NSCap Lab Report

Project1

1. Show the configuration commands you made on each node to provide Internet connectivity for hosts and briefly explain the purpose of the commands.

- BRG1

```
ip fou add port 33333 ipproto 47
ip link add GRE type gretap remote 140.113.0.2 local 172.27.0.5 key 0 encap fou enca

ip link set GRE up
ip link add br0 type bridge
brctl addif br0 bh1upveth
brctl addif br0 GRE
ip link set br0 up
```

- BRG2

```
ip fou add port 33333 ipproto 47
ip link add GRE2 type gretap remote 140.113.0.2 local 172.27.0.6 key 1 encap fou enc

ip link set GRE2 up
ip link add br0 type bridge
brctl addif br0 bh2upveth
brctl addif br0 GRE2
ip link set br0 up
```

- BRGR

```
ip addr add 140.113.0.2/24 dev mbrightveth
ip addr add 20.0.0.2/8 dev brvmupveth
ip fou add port 55555 ipproto 47

# auto tunnel creation flow
echo "include /usr/local/lib/" >> /etc/ld.so.conf
cd /root/libpcap/
./configure
make
make install
cd ../
g++ /root/0616078.cpp -lpcap

ip link add br0 type bridge
brctl addif br0 brvmupveth
```

- The above configs are to add ip address to brg1, brg2, brgr, and to specify the gre tunnel interface they are going to use. I use 33333 port for brg1 and brg2 to send and receive the gre over udp packet, and 55555 port for brgr. The `brctl` command adds a bridge in brg1, brg2, brgr to bind the gretap interface with the bridge.

- Edge

```
# This is edge config
# dhcp
ip addr add 172.27.0.1/24 dev eupveth
ip addr add 140.114.0.1/24 dev emleftveth
touch /var/lib/dhcp/dhcpd.leases
/usr/sbin/dhcpd -4 -pf /run/dhcp-server-dhcpd.pid -cf /root/edge-dhcpd.conf eupveth

# NAT
iptables -t nat -A POSTROUTING -s 172.27.0.0/24 -o emleftveth -j MASQUERADE

# Routing
route add -net 140.113.0.0/24 gw 140.114.0.2
```

```
# This is edge dhcpd.conf
subnet 172.27.0.0 netmask 255.255.255.0 {
    range 172.27.0.5 172.27.0.100;
    option routers 172.27.0.1;
    option subnet-mask 255.255.255.0;
}
```

- Edge NAT table
  - ```
    root@f7e988e83a83:/# iptables -t nat -L
    Chain PREROUTING (policy ACCEPT)
    target     prot opt source               destination

    Chain INPUT (policy ACCEPT)
    target     prot opt source               destination

    Chain OUTPUT (policy ACCEPT)
    target     prot opt source               destination

    Chain POSTROUTING (policy ACCEPT)
    target     prot opt source               destination
    MASQUERADE  all  --  172.27.0.0/24        anywhere
    ```

- The above config specify the dhcpd.conf used in edge and the init config for edge. The init config will setup the ip addr, NAT rule, and Routing rule.

- GWr

```
# This is the command for GWr(namely the Ubuntu VM)
iptables -t nat -A POSTROUTING -s 20.0.0.0/8 -o ens33 -j MASQUERADE

/usr/sbin/dhcpd -4 -pf /run/dhcp-server-dhcpd.pid -cf ./gwr-dhcpd.conf brvmdownveth
```
```

```
# This is the gwr dhcpd.conf
subnet 20.0.0.0 netmask 255.0.0.0 {
    range 20.0.0.10 20.0.0.100;
    option routers 20.0.0.1;
    option subnet-mask 255.0.0.0;
    option domain-name-servers 8.8.8.8;
}
```

- GWr NAT table
  - ```
    # tommytyc @ ubuntu in ~/NSCap/project1 on git:main x [13:19:19]
    $ sudo iptables -t nat -L
    [sudo] password for tommytyc:
    Chain PREROUTING (policy ACCEPT)
    target     prot opt source               destination
    DOCKER     all  --  anywhere             anywhere             ADDRTYPE match dst-type LOCAL

    Chain INPUT (policy ACCEPT)
    target     prot opt source               destination

    Chain OUTPUT (policy ACCEPT)
    target     prot opt source               destination
    DOCKER     all  --  anywhere            !localhost/8          ADDRTYPE match dst-type LOCAL

    Chain POSTROUTING (policy ACCEPT)
    target     prot opt source               destination
    MASQUERADE  all  --  172.17.0.0/16        anywhere
    MASQUERADE  all  --  20.0.0.0/8           anywhere

    Chain DOCKER (2 references)
    target     prot opt source               destination
    RETURN     all  --  anywhere             anywhere
    ```
- The above command and dhcp config are for gwr. The command will setup the nat rule and dhcp by my gwr-dhcpd.conf.

2. Show interfaces list on node BRGr, BRG1, BRG2.
   - BRGr
     - ```
       root@9cc8d036e7ae:/# ip addr
       1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
           link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
           inet 127.0.0.1/8 scope host lo
              valid_lft forever preferred_lft forever
       2: br0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1450 qdisc noqueue state UP group default qlen 1000
           link/ether 0e:9d:b2:ec:87:6c brd ff:ff:ff:ff:ff:ff
       3: gre0@NONE: <NOARP> mtu 1452 qdisc noop state DOWN group default qlen 1000
           link/gre 0.0.0.0 brd 0.0.0.0
       4: gretap0@NONE: <BROADCAST,MULTICAST> mtu 1462 qdisc noop state DOWN group default qlen 1000
           link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
       5: erspan0@NONE: <BROADCAST,MULTICAST> mtu 1450 qdisc noop state DOWN group default qlen 1000
           link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
       6: GRE0@NONE: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1450 qdisc fq_codel master br0 state UNKNOWN group default qlen 1000
           link/ether 0e:9d:b2:ec:87:6c brd ff:ff:ff:ff:ff:ff
       7: GRE1@NONE: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1450 qdisc fq_codel master br0 state UNKNOWN group default qlen 1000
           link/ether ae:4a:e8:ca:7c:7b brd ff:ff:ff:ff:ff:ff
       11: mbrightveth@if12: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
           link/ether da:68:6c:69:7a:21 brd ff:ff:ff:ff:ff:ff link-netnsid 0
           inet 140.113.0.2/24 scope global mbrightveth
              valid_lft forever preferred_lft forever
       14: brvmupveth@if13: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master br0 state UP group default qlen 1000
           link/ether 6a:5a:ce:b5:9f:b8 brd ff:ff:ff:ff:ff:ff link-netnsid 1
           inet 20.0.0.2/8 scope global brvmupveth
              valid_lft forever preferred_lft forever
       ```
   - BGR1

```
root@6b26c7b3a7c7:/# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: gre0@NONE: <NOARP> mtu 1452 qdisc noop state DOWN group default qlen 1000
    link/gre 0.0.0.0 brd 0.0.0.0
3: gretap0@NONE: <BROADCAST,MULTICAST> mtu 1462 qdisc noop state DOWN group default qlen 1000
    link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
4: erspan0@NONE: <BROADCAST,MULTICAST> mtu 1450 qdisc noop state DOWN group default qlen 1000
    link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
5: bh1upveth@if6: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master br0 state UP group default qlen 1000
    link/ether 32:cf:2b:1a:db:95 brd ff:ff:ff:ff:ff:ff link-netnsid 0
6: GRE@NONE: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1450 qdisc fq_codel master br0 state UNKNOWN group default qlen 1000
    link/ether 2e:89:4d:ce:db:bf brd ff:ff:ff:ff:ff:ff
7: br0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1450 qdisc noqueue state UP group default qlen 1000
    link/ether 2e:89:4d:ce:db:bf brd ff:ff:ff:ff:ff:ff
16: 1downveth@if15: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 32:82:f8:65:0a:97 brd ff:ff:ff:ff:ff:ff link-netnsid 1
    inet 172.27.0.5/24 brd 172.27.0.255 scope global 1downveth
       valid_lft forever preferred_lft forever
```

- BRG2

```
root@f628c974180a:/# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: gre0@NONE: <NOARP> mtu 1452 qdisc noop state DOWN group default qlen 1000
    link/gre 0.0.0.0 brd 0.0.0.0
3: gretap0@NONE: <BROADCAST,MULTICAST> mtu 1462 qdisc noop state DOWN group default qlen 1000
    link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
4: erspan0@NONE: <BROADCAST,MULTICAST> mtu 1450 qdisc noop state DOWN group default qlen 1000
    link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
5: GRE2@NONE: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1450 qdisc fq_codel master br0 state UNKNOWN group default qlen 1000
    link/ether 12:e0:90:69:9a:fd brd ff:ff:ff:ff:ff:ff
6: br0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1450 qdisc noqueue state UP group default qlen 1000
    link/ether 12:e0:90:69:9a:fd brd ff:ff:ff:ff:ff:ff
7: bh2upveth@if8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master br0 state UP group default qlen 1000
    link/ether 7a:7f:f4:21:70:3c brd ff:ff:ff:ff:ff:ff link-netnsid 0
18: 2downveth@if17: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 42:93:7b:0c:b8:06 brd ff:ff:ff:ff:ff:ff link-netnsid 1
    inet 172.27.0.6/24 brd 172.27.0.255 scope global 2downveth
       valid_lft forever preferred_lft forever
```

- We can see that BRGr and BRG1, BRG2 have successfully built GRE tunnel between them.

3. Capture packets and take screenshots on node.
   - BRG1
     - in

```
root@6b26c7b3a7c7:/# tcpdump -i bh1upveth
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on bh1upveth, link-type EN10MB (Ethernet), capture size 262144 bytes
06:46:38.548347 IP 20.0.0.10 > 8.8.8.8: ICMP echo request, id 101, seq 1, length 64
06:46:38.554398 IP 8.8.8.8 > 20.0.0.10: ICMP echo reply, id 101, seq 1, length 64
06:46:39.549786 IP 20.0.0.10 > 8.8.8.8: ICMP echo request, id 101, seq 2, length 64
06:46:39.554508 IP 8.8.8.8 > 20.0.0.10: ICMP echo reply, id 101, seq 2, length 64
06:46:40.551976 IP 20.0.0.10 > 8.8.8.8: ICMP echo request, id 101, seq 3, length 64
06:46:40.558158 IP 8.8.8.8 > 20.0.0.10: ICMP echo reply, id 101, seq 3, length 64
06:46:41.553532 IP 20.0.0.10 > 8.8.8.8: ICMP echo request, id 101, seq 4, length 64
06:46:58.745119 IP 20.0.0.10 > 8.8.8.8: ICMP echo request, id 102, seq 5, length 64
06:46:58.757469 IP 8.8.8.8 > 20.0.0.10: ICMP echo reply, id 102, seq 5, length 64
06:46:59.747690 IP 20.0.0.10 > 8.8.8.8: ICMP echo request, id 102, seq 6, length 64
06:46:59.754416 IP 8.8.8.8 > 20.0.0.10: ICMP echo reply, id 102, seq 6, length 64
06:47:00.749629 IP 20.0.0.10 > 8.8.8.8: ICMP echo request, id 102, seq 7, length 64
06:47:00.756694 IP 8.8.8.8 > 20.0.0.10: ICMP echo reply, id 102, seq 7, length 64
^C
13 packets captured
26 packets received by filter
13 packets dropped by kernel
```

     - out

```
root@6b26c7b3a7c7:/# tcpdump -i 1downveth
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on 1downveth, link-type EN10MB (Ethernet), capture size 262144 bytes
06:50:01.050553 IP 172.27.0.5.33333 > 140.113.0.2.55555: UDP, length 106
^C
```

     - The original packet sent to google is from h1(20.0.0.10), and it is changed into the ip(which is 172.27.0.5, port 33333) brg1 got from edge dhcp after sent by brg1. That means the packet is in the GRE tunnel now.

- Access Router
  - in
    - ```
      root@13f5b865f013:/# tcpdump -i emrightveth
      tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
      listening on emrightveth, link-type EN10MB (Ethernet), capture size 262144 bytes
      06:52:18.314846 IP 140.114.0.1.33333 > 140.113.0.2.55555: UDP, length 106
      06:52:18.322675 IP 140.113.0.2.55555 > 140.114.0.1.33333: UDP, length 106
      06:52:19.316809 IP 140.114.0.1.33333 > 140.113.0.2.55555: UDP, length 106
      06:52:19.323878 IP 140.113.0.2.55555 > 140.114.0.1.33333: UDP, length 106
      06:52:20.318595 IP 140.114.0.1.33333 > 140.113.0.2.55555: UDP, length 106
      06:52:20.325897 IP 140.113.0.2.55555 > 140.114.0.1.33333: UDP, length 106
      ^C
      6 packets captured
      6 packets received by filter
      0 packets dropped by kernel
      ```
  - out
    - ```
      root@13f5b865f013:/# tcpdump -i mbleftveth
      tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
      listening on mbleftveth, link-type EN10MB (Ethernet), capture size 262144 bytes
      06:59:19.278092 IP 140.114.0.1.33333 > 140.113.0.2.55555: UDP, length 106
      06:59:19.286757 IP 140.113.0.2.55555 > 140.114.0.1.33333: UDP, length 106
      06:59:20.279341 IP 140.114.0.1.33333 > 140.113.0.2.55555: UDP, length 106
      06:59:20.285351 IP 140.113.0.2.55555 > 140.114.0.1.33333: UDP, length 106
      06:59:21.281885 IP 140.114.0.1.33333 > 140.113.0.2.55555: UDP, length 106
      06:59:21.286289 IP 140.113.0.2.55555 > 140.114.0.1.33333: UDP, length 106
      ^C
      6 packets captured
      6 packets received by filter
      0 packets dropped by kernel
      ```
  - The packet is totally in the GRE tunnel now(we can only see that the packet is for 140.114.0.1 port 33333, because it is transformed by the NAT on Edge Router, and 140.113.0.2 port 55555, and we can not see the original packet is for the ICMP pinging between h1 and google).
- BRGr
  - in
    - ```
      root@9cc8d036e7ae:/# tcpdump -i mbrightveth
      tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
      listening on mbrightveth, link-type EN10MB (Ethernet), capture size 262144 bytes
      07:00:47.469191 IP 140.114.0.1.33333 > 140.113.0.2.55555: UDP, length 106
      07:00:47.475249 IP 140.113.0.2.55555 > 140.114.0.1.33333: UDP, length 106
      07:00:47.493351 IP 140.114.0.1.33333 > 140.113.0.2.55555: UDP, length 50
      07:00:47.493429 IP 140.113.0.2.55555 > 140.114.0.1.33333: UDP, length 50
      07:00:48.471883 IP 140.114.0.1.33333 > 140.113.0.2.55555: UDP, length 106
      07:00:48.477929 IP 140.113.0.2.55555 > 140.114.0.1.33333: UDP, length 106
      ^C
      6 packets captured
      6 packets received by filter
      0 packets dropped by kernel
      ```
  - out
    - ```
      root@9cc8d036e7ae:/# tcpdump -i brvmupveth
      tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
      listening on brvmupveth, link-type EN10MB (Ethernet), capture size 262144 bytes
      07:01:58.648513 IP 20.0.0.10 > 8.8.8.8: ICMP echo request, id 105, seq 580, length 64
      07:01:58.653838 IP 8.8.8.8 > 20.0.0.10: ICMP echo reply, id 105, seq 580, length 64
      07:01:59.650931 IP 20.0.0.10 > 8.8.8.8: ICMP echo request, id 105, seq 581, length 64
      07:01:59.656242 IP 8.8.8.8 > 20.0.0.10: ICMP echo reply, id 105, seq 581, length 64
      ^C
      4 packets captured
      4 packets received by filter
      0 packets dropped by kernel
      ```
  - After the packet passes through BRGr, the tunnel will decap the GRE header and we can see that the original packet is ICMP pinging between h1 and google.
- GWr
  - in

- in

```
# tommytyc @ ubuntu in ~/NSCap/project1 on git:main x [15:05:12]
$ sudo tcpdump -i brvmdownveth
[sudo] password for tommytyc:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on brvmdownveth, link-type EN10MB (Ethernet), capture size 262144 bytes
15:05:34.133569 IP 20.0.0.10 > dns.google: ICMP echo request, id 105, seq 795, length 64
15:05:34.138036 IP dns.google > 20.0.0.10: ICMP echo reply, id 105, seq 795, length 64
15:05:35.136449 IP 20.0.0.10 > dns.google: ICMP echo request, id 105, seq 796, length 64
15:05:35.143276 IP dns.google > 20.0.0.10: ICMP echo reply, id 105, seq 796, length 64
15:05:36.137768 IP 20.0.0.10 > dns.google: ICMP echo request, id 105, seq 797, length 64
15:05:36.142615 IP dns.google > 20.0.0.10: ICMP echo reply, id 105, seq 797, length 64
^C
6 packets captured
6 packets received by filter
0 packets dropped by kernel
```

- out

```
# tommytyc @ ubuntu in ~/NSCap/project1 on git:main x [15:05:36]
$ sudo tcpdump -i ens33
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens33, link-type EN10MB (Ethernet), capture size 262144 bytes
15:06:35.275462 IP ubuntu > dns.google: ICMP echo request, id 105, seq 856, length 64
15:06:35.278644 IP ubuntu.42247 > _gateway.domain: 46699+ [1au] PTR? 8.8.8.8.in-addr.arpa. (49)
15:06:35.285991 IP _gateway.domain > ubuntu.42247: 46699 1/0/1 PTR dns.google. (73)
15:06:35.286791 IP dns.google > ubuntu: ICMP echo reply, id 105, seq 856, length 64
15:06:35.287009 IP ubuntu.56234 > _gateway.domain: 1995+ [1au] PTR? 128.22.168.192.in-addr.arpa. (56)
15:06:35.293596 IP _gateway.domain > ubuntu.56234: 1995 NXDomain 0/1/1 (115)
15:06:35.293777 IP ubuntu.56234 > _gateway.domain: 1995+ PTR? 128.22.168.192.in-addr.arpa. (45)
15:06:35.296792 IP _gateway.domain > ubuntu.56234: 1995 NXDomain 0/1/0 (104)
15:06:35.298501 IP ubuntu.39057 > _gateway.domain: 35814+ [1au] PTR? 2.22.168.192.in-addr.arpa. (54)
15:06:35.302323 IP _gateway.domain > ubuntu.39057: 35814 NXDomain 0/1/1 (113)
15:06:35.302501 IP ubuntu.39057 > _gateway.domain: 35814+ PTR? 2.22.168.192.in-addr.arpa. (43)
15:06:35.307276 IP _gateway.domain > ubuntu.39057: 35814 NXDomain 0/1/0 (102)
15:06:36.277297 IP ubuntu > dns.google: ICMP echo request, id 105, seq 857, length 64
15:06:36.284083 IP dns.google > ubuntu: ICMP echo reply, id 105, seq 857, length 64
^C
14 packets captured
14 packets received by filter
0 packets dropped by kernel
```

- After the packet is transformed by the NAT on GWr, it will be sent to google, and we can only see the packet is from `ubuntu` and not able to see the original IP address.

- The reverse direction(from google to h1) are quite similar with the above. The key idea of the packet forwarding in the topology is the GRE tunnel between BRG1 and BRGr, and the NAT on Edge and GWr, so we can see that the source ip address(with source udp port) and the destination ip address(with the destination udp port) keep changing while passing through different device.

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.

   - We have setup the **key** option while building up the GRE tunnel. I use key 0 for BRG1 and 1 for BRG2. So, when Google DNS sends ICMP response to h1, BRGr will use key 0 to send the packet, which is the tunnel between BRG1 and BRGr.