Basic Security Best Practices for networking

- **Secure Location:** Be sure to locate your Cisco routers and switches in a secure location — a locked room where limited access is permitted.
- **Disable Ports:** In high secure environments, you should disable unused ports so that unauthorized systems cannot connect to the network.
- **Configure Port Security:** In order to control which systems can connect to the enabled ports, use port security to limit which MAC addresses can connect to which ports.
- **Set Passwords:** Be sure to configure passwords on the console port, auxiliary port, and the vty ports. Also configure the enable secret for access to priv exec mode.
- **Login Command:** Do not forget the login command after setting the password on the port. The login command tells the Cisco device that anyone connecting must log in and forces the prompt for a password.
- **Login Local Command:** If you are looking to create usernames and passwords for login, then use the *login local* command to tell the Cisco device that you wish to authenticate persons by the usernames and password configured on the device.
- **Encrypt Passwords:** Be sure to encrypt all passwords in the configuration with the *service password-encryption* command!
- **Banners:** Be sure to configure banners that do not have the word "welcome" in the message or any other inviting phrases. You want to make sure that the banners indicate that unauthorized access is prohibited.
- **Secure Communication:** To remotely manage the device, use SSH instead of telnet as the communication is encrypted.