Copyright Notice:  
All images and screenshots used in this document are the property of CBT Nuggets. Used for educational purposes only. This document is licensed under a Creative Commons Attribution 4.0 International License.

In this lab, I got to see (physically) what switches, routers, and NGFWs look like (Cisco and Fortinet brand ones). I also got to learn and test for myself on live machines what the functions of the different network appliances are at each layer. In the below example, I accessed Switch 1 through the Multi-Tabbed PuTTY software and used the ‘show mac address-table’ as was the syntax on that model of switch for showing it. Realizing that the interface with a mac address for the pc with ip 10.12.0.51 was not populated in that switches’ mac address table, I ran the ping command on PC-12 on the PC-12 tab below, resulting in the second show mac address-table command on SW-1 being populated wit the new mac address ending in 6802 on the gigabit interface 1/1. I also performed a ping trace over the routers on the network to Server1 at 23.1.2.100 to map out, depending on the routing protocols the routers use, the exact path of packets on the network, including useful performance statistics in milliseconds, with the ‘-d’ flag being used to not do name resolution for those routers (non-invasive checks, ip only). Each router’s address is usually the first few addresses after a particular network id at whichever interface (e.g. with 10.23.0.0/24 R3 in the image is 10.23.0.3). There is ipv6, VLANs, & Subnetting in other labs.

A screenshot of a computer

AI-generated content may be incorrect.

In addition to all of that, the trainer in one of the videos on this page explained what the function of a Firewall is- that it can be used like a router to forward ip traffic from one device to another over it, allowing and denying traffic going in one port/interface and out another. Firewalls of the NGFW variety can utilize Proxies on both end to better cache and filter certain types of traffic through it more accurately, and use VPNs, decryption of rouge SSH/SSL sessions, and more- selectable from a list of possible policies. There are several courses on hands-on configurations of Fortinet, Palo Alto, Cisco, and other NGFWs that I could do- and with the teacher Keith Barker on CBT Nuggets, you can expect it will be very in-depth and too the point. Depends on the business you work for which brand is used.

…It is very interesting what taking this course with hands-on labs is like, given I already passed the Network+ Exam with an 810/900. The **hands-on projects**, *however short they are individually*, **do divulge information in a better way than the Network+ book** ever could- as it requires you to simulate a production environment, always speak on-point, & have a positive attitude.