Running Head: SSH AND PORT SECURITY

Week 3 Lab: SSH and Port Security

Jered McClure

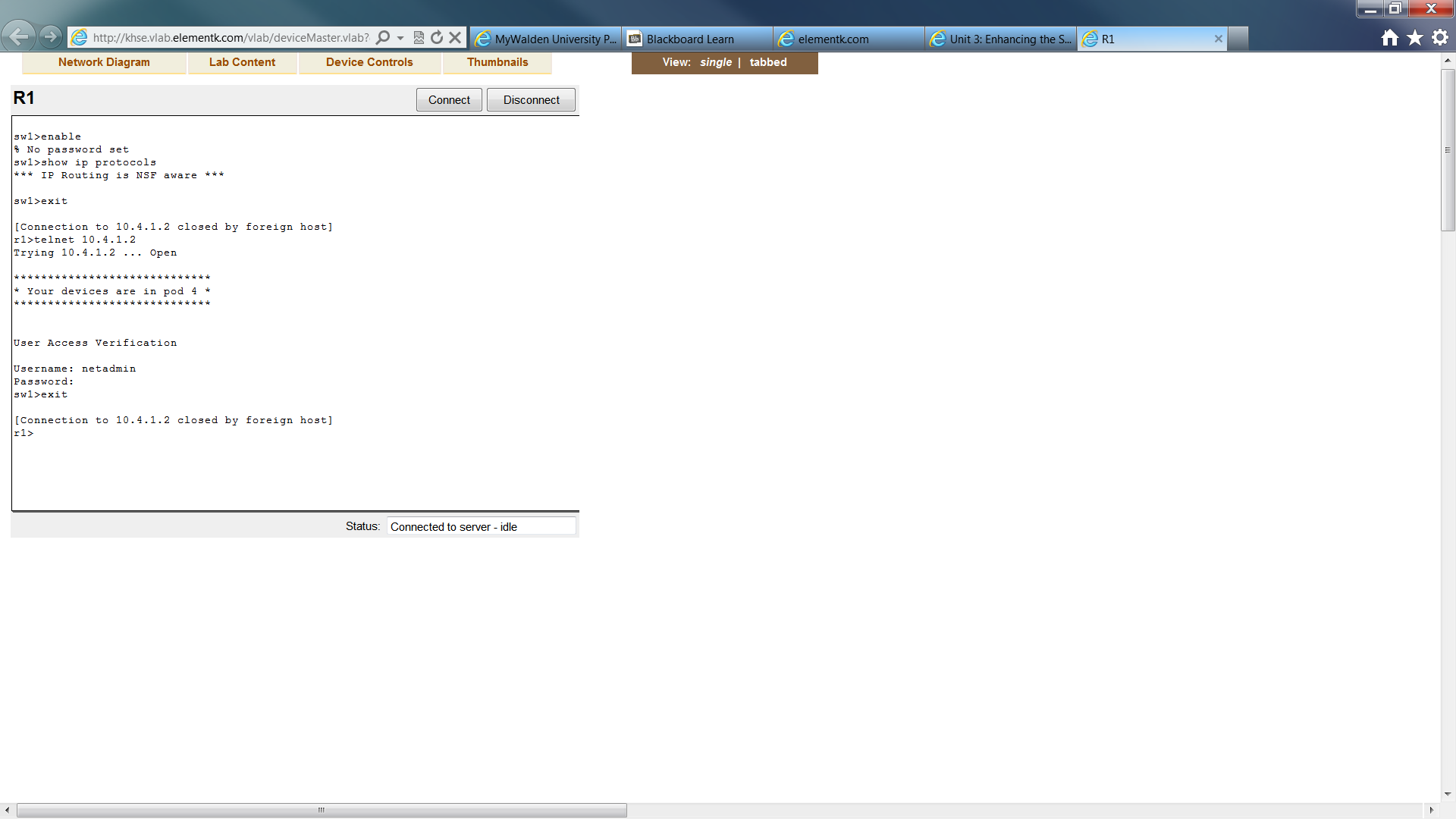
Walden University

Week 3 Lab: SSH and Port Security

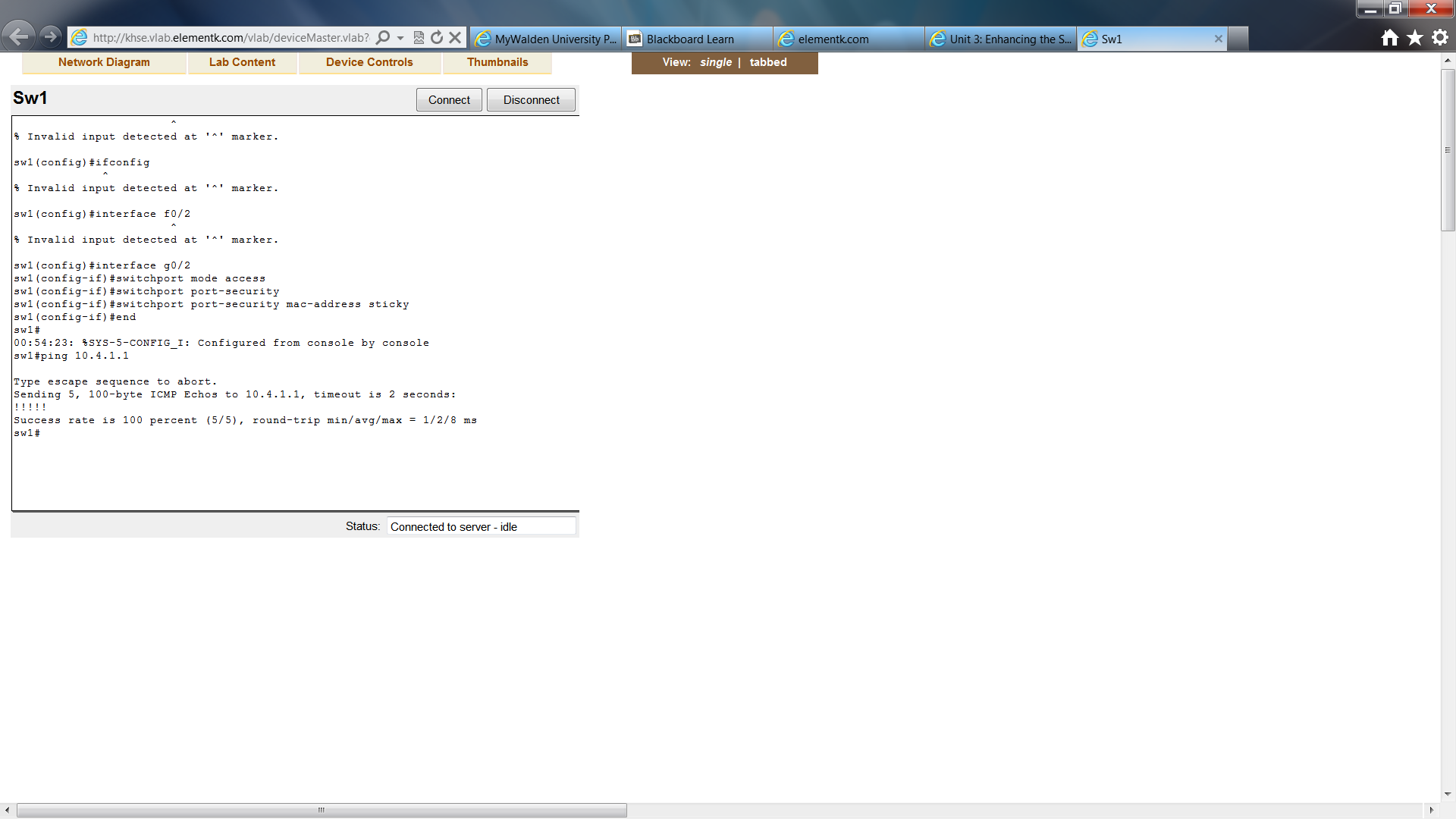
Screenshot of SSH to SW1 from R1:



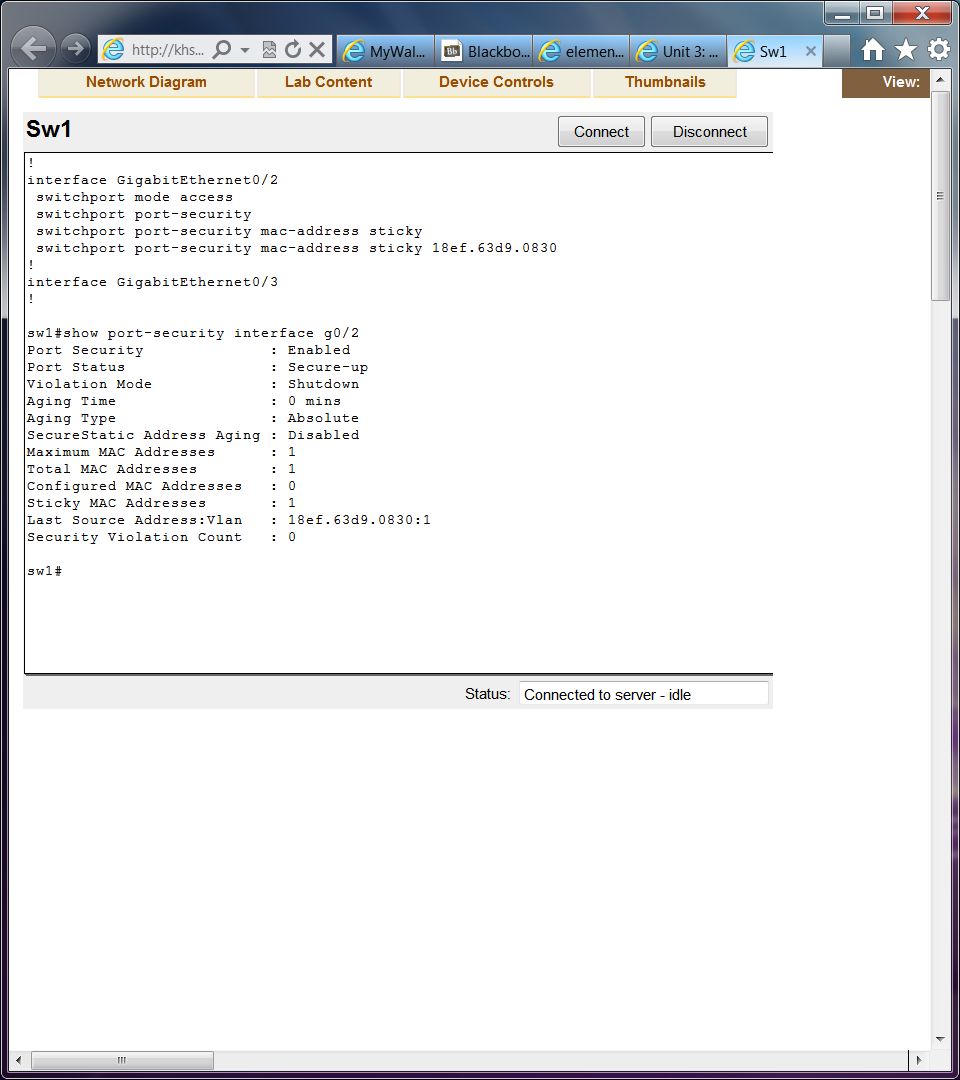
Screenshot of Telnet to SW1 from R1:



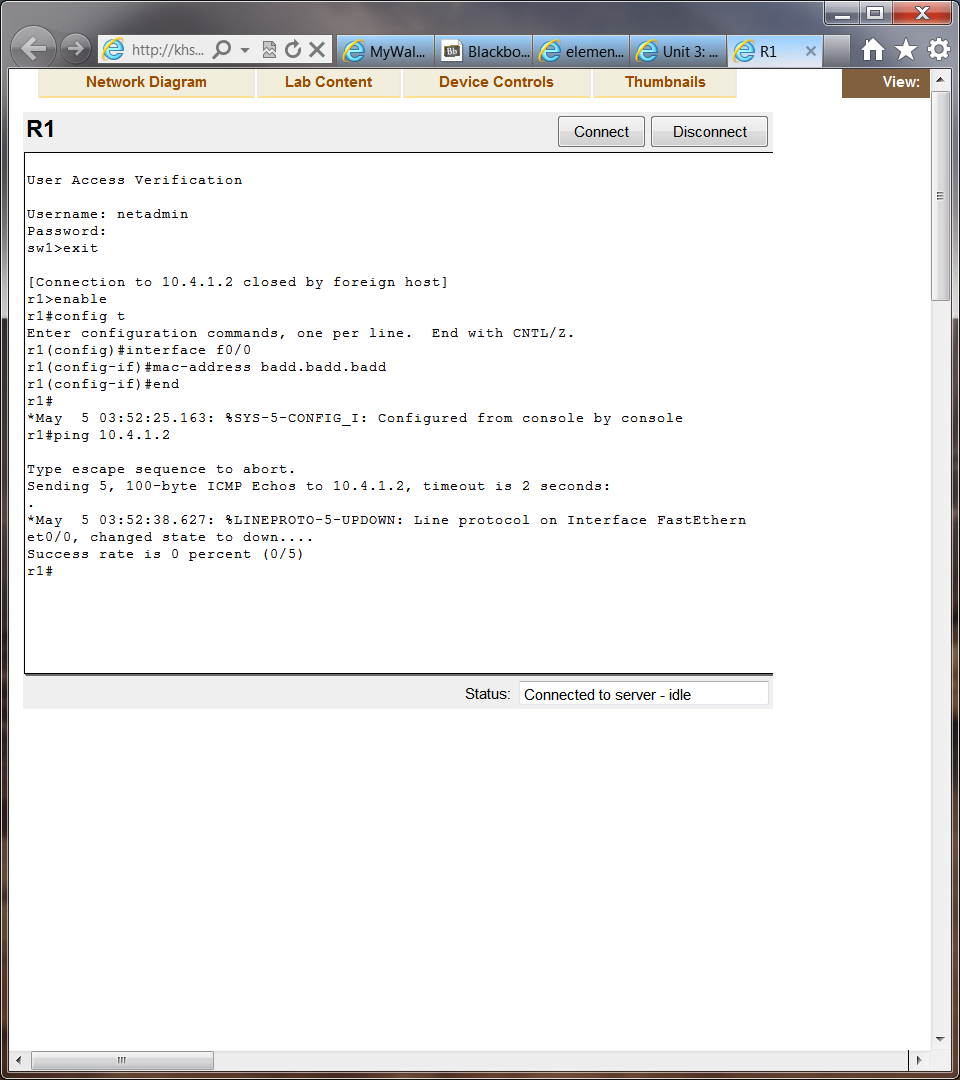
Screenshot of port-security with sticky:



Screenshot of port-security on interface g0/2:



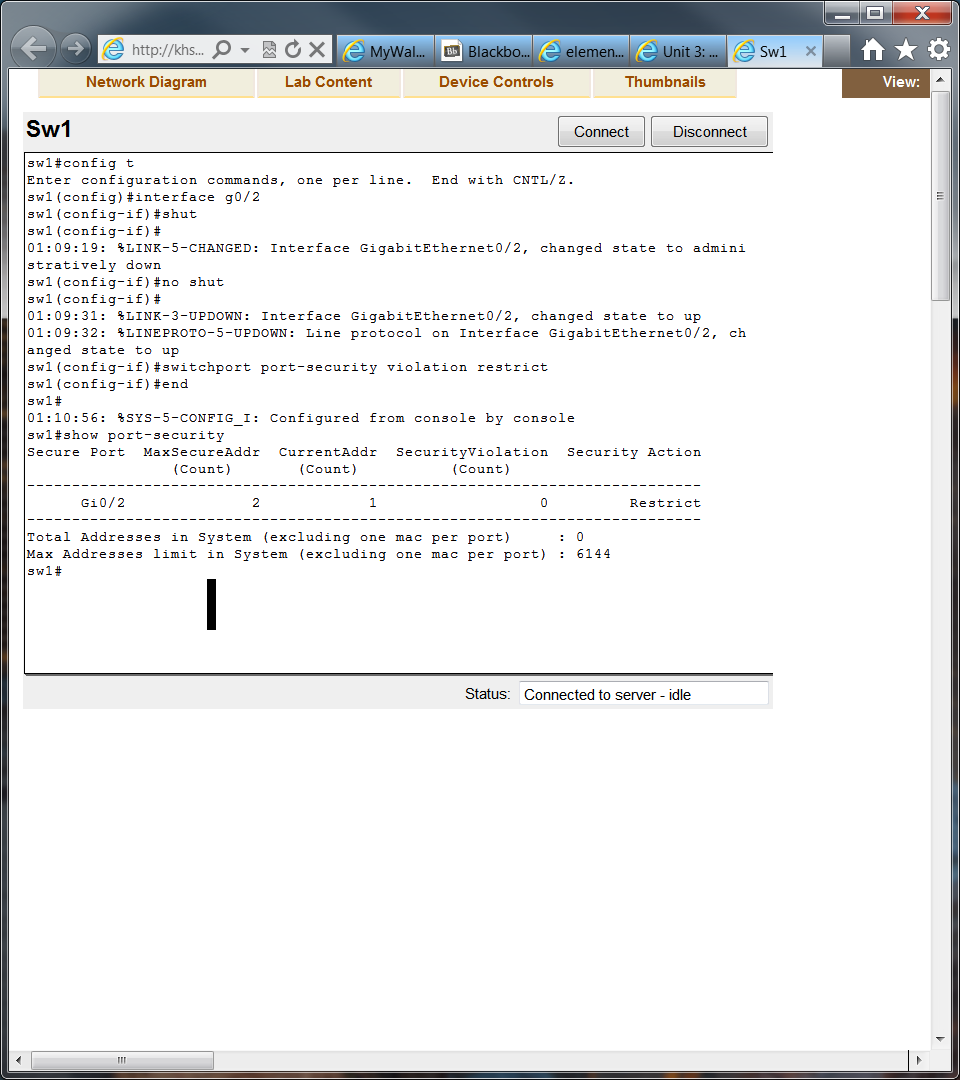
Screenshot of R1 mac address invalidation and ping failure:



Screenshot of SW1 showing the port security violation of badd.badd.badd:



Screenshot verifying the new port security on SW1:



Screenshot showing the arp clear on SW1 and then confirmation ping to R1:



Telnet should not be an option nor required for any circumstance. It is an insecure method of data transport that can be easily subject to man in the middle sniffing. In the event of a router failure of such magnitude that a technician needed to remote into the machine remotely, SSH is always an option. To say that they would not have access to a SSH terminal is the equivalent of saying they do not have access to a telnet terminal. Both require the internet, and therefore, a SSH is only a download away.

SSH key distribution without direct access can be met through physical transfer (USB or external HDD) or digital transfer (network storage/file share), email transfer is not recommended as it is an unsecure mode of data transportation. Nevertheless, in dire emergency, such transfer is still an option. The most secure method is through password encryption of the SSH key through a RAR or other type of compression medium, and the password stored in a password managed warehouse, such as KeePass (Reichi, 2012).

When one set of SSH need to be shared amongst multiple devices on a network, and some of those devices do not require a password to access SSH, security becomes a concern. This can be easily rectified by ensure those devices that do not require an SSH password are password secure themselves. Also, only authorized personnel are allowed to know the passwords to those particular systems.

The idea that the network administrator would become overloaded with security port changes during hardware mac movements is a concern. However, one must remember, this is their job. Nevertheless, delegation, proper port configuration, and project planning can decrease the overall workload which may be required during large hardware movements. The easiest method would be to give access to all ports on the network to those pieces of hardware which are allowed access to the network. This would remove any work required for port enabling during large moves.

Reference

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

Reichi, D. (2012). *KeePass Password Safe.* Retrieved May 4, 2012, from KeePass: http://keepass.info/