Name: Kwa Li Ying
Student ID: 1003833

50.012 Networks Lab 5

(Screenshot evidences at the back of the writeup)

Topology

IP addresses of all routers:

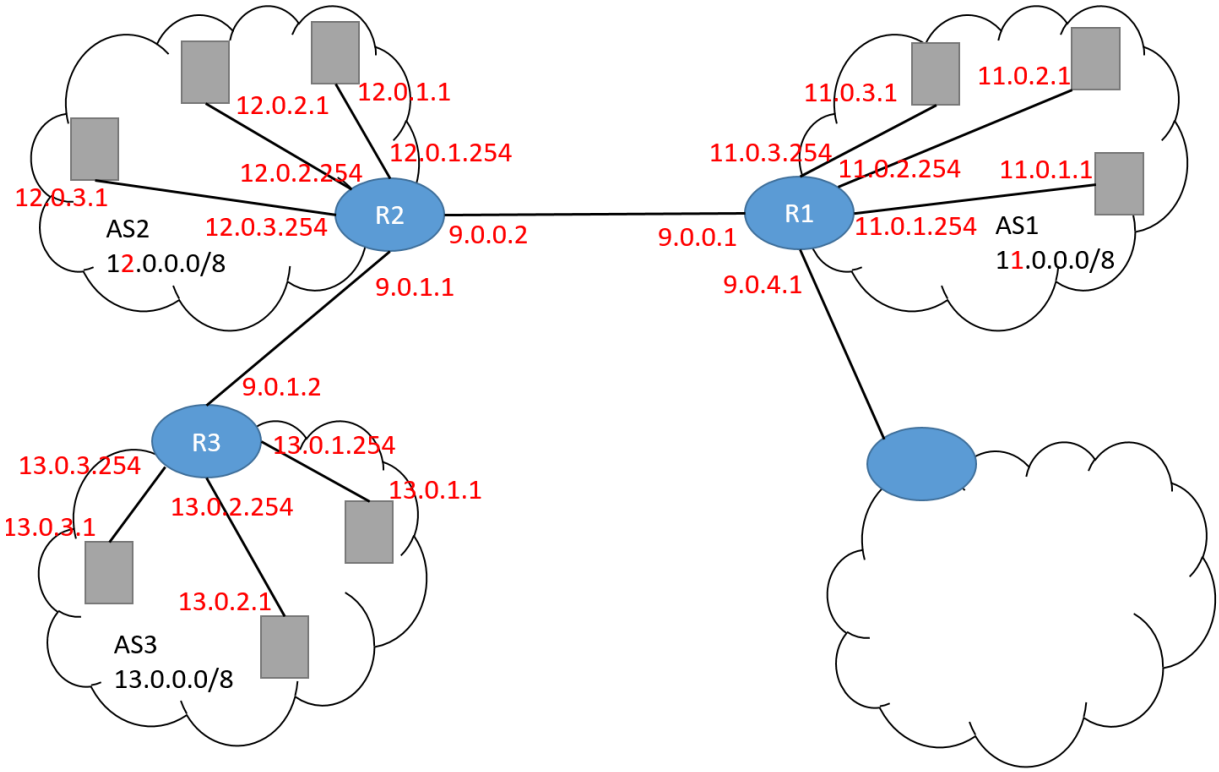
Router	Interface	IP Address
R1	R1-eth1	11.0.1.254
	R1-eth2	11.0.2.254
	R1-eth3	11.0.3.254
	R1-eth4	9.0.0.1
	R1-eth5	9.0.4.1
R2	R2-eth1	12.0.1.254
	R2-eth2	12.0.2.254
	R2-eth3	12.0.3.254
	R2-eth4	9.0.0.2
	R2-eth5	9.0.1.1
R3	R3-eth1	13.0.1.254
	R3-eth2	13.0.2.254
	R3-eth3	13.0.3.254
	R3-eth4	9.0.1.2

Hosts/IPs in all the ASs:

AS	Host	Interface	IP Address
AS1	h11	h11-eth0	11.0.1.1
	h12	h12-eth0	11.0.2.1
	h13	h13-eth0	11.0.3.1
AS2	h21	h21-eth0	12.0.1.1
	h22	h22-eth0	12.0.2.1
	h23	h23-eth0	12.0.3.1
AS3	h31	h31-eth0	13.0.1.1
	h32	h32-eth0	13.0.2.1
	h33	h33-eth0	13.0.3.1

Name: Kwa Li Ying
Student ID: 1003833

Annotated diagram:



Name: Kwa Li Ying
Student ID: 1003833

BGP Traffic

Observation (before modification)

After `clear bgp external` was executed to clear the routes, according to the wireshark's capture of packets on R1-eth0, the occasional BGP 'KEEP ALIVE' and TCP packets were stopped completely for a few seconds. Then, special packets such as BGP 'NOTIFICATION' and 'OPEN' message packets were received and the BGP connection was re-established and the occasional BGP and TCP packets resume.

During the moment where the BGP 'KEEP ALIVE' packets were stopped, h11 is unable to reach h33 (checked by executing `h11 ping h33` on the mininet console). When the BGP packets resumed the packet exchange, h11 can reach h33 again. The connection between the 2 hosts is temporarily lost when the routes were cleared because without the BGP protocol to advertise the path to hosts on the other AS, the BGP routing would not be set up and a host in AS1 would not be able to reach AS3 and vice versa.

R1 cannot reach h33 (checked by executing `R1 ping h33` on the mininet console) throughout the re-establishing routes process.

Modification

In bgpd-R2.conf, an extra line was added: "network 9.0.0.0/8".

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

hostname bgpd-R2
password zebra
enable password zebra

router bgp 2
  bgp router-id 9.0.0.2
  network 12.0.0.0/8
  network 9.0.0.0/8
  neighbor 9.0.0.1 remote-as 1
  neighbor 9.0.0.1 update-source 9.0.0.2
  neighbor 9.0.0.1 ebgp-multihop
  neighbor 9.0.0.1 next-hop-self
  neighbor 9.0.0.1 timers 5 5

  neighbor 9.0.1.2 remote-as 3
  neighbor 9.0.1.2 update-source 9.0.1.1
  neighbor 9.0.1.2 ebgp-multihop
  neighbor 9.0.1.2 next-hop-self
  neighbor 9.0.1.2 timers 5 5


log file /tmp/R2-bgpd.log

debug bgp as4
debug bgp events
debug bgp filters
debug bgp fsm
debug bgp keepalives
debug bgp updates

!
log stdout
```

Name: Kwa Li Ying
Student ID: 1003833

Observation (after modification)

Both h11 and R1 can reach h33 (checked by executing `h11 ping h33` and `R1 ping h33` respectively).

Explanation

Initially, h11 can reach h33 (13.0.1.1) but R1 cannot reach h33.

h11 can reach h33 because R3 advertises AS3's subnet (i.e. 13.0.0.0/8) to its neighbor R2 and R2 advertises this fact to R1. Thus all hosts in AS1 can reach all hosts in AS3. In fact, since all gateway routers advertise their AS's subnet to their neighbors, any host in any AS can reach any host in any other subnet.

However, R1 cannot reach h33 because R1's IP addresses are not considered part of AS1's hosts. R1's network interfaces are links to the hosts in AS1 but these interfaces (i.e. R1-eth1, R1-eth2, R1-eth3) are not hosts themselves.

In order R1 to reach a host in AS3, R2 has to advertise that it can reach both routers as hosts. This is done by adding the 9.0.0.0/8 subnet to R2's advertising, so that the BGP protocol will recognise R1's eth4 and R3's eth4 as hosts to be reached. Once this is added, hosts in AS3 can reach R1 and hosts in AS1 can reach R3.

Name: Kwa Li Ying
Student ID: 1003833

BGP Attack

Before the attack started, h11 continuously contacts a webserver on 13.0.1.1 from R1. This can be seen as the packets captured on Wireshark flow to and from 9.0.0.1 and 13.0.1.1, as well as 9.0.0.1 and 9.0.0.2 which reflect the KEEPALIVE message between R1 and R2. The website.sh script also reflects that h11 is connecting to the default webserver, and we deduce that this webserver originates from h31 in AS3 since the packets reveal that the eth4 (9.0.0.1) interface of R1 is interacting with the webserver.

After the attack started, a TCP connection between 9.0.4.1 and 9.0.4.2 was established. Soon after, packets stop flowing to and from 9.0.0.1 and 13.0.0.1, and starts slowing to and from 9.0.4.1 and 13.0.0.1. The KEEPALIVE messages now show that there is a connection between 9.0.0.1 and 9.0.0.2, as well as 9.0.4.1 and 9.0.4.2. The website.sh script now reflects that h11 is connecting to the attacker web server, and we deduce that this webserver originates from h41 in AS4 since the packets reveal that the eth5 (9.0.4.1) interface of R1 is interacting with the webserver.

The fact that h11 contacts the webserver from AS4 instead of AS3 suggests that this path has a lower cost of traversal.

Name: Kwa Li Ying
Student ID: 1003833

Screenshots

Topology

Nodes:

```
mininet> nodes
available nodes are:
R1 R2 R3 R4 c0 h11 h12 h13 h21 h22 h23 h31 h32 h33 h41 h42 h43
```

Net (network connections):

```
mininet> net
h11 h11-eth0:R1-eth1
h12 h12-eth0:R1-eth2
h13 h13-eth0:R1-eth3
h21 h21-eth0:R2-eth1
h22 h22-eth0:R2-eth2
h23 h23-eth0:R2-eth3
h31 h31-eth0:R3-eth1
h32 h32-eth0:R3-eth2
h33 h33-eth0:R3-eth3
h41 h41-eth0:R4-eth1
h42 h42-eth0:R4-eth2
h43 h43-eth0:R4-eth3
R1 R1-eth1:h11-eth0 R1-eth2:h12-eth0 R1-eth3:h13-eth0 R1-eth4:R2-eth4 R1-eth5:R4-eth4
R2 R2-eth1:h21-eth0 R2-eth2:h22-eth0 R2-eth3:h23-eth0 R2-eth4:R1-eth4 R2-eth5:R3-eth4
R3 R3-eth1:h31-eth0 R3-eth2:h32-eth0 R3-eth3:h33-eth0 R3-eth4:R2-eth5
R4 R4-eth1:h41-eth0 R4-eth2:h42-eth0 R4-eth3:h43-eth0 R4-eth4:R1-eth5
c0
```

Ifconfig (for each router):

```
mininet> R1 ifconfig
R1-eth1   Link encap:Ethernet  HWaddr 12:12:59:c3:8a:fc
          inet addr:11.0.1.254  Bcast:11.0.1.255  Mask:255.255.255.0
          inet6 addr: fe80::1012:59ff:fec3:8afc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:11 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1170 (1.1 KB)  TX bytes:1170 (1.1 KB)

R1-eth2   Link encap:Ethernet  HWaddr 02:f9:31:73:d2:5d
          inet addr:11.0.2.254  Bcast:11.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::f9:31ff:fe73:d25d/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 a6:10:0b:a0:5c:c4
          inet addr:11.0.3.254  Bcast:11.0.3.255  Mask:255.255.255.0
          inet6 addr: fe80::a410:bff:fea0:5cc4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:11 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:1170 (1.1 KB)  TX bytes:648 (648.0 B)

R1-eth4   Link encap:Ethernet  HWaddr e2:9b:0a:d7:e9:2b
          inet addr:9.0.0.1  Bcast:9.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::e09b:aff:fed7:e92b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2486 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3055 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:197895 (197.8 KB)  TX bytes:235346 (235.3 KB)

R1-eth5   Link encap:Ethernet  HWaddr 76:f6:17:8b:10:76
          inet addr:9.0.4.1  Bcast:9.0.4.255  Mask:255.255.255.0
          inet6 addr: fe80::74f6:17ff:fe8b:1076/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10 errors:0 dropped:0 overruns:0 frame:0
          TX packets:100 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:828 (828.0 B)  TX bytes:4608 (4.6 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:45 errors:0 dropped:0 overruns:0 frame:0
          TX packets:45 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3960 (3.9 KB)  TX bytes:3960 (3.9 KB)
```

```
mininet> R2 ifconfig
R2-eth1   Link encap:Ethernet  HWaddr f6:4c:37:1c:a5:c0
          inet addr:12.0.1.254  Bcast:12.0.1.255  Mask:255.255.255.0
          inet6 addr: fe80::f44c:37ff:fe1c:a5c0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:11 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1170 (1.1 KB)  TX bytes:1170 (1.1 KB)

R2-eth2   Link encap:Ethernet  HWaddr 36:92:86:ec:79:3d
          inet addr:12.0.2.254  Bcast:12.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::3492:86ff:feec:793d/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 ca:7f:47:15:f3:6e
          inet addr:12.0.3.254  Bcast:12.0.3.255  Mask:255.255.255.0
          inet6 addr: fe80::c87f:47ff:fe15:f36e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:11 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1170 (1.1 KB)  TX bytes:1170 (1.1 KB)

R2-eth4   Link encap:Ethernet  HWaddr 7e:4f:4c:09:c9:32
          inet addr:9.0.0.2  Bcast:9.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::7c4f:4cff:fe09:c932/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3469 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2835 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:267230 (267.2 KB)  TX bytes:225489 (225.4 KB)

R2-eth5   Link encap:Ethernet  HWaddr 9e:f1:27:d7:6f:30
          inet addr:9.0.1.1  Bcast:9.0.1.255  Mask:255.255.255.0
          inet6 addr: fe80::9cf1:27ff:fed7:6f30/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3471 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2846 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:267026 (267.0 KB)  TX bytes:225891 (225.8 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)
```

Name: Kwa Li Ying
Student ID: 1003833

```
mininet> R3 ifconfig
R3-eth1   Link encap:Ethernet  HWaddr ca:2e:8c:bf:c4:08
          inet addr:13.0.1.254  Bcast:13.0.1.255  Mask:255.255.255.0
          inet6 addr: fe80::c82e:8cff:febf:c408/64 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 8e:d9:0a:d2:80:36
          inet addr:13.0.2.254  Bcast:13.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::8cd9:aff:fed2:8036/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:11 errors:0 dropped:2 overruns:0 frame:0
          TX packets:11 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1170 (1.1 KB)  TX bytes:1170 (1.1 KB)

R3-eth3   Link encap:Ethernet  HWaddr b2:04:7a:b7:58:9f
          inet addr:13.0.3.254  Bcast:13.0.3.255  Mask:255.255.255.0
          inet6 addr: fe80::b004:7aff:feb7:589f/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 7a:21:88:90:3c:0c
          inet addr:9.0.1.2  Bcast:9.0.1.255  Mask:255.255.255.0
          inet6 addr: fe80::7821:88ff:fe90:3c0c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3537 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4367 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:280978 (280.9 KB)  TX bytes:335643 (335.6 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: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)
```

```
mininet> R4 ifconfig
R4-eth1   Link encap:Ethernet  HWaddr 72:58:91:f4:2b:b7
          inet6 addr: fe80::7058:91ff:fef4:2bb7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:11 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1170 (1.1 KB)  TX bytes:1170 (1.1 KB)

R4-eth2   Link encap:Ethernet  HWaddr 5a:5d:29:97:d8:d2
          inet6 addr: fe80::585d:29ff:fe97:d8d2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:11 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:906 (906.0 B)  TX bytes:1170 (1.1 KB)

R4-eth3   Link encap:Ethernet  HWaddr 3a:77:11:90:91:bf
          inet6 addr: fe80::3877:11ff:fe90:91bf/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:11 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10 errors:0 dropped:1 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1170 (1.1 KB)  TX bytes:1080 (1.0 KB)

R4-eth4   Link encap:Ethernet  HWaddr fa:f6:c1:7c:77:26
          inet6 addr: fe80::f8f6:c1ff:fe7c:7726/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:136 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6120 (6.1 KB)  TX bytes:828 (828.0 B)
```

Ifconfig (for each node)

```
mininet> h11 ifconfig
h11-eth0  Link encap:Ethernet  HWaddr 5e:71:d2:ba:8e:3d
          inet addr:11.0.1.1  Bcast:11.0.1.255  Mask:255.255.255.0
          inet6 addr: fe80::5c71:d2ff:feba:8e3d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:11 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1170 (1.1 KB)  TX bytes:1170 (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: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)
```

```
mininet> h12 ifconfig
h12-eth0  Link encap:Ethernet  HWaddr ca:1d:59:78:3c:de
          inet addr:11.0.2.1  Bcast:11.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::c81d:59ff:fe78:3cde/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)
```

```
mininet> h13 ifconfig
h13-eth0  Link encap:Ethernet  HWaddr 0e:cb:0f:93:d0:ce
          inet addr:11.0.3.1  Bcast:11.0.3.255  Mask:255.255.255.0
          inet6 addr: fe80::ccb:fff:fe93:d0ce/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:648 (648.0 B)  TX bytes:1170 (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: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)
```

```
mininet> h21 ifconfig
h21-eth0  Link encap:Ethernet  HWaddr 56:65:08:44:08:62
          inet addr:12.0.1.1  Bcast:12.0.1.255  Mask:255.255.255.0
          inet6 addr: fe80::5465:8ff:fe44:862/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:11 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1170 (1.1 KB)  TX bytes:1170 (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: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)
```

```
mininet> h22 ifconfig
h22-eth0  Link encap:Ethernet  HWaddr 22:20:c4:07:20:75
          inet addr:12.0.2.1  Bcast:12.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::2020:c4ff:fe07:2075/64 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)
```

```
mininet> h23 ifconfig
h23-eth0  Link encap:Ethernet  HWaddr 16:91:98:04:14:0c
          inet addr:12.0.3.1  Bcast:12.0.3.255  Mask:255.255.255.0
          inet6 addr: fe80::1491:98ff:fe04:140c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:11 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1170 (1.1 KB)  TX bytes:1170 (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: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)
```

Name: Kwa Li Ying
Student ID: 1003833

```
h31-eth0  Link encap:Ethernet  HWaddr 52:da:c4:b5:81:ed
          inet addr:13.0.1.1  Bcast:13.0.1.255  Mask:255.255.255.0
          inet6 addr: fe80::50da:c4ff:feb5:81ed/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)
```

```
mininet> h32 ifconfig
h32-eth0  Link encap:Ethernet  HWaddr 16:df:87:86:76:d7
          inet addr:13.0.2.1  Bcast:13.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::14df:87ff:fe86:76d7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:11 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11 errors:0 dropped:1 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1170 (1.1 KB)  TX bytes:1170 (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: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)
```

```
mininet> h33 ifconfig
h33-eth0  Link encap:Ethernet  HWaddr 26:f8:f9:53:d0:da
          inet addr:13.0.3.1  Bcast:13.0.3.255  Mask:255.255.255.0
          inet6 addr: fe80::24f8:f9ff:fe53:d0da/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)
```

Name: Kwa Li Ying
Student ID: 1003833

BGP Traffic

h11 pinging h33 (before modification):

```
mininet> h11 ping h33
PING 13.0.3.1 (13.0.3.1) 56(84) bytes of data.
From 11.0.1.254 icmp_seq=1 Destination Net Unreachable
From 11.0.1.254 icmp_seq=2 Destination Net Unreachable
^C
--- 13.0.3.1 ping statistics ---
10 packets transmitted, 0 received, +2 errors, 100% packet loss, time 9000ms
```

```
mininet> h11 ping h33
PING 13.0.3.1 (13.0.3.1) 56(84) bytes of data.
64 bytes from 13.0.3.1: icmp_seq=4 ttl=61 time=0.113 ms
64 bytes from 13.0.3.1: icmp_seq=5 ttl=61 time=0.043 ms
64 bytes from 13.0.3.1: icmp_seq=6 ttl=61 time=0.106 ms
64 bytes from 13.0.3.1: icmp_seq=7 ttl=61 time=0.058 ms
^C
--- 13.0.3.1 ping statistics ---
7 packets transmitted, 4 received, 42% packet loss, time 6023ms
rtt min/avg/max/mdev = 0.043/0.080/0.113/0.030 ms
```

R1 pinging h33 (before modification):

```
mininet> R1 ping h33
^CPING 13.0.3.1 (13.0.3.1) 56(84) bytes of data.

--- 13.0.3.1 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 999ms
```

bgpd show ip bgp (before modification):

```
bgpd-R1# show 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         9.0.0.2                                0 2 3 i

Total number of prefixes 3
```

h11 pinging h33 (after modification):

```
mininet> h11 ping h33
PING 13.0.3.1 (13.0.3.1) 56(84) bytes of data.
64 bytes from 13.0.3.1: icmp_seq=1 ttl=61 time=0.091 ms
^C
--- 13.0.3.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.091/0.091/0.091/0.000 ms
```

Name: Kwa Li Ying
Student ID: 1003833

R1 pinging h33 (after modification):

```
mininet> R1 ping h33
PING 13.0.3.1 (13.0.3.1) 56(84) bytes of data.
64 bytes from 13.0.3.1: icmp_seq=1 ttl=62 time=0.036 ms
64 bytes from 13.0.3.1: icmp_seq=2 ttl=62 time=0.046 ms
^C
--- 13.0.3.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.036/0.041/0.046/0.005 ms
```

bgpd show ip bgp (after modification):

```
bgpd-R1# show 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
*> 9.0.0.0          9.0.0.2                  0             0 2 i
*> 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         9.0.0.2                                0 2 3 i

Total number of prefixes 4
```

Name: Kwa Li Ying
Student ID: 1003833

BGP Attack

Connecting to the website (before the attack):

```
bowen@bowen-VirtualBox:~/Documents/lab5$ ./website.sh R1
Wed Dec 2 15:01:06 SGT 2020 -- <h1>Default web server</h1>
Wed Dec 2 15:01:07 SGT 2020 -- <h1>Default web server</h1>
Wed Dec 2 15:01:08 SGT 2020 -- <h1>Default web server</h1>
Wed Dec 2 15:01:09 SGT 2020 -- <h1>Default web server</h1>
Wed Dec 2 15:01:10 SGT 2020 -- <h1>Default web server</h1>
Wed Dec 2 15:01:11 SGT 2020 -- <h1>Default web server</h1>
Wed Dec 2 15:01:13 SGT 2020 -- <h1>Default web server</h1>
Wed Dec 2 15:01:14 SGT 2020 -- <h1>Default web server</h1>
Wed Dec 2 15:01:15 SGT 2020 -- <h1>Default web server</h1>
Wed Dec 2 15:01:16 SGT 2020 -- <h1>Default web server</h1>
Wed Dec 2 15:01:17 SGT 2020 -- <h1>Default web server</h1>
```

Packet capture on R1 (before the attack):

No.	Time	Source	Destination	Protocol	Length	Info
157	6.516568778	13.0.1.1	9.0.0.1	HTTP	96	Continuation
158	6.516569585	9.0.0.1	13.0.1.1	TCP	68	40366 → 80 [ACK] Seq=73 Ack=147 Win=29696 Len=…
159	6.516650201	13.0.1.1	9.0.0.1	TCP	68	80 → 40366 [FIN, ACK] Seq=147 Ack=73 Win=29184…
160	6.517530430	9.0.0.1	13.0.1.1	TCP	68	40366 → 80 [FIN, ACK] Seq=73 Ack=148 Win=29696…
161	6.517566804	13.0.1.1	9.0.0.1	TCP	68	80 → 40366 [ACK] Seq=148 Ack=74 Win=29184 Len=…
162	7.048134691	9.0.0.1	9.0.0.2	BGP	87	KEEPALIVE Message
163	7.048159890	9.0.0.2	9.0.0.1	TCP	68	59909 → 179 [ACK] Seq=134 Ack=153 Win=58 Len=0…
164	7.048400676	9.0.0.2	9.0.0.1	BGP	87	KEEPALIVE Message
165	7.087653342	9.0.0.1	9.0.0.2	TCP	68	179 → 59909 [ACK] Seq=153 Ack=153 Win=57 Len=0…
166	7.686705508	9.0.0.1	13.0.1.1	TCP	76	40367 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=146…
167	7.686737359	13.0.1.1	9.0.0.1	TCP	76	80 → 40367 [SYN, ACK] Seq=0 Ack=1 Win=28960 Le…
168	7.686745251	9.0.0.1	13.0.1.1	TCP	68	40367 → 80 [ACK] Seq=1 Ack=1 Win=29696 Len=0 T…
169	7.692647016	9.0.0.1	13.0.1.1	HTTP	140	GET / HTTP/1.1
170	7.692680989	13.0.1.1	9.0.0.1	TCP	68	80 → 40367 [ACK] Seq=1 Ack=73 Win=29184 Len=0 …

Packet capture on R1 (DURING the attack):

230	9.831180687	9.0.0.1	13.0.1.1	TCP	68	40369 → 80 [FIN, ACK] Seq=73 Ack=148 Win=29696…
231	9.831191050	13.0.1.1	9.0.0.1	TCP	68	80 → 40369 [ACK] Seq=148 Ack=74 Win=29184 Len=…
232	10.052709742	9.0.0.1	9.0.0.2	BGP	87	KEEPALIVE Message
233	10.052878472	9.0.0.2	9.0.0.1	BGP	87	KEEPALIVE Message
234	10.052882010	9.0.0.1	9.0.0.2	TCP	68	179 → 59909 [ACK] Seq=210 Ack=210 Win=57 Len=0…
235	10.850931664	9.0.4.2	9.0.4.1	TCP	76	46882 → 179 [SYN] Seq=0 Win=29200 Len=0 MSS=14…
236	10.850956231	9.0.4.1	9.0.4.2	TCP	76	179 → 46882 [SYN, ACK] Seq=0 Ack=1 Win=28960 L…
237	10.850969740	9.0.4.2	9.0.4.1	TCP	68	46882 → 179 [ACK] Seq=1 Ack=1 Win=29696 Len=0 …
238	10.851032699	9.0.4.2	9.0.4.1	BGP	121	OPEN Message
239	10.851035757	9.0.4.1	9.0.4.2	TCP	68	179 → 46882 [ACK] Seq=1 Ack=54 Win=29184 Len=0…
240	10.851233746	9.0.4.1	9.0.4.2	BGP	140	OPEN Message, KEEPALIVE Message
241	10.851240309	9.0.4.2	9.0.4.1	TCP	68	46882 → 179 [ACK] Seq=54 Ack=73 Win=29696 Len=…
242	10.851341586	9.0.4.2	9.0.4.1	BGP	106	KEEPALIVE Message, KEEPALIVE Message
243	10.851397077	9.0.4.1	9.0.4.2	BGP	87	KEEPALIVE Message

Connecting to the website (after the attack):

```
Wed Dec 2 15:01:35 SGT 2020 -- <h1>Default web server</h1>
Wed Dec 2 15:01:36 SGT 2020 -- <h1>Default web server</h1>
Wed Dec 2 15:01:37 SGT 2020 -- <h1>Default web server</h1>
Wed Dec 2 15:01:38 SGT 2020 -- <h1>*** Attacker web server ***</h1>
Wed Dec 2 15:01:39 SGT 2020 -- <h1>*** Attacker web server ***</h1>
Wed Dec 2 15:01:40 SGT 2020 -- <h1>*** Attacker web server ***</h1>
Wed Dec 2 15:01:41 SGT 2020 -- <h1>*** Attacker web server ***</h1>
Wed Dec 2 15:01:42 SGT 2020 -- <h1>*** Attacker web server ***</h1>
Wed Dec 2 15:01:43 SGT 2020 -- <h1>*** Attacker web server ***</h1>
Wed Dec 2 15:01:45 SGT 2020 -- <h1>*** Attacker web server ***</h1>
Wed Dec 2 15:01:46 SGT 2020 -- <h1>*** Attacker web server ***</h1>
Wed Dec 2 15:01:47 SGT 2020 -- <h1>*** Attacker web server ***</h1>
Wed Dec 2 15:01:48 SGT 2020 -- <h1>*** Attacker web server ***</h1>
Wed Dec 2 15:01:49 SGT 2020 -- <h1>*** Attacker web server ***</h1>
```

Packet capture on R1 (after the attack):

263	10.879009627	13.0.1.1	9.0.0.1	TCP	68	80 → 40371 [ACK] Seq=148 Ack=74 Win=29184 Len=…
264	10.887910928	9.0.4.2	9.0.4.1	TCP	68	46882 → 179 [ACK] Seq=92 Ack=92 Win=29696 Len=…
265	11.053428517	9.0.0.1	9.0.0.2	BGP	87	KEEPALIVE Message
266	11.053569126	9.0.0.2	9.0.0.1	BGP	87	KEEPALIVE Message
267	11.053571986	9.0.0.1	9.0.0.2	TCP	68	179 → 59909 [ACK] Seq=229 Ack=229 Win=57 Len=0…
268	11.852882606	9.0.4.1	9.0.4.2	BGP	246	KEEPALIVE Message, UPDATE Message, UPDATE Mess…
269	11.852899937	9.0.4.2	9.0.4.1	TCP	68	46882 → 179 [ACK] Seq=92 Ack=270 Win=30720 Len…
270	11.853141473	9.0.4.2	9.0.4.1	BGP	140	KEEPALIVE Message, UPDATE Message
271	11.891512324	9.0.4.1	9.0.4.2	TCP	68	179 → 46882 [ACK] Seq=270 Ack=164 Win=29184 Le…
272	11.903659890	9.0.4.1	9.0.4.2	BGP	93	UPDATE Message
273	11.919187350	9.0.4.1	13.0.1.1	TCP	76	37430 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=146…
274	11.919213847	13.0.1.1	9.0.4.1	TCP	76	80 → 37430 [SYN, ACK] Seq=0 Ack=1 Win=28960 Le…
275	11.919222213	9.0.4.1	13.0.1.1	TCP	68	37430 → 80 [ACK] Seq=1 Ack=1 Win=29696 Len=0 T…
276	11.919335734	9.0.4.1	13.0.1.1	HTTP	140	GET / HTTP/1.1