Running Head: NETWORK RECONFIGURATION

Lab 6: Network Reconfiguration

Jered McClure

Walden University

Lab 6: Network Reconfiguration

Screenshot showing successful ping to g0/11 on SW1:



Screenshot showing successful ping to SW1 from R1:



Copying the officeswitch file from 10.4.1.5, note that this file is invalid for this switch as it uses gigabit connections and the file requires fastethernet:



Setting sw8 to SW1:



Setting up vlan 1:



Setting default gateway:



Setting username and password:



Setting security on the lines and a message to be displayed when connecting on those lines:



Setting domain name and generating RSA crypto key:



Setting SSH to Version 2 and forcing SSH on VTY lines 0 to 15:



Setting Switch port security (note that I use g0/2 rather than f0/2 because this is a gigabit switch):



R1 basic configuration, note that the hostname is already R1:



Setting line security and a banner MOTD on R1:


Setting domain name, creating a crypto key, enabling SSH version 2, and forcing SSH on VTY lines 0 to 15 on R1:



Setting up DHCP on R1:



Setting up RIP on R1:



 Overall, my settings were spot on. However, there were a few discrepancies in terms of additional user accounts being accidentally created. On SW1, I had somehow managed to create an additional user called \, yep, just a backslash. This probably occurred when I typed “username \?” but forgot to enter the question mark. In addition, the banner MOTD was not entered correctly on either machine. Seems I did not put “#” at the end of the message telling the system it had ended (Simulation Exams, NA).

 In order to reduce the likelihood of an error that critically disables a node, an image of the node should be taken and stored elsewhere before configuration takes place. The downfall of this is if the pre-existing image is already faulty, or if there is no place to store the image. An alternative would be to have a master node permanently available to pull an image from which was preconfigured with the correct settings. Once again, this can have its faults if an unknown error creeps into the master device, or it is unfeasible to maintain a master device due to funding or resource restraints.

 As for the notes that were left, they were quite clear and concise considering the individual probably was leaving in a rush, or did not want to leave at all. The three things to leave to a successor would be the username and passwords of all devices, IP ranges and locations, and a map of the network. Using these three things, any administrator should be able to fall in place managing a network, albeit with a bit of difficulty. There will always be some configurations that only the administrator on hand will be aware. This is usually due to time constraints and no access to proper documentation resources.

 In terms of best practice, the steps we took were fairly on the money. Telnet was never used and all lines were password protected. However, I would have personally used OSPF over RIPv2 or EIGRP. RIPv2 is an older protocol that can actually put a large load on the network without actually increasing performance. EIGRIP is proprietary, and as such, would preclude the use of any non-Cisco routers (Meyers, 2009, p. sec 5186). OSPF has the smallest routing table of the bunch, and outputs the least load to setup those routes. Also, it is a network standard used by all routers.

Reference

Meyers, M. (2009). *CompTIA Netowrk+ Guide to Managing and Troubleshooting Networks* (2nd ed.). McGraw-Hill.

Simulation Exams. (NA). *CCNA 640-802 Exam Practice Questions.* Retrieved May 26, 2012, from IT Certification Practice Exams: http://www.simulationexams.com/SampleQuestions/ccna\_q7.htm