SUTD 2021 50.012 Lab 5 Writeup Submission Document

> Project Group 2 Members:
>
> - James Raphael Tiovalen / 1004555
> - Velusamy Sathiakumar Ragul Balaji / 1004101
> - Han Xing Yi / 1004330
> - Huang He / 1004561
> - Qiao Yingjie / 1004514
> - Zhang Peiyuan / 1004539

Submission Answers

Topology

IP addresses of all routers:

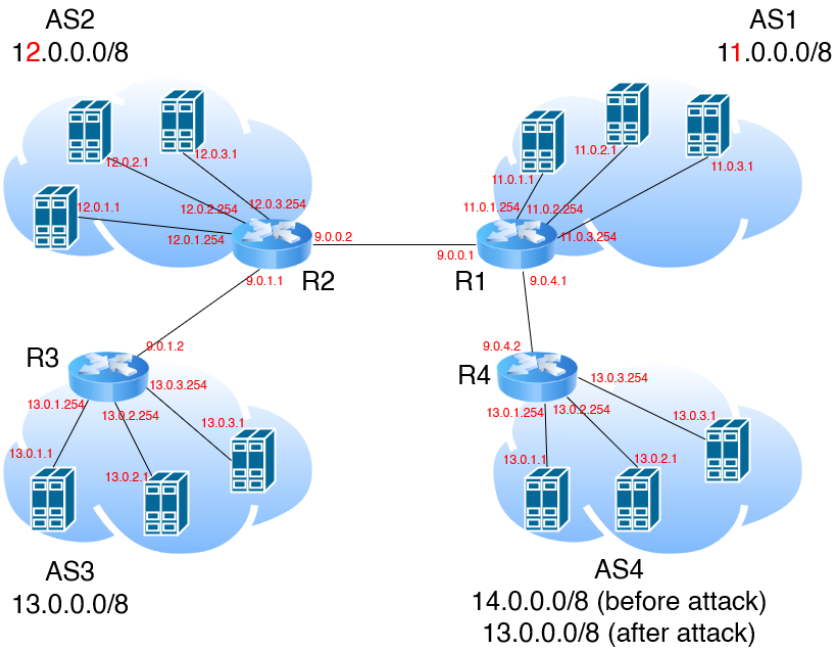
Router	Interface	IP Address
R1	R1-eth1	11.0.1.254
	R1-eth2	11.0.2.254
	R1-eth3	11.0.3.254
	R1-eth4	9.0.0.1
	R1-eth5	9.0.4.1
R2	R2-eth1	12.0.1.254
	R2-eth2	12.0.2.254
	R2-eth3	12.0.3.254
	R2-eth4	9.0.0.2
	R2-eth5	9.0.1.1
R3	R3-eth1	13.0.1.254
	R3-eth2	13.0.2.254
	R3-eth3	13.0.3.254
	R3-eth4	9.0.1.2

Router	Interface	IP Address
R4	R4-eth1	13.0.1.254
	R4-eth2	13.0.2.254
	R4-eth3	13.0.3.254
	R4-eth4	9.0.4.2

Hosts/IPs in the ASes:

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
AS4	h41	h41-eth0	13.0.1.1
	h42	h42-eth0	13.0.2.1
	h43	h43-eth0	13.0.3.1

Topology Diagram:



BGP Traffic

Before the `clear bgp external` command was executed, according to the Wireshark packet capture log on the `R1-eth4` interface, there is a constant stream of bidirectional BGP KEEPALIVE and TCP packets being periodically sent between `9.0.0.1` and `9.0.0.2`. After the `clear bgp external` command was executed on router R1, the occasional sending of BGP KEEPALIVE and TCP packets were stopped completely for a few seconds. Then, special BGP NOTIFICATION and BGP OPEN message packets were transmitted from `9.0.0.1` to `9.0.0.2` and back, and BGP UPDATE packets were sent between `9.0.1.1` and `9.0.1.2`, after which, the BGP connection was re-established and the occasional normal stream of BGP KEEPALIVE and TCP packets resume.

During the period whereby the BGP KEEPALIVE packets were not being sent, h11 was unable to reach h31 (`13.0.1.1`) and h33 (`13.0.3.1`) (which can be checked by executing the `h11 ping h31` and `h11 ping h33` commands on the Mininet console and which would print `Destination Net Unreachable` log messages). When the stream of BGP KEEPALIVE exchange packets resume, h11 was able to reach both h31 and h33 again. The connection between the hosts was temporarily lost when the routes were cleared because without the BGP protocol advertising the path to hosts located in other ASes, the BGP routing would not be set up and thus any hosts in AS1 would not be able to reach any hosts in AS3, and vice versa.

Throughout the BGP route traffic re-establishment process, R1 was not able to reach h31 and h33 (which can be checked by executing the `R1 ping h31` and `R1 ping h33` commands on the Mininet console). During the period whereby BGP KEEPALIVE packets were not being sent, a `Network is unreachable` error message was displayed, whereas during the normal period whereby BGP KEEPALIVE packets were sent, the console was simply stuck after executing the `R1 ping h31` and `R1 ping h33` commands without any output being returned.

To fix this, we add the line `network 9.0.0.0/8` to the `bgpd-R2.conf` BGP configuration file. After this modification, both h11 and R1 are now able to reach both h31 and h33 by running the aforementioned `ping` commands.

Initially, before the fix, h11 was able to reach h31 and h33, but R1 was not able to reach h31 and h33. h11 could reach h31 and h33 because R3 advertises AS3's subnet (`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 corresponding subnet to their neighbors, any host in any AS can reach any host in any other AS.

However, R1 cannot reach h31 and h33 because R1's IP addresses are not considered to be part of AS1's hosts. R1's network interfaces are links to the hosts in AS1, but these interfaces (`R1-eth1`, `R1-eth2`, `R1-eth3`) are not hosts themselves.

In order for R1 to be able to reach h31 and h33 (or any host in AS3, for that matter), R2 has to advertise that it can reach both routers as hosts. This can be done by adding the `9.0.0.0/8` subnet to R2's advertisement messages, so that the BGP protocol will recognize `R1-eth4` and `R3-eth4` as hosts that can be reached. Once this is added, hosts in AS3 can reach R1 and hosts in AS1 can reach R3.

BGP Attack

Before the attack was executed, h11 continuously contacts a webserver on 13.0.1.1 from R1. This can be seen from the TCP and HTTP data packets captured on Wireshark flowing to and from `9.0.0.1` and `13.0.1.1`, as well as the usual periodic BGP KEEPALIVE messages between `9.0.0.1` (R1) and `9.0.0.2` (R2). The `website.sh` script also reflects that h11 is connecting to the default web server, and we can deduce that this webserver originates from h31 (`13.0.1.1`) in AS3 since the packets reveal that the `R1-eth4` interface (`9.0.0.1`) is interacting with the webserver.

To execute the BGP spoofing/hijacking attack, we modify the `network 14.0.0.0/8` line in the `bgpd-R4.conf` file to `network 13.0.0.0/8`.

After the attack started (by executing the `start_rogue.sh` script), a TCP connection consisting of several TCP and BGP OPEN packets between `9.0.4.1` and `9.0.4.2` was established. Soon after, several BGP UPDATE packets were sent between `9.0.4.1` and `9.0.4.2`, after which, data packets between `9.0.0.1` and `13.0.1.1` stop being transmitted/transferred, while data packets between `9.0.4.1` and `13.0.1.1` start flowing. The BGP KEEPALIVE messages now indicate that there is a connection between `9.0.0.1` and `9.0.0.2`, as well as between `9.0.4.1` and `9.0.4.2`. The `website.sh` script also 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 `R1-eth5` interface (`9.0.4.1`) is interacting with the webserver.

The fact that h11 prefers to contact the webserver from AS4 instead of from AS4 possibly suggests that this path has a lower traversal cost.

After the attack was stopped (by executing the `stop_rogue.sh` script), several TCP packets were sent between `9.0.4.1` and `9.0.4.2` to close the TCP connection, after which several BGP UPDATE packets were sent between `9.0.0.1` and `9.0.0.2`, and then the traffic was restored back to normal (i.e., h11 would contact the default web server in AS3 once more).