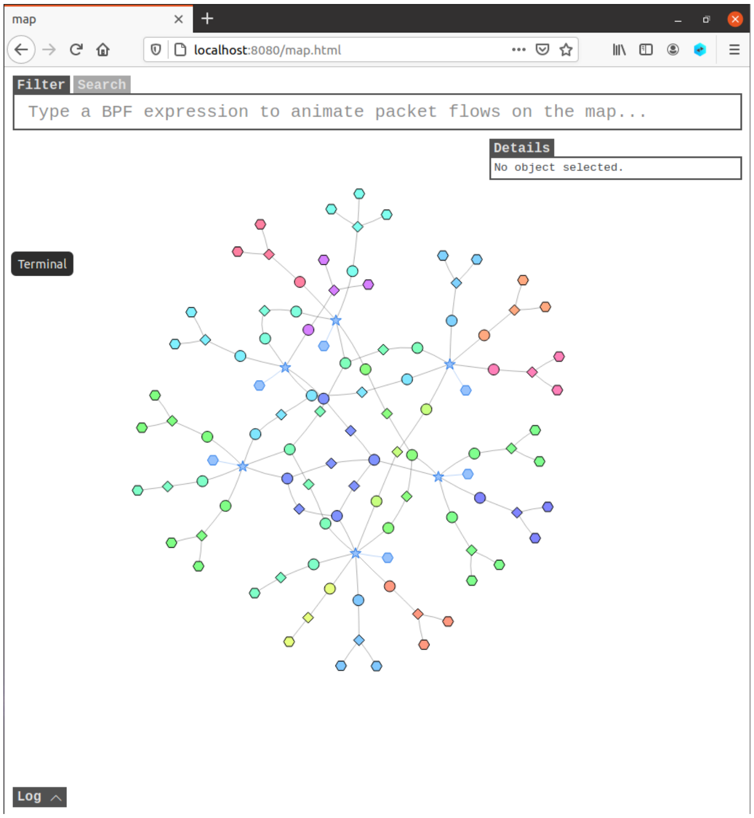
Leonardo Blas

BGP Exploration and Attack Lab

The Border Gateway Protocol (BGP) is the standard exterior protocol to exchange routing and reachability information among autonomous systems (AS) on the Internet. It is also called the “glue” of the Internet. On a similar note, the internet connects autonomous systems together, but routing protocols dictate the paths packets take.

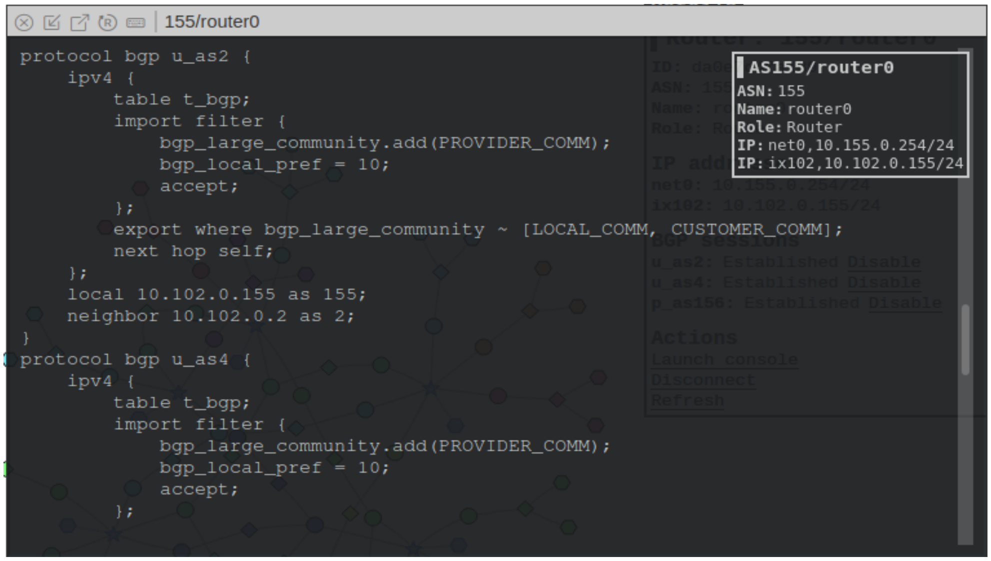
In this lab, we cover the most common and severe BGP attack, BGP hijacking. This attack can hijack a network prefix, causing the traffic to the target prefix to be rerouted, and eventually dropped. In this lab, this is covered through a “blackhole” functionality. Furthermore, this type of attack is very common. Additionally, this lab teaches how to defend from this attack and regain the stolen packets back. We do this by creating two prefixes for every prefix attacked, in this case 10.154.0.0/24, and creating these prefixes such that they are a bit longer, in this case 25 instead of 24.

Setup



In this image, we see the network we will be working with.

Task 1.a.1

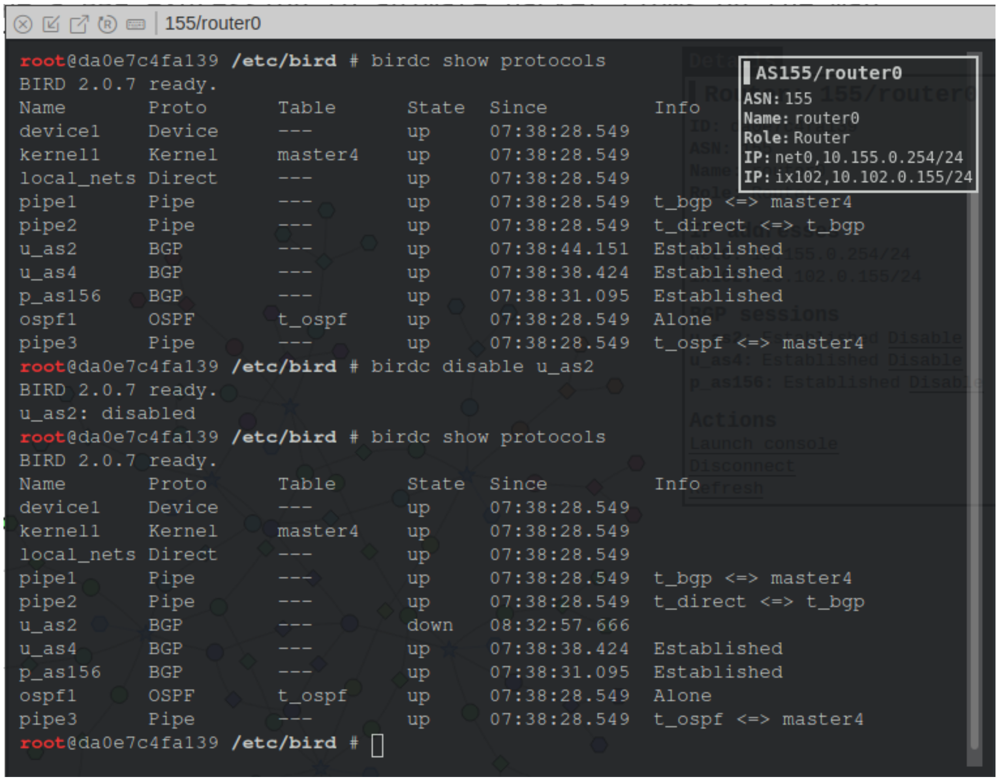


```
protocol bgp u_as2 {
    ipv4 {
        table t_bgp;
        import filter {
            bgp_large_community.add(PROVIDER_COMM);
            bgp_local_pref = 10;
            accept;
        };
        export where bgp_large_community ~ [LOCAL_COMM, CUSTOMER_COMM];
        next hop self;
    };
    local 10.102.0.155 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;
        };
```

AS155/router0
ASN: 155
Name: router0
Role: Router
IP: net0,10.155.0.254/24
IP: ix102,10.102.0.155/24

In this snippet, we identify AS-155's peers, AS-2 and AS-4.

Task 1.a.2

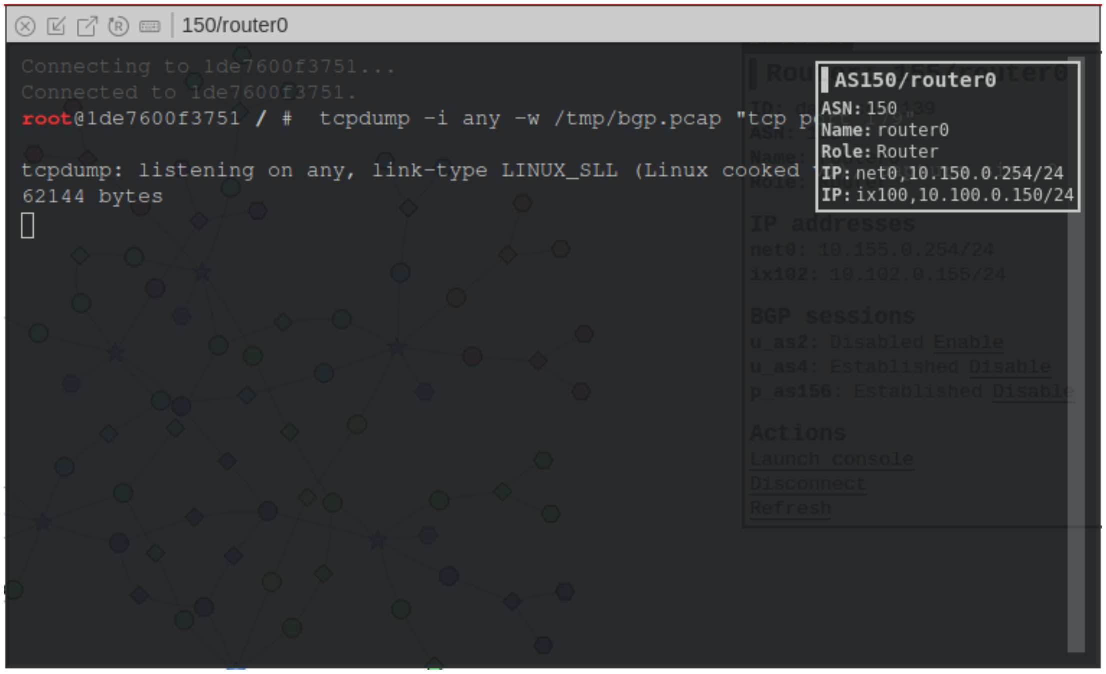


```
root@da0e7c4fa139 /etc/bird # birdc show protocols
BIRD 2.0.7 ready.
Name       Proto      Table      State  Since         Info
device1    Device     ---        up     07:38:28.549
kernel1    Kernel     master4    up     07:38:28.549
local_nets Direct     ---        up     07:38:28.549
pipe1      Pipe       ---        up     07:38:28.549  t_bgp <=> master4
pipe2      Pipe       ---        up     07:38:28.549  t_direct <=> t_bgp
u_as2      BGP        ---        up     07:38:44.151  Established
u_as4      BGP        ---        up     07:38:38.424  Established
p_as156    BGP        ---        up     07:38:31.095  Established
ospf1      OSPF       t_ospf     up     07:38:28.549  Alone
pipe3      Pipe       ---        up     07:38:28.549  t_ospf <=> master4
root@da0e7c4fa139 /etc/bird # birdc disable u_as2
BIRD 2.0.7 ready.
u_as2: disabled
root@da0e7c4fa139 /etc/bird # birdc show protocols
BIRD 2.0.7 ready.
Name       Proto      Table      State  Since         Info
device1    Device     ---        up     07:38:28.549
kernel1    Kernel     master4    up     07:38:28.549
local_nets Direct     ---        up     07:38:28.549
pipe1      Pipe       ---        up     07:38:28.549  t_bgp <=> master4
pipe2      Pipe       ---        up     07:38:28.549  t_direct <=> t_bgp
u_as2      BGP        ---        down   08:32:57.666
u_as4      BGP        ---        up     07:38:38.424  Established
p_as156    BGP        ---        up     07:38:31.095  Established
ospf1      OSPF       t_ospf     up     07:38:28.549  Alone
pipe3      Pipe       ---        up     07:38:28.549  t_ospf <=> master4
root@da0e7c4fa139 /etc/bird # 
```

AS155/router0
ASN: 155
Name: router0
Role: Router
IP: net0,10.155.0.254/24
IP: ix102,10.102.0.155/24

In this snippet, we disable AS-2 as AS-155's peer.

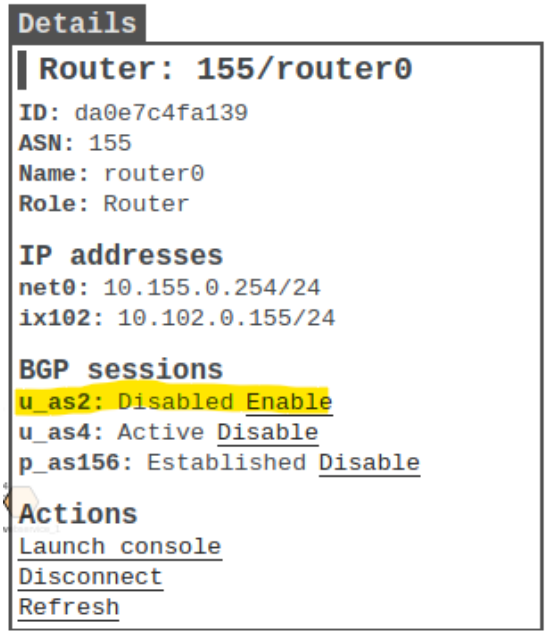
Task 1.b



```
Connecting to 1de7600f3751...
Connected to 1de7600f3751.
root@1de7600f3751 / #  tcpdump -i any -w /tmp/bgp.pcap "tcp p

tcpdump: listening on any, link-type LINUX_SLL (Linux cooked 
62144 bytes
```

AS150/router0
ASN: 150
Name: router0
Role: Router
IP: net0,10.150.0.254/24
IP: ix100,10.100.0.150/24

In this snippet, we listen on AS-150's router.



Details

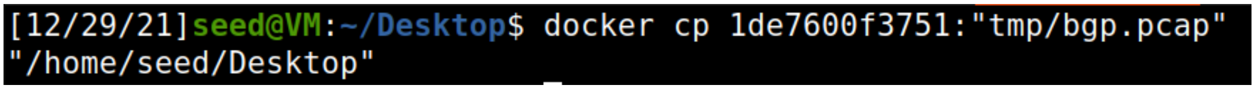
Router: 155/router0
ID: da0e7c4fa139
ASN: 155
Name: router0
Role: Router

IP addresses
net0: 10.155.0.254/24
ix102: 10.102.0.155/24

BGP sessions
u_as2: Disabled Enable
u_as4: Active Disable
p_as156: Established Disable

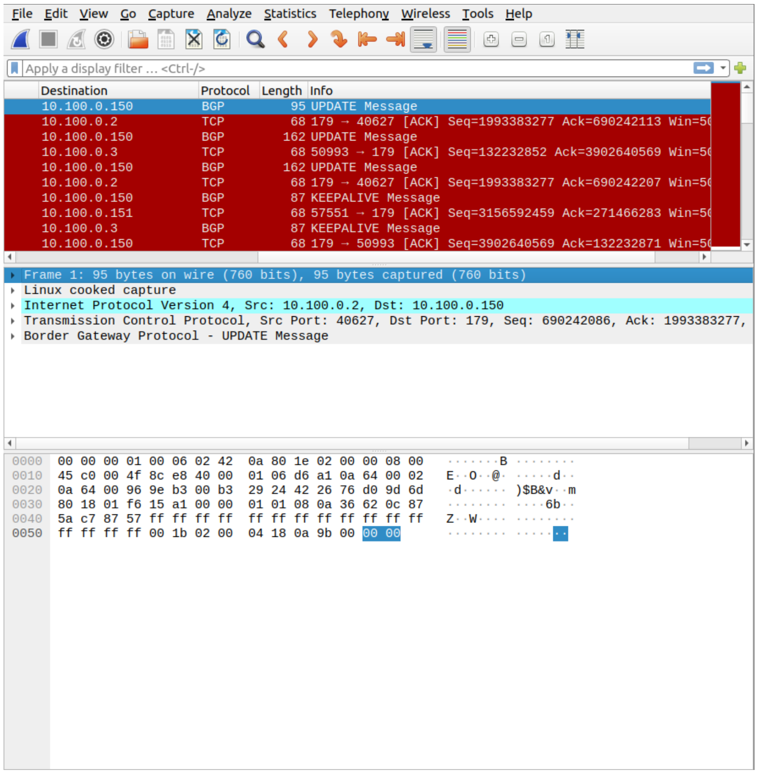
Actions

In this snippet, we try to trigger changes on AS-150 altering AS-155's connection with AS-2.



```
[12/29/21]seed@VM:~/Desktop$ docker cp 1de7600f3751:"tmp/bgp.pcap"
"/home/seed/Desktop"
```

In this snippet, we export the packets we sniffed from AS-150's router as a pcap file.

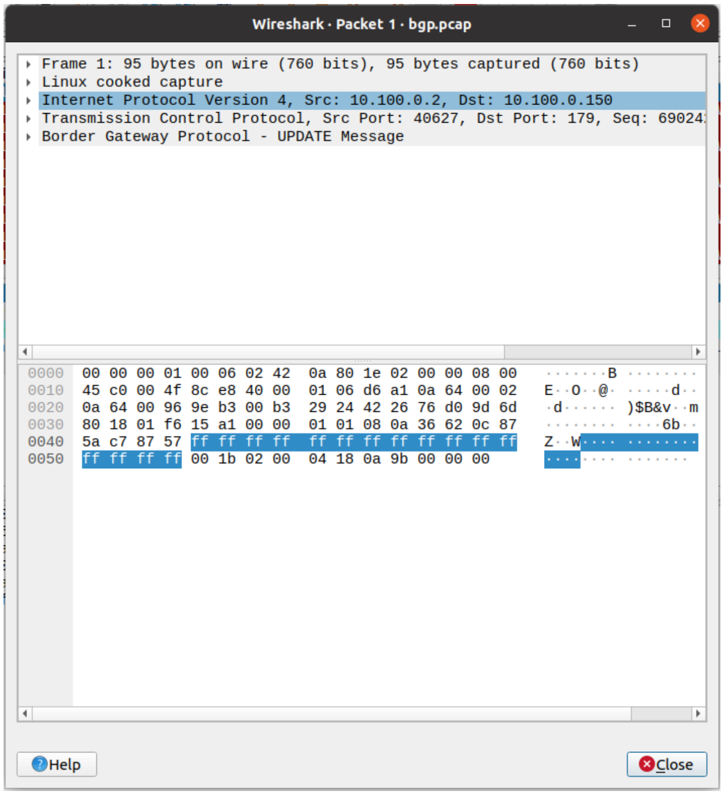

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
Destination     Protocol  Length  Info
10.100.0.150    BGP           95  UPDATE Message
10.100.0.2      TCP           68  179 → 40627 [ACK] Seq=1993383277 Ack=690242113 Win=5(
10.100.0.150    BGP          162  UPDATE Message
10.100.0.3      TCP           68  50993 → 179 [ACK] Seq=132232852 Ack=3902640569 Win=5(
10.100.0.150    BGP          162  UPDATE Message
10.100.0.2      TCP           68  179 → 40627 [ACK] Seq=1993383277 Ack=690242207 Win=5(
10.100.0.150    BGP           87  KEEPALIVE Message
10.100.0.151    TCP           68  57551 → 179 [ACK] Seq=3156592459 Ack=271466283 Win=5(
10.100.0.3      BGP           87  KEEPALIVE Message
10.100.0.150    TCP           68  179 → 50993 [ACK] Seq=3902640569 Ack=132232871 Win=5(
```

```
› Frame 1: 95 bytes on wire (760 bits), 95 bytes captured (760 bits)
› Linux cooked capture
› Internet Protocol Version 4, Src: 10.100.0.2, Dst: 10.100.0.150
› Transmission Control Protocol, Src Port: 40627, Dst Port: 179, Seq: 690242086, Ack: 1993383277,
› Border Gateway Protocol - UPDATE Message
```

```
0000  00 00 00 01 00 06 02 42  0a 80 1e 02 00 00 08 00   ·······B ········
0010  45 c0 00 4f 8c e8 40 00  01 06 d6 a1 0a 64 00 02   E··O··@· ·····d··
0020  0a 64 00 96 9e b3 00 b3  29 24 42 26 76 d0 9d 6d   ·d······ )$B&v··m
0030  80 18 01 f6 15 a1 00 00  01 01 08 0a 36 62 0c 87   ········ ····6b··
0040  5a c7 87 57 ff ff ff ff  ff ff ff ff ff ff ff ff   Z··W···· ········
0050  ff ff ff ff 00 1b 02 00  04 18 0a 9b 00 00 00      ········ ·······
```

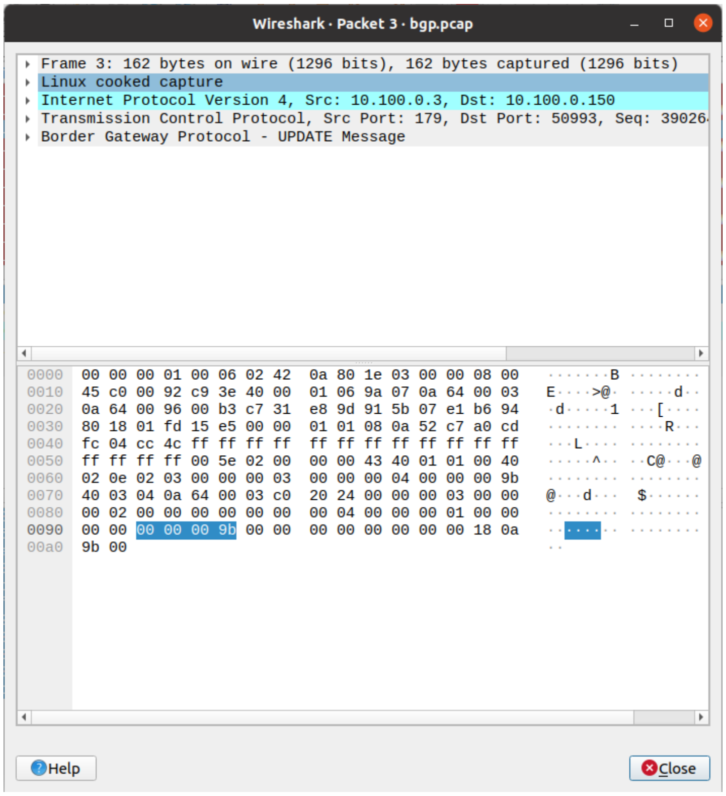
In this snippet, we import the pcap file into Wireshark.



```
› Frame 1: 95 bytes on wire (760 bits), 95 bytes captured (760 bits)
› Linux cooked capture
› Internet Protocol Version 4, Src: 10.100.0.2, Dst: 10.100.0.150
› Transmission Control Protocol, Src Port: 40627, Dst Port: 179, Seq: 69024
› Border Gateway Protocol - UPDATE Message
```

```
0000  00 00 00 01 00 06 02 42  0a 80 1e 02 00 00 08 00   ·······B ········
0010  45 c0 00 4f 8c e8 40 00  01 06 d6 a1 0a 64 00 02   E··O··@· ·····d··
0020  0a 64 00 96 9e b3 00 b3  29 24 42 26 76 d0 9d 6d   ·d······ )$B&v··m
0030  80 18 01 f6 15 a1 00 00  01 01 08 0a 36 62 0c 87   ········ ····6b··
0040  5a c7 87 57 ff ff ff ff  ff ff ff ff ff ff ff ff   Z··W···· ········
0050  ff ff ff ff 00 1b 02 00  04 18 0a 9b 00 00 00      ········ ·······
```

In this snippet, we appreciate a route advertisement message after deactivating AS-2 in AS-155.

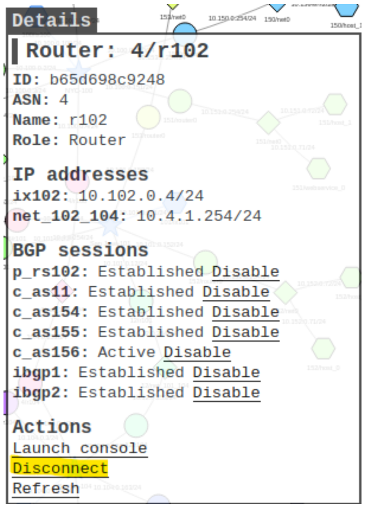


```
▸ Frame 3: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits)
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 10.100.0.3, Dst: 10.100.0.150
▸ Transmission Control Protocol, Src Port: 179, Dst Port: 50993, Seq: 39026
▸ Border Gateway Protocol - UPDATE Message
```

```
0000  00 00 00 01 00 06 02 42  0a 80 1e 03 00 00 08 00   ·······B ········
0010  45 c0 00 92 c9 3e 40 00  01 06 9a 07 0a 64 00 03   E····>@· ·····d··
0020  0a 64 00 96 00 b3 c7 31  e8 9d 91 5b 07 e1 b6 94   ·d·····1 ···[····
0030  80 18 01 fd 15 e5 00 00  01 01 08 0a 52 c7 a0 cd   ········ ····R···
0040  fc 04 cc 4c ff ff ff ff  ff ff ff ff ff ff ff ff   ···L···· ········
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   ········ ········
0070  40 03 04 0a 64 00 03 c0  20 24 00 00 00 03 00 00   @···d···  $······
0080  00 02 00 00 00 00 00 00  00 04 00 00 00 01 00 00   ········ ········
0090  00 00 00 00 00 9b 00 00  00 00 00 00 00 00 18 0a   ········ ········
00a0  9b 00                                              ··
```

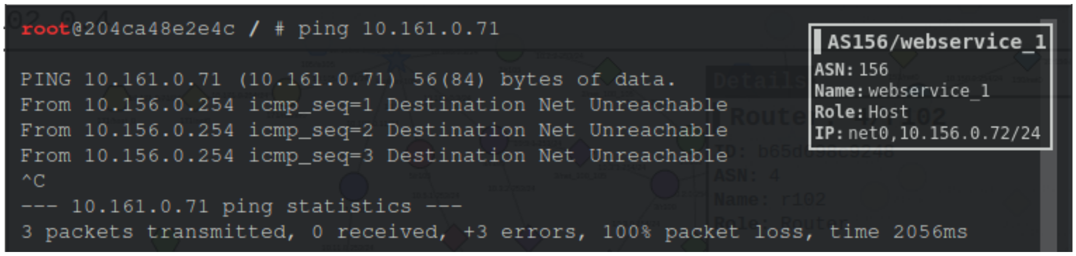
In this snippet, we appreciate a route withdrawal message after deactivating AS-2 in AS-155.

Task 1.c



```
Details
Router: 4/r102
ID: b65d698c9248
ASN: 4
Name: r102
Role: Router

IP addresses
ix102: 10.102.0.4/24
net_102_104: 10.4.1.254/24

BGP sessions
p_rs102: Established Disable
c_as11: Established Disable
c_as154: Established Disable
c_as155: Established Disable
c_as156: Active Disable
ibgp1: Established Disable
ibgp2: Established Disable

Actions
Launch console
Disconnect
Refresh
```

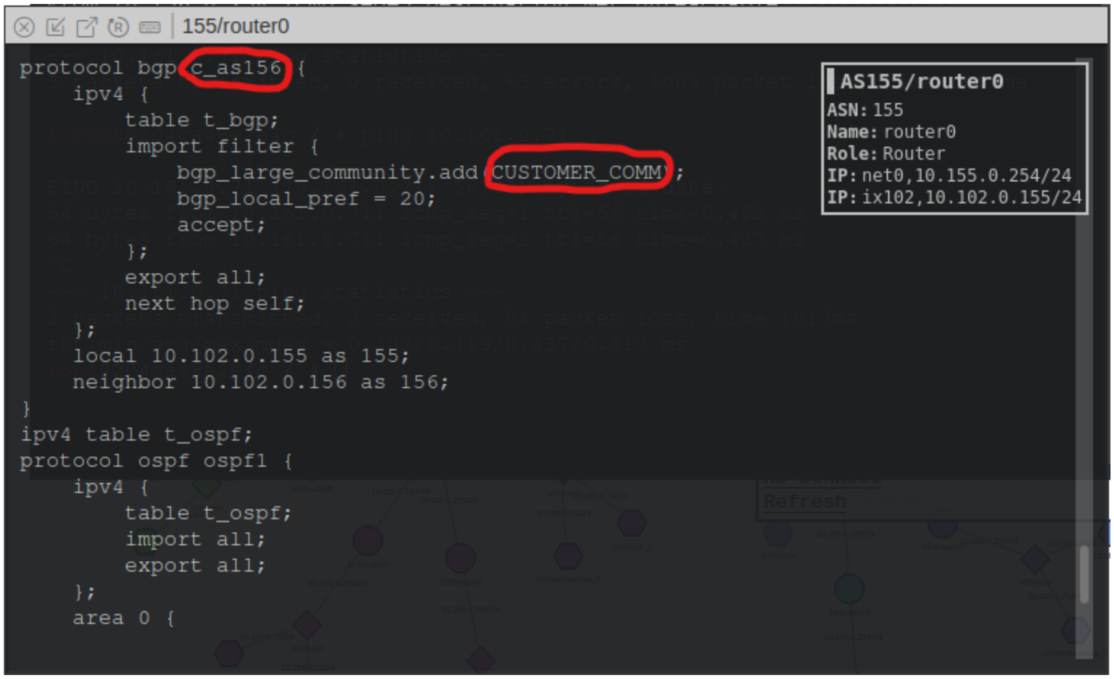
In this snippet, we disable AS-4’s router.



```
root@204ca48e2e4c / # 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
^C
--- 10.161.0.71 ping statistics ---
3 packets transmitted, 0 received, +3 errors, 100% packet loss, time 2056ms
```

AS156/webservice_1
ASN: 156
Name: webservice_1
Role: Host
IP: net0,10.156.0.72/24

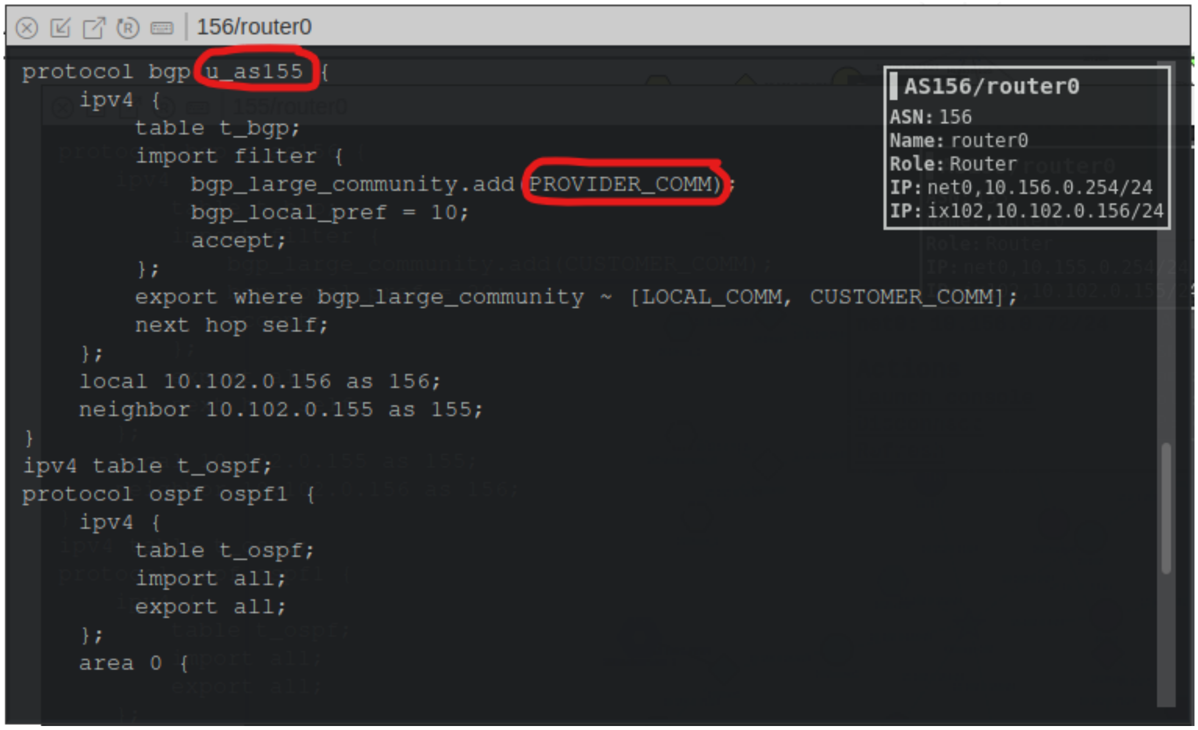
In this snippet, we test the connectivity in AS-156. We see it is unreachable.



```
protocol bgp c_as156 {
    ipv4 {
        table t_bgp;
        import filter {
            bgp_large_community.add(CUSTOMER_COMM);
            bgp_local_pref = 20;
            accept;
        };
        export all;
        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 {
```

AS155/router0
ASN: 155
Name: router0
Role: Router
IP: net0,10.155.0.254/24
IP: ix102,10.102.0.155/24

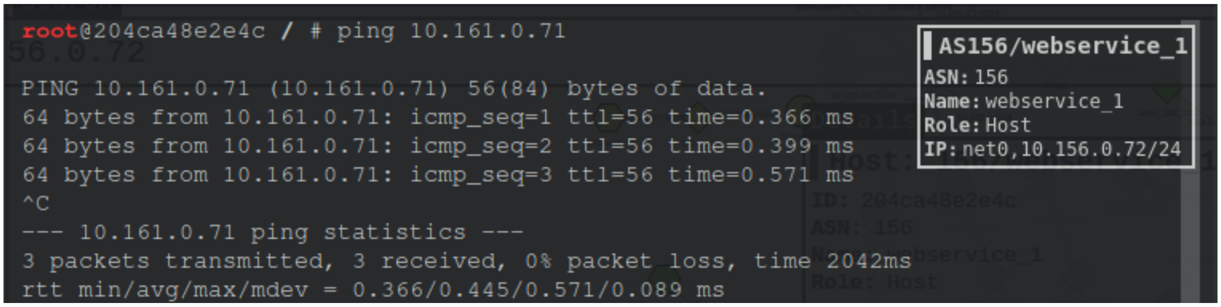
In this snippet, we make AS-156 a customer of AS-155.



```
protocol bgp u_as155 {
    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 10.102.0.156 as 156;
    neighbor 10.102.0.155 as 155;
}
ipv4 table t_ospf;
protocol ospf ospf1 {
    ipv4 {
        table t_ospf;
        import all;
        export all;
    };
    area 0 {
```

AS156/router0
ASN: 156
Name: router0
Role: Router
IP: net0,10.156.0.254/24
IP: ix102,10.102.0.156/24

In this snippet, we make AS-155 a provider of AS-156.

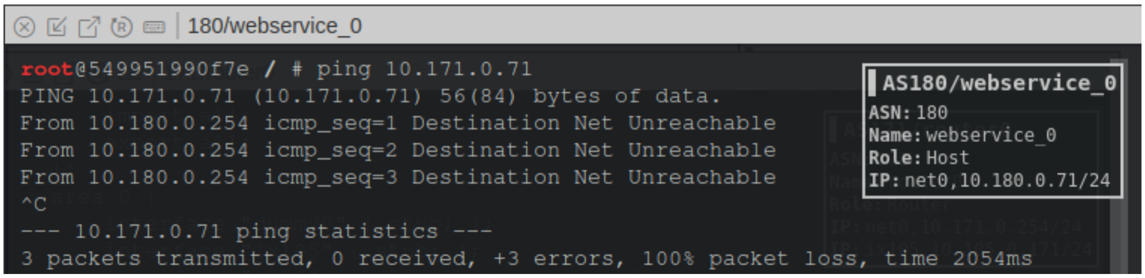


```
root@204ca48e2e4c / # ping 10.161.0.71

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=0.366 ms
64 bytes from 10.161.0.71: icmp_seq=2 ttl=56 time=0.399 ms
64 bytes from 10.161.0.71: icmp_seq=3 ttl=56 time=0.571 ms
^C
--- 10.161.0.71 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2042ms
rtt min/avg/max/mdev = 0.366/0.445/0.571/0.089 ms
```

AS156/webservice_1
ASN: 156
Name: webservice_1
Role: Host
IP: net0,10.156.0.72/24

In this snippet, we test connectivity in AS-156. We see we regained connectivity.

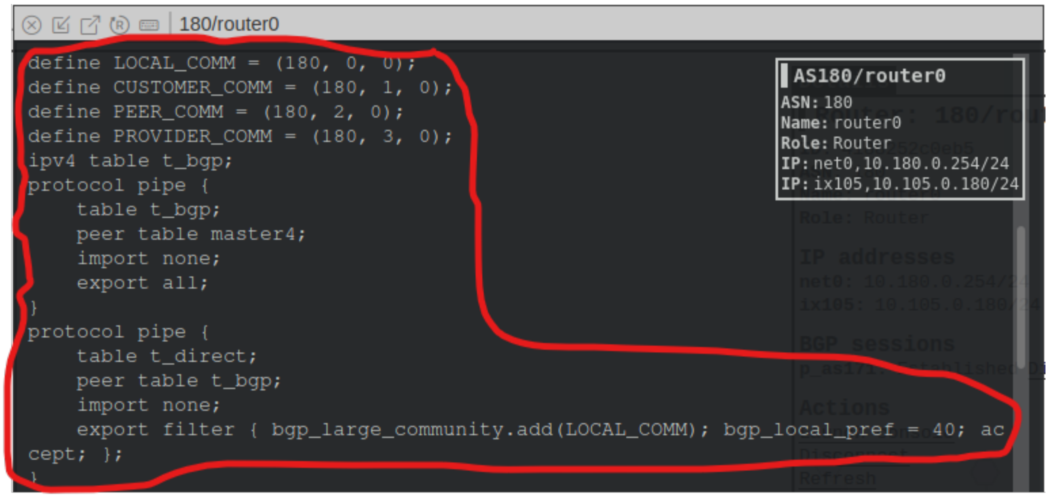
Task 1.d



```
root@549951990f7e / # ping 10.171.0.71
PING 10.171.0.71 (10.171.0.71) 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
^C
--- 10.171.0.71 ping statistics ---
3 packets transmitted, 0 received, +3 errors, 100% packet loss, time 2054ms
```

AS180/webservice_0
ASN: 180
Name: webservice_0
Role: Host
IP: net0,10.180.0.71/24

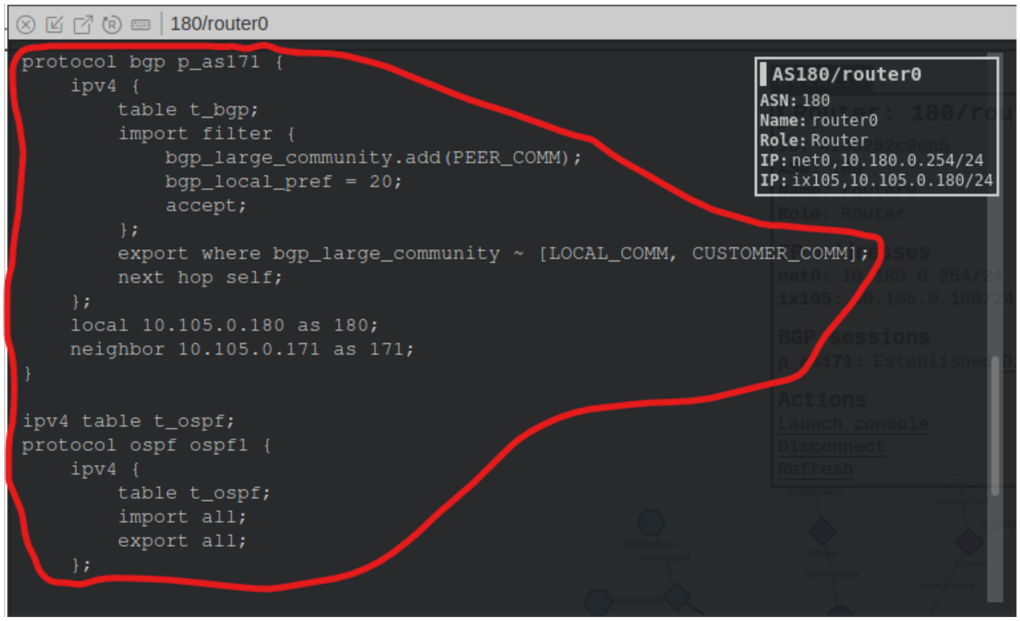
In this snippet, we test the connectivity between AS-180 and AS-171. We see there is no connection.



```
define LOCAL_COMM = (180, 0, 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; ac
cept; };
}
```

AS180/router0
ASN: 180
Name: router0
Role: Router
IP: net0,10.180.0.254/24
IP: ix105,10.105.0.180/24

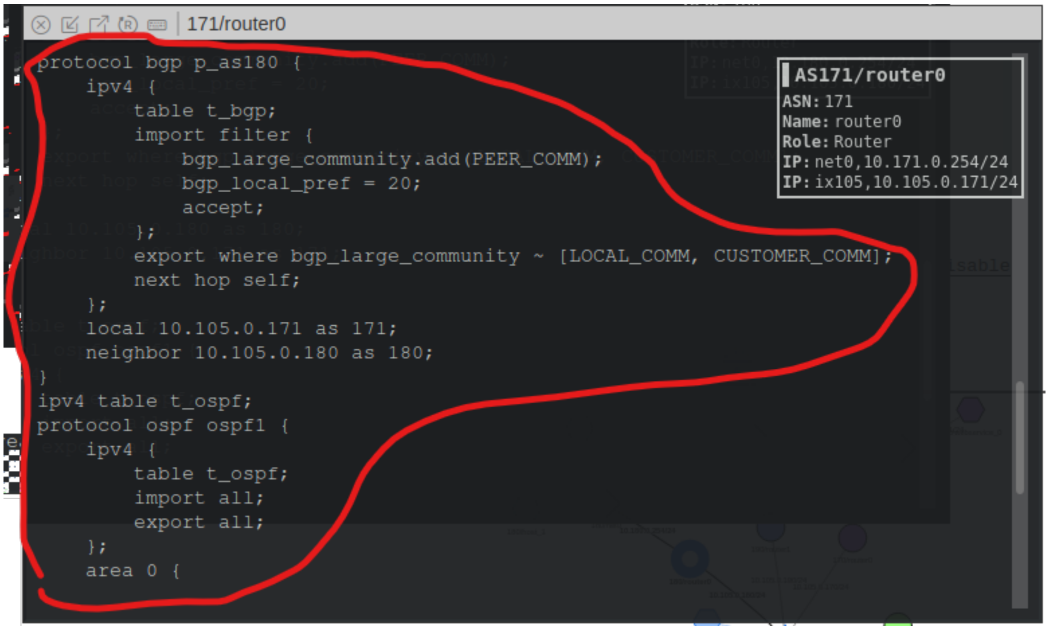
In this snippet, we add code to allow AS-180 accommodate AS-171 as a peer.



```
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;
    };
```

AS180/router0
ASN: 180
Name: router0
Role: Router
IP: net0,10.180.0.254/24
IP: ix105,10.105.0.180/24

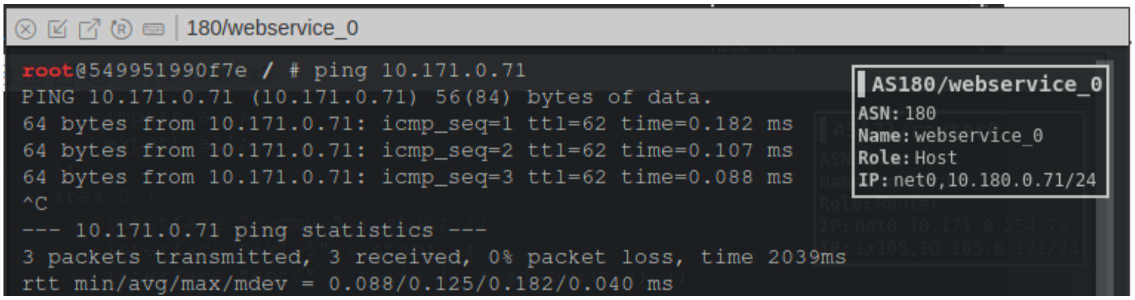
In this snippet, we make AS-171 a peer of AS-180.



```
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 {
```

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

In this snippet, we make AS-180 a peer of AS-171.

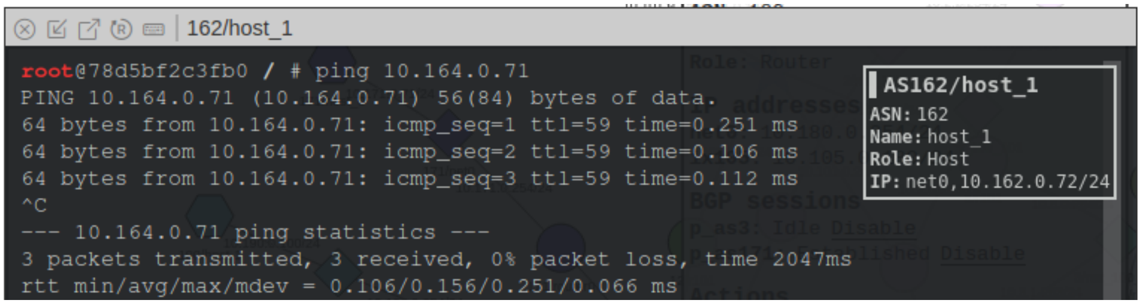


```
root@549951990f7e / # ping 10.171.0.71
PING 10.171.0.71 (10.171.0.71) 56(84) bytes of data.
64 bytes from 10.171.0.71: icmp_seq=1 ttl=62 time=0.182 ms
64 bytes from 10.171.0.71: icmp_seq=2 ttl=62 time=0.107 ms
64 bytes from 10.171.0.71: icmp_seq=3 ttl=62 time=0.088 ms
^C
--- 10.171.0.71 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2039ms
rtt min/avg/max/mdev = 0.088/0.125/0.182/0.040 ms
```

```
AS180/webservice_0
ASN: 180
Name: webservice_0
Role: Host
IP: net0,10.180.0.71/24
```

In this snippet, we test the connection between AS-180 and AS-171. We now see a connection.

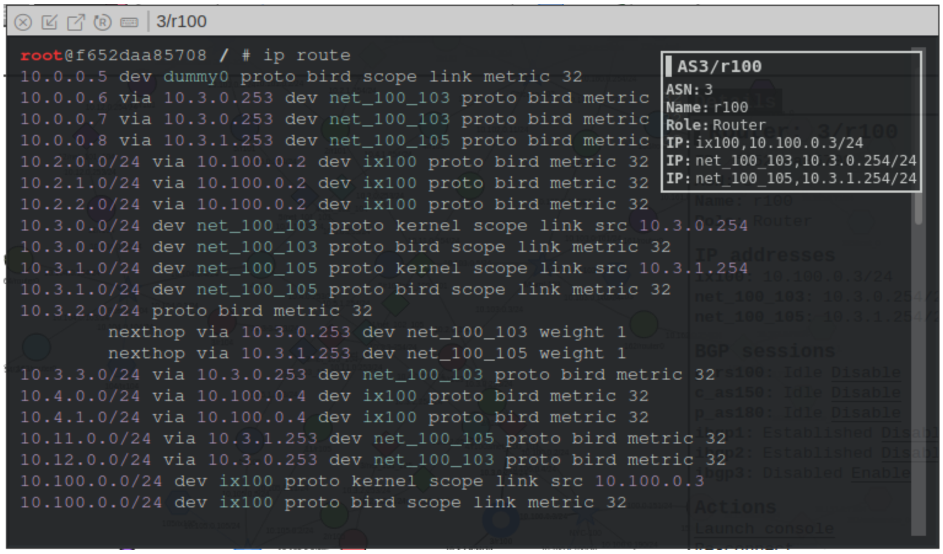
Task 2.a



```
root@78d5bf2c3fb0 / # ping 10.164.0.71
PING 10.164.0.71 (10.164.0.71) 56(84) bytes of data.
64 bytes from 10.164.0.71: icmp_seq=1 ttl=59 time=0.251 ms
64 bytes from 10.164.0.71: icmp_seq=2 ttl=59 time=0.106 ms
64 bytes from 10.164.0.71: icmp_seq=3 ttl=59 time=0.112 ms
^C
--- 10.164.0.71 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2047ms
rtt min/avg/max/mdev = 0.106/0.156/0.251/0.066 ms
```

```
AS162/host_1
ASN: 162
Name: host_1
Role: Host
IP: net0,10.162.0.72/24
```

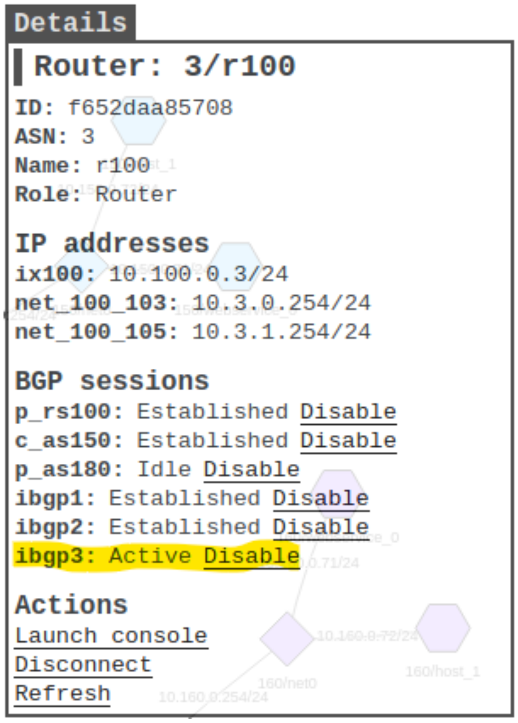
In this snippet, we ping AS-3 from AS-162.



```
root@f652daa85708 / # ip route
10.0.0.5 dev dummy0 proto bird scope link metric 32
10.0.0.6 via 10.3.0.253 dev net_100_103 proto bird metric
10.0.0.7 via 10.3.0.253 dev net_100_103 proto bird metric
10.0.0.8 via 10.3.1.253 dev net_100_105 proto bird metric
10.2.0.0/24 via 10.100.0.2 dev ix100 proto bird metric 32
10.2.1.0/24 via 10.100.0.2 dev ix100 proto bird metric 32
10.2.2.0/24 via 10.100.0.2 dev ix100 proto bird metric 32
10.3.0.0/24 dev net_100_103 proto kernel scope link src 10.3.0.254
10.3.0.0/24 dev net_100_103 proto bird scope link metric 32
10.3.1.0/24 dev net_100_105 proto kernel scope link src 10.3.1.254
10.3.1.0/24 dev net_100_105 proto bird scope link metric 32
10.3.2.0/24 proto bird metric 32
        nexthop via 10.3.0.253 dev net_100_103 weight 1
        nexthop via 10.3.1.253 dev net_100_105 weight 1
10.3.3.0/24 via 10.3.0.253 dev net_100_103 proto bird metric 32
10.4.0.0/24 via 10.100.0.4 dev ix100 proto bird metric 32
10.4.1.0/24 via 10.100.0.4 dev ix100 proto bird metric 32
10.11.0.0/24 via 10.3.1.253 dev net_100_105 proto bird metric 32
10.12.0.0/24 via 10.3.0.253 dev net_100_103 proto bird metric 32
10.100.0.0/24 dev ix100 proto kernel scope link src 10.100.0.3
10.100.0.0/24 dev ix100 proto bird scope link metric 32
```

AS3/r100
ASN: 3
Name: r100
Role: Router
IP: ix100,10.100.0.3/24
IP: net_100_103,10.3.0.254/24
IP: net_100_105,10.3.1.254/24

In this snippet, we see AS-3's routes before disabling IBGP3 on AS-3.



Router: 3/r100

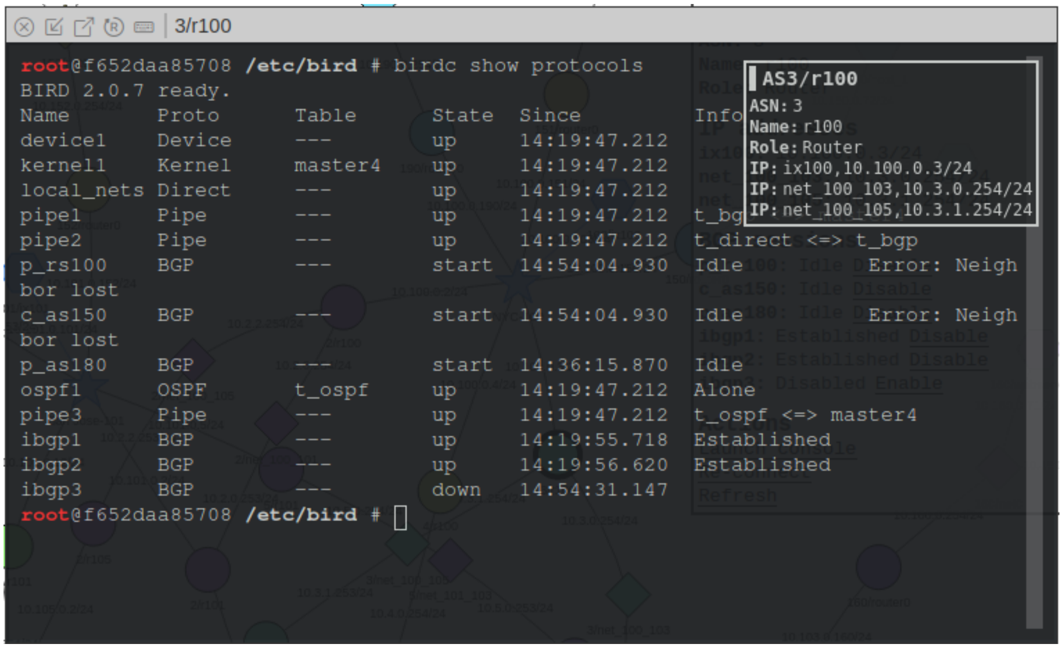
ID: f652daa85708
ASN: 3
Name: r100
Role: Router

IP addresses
ix100: 10.100.0.3/24
net_100_103: 10.3.0.254/24
net_100_105: 10.3.1.254/24

BGP sessions
p_rs100: Established Disable
c_as150: Established Disable
p_as180: Idle Disable
ibgp1: Established Disable
ibgp2: Established Disable
ibgp3: Active Disable

Actions

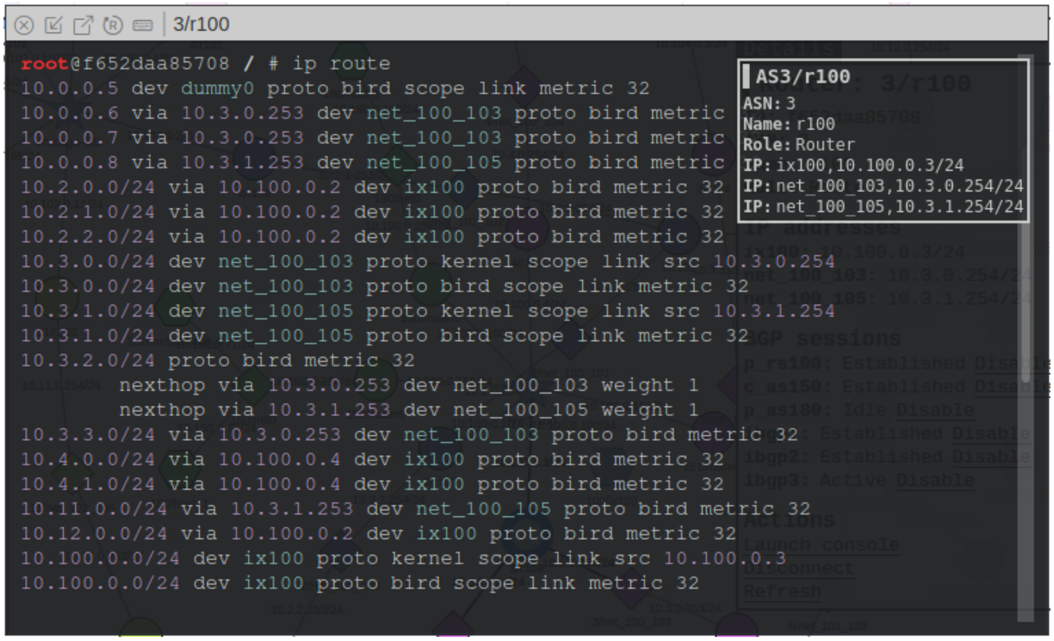
In this snippet, we see AS-3's IBGP3, on IX-103, before being disabled.



```
root@f652daa85708 /etc/bird # birdc show protocols
BIRD 2.0.7 ready.
Name       Proto      Table      State  Since         Info
device1    Device     ---        up     14:19:47.212
kernel1    Kernel     master4    up     14:19:47.212
local_nets Direct     ---        up     14:19:47.212
pipe1      Pipe       ---        up     14:19:47.212  t_bg
pipe2      Pipe       ---        up     14:19:47.212  t_direct <=> t_bgp
p_rs100    BGP        ---        start  14:54:04.930  Idle          Error: Neigh
bor lost
c_as150    BGP        ---        start  14:54:04.930  Idle          Error: Neigh
bor lost
p_as180    BGP        ---        start  14:36:15.870  Idle
ospf1      OSPF       t_ospf     up     14:19:47.212  Alone
pipe3      Pipe       ---        up     14:19:47.212  t_ospf <=> master4
ibgp1      BGP        ---        up     14:19:55.718  Established
ibgp2      BGP        ---        up     14:19:56.620  Established
ibgp3      BGP        ---        down   14:54:31.147
root@f652daa85708 /etc/bird # 
```

```
AS3/r100
ASN: 3
Name: r100
Role: Router
IP: ix100,10.100.0.3/24
IP: net_100_103,10.3.0.254/24
IP: net_100_105,10.3.1.254/24
```

In this snippet, we disable IBGP3, on IX-103, on AS-3.

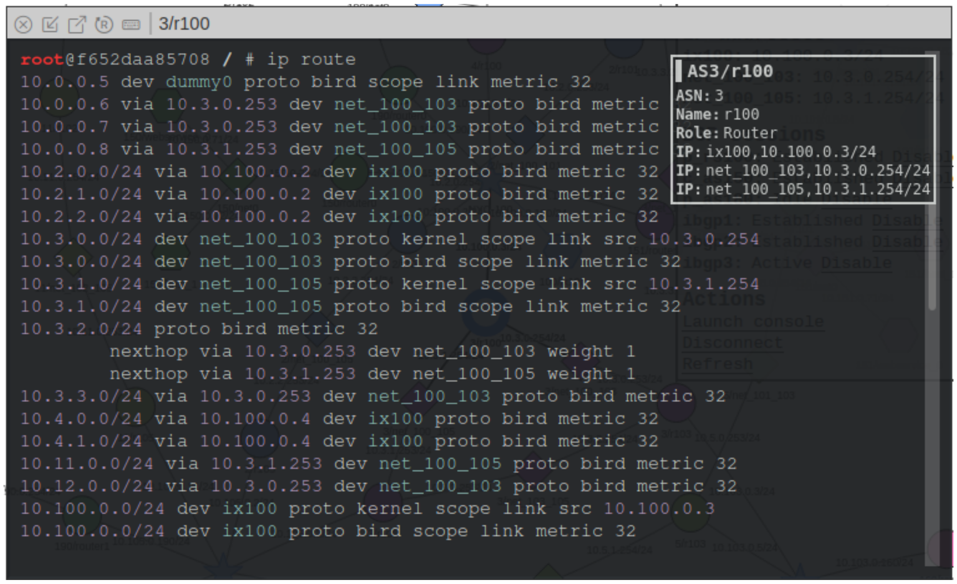


```
root@f652daa85708 / # ip route
10.0.0.5 dev dummy0 proto bird scope link metric 32
10.0.0.6 via 10.3.0.253 dev net_100_103 proto bird metric
10.0.0.7 via 10.3.0.253 dev net_100_103 proto bird metric
10.0.0.8 via 10.3.1.253 dev net_100_105 proto bird metric
10.2.0.0/24 via 10.100.0.2 dev ix100 proto bird metric 32
10.2.1.0/24 via 10.100.0.2 dev ix100 proto bird metric 32
10.2.2.0/24 via 10.100.0.2 dev ix100 proto bird metric 32
10.3.0.0/24 dev net_100_103 proto kernel scope link src 10.3.0.254
10.3.0.0/24 dev net_100_103 proto bird scope link metric 32
10.3.1.0/24 dev net_100_105 proto kernel scope link src 10.3.1.254
10.3.1.0/24 dev net_100_105 proto bird scope link metric 32
10.3.2.0/24 proto bird metric 32
        nexthop via 10.3.0.253 dev net_100_103 weight 1
        nexthop via 10.3.1.253 dev net_100_105 weight 1
10.3.3.0/24 via 10.3.0.253 dev net_100_103 proto bird metric 32
10.4.0.0/24 via 10.100.0.4 dev ix100 proto bird metric 32
10.4.1.0/24 via 10.100.0.4 dev ix100 proto bird metric 32
10.11.0.0/24 via 10.3.1.253 dev net_100_105 proto bird metric 32
10.12.0.0/24 via 10.100.0.2 dev ix100 proto bird metric 32
10.100.0.0/24 dev ix100 proto kernel scope link src 10.100.0.3
10.100.0.0/24 dev ix100 proto bird scope link metric 32
```

```
AS3/r100
ASN: 3
Name: r100
Role: Router
IP: ix100,10.100.0.3/24
IP: net_100_103,10.3.0.254/24
IP: net_100_105,10.3.1.254/24
```

In this snippet, we see AS-3’s routes after disabling IBGP3, on IX-103, on AS-3. Notice the third last bullet point. The connection now goes through 10.100.0.2 instead of 10.3.0.253.

Task 2.b

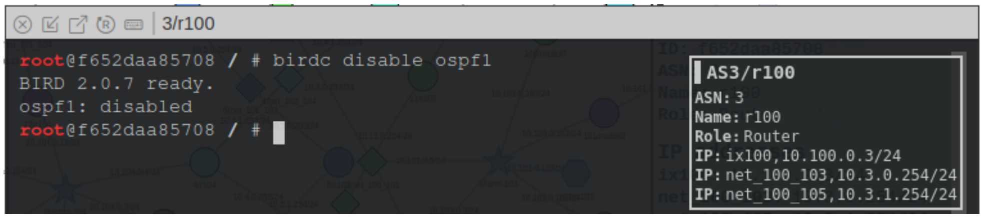


3/r100

```
root@f652daa85708 / # ip route
10.0.0.5 dev dummy0 proto bird scope link metric 32
10.0.0.6 via 10.3.0.253 dev net_100_103 proto bird metric
10.0.0.7 via 10.3.0.253 dev net_100_103 proto bird metric
10.0.0.8 via 10.3.1.253 dev net_100_105 proto bird metric
10.2.0.0/24 via 10.100.0.2 dev ix100 proto bird metric 32
10.2.1.0/24 via 10.100.0.2 dev ix100 proto bird metric 32
10.2.2.0/24 via 10.100.0.2 dev ix100 proto bird metric 32
10.3.0.0/24 dev net_100_103 proto kernel scope link src 10.3.0.254
10.3.0.0/24 dev net_100_103 proto bird scope link metric 32
10.3.1.0/24 dev net_100_105 proto kernel scope link src 10.3.1.254
10.3.1.0/24 dev net_100_105 proto bird scope link metric 32
10.3.2.0/24 proto bird metric 32
        nexthop via 10.3.0.253 dev net_100_103 weight 1
        nexthop via 10.3.1.253 dev net_100_105 weight 1
10.3.3.0/24 via 10.3.0.253 dev net_100_103 proto bird metric 32
10.4.0.0/24 via 10.100.0.4 dev ix100 proto bird metric 32
10.4.1.0/24 via 10.100.0.4 dev ix100 proto bird metric 32
10.11.0.0/24 via 10.3.1.253 dev net_100_105 proto bird metric 32
10.12.0.0/24 via 10.3.0.253 dev net_100_103 proto bird metric 32
10.100.0.0/24 dev ix100 proto kernel scope link src 10.100.0.3
10.100.0.0/24 dev ix100 proto bird scope link metric 32
```

AS3/r100
ASN: 3
Name: r100
Role: Router
IP: ix100,10.100.0.3/24
IP: net_100_103,10.3.0.254/24
IP: net_100_105,10.3.1.254/24

In this snippet, we see AS-3's routes before disabling OSPG on AS-3.

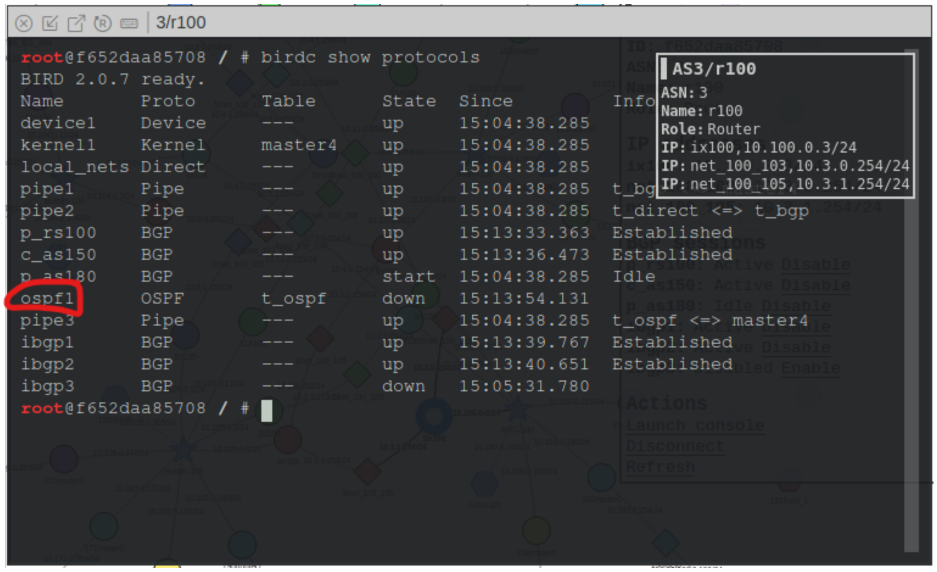


3/r100

```
root@f652daa85708 / # birdc disable ospf1
BIRD 2.0.7 ready.
ospf1: disabled
root@f652daa85708 / #
```

AS3/r100
ASN: 3
Name: r100
Role: Router
IP: ix100,10.100.0.3/24
IP: net_100_103,10.3.0.254/24
IP: net_100_105,10.3.1.254/24

In this snippet, we disable OSPF on AS-3.

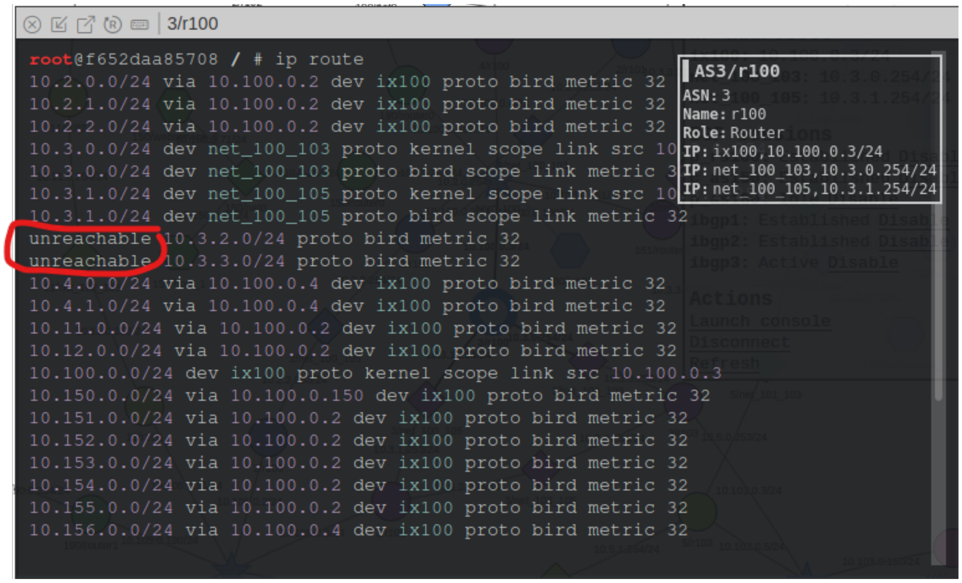


3/r100

```
root@f652daa85708 / # birdc show protocols
BIRD 2.0.7 ready.
Name       Proto      Table      State  Since          Info
device1    Device     ---        up     15:04:38.285
kernel1    Kernel     master4    up     15:04:38.285
local_nets Direct     ---        up     15:04:38.285
pipe1      Pipe       ---        up     15:04:38.285   t_bg
pipe2      Pipe       ---        up     15:04:38.285   t_direct <=> t_bgp
p_rs100    BGP        ---        up     15:13:33.363   Established
c_as150    BGP        ---        up     15:13:36.473   Established
p_as180    BGP        ---        start  15:04:38.285   Idle
ospf1      OSPF       t_ospf     down   15:13:54.131
pipe3      Pipe       ---        up     15:04:38.285   t_ospf <=> master4
ibgp1      BGP        ---        up     15:13:39.767   Established
ibgp2      BGP        ---        up     15:13:40.651   Established
ibgp3      BGP        ---        down   15:05:31.780
root@f652daa85708 / #
```

AS3/r100
ASN: 3
Name: r100
Role: Router
IP: ix100,10.100.0.3/24
IP: net_100_103,10.3.0.254/24
IP: net_100_105,10.3.1.254/24

In this snippet, we verify OSPF has been disabled on AS-3.

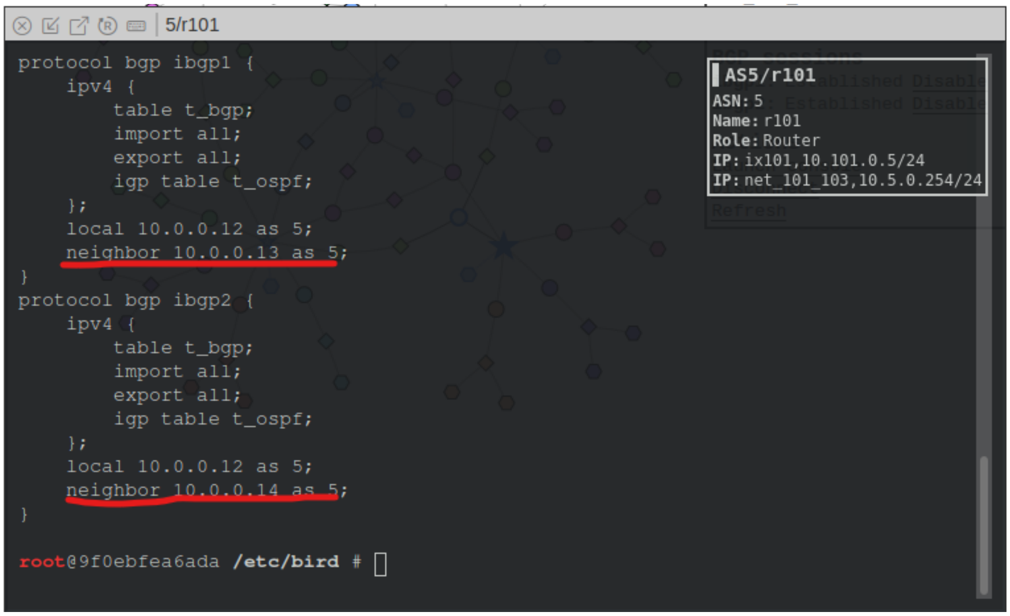


```
root@f652daa85708 / # ip route
10.2.0.0/24 via 10.100.0.2 dev ix100 proto bird metric 32
10.2.1.0/24 via 10.100.0.2 dev ix100 proto bird metric 32
10.2.2.0/24 via 10.100.0.2 dev ix100 proto bird metric 32
10.3.0.0/24 dev net_100_103 proto kernel scope link src 10
10.3.0.0/24 dev net_100_103 proto bird scope link metric 3
10.3.1.0/24 dev net_100_105 proto kernel scope link src 10
10.3.1.0/24 dev net_100_105 proto bird scope link metric 32
unreachable 10.3.2.0/24 proto bird metric 32
unreachable 10.3.3.0/24 proto bird metric 32
10.4.0.0/24 via 10.100.0.4 dev ix100 proto bird metric 32
10.4.1.0/24 via 10.100.0.4 dev ix100 proto bird metric 32
10.11.0.0/24 via 10.100.0.2 dev ix100 proto bird metric 32
10.12.0.0/24 via 10.100.0.2 dev ix100 proto bird metric 32
10.100.0.0/24 dev ix100 proto kernel scope link src 10.100.0.3
10.150.0.0/24 via 10.100.0.150 dev ix100 proto bird metric 32
10.151.0.0/24 via 10.100.0.2 dev ix100 proto bird metric 32
10.152.0.0/24 via 10.100.0.2 dev ix100 proto bird metric 32
10.153.0.0/24 via 10.100.0.2 dev ix100 proto bird metric 32
10.154.0.0/24 via 10.100.0.2 dev ix100 proto bird metric 32
10.155.0.0/24 via 10.100.0.2 dev ix100 proto bird metric 32
10.156.0.0/24 via 10.100.0.4 dev ix100 proto bird metric 32
```

```
AS3/r100
ASN: 3
Name: r100
Role: Router
IP: ix100,10.100.0.3/24
IP: net_100_103,10.3.0.254/24
IP: net_100_105,10.3.1.254/24
```

In this snippet, we see AS-3's routes after disabling OSPF. Notice how some locations became unreachable after disabling OSPF.

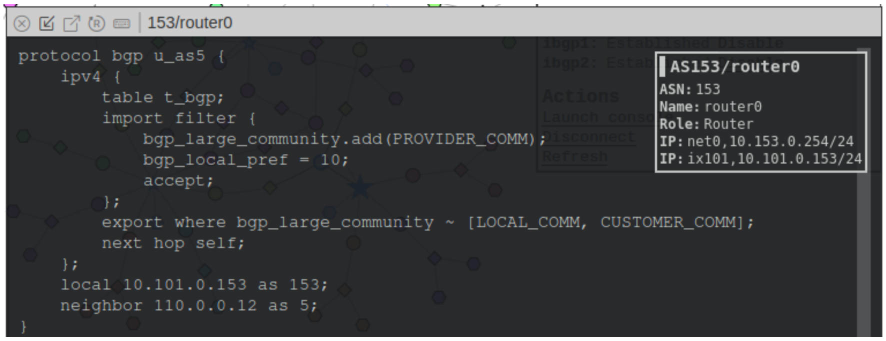
Task 2.c



```
protocol bgp ibgp1 {
    ipv4 {
        table t_bgp;
        import all;
        export all;
        igp table t_ospf;
    };
    local 10.0.0.12 as 5;
    neighbor 10.0.0.13 as 5;
}
protocol bgp ibgp2 {
    ipv4 {
        table t_bgp;
        import all;
        export all;
        igp table t_ospf;
    };
    local 10.0.0.12 as 5;
    neighbor 10.0.0.14 as 5;
}

root@9f0ebfea6ada /etc/bird #
```

```
AS5/r101
ASN: 5
Name: r101
Role: Router
IP: ix101,10.101.0.5/24
IP: net_101_103,10.5.0.254/24
```

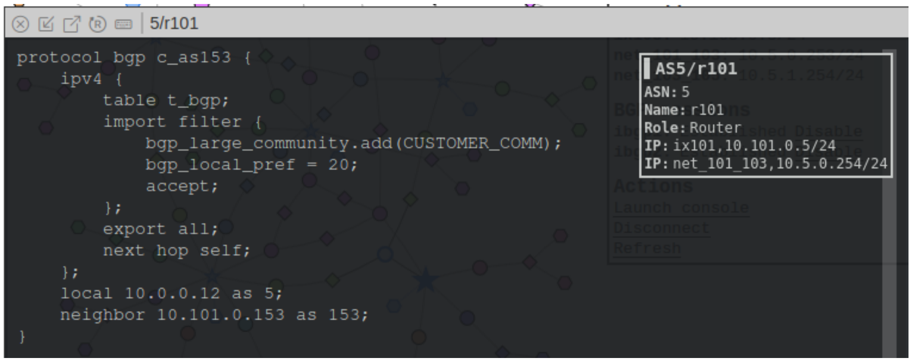
In this snippet, we see AS-5's, on IX-101, IBGP configuration. Notice the different locations labeled as 5. This implies other AS-5 locations on the network.



```
protocol bgp u_as5 {
    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 10.101.0.153 as 153;
    neighbor 110.0.0.12 as 5;
}
```

```
AS153/router0
ASN: 153
Name: router0
Role: Router
IP: net0,10.153.0.254/24
IP: ix101,10.101.0.153/24
```

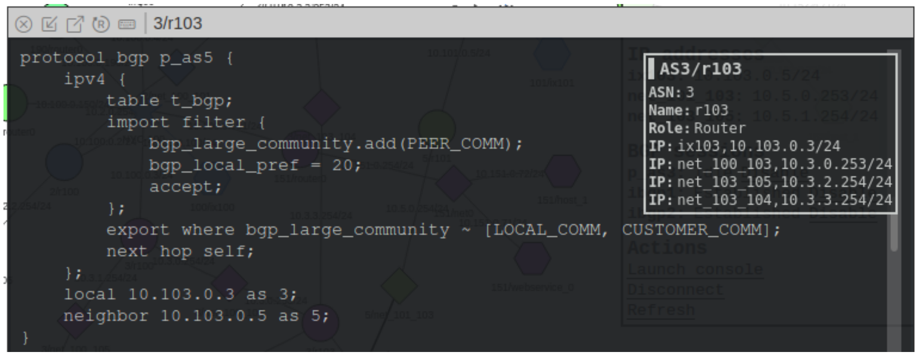
In this snippet, we see AS-5, on IX-101, is a provider to AS-153.



```
protocol bgp c_as153 {
    ipv4 {
        table t_bgp;
        import filter {
            bgp_large_community.add(CUSTOMER_COMM);
            bgp_local_pref = 20;
            accept;
        };
        export all;
        next hop self;
    };
    local 10.0.0.12 as 5;
    neighbor 10.101.0.153 as 153;
}
```

```
AS5/r101
ASN: 5
Name: r101
Role: Router
IP: ix101,10.101.0.5/24
IP: net_101_103,10.5.0.254/24
```

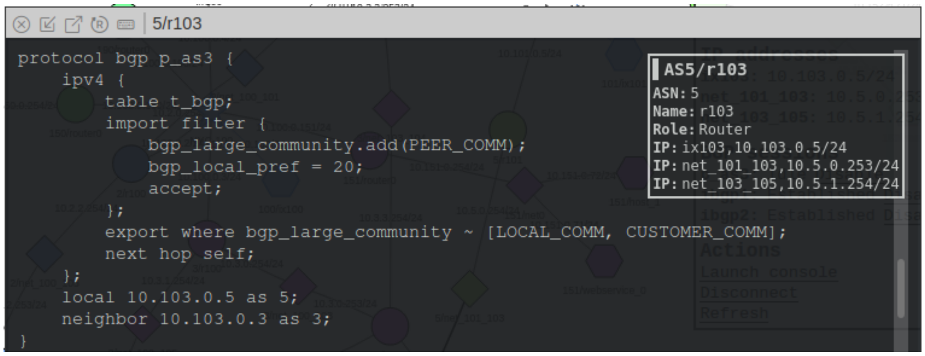
In this snippet, we see AS-153 is a customer to AS-5 on IX-101.



```
protocol bgp p_as5 {
    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 10.103.0.3 as 3;
    neighbor 10.103.0.5 as 5;
}
```

```
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
```

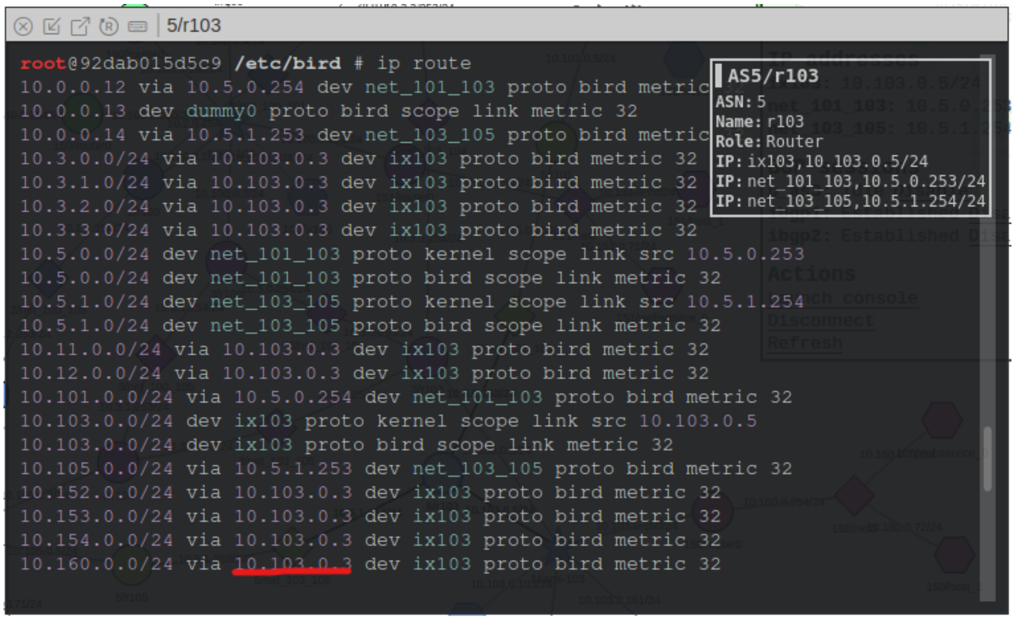
In this snippet, we make AS-5, on IX-101, a peer to AS-3.



```
protocol bgp p_as3 {
    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 10.103.0.5 as 5;
    neighbor 10.103.0.3 as 3;
}
```

```
AS5/r103
ASN: 5
Name: r103
Role: Router
IP: ix103,10.103.0.5/24
IP: net_101_103,10.5.0.253/24
IP: net_103_105,10.5.1.254/24
```

In this snippet, we make AS-3 a peer to AS-5 on IX-101.

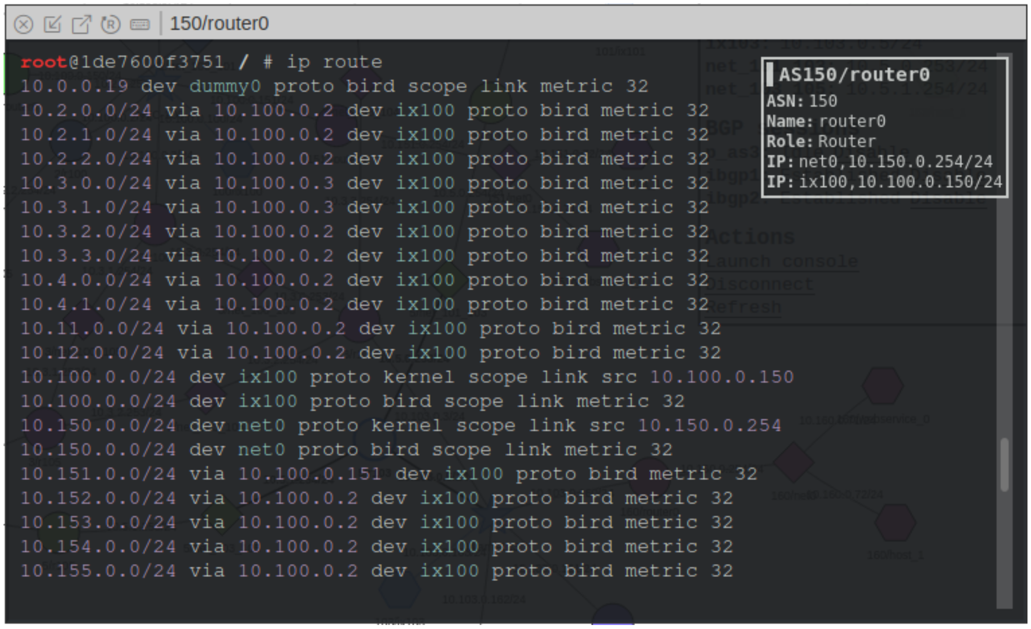


```
root@92dab015d5c9 /etc/bird # ip route
10.0.0.12 via 10.5.0.254 dev net_101_103 proto bird metric
10.0.0.13 dev dummy0 proto bird scope link metric 32
10.0.0.14 via 10.5.1.253 dev net_103_105 proto bird metric
10.3.0.0/24 via 10.103.0.3 dev ix103 proto bird metric 32
10.3.1.0/24 via 10.103.0.3 dev ix103 proto bird metric 32
10.3.2.0/24 via 10.103.0.3 dev ix103 proto bird metric 32
10.3.3.0/24 via 10.103.0.3 dev ix103 proto bird metric 32
10.5.0.0/24 dev net_101_103 proto kernel scope link src 10.5.0.253
10.5.0.0/24 dev net_101_103 proto bird scope link metric 32
10.5.1.0/24 dev net_103_105 proto kernel scope link src 10.5.1.254
10.5.1.0/24 dev net_103_105 proto bird scope link metric 32
10.11.0.0/24 via 10.103.0.3 dev ix103 proto bird metric 32
10.12.0.0/24 via 10.103.0.3 dev ix103 proto bird metric 32
10.101.0.0/24 via 10.5.0.254 dev net_101_103 proto bird metric 32
10.103.0.0/24 dev ix103 proto kernel scope link src 10.103.0.5
10.103.0.0/24 dev ix103 proto bird scope link metric 32
10.105.0.0/24 via 10.5.1.253 dev net_103_105 proto bird metric 32
10.152.0.0/24 via 10.103.0.3 dev ix103 proto bird metric 32
10.153.0.0/24 via 10.103.0.3 dev ix103 proto bird metric 32
10.154.0.0/24 via 10.103.0.3 dev ix103 proto bird metric 32
10.160.0.0/24 via 10.103.0.3 dev ix103 proto bird metric 32
```

```
AS5/r103
ASN: 5
Name: r103
Role: Router
IP: ix103,10.103.0.5/24
IP: net_101_103,10.5.0.253/24
IP: net_103_105,10.5.1.254/24
```

In this snippet, we see AS-5's routes and notice that some of its connections go through AS-3. This proves AS-5 and AS-3 are peers.

Task 3.a

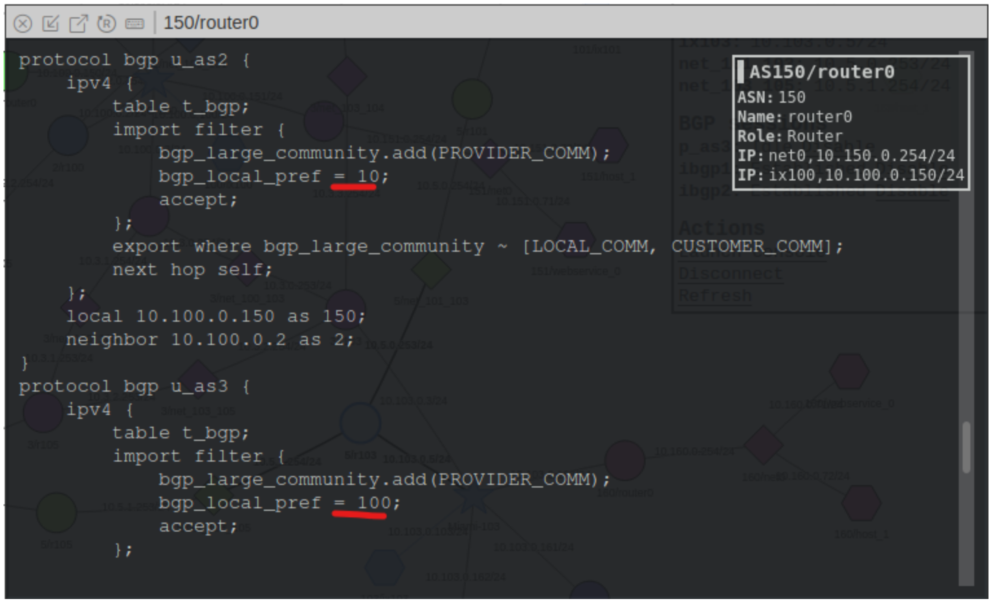


```
root@1de7600f3751 / # ip route
10.0.0.19 dev dummy0 proto bird scope link metric 32
10.2.0.0/24 via 10.100.0.2 dev ix100 proto bird metric 32
10.2.1.0/24 via 10.100.0.2 dev ix100 proto bird metric 32
10.2.2.0/24 via 10.100.0.2 dev ix100 proto bird metric 32
10.3.0.0/24 via 10.100.0.3 dev ix100 proto bird metric 32
10.3.1.0/24 via 10.100.0.3 dev ix100 proto bird metric 32
10.3.2.0/24 via 10.100.0.2 dev ix100 proto bird metric 32
10.3.3.0/24 via 10.100.0.2 dev ix100 proto bird metric 32
10.4.0.0/24 via 10.100.0.2 dev ix100 proto bird metric 32
10.4.1.0/24 via 10.100.0.2 dev ix100 proto bird metric 32
10.11.0.0/24 via 10.100.0.2 dev ix100 proto bird metric 32
10.12.0.0/24 via 10.100.0.2 dev ix100 proto bird metric 32
10.100.0.0/24 dev ix100 proto kernel scope link src 10.100.0.150
10.100.0.0/24 dev ix100 proto bird scope link metric 32
10.150.0.0/24 dev net0 proto kernel scope link src 10.150.0.254
10.150.0.0/24 dev net0 proto bird scope link metric 32
10.151.0.0/24 via 10.100.0.151 dev ix100 proto bird metric 32
10.152.0.0/24 via 10.100.0.2 dev ix100 proto bird metric 32
10.153.0.0/24 via 10.100.0.2 dev ix100 proto bird metric 32
10.154.0.0/24 via 10.100.0.2 dev ix100 proto bird metric 32
10.155.0.0/24 via 10.100.0.2 dev ix100 proto bird metric 32
```

```
AS150/router0
ASN: 150
Name: router0
Role: Router
IP: net0,10.150.0.254/24
IP: ix100,10.100.0.150/24
```

In this snippet, we show AS-150 routes. We notice several locations are accessed using the same path. This is because these are the most optimal routes. In this case, optimal means short, and this optimization is possible because AS-150 implements the OSPF protocol.

Task 3.b



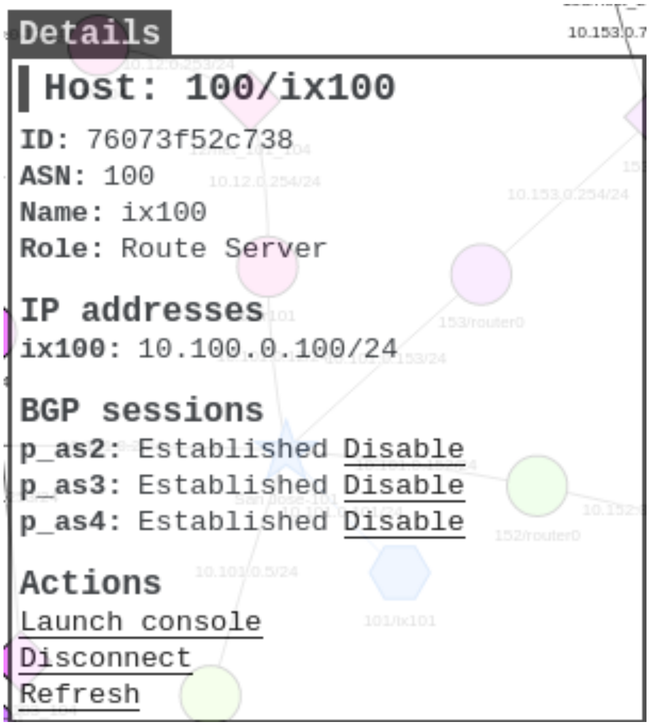
150/router0

```
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 10.100.0.150 as 150;
    neighbor 10.100.0.2 as 2;
}
protocol bgp u_as3 {
    ipv4 {
        table t_bgp;
        import filter {
            bgp_large_community.add(PROVIDER_COMM);
            bgp_local_pref = 100;
            accept;
        };
```

AS150/router0
ASN: 150
Name: router0
Role: Router
IP: net0,10.150.0.254/24
IP: ix100,10.100.0.150/24

In this snippet, we give preference to AS-3, over AS-2, in AS-150. We do this by increasing its bgp_local_pref parameter.

Task 4



Details

Host: 100/ix100

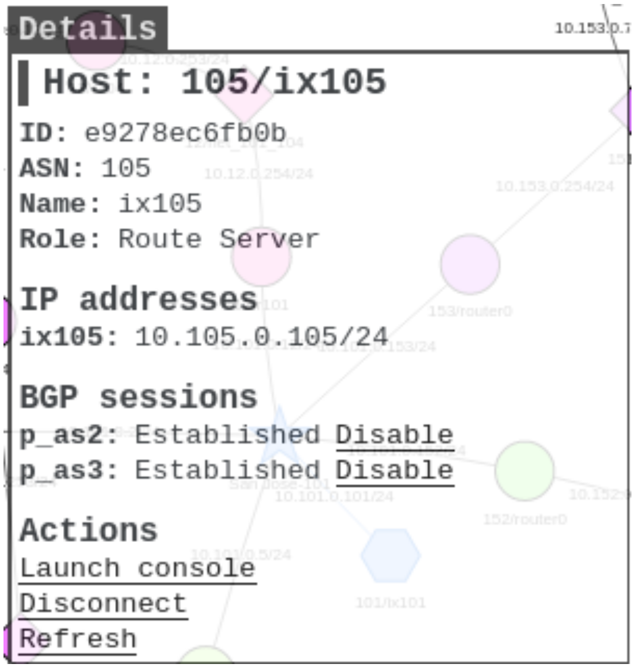
ID: 76073f52c738
ASN: 100
Name: ix100
Role: Route Server

IP addresses
ix100: 10.100.0.100/24

BGP sessions
p_as2: Established Disable
p_as3: Established Disable
p_as4: Established Disable

Actions
Launch console
Disconnect
Refresh

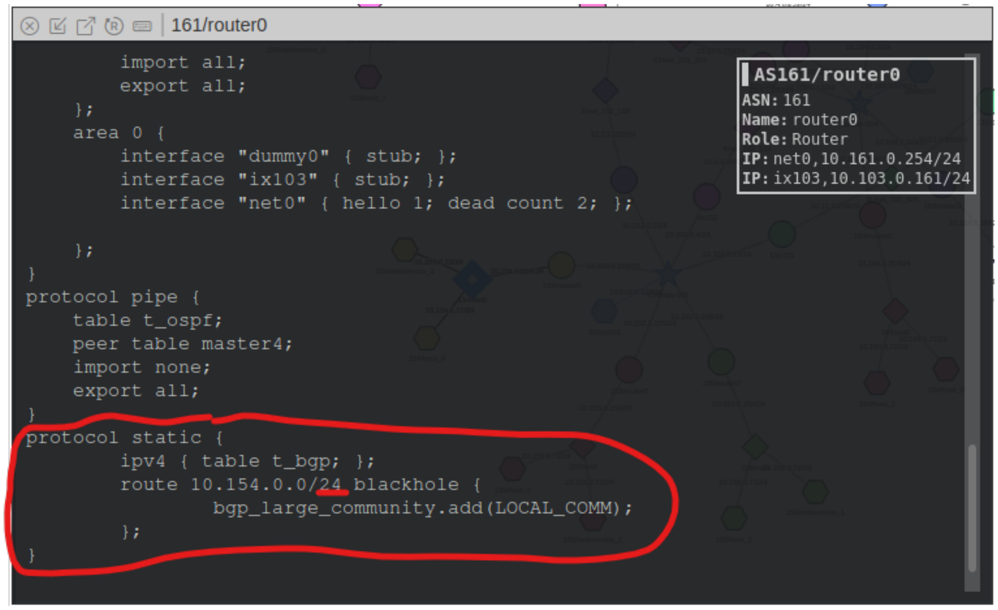
In this snippet, we identify a host that connects with one AS-190, but not with the other AS-190.



```
Details
Host: 105/ix105
ID: e9278ec6fb0b
ASN: 105
Name: ix105
Role: Route Server

IP addresses
ix105: 10.105.0.105/24

BGP sessions
p_as2: Established Disable
p_as3: Established Disable

Actions
Launch console
Disconnect
Refresh
```

In this snippet, we identify another host that connects with one AS-190, but not with the other AS-190.

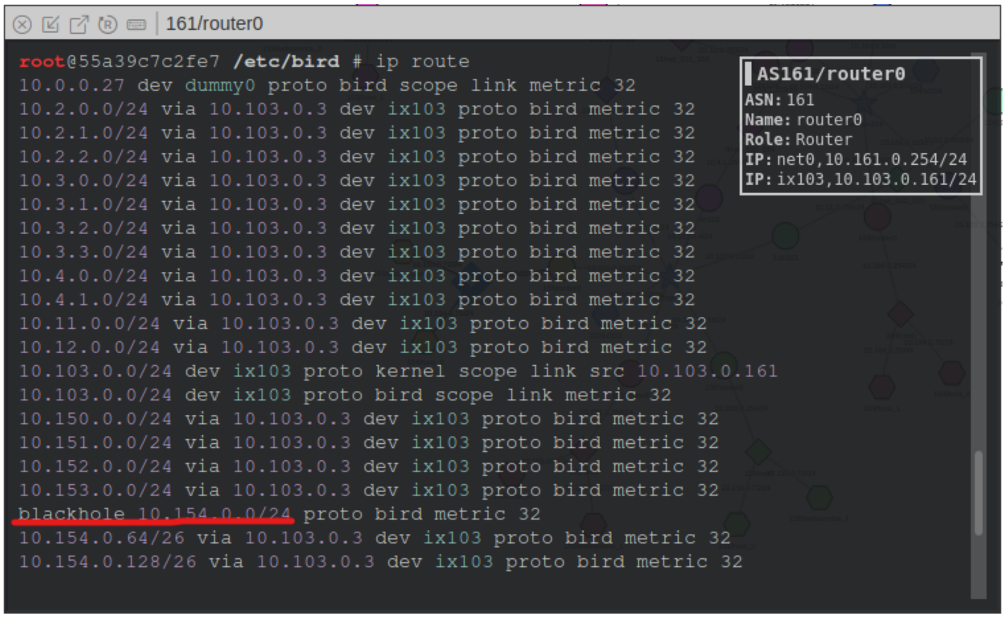
Task 5.a



```
        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;
}
protocol static {
        ipv4 { table t_bgp; };
        route 10.154.0.0/24 blackhole {
                bgp_large_community.add(LOCAL_COMM);
        };
}
```

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

In this snippet, we create a blackhole in AS-154 by modifying AS-161 router’s configuration.

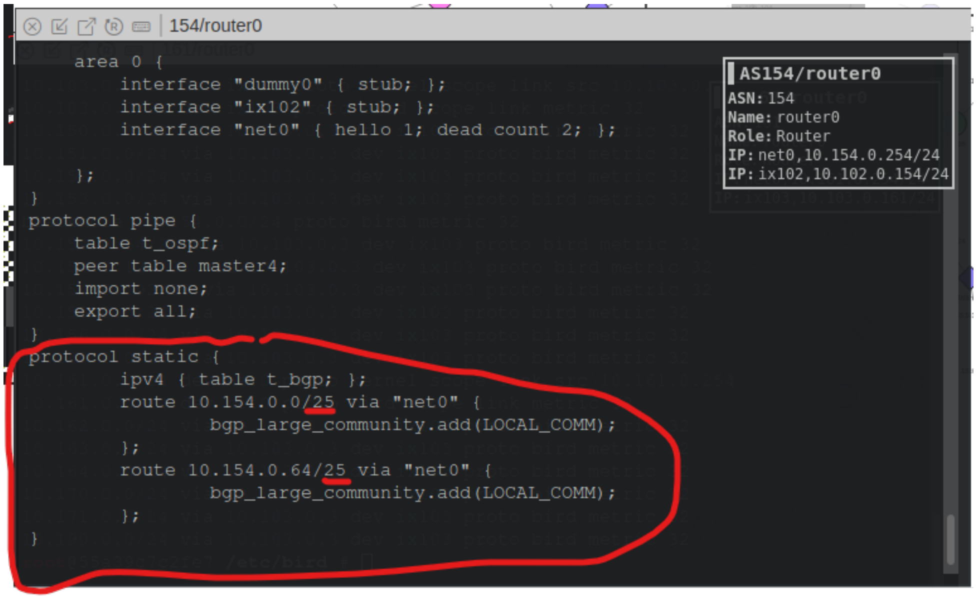


```
root@55a39c7c2fe7 /etc/bird # ip route
10.0.0.27 dev dummy0 proto bird scope link metric 32
10.2.0.0/24 via 10.103.0.3 dev ix103 proto bird metric 32
10.2.1.0/24 via 10.103.0.3 dev ix103 proto bird metric 32
10.2.2.0/24 via 10.103.0.3 dev ix103 proto bird metric 32
10.3.0.0/24 via 10.103.0.3 dev ix103 proto bird metric 32
10.3.1.0/24 via 10.103.0.3 dev ix103 proto bird metric 32
10.3.2.0/24 via 10.103.0.3 dev ix103 proto bird metric 32
10.3.3.0/24 via 10.103.0.3 dev ix103 proto bird metric 32
10.4.0.0/24 via 10.103.0.3 dev ix103 proto bird metric 32
10.4.1.0/24 via 10.103.0.3 dev ix103 proto bird metric 32
10.11.0.0/24 via 10.103.0.3 dev ix103 proto bird metric 32
10.12.0.0/24 via 10.103.0.3 dev ix103 proto bird metric 32
10.103.0.0/24 dev ix103 proto kernel scope link src 10.103.0.161
10.103.0.0/24 dev ix103 proto bird scope link metric 32
10.150.0.0/24 via 10.103.0.3 dev ix103 proto bird metric 32
10.151.0.0/24 via 10.103.0.3 dev ix103 proto bird metric 32
10.152.0.0/24 via 10.103.0.3 dev ix103 proto bird metric 32
10.153.0.0/24 via 10.103.0.3 dev ix103 proto bird metric 32
blackhole 10.154.0.0/24 proto bird metric 32
10.154.0.64/26 via 10.103.0.3 dev ix103 proto bird metric 32
10.154.0.128/26 via 10.103.0.3 dev ix103 proto bird metric 32
```

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

In this snippet, we test the blackhole by displaying AS-161's routes. Note the blackhole on AS-154.

Task 5.b

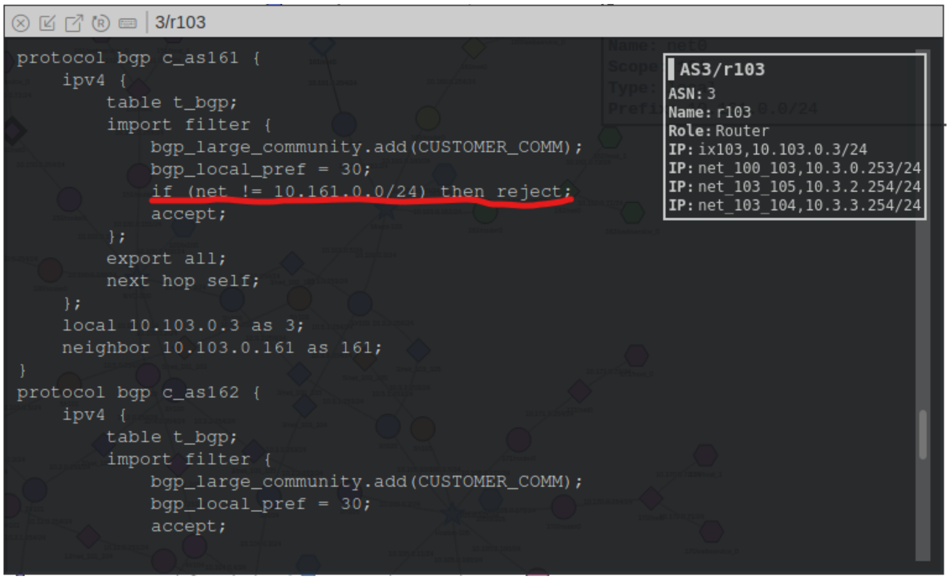


```
    area 0 {
        interface "dummy0" { stub; };
        interface "ix102" { stub; };
        interface "net0" { hello 1; dead count 2; };

    };
}
protocol pipe {
    table t_ospf;
    peer table master4;
    import none;
    export all;
}
protocol static {
        ipv4 { table t_bgp; };
        route 10.154.0.0/25 via "net0" {
                bgp_large_community.add(LOCAL_COMM);
        };
        route 10.154.0.64/25 via "net0" {
                bgp_large_community.add(LOCAL_COMM);
        };
}
```

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

In this snippet, we modify AS-154 router's configuration to fight the attack and get its traffic back. We do this by creating two prefixes for every prefix attacked, in this case only 10.154.0.0/24, and creating these prefixes such that they are a bit longer, in this case 25 instead of 24.

Task 5.c



```
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;
```

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

In this snippet, we modify AS-3 router's configuration to stop AS-161's fake announcements. We do this by only allowing the importing of routes into AS-161.