LAB # 7

REMOTE ACCESSING OF SWITCH SECURE SHELL (ssh)

**OBJECTIVE**

To configure Secure Shell for remote access of switch

# Theory

Secure Shell (SSH) is set of programs which employ public/private key technology for authenticating and encrypting sessions between user accounts on distributed hosts on the Internet.

SSH works by the exchange and verification of information, using public and private keys, to identify hosts and users. It then provides encryption of subsequent communication, also by the use of public/private key cryptography.

As a system administrator, you generate a public and private key pair for the system itself. By use of this information contained within the system itself, the possibility of someone spoofing the system's identity by faking IP addresses or mugging up DNS records that associate IP addresses and domain names is removed. You would have to break into the system and steal its private key in order to successfully pretend to be that system. This is a big improvement in security.

* **Create a local user name**

Switch(config)#**username ssuet password ccn**

* **Assign a domain name**

Switch(config)#**ip domain-name ssuet.com**

* **Following Command takes few a min to generate key**

**SSH** uses encryption keys to encrypt the data exchanged in an SSH session.

ccn(config)#**crypto key generate rsa**

How many bits in the modulus [512]: **768**

ccn(config)#**enable password cisco**

* **Configure vty ports for using SSH**

ccn(config-line)#**line vty 0 15**

ccn(config-line)#**login local**

ccn(config-line)#**transport input ssh**

OR

ccn(config)# **line vty 0 15**

ccn(config-line)# **login local**

ccn(config-line)# **transport input ssh telnet**

* **Apply these commands**

ccn(config)# **interface vlan 1**

ccn(config-if)# **ip address 10.0.0.1 255.0.0.0**

ccn(config-if)# **no shutdown**

ccn(config-if)# **exit**

* **Creating SSH session with Cisco device, , go to command prompt and type**

C:\>**SSH -L ssuet 10.0.0.1**

Open

* **Enter the password configured in step 1**

Password:

ccn>

* **Verification of SSH**

ccn# **show crypto key mypubkey rsa**

ccn(config)#**do** **show line**

Tty Typ Tx/Rx A Modem Roty AccO AccI Uses Noise Overruns Int

0 CTY - - - - - 0 0 0/0 -

129 AUX 9600/9600 - - - - - 0 0 0/0 -

**\*** 130 VTY - - - - - 67 0 0/0 -

131 VTY - - - - - 0 0 0/0 -

132 VTY - - - - - 0 0 0/0 -

133 VTY - - - - - 0 0 0/0 -

134 VTY - - - - - 0 0 0/0 -

135 VTY - - - - - 0 0 0/0 -

136 VTY - - - - - 0 0 0/0 -

137 VTY - - - - - 0 0 0/0 -

138 VTY - - - - - 0 0 0/0 -

139 VTY - - - - - 0 0 0/0 -

140 VTY - - - - - 0 0 0/0 -

141 VTY - - - - - 0 0 0/0 -

142 VTY - - - - - 0 0 0/0 -

143 VTY - - - - - 0 0 0/0 -

144 VTY - - - - - 0 0 0/0 -

145 VTY - - - - - 0 0 0/0 -

* **‘\*’ shows the active telnet Session**

ccn# **show users**

Line User Host(s) Idle Location

0 con 0 idle 00:00:00

\* 67 vty 0 ssuet idle 00:00:45

* **To close telent or SSH connection**

ccn#**clear line vty 0**

**EXERCISE QUESTIONS**

1. Name the encryption techniques use for key encryption.
2. What are the ports numbers for SSH?
3. Write difference between Telnet and SSH
4. Why do we use***‘login’*** command after setting password on VTY lines?