WEP on an Autonomous Access Point Configuration Example

Document ID: 116585

Contributed by Debashree Jena, Cisco TAC Engineer.
Oct 18, 2013

Contents

Introduction

This document describes how to use and configure Wired Equivalent Privacy (WEP) on a Cisco Autonomous Access Point (AP).

Prerequisites

Requirements

This document assumes that you can make an administrative connection to the WLAN devices, and that the devices function normally in an unencrypted environment. In order to configure a standard 40−bit WEP, you must have two or more radio units that communicate with each other.

Components Used

The information in this document is based on an 1140 AP that runs Cisco IOS® Release15.2JB.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

WEP is the encryption algorithm built into the 802.11 (Wi−Fi) standard. WEP uses the stream cipher RC4 for confidentiality, and the Cyclic Redundancy Check−32 (CRC−32) checksum for integrity .

Standard 64−bit WEP uses a 40 bit key (also known as WEP−40), which is concatenated with a 24−bit initialization vector (IV) in order to form the RC4 key. A 64−bit WEP key is usually entered as a string of 10

hexadecimal (base 16) characters (zero through nine and A−F). Each character represents four bits, and ten digits of four bits each equals 40 bits; if you add the 24−bit IV, it produces the complete 64−bit WEP key.

A 128−bit WEP key is usually entered as a string of 26 hexadecimal characters. Twenty−six digits of four bits each equals104 bits; if you add the 24−bit IV, it produces the complete 128−bit WEP key. Most devices allow the user to enter the key as 13 ASCII characters.

Authentication Methods

Two methods of authentication can be used with WEP: Open System Authentication and Shared Key Authentication.

With Open System Authentication, the WLAN client does not need to provide credentials to the AP for authentication. Any client can authenticate with the AP, and then attempt to associate. In effect, no authentication occurs. Subsequently, WEP keys can be used in order to encrypt data frames. At this point, the client must have the correct keys.

With Shared Key Authentication, the WEP key is used for authentication in a four−step, challenge−response handshake:

1. The client sends an authentication request to the AP.
2. The AP replies with a clear−text challenge.
3. The client encrypts the challenge−text with the configured WEP key, and responds with another authentication request.
4. The AP decrypts the response. If the response matches the challenge−text, the AP sends a positive reply.

After the authentication and association, the pre−shared WEP key is also used in order to encrypt the data frames with RC4.

At first glance, it might seem as though Shared Key Authentication is more secure than Open System Authentication, since the latter offers no real authentication. However, the reverse is true. It is possible to derive the keystream used for the handshake if you capture the challenge frames in Shared Key Authentication. Hence, it is advisable to use Open System Authentication for WEP authentication, rather than Shared Key Authentication.

Temporal Key Integrity Protocol (TKIP) was created in order to address these WEP issues. Similar to WEP, TKIP uses RC4 encryption. However, TKIP enhances WEP with the addition of measures such as per−packet key hashing, Message Integrity Check (MIC), and Broadcast key rotation in order to address known WEP vulnerabilities. TKIP uses the RC4 stream cipher with 128−bit keys for encryption and 64−bit keys for authentication.

Configure

This section provides the GUI and CLI configurations for WEP.

GUI Configuration

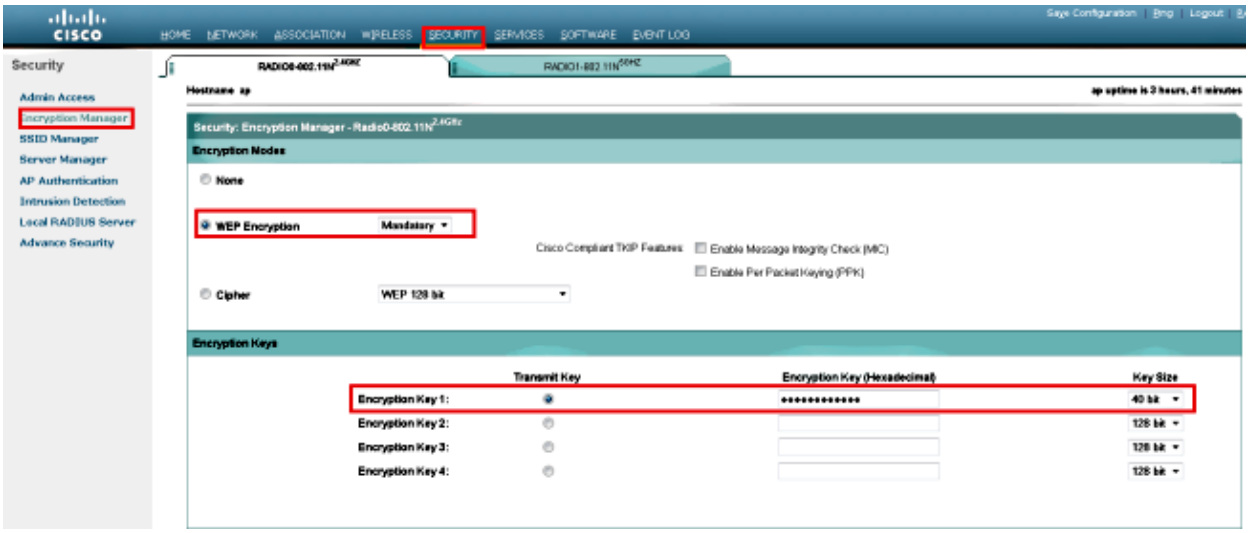
Complete these steps in order to configure WEP with the GUI.

1. Connect to the AP through the GUI.
2. From the Security menu on the left−side of the window, choose ***Encryption Manager*** for the radio interface to which you want to configure your static WEP keys.

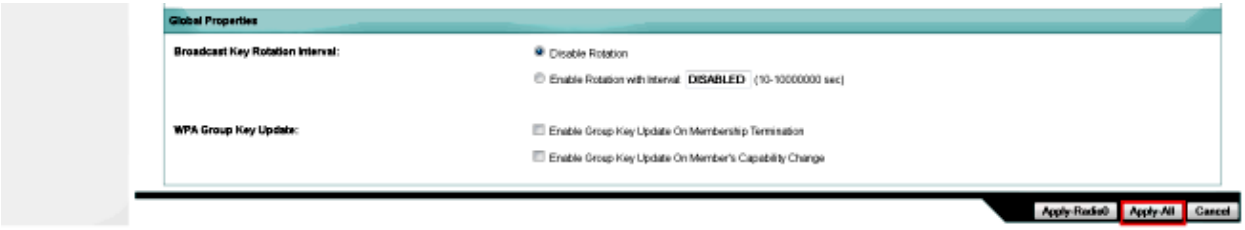
3. Under Encryption Modes, click ***WEP Encryption***, and select ***Mandatory*** from the drop−down menu for the client.

   The Encryption Modes used by Station are:
   - ***Default (No Encryption)*** − Requires clients to communicate with the AP without any data encryption. This setting is not recommended.
   - ***Optional*** − Allows clients to communicate with the AP either with or without data encryption. Typically, you use this option when you have client devices that cannot make a WEP connection, such as non−Cisco clients in a 128−bit WEP environment.
   - ***Mandatory (Full Encryption)*** − Requires clients to use data encryption when they communicate with the AP. Clients who do not use data encryption are not allowed to communicate. This option is recommended if you wish to maximize the security of your WLAN.
4. Under Encryption Keys, select the ***Transmit Key*** radio button, and enter the 10−digit hexadecimal key. Ensure that the Key Size is set to ***40 bit***.

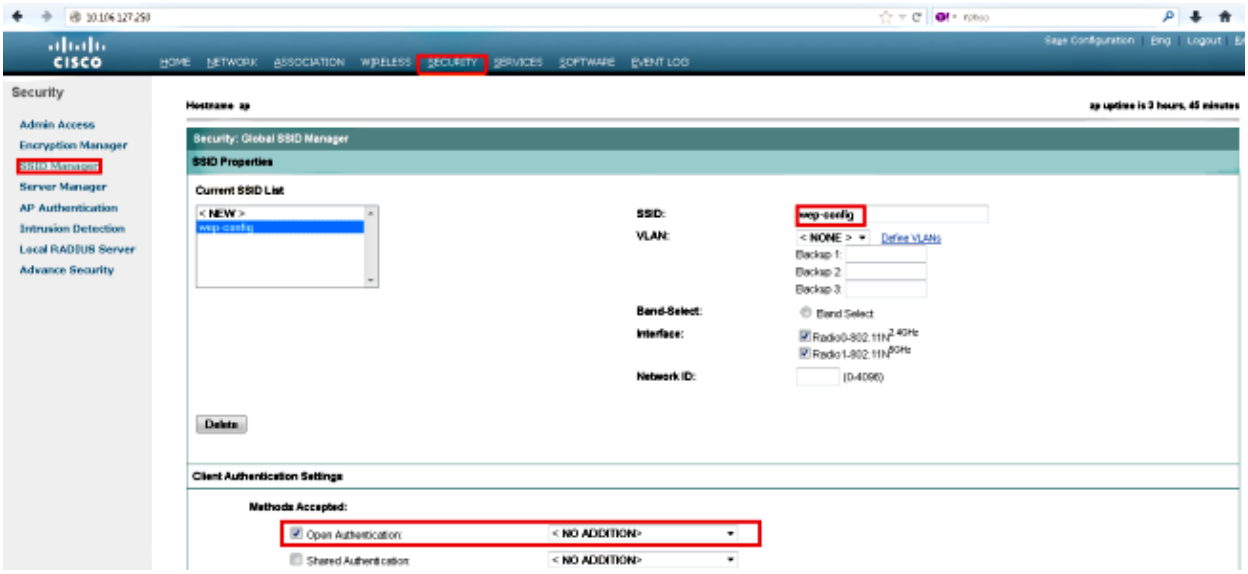
   Enter 10 hexadecimal digits for 40−bit WEP keys, or 26 hexadecimal digits for 128−bit WEP keys. The keys can be any combination of these digits:
   - 0 to 9
   - a to f
   - A to F



5. Click ***Apply−All*** in order to apply the configuration on both of the radios.



6. Create a Service Set Identifier (SSID) with ***Open Authentication***, and click ***Apply*** in order to enable it on both the radios.



7. Navigate to the network, and enable the radios for ***2.4 GHz*** and ***5 GHz*** in order to get them running.

CLI Configuration

Use this section in order to configure WEP with the CLI.

```
ap#show run
Building configuration...

Current configuration : 1794 bytes
!
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap
!
!
logging rate-limit console 9
enable secret 5 $1$kxBl$OhRR4QtTUVDUA9GakGDFs1
!
no aaa new-model
ip cef
!
!
!
```

```
dot11 syslog
!
  dot11 ssid wep-config
  authentication open
  guest-mode
!
!
crypto pki token default removal timeout 0
!
!
username Cisco password 7 0802455D0A16
!
!
bridge irb
!
!
!
interface Dot11Radio0
 no ip address
 !
 encryption key 1 size 40bit 7 447B6D514EB7 transmit-key
 encryption mode wep mandatory
 !
 ssid wep-config
 !
 antenna gain 0
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio1

 no ip address
 !
 encryption key 1 size 40bit 7 447B6D514EB7 transmit-key
 encryption mode wep mandatory
 !
 ssid wep-config
 !
 antenna gain 0
 dfs band 3 block
 channel dfs
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface GigabitEthernet0
 no ip address
 duplex auto
 speed auto
 no keepalive
 bridge-group 1
 bridge-group 1 spanning-disabled
 no bridge-group 1 source-learning
!
interface BVI1
 ip address dhcp
!
```

```
ip forward-protocol nd
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip route 0.0.0.0 0.0.0.0 10.106.127.4
!
bridge 1 route ip
!
!
!
line con 0
line vty 0 4
login local
transport input all
!
end
```

Verify

Enter this command in order to confirm that your configuration works properly:

```
ap#show dot11 associations
802.11 Client Stations on Dot11Radio0:
SSID [wep-config] :
MAC Address    IP address      Device        Name           Parent         State
1cb0.94a2.f64c 10.106.127.251  unknown       -              self           Assoc
```

Troubleshoot

Use this section in order to troubleshoot your configuration.

Note: Refer to Important Information on Debug Commands before you use ***debug*** commands.

These ***debug*** commands are useful in order to troubleshoot the configuration:

- ***debug dot11 events*** − Enables the debug for all dot1x events.
- ***debug dot11 packets*** − Enables the debug for all dot1x packets.

Here is an example of the log that displays when the client successfully associates to the WLAN:

```
*Mar  1 02:24:46.246: %DOT11-6-ASSOC: Interface Dot11Radio0, Station
1cb0.94a2.f64c Associated KEY_MGMT[NONE]
```

When the client enters the wrong key, this error displays:

```
*Mar  1 02:26:00.741: %DOT11-4-ENCRYPT_MISMATCH: Possible encryption key
mismatch between interface Dot11Radio0 and station 1cb0.94a2.f64c
*Mar  1 02:26:21.312: %DOT11-6-DISASSOC: Interface Dot11Radio0, Deauthenticating
Station 1cb0.94a2.f64c Reason: Sending station has left the BSS
*Mar  1 02:26:21.312: *** Deleting client 1cb0.94a2.f64c
```

Updated: Oct 18, 2013 Document ID: 116585