# 使用ACS 5.2和WLC配置PEAP和EAP-FAST

目录

简介 <u>先决条件</u> 要求 使用的组件 规则 配置 网络图 假设 配置步骤 配置 RADIUS 服务器 配置网络资源 配置用户 定义策略元素 应用访问策略 <u>配置 WLC</u> 用身份验证服务器的详细信息配置 WLC 配置动态接口 (VLAN) <u>配置 WLAN (SSID)</u> 配置无线客户端实用程序 PEAP-MSCHAPv2(user1) EAP-FAST(user2) <u>验证</u> 验证user1(PEAP-MSCHAPv2) <u>验证user2(EAP-FAST)</u> 故障排除 故障排除命令 相关信息

## 简介

本文档说明如何使用外部RADIUS服务器(例如访问控制服务器(ACS)5.2)配置无线LAN控制器 (WLC)以进行可扩展身份验证协议(EAP)身份验证。

## 先决条件

### 要求

尝试进行此配置之前,请确保满足以下要求:

- 具有WLC和轻量接入点(LAP)的基本知识
- 具有AAA服务器的功能知识
- 全面了解无线网络和无线安全问题

使用的组件

本文档中的信息基于以下软件和硬件版本:

- 运行固件版本 7.0.220.0 的 Cisco 5508 WLC
- Cisco 3502 系列 LAP
- 带英特尔6300-N驱动程序14.3版的Microsoft Windows 7本地请求方
- 运行 5.2 版的 Cisco 安全 ACS
- Cisco 3560 系列交换机

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。

#### 规则

有关文档约定的更多信息,请参考 Cisco 技术提示约定。

## 配置

本部分提供有关如何配置本文档所述功能的信息。

注意:要获取此部分中所用命令的更多信息,可使用<u>命令查找工具</u>(仅限<u>已注册</u>客户)。

#### 网络图

本文档使用以下网络设置:



下面是此图中使用的组件的配置详细信息:

- ACS (RADIUS) 服务器的 IP 地址为 192.168.150.24。
- WLC的管理和AP管理器接口地址为192.168.75.44。
- DHCP服务器地址为192.168.150.25。
- 整个配置中都使用VLAN 253。两个用户都连接到同一个SSID"goa"。但是, user1配置为使用 PEAP-MSCHAPv2进行身份验证, user2配置为使用EAP-FAST进行身份验证。
- 用户将分配到VLAN 253中:
  - VLAN 253:192.168.153.x/24。网关:192.168.153.1
  - VLAN 75:192.168.75.x/24。网关:192.168.75.1

- 所有第3层VLAN都配置了交换机。
- 为DHCP服务器分配了一个DHCP作用域。
- 网络中的所有设备之间都存在第3层连接。
- LAP已连接到WLC。
- 每个VLAN都使用/24掩码。
- ACS 5.2已安装自签名证书。

## 配置步骤

此配置分为三个高级步骤:

- 1. <u>配置 RADIUS 服务器。</u>
- 2. <u>配置WLC。</u>
- 3. <u>配置无线客户端实用程序。</u>

## 配置 RADIUS 服务器

RADIUS服务器配置分为四个步骤:

- 1. <u>配置网络资源。</u>
- 2. <u>配置用户.</u>
- 3. <u>定义策略元素。</u>
- 4. <u>应用访问策略。</u>

ACS 5.x是基于策略的访问控制系统。也就是说,ACS 5.x使用基于规则的策略模型,而不是4.x版 本中使用的基于组的模型。

ACS 5.x基于规则的策略模型提供比旧的基于组的方法更强大、更灵活的访问控制。

在旧的基于组的模型中,一个组定义策略,因为它包含三种类型的信息并将它们关联在一起:

- 身份信息 此信息可以基于AD或LDAP组中的成员资格或内部ACS用户的静态分配。
- 其他限制或条件 时间限制、设备限制等。
- 权限 VLAN或Cisco IOS®<sup>权</sup>限级别。

ACS 5.x策略模型基于以下形式的规则:

• 如果condition,则结果

例如,我们使用为基于组的模型描述的信息:

• 如果为identity-condition、restriction-condition,则为authorization-profile。

因此,我们可以灵活地限制在什么条件下允许用户访问网络,以及在满足特定条件时允许什么授权 级别。

配置网络资源

在本节中,我们将为RADIUS服务器上的WLC配置AAA客户端。

此过程说明如何在 RADIUS 服务器上将 WLC 添加为 AAA 客户端,以便 WLC 可以将用户凭证传递 到 RADIUS 服务器。

请完成以下步骤:

1. 从ACS GUI中,转到Network Resources > Network Device Groups > Location,然后单击 Create(位于底部)。

cisco Secure ACS					
🕨 💮 My Workspace	Network Resources > Network Device Groups > Location				
🔹 🦣 Network Resources	Network Device Groups				
<ul> <li>Network Device Groups</li> <li>Location</li> </ul>	Filter: Match if: Go 🔻				
Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers	Name      Description     All Locations				
Busers and Identity Stores					
► Sport Policy Elements					
► 🔂 Access Policies					
Monitoring and Reports					
🕞 🍕 System Administration					

2. 添加必填字段,然后单击Submit。

Device Group -	General	
o Name.	LAB	
Description	LAB Devices	
o Parent:	All Locations	Select
= Required fi	elds	

现在您将看到以下屏幕:

cisco Cisco Secure A	CS
🕨 😽 My Workspace	Network Resources > Network Device Groups > Location
👻 🐙 Network Resources	Network Device Groups
<ul> <li>Network Device Groups</li> <li>Location</li> </ul>	Filter: Match if:
Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers	Image: Name     ▲     Description       Image: The second secon
Users and Identity Stores	LAB LAB Devices
Policy Elements	
Access Policies	
Monitoring and Reports	
System Administration	

3. 单击Device Type > Create。

cisco Cisco Secure A	CS	
► 🚭 My Workspace	Network Resources > Network Device Groups > Device Type > Create	
In Network Resources      Network Device Groups     Location      Device Type      Network Devices and AAA Clients     Default Network Device     External RADIUS Servers	Device Group - General         Image: State         Image: State	Select
Users and Identity Stores		
Policy Elements		
Access Policies		
Monitoring and Reports		
<ul> <li>System Administration</li> </ul>		

4. 单击"Submit"。现在您将看到以下屏幕:

cisco Cisco Secure A	CS
▶ 🚭 My Workspace	Network Resources > Network Device Groups > Device Type
🔹 🧤 Network Resources	Network Device Groups
Network Device Groups     Location     Device Type	Filter: Go 🗢
Network Devices and AAA Clients	Name   Description
Default Network Device External RADIUS Servers	All Device Types All Device Types
B Users and Identity Stores	5508 Wireless LAN Controller
Policy Elements	
Access Policies	
Monitoring and Reports	
System Administration	

- 5. 转至Network Resources > Network Devices and AAA Clients。
- 6. 单击Create,然后填写详细信息,如下所示:

+ 🚯 My Workspace	Network Resources > Net	work Devices and AAA Clerks > Create		
Location     Device Groups     Location     Device Type     Network Devices and AAACtionts     Default Network Device     External RADIUS Servers	Name: WL Description: Win Network Device Gro Location Device Type	C-5508 eless LAN Controller All Locations:LAB All Device Types:5508	Salect Salect	
Busers and Identity Stores     Policy Elements     Access Policies     Monitoring and Reports	IP Address G Single IP Ad 9 IP: 192 108 75	Idress C IP Range(s)	Auther > TAC = RAD	ntication Options ACS+ NUS Shared Secret  cisco
<ul> <li>System Administration</li> </ul>	6 - Required fields			CoAlport (1700 Enable KeyWiap Key Encryption Key: Wessage Authenticator Code Key: Key Input Format C ABCII C HEXADECIMAL

7. 单击"Submit"。现在您将看到以下屏幕:

ler.		<ul> <li>Match it.</li> </ul>	•	G0 🔻	
	Name 🔺	IP / Mask	NDG:Location	NDG:Device Type	Description
	WLC-5508	192.168.75.44/32	All Locations:LAB	All Device Types:5508	Wireless LAN Controller

## 配置用户

在本节中,我们将在ACS上创建本地用户。用户(user1和user2)都分配到名为"无线用户"的组。

1. 转至Users and Identity Stores > Identity Groups > Create。

cisco Cisco Secure ACS					
► S My Workspace	Users and identity Stores > Identity Groups > Create				
In Network Resources					
🔹 🏰 Users and Identity Stores	General 8 Name: Wireless Users				
Identity Groups	Description: Wireless Users authenticating over wireless				
<ul> <li>Internal Identity Stores</li> <li>Users</li> </ul>	o Parent All Groups Select				
Hosts	• = Required telds				
External Identity Stores					
Active Directory					
RSA SecurID Token Servers					
RADIUS Identity Servers Certificate Authorities					
Certificate Authentication Profile					
Identity Store Sequences					
<ul> <li>Sp. Policy Elements</li> </ul>					

2. 单击Submit后,页面将如下所示:

cisco Cisco Secure Ad	CS		
🕨 🖑 My Workspace	Users and Identity Stores > Identity Groups		
Network Resources	Identity Groups		
🔹 🙀 Users and Identity Stores	Filter: 💌 Match it: 💌 Go 🔝		
Identity Groups Internal Identity Stores Users Hosts External Identity Stores LDAP Active Directory	Image:		
RSA SecuriD Token Servers RADIUS Identity Servers Certificate Authorities Certificate Authoritication Profile Identity Store Sequences Policy Elements			

- 3. 创建用户user1和user2,并将它们分配到"Wireless Users"组。
  - a. 单击Users and Identity Stores > Identity Groups > Users > Create。

cisco Cisco Secure AC	S
▶ 🚳 My Workspace	Users and identity Stores > Internal identity Stores > Users > Create
Network Resources	General
🔹 🏭 Users and Identity Stores	o Name: User1 Status: Enabled ▼ 0
Identity Groups     Internal Identity Stores	Description: PEAP:mschapv2 users
Users	Identity Group: All Groups: Wireless Users
Hosts External Identity Stores Certificate Authorities Certificate Authentication Profile Identity Store Sequences	Password Information Password must • Contain 4 - 32 characters
Policy Elements	C Password:
Access Policies	Confirm Paseword:
<ul> <li>Moniforing and Reports</li> </ul>	Change password on next login
<ul> <li>System Administration</li> </ul>	User Information There are no additional identity attributes defined for user records • = Required fields

b. 同样,创建user2。

🖌 🚭 My Workspace	Users and Identity Stores > Internal Identity Stores > Users > Create
An Network Resources	Connect
👷 🏭 Users and Identity Stores 🕬	Status: Enabled T @
Identity Groups	Description: FAPFAST user
<ul> <li>Internal Identity Stores</li> </ul>	0 Identity Crown All Crowne Wireless Lisers Select
Hosts	
<ul> <li>External identity Stores</li> </ul>	Password Information
Certificate Authorities	Password must
Certificate Authentication Profile	<ul> <li>Contain 4 - 32 characters</li> </ul>
So Policy Elements	Password:
Access Policies	Confirm
- En Lionitaring and Deports	Password:
	Change password on next login
<ul> <li>Mystem Administration</li> </ul>	Liser Information

屏幕将如下所示:

cisco Cisco Secure A	ACS			
🖌 🚭 My Workspace	Users and Identity Store	s > Internal identity Stor	es > Users	
► 157 Network Resources	Internal Users			
Gauge Contract C	Filter:	• Match it:	▼ G0 マ	
Internal Identity Stores	C Status	User Name	<ul> <li>Identity Group</li> </ul>	Description
Users		user1	All Groups:Wireless Users	PEAP:mschapv2 users
<ul> <li>External Identity Stores</li> </ul>	F 9	user2	All Groups:Wireless Users	EAPFAST user
Certificate Authorities Certificate Authentication Profile Identity Store Sequences				
Policy Elements				

### 定义策略元素

验证Permit Access已设置。

cisco Cisco Secure A	CS
<ul> <li>My Workspace</li> </ul>	Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles
Network Resources	Authorization Profiles
Users and Identity Stores	Filter Match it G0 V
👻 🎭 Policy Elements	
Session Conditions     Authorization and Permissions	Permit Access
<ul> <li>Network Access Authorization Profiles</li> </ul>	
Device Administration     Named Permission Objects	
Access Policies	
► 🔝 Monitoring and Reports	
🖌 🍓 System Administration	

### 应用访问策略

在本节中,我们将选择要使用的身份验证方法以及配置规则的方式。我们将根据前面的步骤创建规 则。

请完成以下步骤:

1. 转至Access Policies > Access Services > Default Network Access > Edit: "Default Network Access"。

cisco Cisco Secure A	CS
+ 🔿 My Workspace	Access Policies > Access Services > Default Network Access > Edit. "Default Network Access"
Network Resources	
Users and Identity Stores	General Allowed Protocols
► Sp. Policy Elements	Name: Default Network Access
🔹 🌉 Access Policies	Description: Default Network Access Service
<ul> <li>Access Services</li> <li>II Service Selection Rules</li> </ul>	Service Type : Network Access
Dafault Device Admin	Policy Structure
🕨 🙆 Default Network Access	Identity
► Ø deleterne	Group Mapping
Monitoring and Reports	Authorization
🖌 🍓 System Administration	

2. 选择您希望无线客户端进行身份验证的EAP方法。在本示例中,我们使用PEAP-MSCHAPv2和EAP-FAST。

cisco Cisco Secure AC	CIS	
🕨 🔗 My Workspace	Access Palicies > Access Services > Default Network Access	s > Edit: "Default Network Access"
+ 🎲 Network Resources		
B Users and Identity Stores	General Allowed Protocols	
Policy Elements	Process Host Lookup	
👻 🌉 Access Policies	Authentication Protocols	
Access Services     El Service Selection Rules     O Default Device Admin     O Default Network Access	Allow PAP/ASCI     Allow CHAP	
Identity Authorization ► Ø deleterne	Allow MS-CHAPv1     Allow MS-CHAPv2	
Monitoring and Reports     System Administration	► I Allow EAP-MD5	
	Allow EAP-TLS	
	Allow LEAP	
	Allow PEAP	
	► MIIow EAP-FAST	
	Preferred EAP protocol LEAP	

+ 🛼 Access Policies	► Allow LEAP
Access Services     Bervice Selection Rules     Opefault Device Admin     Opefault Device Admin     Opefault Network Access     Identity     Authorization     Ø deleteme     Monitoring and Reports     Ø System Administration	✓ ✓ Allow PEAP     PEAP Inner Methods     ✓ Allow EAP-I/IS-CHAP/2     ✓ Allow Password Change Retries: 1     ✓ Allow EAP-GTC     ✓ Allow Password Change Retries: 1
	<ul> <li>Now EAP-FAST</li> <li>EAP-FAST Inner Methods</li> <li>Allow EAP-MS-CHAPV2</li> <li>Allow Password Change Retries: 3</li> <li>Allow EAP-GTC</li> <li>Allow TLS-Renegotiation</li> <li>Use PACs DontUse PACs</li> <li>Tunnel PAC Time To Live: 90 Days v</li> <li>Proactive PAC update will occur after 10 % of PAC Time To Live has expired</li> <li>Allow Authenticated in-Band PAC Provisioning</li> <li>Server Returns Access Accept After Authenticsted Provisioning</li> <li>Barver Returns Access Accept After Authenticsted Provisioning</li> <li>Allow Machine Authentication</li> <li>Machine PAC Time To Live: 1 Weeks v</li> <li>Enable Stateless Bession Resume</li> <li>Authorization PAC Time To Live: 1 Hours v</li> </ul>

- 3. 单击"Submit"。
- 4. 验证您选择的身份组。在本示例中,我们使用Internal Users,这是我们在ACS上创建的。保存更改。

<ul> <li>Single result</li> </ul>	selection C Rule based result selection
Identity Source:	temal Users Select
	Advanced Options
	authentication failed Reject 📼
	user not found Reject 💌
	process failed Drop 💌
	te: For authentications using PEAP, LEAP, EAP-FAST or RADIUS MSCHAP it is not possible to continue posssing when authentication fails or user is not found. If continue option is selected in these cases, requests will rejected

5. 要验证授权配置文件,请转到访问策略 > 访问服务 > 默认网络访问 > 授权。

您可以自定义在什么条件下允许用户访问网络,以及经过身份验证后通过什么授权配置文件 (属性)。此精细度仅在ACS 5.x中可用。在本示例中,我们选择Location、Device Type、 Protocol、Identity Group和EAP Authentication Method。



- 6. 单击确定, 然后单击保存更改。
- 7. 下一步是创建规则。如果未定义规则,则允许客户端在不带任何条件的情况下访问。单击Create > Rule-1。此规则适用于"无线用户"组中的用户。

Access Policies > Access Services > Default Network Access > Authorizati				
Standard Policy Exception Policy				
Network Access Authorization Petine				1
Filter: Status Cisco Secure ACS - Mosilia Feet	юн		×	
192160150.24 https://25	2.168.150.24/acsadmin/Poli	cyInputAction.do	合	
I Status Feame NE		-		
No data to display General		<b>V</b>		
Name: Ftule-1	Status: Enabled	- 8		
Conditions	ize button in the lower ri ions and results are avai	ght area of the policy rules screen co Nable here for use in policy rules.	ntrois which	
VDG:Location:	in	All Locations LAB	Select	
VDG.Device Type:	in	All Device Types 5500	Select	
Status       Name         No data to display             Image: Status       Name             Image: Status       Image: Status             Image: Status				
Identity Group:	in	<ul> <li>VI Groups Wireless Users</li> </ul>	Select	
Eap Authentication 18	ethod:  -ANY-			
Results Authorization Profiles:		1		
Select Deselect		You may select multiple authorization pro defined in multiple profiles will use the v profile defined.	ofiles. Attributes alue from the first	
" E Defaut Fr			THEP	
Create  * Duplicate  * Edit Delete A Move te	×		Custemiza	HtCount

8. 保存更改。屏幕将如下所示:

Network A	Access As	thorization Policy					
Filter. St	atus	- Nati	ch it Equals 💽 Enat	ied - Ci	ear Filter Go 🔻		
Status	Name	NDG:Location	NDG Device Type	Condition Protocol	identity Group	Eap Authentication Nethod	Results Authorization Profile
	Rule-1	in All Locations:LAB	in All Device Types 5508	match Radius	in All Groups:Wireless Users	-4117-	Permit Access
	_						
Default		The rules defined or 1	no enabled rule matches.				Pormit Access

如果希望拒绝不匹配条件的用户,请编辑默认规则以显示"拒绝访问"。

9. 现在我们将定义服务选择规则。使用此页可以配置简单策略或基于规则的策略,以确定将哪种服务应用于传入请求。在本示例中,使用基于规则的策略。

Access C Si Servi Filter	Policies : ingle re: ce Sele r. Statu	Access i suit select ction Poli	ton (*) F icy Natch it	Service Selection Rule based resul	Rules selection	Clear Filter	00   -	
		Status	Name	Protocol	Conditions		Resulta	Hit Count
1		0	Rule-1	match Radius			Default Network Access	0
2	sa Policies - Access Berukes - Service Selection Rules Single result selection Policy Iter: Status  Name Protocol Service Htt Count Protocol Rule-1 match Radius Default Network Access 0 Rule-2 match Tacacs Default Device Admin 0							

## 配置 WLC

此配置要求执行下列步骤:

- 1. <u>用身份验证服务器的详细信息配置 WLC.</u>
- 2. <u>配置动态接口(VLAN)。</u>
- 3. <u>配置WLAN(SSID)。</u>

用身份验证服务器的详细信息配置 WLC

必须配置WLC,使其可以与RADIUS服务器进行通信,以便对客户端进行身份验证,以及执行任何 其他事务。

请完成以下步骤:

- 1. 从控制器 GUI 中,单击 Security。
- 2. 输入 RADIUS 服务器的 IP 地址以及在 RADIUS 服务器和 WLC 之间使用的共享密钥。

此共享密钥应与RADIUS服务器中配置的密钥相同。

cisco	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
Security	RADIUS Authenti	cation Server	s > New					
<ul> <li>AAA</li> <li>General</li> <li>RADIUS</li> <li>Authentication Accounting Falback</li> <li>TACACS+ LDAP</li> <li>Local Net Users</li> <li>MAC Filtering</li> <li>Disablad Clients</li> <li>User Login Policies</li> <li>AP Policies</li> <li>Pasword Policies</li> <li>Pasword Policies</li> </ul>	Server Index (Priorit Server IP Address Shared Secret Form Shared Secret Confirm Shared Sec Key Wrap Port Number Server Status	ty) et ret	1 x 192.168.150.2 ASCII x  (Designed for 1812 Cnabled x	r FIPS custom	ers and requires a	key wrap compl	ant RADI	US server)
Local EAP	Support for RFC 357	6	Enabled -					
Priority Order	Server Timeout		2 aecond	a				
Certificate	Network User		🗷 Enable					
Access Control Lists	Management		🖻 Enable					
Wireless Protection     Policies	IPSec		Enable					
Web Auth								
Advanced								

配置动态接口 (VLAN)

此过程介绍如何在WLC上配置动态接口。

请完成以下步骤:

1. 动态接口是在控制器GUI的Controller > Interfaces窗口中配置的。

սիսիս cisco	MONITOR M		OLLER WIREL	ess <u>s</u> ecurity	MANAGEMENT
Controller General Inventory Interfaces Interface Groups Multicast Network Routes Network Routes Network Routes Nobility Management Ports NTP CDP Advanced	Interfaces > Interface Nar VLAN Id	New me <u>vlan253</u> 253			

2. 单击 Apply。

这会将您带到此动态接口(这里为 VLAN 253)的 Edit 窗口中。

3. 输入此动态接口的 IP 地址和默认网关。

uluilu cisco	MONITOR WLANS C	ONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT
Controller	Interfaces > Edit				
General Inventory Interfaces Interface Groups	Ceneral Information	vlan253			
Multicast Network Routes	NAC Address	00:24:91	7:09:03:cf		
Mobility Management     Ports	Guest Lan Quarantine Quarantine Map Id				
CDP     Advanced	Physical Information	d to a LAG.			
	Enable Dynamic AP Management				
	Interface Address				
	VLAN Identifier	253			
	IP Address	192.168.153	3.81		
	Netmask	255.255.258	5.0		
	DHCB Information	1.00.000.000			
	Primary DHCP Server Secondary DHCP Serve	13 r	2,168,150,25		
	Access Control List				
	ACL Name	n	one -		
	Note: Changing the Interfa temporarily disabled and t some clients.	ice peremeters hus may result	causes the WL in loss of conn	Alls to be ectivity for	

- 4. 单击 Apply。
- 5. 配置的接口如下所示:

cisco	MONITOR	<u>W</u> LANs		WIRELESS	<u>s</u> ecurity	MANAGEMENT	COMMAND	DS HELP	FEEDBACK	
Controller	Interfaces	ŝ								
Inventory	Interface	Name	1	/LAN Identifier	IP Addres	s Interfa	e Type D	ynamic AP I	1anagement	
Interfaces	manageme	nt	-	75	192.168.75	.44 Static	Er	nabled		
Interface Groups	service-por	±	,	N/A.	0.0.0.0	Static	Ne	ot Supported		
Multicast	virtual		1	N/A.	1.1.1.1	Static	No	ot Supported		
Network Routes	<u>vlan253</u>		;	253	192.168.15	3.81 Dynamic	D	isabled		
Internal DHCP Server										
Mobility Management										
Ports										
▶ NTP										
COP										
Advanced										

配置 WLAN (SSID)

此过程说明如何在 WLC 中配置 WLAN。

请完成以下步骤:

- 1. 从控制器GUI中,转到WLANs > Create New以创建新的WLAN。此时会显示 New WLANs 窗口。
- 2. 输入 WLAN ID 和 WLAN SSID 信息。

您可以输入任何名称作为WLAN SSID。本示例使用goa作为WLAN SSID。

cisco		<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	COMMANDS
WLANS	WLANs >	New					
<ul> <li>WLANS</li> <li>WLANS</li> <li>▶ Advanced</li> </ul>	Type Profile Na SSID ID	n ma	WLAA goos goos 1				

3. 单击Apply以转到WLAN目标的Edit窗口。

cisco			WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
WLANs	WLANs > Edit 'ge	ba'					
WLANS WLANS	General Secur	ity QoS	Advanced				
<ul> <li>Advanced</li> <li>AP Groups</li> </ul>	Profile Name Type SSID Status Security Policies Radio Policy Interface/Interfac Group(G) Multicast Man Feat Broadcast SSID	goa WLAN goa [WPA2]] (Modificati All ture ⊂ Inable P Inable	ed Auth(802.1X ons done under U	+ CCKM)] r security tab (	will appear after ap	oplying the chang	yes.)

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY
WLANs	WLANs > Edit 'goa'
WLANS WLANS	General Security QoS Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Løyer 2 Security VPA+WPA2 -
	WPA+WPA2 Parameters
	WPA Policy
	WPA2 Policy R WPA2 Encryption RAES TRIP
	Auth Key Mgmt 802.1X+CCKN .

WLANs > Edit 'goa'		
General Security QoS	Advanced	
Layer 2 Layer 3 AAA Ser	vers	
Select AAA servers below to over	ide use of default servers on this WLAN	
Radius Servers		LDAP Servers
Radius Server Overwrite interface	Enabled	Server 1 None •
	Authentication Servers Accounting Servers	Server 2 None 💌
	Enabled Enabled	Server 3 None 💌
Server 1	IP:192.168.150.24, Port:1812 V None V	
Server 2	None v None v	
Server 3	None × None ×	
Local EAP Authentication		•
Local EAP Authentication Enabl	ed	
Authentication priority order for	0r	
web-auth user		
Not Used	Order Used For Authentication	
•		

#### WLANs > Edit 'goa'

Allow AAA Override Enabled	DHCP
Coverage Hole Detection 🔽 Enabled Enable Bession Timeout 🔽	DHCP Server Override
Aironet IE Penabled	DHCP Addr. Assignment 🔽 Required
Diagnostic Channel Fenabled	Management Frame Protection (MFP)
IPv6 Enable 2	an at an a st. A. Disting
Override Interface ACL None -	MPP Client Protection 2 [Disabled ]
P2P Blocking Action Disabled -	DTIM Period (in beacon intervals)
Client Exclusion 2 Enabled	802.11a/n (1 - 255) 1
Maximum Allowed	802.11b/g/n (1 - 255) 1
Cliente 2 Contraction Contraction	NAC
Static IP Tunneling 😰 🗆 Enabled	NAC State None -
Channel Scanning Defer	Load Balancing and Band Select
Scan Defer Priority 0 1 2 3 4 5 6 7	Client Load Balancing
	Client Band Select
Scan Defer Time(msecs) 100	Parether Ollant

# 配置无线客户端实用程序

PEAP-MSCHAPv2(user1)

在我们的测试客户端中,我们使用的是运行14.3驱动程序版本的Intel 6300-N卡的Windows 7原生 Supplicant客户端。建议使用供应商提供的最新驱动程序进行测试。

要在Windows零配置(WZC)中创建配置文件,请完成以下步骤:

- 1. 转至控制面板 > 网络和Internet > 管理无线网络。
- 2. 单击Add选项卡。
- 3. 单击Manually create a network profile。

🕞 🎿 Man	ually connect to a wireless network	• ×
How d	o you want to add a network?	
	Manually create a network profile This creates a new network profile or locates an existing network and saves a profile for the network on your computer. You need to know the network name (SSID) and security key (if applicable).	
	This creates a temporary network for sharing files or an Internet connection	Cancel

4. 添加在WLC上配置的详细信息。

注意:SSID区分大小写。

5. 单击 Next。

Network name:	goa	
Security type:	WPA2-Enterprise	
Encryption type:	AES	
Security Key:	Hide characters	
V Start this connec	ction automatically	
Connect even if	the network is not broadcasting	

6. 单击Change connection settings以仔细检查设置。

Manually connect to a wireless network	X
Successfully added goa	
Change connection settings Open the connection properties so that I can change the settings.	
	Class
	Close

7. 确保已启用PEAP。

goa Wireless Network Pr	operties	23		
Connection Security				
	[			
Security type:	WPA2-Enterprise			
Encryption type:	AES 👻			
Choose a network aut	hentication method:			
Microsoft: Protected E	EAP (PEAP) 🔻 Settings			
Remember my credentials for this connection each				
time I'm logged on				
Advanced settings				
	OK	ncel		

goa Wireless Network Properties
Connection
Security type: WPA2-Enterprise
Encryption type: AES
Choose a network authentication method:
Microsoft: Protected EAP (PEAP)    Settings
Remember my credentials for this connection each time I'm logged on
Advanced settings
OK Cancel

8. 在本示例中,我们未验证服务器证书。如果选中此框且无法连接,请尝试禁用该功能并再次测 试。

Protected EAP Properties
When connecting:
Validate server certificate
Connect to these servers:
Trusted Root Certification Authorities:
AAA Certificate Services
C AddTrust External CA Root
Class 3 Public Primary Certification Authority
Class 3 Public Primary Certification Authority
DigiCert Assured ID Root CA
DigiCert High Assurance EV Root CA
Do not prompt user to authorize new servers or trusted certification authorities.
Select Authentication Method:
Secured password (EAP-MSCHAP v2)
Enable Fast Reconnect
Enforce Network Access Protection
Enable Identity Brivacy
OK Cancel

9. 或者,您可以使用您的Windows凭据登录。但是,在本例中,我们不打算使用它。Click OK.

-	EAP MSCHAPv2 Properties
	When connecting:
	Automatically use my Windows logon name and password (and domain if any).
CONTRACTOR DE LA CONTRA	OK Cancel

10. 单击Advanced settings以配置用户名和密码。

Connection Security			
Security type: WPA2-Enterprise   Encryption type: AES			
Choose a network authentication method: Microsoft: Protected EAP (PEAP) ▼ Settings Remember my credentials for this connection each time I'm logged on			
Advanced settings			
OK Cance			

Advanced settings				
802.1X settings 802.11 settings				
Specify authentication mode:				
User authentication    Save credentials				
Delete credentials for all users				
Enable single sign on for this network				
Perform immediately before user logon				
Perform immediately after user logon				
Maximum delay (seconds): 10				
Allow additional dialogs to be displayed during single sign on				
This network uses separate virtual LANs for machine and user authentication				
OK Cancel				

Save crede	ntials	
Saving your cr	edentials allows your o	computer to connect to the network
when you re h	of logged on (for exam	ipie, to download updates).
STY 2	user1	
	••••	

您的客户端实用程序现已准备好连接。

EAP-FAST(user2)

在我们的测试客户端中,我们使用的是运行14.3驱动程序版本的Intel 6300-N卡的Windows 7原生 Supplicant客户端。建议使用供应商提供的最新驱动程序进行测试。

要在WZC中创建配置文件,请完成以下步骤:

- 1. 转至控制面板 > 网络和Internet > 管理无线网络。
- 2. 单击Add选项卡。
- 3. 单击Manually create a network profile。





4. 添加在WLC上配置的详细信息。

注意:SSID区分大小写。

5. 单击 Next。

Network name:	goa	
Security type:	WPA2-Enterprise 👻	
Encryption type:	AES	
Security Key:	Hide characters	
Start this connec	ction automatically	
Connect even if	the network is not broadcasting	

6. 单击Change connection settings以仔细检查设置。

all Manually connect to a wireless natural	
Successfully added goa	
<ul> <li>Change connection settings</li> <li>Open the connection properties so that I can change the settings.</li> </ul>	
	Close

7. 确保已启用EAP-FAST。

注意:默认情况下,WZC没有EAP-FAST作为身份验证方法。您必须从第三方供应商下载该 实用程序。在本示例中,由于它是英特尔卡,因此系统中安装了英特尔PROSet。

goa Wireless Network Pr	operties	
Connection Security		
Security type: Encryption type:	WPA2-Enterprise   AES	
Choose a network aut Cisco: EAP-FAST Microsoft: Smart Card Microsoft: Protected B Cisco: LEAP Cisco: PEAP Cisco: PEAP Cisco: EAP-FAST Intel: EAP-SIM Intel: EAP-SIM Intel: EAP-AKA Advanced settings	hentication method: I or other certificate AP (PEAP) I n each	
<u>.</u>	ОК Са	ncel

goa Wireless Network Properties	23		
Connection			
Security type: WPA2-Enterprise   Encryption type: AES			
Choose a network authentication method: Cisco: EAP-FAST Settings Remember my credentials for this connection each time I'm logged on			
Advanced settings			
OK Car	ncel		

8. 启用Allow automatic PAC provisioning,并确保未选中Validate server certificate。

EAP-FAST Properties			
Connection User Credentials Authentication About	1		
<ul> <li>Use anonymous outer identity anonymous</li> <li>Use Protected Access Credentials (PAC)</li> <li>Allow automatic PAC provisioning</li> <li>PAC Authority:</li> <li>None</li> </ul>			
Validate server certificate Connect to only these servers: Trusted Root Certificate Authority			
<ul> <li>AAA Certificate Services</li> <li>AddTrust External CA Root</li> <li>Class 3 Public Primary Certification Authority</li> <li>Class 3 Public Primary Certification Authority</li> <li>DigiCert Assured ID Root CA</li> <li>DigiCert High Assurance EV Root CA</li> <li>DST Root CA X3</li> <li>To not prompt user to authorize new servers or trusted certification authorities.</li> </ul>			
OK Cancel Help			

9. 单击User Credentials选项卡,并输入user2的凭据。或者,您可以使用您的Windows凭据登录 。但是,在本例中,我们不打算使用它。

EAP-FAST Properties					
Connection	User Credentials	Authentication About			
<ul> <li>Use certificate on this computer</li> <li>Use one-time password</li> <li>Use Windows username and password</li> <li>Prompt automatically for username and password</li> </ul>					
Usern	name: us	ser2			
Passv	word:	••••			
Confi	rm password:	••••			
<b>₽</b>					
		OK Cancel Help			

10. Click OK.

EAP-FAST Properties	? ×
Connection User Credentials Authentication About	
Select authentication method:	
Any method 🔹	Configure
Enable Fast Reconnect	
Enable Posture validation	
OK Car	Help

您的客户端实用程序现已准备好连接user2。

注意:当用户2尝试进行身份验证时,RADIUS服务器将发送PAC。接受PAC以完成身份验证。



验证

使用本部分可确认配置能否正常运行。

<u>命令输出解释程序(仅限注册用户)(OIT) 支持某些 show 命令。</u>使用 OIT 可查看对 show 命令输 出的分析。

验证user1(PEAP-MSCHAPv2)

从WLC GUI中,转到Monitor > Clients,然后选择MAC地址。

#### Clients > Detail

#### **Client Properties**

MAC Address	00:24:d7:ae:f1:98	
IP Address	192,168,153,107	
Client Type	Regular	
User Nerve	user1	
Port Number	13	
Interface	vian253	
VLAN ID	253	
CCX Version	CCXv4	•
E2E Version	E2Ev1	
Mobility Role	Local	
Mobility Peer IP Address	N/A	
Policy Manager State	RLIN	
Management Frame Protection	No	
UpTime (Sec)	12	
Power Save Mode	OFF	
Current TxRateSet		
Data RateSet	6.0,9.0,12.0,18.0,24.0,3 0	6.0,48.0,54.

#### **AP** Properties

AP Address	2c:3f:38:c1:3c:f0
AP Name	3502e
AP Type	802.iian
WLAN Profile	goa
Status	Associated
Association ID	1
802.11 Authentication	Open System
Reason Code	1
Status Code	0
CF Pollable	Not Implemented
CF Pol Request	Not Implemented
Short Preamble	Not Implemented
PBCC	Not Implemented
Channel Agility	Nat Implemented
Re-authentication timeout	86365
Remaining Re-authentication timeout	0
WEP State	WEP Enable

#### Security Information

Security Policy Completed	Yes
Ройсу Туре	REN (WPA2)
Encryption Cipher	CCMP (AES)
EAP Type	PEAP
SNMP NAC State	Access
Redius NAC State	RUN

### WLC RADIUS统计信息:

#### <#root>

(Cisco Controller) >

show radius auth statistics

Authentication Servers:
Server Index 1
Server Address 192.168.150.24
Msg Round Trip Time 1 (msec)
First Requests 8
Retry Requests 0
Accept Responses 1
Reject Responses 0
Challenge Responses7
Malformed Msgs 0
Bad Authenticator Msgs0

Pending Requests	0
Timeout Requests	0
Unknowntype Msgs	0
Other Drops	0

ACS日志:

- 1. 要查看Hit计数,请完成以下步骤:
  - a. 如果在身份验证的15分钟内检查日志,请确保刷新命中计数。

) SI	ngle re	sult selec	ton 🏵 F	lule based result selection			
iervi	ce Sele	action Pol	icy				
Filter	: Stat.	.is _=	Match if:	Equals - Enabled	- Clear Filter	Go 🔻	
		Status	Name	Condition Protocol	5	Results Service	Hit Cour
1			Rule-1	match Radius		Default Network Access	1
2		0	Rule-2	match Tacaca		Default Davica Admin	0

b. 在同一页底部有一个点击计数选项卡。

etwork A	etwork Access Authorization Policy											
Filter: Status 🔹 Match if: Equals 💌 Enabled 💌 Clear Filter Go 🛩												
Name	NDG:Location	NDG:Device Type	Conditi Protocol	ons Identity Group	Eap Authentication Method	Results Authorization Profiles	HitCou					
Rule-1	in All Locations LAB	in All Device Types:5508	match Radius	in All Groups:Wireless Users	-ANY-	Permit Access	1					

2. 单击Monitoring and Reports,此时会显示New弹出窗口。转至Authentications -Radius - Today。您也可以单击Details以验证应用了哪个服务选择规则。

199							Launch Inter	nactive Veneer
Showing Page 1 of 1		6	Colo Page: Ge					
AAA Protocol > RADIUS Authentication								
Authentication Status : Pass or Fail Date : Jonuary 29, 2012 05:40 PM - J	January 29, 2012 06:10 PM (1	.oot 30 Minutes (Lost Hour	I Loot 12 Hours   Tedar   Yes	tendlay i Last 7 Do	e (Lost 30 Dava )			
Generated on January 29, 2012 6:10:42 PM EST								
Reited -Fast R-Fall R-Click for details R-Mour	a over item for additional info	mater						
Logged At RADUS NAS Details I	Usemane MAC1P Address	Access Service	Authentication Method	Natwork Device	NAS IP Address	NAS Port ID	CTS Security Group	ACS Instance
Jan 29, 12 6:07:37.943 PM 🕜 🧠	uper1 00-24-d7-ap-f1-56	Default Notesrk Access	PEAP (EAP-MSCHAP/2)	WLC-5508	192.168.75.44			SALIL-ACS52

## 验证user2(EAP-FAST)

## 从WLC GUI中,转到Monitor > Clients,然后选择MAC地址。

Clients > Detail

Client Properties			AP Properties	
MAC Address	00:24:d7:setf1:98		AP Address	2cr3fr38rc1r3crf0
1P Address	192.168.153.111		AP Name	3502e
Client Type	Regular		AP Type	002.11an
User Name	user2		WLAN Profile	goa
Port Number	13		Status	Associated
Interface	vlan253		Association 1D	1
VLAN ID	253		802.11 Authentication	Open System
CCX Version	CCXV4		Reason Code	1
E2E Version	E2Ev1		Status Code	0
Mobility Role	Local		CF Pollable	Not Implemented
Mobility Peer IP Address	N/A		CF Poll Request	Not Implemented
Policy Manager State	RUN		Short Preamble	Not Implemented
Management Frame Protection	No		PBCC	Not Implemented
UpTime (Sec)	29		Chennel Agility	Not Implemented
Power Save Mode	OFF		Re-authentication timeout	86392
Current TxRateSet	m15 6.0.9.0.12.0.18.0.24	0 36.0.48.0.54	Remaining Re-authentication timeout	0
Data ReteSet	0		WEP State	WEP Enable

#### Security Information

Security Policy Completed	Yes
Policy Type	RSN (WPA2)
Encryption Cipher	CCMP (AES)
ЕАР Туре	EAP-FAST
SNMP NAC State	Access
Radius NAC State	RUN

ACS日志:

1. 要查看Hit计数,请完成以下步骤:

a. 如果在身份验证后15分钟内检查日志,请确保刷新HIT计数。

Servio	ce Sel	ection Pol	нсу					
Filter:	Stat	US <u>-</u>	Match It	Equals -	Enabled -	Clear Filter	Go 🗢	
	E	Status	Name	Protocol	Conditions		Results Service	Hit Cou
1		0	Rule-1	match Radius			Default Network Access	3
2		۲	Rule-2	match Tacaca			Default Device Admin	0

b. 在同一页底部有一个点击计数选项卡。

lietwork A	Access Authorization F	Policy					
Filter: St	atus	<ul> <li>Match if: Equals</li> </ul>	<ul> <li>Enabled</li> </ul>	🔹 Clear Filler 🛛 😨			
Name	NDG:Location	NDG:Device Type	Conditi Protocol	ions Identity Group	Eap Authentication Method	Results Authorization Profiles	Hit Cou
Rule-1	in All Locations:LAB	in All Device Types:5508	match Radius	in All Groups: Wireless Users	-ANY-	Permit Access	2

2. 单击Monitoring and Reports,此时会显示New弹出窗口。转至Authentications -Radius - Today。您也可以单击Details以验证应用了哪个服务选择规则。

23	4 🖻							222222222222	2222222222222222222			La	unch Interactive	Vewer
	Showing P	ege 1	of 1		1000	real Press	Next Last	I Get	to Page: Ge					
AAA Pr	otocol > R	ADIUS	Authen	ticatio	n									
Authenti Data :	ication Statu	s : Pas Jan	os or Fail umary 29, 2	012 05:	STPM -	January 29, 3	2012 06:23 PM (La	st 30 Nitrutes   Last Hour   L	ast 12 Hours   Today   Yesterday	Last7 Days (Las	20 Days )			
Generat	ed on Janua	y 29, 2	912 6 23	17 PM E	ST									
Perios	d N-fail	A-0	Sich for de	tala	Q -Head	aa over itere	for additional inform	nation						
	Logged At		RACIUS Status	NAS Failure	Details	Usemane	MAC/IP Address	Access Service	Authentication Method	Natwork Device	NAS IP Address	NAS Port ID	CTS Security Group	ACS INS
Jan 29,	126.19.27.3	70 PM	*		94	user2	10.24 d7-ap-P1-98	Default Network Access	EAP-FAST (EAP-MSCHWP42)	WLC-5508	192.168.75.44			SALL-A
Jan 29.	12 6 07 37 5	43 PM	*		4	user1	00-24-d7-ae-f1-98	Default Network Access	PEAP (EAP-MSCHAPV2)	WLC-5508	192 168 75.44			SALL-A

## 故障排除

本部分提供的信息可用于对配置进行故障排除。

### 故障排除命令

<u>命令输出解释程序(仅限注册用户)(OIT) 支持某些 show 命令。</u>使用 OIT 可查看对 show 命令输 出的分析。

注意:使用<u>debug命令之前,请参</u>阅有关Debug命令的重要信息。

1. 如果遇到任何问题,请在WLC上发出以下命令:

- debug client <mac add of the client>
- debug aaa all enable
- show client detail <mac addr> 验证策略管理器状态。
- show radius auth statistics 验证故障原因。
- debug disable-all 关闭调试。
- · clear stats radius auth all Clear radius statistics on the WLC。

2. 验证ACS中的日志并记录故障原因。

## 相关信息

• <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)。