统一无线网络先的PEAP与Microsoft互联网认证服 务(IAS)

目录

简介 先决条件 要求 使用的组件 规则 PEAP 概述 配置 网络图 配置 配置 Microsoft Windows 2003 Server 配置 Microsoft Windows 2003 Server 在 Microsoft Windows 2003 Server 上安装和配置 DHCP 服务 安装并配置Microsoft Windows 2003 Server作为证书颁发机构(CA)服务器 将客户端连接到域 在 Microsoft Windows 2003 Server 上安装 Internet 身份验证服务并请求证书 为 PEAP-MS-CHAP v2 身份验证配置 Internet 身份验证服务 将用户添加到 Active Directory 允许用户进行无线访问 配置无线局域网控制器和轻量 AP 通过 MS IAS RADIUS 服务器为 RADIUS 身份验证配置 WLC 为客户端配置 WLAN 配置无线客户端 为 PEAP-MS CHAPv2 身份验证配置无线客户端 验证与故障排除 相关信息

<u>简介</u>

本文档提供了一个配置示例,在使用 Microsoft Internet 身份验证服务 (IAS) 作为 RADIUS 服务器的 Cisco 统一无线网络中设置受保护的可扩展的身份验证协议 (PEAP) 与 Microsoft 质询握手身份验证 协议 (MS-CHAP) 版本 2 身份验证。

<u>先决条件</u>



假设读者已经掌握基本的 Windows 2003 安装和 Cisco 控制器安装,因为本文档仅涵盖有助于开展 测试的特定配置。

注意:本文档旨在为读者提供有关MS服务器上进行PEAP - MS CHAP身份验证所需的配置的示例 。本部分所示的 Microsoft 服务器配置在实验室中进行了测试,确认能按照预期工作。如果在配置 Microsoft 服务器时遇到问题,请联系 Microsoft 以获取帮助。Cisco TAC 不支持 Microsoft Windows 服务器配置。

有关Cisco 4400系列控制器的初始安装和配置信息,请参阅<u>快速入门指南:Cisco 4400系列无线</u> LAN控制器。

有关 Microsoft Windows 2003 安装和配置指南,请访问安装 Windows Server 2003 R2。

开始之前,请在测试实验室中的每台服务器上安装 Microsoft Windows Server 2003 SP1 操作系统 并更新所有 Service Pack。安装控制器和轻量接入点 (LAP) 并确保配置了最新的软件更新。

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 4.0 版的 Cisco 4400 系列控制器
- Cisco 1131 轻量接入点协议 (LWAPP) AP
- 安装了Internet身份验证服务(IAS)、证书颁发机构(CA)、DHCP和域名系统(DNS)服务的 Windows 2003企业服务器(SP1)
- 带有SP 2的Windows XP Professional(以及更新的Service Pack)和Cisco Aironet 802.11a/b/g无线网络接口卡(NIC)
- Aironet Desktop Utility 4.0 版
- Cisco 3560 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。

<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>PEAP 概述</u>

PEAP使用传输级安全(TLS)在身份验证PEAP客户端(例如无线笔记本电脑)和PEAP身份验证器 (例如Microsoft Internet身份验证服务(IAS)或任何RADIUS服务器之间创建加密通道。PEAP 不指定 身份验证方法,但为可通过由 PEAP 提供的 TLS 加密通道进行操作的其他 EAP 身份验证协议(例 如 EAP-MSCHAPv2)提供附加的安全性。PEAP 身份验证过程主要包括两个阶段:

PEAP阶段1:TLS加密通道

无线客户端将与 AP 相关联。在客户端与接入点 (LAP) 之间创建安全关联之前,基于 IEEE 802.11 的关联会提供开放式系统或共享密钥身份验证。在客户端与接入点之间成功建立基于 IEEE 802.11 的关联之后,TLS 会话就会与 AP 进行协商。在无线客户端与 IAS 服务器之间的身份验证成功完成 之后,TLS 会话就会在它们之间进行协商。在此协商中派生的密钥将用来加密随后的所有通信。

PEAP阶段2:EAP身份验证通信

EAP 通信(包括 EAP 协商)发生在由 PEAP 在 PEAP 认证过程的第一阶段中创建的 TLS 通道内 。IAS 服务器使用 EAP-MS-CHAP v2 对无线客户端进行身份验证。LAP 和控制器仅在无线客户端 与 RADIUS 服务器之间转发消息。WLC 和 LAP 无法解密这些消息,因为它不是 TLS 终点。

在发生 PEAP 第一阶段并且在 IAS 服务器与 802.1X 无线客户端之间创建了 TLS 通道之后,为了在 用户获得 PEAP-MS-CHAP v2 提供的基于密码的有效凭证时成功完成身份认证,RADIUS 消息顺序 如下:

- 1. IAS服务器向客户端发送身份请求消息: EAP-Request/Identity。
- 2. 客户端使用身份响应消息进行响应: EAP-Response/Identity。
- 3. IAS服务器发送MS-CHAP v2询问消息:EAP-Request/EAP-Type=EAP MS-CHAP-V2(询问)。
- 4. 客户端使用MS-CHAP v2质询和响应进行响应:EAP-Response/EAP-Type=EAP-MS-CHAP-V2(响应)。
- 5. 当服务器成功对客户端进行身份验证时,IAS服务器会发回MS-CHAP v2成功数据包:EAP-Request/EAP-Type=EAP-MS-CHAP-V2(成功)。
- 6. 当客户端成功对服务器进行身份验证时,客户端将使用MS-CHAP v2成功数据包进行响应 :EAP-Response/EAP-Type=EAP-MS-CHAP-V2(成功)。
- 7. IAS 服务器发送一个指示身份验证成功的 EAP-TLV。
- 8. 客户端回复一个 EAP-TLV 状态成功消息。
- 服务器完成身份验证并使用明文发送 EAP 成功消息。如果部署了 VLAN 用于客户端隔离,则 此消息中还包含 VLAN 属性。

配置

本文档提供一个 PEAP MS-CHAP v2 配置示例。

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:



在此设置中, Microsoft Windows 2003 Server 担当以下角色:

- Wireless.com 域的域控制器
- DHCP/DNS 服务器
- 证书颁发机构(CA)服务器
- Active Directory 用于维护用户数据库
- •互联网身份验证服务(IAS) 对无线用户进行身份验证

此服务器通过第2层交换机连接到有线网络(如图所示)。

无线LAN控制器(WLC)和注册的LAP也通过第2层交换机连接到网络。

无线客户端 C1 和 C2 将使用 Wi-Fi 保护访问 2 (WPA2) - PEAP MSCHAP v2 身份验证来连接到无 线网络。

目标是配置 Microsoft 2003 Server、无线局域网控制器和轻量 AP,以便通过 PEAP MSCHAP v2 身份验证对无线客户端进行身份验证。

下一部分解释如何为此设置配置设备。

<u>配置</u>

本部分介绍在此 WLAN 中设置 PEAP MS-CHAP v2 身份验证时所需的配置:

- 配置 Microsoft Windows 2003 Server
- 配置无线局域网控制器(WLC)和轻量AP
- 配置无线客户端

首先配置 Microsoft Windows 2003 Server。

配置 Microsoft Windows 2003 Server

配置 Microsoft Windows 2003 Server

按照"网络设置"部分所述,请在网络中使用 Microsoft Windows 2003 Server 来执行以下功能。

- 域控制器 用于 Wireless 域
- DHCP/DNS 服务器
- •证书颁发机构(CA)服务器
- Internet身份验证服务(IAS)-用于对无线用户进行身份验证
- Active Directory 用于维护用户数据库

为这些服务配置 Microsoft Windows 2003 Server。首先将 Microsoft Windows 2003 Server 配置为 域控制器。

将 Microsoft Windows 2003 Server 配置为域控制器

要将 Microsoft Windows 2003 Server 配置为域控制器,请完成以下步骤:

1. 单击**开始**,单击"运行",键入 dcpromo.exe,然后单击"确定"以启动 Active Directory 安装向导



2. 单击下一步运行 Active Directory 安装向导。

P	Perating System Compatibility Improved security settings in Windows Server 2003 affect older versions of Windows.
	Domain controllers running Windows Server 2003 implement security settings that require clients and other servers to communicate with those domain controllers in a more secure way.
	Some older versions of Windows, including Windows 95 and Windows NT 4.0 SP3 or earlier, do not meet these requirements. Similarly, some non-Windows systems, including Apple Mac OS X and SAMBA clients, might not meet these requirements.
	For more information, see <u>Compatibility Help</u> .
	< Back Next > Cancel

3. 要创建新域,请选择新域的**域控制器选项。**

Specify	ontroller Type the role you want this server to have.
Do you addition	want this server to become a domain controller for a new domain or an al domain controller for an existing domain?
• Dor	nain controller for a new domain
Sele This	ect this option to create a new child domain, new domain tree, or new forest. s server will become the first domain controller in the new domain.
C Add	litional domain controller for an existing domain
⚠	Proceeding with this option will delete all local accounts on this server.
	All cryptographic keys will be deleted and should be exported before continuing.
	All encrypted data, such as EFS-encrypted files or e-mail, should be decrypted before continuing or it will be permanently inaccessible.

4. 单击下一步创建一个新的域树森林。

Active Directory Installation Wizard
Create New Domain Select which type of domain to create.
Create a new:
Domain in a new forest
Select this option if this is the first domain in your organization or if you want the new domain to be completely independent of your current forest.
Child domain in an existing domain tree
If you want the new domain to be a child of an existing domain, select this option. For example, you could create a new domain named headquarters.example.microsoft.com as a child domain of the domain example.microsoft.com.
O Domain tree in an existing forest
If you don't want the new domain to be a child of an existing domain, select this option. This will create a new domain tree that is separate from any existing trees.
< <u>B</u> ack <u>N</u> ext > Cancel

5. 如果系统上没有安装 DNS,此向导将为您提供选项用于配置 DNS。选择**否,在本计算机上安 装和配置 DNS。**单击 Next。

ctive Directory Installation Wizard	×
Install or Configure DNS You can configure or install Domain Naming Service (DNS) on this computer.	\$
Domain Naming Service (DNS) is not configured on this computer. Is DNS already running on this network?	
○ Yes, I will configure the DNS client	
No, just install and configure DNS on this computer	
< Back Next > 0	Cancel

6. 为新域键入完整的 DNS 名称。本示例中使用 Wireless.com,然后单击"下一步"。

ve Directory Installation	Wizard
New Domain Name Specify a name for the ne	ew domain.
Type the full DNS name fi (for example: headquarte	ior the new domain ers.example.microsoft.com).
Eull DNS name for new d	lomain:
Wireless.com	
•	

7. 为域输入 NETBIOS 名称,然后单击**下一步**。本示例使用 **WIRELESS**。

ctive Directory Installation Wi	zard
NetBIOS Domain Name Specify a NetBIOS name for	the new domain.
This is the name that users o domain. Click Next to accept	f earlier versions of Windows will use to identify the new t the name shown, or type a new name.
Domain NetBIOS name:	WIRELESS
	< <u>Back</u> <u>N</u> ext> Cancel

8. 为域选择数据库和日志位置。单击 Next。

ectory database and log	files.
re the database and the	log on separate
ctory database?	
	Browse
story log?	
	Br <u>o</u> wse
	Br <u>o</u> wse
	Br <u>o</u> wse
	ectory database and log re the database and the story database?

9. 选择 Sysvol 文件夹的位置。单击 Next。

ctive Directory Installation Wizard		
Shared System Volume Specify the folder to be shared as the syst	em volume.	<i>₩</i>
The SYSVOL folder stores the server's co of the SYSVOL folder are replicated to all	by of the domain's public file domain controllers in the do	es. The contents main.
The SYSVOL folder must be located on a	n NTFS volume.	
Enter a location for the SYSVOL folder.		
Eolder location:		
C:\WINDOWS\SYSVOL		B <u>r</u> owse
	< <u>Back</u> <u>N</u> ex	t> Cancel

10. 选择用户和组的默认权限。单击 Next。

Pe	rmissions				
	Select default permissions for	r user and grou	ip objects.		
	Some server programs, such stored on domain controllers.	as Windows N	IT Remote Acces	ss Service, read i	information
Permissions compatible with pre-Windows 2000 server operating systems					
Select this option if you run server programs on pre-Windows 2000 server op systems or on Windows 2000 or Windows Server 2003 operating systems tha members of pre-Windows 2000 domains.			operating that are		
	🕐 \Lambda Anonymous users c	an read inform	ation on this dom	ain.	
	 Permissions compatible o operating systems 	nly with Windo	ws 2000 or Wind	lows Server 2003	3
	Select this option if you ru Server 2003 operating sy authenticated users can i	un server progr istems that are read informatio	ams only on Wind members of Activ n on this domain.	dows 2000 or Wi /e Directory dom/	indows ains. Only
			Z Back	Nevts	Ca
				Howy	
ξŦ		۶			
e	Directory Installation Wi	zard			
ir	ectory Services Restore I This password is used when Mode.	Mode Admin you start the c	istrator Passw omputer in Direct	ord ory Services Res	store
	Type and confirm the passwo when this server is started in	ord you want to Directory Serv) assign to the Ad ices Restore Mod	lministrator accou Je.	unt used
	The restore mode Administrat account. The passwords for both.	tor account is o the accounts r	different from the night be different,	domain Administr . so be sure to rer	ator member
	Restore Mode Password:	•••••	•		
	Confirm password:	•••••	•		
	For more information about D	irectory Servic	es Restore Mode	, see <u>Active Dire</u>	ctory Hel

12. 单击下一步接受以前设置的域选项。

6 ur	nmary Review and confirm the options you selected.
	You chose to:
	Configure this server as the first domain controller in a new forest of domain trees.
	The new domain name is Wireless.com. This is also the name of the new forest.
	The NetBIOS name of the domain is WIRELESS
	Database folder: C:\WINDOWS\NTDS Log file folder: C:\WINDOWS\NTDS SYSVOL folder: C:\WINDOWS\SYSVOL
	The password of the new domain administrator will be the same as the password of the administrator of this computer.
	To change an option, click Back. To begin the operation, click Next.

13. 单击完成关闭 Active Directory 安装向导。



Windows must be restarted before Directory Installation wizard take	e the changes made by the Active effect.

通过这些步骤,您已经将 Microsoft Windows 2003 Server 配置为域控制器,并且创建了新域 Wireless.com。下一步是在服务器上配置 DHCP 服务。

在 Microsoft Windows 2003 Server 上安装和配置 DHCP 服务

Microsoft 2003 Server 上的 DHCP 服务用于向无线客户端提供 IP 地址。要在此服务器上安装和配置 DHCP 服务,请完成以下步骤:

- 1. 在"控制面板"中单击添加或删除程序。
- 2. 单击添加/删除 Windows 组件。
- 3. 选择**网络服务,然后单击"详细信息"。**
- 4. 选择Dynamic Host Configuration Protocol(DHCP),然后单击OK。

ubcomponents of Networking Services:	
Z P Domain Name System (DNS)	1.7 MB
Dynamic Host Configuration Protocol (DHCP)	0.0 MB
🗌 畏 Internet Authentication Service	0.0 MB
🗆 🚚 Remote Access Quarantine Service	0.1 MB
🗌 🗐 RPC over HTTP Proxy	0.0 MB
🗆 🚚 Simple TCP/IP Services	0.0 MB 🚽
🗆 🚚 Windows Internet Name Service (WINS)	0.9 MB 🗾
Description: Sets up a DHCP server that automatically a addresses to client computers on the same	ssigns temporary IP network.
Fotal disk space required: 3.4 MB	Details
	2

5. 单击下一步安装 DHCP 服务。

ws Components Wizard	
indows Components You can add or remove components of Windows.	
To add or remove a component, click the checkbox. A sh part of the component will be installed. To see what's inclu Details.	naded box means that only uded in a component, click
Components:	
🔲 🖂 🥶 Internet Explorer Enhanced Security Configuration	0.0 MB 🔺
🗔 🚉 Management and Monitoring Tools	6.3 MB
🗹 🚔 Networking Services	2.7 MB 💻
🔲 🚉 Other Network File and Print Services	0.0 MB
🗖 📾 Bemote Storage	4.2 MB 🗾
Description: Contains a variety of specialized, network-rel	lated services and protocols.
Total disk space required: 3.4 MB	Dataite
Space available on disk: 7212.1 MB	
< <u>B</u> ack <u>N</u> ext>	Cancel He

6. 单击完成完成安装。



- 7. 要配置 DHCP 服务,请单击**开始 > 程序 > 管理工具**,然后单击 DHCP 管理单元。
- 8. 选择 DHCP 服务器 tsweb-lapt.wireless.com(在本示例中)。
- 9. 单击操作,然后单击"授权"授权 DHCP 服务。



- 10. 在控制台树中,右键单击 **tsweb-lapt.wireless.com,然后单击"新建范围"为无线客户端定义** IP 地址范围。
- 11. 在"新建范围"向导的"欢迎使用新建范围向导"页上,单击**下一步**。



12. 在"范围名称"页上,键入 DHCP 范围的名称。本示例中使用 **DHCP-Clients 作为范围名称。** 单击 **Next**。

Scope Name	regide en identificier er en en Verender herre Mer er Kenner 💦
providing a de	scription.
Type a name a how the scope	and description for this scope. This information helps you quickly identify is is to be used on your network.
N <u>a</u> me:	DHCP-Clients
Description:	DHCP Server for Wireless Clients
	< <u>B</u> ack <u>N</u> ext > Canc
• 地址范围"页上	<u>〈Back Next〉</u> Canc ,输入范围的开始和结束 IP 地址,然后单击下 一步 。

Enter the range of ac	dresses	that th	ne soc	ope dis	stributes.			
<u>S</u> tart IP address:	10 .	77.	244 .	. 218	1			
End IP address:	10.	77.	244 .	. 219	1			
A subnet mask define IDs and how many bi length or as an IP ad	es how m its to use Idress.	nany b for th	aits of ie hos	an IP t ID, Y	address to u 'ou can spec	se for th tify the s	e netwo ubnet m	rk/subnet ask by
A subnet mask define IDs and how many bi length or as an IP ad Length:	es how rr its to use Idress. 8	nany b for th	oits of ie hos	an IP : t ID, Y	address to u 'ou can spec	se for th ify the s	e netwo ubnet m	rk/subnet ask by
A subnet mask define IDs and how many bi length or as an IP ad Length: Subnet mask:	es how rr its to use Idress. 8 255 .	nany b for th	pits of lie hos	an IP t ID. Y	address to u 'ou can spec	se for th cify the s	e netwo ubnet m	rk/subnet ask by

14. 在"添加排除项"页上,指出您希望保留/从 DHCP 范围中排除的 IP 地址。单击 Next。

Add Exclusions Exclusions are addres server.	sses or a range of addresses that are not distributed by the
Type the IP address r	ange that you want to exclude. If you want to exclude a single
Start IP address:	End IP address:
	Add
Excluded address ran	ge:
	Remo⊻e
1	
	< <u>Back</u> <u>Next</u> Lance

15. 在"租期"页上,指定租期,然后单击**下一步**。

The lease d	uration specifi	es how long a	client can use an	IP address from this	Z
Lease durat connected t portable cor Likewise, fo locations, lo	ons should typ o the same ph puters or dial- r a stable netw nger lease dur	pically be equal ysical network. up clients, sho ork that consis ations are more	to the average ti For mobile netwo rter lease duration its mainly of deskt appropriate.	me the computer is orks that consist mair is can be useful. op computers at fixe	nly of d
Set the dura	tion for scope	leases when d	istributed by this s	erver.	
Limited to:					
Days:	H <u>o</u> urs: <u>M</u> 0 + 0	inutes:			

16. 在"配置 DHCP 选项"页上,选择**是,我要立即配置 DHCP 选项**,然后单击"下一步"。

Configure DHCP Options You have to configure the most co scope.	ommon DHCP options before clients can use the
When clients obtain an address, th addresses of routers (default gatev scope.	ney are given DHCP options such as the IP vays), DNS servers, and WINS settings for that
The settings you select here are fo Server Options folder for this serve	or this scope and override settings configured in the r.
Do you want to configure the DHC	P options for this scope now?
Yes, I want to configure these	options now
O No, I will configure these option	ns later

17. 如果有默认的网关路由器,请在"路由器(默认网关)"页上指定网关路由器的 IP 地址,然后 单击**下一步**。

IP address:	Tor a roater used by clients, enter the dubless b	CIUYY.
	Add	
10.77.244.220	<u>H</u> emove	
	Шр	
	D <u>o</u> wn	

18. 在"域名和 DNS 服务器"页上,键入以前配置的域名。本示例中使用 Wireless.com。输入服务器的 IP 地址。单击 Add。

The Domain Name System (DNS) ma clients on your network.	ps and translates domain names	used by
You can specify the parent domain you wa DNS name resolution.	ant the client computers on your	network to use for
Parent do <u>m</u> ain: Wireless.com		
servers. <u>S</u> erver name:	I <u>P</u> address:	A <u>d</u> d
Besolve	10.77.244.217	<u>R</u> emove
11200140		
11230140		<u>Ш</u> р

19. 单击 **Next**。

20. 在"WINS 服务器"页上,单击**下一步**。

21. 在"激活范围"页上,选择**是,我要立即激活范围**,然后单击"下一步"。

New Scope Wizard			
Activate Scope Clients can obtain address leases only if a so	cope is activated	ł.	(D)
Do you want to activate this scope now?			
Yes, I want to activate this scope now			
O No, I will activate this scope later			
	< Back	Next >	Cancel
			1
在"完成新建范围"向导页上,单击 完成 。			
New Scope Wizard			



To close this wizard, click Finish.

< Back

Finish

Cancel

23. 在"DHCP 管理单元"窗口中,验证所创建的 DHCP 范围已处于活动状态。

🛄 DenCP				
Elle Action View Help				Os
+ → 🛍 🗷 × 🗗 8 8 🕸 🗐 🖵 9	P			
Фоно	teach-laptaineleos.com [10.77.244.217]			
E- C [Sweb-lapt, wireless, con [10,77,244,217]	Cariteria al DHCP Server	2.8.6	Description	
B Server Optione	Scape [172.16.0.0] DHCP-Clients	** Active **	DHCP Server for Wireless Clients	
	Server Options			
	1			
	1			
	1			
	1			
	1			
	1			
	1			
	I			
- 11 1	10			
😰 Start 🖉]l∰teeta			🔲 🗧 🛢 🖉 🕅 🖏 Vi

在服务器上启用DHCP/DNS后,请将该服务器配置为企业证书颁发机构(CA)服务器。

安装并配置Microsoft Windows 2003 Server作为证书颁发机构(CA)服务器

具有 EAP-MS-CHAPv2 的 PEAP 可根据服务器上现有的证书来验证 RADIUS 服务器。此外,服务器证书必须由受客户端计算机信任的公共证书颁发机构(CA)颁发(即,公共CA证书已经存在于客户端计算机证书存储库的受信任的根证书颁发机构文件夹中)。在本示例中,将Microsoft Windows 2003服务器配置为向Internet身份验证服务(IAS)颁发证书的证书颁发机构(CA)。

要在此服务器上安装和配置证书服务,请完成以下步骤:

- 1. 在"控制面板"中单击添加或删除程序。
- 2. 单击添加/删除 Windows 组件。
- 3. 单击**证书服务**。

Vindows Components You can add or remove components of Windows.	
To add or remove a component, click the checkbox. A sharpart of the component will be installed. To see what's includ Details.	ded box means that only led in a component, click
Components:	
💌 📻 Accessories and Utilities	4.9 MB 🔺
Application Server	34.4 MB 💻
🗹 🙀 Certificate Services	1.8 MB
🔲 🛄 E-mail Services	1.1 MB
Eax Services	7.9 MB 工
Description: Installs a certification authority (CA) to issue cer public key security programs.	rtificates for use with
Total disk space required: 13.8 MB	Details
Space available on disk: 7310.6 MB	
< <u>B</u> ack <u>N</u> ext >	Cancel He
示警告消息"安装证书服务后,就不能重命名此计算机,也	回不能将其加入域或从域

1	After installing Certificate Services, the machine name and domain membership may not be changed due to the binding of the machine name to CA information stored in the Active Directory. Changing the machine name or domain membership would invalidate the certificates issued from the CA. Please ensure the proper machine name and domain membership are configured before installing Certificate Services. Do you want to continue?
	<u>Y</u> es <u>N</u> o
5. 在"证	书颁发机构类型"下,选择 企业根 CA ,然后单击"下一步"。

do	ws Components Wizard
CA	Type Select the type of CA you want to set up.
	Enterprise root CA
	C Enterprise subordinate CA
	C Stand-alone root CA
	C Stand-alone subordinate CA
	Description of CA type The most trusted CA in an enterprise. Should be installed before any other CA.
	Use custom settings to generate the key pair and CA certificate
	< Back Next > Cancel Help

6. 输入用于标识 CA 的名称。本示例使用 Wireless-CA。单击 Next。

Common name for this CA:	
Wireless-CA	
Distinguished name suffix:	
DC=Wireless,DC=com	
Preview of distinguished na	ame:
CN=Wireless-CA,DC=Wire	less,DC=com
∐	Expiration date:

7. 这就为证书数据库存储创建了一个"证书日志"目录。单击 Next。

indows (omponents Wizard					
Certifi En infe	cate Database Setti er locations for the cert prmation.	ings tificate database	e, database log	, and configura	ation	Ř
<u>C</u> e	tificate database:					
C	WINDOWS\system32	\CertLog			Browse	
Ce	tificate <u>d</u> atabase log:					
C:	WINDOWS\system32	\CertLog			Browse	
I.	Store configuration info Shared folder:	ormation in a sha	ared folder		Browse	
	<u>Store configuration info</u> S <u>hared folder:</u> Preserve <u>existing certif</u>	ormation in a sha icate database	ared folder		Bīowse	

Microsoft	
	To complete the installation, Certificate Services must temporarily stop the Internet Information Services. Do you want to stop the service now?
	<u>Y</u> es <u>N</u> o

9. 单击Finish完成证书颁发机构(CA)服务的安装。



下一步是在 Microsoft Windows 2003 Server 上安装和配置 Internet 身份验证服务。

<u>将客户端连接到域</u>

下一步是将客户端连接到有线网络,并从新域下载域特有的信息。也就是说,将客户端连接到域。 为此,请完成以下步骤:

- 1. 使用直通以太网电缆将客户端连接到有线网络。
- 2. 启动客户端,并用客户端的用户名/密码进行登录。
- 3. 单击开始;单击运行;键入cmd;然后单击确定。
- 4. 在命令提示符下,键入 ipconfig,然后按 Enter 键,以便验证 DHCP 能够正常使用,并且客户 端从 DHCP 服务器收到了 IP 地址。
- 5. 要将客户端加入域中,请右键单击我的电脑,然后选择"属性"。
- 6. 单击 Computer Name 选项卡。
- 7. 单击 Change。
- 8. 单击Domain;键入wireless.com;然后单击OK。

ou compu	an change the name and the membership of this ter. Changes may affect access to network resources.
ompu	iter name:
lient	1
ull co lient1 Men	mputer name: More ber of Domain:
Ŭ	Wireless
0	Workgroup:
	WORKGROUP
	WURKGRUUP

键入用户名 Administrator 以及	客户端所加入的域特有	前的密码。 (这是服务器上的	Active
	Computer Name C	hanges	? 🗙
	Enter the name and p to join the domain.	assword of an account with per	mission
	<u>U</u> ser name:	🕵 administrator	×
	Password:	•••••	
		ОК Са	ancel
Directory 中的管理员帐户。)			



- 10. Click OK.
- 11. 单击是重新启动计算机。
- 12. 计算机重新启动后,使用以下信息登录:用户名= Administrator;密码= <domain password>;域= Wireless。
- 13. 右键单击**我的电脑**,然后单击"属性"。
- 14. 单击计算机名称选项卡,以便验证您是在 Wireless.com 域中。

System Proper	ties			? 🛛		
System Re	store	Automa	Remote			
General	Com	puter Name	Hardware	Advanced		
Wind on th	your computer					
Computer <u>d</u> esc	ription:					
		For example: "I Computer".	Kitchen Computer'' (or ''Mary's		
Full computer n	iame:	Client1.Wireless.com				
Domain:		Wireless.com				
To use the Net domain and cre ID. To rename this	work Iden ate a loca computer	tification Wizard al user account, i or join a domain	to join a click Network , click Change.	Network ID		
🔥 Changes	will take e	effect after you re	estart this computer.	Apply		

15. 下一步是验证客户端从服务器收到了 CA 证书(信任)。

- 16. 单击Start;单击Run;键入mmc,然后单击OK。
- 17. 单击**文件**,然后单击"添加/删除"管理单元。

Add/Remov	e Snap	in					? ×
Standalone	Extensi	ons					
Use this pa	ge to ado	d or remove	e a standalo	ine Snap-i	n from the co	onsole.	
Snap-ins a	ided to:	🔁 Cons	ole Root			~	
							00000
Description	m						
Add		Remove	Ab	iout)			
					OK	Ca	ncel

18. 单击 **Add**。

19. 选择**证书**,然后单击"添加"。

Add Standalone Snap-in

Snap-in	Vendor	1
🗽 .NET Framework 1.1 Configuration	Microsoft Corporation	
🚔 ActiveX Control	Microsoft Corporation	1000
🗿 Certificates	Microsoft Corporation	
Component Services	Microsoft Corporation	
🛃 Computer Management	Microsoft Corporation	
🛃 Device Manager	Microsoft Corporation	
💕 Disk Defragmenter	Microsoft Corp, Executi	
🖥 Disk Management	Microsoft and VERITAS	
🔄 Event Viewer	Microsoft Corporation	
Folder	Microsoft Corporation	1
Description he Certificates snap-in allows you to bro ertificate stores for yourself, a service, o	wse the contents of the r a computer.	

?

20. 选择**计算机帐户**,然后单击"下一步"。

Certificates snap-in	
This snap-in will always manage certificates for:	
O My user account	
O Service account	
 Computer account 	
	< Back Next > Cancel

21. 单击完成接受默认的本地计算机。

Select Computer		×
Select the computer you war This snap-in will always ma O Local computer: (the c	nt this snap-in to manage. nage: computer this console is running on)	
Allow the selected cor only applies if you sav	nputer to be changed when launching from the command line. This e the console.	
	< Back Finish Cancel	

22. 单击**关闭**,然后单击"确定"。

23. 展开Certificates(Local Computer);展开Trusted Root Certification Authorities;然后单击

Certificates。在列表中查找 Wireless。

		our certification nation messee	mineeneeg			
File Action View Favorites Win	dow Help					-140
	3 🕼	I	1	1		10.
Console Root	Issued To /	Disued by	Expendion Date	Intended Purposes	Priendly Name	Stati
E Bersonal	ISSUES OF A CONTRACTOR OF A CO	SERVICIOS DE CERTIFICACION - A	3/10/2009	Secure Email, Server	SERVICIOS DE CERT	
E-M Tusted Boot Certification Author	221StA Secure Client CA	SIA Secure Client CA	7/9/2019	Secure Enal, Server	Societa Interbancari	
Certificates	ChilSIA Secure Server CA	SIA Secure Server CA	7/9/2019	Secure Email, Server	Societa Interbancari	
E Enterprise Trust	224 Swisskey Root CA	Swisskey Root CA	1/1/2016	Secure Enal, Server	Selisskey Root CA	
E intermediate Certification Author	CallSymantec Root CA	Symantec Root CA	5/1/2011	<ab< td=""><td><none></none></td><td></td></ab<>	<none></none>	
E - In Trusted Publishers	TC TrustCenter Class I CA	TC TrustCenter Class 1 CA	1/1/2011	Secure Email, Server	TC TrustCenter Clas	
E - O Untrusted Certificates	TC TrustCenter Class 2 CA	TC TrustCenter Class 2 CA	1/1/2011	Secure Email, Server	TC TrustCenter Clas	
E-00 Third-Party Root Certification Au	TC TrustCenter Class 3 CA	TC TrustCenter Class 3 CA	1/1/2011	Secure Email, Server	TC TrustCenter Clas	
E - 🔯 Trusted People	TC TrustCenter Class 4 CA	TC TrustCenter Class 4 CA	1/1/2011	Secure Email, Server	TC TrustCenter Clas	
H- 🚾 SPC	TC TrustCenter Time Stamping CA	TC TrustCenter Time Staniping CA	1/1/2011	Time Stamping	TC TrustCenter Time	j.
_	Thavte Personal Basic CA	Thavite Personal Basic CA	1/1/2021	Client Authentication	Thave Personal Bas	
	Thawte Personal Freemail CA	Thavite Personal Freemail CA	1/1/2021	Client Authentication	Thavke Personal Fre	,
	Thavte Personal Premium CA	Thavite Personal Premium CA	1/1/2021	Client Authentication	Thavke Personal Pre	,
	Thawte Premium Server CA	Thavite Premium Server CA	1/1/2021	Server Authenticatio	Thavke Premium Ser	
	Thavte Server CA	Thavite Server CA	1/1/2021	Server Authenticatio	Thanke Server CA	
	Thavte Timestamping CA	Thavite Timestamping CA	1/1/2021	Time Stamping	Thavke Timestampin	
	UTN - DATACorp 59C	UTN - DATACorp SGC	6/25/2019	Server Authentication	UTN - DATACorp SGC	
	SUTN-USERFirst-Client Authenticati	UTN-USERFirst-Client Authentication	7/9/2019	Secure Email	UTN - USERFirst-Cle	
	EHUTN-USERFirst-Hardware	UTN-USER First-Hardware	7/9/2019	Server Authentication	UTN - USER First-Har	
	Edutted USERFirst Network Applications	UTN-LISED First-Network Applications	7010(2019	Secure Email, Server	UTN - USER First-Net	
	The INFREE At-Object	UTN-I ISER First-Object	7/10/2019	Time Stampion, Code	LITN - LISER First-Object	
	Elization Connectal Software Dubl	VariSian Commercial Software Dublis	12/31/1000	Serve Final Code S	Verifies Commercial	L.
	WariSon Comparial Software Public	Verlagh Commercial Software Publis	1/012004	Secure Ernel, Code S	VeriSign Commercial	
	Stratter Tedi deal Solovare Public	Verdige balk dual Software Publishing	122212100	Secure Entail, Code S	Verbigh Commercial	
	The second secon	Verbigh Individual Software Publishe	110/2004	Secure Entel, Code S	Verbigh Individual 5	
	Conversion Individual Software Publis	versign individual Software Publishe	1/8/2004	Secure Entail, Code S	vensign Individual 5	
	220 Ventsign Trust Network	Verbign Trust Network	2/19/2018	Secure Enal, Clent	venbign Class 2 Print	
	Califyrensign Trust Network	Verbigh Trust Network	8/2/2028	Secure Email, Client	verisign Class 2 Prin	
	221VeriSign Trust Network	VeriSign Trust Network	5/19/2018	Secure Enail, Clent	Veri5ign Class 3 Prim	
	VeriSign Trust Network	VeriSign Trust Network	8/2/2028	Secure Enail, Client	VeriSign Class 3 Prim	
	WeriSign Trust Network	VeriSign Trust Network	5/19/2018	Secure Email, Client	VeriSign Class 4 Prim	
	VeriSign Trust Network	VeriSign Trust Network	8/2/2028	Secure Email, Client	VeriSign Class 1 Prim	
	VeriSign Trust Network	VeriSign Trust Network	8/2/2028	Secure Enail, Clent	VeriSign Class 4 Prim	
	VeriSign Trust Network	VeriSign Trust Network	5/19/2018	Secure Email, Client	VeriSign Class 1 Prim	
	E Wreless-CA	Wireless-CA	12/17/2012	<al></al>	<hone></hone>	
	Dicert EZ by DST	Xcert EZ by DST	7/11/2009	Secure Enail, Server	Xcert EZ by DST	
[<u>x</u>]	<				and the second se	>
ted Root Certification Authorities store co	ntains 109 certificates.					
				And the second s		-

24. 重复此过程,以便将更多客户端添加到域中。

在 Microsoft Windows 2003 Server 上安装 Internet 身份验证服务并请求证书

在此设置中,Internet身份验证服务(IAS)用作RADIUS服务器,通过PEAP身份验证对无线客户端进 行身份验证。

要在服务器上安装和配置 IAS,请完成以下步骤。

- 1. 在"控制面板"中单击添加或删除程序。
- 2. 单击添加/删除 Windows 组件。
- 3. 选择网络服务,然后单击"详细信息"。
- 4. 选择Internet Authentication Service;单击OK;然后单击Next。

rvices				2
ve a compone ent will be insta	ent, click the check l alled. To see what's i	oox. A shaded box ncluded in a comp	means that only ponent, click Deta	part iils.
s of Networkir	ng Services:			
Name Syster	n (DNS)		1.7 MB	
c Host Config	uration Protocol (DH	CP)	0.0 MB	
Authenticatic	n Service		0.0 MB	
Access Qua	rantine Service		0.1 MB	
er HTTP Pro	φ.		0.0 MB	
TCP/IP Servio	ces		0.0 MB	_
vs Internet Na	me Service (WINS)		0.9 MB	-
Enables authe users, IAS sup	ntication, authorizati ports the RADIUS p	on and accounting rotocol.	g of dial-up and VI	PN
e required:	3.4 MB		Details	
e on disk:	7208.2 MB		<u>10</u> ,05(1)(9).	
		ПК	Cancel	
	rvices ve a compone int will be insta s of Networkin Name Syster ic Host Config Authenticatio Access Quar ver HTTP Prov TCP/IP Servic vs Internet Na Enables authe users. IAS sup e required: a on disk:	rvices ve a component, click the check t ent will be installed. To see what's i s of Networking Services: Name System (DNS) ic Host Configuration Protocol (DH Authentication Service e Access Quarantine Service ver HTTP Proxy TCP/IP Services vs Internet Name Service (WINS) Enables authentication, authorization users. IAS supports the RADIUS pro- e required: 3.4 MB e on disk: 7208.2 MB	ve a component, click the check box. A shaded box ent will be installed. To see what's included in a comp s of Networking Services: Name System (DNS) ic Host Configuration Protocol (DHCP) Authentication Service e Access Quarantine Service ver HTTP Proxy TCP/IP Services vs Internet Name Service (WINS) Enables authentication, authorization and accounting users. IAS supports the RADIUS protocol. e required: 3.4 MB e on disk: 7208.2 MB	vices ve a component, click the check box. A shaded box means that only ent will be installed. To see what's included in a component, click Details of Networking Services: Name System (DNS) 1.7 MB c Host Configuration Protocol (DHCP) 0.0 MB Authentication Service 0.1 MB Access Quarantine Service 0.1 MB ver HTTP Proxy 0.0 MB TCP/IP Services 0.0 MB Enables authentication, authorization and accounting of dial-up and VI users. IAS supports the RADIUS protocol. e required: 3.4 MB Details.

5. 单击**完成完成 IAS 的安装。**

Windows Components Wizard	J	X
	Completing the Windows Components Wizard You have successfully completed the Windows Components Wizard.	
	To close this wizard, click Finish.	
	< Back Finish	Help

- 6. 下一步是安装Internet身份验证服务(IAS)的计算机证书。
- 7. <u>单击Start;单击Run;键入mmc;然后单击OK</u>。

🚡 Console I - [Console Root						×
🐞 Elle Action Year Favo	grites Window Help					_1@12
← → 🔟 🖻 🔮 🖬						
🔄 Canacle Roat	News					
				There are no items to show	in this view.	
	1					
* Qarl 4 4	Network Connections	Down	A dograph - IDE2 1040	bternet in there also	Stresslet - freesh	
	C	1 million	The sector burginger		Consect freeses	 - Comment Matter

- 8. 在文件菜单中单击**控制台,然后选择"添加/删除"管理单元。**
- 9. 单击**添加添加管理单元。**

Add/Remove Snap-in	? ×
Standalone Extensions	
Use this page to add or remove a stand-alone snap-in from the co	onsole.
Snap-ins added to: Console Root	
Description	
Add <u>R</u> emove About	
ОК	Cancel

10. 从管理单元列表中选择**证书,然后单击"添加"。**

inan-in	Vendor	
NET Framework 1.1 Configuration	Microsoft Corporation	
Active Directory Domains and Trusts	Microsoft Corporation	
Active Directory Sites and Services	Microsoft Corporation	
Active Directory Users and Compu	Microsoft Corporation	
ActiveX Control	Microsoft Corporation	
🤣 ADSI Edit	Microsoft Corporation	
🔀 Authorization Manager	Microsoft Corporation	
Certificate Templates	Microsoft Corporation	
Certificates	Microsoft Corporation	
Certification Authority	Microsoft Corporation	•
_		-
十算机帐户 ,然后单击"下一步"。	<u>A</u> dd <u>C</u> los	e
计 算机帐户 ,然后单击"下一步"。 i <mark>ficates snap-in</mark> bis spap-in will always manage certificates f	<u>A</u> dd <u>⊂</u> los	e
计算机帐户 ,然后单击"下一步"。 <mark>ificates snap-in</mark> This snap-in will always manage certificates f	<u>A</u> dd <u>C</u> los	e]
计算机帐户,然后单击"下一步"。 ificates snap-in This snap-in will always manage certificates f ① <u>My</u> user account	Add <u>C</u> los	e]
计算机帐户 ,然后单击"下一步"。 ificates snap-in This snap-in will always manage certificates f O <u>My</u> user account O <u>S</u> ervice account O <u>Computer account</u>	<u>A</u> dd <u>C</u> los	e
计算机帐户 ,然后单击"下一步"。 ificates snap-in This snap-in will always manage certificates f ○ My user account ○ <u>S</u> ervice account ● <u>Computer account</u>	<u>A</u> dd <u>C</u> los	e
计算机帐户,然后单击"下一步"。 ificates snap-in [*] his snap-in will always manage certificates f [©] <u>My</u> user account [©] <u>Service account</u> • <u>Computer account</u>	<u>A</u> dd <u>C</u> los	e
计算机帐户,然后单击"下一步"。 ificates snap-in [™] his snap-in will always manage certificates f [™] My user account [®] Service account [®] Computer account	<u>A</u> dd <u>⊂</u> los for:	e

x

el

12. 选择**本地计算机**,然后单击"完成"。

elect the computer you wa	ant this snap-in to manage.		
This snap-in will always m	anage:		
 Local computer: [the 	computer this console is i	running on į	
C Another computer:			Biowse
only applies if you sa	ve the console.		
only applies if you sa	ve the console.		
only applies if you sa	ve the console.		
only applies if you sa	ve the console.		

- 13. 单击**关闭**,然后单击"确定"。
- 14. 展开Certificates(Local Computer);右键单击Personal folder;选择All tasks,然后选择 Request New Certificate。

🚡 Console I - [Console Reet]		
🐒 Sile diction given Rangelter Window Help		-1012
Concide Rost Concide Rost Conci	Peret Peret	
Request a new certificate from a certification authority (CA)	loran	

15. 在**欢迎使用证书请求向导上,单击下一步。**



16. 选择**域控制器证书模板(如果您从 DC 以外的服务器上请求计算机证书,请选择"计算机"证书** 模板),然后单击"下一步"。

tificate	Request Wizaro				
Certifica	te Types				
A ce	rtificate type cont	ains preset prop	perties for certificate	es.	
Selection	t a certificate typ have permissions	e for your requ for and that are	est. You can access available from a tru	only certificate ty isted CA.	pes that
Certi	ficate types:				
Dir Do Do	ectory Email Repli main Controller main Controller Au	ation Ithentication			
To se	elect a cryptograp	hic service prov	rider and a CA, selec	t Advanced.	
J_] r	<u>ancen</u>				
			< Back	Next >	Capce
			- Eack	Town	Conco

17. 键入证书的名称和说明。

icate Request Wizard				
rtificate Friendly Name an	d Description			
You can provide a name a certificate.	and description that help	you quickly	identify a speci	ific
Type a friendly name and	description for the new	certificate.		
Friendly name:				
PEAP-Wireless				
Description				
TAS Server Certificate -	802.1X Authentication			
1				
J				
1				

18. 单击完成完成证书请求向导。

Certificate Request Wizard		×
	Completing the Certificate Request Wizard You have successfully completed the Certificate Request wizard. You have specified the following settings:	
	Friendly Name PEAP-Wireless Computer Name TSWEB-LAPT Certificate Template Domain Controller	
	< <u>B</u> ack Finish Cancel	
Certificate Request Wizard The certificate request	×I : was successful.	
ОК		

为 PEAP-MS-CHAP v2 身份验证配置 Internet 身份验证服务

现在,您已经安装了 IAS 并为其请求了一个证书,可以开始为身份验证配置 IAS 了。 请完成以下步骤:

- 1. 单击**开始 > 程序 > 管理工具**,然后单击"Internet 身份验证服务"管理单元。
- 2. 右键单击Internet身份验证服务(IAS),然后单击在Active Directory中注册服务。

🖓 Internet Authentication Sec	reke		X
Elle Action Yerr Help			
+ + 🔟 🗗 🔮 🔟	• •		
Comparing Der Step ← → IE → IE → IE ← IE Particle Access Factor State R → Rende Access Factor State Factor Access Factor Request Proce	(iii) Set Service Sep Service Register Service Yew Poperties Etab	reae to Inferret Authentication Service frentication Service (IKG) to authenticate, authentica, and account for dai-up, VRA, wireless and Dhemet connections to your network. You can also configure IKG to Forward possible to any access ensure that is compatible with Ramote Authentication Dai-In User Service (RADDLE). to read the remote access properties of user accounts in Addre Directory, on the Addre menu, disk Ragister Server in Active Directory, stian about setting up IAG, deployment scenarios, and troubleshooting, see Help.	e
Register Server in Active Directory			
🐮 Start 🖉 🔮	Network Connections	2 Advarget - [DH2]19400 🗣 Internet Authentikals. 🛛 🖉 🖉 🕅 🖏 🖓	7:07 PM

3. 系统将显示**Register Internet Authentication Service in Active Directory**对话框;单击**确定**。这 使 IAS 能够对 Active Directory 中的用户进行身份验证。 Register Internet Authentication Server in Active Directory:

OK

Register Internet	Authentication Serve	r in Active Director	γ:

To enable IAS to authenticate users in the Active Directory, the computers running IAS must be authorized to read users' dial-in properties from the domain.

Cancel

Do you wish to authorize this computer to read users' dial-in-properties from the Wireless.com domain?

4. 在下一个对话框中单击确定

Server r	egistered:
	This computer is now authorized to read users' dial-in properties from domain Wireless.com. To authorize this computer to read users' dial-in properties from other domains, you must register this computer to be a member of the RAS/IAS Servers Group in that domain.
	COK COK

- 5. 在 MS IAS 服务器上添加无线局域网控制器作为 AAA 客户端。
- 6. 右键单击 RADIUS 客户端,然后选择"新建 RADIUS 客户端"。

The disting Mana Lake				
Internet Authentication Service (Local) Autoritation Service (Local) Autoritation (Local) Remote Acce Autoritation (Local) Connection (Local) Autoritation (Local)	Marrer	ote t 2		
er Clerit Raat 🛛 🎉 Network Connections	 	ngni: - [1942],12450 🗣 Internet Authoriticata	-	
建入客户端的名称(本示例中为 WLC),然后输入 WLC I	的 IP 地址。单i	击 Next。
Type a friendly	y name and either a	n IP Address or DNS n	name for the clien	
Literally name.		IWLL		
Client a <u>d</u> dress	(IP or DNS):			
10.77.244.21	q			Verify

8. 在下一页的Client-Vendor下,选择**RADIUS Standard**;输入共享密钥;然后单击**Finish**。 9. 请注意,WLC 已作为 AAA 客户端添加到 IAS 上。

🖓 Internet Authentication Service					15×
Elle &dition Yerk Help					Oere
Internet Authentication Service (Local)	Priendly Name /	Address	Protocol	Client/Vendor	
R- CALINE CIEVES	1 W.C	10.77.244.210	RADELS	RADIUS Standard	
B Remote Access Policies					
8- Connection Request Proceeding					
	1				
	1				
	1				
	1				
	1				
🏖 Start 🛛 🍎 👘 🖄 Network Connections	<u>₽</u> aco	A drange	- [DNS,19450	Platemet Authenticals.	

- 10. 为客户端创建远程访问策略。
- 11. 为此,请右键单击**远程访问策略**,然后选择"新建远程访问策略"。

Ele gution Verv Letto → → 12 (E) 3 (E) (E) 12 → Internet Austremication Service (Local) → Prevente Access Logging → Devente Access Policy → Connection Re → Connection Re	ierres Crister Crister Connections to Atlances and Resolte 1 Connections to other access servers 2	
	ierres Crister Crister Connections to Microsoft Routing and Remote 1 Connections to other access servers 2	
Internet Authentication Service (Local) ANDIAS Clents Service Access Logging Connection R Connection R New Remote Access Bolicy	ierres Croter Connections to Microsoft Routing and Remote 1 Connections to other access servers 2	
jikev • Rajnash Expertigen: Bélip		

12. 键入远程访问策略的名称。本示例中使用名称 PEAP。然后,单击下一步。

w Remote Acce	ss Policy Wizard
Policy Configu The wizard o	ration Method can create a typical policy, or you can create a custom policy.
How do you v	vant to set up this policy?
	e wizard to set up a typical policy for a common scenario
C Set up	a custom policy
Policy name:	PEAP-Wireless
	Example: Authenticate all VPN connections.
	< <u>B</u> ack <u>N</u> ext > Cancel

13. 根据您的需要选择策略属性。本示例中选择 Wireless。

w Remo	te Access Policy Wizard
Acces Pol	s Method licy conditions are based on the method used to gain access to the network.
Selec	st the method of access for which you want to create a policy.
C	<u>⊻</u> PN
	Use for all VPN connections. To create a policy for a specific VPN type, go back to the previous page, and select Set up a custom policy.
C	<u>D</u> ial-up
	Use for dial-up connections that use a traditional phone line or an Integrated Services Digital Network (ISDN) line.
G	Wireless
	Use for wireless LAN connections only.
C	Ethernet
	Use for Ethernet connections, such as connections that use a switch.

14. 在下一页上,选择**用户,以便将此远程访问策略应用于用户列表。**

Remote Access Policy Wizard	
User or Group Access You can grant access to individual users, or you can grant access to selec groups.	cted
 Grant access based on the following: User access permissions are specified in the user account. Group Individual user permissions override group permissions. 	
Group name:	A <u>d</u> d
	<u>H</u> emove
, 	

15. 在"身份验证方法"下,选择**受保护的 EAP (PEAP)**,然后单击"配置"。

Authentication Meth EAP uses different t	ods ypes of security devices to a	uthenticate users.		
Select the EAP type	for this policy.			
<u>T</u> ype:				
Protected EAP (PE/	AP)		Confi	igure
		< <u>B</u> ack <u>N</u>	ext >	Car
呆护的 EAP 属性页上		< <u>B</u> ack <u>N</u> 菜单中选择适当	ext> 的证书, 然	Car 《后单ī
呆护的 EAP 属性页上 rotected EAP Prope	,从"已颁发的证书"下拉 rties	< <u>B</u> ack N 菜单中选择适当	ext> 的证书,然	Car 《后单i ?义
R护的 EAP 属性页上 rotected EAP Prope This server identifies if Select the certificate t	<mark>,从"已颁发的证书"下拉 rties</mark> self to callers before the co hat you want it to use as pr	< <u>B</u> ack N 菜单中选择适当 onnection is compl roof of identity.	ext> 的证书,条 eted.	Ca 《后单i ?文
を护的 EAP 属性页上 otected EAP Prope This server identifies it Select the certificate t	,从"已颁发的证书"下拉 rties self to callers before the co hat you want it to use as pr	< <u>B</u> ack N 菜单中选择适当 onnection is compl roof of identity.	ext> 的证书, 然 eted.	Car 《后单i ? ×
そ かめ EAP 属性页上 otected EAP Prope This server identifies if Select the certificate t Certificate issued	<mark>. , 从"已颁发的证书"下拉 rties</mark> self to callers before the co hat you want it to use as pr Itsweb-lapt. Wireless .	< <u>B</u> ack N 菜单中选择适当 onnection is complete roof of identity.	ext> 的证书, <i>条</i> eted.	Car 《后单i ? ×
R护的 EAP 属性页上 This server identifies il Select the certificate t Certificate issued Friendly name:	,从"已颁发的证书"下拉 rties self to callers before the co hat you want it to use as pr Itsweb-lapt .Wireless PEAP-Wireless	< <u>B</u> ack N 菜单中选择适当 onnection is compl roof of identity.	ext >	Ca 《后单i ? ×
永护的 EAP 属性页上 rotected EAP Prope This server identifies if Select the certificate t Certificate issued Friendly name: Issuer:	. , 从"已颁发的证书"下拉 rties self to callers before the co hat you want it to use as pr Itsweb-lapt.Wireless PEAP-Wireless Wireless-CA	< <u>Back</u> N 菜单中选择适当 onnection is compl roof of identity.	ext> 的证书, 然 eted.	Ca 《后单i ? ×
采护的 EAP 属性页上 rotected EAP Prope This server identifies il Select the certificate t Certificate issued Friendly name: Issuer: Expiration date:	. , 从"已颁发的证书"下拉 rties self to callers before the co hat you want it to use as pr Itsweb-lapt.Wireless PEAP-Wireless Wireless-CA 12/16/2008 5:53:02 f	< <u>Back</u> N 菜单中选择适当 onnection is compl roof of identity.	ext > / 的证书,然 eted.	Ca 《后单i ?×
泉护的 EAP 属性页上 rotected EAP Prope This server identifies if Select the certificate t Certificate issued Friendly name: Issuer: Expiration date: 「 Enable Fast Recor	. , 从"已颁发的证书"下拉 rties self to callers before the co hat you want it to use as pr itsweb-lapt.Wireless PEAP-Wireless Wireless-CA 12/16/2008 5:53:02 F	< <u>Back</u> N 菜单中选择适当 onnection is compl roof of identity.	ext > 的证书,然 eted.	Ca 《后单i ?×
呆护的 EAP 属性页上 rotected EAP Prope This server identifies if Select the certificate t Certificate issued Friendly name: Issuer: Expiration date: 「 Enable Fast Recor Eap Types	. , 从"已须发的证书"下拉 rties self to callers before the co hat you want it to use as po Itsweb-lapt . Wireless PEAP-Wireless Wireless-CA 12/16/2008 5:53:02 P	< <u>Back</u> N 菜单中选择适当 onnection is complete roof of identity.	ext > 的证书, % eted.	Ca 《后单i ?×
呆护的 EAP 属性页上 rotected EAP Prope This server identifies if Select the certificate t Certificate issued Friendly name: Issuer: Expiration date: 「」Enable Fast Recor Eap Types Secured password (E	L,从"已颁发的证书"下拉 rties self to callers before the co hat you want it to use as pr Lsweb-lapt.Wireless PEAP-Wireless Wireless-CA 12/16/2008 5:53:02 F nect	< <u>Back</u> N 菜单中选择适当 onnection is compl roof of identity. com	ext > 的证书, & eted.	Car 然后单i ? ×

OK

Cancel

1

Edit

L

Remove

Add

"0

17. 验证远程访问策略的详细信息,然后单击**完成**。

New Remote Access Policy Wizard

Completing the New Remote Access Policy Wizard You have successfully completed the New Remote Access
Policy Wizard. You created the following policy:
PEAP-Wireless
Conditions: NAS-Port-Type matches "Wireless - Other OR Wireless - IEEE 802.11"
Authentication: EAP(Protected EAP (PEAP))
Encryption: Basic, Strong, Strongest, No encryption
To close this wizard, click Finish.
< <u>B</u> ack <u>Finish</u> Cancel

×

18. 远程访问策略就已经添加到列表中。



19. 右键单击此策略,然后单击**属性**。在"如果连接请求满足指定的条件"下选择**授予远程访问权限**

PEAP Properties			? X		
Settings					
Specify the conditions that c	connection requ	ests must match.			
Policy <u>c</u> onditions:					
NAS+Fort-Type matches w	vireless - Other (E 602. T		
Add <u>E</u> dit	<u>R</u> emo	ve			
If connection requests match associated profile will be app	h the conditions blied to the conn	specified in this p ection.	policy, the		
Edit Profile)					
Unless individual access per policy controls access to the	rmissions are spo e network.	ecified in the user	profile, this		
If a connection request mate Deny remote access per	ches the specifie mission	d conditions:			
Grant remote access per Grant for Grant for Grant for G	<u>G</u> rant remote access permission				
	OK	Cancel	Apply		

将用户添加到 Active Directory

o

在此设置中,需要在 Active Directory 上维护用户数据库。

要将用户添加到 Active Directory 数据库中,请完成以下步骤:

1. 在"Active Directory用户和计算机"控制台树中,右键单击**用户**;单击**新建**;然后单击**用户**。



2. 在"新建对象 - 用户"对话框中,键入无线用户的名称。本示例在"名字"字段中使用名称 WirelessUser**,并在"用户登录名"字段中使用"WirelessUser"。**单击 Next。

w Object - User				J
😭 Create	in: Wireless	.com/Users		
<u>F</u> irst name:	Client 1		Initials:	
Last name:				
Full name:	Client 1			
User logon name:				
Client1		@Wireles:	s.com	•
, User logon name (pre-Windows 2	2000]:		
WIRELESS		Client1		
,		/		
		< <u>B</u> ack	<u>N</u> ext>	Cancel

3. 在"新建对象 – 用户"对话框中,在"密码"和"确认密码"字段中键入您选择的密码。清除**用户必须** 在下次登录时更改密码复选框,然后单击"下一步"。

Password		
Confirm password:	•••••	
User <u>m</u> ust change p	assword at next logon	
User cannot change	e password	
Password never exp	vires	
Account is disabled		

S	Create in:	Wireless.cr	om/Users		
When y	ou click Finisł	n, the followin;	g object will b	e created:	
Full nan	ne: Client 1				
User log	jon name: Cli	ent1@Wirele:	ss.com		
			(Pack	Timich] [

5. 重复步骤 2 到步骤 4,以便创建更多用户帐户。

<u>允许用户进行无线访问</u>

请完成以下步骤:

- 1. 在Active Directory用户和计算机控制台树中,单击**Users**文件夹;右键单击**WirelessUser**;单击**Properties**;然后转到**Dial-in**选项卡。
- 2. 选择**允许访问**,然后单击"确定"。

ient 1 Properties	?
Remote controlTerminal ServicGeneralAddressAccountProfileMember OfDial-inEnvice	ces Profile COM+ Telephones Organization vironment Sessions
Remote Access Permission (Dial-in or VPN)	·
Allow access	
C Deny access	
C Control access through Remote Access	Policy
☐ ⊻erify Caller-ID:	
Callback Options	
No <u>C</u> allback	
C Set by Caller (Routing and Remote Acce	ess Service only)
C Always Callback to:	
Assign a Static IP Address	
Apply Static Boutes	
Define routes to enable for this Dial-in connection.	Static Ro <u>u</u> tes
ОК	Cancel <u>Apply</u>

配置无线局域网控制器和轻量 AP

现在要为此设置配置无线设备。这包括配置无线局域网控制器、轻量 AP 和无线客户端。

通过 MS IAS RADIUS 服务器为 RADIUS 身份验证配置 WLC

首先要配置 WLC,以便使用 MS IAS 作为身份验证服务器。需要配置 WLC 以便将用户凭证转发到

外部 RADIUS 服务器。然后,外部 RADIUS 服务器验证用户凭证,并向无线客户端提供访问权限 。为此,请在**安全性 > RADIUS 验证页中添加 MS IAS 服务器作为 RADIUS 服务器。**

请完成以下步骤:

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,单击新建定义 RADIUS 服务器。

ca Statema					Save C	orfiguration Ping	Logout Ref
h. A.	MONITOR WLANS CONTR	OLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
ecurity	RADIUS Authentication Ser	vers > New				< Back	Apply
AA General	Server Index (Priority)	1 🛩					
RADIUS Authentication RADIUS Accounting Local Net Users	Server IPAddress	10.77.244.198					
MAC Filtering Disabled Clients	Shared Secret Format	ASCII 👻					
User Login Policies AP Policies	Shared Secret	•••••]	
ccess Control Lists PSec Certificates	Confirm Shared Secret	•••••					
CA Certificate ID Certificate	Key Wrap						
Veb Auth Certificate							
Vireless Protection Policies	Port Number	1812					
Trusted AP Policies Rogue Policies Standard Signatures	Server Status	Enabled 💌					
Custom Signatures Client Exclusion Policies	Support for RFC 3576	Enabled 💌					
AP Authentication	Retransmit Timeout	2 seconds					
	Network User	Enable					
	Management	Enable					
	IPSec	🖾 Enable					

2. 在 RADIUS 身份验证服务器 > 新建页中定义 RADIUS 服务器参数。这些参数包括 RADIUS 服务器的 IP 地址、共享密钥、端口号和服务器状态。"网络用户"和"管理"复选框决定基于 RADIUS 的身份验证是否适用于管理和网络用户。本示例使用 IP 地址为 10.77.244.198 的 MS IAS 作为 RADIUS 服务器。

ISCO SPOTENCE			901				Save Configurat	ion Ping Logo	ut Ref
Cara with	DADUIG	WLANS C	ONTROLLER	WIRELESS 5	ECURITY	MANAGEMENT (OMMANDS HELP	and a second second	
AAA General RADIUS Authentication RADIUS Authentication Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	Call Stat Credent Use AES	Authenticatio tion ID Type ials Caching Key Wrap	IP Address		Rest	188-44	Admin Statu	Apply New	
Access Control Lists	User	ranagement	Index	activer Address	Pars	ir set.	Autom Statu	•	
IPSec Certificates CA Certificate ID Certificate Web Auth Certificate Wireless Protection Policies Trusted AP Policies Rogue Policies Standard Signatures Custom Signatures Client Exclusion Policies AP Authentication			1	10.77.244.198	1812	Disabled	Enabled	EGI Remove	Eina

- 3. 单击 Apply。
- 4. MS IAS 服务器已作为 RADIUS 服务器添加到 WLC 中,并且可用于对无线客户端进行身份验证。

<u>为客户端配置 WLAN</u>

配置无线客户端要连接到的 SSID (WLAN)。本示例中将创建 SSID,并将其命名为 PEAP。

将第 2 层身份验证定义为 WPA2,使客户端能够执行基于 EAP 的身份验证(本示例中为 PEAP-MSCHAPv2)并使用 AES 作为加密机制。将其他所有值均保留默认值。

注意:本文档将WLAN与管理接口绑定。当您的网络中有多个 VLAN 时,可以创建一个单独的 VLAN 并将其绑定到 SSID。有关如何在 WLC 上配置 VLAN 的信息,请参阅<u>无线局域网控制器上的</u> <u>VLAN 配置示例</u>。

要在 WLC 上配置 WLAN,请完成以下步骤:

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. 选择**新建创建新的 WLAN。**输入 WLAN 的 WLAN ID 和 WLAN SSID,然后单击**应用**。

3 · 0 · 🗈 🖻	6 P 🛠 🛛 🕅	a. 🕹 🖂 🥸					🦓 <u>- 8 ×</u>
Dises Sestems					Save Co	onfiguration Fing	Logout Refresh
WLANS	WLANs > New	CONTROLLER WIRELESS	SECORITY	MARAGERENT	COMMANDS	< Back	Apply
WLANS WLANS	WLAN ID	1 ¥					
AP Groups VLAN	WLAN SSID	PEAP					

3. 创建新 WLAN 后,就会显示新 WLAN 的 WLAN > Edit 页。在此页上,可以定义各种特定于此 WLAN 的参数,包括常规策略、RADIUS 服务器、安全策略和 802.1x 参数。

CINCO STOTEME				Save Confi	iguration Fing Logout Refr
alle alle	MONITOR WLANS CI	ONTROLLER WIRELESS	SECURITY MANAGEMEN	t commands h	ÆUP
WLANs	WLANs > Edit				< Back Apply
WLANS	WLAN ID	1			
AP Groups VLAN	Profile Name	PEAP			
	WLAN SSID	PEAP			
	General Policies			Security Policies	s
	Radio Policy	All		IPv6 Enable	
	Admin Status	Enabled			
	Session Timeout (secs)	0		Layer 2 Security	WPA1+WPA2
	Quality of Service (QoS)	Silver (best effort)			MAC Filtering
	WMM Policy	Disabled 💌		Layer 3 Security	None
	7920 Phone Support	Client CAC Limit CAP	CAC Limit		Web Policy *
	Broadcast SSID	Enabled			
	Aironet IE	Enabled			
	Allow AAA Override	Enabled		* Web Policy can IPsec.	not be used in combination with
	Client Exclusion	Enabled ** 60		TT When client as	school on it applied a time out
	Dillon Granus	Timeout V	alue (secs)	value of zero me	ans infinity(will require
	DHCP Server	Deveringe		*** CKIP is not s	upported by 10xx APs
	DHCP Addr. Assignment	Required			
	Interface Name	management 💌			
	MFP Version Required	1			
	Generation	Global MFP Disabled)			
	H-REAP Local Switching				
	* H-REAP Local Switchin authentications.	g not supported with IPSEC,	CRANITE and FORTRESS		

4. 选中"常规策略"下的**管理状态,以便启用 WLAN。**如果希望 AP 在其信标帧中广播 SSID,请 选中**广播 SSID**。

5. 在"第 2 层安全性"下,选择 WPA1+WPA2。这将在 WLAN 上启用 WPA。向下滚动该页,然 后选择 WPA 策略。本示例使用 WPA2 和 AES 加密。从"RADIUS 服务器"下的下拉菜单中选 择相应的 RADIUS 服务器。本示例中使用 10.77.244.198(MS IAS 服务器的 IP 地址)。可以 根据 WLAN 网络的需要修改其他参数。

	Cinco Svorcus							Save O	onfiguration	Ping	Logout	Refre	sh
	ds.ds	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP				
	WLANs	WPA1+WP Paramete	PA2 rs			-							*
	WLANS WLANS AP Groups VLAN	WPA1 Poli WPA2 Poli WPA2 Enc	icy icy ryption	⊡ R Maes	Пткјр								
		Auth Key	Mgmt	802.1x	×								
~	¥ ± ▲	·n n											
6.	卑击 Apply。							Save C	onfiguration	Ping	Logout	Refre	sh
	Acres	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP				
	WLANs	WLANS											
	WLANS WLANS WLANS	WLANS Profile Na	me	w	LAN WLAN S	SID	At	lmin Secur	ity Policies				1
	WLANS WLANS WLANS AP Groups VLAN	WLANS Profile Na	me	W 10	PEAP	SID	A4 St	lmin Secur atus Secur	ity Policies 2][Auth(80	2.1x)]		Edit I	II Rem



为 PEAP-MS CHAPv2 身份验证配置无线客户端

本示例提供有关如何使用 Cisco Aironet Desktop Utility 配置无线客户端的信息。在配置客户端适配 器之前,请确保使用了最新版本的固件和实用程序。在 Cisco.com 上的无线下载页中查找最新版本 的固件和实用程序。

要用 ADU 来配置 Cisco Aironet 802.11 a/b/g 无线客户端适配器,请完成以下步骤:

- 1. 打开 Aironet Desktop Utility。
- 2. 单击 Profile Management, 然后单击"New"以定义配置文件。
- 3. 在"General"选项卡下,输入配置文件名称和 SSID。本示例中使用您在 WLC (PEAP) 上配置的 SSID。

Profile Management	2 🔀
General Security Advanc	ed
- Profile Settings	
Profile Name:	PEAP-MSCHAPv2
Client Name:	CLIENT1
Network Names	
SSID1:	PEAP
SSID2:	
SSID3:	
	UK Cancel

4. 选择Security选项卡;选择**WPA/WPA2/CCKM**;在WPA/WPA2/CCKM EAP下,键入**PEAP** [EAP-MSCHAPv2],然后单击Configure。

Profile Management			?
General Security Advanced			
-Set Security Options			
WPA/WPA2/CCKM WPA/WPA2 Passphrase	WPA/WPA2/CCKM EAP Type:	PEAP (EAP-MSCHAP V2)	
O 802.1x	802.1x EAP Type:	EAP-FAST	
Pre-Shared Key (Static WEP) None			
Configure	Allow Association to Mixed Ce Profile Locked	ils	
Group Policy Delay:	60 Sec	Controller To: 0 Sec	
		OK Can	cel

5. 选择 Validate Server Certificate,然后在"Trusted Root Certificate Authorities"下拉菜单下选择 "Wireless-CA"。

Configure PEAP (EAP-MSCHAP V2)
Use Machine Information for Domain Logon
Validate Server Identity
Trusted Root Certification Authorities
Wireless-CA 😒
When connecting, use:
O Certificate
 User Name and Password
Use Windows User Name and Password User Information for PEAP (EAP-MSCHAP V2) Authentication
User Name: Administrator
Password:
Confirm Password:
Advanced OK Cancel

6. 单击 OK,然后激活该配置文件。注意:将Protected EAP-Microsoft Challenge Handshake Authentication Protocol Version 2(PEAP-MSCHAPv2)与Microsoft XP SP2配合使用时,无线 卡由Microsoft Wireless Zero Configuration(WZC)管理,您必须应用Microsoft修补程序 KB885453。这可以防止与 PEAP 快速恢复相关的几个身份验证问题。

验证与故障排除

要验证配置是否按预期工作,请在无线客户端 Client1 上激活配置文件 PEAP-MSCHAPv2。

😨 Cisco Aironet Desktop Utility	y - Current Profile: PEAP-M	SCHAPv2 🛛 🛛 🔀
Action Options Help		
Current Status Profile Management	Diagnostics	
CISCO SYSTEMS		
Profile Name:	PEAP-MSCHAPv2	
Link Status:	Authenticated	Network Type: Infrastructure
Wireless Mode:	5 GHz 54 Mbps	Current Channel: 64
Server Based Authentication:	PEAP (EAP-MSCHAP V2)	Data Encryption: AES
IP Address:	10.77.244.218	
Signal Strength:		
		Advanced

当 ADU 上激活配置文件 PEAP-MSCHAPv2 后,客户端将执行 802.11 开放式身份验证,然后执行 PEAP-MSCHAPv2 身份验证。这是一个成功的 PEAP-MSCHAPv2 身份验证示例。

请使用调试命令来了解发生的事件顺序。

<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。

以下调试命令在无线局域网控制器上非常有用。

- debug dot1x events enable—用于配置 802.1x 事件的调试
- debug aaa events enable—用于配置 AAA 事件的调试
- debug mac addr <mac 地址>—用于使用 debug mac 命令配置 MAC 调试
- debug dhcp message enable—用于配置 DHCP 错误消息的调试

下面是 debug dot1x events enable 命令和 debug client <mac 地址> 命令的输出示例。

debug dot1x events enable :

Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Received EAPOL START from
 mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Sending EAP-Request/Identity to
 mobile 00:40:96:ac:e6:57 (EAP Id 2)
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Received Identity Response (count=2) from
 mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for
 mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to
 mobile 00:40:96:ac:e6:57 (EAP Id 3)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from

mobile 00:40:96:ac:e6:57 (EAP Id 3, EAP Type 25)

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 4) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 4, EAP Type 25) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 5) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 5, EAP Type 25) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 6) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 6, EAP Type 25) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 7) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 7, EAP Type 25) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 8) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 8, EAP Type 25) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 9) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 9, EAP Type 25) Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 10) Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 10, EAP Type 25) Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 11) Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 11, EAP Type 25) Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 12) Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 12, EAP Type 25) Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Processing Access-Accept for mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Creating a new PMK Cache Entry for station 00:40:96:ac:e6:57 (RSN 0) Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending EAP-Success to mobile 00:40:96:ac:e6:57 (EAP Id 13) Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending default RC4 key to mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending Key-Mapping RC4 key to

mobile 00:40:96:ac:e6:57

Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Received Auth Success while in Authenticating state for mobile 00:40:96:ac:e6:57

debug mac addr <MAC 地址>:

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Association received from mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 STA: 00:40:96:ac:e6:57 rates (8): 12 18 24 36 48 72 96 108 0 0 0 0 0 0 0 0 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN (20) Change state to START (0) Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 10.77.244.218 START (0) Initializing policy Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 10.77.244.218 START (0) Change state to AUTHCHECK (2) Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 10.77.244.218 AUTHCHECK (2) Change state to 8021X_REQD (3) Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 10.77.244.218 8021X_REQD (3) Plumbed mobile LWAPP rule on AP 00:0b:85:51:5a:e0 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Changing state for mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0 from Associated to Associated Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Stopping deletion of Mobile Station: 00:40:96:ac:e6:57 (callerId: 48) Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Sending Assoc Response to station 00:40:96:ac:e6:57 on BSSID 00:0b:85:51:5a:e0 (status 0) Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Changing state for mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0 from Associated to Associated Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 10.77.244.218 Removed NPU entry. Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 dot1x - moving mobile 00:40:96:ac:e6:57 into Connecting state Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Sending EAP-Request/Identity to mobile 00:40:96:ac:e6:57 (EAP Id 1) Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Received EAPOL START from mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 EAP State update from Connecting to Authenticating for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 dot1x moving mobile 00:40:96:ac:e6:57 into Authenticating state Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Req state (id=3) for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 3) Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 3, EAP Type 25) Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Req state (id=4) for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 4) Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 4, EAP Type 25) Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57

```
Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
  Entering Backend Auth Req state (id=5) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 5)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 5, EAP Type 25)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
  Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Entering Backend Auth Req state (id=6) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 6)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
  Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 9, EAP Type 25)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
  Entering Backend Auth Req state (id=10) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 10)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
  Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 10, EAP Type 25)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
  Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
  Entering Backend Auth Req state (id=11) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
  Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 11)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
  Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 11, EAP Type 25)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
  Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
  Processing Access-Accept for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Creating a new PMK Cache Entry for station 00:40:96:ac:e6:57 (RSN 0)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Sending EAP-Success to mobile 00:40:96:ac:e6:57 (EAP Id 12)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Sending default RC4 key to mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Sending Key-Mapping RC4 key to mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218
   8021X_REQD (3) Change state to L2AUTHCOMPLETE (4)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218
  L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP 00:0b:85:51:5a:e0
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218
  L2AUTHCOMPLETE (4) Change state to RUN (20)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
   (20) Reached PLUMBFASTPATH: from line 4041
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
  (20) Replacing Fast Path rule
 type = Airespace AP Client
 on AP 00:0b:85:51:5a:e0, slot 0, interface = 2
 ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN (20)
 Card = 0 (slot 0), InHandle = 0 \times 00000000,
```

```
OutHandle = 0x0000000, npuCryptoFlag = 0x0000
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
(20) Successfully plumbed mobile rule (ACL ID 255)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
(20) Reached RETURN: from line 4041
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Entering Backend
Auth Success state (id=12) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Received Auth Success
while in Authenticating state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 dot1x -
moving mobile 00:40:96:ac:e6:57 into Authenticated state
```

注意:如果使用Microsoft Supplicant客户端通过Cisco Secure ACS进行PEAP身份验证,则客户端 可能无法成功进行身份验证。有时初始连接能够成功进行身份验证,但是随后的快速连接身份验证 尝试不能成功连接。这是已知问题。有关此问题的详细信息及其修正方法,请参阅<u>此处 。</u>

相关信息

- ACS 4.0 和 Windows 2003 中统一无线网络下的 PEAP
- WLAN 控制器 (WLC) 中 EAP 身份验证的配置示例
- •无线局域网控制器(WLC)软件升级到版本3.2、4.0和4.1
- Cisco 4400 系列无线局域网控制器配置指南
- <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)。