Table of Contents

WPA Configuration Overview

To get Cisco Aironet drivers, firmware and utility software, follow this link to the Cisco Wireless Software Center.

Introduction

This document provides a sample configuration for Wi−Fi Protected Access (WPA), the interim security standard used by Wi−Fi Alliance members.

Prerequisites

Requirements

Before you begin this configuration, ensure that you meet these requirements:

- Thorough knowledge of wireless networks and wireless security issues
- Knowledge of EAP security methods

Components Used

The information in this document is based on the software and hardware versions below.

- Cisco IOS−based access points
- IOS Release 12.2(15)JA or later, preferably the latest version of IOS (although WPA has been supported since 12.2(11)JA
- WPA−compliant network interface card (NIC) and its WPA−compliant client software

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you work in a live network, ensure that you understand the potential impact of any command before you use it.

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 to provide 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. Once an EAP/802.1x association is made between the client device and the authentication server, WPA key management is negotiated between the access point (AP) and the WPA−compliant client device.

Cisco access point 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 is referred to as migration mode and allows for a phased approach to migrate to WPA. Migration mode is not covered in this document, in the interest of providing 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), intended for use in SOHO or home wireless networks. Current versions of Aironet Client Utility (ACU) and Aironet Desktop Utility (ADU) from Cisco do not support WPA−PSK. Wireless Zero Configuration utility from Microsoft Windows supports WPA−PSK for most wireless cards, as do AEGIS Client from Meetinghouse Communications , Odyssey client from Funk Software, and OEM client utilities from some manufacturers . You can configure WPA−PSK when you:

1. Define the Encryption Mode as Cipher TKIP on the Encryption Manager tab
2. Define the authentication type, the use of authenticated key management, and the pre−shared key on the SSID Manager tab of the GUI
3. No configuration is required on the Server Manager tab.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Configure

WPA builds on the current EAP/802.1x methods. This document assumes you have a LEAP, EAP, or PEAP configuration that works prior to when you add the configuration to engage WPA.

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

Note: To find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only) .

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) 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.

If your network has clients that are:

- Cisco clients use Network−EAP
- Third party clients (include CCX compliant products) use Open with EAP
- A combination of both Cisco and third party clients choose both Network−EAP and Open with EAP

CLI Configuration

This document uses these configurations:

- A LEAP configuration that exist and works
- IOS release 12.2(15)JA for the IOS based access points

Access Point

```
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 used by WPA.  The TKIP
!−−− method is the most secure, using the Wi−Fi defined version of TKIP.


 !
 ssid WPAlabap1200
    authentication open eap eap_methods

!−−− Defines method for the underlying EAP when third party clients are in use.

    authentication open network−eap eap_methods

!−−− Defines method for the underlying EAP when Cisco clients are in use.

    authentication key−management wpa

!−−− 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
```

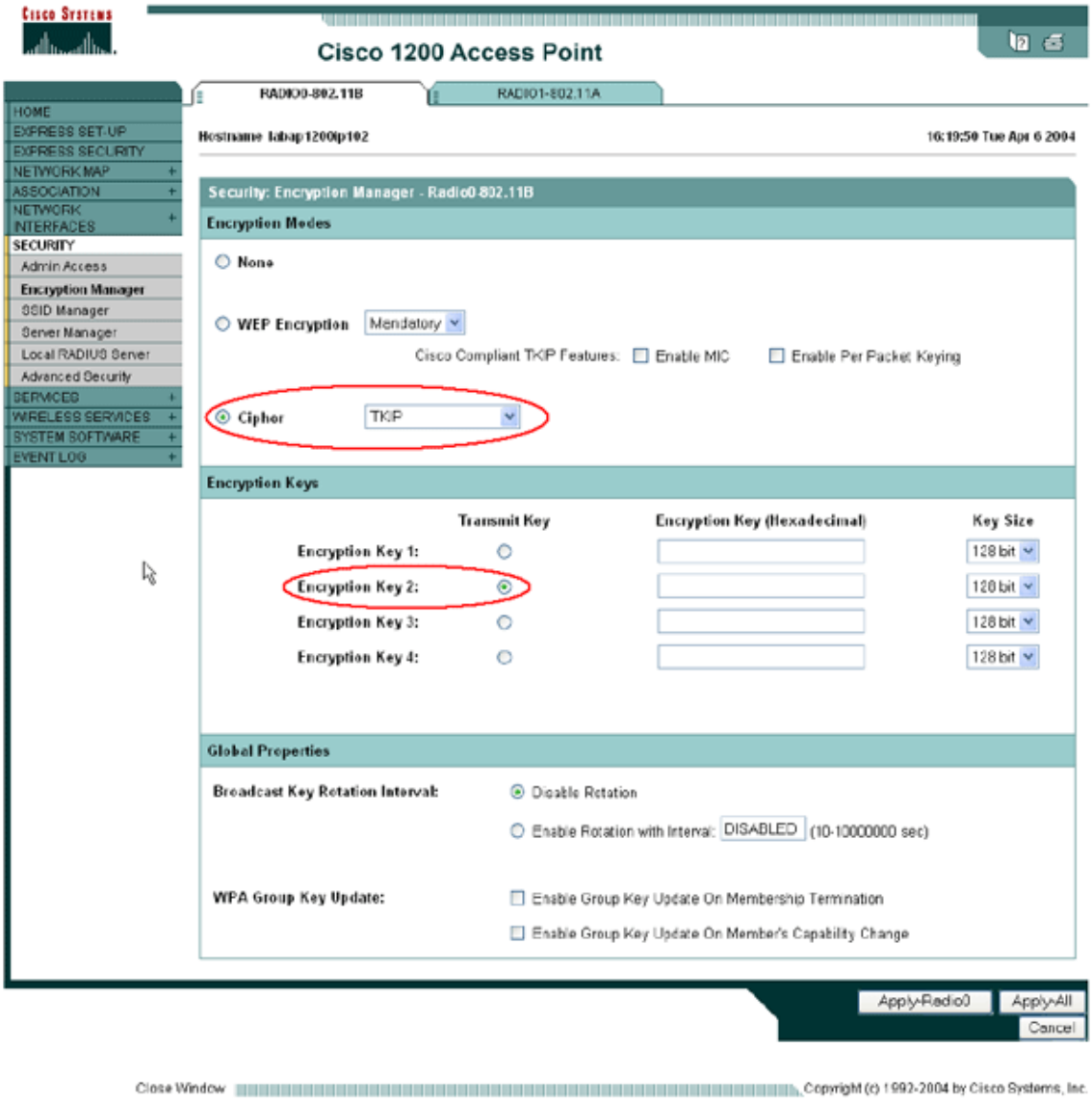
```
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
.
.
.
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
interface BVI1
 ip address 192.168.2.108 255.255.255.0
!--- 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

!--- Defines where RADIUS server is and key between 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

To configure the access point for WPA, follow these steps.

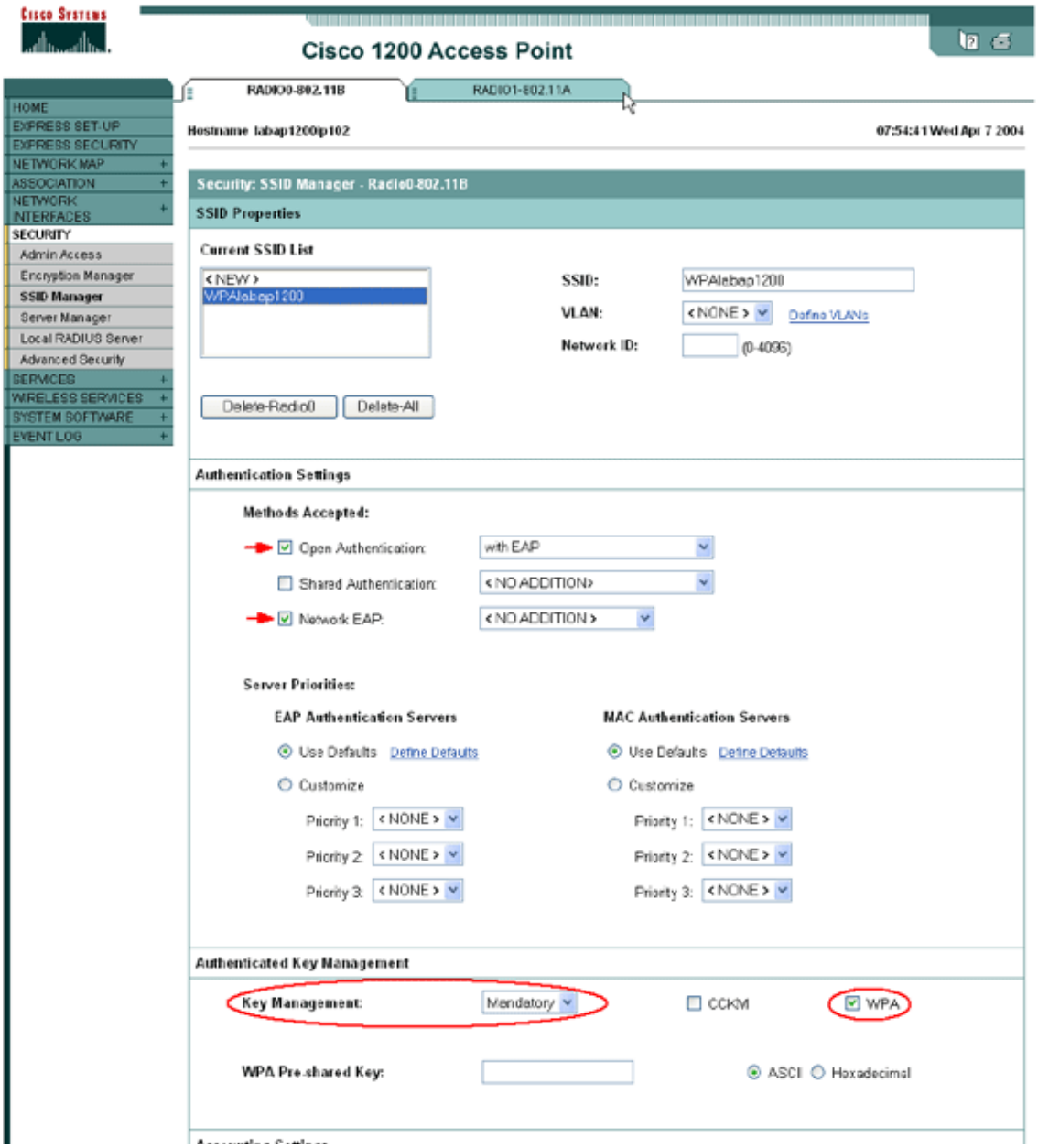
1. Setup the Encryption Manager

   - ♦ Enable Cipher for TKIP.
   - ♦ Clear the value in Key 1.
   - ♦ Set Encryption Key 2 as the Transmit Key.
   - ♦ Click the Apply−Radio# button.



2. Setup the SSID Manager

- Select the desired SSID from Current SSID List.
- Choose an appropriate authentication method, by which type of client cards used. If EAP worked prior to the addition of WPA, you should not require change.
- Enable key management. First choose Mandatory from the pulldown box, then check the box to choose WPA.
- Click **Apply−*Radio#***

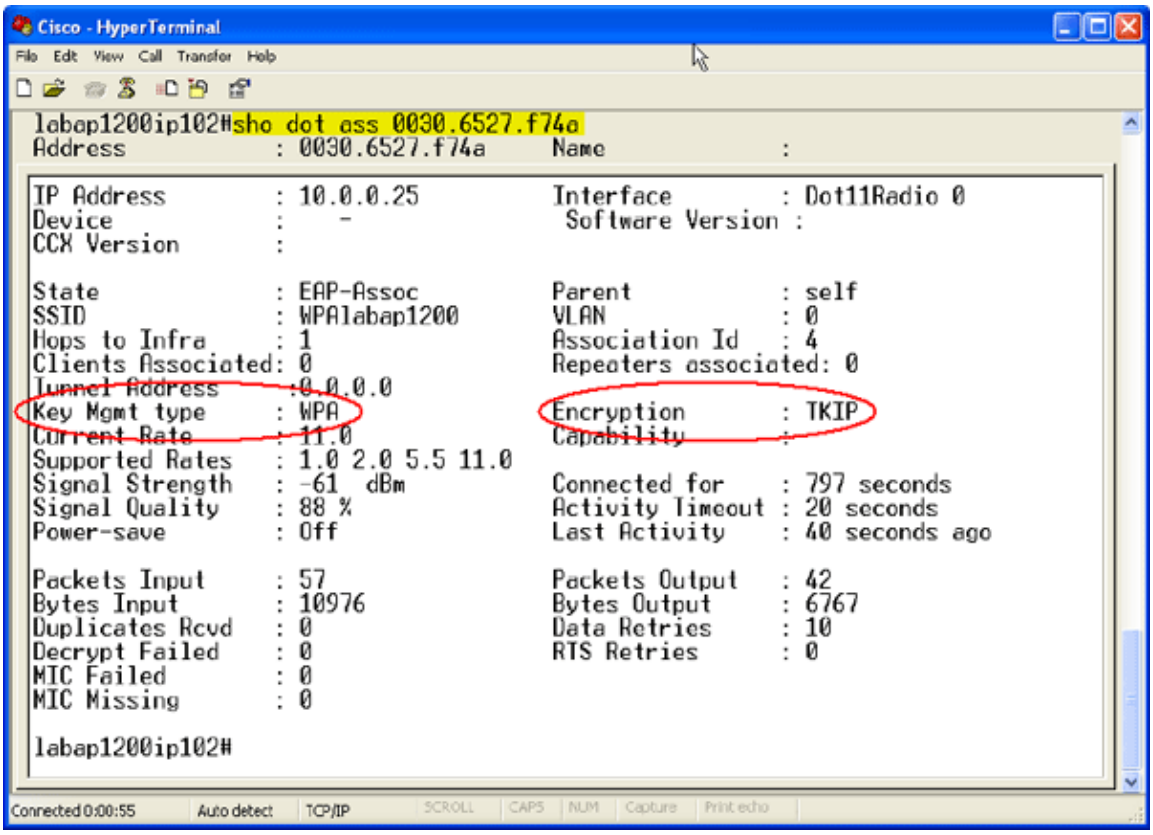


Verify

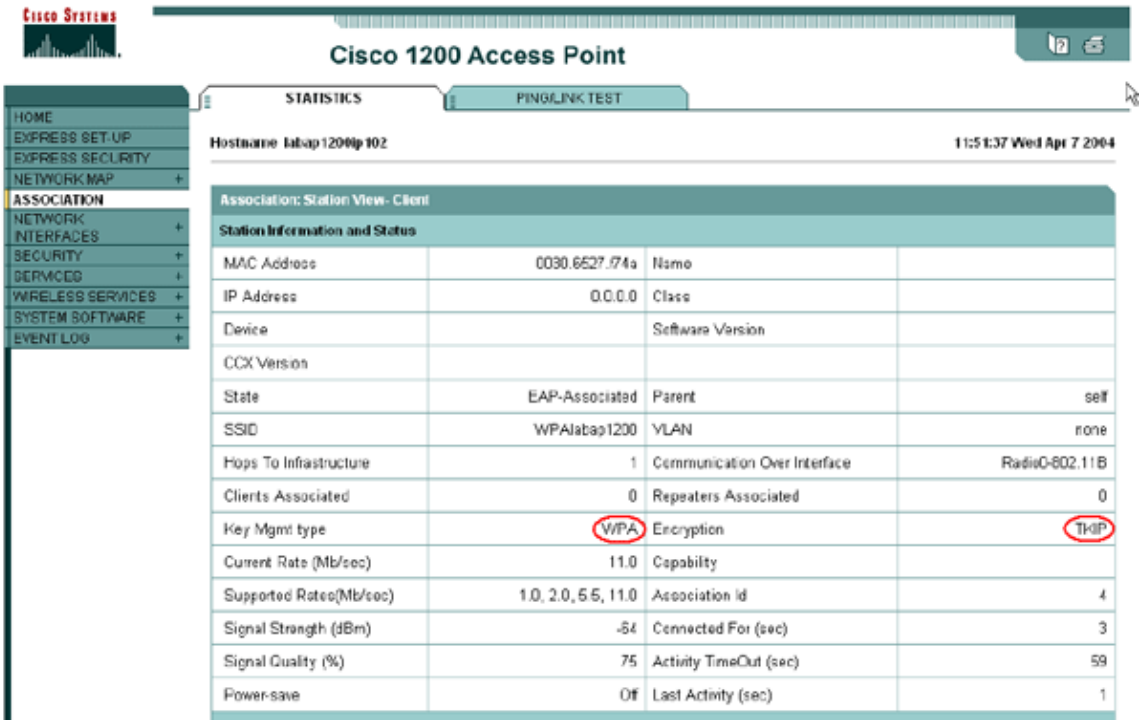
This section provides information you can use to confirm your configuration works properly.

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

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



- The Association Table entry for a given client should also indicate Key Management as **WPA** and Encryption as **TKIP**. From the Association Table, click a givenMAC address for a client 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. Follow the instructions to troubleshoot your configuration.

1. If this LEAP, EAP, or PEAP configuration is not thoroughly tested prior to WPA implementation, you must follow these steps:

    a. Temporarily disable the WPA encryption mode
    b. Re−enable the appropriate EAP
    c. Confirm that the authentication works
2. Verify that the configuration of the client matches that of the access point. For example, when the access point is configured for WPA and TKIP, confirm that the settings match those configured in the client.

Troubleshoot Commands

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

Note: Before you issue **debug** commands, refer to Important Information on Debug Commands.

WPA key management involves a 4−way handshake after EAP authentication successfully completes. These four messages are seen in debugs. If EAP does not successfully authenticate the client or if the messages are not seen, follow these steps:

1. Temporarily disable WPA
2. Re−enable the appropriate EAP
3. Confirm that the authentication works

- **debug dot11 aaa manager keys** − This debug shows the handshake that happens between the access point and the WPA client, as the PTK and GTK negotiate. This debug was introduced in IOS 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=0
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=0
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
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 8
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=0
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
labap1200ip102#
```

If no debug outputs appear, verify that the terminal monitor **term mon** is enabled (if you use a telnet session), that the debugs are enabled, and that the client is appropriately configured for WPA.

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

- **debug dot11 aaa authenticator state−machine** This debug shows the various states of negotiations a client goes through as it associates and authenticates, indicated by their state names. This debug was introduced in IOS release 12.2(15)JA, and obsoletes debug dot11 aaa dot1x state−machine in that and subsequent releases.
- **debug dot11 aaa dot1x state−machine** This debug shows the various states of negotiations a client goes through as it associates and authenticates, indicated by their state names. In IOS releases prior to 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. This detailed information shows what each participant in the negotiation sends, and what the response is of the other participant . It can also be used in conjunction with `DEBUG RADIUS AUTHENTICATION`. This debug was introduced in IOS release 12.2(15)JA and obsoletes debug dot11 aaa dot1x process in that and subsequent releases.
- **debug dot11 aaa dot1x process** This debug is helpful to diagnose problems with negotiated communications. This detailed information shows what each participant in the negotiation sends, and what the response is of the other participant . It can also be used in conjunction with `DEBUG RADIUS AUTHENTICATION`. In IOS releases prior to 12.2(15)JA, this debug shows the WPA key management negotiation.

NetPro Discussion Forums − Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums − Featured Conversations for Wireless
Wireless − Mobility: WLAN Radio Standards
Wireless − Mobility: Security and Network Management
Wireless − Mobility: Getting Started with Wireless
Wireless − Mobility: General

Related Information

- **Configuring Cipher Suites and WEP**
- **Configuring Authentication Types**
- **Wi−Fi Protected Access (WPA) Security Website**
- **Technical Support − Cisco Systems**