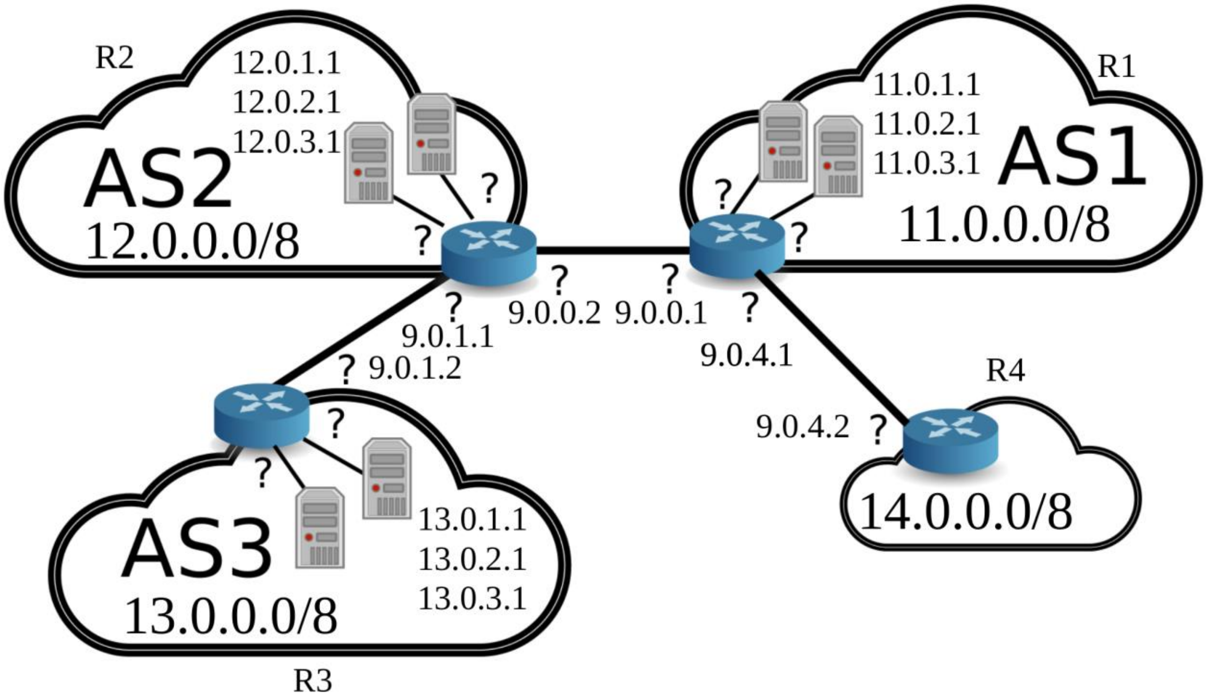
Dabin Lee | 1000727 |50.012 Networks Lab 5

1. The topology of the network



2. What was it initially not possible to reach 13.0.1.1 from AS1? How did you find out/ what did you do to fix this?

   It was not possible to reach 13.0.1.1 form AS1 because of the BGP configuration of RS2. The only way to arrive at 13.0.1.1 (AS3) is to pass by R2(AS2) and the BGP configuration of R2(AS2) only informed other routers its ability to connect to AS1.The following lines were added to inform other routers about R2(AS2)'s ability to connect to R3(AS3) and R1(AS1).

   ```
   network 12.0.0.0/8
   network 9.0.0.0/24
   network 9.0.1.0/24
   ```

3. Describe the BGP traffic you were able to observe during re-establishment of routes.

   The BGP traffics starts with few exchanges of the *OPEN Message* and *NOTIFICATION Message* between R1 and R2. Then, both of Routers enter *OpenConfirm State* and eventually enter *Established State* with the exchange of *KEEPALIVE Message*. Then R2 and R1 exchanges *UPDATE Message* containing *Network Layer Reachability Information (NLRI)*. R2 sends R1 NLRI of *13.0.0.0/8*, *9.0.0.0/24*, *9.0.1.0/24* and *12.0.0.0/8*. R1 sends R2 NLRI of *9.0.0.0/24* and *11.0.0.0/8*. R2 and R1 exchange *KEEPALIVE Message* every second.

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

   When the attack.sh was executed, R4 sent the *OPEN Message* to R1. After few changes of *KEEPALIVE Messages*, R4 sends *UDPATE Message* with *NLRI* of *13.0.0.0/8* and *14.0.0.0/8*. After this, TCP packets which were originally sent to real 13.0.1.1 through 9.0.0.1 are redirected to attacker’s 13.0.1.1 through 9.0.4.1. The route from R1 to 13.0.1.1 changed from via R2 to via R4.