

# Mininet Assignment Report

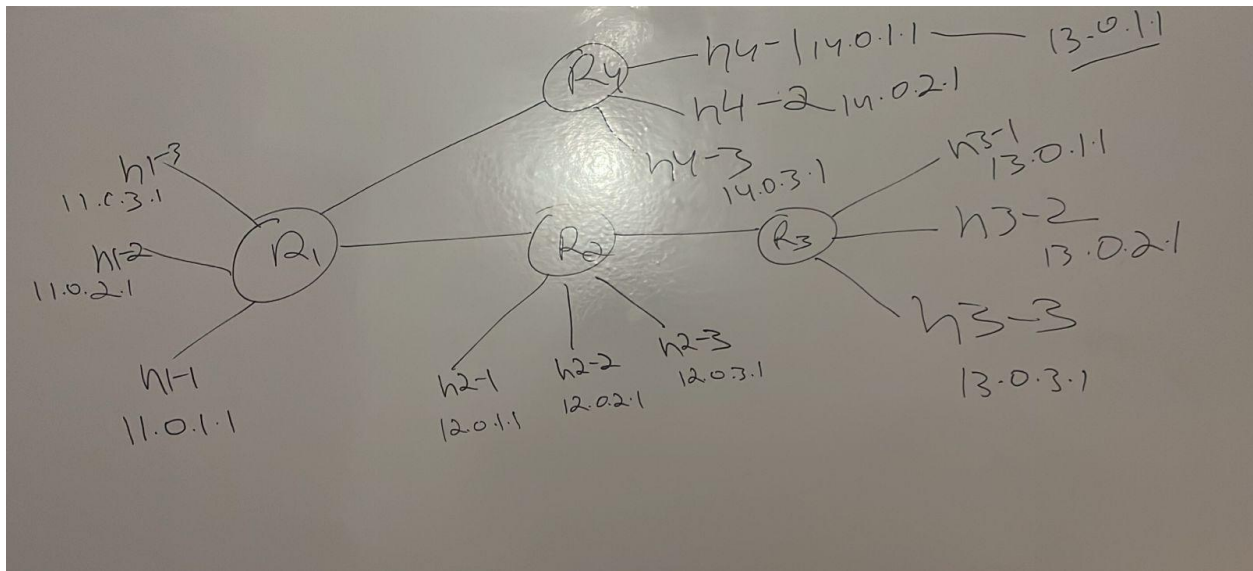
Sanyam Kaul - CS23MTECH14011

Bhargav Patel - CS23MTECH11026

Arnab Ghosh - CS23MTECH11025

---

Ans 1.



4 routers represent 4 subnets - R1, R2, R3 and R4

Each subnet has 3 hosts as represented in the diagram above

## Ans 2.

Snapshots of Interfaces with IP address info: -

R1 -

```
root@mininet-vml:/bgp# ifconfig
R1-eth1  Link encap:Ethernet  HWaddr a2:d1:48:3c:32:23
          inet addr:11.0.1.254  Bcast:11.0.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a0d1:48ff:fe3c:3223/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:948 errors:0 dropped:0 overruns:0 frame:0
          TX packets:948 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:71032 (71.0 KB)  TX bytes:77697 (77.6 KB)

R1-eth2  Link encap:Ethernet  HWaddr ce:6f:55:d5:20:ac
          inet addr:11.0.2.254  Bcast:11.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::cc6f:55ff:fed5:20ac/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:648 (648.0 B)  TX bytes:648 (648.0 B)

R1-eth3  Link encap:Ethernet  HWaddr a6:61:7f:18:14:48
          inet addr:11.0.3.254  Bcast:11.0.3.255  Mask:255.255.255.0
          inet6 addr: fe80::a61:7fff:fe18:1448/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:29 errors:0 dropped:0 overruns:0 frame:0
          TX packets:29 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2594 (2.5 KB)  TX bytes:2594 (2.5 KB)

R1-eth4  Link encap:Ethernet  HWaddr 86:6a:6e:c6:7e:a0
          inet addr:9.0.0.1  Bcast:9.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::846a:6eff:fec6:7ea0/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:12246 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12712 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:957386 (957.3 KB)  TX bytes:983266 (983.2 KB)

R1-eth5  Link encap:Ethernet  HWaddr 0a:05:cd:d9:27:3a
          inet addr:9.0.4.1  Bcast:9.0.4.255  Mask:255.255.255.0
          inet6 addr: fe80::805:cdff:fed9:273a/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3534 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4231 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:278975 (278.8 KB)  TX bytes:323900 (323.9 KB)

lo       Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:300 errors:0 dropped:0 overruns:0 frame:0
          TX packets:300 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:25010 (25.0 KB)  TX bytes:25010 (25.0 KB)

root@mininet-vml:/bgp#
```

R2 -

**Node: R2**

```
root@mininet-vm:~/bgp# ifconfig
R2-eth1  Link encap:Ethernet  HWaddr c6:6e:22:b2:a5:64
         inet addr:12.0.1.254  Bcast:12.0.1.255  Mask:255.255.255.0
         inet6 addr: fe80::c46e:22ff:feb2:a564/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:122 errors:0 dropped:0 overruns:0 frame:0
         TX packets:122 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:8956 (8.9 KB)  TX bytes:9770 (9.7 KB)

R2-eth2  Link encap:Ethernet  HWaddr de:40:ad:0c:ca:64
         inet addr:12.0.2.254  Bcast:12.0.2.255  Mask:255.255.255.0
         inet6 addr: fe80::dc40:adff:fe0c:ca64/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:8 errors:0 dropped:0 overruns:0 frame:0
         TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:648 (648.0 B)  TX bytes:648 (648.0 B)

R2-eth3  Link encap:Ethernet  HWaddr e6:28:f3:c5:c4:81
         inet addr:12.0.3.254  Bcast:12.0.3.255  Mask:255.255.255.0
         inet6 addr: fe80::e428:f3ff:fec5:c481/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:8 errors:0 dropped:0 overruns:0 frame:0
         TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:648 (648.0 B)  TX bytes:648 (648.0 B)

R2-eth4  Link encap:Ethernet  HWaddr 6e:eb:5f:db:a7:11
         inet addr:9.0.0.2  Bcast:9.0.0.255  Mask:255.255.255.0
         inet6 addr: fe80::6ceb:5fff:fedb:a711/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:12558 errors:0 dropped:0 overruns:0 frame:0
         TX packets:12070 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:971145 (971.1 KB)  TX bytes:943813 (943.8 KB)

R2-eth5  Link encap:Ethernet  HWaddr 46:d0:8c:23:10:19
         inet addr:9.0.1.1  Bcast:9.0.1.255  Mask:255.255.255.0
         inet6 addr: fe80::44d0:8cff:fe23:1019/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:12269 errors:0 dropped:0 overruns:0 frame:0
         TX packets:12531 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:958534 (958.5 KB)  TX bytes:969861 (969.8 KB)

lo       Link encap:Local Loopback
         inet addr:127.0.0.1  Mask:255.0.0.0
         inet6 addr: ::1/128 Scope:Host
         UP LOOPBACK RUNNING  MTU:65536  Metric:1
         RX packets:177 errors:0 dropped:0 overruns:0 frame:0
         TX packets:177 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         RX bytes:14674 (14.6 KB)  TX bytes:14674 (14.6 KB)

root@mininet-vm:~/bgp#
```

```
Node: R3
root@mininet-vm:~/bgp# ifconfig
R3-eth1  Link encap:Ethernet  HWaddr 56:d0:33:b6:4c:a0
        inet addr:13.0.1.254  Bcast:13.0.1.255  Mask:255.255.255.0
        inet6 addr: fe80::54d0:33ff:feb6:4ca0/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:845 errors:0 dropped:0 overruns:0 frame:0
        TX packets:845 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:68390 (68.3 KB)  TX bytes:62322 (62.3 KB)

R3-eth2  Link encap:Ethernet  HWaddr 2e:8e:77:5e:77:2b
        inet addr:13.0.2.254  Bcast:13.0.2.255  Mask:255.255.255.0
        inet6 addr: fe80::2c8e:77ff:fe5e:772b/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:8 errors:0 dropped:0 overruns:0 frame:0
        TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:648 (648.0 B)  TX bytes:648 (648.0 B)

R3-eth3  Link encap:Ethernet  HWaddr fe:25:05:19:ce:39
        inet addr:13.0.3.254  Bcast:13.0.3.255  Mask:255.255.255.0
        inet6 addr: fe80::fc25:5ff:fe19:ce39/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:8 errors:0 dropped:0 overruns:0 frame:0
        TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:648 (648.0 B)  TX bytes:648 (648.0 B)

R3-eth4  Link encap:Ethernet  HWaddr ae:77:48:e8:26:f1
        inet addr:9.0.1.2  Bcast:9.0.1.255  Mask:255.255.255.0
        inet6 addr: fe80::ac77:48ff:fee8:26f1/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:12773 errors:0 dropped:0 overruns:0 frame:0
        TX packets:12487 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:988588 (988.5 KB)  TX bytes:975677 (975.6 KB)

lo       Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

root@mininet-vm:~/bgp#
```

```
Node: R4
root@mininet-vm:~/bgp# ifconfig
R4-eth1  Link encap:Ethernet  HWaddr 2a:42:0f:e9:fc:0e
        inet addr:13.0.1.254 Bcast:13.0.1.255 Mask:255.255.255.0
        inet6 addr: fe80::2842:fff:fee9:fc0e/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:211 errors:0 dropped:0 overruns:0 frame:0
        TX packets:211 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:17425 (17.4 KB)  TX bytes:16014 (16.0 KB)

R4-eth2  Link encap:Ethernet  HWaddr c6:3e:93:b3:9c:ff
        inet addr:13.0.2.254 Bcast:13.0.2.255 Mask:255.255.255.0
        inet6 addr: fe80::c43e:93ff:feb3:9cff/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:8 errors:0 dropped:0 overruns:0 frame:0
        TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:648 (648.0 B)  TX bytes:648 (648.0 B)

R4-eth3  Link encap:Ethernet  HWaddr fa:e8:6b:46:ee:fc
        inet addr:13.0.3.254 Bcast:13.0.3.255 Mask:255.255.255.0
        inet6 addr: fe80::f8e8:6bff:fe46:eeff/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:8 errors:0 dropped:0 overruns:0 frame:0
        TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:648 (648.0 B)  TX bytes:648 (648.0 B)

R4-eth4  Link encap:Ethernet  HWaddr a6:c2:2a:36:fb:54
        inet addr:9.0.4.2 Bcast:9.0.4.255 Mask:255.255.255.0
        inet6 addr: fe80::a4c2:2aff:fe36:fb54/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:4300 errors:0 dropped:0 overruns:0 frame:0
        TX packets:3545 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:324813 (324.8 KB)  TX bytes:279791 (279.7 KB)

lo       Link encap:Local Loopback
        inet addr:127.0.0.1 Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

root@mininet-vm:~/bgp#
```

Hosts' IP addresses are mentioned in the diagram in the previous answer

Hosts of AS4 do not have any IP address at this time. They are assigned IP addresses when we run the `./start_router.py` script

Ans 3.

h3-1 is reachable from h1-1

```
Node: h1-1
64 bytes from 11.0.3.1: icmp_seq=1 ttl=63 time=0.186 ms
64 bytes from 11.0.3.1: icmp_seq=2 ttl=63 time=0.025 ms
64 bytes from 11.0.3.1: icmp_seq=3 ttl=63 time=0.028 ms
64 bytes from 11.0.3.1: icmp_seq=4 ttl=63 time=0.026 ms
64 bytes from 11.0.3.1: icmp_seq=5 ttl=63 time=0.028 ms
64 bytes from 11.0.3.1: icmp_seq=6 ttl=63 time=0.046 ms
64 bytes from 11.0.3.1: icmp_seq=7 ttl=63 time=0.030 ms
64 bytes from 11.0.3.1: icmp_seq=8 ttl=63 time=0.032 ms
64 bytes from 11.0.3.1: icmp_seq=9 ttl=63 time=0.028 ms
64 bytes from 11.0.3.1: icmp_seq=10 ttl=63 time=0.029 ms
64 bytes from 11.0.3.1: icmp_seq=11 ttl=63 time=0.045 ms
64 bytes from 11.0.3.1: icmp_seq=12 ttl=63 time=0.027 ms
64 bytes from 11.0.3.1: icmp_seq=13 ttl=63 time=0.063 ms
64 bytes from 11.0.3.1: icmp_seq=14 ttl=63 time=0.030 ms
64 bytes from 11.0.3.1: icmp_seq=15 ttl=63 time=0.026 ms
64 bytes from 11.0.3.1: icmp_seq=16 ttl=63 time=0.024 ms
64 bytes from 11.0.3.1: icmp_seq=17 ttl=63 time=0.044 ms
64 bytes from 11.0.3.1: icmp_seq=18 ttl=63 time=0.029 ms
64 bytes from 11.0.3.1: icmp_seq=19 ttl=63 time=0.028 ms
^C
--- 11.0.3.1 ping statistics ---
19 packets transmitted, 19 received, 0% packet loss, time 17998ms
rtt min/avg/max/mdev = 0.024/0.040/0.186/0.036 ms
root@mininet-vm:~/bgp#
```

H3-1 reachable from h2-1

```
Node: h2-1
root@mininet-vm:~/bgp# ping 13.0.1.1
PING 13.0.1.1 (13.0.1.1) 56(84) bytes of data.
64 bytes from 13.0.1.1: icmp_seq=1 ttl=62 time=0.269 ms
64 bytes from 13.0.1.1: icmp_seq=2 ttl=62 time=0.031 ms
64 bytes from 13.0.1.1: icmp_seq=3 ttl=62 time=0.034 ms
64 bytes from 13.0.1.1: icmp_seq=4 ttl=62 time=0.044 ms
^C
--- 13.0.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.031/0.094/0.269/0.101 ms
root@mininet-vm:~/bgp#
```

H3-1 reachable from h1-2

```
Node: h1-2
root@mininet-vm:~/bgp# ping 13.0.1.1
PING 13.0.1.1 (13.0.1.1) 56(84) bytes of data.
64 bytes from 13.0.1.1: icmp_seq=1 ttl=62 time=0.817 ms
64 bytes from 13.0.1.1: icmp_seq=2 ttl=62 time=0.072 ms
64 bytes from 13.0.1.1: icmp_seq=3 ttl=62 time=0.043 ms
64 bytes from 13.0.1.1: icmp_seq=4 ttl=62 time=0.029 ms
64 bytes from 13.0.1.1: icmp_seq=5 ttl=62 time=0.029 ms
64 bytes from 13.0.1.1: icmp_seq=6 ttl=62 time=0.032 ms
^C
--- 13.0.1.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5000ms
rtt min/avg/max/mdev = 0.029/0.170/0.817/0.289 ms
root@mininet-vm:~/bgp#
```

Ans4

The BGP tables provide information about the learned routes to different hosts in different ASes

R1 BGP table

```
mininet@mininet-vm: ~/bgp
File Edit Tabs Help
Escape character is '^]'.
Hello, this is Quagga (version 0.99.22.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

User Access Verification

Password:
bgpd-R1> en
Password:
bgpd-R1# sh ip bgp
BGP table version is 0, local router ID is 9.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network        Next Hop           Metric LocPrf Weight Path
*> 11.0.0.0        0.0.0.0              0         32768 i
*> 12.0.0.0        9.0.0.2              0           2 2 i
*> 13.0.0.0        9.0.0.2              0           2 2 3 i

Total number of prefixes 3
bgpd-R1#
```

A brief explanation of the different fields of the table:-

Network - This is the network address of the destination network in CIDR notation

Next Hop - This field provides the IP address of the next hop router to reach the destination network

Metric - This indicates the cost of the path (a lower cost is preferred)

LocPrf - Stands for Local Preference. It is a value used within the AS to influence the outbound routing decisions

Weight - A CISCO-specific parameter indicating the local preference for a route

Path - It shows the route's path through different ASes. The 'i' value means that the route was learned from an interior gateway protocol. For example, as per the table if a packet has to be delivered to a host in AS3 then first R1 will deliver it to R2 (lp - 9.0.0.2), then R@ will deliver it to R3 and finally the internal route from R3 to host will be learned at R3 only. That's why the weighted path says '2 3 i'

Ans 5

```
mininet@mininet-vm: ~/bgp
File Edit Tabs Help
Escape character is '^]'.
Hello, this is Quagga (version 0.99.22.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

User Access Verification

Password:
bgpd-R2> en
Password:
bgpd-R2# sh ip bgp
BGP table version is 0, local router ID is 9.0.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network        Next Hop        Metric LocPrf Weight Path
*> 11.0.0.0        9.0.0.1          0         0 1 i
*> 12.0.0.0        0.0.0.0          0        32768 i
*> 13.0.0.0        9.0.1.2          0         0 3 i

Total number of prefixes 3
bgpd-R2#
```

The next hop, weight and Path values are different for Network CIDRs as compared to R1

Since 12.0.0.0 is the local AS of R2 that's why its Next Hop is 0.0.0.0 and Path is 'i'.

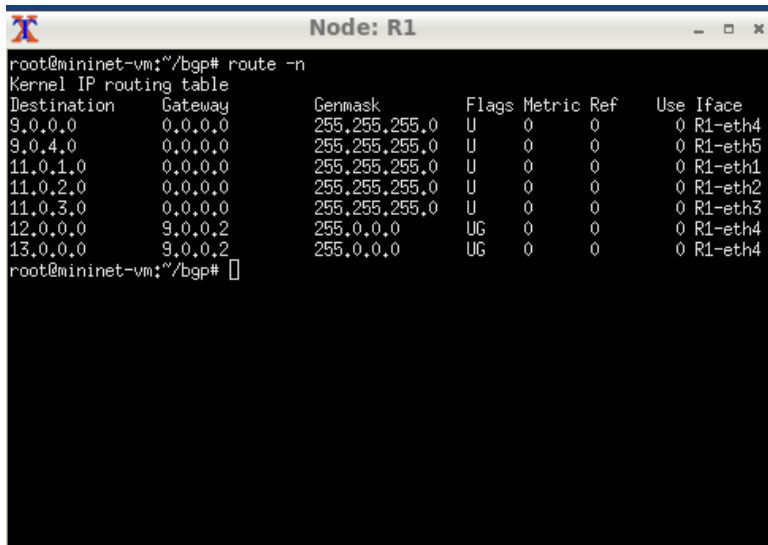
In the case of R1 11.0.0.0 is the local AS, so its next hop is 0.0.0.0 and Path is 'i'.



Also, note that the Path to go to 11.0.0.0 is '1 i' which means that the packet will be delivered to R1 in the next hop (Next hop - 9.0.0.1) and the Path to go to 13.0.0.0 is '3 i' which means that the packet will be delivered to R3 in next hop (9.0.1.2)

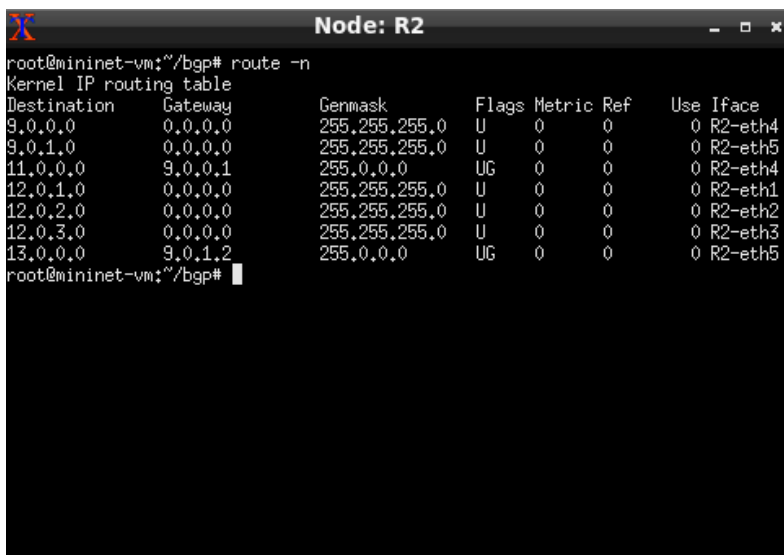
Ans 6

R1 forwarding table

A terminal window titled "Node: R1" showing the output of the command "root@mininet-vm:~/bgp# route -n". It displays the Kernel IP routing table with columns for Destination, Gateway, Genmask, Flags, Metric, Ref, Use, and Iface. The table lists routes for destinations 9.0.0.0, 9.0.4.0, 11.0.1.0, 11.0.2.0, 11.0.3.0, 12.0.0.0, and 13.0.0.0, all pointing to gateway 0.0.0.0 and using interfaces R1-eth4 through R1-eth5. The last two entries (12.0.0.0 and 13.0.0.0) are marked with 'UG' in the Flags column.

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
9.0.0.0	0.0.0.0	255.255.255.0	U	0	0	0	R1-eth4
9.0.4.0	0.0.0.0	255.255.255.0	U	0	0	0	R1-eth5
11.0.1.0	0.0.0.0	255.255.255.0	U	0	0	0	R1-eth1
11.0.2.0	0.0.0.0	255.255.255.0	U	0	0	0	R1-eth2
11.0.3.0	0.0.0.0	255.255.255.0	U	0	0	0	R1-eth3
12.0.0.0	9.0.0.2	255.0.0.0	UG	0	0	0	R1-eth4
13.0.0.0	9.0.0.2	255.0.0.0	UG	0	0	0	R1-eth4

R2 forwarding table

A terminal window titled "Node: R2" showing the output of the command "root@mininet-vm:~/bgp# route -n". It displays the Kernel IP routing table with columns for Destination, Gateway, Genmask, Flags, Metric, Ref, Use, and Iface. The table lists routes for destinations 9.0.0.0, 9.0.1.0, 11.0.0.0, 12.0.1.0, 12.0.2.0, 12.0.3.0, and 13.0.0.0, all pointing to gateway 0.0.0.0 and using interfaces R2-eth4 through R2-eth5. The last two entries (12.0.0.0 and 13.0.0.0) are marked with 'UG' in the Flags column.

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
9.0.0.0	0.0.0.0	255.255.255.0	U	0	0	0	R2-eth4
9.0.1.0	0.0.0.0	255.255.255.0	U	0	0	0	R2-eth5
11.0.0.0	9.0.0.1	255.0.0.0	UG	0	0	0	R2-eth4
12.0.1.0	0.0.0.0	255.255.255.0	U	0	0	0	R2-eth1
12.0.2.0	0.0.0.0	255.255.255.0	U	0	0	0	R2-eth2
12.0.3.0	0.0.0.0	255.255.255.0	U	0	0	0	R2-eth3
13.0.0.0	9.0.1.2	255.0.0.0	UG	0	0	0	R2-eth5

The forwarding table is used locally the the router. We can see the routing table of R1 and infer that it is giving details about which interface the packet will be forwarded to if it is supposed to

be delivered to a particular IP address. The IP address can be of a host connected with R1 or is present in a different AS.

The interface information about the hosts connected to R1 is filled in the Forwarding table by Intra-Routing protocol which could be OSPF, IS-IS, RIP etc. The interface information about the network addresses of other ASes is filled in the Forwarding table by BGP

## Ans 7

Wireshark snapshot depicting TCP and HTTP packets flowing in the network when h1-1 is sending GET requests to the server running on host h3-1 :-

The image shows a Wireshark network traffic capture window. The title bar indicates it's running on Oracle VM VirtualBox. The main window shows a list of captured packets, with the first 100 packets displayed. The packets are primarily TCP and HTTP traffic. The first packet is a GET request from h1-1 to h3-1. The subsequent packets are TCP segments and HTTP responses. The packet list shows the following details:

No.	Time	Source	Destination	Protocol	Length	Info
52	2.078853000	13.0.1.1	11.0.1.1	TCP	91	[TCP segment of a reassembled PDU]
53	2.078854000	11.0.1.1	13.0.1.1	TCP	66	34210 > http [ACK] Seq=73 Ack=117 Win=29696 Len=0 TSval=757159 TSecr=757159
54	2.078861000	13.0.1.1	11.0.1.1	TCP	68	[TCP segment of a reassembled PDU]
55	2.078862000	11.0.1.1	13.0.1.1	TCP	66	34210 > http [ACK] Seq=73 Ack=119 Win=29696 Len=0 TSval=757159 TSecr=757159
56	2.078868000	13.0.1.1	11.0.1.1	HTTP	94	Continuation or non-HTTP traffic
57	2.078869000	11.0.1.1	13.0.1.1	TCP	66	34210 > http [ACK] Seq=73 Ack=147 Win=29696 Len=0 TSval=757159 TSecr=757159
58	2.078885000	13.0.1.1	11.0.1.1	TCP	66	http > 34210 [FIN, ACK] Seq=147 Ack=73 Win=29184 Len=0 TSval=757159 TSecr=7
59	2.078930000	11.0.1.1	13.0.1.1	TCP	66	34210 > http [FIN, ACK] Seq=73 Ack=148 Win=29696 Len=0 TSval=757159 TSecr=7
60	2.078939000	13.0.1.1	11.0.1.1	TCP	66	http > 34210 [ACK] Seq=148 Ack=74 Win=29184 Len=0 TSval=757159 TSecr=757159
61	3.114447000	11.0.1.1	13.0.1.1	TCP	74	34211 > http [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=757418
62	3.114471000	13.0.1.1	11.0.1.1	TCP	74	http > 34211 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TS
63	3.114477000	11.0.1.1	13.0.1.1	TCP	66	34211 > http [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=757418 TSecr=757418
64	3.114607000	11.0.1.1	13.0.1.1	HTTP	138	GET / HTTP/1.1
65	3.114623000	13.0.1.1	11.0.1.1	TCP	66	http > 34211 [ACK] Seq=1 Ack=73 Win=29184 Len=0 TSval=757418 TSecr=757418
66	3.115131000	11.0.1.1	13.0.1.1	TCP	83	[TCP segment of a reassembled PDU]
67	3.115134000	11.0.1.1	13.0.1.1	TCP	66	34211 > http [ACK] Seq=73 Ack=18 Win=29696 Len=0 TSval=757419 TSecr=757419
68	3.115147000	13.0.1.1	11.0.1.1	TCP	103	[TCP segment of a reassembled PDU]
69	3.115148000	11.0.1.1	13.0.1.1	TCP	66	34211 > http [ACK] Seq=73 Ack=55 Win=29696 Len=0 TSval=757419 TSecr=757419
70	3.115162000	13.0.1.1	11.0.1.1	TCP	103	[TCP segment of a reassembled PDU]
71	3.115162000	11.0.1.1	13.0.1.1	TCP	66	34211 > http [ACK] Seq=73 Ack=92 Win=29696 Len=0 TSval=757419 TSecr=757419
72	3.115170000	13.0.1.1	11.0.1.1	TCP	91	[TCP segment of a reassembled PDU]
73	3.115171000	11.0.1.1	13.0.1.1	TCP	66	34211 > http [ACK] Seq=73 Ack=117 Win=29696 Len=0 TSval=757419 TSecr=757419
74	3.115179000	13.0.1.1	11.0.1.1	TCP	68	[TCP segment of a reassembled PDU]
75	3.115179000	11.0.1.1	13.0.1.1	TCP	66	34211 > http [ACK] Seq=73 Ack=119 Win=29696 Len=0 TSval=757419 TSecr=757419
76	3.115187000	13.0.1.1	11.0.1.1	HTTP	94	Continuation or non-HTTP traffic
77	3.115188000	11.0.1.1	13.0.1.1	TCP	66	34211 > http [ACK] Seq=73 Ack=147 Win=29696 Len=0 TSval=757419 TSecr=757419
78	3.115205000	13.0.1.1	11.0.1.1	TCP	66	http > 34211 [FIN, ACK] Seq=147 Ack=73 Win=29184 Len=0 TSval=757419 TSecr=7
79	3.115253000	11.0.1.1	13.0.1.1	TCP	66	34211 > http [FIN, ACK] Seq=73 Ack=148 Win=29696 Len=0 TSval=757419 TSecr=7
80	3.115261000	13.0.1.1	11.0.1.1	TCP	66	http > 34211 [ACK] Seq=148 Ack=74 Win=29184 Len=0 TSval=757419 TSecr=757419
81	4.169809000	11.0.1.1	13.0.1.1	TCP	74	34212 > http [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=757682
82	4.169987000	13.0.1.1	11.0.1.1	TCP	74	http > 34212 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TS
83	4.170024000	11.0.1.1	13.0.1.1	TCP	66	34212 > http [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=757682 TSecr=757682
84	4.170723000	11.0.1.1	13.0.1.1	HTTP	138	GET / HTTP/1.1
85	4.170830000	13.0.1.1	11.0.1.1	TCP	66	http > 34212 [ACK] Seq=1 Ack=73 Win=29184 Len=0 TSval=757682 TSecr=757682
86	4.171292000	13.0.1.1	11.0.1.1	TCP	83	[TCP segment of a reassembled PDU]
87	4.171298000	11.0.1.1	13.0.1.1	TCP	66	34212 > http [ACK] Seq=73 Ack=18 Win=29696 Len=0 TSval=757682 TSecr=757682
88	4.171329000	13.0.1.1	11.0.1.1	TCP	103	[TCP segment of a reassembled PDU]
89	4.171332000	11.0.1.1	13.0.1.1	TCP	66	34212 > http [ACK] Seq=73 Ack=55 Win=29696 Len=0 TSval=757682 TSecr=757682
90	4.171424000	13.0.1.1	11.0.1.1	TCP	103	[TCP segment of a reassembled PDU]
91	4.171427000	11.0.1.1	13.0.1.1	TCP	66	34212 > http [ACK] Seq=73 Ack=92 Win=29696 Len=0 TSval=757682 TSecr=757682
92	4.171477000	13.0.1.1	11.0.1.1	TCP	91	[TCP segment of a reassembled PDU]
93	4.171481000	11.0.1.1	13.0.1.1	TCP	66	34212 > http [ACK] Seq=73 Ack=117 Win=29696 Len=0 TSval=757682 TSecr=757682

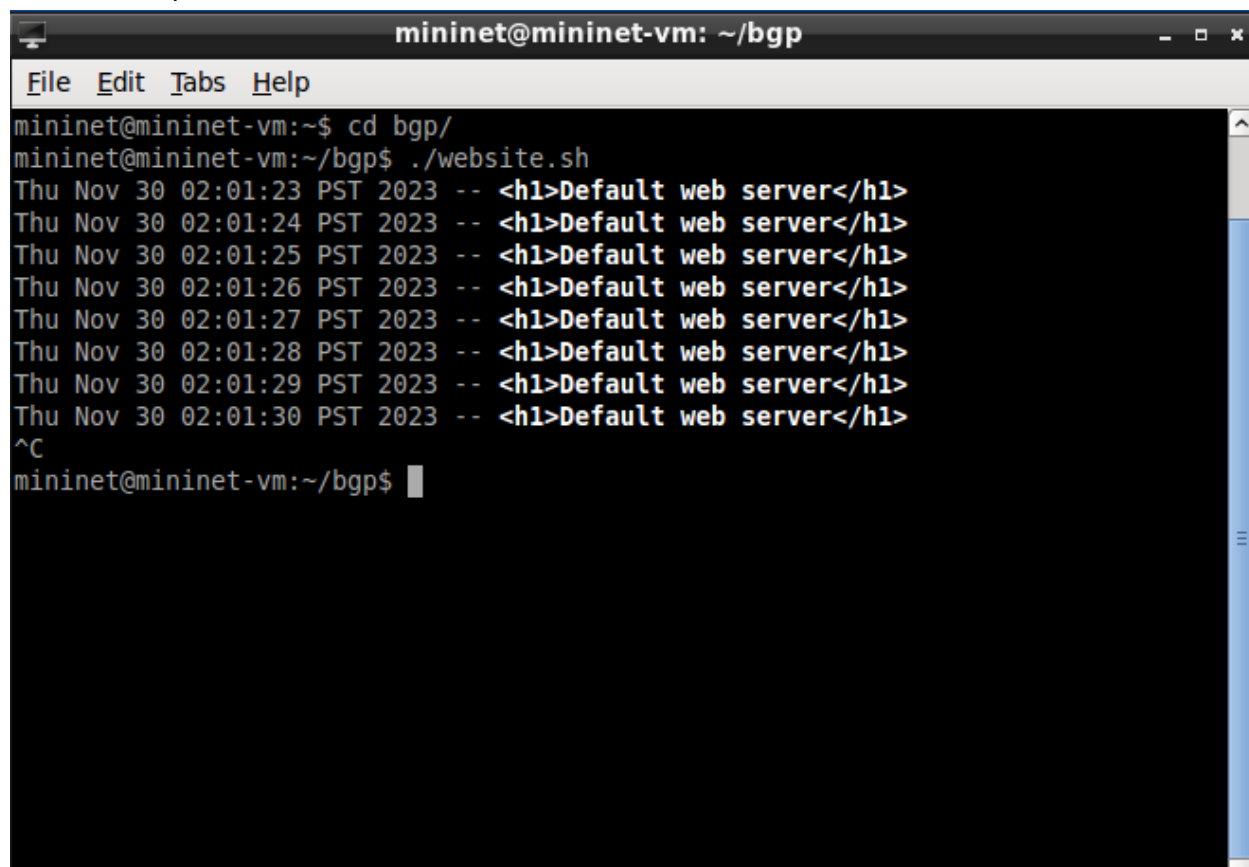
The packet details pane shows the following information for the selected packet (No. 84):

- Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
- Ethernet II, Src: b2:73:44:9c:ce:50 (b2:73:44:9c:ce:50), Dst: a2:d1:48:3c:32:23 (a2:d1:48:3c:32:23)
- Internet Protocol Version 4, Src: 11.0.1.1 (11.0.1.1), Dst: 13.0.1.1 (13.0.1.1)
- Transmission Control Protocol, Src Port: 34208 (34208), Dst Port: http (80), Seq: 0, Len: 0

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 a2 d1 48 3c 32 23 b2 73 44 9c ce 50 08 00 45 00 ..H<2#.s D..P..E.
0010 00 3c 2b cc 40 00 40 06 f4 ee 0b 00 01 01 0d 00 .<+.@.@. ....
0020 01 01 85 a0 00 50 d0 62 a0 6c 00 00 00 00 a0 02 ....P.b.l.....
0030 72 10 1a 30 00 00 02 04 05 b4 04 02 08 0a 00 0b r..0.....
```

Terminal snapshot: -

A terminal window titled "mininet@mininet-vm: ~/bgp" with a menu bar (File, Edit, Tabs, Help). The terminal shows a user navigating to the "bgp/" directory and running a script "website.sh". The script outputs eight lines of log messages, each containing a timestamp, a log level "--", and an HTML header tag "<h1>Default web server</h1>". The user then presses Ctrl-C (^C) to stop the script, returning to the shell prompt.

```
mininet@mininet-vm:~$ cd bgp/
mininet@mininet-vm:~/bgp$ ./website.sh
Thu Nov 30 02:01:23 PST 2023 -- <h1>Default web server</h1>
Thu Nov 30 02:01:24 PST 2023 -- <h1>Default web server</h1>
Thu Nov 30 02:01:25 PST 2023 -- <h1>Default web server</h1>
Thu Nov 30 02:01:26 PST 2023 -- <h1>Default web server</h1>
Thu Nov 30 02:01:27 PST 2023 -- <h1>Default web server</h1>
Thu Nov 30 02:01:28 PST 2023 -- <h1>Default web server</h1>
Thu Nov 30 02:01:29 PST 2023 -- <h1>Default web server</h1>
Thu Nov 30 02:01:30 PST 2023 -- <h1>Default web server</h1>
^C
mininet@mininet-vm:~/bgp$
```

Ans 8

GET request being sent from h2-1 to h3-1: -

```
mininet@mininet-vm: ~/bgp
File Edit Tabs Help
mininet@mininet-vm:~/bgp$ ./website2.sh
Thu Nov 30 02:24:15 PST 2023 -- <h1>Default web server</h1>
Thu Nov 30 02:24:16 PST 2023 -- <h1>Default web server</h1>
Thu Nov 30 02:24:17 PST 2023 -- <h1>Default web server</h1>
^C
mininet@mininet-vm:~/bgp$
```

Mininet-Tutorial [Running] - Oracle VM VirtualBox

\*h2-1-eth0 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
13	0.000430000	12.0.1.1	13.0.1.1	TCP	66	57856 > http [ACK] Seq=73 Ack=117 Win=29696 Len=0 TSval=871090 TSecr=871090
14	0.000445000	13.0.1.1	12.0.1.1	TCP	68	[TCP segment of a reassembled PDU]
15	0.000446000	12.0.1.1	13.0.1.1	TCP	66	57856 > http [ACK] Seq=73 Ack=119 Win=29696 Len=0 TSval=871090 TSecr=871090
16	0.000453000	13.0.1.1	12.0.1.1	HTTP	94	Continuation or non-HTTP traffic
17	0.000454000	12.0.1.1	13.0.1.1	TCP	66	57856 > http [ACK] Seq=73 Ack=147 Win=29696 Len=0 TSval=871090 TSecr=871090
18	0.000472000	12.0.1.1	12.0.1.1	TCP	66	http > 57856 [FIN, ACK] Seq=147 Ack=73 Win=29184 Len=0 TSval=871090 TSecr=8
19	0.000555000	12.0.1.1	13.0.1.1	TCP	66	57856 > http [FIN, ACK] Seq=73 Ack=148 Win=29696 Len=0 TSval=871090 TSecr=8
20	0.000565000	13.0.1.1	12.0.1.1	TCP	66	http > 57856 [ACK] Seq=148 Ack=74 Win=29184 Len=0 TSval=871090 TSecr=871090
21	1.058744000	12.0.1.1	13.0.1.1	TCP	74	57857 > http [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=871354
22	1.058766000	13.0.1.1	12.0.1.1	TCP	74	http > 57857 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TS
23	1.058771000	12.0.1.1	13.0.1.1	TCP	66	57857 > http [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=871354 TSecr=871354
24	1.058862000	12.0.1.1	13.0.1.1	HTTP	138	GET / HTTP/1.1
25	1.058873000	13.0.1.1	12.0.1.1	TCP	66	http > 57857 [ACK] Seq=1 Ack=73 Win=29184 Len=0 TSval=871354 TSecr=871354
26	1.058968000	13.0.1.1	12.0.1.1	TCP	83	[TCP segment of a reassembled PDU]
27	1.058969000	12.0.1.1	13.0.1.1	TCP	66	57857 > http [ACK] Seq=73 Ack=18 Win=29696 Len=0 TSval=871354 TSecr=871354
28	1.058980000	13.0.1.1	12.0.1.1	TCP	103	[TCP segment of a reassembled PDU]
29	1.058982000	12.0.1.1	13.0.1.1	TCP	66	57857 > http [ACK] Seq=73 Ack=55 Win=29696 Len=0 TSval=871354 TSecr=871354
30	1.058994000	13.0.1.1	12.0.1.1	TCP	103	[TCP segment of a reassembled PDU]
31	1.058995000	12.0.1.1	13.0.1.1	TCP	66	57857 > http [ACK] Seq=73 Ack=92 Win=29696 Len=0 TSval=871354 TSecr=871354
32	1.059001000	12.0.1.1	12.0.1.1	TCP	91	[TCP segment of a reassembled PDU]
33	1.059002000	12.0.1.1	13.0.1.1	TCP	66	57857 > http [ACK] Seq=73 Ack=117 Win=29696 Len=0 TSval=871354 TSecr=871354
34	1.059008000	13.0.1.1	12.0.1.1	TCP	68	[TCP segment of a reassembled PDU]
35	1.059009000	12.0.1.1	13.0.1.1	TCP	66	57857 > http [ACK] Seq=73 Ack=119 Win=29696 Len=0 TSval=871354 TSecr=871354
36	1.059015000	13.0.1.1	12.0.1.1	HTTP	94	Continuation or non-HTTP traffic
37	1.059015000	12.0.1.1	13.0.1.1	TCP	66	57857 > http [ACK] Seq=73 Ack=147 Win=29696 Len=0 TSval=871354 TSecr=871354
38	1.059030000	13.0.1.1	12.0.1.1	TCP	66	http > 57857 [FIN, ACK] Seq=147 Ack=73 Win=29184 Len=0 TSval=871354 TSecr=8
39	1.059095000	12.0.1.1	13.0.1.1	TCP	66	57857 > http [FIN, ACK] Seq=73 Ack=148 Win=29696 Len=0 TSval=871354 TSecr=8
40	1.059104000	13.0.1.1	12.0.1.1	TCP	66	http > 57857 [ACK] Seq=148 Ack=74 Win=29184 Len=0 TSval=871354 TSecr=871354
41	2.100947000	12.0.1.1	13.0.1.1	TCP	74	57858 > http [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=871615
42	2.100993000	13.0.1.1	12.0.1.1	TCP	74	http > 57858 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TS
43	2.101000000	12.0.1.1	13.0.1.1	TCP	66	57858 > http [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=871615 TSecr=871615
44	2.101122000	12.0.1.1	13.0.1.1	HTTP	138	GET / HTTP/1.1
45	2.101135000	13.0.1.1	12.0.1.1	TCP	66	http > 57858 [ACK] Seq=1 Ack=73 Win=29184 Len=0 TSval=871615 TSecr=871615
46	2.101250000	13.0.1.1	12.0.1.1	TCP	83	[TCP segment of a reassembled PDU]
47	2.101259000	12.0.1.1	13.0.1.1	TCP	66	57858 > http [ACK] Seq=73 Ack=18 Win=29696 Len=0 TSval=871615 TSecr=871615
48	2.101270000	13.0.1.1	12.0.1.1	TCP	103	[TCP segment of a reassembled PDU]
49	2.101272000	12.0.1.1	13.0.1.1	TCP	66	57858 > http [ACK] Seq=73 Ack=55 Win=29696 Len=0 TSval=871615 TSecr=871615
50	2.101284000	13.0.1.1	12.0.1.1	TCP	103	[TCP segment of a reassembled PDU]
51	2.101285000	12.0.1.1	13.0.1.1	TCP	66	57858 > http [ACK] Seq=73 Ack=92 Win=29696 Len=0 TSval=871615 TSecr=871615
52	2.101291000	13.0.1.1	12.0.1.1	TCP	91	[TCP segment of a reassembled PDU]
53	2.101292000	12.0.1.1	13.0.1.1	TCP	66	57858 > http [ACK] Seq=73 Ack=117 Win=29696 Len=0 TSval=871615 TSecr=871615
54	2.101298000	13.0.1.1	12.0.1.1	TCP	68	[TCP segment of a reassembled PDU]

> Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0  
> Ethernet II, Src: aa:11:cc:67:e8:c3 (aa:11:cc:67:e8:c3), Dst: c6:6e:22:b2:a5:64 (c6:6e:22:b2:a5:64)  
> Internet Protocol Version 4, Src: 12.0.1.1 (12.0.1.1), Dst: 13.0.1.1 (13.0.1.1)  
> Transmission Control Protocol, Src Port: 57856 (57856), Dst Port: http (80), Seq: 0, Len: 0

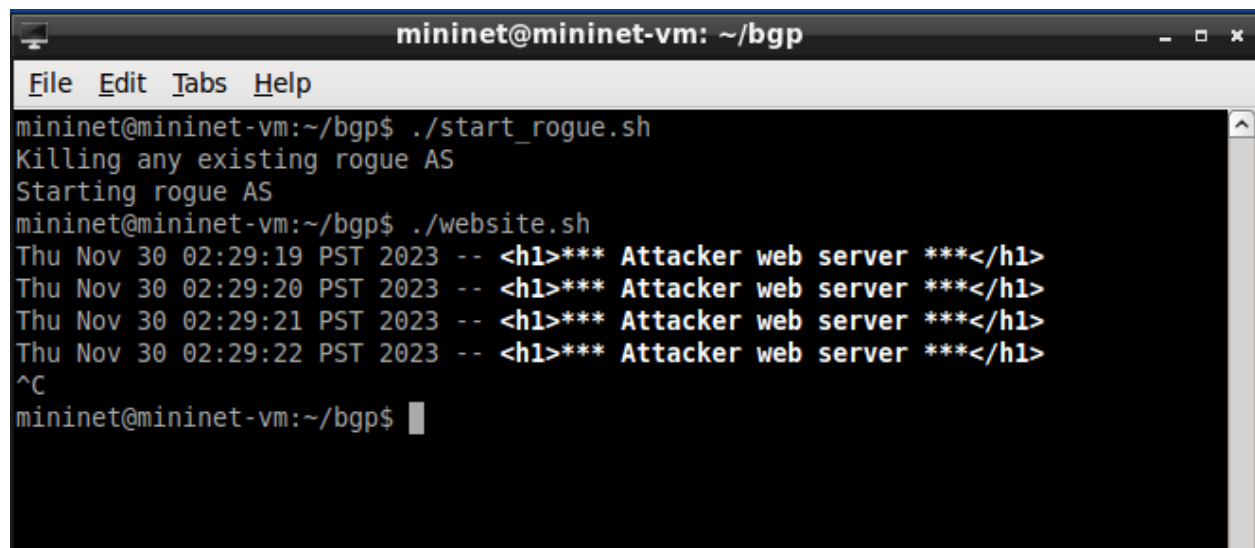
0000 c6 6e 22 b2 a5 64 aa 11 cc 67 e8 c3 08 00 45 00 .n..d...g...E.  
0010 00 3c f9 d9 40 00 40 06 25 e1 0c 00 01 01 0d 00 <..@.@.%.....  
0020 01 01 e2 00 00 50 7b bd b3 6b 00 00 00 00 a0 02 ....P{. .k.....  
0030 72 10 1b 30 00 00 02 04 05 b4 04 02 08 0a 00 0d r..0.....

File: /tmp/wireshark\_pcapng... Packets: 60 · Displayed: 60 (100.0%) · Dropped: 0 (0.0%) Profile: Default

\*h2-1-eth0 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

Ans 9

GET requests going to attacker host (h4-1) instead of original hos when I am running the website.sh: -

A terminal window titled "mininet@mininet-vm: ~/bgp" with a menu bar (File, Edit, Tabs, Help). The terminal shows the following commands and output:

```
mininet@mininet-vm:~/bgp$ ./start_rogue.sh
Killing any existing rogue AS
Starting rogue AS
mininet@mininet-vm:~/bgp$ ./website.sh
Thu Nov 30 02:29:19 PST 2023 -- <h1>*** Attacker web server ***</h1>
Thu Nov 30 02:29:20 PST 2023 -- <h1>*** Attacker web server ***</h1>
Thu Nov 30 02:29:21 PST 2023 -- <h1>*** Attacker web server ***</h1>
Thu Nov 30 02:29:22 PST 2023 -- <h1>*** Attacker web server ***</h1>
^C
mininet@mininet-vm:~/bgp$
```

The Attacker has been able to fool the network into believing that the original web server is running in his host but it's a fake server

Ans 10

Changed host to h1-2 in website2.sh and the GET requests are still going to the attacker web server: -

```
mininet@mininet-vm:~/bgp$ ./website2.sh
Thu Nov 30 10:56:41 PST 2023 -- <h1>*** Attacker web server ***</h1>
Thu Nov 30 10:56:42 PST 2023 -- <h1>*** Attacker web server ***</h1>
Thu Nov 30 10:56:43 PST 2023 -- <h1>*** Attacker web server ***</h1>
Thu Nov 30 10:56:44 PST 2023 -- <h1>*** Attacker web server ***</h1>
Thu Nov 30 10:56:45 PST 2023 -- <h1>*** Attacker web server ***</h1>
Thu Nov 30 10:56:46 PST 2023 -- <h1>*** Attacker web server ***</h1>
^C
mininet@mininet-vm:~/bgp$ █
```

When I changed the host to h3-1 and used it, the requests were going to the correct server. Looks, like all the hosts in AS1 have been fooled into believing that the path to the webserver has been updated.

Ans 11

BGP table to R1 after running start\_rogue.sh :-

```
mininet@mininet-vm: ~/bgp
File Edit Tabs Help

Hello, this is Quagga (version 0.99.22.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

User Access Verification

Password:
bgpd-R1> en
Password:
bgpd-R1# sh ip bgp
BGP table version is 0, local router ID is 9.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network        Next Hop           Metric LocPrf Weight Path
*> 11.0.0.0        0.0.0.0              0         32768 i
*> 12.0.0.0        9.0.0.2              0           0 2 i
*> 13.0.0.0        9.0.4.2              0           0 4 i
*                  9.0.0.2              0           0 2 3 i

Total number of prefixes 3
bgpd-R1#
```

We can see in the table that now there are 2 paths to reach 13.0.0.0 which is AS3. One is the old path - '2 3 i' for which the next hop is R2. The other is the new path - '4 i' for which the next hop is R4. Since the latter is the shortest path, all hosts of R1 will be using this new path to reach h3-1

BGP table to R2 after running start\_rogue.sh : -

```
mininet@mininet-vm: ~/bgp
File Edit Tabs Help

Hello, this is Quagga (version 0.99.22.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

User Access Verification

Password:
bgpd-R2> en
Password:
bgpd-R2# sh ip bgp
BGP table version is 0, local router ID is 9.0.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network        Next Hop           Metric LocPrf Weight Path
*> 11.0.0.0        9.0.0.1             0         0 1 i
*> 12.0.0.0        0.0.0.0             0        32768 i
* 13.0.0.0        9.0.0.1             0         0 1 4 i
*>                 9.0.1.2             0         0 3 i

Total number of prefixes 3
bgpd-R2#
```

We can see here that for R2 path - '3 i' is still the shortest path to reach h3-1. This is the reason why requests from hosts of R2 are going to the correct server



Forwarding table to R1 after running start\_rogue.sh : -

```
Node: R1
root@mininet-vm:~/bgp# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
9.0.0.0 0.0.0.0 255.255.255.0 U 0 0 0 R1-eth4
9.0.4.0 0.0.0.0 255.255.255.0 U 0 0 0 R1-eth5
11.0.1.0 0.0.0.0 255.255.255.0 U 0 0 0 R1-eth1
11.0.2.0 0.0.0.0 255.255.255.0 U 0 0 0 R1-eth2
11.0.3.0 0.0.0.0 255.255.255.0 U 0 0 0 R1-eth3
12.0.0.0 9.0.0.2 255.0.0.0 UG 0 0 0 R1-eth4
13.0.0.0 9.0.4.2 255.0.0.0 UG 0 0 0 R1-eth5
root@mininet-vm:~/bgp#
```

Note that the Gateway for 13.0.0.0 is not set to 9.0.4.2. This is the gateway which connects R1 to R4. Earlier the gateway being used for 12.0.0.0 was 9.0.0.2 which connects R1 to R2.

Forwarding table to R2 after running start\_rogue.sh : -

```
Node: R2
root@mininet-vm:~/bgp# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
9.0.0.0 0.0.0.0 255.255.255.0 U 0 0 0 R2-eth4
9.0.1.0 0.0.0.0 255.255.255.0 U 0 0 0 R2-eth5
11.0.0.0 9.0.0.1 255.0.0.0 UG 0 0 0 R2-eth4
12.0.1.0 0.0.0.0 255.255.255.0 U 0 0 0 R2-eth1
12.0.2.0 0.0.0.0 255.255.255.0 U 0 0 0 R2-eth2
12.0.3.0 0.0.0.0 255.255.255.0 U 0 0 0 R2-eth3
13.0.0.0 9.0.1.2 255.0.0.0 UG 0 0 0 R2-eth5
root@mininet-vm:~/bgp#
```

Note here that the gateway for 13.0.0.0 in the case of R2 is still 9.0.1.2 which connects R2 to R3

Ans 12

Sniffed packets at the interface connecting R4 and R1 and can see that the BGP advertisements of R4 are being sent to and accepted by R1: -

Wireshark 1.10.6 (v1.10.6 from master-1.10) - Capturing from R4-eth4

Filter: bgp

No.	Time	Source	Destination	Protocol	Length	Info
6	0.001049000	9.0.4.2	9.0.4.1	BGP	119	OPEN Message
8	0.001774000	9.0.4.1	9.0.4.2	BGP	138	OPEN Message, KEEPALIVE Message
10	0.002478000	9.0.4.2	9.0.4.1	BGP	104	KEEPALIVE Message, KEEPALIVE Message
11	0.002763000	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
13	1.009239000	9.0.4.1	9.0.4.2	BGP	242	KEEPALIVE Message, UPDATE Message, UPDATE Message, UPDATE Message
15	1.009515000	9.0.4.2	9.0.4.1	BGP	138	KEEPALIVE Message, UPDATE Message
17	1.060728000	9.0.4.1	9.0.4.2	BGP	91	UPDATE Message
19	2.011659000	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
21	2.013067000	9.0.4.2	9.0.4.1	BGP	85	KEEPALIVE Message
23	3.013131000	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
24	3.013229000	9.0.4.2	9.0.4.1	BGP	85	KEEPALIVE Message
26	4.015335000	9.0.4.2	9.0.4.1	BGP	85	KEEPALIVE Message
28	4.015625000	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
30	5.018378000	9.0.4.2	9.0.4.1	BGP	85	KEEPALIVE Message
31	5.018710000	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
33	6.020509000	9.0.4.2	9.0.4.1	BGP	85	KEEPALIVE Message
34	6.020810000	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
36	7.022731000	9.0.4.2	9.0.4.1	BGP	85	KEEPALIVE Message
37	7.023067000	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
39	8.023901000	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
41	8.024256000	9.0.4.2	9.0.4.1	BGP	85	KEEPALIVE Message
43	9.025151000	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
44	9.025602000	9.0.4.2	9.0.4.1	BGP	85	KEEPALIVE Message
46	10.027047000	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
47	10.027333000	9.0.4.2	9.0.4.1	BGP	85	KEEPALIVE Message
49	11.028780000	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
50	11.029004000	9.0.4.2	9.0.4.1	BGP	85	KEEPALIVE Message

Frame 17: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface 0

- Ethernet II, Src: e2:8e:c2:14:1e:85 (e2:8e:c2:14:1e:85), Dst: 96:88:38:be:43:9b (96:88:38:be:43:9b)
- Internet Protocol Version 4, Src: 9.0.4.1 (9.0.4.1), Dst: 9.0.4.2 (9.0.4.2)
- Transmission Control Protocol, Src Port: bgp (179), Dst Port: 46766 (46766), Seq: 268, Ack: 164, Len: 25
- Border Gateway Protocol - UPDATE Message
  - Marker: ffffffffffffffffffffffffffffffff
  - Length: 25
  - Type: UPDATE Message (2)
  - Unfeasible routes length: 2 bytes
  - Withdrawn routes:
    - 13.0.0.0/8
  - Total path attribute length: 0 bytes

In the opened packet, we can see that R1 is telling R2 that it has withdrawn the old path to go to 13.0.0.0/8 . We can see the BGP OPEN and BGP Keep alive packets as well which are used to start the BGP transactions keep the connection alive.

Capturing from R4-eth4 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]						
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help						
<div> <div>Filter: bgp</div> <div>Expression... Clear Apply Save</div> </div>						
No.	Time	Source	Destination	Protocol	Length	Info
6	0.001049000	9.0.4.2	9.0.4.1	BGP	119	OPEN Message
8	0.001774000	9.0.4.1	9.0.4.2	BGP	138	OPEN Message, KEEPALIVE Message
10	0.002478000	9.0.4.2	9.0.4.1	BGP	104	KEEPALIVE Message, KEEPALIVE Message
11	0.002763000	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
13	1.009239000	9.0.4.1	9.0.4.2	BGP	242	KEEPALIVE Message, UPDATE Message, UPDATE Message, UPDATE Message
15	1.009515000	9.0.4.2	9.0.4.1	BGP	138	KEEPALIVE Message, UPDATE Message
17	1.060728000	9.0.4.1	9.0.4.2	BGP	91	UPDATE Message
19	2.011659000	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
21	2.013067000	9.0.4.2	9.0.4.1	BGP	85	KEEPALIVE Message
23	3.013131000	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
24	3.013229000	9.0.4.2	9.0.4.1	BGP	85	KEEPALIVE Message
26	4.015335000	9.0.4.2	9.0.4.1	BGP	85	KEEPALIVE Message
28	4.015625000	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
30	5.018378000	9.0.4.2	9.0.4.1	BGP	85	KEEPALIVE Message
31	5.018710000	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
33	6.020509000	9.0.4.2	9.0.4.1	BGP	85	KEEPALIVE Message
34	6.020810000	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
36	7.022731000	9.0.4.2	9.0.4.1	BGP	85	KEEPALIVE Message
37	7.023067000	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
39	8.023901000	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
41	8.024256000	9.0.4.2	9.0.4.1	BGP	85	KEEPALIVE Message
43	9.025151000	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
44	9.025602000	9.0.4.2	9.0.4.1	BGP	85	KEEPALIVE Message
46	10.027047000	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
47	10.027333000	9.0.4.2	9.0.4.1	BGP	85	KEEPALIVE Message
49	11.028780000	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
50	11.029004000	9.0.4.2	9.0.4.1	BGP	85	KEEPALIVE Message

Frame 6: 119 bytes on wire (952 bits), 119 bytes captured (952 bits) on interface 0

Ethernet II, Src: 96:88:38:be:43:9b (96:88:38:be:43:9b), Dst: e2:8e:c2:14:1e:85 (e2:8e:c2:14:1e:85)

Internet Protocol Version 4, Src: 9.0.4.2 (9.0.4.2), Dst: 9.0.4.1 (9.0.4.1)

Transmission Control Protocol, Src Port: 46766 (46766), Dst Port: bgp (179), Seq: 1, Ack: 1, Len: 53

Border Gateway Protocol - OPEN Message

Marker: ffffffffffffffffffffffffffffffff

Length: 53

Type: OPEN Message (1)

Version: 4

My AS: 4

Hold Time: 5

BGP Identifier: 9.0.4.2 (9.0.4.2)

Optional Parameters Length: 24

Optional Parameters

Here, in the BGP open packet sent by R2 to R1, we can see that R4 is telling R1 that his AS is 4 and IP is 9.0.4.2

No.	Time	Source	Destination	Protocol	Length	Info
6	0.001049000	9.0.4.2	9.0.4.1	BGP	119	OPEN Message
8	0.001774000	9.0.4.1	9.0.4.2	BGP	138	OPEN Message, KEEPALIVE Message
10	0.002478000	9.0.4.2	9.0.4.1	BGP	104	KEEPALIVE Message, KEEPALIVE Message
11	0.002763000	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
13	1.009239000	9.0.4.1	9.0.4.2	BGP	242	KEEPALIVE Message, UPDATE Message, UPDATE Message, UPDATE Message
15	1.009515000	9.0.4.2	9.0.4.1	BGP	138	KEEPALIVE Message, UPDATE Message
17	1.060728000	9.0.4.1	9.0.4.2	BGP	91	UPDATE Message
19	2.011659000	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
21	2.013067000	9.0.4.2	9.0.4.1	BGP	85	KEEPALIVE Message
23	3.013131000	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
24	3.013229000	9.0.4.2	9.0.4.1	BGP	85	KEEPALIVE Message
26	4.015335000	9.0.4.2	9.0.4.1	BGP	85	KEEPALIVE Message
28	4.015625000	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
30	5.018378000	9.0.4.2	9.0.4.1	BGP	85	KEEPALIVE Message
31	5.018710000	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
33	6.020509000	9.0.4.2	9.0.4.1	BGP	85	KEEPALIVE Message
34	6.020810000	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
36	7.022731000	9.0.4.2	9.0.4.1	BGP	85	KEEPALIVE Message
37	7.023067000	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
39	8.023901000	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
41	8.024256000	9.0.4.2	9.0.4.1	BGP	85	KEEPALIVE Message
43	9.025151000	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
44	9.025602000	9.0.4.2	9.0.4.1	BGP	85	KEEPALIVE Message
46	10.027047000	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
47	10.027333000	9.0.4.2	9.0.4.1	BGP	85	KEEPALIVE Message
49	11.028780000	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
50	11.029004000	9.0.4.2	9.0.4.1	BGP	85	KEEPALIVE Message

```

> Frame 8: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface 0
> Ethernet II, Src: e2:8e:c2:14:1e:85 (e2:8e:c2:14:1e:85), Dst: 96:88:38:be:43:9b (96:88:38:be:43:9b)
> Internet Protocol Version 4, Src: 9.0.4.1 (9.0.4.1), Dst: 9.0.4.2 (9.0.4.2)
> Transmission Control Protocol, Src Port: bgp (179), Dst Port: 46766 (46766), Seq: 1, Ack: 54, Len: 72
> Border Gateway Protocol - OPEN Message
  Marker: ffffffffffffffffffffffffffffffff
  Length: 53
  Type: OPEN Message (1)
  Version: 4
  My AS: 1
  Hold Time: 5
  BGP Identifier: 9.0.0.1 (9.0.0.1)
  Optional Parameters Length: 24
  > Optional Parameters
> Border Gateway Protocol - KEEPALIVE Message

```

R1 has replied with its BGP OPEN message and has told R4 that its AS is 1. After this the paths have been updated as shown in the first snapshot of this answer.

Also, I can see the ARP request response happening at the time of running start\_rogue.sh, when the GET requests were going to h3-1. This indicates that the IP address which was of h3-1 was advertised by h4-1 and that's why the ARP request was triggered when the GET request packet reached R4 for the first time: -

h1-1-eth0 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
94	4.154720000	13.0.1.1	11.0.1.1	TCP	68	34266 > http [ACK] Seq=73 Ack=117 Win=29696 Len=0 TSval=1349305 TSecr=13493
95	4.154730000	13.0.1.1	11.0.1.1	TCP	66	34266 > http [ACK] Seq=73 Ack=119 Win=29696 Len=0 TSval=1349305 TSecr=13493
96	4.154740000	13.0.1.1	11.0.1.1	HTTP	94	Continuation or non-HTTP traffic
97	4.154743000	13.0.1.1	11.0.1.1	TCP	66	34266 > http [ACK] Seq=73 Ack=147 Win=29696 Len=0 TSval=1349305 TSecr=13493
98	4.154759000	13.0.1.1	11.0.1.1	TCP	66	http > 34266 [FIN, ACK] Seq=147 Ack=73 Win=29184 Len=0 TSval=1349305 TSecr=
99	4.154804000	11.0.1.1	13.0.1.1	TCP	66	34266 > http [FIN, ACK] Seq=73 Ack=148 Win=29696 Len=0 TSval=1349305 TSecr=
100	4.154812000	13.0.1.1	11.0.1.1	TCP	66	http > 34266 [ACK] Seq=148 Ack=74 Win=29184 Len=0 TSval=1349305 TSecr=13493
101	5.010882000	a2:d1:48:3c:32:23	b2:73:44:9c:ce:50	ARP	42	Who has 11.0.1.1? Tell 11.0.1.254
102	5.010891000	b2:73:44:9c:ce:50	a2:d1:48:3c:32:23	ARP	42	11.0.1.1 is at b2:73:44:9c:ce:50
103	5.189492000	11.0.1.1	13.0.1.1	TCP	74	http > 34267 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1349564
104	5.189517000	13.0.1.1	11.0.1.1	TCP	74	http > 34267 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TS
105	5.189522000	11.0.1.1	13.0.1.1	TCP	66	34267 > http [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=1349564 TSecr=1349564
106	5.189619000	11.0.1.1	13.0.1.1	HTTP	138	GET / HTTP/1.1
107	5.189630000	13.0.1.1	11.0.1.1	TCP	66	http > 34267 [ACK] Seq=1 Ack=73 Win=29184 Len=0 TSval=1349564 TSecr=1349564
108	5.189714000	13.0.1.1	11.0.1.1	TCP	83	[TCP segment of a reassembled PDU]
109	5.189715000	11.0.1.1	13.0.1.1	TCP	66	34267 > http [ACK] Seq=73 Ack=18 Win=29696 Len=0 TSval=1349564 TSecr=134956
110	5.189726000	13.0.1.1	11.0.1.1	TCP	103	[TCP segment of a reassembled PDU]
111	5.189727000	11.0.1.1	13.0.1.1	TCP	66	34267 > http [ACK] Seq=73 Ack=55 Win=29696 Len=0 TSval=1349564 TSecr=134956
112	5.189740000	13.0.1.1	11.0.1.1	TCP	103	[TCP segment of a reassembled PDU]
113	5.189741000	11.0.1.1	13.0.1.1	TCP	66	34267 > http [ACK] Seq=73 Ack=92 Win=29696 Len=0 TSval=1349564 TSecr=134956
114	5.189748000	13.0.1.1	11.0.1.1	TCP	91	[TCP segment of a reassembled PDU]
115	5.189748000	11.0.1.1	13.0.1.1	TCP	66	34267 > http [ACK] Seq=73 Ack=117 Win=29696 Len=0 TSval=1349564 TSecr=13495
116	5.189755000	13.0.1.1	11.0.1.1	TCP	68	[TCP segment of a reassembled PDU]

Frame 102: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0  
 Ethernet II, Src: b2:73:44:9c:ce:50 (b2:73:44:9c:ce:50), Dst: a2:d1:48:3c:32:23 (a2:d1:48:3c:32:23)  
 Address Resolution Protocol (reply)  
 Hardware type: Ethernet (1)  
 Protocol type: IP (0x0800)  
 Hardware size: 6  
 Protocol size: 4  
 Opcode: reply (2)  
 Sender MAC address: b2:73:44:9c:ce:50 (b2:73:44:9c:ce:50)  
 Sender IP address: 11.0.1.1 (11.0.1.1)  
 Target MAC address: a2:d1:48:3c:32:23 (a2:d1:48:3c:32:23)  
 Target IP address: 11.0.1.254 (11.0.1.254)

## Ans 13

In an ideal scenario, all the packets from R1 intended to go to a host in R3 are forwarded to R2. R2 then forwards them to R3 and R3 forwards them to the specific host based on the IP address and MAC address. When R4 joins the network it connects itself to R1. Then every host of R4 advertises the IP address used by the hosts of R3. h4-1 advertises the IP address of h3-1, h4-2 advertises the address of h3-2 and so on. This updates the BGP and forwarding table of R1 because R1 thinks that now there is a shorter path to reach the hosts of R3. This is why all the traffic going from R1 to R3 through R2 now starts to go to R4.

## Ans 14

I ran ping multiple times on h3-1 IP address - 13.0.1.1 and found that after running the start\_rogue.sh script the pings are taking less RTT on average as compared to the pings which were sent before running the start\_rogue.sh script. This makes sense, as this IP is now being advertised by h4-1 which is the attacker's host. H4-1 is just 1 hop away from R1 whereas h3-1 is 2 hops away. So the BGP and forwarding tables have been updated for this IP and the shorter path has been updated. This is the reason the requests are going to the attacker host now.

Ans 15

Original code in bgp.py: -

```
def getIP(hostname):
    AS, idx = hostname.replace('h', '').split('-')
    AS = int(AS)
    if AS == 4:
        AS = 3
    ip = '%s.0.%s.1/24' % (10+AS, idx)
    return ip

def getGateway(hostname):
    AS, idx = hostname.replace('h', '').split('-')
    AS = int(AS)
    # This condition gives AS4 the same IP range as AS3 so it can be an
    # attacker.
    if AS == 4:
        AS = 3
    gw = '%s.0.%s.254' % (10+AS, idx)
    return gw
```

Modified code: -

```

def getIP(hostname):
    AS, idx = hostname.replace('h', '').split('-')
    AS = int(AS)
    if hostname == 'h4-1':
        AS = 3
        idx = 1
    ip = '%s.0.%s.1/24' % (10+AS, idx)
    return ip

def getGateway(hostname):
    AS, idx = hostname.replace('h', '').split('-')
    AS = int(AS)
    # This condition gives AS4 the same IP range as AS3 so it can be an
    # attacker.
    if hostname == 'h4-1':
        AS = 3
        idx = 1
    gw = '%s.0.%s.254' % (10+AS, idx)
    return gw

```

This will give the IP of h3-1 to h4-1. The IP addresses of h4-2 and h4-3 will be new and not the same as h3-2 and h3-3.

h4-2 new IP - 14.0.2.1

h4-3 new IP - 14.0.3.1

IPs of R4 hosts when bgp.py is used to set up topology: -

```
Node: h4-2
root@mininet-virtual-machine:~# bgp# ifconfig
h4-2-eth0 Link encap:Ethernet HWaddr fa:dd:15:74:84:38
          inet addr:13.0.2.1 Bcast:13.0.2.255 Mask:255.255.255.0
          inet6 addr: fe80::f8dd:15ff:fe74:8438/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:648 (648.0 B) TX bytes:648 (648.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:65536 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

root@mininet-virtual-machine:~# bgp#

Node: h4-3
root@mininet-virtual-machine:~# bgp# ifconfig
h4-3-eth0 Link encap:Ethernet HWaddr fa:d0:b1:8d:21:e9
          inet addr:13.0.3.1 Bcast:13.0.3.255 Mask:255.255.255.0
          inet6 addr: fe80::f8d0:b1ff:fe8d:21e9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:648 (648.0 B) TX bytes:648 (648.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:65536 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

root@mininet-virtual-machine:~# bgp#

Node: h4-1
root@mininet-virtual-machine:~# bgp# ifconfig
h4-1-eth0 Link encap:Ethernet HWaddr 12:06:d7:b7:47:1e
          inet addr:13.0.1.1 Bcast:13.0.1.255 Mask:255.255.255.0
          inet6 addr: fe80::1006:d7ff:feb7:471e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:648 (648.0 B) TX bytes:648 (648.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:65536 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

root@mininet-virtual-machine:~# bgp#
```

IPs of R4 hosts when bgp\_modified.py is used to set-up topology: -



```
Node: h4-1
root@mininet-virtual-machine:~# ifconfig
h4-1-eth0 Link encap:Ethernet HWaddr 8a:d1:9e:06:52:ea
          inet addr:13.0.1.1 Bcast:13.0.1.255 Mask:255.255.255.0
          inet6 addr: fe80::88d1:9eff:fe06:52ea/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:648 (648.0 B) TX bytes:648 (648.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:65536 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

root@mininet-virtual-machine:~#

Node: h4-2
root@mininet-virtual-machine:~# ifconfig
h4-2-eth0 Link encap:Ethernet HWaddr 52:5d:b2:f9:5f:a7
          inet addr:14.0.2.1 Bcast:14.0.2.255 Mask:255.255.255.0
          inet6 addr: fe80::505d:b2ff:fe5f:5fa7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:648 (648.0 B) TX bytes:648 (648.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:65536 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

root@mininet-virtual-machine:~#

Node: h4-3
root@mininet-virtual-machine:~# ifconfig
h4-3-eth0 Link encap:Ethernet HWaddr 96:52:bf:e8:5f:03
          inet addr:14.0.3.1 Bcast:14.0.3.255 Mask:255.255.255.0
          inet6 addr: fe80::9452:bfff:fe85:f03/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:648 (648.0 B) TX bytes:648 (648.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:65536 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

root@mininet-virtual-machine:~#
```

Next, we need to change the inet address of R4 router's interfaces which connect with h4-2 and h4-3

For this we need to update the bgpd-R4.conf and zebra-R4.conf files.

Original bgpd-conf file: -

```

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

hostname bgpd-R4
password en
enable password en

router bgp 4
  bgp router-id 9.0.4.2
  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
debug bgp filters
debug bgp fsm
debug bgp keepalives
debug bgp updates

!
log stdout

```

## Modified bgpd-conf file: -

```

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

hostname bgpd-R4
password en
enable password en

router bgp 4
  bgp router-id 9.0.4.2
  network 13.0.1.0/24
  network 14.0.0.0/8
  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
debug bgp filters
debug bgp fsm
debug bgp keepalives
debug bgp updates

!
log stdout

```

2 network IPs are added for R4 now - one is 13.0.1.0/24 which is used for hacking and the other is 14.0.0.0/8 which will be used for the remaining hosts.

Original zebra-R4.conf file: -

```
! *- zebra *-

hostname R4
password en
enable password en

!

interface lo
| ip address 127.0.0.1/32
|
interface R4-eth1
| ip address 13.0.1.254/24
|
interface R4-eth2
| ip address 13.0.2.254/24
|
interface R4-eth3
| ip address 13.0.3.254/24
|
!

interface R4-eth4
| ip address 9.0.4.2/24
|
log file /tmp/R4.log
```

Modified zebra-R4.conf file: -

---

```
! *- zebra *-  
  
hostname R4  
password en  
enable password en  
  
!  
  
interface lo  
  ip address 127.0.0.1/32  
  
interface R4-eth1  
  ip address 13.0.1.254/24  
  
interface R4-eth2  
  ip address 14.0.2.254/24  
  
interface R4-eth3  
  ip address 14.0.3.254/24  
  
!  
  
interface R4-eth4  
  ip address 9.0.4.2/24  
  
log file /tmp/R4.log
```

Note that R4-eth2 and R4-eth3 are now updated to connect with the updated Ip addresses of h4-2 and h4-3 hosts.

R4 ifconfig details after making the changes: -

```

root@mininet-vm:~/bgp# ifconfig
R4-eth1  Link encap:Ethernet  HWaddr 26:bd:d1:b6:34:1f
         inet addr:13.0.1.254  Bcast:13.0.1.255  Mask:255.255.255.0
         inet6 addr: fe80::24bd:d1ff:feb6:341f/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:8 errors:0 dropped:0 overruns:0 frame:0
         TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:648 (648.0 B)  TX bytes:648 (648.0 B)

R4-eth2  Link encap:Ethernet  HWaddr 12:8b:ec:51:b0:06
         inet addr:14.0.2.254  Bcast:14.0.2.255  Mask:255.255.255.0
         inet6 addr: fe80::108b:ecff:fe51:b006/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:8 errors:0 dropped:0 overruns:0 frame:0
         TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:648 (648.0 B)  TX bytes:648 (648.0 B)

R4-eth3  Link encap:Ethernet  HWaddr 42:83:01:15:23:9e
         inet addr:14.0.3.254  Bcast:14.0.3.255  Mask:255.255.255.0
         inet6 addr: fe80::4083:1fff:fe15:239e/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:8 errors:0 dropped:0 overruns:0 frame:0
         TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:648 (648.0 B)  TX bytes:648 (648.0 B)

R4-eth4  Link encap:Ethernet  HWaddr ae:5d:4f:7d:aa:7c
         inet addr:9.0.4.2  Bcast:9.0.4.255  Mask:255.255.255.0
         inet6 addr: fe80::ac5d:4fff:fe7d:aa7c/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:24 errors:0 dropped:0 overruns:0 frame:0
         TX packets:19 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:1680 (1.6 KB)  TX bytes:1421 (1.4 KB)

lo       Link encap:Local Loopback
         inet addr:127.0.0.1  Mask:255.0.0.0
         inet6 addr: ::1/128 Scope:Host
         UP LOOPBACK RUNNING  MTU:65536  Metric:1
         RX packets:0 errors:0 dropped:0 overruns:0 frame:0
         TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

root@mininet-vm:~/bgp# █

```

Note that R4-eth1 has inet address - 13.0.1.254 where has the inet addresses of all other interfaces are starting with 14 now.

Updated bgp table of R1: -

```

      Network      Next Hop      Metric LocPrf Weight Path
*> 11.0.0.0        0.0.0.0          0         32768 i
*> 12.0.0.0        9.0.0.2          0         0 2 i
*> 13.0.0.0        9.0.0.2          0         0 2 3 i
*> 13.0.1.0/24     9.0.4.2          0         0 4 i
*> 14.0.0.0        9.0.4.2          0         0 4 i

Total number of prefixes 5
bgpd-R1#

```

Note here that now there are 2 new entries - 13.0.1.0/24 and 14.0.0.0 in the table. The paths for both of these entries are - '4 i'. Hence, all the requests to 13.0.1.1 Ip address will go to R4 and eventually to attacker web server. Also, all the requests to remaining R4 hosts will also go to R4 as they will get matched with the 14.0.0.0 network IP.

Note that, all the request to R3 hosts (apart from h1-1) will go to R3 only and the same has been highlighted by the path of 13.0.0.0 network IP which is - '2 3 i'

Longest Prefix matching will come into play here and the requests to 13.0.1.1 (h1-1) will go to R4 as they will be matched with 13.0.1.0/24

Updated routing table of R1 :-

```

root@mininet-vm:~/bgp# route -n
Kernel IP routing table
Destination    Gateway      Genmask      Flags Metric Ref    Use Iface
9.0.0.0        0.0.0.0      255.255.255.0 U        0      0      0 R1-eth4
9.0.4.0        0.0.0.0      255.255.255.0 U        0      0      0 R1-eth5
11.0.1.0       0.0.0.0      255.255.255.0 U        0      0      0 R1-eth1
11.0.2.0       0.0.0.0      255.255.255.0 U        0      0      0 R1-eth2
11.0.3.0       0.0.0.0      255.255.255.0 U        0      0      0 R1-eth3
12.0.0.0       9.0.0.2      255.0.0.0    UG       0      0      0 R1-eth4
13.0.0.0       9.0.0.2      255.0.0.0    UG       0      0      0 R1-eth4
13.0.1.0       9.0.4.2      255.255.255.0 UG       0      0      0 R1-eth5
14.0.0.0       9.0.4.2      255.0.0.0    UG       0      0      0 R1-eth5
root@mininet-vm:~/bgp#

```

Note that every packet which get matched with 13.0.0.0 will be sent to R1-eth4 (R2). Every packet which get matched with 13.0.1.0 ( longest prefix matching) and 14.0.0.0 will be sent to R1-eth5(R4)

## ANTI-PLAGIARISM Statement <Include it in your report>

*We certify that this assignment/report is our own work, based on our personal study and/or research and that we have acknowledged all material and sources used in its preparation, whether they be books, articles, packages, datasets, reports, lecture notes, and any other kind of document, electronic or personal communication. We also certify that this assignment/report has not previously been submitted for assessment/project in any other course lab, except where specific permission has been granted from all course instructors involved, or at any other time in this course, and that we have not copied in part or whole or otherwise plagiarized the work of other students and/or persons. Additionally, we acknowledge that we may have used AI tools, such as language models (e.g., ChatGPT, Bard), for assistance in generating and refining my assignment, and we have made all reasonable efforts to ensure that such usage complies with the academic integrity policies set for the course. I pledge to uphold the principles of honesty and responsibility at CSE@IITH. In addition, we understand our responsibility to report honour violations by other students if we become aware of it.*

Sanyam Kaul - CS23MTECH14011

Bhargav Patel - CS23MTECH11026

Arnab Ghosh - CS23MTECH11025

Date: 1/12/2023

## References:

- <https://github.com/mininet/mininet/wiki/BGP-Path-Hijacking-Attack-Demo>
- <https://bitbucket.org/jvimal/bgp/src/master/>