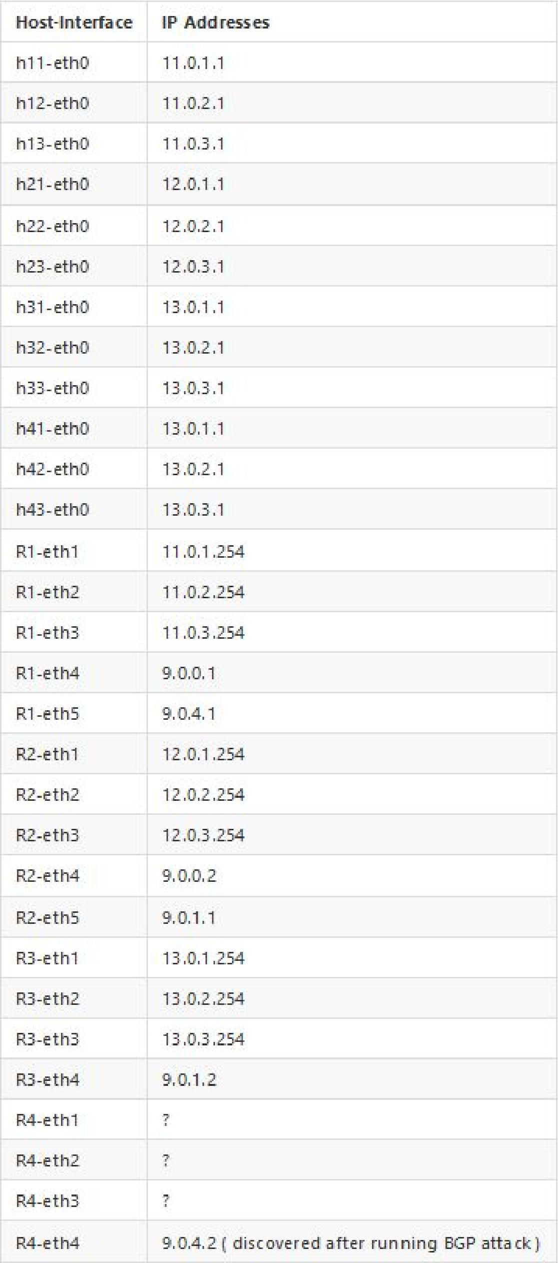
Lab 5
Tan Shin Jie 1003715

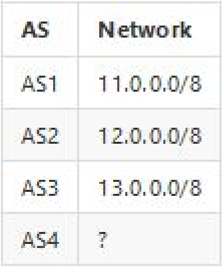
Note: this lab is completed with Tharun 1003379

Host-Interfaces and IP Addresses



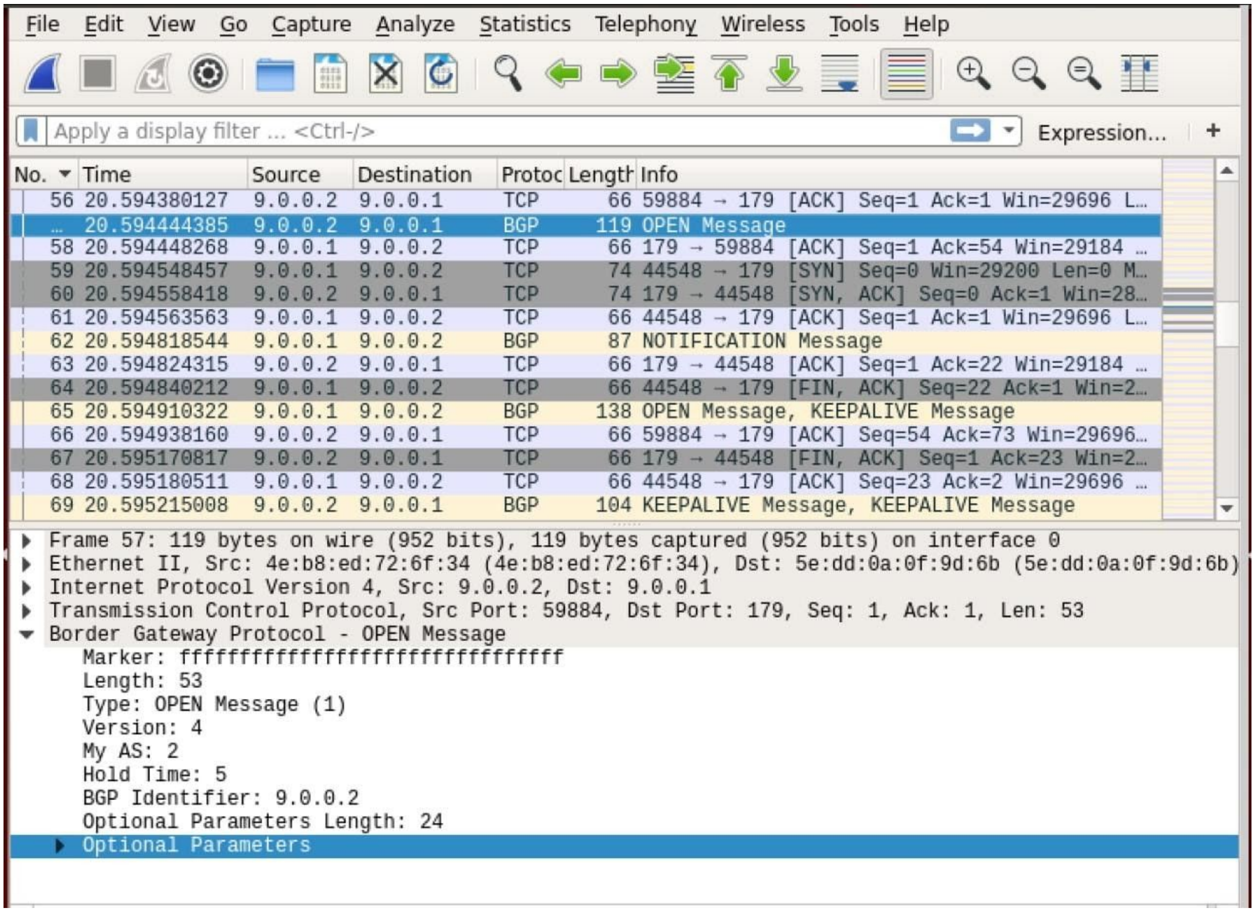
Host-Interface	IP Addresses
h11-eth0	11.0.1.1
h12-eth0	11.0.2.1
h13-eth0	11.0.3.1
h21-eth0	12.0.1.1
h22-eth0	12.0.2.1
h23-eth0	12.0.3.1
h31-eth0	13.0.1.1
h32-eth0	13.0.2.1
h33-eth0	13.0.3.1
h41-eth0	13.0.1.1
h42-eth0	13.0.2.1
h43-eth0	13.0.3.1
R1-eth1	11.0.1.254
R1-eth2	11.0.2.254
R1-eth3	11.0.3.254
R1-eth4	9.0.0.1
R1-eth5	9.0.4.1
R2-eth1	12.0.1.254
R2-eth2	12.0.2.254
R2-eth3	12.0.3.254
R2-eth4	9.0.0.2
R2-eth5	9.0.1.1
R3-eth1	13.0.1.254
R3-eth2	13.0.2.254
R3-eth3	13.0.3.254
R3-eth4	9.0.1.2
R4-eth1	?
R4-eth2	?
R4-eth3	?
R4-eth4	9.0.4.2 (discovered after running BGP attack)

Announced Network



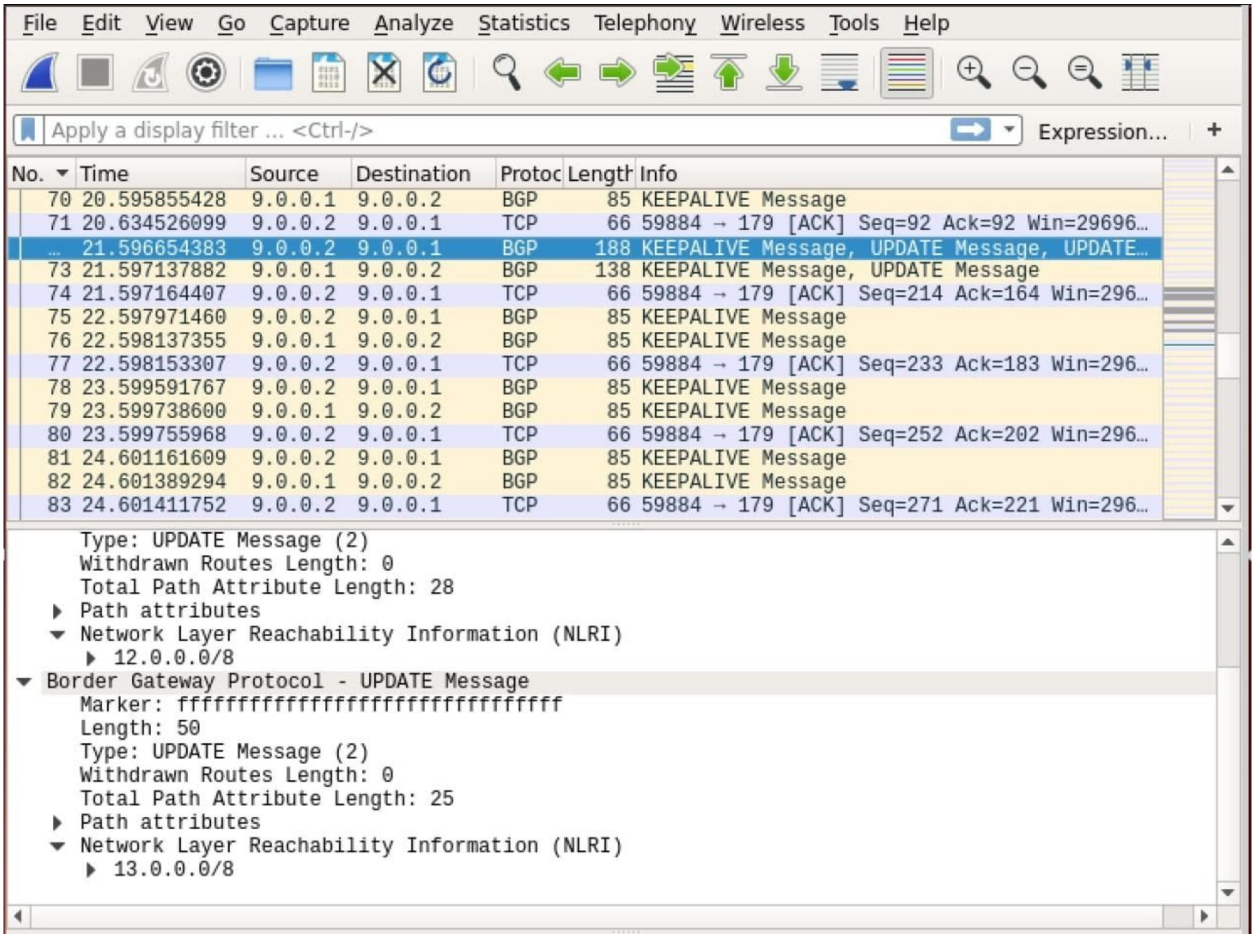
AS	Network
AS1	11.0.0.0/8
AS2	12.0.0.0/8
AS3	13.0.0.0/8
AS4	?

BGP Re-Establishment Traffic



```
No.  Time         Source   Destination  Protoc Length Info
 56 20.594380127  9.0.0.2  9.0.0.1      TCP     66 59884 → 179 [ACK] Seq=1 Ack=1 Win=29696 L…
  … 20.594444385  9.0.0.2  9.0.0.1      BGP    119 OPEN Message
 58 20.594448268  9.0.0.1  9.0.0.2      TCP     66 179 → 59884 [ACK] Seq=1 Ack=54 Win=29184 …
 59 20.594548457  9.0.0.1  9.0.0.2      TCP     74 44548 → 179 [SYN] Seq=0 Win=29200 Len=0 M…
 60 20.594558418  9.0.0.2  9.0.0.1      TCP     74 179 → 44548 [SYN, ACK] Seq=0 Ack=1 Win=28…
 61 20.594563563  9.0.0.1  9.0.0.2      TCP     66 44548 → 179 [ACK] Seq=1 Ack=1 Win=29696 L…
 62 20.594818544  9.0.0.1  9.0.0.2      BGP     87 NOTIFICATION Message
 63 20.594824315  9.0.0.2  9.0.0.1      TCP     66 179 → 44548 [ACK] Seq=1 Ack=22 Win=29184 …
 64 20.594840212  9.0.0.1  9.0.0.2      TCP     66 44548 → 179 [FIN, ACK] Seq=22 Ack=1 Win=2…
 65 20.594910322  9.0.0.1  9.0.0.2      BGP    138 OPEN Message, KEEPALIVE Message
 66 20.594938160  9.0.0.2  9.0.0.1      TCP     66 59884 → 179 [ACK] Seq=54 Ack=73 Win=29696…
 67 20.595170817  9.0.0.2  9.0.0.1      TCP     66 179 → 44548 [FIN, ACK] Seq=1 Ack=23 Win=2…
 68 20.595180511  9.0.0.1  9.0.0.2      TCP     66 44548 → 179 [ACK] Seq=23 Ack=2 Win=29696 …
 69 20.595215008  9.0.0.2  9.0.0.1      BGP    104 KEEPALIVE Message, KEEPALIVE Message

▶ Frame 57: 119 bytes on wire (952 bits), 119 bytes captured (952 bits) on interface 0
▶ Ethernet II, Src: 4e:b8:ed:72:6f:34 (4e:b8:ed:72:6f:34), Dst: 5e:dd:0a:0f:9d:6b (5e:dd:0a:0f:9d:6b)
▶ Internet Protocol Version 4, Src: 9.0.0.2, Dst: 9.0.0.1
▶ Transmission Control Protocol, Src Port: 59884, Dst Port: 179, Seq: 1, Ack: 1, Len: 53
▼ Border Gateway Protocol - OPEN Message
    Marker: ffffffffffffffffffffffffffffffff
    Length: 53
    Type: OPEN Message (1)
    Version: 4
    My AS: 2
    Hold Time: 5
    BGP Identifier: 9.0.0.2
    Optional Parameters Length: 24
  ▶ Optional Parameters
```

We performed Wireshark capture on R1, listening on eth4, the interface device connected with R2. The screenshots depict the traffic after we ran the command “clear bgp external” on R1. The communication starts with a new TCP connection establishment between the two routers before they start exchanging any message. After the TCP handshake, router R2 first sends a BGP OPEN message to R1 (No57). The OPEN message contains information about the BGP Protocol used such as the version, AS number, Hold Time, BGP Identifier, and some other optional parameters. We noticed a NOTIFICATION message is sent from R1 which could be caused by one of the following errors occurring with the BGP session: hold timer expiring, neighbor capabilities change, or a BGP session reset is requested. After that, R1 sends its own OPEN message with its respective details together with a KEEPALIVE message (No65). R2 subsequently responded with two KEEPALIVE messages(No69). We believe the second KEEPALIVE message is a response to the NOTIFICATION Message from R1. The BGP connection between R1 and R2 is now established, and KEEPALIVE messages are repeatedly exchanged according to the agreed Hold Time.



```
No.  Time          Source   Destination Protoc Lengtł Info
70 20.595855428   9.0.0.1  9.0.0.2     BGP     85 KEEPALIVE Message
71 20.634526099   9.0.0.2  9.0.0.1     TCP     66 59884 → 179 [ACK] Seq=92 Ack=92 Win=29696…
…  21.596654383   9.0.0.2  9.0.0.1     BGP    188 KEEPALIVE Message, UPDATE Message, UPDATE…
73 21.597137882   9.0.0.1  9.0.0.2     BGP    138 KEEPALIVE Message, UPDATE Message
74 21.597164407   9.0.0.2  9.0.0.1     TCP     66 59884 → 179 [ACK] Seq=214 Ack=164 Win=296…
75 22.597971460   9.0.0.2  9.0.0.1     BGP     85 KEEPALIVE Message
76 22.598137355   9.0.0.1  9.0.0.2     BGP     85 KEEPALIVE Message
77 22.598153307   9.0.0.2  9.0.0.1     TCP     66 59884 → 179 [ACK] Seq=233 Ack=183 Win=296…
78 23.599591767   9.0.0.2  9.0.0.1     BGP     85 KEEPALIVE Message
79 23.599738600   9.0.0.1  9.0.0.2     BGP     85 KEEPALIVE Message
80 23.599755968   9.0.0.2  9.0.0.1     TCP     66 59884 → 179 [ACK] Seq=252 Ack=202 Win=296…
81 24.601161609   9.0.0.2  9.0.0.1     BGP     85 KEEPALIVE Message
82 24.601389294   9.0.0.1  9.0.0.2     BGP     85 KEEPALIVE Message
83 24.601411752   9.0.0.2  9.0.0.1     TCP     66 59884 → 179 [ACK] Seq=271 Ack=221 Win=296…
```

```
    Type: UPDATE Message (2)
    Withdrawn Routes Length: 0
    Total Path Attribute Length: 28
  ▸ Path attributes
  ▾ Network Layer Reachability Information (NLRI)
    ▸ 12.0.0.0/8
▾ Border Gateway Protocol - UPDATE Message
    Marker: ffffffffffffffffffffffffffffffff
    Length: 50
    Type: UPDATE Message (2)
    Withdrawn Routes Length: 0
    Total Path Attribute Length: 25
  ▸ Path attributes
  ▾ Network Layer Reachability Information (NLRI)
    ▸ 13.0.0.0/8
```

After connection establishment, R2 sent 2 UPDATE messages together with one of

the KEEPALIVE message(No72). UPDATE messages contain information used to notify peers about path changes and network layer reachability. From the screenshot, we can see R2 was notifying R1 about 2 paths: one to itself (12.0.0.0/8) and another to AS3(13.0.0.0/8). R1 also responds with an UPDATE message that contains path information to itself(11.0.0.0/8) (No73).

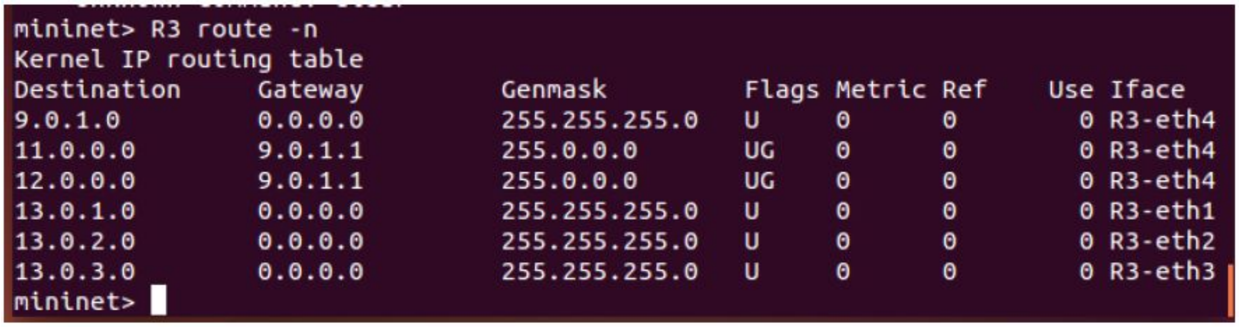
Reaching h31 (13.0.1.1) from h11

We are able to reach h31 from h11 through ping.

Reaching h31 (13.0.1.1) from R1

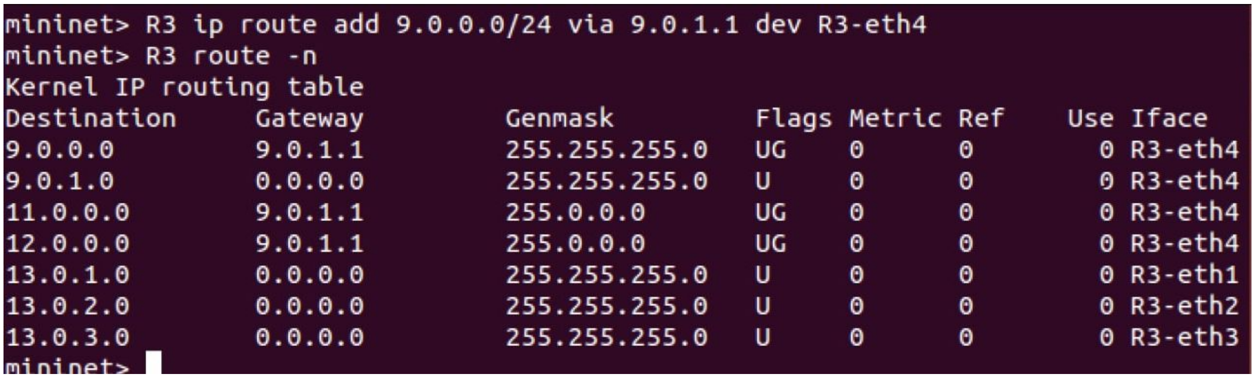
We are unable to reach h31 from R3

The reason behind this is because R3’s routing table contains an entry that instructs it to send packets from h1* host whose IP address matches 11.0.0.0/8 mask but does not contains an entry about routing on R1’s IP address (9.0.0.1).



```
mininet> R3 route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
9.0.1.0         0.0.0.0         255.255.255.0   U     0      0        0 R3-eth4
11.0.0.0        9.0.1.1         255.0.0.0       UG    0      0        0 R3-eth4
12.0.0.0        9.0.1.1         255.0.0.0       UG    0      0        0 R3-eth4
13.0.1.0        0.0.0.0         255.255.255.0   U     0      0        0 R3-eth1
13.0.2.0        0.0.0.0         255.255.255.0   U     0      0        0 R3-eth2
13.0.3.0        0.0.0.0         255.255.255.0   U     0      0        0 R3-eth3
mininet>
```

We used the command: “ip route add [network/subnetmask] via [gateway] dev [interface]” to add R1 routing into R3’s routing table in order to resolve the issue

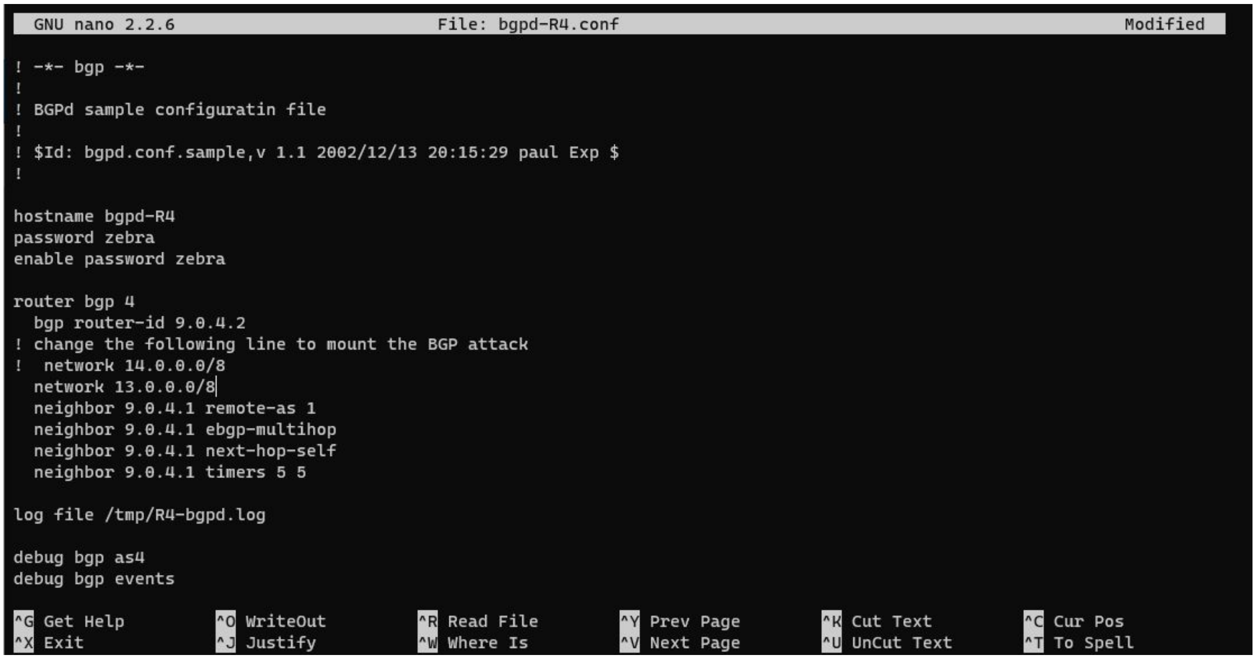


```
mininet> R3 ip route add 9.0.0.0/24 via 9.0.1.1 dev R3-eth4
mininet> R3 route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
9.0.0.0         9.0.1.1         255.255.255.0   UG    0      0        0 R3-eth4
9.0.1.0         0.0.0.0         255.255.255.0   U     0      0        0 R3-eth4
11.0.0.0        9.0.1.1         255.0.0.0       UG    0      0        0 R3-eth4
12.0.0.0        9.0.1.1         255.0.0.0       UG    0      0        0 R3-eth4
13.0.1.0        0.0.0.0         255.255.255.0   U     0      0        0 R3-eth1
13.0.2.0        0.0.0.0         255.255.255.0   U     0      0        0 R3-eth2
13.0.3.0        0.0.0.0         255.255.255.0   U     0      0        0 R3-eth3
mininet>
```

After that, we were able to ping h31 from R1.

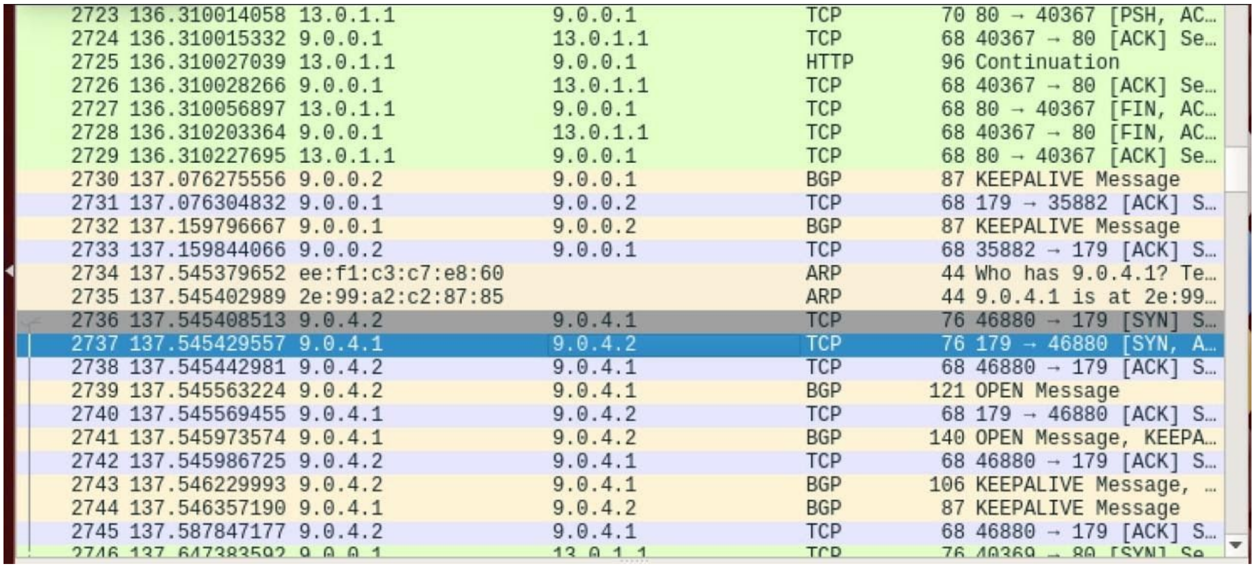
BGP Attack!

To launch to attack, we modified the network field of the bgpd-R4.conf as below.



```
  GNU nano 2.2.6                    File: bgpd-R4.conf                              Modified

! -*- bgp -*-
!
! BGPd sample configuratin file
!
! $Id: bgpd.conf.sample,v 1.1 2002/12/13 20:15:29 paul Exp $
!

hostname bgpd-R4
password zebra
enable password zebra

router bgp 4
  bgp router-id 9.0.4.2
! change the following line to mount the BGP attack
!  network 14.0.0.0/8
  network 13.0.0.0/8
  neighbor 9.0.4.1 remote-as 1
  neighbor 9.0.4.1 ebgp-multihop
  neighbor 9.0.4.1 next-hop-self
  neighbor 9.0.4.1 timers 5 5

log file /tmp/R4-bgpd.log

debug bgp as4
debug bgp events

^G Get Help     ^O WriteOut     ^R Read File    ^Y Prev Page    ^K Cut Text     ^C Cur Pos
^X Exit         ^J Justify      ^W Where Is     ^V Next Page    ^U UnCut Text   ^T To Spell
```

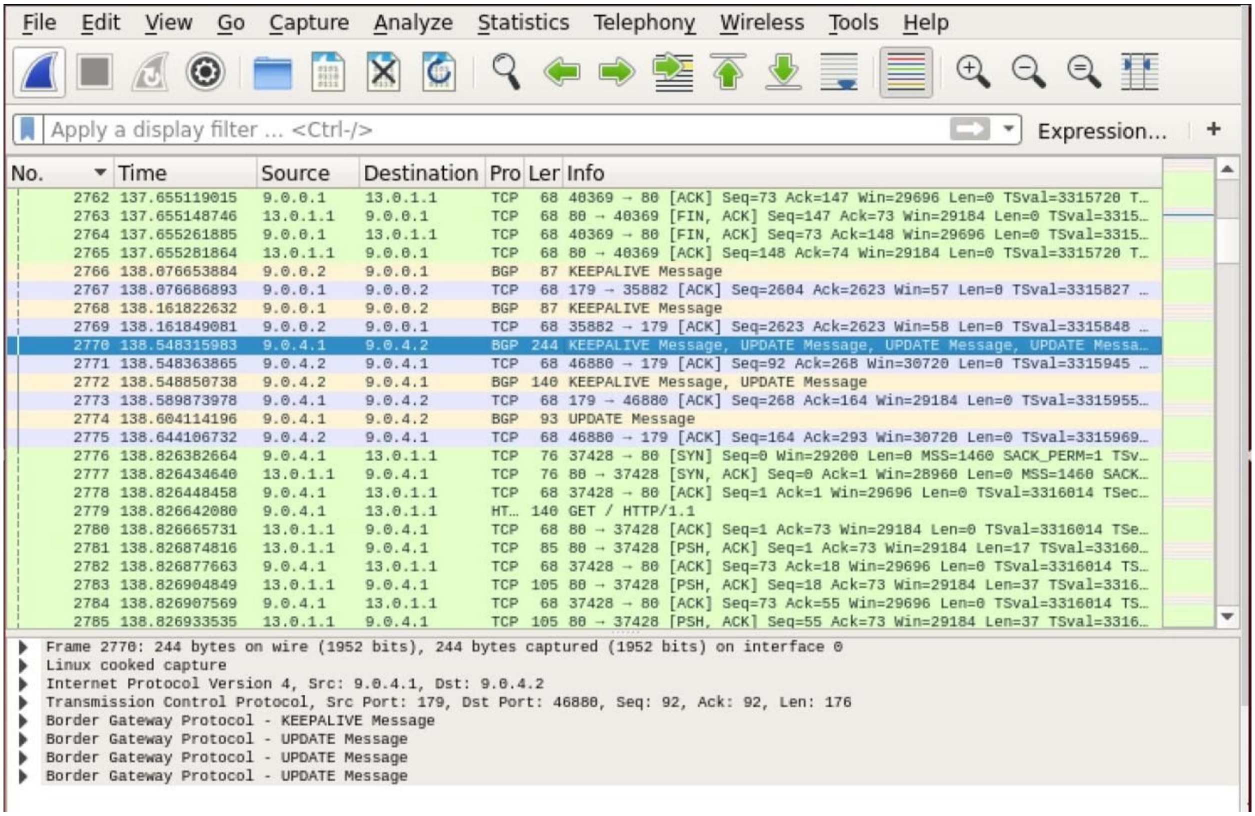
Essentially what we did is to let R4 announce to the network that it has paths that route packets from 13.0.0.0/8.



```
2723 136.310014058 13.0.1.1           9.0.0.1     TCP     70 80 → 40367 [PSH, AC…
2724 136.310015332 9.0.0.1            13.0.1.1    TCP     68 40367 → 80 [ACK] Se…
2725 136.310027039 13.0.1.1           9.0.0.1     HTTP    96 Continuation
2726 136.310028266 9.0.0.1            13.0.1.1    TCP     68 40367 → 80 [ACK] Se…
2727 136.310056897 13.0.1.1           9.0.0.1     TCP     68 80 → 40367 [FIN, AC…
2728 136.310203364 9.0.0.1            13.0.1.1    TCP     68 40367 → 80 [FIN, AC…
2729 136.310227695 13.0.1.1           9.0.0.1     TCP     68 80 → 40367 [ACK] Se…
2730 137.076275556 9.0.0.2            9.0.0.1     BGP     87 KEEPALIVE Message
2731 137.076304832 9.0.0.1            9.0.0.2     TCP     68 179 → 35882 [ACK] S…
2732 137.159796667 9.0.0.1            9.0.0.2     BGP     87 KEEPALIVE Message
2733 137.159844066 9.0.0.2            9.0.0.1     TCP     68 35882 → 179 [ACK] S…
2734 137.545379652 ee:f1:c3:c7:e8:60              ARP     44 Who has 9.0.4.1? Te…
2735 137.545402989 2e:99:a2:c2:87:85              ARP     44 9.0.4.1 is at 2e:99…
2736 137.545408513 9.0.4.2            9.0.4.1     TCP     76 46880 → 179 [SYN] S…
2737 137.545429557 9.0.4.1            9.0.4.2     TCP     76 179 → 46880 [SYN, A…
2738 137.545442981 9.0.4.2            9.0.4.1     TCP     68 46880 → 179 [ACK] S…
2739 137.545563224 9.0.4.2            9.0.4.1     BGP    121 OPEN Message
2740 137.545569455 9.0.4.1            9.0.4.2     TCP     68 179 → 46880 [ACK] S…
2741 137.545973574 9.0.4.1            9.0.4.2     BGP    140 OPEN Message, KEEPA…
2742 137.545986725 9.0.4.2            9.0.4.1     TCP     68 46880 → 179 [ACK] S…
2743 137.546229993 9.0.4.2            9.0.4.1     BGP    106 KEEPALIVE Message, …
2744 137.546357190 9.0.4.1            9.0.4.2     BGP     87 KEEPALIVE Message
2745 137.587847177 9.0.4.2            9.0.4.1     TCP     68 46880 → 179 [ACK] S…
2746 137.647383592 9.0.0.1            13.0.1.1    TCP     76 40369 → 80 [SYN] Se
```

Before the attack, we can see the HTTP request was responded to by source 9.0.0.1.

When the attack starts, a new BGP session was initiated between R1 and R4 similar to the one between R1 and R2 described above.

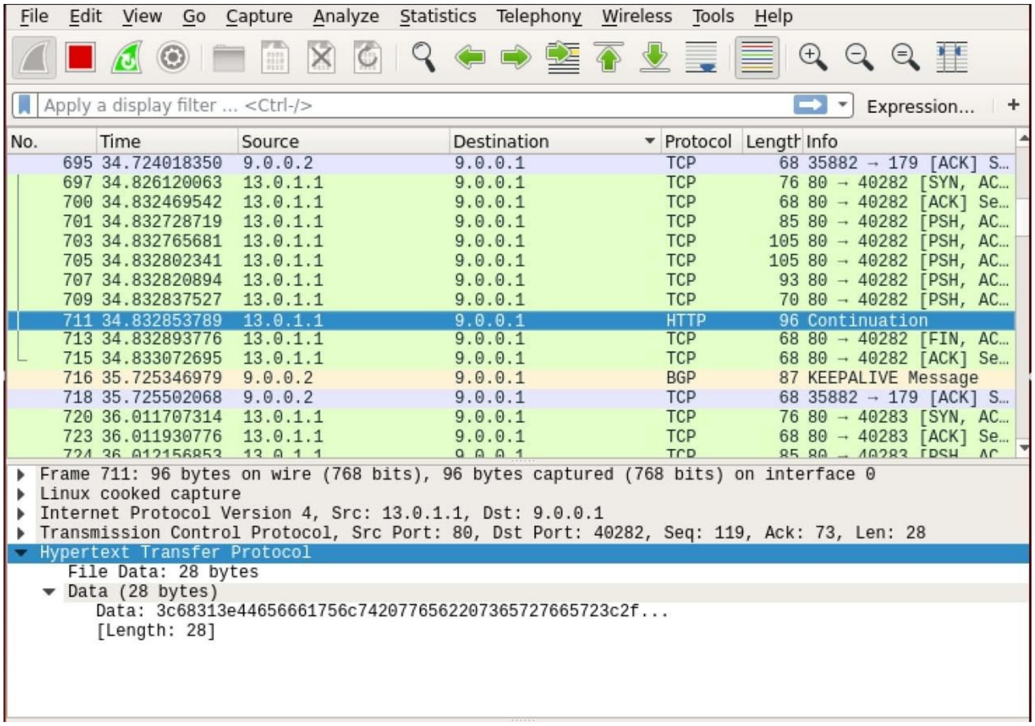


```
No.    Time         Source     Destination  Pro Ler Info
  2762 137.655119015 9.0.0.1    13.0.1.1     TCP  68 40369 → 80 [ACK] Seq=73 Ack=147 Win=29696 Len=0 TSval=3315720 T…
  2763 137.655148746 13.0.1.1   9.0.0.1      TCP  68 80 → 40369 [FIN, ACK] Seq=147 Ack=73 Win=29184 Len=0 TSval=3315…
  2764 137.655261885 9.0.0.1    13.0.1.1     TCP  68 40369 → 80 [FIN, ACK] Seq=73 Ack=148 Win=29696 Len=0 TSval=3315…
  2765 137.655281864 13.0.1.1   9.0.0.1      TCP  68 80 → 40369 [ACK] Seq=148 Ack=74 Win=29184 Len=0 TSval=3315720 T…
  2766 138.076653884 9.0.0.2    9.0.0.1      BGP  87 KEEPALIVE Message
  2767 138.076686893 9.0.0.1    9.0.0.2      TCP  68 179 → 35882 [ACK] Seq=2604 Ack=2623 Win=57 Len=0 TSval=3315827 …
  2768 138.161822632 9.0.0.1    9.0.0.2      BGP  87 KEEPALIVE Message
  2769 138.161849081 9.0.0.2    9.0.0.1      TCP  68 35882 → 179 [ACK] Seq=2623 Ack=2623 Win=58 Len=0 TSval=3315848 …
  2770 138.548315983 9.0.4.1    9.0.4.2      BGP 244 KEEPALIVE Message, UPDATE Message, UPDATE Message, UPDATE Messa…
  2771 138.548363865 9.0.4.2    9.0.4.1      TCP  68 46880 → 179 [ACK] Seq=92 Ack=268 Win=30720 Len=0 TSval=3315945 …
  2772 138.548850738 9.0.4.2    9.0.4.1      BGP 140 KEEPALIVE Message, UPDATE Message
  2773 138.589873978 9.0.4.1    9.0.4.2      TCP  68 179 → 46880 [ACK] Seq=268 Ack=164 Win=29184 Len=0 TSval=3315955…
  2774 138.604114196 9.0.4.1    9.0.4.2      BGP  93 UPDATE Message
  2775 138.644106732 9.0.4.2    9.0.4.1      TCP  68 46880 → 179 [ACK] Seq=164 Ack=293 Win=30720 Len=0 TSval=3315969…
  2776 138.826382664 9.0.4.1    13.0.1.1     TCP  76 37428 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSv…
  2777 138.826434640 13.0.1.1   9.0.4.1      TCP  76 80 → 37428 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK…
  2778 138.826448458 9.0.4.1    13.0.1.1     TCP  68 37428 → 80 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=3316014 TSec…
  2779 138.826642080 9.0.4.1    13.0.1.1     HT… 140 GET / HTTP/1.1
  2780 138.826665731 13.0.1.1   9.0.4.1      TCP  68 80 → 37428 [ACK] Seq=1 Ack=73 Win=29184 Len=0 TSval=3316014 TSe…
  2781 138.826874816 13.0.1.1   9.0.4.1      TCP  85 80 → 37428 [PSH, ACK] Seq=1 Ack=73 Win=29184 Len=17 TSval=33160…
  2782 138.826877663 9.0.4.1    13.0.1.1     TCP  68 37428 → 80 [ACK] Seq=73 Ack=18 Win=29696 Len=0 TSval=3316014 TS…
  2783 138.826904849 13.0.1.1   9.0.4.1      TCP 105 80 → 37428 [PSH, ACK] Seq=18 Ack=73 Win=29184 Len=37 TSval=3316…
  2784 138.826907569 9.0.4.1    13.0.1.1     TCP  68 37428 → 80 [ACK] Seq=73 Ack=55 Win=29696 Len=0 TSval=3316014 TS…
  2785 138.826933535 13.0.1.1   9.0.4.1      TCP 105 80 → 37428 [PSH, ACK] Seq=55 Ack=73 Win=29184 Len=37 TSval=3316…
```

```
▶ Frame 2770: 244 bytes on wire (1952 bits), 244 bytes captured (1952 bits) on interface 0
▶ Linux cooked capture
▶ Internet Protocol Version 4, Src: 9.0.4.1, Dst: 9.0.4.2
▶ Transmission Control Protocol, Src Port: 179, Dst Port: 46880, Seq: 92, Ack: 92, Len: 176
▶ Border Gateway Protocol - KEEPALIVE Message
▶ Border Gateway Protocol - UPDATE Message
▶ Border Gateway Protocol - UPDATE Message
▶ Border Gateway Protocol - UPDATE Message
```

After the UPDATE Message exchange between R1 and R4. We can see the source port changed to 9.0.4.1, indicating that 13.0.1.1 is now the malicious host.

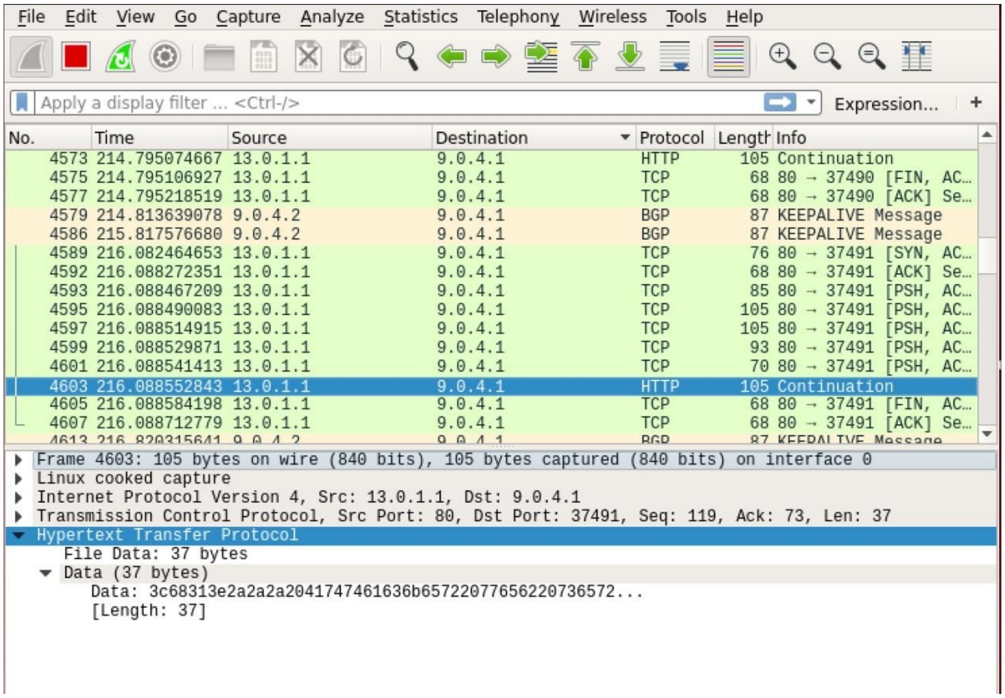
Original packet size is 28 bytes from source 9.0.0.1



```
No.   Time          Source        Destination    Protocol Length Info
  695 34.724018350  9.0.0.2       9.0.0.1        TCP        68 35882 → 179 [ACK] S…
  697 34.826120063  13.0.1.1      9.0.0.1        TCP        76 80 → 40282 [SYN, AC…
  700 34.832469542  13.0.1.1      9.0.0.1        TCP        68 80 → 40282 [ACK] Se…
  701 34.832728719  13.0.1.1      9.0.0.1        TCP        85 80 → 40282 [PSH, AC…
  703 34.832765681  13.0.1.1      9.0.0.1        TCP       105 80 → 40282 [PSH, AC…
  705 34.832802341  13.0.1.1      9.0.0.1        TCP       105 80 → 40282 [PSH, AC…
  707 34.832820894  13.0.1.1      9.0.0.1        TCP        93 80 → 40282 [PSH, AC…
  709 34.832837527  13.0.1.1      9.0.0.1        TCP        70 80 → 40282 [PSH, AC…
  711 34.832853789  13.0.1.1      9.0.0.1        HTTP       96 Continuation
  713 34.832893776  13.0.1.1      9.0.0.1        TCP        68 80 → 40282 [FIN, AC…
  715 34.833072695  13.0.1.1      9.0.0.1        TCP        68 80 → 40282 [ACK] Se…
  716 35.725346979  9.0.0.2       9.0.0.1        BGP        87 KEEPALIVE Message
  718 35.725502068  9.0.0.2       9.0.0.1        TCP        68 35882 → 179 [ACK] S…
  720 36.011707314  13.0.1.1      9.0.0.1        TCP        76 80 → 40283 [SYN, AC…
  723 36.011930776  13.0.1.1      9.0.0.1        TCP        68 80 → 40283 [ACK] Se…
  724 36.012156853  13.0.1.1      9.0.0.1        TCP        85 80 → 40283 [PSH, AC…
```

```
▶ Frame 711: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface 0
▶ Linux cooked capture
▶ Internet Protocol Version 4, Src: 13.0.1.1, Dst: 9.0.0.1
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 40282, Seq: 119, Ack: 73, Len: 28
▼ Hypertext Transfer Protocol
    File Data: 28 bytes
  ▼ Data (28 bytes)
      Data: 3c68313e44656661756c7420776562207365727665723c2f...
      [Length: 28]
```

The malicious packet size is 37 bytes from source 9.0.4.1



```
No.   Time           Source        Destination    Protocol Length Info
 4573 214.795074667  13.0.1.1      9.0.4.1        HTTP      105 Continuation
 4575 214.795106927  13.0.1.1      9.0.4.1        TCP        68 80 → 37490 [FIN, AC…
 4577 214.795218519  13.0.1.1      9.0.4.1        TCP        68 80 → 37490 [ACK] Se…
 4579 214.813639078  9.0.4.2       9.0.4.1        BGP        87 KEEPALIVE Message
 4586 215.817576680  9.0.4.2       9.0.4.1        BGP        87 KEEPALIVE Message
 4589 216.082464653  13.0.1.1      9.0.4.1        TCP        76 80 → 37491 [SYN, AC…
 4592 216.088272351  13.0.1.1      9.0.4.1        TCP        68 80 → 37491 [ACK] Se…
 4593 216.088467209  13.0.1.1      9.0.4.1        TCP        85 80 → 37491 [PSH, AC…
 4595 216.088490083  13.0.1.1      9.0.4.1        TCP       105 80 → 37491 [PSH, AC…
 4597 216.088514915  13.0.1.1      9.0.4.1        TCP       105 80 → 37491 [PSH, AC…
 4599 216.088529871  13.0.1.1      9.0.4.1        TCP        93 80 → 37491 [PSH, AC…
 4601 216.088541413  13.0.1.1      9.0.4.1        TCP        70 80 → 37491 [PSH, AC…
 4603 216.088552843  13.0.1.1      9.0.4.1        HTTP      105 Continuation
 4605 216.088584198  13.0.1.1      9.0.4.1        TCP        68 80 → 37491 [FIN, AC…
 4607 216.088712779  13.0.1.1      9.0.4.1        TCP        68 80 → 37491 [ACK] Se…
 4613 216.820315641  9.0.4.2       9.0.4.1        BGP        87 KEEPALIVE Message
```

```
▶ Frame 4603: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface 0
▶ Linux cooked capture
▶ Internet Protocol Version 4, Src: 13.0.1.1, Dst: 9.0.4.1
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 37491, Seq: 119, Ack: 73, Len: 37
▼ Hypertext Transfer Protocol
    File Data: 37 bytes
  ▼ Data (37 bytes)
      Data: 3c68313e2a2a2a2041747461636b65722077656220736572...
      [Length: 37]
```