Lab 8.3.1.1 Configure Basic AP security through GUI

Estimated Time: 30 minutes

Number of Team Members: Students will work in teams of two.

Objective

In this lab, the student will learn the following objectives:

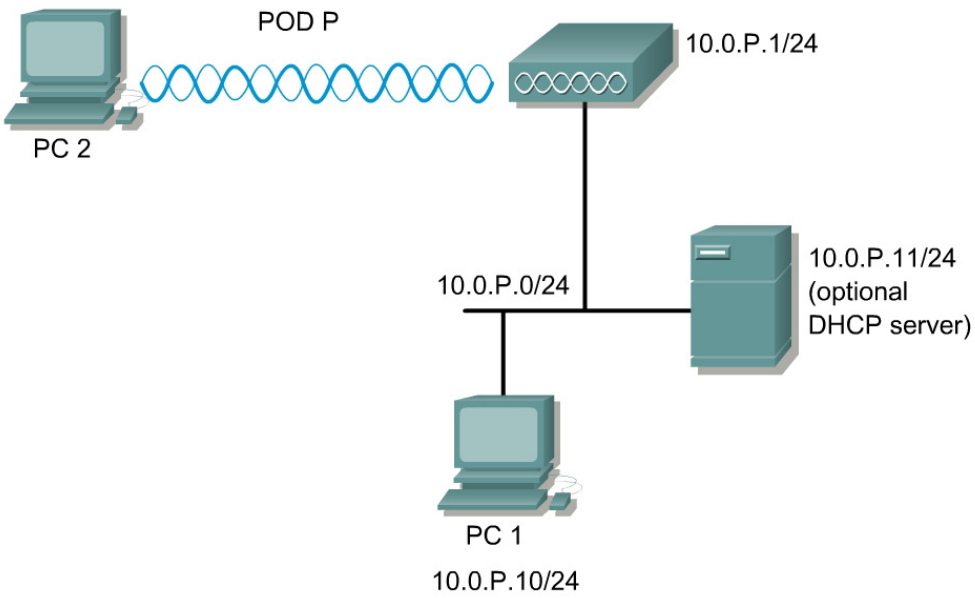
- Password protect the console
- Define administrator accounts
- Configure accurate time and check firmware
- Configure SSH
- Disable telnet and web (optional)

Scenario

Students will learn to secure the AP through GUI. The security policy of the company mandates all devices should be locked down according to minimum standards. Also, SSH must be used for remote management.

SSH is a program, similar to Telnet, which allows a network administrator to log into another computer over a network. SSH allows an administrator to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure networks. There are currently two versions of SSH available: SSH Version 1 and SSH Version 2. Only SSH Version 1 is implemented in the Cisco IOS software.

Topology



Preparation

Team	AP Name	SSID	Address
1	Pod1	AP1	10.0.1.1/24
2	Pod2	AP2	10.0.2.1/24

The instructor should have a working wired network. PC1 should be connected to the wired network. Prior to starting the lab, ensure that each host PC is loaded with a SSH client. There are numerous SSH clients available for free on the Internet. The lab was developed using the PuTTY SSH client.

Tools and Resources

Each team will need:

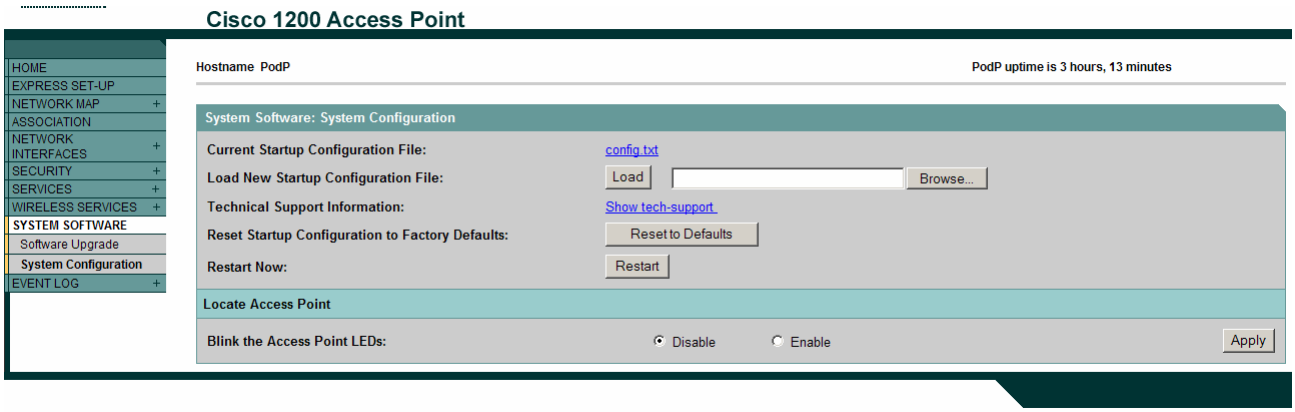
- AP
- PC or laptop
- Console cable
- SSH client software

Additional Materials:

http://www.cisco.com/en/US/products/hw/wireless/ps430/products_installation_and_configuration_guide_book09186a0080147d69.html

http://www.chiark.greenend.org.uk/~sgtatham/putty/

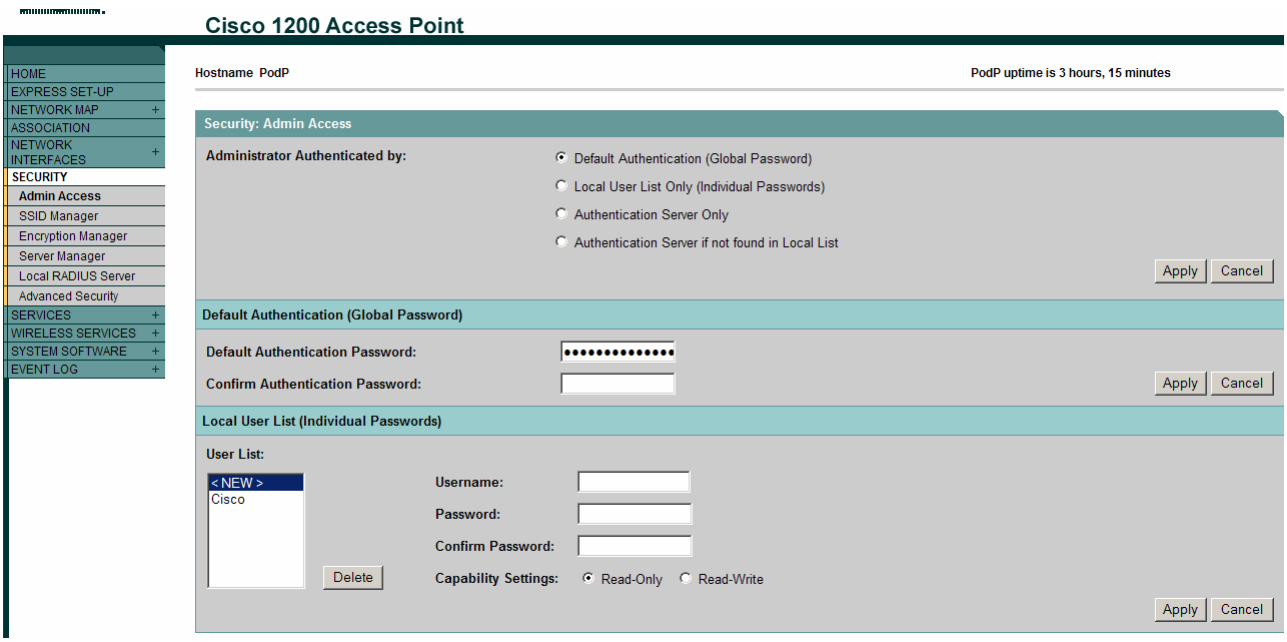
Step 1 Configure basic AP settings



a. If there is an existing configuration on the AP, erase the configuration and reload either through GUI or IOS CLI.

b. Configure the hostname, SSID, and BVI interface according to the Preparation table.

Step 2 Configure a new administrator account



One of the easiest ways for hackers to gain access to network devices is by using default usernames and passwords.

a. Configure a new administrator account from the **SECURITY>Admin Access** page. Give this user Read-Write privileges.

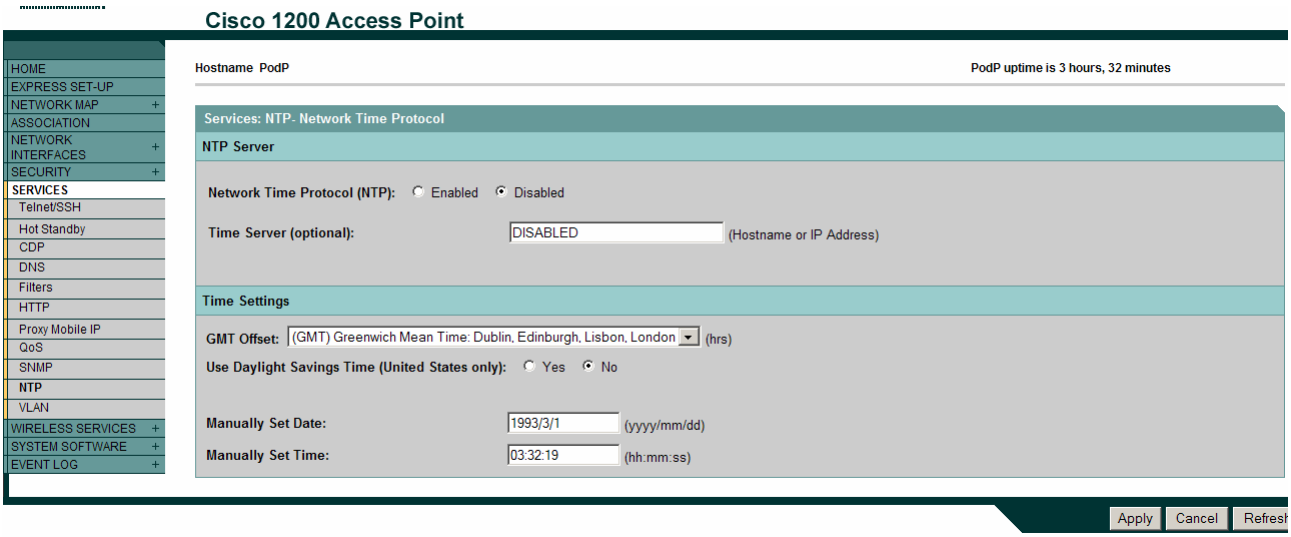
   Username: clsCo123

   Password: clsCo123

b. In a production environment, it is necessary to delete the old account. However, in the lab, do not remove the existing account. Also, it is important to encrypt the passwords in the configurations if there are multiple administrator accounts with various privilege levels. By default, this is enabled on the AP 1200. Notice the password is bulleted out.

c. Enable only Local User List Only and click **Apply**. At this point, the AP will require authentication with the new Username.

Step 3 Configure accurate time



In order to keep track on any potential attacks, it is important to maintain proper time.

a. From the **SERVICES>NTP** page manually set the correct time and date. Click **Apply** to save the changes.

Step 4 Verify the AP image file

Many attacks can be prevented by maintaining the most up to date image. In order to keep up with any vulnerabilities in Cisco products go to:

http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_tech_note09186a0080132a8a.shtml

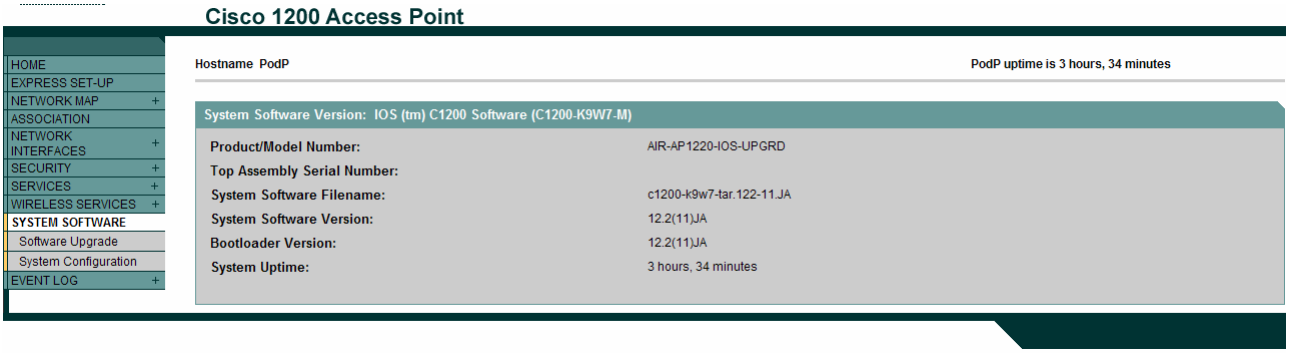
a. Are there any wireless vulnerabilities listed? If so, what are they?

_____

_____

_____

b. From the **SYSTEM SOFTWARE** main page, check the current image.



c. What version is running?

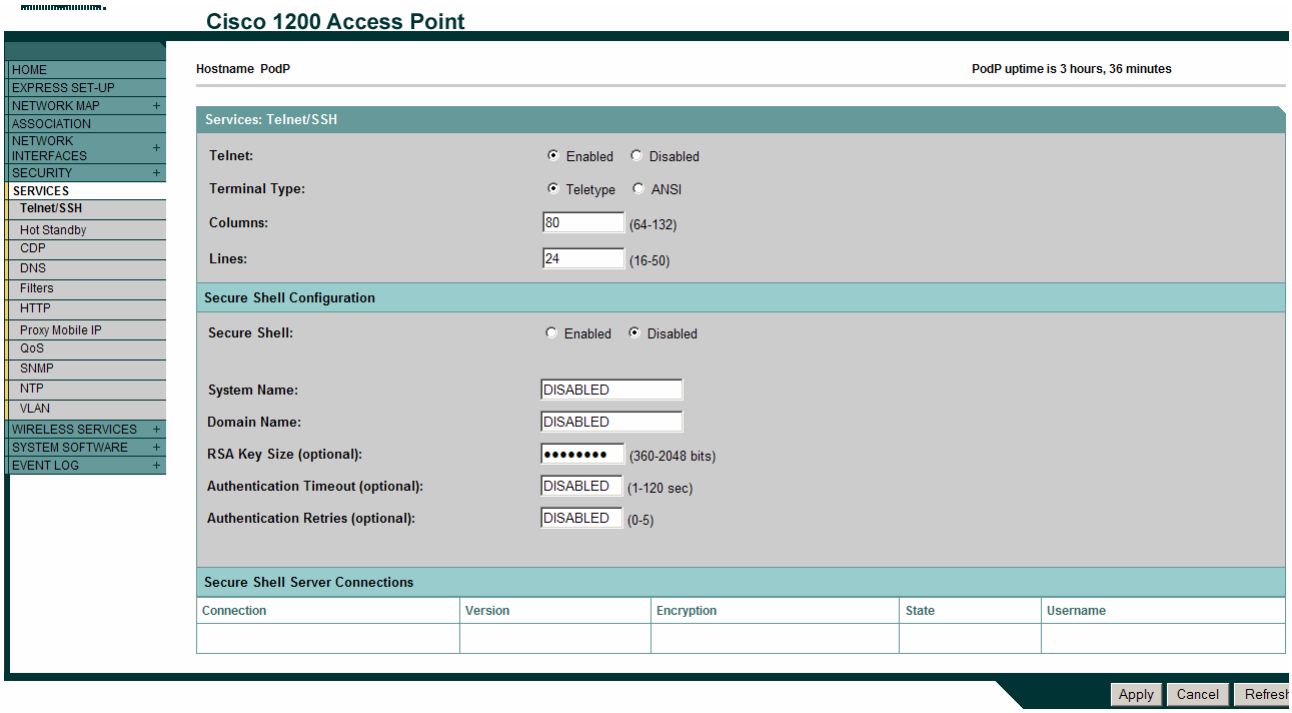
_____

d. Does this AP have any known vulnerabilities?

_____

Step 5 Configure SSH

In some circumstances, attackers may be able to use a packet analyzer to intercept telnet passwords, which may enable them to gain access to the AP or other networking devices. The SSH protocol is a secure form of telnet, providing both authentication and encryption.



a. From the **SERVICES>Telnet/SSH** page enable Secure Shell.

b. Enter the System name of PodP (where P is the pod number).

c. Enter a domain name of fwl.com.

d. Enter a key size (optional).

e. Keep the default Timeout and Retries values.

f. Click Apply.

g. What is the default size, in bits, of the key modulus?

_____

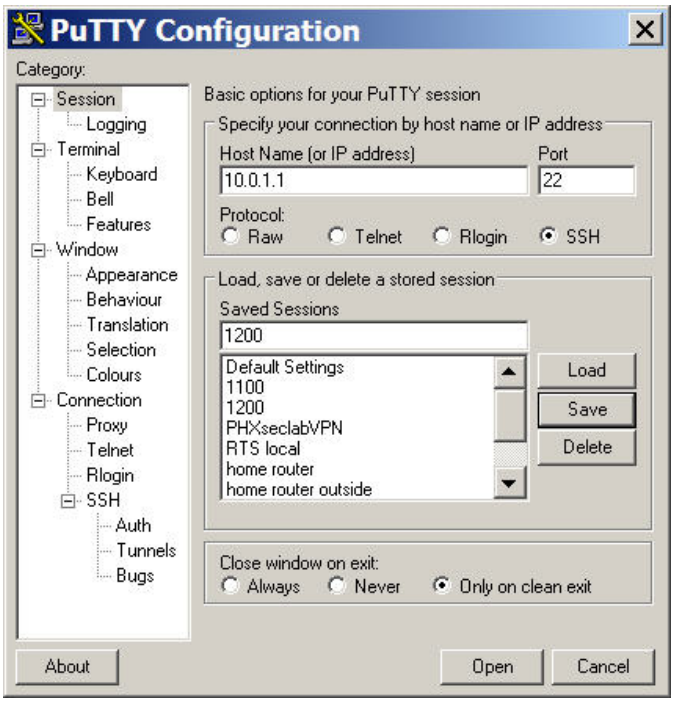
h. Press **OK** to accept the default key size and continue.

Note In a production environment, after enabling SSH, telnet and http should be disabled.

Step 6 Communicating between a SSH PC (client) to AP (server)

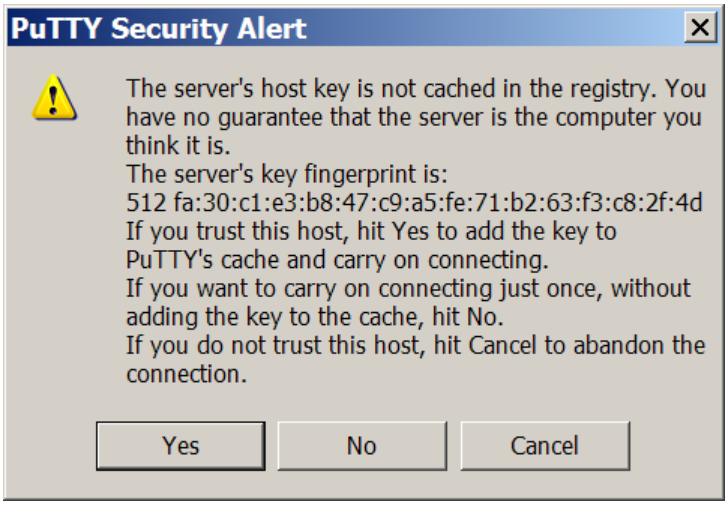
The basic settings to allow a PC and an AP to establish a SSH session are now configured. In order to establish a SSH session, launch the SSH client from the student PC.

a. The configurations will vary among different SSH clients. If PuTTY is being used as the SSH client, following these instructions. Launch the PuTTY.exe file and a pane with various configuration options will open.

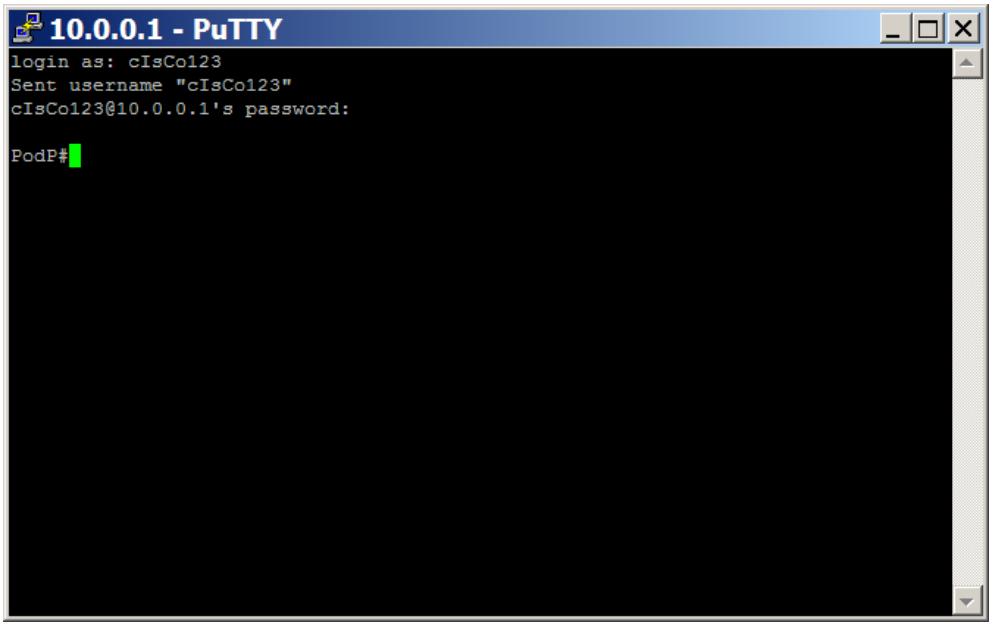


b. In the “Host Name (or IP address)” input box, enter the IP address of the pod AP. Next, change the protocol to “SSH”. These two values must be sent to establish the SSH. To test the connection, press the **Open** command button at the bottom of the window.

c. The SSH Client will popup a Security Alert window. Click **Yes** to trust the host.



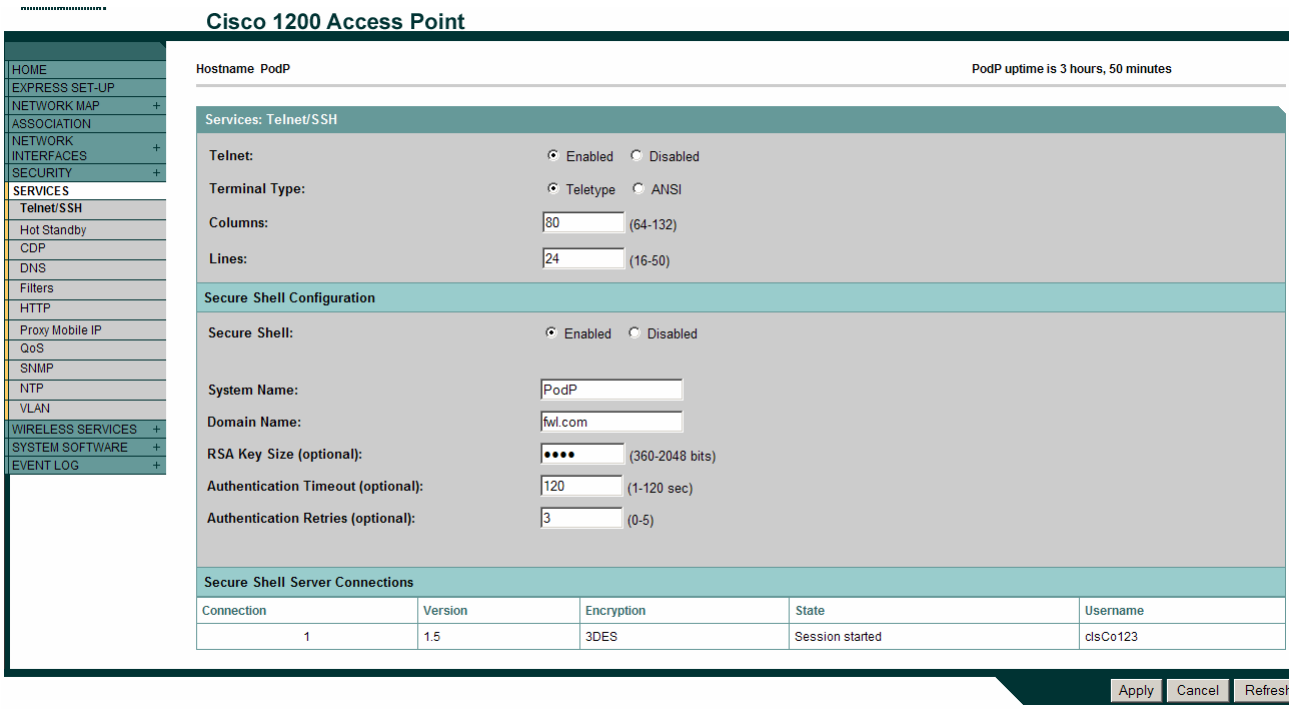
d. The SSH client will prompt for the local username and password that was previously set on the Pod AP. Enter the “**clsCo123**” for the username and “**clsCo123**” for the password.



e. Was the SSH connection successful? If so, how is the prompt displayed?

_____

Step 7 Verify SSH Connections



a. From the **SERVICES>Telnet/SSH** Page, view the active SSH sessions.

b. Fill in the appropriate values in the table below based on the active Secure Shell Server Connections.

Connection	Version	Encryption	State	Username

c. Reset the AP back to the factory default configuration.

