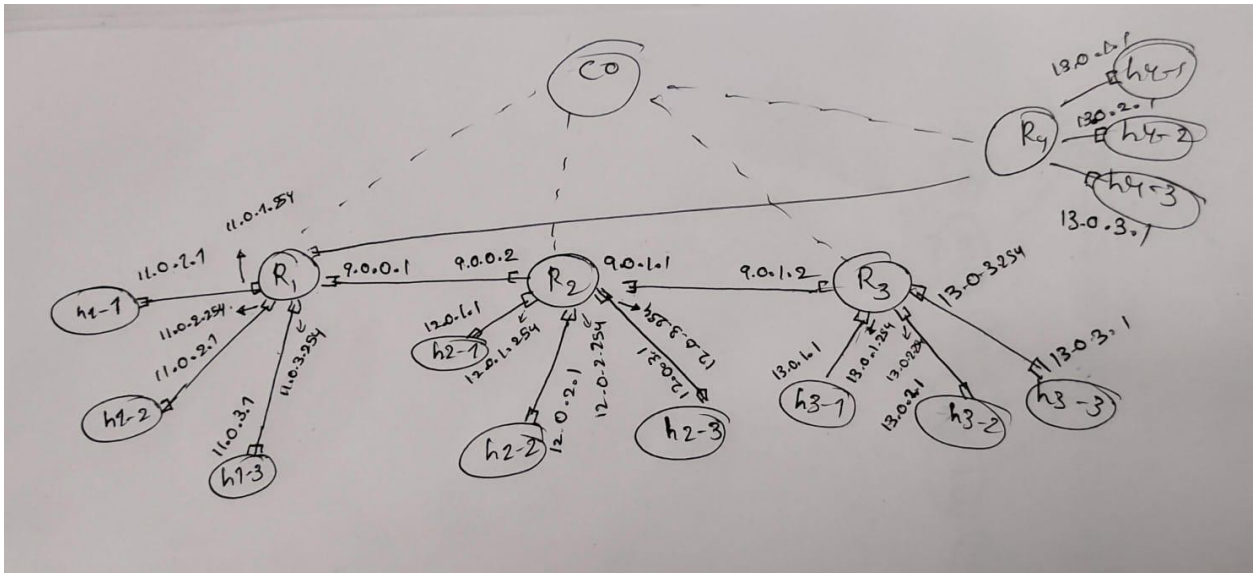
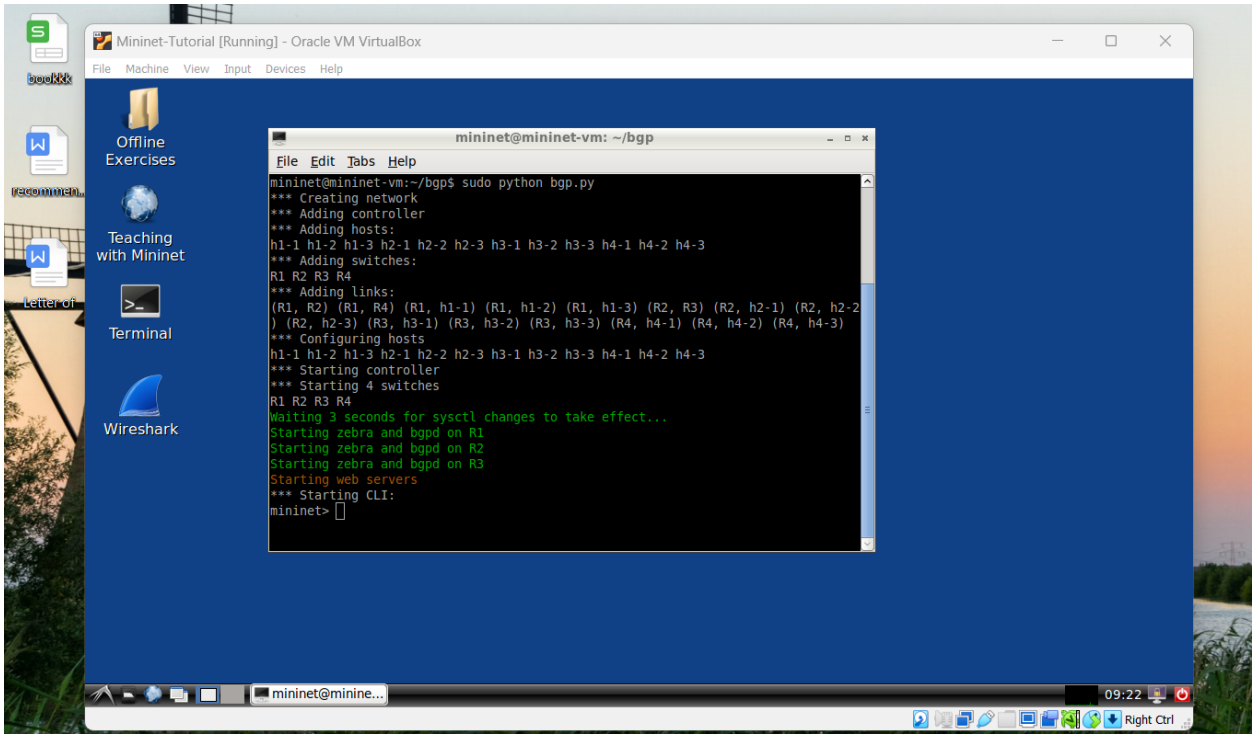
ACN Mininet Assignment: BGP Hijacking

Yash Shukla – cs23mtech14018
Punith Kumar Pulicharla – cs23mtech11032
C.A Rakshith Ram – sm22mtech12003

Answer 1 :



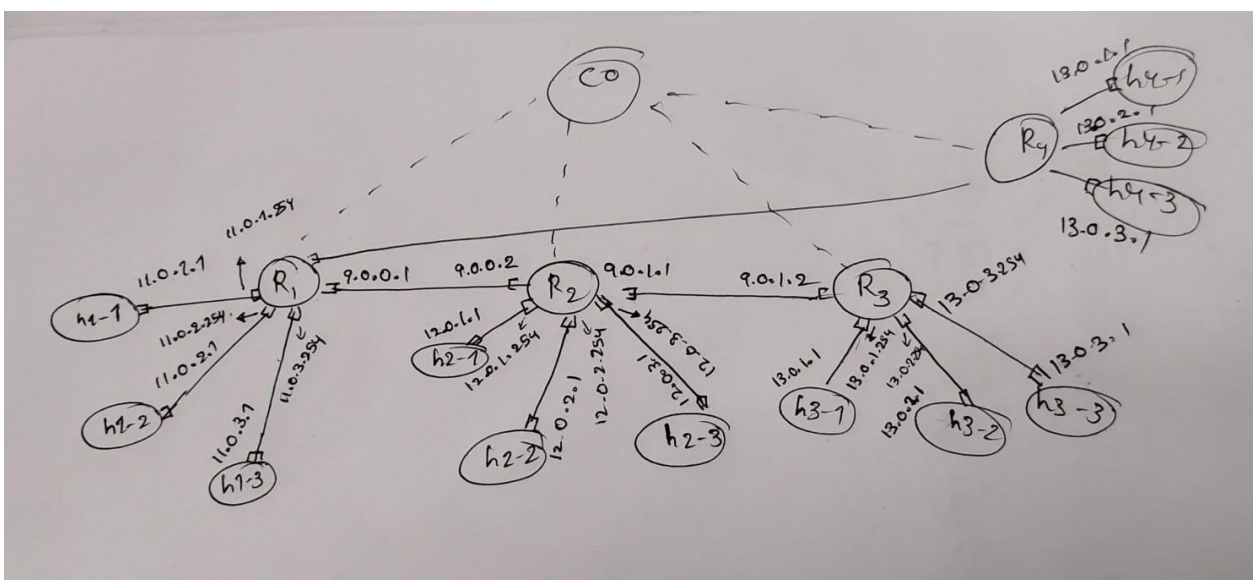
In total 12 Hosts are there and
4 Routers in Each Subset
Each Router having 3 Hosts



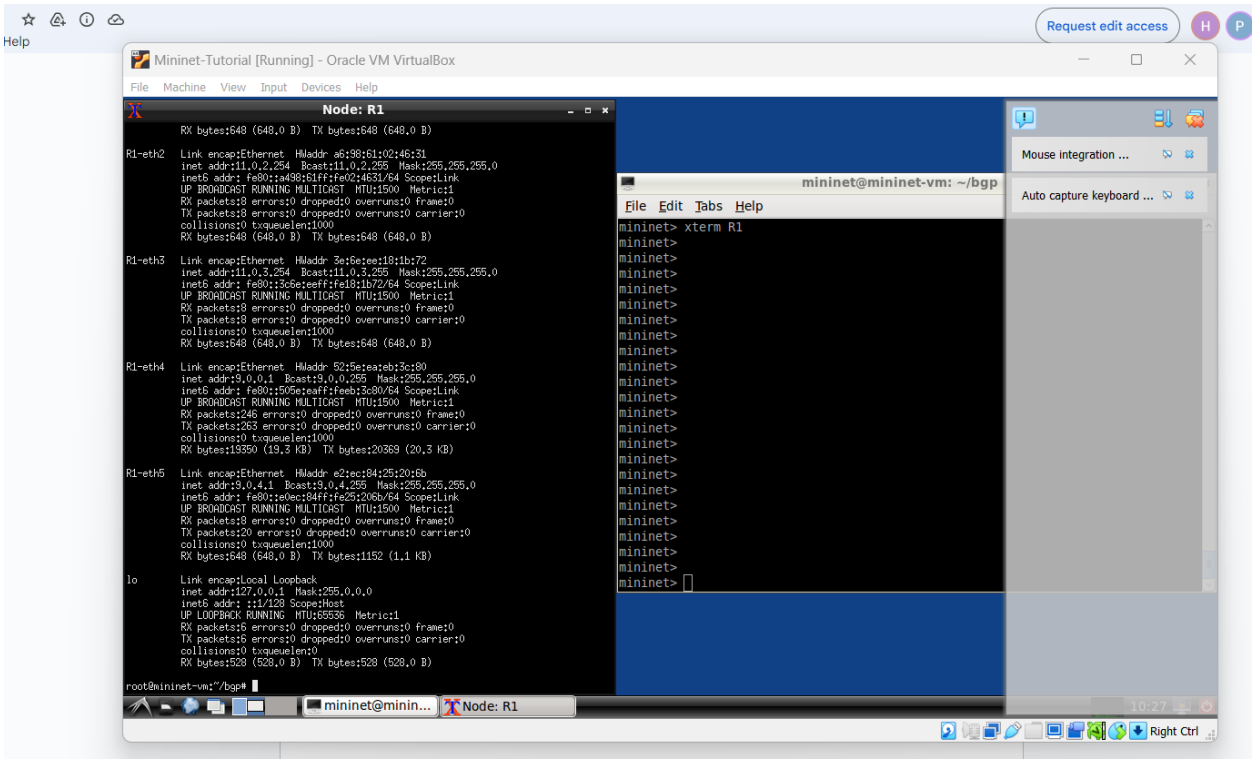
Answer 2 :

Available InterFace are shown below with their IP Addresses

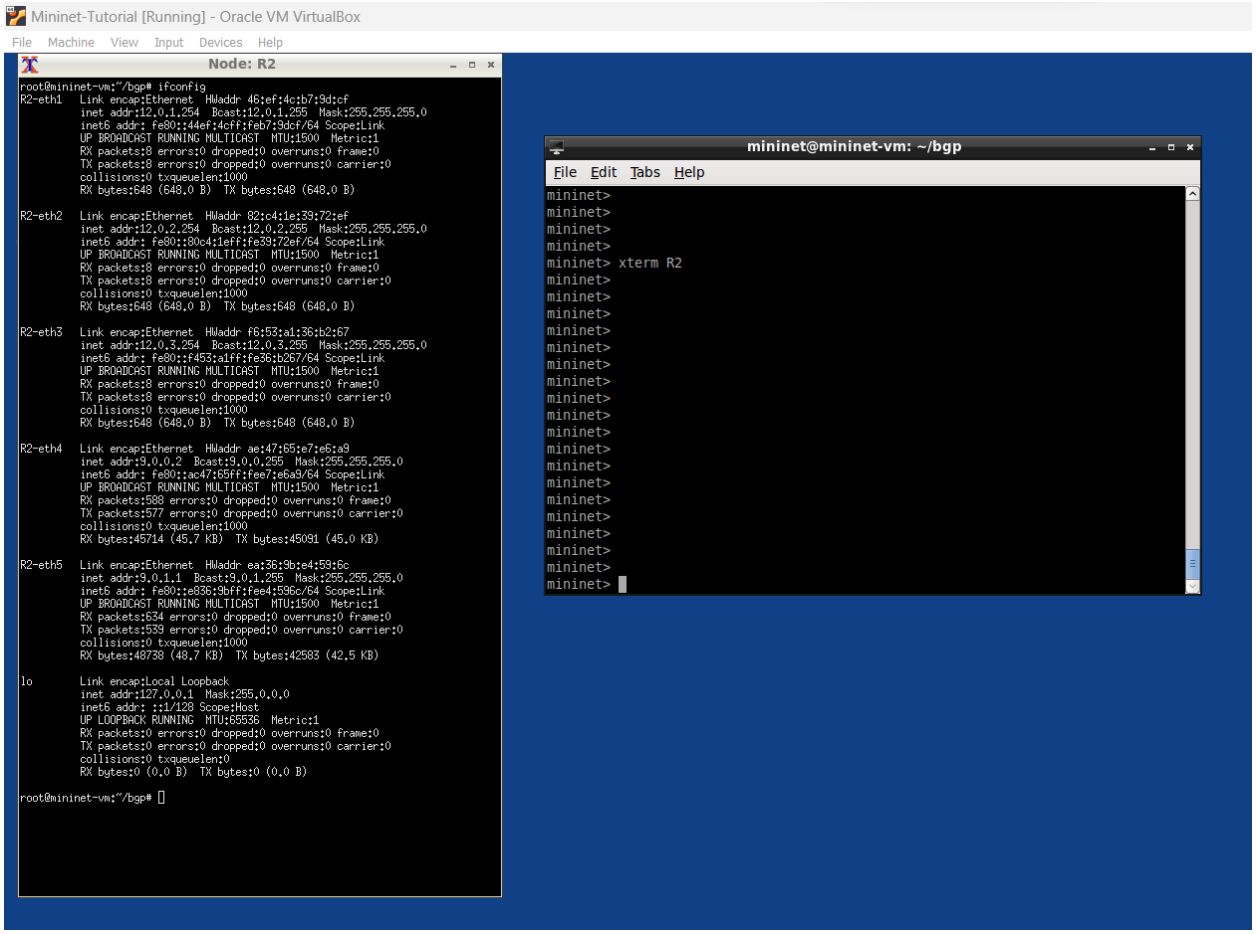
Ip Addresses are shown in the Topology Diagram :



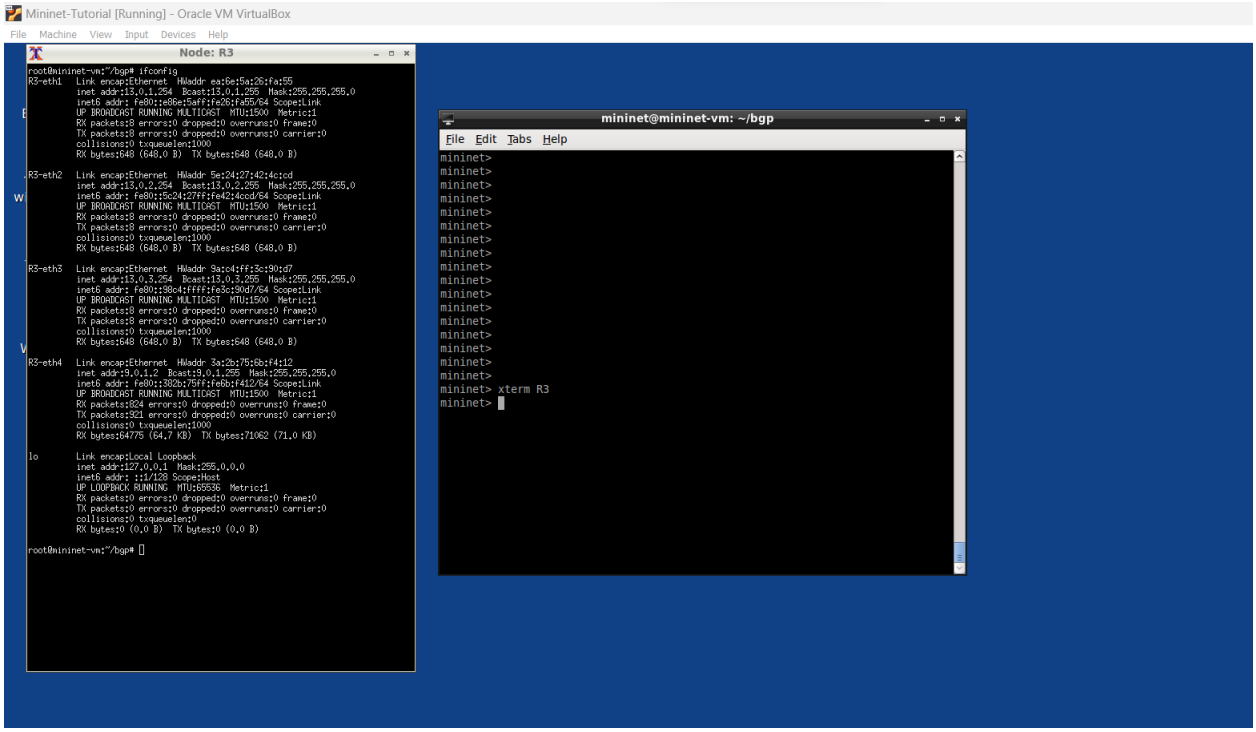
In node ： R1



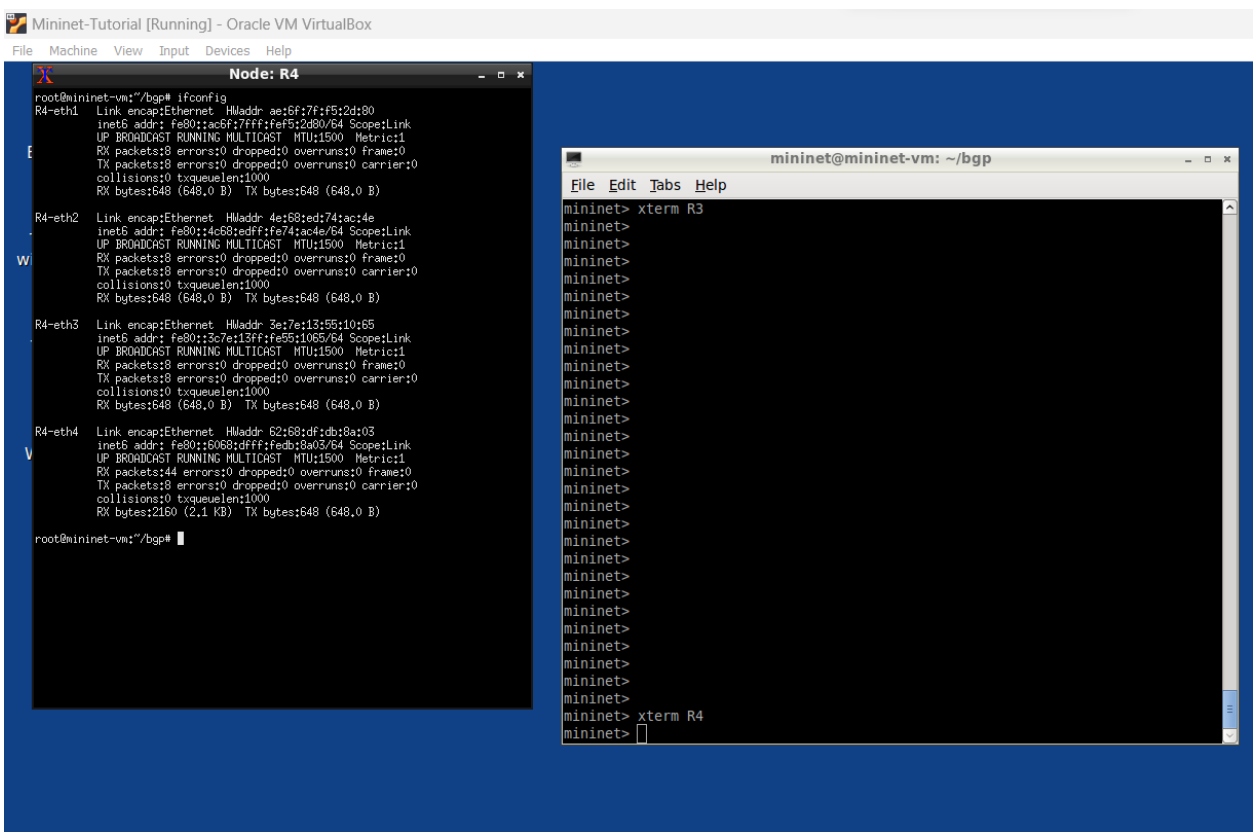
In Node ：R2


Mininet-Tutorial [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Node: R2
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::44ef:4cff:feb7:9dcf/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-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 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 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 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 ae:47:65:e7:e6:a9
inet addr:9.0.0.2 Bcast:9.0.0.255 Mask:255.255.255.0
inet6 addr: fe80::ac47:65ff:fee7:e6a9/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:588 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::e836:9bff:fee4:596c/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:634 errors:0 dropped:0 overruns:0 frame:0
TX packets:539 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-vm: ~/bgp
File Edit Tabs Help
mininet>
mininet>
mininet>
mininet>
mininet> xterm R2
mininet>
mininet>
mininet>
mininet>
mininet>
mininet>
mininet>
mininet>
mininet>
mininet>
mininet>
mininet>
mininet>
mininet>
mininet>
mininet>
mininet>
mininet>

In Node : R3

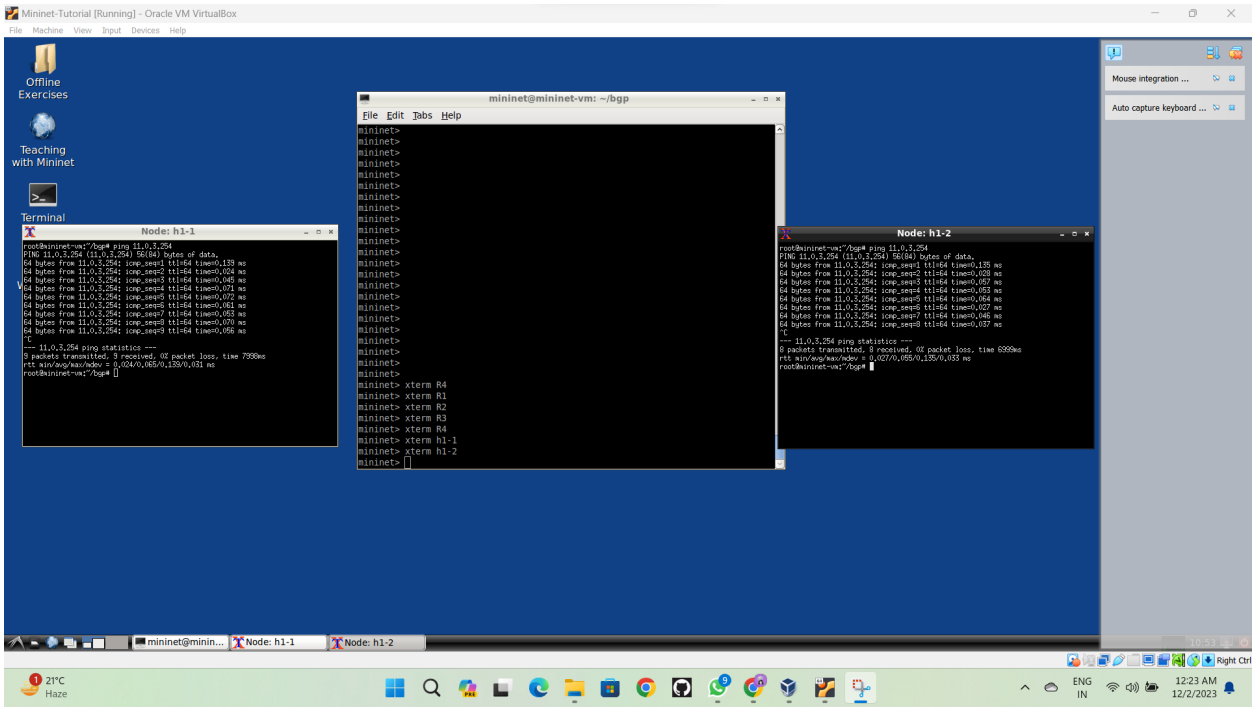

Mininet-Tutorial [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Node: R3
root@mininet-vm:~/bgp# ifconfig
R3-eth1 Link encap:Ethernet HWaddr ea:6e:5a:26:fa:55
inet addr:13.0.1.254 Bcast:13.0.1.255 Mask:255.255.255.0
inet6 addr: fe80::e66e:5aff:fe26:fa55/64 Scope:Link
UP BROADCAST 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-eth2 Link encap:Ethernet HWaddr 5e:24:27:42:4c:cd
inet addr:13.0.2.254 Bcast:13.0.2.255 Mask:255.255.255.0
inet6 addr: fe80::5c24:27ff:fe42:4ccd/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 9a:c4:ff:3c:90:d7
inet addr:13.0.3.254 Bcast:13.0.3.255 Mask:255.255.255.0
inet6 addr: fe80::98c4:ffff:fe3c:90d7/64 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 3a:2b:75:6b:f4:12
inet addr:9.0.1.2 Bcast:9.0.1.255 Mask:255.255.255.0
inet6 addr: fe80::382b:75ff:fe6b:f412/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:824 errors:0 dropped:0 overruns:0 frame:0
TX packets:321 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:64775 (64.7 KB) TX bytes:71062 (71.0 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-vm: ~/bgp
File Edit Tabs Help
mininet>
mininet> xterm R3
mininet>

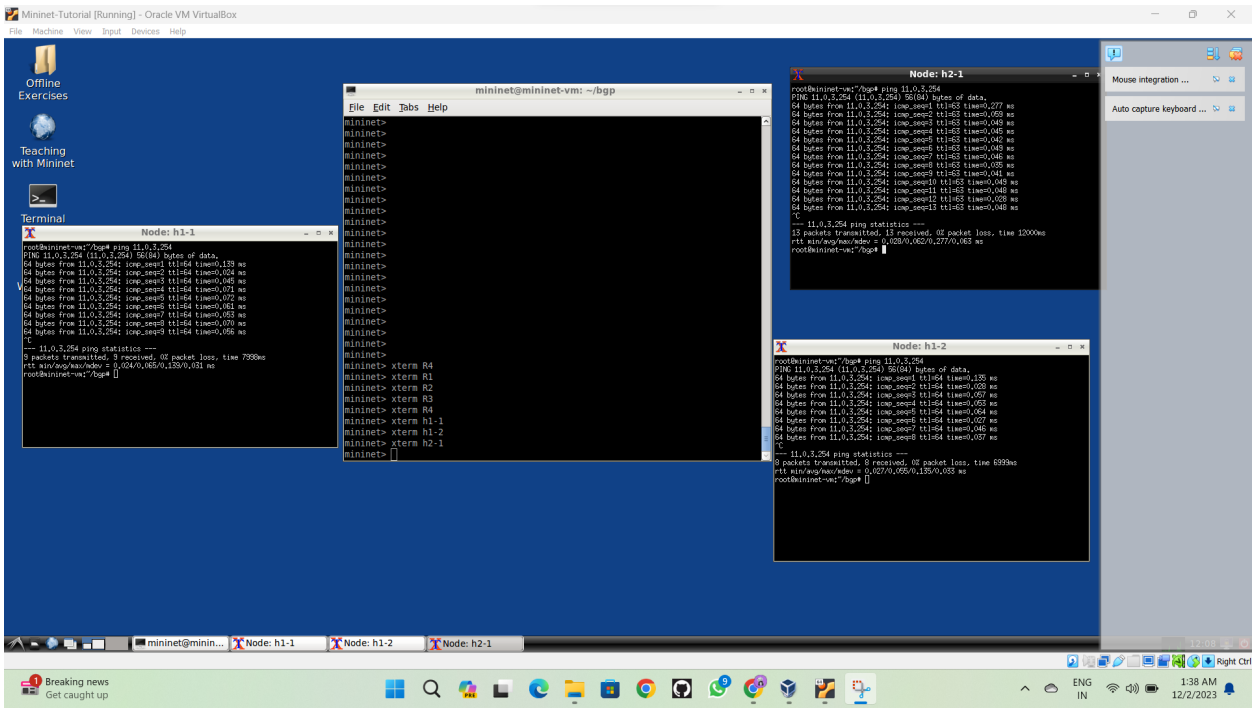
In Node : R4


Mininet-Tutorial [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Node: R4
root@mininet-vm:~/bgp# ifconfig
R4-eth1 Link encap:Ethernet HWaddr ae:6f:7f:f5:2d:80
inet6 addr: fe80::ac6f:7fff:fef5:2d80/64 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 4e:68:ed:74:ac:4e
inet6 addr: fe80::4c68:edff:fe74:ac4e/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 3e:7e:13:55:10:65
inet6 addr: fe80::3c7e:13ff:fe55:1065/64 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 62:68:df:db:8a:03
inet6 addr: fe80::6068:dfff:fedb:8a03/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:44 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:2160 (2.1 KB) TX bytes:648 (648.0 B)
root@mininet-vm:~/bgp#
mininet@mininet-vm: ~/bgp
File Edit Tabs Help
mininet> xterm R3
mininet> xterm R4
mininet>

Ip Addresses of R4 havent been assigned yet , the allocation of the ip addresses will be assigned when the start rogue script initiates.

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

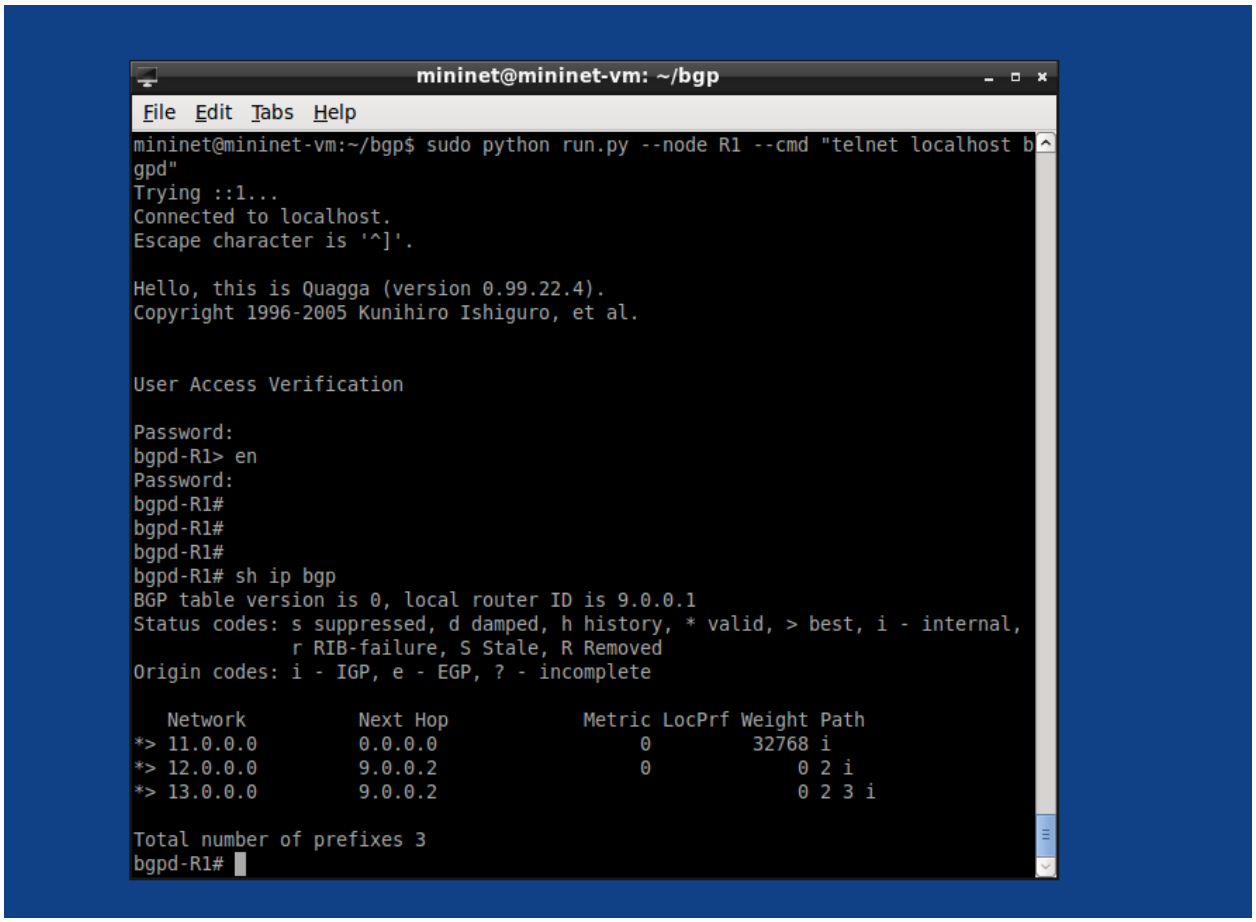
Host 3-1 is Accessible and can be reached by host 1 -1 & 2 -1 & 1 -2 in a networked environment.

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

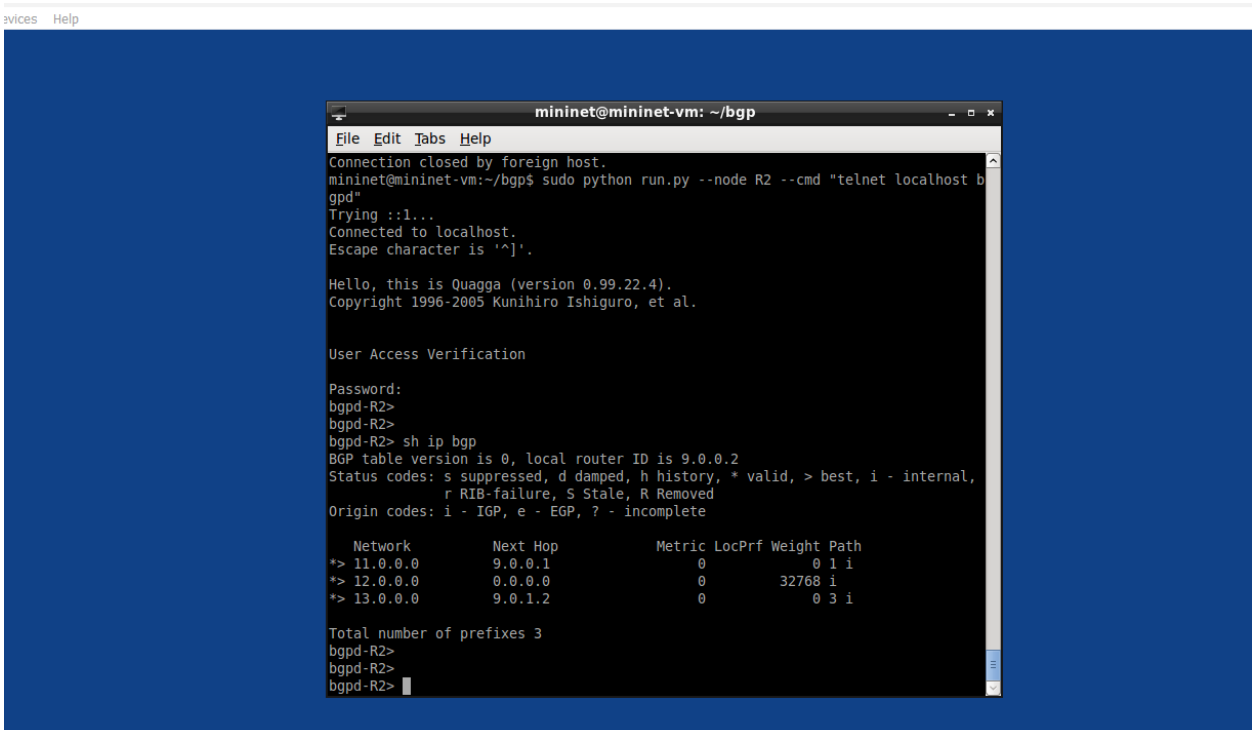
Here is the information and Screenshot of R1 :



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 cider

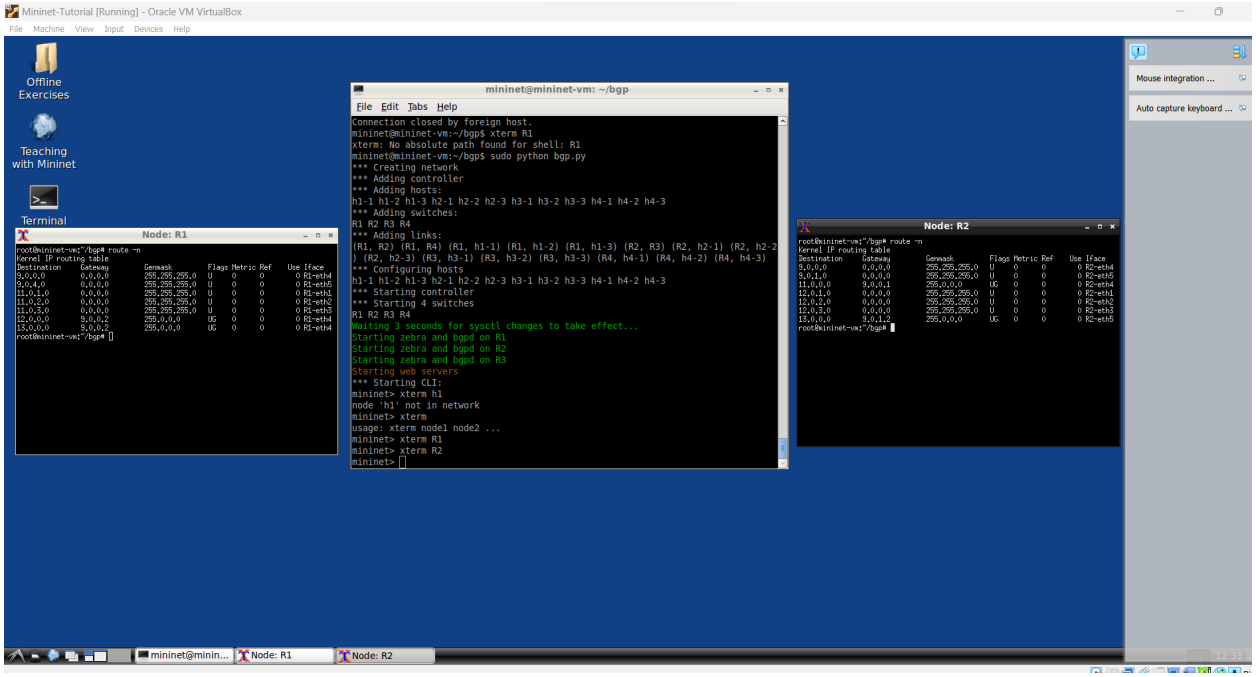
Here is the information and Screenshot of R2 :



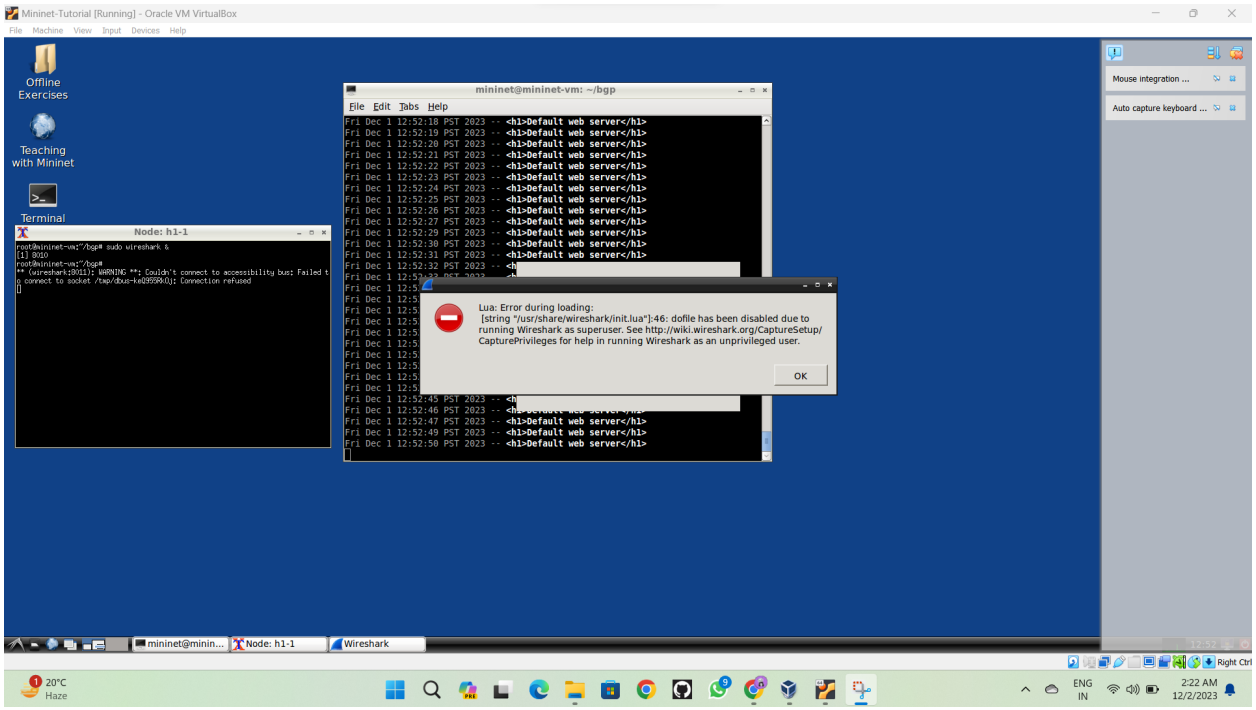
Answer 6 :

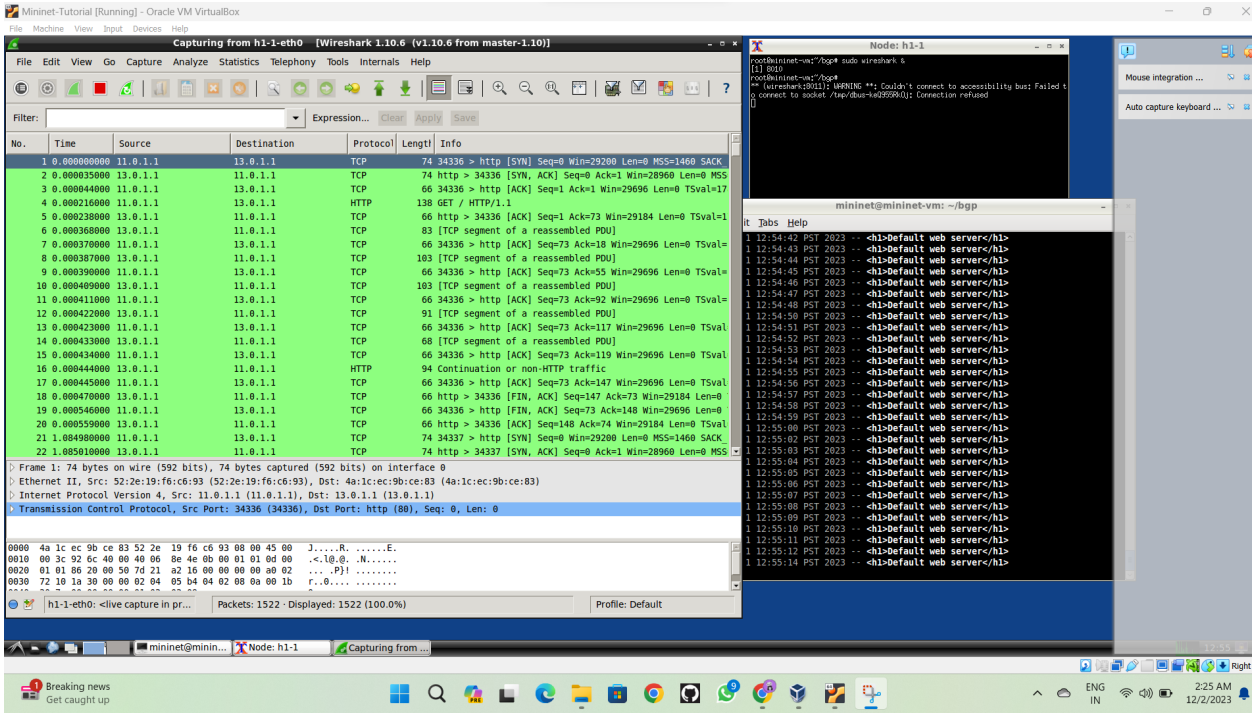
BGP Table : contains routes learned from eBGP peers ,
It may store multiple paths to destination.
Forwarding Table : Stored and used in each routers and provides information about next path where destination is ,and then forwards that packet to that interface and this tables are populated using RIP,OSPF,.. 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 :

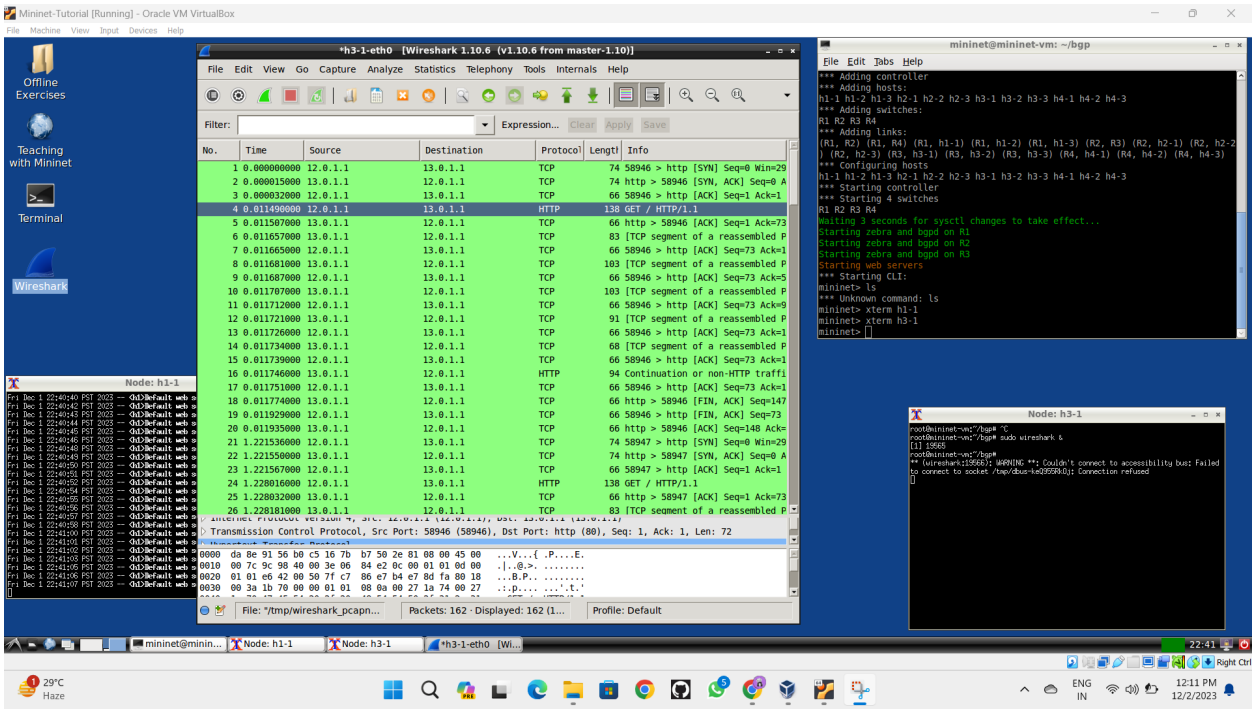


Answer 7 : Screenshots of wireshark and terminal are shown in below screenshot.



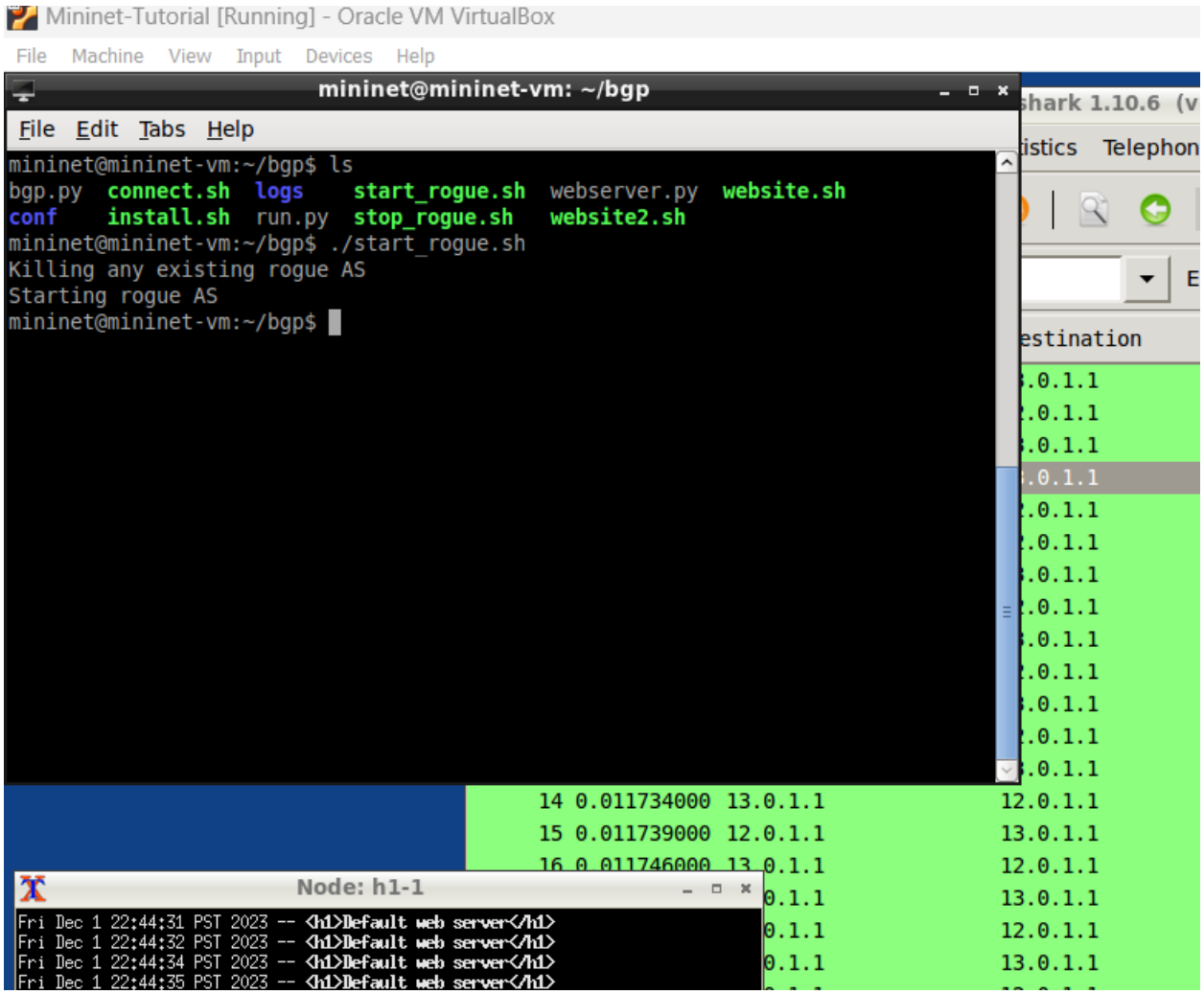

Mininet-Tutorial [Running] - Oracle VM VirtualBox
Capturing from h1-1-eth0 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
Node: h1-1
mininet@mininet-vm: ~/bgp

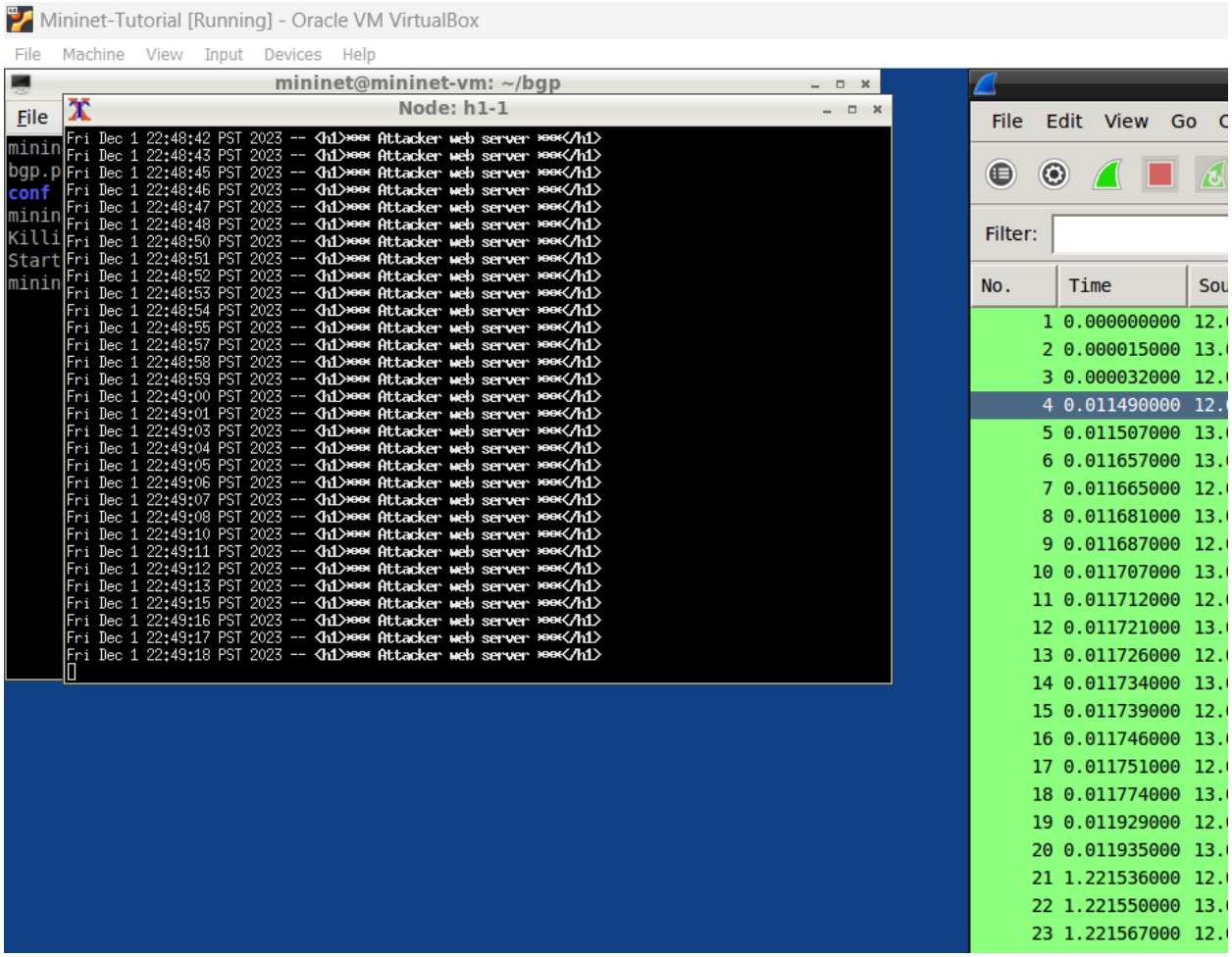
Answer 8 :


Mininet-Tutorial [Running] - Oracle VM VirtualBox
*h3-1-eth0 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
mininet@mininet-vm: ~/bgp
Node: h1-1
Node: h3-1

Answer 9 :

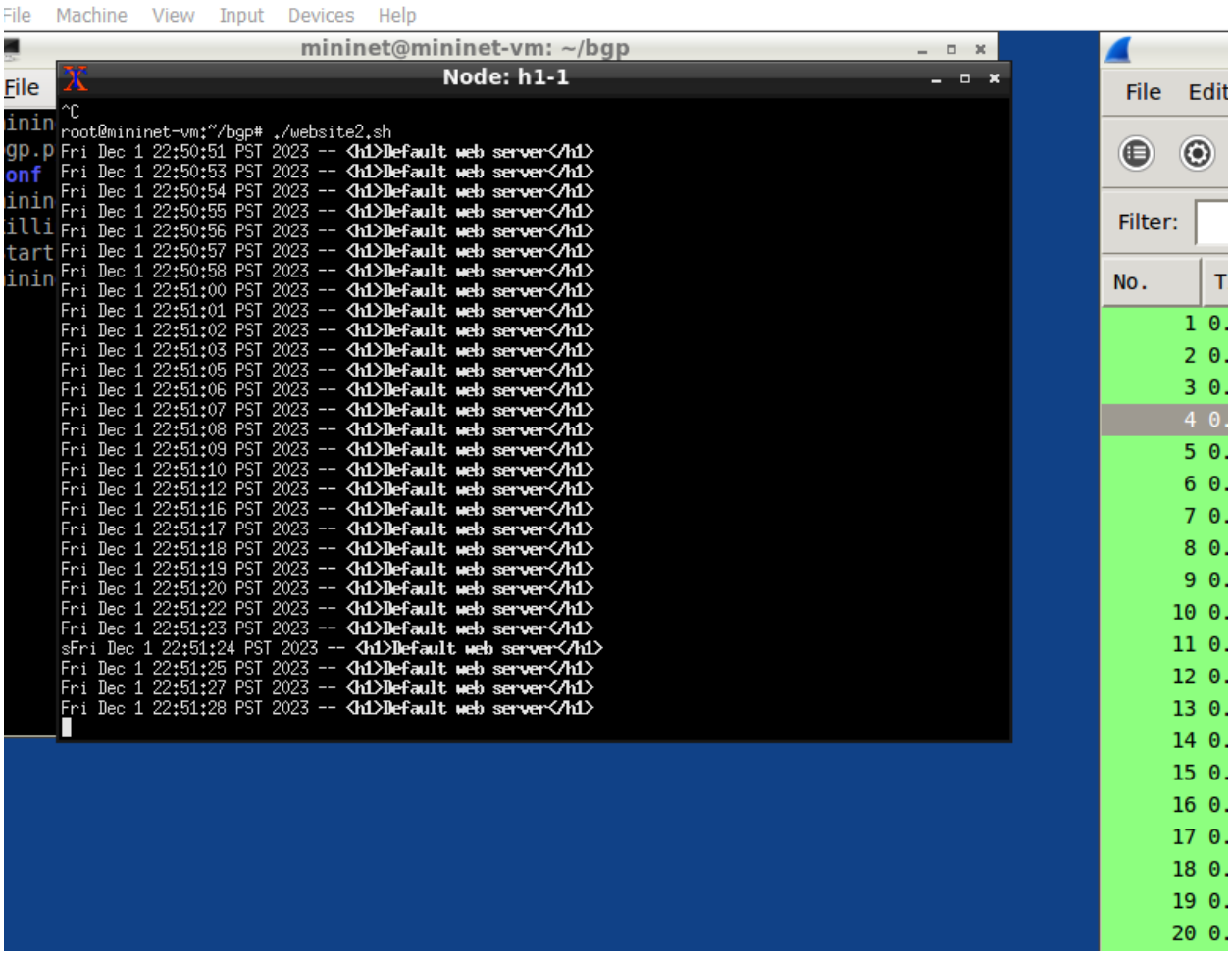
When ran the command ./website.sh GET request is sent to the attacker.
Not the target destination





Answer 10 :

<u>Request going to default web server : Shown in Below Screenshot</u>

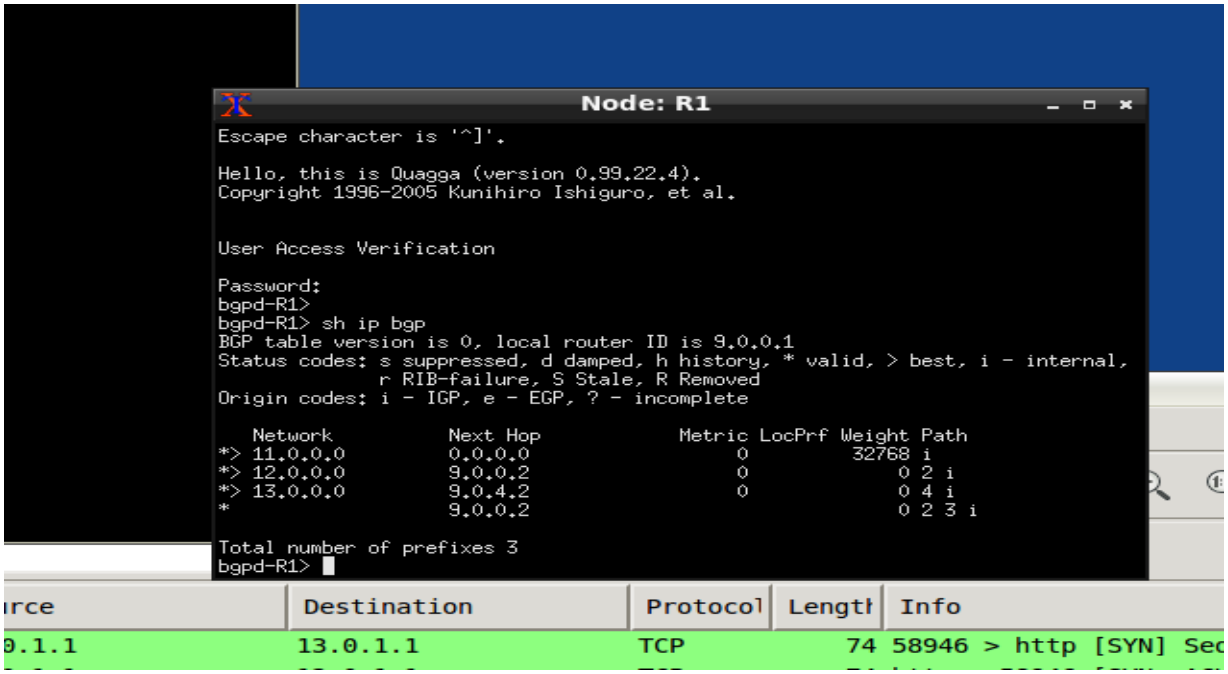


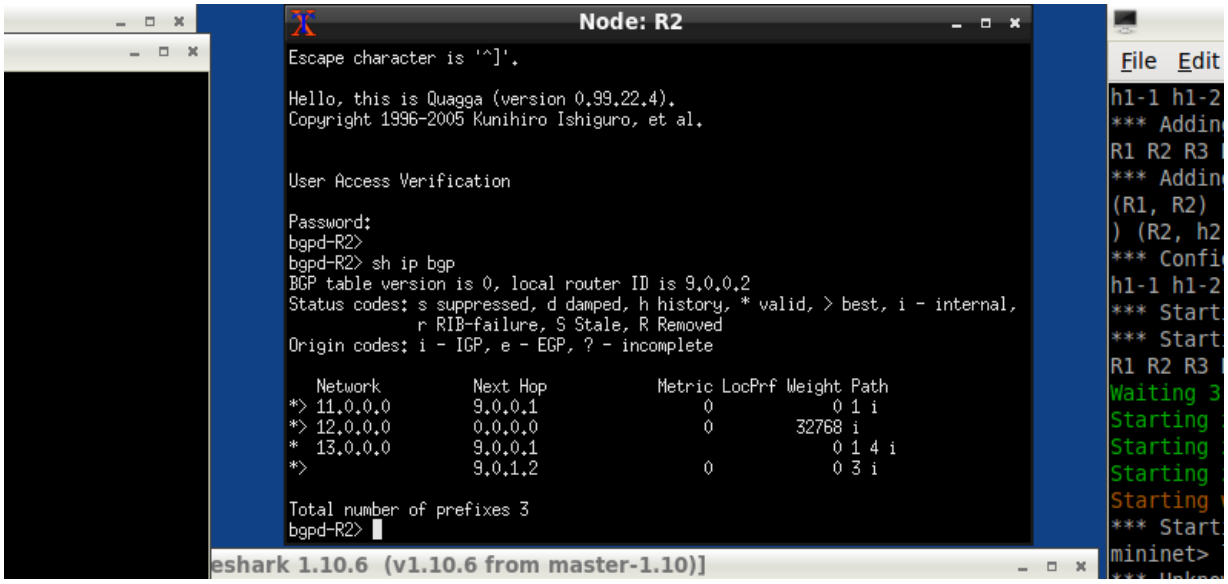
Answer 11 :

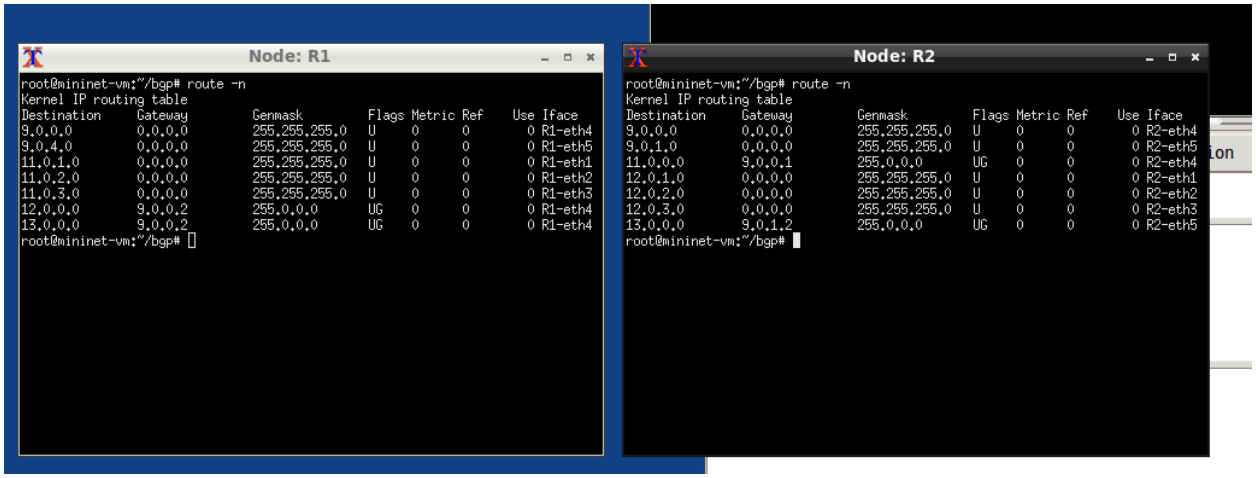
As Router R1 and Router R2 tables shown below:

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.

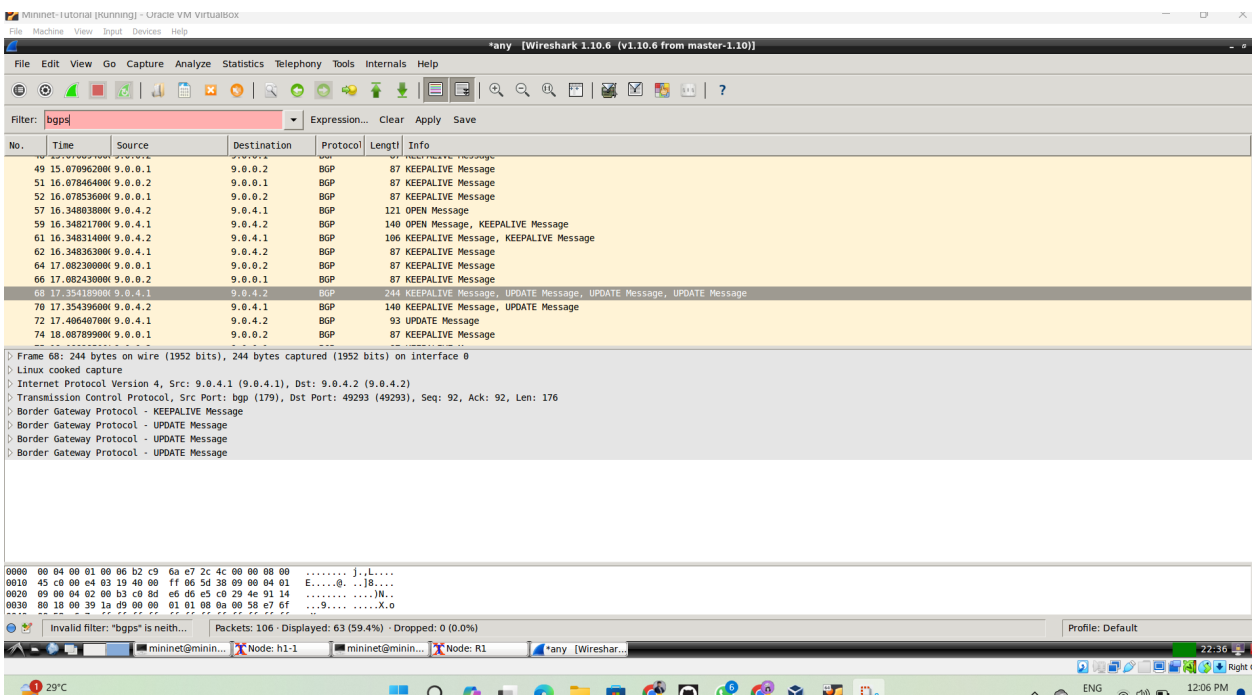

Node: R1
Escape character is '^]'.
Hello, this is Quagga (version 0.99.22.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.
User Access Verification
Password:
bgpd-R1>
bgpd-R1> sh ip bgp
BGP table version is 0, local router ID is 9.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, 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 0 2 i
*> 13.0.0.0 9.0.4.2 0 0 4 i
* 9.0.0.2 0 2 3 i
Total number of prefixes 3
bgpd-R1>
Destination
Protocol
Info
13.0.1.1
TCP
74 58946 > http [SYN] Sec

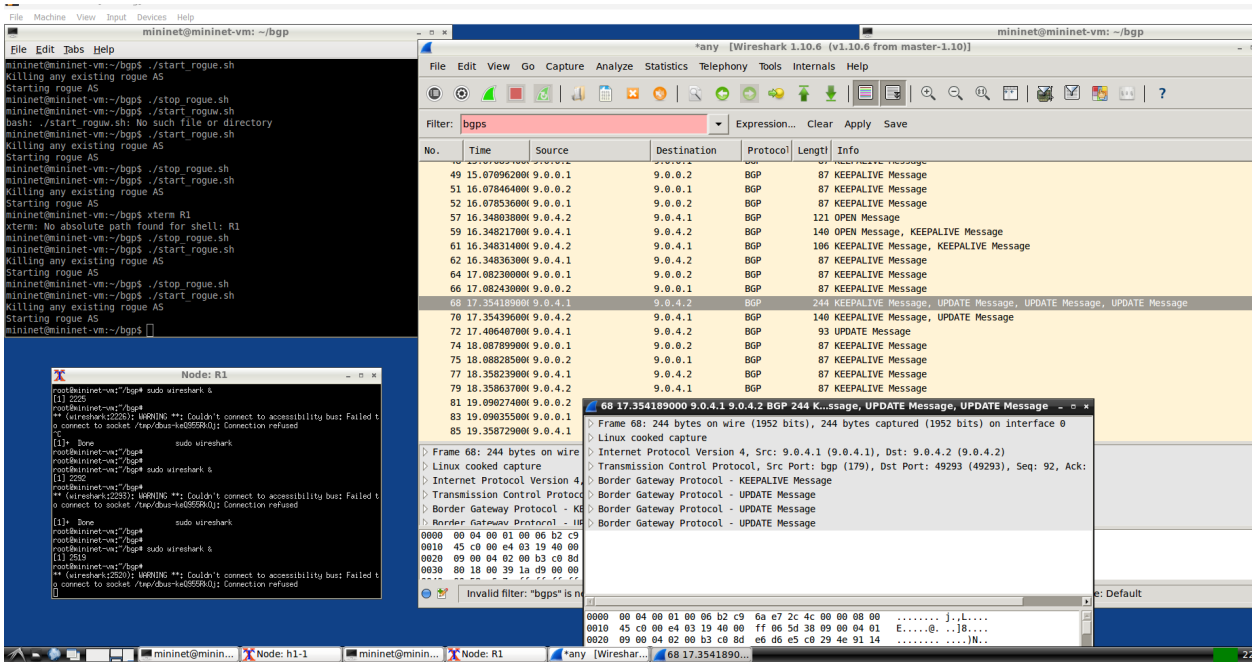

Node: R2
Escape character is '^]'.
Hello, this is Quagga (version 0.99.22.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.
User Access Verification
Password:
bgpd-R2>
bgpd-R2> sh ip bgp
BGP table version is 0, local router ID is 9.0.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, 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 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 0 3 i
Total number of prefixes 3
bgpd-R2>
eshark 1.10.6 (v1.10.6 from master-1.10)]
File Edit
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>



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 packetts 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

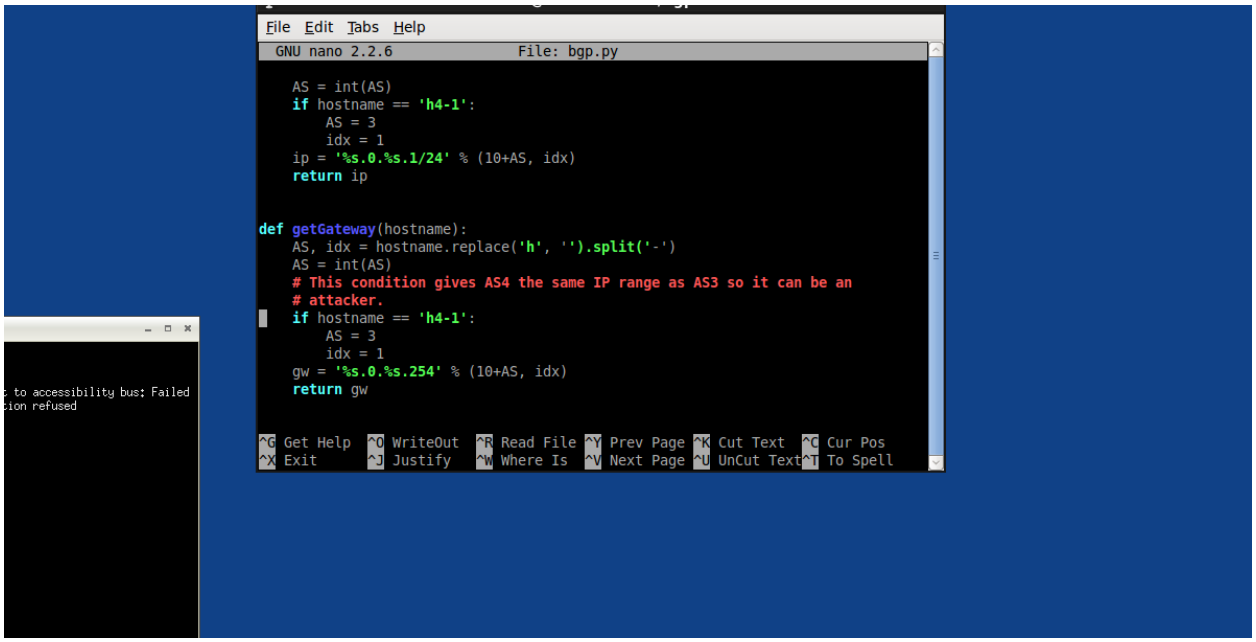
Bgp and forwarding tables are updated to include this advertise this addresses fro m router 4 , then r1 updates its path to choose its new path from newly updated tables. And every other router traffic is also redirected though this new path instead of following old.

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 :

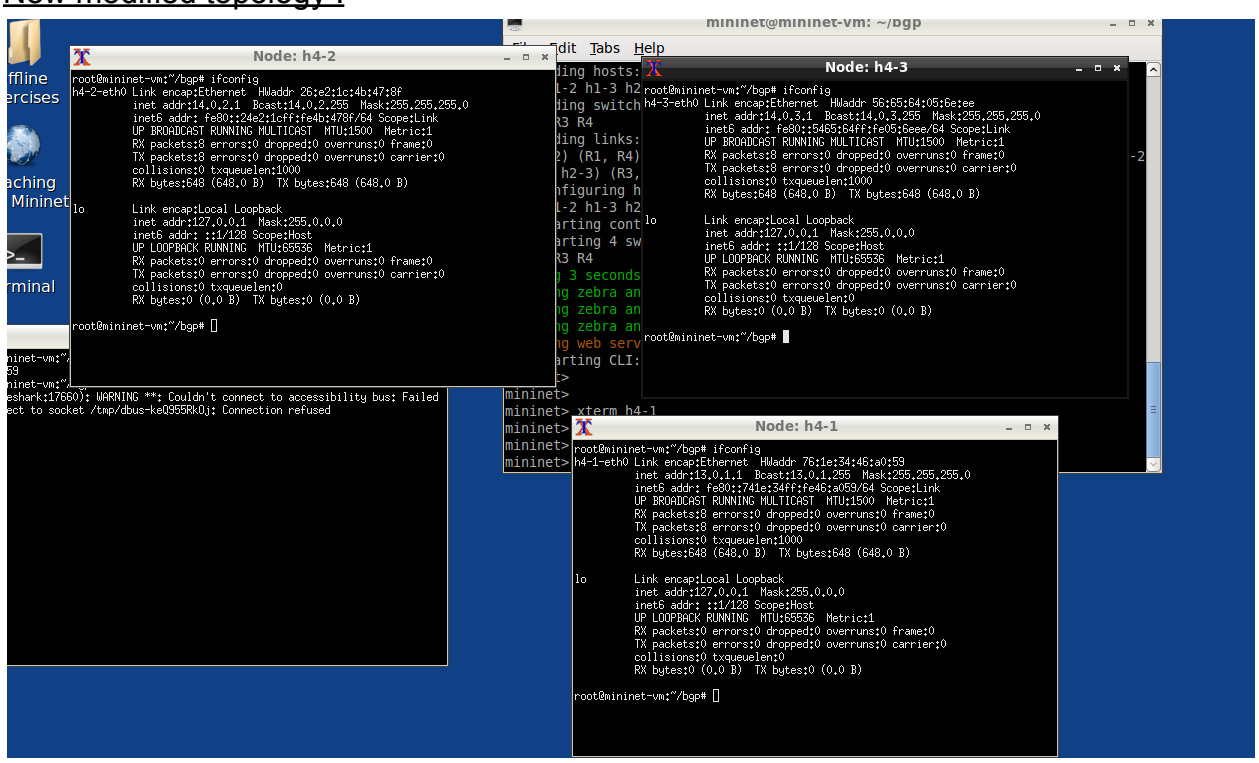
<u>Step 1 : modifying old bgp.py code to new bgp.py</u>



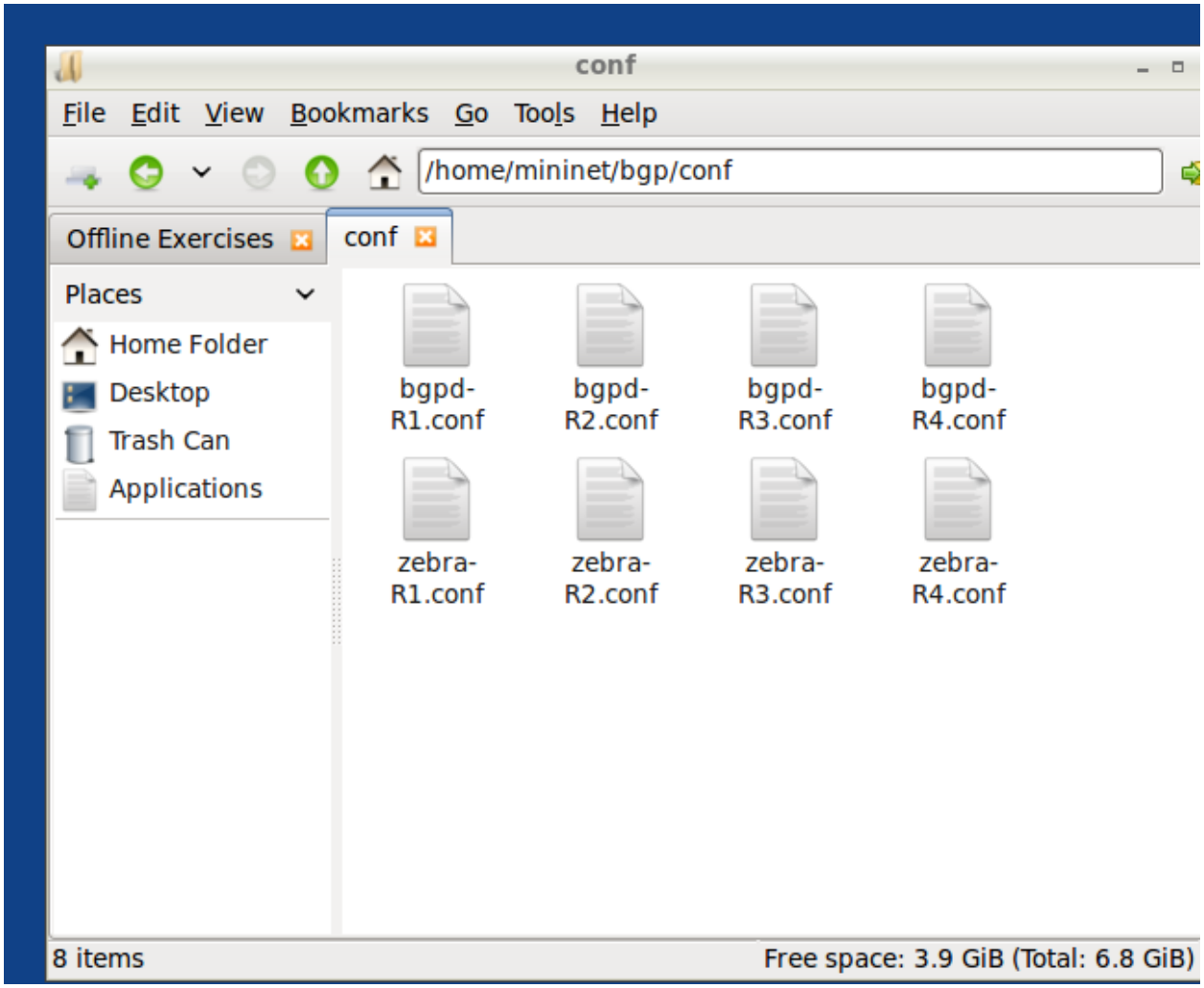
Here I am modifying and assigning the host 3 to host 4 ip addresses

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

New modified topology :



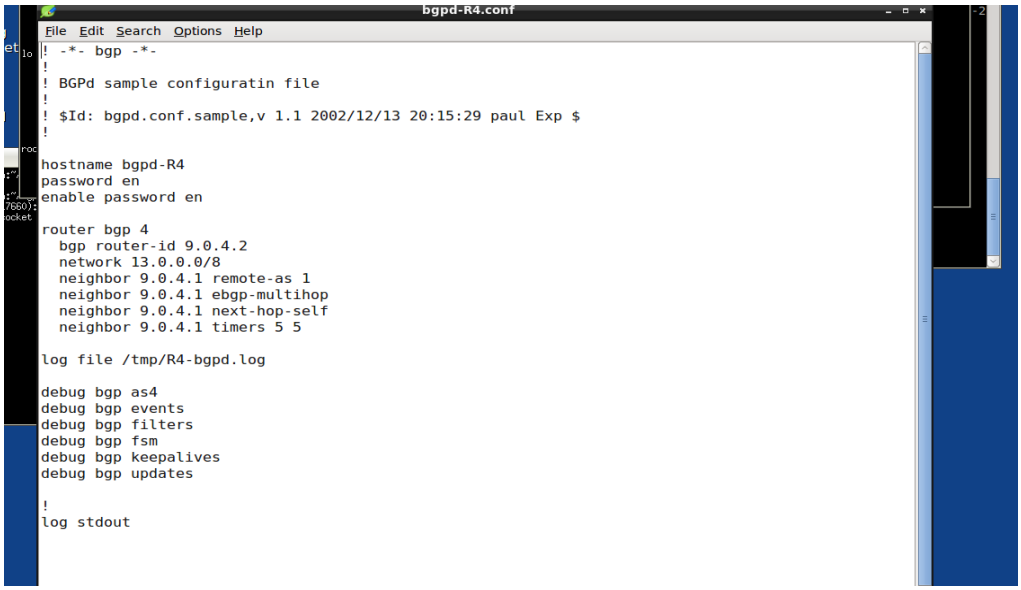
Step - 2: Changing Conf files for bgpd-4 and zebra-4



In router bgp 4

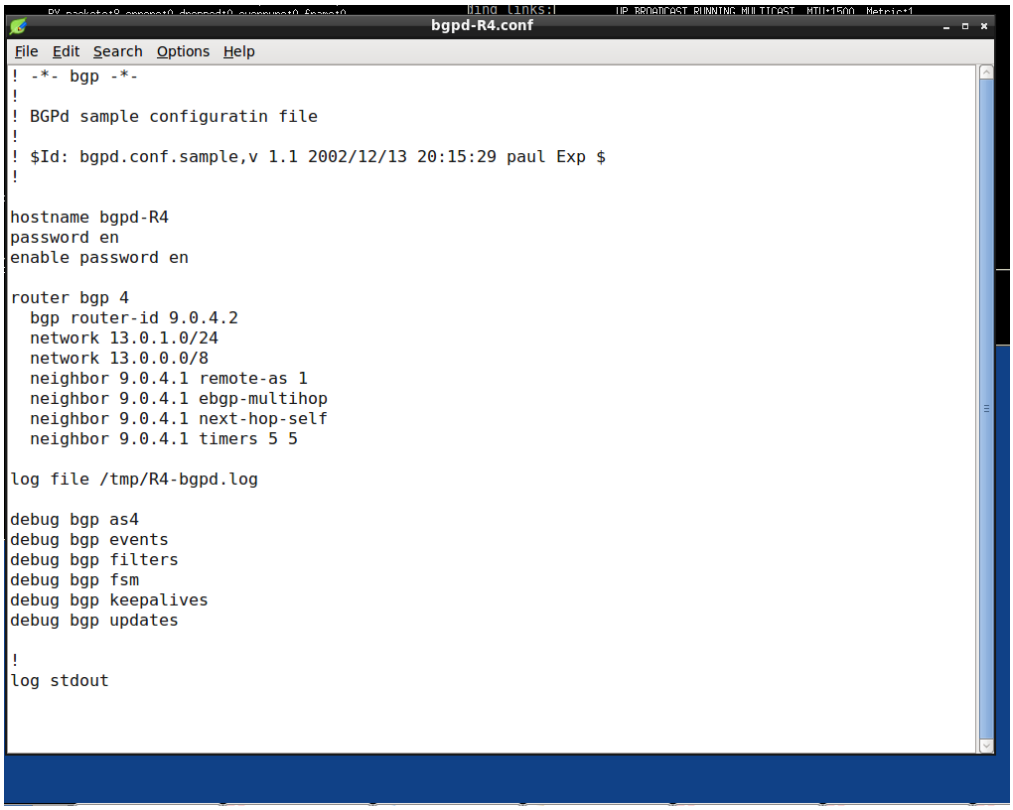
– Old bgpd -4.conf modified

Network 13.0.1.0/24 added & network



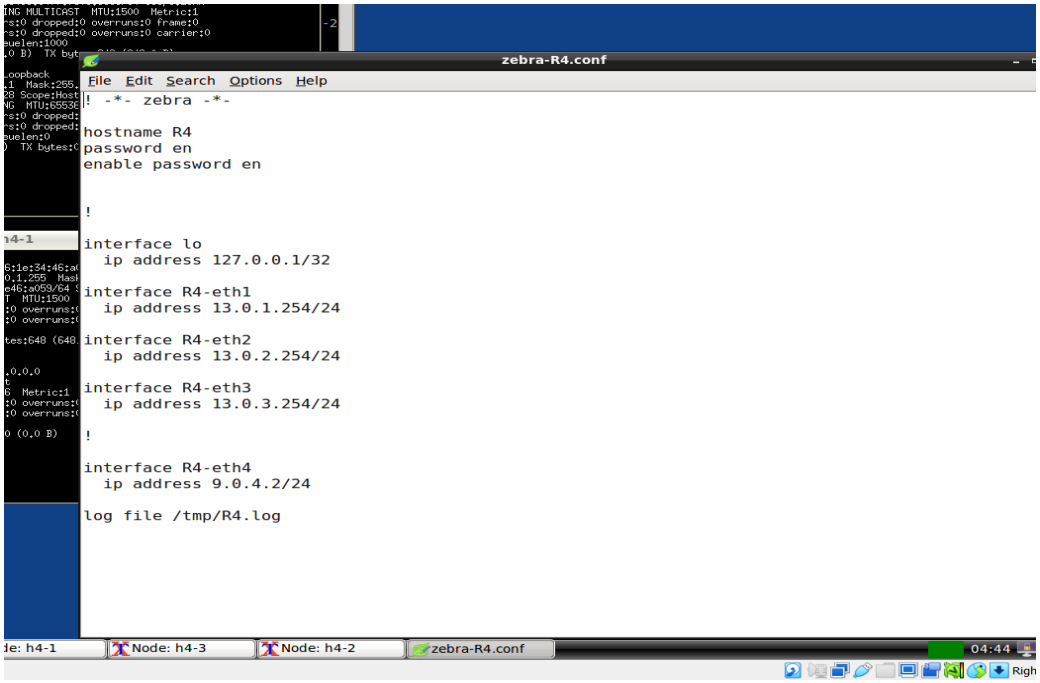
```
! -*- bgp -*-
!
! BGPd sample configuratin file
!
! $Id: bgpd.conf.sample,v 1.1 2002/12/13 20:15:29 paul Exp $
!

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 :

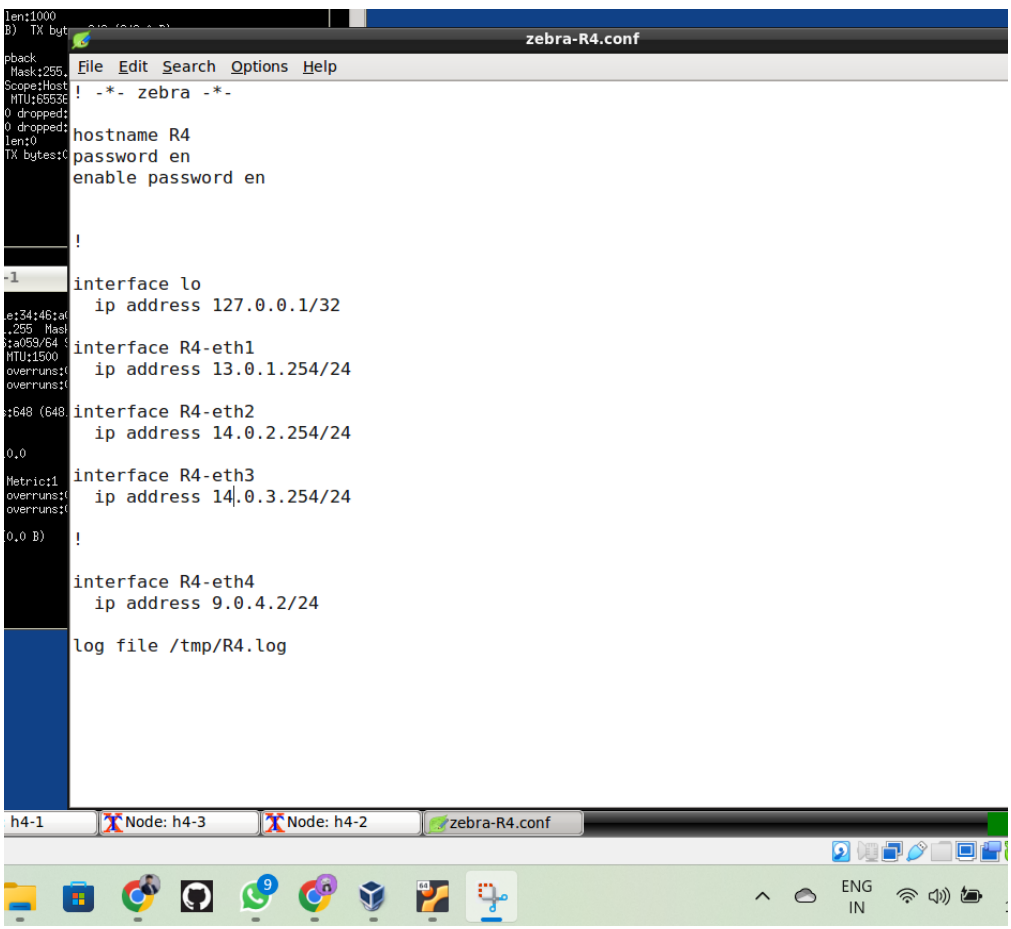


```
! -*- bgp -*-
!
! BGPd sample configuratin file
!
! $Id: bgpd.conf.sample,v 1.1 2002/12/13 20:15:29 paul Exp $
!

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



New zebra.conf file :



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

```
Node: R1
root@mininet-vm:~/bgp# sh ip bgp
sh: 0: Can't open ip
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
root@mininet-vm:~/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:158828 (158.8 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-vm:~/bgp#
[*h3-1-eth0  [W...   conf   Node: h4-1
```

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/