Part 4 Design and implement a countermeasure to the attack from Part3

I. Abstract:

In an ideal world, there would be filters on all BGP sessions that only allow prefixes that are actually supposed to come in over that BGP session. In Part3 practice, ISPs tend to get new IP address blocks to prevent the false origin prefix attack. This means that once an ISP accepts a prefix advertised by a customer, that prefix will be widely propagated.

II. Modified files:

bgpd-R1.conf

bgpd-R2.conf

bgpd-R3.conf

bgpd-R4.conf

bgpd-R5.conf

III. Description of changes:

Added AS prefix filter to prevent the malicious/unknown IP connections. Prelist all the AS ip permits and filter out unknown ones, sample code is like below:

R5

```
ip prefix-list customer-a seq 5 permit 9.0.5.5/24 le 32

ip prefix-list customer-a seq 10 permit 9.0.8.5/24 le 32

ip prefix-list customer-a seq 15 permit 9.0.6.4/24 le 32

neighbor 9.0.7.6 prefix-list customer-a in (for any new AS added to the system)
```

R4

```
ip prefix-list customer-a seq 5 permit 9.0.2.2/24 le 32

ip prefix-list customer-a seq 10 permit 9.0.3.4/24 le 32

ip prefix-list customer-a seq 15 permit 9.0.6.5/24 le 32
```

R3

```
ip prefix-list customer-a seq 5 permit 9.0.4.1/24 le 32

ip prefix-list customer-a seq 10 permit 9.0.1.1/24 le 32

ip prefix-list customer-a seq 15 permit 9.0.3.3/24 le 32

ip prefix-list customer-a seq 20 permit 9.0.8.6/24 le 32
```

R2

ip prefix-list customer-a seq 5 permit 9.0.0.1/24 le 32

ip prefix-list customer-a seq 10 permit 9.0.1.2/24 le 32

ip prefix-list customer-a seq 15 permit 9.0.2.1/24 le 32

ip prefix-list customer-a seq 20 permit 9.0.5.6/24 le 32

R1

ip prefix-list customer-a seq 5 permit 9.0.0.2/24 le 32

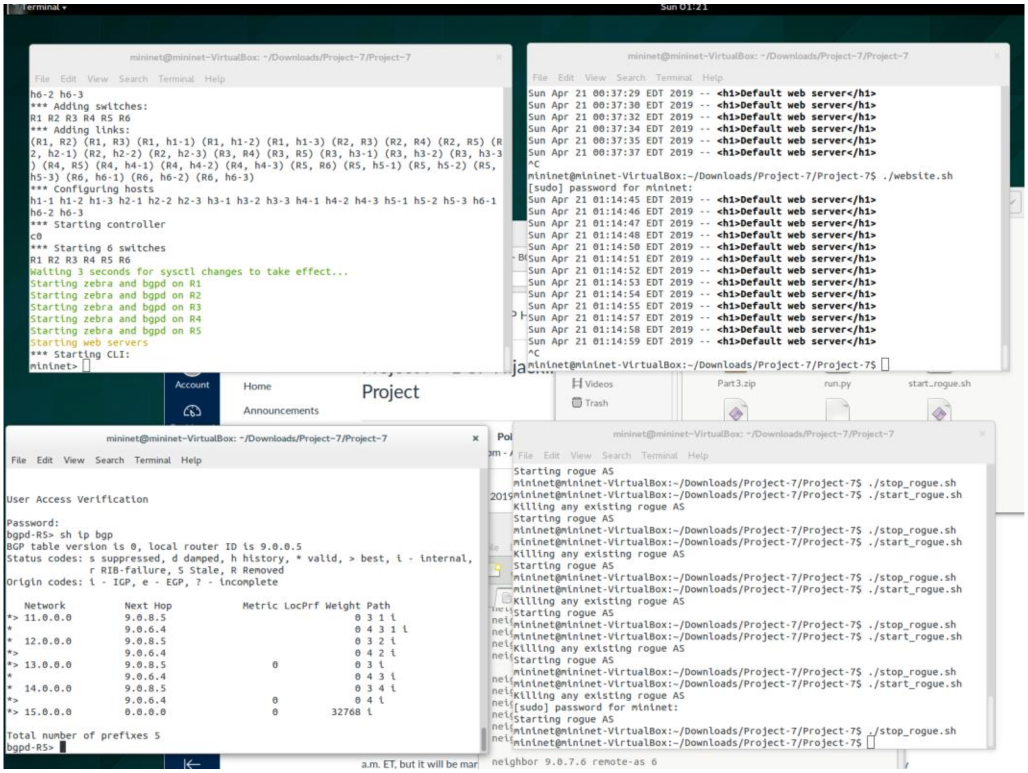
ip prefix-list customer-a seq 10 permit 9.0.4.2/24 le 32

IV. Instructions for demonstration

Similar to Part 2

1. Run sudo python bgp.py
2. Run ./connect.sh in another terminal
3. Run ./website.sh in the third terminal
4. Run ./start_rogue.sh and ./stop_rogue.sh in the fourth terminal
5. Run sh ip bgp or sh ip bgp summary in terminal 2 to ensure the hijack prefix attack falls.

Below figure shows how the victim AS routing table maintain its original state:



Terminal ▾
Sun 01:21
mininet@mininet-VirtualBox: ~/Downloads/Project-7/Project-7
File Edit View Search Terminal Help
Account
Home
Announcements
Project
Videos
Trash
Part3.zip
run.py
start_rogue.sh

```
h6-2 h6-3
*** Adding switches:
R1 R2 R3 R4 R5 R6
*** Adding links:
(R1, R2) (R1, R3) (R1, h1-1) (R1, h1-2) (R1, h1-3) (R2, R3) (R2, R4) (R2, R5) (R
2, h2-1) (R2, h2-2) (R2, h2-3) (R3, R4) (R3, R5) (R3, h3-1) (R3, h3-2) (R3, h3-3
) (R4, R5) (R4, h4-1) (R4, h4-2) (R4, h4-3) (R5, R6) (R5, h5-1) (R5, h5-2) (R5,
h5-3) (R6, h6-1) (R6, h6-2) (R6, h6-3)
*** Configuring 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 h5-1 h5-2 h5-3 h6-1
h6-2 h6-3
*** Starting controller
c0
*** Starting 6 switches
R1 R2 R3 R4 R5 R6
Waiting 3 seconds for sysctl changes to take effect...
Starting zebra and bgpd on R1
Starting zebra and bgpd on R2
Starting zebra and bgpd on R3
Starting zebra and bgpd on R4
Starting zebra and bgpd on R5
Starting web servers
*** Starting CLI:
mininet> 
```

```
Sun Apr 21 00:37:29 EDT 2019 -- <h1>Default web server</h1>
Sun Apr 21 00:37:30 EDT 2019 -- <h1>Default web server</h1>
Sun Apr 21 00:37:32 EDT 2019 -- <h1>Default web server</h1>
Sun Apr 21 00:37:34 EDT 2019 -- <h1>Default web server</h1>
Sun Apr 21 00:37:35 EDT 2019 -- <h1>Default web server</h1>
Sun Apr 21 00:37:37 EDT 2019 -- <h1>Default web server</h1>
^C
mininet@mininet-VirtualBox:~/Downloads/Project-7/Project-7$ ./website.sh
[sudo] password for mininet:
Sun Apr 21 01:14:45 EDT 2019 -- <h1>Default web server</h1>
Sun Apr 21 01:14:46 EDT 2019 -- <h1>Default web server</h1>
Sun Apr 21 01:14:47 EDT 2019 -- <h1>Default web server</h1>
Sun Apr 21 01:14:48 EDT 2019 -- <h1>Default web server</h1>
Sun Apr 21 01:14:50 EDT 2019 -- <h1>Default web server</h1>
Sun Apr 21 01:14:51 EDT 2019 -- <h1>Default web server</h1>
Sun Apr 21 01:14:52 EDT 2019 -- <h1>Default web server</h1>
Sun Apr 21 01:14:53 EDT 2019 -- <h1>Default web server</h1>
Sun Apr 21 01:14:54 EDT 2019 -- <h1>Default web server</h1>
Sun Apr 21 01:14:55 EDT 2019 -- <h1>Default web server</h1>
Sun Apr 21 01:14:57 EDT 2019 -- <h1>Default web server</h1>
Sun Apr 21 01:14:58 EDT 2019 -- <h1>Default web server</h1>
Sun Apr 21 01:14:59 EDT 2019 -- <h1>Default web server</h1>
^C
mininet@mininet-VirtualBox:~/Downloads/Project-7/Project-7$ 
```

```
User Access Verification

Password:
bgpd-R5> sh ip bgp
BGP table version is 0, local router ID is 9.0.0.5
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         9.0.8.5                                0 3 1 i
*                   9.0.6.4                                0 4 3 1 i
*  12.0.0.0         9.0.8.5                                0 3 2 i
*>                  9.0.6.4                                0 4 2 i
*> 13.0.0.0         9.0.8.5                  0             0 3 i
*                   9.0.6.4                                0 4 3 i
*  14.0.0.0         9.0.8.5                                0 3 4 i
*>                  9.0.6.4                  0             0 4 i
*> 15.0.0.0         0.0.0.0                  0         32768 i

Total number of prefixes 5
bgpd-R5> 
```

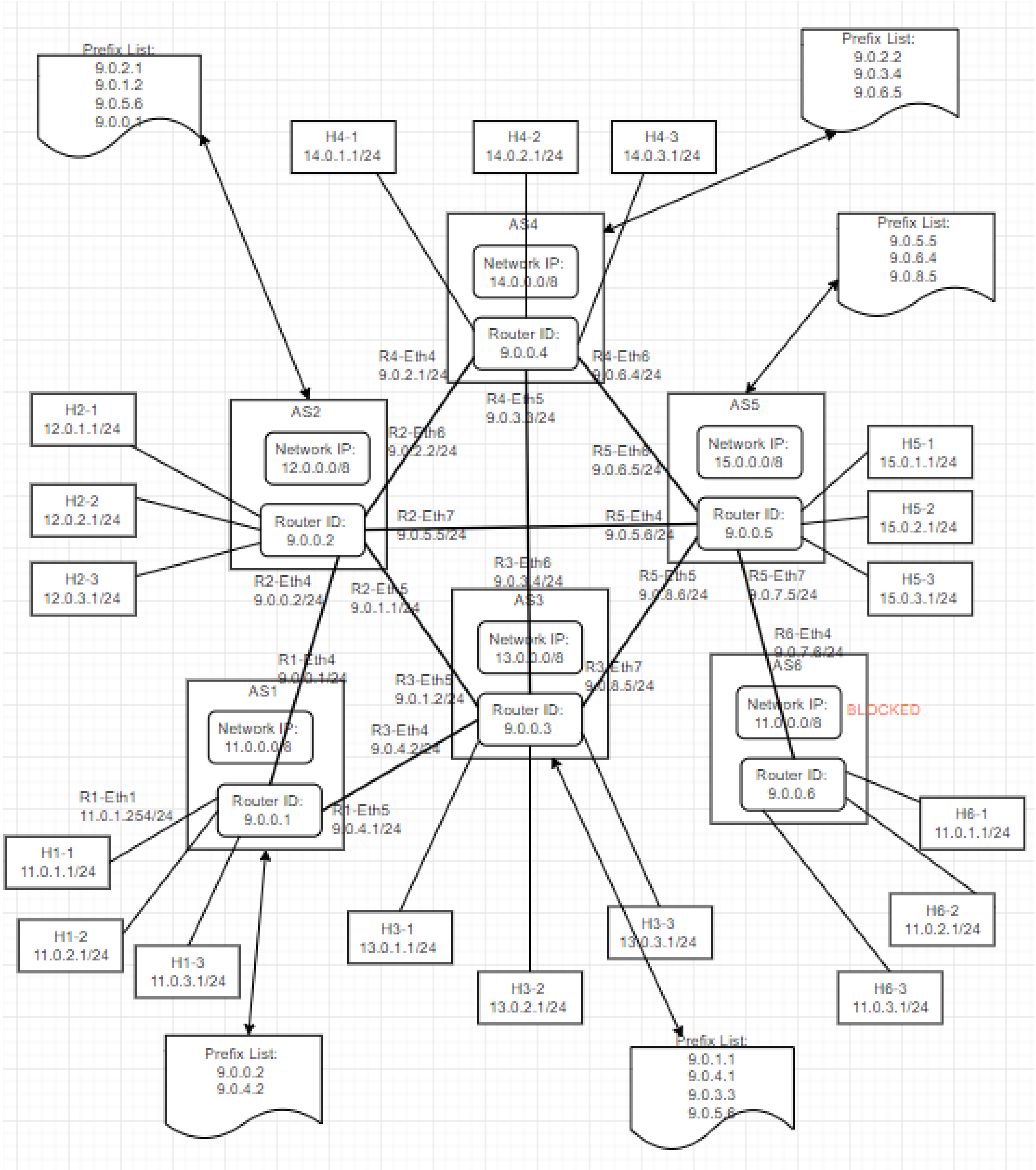
```
Starting rogue AS
mininet@mininet-VirtualBox:~/Downloads/Project-7/Project-7$ ./stop_rogue.sh
mininet@mininet-VirtualBox:~/Downloads/Project-7/Project-7$ ./start_rogue.sh
Killing any existing rogue AS
Starting rogue AS
mininet@mininet-VirtualBox:~/Downloads/Project-7/Project-7$ ./stop_rogue.sh
mininet@mininet-VirtualBox:~/Downloads/Project-7/Project-7$ ./start_rogue.sh
Killing any existing rogue AS
Starting rogue AS
mininet@mininet-VirtualBox:~/Downloads/Project-7/Project-7$ ./stop_rogue.sh
mininet@mininet-VirtualBox:~/Downloads/Project-7/Project-7$ ./start_rogue.sh
Killing any existing rogue AS
Starting rogue AS
mininet@mininet-VirtualBox:~/Downloads/Project-7/Project-7$ ./stop_rogue.sh
mininet@mininet-VirtualBox:~/Downloads/Project-7/Project-7$ ./start_rogue.sh
Killing any existing rogue AS
Starting rogue AS
mininet@mininet-VirtualBox:~/Downloads/Project-7/Project-7$ ./stop_rogue.sh
mininet@mininet-VirtualBox:~/Downloads/Project-7/Project-7$ ./start_rogue.sh
Killing any existing rogue AS
[sudo] password for mininet:
Starting rogue AS
mininet@mininet-VirtualBox:~/Downloads/Project-7/Project-7$ ./stop_rogue.sh
mininet@mininet-VirtualBox:~/Downloads/Project-7/Project-7$ 
```

```
neighbor 9.0.7.6 remote-as 6
```

V. Summary

This approach will block any attack as well as any unknown new AS, in case any AS need to be added to the mininet system, a new filter will be implemented to include them. In real world, ISPs carefully filter prefixes they receive from their customers.

This is a simple prefix list approach that allows the prefixes held by the customer (and the customer's customers) will do the trick for countermeasure from Part 3. See figure below:



Prefix List:
9.0.2.1
9.0.1.2
9.0.5.6
9.0.0.1
H4-1
14.0.1.1/24
H4-2
14.0.2.1/24
H4-3
14.0.3.1/24
Prefix List:
9.0.2.2
9.0.3.4
9.0.6.5
AS4
Network IP:
14.0.0.0/8
Router ID:
9.0.0.4
Prefix List:
9.0.5.5
9.0.6.4
9.0.8.5
R4-Eth4
9.0.2.1/24
R4-Eth6
9.0.6.4/24
R4-Eth5
9.0.3.3/24
H2-1
12.0.1.1/24
AS2
Network IP:
12.0.0.0/8
R2-Eth6
9.0.2.2/24
R5-Eth6
9.0.6.5/24
AS5
Network IP:
15.0.0.0/8
H5-1
15.0.1.1/24
H2-2
12.0.2.1/24
Router ID:
9.0.0.2
R2-Eth7
9.0.5.5/24
R5-Eth4
9.0.5.6/24
Router ID:
9.0.0.5
H5-2
15.0.2.1/24
H2-3
12.0.3.1/24
R2-Eth4
9.0.0.2/24
R2-Eth5
9.0.1.1/24
R3-Eth6
9.0.3.4/24
R5-Eth5
9.0.8.6/24
R5-Eth7
9.0.7.5/24
H5-3
15.0.3.1/24
AS3
Network IP:
13.0.0.0/8
R6-Eth4
9.0.7.6/24
AS6
R1-Eth4
9.0.0.1/24
R3-Eth5
9.0.1.2/24
R3-Eth7
9.0.8.5/24
AS1
Network IP:
11.0.0.0/8
Router ID:
9.0.0.3
Network IP:
11.0.0.0/8
BLOCKED
R3-Eth4
9.0.4.2/24
Router ID:
9.0.0.6
R1-Eth1
11.0.1.254/24
Router ID:
9.0.0.1
R1-Eth5
9.0.4.1/24
H6-1
11.0.1.1/24
H1-1
11.0.1.1/24
H1-2
11.0.2.1/24
H1-3
11.0.3.1/24
H3-1
13.0.1.1/24
H3-3
13.0.3.1/24
H6-2
11.0.2.1/24
H3-2
13.0.2.1/24
H6-3
11.0.3.1/24
Prefix List:
9.0.0.2
9.0.4.2
Prefix List:
9.0.1.1
9.0.4.1
9.0.3.3
9.0.5.6