**Lab Assignment 07:**

**Running BGP**

Micah Flack

Department of Computer Science, Dakota State University

CSC-840-DT1, Cyber Operations I

Dr. Michael Ham

October 11, 2022

**Take a screenshot of your network diagram.**

Graphical user interface, application

Description automatically generated

**Show AS1000s routing table; it should have a BGP route pointing to the 2001:23:23:23::/64 network.**

Text

Description automatically generated

**Take a screenshot of your successful pings from AS1000 to 2001:23:23:23::2**

Graphical user interface, text

Description automatically generated

**Using vtysh, show the MD5 authentication in your AS2000 and AS3000**

Text

Description automatically generated

I’m assuming that the part we are looking for as “verification” is the line that indicates:

“Peer Authentication Enabled”. I don’t know how else to show this other than the commands used.

> vtysh

ns# configure terminal

ns(config)#router bgp 2000

ns(config-router)#neighbor 2001:23:23:23::2 remote-as 3000

ns(config-router)#neighbor 2001:23:23:23::2 password “micahflack”

ns(config-router)#redistribute kernel

ns(config-router)#exit

And then vice versa for the pfsense-3000 going to the 2000 box. This does break route advertisement from AS2000 to AS1000 for the 2001:23:23:23::/64 route though.

**On AS3000, look at the BGP IPv6 Routes (pfSense web interface Services → FRR BGP → Status → BGP IPv6 Routes). AS3000 should think part of the hijacked network is reachable on AS2000 and the rest of the network is reachable on AS1000.**

Pfsense-3000 or AS3000

Text

Description automatically generated

So, the route-map shows it using AS2000 as the first stop because of /128 and then AS1000 afterwards.