

BGP Hijacking – Mininet Assignment

Group-6

Nelli Prithvi Raj

cs23mtech11012@iith.ac.in

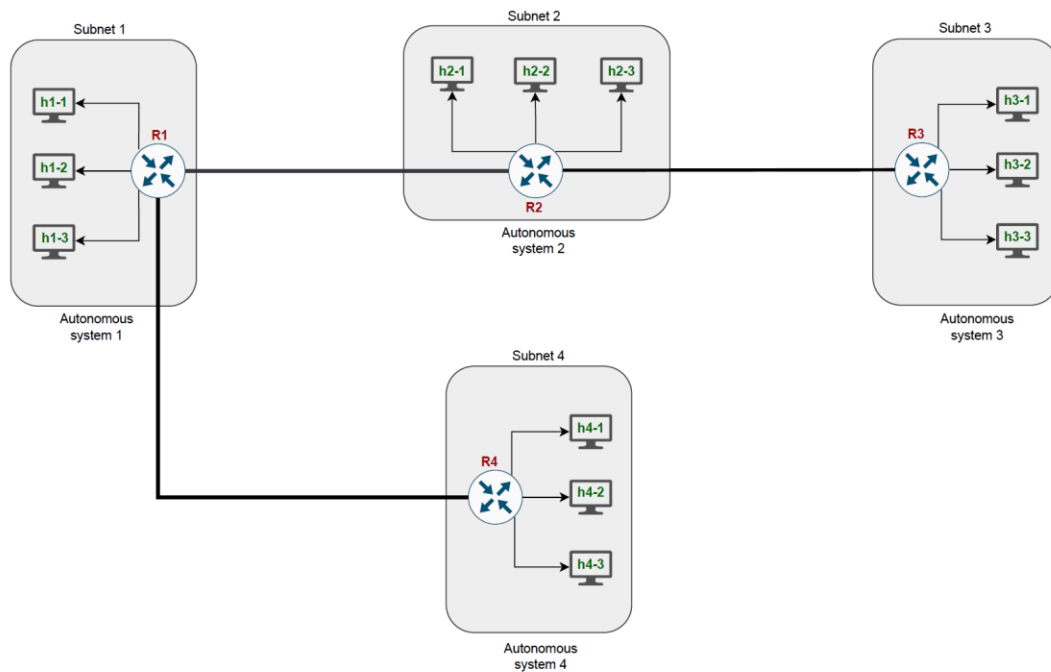
Naveen Nayak

cs23mtech11011@iith.ac.in

Soumya Kumar

sm23mtech11010@iith.ac.in

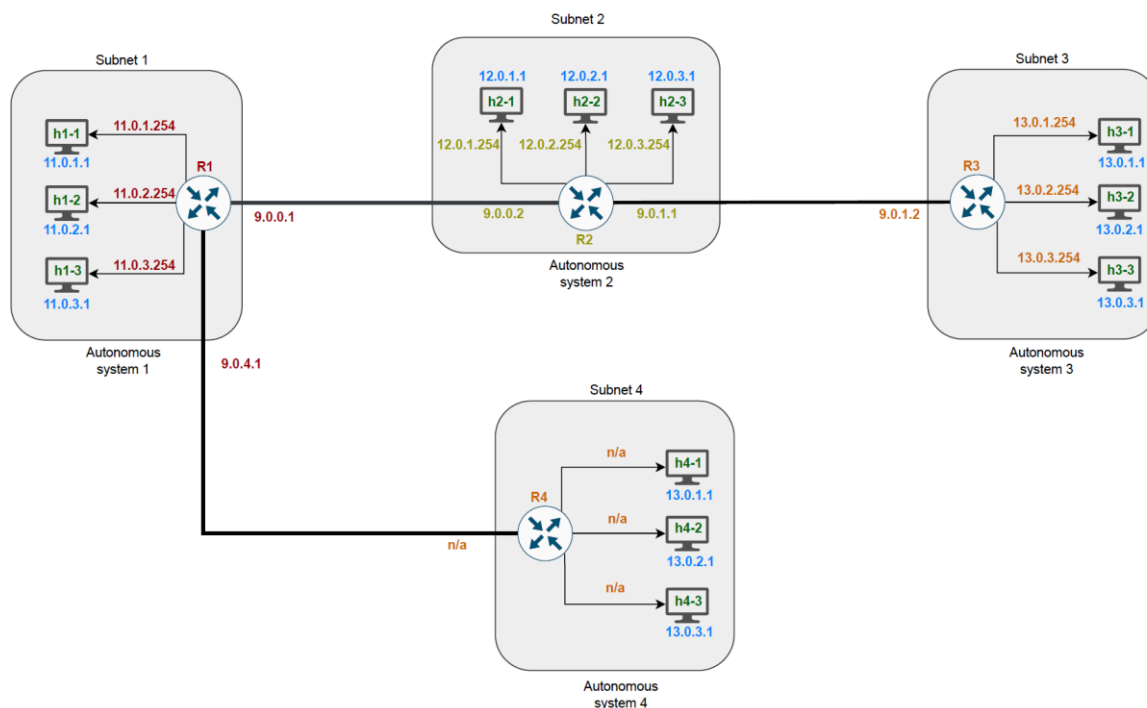
Q1) There are 12 hosts (h1-1,h1-2,h1-3,h2-1,h2-2,h2-3,h3-1,h3-2,h3-3,h4-1,h4-2,h4-3) and 4 Routers(R1,R2,R3,R4) . Among the 4 subnets, each subnet has 3 hosts.



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

```

Node: h1-1
root@mininet-vml:/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=61 time=0.083 ms
64 bytes from 13.0.1.1: icmp_seq=2 ttl=61 time=0.084 ms
64 bytes from 13.0.1.1: icmp_seq=3 ttl=61 time=0.085 ms
64 bytes from 13.0.1.1: icmp_seq=4 ttl=61 time=0.084 ms
64 bytes from 13.0.1.1: icmp_seq=5 ttl=61 time=0.090 ms
64 bytes from 13.0.1.1: icmp_seq=6 ttl=61 time=0.090 ms
64 bytes from 13.0.1.1: icmp_seq=7 ttl=61 time=0.101 ms
64 bytes from 13.0.1.1: icmp_seq=8 ttl=61 time=0.085 ms
64 bytes from 13.0.1.1: icmp_seq=9 ttl=61 time=0.093 ms
64 bytes from 13.0.1.1: icmp_seq=10 ttl=61 time=0.094 ms
64 bytes from 13.0.1.1: icmp_seq=11 ttl=61 time=0.094 ms
^C
--- 13.0.1.1 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 9996ms
rtt min/avg/max/mdev = 0.083/0.089/0.101/0.009 ms
root@mininet-vml:/bgp#

```

- From h1-2 to h3-1

```

Node: h1-2
root@mininet-vml:/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=61 time=0.291 ms
64 bytes from 13.0.1.1: icmp_seq=2 ttl=61 time=0.086 ms
64 bytes from 13.0.1.1: icmp_seq=3 ttl=61 time=0.093 ms
64 bytes from 13.0.1.1: icmp_seq=4 ttl=61 time=0.118 ms
64 bytes from 13.0.1.1: icmp_seq=5 ttl=61 time=0.093 ms
64 bytes from 13.0.1.1: icmp_seq=6 ttl=61 time=0.094 ms
64 bytes from 13.0.1.1: icmp_seq=7 ttl=61 time=0.096 ms
64 bytes from 13.0.1.1: icmp_seq=8 ttl=61 time=0.093 ms
64 bytes from 13.0.1.1: icmp_seq=9 ttl=61 time=0.098 ms
64 bytes from 13.0.1.1: icmp_seq=10 ttl=61 time=0.094 ms
64 bytes from 13.0.1.1: icmp_seq=11 ttl=61 time=0.114 ms
64 bytes from 13.0.1.1: icmp_seq=12 ttl=61 time=0.091 ms
^C
--- 13.0.1.1 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 10998ms
rtt min/avg/max/mdev = 0.086/0.113/0.291/0.055 ms
root@mininet-vml:/bgp#

```

- From h2-1 to h3-1

```

Node: h2-1
root@mininet-vml:/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=0.064 ms
64 bytes from 13.0.1.1: icmp_seq=2 ttl=62 time=0.104 ms
64 bytes from 13.0.1.1: icmp_seq=3 ttl=62 time=0.085 ms
64 bytes from 13.0.1.1: icmp_seq=4 ttl=62 time=0.103 ms
64 bytes from 13.0.1.1: icmp_seq=5 ttl=62 time=0.096 ms
64 bytes from 13.0.1.1: icmp_seq=6 ttl=62 time=0.106 ms
64 bytes from 13.0.1.1: icmp_seq=7 ttl=62 time=0.128 ms
64 bytes from 13.0.1.1: icmp_seq=8 ttl=62 time=0.094 ms
64 bytes from 13.0.1.1: icmp_seq=9 ttl=62 time=0.105 ms
64 bytes from 13.0.1.1: icmp_seq=10 ttl=62 time=0.087 ms
64 bytes from 13.0.1.1: icmp_seq=11 ttl=62 time=0.098 ms
64 bytes from 13.0.1.1: icmp_seq=12 ttl=62 time=0.106 ms
64 bytes from 13.0.1.1: icmp_seq=13 ttl=62 time=0.099 ms
64 bytes from 13.0.1.1: icmp_seq=14 ttl=62 time=0.112 ms
64 bytes from 13.0.1.1: icmp_seq=15 ttl=62 time=0.188 ms
64 bytes from 13.0.1.1: icmp_seq=16 ttl=62 time=0.109 ms
64 bytes from 13.0.1.1: icmp_seq=17 ttl=62 time=0.087 ms
^C
--- 13.0.1.1 ping statistics ---
17 packets transmitted, 17 received, 0% packet loss, time 1601ms
rtt min/avg/max/mdev = 0.064/0.104/0.188/0.025 ms
root@mininet-vml:/bgp#

```

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

```

Node: h1-1
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> 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>

```

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

The entries are same as R1 but Routes are different

```
Node: h2-1
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> 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>
```

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.

```
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 9.0.0.2 255.0.0.0 UG 0 0 0 R1-eth4
root@mininet-vm:~/bgp#
```

```
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#
```

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

No.	Time	Source	Destination	Protocol	Length	Info
20	5.924429000	11.0.1.1	13.0.1.1	HTTP	140	GET / HTTP/1.1
32	5.924720000	13.0.1.1	11.0.1.1	HTTP	96	Continuation or non-HTTP traffic
42	6.986637000	11.0.1.1	13.0.1.1	HTTP	140	GET / HTTP/1.1
54	6.986952000	13.0.1.1	11.0.1.1	HTTP	96	Continuation or non-HTTP traffic
66	8.064766000	11.0.1.1	13.0.1.1	HTTP	140	GET / HTTP/1.1
78	8.065119000	13.0.1.1	11.0.1.1	HTTP	96	Continuation or non-HTTP traffic
88	9.145502000	11.0.1.1	13.0.1.1	HTTP	140	GET / HTTP/1.1
100	9.145837000	13.0.1.1	11.0.1.1	HTTP	96	Continuation or non-HTTP traffic
110	10.217772000	11.0.1.1	13.0.1.1	HTTP	140	GET / HTTP/1.1
122	10.218085000	13.0.1.1	11.0.1.1	HTTP	96	Continuation or non-HTTP traffic
132	11.293303000	11.0.1.1	13.0.1.1	HTTP	140	GET / HTTP/1.1
144	11.293544000	13.0.1.1	11.0.1.1	HTTP	96	Continuation or non-HTTP traffic
154	12.352121000	11.0.1.1	13.0.1.1	HTTP	140	GET / HTTP/1.1
166	12.352364000	13.0.1.1	11.0.1.1	HTTP	96	Continuation or non-HTTP traffic

▶ Frame 20: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0

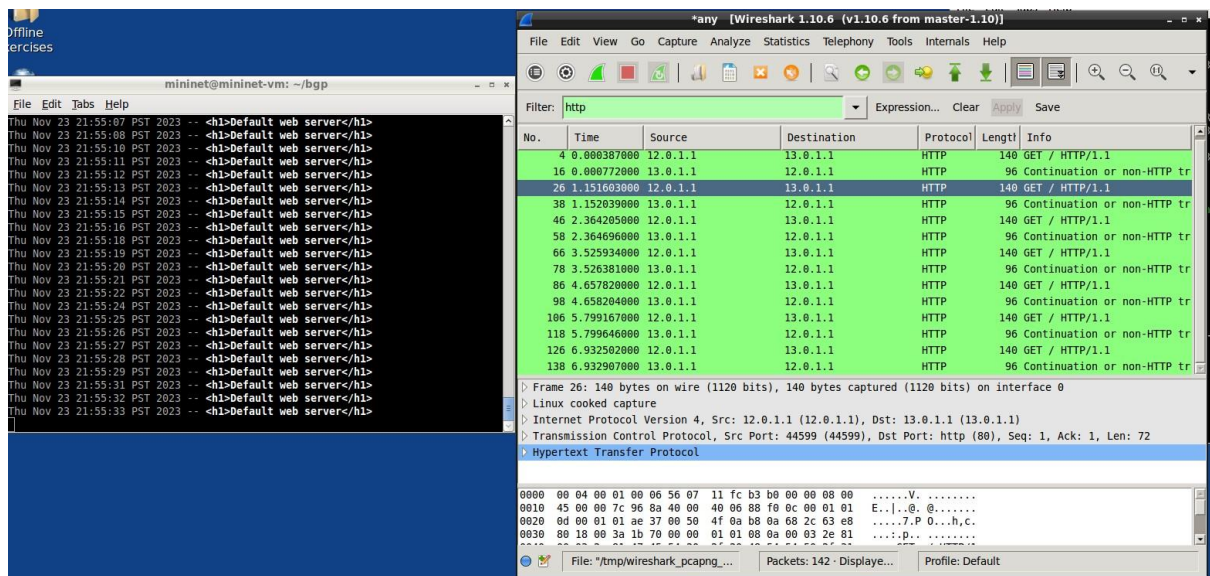
▶ Linux cooked capture

▶ 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: 49603 (49603), Dst Port: http (80), Seq: 1, Ack: 1, Len: 72

▶ Hypertext Transfer Protocol

Q8) Get request from the h2-1 In wireshark



The code for website2.sh is given below

```

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

~/bin/bash

node=${1:-h2-1}
bold='tput bold'
normal='tput sgr0'

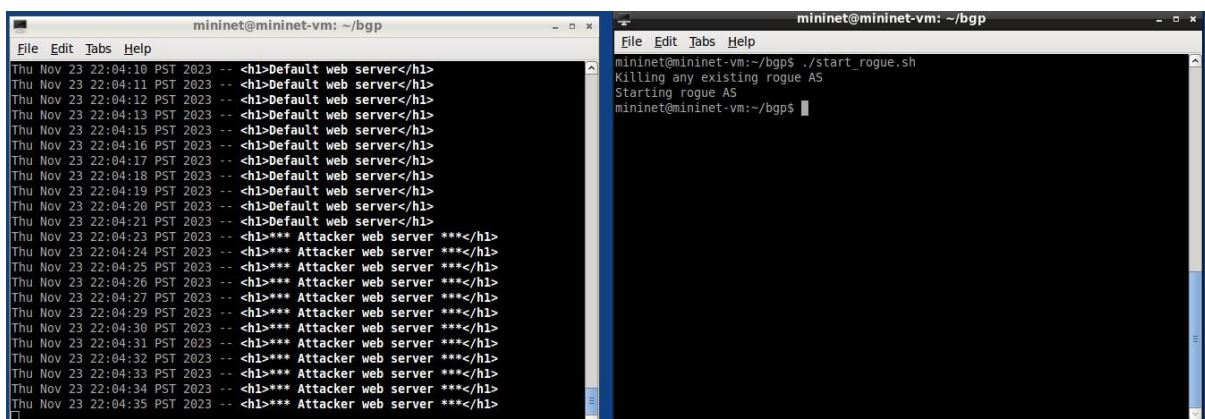
while true; do
    out=$(sudo python run.py --node $node --cmd "curl -s 13.0.1.1")
    date=$(date)
    echo $date -- $bold$out$normal
    sleep 1
done

"website2.sh" 13L, 217C
1,1 All

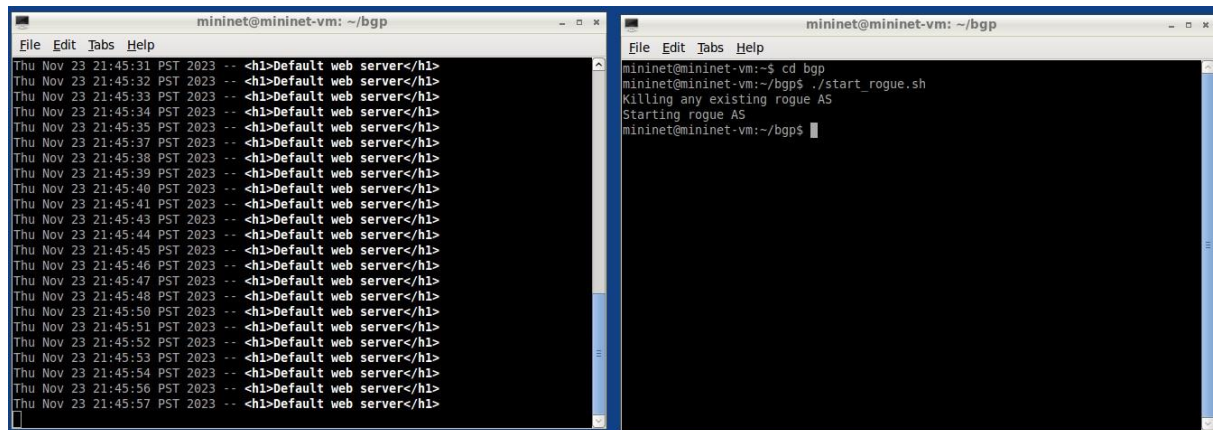
```

Q9) h4 bgp attack with start_rougue.sh script

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



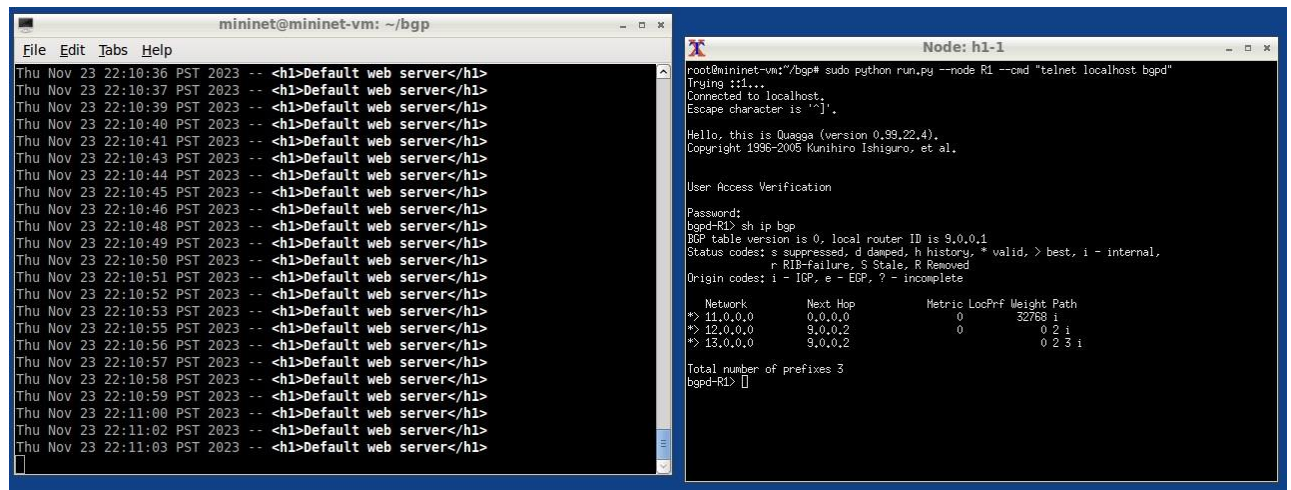
Q10) From h2-1 it is not changing from rouge because AS3 is the shortest path(1 hop) where as attacker(AS4) has 2 hops



```
mininet@mininet-vm: ~/bgp
File Edit Tabs Help
Thu Nov 23 21:45:31 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 21:45:32 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 21:45:33 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 21:45:34 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 21:45:35 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 21:45:37 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 21:45:38 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 21:45:39 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 21:45:40 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 21:45:41 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 21:45:43 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 21:45:44 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 21:45:45 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 21:45:46 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 21:45:47 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 21:45:48 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 21:45:50 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 21:45:51 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 21:45:52 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 21:45:53 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 21:45:54 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 21:45:56 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 21:45:57 PST 2023 --<h1>Default web server</h1>

mininet@mininet-vm:~/bgp$ cd bgp
mininet@mininet-vm:~/bgp$ ./start_rouge.sh
Killing any existing rouge AS
Starting rouge AS
mininet@mininet-vm:~/bgp$
```

Q11) Before BGP attack, bgp table from R1



```
mininet@mininet-vm: ~/bgp
File Edit Tabs Help
Thu Nov 23 22:10:36 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 22:10:37 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 22:10:39 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 22:10:40 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 22:10:41 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 22:10:43 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 22:10:44 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 22:10:45 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 22:10:46 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 22:10:48 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 22:10:49 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 22:10:50 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 22:10:51 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 22:10:52 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 22:10:53 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 22:10:55 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 22:10:56 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 22:10:57 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 22:10:58 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 22:10:59 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 22:11:00 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 22:11:02 PST 2023 --<h1>Default web server</h1>
Thu Nov 23 22:11:03 PST 2023 --<h1>Default web server</h1>

Node: h1-1
root@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.

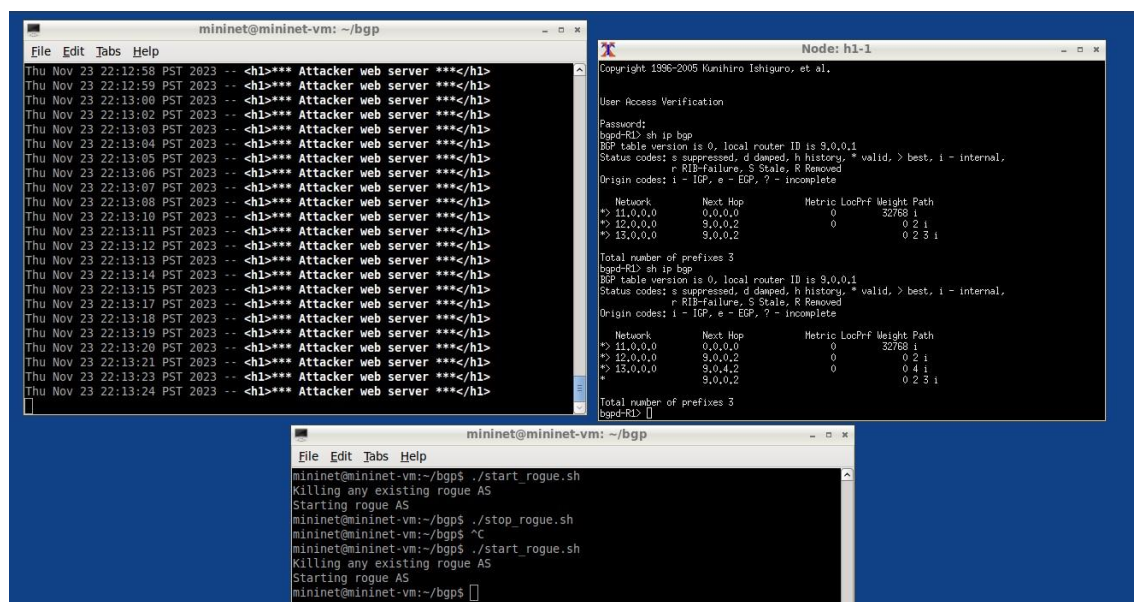
User Access Verification

Password:
bgpd-R1# 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#
```

After BGP attack, bgp table from R1



```
mininet@mininet-vm: ~/bgp
File Edit Tabs Help
Thu Nov 23 22:12:58 PST 2023 --<h1>*** Attacker web server ***</h1>
Thu Nov 23 22:12:59 PST 2023 --<h1>*** Attacker web server ***</h1>
Thu Nov 23 22:13:00 PST 2023 --<h1>*** Attacker web server ***</h1>
Thu Nov 23 22:13:02 PST 2023 --<h1>*** Attacker web server ***</h1>
Thu Nov 23 22:13:03 PST 2023 --<h1>*** Attacker web server ***</h1>
Thu Nov 23 22:13:04 PST 2023 --<h1>*** Attacker web server ***</h1>
Thu Nov 23 22:13:05 PST 2023 --<h1>*** Attacker web server ***</h1>
Thu Nov 23 22:13:06 PST 2023 --<h1>*** Attacker web server ***</h1>
Thu Nov 23 22:13:07 PST 2023 --<h1>*** Attacker web server ***</h1>
Thu Nov 23 22:13:08 PST 2023 --<h1>*** Attacker web server ***</h1>
Thu Nov 23 22:13:10 PST 2023 --<h1>*** Attacker web server ***</h1>
Thu Nov 23 22:13:11 PST 2023 --<h1>*** Attacker web server ***</h1>
Thu Nov 23 22:13:12 PST 2023 --<h1>*** Attacker web server ***</h1>
Thu Nov 23 22:13:13 PST 2023 --<h1>*** Attacker web server ***</h1>
Thu Nov 23 22:13:14 PST 2023 --<h1>*** Attacker web server ***</h1>
Thu Nov 23 22:13:15 PST 2023 --<h1>*** Attacker web server ***</h1>
Thu Nov 23 22:13:17 PST 2023 --<h1>*** Attacker web server ***</h1>
Thu Nov 23 22:13:18 PST 2023 --<h1>*** Attacker web server ***</h1>
Thu Nov 23 22:13:19 PST 2023 --<h1>*** Attacker web server ***</h1>
Thu Nov 23 22:13:20 PST 2023 --<h1>*** Attacker web server ***</h1>
Thu Nov 23 22:13:21 PST 2023 --<h1>*** Attacker web server ***</h1>
Thu Nov 23 22:13:23 PST 2023 --<h1>*** Attacker web server ***</h1>
Thu Nov 23 22:13:24 PST 2023 --<h1>*** Attacker web server ***</h1>

Node: h1-1
Copyright 1996-2005 Kunihiro Ishiguro, et al.

User Access Verification

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 i
*> 13.0.0.0         9.0.0.2              0           2 3 i

Total number of prefixes 3
bgpd-R1#

mininet@mininet-vm:~/bgp$ ./start_rouge.sh
Killing any existing rouge AS
Starting rouge AS
mininet@mininet-vm:~/bgp$ ./stop_rouge.sh
mininet@mininet-vm:~/bgp$ ^c
mininet@mininet-vm:~/bgp$ ./start_rouge.sh
Killing any existing rouge AS
Starting rouge AS
mininet@mininet-vm:~/bgp$
```


The image shows two terminal windows. The left window, titled 'mininet@mininet-vm: ~/bgp', displays a series of commands and their outputs for configuring a BGP network. The commands are: `<h1>*** Attacker web server ***</h1>`, `<h1>Default web server</h1>`, and `<h1>Default web server</h1>`. The right window, titled 'Node: h1-1', shows the output of a telnet session to the local host. It displays the IP address '192.168.1.1', the version 'Quagga (version 0.99.22.4)', and the copyright notice 'Copyright 1996-2005 Kunihiro Ishiguro, et al.'. It also shows the 'User Access Verification' prompt and the password 'bgpd-R2'. The output of the `show ip bgp` command is also displayed, showing the BGP table version, local router ID, and status codes.

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

Thu Nov 23 22:14:55 PST 2023 -- <h1>*** Attacker web server ***</h1>
Thu Nov 23 22:14:56 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:14:57 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:14:58 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:14:59 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:15:00 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:15:02 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:15:03 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:15:04 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:15:05 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:15:06 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:15:07 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:15:08 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:15:09 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:15:11 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:15:12 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:15:13 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:15:14 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:15:15 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:15:16 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:15:18 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:15:19 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:15:20 PST 2023 -- <h1>Default web server</h1>

Node: h1-1
mininet@mininet-vm:~/bgp$ sudo python run.py --node R2 --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-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          9.0.0.0              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>
```

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

Thu Nov 23 22:19:51 PST 2023 --> <h1>*** Attacker web server ***</h1>
Thu Nov 23 22:19:52 PST 2023 --> <h1>*** Attacker web server ***</h1>
Thu Nov 23 22:19:53 PST 2023 --> <h1>*** Attacker web server ***</h1>
Thu Nov 23 22:19:54 PST 2023 --> <h1>*** Attacker web server ***</h1>
Thu Nov 23 22:19:55 PST 2023 --> <h1>*** Attacker web server ***</h1>
Thu Nov 23 22:19:56 PST 2023 --> <h1>*** Attacker web server ***</h1>
Thu Nov 23 22:19:57 PST 2023 --> <h1>*** Attacker web server ***</h1>
Thu Nov 23 22:19:59 PST 2023 --> <h1>*** Attacker web server ***</h1>
Thu Nov 23 22:20:00 PST 2023 --> <h1>*** Attacker web server ***</h1>
Thu Nov 23 22:20:01 PST 2023 --> <h1>*** Attacker web server ***</h1>
Thu Nov 23 22:20:02 PST 2023 --> <h1>*** Attacker web server ***</h1>
Thu Nov 23 22:20:03 PST 2023 --> <h1>*** Attacker web server ***</h1>
Thu Nov 23 22:20:04 PST 2023 --> <h1>*** Attacker web server ***</h1>
Thu Nov 23 22:20:05 PST 2023 --> <h1>*** Attacker web server ***</h1>
Thu Nov 23 22:20:06 PST 2023 --> <h1>*** Attacker web server ***</h1>
Thu Nov 23 22:20:08 PST 2023 --> <h1>*** Attacker web server ***</h1>
Thu Nov 23 22:20:09 PST 2023 --> <h1>*** Attacker web server ***</h1>
Thu Nov 23 22:20:10 PST 2023 --> <h1>*** Attacker web server ***</h1>
Thu Nov 23 22:20:11 PST 2023 --> <h1>*** Attacker web server ***</h1>
Thu Nov 23 22:20:12 PST 2023 --> <h1>*** Attacker web server ***</h1>
Thu Nov 23 22:20:13 PST 2023 --> <h1>*** Attacker web server ***</h1>
Thu Nov 23 22:20:14 PST 2023 --> <h1>*** Attacker web server ***</h1>
Thu Nov 23 22:20:16 PST 2023 --> <h1>*** Attacker web server ***</h1>

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

mininet@mininet-vm:~/bgp$ ./start_rogue.sh
Killing any existing rogue AS
Starting rogue AS
mininet@mininet-vm:~/bgp$
```

No.	Time	Source	Destination	Protocol	Length	Info
8	57.62631000	9.0.4.2	9.0.4.1	BGP	119	OPEN Message
10	57.62686200	9.0.4.1	9.0.4.2	BGP	138	OPEN Message, KEEPALIVE Message
12	57.62711100	9.0.4.2	9.0.4.1	BGP	104	KEEPALIVE Message, KEEPALIVE Message
13	57.62727200	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
15	58.62972000	9.0.4.1	9.0.4.2	BGP	242	KEEPALIVE Message, UPDATE Message, UPDATE Message, UPDATE Message
17	58.63261500	9.0.4.2	9.0.4.1	BGP	138	KEEPALIVE Message, UPDATE Message
19	58.68408700	9.0.4.1	9.0.4.2	BGP	91	UPDATE Message
41	59.63116800	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
43	59.63191300	9.0.4.2	9.0.4.1	BGP	85	KEEPALIVE Message
65	60.63142400	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
66	60.63214800	9.0.4.2	9.0.4.1	BGP	85	KEEPALIVE Message
68	61.63238900	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
69	61.63265900	9.0.4.2	9.0.4.1	BGP	85	KEEPALIVE Message

Frame 15: 242 bytes on wire (1936 bits), 242 bytes captured (1936 bits) on interface 0

Ethernet II, Src: 66:69:04:f3:95:d1 (66:69:04:f3:95:d1), Dst: 1e:3d:f1:bb:2d:ed (1e:3d:f1:bb:2d:ed)

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: 38756 (38756), Seq: 92, Ack: 92, Len: 176

Border Gateway Protocol - KEEPALIVE Message

Border Gateway Protocol - UPDATE Message

Border Gateway Protocol - UPDATE Message

Border Gateway Protocol - UPDATE Message

No.	Time	Source	Destination	Protocol	Length	Info
15	58.62972000	9.0.4.1	9.0.4.2	BGP	242	KEEPALIVE Message, UPDATE Message, UPDATE Message, UPDATE Message
17	58.63261500	9.0.4.2	9.0.4.1	BGP	138	KEEPALIVE Message, UPDATE Message
Path attributes						
ORIGIN: IGP (4 bytes)						
AS_PATH: 1 (10 bytes)						
NEXT_HOP: 9.0.4.1 (7 bytes)						
MULTI_EXIT_DISC: 0 (7 bytes)						
Network layer reachability information: 2 bytes						
Border Gateway Protocol - UPDATE Message						
Marker: ffffffffffffffffffffffffffffffff						
Length: 50						
Type: UPDATE Message (2)						
Unfeasible routes length: 0 bytes						
Total path attribute length: 25 bytes						
Path attributes						
ORIGIN: IGP (4 bytes)						
AS_PATH: 1 2 (14 bytes)						
NEXT_HOP: 9.0.4.1 (7 bytes)						
Network layer reachability information: 2 bytes						
Border Gateway Protocol - UPDATE Message						
Marker: ffffffffffffffffffffffffffffffff						
Length: 54						
Type: UPDATE Message (2)						
Unfeasible routes length: 0 bytes						
Total path attribute length: 29 bytes						
Path attributes						
ORIGIN: IGP (4 bytes)						
AS_PATH: 1 2 3 (18 bytes)						
NEXT_HOP: 9.0.4.1 (7 bytes)						
Network layer reachability information: 2 bytes						

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

15	58.62972000	9.0.4.1	9.0.4.2	BGP	242	KEEPALIVE Message, UPDATE Message, UPDATE Message, UPDATE Message
17	58.63261500	9.0.4.2	9.0.4.1	BGP	138	KEEPALIVE Message, UPDATE Message
19	58.68408700	9.0.4.1	9.0.4.2	BGP	91	UPDATE Message
41	59.63116800	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
43	59.63191300	9.0.4.2	9.0.4.1	BGP	85	KEEPALIVE Message
65	60.63142400	9.0.4.1	9.0.4.2	BGP	85	KEEPALIVE Message
Frame 19: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface 0						
Ethernet II, Src: 66:69:04:f3:95:d1 (66:69:04:f3:95:d1), Dst: 1e:3d:f1:bb:2d:ed (1e:3d:f1:bb:2d:ed)						
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: 38756 (38756), 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						

Q13) Normally AS3 is hosting a website and that website is accessed by AS1 via AS2, There is an attacker's network AS4 it pretends as a AS3 and grabs 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 Rogue is successfully fooled AS1 but not AS2 hosts because of the path distance

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

The image displays two screenshots from a network analysis session. The left screenshot is a Wireshark capture showing ICMP Echo (ping) requests and replies between 11.0.1.1 and 13.0.1.1. The right screenshot shows a terminal window with the output of a 'ping' command, indicating a round-trip time (RTT) of 0.75ms. Below the terminal window, a 'mininet' terminal window shows the network topology, including a default web server and an attacker web server.

Wireshark Capture (Left):

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	11.0.1.1	13.0.1.1	ICMP	100	Echo (ping) request
2	0.000075000	13.0.1.1	11.0.1.1	ICMP	100	Echo (ping) reply
3	0.999276000	11.0.1.1	13.0.1.1	ICMP	100	Echo (ping) request
4	0.999348000	13.0.1.1	11.0.1.1	ICMP	100	Echo (ping) reply
5	1.999873000	11.0.1.1	13.0.1.1	ICMP	100	Echo (ping) request
6	1.999165000	13.0.1.1	11.0.1.1	ICMP	100	Echo (ping) reply
7	2.999832000	11.0.1.1	13.0.1.1	ICMP	100	Echo (ping) request
8	2.999165000	13.0.1.1	11.0.1.1	ICMP	100	Echo (ping) reply
9	3.999844000	11.0.1.1	13.0.1.1	ICMP	100	Echo (ping) request
10	3.999190000	13.0.1.1	11.0.1.1	ICMP	100	Echo (ping) reply
11	4.999874000	11.0.1.1	13.0.1.1	ICMP	100	Echo (ping) request
12	4.999145000	13.0.1.1	11.0.1.1	ICMP	100	Echo (ping) reply
13	5.000930000	6a:3a:2a:95:ee:ab	44 Who has 11.0.1.1?	ARP	44	Who has 11.0.1.1?
14	5.007101000	f2:b3:19:e4:d9:84	44 Who has 11.0.1.1?	ARP	44	Who has 11.0.1.1?

Terminal Output (Right):

```
root@mininet-vm:~# 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=61 time=0.102 ms
64 bytes from 13.0.1.1: icmp_seq=2 ttl=61 time=0.110 ms
64 bytes from 13.0.1.1: icmp_seq=3 ttl=61 time=0.139 ms
64 bytes from 13.0.1.1: icmp_seq=4 ttl=61 time=0.113 ms
64 bytes from 13.0.1.1: icmp_seq=5 ttl=61 time=0.115 ms
64 bytes from 13.0.1.1: icmp_seq=6 ttl=61 time=0.110 ms
64 bytes from 13.0.1.1: icmp_seq=7 ttl=61 time=0.112 ms
64 bytes from 13.0.1.1: icmp_seq=8 ttl=61 time=0.113 ms
^C
--- 13.0.1.1 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 799ms
rtt min/avg/max/ndev = 0.102/0.114/0.139/0.009 ms
root@mininet-vm:~# bgp
```

mininet Terminal (Bottom Right):

```
mininet@mininet-vm: ~$ bgp
Thu Nov 23 22:33:47 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:33:48 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:33:49 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:33:50 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:33:51 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:33:52 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:33:53 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:33:54 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:33:55 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:33:56 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:33:57 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:33:58 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:33:59 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:34:01 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:34:02 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:34:03 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:34:04 PST 2023 -- <h1>Default web server</h1>
```

BGP attack, In wireshark the RTT is 0.60ms

The image displays two screenshots from a network analysis session during a BGP attack. The left screenshot is a Wireshark capture showing ICMP Echo (ping) requests and replies between 11.0.1.1 and 13.0.1.1. The right screenshot shows a terminal window with the output of a 'ping' command, indicating a round-trip time (RTT) of 0.60ms. Below the terminal window, a 'mininet' terminal window shows the network topology, including a default web server and an attacker web server.

Wireshark Capture (Left):

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	11.0.1.1	13.0.1.1	ICMP	100	Echo (ping) request
2	0.000060000	13.0.1.1	11.0.1.1	ICMP	100	Echo (ping) reply
3	0.999549000	11.0.1.1	13.0.1.1	ICMP	100	Echo (ping) request
4	0.999610000	13.0.1.1	11.0.1.1	ICMP	100	Echo (ping) reply
5	1.999563000	11.0.1.1	13.0.1.1	ICMP	100	Echo (ping) request
6	1.999623000	13.0.1.1	11.0.1.1	ICMP	100	Echo (ping) reply
7	3.000112000	11.0.1.1	13.0.1.1	ICMP	100	Echo (ping) request
8	3.000173000	13.0.1.1	11.0.1.1	ICMP	100	Echo (ping) reply
9	3.999110000	11.0.1.1	13.0.1.1	ICMP	100	Echo (ping) request
10	3.999171000	13.0.1.1	11.0.1.1	ICMP	100	Echo (ping) reply
11	4.998689000	11.0.1.1	13.0.1.1	ICMP	100	Echo (ping) request
12	4.998752000	13.0.1.1	11.0.1.1	ICMP	100	Echo (ping) reply
13	5.999322000	11.0.1.1	13.0.1.1	ICMP	100	Echo (ping) request
14	5.999385000	13.0.1.1	11.0.1.1	ICMP	100	Echo (ping) reply

Terminal Output (Right):

```
root@mininet-vm:~# 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=0.067 ms
64 bytes from 13.0.1.1: icmp_seq=2 ttl=62 time=0.132 ms
64 bytes from 13.0.1.1: icmp_seq=3 ttl=62 time=0.088 ms
64 bytes from 13.0.1.1: icmp_seq=4 ttl=62 time=0.083 ms
^C
--- 13.0.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/ndev = 0.067/0.092/0.132/0.025 ms
root@mininet-vm:~# bgp
```

mininet Terminal (Bottom Right):

```
mininet@mininet-vm: ~$ bgp
Thu Nov 23 22:35:59 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:36:00 PST 2023 -- <h1>Default web server</h1>
Thu Nov 23 22:36:01 PST 2023 -- <h1>*** Attacker web server ***</h1>
Thu Nov 23 22:36:02 PST 2023 -- <h1>*** Attacker web server ***</h1>
Thu Nov 23 22:36:03 PST 2023 -- <h1>*** Attacker web server ***</h1>
Thu Nov 23 22:36:04 PST 2023 -- <h1>*** Attacker web server ***</h1>
Thu Nov 23 22:36:05 PST 2023 -- <h1>*** Attacker web server ***</h1>
Thu Nov 23 22:36:06 PST 2023 -- <h1>*** Attacker web server ***</h1>
Thu Nov 23 22:36:07 PST 2023 -- <h1>*** Attacker web server ***</h1>
Thu Nov 23 22:36:08 PST 2023 -- <h1>*** Attacker web server ***</h1>
Thu Nov 23 22:36:09 PST 2023 -- <h1>*** Attacker web server ***</h1>
Thu Nov 23 22:36:10 PST 2023 -- <h1>*** Attacker web server ***</h1>
Thu Nov 23 22:36:11 PST 2023 -- <h1>*** Attacker web server ***</h1>
Thu Nov 23 22:36:12 PST 2023 -- <h1>*** Attacker web server ***</h1>
Thu Nov 23 22:36:13 PST 2023 -- <h1>*** Attacker web server ***</h1>
Thu Nov 23 22:36:15 PST 2023 -- <h1>*** Attacker web server ***</h1>
^C
mininet@mininet-vm:~# bgp
```

Q15) Original code for bgp.py

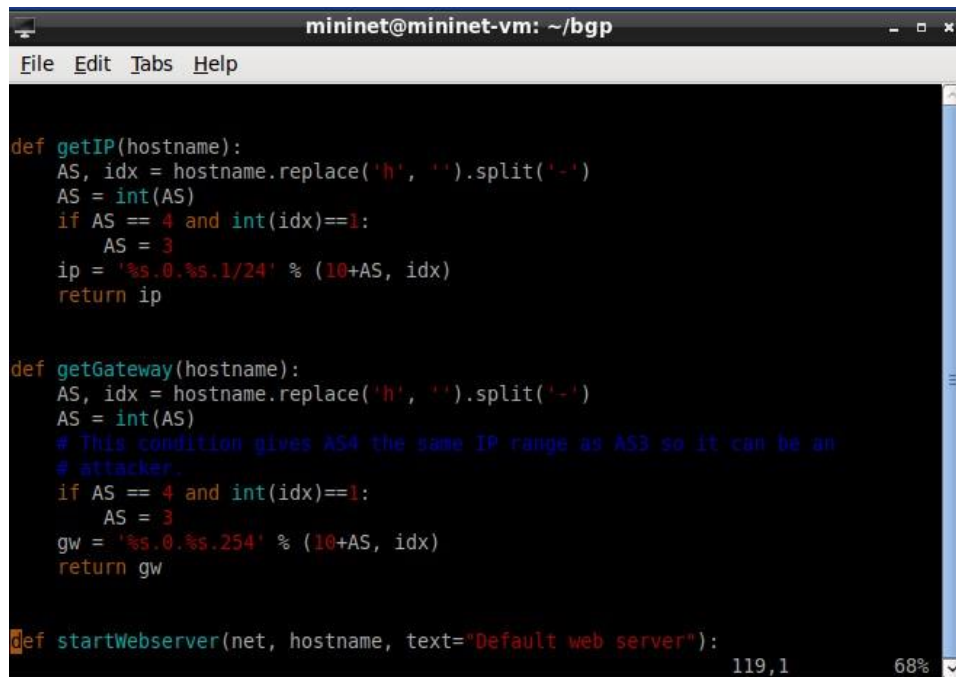
```
def getIP(hostname):
    AS, idx = hostname.replace('h', '').split('-')
    AS = int(AS)
    if AS == 4:
        AS = 3
    ip = '%s.0.%s.1/24' % (10+AS, idx)
    return ip

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



```
def getIP(hostname):
    AS, idx = hostname.replace('h', '').split('-')
    AS = int(AS)
    if AS == 4 and int(idx)==1:
        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 and int(idx)==1:
        AS = 3
    gw = '%s.0.%s.254' % (10+AS, idx)
    return gw

def startWebserver(net, hostname, text="Default web server"):
```

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

```
mininet@mininet-vm: ~/bgp/conf
File Edit Tabs 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 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
"bgpd-R4.conf" 31L, 514C 1,1 Top
```

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

Node: h4-1	Node: h4-2
<pre>root@mininet-vm:~/bgp# ifconfig h4-1-eth0 Link encap:Ethernet HWaddr c6:79:30:45:b2:f6 inet addr:13.0.1.1 Bcast:13.0.1.255 Mask:255.255.255,0 inet6 addr: fe80::c479:30ff:fe45:b2f6/64 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#</pre>	<pre>root@mininet-vm:~/bgp# ifconfig h4-2-eth0 Link encap:Ethernet HWaddr f6:26:39:c0:97:8b inet addr:14.0.2.1 Bcast:14.0.2.255 Mask:255.255.255,0 inet6 addr: fe80::f426:39ff:fec0:978b/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#</pre>

The modified Zebra configuration path

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

!

"zebra-R4.conf" 28L, 311C 1,1 Top
```

The new bgp path at R1 from h1-1

```
Node: h1-1
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> 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
*> 13.0.1.0/24     9.0.4.2          0           4 i
*> 14.0.0.0        9.0.4.2          0           4 i

Total number of prefixes 5
bgpd-R1>
```

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