**50.012 Networks Lab 5 Group 11**

Victoria Yong | 1004455

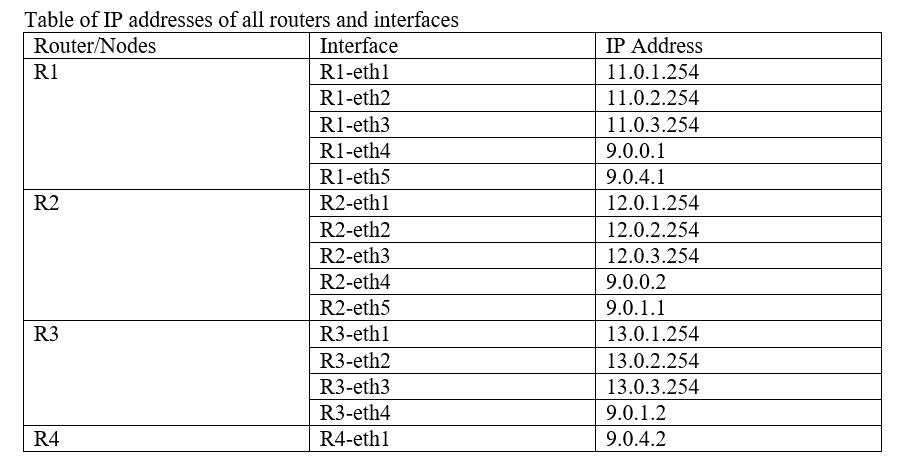
Leon Tjandra | 1004353

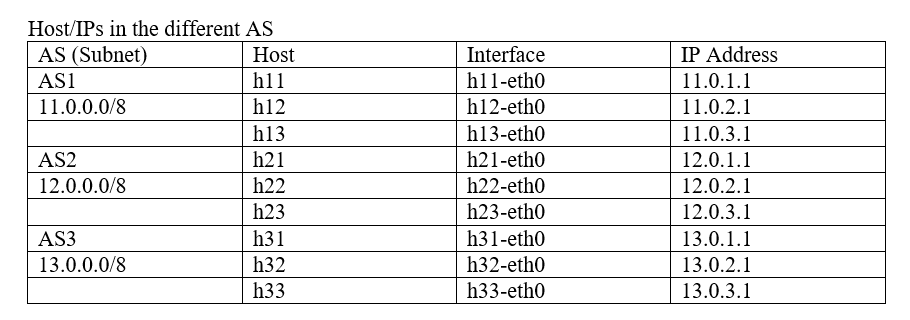
Ivan Tandyajaya | 1004572

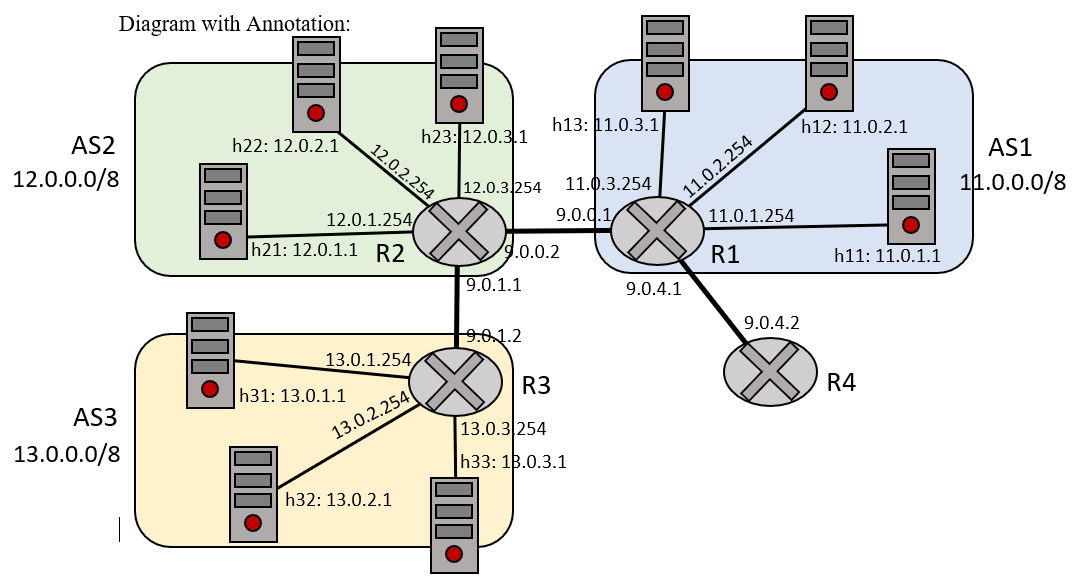
Daniel Tan |1004375

Joshua Samjaya | 1004423

**Q1. Network Topology**

****





**Q2. Describe in detail the BGP traffic you were able to observe during re-establishment of routes.**

After performing the clear bgp external command, which causes the exchange of FIN packets to close the connection between R1 interfaces, the network attempts re-establishment of routes. After a few moments, the BGP connection will be reestablished when R1 sends out SYN packets to R2 through interface R1-eth4, requesting for a connection. Upon successful establishment of the connection between R1 and R2, BGP KEEP-ALIVE and TCP packets will be exchanged once more. During the re-establishment of routes, the host h11 is unable to reach h33 since the BGP connection is stopped for a while, the AS reachability will not be able to be broadcasted.

**Q3. Was it initially possible to reach 13.0.1.1 from AS1 (h11 and R1, respectively)? If it didn’t work initially, what caused that and what did you do to fix it?**

**a. From h11, try to reach h33. Does it work? If no, why not?**

=> R1 is able to reach h33.

The BGP protocol allows broadcasting of the subnet/AS reachability information, thus host h11 which is part of subnet AS1 is able to reach any host in AS2 and AS3 and this includes h33 because the routers R1, R2 and R3 broadcasts their own subnet reachability information to its neighboring routers, this also means any host in any of the 3 AS can reach any other host in any of the 3 AS and knows their IP addresses.

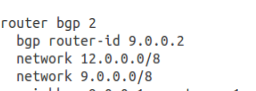
**b. From R1, try to reach 13.0.1.1. Does it work? If no, why not?**

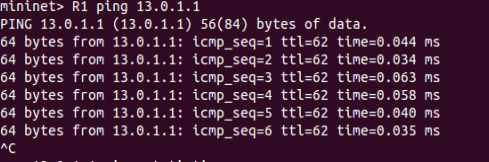
=> R1 is unable to reach the IP address 13.0.1.1 which is the IP address of h33.

Previously, when considering h11 to h33, the hosts in AS1 are able to reach a host in AS3 because the AS reachability information is broadcasted since the interface of router R1 is not considered a host in AS1.

**C. Modify the configuration files to allow R1 to reach 13.0.1.1.**

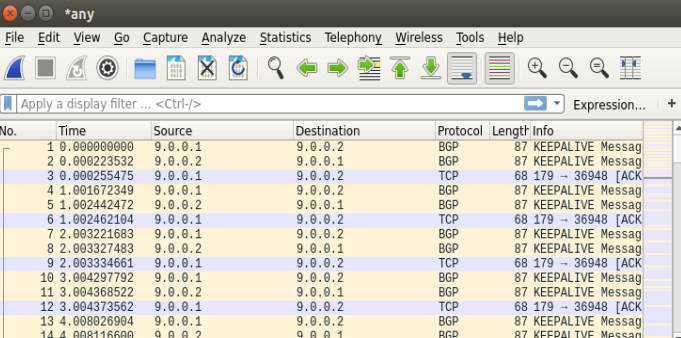
To help R1 to reach 13.0.1.1 we modified the file bgpd-R2.conf and added the line: network 9.0.0.0/8 which will make R2 recognize that the new “subnet” are hosts, that includes the interfaces within that address space. This allows R1’s interfaces, specifically R1-eth4 and R1-eth5, to receive the 13.0.0.0/8 subnet addresses advertised by R3 through R2 since it is now considered a host as well.



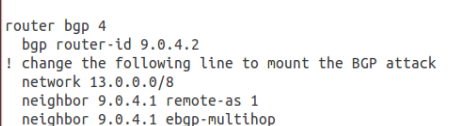


**Q4. Describe in detail what happened when you started the attack on BGP.**

Before bgpd-R4.conf was modified and the attack was not yet carried out, we can observe that a host in AS1 continuously contacts the webserver on 13.0.1.1 from router R1. We can verify this by looking at the Wireshark captured files in R1 interfaces, which shows exchanging BGP KEEP-ALIVE packets and TCP packets between R1 and R2, as well as by looking at the output of ./website.sh.



The attacker resides in AS4. We modified bgpd-R4.conf, by changing the line: network 14.0.0.0/8 into network 13.0.0.0/8, to spoof and broadcast AS4 (attacker AS) as AS3 in hopes of redirecting the host in AS1 into the attacker website instead, trying to make the next hop to be AS4 instead of AS2. The idea is to generate a shorter hop path traversal which redirects to AS4 instead of going to AS2. The modified config snippet is provided below:



After the attack using ./start\_rogue is carried out, we monitor the Wireshark packets. From the Wireshark capture below, we can see that a TCP connection has been established between the host in AS1 through the interface 9.0.4.1 and the interface 9.0.4.2 in AS4 indicating that there is some form of redirection of messages from host in AS1 to the attacker. More packets will be redirected to the destination 9.0.4.2 instead of 9.0.0.2 and this is indicated by more BGP KEEPALIVE messages which have the destination 9.0.4.2 instead of 9.0.0.2. By running ./website.sh, we can see that the host in AS1 contacted the attacker’s website instead of the actual website at 13.0.1.1.

