

WPA Configuration Overview

Document ID: 44721

You need a valid Cisco.com account in order to download Cisco Aironet drivers, firmware, and utilities from Downloads – Wireless (registered customers only) . If you do not have a Cisco.com account, register for free at the Cisco.com Registration page.

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Background Theory
- Conventions

Configure

- Network EAP or Open Authentication with EAP
- CLI Configuration
- GUI Configuration

Verify

Troubleshoot

- Troubleshoot Procedure
- Troubleshoot Commands

Related Information

Introduction

This document provides a sample configuration for Wi-Fi Protected Access (WPA), the interim security standard that Wi-Fi Alliance members use.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Thorough knowledge of wireless networks and wireless security issues
- Knowledge of Extensible Authentication Protocol (EAP) security methods

Components Used

The information in this document is based on these software and hardware versions:

- Cisco IOS® Software-based access points (APs)
- Cisco IOS Software Release 12.2(15)JA or later

Note: Preferably, use the latest Cisco IOS Software release, even though WPA is supported in Cisco IOS Software Release 12.2(11)JA and later. In order to obtain the latest Cisco IOS Software release,

refer to Downloads (registered customers only) .

- A WPA-compliant network interface card (NIC) and its WPA-compliant client software

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 Theory

Security features in a wireless network, such as WEP, are weak. The Wi-Fi Alliance (or WECA) industry group devised a next-generation, interim security standard for wireless networks. The standard provides defense against weaknesses until the IEEE organization ratifies the 802.11i standard.

This new scheme builds on current EAP/802.1x authentication and dynamic key management, and adds stronger cipher encryption. After the client device and the authentication server make an EAP/802.1x association, WPA key management is negotiated between the AP and the WPA-compliant client device.

Cisco AP products also provide for a hybrid configuration in which both legacy WEP-based EAP clients (with legacy or no key management) work in conjunction with WPA clients. This configuration is referred to as migration mode. Migration mode allows for a phased approach to migrate to WPA. This document does not cover migration mode. This document provides an outline for a pure WPA-secured network.

In addition to enterprise- or corporate-level security concerns, WPA also provides a Pre-Shared Key version (WPA-PSK) that is intended for use in small office, home office (SOHO) or home wireless networks. Cisco Aironet Client Utility (ACU) does not support WPA-PSK. The Wireless Zero Configuration utility from Microsoft Windows supports WPA-PSK for most wireless cards, as do these utilities:

- AEGIS Client from Meetinghouse Communications

Note: Refer to EOS and EOL Announcement for the Meetinghouse AEGIS Product Line.

- Odyssey client from Funk Software

Note: Refer to Juniper Networks Customer Support Center .

- Original equipment manufacturer (OEM) client utilities from some manufacturers

You can configure WPA-PSK when:

- You define the Encryption Mode as Cipher Temporal Key Integrity Protocol (TKIP) on the Encryption Manager tab.
- You define the authentication type, the use of authenticated key management, and the pre-shared key on the Service Set Identifier (SSID) Manager tab of the GUI.
- No configuration is required on the Server Manager tab.

In order to enable WPA-PSK through the command-line interface (CLI), enter these commands. Start from the configuration mode:

```
AP(config)#interface dot11Radio 0
AP(config-if)#encryption mode ciphers tkip
AP(config-if)#ssid ssid_name

AP(config-if-ssid)#authentication open
AP(config-if-ssid)#authentication key-management wpa
AP(config-if-ssid)#wpa-psk ascii pre-shared_key
```

Note: This section provides only the configuration that is relevant to WPA–PSK. The configuration in this section is only to give you an understanding on how to enable WPA–PSK and is not the focus of this document. This document explains how to configure WPA.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Configure

WPA builds on the current EAP/802.1x methods. This document assumes that you have a Light EAP (LEAP), EAP, or Protected EAP (PEAP) configuration that works before you add the configuration in order to engage WPA.

This section presents the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network EAP or Open Authentication with EAP

In any EAP/802.1x–based authentication method, you may question what the differences are between Network–EAP and Open authentication with EAP. These items refer to values in the Authentication Algorithm field in the headers of management and association packets. Most manufacturers of wireless clients set this field at the value 0 (Open authentication), and then signal their desire to do EAP authentication later in the association process. Cisco sets the value differently, from the start of association with the Network EAP flag.

Use the authentication method that this list indicates if your network has clients that are:

- Cisco clients Use Network–EAP.
- Third–party clients (which include Cisco Compatible Extensions [CCX]–compliant products) Use Open authentication with EAP.
- A combination of both Cisco and third–party clients Choose both Network–EAP and Open authentication with EAP.

CLI Configuration

This document uses these configurations:

- A LEAP configuration that exists and works
- Cisco IOS Software Release 12.2(15)JA for the Cisco IOS Software–based APs

AP

```
ap1#show running-config
Building configuration...
.
.
.
aaa new-model
!
aaa group server radius rad_eap
server 192.168.2.100 auth-port 1645 acct-port 1646
.
```

```

.
aaa authentication login eap_methods group rad_eap
.
.
!
bridge irb
!
interface Dot11Radio0
no ip address
no ip route-cache
!
encryption mode ciphers tkip

!--- This defines the cipher method that WPA uses. The TKIP
!--- method is the most secure, with use of the Wi-Fi-defined version of TKIP.

!
ssid WPAlabap1200
authentication open eap eap_methods

!--- This defines the method for the underlying EAP when third-party clients
!--- are in use.

authentication network-eap eap_methods

!--- This defines the method for the underlying EAP when Cisco clients are in use.

authentication key-management wpa

!--- This engages WPA key management.

!
speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
rts threshold 2312
channel 2437
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
.
.
.
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
bridge-group 1
no bridge-group 1 source-learning
bridge-group 1 spanning-disabled
!
interface BVI1
ip address 192.168.2.108 255.255.255.0

!--- This is the address of this unit.

no ip route-cache
!
ip default-gateway 192.168.2.1

```

```
ip http server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag/ivory/1100
ip radius source-interface BVI1
snmp-server community cable RO
snmp-server enable traps tty
radius-server host 192.168.2.100 auth-port 1645 acct-port 1646 key shared_secret

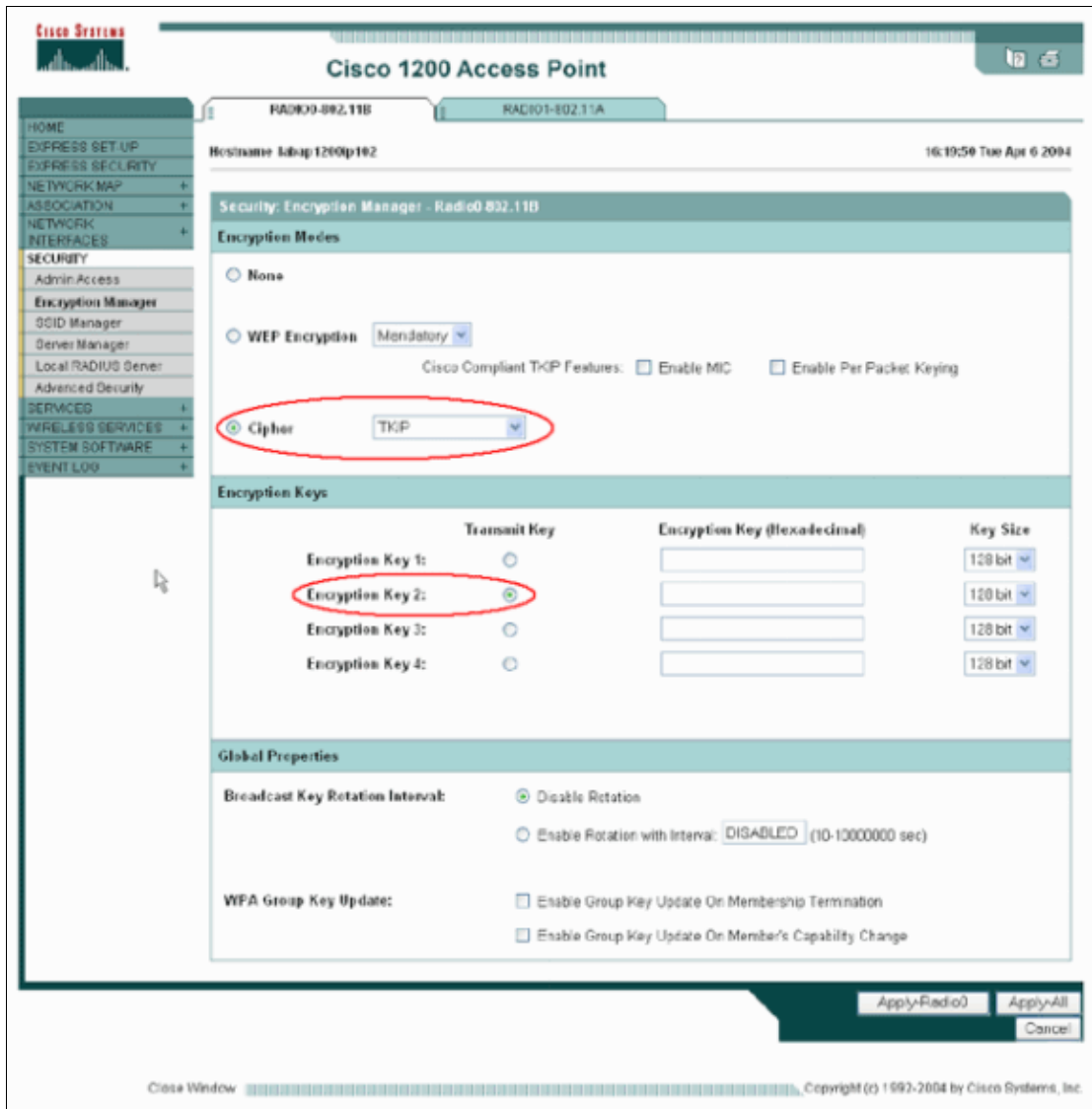
!--- This defines where the RADIUS server is and the key between the AP and server.

radius-server retransmit 3
radius-server attribute 32 include-in-access-req format %h
radius-server authorization permit missing Service-Type
radius-server vsa send accounting
bridge 1 route ip
!
!
line con 0
line vty 5 15
!
end
!
end
```

GUI Configuration

Complete these steps in order to configure the AP for WPA:

1. Complete these steps in order to set up the Encryption Manager:
 - a. Enable Cipher for TKIP.
 - b. Clear the value in Encryption Key 1.
 - c. Set Encryption Key 2 as the Transmit Key.
 - d. Click **Apply–Radio#** .



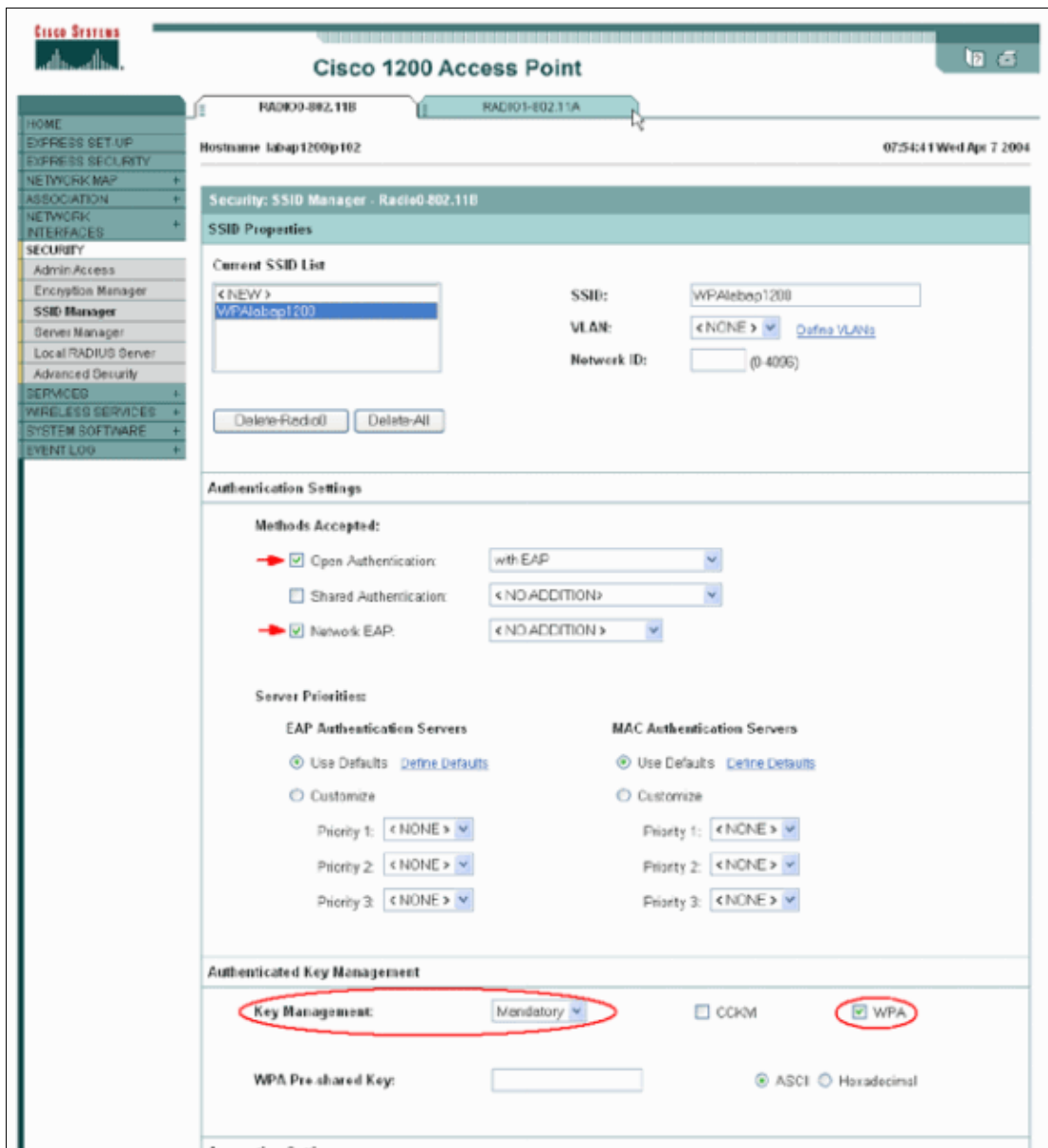
2. Complete these steps in order to set up the SSID Manager:

- a. Select the desired SSID from Current SSID List.
- b. Choose an appropriate authentication method.

Base this decision on the type of client cards that you use. See the Network EAP or Open Authentication with EAP section of this document for more information. If EAP worked before the addition of WPA, a change is probably not necessary.

c. Complete these steps in order to enable key management:

- a. Choose **Mandatory** from the Key Management drop-down menu.
- b. Check the WPA check box.
- d. Click **Apply-Radio#** .

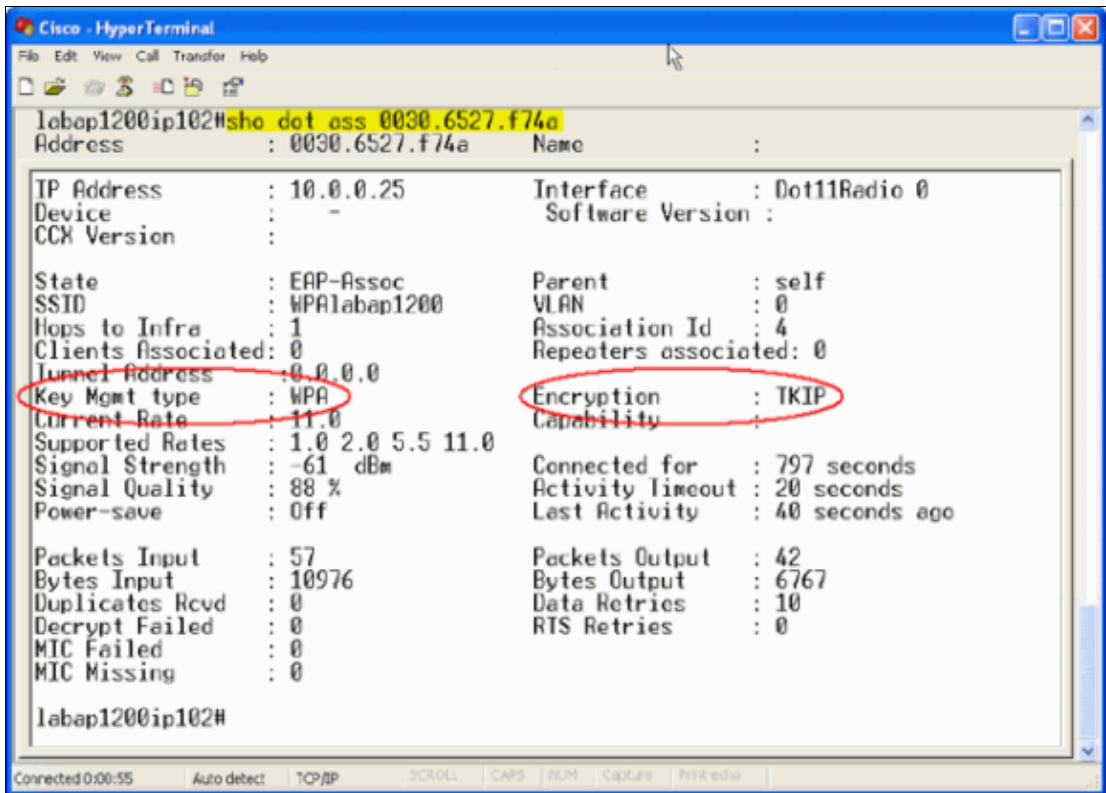


Verify

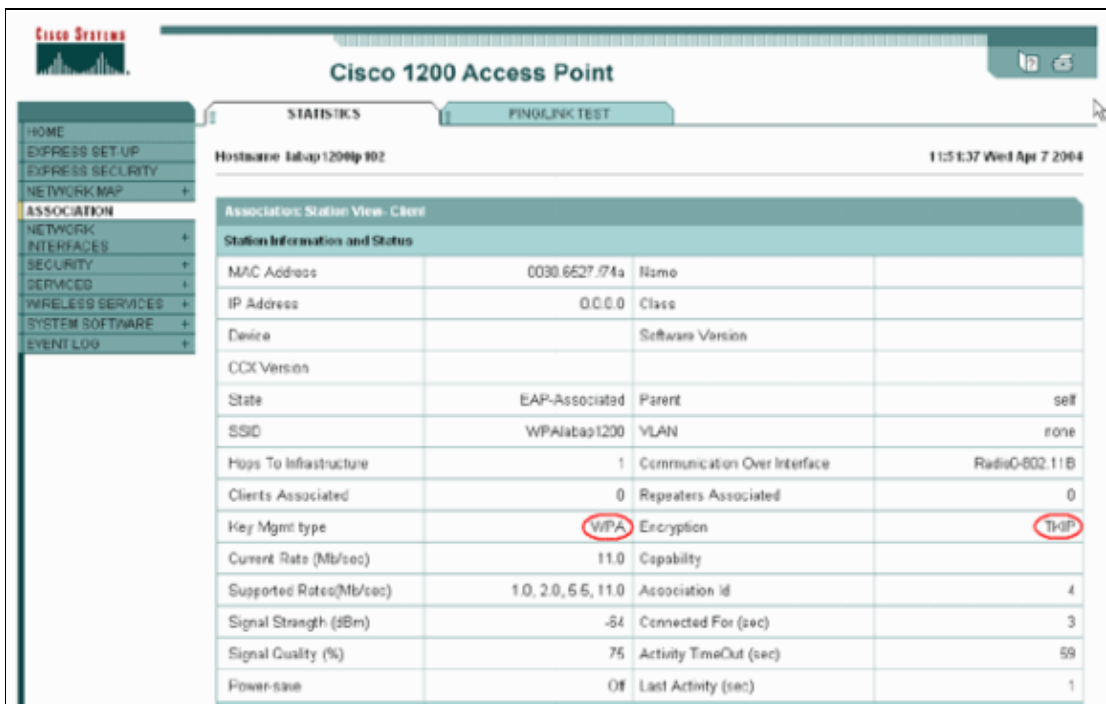
Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **show dot11 association mac_address** This command displays information about a specifically identified associated client. Verify that the client negotiates Key Management as **WPA** and Encryption as **TKIP**.



- The Association table entry for a particular client must also indicate Key Management as **WPA** and Encryption as **TKIP**. In the Association table, click a particular MAC address for a client in order to see the details of the association for that client.



Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Troubleshoot Procedure

This information is relevant to this configuration. Complete these steps in order to troubleshoot your configuration:

1. If this LEAP, EAP, or PEAP configuration has not been thoroughly tested before WPA implementation, you must complete these steps:
 - a. Temporarily disable the WPA encryption mode.
 - b. Reenable the appropriate EAP.
 - c. Confirm that the authentication works.
2. Verify that the configuration of the client matches that of the AP.

For example, when the AP is configured for WPA and TKIP, confirm that the settings match the settings that are configured in the client.

Troubleshoot Commands

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

WPA key management involves a four-way handshake after EAP authentication successfully completes. You can see these four messages in debugs. If EAP does not successfully authenticate the client or if you do not see the messages, complete these steps:

1. Temporarily disable WPA.
2. Reenable the appropriate EAP.
3. Confirm that the authentication works.

This list describes the debugs:

- **debug dot11 aaa manager keys** This debug shows the handshake that happens between the AP and the WPA client as the pairwise transient key (PTK) and group transient key (GTK) negotiate. This debug was introduced in Cisco IOS Software Release 12.2(15)JA.

```
debug dot11 aaa manager keys
labap1200ip102#
Apr  7 16:29:57.908: dot11_dot1x_build_ptk_handshake: building PTK msg 1 for
0030.6527.f74a
Apr  7 16:29:59.190: dot11_dot1x_verify_ptk_handshake: verifying PTK msg 2 from
0030.6527.f74a
Apr  7 16:29:59.191: dot11_dot1x_verify_eapol_header: Warning: Invalid key info
(exp=0x381, act=0x109)
Apr  7 16:29:59.191: dot11_dot1x_verify_eapol_header: Warning: Invalid key len
(exp=0x20, act=0x0)
Apr  7 16:29:59.192: dot11_dot1x_build_ptk_handshake: building PTK msg 3 for
0030.6527.f74a
Apr  7 16:29:59.783: dot11_dot1x_verify_ptk_handshake: verifying PTK msg 4 from
0030.6527.f74a
Apr  7 16:29:59.783: dot11_dot1x_verify_eapol_header: Warning: Invalid key info
(exp=0x381, act=0x109)
Apr  7 16:29:59.783: dot11_dot1x_verify_eapol_header: Warning: Invalid key len
(exp=0x20, act=0x0)
Apr  7 16:29:59.788: dot11_dot1x_build_gtk_handshake: building GTK msg 1 for
0030.6527.f74a
Apr  7 16:29:59.788: dot11_dot1x_build_gtk_handshake: dot11_dot1x_get_multicast_key
len 32 index 1
Apr  7 16:29:59.788: dot11_dot1x_hex_dump: GTK: 27 CA 88 7D 03 D9 C4 61 FD 4B BE 71
```

```
EC F7 43 B5 82 93 57 83
Apr  7 16:30:01.633: dot11_dot1x_verify_gtk_handshake: verifying GTK msg 2 from
0030.6527.f74a
Apr  7 16:30:01.633: dot11_dot1x_verify_eapol_header: Warning: Invalid key info
(exp=0x391, act=0x301)
Apr  7 16:30:01.633: dot11_dot1x_verify_eapol_header: Warning: Invalid key len
(exp=0x20, act=0x0)
Apr  7 16:30:01.633: %DOT11-6-ASSOC: Interface Dot11Radio0, Station 0030.6527.f74a
Associated KEY_MGMT[WPA]
labap1200ip102#
```

If no debug outputs appear, verify these items:

- ◆ The terminal monitor **term mon** is enabled (if you use a Telnet session).
- ◆ The debugs are enabled.
- ◆ The client is appropriately configured for WPA.

If the debug shows that PTK and/or GTK handshakes are built but not verified, check the WPA supplicant software for the correct configuration and up-to-date version.

- **debug dot11 aaa authenticator state-machine** This debug shows the various states of negotiations that a client goes through as it associates and authenticates. The state names indicate these states. This debug was introduced in Cisco IOS Software Release 12.2(15)JA. The debug obsoletes the **debug dot11 aaa dot1x state-machine** command in Cisco IOS Software Release 12.2(15)JA and later.
- **debug dot11 aaa dot1x state-machine** This debug shows the various states of negotiations that a client goes through as it associates and authenticates. The state names indicate these states. In Cisco IOS Software releases that are earlier than Cisco IOS Software Release 12.2(15)JA, this debug also shows the WPA key management negotiation.
- **debug dot11 aaa authenticator process** This debug is most helpful to diagnose problems with negotiated communications. The detailed information shows what each participant in the negotiation sends and shows the response of the other participant. You can also use this debug in conjunction with the **debug radius authentication** command. This debug was introduced in Cisco IOS Software Release 12.2(15)JA. The debug obsoletes the **debug dot11 aaa dot1x process** command in Cisco IOS Software Release 12.2(15)JA and later.
- **debug dot11 aaa dot1x process** This debug is helpful to diagnose problems with negotiated communications. The detailed information shows what each participant in the negotiation sends and shows the response of the other participant. You can also use this debug in conjunction with the **debug radius authentication** command. In Cisco IOS Software releases that are earlier than Cisco IOS Software Release 12.2(15)JA, this debug shows the WPA key management negotiation.

Related Information

- [Configuring Cipher Suites and WEP](#)
- [Configuring Authentication Types](#)
- [WPA2 – Wi-Fi Protected Access 2](#)
- [Wi-Fi Protected Access 2 \(WPA 2\) Configuration](#)
- [Technical Support & Documentation – Cisco Systems](#)