Project 4 Extra Credit

- **A brief summary of how your solution counters the attack**
    a. My solution implements MD5 authentication at the router level, using Quagga. Basically, each router shares a secret password to ensure that the messages between them are authentic and prevent fraudulent connections from attacker autonomous systems. MD5 authentication will prevent the interference with the routing tables when authentic peer relationships are established; thus, preventing prefix hijacking.
- A list of files you modified from Part 3 or created in order to implement the countermeasure.
    a. The files modified were the bgpd-R (X).conf files for each router. I also added connect5.sh for conveniently connection to AS5, which is the AS, whose routing table changes when the Rogue AS starts the attack.
- **A brief description of what is changed in each file, (or the purpose of newly created files) including how it functions as a part of the larger system.**
    a. Quagga provides out of the box configuration for MD5 authentication between peers, based on RFC2385 by using the command: neighbor <<ip-address>> password <<pass>>
- **Instructions for demonstrating the countermeasure, including instructions for installing required software / libraries.**
    a. Unzip eplaza3_Project5_Part4
    b. Open a terminal window: **sudo python bgp.py**
    c. Open another terminal window: **./connect5.sh**, then run **sh ip bgp** to see the routing table before the rogue attack starts.
    d. Open another terminal window and run: **./website.sh**
    e. Open another terminal window: **./start_rogue.sh**
    f. Rerun **sh ip bgp** in the terminal where you ran **./connect5.sh** to see that the routing table does not contain an entry for **9.0.6.1**, which is the attacker AS address.
    g. Additionally, you can go back to terminal 3 where you ran **./website.sh** and you will not see **Attacker web server** message in the console.
- **A brief closing containing any additional information the grader may need to reproduce your countermeasure and contact information (if different than your GT student email address) in case the grade has questions.**
    a. The countermeasure can be ran by executing the steps details above. For more information, you may also refer to page 2 of the assignment where the rogue attack details are explained. In case, you run into any problems, please email me at elsamrodco@gatech.edu