BGP Hijacking – Mininet Assignment

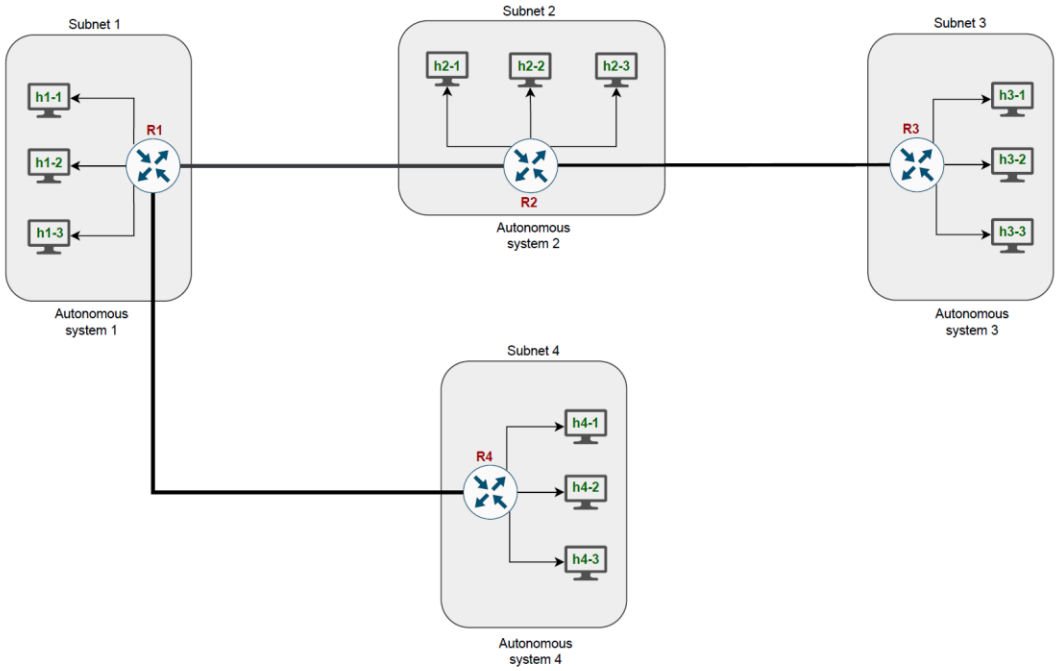
Group-6

Nelli Prithvi Raj
cs23mtech11012@iith.ac.in

Naveen Nayak
cs23mtech11011@iith.ac.in

Soumya Kumar
sm23mtech11010@iith.ac.in

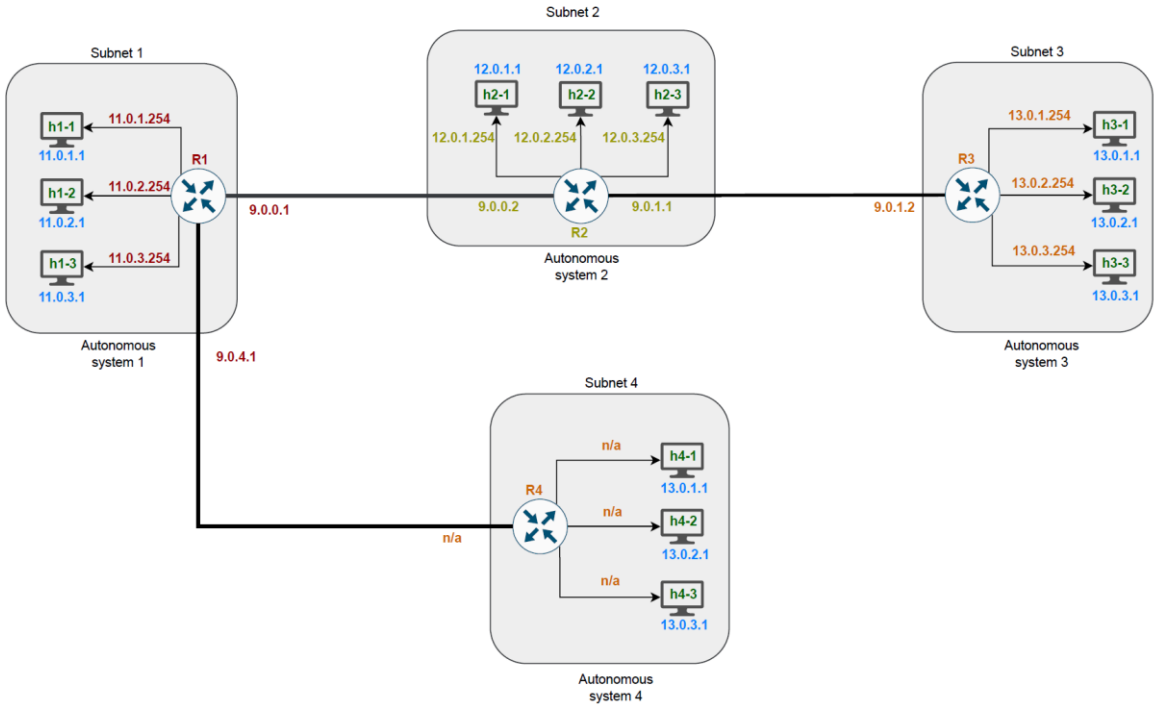
Q1) There are 12 hosts (h1-1,h1-2,h1-3,h2-1,h2-2,h2-3,h3-1,h3-2,h3-3,h4-1,h4-2,h4-3) and 4 Routers(R1,R2,R3,R4) . Among the 4 subnets, each subnet has 3 hosts.



Q2) The IP addresses for the 12 hosts, 4 routers and their interfaces are mentioned in below tables

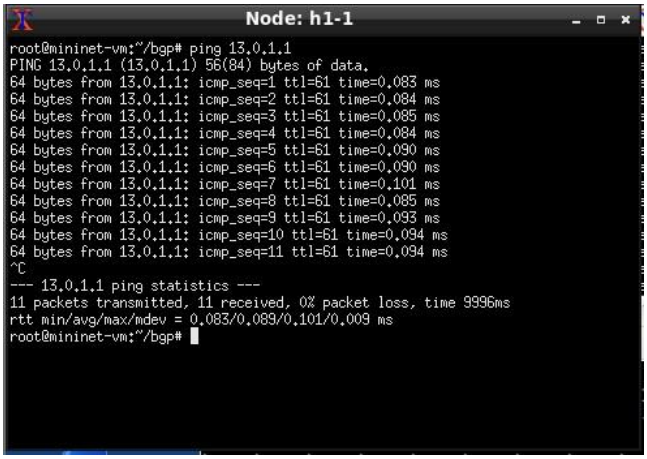
Host	interfaces	IPv4
h1-1	eth0	11.0.1.1
	lo	127.0.0.1
h1-2	eth0	11.0.2.1
	lo	127.0.0.1
h1-3	eth0	11.0.3.1
	lo	127.0.0.1
h2-1	eth0	12.0.1.1
	lo	127.0.0.1
h2-2	eth0	12.0.2.1
	lo	127.0.0.1
h2-3	eth0	12.0.3.1
	lo	127.0.0.1
h3-1	eth0	13.0.1.1
	lo	127.0.0.1
h3-2	eth0	13.0.2.1
	lo	127.0.0.1
h3-3	eth0	13.0.3.1
	lo	127.0.0.1
h4-1	eth0	13.0.1.1
	lo	127.0.0.1
h4-2	eth0	13.0.2.1
	lo	127.0.0.1
h4-3	eth0	13.0.3.1
	lo	127.0.0.1

Router	interface	IPv4
R1	eth1	11.0.1.254
	eth2	11.0.2.254
	eth3	11.0.3.254
	eth4	9.0.0.1
	eth5	9.0.4.1
	lo	127.0.0.1
R2	eth1	12.0.1.254
	eth2	12.0.2.254
	eth3	12.0.3.254
	eth4	9.0.0.2
	eth5	9.0.1.1
	lo	127.0.0.1
R3	eth1	13.0.1.254
	eth2	13.0.2.254
	eth3	13.0.3.254
	eth4	9.0.1.2
	lo	127.0.0.1
R4	eth1	n/a
	eth2	n/a
	eth3	n/a
	eth4	n/a

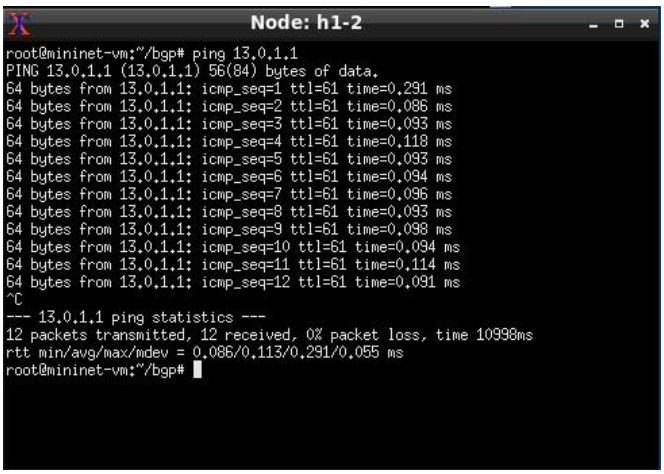


Q3) Checking the reachability through PING command to h3-1 host from h1-1,h1-2,h2-1 hosts

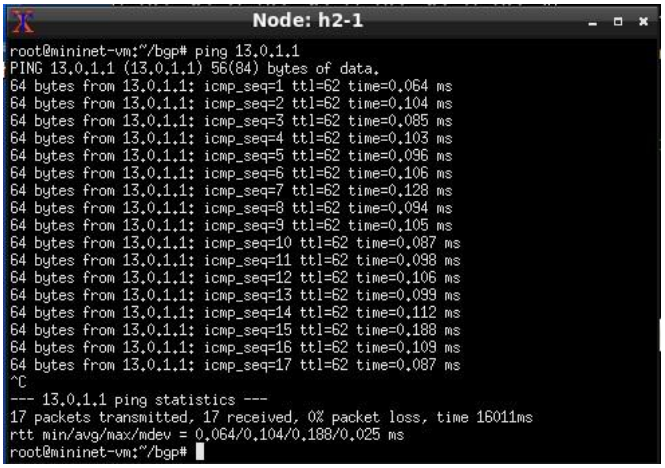
- From h1-1 to h3-1



- From h1-2 to h3-1



- From h2-1 to h3-1



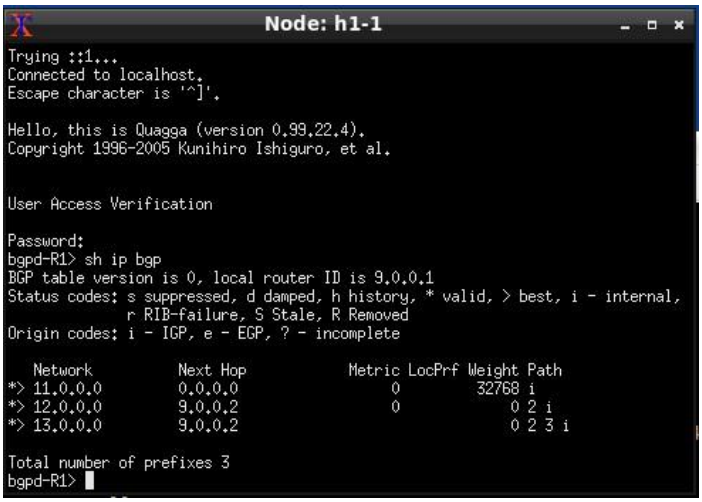
Q4) Router R1 BGP routing table is connected from h1-1 via telnet

Network: Network id's where R1 can accessible

Next Hop: The immediate neighbour that it should reach

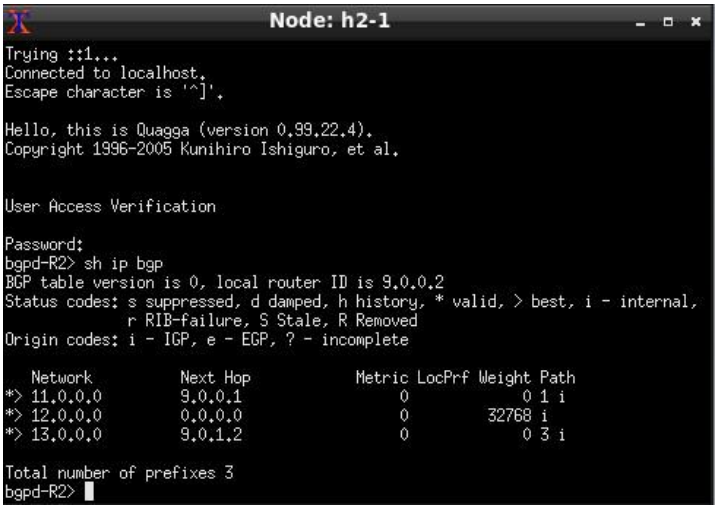
Weight: it gives the cost to that path

Path: Shows the path to reach the host



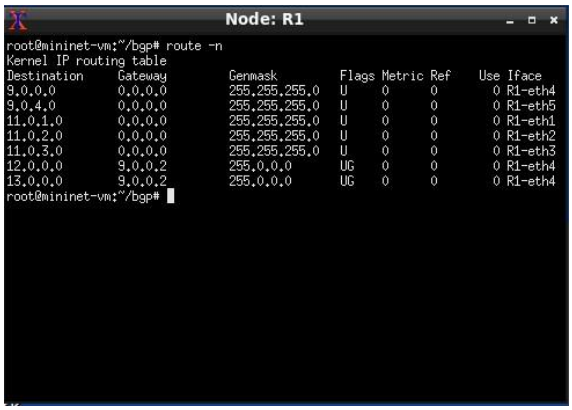
Q5) Router R2 BGP routing table is connected from h2-1 via telnet

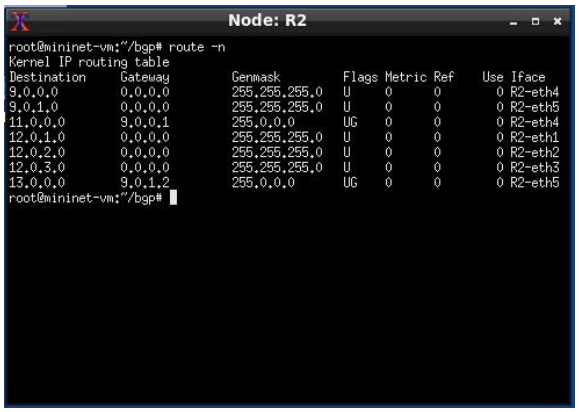
The entries are same as R1 but Routes are different



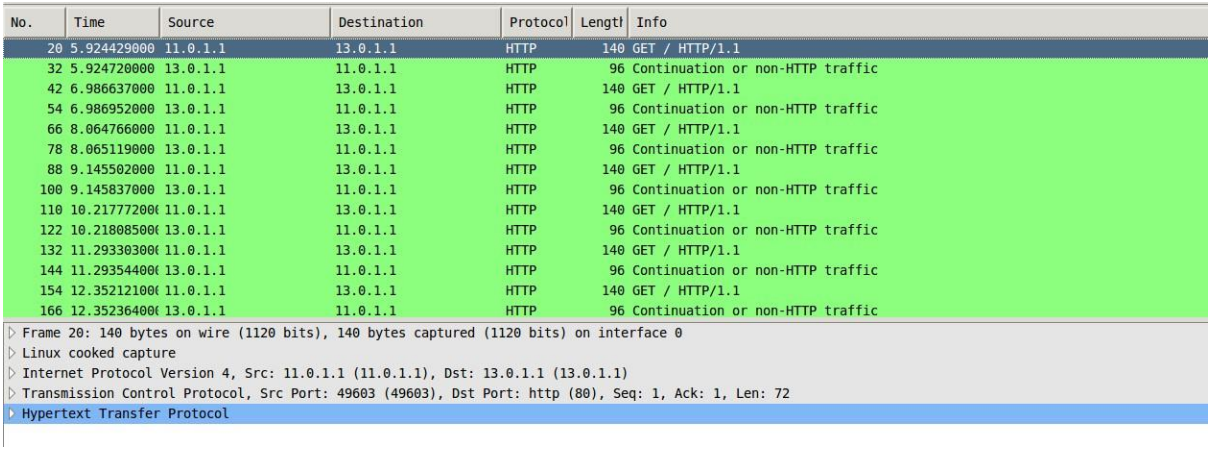
Q6) The BGP routing table consists of all AS paths and it contains all network id's.

The forwarding tables contains all ip's of its subnet and a packet will decide to go longest prefix match for the destination.

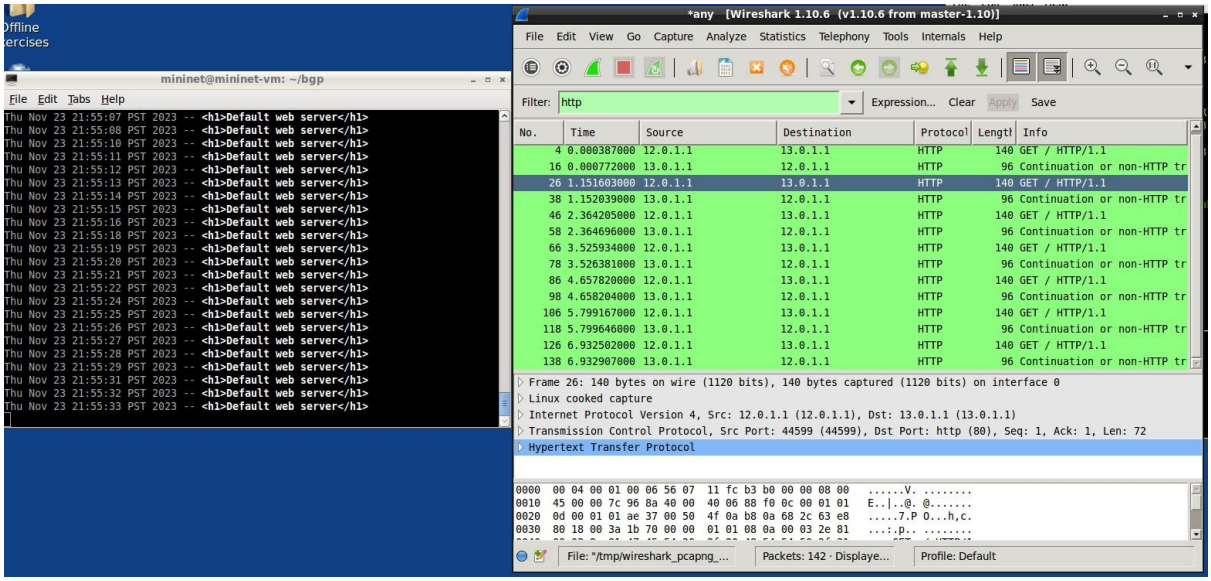




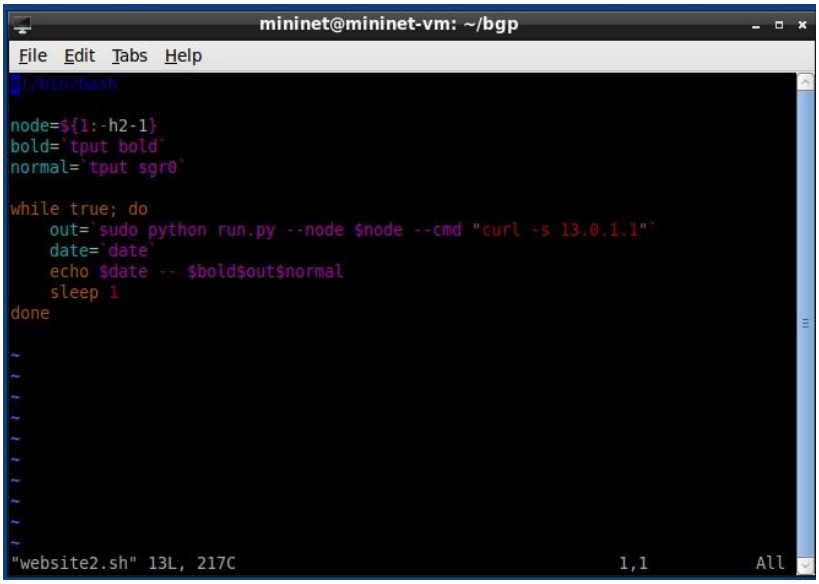
Q7) Capturing packets from h1-1 to h3-1 via wireshark



Q8) Get request from the h2-1 In wireshark

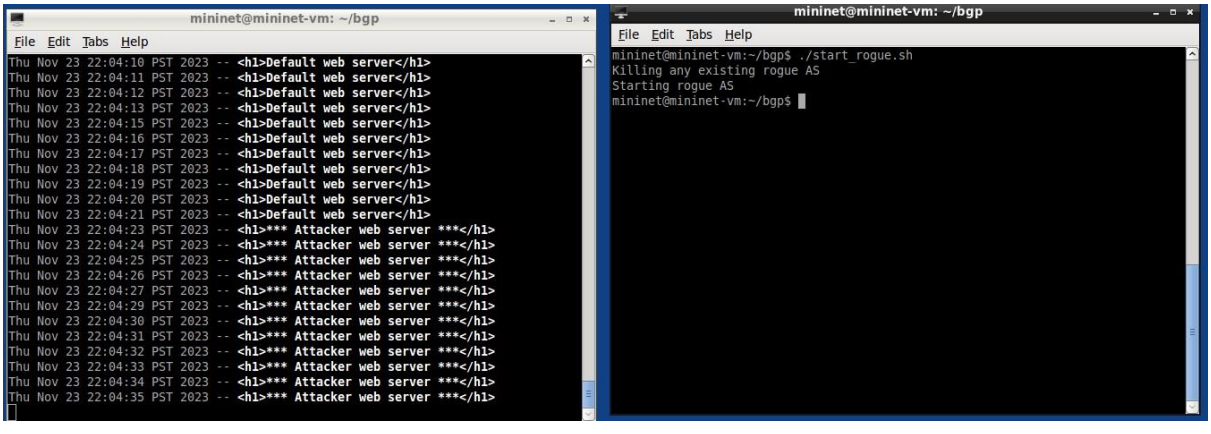


The code for website2.sh is given below

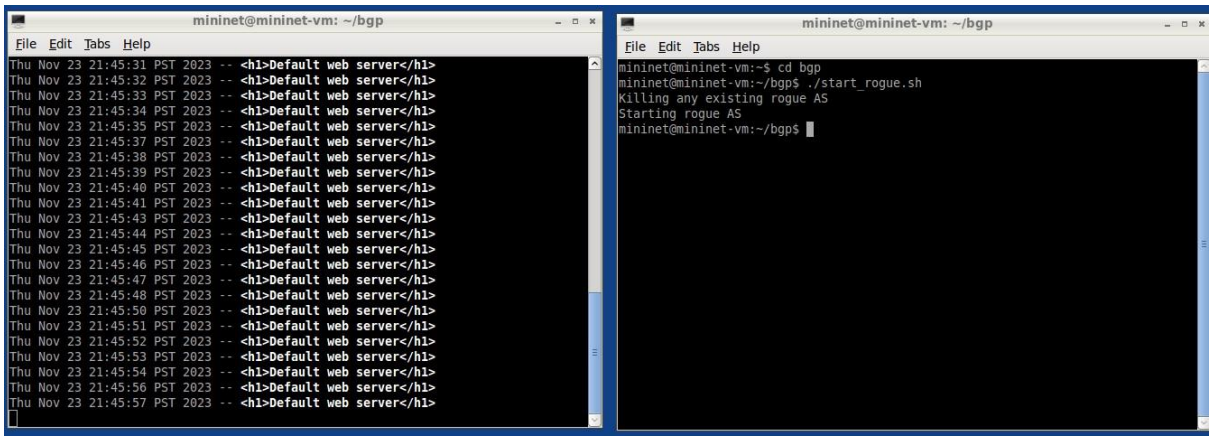


Q9) h4 bgp attack with start_rougue.sh script

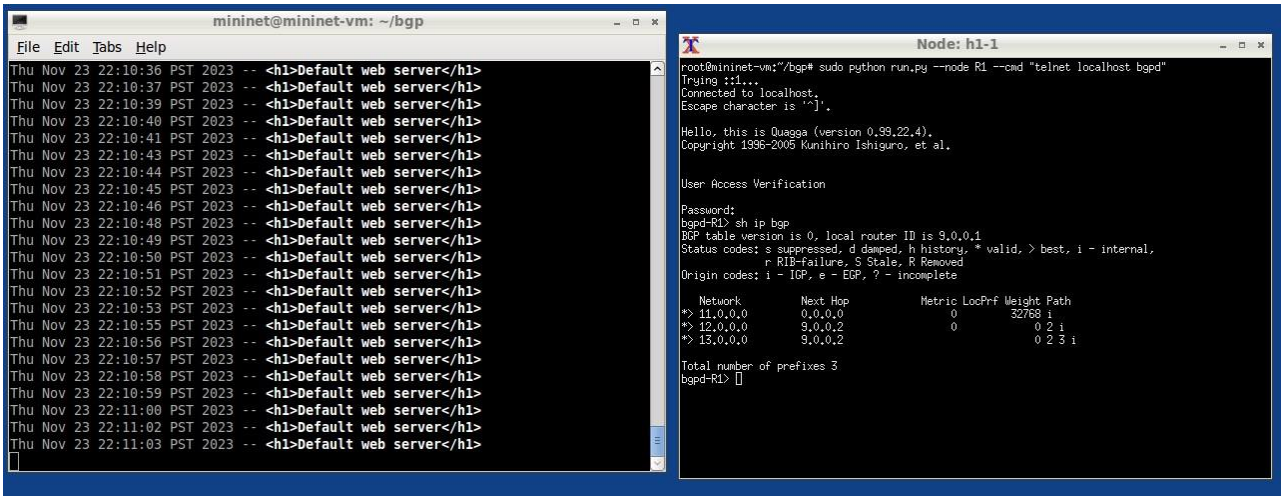
Now the packets are going from h3-1 to h4-1



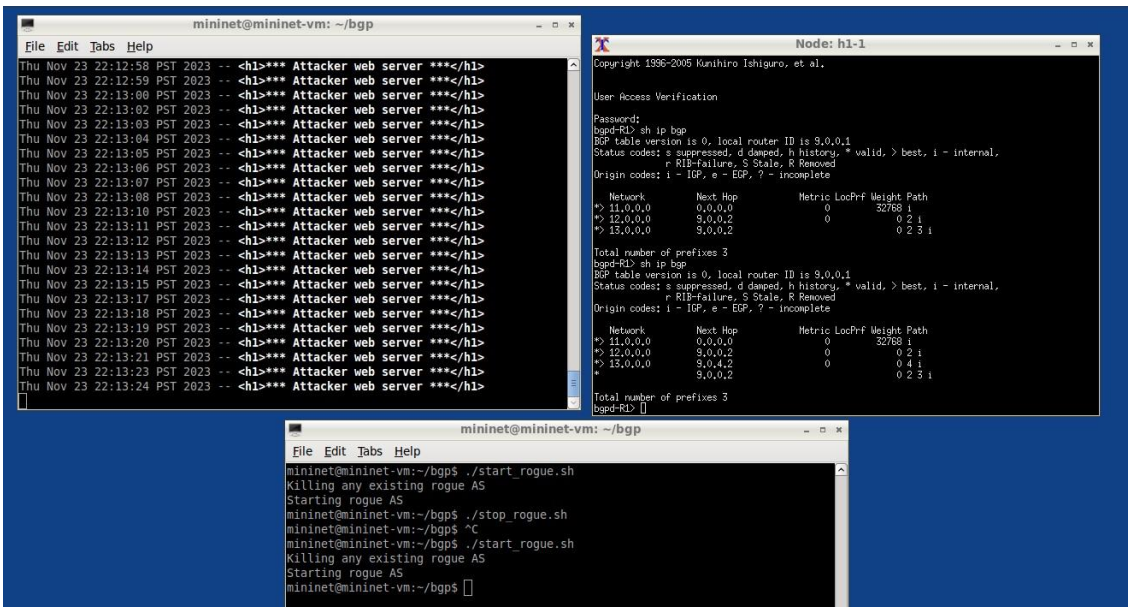
Q10) From h2-1 it is not changing from rouge because AS3 is the shortest path(1 hop) where as attacker(AS4) has 2 hops



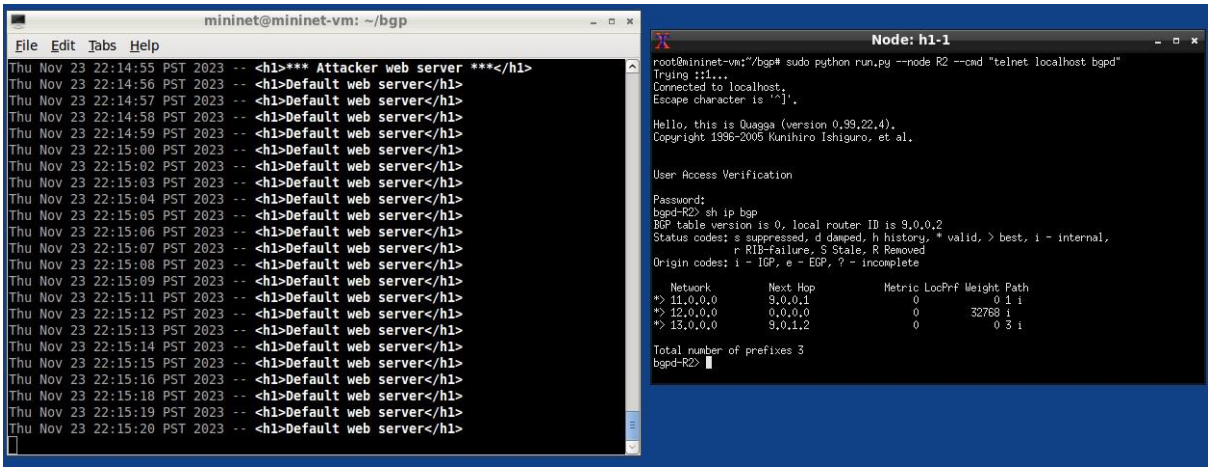
Q11) Before BGP attack, bgp table from R1



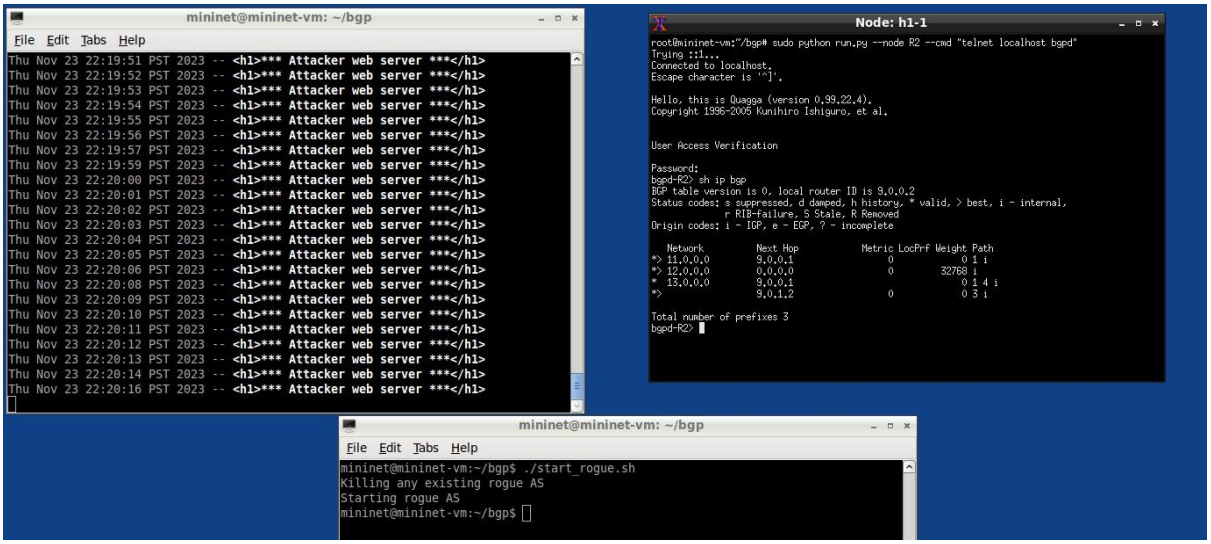
After BGP attack, bgp table from R1



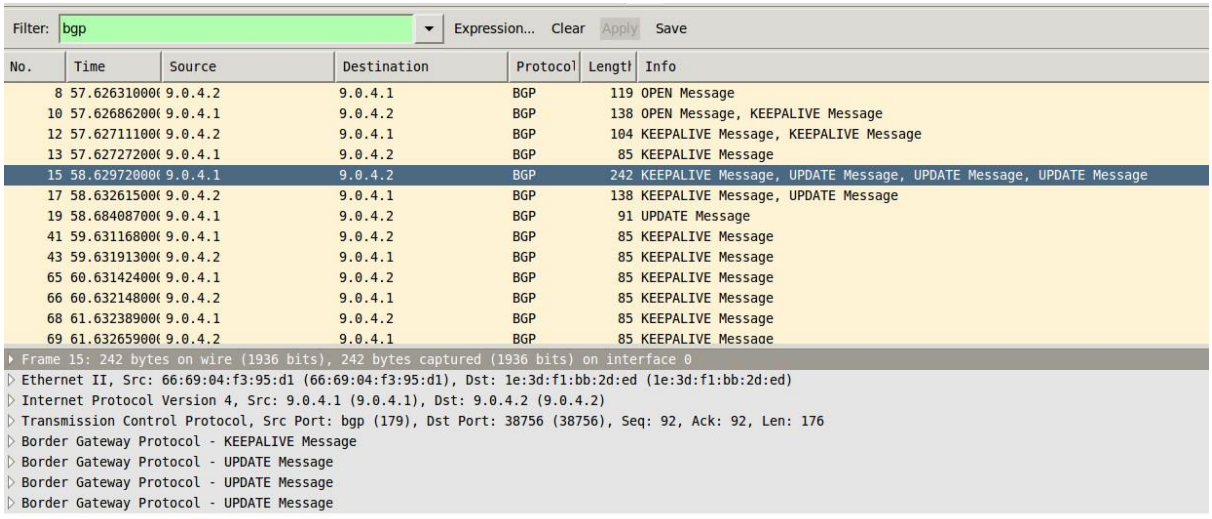
Before BGP attack, bgp table from R2

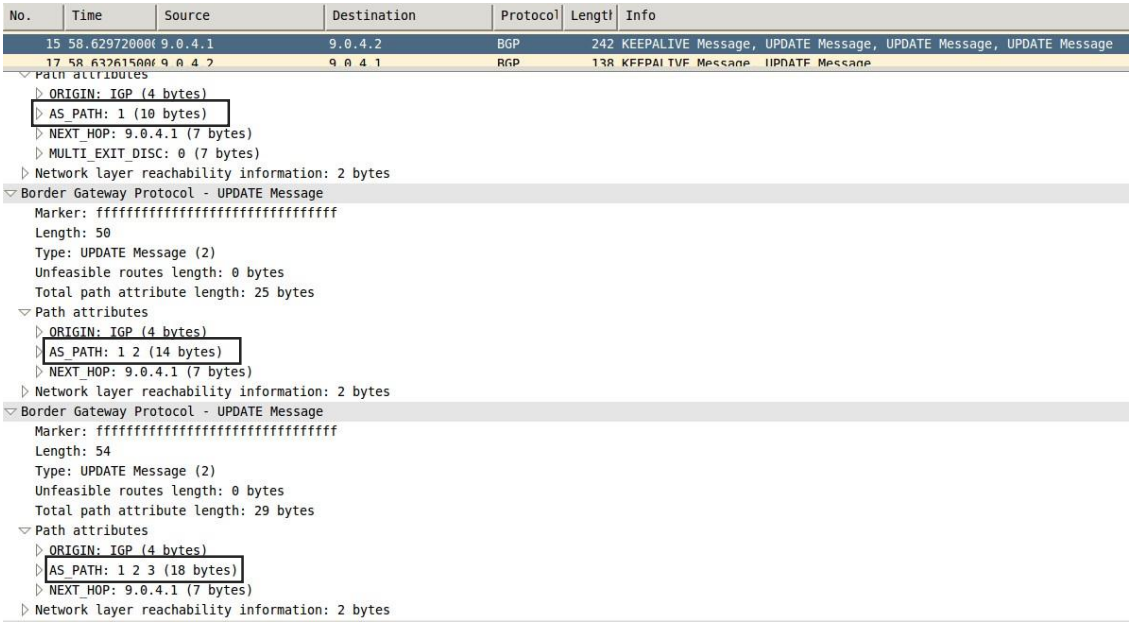


After BGP attack, bgp table from R2

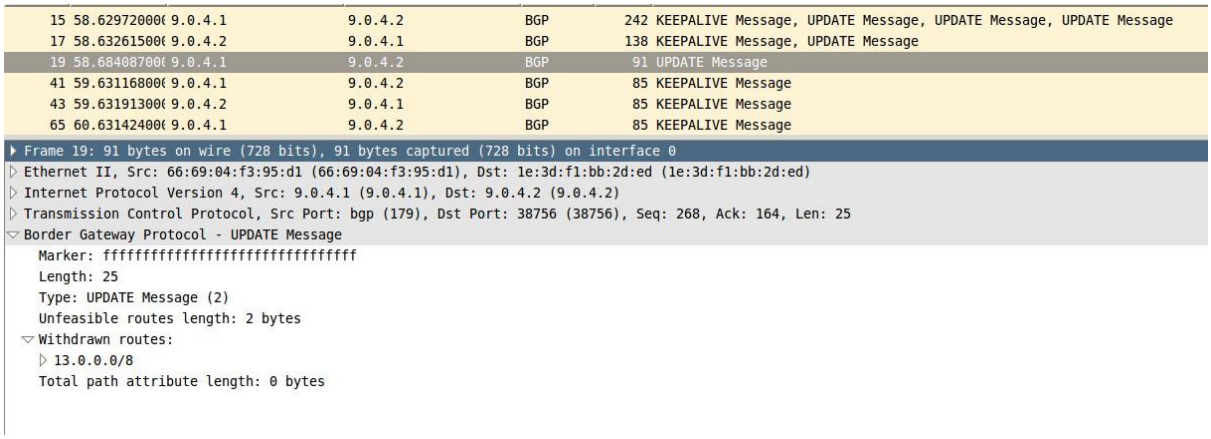


Q12) Started capturing packets in wireshark from R1





RS4 is sending the path of AS4 to R1 and AS4 trying to act as a AS3 , From R1 AS4 is the shortest path so the path has been changed from AS3 to As4

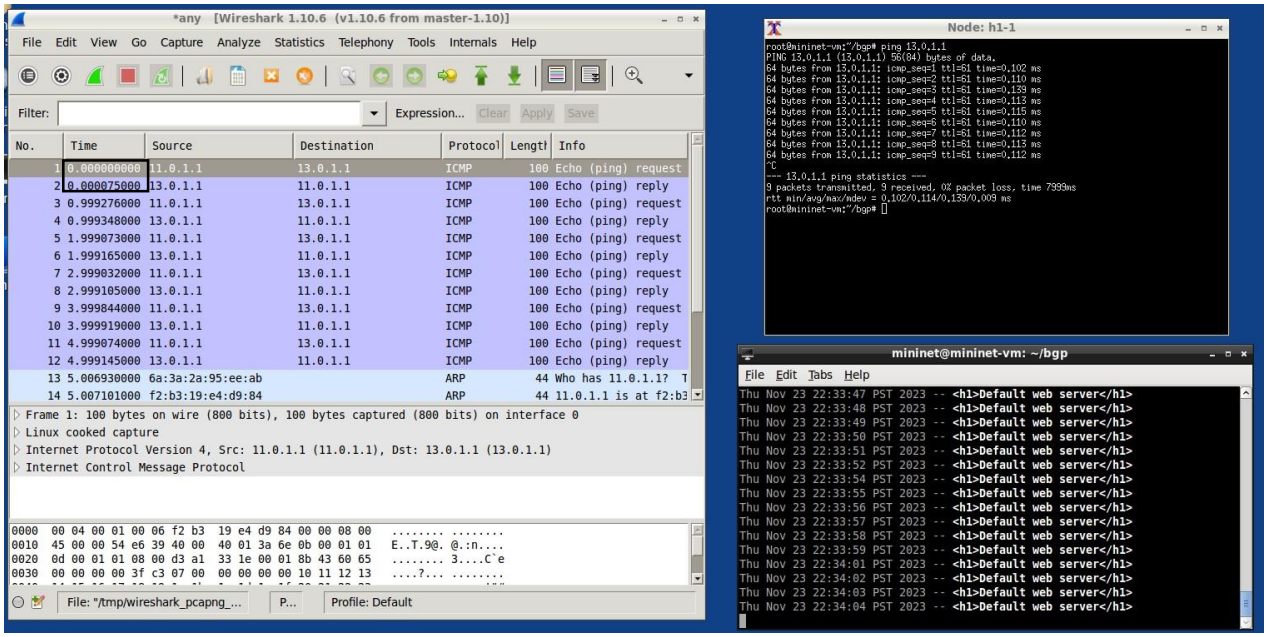


Q13) Normally AS3 is hosting a website and that website is accessing by AS1 via AS2, There a attacker's network AS4 it pretends as a AS3 and grab AS1 path to AS4 as it is the shortest path without any intermediate.

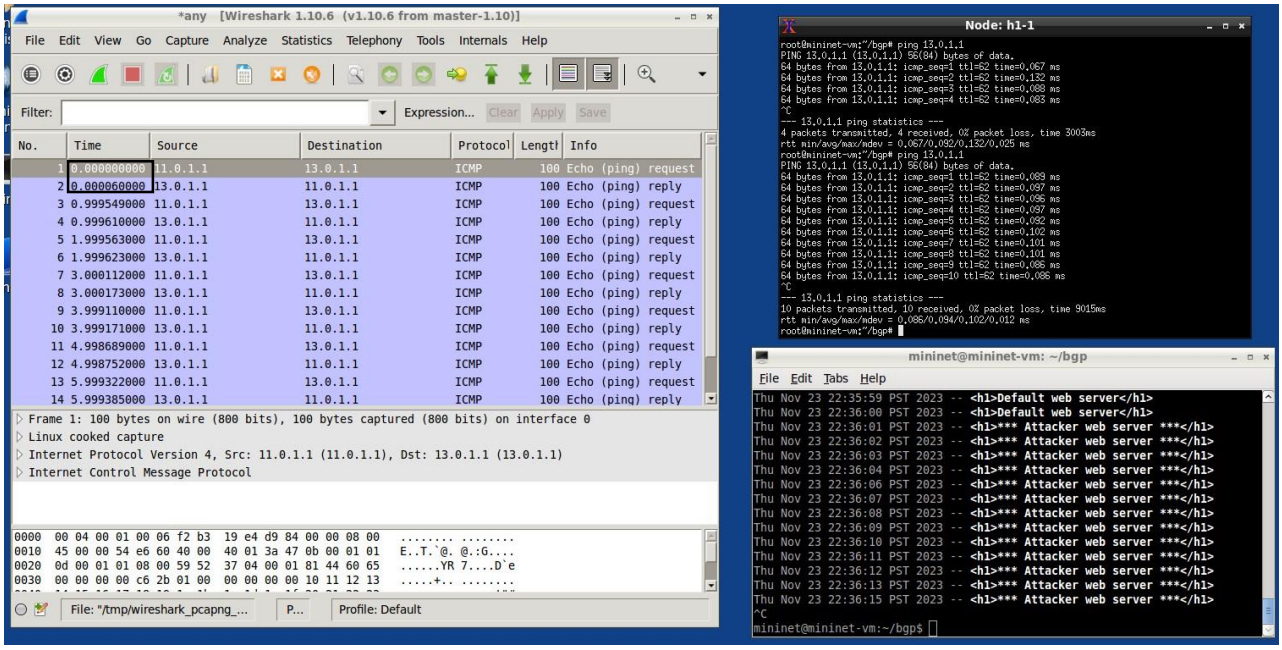
The Rogue in AS4 will start capturing packets by running "start_rogue.sh" program, path will be changed and to stop "stop_rogue.sh" should run.

The Rouge is successfully fooled AS1 but not AS2 hosts because of the path distance

Q14) Before BGP attack, In wireshark the RTT is 0.75ms



BGP attack, In wireshark the RTT is 0.60ms

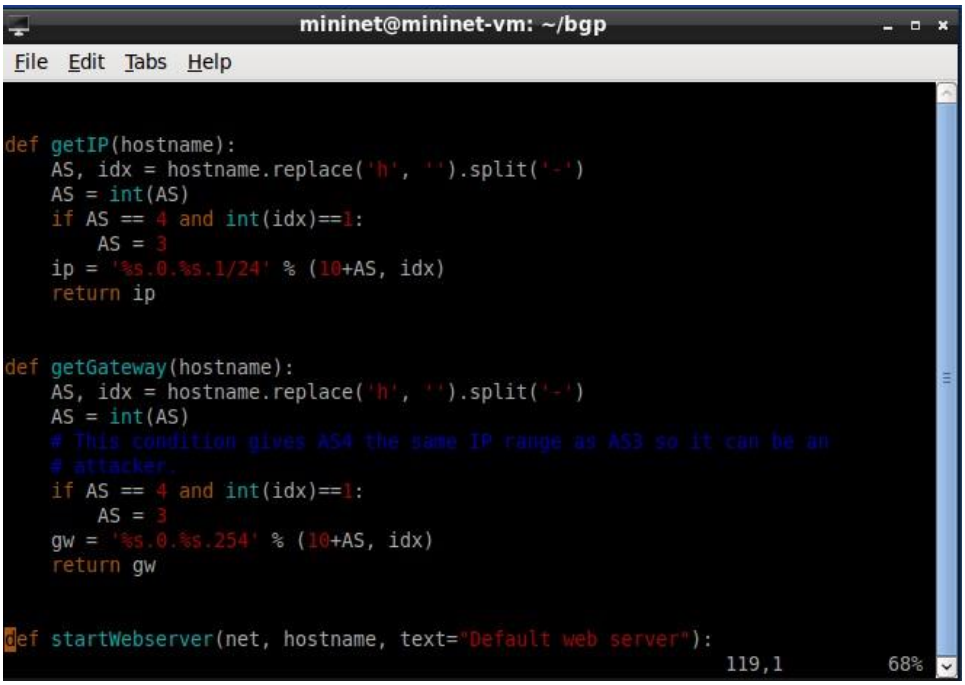


Q15) Original code for bgp.py

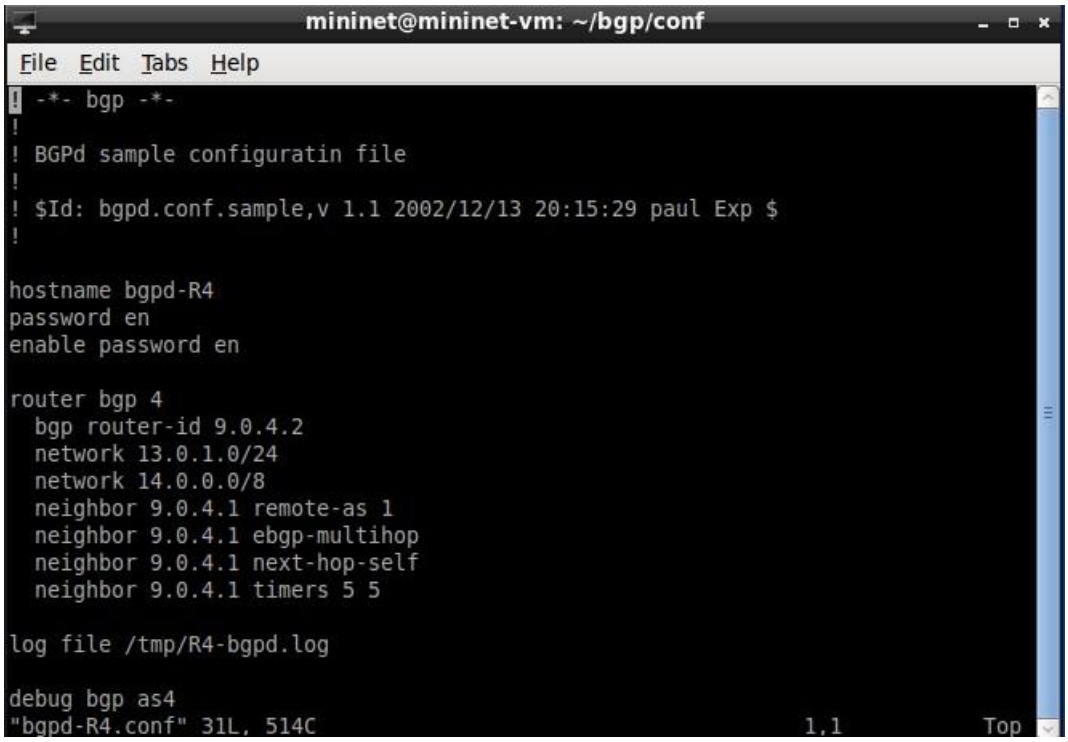
```
def getIP(hostname):
    AS, idx = hostname.replace('h', '').split('-')
    AS = int(AS)
    if AS == 4:
        AS = 3
    ip = '%s.0.%s.1/24' % (10+AS, idx)
    return ip


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


def startWebserver(net, hostname, text="Default web server"):
    host = net.getNodeByName(hostname)
    return host.popen("python webserver.py --text '%s'" % text, shell=True)
```

The attacker's network h4 wants to attack h3-1 only From AS3. So we need to have same IP address of the h4-1 and h3-1

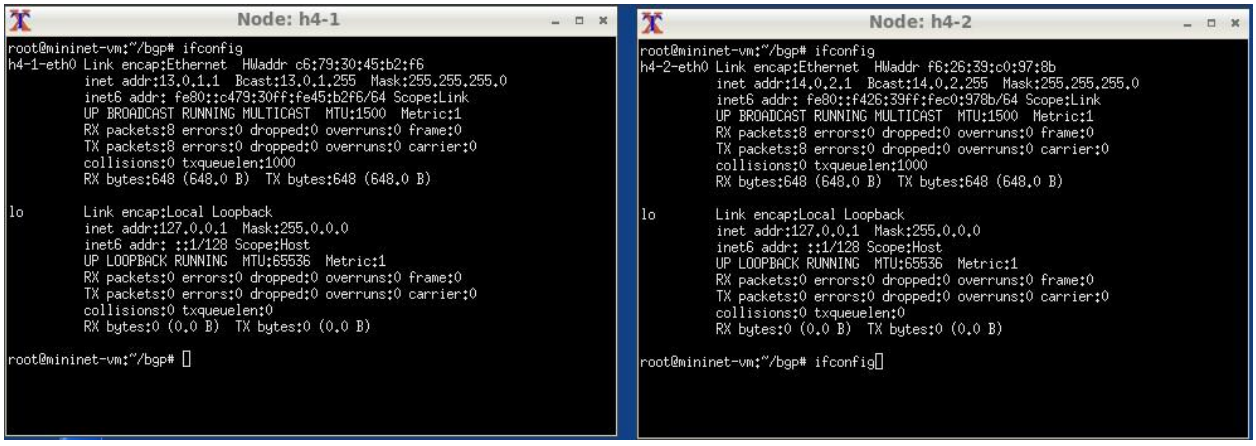
Modified Code for the bgp.py



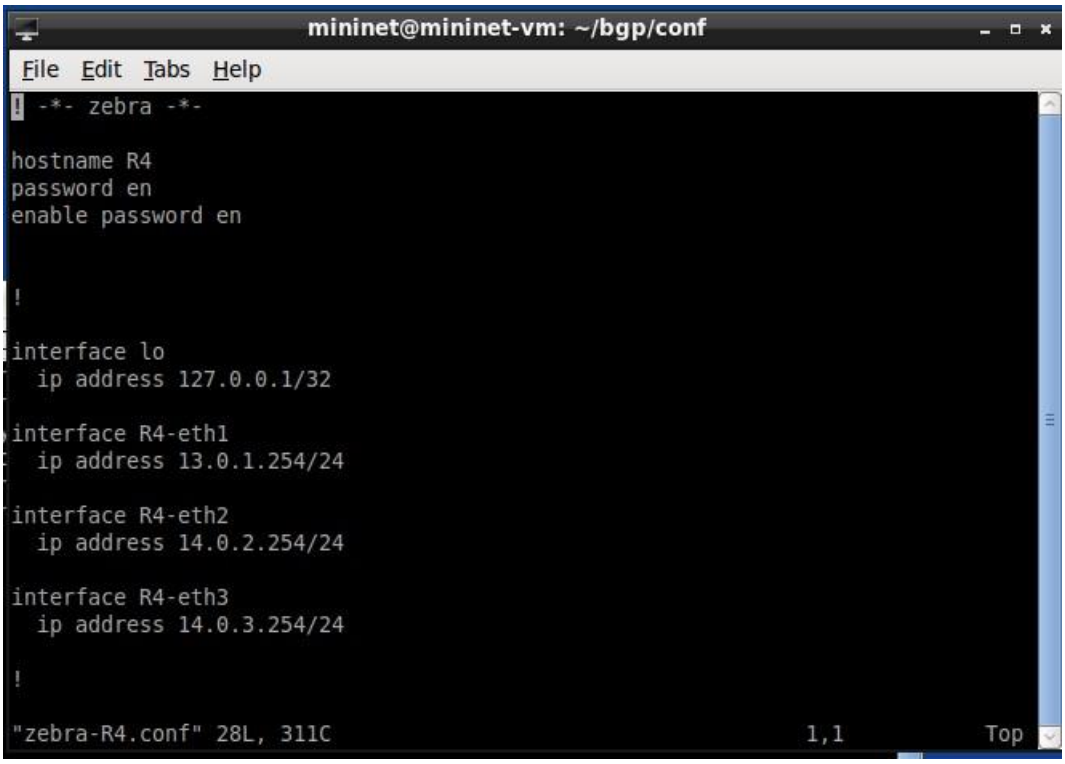
The modification inside bgp config file, we added 13.0.1.0/24 for longest prefix matching so it will get the priority



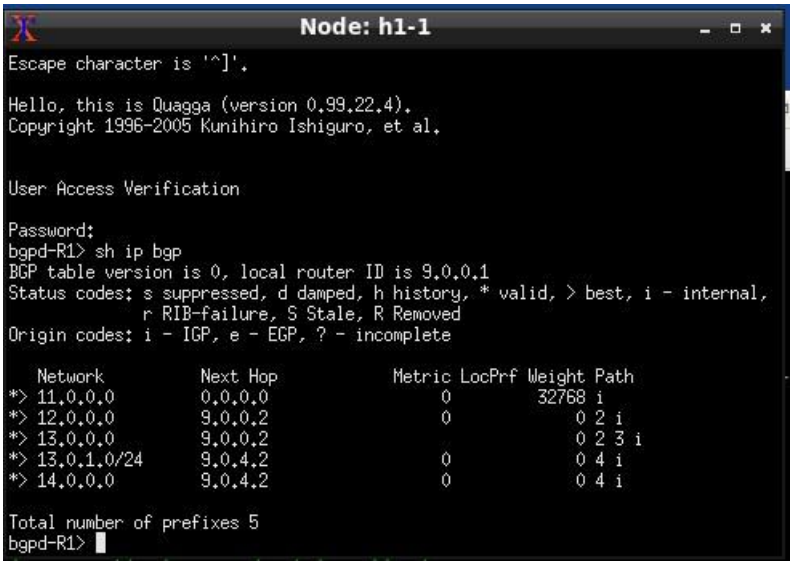
After changing those we can see the difference between h4-1 and h4-2



The modified Zebra configuration path



The new bgp path at R1 from h1-1



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.

Names <Roll Nos>: cs23mtech11012

Date: 03-12-2023

Signatures: Nelli Prithvi Raj

Names <Roll Nos>: cs23mtech11011

Date: 03-12-2023

Signatures: Naveen Nayak

Names <Roll Nos>: sm23mtech11010

Date: 03-12-2023

Signatures: saumya Kumar