# Telnet and SSH

Telnet and SSH (Secure Shell) both give us terminal access to a remote host. SSH is encrypted using the same technology used for secure web access (HTTPS). Telnet is sent in plain text, including the user name and password.

## Access to Cisco Routers--Telnet

To configure telnet access to a Cisco router, we have to configure a password. We also have to configure a password for enable mode access. It helps to give the routers different names so we can tell them apart. Use the following commands.

*enable  
configure terminal  
hostname RouterA (or B or C, as appropriate)  
enable secret svgs (from now on the password to enter enable mode is svgs)  
line vty 0 4  
 password svgs*

Now, you can use PUTTY to connect to the router. Select telnet instead of serial, and enter the IP address of the router.

## Telnet--no security

Once you have telnet working, disconnect PUTTY from the router. Start a packet capture using Wireshark, and then log in to the router again with PUTTY and telnet. Enter the command, enable, and the enable password. Enter show running-configuration. Then log out and stop the packet capture.

Examine the packet capture. You should be able to see everything, including passwords, in plain text. Anyone who can intercept your packets can see this too.

## Access to Cisco Routers--SSH

To use SSH, we need to enter a domain and create keys (we’ll discuss keys in detail when we discuss HTTPS.)

ip domain name svgs.k12.va.us  
crypto key generate rsa

Then tell the router to generate 2048 bit keys.

ip ssh version 2

Now you should be able to select SSH in PUTTY and log in to the router using SSH. Repeat the same packet capture experiment you did with telnet. This time, you will see PUTTY and the router negotiate encryption, and then everything else will be unreadable.