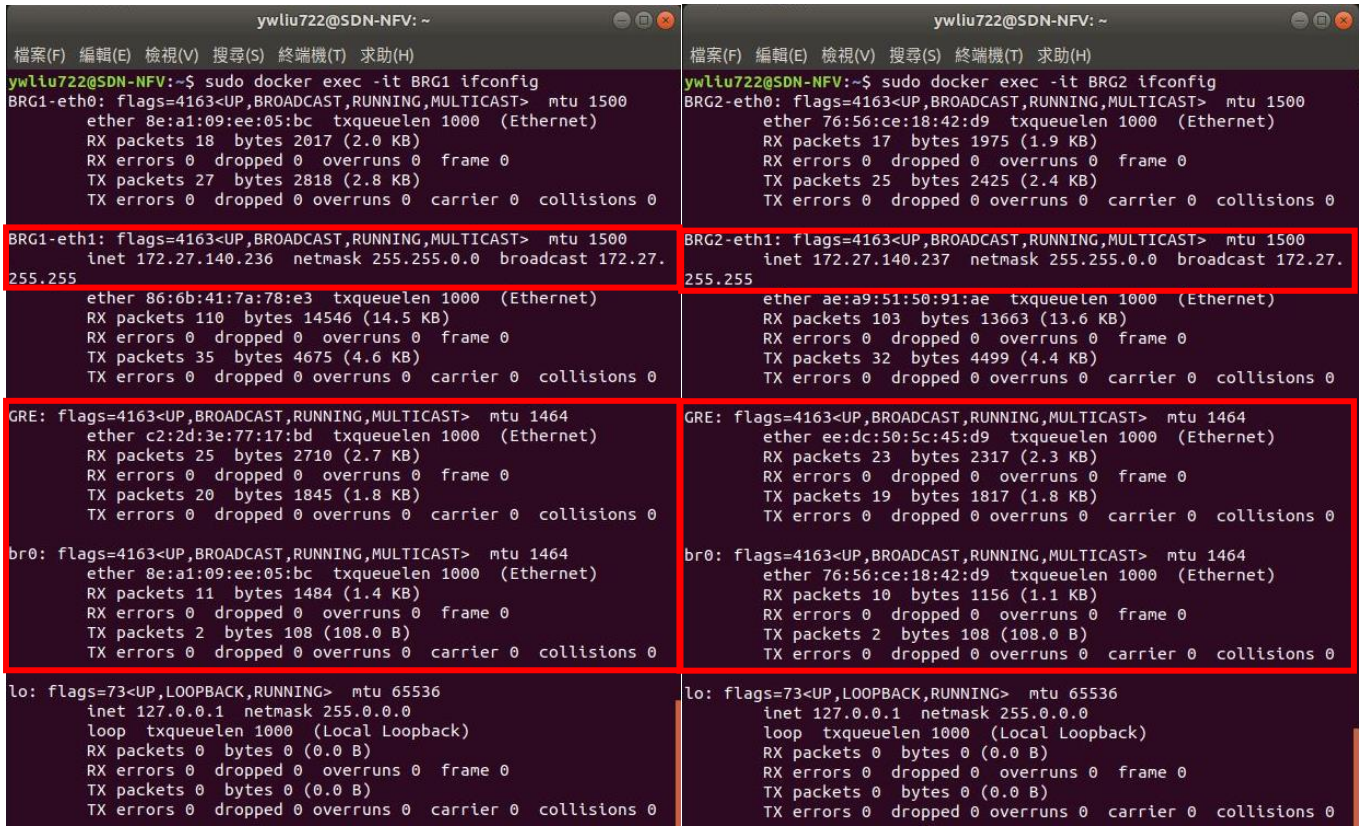
■ NAT rules for hosts (show NAT tables to justify your answer)

(1) sudo iptables -t nat -A POSTROUTING -s 20.0.0.0/8 -j MASQUERADE

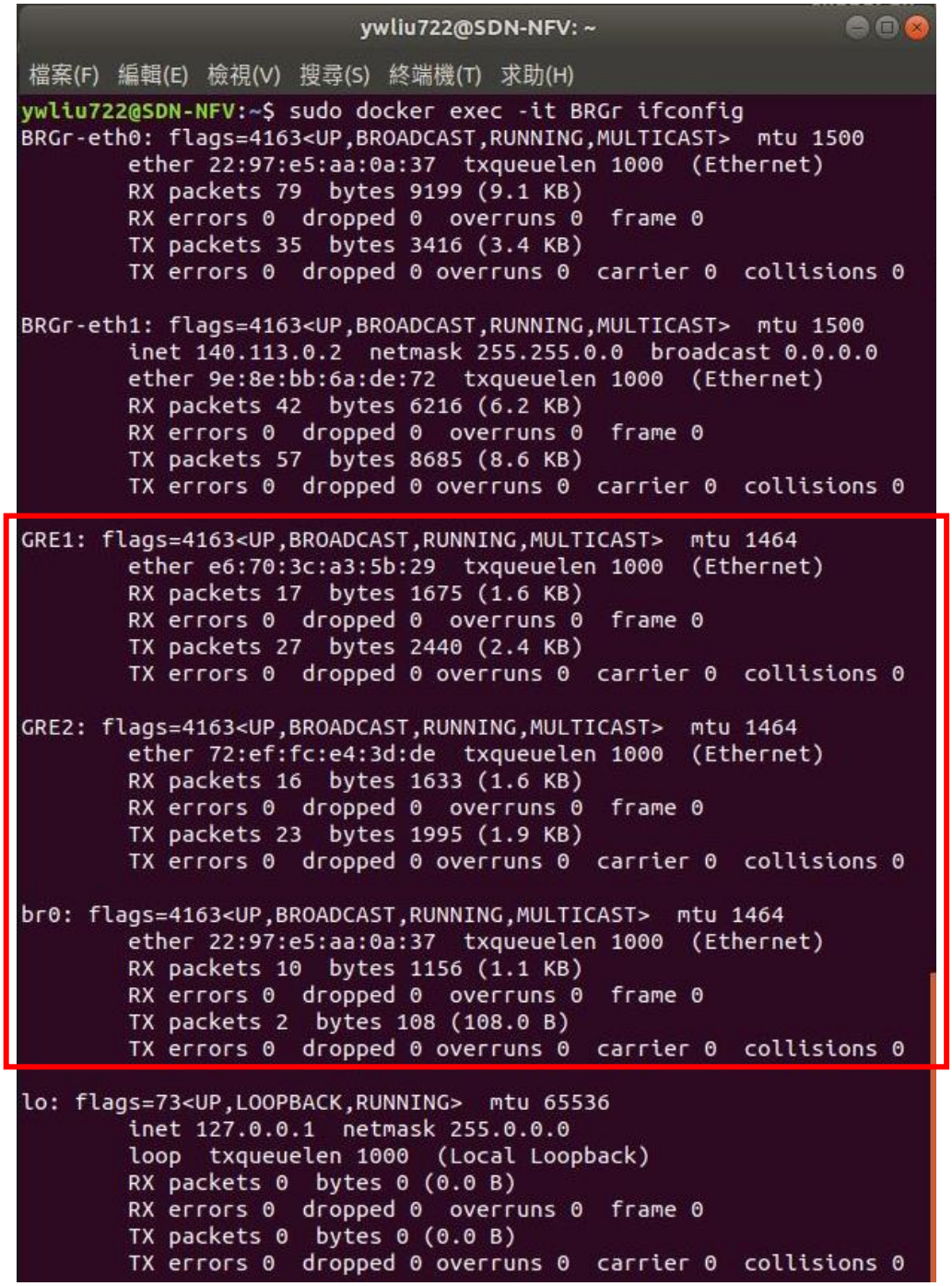


➔ 將來自 20.0.0.0/8 網段的所有封包做 NAT translate，轉換之目標 IP 則是由 iptables 從介面當中選擇適合之目標 IP，以將封包送往 VM 外。

2. Show interfaces list on node BRGr and BRG1, 2 (10%)



- 上方左圖爲 BRG1 的介面列表、右圖爲 BRG2 的介面列表。可以從上方的紅框得知，BRG1 以及 BRG2 皆透過 edge router 上的 DHCP server 取得 IP 位置，也透過指令建立起和 BRGr 間的 GRETAP 通道介面，其中 br0 爲 GRE 和 LAN port 間做爲橋接用途之裝置，若無此裝置則在 GRE Tunnel 建立後 無法順利傳輸。



- 此圖爲 BRGr 的介面列表。其中 BRGr-eth0 以及 BRGr-eth1 爲 container 間互相連接的裝置在 auto creation 的程式中不會修改此二介面。GRE1 以及 GRE2 則是透過 auto creation 程式過濾 foo over udp 封包後建立而成，此二介面分別和 BRG1 以及 BRG2 建立 GRE Tunnel 所有來自此二 host 的封包皆會由此進入。br0 則是將 GRE1 以及 GRE2 和 BRGr-eth0 間做爲橋接用途之裝置，若無此裝置則在 GRE Tunnel 建立後無法順利傳輸。最後 lo 則爲 loopback interface 此一介面爲 localhost 所使用，在這次 Lab 當中不會使用。

3. Capture packets and take screenshots on node (10%)
   ■ BRG1 input/output

```
ywliu722@SDN-NFV:~$ docker exec -it BRG1 tcpdump -i BRG1-eth0 -XX -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on BRG1-eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
07:44:25.189938 IP 20.0.0.17 > 8.8.8.8: ICMP echo request, id 68, seq 1, length
64
        0x0000:  ca0e 348b aa33 1695 f8e6 e1ad 0800 4500  ..4..3........E.
        0x0010:  0054 b4d3 4000 4001 61b5 1400 0011 0808  .T..@.@.a.......
        0x0020:  0808 0800 8bd5 0044 0001 59cc 8360 0000  .......D..Y..`..
        0x0030:  0000 cde5 0200 0000 0000 1011 1213 1415  ................
        0x0040:  1617 1819 1a1b 1c1d 1e1f 2021 2223 2425  ..........!"#$%
        0x0050:  2627 2829 2a2b 2c2d 2e2f 3031 3233 3435  &'()*+,-./012345
        0x0060:  3637                                     67
```

```
ywliu722@SDN-NFV:~$ docker exec -it BRG1 tcpdump -i BRG1-eth1 -XX -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on BRG1-eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
07:44:25.189966 IP 172.27.140.236.11111 > 140.113.0.2.33333: UDP, length 106
        0x0000:  0acf 2b98 bde3 866b 417a 78e3 0800 4500  ..+....kAzx...E.
        0x0010:  0086 0576 4000 4011 6f76 ac1b 8cec 8c71  ...v@.@.ov.....q
        0x0020:  0002 2b67 8235 0072 0000 2000 6558 0000  ..+g.5.r....eX..
        0x0030:  2b67 ca0e 348b aa33 1695 f8e6 e1ad 0800  +g..4..3........
        0x0040:  4500 0054 b4d3 4000 4001 61b5 1400 0011  E..T..@.@.a.....
        0x0050:  0808 0808 0800 8bd5 0044 0001 59cc 8360  .........D..Y..`
        0x0060:  0000 0000 cde5 0200 0000 0000 1011 1213  ................
        0x0070:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  ............!"#
        0x0080:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0090:  3435 3637                                4567
```

- 上方兩張圖分別爲 h1 發送 icmp request 後，於 BRG1-eth0(input)以及 BRG1-eth1(output)擷取到之封包。兩者最主要的差別爲輸出時爲了將 h1 的封包透過 GRE Tunnel 傳送至 GWr，故需要在封包前面加上 Outer MAC、Outer IP 以及 UDP header，相較於上次的 Lab4，除了爲了將兩個 LAN 模擬爲同一個 LAN 所以需要 GRE 封裝，這次也因爲途中會經過 NAT translate 所以需要 port 來進行 IP/port 轉換，故採用了 GRE over UDP 的技術來達到此效果。

```
07:44:25.203193 IP 140.113.0.2.33333 > 172.27.140.236.11111: UDP, length 106
        0x0000:  866b 417a 78e3 0acf 2b98 bde3 0800 4500  .kAzx...+.....E.
        0x0010:  0086 02fd 4000 7011 41ef 8c71 0002 ac1b  ....@.p.A..q....
        0x0020:  8cec 8235 2b67 0072 0000 2000 6558 0000  ...5+g.r....eX..
        0x0030:  2b67 1695 f8e6 e1ad ca0e 348b aa33 0800  +g........4..3..
        0x0040:  4500 0054 95ae 0000 7201 8eda 0808 0808  E..T....r.......
        0x0050:  1400 0011 0000 93d5 0044 0001 59cc 8360  .........D..Y..`
        0x0060:  0000 0000 cde5 0200 0000 0000 1011 1213  ................
        0x0070:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  ............!"#
        0x0080:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0090:  3435 3637                                4567
```

```
07:44:25.203211 IP 8.8.8.8 > 20.0.0.17: ICMP echo reply, id 68, seq 1, length 64
        0x0000:  1695 f8e6 e1ad ca0e 348b aa33 0800 4500  ........4..3..E.
        0x0010:  0054 95ae 0000 7201 8eda 0808 0808 1400  .T....r.........
        0x0020:  0011 0000 93d5 0044 0001 59cc 8360 0000  .......D..Y..`..
        0x0030:  0000 cde5 0200 0000 0000 1011 1213 1415  ................
        0x0040:  1617 1819 1a1b 1c1d 1e1f 2021 2223 2425  ..........!"#$%
        0x0050:  2627 2829 2a2b 2c2d 2e2f 3031 3233 3435  &'()*+,-./012345
        0x0060:  3637                                     67
```

- 上方兩張圖分別爲 Google DNS 發送 icmp reply 後，於 BRG1-eth1(input)以及 BRG1-eth0(output)擷取到之封包。兩者最大差別仍爲封包前方的 header，因爲 h1 並不知道 GRE Tunnel 的存在，故需要將封裝而另外加上的 header 移除後，方能將封包回傳給 h1。

■ Access Router(edge router) input/output

```
ywliu722@SDN-NFV:~$ docker exec -it edge tcpdump -i edge-eth1 -XX -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on edge-eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
07:44:25.189984 IP 172.27.140.236.11111 > 140.113.0.2.33333: UDP, length 106
        0x0000:  0acf 2b98 bde3 866b 417a 78e3 0800 4500  ..+....kAzx...E.
        0x0010:  0086 0576 4000 4011 6f76 ac1b 8cec 8c71  ...v@.@.ov.....q
        0x0020:  0002 2b67 8235 0072 0000 2000 6558 0000  ..+g.5.r....eX..
        0x0030:  2b67 ca0e 348b aa33 1695 f8e6 e1ad 0800  +g..4..3........
        0x0040:  4500 0054 b4d3 4000 4001 61b5 1400 0011  E..T..@.@.a.....
        0x0050:  0808 0808 0800 8bd5 0044 0001 59cc 8360  .........D..Y..`
        0x0060:  0000 0000 cde5 0200 0000 0000 1011 1213  ................
        0x0070:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  .............!"#
        0x0080:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0090:  3435 3637                                4567
```

```
ywliu722@SDN-NFV:~$ docker exec -it edge tcpdump -i edge-eth0 -XX -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on edge-eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
07:44:25.190001 IP 140.114.0.1.11111 > 140.113.0.2.33333: UDP, length 106
        0x0000:  0e9a 48a9 b3e7 82d9 2e26 0bb8 0800 4500  ..H......&....E.
        0x0010:  0086 0576 4000 3f11 1d0b 8c72 0001 8c71  ...v@.?....r...q
        0x0020:  0002 2b67 8235 0072 0000 2000 6558 0000  ..+g.5.r....eX..
        0x0030:  2b67 ca0e 348b aa33 1695 f8e6 e1ad 0800  +g..4..3........
        0x0040:  4500 0054 b4d3 4000 4001 61b5 1400 0011  E..T..@.@.a.....
        0x0050:  0808 0808 0800 8bd5 0044 0001 59cc 8360  .........D..Y..`
        0x0060:  0000 0000 cde5 0200 0000 0000 1011 1213  ................
        0x0070:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  .............!"#
        0x0080:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0090:  3435 3637                                4567
```

- 上方兩張圖分別爲 h1 發送 icmp request 後，於 edge-eth1(input)以及 edge-eth0(output)擷取到之封包。除了因裝置間傳送而有不同的 Ethernet header 之外，最主要還是因爲 edge router 爲了區隔內外網而有設置 NAT，所以由 BRG1 產生的 GRE 封裝封包之 Outer IP header 中的 source IP 以及 UDP header 中的 source port 會因爲 NAT 而有所改變(這邊 UDP port 沒改變是因爲沒有其他程式在使用此 port)。

```
07:44:25.203172 IP 140.113.0.2.33333 > 140.114.0.1.11111: UDP, length 106
        0x0000:  82d9 2e26 0bb8 0e9a 48a9 b3e7 0800 4500  ...&....H.....E.
        0x0010:  0086 02fd 4000 7111 ed83 8c71 0002 8c72  ....@.q....q...r
        0x0020:  0001 8235 2b67 0072 0000 2000 6558 0000  ...5+g.r....eX..
        0x0030:  2b67 1695 f8e6 e1ad ca0e 348b aa33 0800  +g........4..3..
        0x0040:  4500 0054 95ae 0000 7201 8eda 0808 0808  E..T....r.......
        0x0050:  1400 0011 0000 93d5 0044 0001 59cc 8360  .........D..Y..`
        0x0060:  0000 0000 cde5 0200 0000 0000 1011 1213  ................
        0x0070:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  .............!"#
        0x0080:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0090:  3435 3637                                4567
```

```
07:44:25.203181 IP 140.113.0.2.33333 > 172.27.140.236.11111: UDP, length 106
        0x0000:  866b 417a 78e3 0acf 2b98 bde3 0800 4500  .kAzx...+.....E.
        0x0010:  0086 02fd 4000 7011 41ef 8c71 0002 ac1b  ....@.p.A..q....
        0x0020:  8cec 8235 2b67 0072 0000 2000 6558 0000  ...5+g.r....eX..
        0x0030:  2b67 1695 f8e6 e1ad ca0e 348b aa33 0800  +g........4..3..
        0x0040:  4500 0054 95ae 0000 7201 8eda 0808 0808  E..T....r.......
        0x0050:  1400 0011 0000 93d5 0044 0001 59cc 8360  .........D..Y..`
        0x0060:  0000 0000 cde5 0200 0000 0000 1011 1213  ................
        0x0070:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  .............!"#
        0x0080:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0090:  3435 3637                                4567
```

- 上方兩張圖分別爲 Google DNS 發送 icmp reply 後，於 edge-eth0(input)以及 edge-eth1(output)擷取到之封包。兩者最大差別程式因爲 NAT 所造成的 destination IP/port translate，因爲內網的裝置並不會知道 edge router 的 WAN IP，且收進來之封包若沒有經過 NAT translate 會找不到對應的目的地，故需要做此改變。

■ BRGr input/output

```
ywliu722@SDN-NFV:~$ docker exec -it BRGr tcpdump -i BRGr-eth1 -XX -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on BRGr-eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
07:44:25.190011 IP 140.114.0.1.11111 > 140.113.0.2.33333: UDP, length 106
        0x0000:  9e8e bb6a de72 de65 5576 81c9 0800 4500  ...j.r.eUv....E.
        0x0010:  0086 0576 4000 3e11 1e0b 8c72 0001 8c71  ...v@.>....r...q
        0x0020:  0002 2b67 8235 0072 0000 2000 6558 0000  ..+g.5.r....eX..
        0x0030:  2b67 ca0e 348b aa33 1695 f8e6 e1ad 0800  +g..4..3........
        0x0040:  4500 0054 b4d3 4000 4001 61b5 1400 0011  E..T..@.@.a.....
        0x0050:  0808 0808 0800 8bd5 0044 0001 59cc 8360  .........D..Y..`
        0x0060:  0000 0000 cde5 0200 0000 0000 1011 1213  ................
        0x0070:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  .............!"#
        0x0080:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0090:  3435 3637                                4567
```

```
ywliu722@SDN-NFV:~$ docker exec -it BRGr tcpdump -i BRGr-eth0 -XX -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on BRGr-eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
07:44:25.190035 IP 20.0.0.17 > 8.8.8.8: ICMP echo request, id 68, seq 1, length
64
        0x0000:  ca0e 348b aa33 1695 f8e6 e1ad 0800 4500  ..4..3........E.
        0x0010:  0054 b4d3 4000 4001 61b5 1400 0011 0808  .T..@.@.a.......
        0x0020:  0808 0800 8bd5 0044 0001 59cc 8360 0000  .......D..Y..`..
        0x0030:  0000 cde5 0200 0000 0000 1011 1213 1415  ................
        0x0040:  1617 1819 1a1b 1c1d 1e1f 2021 2223 2425  ...........!"#$%
        0x0050:  2627 2829 2a2b 2c2d 2e2f 3031 3233 3435  &'()*+,-./012345
        0x0060:  3637                                     67
```

- 上方兩張圖分別爲 h1 發送 icmp request 後，於 BRGr-eth1(input)以及 BRGr-eth0(output)擷取到之封包。兩者最大差別爲封包前方的 header，因爲 GWr 並不知道 GRE Tunnel 的存在，故需要將封裝而另外加上的 header 移除後，方能將封包傳給 GWr 並傳至 VM 外。

```
07:44:25.203133 IP 8.8.8.8 > 20.0.0.17: ICMP echo reply, id 68, seq 1, length 64
        0x0000:  1695 f8e6 e1ad ca0e 348b aa33 0800 4500  ........4..3..E.
        0x0010:  0054 95ae 0000 7201 8eda 0808 0808 1400  .T....r.........
        0x0020:  0011 0000 93d5 0044 0001 59cc 8360 0000  .......D..Y..`..
        0x0030:  0000 cde5 0200 0000 0000 1011 1213 1415  ................
        0x0040:  1617 1819 1a1b 1c1d 1e1f 2021 2223 2425  ...........!"#$%
        0x0050:  2627 2829 2a2b 2c2d 2e2f 3031 3233 3435  &'()*+,-./012345
        0x0060:  3637                                     67
```

```
07:44:25.203181 IP 140.113.0.2.33333 > 172.27.140.236.11111: UDP, length 106
        0x0000:  866b 417a 78e3 0acf 2b98 bde3 0800 4500  .kAzx...+.....E.
        0x0010:  0086 02fd 4000 7011 41ef 8c71 0002 ac1b  ....@.p.A..q....
        0x0020:  8cec 8235 2b67 0072 0000 2000 6558 0000  ...5+g.r....eX..
        0x0030:  2b67 1695 f8e6 e1ad ca0e 348b aa33 0800  +g........4..3..
        0x0040:  4500 0054 95ae 0000 7201 8eda 0808 0808  E..T....r.......
        0x0050:  1400 0011 0000 93d5 0044 0001 59cc 8360  .........D..Y..`
        0x0060:  0000 0000 cde5 0200 0000 0000 1011 1213  ................
        0x0070:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  .............!"#
        0x0080:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0090:  3435 3637                                4567
```

- 上方兩張圖分別爲 Google DNS 發送 icmp reply 後，於 BRGr-eth0(input)以及 BRGr-eth1(output)擷取到之封包。兩者最主要的差別仍爲輸出時爲了將來自 GWr 的封包透過 GRE Tunnel 傳送至 h1，故需要在封包前面加上 Outer MAC、Outer IP 以及 UDP header，相較於上次的 Lab4，除了爲了將兩個 LAN 模擬爲同一個 LAN 所以需要 GRE 封裝，這次也因爲途中會經過 NAT translate 所以需要 port 來進行 IP/port 轉換，故採用了 GRE over UDP 的技術來達到此效果。

■ GWr input/output

```
ywliu722@SDN-NFV:~$ sudo tcpdump -i veth -XX -n
[sudo] password for ywliu722:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on veth, link-type EN10MB (Ethernet), capture size 262144 bytes
15:44:25.190040 IP 20.0.0.17 > 8.8.8.8: ICMP echo request, id 68, seq 1, length
64
        0x0000:  ca0e 348b aa33 1695 f8e6 e1ad 0800 4500  ..4..3........E.
        0x0010:  0054 b4d3 4000 4001 61b5 1400 0011 0808  .T..@.@.a.......
        0x0020:  0808 0800 8bd5 0044 0001 59cc 8360 0000  .......D..Y..`..
        0x0030:  0000 cde5 0200 0000 0000 1011 1213 1415  ................
        0x0040:  1617 1819 1a1b 1c1d 1e1f 2021 2223 2425  ..........!"#$%
        0x0050:  2627 2829 2a2b 2c2d 2e2f 3031 3233 3435  &'()*+,-./012345
        0x0060:  3637                                     67
```

```
ywliu722@SDN-NFV:~$ sudo tcpdump -i enp0s3 -XX -n
[sudo] password for ywliu722:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
15:44:25.190055 IP 10.0.2.15 > 8.8.8.8: ICMP echo request, id 68, seq 1, length
64
        0x0000:  5254 0012 3502 0800 27bb 0abc 0800 4500  RT..5...'.....E.
        0x0010:  0054 b4d3 4000 3f01 6ab7 0a00 020f 0808  .T..@.?.j.......
        0x0020:  0808 0800 8bd5 0044 0001 59cc 8360 0000  .......D..Y..`..
        0x0030:  0000 cde5 0200 0000 0000 1011 1213 1415  ................
        0x0040:  1617 1819 1a1b 1c1d 1e1f 2021 2223 2425  ..........!"#$%
        0x0050:  2627 2829 2a2b 2c2d 2e2f 3031 3233 3435  &'()*+,-./012345
        0x0060:  3637                                     67
```

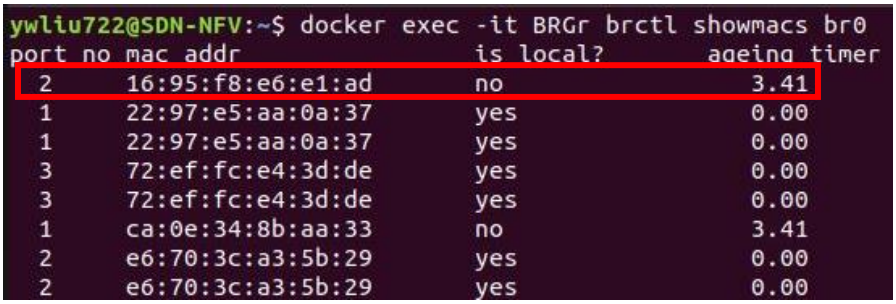
- 上方兩張圖分別爲 h1 發送 icmp request 後，於 veth(input)以及 enp0s3(output)擷取到之封包。除了因裝置間傳送而有不同的 Ethernet header 之外，最主要還是因爲 GWr 爲了區隔實驗環境以及 VM 而有設置 NAT，將 source IP 轉換爲 VM 對外網卡的 IP，使得封包可以透過該網卡傳輸至外網。

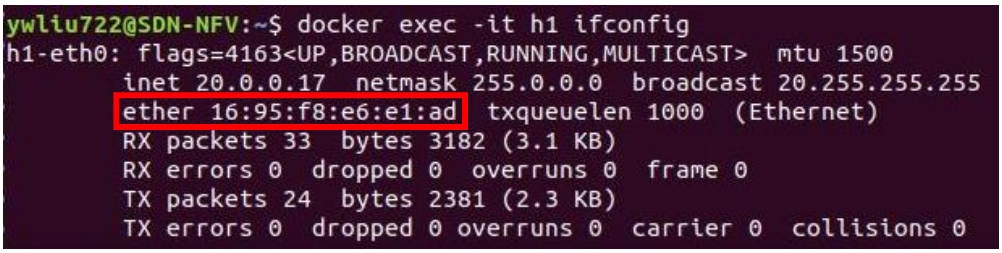
```
15:44:25.203102 IP 8.8.8.8 > 10.0.2.15: ICMP echo reply, id 68, seq 1, length 64
        0x0000:  0800 27bb 0abc 5254 0012 3502 0800 4500  ..'...RT..5...E.
        0x0010:  0054 95ae 0000 7301 95dc 0808 0808 0a00  .T....s.........
        0x0020:  020f 0000 93d5 0044 0001 59cc 8360 0000  .......D..Y..`..
        0x0030:  0000 cde5 0200 0000 0000 1011 1213 1415  ................
        0x0040:  1617 1819 1a1b 1c1d 1e1f 2021 2223 2425  ..........!"#$%
        0x0050:  2627 2829 2a2b 2c2d 2e2f 3031 3233 3435  &'()*+,-./012345
        0x0060:  3637                                     67
```

```
15:44:25.203129 IP 8.8.8.8 > 20.0.0.17: ICMP echo reply, id 68, seq 1, length 64
        0x0000:  1695 f8e6 e1ad ca0e 348b aa33 0800 4500  ........4..3..E.
        0x0010:  0054 95ae 0000 7201 8eda 0808 0808 1400  .T....r.........
        0x0020:  0011 0000 93d5 0044 0001 59cc 8360 0000  .......D..Y..`..
        0x0030:  0000 cde5 0200 0000 0000 1011 1213 1415  ................
        0x0040:  1617 1819 1a1b 1c1d 1e1f 2021 2223 2425  ..........!"#$%
        0x0050:  2627 2829 2a2b 2c2d 2e2f 3031 3233 3435  &'()*+,-./012345
        0x0060:  3637                                     67
```

- 上方兩張圖分別爲 Google DNS 發送 icmp reply 後，於 enp0s3(input)以及 veth (output)擷取到之封包。兩者最大差別程式因爲 NAT 所造成的 destination IP translate，因爲實驗環境內的裝置並不會知道 GWr 的 WAN IP，且收進來之封包若沒有經過 NAT translate 會找不到對應的目的地，故需要做此改變。

4. BRGr will receive ping responses from Google DNS. Briefly describe how BRGr determines the GRE interface to tunnel the response packets back to BRG1. (10%)





- 上圖爲 BRGr 執行 brctl showmacs br0 指令後得到之 MAC Learning Address Table、下圖爲 h1 上 h1-eth0 的網卡資訊。由上二圖可以得知 h1-eth0 的 MAC address 出現在 table 上，也對應著特定的 port，其他的 MAC address 也各自對應著不同的 port，由此可知 kernel 是透過 MAC learning 決定封包的路徑。