# 在Cisco 统一无线网络的Wi-Fi Protected Access (WPA) 配置示例

# 目录

 简介

 先决条件

 要求

 使用的组件

 规则

 WPA 和 WPA2 支持

 网络设置

 针对 WPA2 企业模式配置设备

 配置 WLC 以便通过外部 RADIUS 服务器进行 RADIUS 身份验证

 针对 WPA2 企业模作模式配置 WLAN

 针对 WPA2 企业操作模式配置无线客户端

 针对 WPA2 个人模式配置设备

 故障排除

 相关信息

# <u>简介</u>

本文档说明如何配置 Cisco 统一无线网络中的 Wi-Fi 安全访问 (WPA)。

# <u>先决条件</u>

# <u>要求</u>

在尝试进行此配置之前,请确保您已具有以下主题的基础知识:

- WPA
- 无线 LAN (WLAN) 安全解决方案**注意:有关**思科WLAN安全解决方案的信息,请参阅<u>思科无线</u> LAN安全概述。

## <u>使用的组件</u>

本文档中的信息基于以下软件和硬件版本:

- Cisco 1000 系列轻量接入点 (LAP)
- 运行固件 4.2.61.0 的 Cisco 4404 无线 LAN 控制器 (WLC)

- •运行固件 4.1 的 Cisco 802.11a/b/g 客户端适配器
- 运行固件 4.1 的 Aironet Desktop Utility (ADU)
- Cisco Secure ACS 服务器版本 4.1

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

#### <u>规则</u>

有关文档约定的更多信息,请参考 Cisco 技术提示约定。

# <u>WPA 和 WPA2 支持</u>

Cisco 统一无线网络支持 Wi-Fi 联盟证书 WPA 和 WPA2。Wi-Fi 联盟于 2003 年引入 WPA。Wi-Fi 联盟于 2004 年引入 WPA2。所有经过 Wi-Fi WPA2 认证的产品都必须能够与经过 Wi-Fi WPA 认证 的产品进行互操作。

WPA 和 WPA2 为最终用户和网络管理员提供了高级别的保证,确保他们的数据保持私密性,并将 对他们网络的访问限制在授权用户范围内。这两种证书都有个人和企业两种操作模式,可满足两个 市场分区的不同需要。每个证书的企业模式使用 IEEE 802.1X 和 EAP 进行身份验证。每个证书的 个人模式使用预共享密钥 (PSK) 进行身份验证。Cisco 建议不要使用个人模式进行企业或政府部署 ,因为该模式使用 PSK 进行用户身份验证。PSK 对于企业环境并不安全。

WPA 可以解决原始 IEEE 802.11 安全实施中出现的所有已知 WEP 漏洞,为企业和小型办公室/家庭办公室 (SOHO) 环境中的 WLAN 提供了一种即时安全解决方案。WPA 使用 TKIP 进行加密。

WPA2 是新一代 Wi-Fi 安全证书。它是 Wi-Fi 联盟对已批准的 IEEE 802.11i 标准的可互操作实现。 它将计数器模式与密码块链消息身份验证码协议 (CCMP) 结合使用,实现了美国国家标准与技术研 究所 (NIST) 建议的 AES 加密算法。WPA2 促进了政府 FIPS 140-2 标准的实行。

	WPA	WPA2
	• 身份验证	• 身份验证
	: IEEE	: IEEE
<u> </u>	802.1X/	802.1X/EA
正业侯氏(正业、政府、 教查)	EAP	Р
¥X FI )	• 加密	• 加密
	: TKIP/	: AES-
	MIC	CCMP
	• 身份验证	• 身份验证
	: PSK	: PSK
个人候氏(SUHU、家庭 /个上)	• 加密	• 加密
(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1	: TKIP/	: AES-
	MIC	CCMP

WPA 与 WPA2 的模式类型比较

在企业操作模式下,WPA 和 WPA2 均使用 802.1X/EAP 进行身份验证。802.1X 为 WLAN 提供客 户端与身份验证服务器之间相互的严格身份验证。另外,802.1X 还可针对每个用户、每个会话提供 动态加密密钥,从而消除了与静态加密密钥相关的管理负担和安全问题。

使用 802.1X,用于身份验证的证书(如登录口令)通过无线介质传输时从不会采用明码或不加密的

形式。尽管 802.1X 身份验证类型为无线 LAN 提供了有力的身份验证,但除 802.1X 以外,加密还 需要使用 TKIP 或 AES,因为标准 802.11 WEP 加密容易受到网络攻击。

共有几种 802.1X 身份验证类型,每种类型提供不同的身份验证方法,但它们依靠同一个框架和 EAP 在客户端与接入点之间进行通信。在所有 WLAN 产品中,Cisco Aironet 产品支持的 802.1X EAP 身份验证类型最多。支持的类型包括:

- <u>Cisco LEAP</u>
- 通过安全隧道的 EAP 灵活身份验证 (EAP-FAST)
- EAP 传输层安全 (EAP-TLS)
- <u>受保护的扩展身份验证协议 (PEAP)</u>
- EAP 隧道 TLS (EAP-TTLS)
- EAP 用户身份模块 (EAP-SIM)

802.1X 身份验证的另一个好处是实现 WLAN 用户组的集中管理,包括基于策略的密钥轮换、动态 密钥分配、动态 VLAN 分配和 SSID 限制。这些功能会轮换加密密钥。

在个人操作模式下,使用预共享密钥(口令)进行身份验证。个人模式只需要一个接入点和客户端 设备,而企业模式通常要求网络中有一个 RADIUS 或其他身份验证服务器。

本文档提供了在 Cisco 统一无线网络中配置 WPA2(企业模式)和 WPA2-PSK(个人模式)的示例。

#### <u>网络设置</u>

在此设置中,Cisco 4404 WLC 和 Cisco 1000 系列 LAP 通过第 2 层交换机连接起来。还有一个外 部 RADIUS 服务器 (Cisco Secure ACS) 也连接到同一个交换机。所有设备都在同一个子网中。接 入点 (LAP) 最初在控制器中注册。需要创建两个无线 LAN,一个用于 WPA2 企业模式,另一个用 于 WPA2 个人模式。

WPA2 — 企业模式WLAN(SSID: WPA2-Enterprise)将使用EAP-FAST对无线客户端进行身份验证 ,使用AES进行加密。Cisco Secure ACS 服务器将用作外部 RADIUS 服务器,用于对无线客户端 进行身份验证。

WPA2 — 个人模式WLAN(SSID: WPA2-PSK)将使用WPA2-PSK使用预共享密钥"abcdefghijk"进行 身份验证。

您需要将设备配置为以下设置:



WLC Management IP address:	10.77.244.204
WLC AP Manager IP address:	10.77.244.205
Wireless Client IP address:	10.77.244.221

Cisco Secure ACS server IP address 10.77.244.196

Subnet Mask used in this example 255.255.255.224

# 针对 WPA2 企业模式配置设备

本部分提供有关如何配置本文档所述功能的信息。

若要针对 WPA2 企业操作模式配置设备,请执行下列步骤:

- 1. <u>配置 WLC 以便通过外部 RADIUS 服务器进行 RADIUS 身份验证</u>
- 2. <u>针对 WPA2 企业模式身份验证 (EAP-FAST) 配置 WLAN</u>
- 3. <u>针对 WPA2 企业模式配置无线客户端</u>

## 配置 WLC 以便通过外部 RADIUS 服务器进行 RADIUS 身份验证

需要配置 WLC 以便将用户凭证转发到外部 RADIUS 服务器。随后,外部 RADIUS 服务器使用 EAP-FAST 验证用户凭证,并提供对无线客户端的访问。

完成以下这些步骤,为外部 RADIUS 服务器配置 WLC:

- 1. 从控制器的 GUI 中选择**安全性和"RADIUS 身份验证",以便显示"RADIUS 身份验证服务器"页** 。然后,请点击new来定义RADIUS服务器。
- 在 RADIUS Authentication Servers > New 页上定义 RADIUS 服务器参数。这些参数包括 : RADIUS 服务器的 IP 地址共享密钥端口号服务器状态本文使用IP地址为10.77.244.196的 ACS服务器。

ahaha					Sa <u>x</u> e Co	nfiguration <u>P</u> ing	Logout   Befresh
CISCO	MONITOR WLANS CONTRO	LLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	RADIUS Authentication S	ervers > New				< Back	Apply
- AAA General	Server Index (Priority)	1 .					
<ul> <li>RADIUS Authentication</li> </ul>	Server IPAddress	10.77.244.196					
Accounting     TACACS+     LDAP	Shared Secret Format	ASCII 💌					
Local Net Users MAC Filtering	Shared Secret	•••••					
Disabled Clients User Login Policies AP Policies	Confirm Shared Secret	****					
Local EAP	Key Wrap	(Designed for F)	IPS customers	and requires a ke	y wrap compliant	RADIUS server)	
Priority Order	Port Number	1812					
▶ Access Control Lists	Port Number	1012					
Wireless Protection Policies	Server Status	Enabled 💌					
▶ Web Auth	Support for RFC 3576	Enabled 💌					
► Advanced	Server Timeout	2 seconds					
	Network User	🗷 Enable					
	Management	🗹 Enable					
	IPSec	Enable					

3. 单击 Apply。

# 针对 WPA2 企业操作模式配置 WLAN

下一步,配置客户端将用于连接到无线网络的 WLAN。用于 WPA2 企业模式的 WLAN SSID 将是 WPA2-Enterprise。本例将此 WLAN 分配到管理接口。

若要配置 WLAN 及其相关参数,请完成下列步骤:

- 1. 从控制器的 GUI 中单击 WLAN 以显示"WLAN"页。此页列出了控制器上现有的 WLAN。
- 2. 单击 New 以创建新的 WLAN。
- 在 WLANs > New 页上输入 WLAN SSID 名称和配置文件名称。然后,单击 Apply。本例使用 WPA2-Enterprise 作为 SSID。

cisco	MONITOR	<u>W</u> LANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	Sage Co COMMANDS	HELP	Logout Befr
WLANs	WLANs>	New						< Back	Apply
WLANS WLANS	Туре		WLAN						
Advanced	WLAN SSI	me D	WPA2-Ent	erprise					

- 4. 创建新 WLAN 后,就会显示新 WLAN 的 **WLAN > Edit 页。**在此页上,可以定义特定于此 WLAN 的各种参数。其中包括"General Policies"、"Security Policies"、"QOS"策略和 "Advanced"参数。
- 5. 根据一般策略,请检查状态检查方框来启用WLAN。



- 6. 如果希望 AP 在其信标帧中广播 SSID,请选中 Broadcast SSID 复选框。
- 7. 单击"Security"选项卡。在"第 2 层安全性"下,选择 WPA+WPA2。此操作将启用 WLAN 的 WPA 身份验证。

						Sage Co	onfiguration <u>P</u> i	ng Logout <u>R</u> efresh
cisco	MONITOR WLANS	CONTROLLER	W1RELESS	SECURITY	MANAGEMENT	COMMANDS	нецр	
WLANs	WLANs > Edit						< Bac	Apply
W MILANIC	General Securi	ty QoS	Advanced					
WLANs	Layer 2 Laye	r 3 AAA S	ervers					
▶ Advanced								-
	Layer 2 Security	WPA+WPA2	<b>x</b>					
		MAC Filterin	a					
	Static WEP Parame	eters						
	802.11 Data Encr	yption Curre	int Key:	104 bits WE	P Static Key (Key )	index = 0)		
		Туре	Key Size	Key Index	Encryption Key	,	Key Form	at
		WEP	not set 💌	1 .			ASCII .	
	Allow Shared Key Authentication	í 🗆 er	abled					
	802.11 Data Encr	yption Curre	nt Key: 0 t	oits CKIP Key	(Key Index= 0)			
		Key	Size Key	Index Encr	yption Key	ĸ	ey Format	
		not	set • 1				ASCII 💌	
		e .						<u>×</u>
	Foot Notes	when they must	el 40x					
	2 CKIP is not support 2 Web Policy cannot b 3 H-REAP Local Switch 4 When client exclusio 5 Client MFP is not act	ed by 20xx mod he used in combi bing is not suppo on is enabled, a live unless WPA	el APs Ination with IPse rted with IPsec, Timeout Value ( 2 is configured	ec , CRANITE aut of zero means	hentication Infinity (will requir	e administrative	override to reset	excluded clients)

8. 向下滚动页面以修改 WPA+WPA2 Parameters。在本例中,选择 WPA2 策略和 AES 加密。

cisco	Sage Configuration : Bing   Logout   Befresh MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANS WLANS WLANS WLANS Advanced	MONITOR       MLANIs       CONTROLLER       WIPELESS       SECURITY       MANAGEMENT       COMMANOS       HELP         WLANs > Edit           Apply         General       Security       QoS       Advanced           Apply         General       Security       QoS       Advanced <td< td=""></td<>
	1 CKIP is not supported by 10xx model APs 2 Web Policy cannot be used in combination with IPsec 3 H-REAP Local Switching is not supported with IPsec, CRANITE authentication 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients) 5 Client MEP is not active unless WPA2 is configured

- 9. 在"Auth Key Mgmt"下,选择 **802.1x**。此操作将为 WLAN 启用采用 802.1x/EAP 身份验证和 AES 加密的 WPA2。
- 10. 单击 AAA Servers 选项卡。在"Authentication Servers"下,选择适当的服务器 IP 地址。在本例中,使用 10.77.244.196 作为 RADIUS 服务器。

	sa⊻e connguration i Eugli rodont i Eus
CISCO	MONITOR WUANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
LANs	WLANs > Edit < Back Apply
NUL ANIA	General Security QoS Advanced
WLANS	Laver 2 Laver 3 AAA Servers
dvanced	
	Select AAA servers below to override use of default servers on this WLAN
	Radius Servers LDAP Servers
	Authentication Servers Accounting Servers Server 1 None
	Enabled Server 2 None
	Server 3 None  Server 3 None
	Server None None N
	Sarvar
	3 None None
	Local EAP Authentication
	Local EAP Authentication Enabled
	Foot Notes
	1 CKIP is not supported by 10xx model APs 2 Web Policy cannot be used in combination with IPsec
	3 H-REAP Local Switching is not supported with IPsec, CRANITE authentication 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
	5 Client MFP is not active unless WPA2 is configured

11. 单击 **Apply**。**注意:**这是需要在控制器上为EAP身份验证配置的唯一EAP设置。所有其他特定于 EAP-FAST 的配置需要在 RADIUS 服务器和需要进行身份验证的客户端上完成。

## 针对 WPA2 企业模式身份验证 (EAP-FAST) 配置 RADIUS 服务器

在本例中,使用 Cisco Secure ACS 作为外部 RADIUS 服务器。若要针对 EAP-FAST 身份验证配 置 RADIUS 服务器,请执行下列步骤:

- 1. 创建一个用于对客户端进行身份验证的用户数据库
- 2. <u>将 WLC 作为 AAA 客户端添加到 RADIUS 服务器</u>
- 3. 使用匿名带内 PAC 配置为 RADIUS 服务器配置 EAP-FAST 身份验证注意: EAP-FAST可以 使用匿名带内PAC调配或经过身份验证的带内PAC调配进行配置。本例使用匿名带内 PAC 配 置。有关采用匿名带内 PAC 配置和经身份验证的带内 PAC 配置对 EAP FAST 进行配置的详 细信息和示例,请参阅使用无线 LAN 控制器和外部 RADIUS 服务器的 EAP-FAST 身份验证 的配置示例。

#### 创建一个用于对 EAP-FAST 客户端进行身份验证的用户数据库

若要在 ACS 上为 EAP-FAST 客户端创建一个用户数据库,请完成下列步骤。本例将 EAP-FAST 客 户端的用户名和口令分别配置为 User1 和 User1。

 从导航栏的 ACS GUI 中选择 User Setup。创建一个新的无线用户,然后单击 Add/Edit 转到 该用户的"编辑"页。

Address 😸 http://127.0	0.0.1:1065/	× 🔁 🛛
CIECO SVETERE	User Setup	
User Setup Setup Setup Setup Setup Seturation Se	VEDEN User: User1 Find Add/Edit List users beginning with letter/number: ABC2KISKLK NOPOBITUYYXX QI25522 List all users Remove Dynamic Users Back to Help	<ul> <li>User Setup and External User Databases</li> <li>Finding a Specific User in the ACS Internal Database</li> <li>Adding a User to the ACS Internal Database</li> <li>Unting Usernames that Beein with a Particular Character</li> <li>Listing All Usernames in the ACS Internal Database</li> <li>Unting Usernames in the ACS Internal Database</li> <li>Chansing a Usernames in the ACS Internal Database</li> <li>Character &amp; User Setup and External User Database</li> <li>Character &amp; User Setup and External User Database</li> <li>Beneve Dynamic User</li> <li>User Setup enables you to configure individual user information, add user, and delete users in the database. User Setup and External User Database</li> <li>Before ACS can authenticate users with an external user database.</li> <li>You must have the database up and running on the external server. For example, if you are uping tokin card authentication, your tokin server must be running and properly configured.</li> <li>You must have configured the applicable parameters in the External User Database Section.</li> <li>You must have configuration overrides Group Setup configuration.</li> <li>If you are database, usernames cannot be located or listed here until the user has successfully authenticated ence.</li> <li>External user database modification must be done from within the external user database. User Secue (successfully authenticated ence.</li> <li>External user database modification must be done from within the external user database. User Secue is the ACS internal database.</li> <li>Notes User Setup does not adder delete usernames in an external user database. (Back to Tio)</li> <li>Finding a Specific User is the ACS internal database.</li> <li>To find a user already in the ACS internal database, type the first few letters of the username in the User field, add an artenisk (*) as a widecard, and click Fied. Find. Finger alfore in the ACS internal database.</li> </ul>

2. 在"User Setup Edit"页中,按本例所示配置"Real Name"、"Description"及"Password"设置。本 文档使用 ACS Internal Database 作为"Password Authentication"。

9ress 🛃 http://127.0.	0.1:1065/	
Cisco Systems	User Setup	
adboadbo	Edit	5 Help
User Setup Setup Components Components Configuration Configuration	User: User1 (New User)  Account Disabled  Supplementary User Info Real Name	Account Disabled     Deleting a Username     Supplementary User Info     Password Authoritication     Comp to which the user is assigned     Callback     Callback     Callback     Chent UP Address Assignment     Advanced Setting     Network Access Restrictions     Max Session
Interface     Configuration     Configuration     Control     Control     Definial User     Database     Porture     Validation     Control     Porture     Porture     Porture     Porture     Porture     Porture     Porture	User Setup ? Password Authentication: ACS Internal Database CiscoSecure PAP (Also used for CHAP/MS-	Account Disable     Deventsodable ACLs     Advanced TACACS - SetUres     TACACS - Enable Centrol     TACACS - Enable Centrol     TACACS - Enable Centrol     TACACS - Enable Centrol     TACACS - Shell Command Authorization     TACACS - Universe     TACACS - Un
Reports and Activity Online Documentation	CHAP/ARAP, if the Separate field is not checked.) Password Confirm Password Separate (CHAP/MS-CHAP/ARAP) Password Confirm Password Sutherit Cancel	Account Disabled Status Select the Account Disabled check box to disable this account: clear the check box to enable the account. [Back to Tep] Deleting a Username The Delete button appears only when you are editing an existing user account, not when you are adding a new user account. To delete the

- 3. 从"Password Authentication"下拉框中选择 ACS Internal Database。
- 4. 配置所需的所有其他参数,然后单击 Submit。

## 将 WLC 作为 AAA 客户端添加到 RADIUS 服务器

若要将控制器定义为 ACS 服务器上的 AAA 客户端,请完成下列步骤:

- 1. 从 ACS GUI 中单击 **Network Configuration。**在"Network Configuration"页的"Add AAA client"部分下,单击 **Add Entry 将 WLC 作为 AAA 客户端添加到 RADIUS 服务器。**
- 2. 在"AAA Client"页中,定义 WLC 名称、IP 地址、共享密钥和身份验证方法 (RADIUS/Cisco Airespace)。有关其他非 ACS 身份验证服务器的信息,请参阅制造商提供的文档。

The State Market Market Market Market	
ge gat gew rgvontes gos gep gdress 👸 http://127.0.0.1:1065/	uns
Network Configuration	×
Conservation Co	<ul> <li>Heip</li> <li>AAA Cleant Hestmanne</li> <li>AAA Cleant Hestmanne</li> <li>AAA Cleant Dr Address</li> <li>Shared Second</li> <li>Shared Second</li></ul>

注意:您在WLC和ACS服务器上配置的共享密钥必须匹配。共享密钥区分大小写。

3. 单击 Submit+Apply。

## 使用匿名带内 PAC 配置为 RADIUS 服务器配置 EAP-FAST 身份验证

## 匿名带内配置

这是 ACS 与最终用户客户端建立安全连接以便为客户端提供新 PAC 的两种带内配置方法之一。此选项允许在最终用户客户端与 ACS 之间进行匿名 TLS 握手。

在对等体对 ACS 服务器进行身份验证之前,此方法在经身份验证的 Diffie-HellmanKey 协商协议 (ADHP) 隧道内操作。

随后,ACS 需要对用户进行 EAP-MS-CHAPv2 身份验证。当用户身份验证成功时,ACS 将与最终 用户客户端建立一条 Diffie-Hellman 隧道。ACS 为用户生成一个 PAC,并将其与此 ACS 的相关信 息一起发送到此隧道中的最终用户客户端。此配置方法在第零阶段使用 EAP-MSCHAPv2 作为身份 验证方法,在第二阶段使用 EAP-GTC。

由于配置了未经身份验证的服务器,因此不可能使用纯文本口令。所以,在隧道内只能使用 MS-CHAP 凭证。MS-CHAPv2 用于证明对等体的身份和接收用于后续身份验证会话的 PAC(EAP-MS-CHAP 将仅用作内部方法)。

若要采用匿名带内配置为 RADIUS 服务器配置 EAP-FAST 身份验证,请完成下列步骤:

1. 在 RADIUS 服务器 GUI 中单击 System Configuration。从"System Configuration"页中选择 Global Authentication Setup。

CiscoSecure ACS - Micros	oft Internet Explorer	Tels -
Ele Edk Yew Favorites	i Iools Help	Links ** Cos
Address ) http://127.0.0.1:1	1065/	o 🗲 🚬
Cisco Svorens S	vstem Configuration	×
adhaadha 80		Hein
User Setup Setup DarredProfile Components Components Configuration Configuration Configuration	Service Control Logging Date Format Control Local Password Management ACS Internal Database Replication ACS Backup ACS Restore ACS Service Management ACS Certificate Setup Global Authentication Setup	Service Central     Legains     Date Fernat Central     Legains     Lecal Personal Central     Lecal Personal Database Replication     ACS Internal Database Replication     ACS Database     ACS Database     ACS Database     ACS Destrice Management     DePends Address     YollP Accessing Configuration     ACS Certificate Setue     Global Authentication Configuration
	Buck to Help	Service Control Select to open the page from which you can stop or restart Cisco Secure ACS pervices. [Back to Top] Select to configure various Cisco Secure ACS reports and customize the type of information that is logged. [Back to Top] Date Format Control Select to configure the date format, either month/day/year or day/month/year, for CSV files and Service Logs and in the GUI. [Back to Top]
8		
🐉 Start 🛛 🚱 🙈	CiscoSecure ACS - Mic	3 7:57 PM

2. 在"Global Authentication"设置页中,单击 EAP-FAST Configuration 转到 EAP-FAST 设置页

o

Ele Edit Yew Fg	ferosoft Internet Explorer ontes	(d) 2 Linis ** 🦧
gdress a http://127.0	0.0.1:1065/	🗵 🛃 😡
Cisco Storens	System Configuration	
The Ultrar	EAP Configuration	2 Help
Setup Setup Stup SharedProfile Components	PEAP Allow EAP-MSCHAPv2 Allow EAP-GTC Allow Posture Validation	Use this page to specify settings for various authentication protocols.  EAP Configuration PEAP EAP-EAST
Network Configuration System Configuration	Allow EAP-TLS Select one or more of the following options: E Certificate SAN comparison	EAP-BLS     EAP-BDS     EAP-MDS     AP-EAP Request Timeest     MS-CHAP-Confirmation
Administration Control	EAP-TLS session timeout (minutes): 120	EAP Configuration EAP is a flexible request-response protocol for arbitrary authentication information (RFC 2284). EAP is layered on top of
Posture Validation	Cisco client initial message: PEAP session timeout (minutes): Enable Fast Reconnect:	another protocol such as UDP, dU2.1x or KAD2US and supports     multiple "authentication" types.     [Back to Top]     PEAP
Activity Online Decomentation	EAP-FAST EAP-FAST Configuration	PEAP is the outer layer protocol for the secure tunnel.
	EAP-TLS Allow EAP-TLS Select one or more of the following options: Certificate SAN comparison	Aleber //AP is a cartificate-based authentication protocol. //AP authentication can occur only after you have completed the required steps on the ACS Certificate Setup page.     Allow EAP-MSCHAPv2 — Use to enable EAP-MSCHAPv2 within MS PEAP authentication. Enable this protocol for any repository that supports MS- CHAPv2, such as Microsoft AD, and the ACS Internal Database.
	Submit Submit + Restart Cancel	
		S Internet

3. 在"EAP-FAST Settings"页中,选中 Allow EAP-FAST 复选框以启用 RADIUS 服务器的 EAP-FAST。

CiscoSecure ACS - !	Microsoft Internet Explorer	
Ele Edt Yew Fg	vorites Iools Help	Links 🍟 🦧
Address http://127.	0.0.1:1065/	💌 🔁 😡
Cisco Systems	System Configuration	X
als als	System Configuration	
	EAP-FAST Configuration	A Help
User Setup		1 mm mm mm mm mm
And L from	EAP-FAST Settings	PAPERAT Configuration Page
Setup	EAD-EAST	Use this page to configure EAD-FAST authentication settings.
SharedProfile	K Allow EAP-EAST	EAP-FAST Settings
- Inner	Active master key TTI	Client initial message     Automatical Transmission
Configuration	Active master key FTC	Allow according to hand PAC previsioning
2 Pol System	Retired master key TTL 3 months	Allow authenticated in-band PAC provisioning
Configuration	Tunnel PAC TTL 1 weeks	Allem stateless session resume
Configuration	Client initial message: tacwebacs	Allowed incomethods
	Authority ID Infor	EAP-ILS session timesut (minutes)
Centrel		EAP-FAST master server     Actual FAP-FAST ensure status
Diternal User	M Allow anonymous in-band PAC provisioning	<ul> <li>OXMACKOC COLLEGISCOM</li> </ul>
D'O I Databases	L) Allow authenticated in-band PAC provisioning	EAP-FAST Settings
Posture Validation	Accept client on authenticated provisioning	Allow EAP-FAST-To enable EAP-FAST authentication, select this check
SulNetwork Access	Require client certificate for provisioning	box.
Profiler	Allow Machine Authentication	Active Master Key TTL -Enter a value for the amount of time that a master
C Reports and	Machine PAC TTL 1 weeks	key is used to generate new Protected Access Credentials (PACs). When the time to live (TTL) defined for the Master Key expires, the master key is
- Ch L Anima	C Allow Stateless session resume	considered ratired and a new master key is generated.
Documentation	Authorization PAC TTL 1 hours	<ul> <li>Retired master key TIL-Enter a value for the amount of time that PACs.</li> </ul>
	Allowed inner methods	generated using a retired master key are acceptable for EAP-FAST authentication. When an endruser client oxins network access using a PAC
	EAP-GTC	based on a retired master key, ACS sends a new PAC to the end-user client.
	EAP-MSCHAPv2	<ul> <li>Tunnel PAC TEL – Enter a value for the amount of time that a PAC is used</li> </ul>
	EAP-TLS	before it expires and must be replaced. If the master key used to generate the Tunnel PAC has not expired, new PAC creation and estimated in
	Submit Submit + Restart Cancel	automatic. If the master key used to generate the Tunnel PAC expired,
	Carear Carear	client with a new PAC.
0		Internet
🐉 Start 🔂 🥭	CiscoSecure ACS - Mic	🦻 7:58 PM

- 4. 根据需要配置"Active master key TTL"/"Retired master key TTL"(TTL 即存活时间)的值,或 按本例所示将其设置为默认值。有关活动和停用的主密钥的信息,请参阅"主密钥"。有关详细 信息,另请参阅"主密钥和 PAC TTL"。"Authority ID Info"字段表示此 ACS 服务器的文本身份 ,最终用户可使用该字段确定要根据哪个 ACS 服务器进行身份验证。必须填写此字段。 "Client initial display message"字段用于指定要发送给使用 EAP-FAST 客户端进行身份验证的 用户的一条消息。最大长度为 40 个字符。只有最终用户客户端支持显示时,用户才会看到该 初始消息。
- 5. 如果希望 ACS 执行匿名带内 PAC 配置,请选中 Allow anonymous in-band PAC provisioning **复选框。**
- 6. Allowed inner methods 此选项确定哪些内部EAP方法可以在EAP-FAST TLS隧道内运行。 对于匿名带内配置,必须启用 EAP-GTC 和 EAP-MS-CHAP 以实现向后兼容。如果选择"Allow anonymous in-band PAC provisioning",则必须选择"EAP-MS-CHAP"(第零阶段)和"EAP-GTC"(第二阶段)。

## <u>针对 WPA2 企业操作模式配置无线客户端</u>

下一步是针对 WPA2 企业操作模式配置无线客户端。

若要针对 WPA2 企业模式配置无线客户端,请完成下列步骤。

- 在"Aironet Desktop Utility"窗口中,单击 Profile Management > New 为 WPA2-Enterprise WLAN 用户创建一个配置文件。如前所述,本文档使用 WLAN/SSID 名称 WPA2-Enterprise 表示无线客户端。
- 2. 在"Profile Management"窗口中,单击 General 选项卡,并按本例所示配置"Profile Name"、 "Client Name"和"SSID"名称。然后单击 OK。

Consul o D LL		
General Security Advance	be	
Profile Settings Profile Name: Client Name:	WPA2-Enterprise Wireless-Client1	
Network Names SSID1: SSID2: SSID3:	WPA2-Enterprise	

3. 单击 Security 选项卡,然后选择"WPA/WPA2/CCKM"以启用 WPA2 操作模式。在 "WPA/WPA2/CCKM EAP Type"下,选择 EAP-FAST。单击 Configure 以配置 EAP-FAST 设 置。

Profile Management		? 🗙
General Security Advanced		
- Set Security Options		
⊙ WPA/WPA2/CCKM	WPA/WPA2/CCKM EAP Type: EAP-FAST	
WPA/WPA2 Passphrase		
○ 802.1x	802.1x EAP Type: LEAP	
O Pre-Shared Key (Static WEP)		
○ None		
Configure	Allow Association to Mixed Cells	
	Limit Time for Finding Domain Controller To: 0 0 sec	
Group Policy Delay:	60 🗘 sec	
	OK C	ancel

4. 在"Configure EAP-FAST"窗口中,选中 Allow Automatic PAC Provisioning 复选框。如果要配 置匿名 PAC 配置,则会将 EAP-MS-CHAP 用作第零阶段内唯一的内部方法。

Configure EAP-FAST	? 🔀
EAP-FAST Authentication Method	
MSCHAPv2 User Name and Password	Configure
Protected Access Credentials (PAC)	
Select One or More PAC Authorities	
	Manage
<	<b>&gt;</b>
Use Any PAC Belonging to the Same Group	
Allow Automatic PAC Provisioning	
Use Machine Information for Domain Logon	
✓ No Network Connection Unless User Is Logged In	
	OK Cancel

- 5. 从"EAP-FAST Authentication Method"下拉框中选择"MSCHAPv2 User Name and Password"作为身份验证方法。单击 **Configure**。
- 6. 在"Configure MSCHAPv2 User Name and Password"窗口中,选择适当的用户名和口令设置 。本例选择 Automatically Prompt for User Name and Password。

rusted Root Certification Au	thorities		
(Any>			~
Jser Name and Password S	ettings		
<ul> <li>Use Temporary User</li> </ul>	Name and Password		
O Use Windows U	Iser Name and Password	1	
Automatically P	rompt for User Name and	Password	
U Manually 1 romp	ctor oser manie and r a		
OUse Saved User Nan	ne and Password		1
User Name:	Administrator		
Password.			
Confirm Password.			
Domain.			

ACS 应注册相同的用户名和口令。如前所述,本例分别使用 User1 和 User1 作为用户名和口 令。另外请注意,这是匿名带内配置。所以,客户端无法验证服务器证书。您需要确保未选中 "Validate Server Identity"复选框。

7. Click OK.

#### <u>验证 WPA2 企业操作模式</u>

若要验证您的 WPA2 企业模式配置是否工作正常,请完成下列步骤:

- 1. 在"Aironet Desktop Utility"窗口中,选择配置文件 WPA2-Enterprise,然后单击"Activate"以激 活无线客户端配置文件。
- 2. 如果已启用"MS-CHAP ver2"作为身份验证方法,客户端将提示输入用户名和口令。

Enter Wireless Network Password						
Please enter your EAP-FAST username and password to log on to the wireless network						
User Name :	User1					
Password :	•••••					
Log on to :						
Card Name :	Cisco Aironet 802.11a/b/g Wireless Adapter					
Profile Name :	WPA-Enterprise					
	OK Cancel					

3. 在 EAP-FAST 进行用户处理的过程中,客户端将提示您向 RADIUS 服务器请求 PAC。当您单击 Yes 时,便会开始进行 PAC 配置。

EAP-FAST Authentication	×
You do not have a valid PAC from the authentication server. Do you want to proceed and request automatic provisioning?	
Yes No	

4. 在第零阶段的 PAC 配置成功后,接着进行第一阶段和第二阶段,成功完成身份验证过程。身份验证成功时,无线客户端将与 WLAN WPA2-Enterprise 建立关联。下面是屏幕截图:

Cisco Aironet Desktop Utility	y - Current Profile: WPA2-E	nterprise 🛛 🖓 🔀
Action Options Help		
Current Status Profile Management	Diagnostics	
CISCO SYSTEMS		
nullinullin. Profile Name:	WPA2-Enterprise	
Link Status:	Authenticated	Network Type: Infrastructure
Wireless Mode:	5 GHz 54 Mbps	Current Channel: 149
Server Based Authentication:	EAP-FAST	Data Encryption: AES
IP Address:	10.77.244.221	
Signal Strength:		Good
		Advanced

您还可以验证 RADIUS 服务器是否收到并验证来自无线客户端的身份验证请求。检查 ACS 服务器上的 Passed Authentications 和 Failed Attempts 报告以完成此操作。在ACS服务器上的 报表和活动下可获得这些报表。

# <u>针对 WPA2 个人模式配置设备</u>

若要针对 WPA2 个人操作模式配置设备,请执行下列步骤:

- 1. 针对 WPA2 个人模式身份验证配置 WLAN
- 2. <u>针对 WPA2 个人模式配置无线客户端</u>

## <u>针对 WPA2 个人操作模式配置 WLAN</u>

您需要配置客户端将用于连接到无线网络的 WLAN。用于 WPA2 个人模式的 WLAN SSID 将是 WPA2-Personal。本例将此 WLAN 分配到管理接口。

若要配置 WLAN 及其相关参数,请完成下列步骤:

- 1. 从控制器的 GUI 中单击 WLAN 以显示"WLAN"页。此页列出了控制器上现有的 WLAN。
- 2. 单击 New 以创建新的 WLAN。
- 3. 在"WLANs > New"页上输入"WLAN SSID"名称、"Profile"名称和"WLAN ID"。然后,单击 Apply。本例使用 WPA2-Personal 作为 SSID。

				-			Sa <u>v</u> e Co	onfiguration Liging	Logout Befresh
cisco	MONITOR	<u>W</u> LANs	CONTROLLER	W1RELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
WLANs	WLANs >	New						< Back	Apply
WLANS	Туре		WLAN						
≱ Advanced	Profile Na	me	WPA2-Per	sonal					
	WLAN SSI	D	WPA2-Per	sonal					

- 创建新 WLAN 后,就会显示新 WLAN 的 WLAN > Edit 页。在此页上,可以定义特定于此 WLAN 的各种参数。其中包括"General Policies"、"Security Policies"、"QOS"策略和 "Advanced"参数。
- 5. 根据一般策略,请检查状态检查方框来启用WLAN。
- 6. 如果希望 AP 在其信标帧中广播 SSID,请选中 Broadcast SSID 复选框。
- 7. 单击"Security"选项卡。在"Layer Security"下,选择 WPA+WPA2。此操作将启用 WLAN 的 WPA 身份验证。

					Sage Co	onfiguration ( Ping -	Logout   <u>R</u> efresh
cisco	MONITOR WLANS CONTR	OLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
WLANs	WLANs > Edit					< Back	Apply
T WI AND	General Security	QoS Advanced					
WLANS	Layer 2 Layer 3	AAA Servers					
Advanced	Layer 2 Security WPA4	WPA2 ×					<u>^</u>
	802.11 Data Encryption	Current Key:	104 bits WE	P Static Key (Key I	ndex = 0)		
	Allow Shared Key	Type Key Size	Key Index	Encryption Key	e	Key Format	
	Authentication	L Enabled					
	CKIP Parameters Z	Current Very 01	as going they	Neu Index- 03			
	802.11 Data Encryption	Current Key: 01	NS CKIP KOY	(key index= 0)			
		Key Size Key	Index Encr	yption Key	K	ey Format	
		not set 💌 1	-			ASCII 💌	
	4	F					<u> </u>
	Foot Notes						
	I CKIP is not supported by 10 2 Web Policy cannot be used i 3 H-REAP Local Switching is n 4 When client exclusion is ent 5 Client MRP is not active unle	hix model APs in combination with IPsec of supported with IPsec sbled, a Timeout Value iss WPA2 is configured	ec , CRANITE aut of zero means	hentication infinity (will requin	e administrative	override to reset exi	oluded clients)

8. 向下滚动页面以修改 WPA+WPA2 Parameters。在本例中,选择 WPA2 策略和 AES 加密。

9. 在"Auth Key Mgmt"下,选择 PSK 以启用 WPA2-PSK。

10. 在适当的字段中输入预共享密钥,如下所示。

cisco	Sage Configuration Bing Logout Br MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	fresh
CISCO WLANS WLANS WLANS Advanced	MONITOR       WLANS       CONTROLLER       WIRELESS       SECURITY       MANAGEMENT       COMMANDS       HELP         WLANS > Edit            Appl         General       Security       QOS       Advanced          Appl         General       Security       QOS       Advanced </td <td><u>у</u></td>	<u>у</u>
	WPA2 Policy       Image: Construction of the c	

注意:WLC上使用的预共享密钥必须与无线客户端上配置的密钥匹配。

11. 单击 Apply。

<u>针对 WPA2 个人模式配置无线客户端</u>

下一步是针对 WPA2 个人操作模式配置无线客户端。

若要针对 WPA2 个人模式配置无线客户端,请完成下列步骤:

- 1. 在"Aironet Desktop Utility"窗口中,单击 **Profile Management > New 为 WPA2-PSK WLAN 用** 户创建一个配置文件。
- 2. 在"Profile Management"窗口中,单击 General 选项卡,并按本例所示配置"Profile Name"、 "Client Name"和"SSID"名称。然后,单击OK。

Profile Management		?×
General Security Advance	ed	
- Profile Settings		
Profile Name:	WPA2-Personal	
Client Name:	Wireless-Client2	
Network Names		
SSID1:	WPA2-Personal	
SSID2.		
SSID3:		
	ОК	ancel

3. 单击 Security 选项卡,然后选择"WPA/WPA2 Passphrase"以启用 WPA2-PSK 操作模式。单击 Configure 以配置 WPA-PSK 预共享密钥。

Profile Management			? 🗙
General Security Advanced			
- Set Security Options			
O WPA/WPA2/CCKM	WPA/WPA2/CCKM EAP Type:	LEAP	
WPA/WPA2 Passphrase			
○ 802.1x	802.1x EAP Type:	LEAP	
O Pre-Shared Key (Static WEP)			
◯ None			
Configure	Allow Association to Mixed Ce Profile Locked	sis	
	Limit Time for Finding Domain	Controller To: 0 🔅 sec	
Group Policy Delay:	60 😂 sec		
		OK Ca	ncel

4. 输入预共享密钥并单击 OK。

Configure WPA/WPA2 Passphrase	• ? 🔀				
Enter a WPA/WPA2 passphrase (8 to 63 ASCII or 64 hexadecimal characters)					
abcdefghijkl					
	OK Cancel				

#### <u>验证 WPA2 个人操作模式</u>

若要验证您的 WPA2 个人模式配置是否工作正常,请完成下列步骤:

- 1. 在"Aironet Desktop Utility"窗口中,选择配置文件 WPA2-Personal,然后单击"Activate"以激活 无线客户端配置文件。
- 2. 激活配置文件后,无线客户端将在身份验证成功时与 WLAN 建立关联。下面是屏幕截图

Cisco Aironet l	Desktop Utility	y - Current Prof	ile: WPA2-Personal	? 🔀
Action Options He	lp			
Current Status Pro	file Management	Diagnostics		
CISCO SYSTEMS				
adhoodho	Profile Name:	WPA2-Personal		
	Link Status:	Authenticated	Network Typ	e: Infrastructure
	Wireless Mode:	5 GHz 54 Mbps	Current Channe	el: 149
Server Base	d Authentication:	None	Data Encryptio	n: AES
	IP Address:	10.77.244.221		
	Signal Strength:			Good
			[	Advanced

# <u>故障排除</u>

本部分提供的信息可用于对配置进行故障排除。

对于配置故障排除,以下 debug 命令将十分有用:

注意:使用debug命令之前,请参阅有关Debug命令的重要信息。

 debug dot1x events enable — 启用所有dot1x事件的调试。下面是基于成功身份验证的 debug 输出示例:**注意:**由于空间限制,此输出的某些行已移至第二行。 (Cisco Controller)>debug dot1x events enable Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Sending EAP -Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 1) Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Received EAPOL START from mobile 00:40:96:af:3e:93 Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 2) Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Received EAP Response packet with mismatching id (currentid=2, eapid=1) from mobile 00:40:96:af:3e:93 Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Received Identity Response (count=2) from mobile 00:40:96:af:3e:93 Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 ..... Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 19, EAP Type 43) Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20) Wed Feb 20 14:20:01 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 43) Wed Feb 20 14:20:29 2007: Creating dot1x interface with key 00:0b:85:91:c3:c0 -0 Wed Feb 20 14:20:29 2007: Resetting the group key timer for 3689 seconds on AP 00:0b:85:91:c3:c0 Wed Feb 20 14:20:29 2007: Creating dot1x interface with key 00:0b:85:91:c3:c0 -1 Wed Feb 20 14:20:29 2007: Resetting the group key timer for 3696 seconds on AP 00:0b:85:91:c3:c0 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAPOL START from mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 22) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received Identity Response (count=3) from mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 22 ===> 19 for STA 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 19) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 19, EAP Type 3) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 43) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 21) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 21, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to

mobile 00:40:96:af:3e:93 (EAP Id 22) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 22, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 23) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 23, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 24) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 24, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 25) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 25, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 26) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 26, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 27) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 27, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Reject for mobile00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Failure to mobile 00:4096:af:3e:93 (EAP Id 27) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Setting quiet timer for 5 seconds for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 1) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 1) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAPOL START from mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 2) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received Identity Response (count=2) from mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 2 ===> 20 for STA 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 3) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 21) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 21, EAP Type 43) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for

mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 22) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 22, EAP Type 43) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 22 ===> 24 for STA 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 24) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 24, EAP Type 43) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 25) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 25, EAP Type 43) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Accept for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Creating a new PMK Cache Entry for tation 00:40:96:af:3e:93 (RSN 0) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP-Success to mobile 00:40:96:af:3e:93 (EAP Id 25) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending default RC4 key to mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending Key-Mapping RC4 key to mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received Auth Success while in Authenticating state for mobile 00:40:96:af:3e:93

• debug dot1x packet enable — 启用802.1x数据包消息的调试。

• debug aaa events enable — 启用所有aaa事件的调试输出。

# 相关信息

- WPA2 Wi-Fi 保护访问 2
- 包含无线局域网控制器和外部 RADIUS 服务器的 EAP-FAST 身份验证配置示例
- WLAN 控制器 (WLC) 中 EAP 身份验证的配置示例
- WPA 配置概述
- •无线产品支持
- <u>技术支持和文档 Cisco Systems</u>

#### 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。