



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:

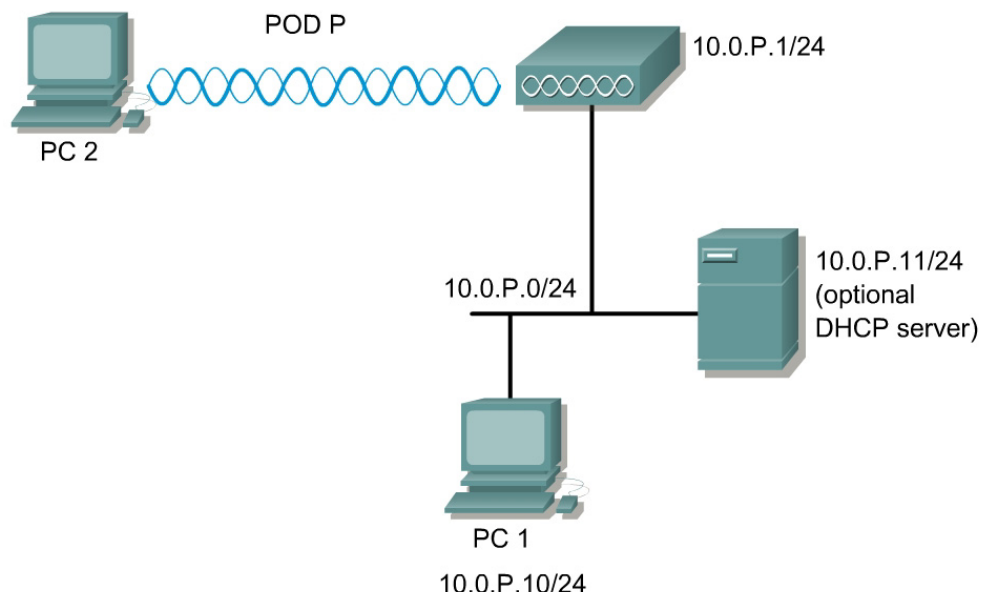
- Password protect the console
- Define administrator accounts
- Configure accurate time and check firmware
- Configure SSH
- Disable telnet and web (optional)

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

<u>Team</u>	<u>AP Name</u>	<u>SSID</u>	<u>Address</u>
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:

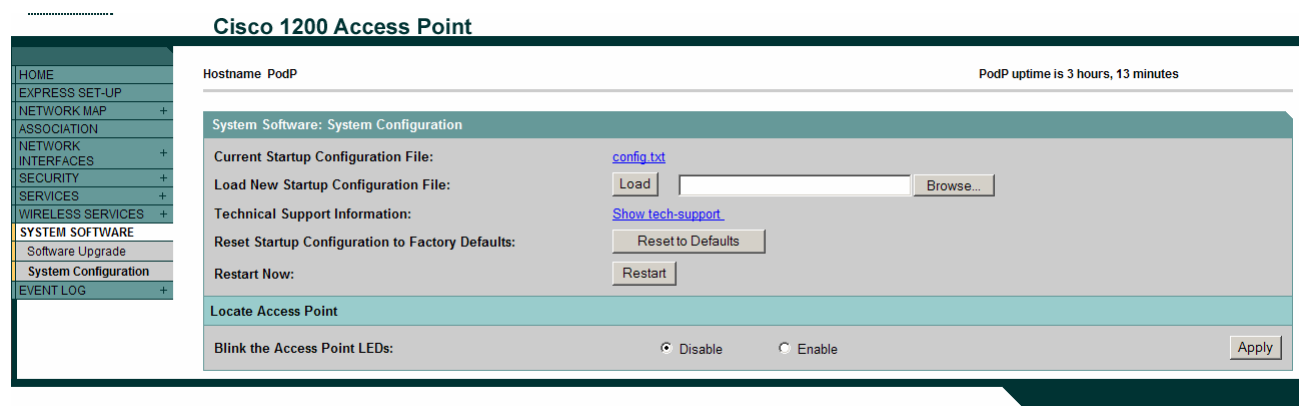
- AP
- PC or laptop
- Console cable
- SSH client software

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



- If there is an existing configuration on the AP, erase the configuration and reload either through GUI or IOS CLI.
- Configure the hostname, SSID, and BVI interface according to the Preparation table.

Step 2 Configure a new administrator account

The screenshot shows the Cisco 1200 Access Point configuration interface. The left sidebar contains a menu with options: HOME, EXPRESS SET-UP, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY (selected), Admin Access (selected), SSID Manager, Encryption Manager, Server Manager, Local RADIUS Server, Advanced Security, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG. The main content area is titled 'Cisco 1200 Access Point' and shows 'Hostname PodP' and 'PodP uptime is 3 hours, 15 minutes'. The 'Security: Admin Access' section is active, showing 'Administrator Authenticated by:' with radio buttons for 'Default Authentication (Global Password)' (selected), 'Local User List Only (Individual Passwords)', 'Authentication Server Only', and 'Authentication Server if not found in Local List'. Below this are fields for 'Default Authentication Password' and 'Confirm Authentication Password'. The 'Local User List (Individual Passwords)' section shows a 'User List' with a table containing a '< NEW >' button and a 'Cisco' entry. To the right of the table are fields for 'Username:', 'Password:', and 'Confirm Password:', and a 'Delete' button. Below the table are 'Capability Settings' with radio buttons for 'Read-Only' (selected) and 'Read-Write'. 'Apply' and 'Cancel' buttons are present at the bottom of each section.

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

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

Username: cIsCo123

Password: cIsCo123

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

The screenshot shows a login dialog box titled 'level 15 access'. It has a 'User name:' field with a dropdown menu showing 'cIsCo123' and a 'Password:' field with a bulleted password. There is a checkbox labeled 'Remember my password' which is unchecked. At the bottom are 'OK' and 'Cancel' buttons. A mouse cursor is pointing at the 'Remember my password' checkbox.

Step 3 Configure accurate time

Cisco 1200 Access Point

Hostname PodP PodP uptime is 3 hours, 32 minutes

Services: NTP- Network Time Protocol

NTP Server

Network Time Protocol (NTP): ☐ Enabled ☒ Disabled

Time Server (optional): (Hostname or IP Address)

Time Settings

GMT Offset: (hrs)

Use Daylight Savings Time (United States only): ☐ Yes ☒ No

Manually Set Date: (yyyy/mm/dd)

Manually Set Time: (hh:mm:ss)

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

- 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

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

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

Cisco 1200 Access Point

Hostname PodP PodP uptime is 3 hours, 34 minutes

System Software Version: IOS (tm) C1200 Software (C1200-K9W7-M)

Product/Model Number: AIR-AP1220-IOS-UPGRD

Top Assembly Serial Number:

System Software Filename: c1200-k9w7-tar.122-11.JA

System Software Version: 12.2(11)JA

Bootloader Version: 12.2(11)JA

System Uptime: 3 hours, 34 minutes

- 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.

The screenshot shows the Cisco 1200 Access Point configuration interface. The left sidebar contains a menu with options like HOME, EXPRESS SET-UP, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, SERVICES, Telnet/SSH, Hot Standby, CDP, DNS, Filters, HTTP, Proxy Mobile IP, QoS, SNMP, NTP, VLAN, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG. The main content area is titled 'Cisco 1200 Access Point' and shows the 'Services: Telnet/SSH' configuration page. The 'Telnet' section has 'Enabled' selected. The 'Terminal Type' is set to 'Teletype'. The 'Columns' are set to 80 (range 64-132) and 'Lines' are set to 24 (range 16-50). The 'Secure Shell Configuration' section has 'Secure Shell' set to 'Disabled'. The 'System Name' is 'DISABLED', 'Domain Name' is 'DISABLED', 'RSA Key Size (optional)' is '360-2048 bits', 'Authentication Timeout (optional)' is 'DISABLED (1-120 sec)', and 'Authentication Retries (optional)' is 'DISABLED (0-5)'. At the bottom, there is a table for 'Secure Shell Server Connections' with columns for Connection, Version, Encryption, State, and Username. The table is currently empty. At the bottom right, there are buttons for 'Apply', 'Cancel', and 'Refresh'.

- From the **SERVICES>Telnet/SSH** page enable Secure Shell.
- Enter the System name of PodP (where P is the pod number).
- Enter a domain name of fwl.com.
- Enter a key size (optional).
- Keep the default Timeout and Retries values.
- Click Apply.
- What is the default size, in bits, of the key modulus?

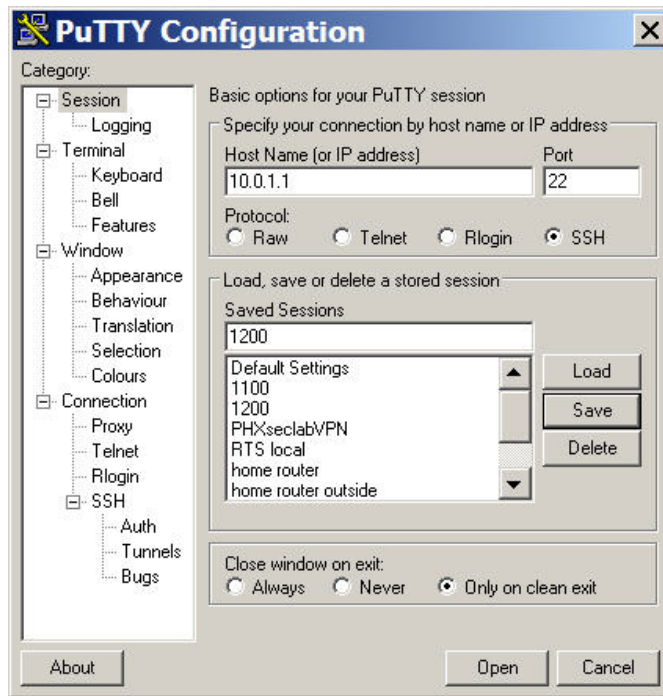
- Press **OK** to accept the default key size and continue.

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

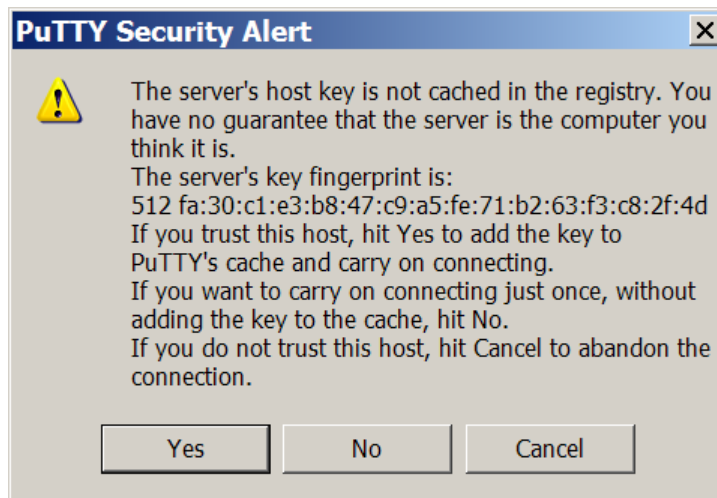
Step 6 Communicating between a SSH PC (client) to AP (server)

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.

- 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

Cisco 1200 Access Point

Hostname PodP PodP uptime is 3 hours, 50 minutes

Services: Telnet/SSH

Telnet: ☒ Enabled ☐ Disabled

Terminal Type: ☒ Teletype ☐ ANSI

Columns: (64-132)

Lines: (16-50)

Secure Shell Configuration

Secure Shell: ☒ Enabled ☐ Disabled

System Name:

Domain Name:

RSA Key Size (optional): (360-2048 bits)

Authentication Timeout (optional): (1-120 sec)

Authentication Retries (optional): (0-5)

Secure Shell Server Connections

Connection	Version	Encryption	State	Username
1	1.5	3DES	Session started	cIsCo123

Apply Cancel Refresh

- 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.