思科統一無線網路中的Wi-Fi保護訪問(WPA)配置 示例

目錄

 簡介

 必要條件

 需求

 擦用元件

 慣例

 WPA和WPA2支援

 網路設定

 為WPA2企業模式配置裝置

 設定WLC以透過外部RADIUS伺服器進行RADIUS驗證

 為WPA2企業模作模式配置WLAN

 為WPA2企業模式身份驗證(EAP-FAST)配置RADIUS伺服器

 為WPA2企業模作模式配置無線客戶端

 為WPA2個人模式配置裝置

 疑難排解

 相關資訊

<u>簡介</u>

本文檔介紹如何在思科統一無線網路中配置Wi-Fi保護訪問(WPA)。

必要條件

<u>需求</u>

嘗試此組態之前,請確認您已瞭解以下主題的基本知識:

• WPA

• 無線區域網路(WLAN)安全解決方案**註:有關**Cisco WLAN安全解決方案的資訊,請參閱 <u>Cisco無線LAN安全概述</u>。

<u>採用元件</u>

本文中的資訊係根據以下軟體和硬體版本:

- Cisco 1000系列輕量型存取點(LAP)
- 執行韌體4.2.61.0的Cisco 4404無線LAN控制器(WLC)

- 運行韌體4.1的Cisco 802.11a/b/g客戶端介面卡
- 運行韌體4.1的Aironet案頭實用程式(ADU)
- Cisco安全ACS伺服器版本4.1

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

<u>慣例</u>

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

WPA和WPA2支援

思科統一無線網路包括對Wi-Fi聯盟認證WPA和WPA2的支援。WPA於2003年由Wi-Fi聯盟推出。 WPA2於2004年由Wi-Fi聯盟推出。所有針對WPA2的Wi-Fi認證產品都必須與針對WPA的Wi-Fi認證 產品互操作。

WPA和WPA2為終端使用者和網路管理員提供了高級別保證,確保他們的資料將保持私有狀態,而 且對其網路的訪問將限制在授權使用者範圍內。兩者都有個人和企業運營模式,可滿足兩個市場細 分的獨特需求。每個的企業模式使用IEEE 802.1X和EAP進行身份驗證。每個的個人模式使用預共 用金鑰(PSK)進行身份驗證。思科不建議對商業或政府部署使用個人模式,因為它使用PSK進行使 用者身份驗證。PSK對企業環境不安全。

WPA解決了原始IEEE 802.11安全實施中存在的所有已知WEP漏洞,為企業和小型辦公室/家庭辦公室(SOHO)環境中的WLAN提供了即時安全解決方案。WPA使用TKIP進行加密。

WPA2是下一代Wi-Fi安全性。它是Wi-Fi聯盟對已批准的IEEE 802.11i標準的互操作性實施。它採用 帶密碼塊鏈結消息驗證碼協定(CCMP)的計數器模式,實現了美國國家標準技術研究所(NIST)推薦的 AES加密演算法。WPA2促進政府FIPS 140-2合規性。

	WPA	WPA2
	• 身份驗證	• 身份驗證
	: IEEE	: IEEE
人类样子 / 人类 政内	802.1X/	802.1X/EA
正未侯氏(正未、政府、 数百)	EAP	Р
¥X FI)	• 加密	• 加密
	: TKIP/	: AES-
	MIC	CCMP
	• 身份驗證	• 身份驗證
	: PSK	: PSK
個人候氏(SURU、家庭 /個↓)	• 加密	• 加密
/IU//)	: TKIP/	: AES-
	MIC	CCMP

WPA和WPA2模式型別的比較

在企業操作模式下,WPA和WPA2都使用802.1X/EAP進行身份驗證。802.1X為WLAN提供客戶端 和身份驗證伺服器之間的強式相互身份驗證。此外,802.1X還提供每使用者、每會話的動態加密金 鑰,從而消除了靜態加密金鑰的管理負擔和安全問題。

在802.1X中,用於身份驗證的憑證(如登入密碼)永遠不會通過無線介質以明文傳輸或未經加密。

儘管802.1X身份驗證型別為無線LAN提供強身份驗證,但除802.1X外,加密還需要TKIP或AES,因 為標準802.11 WEP加密容易受到網路攻擊。

有幾種802.1X身份驗證型別,每種型別都提供不同的身份驗證方法,同時依賴相同的框架和EAP在 客戶端和接入點之間進行通訊。Cisco Aironet產品支援的802.1X EAP身份驗證型別比任何其他 WLAN產品都多。支援的型別包括:

- <u>Cisco LEAP</u>
- EAP 通過安全隧道的靈活身份驗證(EAP-FAST)
- EAP 傳輸層安全(EAP-TLS)
- <u>受保護的可擴充驗證</u>通訊協定(PEAP)
- EAP 隧道TLS(EAP-TTLS)
- EAP-Subscriber Identity Module(EAP-SIM)

802.1X身份驗證的另一個好處是集中管理WLAN使用者組,包括基於策略的金鑰輪替、動態金鑰分 配、動態VLAN分配和SSID限制。這些功能可旋轉加密金鑰。

在個人操作模式下,預共用金鑰(密碼)用於身份驗證。個人模式只需要接入點和客戶端裝置,而 企業模式通常需要網路上的RADIUS或其他身份驗證伺服器。

本文檔提供在思科統一無線網路中配置WPA2(企業模式)和WPA2-PSK(個人模式)的示例。

網路設定

在此設定中,Cisco 4404 WLC和Cisco 1000系列LAP通過第2層交換機連線。外部RADIUS伺服器 (Cisco Secure ACS)也連線到同一交換器。所有裝置都位於同一個子網中。存取點(LAP)初始註冊到 控制器。需要建立兩個無線LAN,一個用於WPA2企業模式,另一個用於WPA2個人模式。

WPA2-Enterprise模式WLAN(SSID: WPA2-Enterprise)將使用EAP-FAST對無線客戶端進行身份驗 證,使用AES進行加密。Cisco Secure ACS伺服器將用作外部RADIUS伺服器,用於驗證無線客戶 端。

WPA2 — 個人模式WLAN(SSID: WPA2-PSK)將使用WPA2-PSK使用預共用金鑰「abcdefghijk」進行身份驗證。

您需要為此設定配置裝置:



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

為WPA2企業模式配置裝置

本節提供用於設定本文件中所述功能的資訊。

執行以下步驟,將裝置配置為WPA2企業運行模式:

- 1. <u>設定WLC以透過外部RADIUS伺服器進行RADIUS驗證</u>
- 2. <u>為WPA2企業模式身份驗證(EAP-FAST)配置WLAN</u>
- 3. <u>為WPA2企業模式配置無線客戶端</u>

設定WLC以透過外部RADIUS伺服器進行RADIUS驗證

需要設定WLC,才能將使用者認證轉送到外部RADIUS伺服器。外部RADIUS伺服器然後使用EAP-FAST驗證使用者認證並提供對無線使用者端的存取。

完成以下步驟,設定外部RADIUS伺服器的WLC:

- 1. 從控制器GUI中選擇**Security**和**RADIUS Authentication**,以顯示「RADIUS Authentication Servers」頁面。接下來,按一下**New**以定義RADIUS伺服器。
- 在RADIUS Authentication Servers > New頁面上定義RADIUS伺服器引數。這些引數包括
 : RADIUS伺服器IP位址共用金鑰連線埠號碼伺服器狀態本文檔使用IP地址為10.77.244.196的 ACS伺服器。

				Sage Co	nfiguration Eing	Logout Befresh
cisco	MONITOR WLANS CONTROL	LER WIRELESS SECURITY	MANAGEMENT	COMMANDS	HELP	
ecurity	RADIUS Authentication Ser	rvers > New			< Back	Apply
AAA General	Server Index (Priority)	1 .				
RADIUS Authentication	ication Server IPAddress	10.77.244.196				
Accounting TACACS+ LDAP	Shared Secret Format	ASCII ×				
Local Net Users MAC Filtering	sers Shared Secret	•••••				
Disabled Clients User Login Policies AP Policies	Policies Confirm Shared Secret	•••••				
Local EAP	Key Wrap	(Designed for FIPS customers)	and requires a key	wrap compliant	RADIUS server)	
Priority Order	der Bort Number	1812				
Access Control Lists	ntrol Lists	1012				
Wireless Protection Policies	rotection Server Status	Enabled 💌				
Web Auth	Support for RFC 3576	Enabled 💌				
Advanced	Server Timeout	2 seconds				
	Network User	🗹 Enable				
	Management	Enable				
	IPSec	Enable				
ecurity AAA General RADIUS Authentication Accounting TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies Local EAP Priority Order Access Control Lists Wireless Protection Policies Web Auth Advanced	RADIUS Authentication Server Server Index (Priority) Server IPAddress Shared Secret Format Shared Secret Confirm Shared Secret Key Wrap Port Number Server Status Support for RFC 3576 Server Timeout Network User Management IPSec	rvers > New I I III III IIII IIII IIII IIII III	and requires a key	r wrap compliant	< Back	A

3. 按一下「Apply」。

<u>為WPA2企業操作模式配置WLAN</u>

接下來,設定使用者端用來連線無線網路的WLAN。WPA2企業模式的WLAN SSID將為WPA2 — 企業。此範例將此WLAN指派給管理介面。

完成以下步驟即可設定WLAN及其相關引數:

- 1. 從控制器的GUI中按一下「**WLANs**」,以顯示「WLANs」頁面。此頁面列出控制器上存在的 WLAN。
- 2. 按一下New以建立一個新的WLAN。
- 在WLANs > New頁面上輸入WLAN SSID名稱和Profile名稱。然後,按一下「Apply」。本示 例使用WPA2-Enterprise作為SSID。

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

- 4. 建立新的WLAN後,系統會顯示新WLAN的**WLAN > Edit**頁面。在此頁面上,您可以定義此 WLAN的特定各種引數。這包括常規策略、安全策略、QOS策略和高級引數。
- 5. 在General Policies下,勾選Status覈取方塊以啟用WLAN。



- 6. 如果您希望AP在其信標幀中廣播SSID,請選中Broadcast SSID覈取方塊。
- 7. 按一下**Security**頁籤。在Layer 2 Security下,選擇**WPA+WPA2**。這將為WLAN啟用WPA身份 驗證。

- alada -					Saye Co	onfiguration <u>P</u> ing	Logout <u>R</u> efresh
CISCO	MONITOR WLANS CONTR	OLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	нецр	_
WLANs	WLANs > Edit					< Back	Apply
	General Security (QoS Advanced					
WLANS WLANS	Laver 2 Laver 3	AAA Servers					
Advanced	coyer 2 coyer o	ANA SELLES					
	Layer 2 Security WPA+	WPA2 ·					
	[MAC	Filtering					
	Static WEP Parameters						
	802.11 Data Encryption	Current Key:	104 bits WE	P Static Key (Key I	index = 0)		
		Type Key Size	Key Index	Encryption Key	1	Key Format	
		WEP not set 💌	112	1		ASCII •	
	Allow Shared Key Authentication	Enabled					_
	CKIP Parameters						
	802.11 Data Encryption	Current Key: 0 t	oits CKIP Key	(Key Index= 0)			
		Key Size Key	Index Encr	yption Key	ĸ	ey Format	
		not set 💌 1	-			ASCII .	
		E					-
	1						
	Foot Notes						
	1 CKIP is not supported by 10	xx model APs					
	2 Web Policy cannot be used i 3 H-REAP Local Switching is n	in combination with IPse ot supported with IPsec	ic , CRANITE aut	hentication			
	4 When client exclusion is ena 5 Client MFP is not active unle	bled, a Timeout Value ss WPA2 is configured	of zero means	infinity (will requir	e administrative	override to reset exc	oluded clients)

8. 向下滾動頁面以修改WPA+WPA2引數。在此示例中,選擇了WPA2策略和AES加密。

cisco	Save Configuration : Eing Logout Befree MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANS WLANS WLANS Advanced	WLANS > Edit < Back

- 9. 在Auth Key Mgmt下,選擇**802.1x**。這將為WLAN啟用使用802.1x/EAP身份驗證和AES加密的 WPA2。
- 10. 按一下**AAA Servers**頁籤。在Authentication Servers下,選擇適當的伺服器IP地址。在本示 例中,10.77.244.196用作RADIUS伺服器。

CISCO MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	
WLANS WLANS > Edit < Back	Apply

11. 按一下「**Apply**」。**注意:**這是需要在控制器上為EAP身份驗證配置的唯一EAP設定。EAP-FAST的所有其他特定配置需要在RADIUS伺服器和需要身份驗證的客戶端上完成。

為WPA2企業模式身份驗證(EAP-FAST)配置RADIUS伺服器

在本示例中,Cisco Secure ACS用作外部RADIUS伺服器。執行以下步驟以配置RADIUS伺服器進行EAP-FAST身份驗證:

- 1. 建立使用者資料庫以驗證客戶端
- 2. <u>將WLC作為AAA使用者端新增到RADIUS伺服器</u>
- 3. <u>使用匿名帶內PAC調配在RADIUS伺服器上配置EAP-FAST身份驗證</u>注意:EAP-FAST可以使 用匿名帶內PAC調配或經過身份驗證的帶內PAC調配進行配置。此示例使用匿名帶內PAC調配 。有關使用匿名帶內PAC調配和經過身份驗證的帶內調配配置EAP FAST的詳細資訊和示例
 - ,請參閱使用無線LAN控制器和外部RADIUS伺服器配置EAP-FAST的示例。

建立使用者資料庫以驗證EAP-FAST客戶端

完成以下步驟,以便為ACS上的EAP-FAST客戶端建立使用者資料庫。此示例將EAP-FAST客戶端 的使用者名稱和密碼分別配置為User1和User1。

 從導航欄中的ACS GUI中選擇User Setup。建立一個新的無線使用者,然後按一下Add/Edit以 轉到此使用者的「編輯」頁。

Cites States User Setup State Hdp	Address http://127.0.0	0.1:1065/	Sector 1 = 1
Deternal User Databases Deternal User Databases Deternal User Deternal User Setup configuration overrides Group Setup configuration. Deternal User Setup Configuration. Decementation Decementation <	Address Petp://127.0.0	User Setup Stort User: User1 Find Add/Edit List users beginning with letter/number: ABCDEFCBFICATE NOPOBSIUTYER Semove Dynamic Users	Vour Setter and External User Databases Vour Setter and External Outside Character Vour Setter and Setter Setter and External Outsideses Sefere ACS Can authenticate users with an external User Outsideses Vour such have the database up and running on the external Server. For example, if you are using taken card authentication, your taken Server must be running and properly configured. You must have configured the applicable parameters in the External User Databases section.
Find. From the list of usernames displayed, click the username whose	Contractor Contractor	Back to Help	Note: User Setup configuration overrides Group Setup configuration. If you rely on the Unknown User Policy in the External User Databases section to create entries in the ACS internal database for users defined in an external user database, usernames cannot be located or listed here until the user has successfully authenticated ence. External user database modification must be done from within the external user database itself, For added security, authorization, and accounting purposes. User Setup leeps track of users who authenticate with an external user database. User Setup leeps track of users in the ACS internal database. Note: User Setup does not add or delete usernames in an external user database. [lisck to Too] Finding a Specific User in the ACS Internal Batabase. To find a user already in the ACS internal database, type the first few latters of the username in the User field, add an arterrisk (*) as a wildcard, and clicks Find. Find. Find. Too find the User field, add an arterrisk (*) as a wildcard, and clicks Find. Find.

 在User Setup Edit頁中,配置真實名稱和說明以及口令設定,如本例所示。本文檔使用ACS內 部資料庫進行口令驗證。

ss 👌 hétp://127.0	0.0.1:1065/	
sco Systems	User Setup	
dhaadha.	Edit	Help
User Setup Group	User: User1 (New User)	Account Disabled Distributed
Shared Profile Components	Account Disabled	Eassword Authentication Group to which the user is assigned Call ack
Network Configuration	Supplementary User Info	Client 3P Address Assignment Advanced SetSing Network Access Restrictions
System Configuration	Description	Han Seations Unant Overlan Account Disable
Configuration Administration Control		Operational able ACLs Advanced TACACS+ Settimus TACACS+ Construct
External User Databases	User Setup	TACACS - College Destroyed TACACS - Shell Command Artherization
Posture Validation	Password Authentication: ACS Internal Database	Command Authorization for Network Device Management Applications TACACS - Unknown Services IETE RADIUS Attributes
Network Access Profiles Reports and	CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not checked.)	RADIUS Yeadar-Specific Attributes
Activity	Password	Account Disabled Status
Documentation	Password	Select the Account Disabled check box to disable this account clear the check box to enable the account.
	Password	Iback to Teel
	Confirm Password	Buleting a Username The Delete button appears only when you are editing an existing user
	Submit Cancel	account, not when you are adding a new user account. To delete the current user account from the database, click Delete . When asked to prefere were action a click De

- 3. 從Password Authentication下拉框中選擇ACS Internal Database。
- 4. 配置所有其他所需的引數,然後按一下Submit。

<u>將WLC作為AAA使用者端新增到RADIUS伺服器</u>

完成以下步驟,即可將控制器定義為ACS伺服器上的AAA使用者端:

- 1. 在ACS GUI上按一下**Network Configuration**。在「Network Configuration」頁面的「Add AAA client」部分下,按一下**Add Entry**,將WLC作為AAA客戶端新增到RADIUS伺服器。
- 2. 在AAA使用者端頁面中,定義WLC的名稱、IP位址、共用密碼和驗證方法(RADIUS/Cisco Airespace)。請參閱製造商提供的文檔,瞭解其它非ACS身份驗證伺服器。

garess i http://127.	0.0.1:1065/	💌 🔁 😡
Cisco Systems	Network Configuration	X
ullbuallbu.	Edit	Help Add Cleant Herbaume
Broup Setup	Add AAA Client	AAA Cleant JP Address Shared Secret Network Device Group RAUUS AND AND AND
Network Configuration	AAA Client Hostname WLC	Arthenticate Using Single Connect TACACS: AAA Client Log Update/Watching Packets from this AAA Client
System Configuration	Shared Secret cisco	Constantial States of the second states and the second states and the second states and the second states and secon
Administration Control	RADIUS Key Wrap Key Encryption Key	address fee accounting packets from this AAA (Bent
Posture Validation	Key	AAA Client Hostname
Network Access Profiles	Key Input Format C ASCII @ Hexadecimal	The AAA Client Hostname is the name assigned to the AAA client.
Reports and Activity	Authenticate Using RADIUS (Cisco Airespace)	[Back to Tep]
Documentation	Single Connect TACACS+ AAA Client (Record stop in accounting on failure) Log Undate/Watchdog Packets from this AAA Client	The AAA Client IP Address is
	Log RADIUS Tunneling Packets from this AAA Client	the IP address assigned to the AAA client.
	Replace RADIUS Port info with Username from this AAA Client	If you want to designate more than one AAA client with a single AAA client action in ACA.
	Match Framed-IP-Address with user IP address for accounting packets from this AAA Client	AAA client to be represented by

注意:您在WLC和ACS伺服器上配置的共用金鑰必須匹配。共用金鑰區分大小寫。

3. 按一下「Submit+Apply」。

使用匿名帶內PAC調配在RADIUS伺服器上配置EAP-FAST身份驗證

匿名帶內調配

這是兩種帶內調配方法之一,其中ACS與終端使用者客戶端建立安全連線,以便為客戶端提供新的 PAC。此選項允許在終端使用者客戶端和ACS之間匿名的TLS握手。

此方法在對等體驗證ACS伺服器之前,在經過身份驗證的Diffie-Hellman金鑰協定協定(ADHP)隧道 內運行。

然後,ACS要求使用者的EAP-MS-CHAPv2身份驗證。成功進行使用者身份驗證後,ACS會與終端 使用者客戶端建立Diffie-Hellman隧道。ACS為該使用者生成一個PAC,並將該PAC連同該ACS的資 訊一起傳送到此隧道中的終端使用者客戶端。此調配方法使用EAP-MSCHAPv2作為零階段的身份 驗證方法,使用EAP-GTC作為第二階段的身份驗證方法。

由於設定了未經身份驗證的伺服器,因此無法使用純文字檔案密碼。因此,隧道內只能使用MS-CHAP憑據。MS-CHAPv2用於證明對等體的身份,並為進一步的身份驗證會話接收PAC(EAP-MS-CHAP將僅用作內部方法)。

完成以下步驟,以便在RADIUS伺服器中配置用於匿名帶內調配的EAP-FAST身份驗證:

1. 在RADIUS伺服器GUI上按一下**System Configuration**。在System Configuration頁面中,選擇 **Global Authentication Setup**。

CiscoSecure ACS - Microsoft Internet Explorer	
Ele Edt Yew Fgvorkes Iools Help	Links ³⁰ Oc
Agdress) http://127.0.0.1:1065/	🗵 🔁 😡
System Configuration	P
adhadha	11-5n
National State Image: Service Control	Service Control Service Control Lessens Data Format Control Lessen Database Resitation ACS Instrema Database Resitation ACS Instrema ACS Instremation ACS Instremation ACS Instremation ACS Instremation ACS Instremation
External User Databases Image: Construction of the construct	Service Control Select to open the page from which you can stop or restart Cisco Secure ACS services. [Rack to Tap] Legging Select to configure various Cisco Secure ACS reports and customize the type of information that is logged. [Rack to Tap] 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. [Rack to Tap]
0	Theres
🐮 Start 😰 🥭 🕴 CiscoSecure ACS - Mic	7:57 10

2. 在Global Authentication setup頁中,按一下**EAP-FAST Configuration**以轉到EAP-FAST設定頁

o

dress a) http://127.0	.0.1:1065/	💌 🛃 Go
Crace Systems	System Configuration	×
Cal Lillean	EAP Configuration	
Settip Group Settip Settip Dared Profile Configuration Suptem Configuration Suptem Configuration Config	PEAP Allow EAP-MSCHAPv2 Allow EAP-GTC Allow Posture Validation Allow EAP-TLS Select one or more of the following options: If Certificate SAN comparison If Certificate Binary comparison EAP-TLS session timeout (minutes): 120 Cisco client initial message: PEAP session timeout (minutes): I20 Enable Fast Reconnect: Image: EAP-EAST	Use this page to specify settings for various authentication protocols. • EAP Configuration • PEAP • EAP-EAST • CAP-E3 • EAP-EAST • CAP-E3 • EAP-EAST • CAP-E3 • EAP Configuration EAP Configuration EAP Configuration EAP is a flexible requestivesponse protocol for arbitrary authentication information (RPC 2204), EAP is layered on top of another protocol such as UDP, 802.1% or RADIUS and supports multiple "authentication" types. EAP PAP PEAP
Documentation	EAP-FAST Configuration EAP-TLS C Allow EAP-TLS Select one or more of the following options:	Note: /EAP is a certificate-based authentication protocol. <i>IEAP</i> authentication can occur only after you have completed the required steps on the ACS Certificate Setup page . • Allow EAP-MSCHAPy2 – Use to enable EAP-MSCHAPy2 within MS PEAP
	Certificate SAN comparison Submit Submit + Restart Cancel	authentication. Enable this protocol for any reportery that supports MS- CHAPv2, such as Microsoft AD, and the ACS Internal Database.

3. 在EAP-FAST設定頁面中,選中Allow EAP-FAST覈取方塊以在RADIUS伺服器中啟用EAP-FAST。

gdress 👌 http://127.0	0.0.1:1065/	o 🛃 💌
Cisco Systems	System Configuration	X
adhoadho.	EAP-FAST Configuration	A Help
User Setup		EAP-FAST Configuration Page
Group Setup	EAP-FAST Settings	Use this page to configure EAP-FAST authentication settings.
Shared Profile Components	Allow EAP-FAST	EAP-FAST Settings Client initial message
System Configuration	Retired master key TTL 3 months	Constanting Advances in chand PAC previousing Allow anthronic settlerational PAC previousing Allow machine authoritication
Interface Configuration	Client initial message: tacwebacs	Allow stateless session resume. Allowed incor methods Certificate Comparison
Administration Control	Authority ID Info: tacwebacs Image: Allow anonymous in-band PAC provisioning	EAP-ILS session timerur (innertes) EAP-EAST master server Actual EAP-EAST server status
Databases	Allow authenticated in-band PAC provisioning Accept client on authenticated provisioning	EAP-FAST Settings
Validation	Require client certificate for provisioning	 Allow EAP-FAST—To enable EAP-FAST authentication, select this check box.
Reports and Activity	Machine PAC TTL 1 weeks	 Active Maxter Key TTL—Enter a value for the amount of time that a master key is used to generate new Protected Access Credentials (PACs). When the time to love (TTL) defined for the Master Key expires, the master key is considered retired and a new master key is generated.
Documentation	Authorization PAC TTL 1 hours Allowed inner methods	 Retired master key TR.—Enter a value for the amount of time that PACs generated using a retired master key are acceptable for EAP-FAST authentication. When an end-user client guins network access using a PAC based on a retired master key. ACS sends a new PAC to the end-user client.
	C EAP-MSCHAPv2 EAP-TLS Submit Submit + Restart Cancel	 Tunnel PAC TR — Enter a value for the amount of time that a PAC is used before it expires and must be replaced. If the marter key used to generate the Tunnel PAC has not expired, new PAC creation and assignment is automatic. If the marter key used to generate the Tunnel PAC expired, automatic or manual provisioning must be avaid to pervice the end-user

- 4. 根據需要配置活動/已停用主金鑰TTL(生存時間)值,或將其設定為預設值(如本例所示)。 有關活動主金鑰和已停用主金鑰的資訊,請參閱主金鑰。此外,請參閱主金鑰和PAC TTL瞭解 詳細資訊。Authority ID Info欄位表示此ACS伺服器的文本標識,終端使用者可以使用該標識來 確定對其進行身份驗證的ACS伺服器。必須填寫此欄位。Client initial display message欄位指 定要傳送給使用EAP-FAST客戶端進行身份驗證的使用者的消息。最大長度為40個字元。僅當 終端使用者客戶端支援顯示時,使用者才會看到初始消息。
- 5. 如果您希望ACS執行匿名帶內PAC調配,請選中允許匿名帶內PAC調配覈取方塊。
- 6. **允許的內部方**法 此選項確定哪些內部EAP方法可以在EAP-FAST TLS隧道內運行。對於匿 名帶內調配,必須啟用EAP-GTC和EAP-MS-CHAP以實現向後相容性。如果選擇Allow anonymous in-band PAC provisioning(允許匿名帶內PAC調配),則必須選擇EAP-MS-CHAP(零階段)和EAP-GTC(第二階段)。

為WPA2企業操作模式配置無線客戶端

下一步是為WPA2企業模式配置無線客戶端。

完成這些步驟,為WPA2企業模式配置無線客戶端。

- 在Aironet案頭實用程式視窗中,按一下Profile Management > New,以便為WPA2-Enterprise WLAN使用者建立配置檔案。如前所述,本文檔將WLAN/SSID名稱用作WPA2-Enterprise用於 無線客戶端。
- 在Profile Management視窗中,按一下General頁籤,然後配置Profile Name、Client Name和 SSID名稱,如本例所示。然後,按一下 OK

Profile Management		? 🗙
General Security Advance	ed	
Profile Settings Profile Name: Client Name:	WPA2-Enterprise Wireless-Client1	
Network Names SSID1: SSID2: SSID3:	WPA2-Enterprise	
	ОК	Cancel

3. 按一下**Security**頁籤,然後選擇**WPA/WPA2/CCKM**以啟用WPA2操作模式。在 WPA/WPA2/CCKM EAP Type下,選擇**EAP-FAST**。按一下**Configure**以配置EAP-FAST設定。

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	
	ОК	ancel

4. 在「配置EAP-FAST」視窗中,選中**允許自動PAC調配**覈取方塊。如果要配置匿名PAC調配 ,EAP-MS-CHAP將用作零階段中唯一的內部方法。

Configure EAP-FAST	? 🔀
EAP-FAST Authentication Method	
MSCHAPv2 User Name and Password	Configure
Protected Access Credentials (PAC)	
Select One or More PAC Authorities	
	Manage
K	>
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. 從EAP-FAST Authentication Method下拉框中選擇MSCHAPv2 User Name and Password作 為身份驗證方法。按一下「**Configure**」。
- 6. 從Configure MSCHAPv2 User Name and Password視窗,選擇相應的使用者名稱和密碼設定。本示例選擇自動提示輸入使用者名稱和密碼。

Always Resume the Secu	re Session	
Validate Server Identity		
Trusted Root Certification Au	Ithorities	
<any></any>		*
User Name and Password S	ettings	
 Use Temporary User 	r Name and Password	
🚫 Use Windows l	User Name and Password	
 Automatically P 	rompt for User Name and Password	
Manually Promp	pt for User Name and Password	
OUse Saved User Nan	me and Password	-
O Use Saved User Nar User Name:	me and Password Administrator	
O Use Saved User Nan User Name: Password:	me and Password Administrator	
O Use Saved User Name User Name Password: Confirm Password:	me and Password Administrator	
O Use Saved User Name User Name Password: Confirm Password: Domain:	me and Password Administrator	
OUse Saved User Name User Name Password Confirm Password Domain	me and Password Administrator	
O Use Saved User Name User Name Password: Confirm Password Domain	me and Password Administrator	
O Use Saved User Name User Name Password: Confirm Password: Domain:	me and Password Administrator	

在ACS中註冊相同的使用者名稱和密碼。如前所述,此示例分別使用User1和User1作為使用 者名稱和密碼。另請注意,這是一個匿名的帶內調配。因此,使用者端無法驗證伺服器憑證。 您需要確保未選中Validate Server Identity覈取方塊。

7. 按一下「OK」(確定)。

<u>驗證WPA2企業運行模式</u>

完成以下步驟以驗證WPA2企業模式配置是否正常工作:

- 1. 在Aironet案頭實用程式視窗中,選擇配置檔案WPA2-Enterprise,然後按一下Activate以啟用 無線客戶端配置檔案。
- 2. 如果您已啟用MS-CHAP ver2作為身份驗證,則客戶端將提示輸入使用者名稱和密碼。

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

3. 在使用者的EAP-FAST處理期間,客戶端將提示您從RADIUS伺服器請求PAC。按一下**Yes**後 ,PAC調配將啟動。

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

4. 在零階段中成功調配PAC後,緊接著進行第一階段和第二階段,並成功執行身份驗證過程。身份驗證成功後,無線客戶端將與WLAN WPA2-Enterprise相關聯。螢幕截圖如下

🛜 Cisco Aironet Desktop Utility	y - Current Profile:	WPA2-Enterprise
<u>A</u> ction <u>O</u> ptions <u>H</u> elp		
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

您還可以驗證RADIUS伺服器是否收到並驗證來自無線使用者端的驗證請求。檢查ACS伺服器 上的Passed Authentications and Failed Attempts報告以完成此操作。這些報告可在ACS伺服 器的「報告和活動」下找到。

<u>為WPA2個人模式配置裝置</u>

執行以下步驟將裝置配置為WPA2-Personal操作模式:

- 1. <u>為WPA2個人模式身份驗證配置WLAN</u>
- 2. <u>為WPA2個人模式配置無線客戶端</u>

<u>為WPA2個人操作模式配置WLAN</u>

您需要設定使用者端用來連線到無線網路的WLAN。WPA2個人模式的WLAN SSID將為WPA2 — 個人。此範例將此WLAN指派給管理介面。

完成以下步驟即可設定WLAN及其相關引數:

- 1. 從控制器的GUI中按一下「**WLANs**」,以顯示「WLANs」頁面。此頁面列出控制器上存在的 WLAN。
- 2. 按一下New以建立一個新的WLAN。
- 在WLANs > New頁面上輸入WLAN SSID名稱、配置檔名稱和WLAN ID。然後,按一下「 Apply」。本示例使用WPA2-Personal作為SSID。

						Sa <u>v</u> e Co	infiguration <u>P</u> ing	Logout <u>R</u> efresh
cisco	MONITOR WLAN		W1RELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
WLANs	WLANs > New						< Back	Apply
WLANS	Туре	WLAN	×					
≱ Advanced	Profile Name	WPA2-Per	rsonal					
	WLAN SSID	WPA2-Per	rsonal					

- 4. 建立新的WLAN後,系統會顯示新WLAN的**WLAN > Edit**頁面。在此頁面上,您可以定義此 WLAN的特定各種引數。這包括常規策略、安全策略、QOS策略和高級引數。
- 5. 在General Policies下,勾選Status覈取方塊以啟用WLAN。
- 6. 如果您希望AP在其信標幀中廣播SSID,請選中Broadcast SSID覈取方塊。
- 7. 按一下**Security**頁籤。在Layer Security下,選擇**WPA+WPA2**。這將為WLAN啟用WPA身份驗 證。

ababa					Sa <u>v</u> e Co	onfiguration (Ping)	Logout Befre
cisco	MONITOR WLANS CONTR	OLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
WLANs	WLANs > Edit General Security C	205 Advanced				< Back	Apply
WLANS WLANS Advanced	Layer 2 Layer 3	AAA Servers					-
	Layer 2 Security WPA+	WPA2 •					
	802.11 Data Encryption	Current Key:	104 bits WE	P Static Key (Key I	index = 0)	Kau Comat	
		WEP not set	1 I	Encryption key	/	ASCII .	
	Allow Shared Key Authentication	Enabled					
	802.11 Data Encryption	Current Key: 0 8	its CKIP Key	(Key Index= 0)			
		Key Size Key	Index Encr	yption Key	к [ey Format ASCII 💌	
	*[F					<u>ب</u>
	Foot Notes I CKIP is not supported by 10 2 Web Policy cannot be used i 3 H-REAP Local Switching is no 4 When client exclusion is ena 5 Client MRP is not active unles	xx model APs n combination with IPsec st supported with IPsec bled, a Timeout Value ss WPA2 is configured	ic , CRANITE aut of zero means	hentication infinity (will requir	e administrative	override to reset exc	luded clients)

8. 向下滾動頁面以修改WPA+WPA2引數。在此示例中,選擇了WPA2策略和AES加密。 9. 在Auth Key Mgmt下,選擇PSK以啟用WPA2-PSK。

10. 在相應的欄位中輸入預共用金鑰,如下所示。

	Sage Configuration Ping Logout Befresh
cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANS WLANS	WLANs > Edit <back 2="" 3="" aaa="" advanced="" apply="" general="" layer="" qos="" security="" servers<="" td=""></back>
▶ Advanced	Key Size Key Index Encryption Key Key Format not set 1 ASCII ASCII MMH Mode Enabled Enabled Key Permutation Enabled 802.1X Parameters Type Key Size © WEP 104 bits
	WPA Policy Image: Constraint of the second
	Foot Nates 1 CKIP is not supported by 10xx model APs 2 Web Policy cannot be used in combination with IPsec 3 M-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 MPP is not active unless WPA2 is configured

注意:WLC上使用的預共用金鑰必須與無線客戶端上配置的金鑰匹配。

11. 按一下「Apply」。

<u>為WPA2個人模式配置無線客戶端</u>

下一步是將無線客戶端配置為WPA2 — 個人操作模式。

完成以下步驟,將無線客戶端配置為WPA2 — 個人模式:

- 1. 在Aironet案頭實用程式視窗中,按一下**Profile Management > New**,以便為WPA2-PSK WLAN使用者建立配置檔案。
- 2. 在Profile Management視窗中,按一下**General**頁籤,然後配置Profile Name、Client Name和 SSID名稱,如本例所示。然後,按一下**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 с	Cancel

3. 按一下Security頁籤,然後選擇WPA/WPA2 Passphrase以啟用WPA2-PSK操作模式。按一下 Configure以配置WPA-PSK預共用金鑰。

Profile Management			? 🔀
General Security Advanced			
- Set Security Options			
WPA/WPA2/CCKM	WPA/WPA2/CCKM EAP Type:	LEAP	¥
• WPA/WPA2 Passphrase			
O 802.1x	802.1x EAP Type:	LEAP	
O Pre-Shared Key (Static WEP)			
O None			
Configure	Allow Association to Mixed Cells		
	Limit Time for Finding Domain	Controller To: 0	tec sec
Group Policy Delay:	60 😂 sec		
			OK Cancel

4. 輸入預共用金鑰,然後按一下OK。

Configure WPA/WPA2 Passphrase	2 🔀			
Enter a WPA/WPA2 passphrase (8 to 63 ASCII or 64 hexadecimal characters)				
abcdefghijkl				
	OK Cancel			

<u>驗證WPA2 — 個人操作模式</u>

完成以下步驟,驗證WPA2-Enterprise模式配置是否正常工作:

- 1. 在Aironet案頭實用程式視窗中,選擇配置檔案WPA2-Personal,然後按一下Activate以啟用無 線客戶端配置檔案。
- 2. 一旦配置檔案被啟用,無線客戶端就會在身份驗證成功後與WLAN關聯。螢幕截圖如下

Cisco Aironet Desktop Utility	y - Current Profile: WPA2-I	Personal 🛛 🛛 🔀
Action Options Help		
Current Status Profile Management	Diagnostics	
CISCO SYSTEMS		
Profile Name:	WPA2-Personal	
Link Status:	Authenticated	Network Type: Infrastructure
Wireless Mode:	5 GHz 54 Mbps	Current Channel: 149
Server Based Authentication:	None	Data Encryption: AES
IP Address:	10.77.244.221	
Signal Strength:		Good
		Advanced

<u>疑難排解</u>

本節提供的資訊可用於對組態進行疑難排解。

以下debug指令對組態疑難排解很有用:

附註:使用 debug 指令之前,請先參閱<u>有關 Debug 指令的重要資訊</u>。

 debug dot1x events enable — 啟用所有dot1x事件的調試。以下是基於成功身份驗證的調試輸 出示例:注意:由於空間限制,此輸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 — 啟用802.1x資料包消息的調試。

• debug aaa events enable — 啟用所有aaa事件的調試輸出。

相關資訊

- WPA2 Wi-Fi保護訪問2
- 使用無線LAN控制器和外部RADIUS伺服器的EAP-FAST身份驗證配置示例
- 使用WLAN控制器(WLC)的EAP驗證組態範例
- WPA配置概述
- 無線產品支援
- 技術支援與文件 Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。