Lab 8.3.1.2 Configure Basic AP Security through IOS CLI

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:

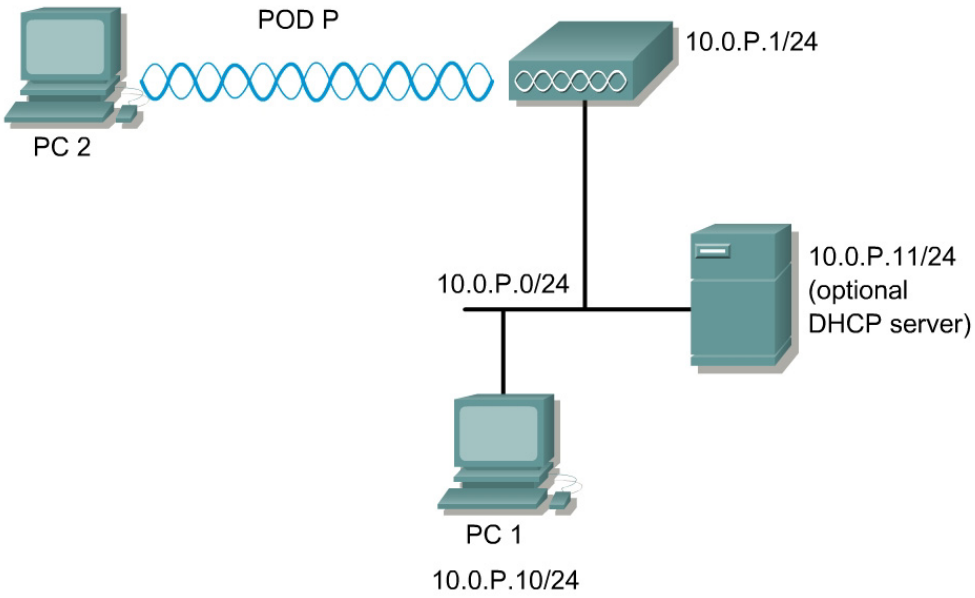
- Password protect the console
- Define administrator accounts
- Configure accurate time and check firmware
- Configure SSH
  - Limit VTY to SSH
  - Access-list to secure SSH
- Disable telnet and web

Scenario

Students will learn to secure the AP through Cisco Internetworking Operating System (IOS). 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/

Command List

In this lab exercise, the following commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Command	Description
crypto key generate rsa	Generates Rivest, Shamir, and Adleman (RSA) key pairs.
hostname	This command changes the APs hostname.
ip domain-name	Defines a default domain name that the Cisco IOS software uses to complete unqualified host names.
ip ssh	Use the **ip ssh** command to configure Secure Shell (SSH) control parameters on the AP.
transport input	Defines which protocols to use to connect to a specific line of the AP.

Step 1 Configure basic AP settings

a. Connect a Cisco rollover cable (console cable) between PC1 and the AP.

b. Open a terminal emulator.

c. Press return to get started.

d. If there is an existing configuration on the AP, erase the configuration and reload.

e. Configure the hostname, SSID, and domain name according to the Preparation table.

```
PodP(config)#
PodP(config)#ip domain-name fwl.com
```

f. Configure a wireless PC or laptop to connect to the AP. This will be used later in the lab to test the security configuration.

g. Remain on PC1 to configure the following steps.

h. While in configuration mode, check the configuration

```
PodP(config)#do show run
```

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.

```
PodP(config)#username cIsCo123 password cIsCo123
```

b. In a production environment, it is necessary to delete the old account.

```
PodP(config)#no username Cisco password Cisco
```


c. 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.

```
PodP(config)#service password-encryption
```

d. While in configuration mode, verify the user accounts and password encryption.

```
PodP(config)#do show run
```

e. Secure the console connection by requiring a password.

```
PodP(config)#line con 0
PodP(config-line)#login
PodP(config-line)#password cIsCo123
```

f. Exit out of the AP and log back in.

```
User Access Verification

Password:
```

g. A more secure method is to require a username and password combination. Return to configuration mode and configure local authentication on the console.

```
PodP(config)#line con 0
PodP(config-line)#login local
```

h. Exit out of the AP and log back in using the username password combination configured in step 2a.

```
User Access Verification

Username:
Password:
PodP>
```

Step 3 Configure accurate time

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

a. Configure the correct time. Use the help feature if needed.

```
PodP#clock set
```

b. Set the correct timezone

```
PodP(config)#clock timezone [name of time zone] [offset in hours]

Example:
PodP(config)#clock timezone PhoenixAZ -7
```


c. (Optional) Configure daylight savings time. Use the help feature or command reference if needed.

```
PodP(config)#clock summer-time
```

d. Check the clock settings while in configuration mode.

```
PodP(config)#do show clock
```

Step 4 Configure MOTD and login banner

a. Configure a message-of-the-day (MOTD). The MOTD banner appears on all connected terminals at login and is useful for sending messages that affect all network users (such as impending system shutdowns).

```
PodP(config)#banner motd #
This is a secure site. Only authorized users are allowed.
For access, contact technical support.
#
PodP(config)#
```

b. Exit out of the console or telnet session to check the MOTD.

```
con0 is now available

Press RETURN to get started.

This is a secure site. Only authorized users are allowed.
For access, contact technical support.
```

c. Configure a login banner. This banner appears after the MOTD banner and before the login prompt.

```
PodP(config)#banner login $
Access for authorized users only. Please enter your username and
password.
$
PodP(config)#
```

d. Exit out of the console to check the banner.

```
con0 is now available

Press RETURN to get started.

This is a secure site. Only authorized users are allowed.
For access, contact technical support.

Access for authorized users only. Please enter your username and
password.

User Access Verification

Username:
```


Step 5 Verify the 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. Check the current image.

```
PodP#show version
```

c. What version is running?

_____

d. Does this AP have any known vulnerabilities?

_____

Step 6 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.

First, begin by generating the asymmetric keys used in the SSH authentication process.

Generate RSA keys

a. Enter the following command in the configuration mode:

```
PodP(config)#crypto key generate rsa ?
```

b. What are the available help options for this command?

_____

Generate RSA keys (continued)

- To enable SSH for local and remote authentication on the AP, enter the command **crypto key generate rsa** and press **Enter**. The AP will respond with a message showing the naming convention for the keys.

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

_____

d. Press **Enter** to accept the default key size and continue.

Step 7 Configure SSH timeouts

a. Configuring SSH timeouts and authentication retries is a way of providing additional security for the connection. Use the command **ip ssh {[time-out seconds]} {authentication-retries integer}** to enable timeouts and authentication retries. Set the SSH timeout to 15 seconds and the amount of retries to 3 by entering the following commands:

```
PodP(config)#ip ssh time-out 15
PodP(config)#ip ssh authentication-retries 3
```

1. What is the maximum timeout value allowed? What is the maximum amount of authentication retries allowed?

_____

Step 8 Configure local authentication and VTY

a. Use the following commands to define a local user and assign SSH communication to the vty lines:

```
PodP(config)# username cisco password student
PodP(config)# line vty 0 4
PodP(config-line)# transport input ssh
PodP(config-line)# login local
```

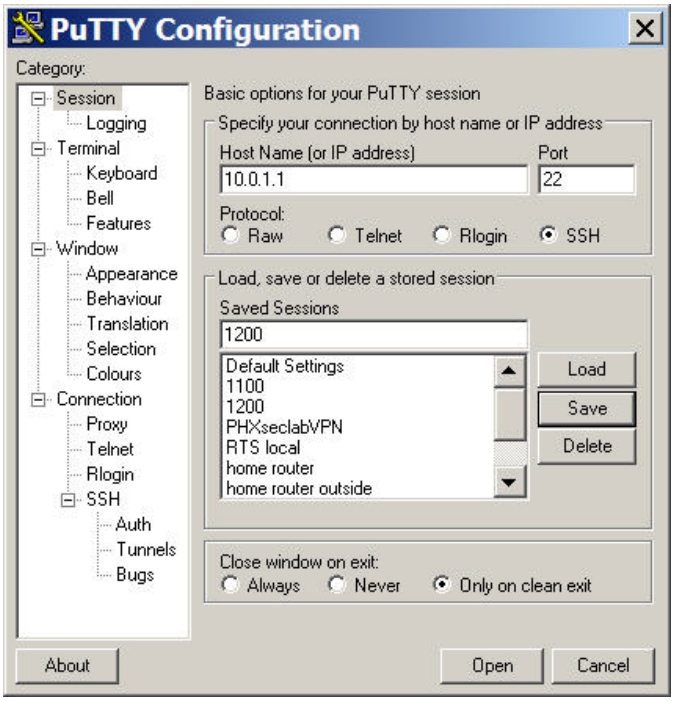
1. What are the available parameters for the **transport input** command?

_____

Step 9 Communicating between a SSH PC (client) to AP (server)

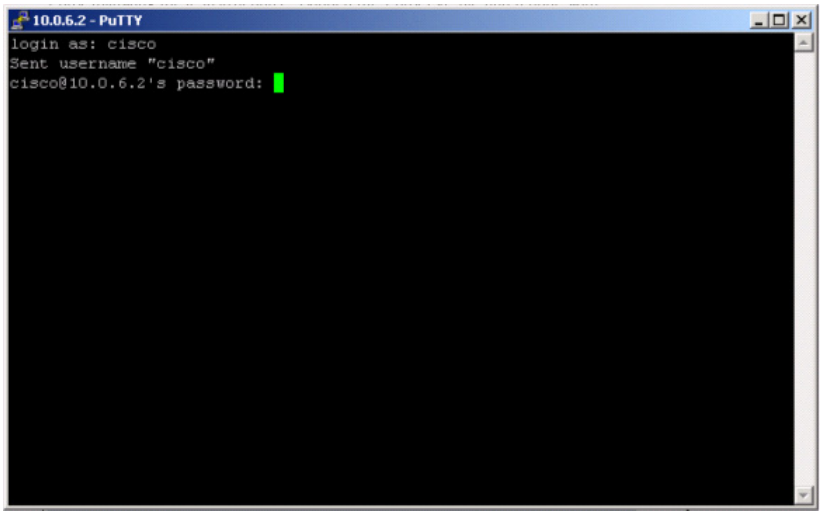
The basic settings to allow a PC and an AP to establish a SSH session are now configured. In order to establish a SSH session, launch the SSH client from the student PC.

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 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.



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

_____

Step 10 debug and verify SSH

Enable debugging

a. Enable debugging of SSH by entering the following commands:

```
PodP(config)#logging on
PodP(config)#exit
PodP#terminal monitor
PodP#debug ip ssh
```

b. SSH debug output

c. Next, open another instance of the SSH client and connect to the AP. Use the correct username and password to log in to the AP. The debug output should be similar to the output below.

```
03:45:37: SSH1: starting SSH control process
03:45:37: SSH1: sent protocol version id SSH-1.5-Cisco-1.25
03:45:37: SSH1: protocol version id is - SSH-1.5-PuTTY-Release-0.53b
03:45:37: SSH1: SSH_SMSG_PUBLIC_KEY msg
03:45:38: SSH1: SSH_CMSG_SESSION_KEY msg - length 112, type 0x03
03:45:38: SSH: RSA decrypt started
03:45:39: SSH: RSA decrypt finished
03:45:39: SSH: RSA decrypt started
03:45:39: SSH: RSA decrypt finished
03:45:39: SSH1: sending encryption confirmation
03:45:39: SSH1: keys exchanged and encryption on
03:45:41: SSH1: SSH_CMSG_USER message received
03:45:41: SSH1: authentication request for userid cisco
03:45:41: SSH1: SSH_SMSG_FAILURE message sent
03:45:44: SSH1: SSH_CMSG_AUTH_PASSWORD message received
03:45:44: SSH1: authentication successful for cisco
03:45:44: SSH1: requesting TTY
```



```
   03:45:44: SSH1: setting TTY - requested: length 24, width 80; set:
length 24, width 80
   03:45:44: SSH1: SSH_CMSG_EXEC_SHELL message received
   03:45:44: SSH1: starting shell for vty03:45:37: SSH1: starting SSH
control process
```

d. To get an idea of the debugging process and the debugging message, open another instance of the SSH client and intentionally enter the wrong username or password. View the debugging output for failed authentication.

   Disable debugging

```
PodP#undebug all
All possible debugging has been turned off
```

e. Viewing SSH sessions

f. Use the **show ssh** command to view the active SSH sessions.

g. Fill in the appropriate values of the table below, based on the output of the **show ssh** command.

Connection	Version	Encryption	State	Username

   Viewing SSH parameters

h. To display the version information and SSH parameters, use the **show ip ssh** command.

i. Is the output displayed exactly as the output below? If not, what are the differences?

_____

_____

_____

```
PodP>sh ip ssh
SSH Enabled - version 1.5
Authentication timeout: 15 secs; Authentication retries: 3
```

Step 11 AP to AP SSH Connection (Optional)

Confirm peer SSH configurations.

a. Verbally communicate with the peer team to ensure the peer AP has been configured to accept a SSH connection. Instead of using a SSH client running on a host computer, the AP will be the SSH client and will establish a connection to the peer AP. By default, the Cisco IOS will act as both a SSH server and SSH client.

b. In order to communicate between the two APs across the wired LAN, the BVI interfaces will have to be on the same subnet. This can be accomplished by changing the masks to 255.255.0.0 on both AP BVI interfaces. One other option is to use a router between the two APs, which will route between the two subnets.

   Test Telnet.

c. When the peer group is ready, enter the **telnet** command and establish connectivity with the peer AP.

```
PodP#telnet 10.0.Q.1  (where Q is the peer team AP)
```


d. Was the Telnet connection successful? Why or why not?

_____

Enter SSH parameters.

e. Enter the following commands to establish a SSH connection to the peer AP:

```
PodP#ssh ?
```

f. What are the additional arguments of the **ssh** command?

_____

g. What encryption algorithms are available?

_____

Establish AP to AP SSH connection.

h. Enter the following command to establish a SSH connection to the peer AP:

```
PodP>ssh -c des -l cisco 10.0.Q.1   (where Q is the peer team AP)
```

This command makes a SSH connection to a peer AP with an address of 10.0.Q.2, DES as the encryption, and cisco as the login username.

i. Was the SSH connection successful?

_____

Verify SSH.

j. Enter the following command to verify the SSH connection:

```
PodP#show ip ssh
PodP#show ssh
```

k. What other commands could be useful to verify and troubleshoot SSH connections?

_____

_____

Step 12 Disable web (optional)

Many security policies may mandate http access to devices be disabled. If https is not available, then SSH is the second best option for secure communication to remote LAN devices.

a. Now that SSH is configured, disable web access to the AP.

```
PodP(config)#
PodP(config)#no ip http server
```

b. Open a web browser and try to connect to the AP?

_____

_____

c. If the configuration was saved to flash, erase the startup configuration and reload the AP.

```
PodP#erase startup-config
PodP#reload
```

