

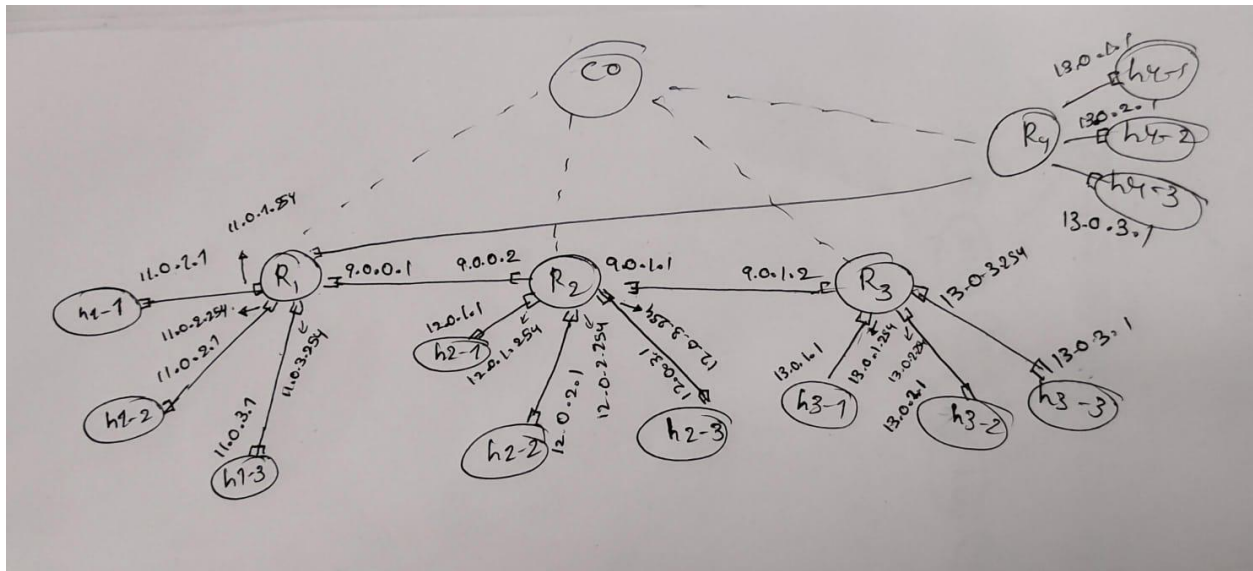
ACN Mininet Assignment: BGP Hijacking

Yash Shukla – cs23mtech14018

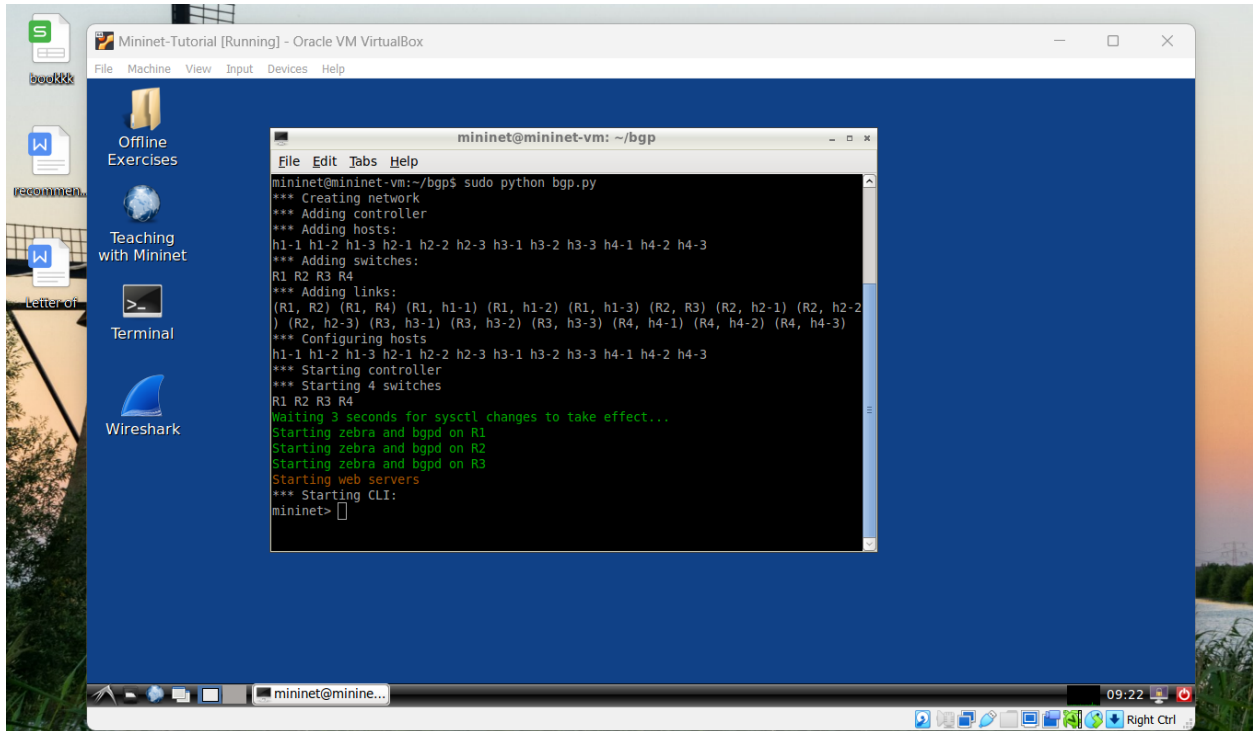
Punith Kumar Pulicharla – cs23mtech11032

C.A Rakshith Ram – sm22mtech12003

Answer 1 :

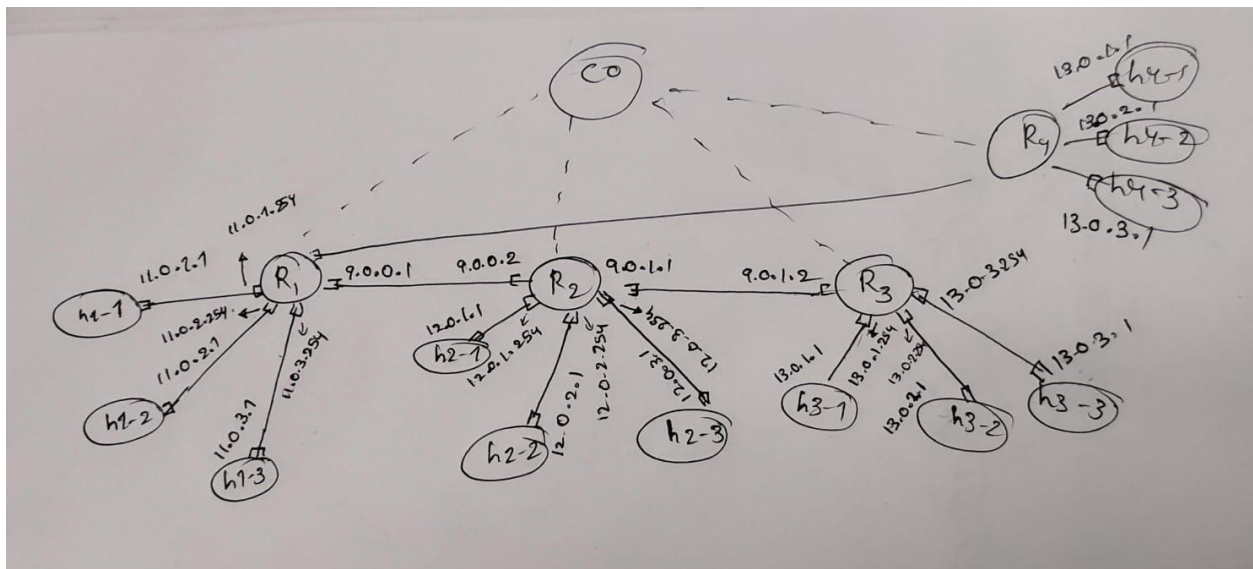


In total 12 Hosts are there and
4 Routers in Each Subset
Each Router having 3 Hosts



Answer 2 :

Available InterFace are shown below with their IP Addresses
Ip Addresses are shown in the Topology Diagram :

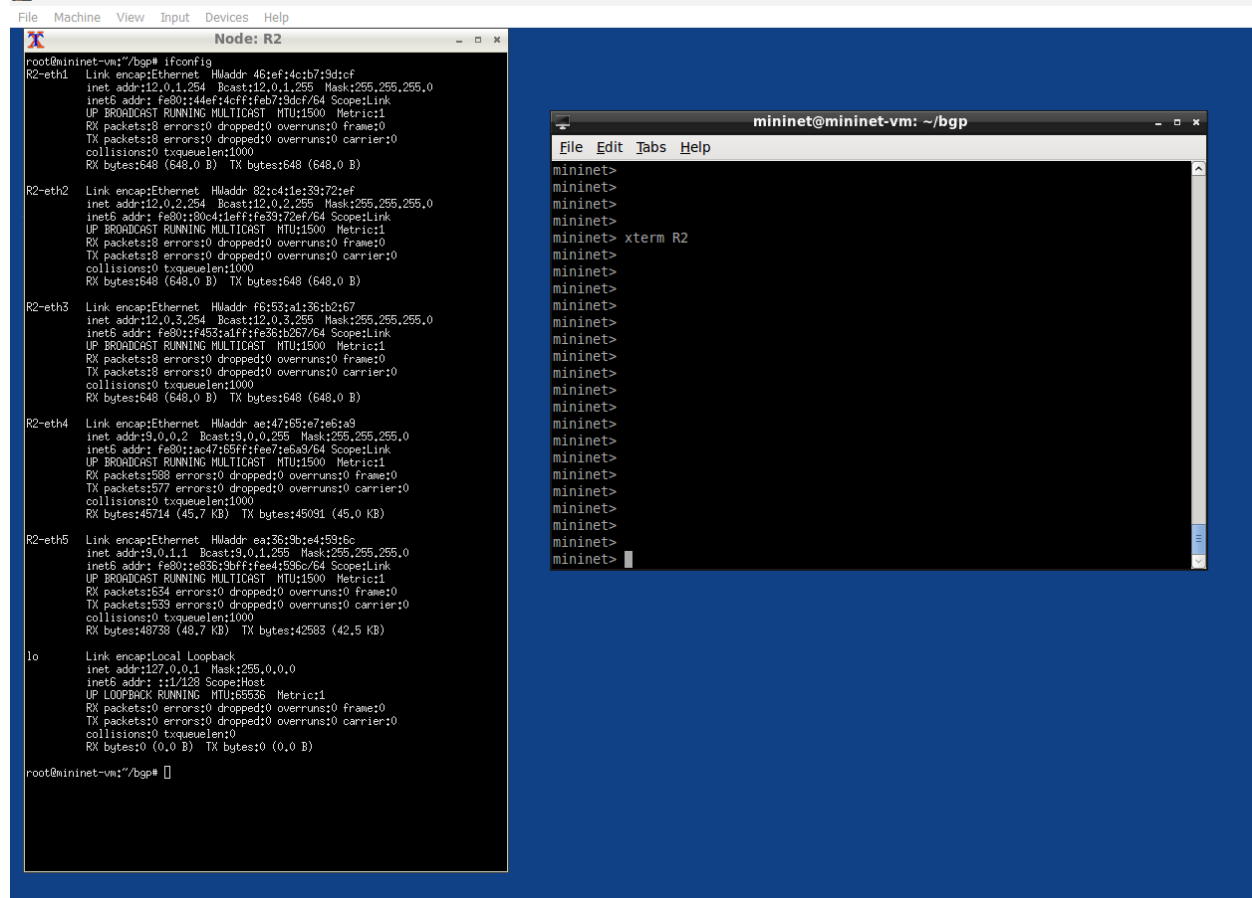


The screenshot displays a Mininet-Tutorial [Running] - Oracle VM VirtualBox window. The main terminal window, titled "Node: R1", shows the output of the "root@mininet-vm:~/bgp" command. The output lists network configuration and statistics for several interfaces:

- ri-eth2:** Link encap:Ethernet HWaddr a6:98:51:a02:46:31. Inet addr:11.0.2.254 Bcast:11.0.2.255 Mask:255.255.255.0. Inet6 addr: fe80::1a98:51ff:fe02:4631/64 Scope:link. UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1. RX packets:18 errors:0 dropped:0 overruns:0 frame:0. TX packets:18 errors:0 dropped:0 overruns:0 carrier:0. collisions:0 txqueuelen:1000. RX bytes:648 (648.0 B) TX bytes:648 (648.0 B).
- ri-eth3:** Link encap:Ethernet HWaddr 3a:6e:ae:18:1b:72. Inet addr:11.0.3.254 Bcast:11.0.3.255 Mask:255.255.255.0. Inet6 addr: fe80::3c6e:aeff:fe18:1b72/64 Scope:link. UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1. RX packets:18 errors:0 dropped:0 overruns:0 frame:0. TX packets:18 errors:0 dropped:0 overruns:0 carrier:0. collisions:0 txqueuelen:1000. RX bytes:648 (648.0 B) TX bytes:648 (648.0 B).
- ri-eth4:** Link encap:Ethernet HWaddr 52:5e:ae:b3:c:18. Inet addr:19.0.0.1 Bcast:19.0.0.255 Mask:255.255.255.0. Inet6 addr: fe80::525e:ae:b3:c:18/64 Scope:link. UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1. RX packets:1246 errors:0 dropped:0 overruns:0 frame:0. TX packets:263 errors:0 dropped:0 overruns:0 carrier:0. collisions:0 txqueuelen:1000. RX bytes:19350 (19.3 KB) TX bytes:20369 (20.3 KB).
- ri-eth5:** Link encap:Ethernet HWaddr e2:ec:84:25:20:b8. Inet addr:19.0.4.1 Bcast:19.0.4.255 Mask:255.255.255.0. Inet6 addr: fe80::e0ec:84ff:fe25:20b8/64 Scope:link. UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1. RX packets:18 errors:0 dropped:0 overruns:0 frame:0. TX packets:120 errors:0 dropped:0 overruns:0 carrier:0. collisions:0 txqueuelen:1000. RX bytes:648 (648.0 B) TX bytes:1152 (1.1 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:5 errors:0 dropped:0 overruns:0 frame:0. TX packets:5 errors:0 dropped:0 overruns:0 carrier:0. collisions:0 txqueuelen:0. RX bytes:528 (528.0 B) TX bytes:528 (528.0 B).

The secondary terminal window, titled "mininet@mininet-vm: ~/bgp", shows the prompt "mininet> xterm R1" and a list of terminal windows.

The bottom status bar shows the VM is running and the host is Windows 10.



```
root@mininet-vm:~/bgp# ifconfig
R2-eth1  Link encap:Ethernet  HWaddr 46:ef:4c:b7:9d:cf
          inet addr:12.0.1.254  Bcast:12.0.1.255  Mask:255.255.255.0
          inet6 addr: fe80::44e7:1cfff:feb7:9d6f/64 ScopeLink
          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-eth2  Link encap:Ethernet  HWaddr 82:c4:1e:39:72:ef
          inet addr:12.0.2.254  Bcast:12.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::80c4:1eff:fe39:72ef/64 ScopeLink
          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 f6:53:a1:36:b2:67
          inet addr:12.0.3.254  Bcast:12.0.3.255  Mask:255.255.255.0
          inet6 addr: fe80::f453:a1ff:fe36:b267/64 ScopeLink
          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 ac:47:85ff:fee7:eba9:64
          inet addr:9.0.0.2  Bcast:9.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::ac47:85ff:fee7:eba9/64 ScopeLink
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:598 errors:0 dropped:0 overruns:0 frame:0
          TX packets:577 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:45714 (45.7 KB)  TX bytes:45091 (45.0 KB)

R2-eth5  Link encap:Ethernet  HWaddr ea:36:9b:e4:59:6c
          inet addr:9.0.1.1  Bcast:9.0.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a836:9bfff:fe4:596c/64 ScopeLink
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1634 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1533 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:48738 (48.7 KB)  TX bytes:42583 (42.5 KB)

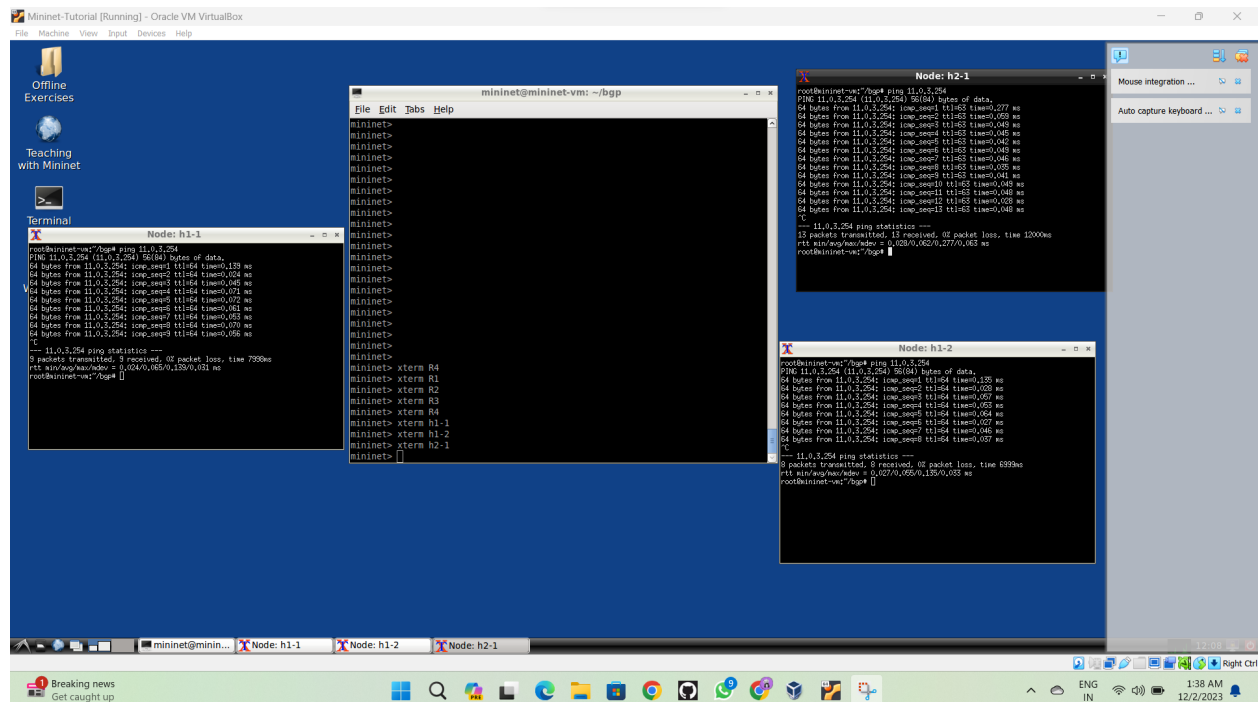
lo       Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
   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

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

```
mininet>
mininet>
mininet>
mininet> xterm R2
mininet>
mininet>
mininet>
mininet>
mininet>
mininet>
mininet>
mininet>
mininet>
mininet>
mininet>
mininet>
mininet>
mininet>
mininet>
```

In Node : R3

Answer 3 :



Host 3 -1 passes the reachability test from host 1 - 1
Host 3 -1 passes the reachability test from host 2 - 1
Host 3 -1 passes the reachability test from host 1 - 2

Host 3-1 is Accessible and can be reached by host 1 -1 & 2 -1 & 1 -2 in a networked environment.

Answer 4 : bgp routing table of the routers

– About the Fields of BGP Routing table ,Routes to different ASes :

network - denotes network id of the destination

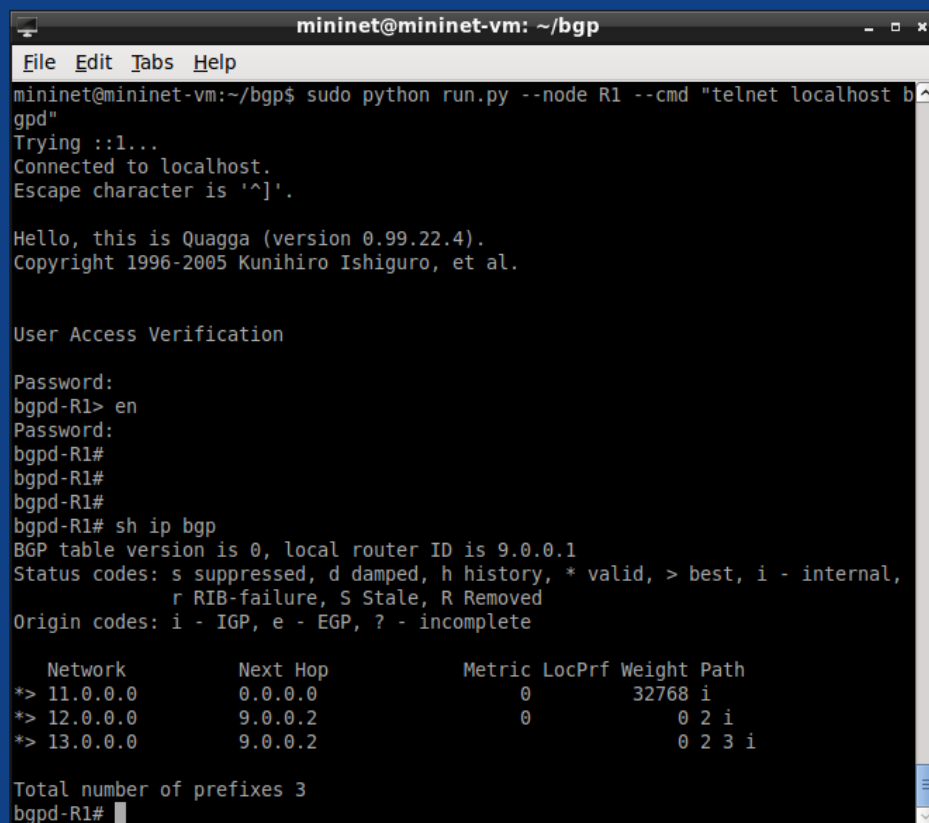
next hop - denotes the next router or device to reach the destination network

LocPref - denotes the local preference to be taken by AS.

Weight - denotes the cost of the route

Path - denotes the AS path to be followed to reach the destination

Here is the information and Screenshot of R1 :



```
mininet@mininet-vm: ~/bgp
File Edit Tabs Help
mininet@mininet-vm:~/bgp$ sudo python run.py --node R1 --cmd "telnet localhost bgpd"
Trying ::1...
Connected to localhost.
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#
bgpd-R1#
bgpd-R1#
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

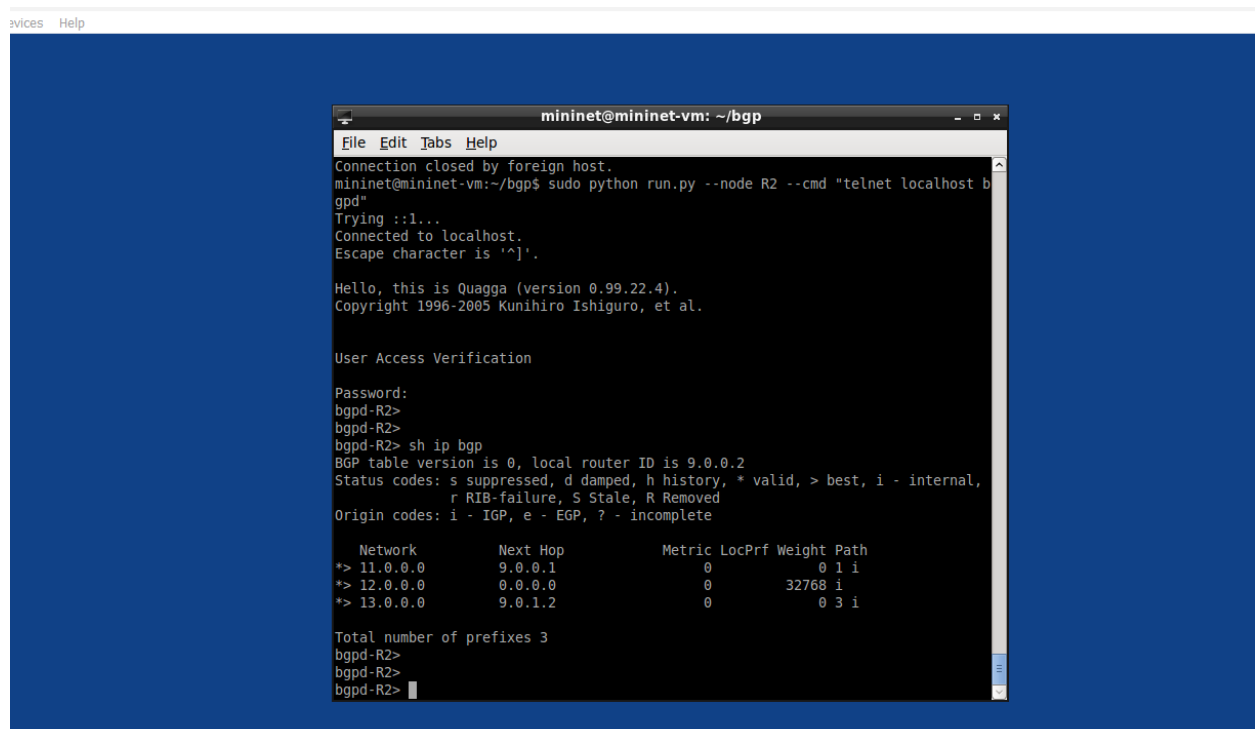
   Network        Next Hop           Metric LocPrf Weight Path
*> 11.0.0.0        0.0.0.0              0         32768 i
*> 12.0.0.0        9.0.0.2              0           2 i
*> 13.0.0.0        9.0.0.2              0           2 3 i

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

Answer 5 :

the entries in the routers different from each other ,From the Table Columns (Next Hop,Weight,Path) attributes are differed, the result shows that the path '1 i' & '3 i' signifying that packet traversal to router R1 as next hop is 9.0.0.1 ,and from source to destination path '3 i' is the destination hop as a next router and same for R2 case
Attributes are different network cidr

Here is the information and Screenshot of R2 :



```
mininet@mininet-vm: ~/bgp
File Edit Tabs Help
Connection closed by foreign host.
mininet@mininet-vm:~/bgp$ sudo python run.py --node R2 --cmd "telnet localhost b
gpd"
Trying ::1...
Connected to localhost.
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>
bgpd-R2>
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>
bgpd-R2>
bgpd-R2>
```

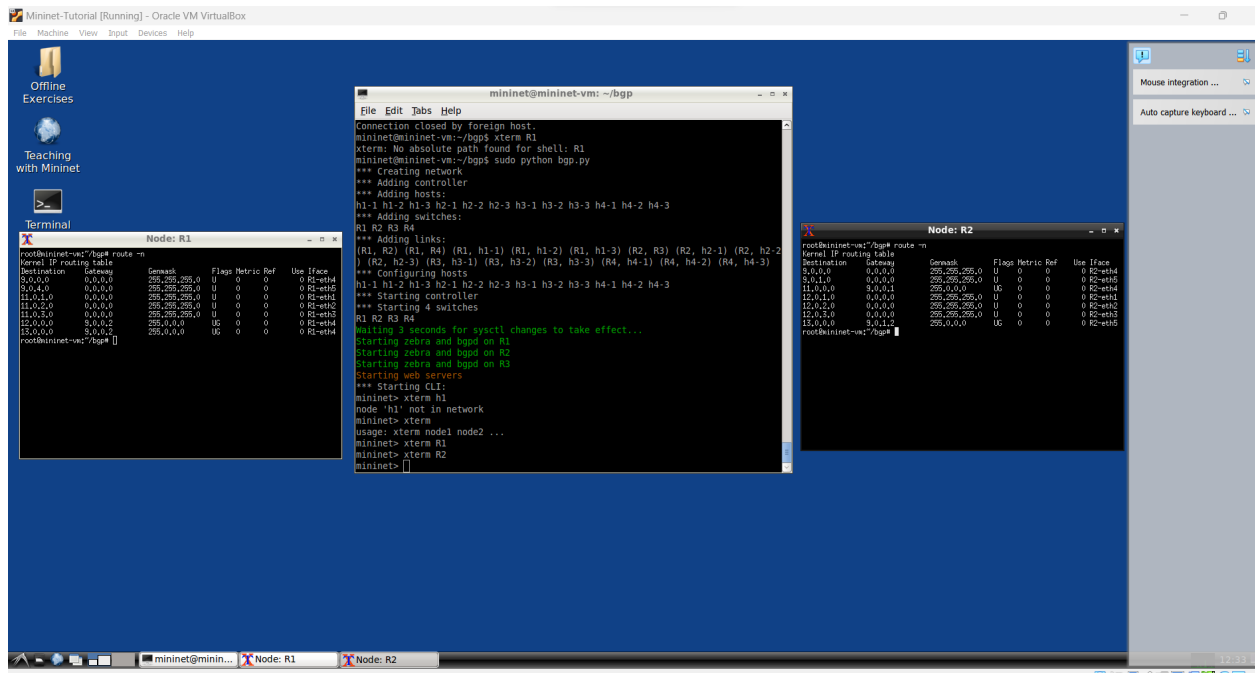
Answer 6 :

BGP Table : contains routes learned from eBGP peers ,
It may store multiple paths to destination.

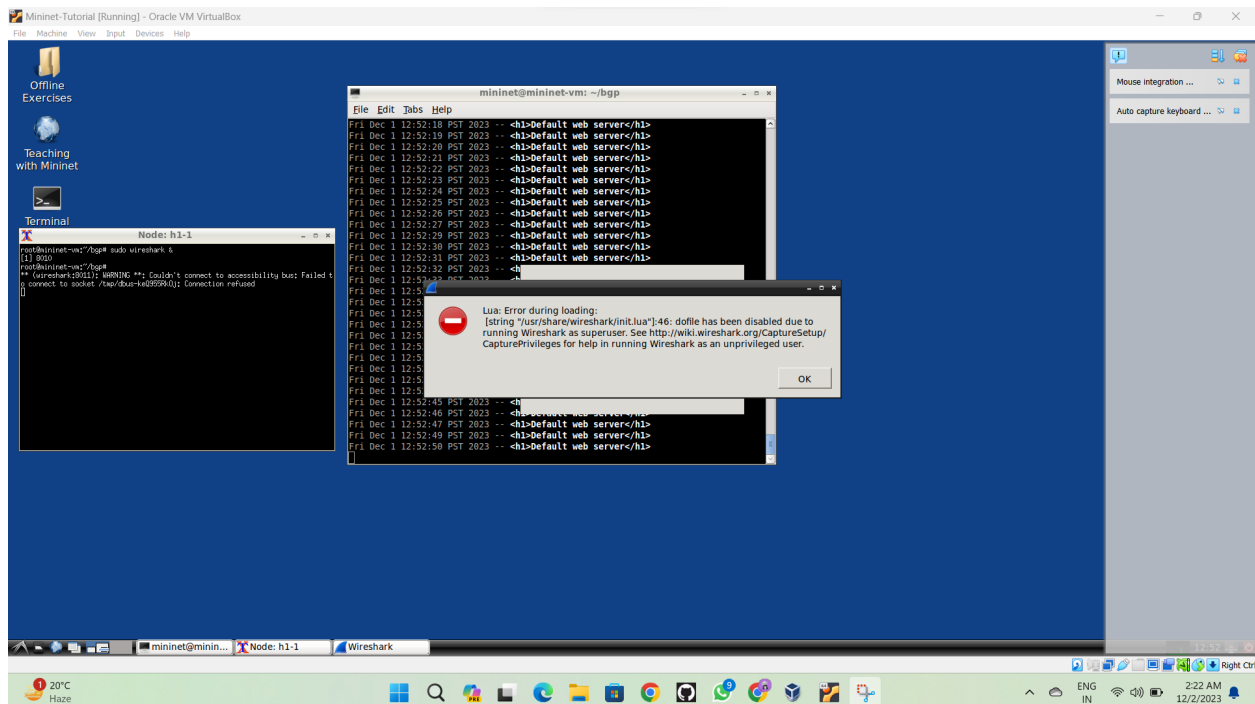
Forwarding Table : Stored and used in each routers and provides information about next path where destination is ,and then forwards that packet to that interface and this tables are populated using RIP,OSPF,.. Through inter local router path calculation or uploaded through SDNs

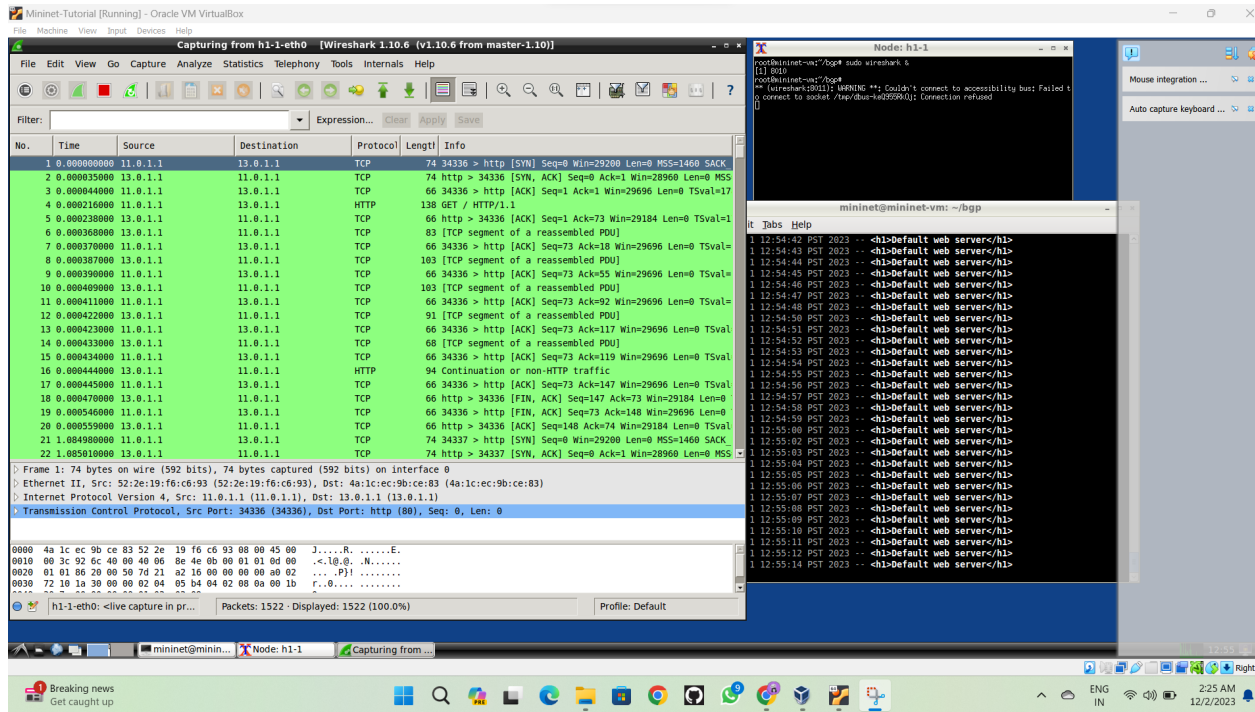
Populating Entries in Forwarding Table :

Before populating it compares with all attributes in a priority wise like next-hop if considered first or not ,what is the local preference AS paths,..
Screenshots of Forwarding Tables of Router 1 and Router 2 are attached below :

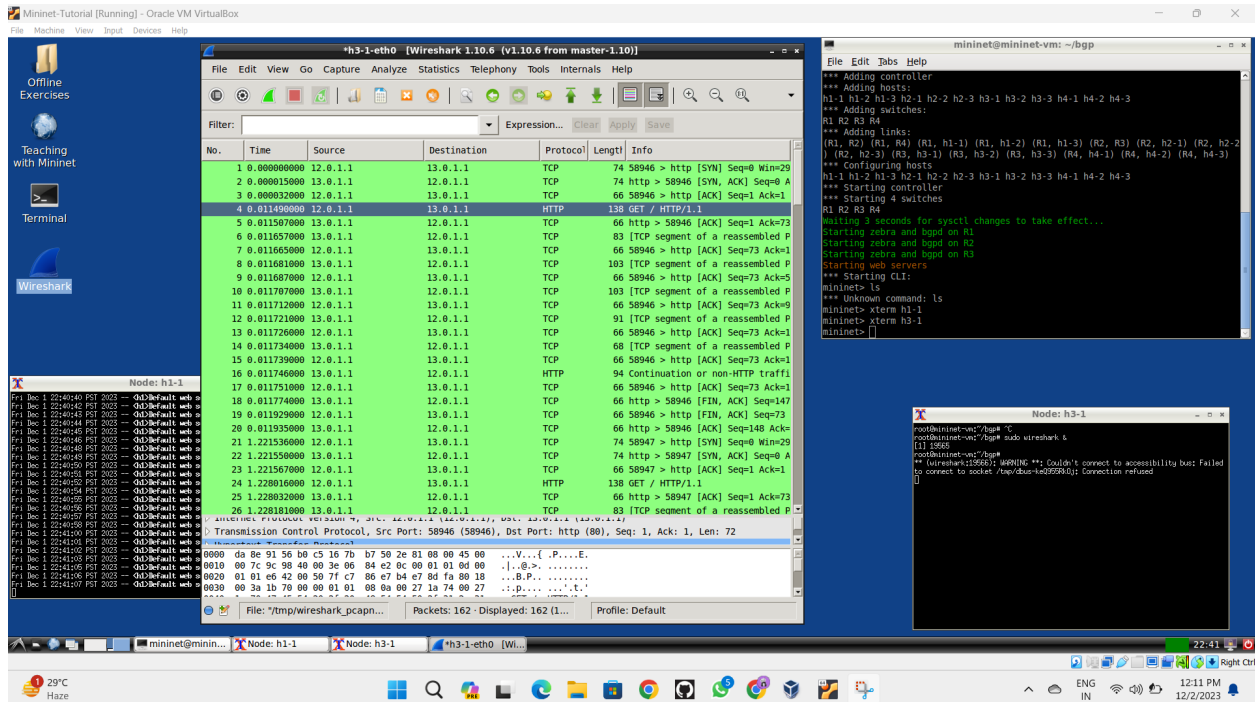


Answer 7 : Screenshots of Wireshark and terminal are shown in below screenshot.





Answer 8 :



When ran the command `./website.sh` GET request is sent to the attacker.
Not the target destination

The screenshot shows a Mininet VM terminal window with the following content:

```

mininet@mininet-vm: ~/bgp$ ls
bgp.py  connect.sh  logs      start_rogue.sh  webserver.py  website.sh
conf    install.sh  run.py    stop_rogue.sh   website2.sh
mininet@mininet-vm:~/bgp$ ./start_rogue.sh
Killing any existing rogue AS
Starting rogue AS
mininet@mininet-vm:~/bgp$

```

The output of the script shows a list of IP addresses for the rogue AS:

```

14 0.011734000 13.0.1.1
15 0.011739000 12.0.1.1
16 0.011746000 13.0.1.1

```

A second terminal window titled "Node: h1-1" is visible at the bottom, showing a list of IP addresses for the host:

```

Fri Dec 1 22:44:31 PST 2023 -- <hd>Default web server</hd>
Fri Dec 1 22:44:32 PST 2023 -- <hd>Default web server</hd>
Fri Dec 1 22:44:33 PST 2023 -- <hd>Default web server</hd>
Fri Dec 1 22:44:34 PST 2023 -- <hd>Default web server</hd>

```

Mininet-Tutorial [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

mininet@mininet-vm: ~/bgp

Node: h1-1

File

mininet
bgp.p
conf
mininet
Killi
Start
mininet

```

Fri Dec 1 22:48:42 PST 2023 -- <id> Attacker web server >>></id>
Fri Dec 1 22:48:43 PST 2023 -- <id> Attacker web server >>></id>
Fri Dec 1 22:48:45 PST 2023 -- <id> Attacker web server >>></id>
Fri Dec 1 22:48:46 PST 2023 -- <id> Attacker web server >>></id>
Fri Dec 1 22:48:47 PST 2023 -- <id> Attacker web server >>></id>
Fri Dec 1 22:48:48 PST 2023 -- <id> Attacker web server >>></id>
Fri Dec 1 22:48:50 PST 2023 -- <id> Attacker web server >>></id>
Fri Dec 1 22:48:51 PST 2023 -- <id> Attacker web server >>></id>
Fri Dec 1 22:48:52 PST 2023 -- <id> Attacker web server >>></id>
Fri Dec 1 22:48:53 PST 2023 -- <id> Attacker web server >>></id>
Fri Dec 1 22:48:54 PST 2023 -- <id> Attacker web server >>></id>
Fri Dec 1 22:48:55 PST 2023 -- <id> Attacker web server >>></id>
Fri Dec 1 22:48:57 PST 2023 -- <id> Attacker web server >>></id>
Fri Dec 1 22:48:58 PST 2023 -- <id> Attacker web server >>></id>
Fri Dec 1 22:48:59 PST 2023 -- <id> Attacker web server >>></id>
Fri Dec 1 22:49:00 PST 2023 -- <id> Attacker web server >>></id>
Fri Dec 1 22:49:01 PST 2023 -- <id> Attacker web server >>></id>
Fri Dec 1 22:49:03 PST 2023 -- <id> Attacker web server >>></id>
Fri Dec 1 22:49:04 PST 2023 -- <id> Attacker web server >>></id>
Fri Dec 1 22:49:05 PST 2023 -- <id> Attacker web server >>></id>
Fri Dec 1 22:49:06 PST 2023 -- <id> Attacker web server >>></id>
Fri Dec 1 22:49:07 PST 2023 -- <id> Attacker web server >>></id>
Fri Dec 1 22:49:08 PST 2023 -- <id> Attacker web server >>></id>
Fri Dec 1 22:49:10 PST 2023 -- <id> Attacker web server >>></id>
Fri Dec 1 22:49:11 PST 2023 -- <id> Attacker web server >>></id>
Fri Dec 1 22:49:12 PST 2023 -- <id> Attacker web server >>></id>
Fri Dec 1 22:49:13 PST 2023 -- <id> Attacker web server >>></id>
Fri Dec 1 22:49:15 PST 2023 -- <id> Attacker web server >>></id>
Fri Dec 1 22:49:16 PST 2023 -- <id> Attacker web server >>></id>
Fri Dec 1 22:49:17 PST 2023 -- <id> Attacker web server >>></id>
Fri Dec 1 22:49:18 PST 2023 -- <id> Attacker web server >>></id>

```

File Edit View Go

Filter:

No.	Time	Sou
1	0.000000000	12.
2	0.000015000	13.
3	0.000032000	12.
4	0.011490000	12.
5	0.011507000	13.
6	0.011657000	13.
7	0.011665000	12.
8	0.011681000	13.
9	0.011687000	12.
10	0.011707000	13.
11	0.011712000	12.
12	0.011721000	13.
13	0.011726000	12.
14	0.011734000	13.
15	0.011739000	12.
16	0.011746000	13.
17	0.011751000	12.
18	0.011774000	13.
19	0.011929000	12.
20	0.011935000	13.
21	1.221536000	12.
22	1.221550000	13.
23	1.221567000	12.

Answer 10 :

Request going to default web server : Shown in Below Screenshot

File Machine View Input Devices Help

mininet@mininet-vm: ~/bgp
Node: h1-1

```

^C
root@mininet-vm:~/bgp# ./website2.sh
Fri Dec 1 22:50:51 PST 2023 -- <h1>Default web server</h1>
Fri Dec 1 22:50:53 PST 2023 -- <h1>Default web server</h1>
Fri Dec 1 22:50:54 PST 2023 -- <h1>Default web server</h1>
Fri Dec 1 22:50:55 PST 2023 -- <h1>Default web server</h1>
Fri Dec 1 22:50:56 PST 2023 -- <h1>Default web server</h1>
Fri Dec 1 22:50:57 PST 2023 -- <h1>Default web server</h1>
Fri Dec 1 22:50:58 PST 2023 -- <h1>Default web server</h1>
Fri Dec 1 22:51:00 PST 2023 -- <h1>Default web server</h1>
Fri Dec 1 22:51:01 PST 2023 -- <h1>Default web server</h1>
Fri Dec 1 22:51:02 PST 2023 -- <h1>Default web server</h1>
Fri Dec 1 22:51:03 PST 2023 -- <h1>Default web server</h1>
Fri Dec 1 22:51:05 PST 2023 -- <h1>Default web server</h1>
Fri Dec 1 22:51:06 PST 2023 -- <h1>Default web server</h1>
Fri Dec 1 22:51:07 PST 2023 -- <h1>Default web server</h1>
Fri Dec 1 22:51:08 PST 2023 -- <h1>Default web server</h1>
Fri Dec 1 22:51:09 PST 2023 -- <h1>Default web server</h1>
Fri Dec 1 22:51:10 PST 2023 -- <h1>Default web server</h1>
Fri Dec 1 22:51:12 PST 2023 -- <h1>Default web server</h1>
Fri Dec 1 22:51:16 PST 2023 -- <h1>Default web server</h1>
Fri Dec 1 22:51:17 PST 2023 -- <h1>Default web server</h1>
Fri Dec 1 22:51:18 PST 2023 -- <h1>Default web server</h1>
Fri Dec 1 22:51:19 PST 2023 -- <h1>Default web server</h1>
Fri Dec 1 22:51:20 PST 2023 -- <h1>Default web server</h1>
Fri Dec 1 22:51:22 PST 2023 -- <h1>Default web server</h1>
Fri Dec 1 22:51:23 PST 2023 -- <h1>Default web server</h1>
sFri Dec 1 22:51:24 PST 2023 -- <h1>Default web server</h1>
Fri Dec 1 22:51:25 PST 2023 -- <h1>Default web server</h1>
Fri Dec 1 22:51:27 PST 2023 -- <h1>Default web server</h1>
Fri Dec 1 22:51:28 PST 2023 -- <h1>Default web server</h1>

```

File Edit

Filter:

No.	T
1	0.
2	0.
3	0.
4	0.
5	0.
6	0.
7	0.
8	0.
9	0.
10	0.
11	0.
12	0.
13	0.
14	0.
15	0.
16	0.
17	0.
18	0.
19	0.
20	0.

Answer 11 :

As Router R1 and Router R2 tables shown below:

In Case of R1 Table ,when will run start rogue command in mininet We can see the routers are updated , the shortest path according to hot potato rule will be used. Two different paths are added and in this case new path is taken where below R2 case old is used.

In Case of R2 Table, there is no change in path since the the request are sent to old path. Ie the default webserver.

```
Node: R1
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>
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 i
*> 13.0.0.0        9.0.4.2             0          4 i
*                  9.0.0.2             0          2 3 i

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

Source	Destination	Protocol	Length	Info
9.1.1	13.0.1.1	TCP	74	58946 > http [SYN] Seq

```
Node: R2
Escape character is '^]'.

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

User Access Verification

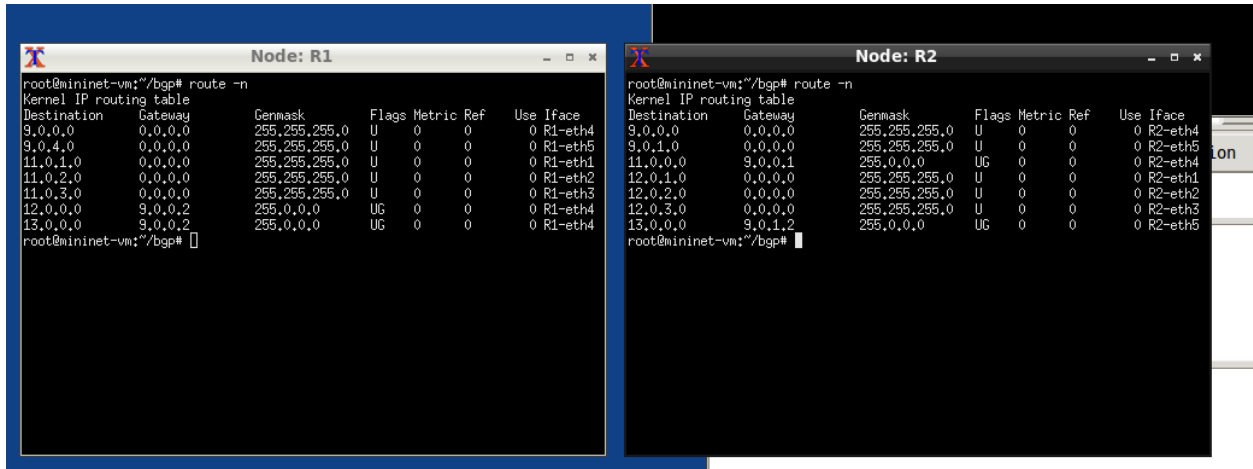
Password:
bgpd-R2>
bgpd-R2> sh ip bgp
BGP table version is 0, local router ID is 9.0.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

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

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

```
h1-1 h1-2
*** Addin
R1 R2 R3
*** Addin
(R1, R2)
) (R2, h2
*** Confi
h1-1 h1-2
*** Start
*** Start
R1 R2 R3
Waiting 3
Starting
Starting
Starting
Starting
*** Start
mininet>
```

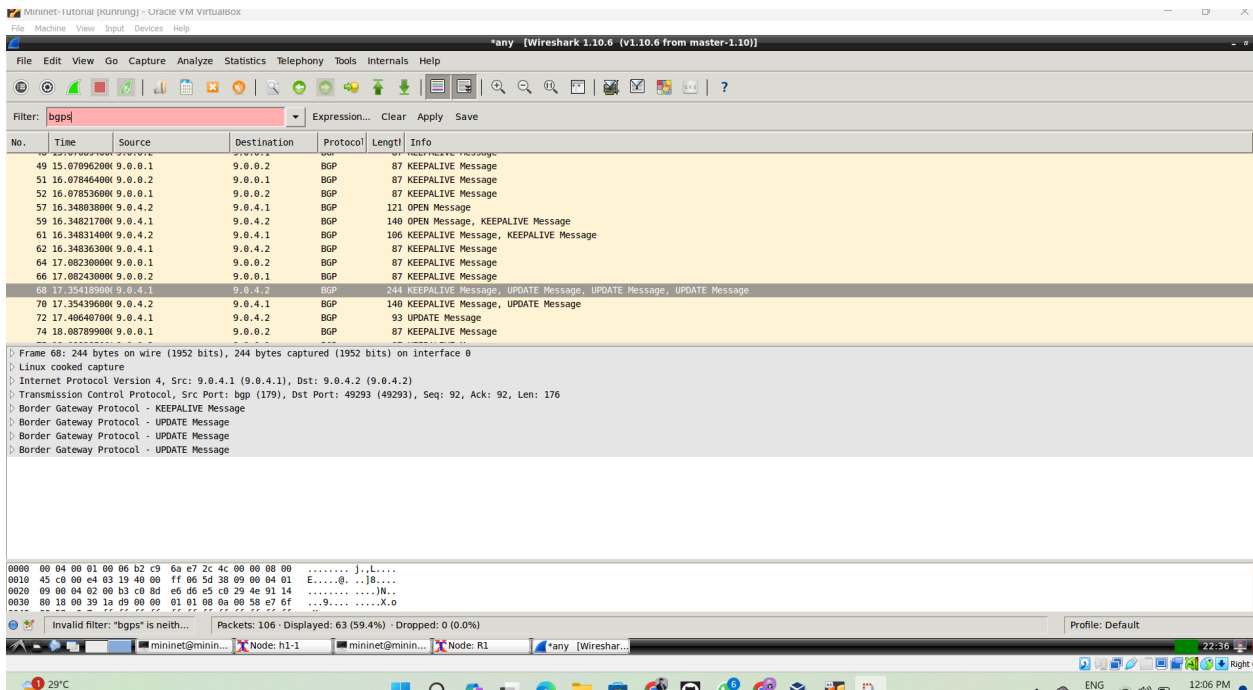
```
reshark 1.10.6 (v1.10.6 from master-1.10)]
```

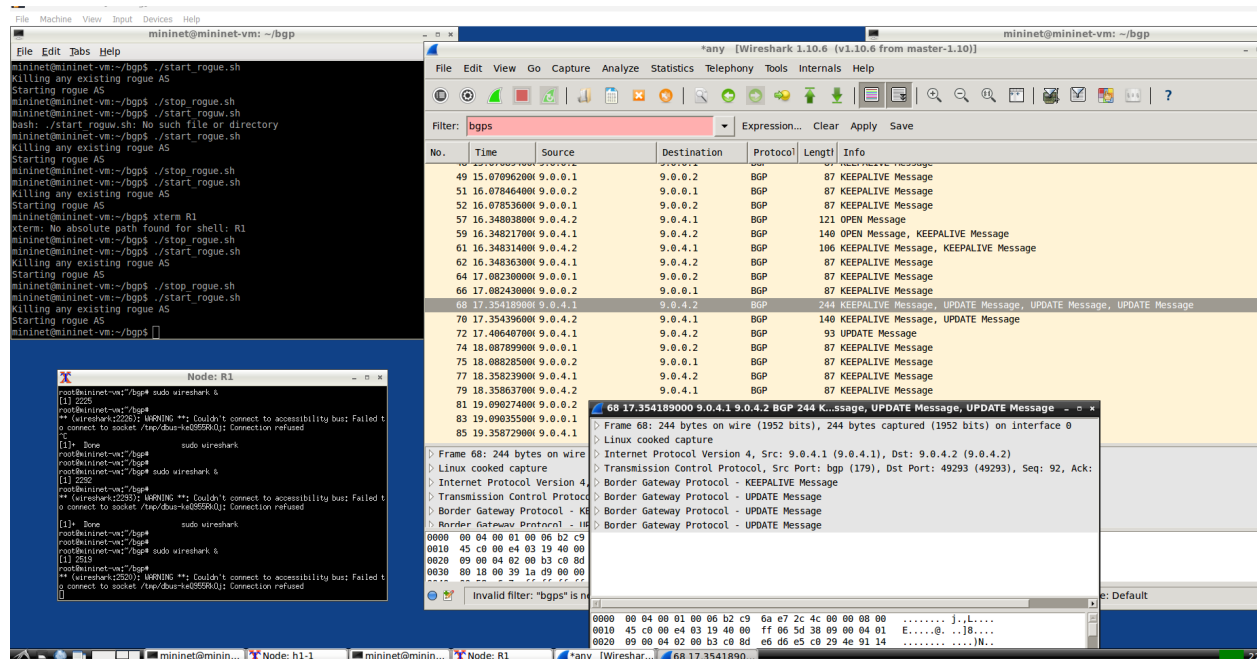


Answer 12 :

As Shown in the Screenshot the UPDATE message, 'Bgp req of Router 4 when broadcasted ,is accepted by router R1 ,BGP open packets and BGP keep alive packets manages and maintains the state of connection as alive.

R1 Replies with the bgp open message , and notify the router about the ASes





Answer 13 :

In this Scenario , the packets from router 1 and having the destination to Router 3 follows the particular sequence that is R : 1→2 , R : 2→3

Advertised of r4 ,ip addresses from r4

Bgp and forwarding tables are updated to include this advertise this addresses from router 4 , then r1 updates its path to choose its new path from newly updated tables.

And every other router traffic is also redirected though this new path instead of following old.

Answer 14 :

Shows a sudden decrease in avg RTT after execution of start rogue script ,it advertises ip 13.0.1.1 from attacker host,bgp updates its tables and notices the new path from h4-1 instead of h3 from router , the ping request is redirected to attacker host

Answer 15 :

Step 1 : modifying old bgp.py code to new bgp.py


```

File Edit Tabs Help
GNU nano 2.2.6 File: bgp.py

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

^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

```

Here I am modifying and assigning the host 3 to host 4 ip addresses

In this modified pic inet addresses of node h4-2 , h4-3 , h4-1

New modified topology :

```

mininet@mininet-vm: ~/bgp
Node: h4-2
root@mininet-vm:~/bgp# ifconfig
h4-2-eth0 Link encap:Ethernet  HWaddr 26:e2:11:c4:b:47:9f
    inet addr:14.0.2.1 Bcast:14.0.2.255 Mask:255.255.255.0
    inet6 addr: fe80::24e2:11c4:b47:9f: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-vm:~/bgp#

mininet@mininet-vm:~/bgp
Node: h4-3
root@mininet-vm:~/bgp# ifconfig
h4-3-eth0 Link encap:Ethernet  HWaddr 56:65:b4:05:67:ee
    inet addr:14.0.3.1 Bcast:14.0.3.255 Mask:255.255.255.0
    inet6 addr: fe80::5665:b4ff:fe05:67ee:54 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-vm:~/bgp#

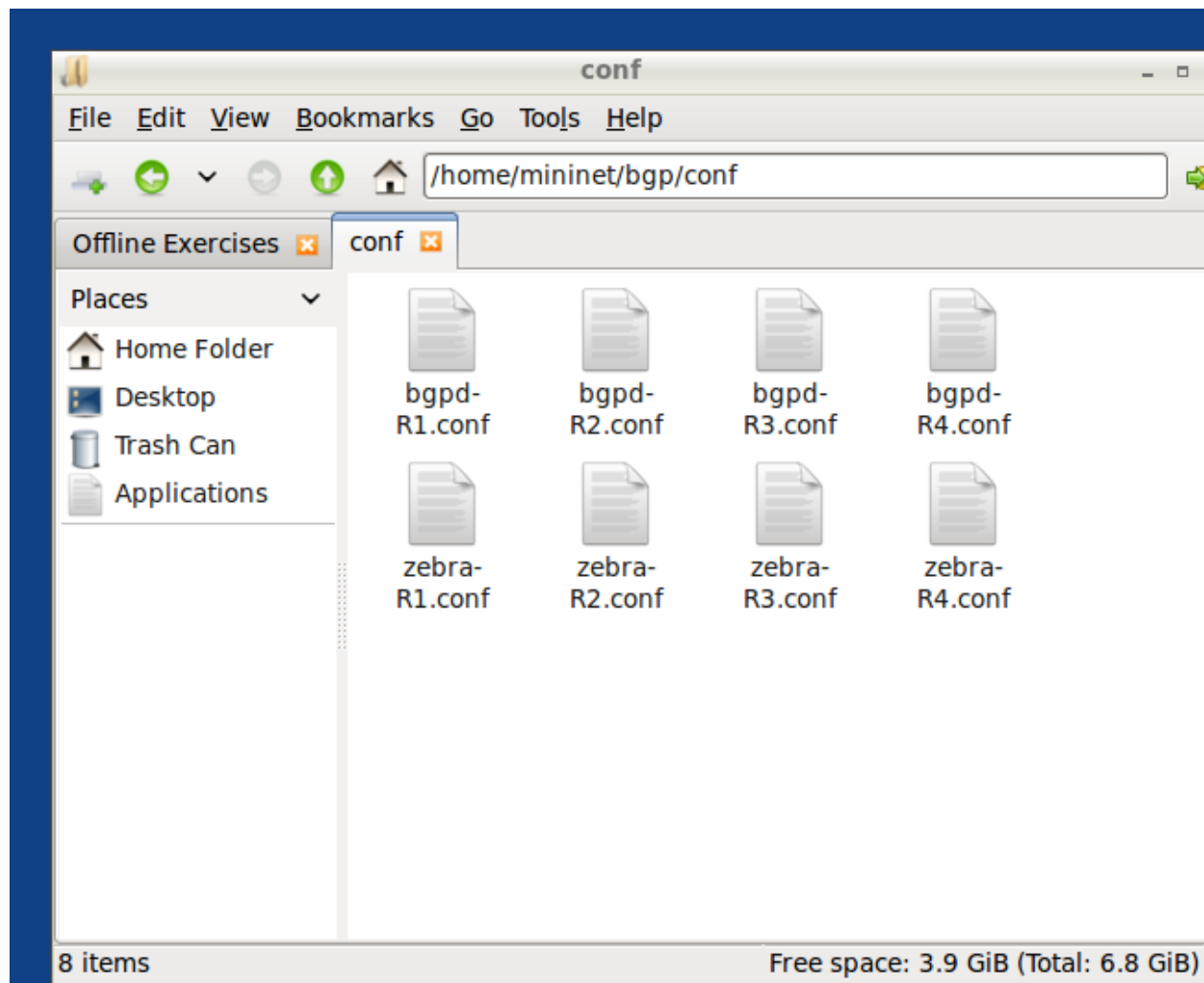
mininet@mininet-vm:~/bgp
Node: h4-1
root@mininet-vm:~/bgp# ifconfig
h4-1-eth0 Link encap:Ethernet  HWaddr 76:1e:34:45:a0:59
    inet addr:13.0.1.1 Bcast:13.0.1.255 Mask:255.255.255.0
    inet6 addr: fe80::741e:34ff:fe46:a059:54 Scope:Link
    UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
    RX 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-vm:~/bgp#

```

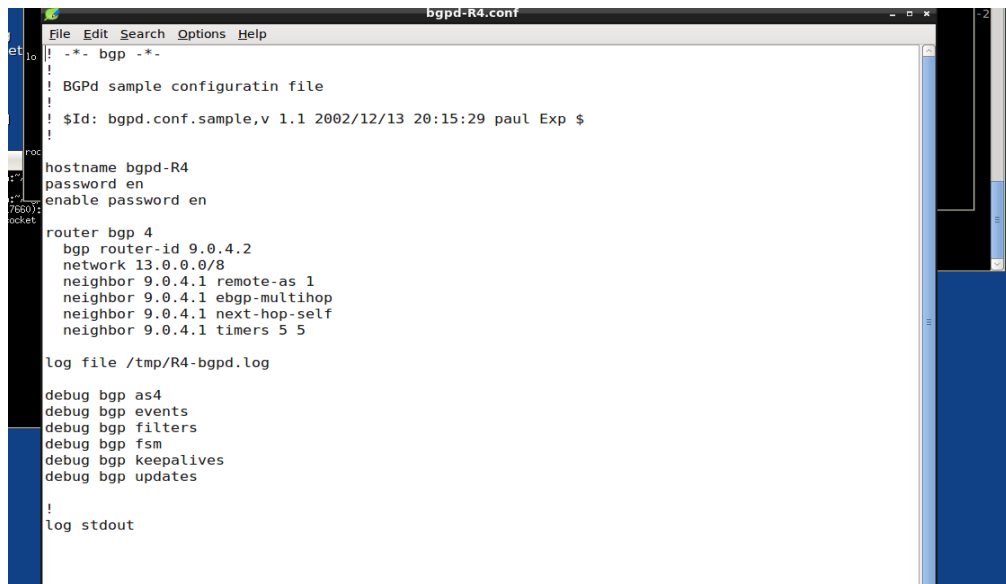
Step - 2: Changing Conf files for bgpd-4 and zebra-4



In router bgp 4

– Old bgpd -4.conf modified

Network 13.0.1.0/24 added & network



```
File Edit Search Options Help
! *- 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

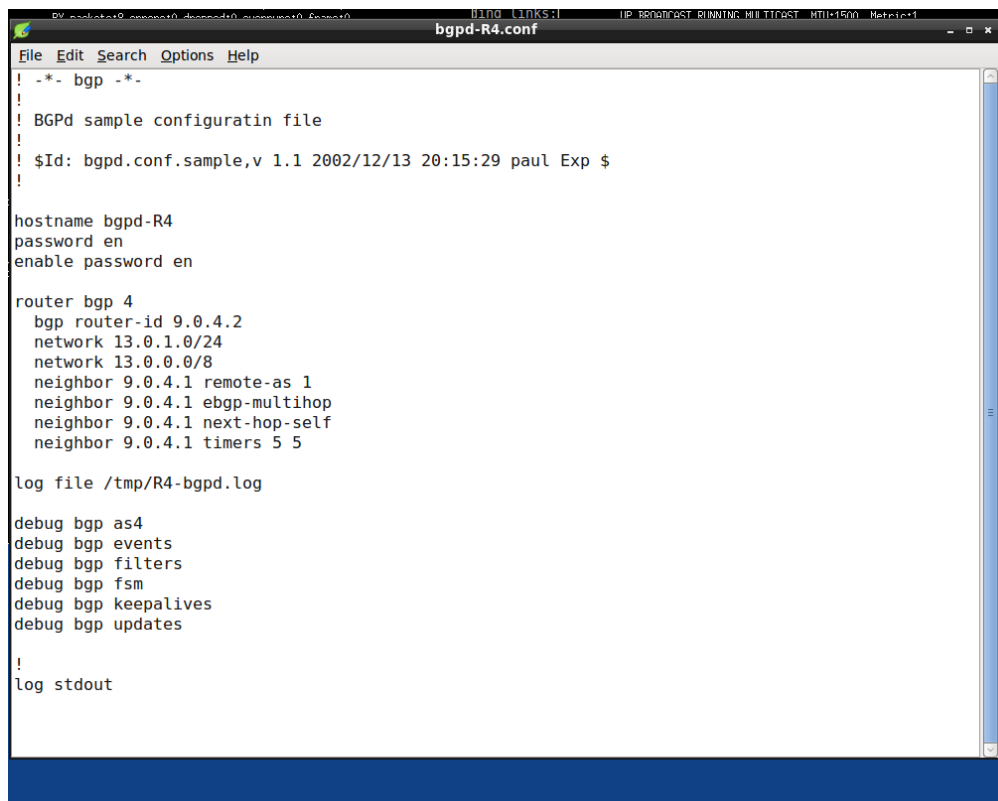
router bgp 4
  bgp router-id 9.0.4.2
  network 13.0.0.0/8
  neighbor 9.0.4.1 remote-as 1
  neighbor 9.0.4.1 ebgp-multihop
  neighbor 9.0.4.1 next-hop-self
  neighbor 9.0.4.1 timers 5 5

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
```

New modified bgp conf :



```
File Edit Search Options Help
! *- 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 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
```

Old conf file : zebra-R4.conf

```
ING MULTICAST MTU:1500 Metric:1
rs:0 dropped:0 overruns:0 frame:0
rs:0 dropped:0 overruns:0 carrier:0
uelen:1000
0 B) TX bytes:0

zebra-R4.conf
File Edit Search Options Help
! *- zebra *-

hostname R4
password en
enable password en

!

h4-1
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
```

New zebra.conf file :

```
len:1000
B) TX bytes:0

zebra-R4.conf
File Edit Search Options Help
! *- zebra *-

hostname R4
password en
enable password en

!

-1
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
```

Here is new route table and forwarding table of Router 1 is which modified by changing the topology

```
Node: R1
root@mininet-virtual-machine:~# sh ip bgp
sh: 0: Can't open ip
root@mininet-virtual-machine:~# bgp# route -n
Kernel IP routing table
Destination      Gateway         Genmask        Flags Metric Ref    Use Iface
0.0.0.0          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
root@mininet-virtual-machine:~# bgp# ifconfig
R1-eth1 Link encap:Ethernet HWaddr 0e:1a:fa:55:50:e5
        inet addr:11.0.1.254 Bcast:11.0.1.255 Mask:255.255.255.0
        inet6 addr: fe80::c1a:faff:fe55:50e5/64 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-eth2 Link encap:Ethernet HWaddr d6:9e:52:17:6e:64
        inet addr:11.0.2.254 Bcast:11.0.2.255 Mask:255.255.255.0
        inet6 addr: fe80::d49e:52ff:fe17:6e64/64 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 ba:74:e8:1e:e3:b2
        inet addr:11.0.3.254 Bcast:11.0.3.255 Mask:255.255.255.0
        inet6 addr: fe80::b874:e8ff:fe1e:e3b2/64 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-eth4 Link encap:Ethernet HWaddr 5a:85:d8:8d:c7:e6
        inet addr:9.0.0.1 Bcast:9.0.0.255 Mask:255.255.255.0
        inet6 addr: fe80::5885:d8ff:fe8d:c7e6/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:2371 errors:0 dropped:0 overruns:0 frame:0
        TX packets:2010 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:182651 (182.6 KB)  TX bytes:159828 (159.8 KB)

R1-eth5 Link encap:Ethernet HWaddr 32:e1:09:45:86:fb
        inet addr:9.0.4.1 Bcast:9.0.4.255 Mask:255.255.255.0
        inet6 addr: fe80::30e1:9ff:fe45:86fb/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:8 errors:0 dropped:0 overruns:0 frame:0
        TX packets:80 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:648 (648.0 B)  TX bytes:3672 (3.6 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:36 errors:0 dropped:0 overruns:0 frame:0
        TX packets:36 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:3168 (3.1 KB)  TX bytes:3168 (3.1 KB)

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

ANTI-PLAGIARISM Statement :

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.

Names <Roll Nos>: Yash Shukla <cs23mtech14018>

Date:03/12/2023

Signatures: Yash Shukla

Names <Roll Nos>:Punith Kumar Pulicharla <cs23mtech11032>

Date:03/12/2023

Signatures:Punith Kumar Pulicharla

Names <Roll Nos>: C.A Rakshith Ram<sm22mtech12003>

Date:03/12/2023

Signatures: C.A Rakshith Ram

References:

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

