Name: Dhanashree Reddy Srinivasa Reddy

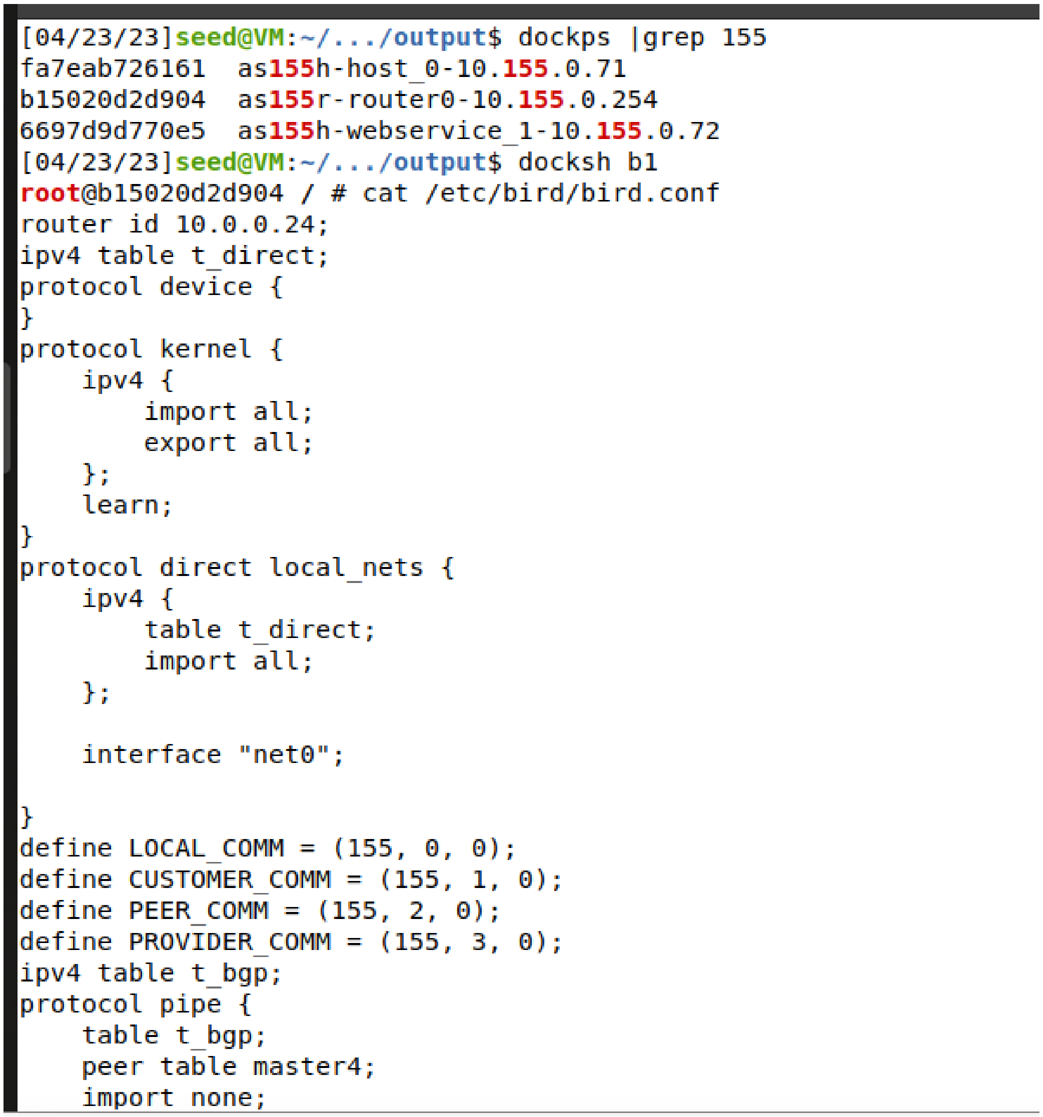
SUID: 393473169

Course: Internet Security

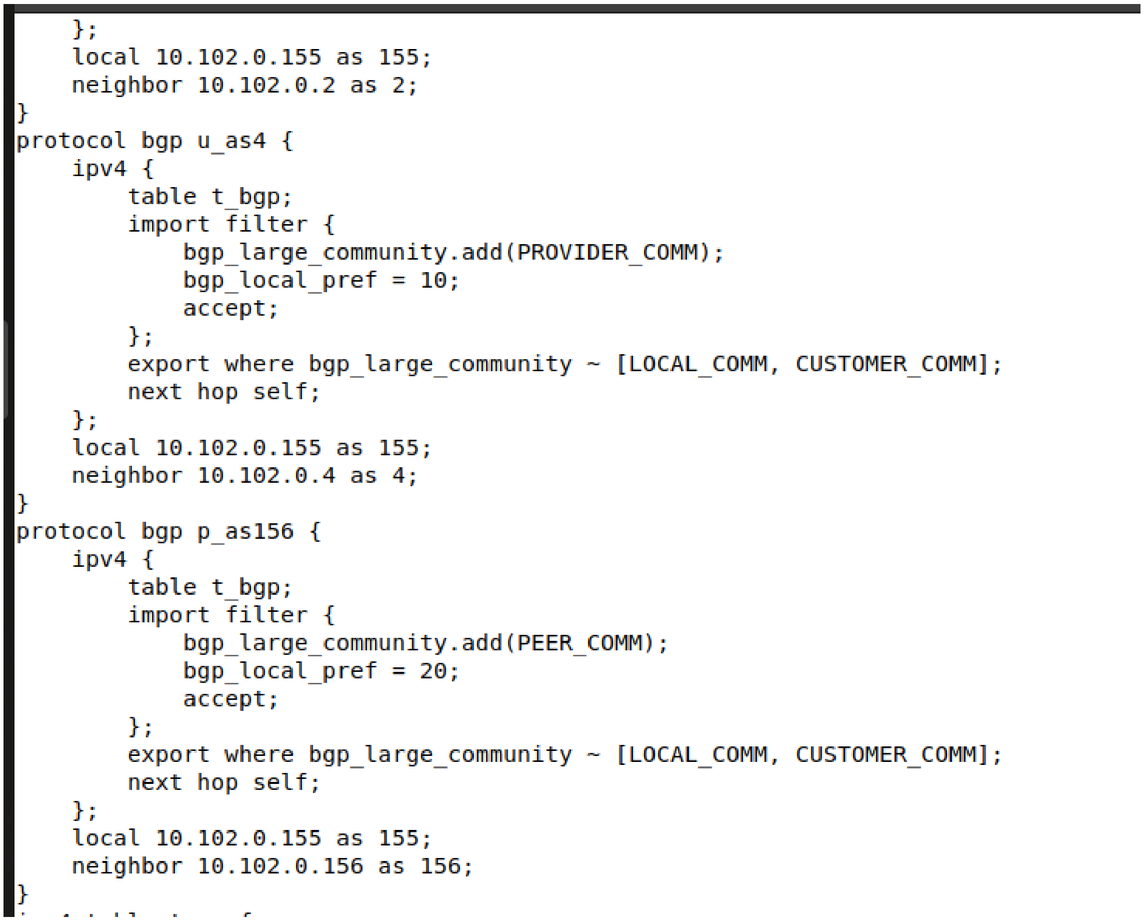
BGP Exploration and Attack Lab

3 Task 1: Stub Autonomous System

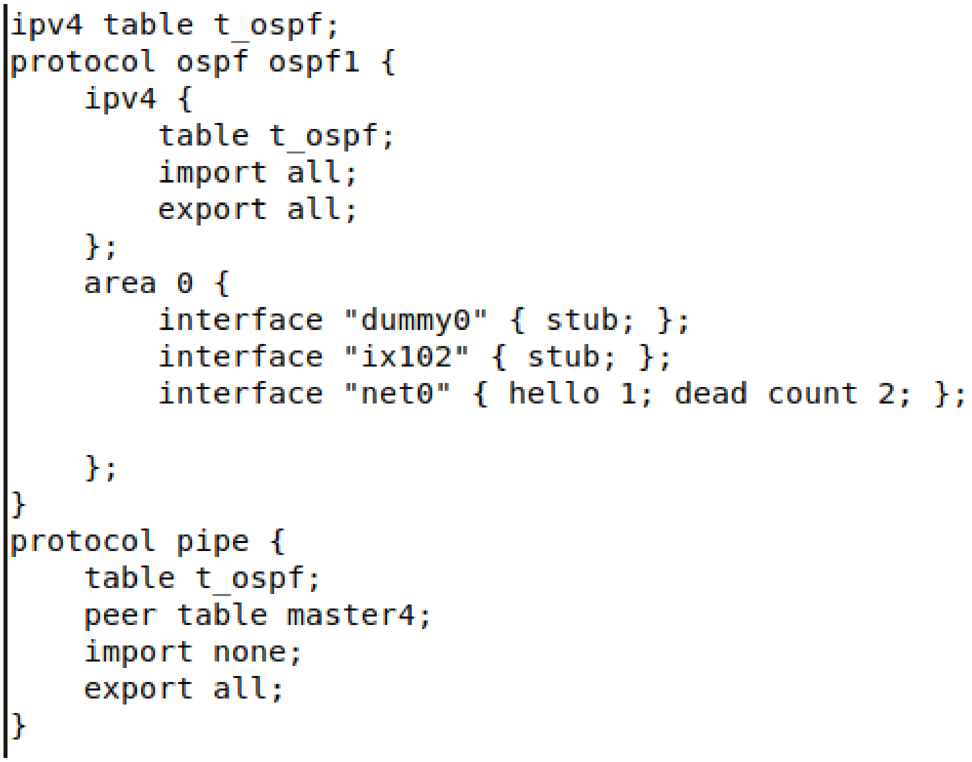
3.1Task 1.a: Understanding AS-155's BGP Configuration



```
[04/23/23]seed@VM:~/.../output$ dockps |grep 155
fa7eab726161  as155h-host_0-10.155.0.71
b15020d2d904  as155r-router0-10.155.0.254
6697d9d770e5  as155h-webservice_1-10.155.0.72
[04/23/23]seed@VM:~/.../output$ docksh b1
root@b15020d2d904 / # cat /etc/bird/bird.conf
router id 10.0.0.24;
ipv4 table t_direct;
protocol device {
}
protocol kernel {
    ipv4 {
        import all;
        export all;
    };
    learn;
}
protocol direct local_nets {
    ipv4 {
        table t_direct;
        import all;
    };

    interface "net0";

}
define LOCAL_COMM = (155, 0, 0);
define CUSTOMER_COMM = (155, 1, 0);
define PEER_COMM = (155, 2, 0);
define PROVIDER_COMM = (155, 3, 0);
ipv4 table t_bgp;
protocol pipe {
    table t_bgp;
    peer table master4;
    import none;
```



```
    };
    local 10.102.0.155 as 155;
    neighbor 10.102.0.2 as 2;
}
protocol bgp u_as4 {
    ipv4 {
        table t_bgp;
        import filter {
            bgp_large_community.add(PROVIDER_COMM);
            bgp_local_pref = 10;
            accept;
        };
        export where bgp_large_community ~ [LOCAL_COMM, CUSTOMER_COMM];
        next hop self;
    };
    local 10.102.0.155 as 155;
    neighbor 10.102.0.4 as 4;
}
protocol bgp p_as156 {
    ipv4 {
        table t_bgp;
        import filter {
            bgp_large_community.add(PEER_COMM);
            bgp_local_pref = 20;
            accept;
        };
        export where bgp_large_community ~ [LOCAL_COMM, CUSTOMER_COMM];
        next hop self;
    };
    local 10.102.0.155 as 155;
    neighbor 10.102.0.156 as 156;
}
```



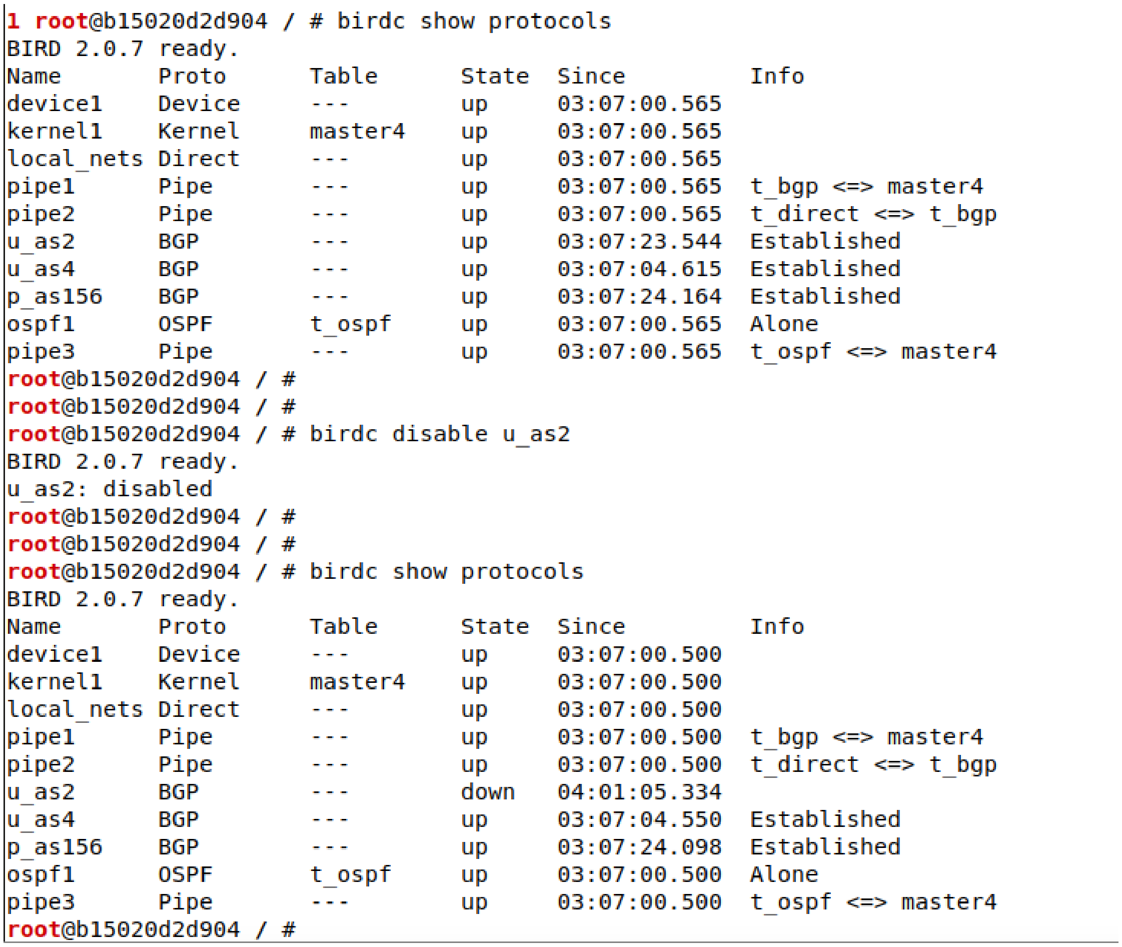
```
ipv4 table t_ospf;
protocol ospf ospf1 {
    ipv4 {
        table t_ospf;
        import all;
        export all;
    };
    area 0 {
        interface "dummy0" { stub; };
        interface "ix102" { stub; };
        interface "net0" { hello 1; dead count 2; };

    };
}
protocol pipe {
    table t_ospf;
    peer table master4;
    import none;
    export all;
}
```

Using cat command can view the configuration file to understand the BGP configuration.

Task 1a2:

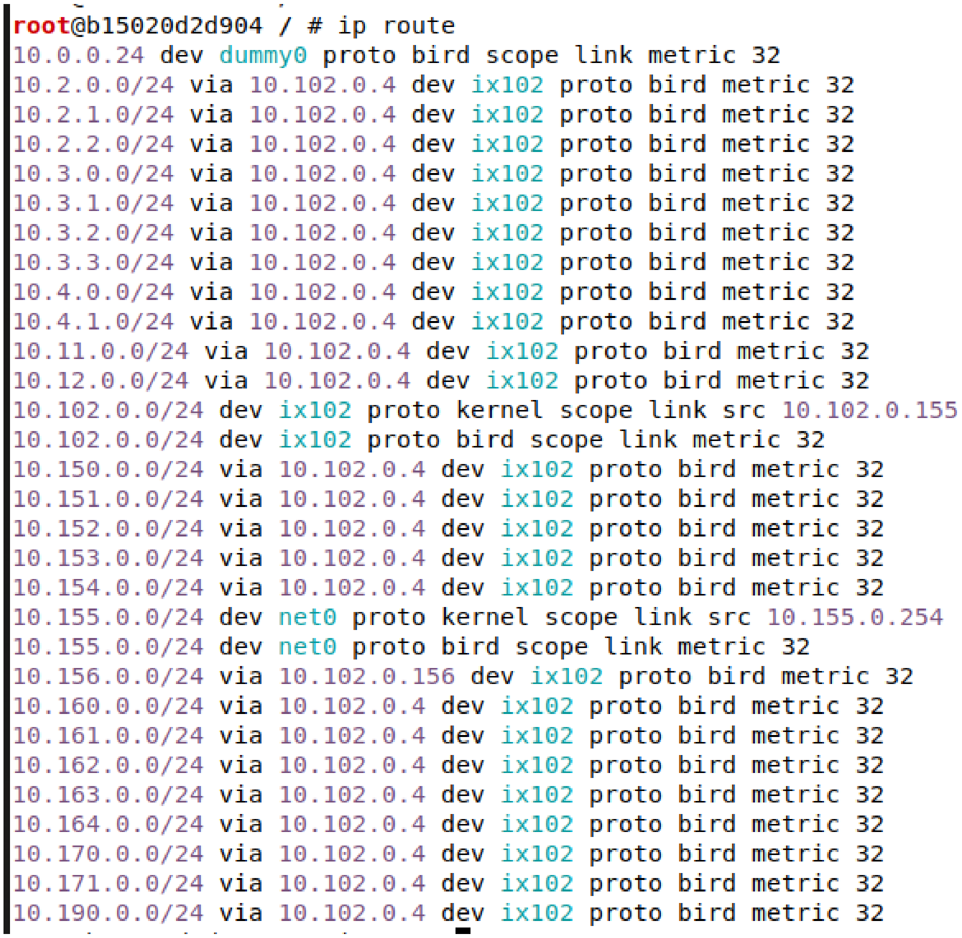
Use the birdc show protocols to know the current protocols and their state

Initially The u-as2, u_as3 and p_as156 state is up and the connection is established.

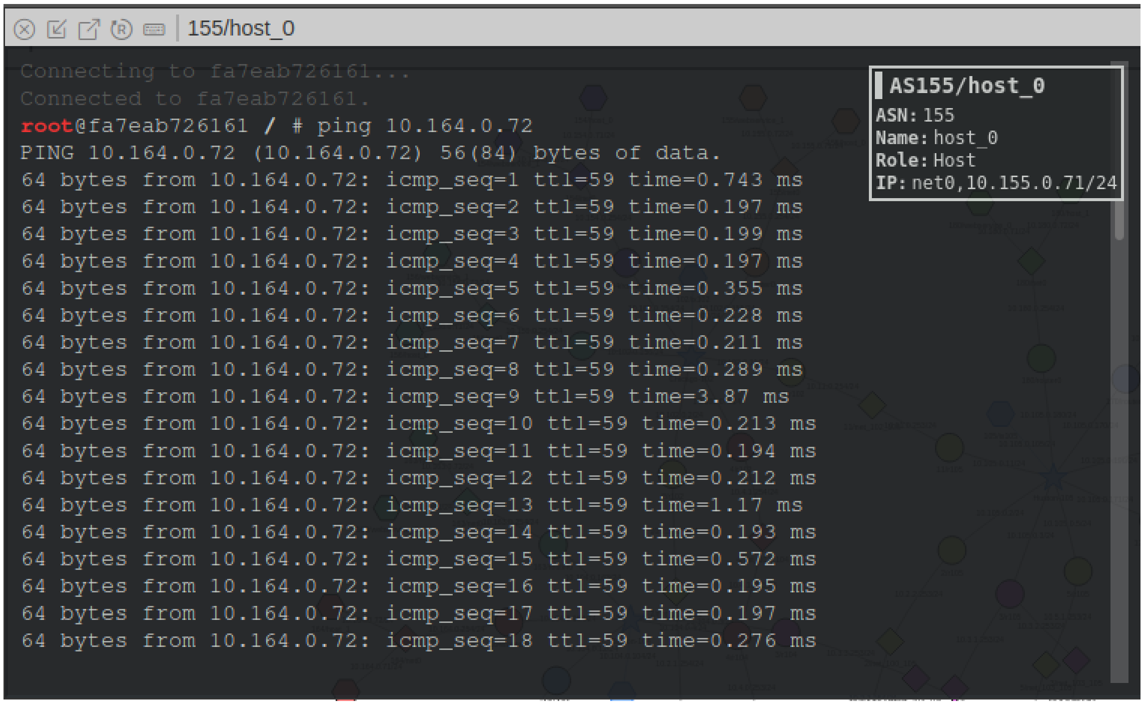


```
1 root@b15020d2d904 / # birdc show protocols
BIRD 2.0.7 ready.
Name       Proto      Table      State  Since         Info
device1    Device     ---        up     03:07:00.565
kernel1    Kernel     master4    up     03:07:00.565
local_nets Direct     ---        up     03:07:00.565
pipe1      Pipe       ---        up     03:07:00.565  t_bgp <=> master4
pipe2      Pipe       ---        up     03:07:00.565  t_direct <=> t_bgp
u_as2      BGP        ---        up     03:07:23.544  Established
u_as4      BGP        ---        up     03:07:04.615  Established
p_as156    BGP        ---        up     03:07:24.164  Established
ospf1      OSPF       t_ospf     up     03:07:00.565  Alone
pipe3      Pipe       ---        up     03:07:00.565  t_ospf <=> master4
root@b15020d2d904 / #
root@b15020d2d904 / #
root@b15020d2d904 / # birdc disable u_as2
BIRD 2.0.7 ready.
u_as2: disabled
root@b15020d2d904 / #
root@b15020d2d904 / #
root@b15020d2d904 / # birdc show protocols
BIRD 2.0.7 ready.
Name       Proto      Table      State  Since         Info
device1    Device     ---        up     03:07:00.500
kernel1    Kernel     master4    up     03:07:00.500
local_nets Direct     ---        up     03:07:00.500
pipe1      Pipe       ---        up     03:07:00.500  t_bgp <=> master4
pipe2      Pipe       ---        up     03:07:00.500  t_direct <=> t_bgp
u_as2      BGP        ---        down   04:01:05.334
u_as4      BGP        ---        up     03:07:04.550  Established
p_as156    BGP        ---        up     03:07:24.098  Established
ospf1      OSPF       t_ospf     up     03:07:00.500  Alone
pipe3      Pipe       ---        up     03:07:00.500  t_ospf <=> master4
root@b15020d2d904 / #
```

Can disable one of the protocols by the command “birdc disable u_as2”, which disables the state of the protocol.



```
root@b15020d2d904 / # ip route
10.0.0.24 dev dummy0 proto bird scope link metric 32
10.2.0.0/24 via 10.102.0.4 dev ix102 proto bird metric 32
10.2.1.0/24 via 10.102.0.4 dev ix102 proto bird metric 32
10.2.2.0/24 via 10.102.0.4 dev ix102 proto bird metric 32
10.3.0.0/24 via 10.102.0.4 dev ix102 proto bird metric 32
10.3.1.0/24 via 10.102.0.4 dev ix102 proto bird metric 32
10.3.2.0/24 via 10.102.0.4 dev ix102 proto bird metric 32
10.3.3.0/24 via 10.102.0.4 dev ix102 proto bird metric 32
10.4.0.0/24 via 10.102.0.4 dev ix102 proto bird metric 32
10.4.1.0/24 via 10.102.0.4 dev ix102 proto bird metric 32
10.11.0.0/24 via 10.102.0.4 dev ix102 proto bird metric 32
10.12.0.0/24 via 10.102.0.4 dev ix102 proto bird metric 32
10.102.0.0/24 dev ix102 proto kernel scope link src 10.102.0.155
10.102.0.0/24 dev ix102 proto bird scope link metric 32
10.150.0.0/24 via 10.102.0.4 dev ix102 proto bird metric 32
10.151.0.0/24 via 10.102.0.4 dev ix102 proto bird metric 32
10.152.0.0/24 via 10.102.0.4 dev ix102 proto bird metric 32
10.153.0.0/24 via 10.102.0.4 dev ix102 proto bird metric 32
10.154.0.0/24 via 10.102.0.4 dev ix102 proto bird metric 32
10.155.0.0/24 dev net0 proto kernel scope link src 10.155.0.254
10.155.0.0/24 dev net0 proto bird scope link metric 32
10.156.0.0/24 via 10.102.0.156 dev ix102 proto bird metric 32
10.160.0.0/24 via 10.102.0.4 dev ix102 proto bird metric 32
10.161.0.0/24 via 10.102.0.4 dev ix102 proto bird metric 32
10.162.0.0/24 via 10.102.0.4 dev ix102 proto bird metric 32
10.163.0.0/24 via 10.102.0.4 dev ix102 proto bird metric 32
10.164.0.0/24 via 10.102.0.4 dev ix102 proto bird metric 32
10.170.0.0/24 via 10.102.0.4 dev ix102 proto bird metric 32
10.171.0.0/24 via 10.102.0.4 dev ix102 proto bird metric 32
10.190.0.0/24 via 10.102.0.4 dev ix102 proto bird metric 32
```

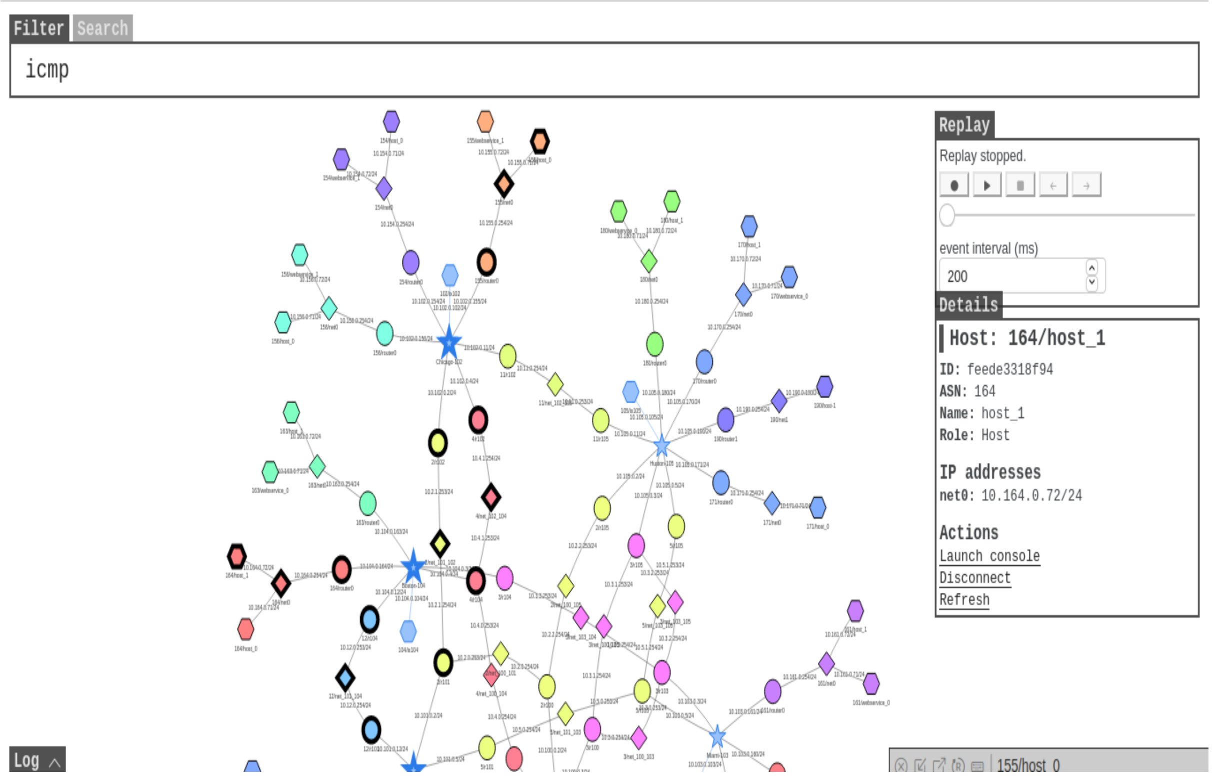


```
Connecting to fa7eab726161...
Connected to fa7eab726161.
root@fa7eab726161 / # ping 10.164.0.72
PING 10.164.0.72 (10.164.0.72) 56(84) bytes of data.
64 bytes from 10.164.0.72: icmp_seq=1 ttl=59 time=0.743 ms
64 bytes from 10.164.0.72: icmp_seq=2 ttl=59 time=0.197 ms
64 bytes from 10.164.0.72: icmp_seq=3 ttl=59 time=0.199 ms
64 bytes from 10.164.0.72: icmp_seq=4 ttl=59 time=0.197 ms
64 bytes from 10.164.0.72: icmp_seq=5 ttl=59 time=0.355 ms
64 bytes from 10.164.0.72: icmp_seq=6 ttl=59 time=0.228 ms
64 bytes from 10.164.0.72: icmp_seq=7 ttl=59 time=0.211 ms
64 bytes from 10.164.0.72: icmp_seq=8 ttl=59 time=0.289 ms
64 bytes from 10.164.0.72: icmp_seq=9 ttl=59 time=3.87 ms
64 bytes from 10.164.0.72: icmp_seq=10 ttl=59 time=0.213 ms
64 bytes from 10.164.0.72: icmp_seq=11 ttl=59 time=0.194 ms
64 bytes from 10.164.0.72: icmp_seq=12 ttl=59 time=0.212 ms
64 bytes from 10.164.0.72: icmp_seq=13 ttl=59 time=1.17 ms
64 bytes from 10.164.0.72: icmp_seq=14 ttl=59 time=0.193 ms
64 bytes from 10.164.0.72: icmp_seq=15 ttl=59 time=0.572 ms
64 bytes from 10.164.0.72: icmp_seq=16 ttl=59 time=0.195 ms
64 bytes from 10.164.0.72: icmp_seq=17 ttl=59 time=0.197 ms
64 bytes from 10.164.0.72: icmp_seq=18 ttl=59 time=0.276 ms
```

AS155/host_0
ASN: 155
Name: host_0
Role: Host
IP: net0,10.155.0.71/24

Before disabling the BGP session with u_as2 using the command, host 10.155.0.71 can communicate with host 10.164.0.72.

After disabling the session with u_as2, host 10.155.0.71 can still communicate with host 10.164.0.72. This is because of the u_as2 BGP connection.



icmp

Replay stopped.

event interval (ms)

200

Host: 164/host_1

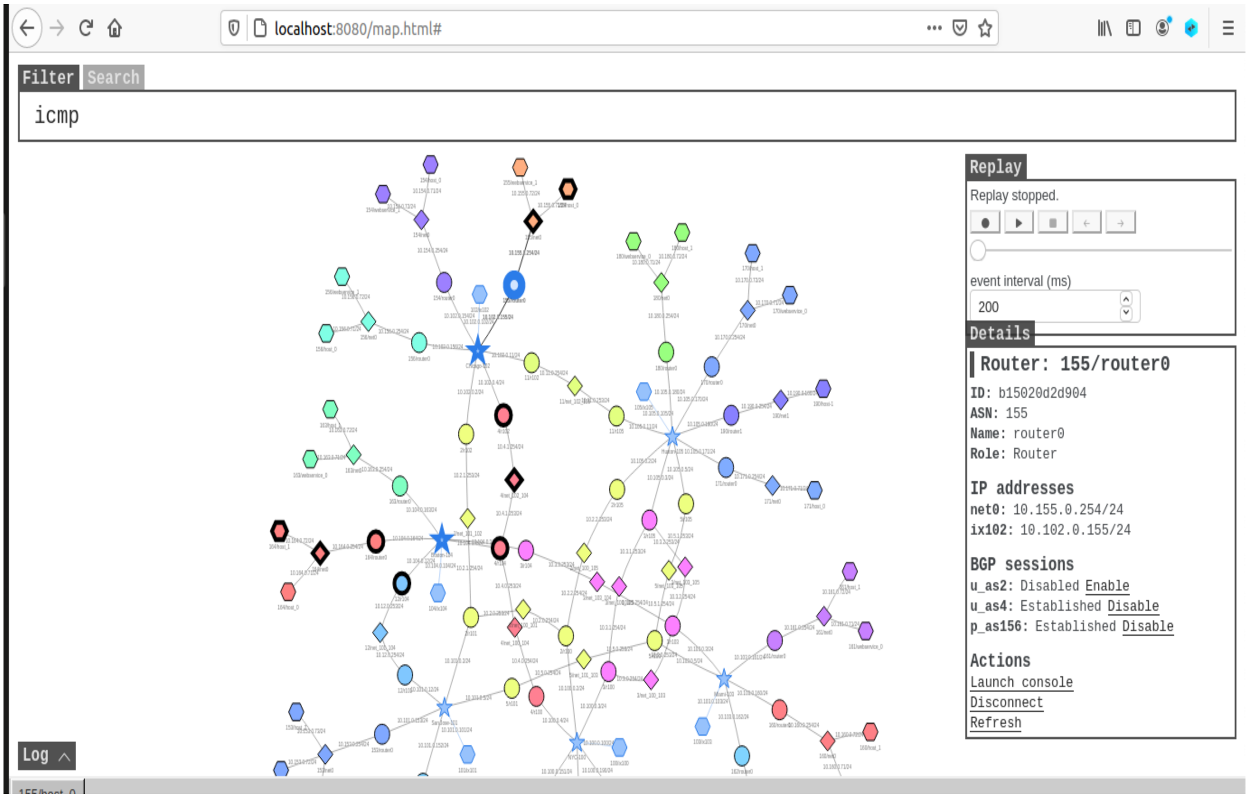
ID: feede3318f94
ASN: 164
Name: host_1
Role: Host

IP addresses

net0: 10.164.0.72/24

Actions

Launch console
Disconnect
Refresh



icmp

Replay stopped.

event interval (ms)

200

Router: 155/router0

ID: b15020d2d904
ASN: 155
Name: router0
Role: Router

IP addresses

net0: 10.155.0.254/24
ix102: 10.102.0.155/24

BGP sessions

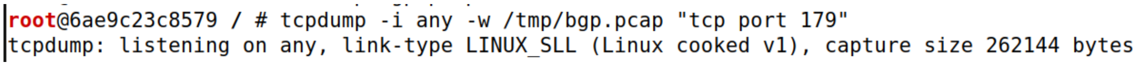
u_as2: Disabled Enable
u_as4: Established Disable
p_as156: Established Disable

Actions

Launch console
Disconnect
Refresh

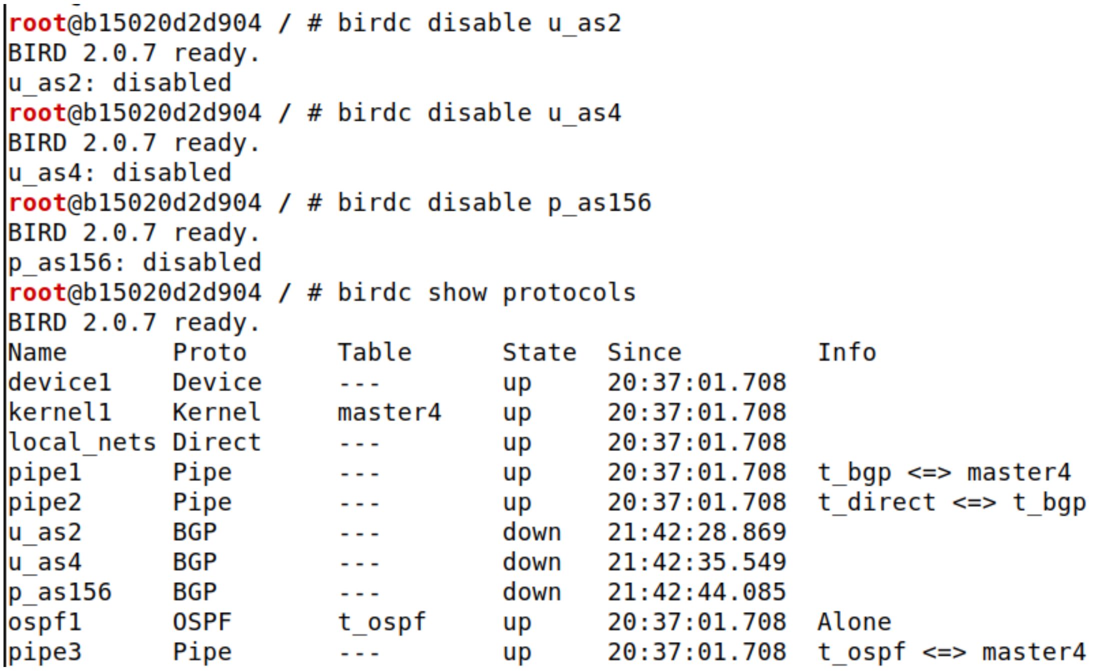
3.2 Task 1.b: Observing BGP UPDATE Messages

We disconnect all the 155 routers and see an update message once it restored



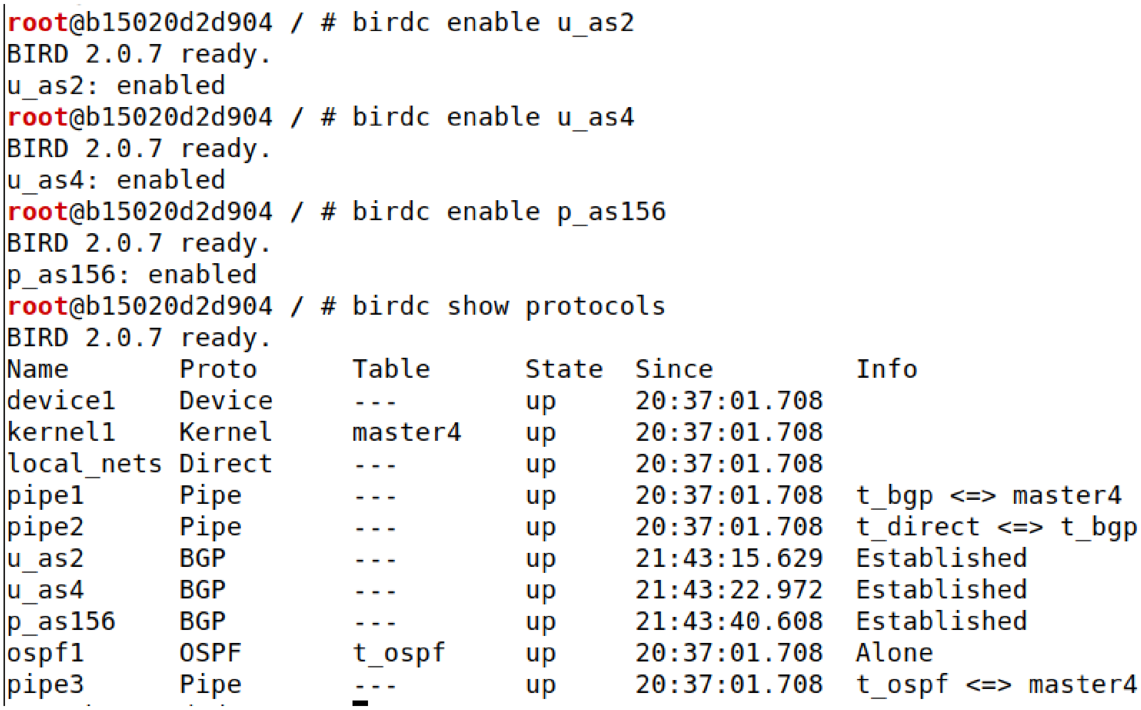
```
root@6ae9c23c8579 / # tcpdump -i any -w /tmp/bgp.pcap "tcp port 179"
tcpdump: listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes
```

Disable

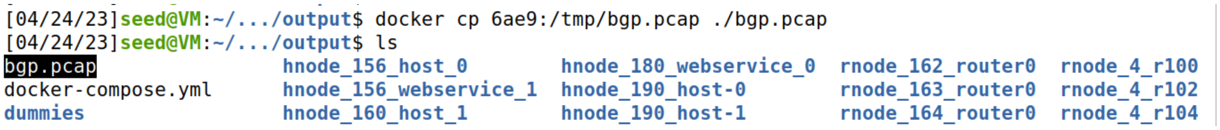


```
root@b15020d2d904 / # birdc disable u_as2
BIRD 2.0.7 ready.
u_as2: disabled
root@b15020d2d904 / # birdc disable u_as4
BIRD 2.0.7 ready.
u_as4: disabled
root@b15020d2d904 / # birdc disable p_as156
BIRD 2.0.7 ready.
p_as156: disabled
root@b15020d2d904 / # birdc show protocols
BIRD 2.0.7 ready.
Name       Proto      Table      State  Since         Info
device1    Device     ---        up     20:37:01.708
kernel1    Kernel     master4    up     20:37:01.708
local_nets Direct     ---        up     20:37:01.708
pipe1      Pipe       ---        up     20:37:01.708  t_bgp <=> master4
pipe2      Pipe       ---        up     20:37:01.708  t_direct <=> t_bgp
u_as2      BGP        ---        down   21:42:28.869
u_as4      BGP        ---        down   21:42:35.549
p_as156    BGP        ---        down   21:42:44.085
ospf1      OSPF       t_ospf     up     20:37:01.708  Alone
pipe3      Pipe       ---        up     20:37:01.708  t_ospf <=> master4
```

Enable

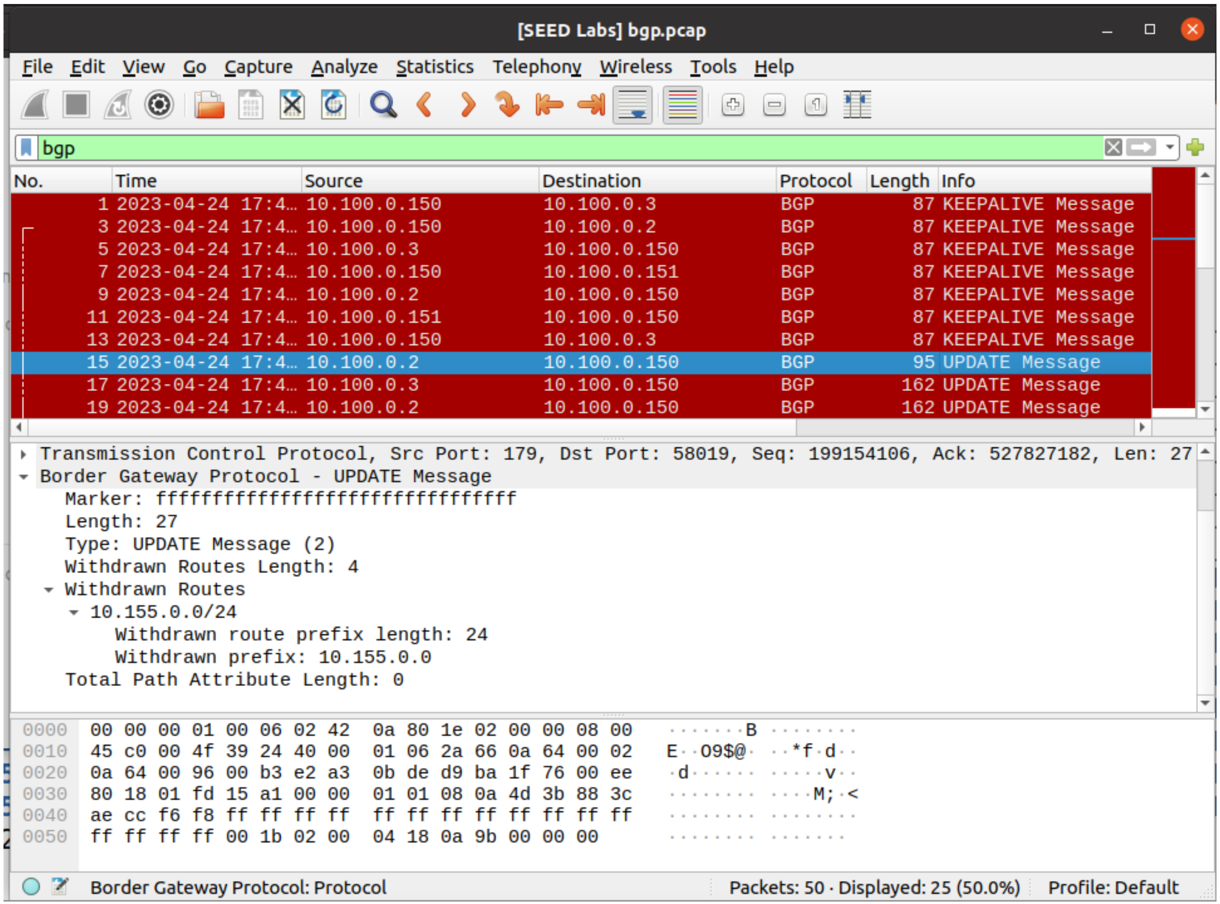


```
root@b15020d2d904 / # birdc enable u_as2
BIRD 2.0.7 ready.
u_as2: enabled
root@b15020d2d904 / # birdc enable u_as4
BIRD 2.0.7 ready.
u_as4: enabled
root@b15020d2d904 / # birdc enable p_as156
BIRD 2.0.7 ready.
p_as156: enabled
root@b15020d2d904 / # birdc show protocols
BIRD 2.0.7 ready.
Name       Proto      Table      State  Since         Info
device1    Device     ---        up     20:37:01.708
kernel1    Kernel     master4    up     20:37:01.708
local_nets Direct     ---        up     20:37:01.708
pipe1      Pipe       ---        up     20:37:01.708  t_bgp <=> master4
pipe2      Pipe       ---        up     20:37:01.708  t_direct <=> t_bgp
u_as2      BGP        ---        up     21:43:15.629  Established
u_as4      BGP        ---        up     21:43:22.972  Established
p_as156    BGP        ---        up     21:43:40.608  Established
ospf1      OSPF       t_ospf     up     20:37:01.708  Alone
pipe3      Pipe       ---        up     20:37:01.708  t_ospf <=> master4
```



```
[04/24/23]seed@VM:~/.../output$ docker cp 6ae9:/tmp/bgp.pcap ./bgp.pcap
[04/24/23]seed@VM:~/.../output$ ls
bgp.pcap            hnode_156_host_0        hnode_180_webservice_0  rnode_162_router0  rnode_4_r100
docker-compose.yml  hnode_156_webservice_1  hnode_190_host-0        rnode_163_router0  rnode_4_r102
dummies             hnode_160_host_1        hnode_190_host-1        rnode_164_router0  rnode_4_r104
```

Updated message is displayed on wireshark

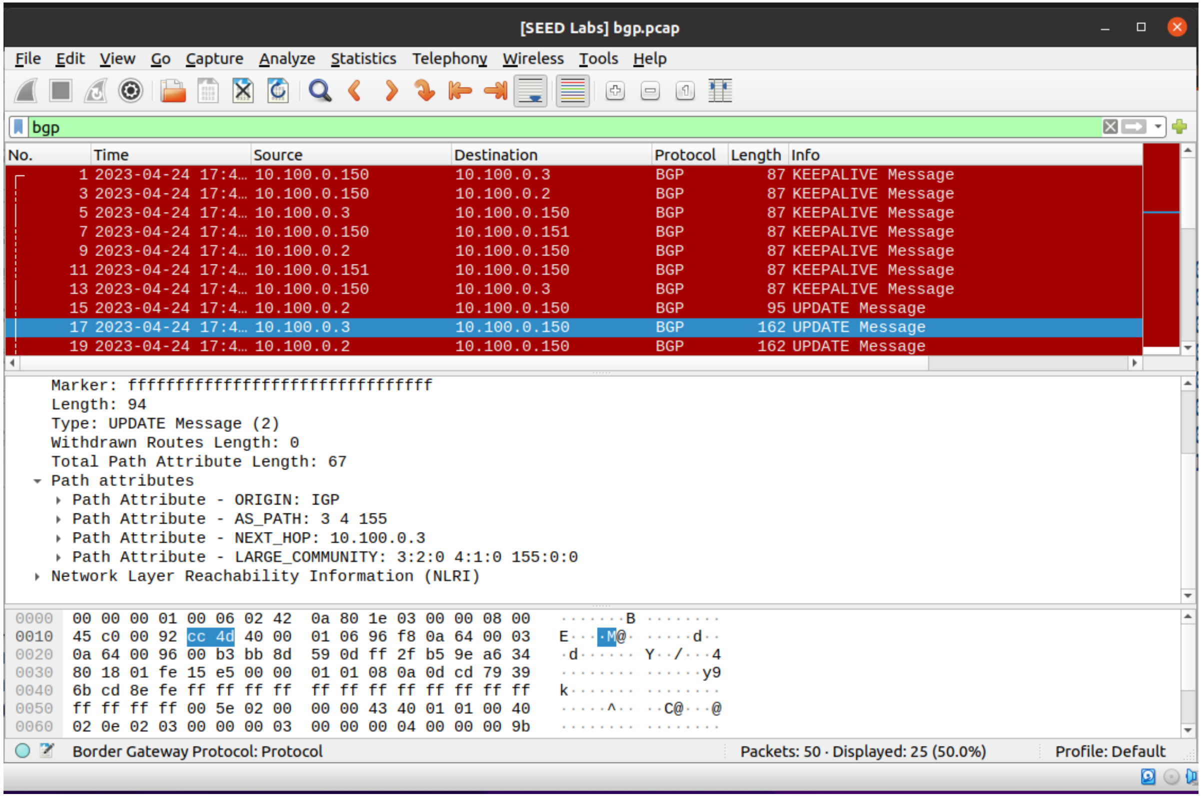

[SEED Labs] bgp.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
bgp

```
No.  Time              Source         Destination    Protocol Length Info
   1 2023-04-24 17:4… 10.100.0.150   10.100.0.3     BGP          87 KEEPALIVE Message
   3 2023-04-24 17:4… 10.100.0.150   10.100.0.2     BGP          87 KEEPALIVE Message
   5 2023-04-24 17:4… 10.100.0.3     10.100.0.150   BGP          87 KEEPALIVE Message
   7 2023-04-24 17:4… 10.100.0.150   10.100.0.151   BGP          87 KEEPALIVE Message
   9 2023-04-24 17:4… 10.100.0.2     10.100.0.150   BGP          87 KEEPALIVE Message
  11 2023-04-24 17:4… 10.100.0.151   10.100.0.150   BGP          87 KEEPALIVE Message
  13 2023-04-24 17:4… 10.100.0.150   10.100.0.3     BGP          87 KEEPALIVE Message
  15 2023-04-24 17:4… 10.100.0.2     10.100.0.150   BGP          95 UPDATE Message
  17 2023-04-24 17:4… 10.100.0.3     10.100.0.150   BGP         162 UPDATE Message
  19 2023-04-24 17:4… 10.100.0.2     10.100.0.150   BGP         162 UPDATE Message
```

```
▸ Transmission Control Protocol, Src Port: 179, Dst Port: 58019, Seq: 199154106, Ack: 527827182, Len: 27
▾ Border Gateway Protocol - UPDATE Message
    Marker: ffffffffffffffffffffffffffffffff
    Length: 27
    Type: UPDATE Message (2)
    Withdrawn Routes Length: 4
  ▾ Withdrawn Routes
    ▾ 10.155.0.0/24
        Withdrawn route prefix length: 24
        Withdrawn prefix: 10.155.0.0
    Total Path Attribute Length: 0
```

```
0000  00 00 00 01 00 06 02 42  0a 80 1e 02 00 00 08 00   ·······B ········
0010  45 c0 00 4f 39 24 40 00  01 06 2a 66 0a 64 00 02   E··O9$@· ··*f·d··
0020  0a 64 00 96 00 b3 e2 a3  0b de d9 ba 1f 76 00 ee   ·d······ ·····v··
0030  80 18 01 fd 15 a1 00 00  01 01 08 0a 4d 3b 88 3c   ········ ····M;·<
0040  ae cc f6 f8 ff ff ff ff  ff ff ff ff ff ff ff ff   ········ ········
0050  ff ff ff ff 00 1b 02 00  04 18 0a 9b 00 00 00      ········ ·······
```

Border Gateway Protocol: Protocol   Packets: 50 · Displayed: 25 (50.0%)   Profile: Default


[SEED Labs] bgp.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
bgp

```
No.  Time              Source         Destination    Protocol Length Info
   1 2023-04-24 17:4… 10.100.0.150   10.100.0.3     BGP          87 KEEPALIVE Message
   3 2023-04-24 17:4… 10.100.0.150   10.100.0.2     BGP          87 KEEPALIVE Message
   5 2023-04-24 17:4… 10.100.0.3     10.100.0.150   BGP          87 KEEPALIVE Message
   7 2023-04-24 17:4… 10.100.0.150   10.100.0.151   BGP          87 KEEPALIVE Message
   9 2023-04-24 17:4… 10.100.0.2     10.100.0.150   BGP          87 KEEPALIVE Message
  11 2023-04-24 17:4… 10.100.0.151   10.100.0.150   BGP          87 KEEPALIVE Message
  13 2023-04-24 17:4… 10.100.0.150   10.100.0.3     BGP          87 KEEPALIVE Message
  15 2023-04-24 17:4… 10.100.0.2     10.100.0.150   BGP          95 UPDATE Message
  17 2023-04-24 17:4… 10.100.0.3     10.100.0.150   BGP         162 UPDATE Message
  19 2023-04-24 17:4… 10.100.0.2     10.100.0.150   BGP         162 UPDATE Message
```

```
    Marker: ffffffffffffffffffffffffffffffff
    Length: 94
    Type: UPDATE Message (2)
    Withdrawn Routes Length: 0
    Total Path Attribute Length: 67
  ▾ Path attributes
    ▸ Path Attribute - ORIGIN: IGP
    ▸ Path Attribute - AS_PATH: 3 4 155
    ▸ Path Attribute - NEXT_HOP: 10.100.0.3
    ▸ Path Attribute - LARGE_COMMUNITY: 3:2:0 4:1:0 155:0:0
  ▸ Network Layer Reachability Information (NLRI)
```

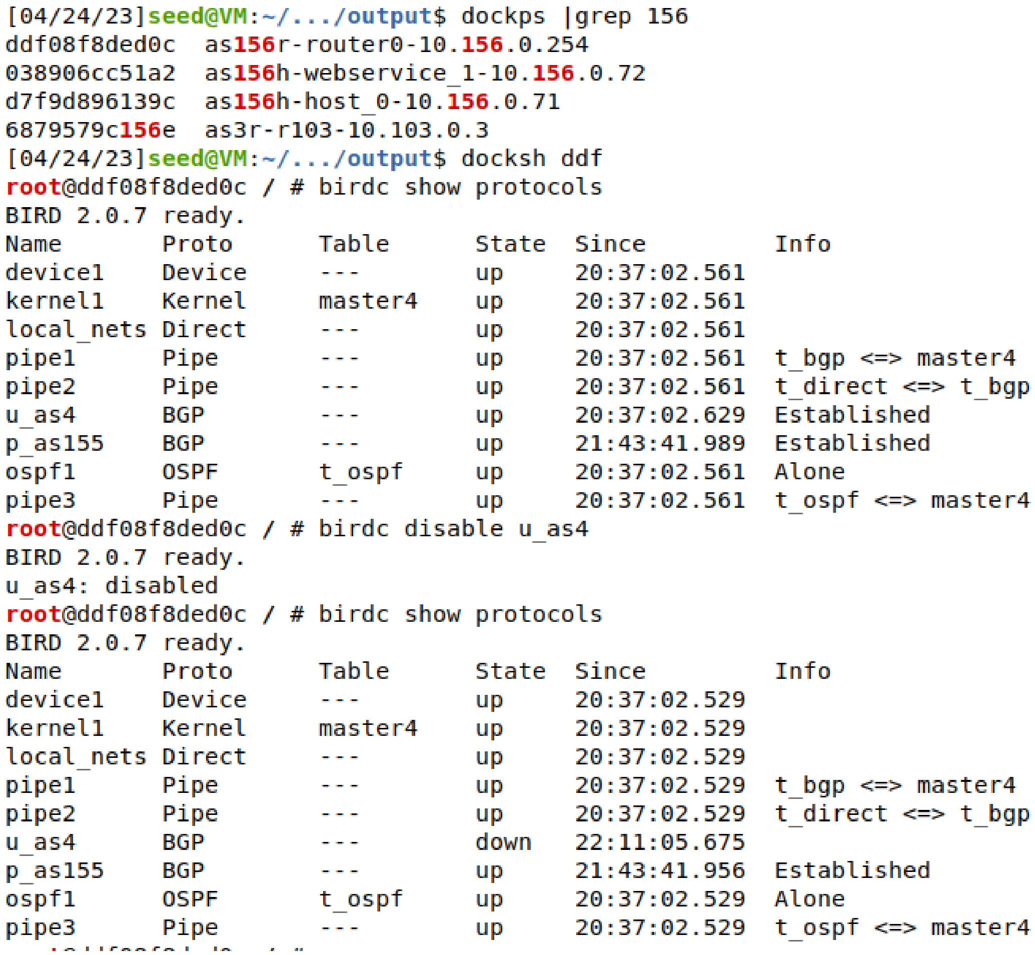
```
0000  00 00 00 01 00 06 02 42  0a 80 1e 03 00 00 08 00   ·······B ········
0010  45 c0 00 92 cc 4d 40 00  01 06 96 f8 0a 64 00 03   E····M@· ·····d··
0020  0a 64 00 96 00 b3 bb 8d  59 0d ff 2f b5 9e a6 34   ·d······ Y··/···4
0030  80 18 01 fe 15 e5 00 00  01 01 08 0a 0d cd 79 39   ········ ······y9
0040  6b cd 8e fe ff ff ff ff  ff ff ff ff ff ff ff ff   k······· ········
0050  ff ff ff ff 00 5e 02 00  00 00 43 40 01 01 00 40   ·····^·· ··C@···@
0060  02 0e 02 03 00 00 00 03  00 00 00 04 00 00 00 9b   ········ ········
```

Border Gateway Protocol: Protocol   Packets: 50 · Displayed: 25 (50.0%)   Profile: Default

3.3 Task 1.c: Experimenting with Large Communities

For this scenario we have to disconnect the connection between AS-4 and AS156, then ping on router 10.156.0.71.

Now, let’s ping 10.155.0.71 and 10.161.0.71 as shown in the below screenshot:

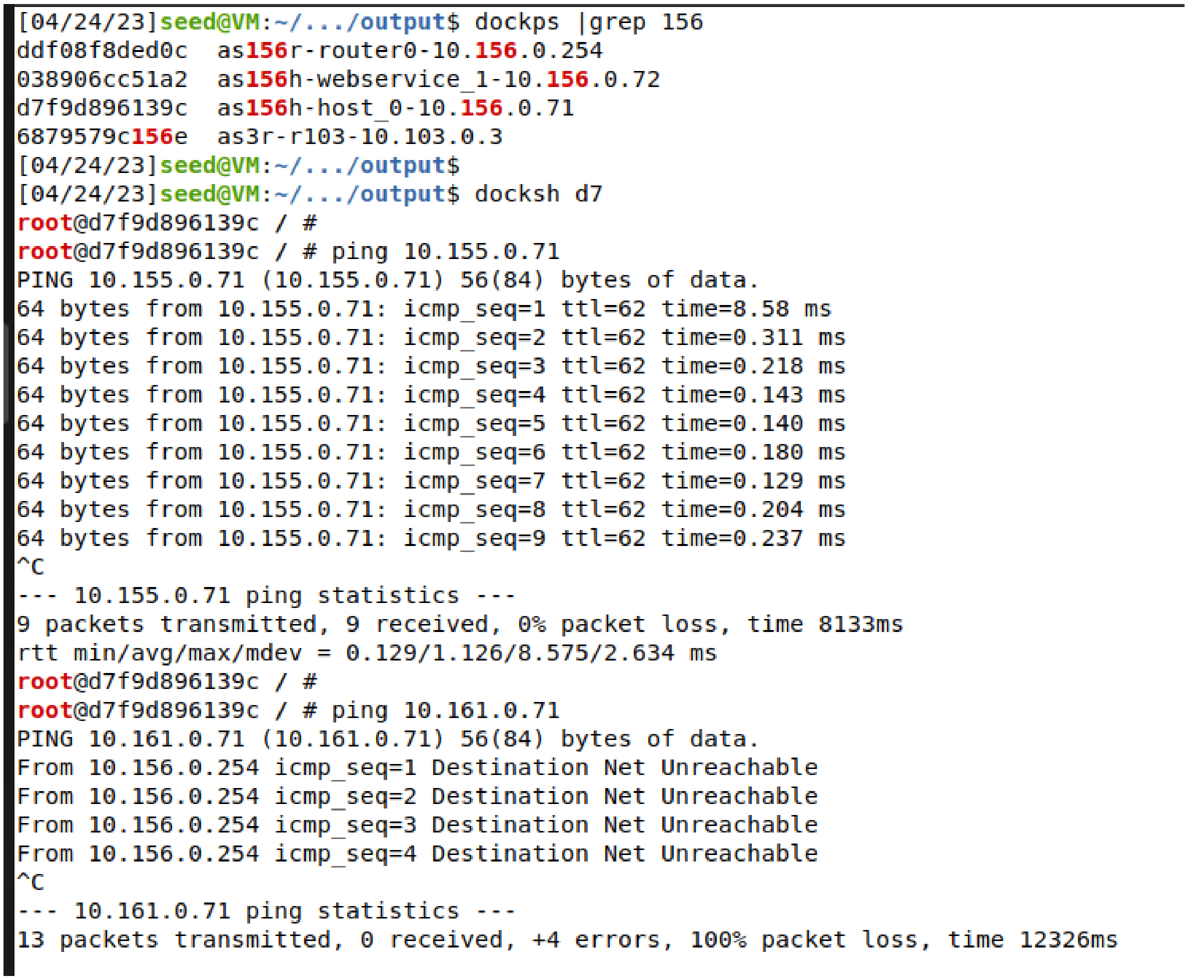


```
[04/24/23]seed@VM:~/.../output$ dockps |grep 156
ddf08f8ded0c  as156r-router0-10.156.0.254
038906cc51a2  as156h-webservice_1-10.156.0.72
d7f9d896139c  as156h-host_0-10.156.0.71
6879579c156e  as3r-r103-10.103.0.3
[04/24/23]seed@VM:~/.../output$ docksh ddf
root@ddf08f8ded0c / # birdc show protocols
BIRD 2.0.7 ready.
Name       Proto      Table      State  Since         Info
device1    Device     ---        up     20:37:02.561
kernel1    Kernel     master4    up     20:37:02.561
local_nets Direct     ---        up     20:37:02.561
pipe1      Pipe       ---        up     20:37:02.561  t_bgp <=> master4
pipe2      Pipe       ---        up     20:37:02.561  t_direct <=> t_bgp
u_as4      BGP        ---        up     20:37:02.629  Established
p_as155    BGP        ---        up     21:43:41.989  Established
ospf1      OSPF       t_ospf     up     20:37:02.561  Alone
pipe3      Pipe       ---        up     20:37:02.561  t_ospf <=> master4
root@ddf08f8ded0c / # birdc disable u_as4
BIRD 2.0.7 ready.
u_as4: disabled
root@ddf08f8ded0c / # birdc show protocols
BIRD 2.0.7 ready.
Name       Proto      Table      State  Since         Info
device1    Device     ---        up     20:37:02.529
kernel1    Kernel     master4    up     20:37:02.529
local_nets Direct     ---        up     20:37:02.529
pipe1      Pipe       ---        up     20:37:02.529  t_bgp <=> master4
pipe2      Pipe       ---        up     20:37:02.529  t_direct <=> t_bgp
u_as4      BGP        ---        down   22:11:05.675
p_as155    BGP        ---        up     21:43:41.956  Established
ospf1      OSPF       t_ospf     up     20:37:02.529  Alone
pipe3      Pipe       ---        up     20:37:02.529  t_ospf <=> master4
```

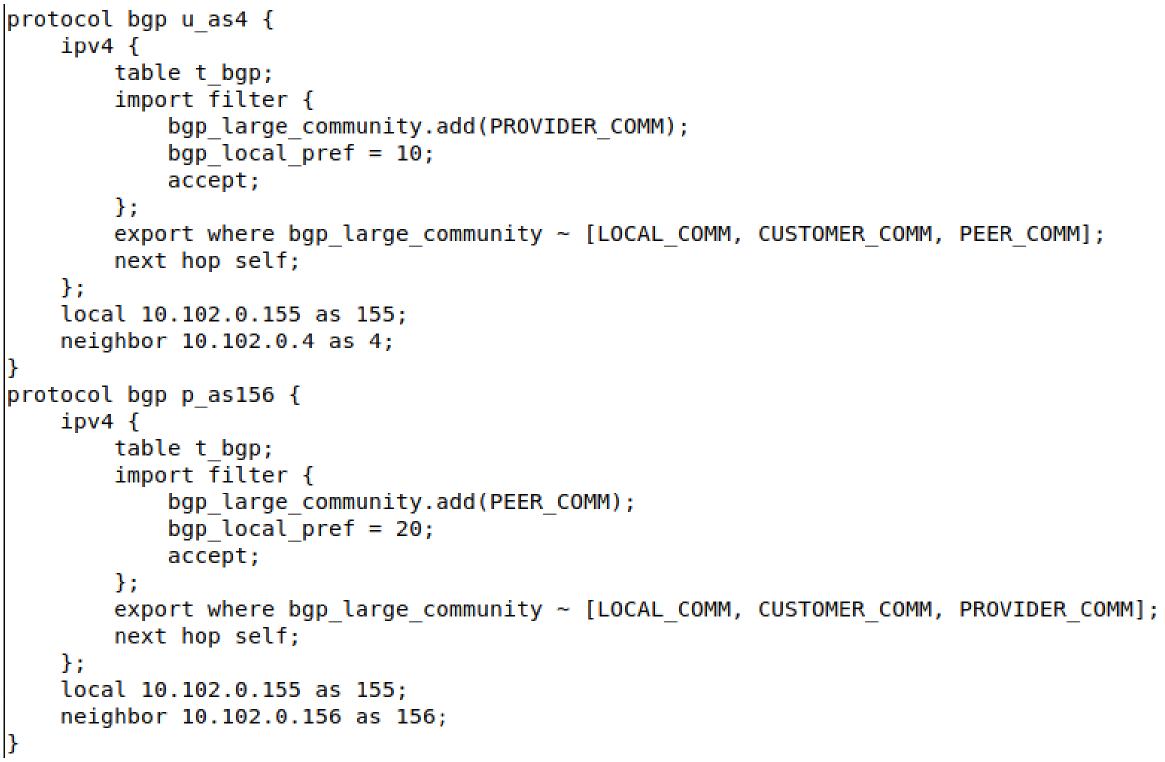
When we try to ping the host 10.155.0.71 it is successful. But when we try to ping the host 10.161.0.71 it is net unreachable as shown in the below screenshot.

Even though AS-156 is connected to the internet through AS-155 , since AS-156 doesn’t have any business dealings with the router AS-155, AS-155 will not forward the packets.

Edit the configuration file of the AS-155 router to realize the forwarding of AS-156 data packets through AS-155.

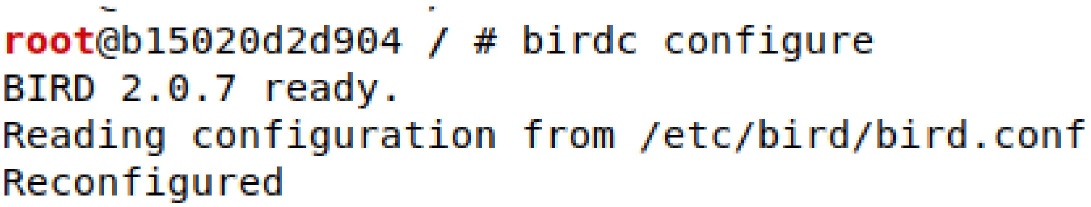


```
[04/24/23]seed@VM:~/.../output$ dockps |grep 156
ddf08f8ded0c  as156r-router0-10.156.0.254
038906cc51a2  as156h-webservice_1-10.156.0.72
d7f9d896139c  as156h-host_0-10.156.0.71
6879579c156e  as3r-r103-10.103.0.3
[04/24/23]seed@VM:~/.../output$
[04/24/23]seed@VM:~/.../output$ docksh d7
root@d7f9d896139c / #
root@d7f9d896139c / # ping 10.155.0.71
PING 10.155.0.71 (10.155.0.71) 56(84) bytes of data.
64 bytes from 10.155.0.71: icmp_seq=1 ttl=62 time=8.58 ms
64 bytes from 10.155.0.71: icmp_seq=2 ttl=62 time=0.311 ms
64 bytes from 10.155.0.71: icmp_seq=3 ttl=62 time=0.218 ms
64 bytes from 10.155.0.71: icmp_seq=4 ttl=62 time=0.143 ms
64 bytes from 10.155.0.71: icmp_seq=5 ttl=62 time=0.140 ms
64 bytes from 10.155.0.71: icmp_seq=6 ttl=62 time=0.180 ms
64 bytes from 10.155.0.71: icmp_seq=7 ttl=62 time=0.129 ms
64 bytes from 10.155.0.71: icmp_seq=8 ttl=62 time=0.204 ms
64 bytes from 10.155.0.71: icmp_seq=9 ttl=62 time=0.237 ms
^C
--- 10.155.0.71 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8133ms
rtt min/avg/max/mdev = 0.129/1.126/8.575/2.634 ms
root@d7f9d896139c / #
root@d7f9d896139c / # ping 10.161.0.71
PING 10.161.0.71 (10.161.0.71) 56(84) bytes of data.
From 10.156.0.254 icmp_seq=1 Destination Net Unreachable
From 10.156.0.254 icmp_seq=2 Destination Net Unreachable
From 10.156.0.254 icmp_seq=3 Destination Net Unreachable
From 10.156.0.254 icmp_seq=4 Destination Net Unreachable
^C
--- 10.161.0.71 ping statistics ---
13 packets transmitted, 0 received, +4 errors, 100% packet loss, time 12326ms
```



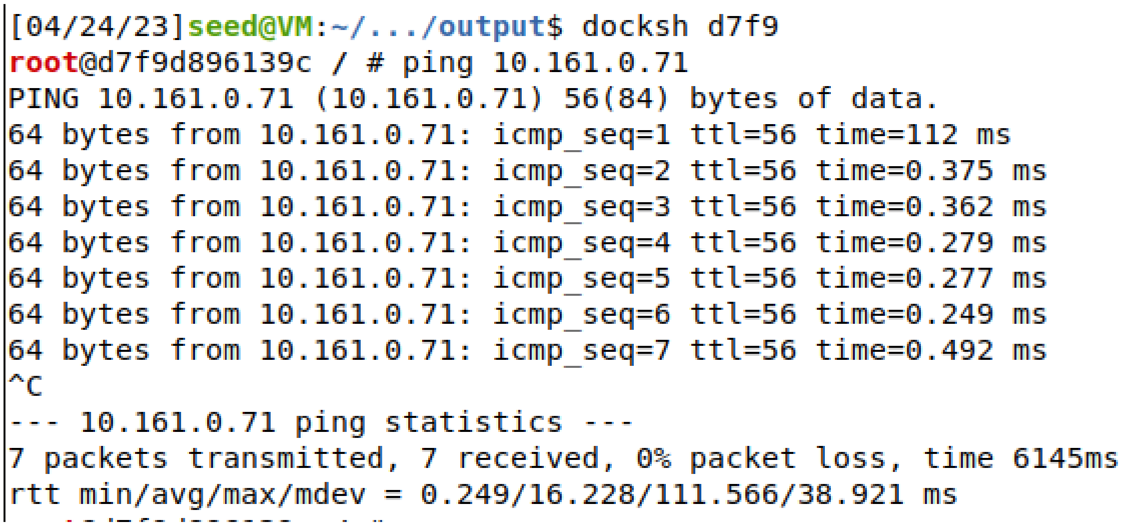
```
protocol bgp u_as4 {
    ipv4 {
        table t_bgp;
        import filter {
            bgp_large_community.add(PROVIDER_COMM);
            bgp_local_pref = 10;
            accept;
        };
        export where bgp_large_community ~ [LOCAL_COMM, CUSTOMER_COMM, PEER_COMM];
        next hop self;
    };
    local 10.102.0.155 as 155;
    neighbor 10.102.0.4 as 4;
}
protocol bgp p_as156 {
    ipv4 {
        table t_bgp;
        import filter {
            bgp_large_community.add(PEER_COMM);
            bgp_local_pref = 20;
            accept;
        };
        export where bgp_large_community ~ [LOCAL_COMM, CUSTOMER_COMM, PROVIDER_COMM];
        next hop self;
    };
    local 10.102.0.155 as 155;
    neighbor 10.102.0.156 as 156;
}
```

Reconfigure the configuration file



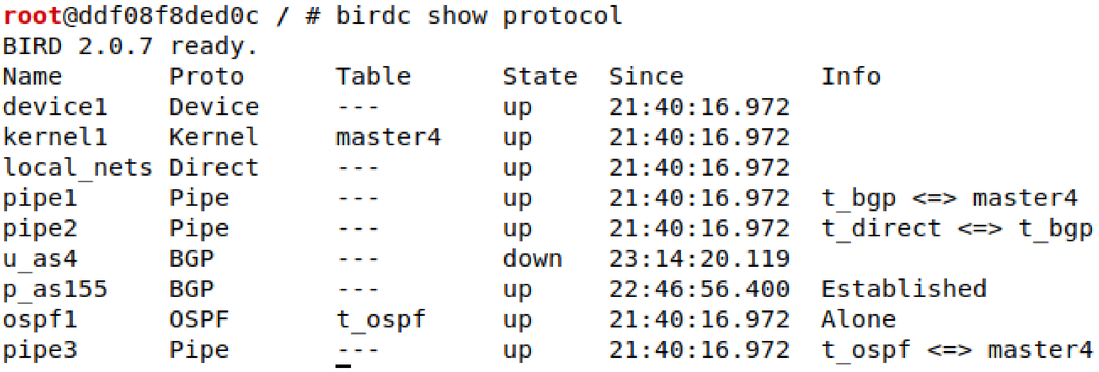
```
root@b15020d2d904 / # birdc configure
BIRD 2.0.7 ready.
Reading configuration from /etc/bird/bird.conf
Reconfigured
```

Now let’s ping from the AS-156 host machine 10.156.0.71 to 10.161.0.71



```
[04/24/23]seed@VM:~/.../output$ docksh d7f9
root@d7f9d896139c / # ping 10.161.0.71
PING 10.161.0.71 (10.161.0.71) 56(84) bytes of data.
64 bytes from 10.161.0.71: icmp_seq=1 ttl=56 time=112 ms
64 bytes from 10.161.0.71: icmp_seq=2 ttl=56 time=0.375 ms
64 bytes from 10.161.0.71: icmp_seq=3 ttl=56 time=0.362 ms
64 bytes from 10.161.0.71: icmp_seq=4 ttl=56 time=0.279 ms
64 bytes from 10.161.0.71: icmp_seq=5 ttl=56 time=0.277 ms
64 bytes from 10.161.0.71: icmp_seq=6 ttl=56 time=0.249 ms
64 bytes from 10.161.0.71: icmp_seq=7 ttl=56 time=0.492 ms
^C
--- 10.161.0.71 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6145ms
rtt min/avg/max/mdev = 0.249/16.228/111.566/38.921 ms
```

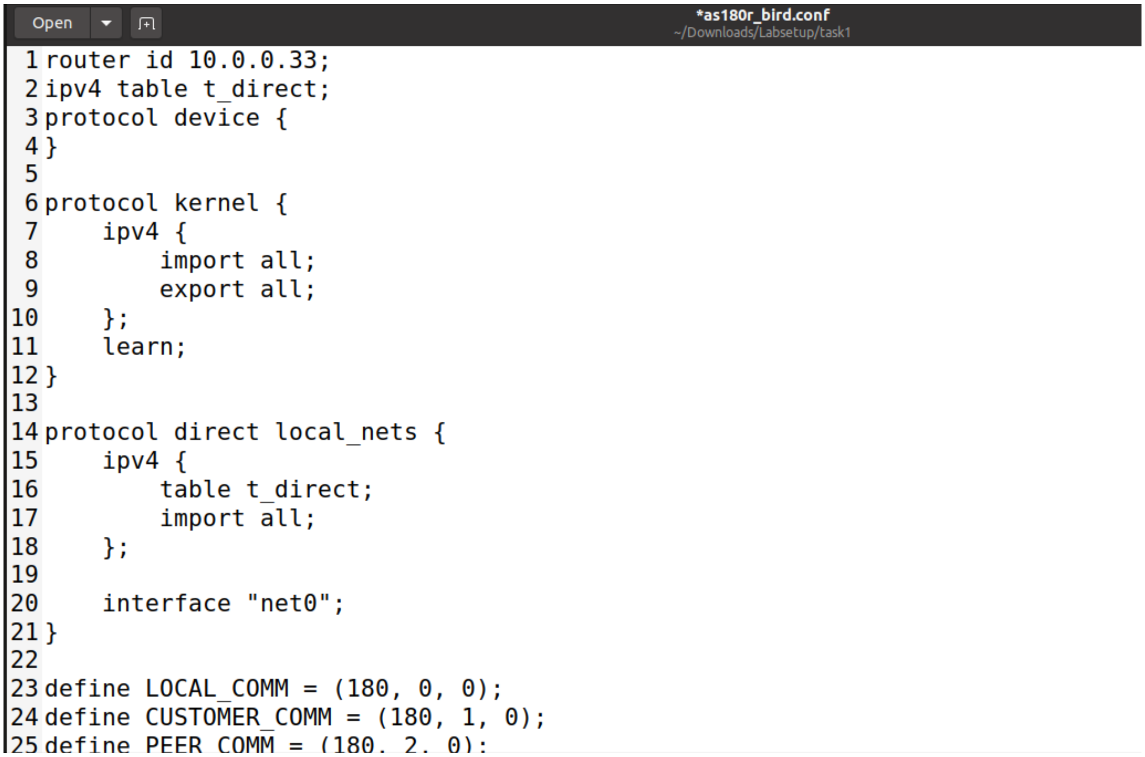
We can see that AS4 is down



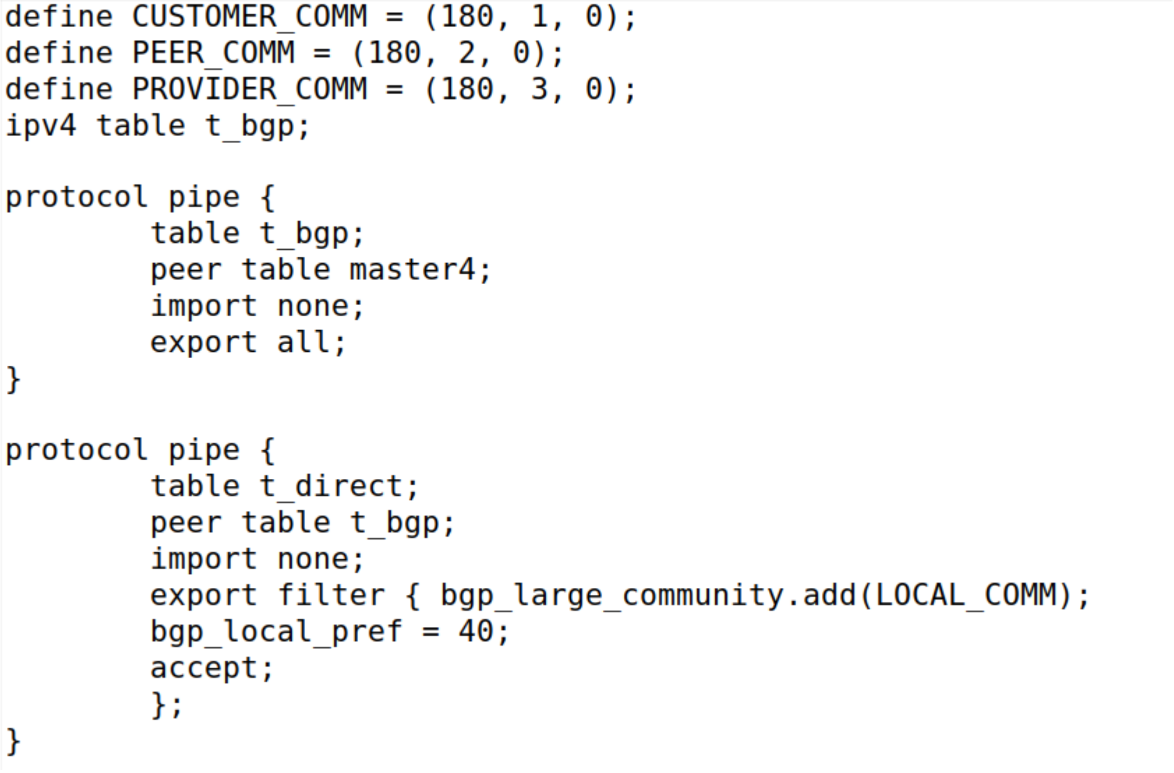
```
root@ddf08f8ded0c / # birdc show protocol
BIRD 2.0.7 ready.
Name       Proto      Table      State  Since         Info
device1    Device     ---        up     21:40:16.972
kernel1    Kernel     master4    up     21:40:16.972
local_nets Direct     ---        up     21:40:16.972
pipe1      Pipe       ---        up     21:40:16.972  t_bgp <=> master4
pipe2      Pipe       ---        up     21:40:16.972  t_direct <=> t_bgp
u_as4      BGP        ---        down   23:14:20.119
p_as155    BGP        ---        up     22:46:56.400  Established
ospf1      OSPF       t_ospf     up     21:40:16.972  Alone
pipe3      Pipe       ---        up     21:40:16.972  t_ospf <=> master4
```

3.4 Task 1.d: Configuring AS-180

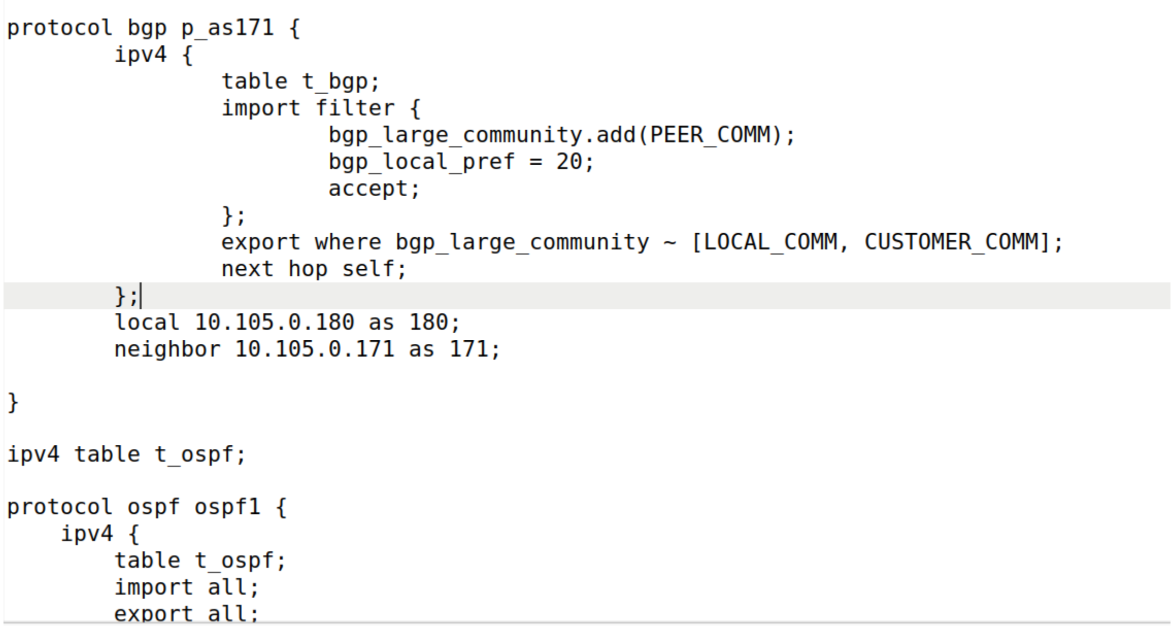
Edit the configuration file of AS180



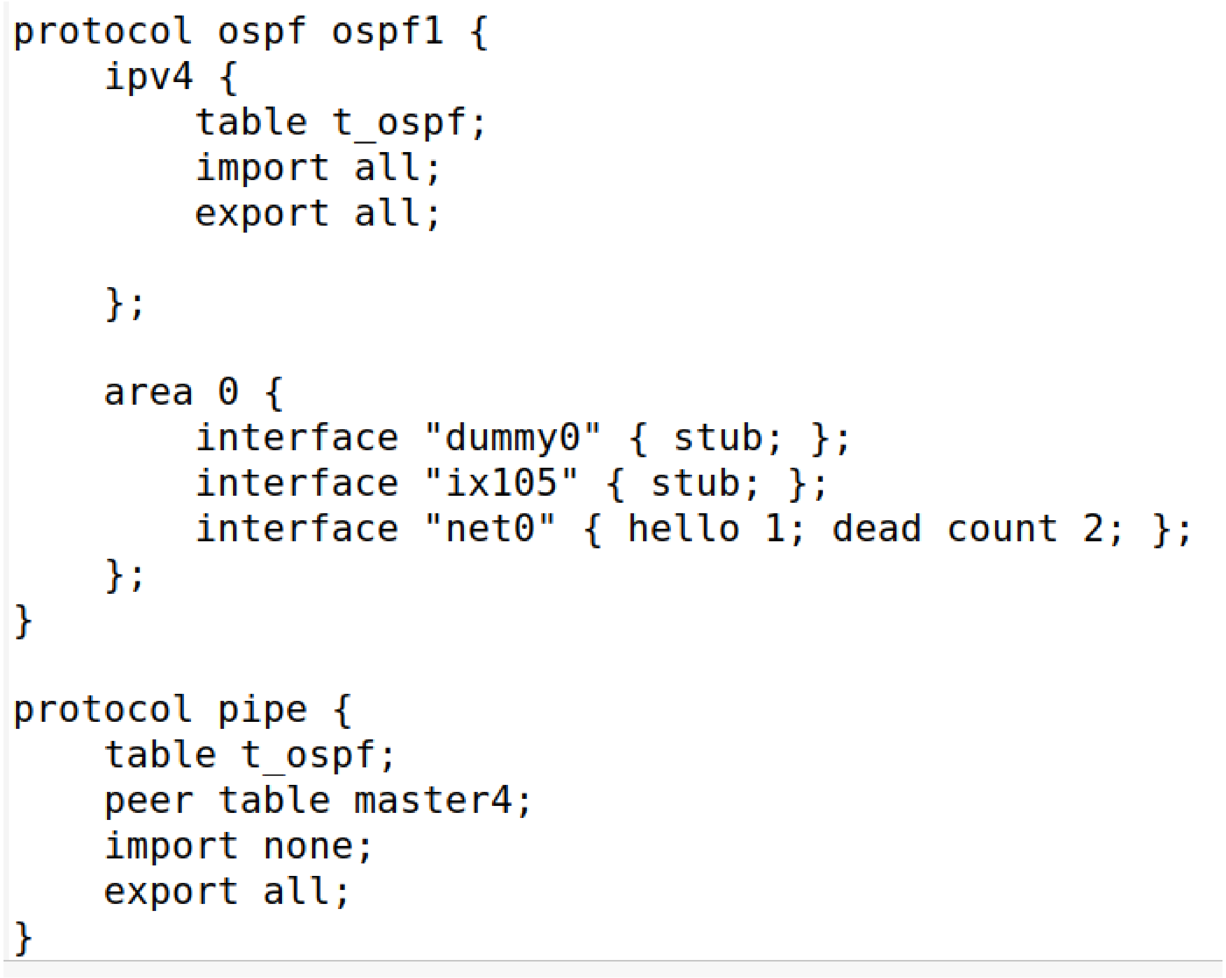
```
router id 10.0.0.33;
ipv4 table t_direct;
protocol device {
}

protocol kernel {
    ipv4 {
        import all;
        export all;
    };
    learn;
}

protocol direct local_nets {
    ipv4 {
        table t_direct;
        import all;
    };

    interface "net0";
}

define LOCAL_COMM = (180, 0, 0);
define CUSTOMER_COMM = (180, 1, 0);
define PEER_COMM = (180, 2, 0);
```



```
define CUSTOMER_COMM = (180, 1, 0);
define PEER_COMM = (180, 2, 0);
define PROVIDER_COMM = (180, 3, 0);
ipv4 table t_bgp;

protocol pipe {
        table t_bgp;
        peer table master4;
        import none;
        export all;
}

protocol pipe {
        table t_direct;
        peer table t_bgp;
        import none;
        export filter { bgp_large_community.add(LOCAL_COMM);
        bgp_local_pref = 40;
        accept;
        };
}
```

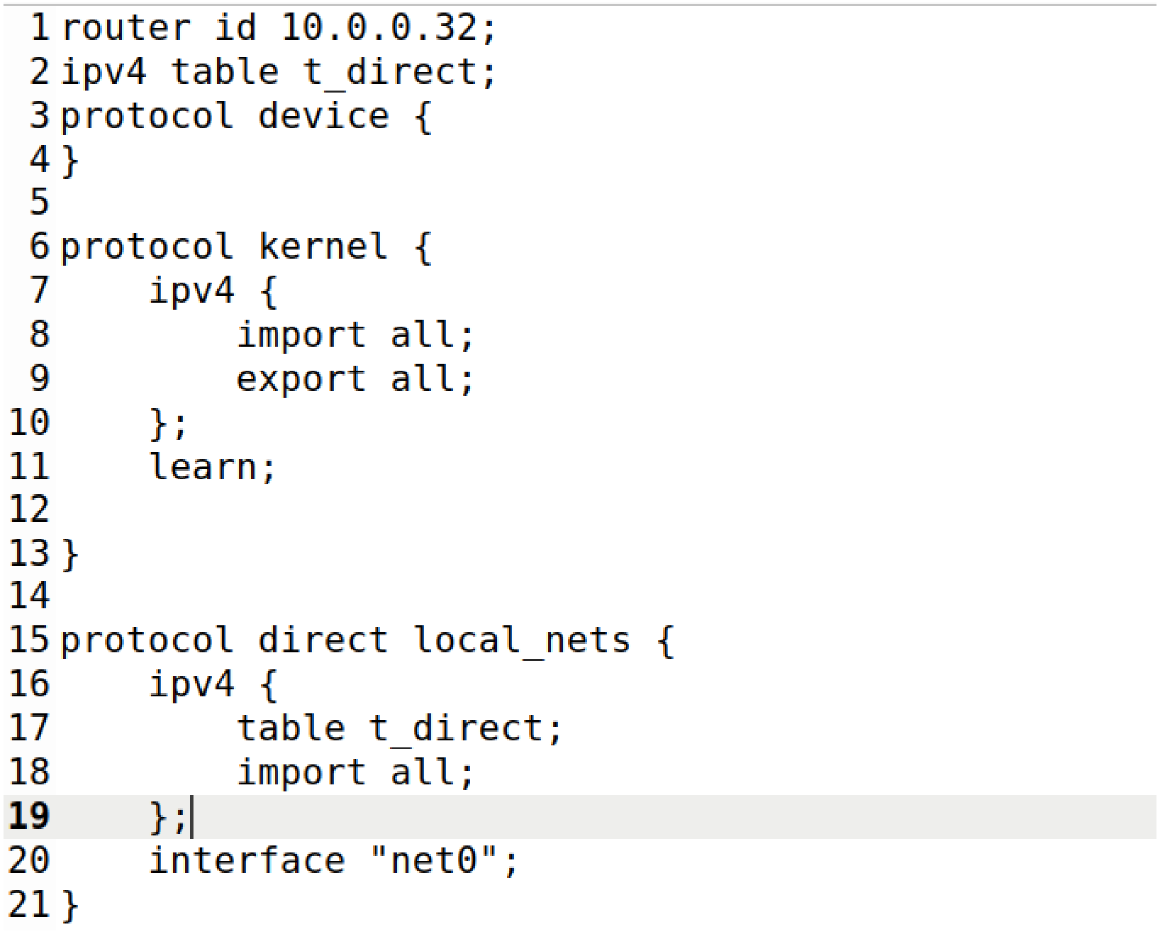


```
protocol bgp p_as171 {
        ipv4 {
                table t_bgp;
                import filter {
                        bgp_large_community.add(PEER_COMM);
                        bgp_local_pref = 20;
                        accept;
                };
                export where bgp_large_community ~ [LOCAL_COMM, CUSTOMER_COMM];
                next hop self;
        };
        local 10.105.0.180 as 180;
        neighbor 10.105.0.171 as 171;

}

ipv4 table t_ospf;

protocol ospf ospf1 {
    ipv4 {
        table t_ospf;
        import all;
        export all;
```

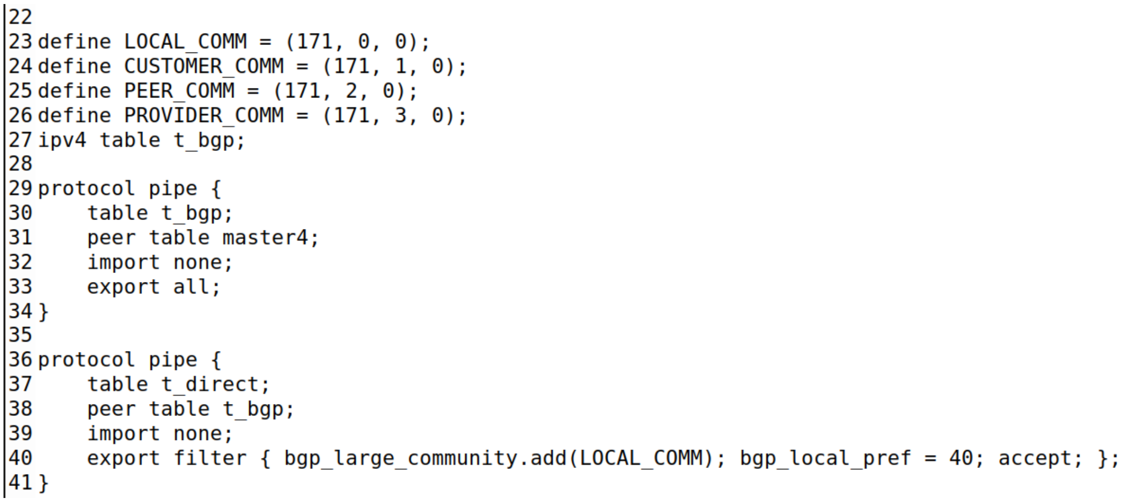


```
protocol ospf ospf1 {
    ipv4 {
        table t_ospf;
        import all;
        export all;

    };

    area 0 {
        interface "dummy0" { stub; };
        interface "ix105" { stub; };
        interface "net0" { hello 1; dead count 2; };
    };
}

protocol pipe {
    table t_ospf;
    peer table master4;
    import none;
    export all;
}
```

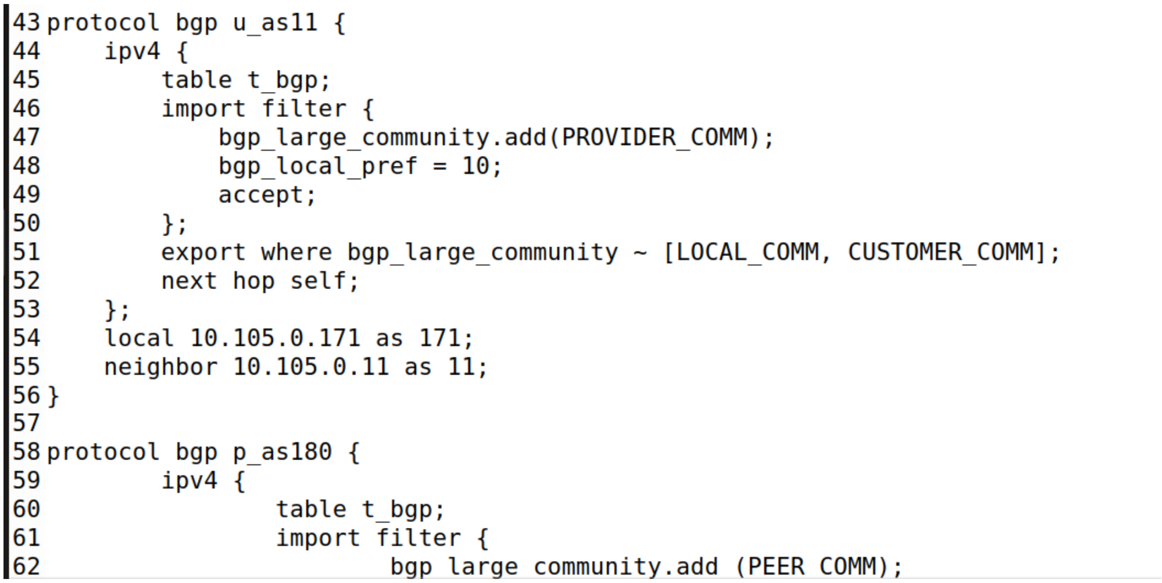
Edit the AS171 configuration file



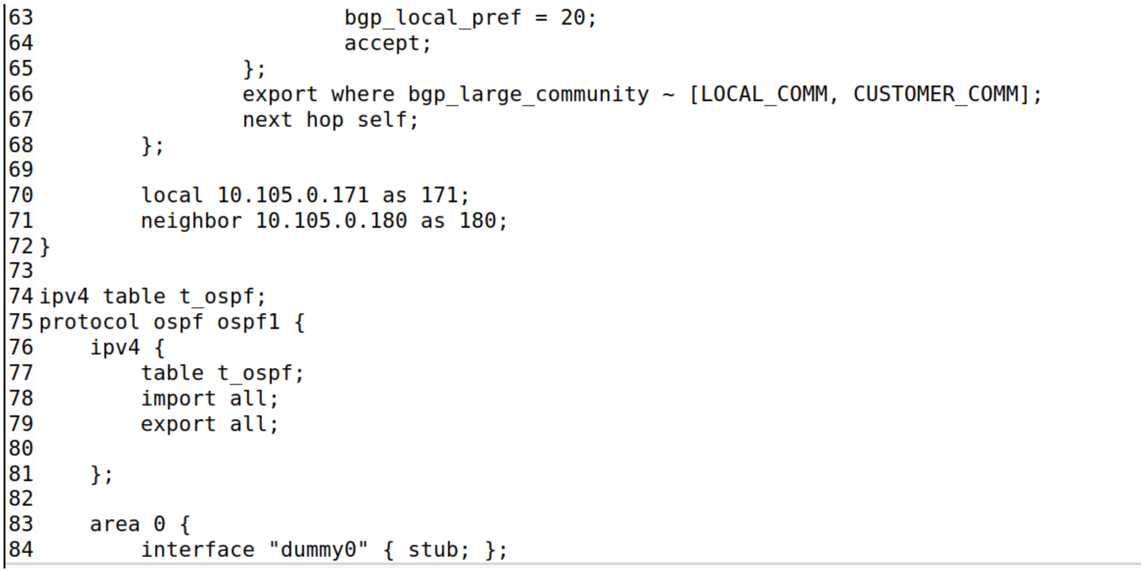
```
router id 10.0.0.32;
ipv4 table t_direct;
protocol device {
}

protocol kernel {
    ipv4 {
        import all;
        export all;
    };
    learn;

}

protocol direct local_nets {
    ipv4 {
        table t_direct;
        import all;
    };
    interface "net0";
}
```



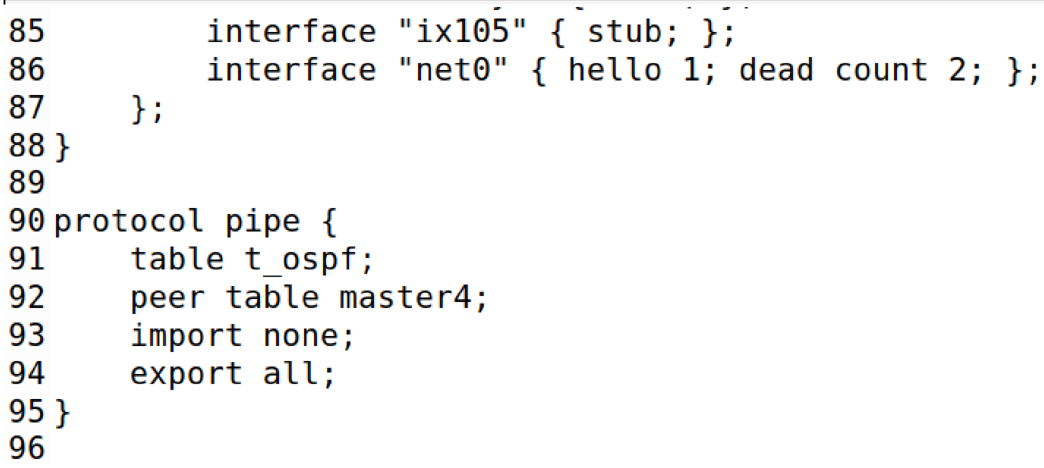
```

define LOCAL_COMM = (171, 0, 0);
define CUSTOMER_COMM = (171, 1, 0);
define PEER_COMM = (171, 2, 0);
define PROVIDER_COMM = (171, 3, 0);
ipv4 table t_bgp;

protocol pipe {
    table t_bgp;
    peer table master4;
    import none;
    export all;
}

protocol pipe {
    table t_direct;
    peer table t_bgp;
    import none;
    export filter { bgp_large_community.add(LOCAL_COMM); bgp_local_pref = 40; accept; };
}
```



```
protocol bgp u_as11 {
    ipv4 {
        table t_bgp;
        import filter {
            bgp_large_community.add(PROVIDER_COMM);
            bgp_local_pref = 10;
            accept;
        };
        export where bgp_large_community ~ [LOCAL_COMM, CUSTOMER_COMM];
        next hop self;
    };
    local 10.105.0.171 as 171;
    neighbor 10.105.0.11 as 11;
}

protocol bgp p_as180 {
        ipv4 {
                table t_bgp;
                import filter {
                        bgp_large_community.add (PEER_COMM);
```

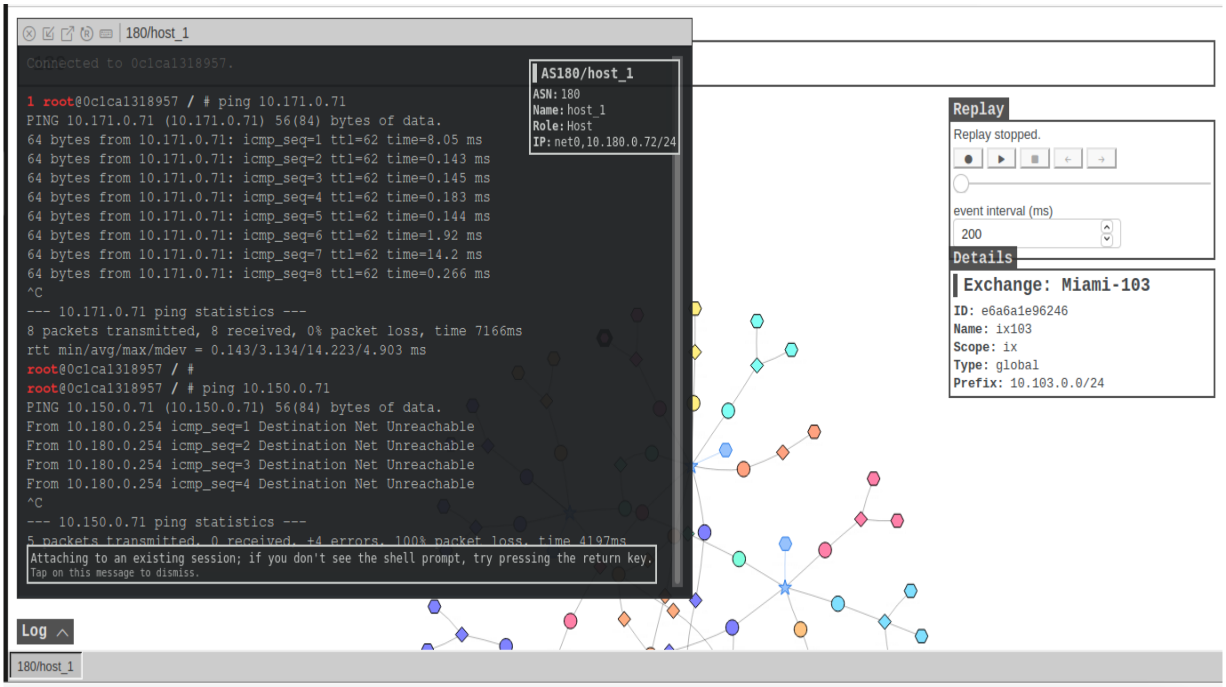


```
                        bgp_local_pref = 20;
                        accept;
                };
                export where bgp_large_community ~ [LOCAL_COMM, CUSTOMER_COMM];
                next hop self;
        };

        local 10.105.0.171 as 171;
        neighbor 10.105.0.180 as 180;
}

ipv4 table t_ospf;
protocol ospf ospf1 {
    ipv4 {
        table t_ospf;
        import all;
        export all;

    };

    area 0 {
        interface "dummy0" { stub; };
```



```
        interface "ix105" { stub; };
        interface "net0" { hello 1; dead count 2; };
    };
}

protocol pipe {
    table t_ospf;
    peer table master4;
    import none;
    export all;
}

```

Now ping 10.171.0.71 as shown below:



180/host_1

```
Connected to 0c1ca1318957.

1 root@0c1ca1318957 / # ping 10.171.0.71
PING 10.171.0.71 (10.171.0.71) 56(84) bytes of data.
64 bytes from 10.171.0.71: icmp_seq=1 ttl=62 time=8.05 ms
64 bytes from 10.171.0.71: icmp_seq=2 ttl=62 time=0.143 ms
64 bytes from 10.171.0.71: icmp_seq=3 ttl=62 time=0.145 ms
64 bytes from 10.171.0.71: icmp_seq=4 ttl=62 time=0.183 ms
64 bytes from 10.171.0.71: icmp_seq=5 ttl=62 time=0.144 ms
64 bytes from 10.171.0.71: icmp_seq=6 ttl=62 time=1.92 ms
64 bytes from 10.171.0.71: icmp_seq=7 ttl=62 time=14.2 ms
64 bytes from 10.171.0.71: icmp_seq=8 ttl=62 time=0.266 ms
^C
--- 10.171.0.71 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7166ms
rtt min/avg/max/mdev = 0.143/3.134/14.223/4.903 ms
root@0c1ca1318957 / #
root@0c1ca1318957 / # ping 10.150.0.71
PING 10.150.0.71 (10.150.0.71) 56(84) bytes of data.
From 10.180.0.254 icmp_seq=1 Destination Net Unreachable
From 10.180.0.254 icmp_seq=2 Destination Net Unreachable
From 10.180.0.254 icmp_seq=3 Destination Net Unreachable
From 10.180.0.254 icmp_seq=4 Destination Net Unreachable
^C
--- 10.150.0.71 ping statistics ---
5 packets transmitted, 0 received, +4 errors, 100% packet loss, time 4197ms
Attaching to an existing session; if you don't see the shell prompt, try pressing the return key.
Tap on this message to dismiss.
```

AS180/host_1
ASN: 180
Name: host_1
Role: Host
IP: net0,10.180.0.72/24

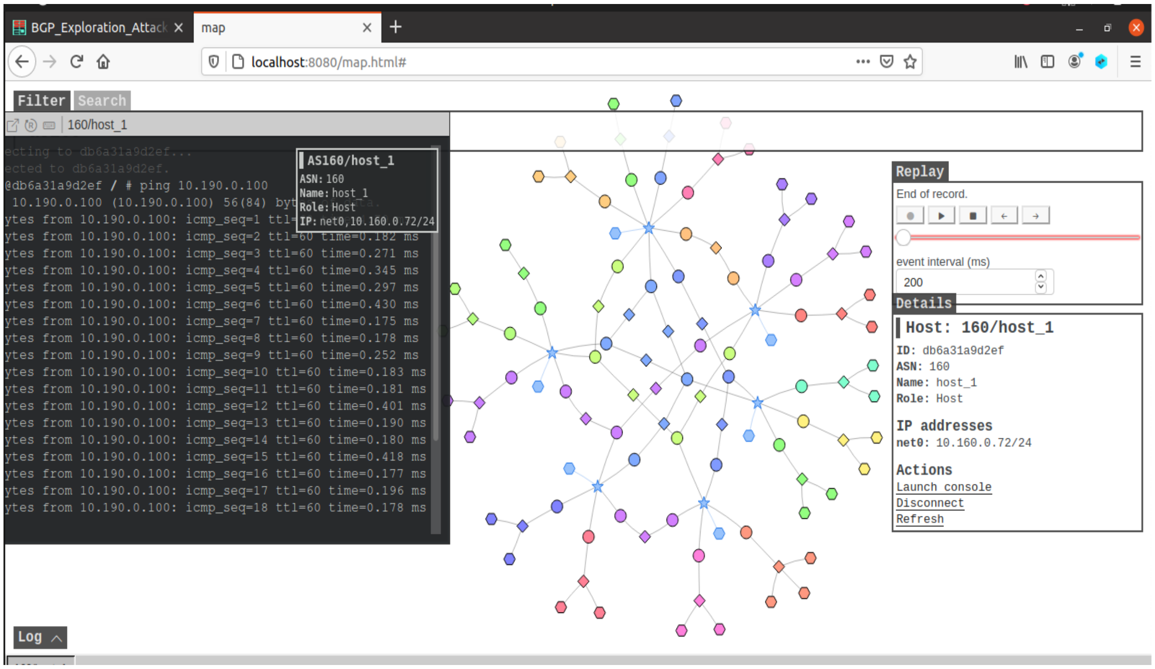
Replay
Replay stopped.
event interval (ms)
200

Details
Exchange: Miami-103
ID: e6a6a1e96246
Name: ix103
Scope: ix
Type: global
Prefix: 10.103.0.0/24

The ping is successful. Can ping host AS180 and AS171 successfully.

6 Task 4: IP Anycast:

Ping 10.190.0.100 on 10.160.0.72 as shown below:



```
ecting to db6a31a9d2ef...
ected to db6a31a9d2ef.
@db6a31a9d2ef / # ping 10.190.0.100
 10.190.0.100 (10.190.0.100) 56(84) bytes of data.
ytes from 10.190.0.100: icmp_seq=1 ttl=
ytes from 10.190.0.100: icmp_seq=2 ttl=60 time=0.182 ms
ytes from 10.190.0.100: icmp_seq=3 ttl=60 time=0.271 ms
ytes from 10.190.0.100: icmp_seq=4 ttl=60 time=0.345 ms
ytes from 10.190.0.100: icmp_seq=5 ttl=60 time=0.297 ms
ytes from 10.190.0.100: icmp_seq=6 ttl=60 time=0.430 ms
ytes from 10.190.0.100: icmp_seq=7 ttl=60 time=0.175 ms
ytes from 10.190.0.100: icmp_seq=8 ttl=60 time=0.178 ms
ytes from 10.190.0.100: icmp_seq=9 ttl=60 time=0.252 ms
ytes from 10.190.0.100: icmp_seq=10 ttl=60 time=0.183 ms
ytes from 10.190.0.100: icmp_seq=11 ttl=60 time=0.181 ms
ytes from 10.190.0.100: icmp_seq=12 ttl=60 time=0.401 ms
ytes from 10.190.0.100: icmp_seq=13 ttl=60 time=0.190 ms
ytes from 10.190.0.100: icmp_seq=14 ttl=60 time=0.180 ms
ytes from 10.190.0.100: icmp_seq=15 ttl=60 time=0.418 ms
ytes from 10.190.0.100: icmp_seq=16 ttl=60 time=0.177 ms
ytes from 10.190.0.100: icmp_seq=17 ttl=60 time=0.196 ms
ytes from 10.190.0.100: icmp_seq=18 ttl=60 time=0.178 ms
```

AS160/host_1
ASN: 160
Name: host_1
Role: Host
IP: net0,10.160.0.72/24

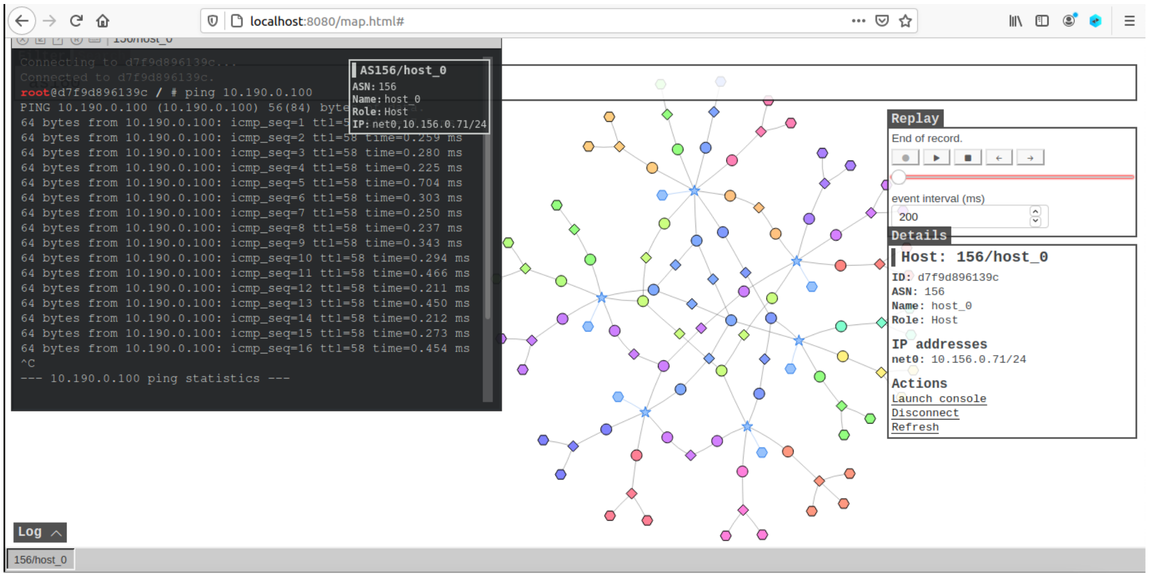
Replay
End of record.
event interval (ms)
200

Details
Host: 160/host_1
ID: db6a31a9d2ef
ASN: 160
Name: host_1
Role: Host

IP addresses
net0: 10.160.0.72/24

Actions
Launch console
Disconnect
Refresh

Now ping 10.190.0.100 on 10.156.0.71 as shown below:



```
Connecting to d7f9d896139c...
Connected to d7f9d896139c.
root@d7f9d896139c / # ping 10.190.0.100
PING 10.190.0.100 (10.190.0.100) 56(84) byte
64 bytes from 10.190.0.100: icmp_seq=1 ttl=5
64 bytes from 10.190.0.100: icmp_seq=2 ttl=58 time=0.259 ms
64 bytes from 10.190.0.100: icmp_seq=3 ttl=58 time=0.280 ms
64 bytes from 10.190.0.100: icmp_seq=4 ttl=58 time=0.225 ms
64 bytes from 10.190.0.100: icmp_seq=5 ttl=58 time=0.704 ms
64 bytes from 10.190.0.100: icmp_seq=6 ttl=58 time=0.303 ms
64 bytes from 10.190.0.100: icmp_seq=7 ttl=58 time=0.250 ms
64 bytes from 10.190.0.100: icmp_seq=8 ttl=58 time=0.237 ms
64 bytes from 10.190.0.100: icmp_seq=9 ttl=58 time=0.343 ms
64 bytes from 10.190.0.100: icmp_seq=10 ttl=58 time=0.294 ms
64 bytes from 10.190.0.100: icmp_seq=11 ttl=58 time=0.466 ms
64 bytes from 10.190.0.100: icmp_seq=12 ttl=58 time=0.211 ms
64 bytes from 10.190.0.100: icmp_seq=13 ttl=58 time=0.450 ms
64 bytes from 10.190.0.100: icmp_seq=14 ttl=58 time=0.212 ms
64 bytes from 10.190.0.100: icmp_seq=15 ttl=58 time=0.273 ms
64 bytes from 10.190.0.100: icmp_seq=16 ttl=58 time=0.454 ms
^C
--- 10.190.0.100 ping statistics ---
```

AS156/host_0
ASN: 156
Name: host_0
Role: Host
IP: net0,10.156.0.71/24

End of record.

event interval (ms) 200

Host: 156/host_0
ID: d7f9d896139c
ASN: 156
Name: host_0
Role: Host

IP addresses
net0: 10.156.0.71/24

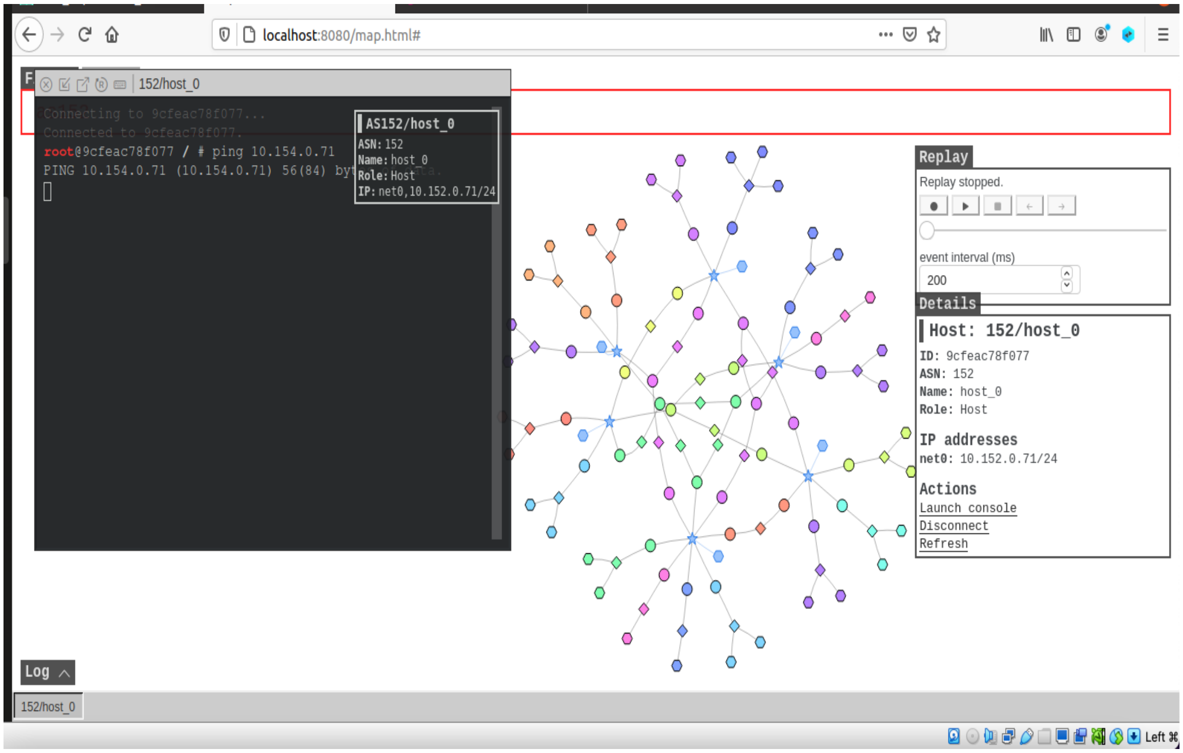
Actions
Launch console
Disconnect
Refresh

We can see that the ICMP packets of the two hosts have been sent to different destination hosts as shown in the above screenshots.

7.1 Task 5.a. Launching the Prefix Hijacking Attack from AS-161:

Modify the configuration information of AS-161 so that all traffic destined for AS-154 is forwarded to AS-161.

The subnet in the configuration needs to cover the entire 10.154.0.0/24:



```
Connecting to 9cfeac78f077...
Connected to 9cfeac78f077.
root@9cfeac78f077 / # ping 10.154.0.71
PING 10.154.0.71 (10.154.0.71) 56(84) bytes of data.
```

AS152/host_0
ASN: 152
Name: host_0
Role: Host
IP: net0,10.152.0.71/24

Replay stopped.

event interval (ms): 200

Details

Host: 152/host_0
ID: 9cfeac78f077
ASN: 152
Name: host_0
Role: Host

IP addresses
net0: 10.152.0.71/24

Actions
Launch console
Disconnect
Refresh

```
protocol static hijacks{
        ipv4 {
                table t_bgp;
        };
        route 10.154.0.0/25 blackhole{
                bgp_large_community.add(LOCAL_COMM);
        };
        route 10.154.0.128/25 blackhole{
                bgp_large_community.add(LOCAL_COMM);
        };
}
```

6.2 Task 5. b. Fighting Back from AS-154:

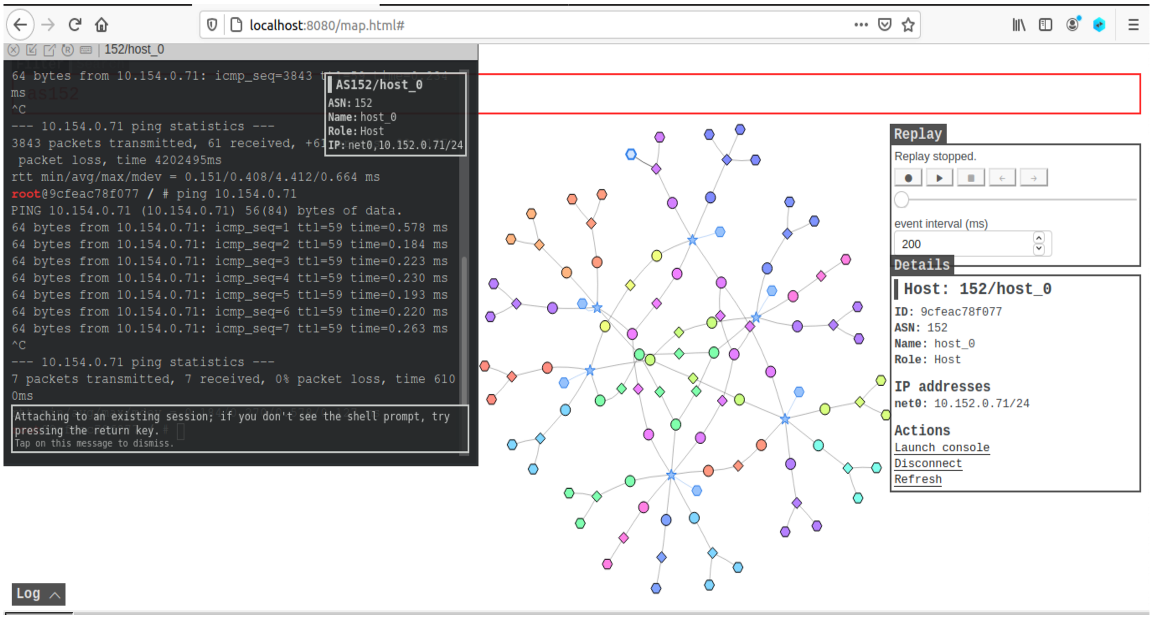
Modify the AS-154 configuration so it gets its own traffic:

Change the routing and add extra bits at the end

```
protocol static {
        ipv4 {
        table t_bgp;
        };

        route 10.154.0.0/26 via "net0"{
                bgp_large_community.add(LOCAL_COMM);
        };

        route 10.154.0.64/26 via "net0"{
                bgp_large_community.add(LOCAL_COMM);
        };

        route 10.154.0.128/26 via "net0"{
                bgp_large_community.add(LOCAL_COMM);
        };

        route 10.154.0.192/26 via "net0"{
                bgp_large_community.add(LOCAL_COMM);
        };
}
```

Ping 10.154.0.71 from 10.152.0.71/24.

Fighting back to make sure packets are sent to the right destination



```
64 bytes from 10.154.0.71: icmp_seq=3843 t
ms
^C
--- 10.154.0.71 ping statistics ---
3843 packets transmitted, 61 received, +61
 packet loss, time 4202495ms
rtt min/avg/max/mdev = 0.151/0.408/4.412/0.664 ms
root@9cfeac78f077 / # ping 10.154.0.71
PING 10.154.0.71 (10.154.0.71) 56(84) bytes of data.
64 bytes from 10.154.0.71: icmp_seq=1 ttl=59 time=0.578 ms
64 bytes from 10.154.0.71: icmp_seq=2 ttl=59 time=0.184 ms
64 bytes from 10.154.0.71: icmp_seq=3 ttl=59 time=0.223 ms
64 bytes from 10.154.0.71: icmp_seq=4 ttl=59 time=0.230 ms
64 bytes from 10.154.0.71: icmp_seq=5 ttl=59 time=0.193 ms
64 bytes from 10.154.0.71: icmp_seq=6 ttl=59 time=0.220 ms
64 bytes from 10.154.0.71: icmp_seq=7 ttl=59 time=0.263 ms
^C
--- 10.154.0.71 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 610
0ms
Attaching to an existing session; if you don't see the shell prompt, try
pressing the return key.
Tap on this message to dismiss.
```

AS152/host_0
ASN: 152
Name: host_0
Role: Host
IP: net0,10.152.0.71/24

Replay stopped.

event interval (ms): 200

Host: 152/host_0
ID: 9cfeac78f077
ASN: 152
Name: host_0
Role: Host

IP addresses
net0: 10.152.0.71/24

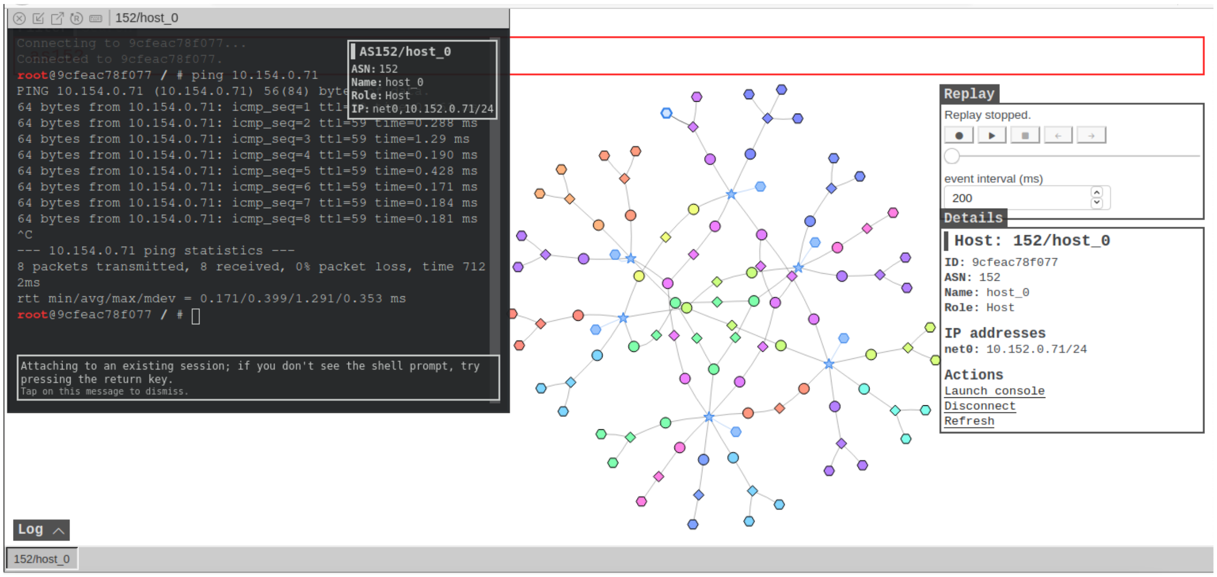
Actions
Launch console
Disconnect
Refresh

6.3 Task 5. c. Fixing the Problem at AS-3:

AS-3 is the only provider of AS-161, AS-3 can modify its own configuration and fix wrong routing:

```
protocol bgp u_as3 {
    ipv4 {
        table t_bgp;
        import filter {
            bgp_large_community.add(CUSTOMER_COMM);
            bgp_local_pref = 30;

            if(net != 10.103.0.0/24) then reject;
            accept;
        };
        export all;
        next hop self;
    };
    local 10.103.0.3 as 3;
    neighbor 10.103.0.161 as 161;
}
```

The configuration of AS-154 rolled back to the previous state, and it can be found that the traffic is still sent to AS-154 correctly:



```
Connecting to 9cfeac78f077...
Connected to 9cfeac78f077.
root@9cfeac78f077 / # ping 10.154.0.71
PING 10.154.0.71 (10.154.0.71) 56(84) byte
64 bytes from 10.154.0.71: icmp_seq=1 ttl=
64 bytes from 10.154.0.71: icmp_seq=2 ttl=59 time=0.288 ms
64 bytes from 10.154.0.71: icmp_seq=3 ttl=59 time=1.29 ms
64 bytes from 10.154.0.71: icmp_seq=4 ttl=59 time=0.190 ms
64 bytes from 10.154.0.71: icmp_seq=5 ttl=59 time=0.428 ms
64 bytes from 10.154.0.71: icmp_seq=6 ttl=59 time=0.171 ms
64 bytes from 10.154.0.71: icmp_seq=7 ttl=59 time=0.184 ms
64 bytes from 10.154.0.71: icmp_seq=8 ttl=59 time=0.181 ms
^C
--- 10.154.0.71 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 712
2ms
rtt min/avg/max/mdev = 0.171/0.399/1.291/0.353 ms
root@9cfeac78f077 / #
```

```
AS152/host_0
ASN: 152
Name: host_0
Role: Host
IP: net0,10.152.0.71/24
```

```
Attaching to an existing session; if you don't see the shell prompt, try
pressing the return key.
Tap on this message to dismiss.
```

Replay stopped.

event interval (ms): 200

Details

Host: 152/host_0

ID: 9cfeac78f077
ASN: 152
Name: host_0
Role: Host

IP addresses

net0: 10.152.0.71/24

Actions

Launch console
Disconnect
Refresh