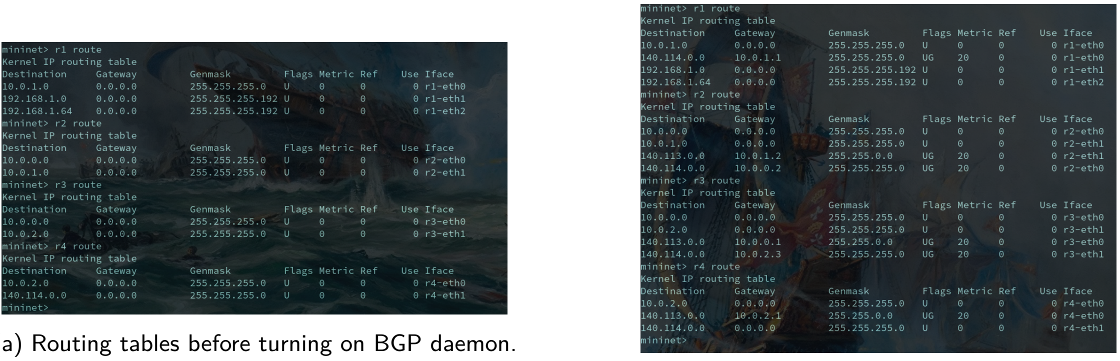
Networks Systems Capstone Lab 3 Report

Andrés Ponce 彭思安

March 28, 2021

1 Part 1

1.1 Take a screenshot of the routing tables before/after on [r1-r4].



```
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>
```

(a) Routing tables before turning on BGP daemon.

```
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        255.255.255.0   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        255.255.255.0   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        255.255.255.0   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>
```

(b) Routing tables after turning on the BGP daemon.

Figure 1: Routing tables of each router.

When the BGP daemon starts the routes will be added to the routing tables of each router.

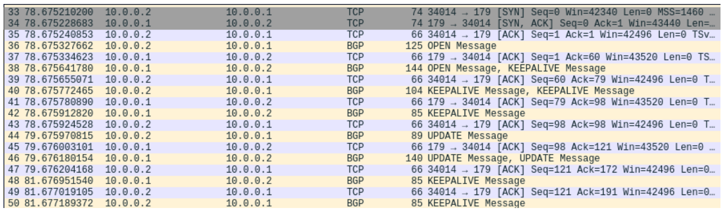
1.2 Telnet zebra and bgpd daemons of [r1-r4] and take screenshots of routes in zebra and bgpd daemons.

1.3 Capture BGP packets from wireshark and take screenshots to verify your answer to the following questions.

1.3.1 Show BGP packets exchanged by r2 and r3.

1.3.2 What will happen to the routing table if you set r4-eth0 down?

If we set r4 down, its address will be flushed from the other routers.



```
33 78.675210200  10.0.0.2       10.0.0.1       TCP     74 34014 → 179 [SYN] Seq=0 Win=42340 Len=0 MSS=1460 …
34 78.675228683  10.0.0.1       10.0.0.2       TCP     74 179 → 34014 [SYN, ACK] Seq=0 Ack=1 Win=43440 Len=…
35 78.675240853  10.0.0.2       10.0.0.1       TCP     66 34014 → 179 [ACK] Seq=1 Ack=1 Win=42496 Len=0 TSv…
36 78.675327662  10.0.0.2       10.0.0.1       BGP    125 OPEN Message
37 78.675334623  10.0.0.1       10.0.0.2       TCP     66 179 → 34014 [ACK] Seq=1 Ack=60 Win=43520 Len=0 TS…
38 78.675641780  10.0.0.1       10.0.0.2       BGP    144 OPEN Message, KEEPALIVE Message
39 78.675655071  10.0.0.2       10.0.0.1       TCP     66 34014 → 179 [ACK] Seq=60 Ack=79 Win=42496 Len=0 T…
40 78.675772465  10.0.0.2       10.0.0.1       BGP    104 KEEPALIVE Message, KEEPALIVE Message
41 78.675780890  10.0.0.1       10.0.0.2       TCP     66 179 → 34014 [ACK] Seq=79 Ack=98 Win=43520 Len=0 T…
42 78.675912820  10.0.0.1       10.0.0.2       BGP     85 KEEPALIVE Message
43 78.675924528  10.0.0.2       10.0.0.1       TCP     66 34014 → 179 [ACK] Seq=98 Ack=98 Win=42496 Len=0 T…
44 79.675970815  10.0.0.2       10.0.0.1       BGP     89 UPDATE Message
45 79.676003101  10.0.0.1       10.0.0.2       TCP     66 179 → 34014 [ACK] Seq=98 Ack=121 Win=43520 Len=0 …
46 79.676180154  10.0.0.1       10.0.0.2       BGP    140 UPDATE Message, UPDATE Message
47 79.676204168  10.0.0.2       10.0.0.1       TCP     66 34014 → 179 [ACK] Seq=121 Ack=172 Win=42496 Len=0…
48 81.676951540  10.0.0.1       10.0.0.2       BGP     85 KEEPALIVE Message
49 81.677019105  10.0.0.2       10.0.0.1       TCP     66 34014 → 179 [ACK] Seq=121 Ack=191 Win=42496 Len=0…
50 81.677189372  10.0.0.2       10.0.0.1       BGP     85 KEEPALIVE Message
```

Figure 2: OPEN, UPDATE, KEEPALIVE messages exchanged by r2 and r3.

1.3.3 How does r3 know that r4 is unreachable? Explain how.

As part of the BGP settings, we set the `timers connect 5` option for each neighbor. A timer counts from zero to the amount of seconds specifiied in the configuration file. If a Keepalive message is not received within that time, that peer information is flushed from the neighbor's routing table. This means that BGP will flush any neighbors who for some reason become inactive for a certain time. Since r3 fails to receive a Keepalive message form r4 when the timer reaches zero, r3 assumes that the neighbor is dead.

1.3.4 How does r2 know that r4 is unreachable? Explain how.

Now that r3 knows that r4 is inactive, it will broadcast that message around the network. When r2 receives information that r4 is inactive, it will also drop flush that route and advertise the message to the other routers.

2 Part 2

2.1 Explain the difference in packet headers.

Once the iptable rules have been set, the information in each packet that goes through the router will have its source or destination changed depending on the rule it matches. The DNAT rule will work whenever we want to access the HTTP server at the given port. Likewise for the SNAT will match any packet coming in from the given subnet, and then the router will change the source field to its own address.