採用Microsoft Internet身份驗證服務(IAS)的統一 無線網路下的PEAP

目錄

簡介 必要條件 需求 採用元件 慣例 PEAP概述 設定 網路圖表 組態 配置Microsoft Windows 2003 Server 配置Microsoft Windows 2003 Server 在Microsoft Windows 2003 Server上安裝並配置DHCP服務 安裝Microsoft Windows 2003 Server並將其配置為證書頒發機構(CA)伺服器 將客戶端連線到域 在Microsoft Windows 2003 Server上安裝Internet身份驗證服務並請求證書 為PEAP-MS-CHAP v2身份驗證配置Internet身份驗證服務 將使用者新增到Active Directory 允許對使用者進行無線訪問 配置無線區域網控制器和輕量AP 通過MS IAS RADIUS伺服器配置WLC進行RADIUS身份驗證 為客戶端配置WLAN 配置無線客戶端 為PEAP-MS CHAPv2身份驗證配置無線客戶端 驗證和疑難排解 相關資訊

<u>簡介</u>

本文提供一個組態範例,用於在以Microsoft Internet Authentication Service(IAS)作為RADIUS伺服 器的思科整合無線網路中設定使用Microsoft Challenge Handshake驗證通訊協定(MS-CHAP)第2版 驗證之受保護可擴充驗證通訊協定(PEAP)。

<u>必要條件</u>



假設讀者瞭解基本的Windows 2003安裝和思科控制器安裝知識,因為本文檔僅介紹便於測試的特定 配置。

注意:本文檔旨在為讀者提供一個示例,說明MS伺服器上進行PEAP - MS CHAP身份驗證所需的 配置。本部分介紹的Microsoft伺服器配置已在實驗室經過測試,並且發現可以按預期工作。如果配 置Microsoft伺服器時遇到問題,請與Microsoft聯絡以獲取幫助。Cisco TAC不支援Microsoft Windows伺服器配置。

有關Cisco 4400系列控制器的初始安裝和配置資訊,請參閱<u>快速入門手冊:Cisco 4400系列無線</u> LAN控制器。

Microsoft Windows 2003安裝及設定指南可在安裝Windows Server 2003 R2 中找到。

開始之前,請在測試實驗室中的每台伺服器上安裝Microsoft Windows Server 2003 SP1作業系統並 更新所有Service Pack。安裝控制器和輕量接入點(LAP),並確保配置最新的軟體更新。

<u>採用元件</u>

本文中的資訊係根據以下軟體和硬體版本:

- •執行韌體版本4.0的Cisco 4400系列控制器
- •思科1131輕量型存取點通訊協定(LWAPP)AP
- 安裝了Internet身份驗證服務(IAS)、證書頒發機構(CA)、DHCP和域名系統(DNS)服務的 Windows 2003 Enterprise Server(SP1)
- Windows XP Professional SP 2(和更新的Service Pack)和Cisco Aironet 802.11a/b/g無線網 路介面卡(NIC)
- Aironet案頭實用程式版本4.0
- Cisco 3560交換器

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

<u>慣例</u>

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

<u>PEAP概述</u>

PEAP使用傳輸級別安全(TLS)在身份驗證PEAP客戶端(如無線筆記型電腦)和PEAP身份驗證器 (如Microsoft Internet身份驗證服務(IAS)或任何RADIUS伺服器之間建立加密通道。PEAP不指定身 份驗證方法,但為其他EAP身份驗證協定提供額外的安全性,例如EAP-MSCHAPv2,這些協定可 以通過PEAP提供的TLS加密通道運行。PEAP身份驗證過程包括兩個主要階段:

PEAP階段1:TLS加密通道

無線客戶端與AP關聯。基於IEEE 802.11的關聯在客戶端和接入點(LAP)之間建立安全關聯之前提供 開放系統或共用金鑰身份驗證。在客戶端和接入點之間成功建立基於IEEE 802.11的關聯之後,與 AP協商TLS會話。在無線客戶端和IAS伺服器之間成功完成身份驗證後,將在它們之間協商TLS會 話。在此協商中匯出的金鑰用於加密所有後續通訊。

PEAP階段2:EAP身份驗證通訊

EAP通訊(包括EAP協商)在PEAP身份驗證過程的第一階段由PEAP建立的TLS通道內發生。 IAS伺服器使用EAP-MS-CHAP v2對無線客戶端進行身份驗證。LAP和控制器僅在無線客戶端和 RADIUS伺服器之間轉發消息。WLC和LAP無法解密這些消息,因為它不是TLS終點。

發生PEAP第1階段後,在IAS伺服器和802.1X無線客戶端之間建立TLS通道,對於成功的身份驗證 嘗試,使用者已使用PEAP-MS-CHAP v2提供有效的基於密碼的憑據,RADIUS消息序列如下:

- 1. IAS伺服器向客戶端傳送身份請求消息: EAP-Request/Identity。
- 2. 客戶端以身份響應消息進行響應: EAP-Response/Identity。
- 3. IAS伺服器傳送MS-CHAP v2質詢消息:EAP-Request/EAP-Type=EAP MS-CHAP-V2(質詢)。
- 4. 客戶端使用MS-CHAP v2質詢和響應進行響應: EAP-Response/EAP-Type=EAP-MS-CHAP-V2(響應)。
- 5. 當伺服器成功驗證客戶端時,IAS伺服器會發回MS-CHAP v2成功資料包:EAP-Request/EAP-Type=EAP-MS-CHAP-V2(成功)。
- 6. 當客戶端成功驗證伺服器時,客戶端使用MS-CHAP v2成功資料包進行響應: EAP-Response/EAP-Type=EAP-MS-CHAP-V2(成功)。
- 7. IAS伺服器傳送一個EAP-TLV,指示身份驗證成功。
- 8. 客戶端以EAP-TLV狀態成功消息進行響應。
- 9. 伺服器完成身份驗證並使用明文傳送EAP-Success消息。如果為客戶端隔離部署了VLAN,則 此消息中會包含VLAN屬性。

<u>設定</u>

本文檔提供配置PEAP MS-CHAP v2的示例。

註:使用Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用以下網路設定:



在此設定中, Microsoft Windows 2003伺服器執行以下角色:

- 域的域控制器Wireless.com
- DHCP/DNS伺服器
- 證書頒發機構(CA)伺服器
- Active Directory 維護使用者資料庫
- 網際網路身份驗證服務(IAS) 對無線使用者進行身份驗證

如圖所示,此伺服器通過第2層交換機連線到有線網路。

無線LAN控制器(WLC)和註冊的LAP也透過第2層交換器連線至網路。

無線客戶端C1和C2將使用Wi-Fi保護訪問2(WPA2)-PEAP MSCHAP v2身份驗證連線到無線網路。

目標是配置Microsoft 2003伺服器、無線LAN控制器和輕量AP,以使用PEAP MSCHAP v2身份驗證 對無線客戶端進行身份驗證。

下一節說明如何為此設定配置裝置。

組態

本節介紹在該WLAN中設定PEAP MS-CHAP v2身份驗證所需的配置:

- 配置Microsoft Windows 2003 Server
- 設定無線LAN控制器(WLC)和輕量AP
- 配置無線客戶端

首先配置Microsoft Windows 2003伺服器。

配置Microsoft Windows 2003 Server

配置Microsoft Windows 2003 Server

如網路設定部分中所述,使用網路中的Microsoft Windows 2003伺服器執行這些功能。

- 域控制器 用於域無線
- DHCP/DNS伺服器
- 證書頒發機構(CA)伺服器
- 網際網路驗證服務(IAS) 對無線使用者進行驗證
- Active Directory —用於維護使用者資料庫

為這些服務配置Microsoft Windows 2003伺服器。首先將Microsoft Windows 2003伺服器配置為域 控制器。

將Microsoft Windows 2003伺服器配置為域控制器

若要將Microsoft Windows 2003伺服器配置為域控制器,請完成以下步驟:

1. 按一下Start,按一下Run,鍵入dcpromo.exe,然後按一下OK以啟動Active Directory安裝嚮導



2. 按一下**下一步**以運行Active Directory安裝嚮導。

Domain controllers running Windows Server 2003 implement security settings that require clients and other servers to communicate with those domain controllers in a secure way. Some older versions of Windows, including Windows 95 and Windows NT 4.0 SP3 earlier, do not meet these requirements. Similarly, some non-Windows systems, inclu Apple Mac OS X and SAMBA clients, might not meet these requirements.	2003 affect older versions of	ersio	ler ve	t olde	affec	2003 -	erverä	ows S	Wind	ttings i	cunty s	WS.	ndow	mpr Min¢
Some older versions of Windows, including Windows 95 and Windows NT 4.0 SP3 earlier, do not meet these requirements. Similarly, some non-Windows systems, inclu Apple Mac OS X and SAMBA clients, might not meet these requirements. For more information, see <u>Compatibility Help</u> .	003 implement security settings that ate with those domain controllers in a r	irity in c	securi Iomair	ent se se do	npleme th tho:	003 im ate witł	ver 20 iunical	vs Ser comn	/indov ers to	nning her sei	ollers r s and c	n contr clients way.	main uire c :ure v)om equi ecu
For more information, see <u>Compatibility Help</u> .	indows 95 and Windows NT 4.0 SP3 rly, some non-Windows systems, inclu of meet these requirements.	dow ows eme	Wind /indov ;quire	and V n-Wi e rec	vs 95 a me no et thes	indows rly, son ot meel	ng Wir Similarl ght noi	ncludi ents. (its, mij	lows, i quirem A clier	of Win nese re I SAMI	ersion: : meet S X ar	older v do nol Mac O	me ol lier, c ple M	iom arlie ppl
							<u>elp</u> .	<u>iility H</u>	<u>mpatit</u>	see <u>C</u>	matior	re infor	more	or n

3. 若要建立新域,請為新域選擇Domain Controller選項。

Domain C Specify	ontroller Type the role you want this server to have.
Do you additior	want this server to become a domain controller for a new domain or an nal domain controller for an existing domain?
• Do	main controller for a new domain
Sel Thi	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.
O <u>A</u> de	ditional 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. 按一下**下一步**以建立新的域樹林。

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. 如果系統中未安裝DNS,嚮導將為您提供配置DNS的選項。選擇**No, Just Install and Configure DNS** on this computer。按「**Next**」(下一步)。

Active Directory Installation Wizard	×
Install or Configure DNS You can configure or install Domain Naming Service (DNS) on this computer.	X
Domain Naming Service (DNS) is not configured on this computer. Is DNS already running on this network?	
C Yes, I will configure the DNS client	
• INO, just install and configure DINS on this computer	
< <u>Back</u> Next>	Cancel

6. 鍵入新域的完整DNS名稱。在此範例中使用Wireless.com,然後按一下「Next」。

New Domain Name Specify a name for the new domain.		So and a second s
Type the full DNS name for the new do (for example: headquarters.example.mic	nain crosoft.com).	
Full DNS name for new domain:		
Wireless.com		
		1

7. 輸入域的NETBIOS名稱,然後按一下**Next**。此範例使用**WIRELESS**。

ctive Directory Installation W	izard
NetBIOS Domain Name Specify a NetBIOS name for	r the new domain.
This is the name that users o domain. Click Next to accep	of earlier versions of Windows will use to identify the new It the name shown, or type a new name.
Domain NetBIOS name:	WIRELESS
	< <u>B</u> ack <u>N</u> ext> Cancel

8. 選擇域的資料庫和日誌位置。按「Next」(下一步)。

ctive Directory Installation Wizard	X
Database and Log Folders Specify the folders to contain the Active Directory database and	l log files.
For best performance and recoverability, store the database and hard disks.	the log on separate
Where do you want to store the Active Directory database?	
<u>D</u> atabase folder:	
C:\WINDOWS\NTDS	Browse
Where do you want to store the Active Directory log?	
C:\WINDOWS\NTDS	Browse
< <u>B</u> ack	<u>N</u> ext > Cancel

9. 選擇Sysvol資料夾的位置。按「**Next**」(下一步)。

tive Directory Installation Wizard		x
Shared System Volume Specify the folder to be shared as the sys	stem volume.	Sold and the second sec
The SYSVOL folder stores the server's co of the SYSVOL folder are replicated to all	ppy of the domain's public fil domain controllers in the do	es. The contents main.
The SYSVOL folder must be located on a	in NTFS volume.	
Enter a location for the SYSVOL folder.		
Eolder location:		
C:\WINDOWS\SYSVOL		B <u>r</u> owse
	< <u>B</u> ack <u>N</u> ex	t> Cancel

10. 選擇使用者和組的預設許可權。按「Next」(下一步)。

Select default permissions fo	or user and group objects.
Some server programs, such stored on domain controllers.	as Windows NT Remote Access Service, read informatio
• Permissions compatible v	with pre-Windows 2000 server operating systems
Select this option if you re systems or on Windows a members of pre-Windows	un server programs on pre-Windows 2000 server operatin 2000 or Windows Server 2003 operating systems that are s 2000 domains.
\Lambda Anonymous users a	can read information on this domain.
 Permissions compatible c operating systems 	only with Windows 2000 or Windows Server 2003
Select this option if you re Server 2003 operating sy authenticated users can	un server programs only on Windows 2000 or Windows ystems that are members of Active Directory domains. Only read information on this domain.
	< <u>B</u> ack <u>N</u> ext > Ca
管理員密碼,然後按一下下- ve Directory Installation Wi	-步。 izard
管理員密碼,然後按一下下一 re Directory Installation Wi Directory Services Restore This password is used when Mode.	-步。 izard Mode Administrator Password you start the computer in Directory Services Restore
管理員密碼,然後按一下下一 Ye Directory Installation Wi Directory Services Restore This password is used when Mode. Type and confirm the passw when this server is started in	ー步。 izard Mode Administrator Password you start the computer in Directory Services Restore ord you want to assign to the Administrator account used Directory Services Restore Mode.
管理員密碼,然後按一下下一 A Directory Installation Wi Directory Services Restore This password is used when Mode. Type and confirm the passwo when this server is started in The restore mode Administra account. The passwords for both.	一步。 izard Mode Administrator Password you start the computer in Directory Services Restore ord you want to assign to the Administrator account used Directory Services Restore Mode. itor account is different from the domain Administrator the accounts might be different, so be sure to remember
管理員密碼,然後按一下下- Perform A State A S	ー步。 izard Mode Administrator Password you start the computer in Directory Services Restore ord you want to assign to the Administrator account used Directory Services Restore Mode. tor account is different from the domain Administrator the accounts might be different, so be sure to remember
管理員密碼,然後按一下下- Pirectory Installation Wi Directory Services Restore This password is used when Mode. Type and confirm the passwo when this server is started in The restore mode Administra account. The passwords for both. Restore Mode Password: Confirm password:	ー步。 izard Mode Administrator Password you start the computer in Directory Services Restore ord you want to assign to the Administrator account used Directory Services Restore Mode. tor account is different from the domain Administrator the accounts might be different, so be sure to remember
管理員密碼,然後按一下下- Pirectory Installation Wi Directory Services Restore This password is used when Mode. Type and confirm the password when this server is started in The restore mode Administra account. The passwords for both. Restore Mode Password: Confirm password: For more information about D	ー步。 izard Mode Administrator Password you start the computer in Directory Services Restore ord you want to assign to the Administrator account used Directory Services Restore Mode. tor account is different from the domain Administrator the accounts might be different, so be sure to remember ●●●●●●● Directory Services Restore Mode, see <u>Active Directory He</u>
管理員密碼,然後按一下下- re Directory Installation Wi Directory Services Restore This password is used when Mode. Type and confirm the password when this server is started in The restore mode Administra account. The passwords for both. Restore Mode Password: Confirm password: For more information about D	-步。 izard Mode Administrator Password you start the computer in Directory Services Restore ord you want to assign to the Administrator account used Directory Services Restore Mode. tor account is different from the domain Administrator the accounts might be different, so be sure to remember

12.	按一	ኮ 下-	-步 接受先前設定的	「域選項」	•
-----	----	-------------	-------------------	-------	---

Sun	mary 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. 按一下**完成**關閉Active Directory安裝嚮導。



Windows must be restarted before the Directory Installation wizard take effe	he changes made by the Active ect.	
	Don't Restart Now	

通過此步驟,您已將Microsoft Windows 2003伺服器配置為域控制器,並建立了新域 Wireless.com。接下來,在伺服器上配置DHCP服務。

在Microsoft Windows 2003 Server上安裝並配置DHCP服務

Microsoft 2003伺服器上的DHCP服務用於為無線客戶端提供IP地址。若要在此伺服器上安裝和配置 DHCP服務,請完成以下步驟:

- 1. 在「Control Panel(控制面板)」中按一下Add or Remove Programs。
- 2. 按一下Add/Remove Windows Components。
- 3. 選擇Networking Services,然後按一下Details。
- 4. 選擇Dynamic Host Configuration Protocol(DHCP), 然後按一下OK。

Ubcomponents of Networking Services:	1 7 40
M Submain Name System (DNS)	
 Eventsion Service 	F) 0.0 MB
Bemote Access Quarantine Service	0.1 MB
	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 automat addresses to client computers on the	tically assigns temporary IP e same network.
Total disk space required: 3.4 MB	Details
Space available on disk: 7224 5 MB	

5. 按一下**下一步**安裝DHCP服務。

indows Components You can add or remove components of Windows.	Ì
To add or remove a component, click the checkbox. A shaded bo part of the component will be installed. To see what's included in a Details.	x means that only 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 MR 🔟
Description: Contains a variety of specialized, network-related serv	vices and protocols.
Total disk space required: 3.4 MB	Details
Space available on disk: 7212.1 MB	

6. 按一下Finish完成安裝。



- 7. 要配置DHCP服務,請按一下**開始>程式>管理工具**,然後按一下**DHCP**管理單元。
- 8. 選擇DHCP伺服器 tsweb-lapt.wireless.com(在本例中)。
- 9. 按一下Action,然後按一下Authorize以授權DHCP服務。



- 10. 在控制檯樹中,按一下右鍵**tsweb-lapt.wireless.com**,然後按一下**New Scope**以定義無線客 戶端的IP地址範圍。
- 11. 在「新建作用域嚮導」的「歡迎使用新建作用域嚮導」頁上,按一下**下一步**。



12. 在Scope Name頁面上,鍵入DHCP作用域的名稱。在本示例中,使用**DHCP-Clients**作為作 用域名稱。按「**Next**」(下一步)。

providing a de	rovide an identifying scope name. You also have the option of scription.
Type a name a how the scope	and description for this scope. This information helps you quickly identify e is to be used on your network.
N <u>a</u> me:	DHCP-Clients
Description:	DHCP Server for Wireless Clients

13. 在「IP地址範圍」頁上,輸入範圍的起始IP地址和結束IP地址,然後按一下**下一步**。

You define the scope addresses.	e address ra	nge by	identify	ing a set o	f conse	cutive IP	1	
Enter the range of ad	dresses tha	t the sc	ope dis	stributes.				
<u>S</u> tart IP address:	10 . 77	. 244	. 218	1				
End IP address:	10 . 77	. 244	. 219					
A subnet mask define	e how mon	, bits of	an IP	addrass to	use for	the nature	rk /oubnot	
A subnet mask define IDs and how many bi length or as an IP ado Length:	es how many ts to use for dress.) bits of the ho:	an IP st ID, Y	address to 'ou can sp	use for ecify the	the netwoi subnet m	rk/subnet ask by	
A subnet mask define IDs and how many bi length or as an IP add Length: Sybnet mask:	es how many ts to use for dress. 8 255 . 0	/ bits of the ho:	an IP st ID. Y . 0	address to 'ou can spi	use for ecify the	the networ subnet m	rk/subnet ask by	
A subnet mask define IDs and how many bi length or as an IP ado <u>L</u> ength: S <u>u</u> bnet mask:	es how many ts to use for dress. 8	bits of the hos . 0	an IP st ID. Y . 0	address to 'ou can spi	use for ecify the	the networ subnet m	rk/subnet ask by	

14. 在Add Exclusions頁面上,提及要從DHCP作用域中保留/排除的IP地址。按「**Next**」(下一步)。

Type the IP addres address, type an a	s range that you w ddress in Start IP a	ant to exclude. If you want to exc ddress only.	lude a single
Start IP address:	End IP add	ress:	
1		Agd	
Excluded address	ange:		
		Hemo <u>v</u> e	

15. 在Lease Duration頁面中提及租用持續時間,然後按一下Next。

w Scope Wizard	
Lease Duration The lease du scope.	ration specifies how long a client can use an IP address from this
Lease duratio connected to portable comp Likewise, for locations, lon	ins should typically be equal to the average time the computer is the same physical network. For mobile networks that consist mainly of puters or dial-up clients, shorter lease durations can be useful. a stable network that consists mainly of desktop computers at fixed ger lease durations are more appropriate.
Set the durati	on for scope leases when distributed by this server.
Days: H	l <u>o</u> urs: <u>M</u> inutes: D 🔆 D ≑
	< Back Next > Cancel

16. 在Configure DHCP options頁上,選擇**Yes, I want to configure DHCP Option now**,然後按 一下**Next**。

Co	Anfigure DHCP Options You have to configure the most common DHCP options before clients can use the scope.
	When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.
	The settings you select here are for this scope and override settings configured in the Server Options folder for this server.
	Do you want to configure the DHCP options for this scope now?
	Yes, I want to configure these options now
	O No, I will configure these options later
	Z Back Nevts Cancel

17. 如果有預設網關路由器,請在Router(Default Gateway)頁面中提及網關路由器的IP地址,然 後按一下**Next**。



18. 在「域名和DNS伺服器」頁面上,鍵入之前配置的域的名稱。在本例中,使用 Wireless.com。輸入伺服器的IP地址。按一下「Add」。

naps and translates domain names want the client computers on your servers on your network, enter the I <u>P</u> address:	s used by network to use for
want the client computers on your servers on your network, enter the I <u>P</u> address:	network to use for
servers on your network, enter the I <u>P</u> address:	IP addresses for thos
servers on your network, enter the I <u>P</u> address:	IP addresses for thos
	Add
/e 10.77.244.217	<u>R</u> emove
	<u>Ш</u> р
	Down
< Back Nex	t> Cancel
	e 10.77.244.217 < <u>B</u> ack <u>N</u> ex

19. 按「**Next**」(下一步)。

20. 在「WINS伺服器」頁上,按一下**下一步**。

21. 在「啟用作用域」頁上,選擇**「是,我想立即啟用作用域」,然**後按一下「下一**步」**。

Activate Scope Clients can obtain address leases only if a s	cope is activate	d.	₹Ţ
Do you want to activate this scope now?			
Yes, I want to activate this scope now			
C No, I will activate this scope later			



< <u>B</u>ack

Finish

23. 在「DHCP管理單元」視窗中,驗證建立的DHCP作用域是否處於活動狀態。

Elle girtion View Help				Close
* > 🗈 🗉 🗡 🗗 🗟 🖻 🛄 📮	4P			
Ф оно-	toweb-lapt.wireless.com [18,77,214,2	17]		
B- Contraction of the second (10.77244-217)	Carteris of DHCP Server	2315	Description	
Server Optione	Scape [172.16.0.0] DHCP-Clients	** Active **	DHCP Server for Wireless Clients	
	Server Options			
	1			
	1			
	1			
	1			
				1
🐮 Start 🛛 🎉 📃 🔍 Network Connections	⊈рнси			🖉 🕈 🛢 🗑 🎆 👯 🔽 KORPM

既然在伺服器上啟用了DHCP/DNS,請將伺服器配置為企業證書頒發機構(CA)伺服器。

安裝Microsoft Windows 2003 Server並將其配置為證書頒發機構(CA)伺服器

使用EAP-MS-CHAPv2的PEAP根據伺服器上存在的證書驗證RADIUS伺服器。此外,伺服器證書必 須由受客戶端電腦信任的公共證書頒發機構(CA)頒發(即,公共CA證書已存在於客戶端電腦證書儲 存上的受信任的根證書頒發機構資料夾中)。在本示例中,將Microsoft Windows 2003伺服器配置 為向Internet身份驗證服務(IAS)頒發證書的證書頒發機構(CA)。

若要在伺服器上安裝和設定憑證服務,請完成以下步驟:

- 1. 在「Control Panel(控制面板)」中按一下「Add or Remove programs(新增/刪除程式)」
- 2. 按一下新增/删除Windows元件。

0

3. 按一下「Certificate Services」。

Windows Components		1		ſ
You can add or remove cor	mponents of Wind	dows.		l
To add or remove a compor part of the component will b Details.	nent, click the ch e installed. To se	neckbox. A sh ee what's inclu	aded box means (ded in a compon	hat only ent, click
<u>C</u> omponents:				
🖉 📻 Accessories and Ut	ilities		4.	9 MB 🔼
🔤 🗹 🧃 Application Server			34.	4 мв 💻
🔽 📴 Certificate Services			1.	8 MB
🗌 🛄 E-mail Services			1.	1 MB
Eax Services				9 MR 💻
Description: Installs a certi public key sec	fication authority l curity programs.	(CA) to issue c	ertificates for use	with
Total disk space required:	13.8 M	В	D	etails
Space available on disk:	7310.6 MI	В	<u>_</u>	ordina
	< Back	Next >	Cancel	He
	L	-		
	talling Certifica	te Services	該雷腦不能重:	新命名

加入	域或	從域。	甘里	除。	是否	要繼	쇎
MH / N	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		1 . 1103	סינא	ᄶᄓ	头颅的	Л

⚠	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?			

5. 在Certificate Authority Type下,選擇Enterprise root CA,然後按一下Next。

lo	ws Components Wizard
CA	Type Select the type of CA you want to set up.
	Enterprise root CA
	© Enterprise subordinate CA
	Stand-alone root CA
	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

6. 輸入用於標識CA的名稱。此範例使用**Wireless-CA**。按「**Next**」(下一步)。

dows Components Wizard		
CA Identifying Information Enter information to identify this	s CA.	Ē
Common name for this CA:		
Wireless-CA		
Distinguished name suffix:		
DC=Wireless,DC=com		
Preview of distinguished name:		
CN=Wireless-CA,DC=Wireless,DC=	=com	
Validity period:	Expiration date:	
5 Years 💌	12/12/2012 7:01 PM	
	(Pack Novita Canad L U	ala
<pre></pre>	Codok Next Cancel He	sib

7. 為證書資料庫儲存建立「證書日誌」目錄。按「Next」(下一步)。

ertificate Database S Enter locations for the information.	ettings certificate database, database lo	g, and configuration
<u>C</u> ertificate database:		
C:\WINDOWS\system	n32\CertLog	Br <u>o</u> wse
Certificate <u>d</u> atabase log	<u>;</u>	
C:\WINDOWS\system	n32\CertLog	Browse
Shared folder:	information in a shared folder	Browse
Shared folder: Preserve existing of	ertificate database	Blowse

Microsof	ft Certificate Services	×
	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. 按一下Finish完成證書頒發機構(CA)服務的安裝。



下一步是在Microsoft Windows 2003伺服器上安裝和配置Internet身份驗證服務。

將客戶端連線到域

下一步是將客戶端連線到有線網路,並從新域下載域特定資訊。換句話說,將客戶端連線到域。為 此,請完成以下步驟:

- 1. 使用直通乙太網電纜將客戶端連線到有線網路。
- 2. 啟動客戶端並使用客戶端的使用者名稱/密碼登入。
- 3. 按一下開始;按一下運行;鍵入cmd;然後按一下確定。
- 4. 在命令提示符下,鍵入ipconfig,然後按一下Enter以驗證DHCP是否正常工作,並且客戶端從 DHCP伺服器收到IP地址。
- 5. 若要將客戶端加入域,請按一下右鍵My Computer, 然後選擇Properties。
- 6. 按一下Computer Name頁籤。
- 7. 按一下「Change」。
- 8. 按一下Domain; 鍵入wireless.com; 然後按一下OK。

You can observe the name and the membership of this	
computer. Changes may affect access to network resources.	
Computer name:	
Client1	
Full computer name: Client1. More Member of O Domain:	
Wireless	
Workgroup:	

9. 鍵入**Username Administrator**以及客戶機加入的域特定的密碼。(這是伺服器上Active

	ne chunges
Enter the name to join the doma	and password of an account with permissio
User name:	🖸 administrator

Directory中的管理員帳戶。



- 10. 按一下「**OK**」(確定)。
- 11. 按一下Yes重新啟動電腦。
- 12. 電腦重新啟動後,使用以下資訊登入:使用者名稱= Administrator;密碼= <domain password>;域= Wireless。
- 13. 按一下右鍵My Computer,然後按一下Properties。
- 14. 按一下Computer Name頁籤,驗證您位於Wireless.com域中。

asin'i ropor				
System Res	store	Automa	Remote	
General Comp		mputer Name	Advanced	
Wind on th	lows use e netwo	es the following inf rk.	ormation to identify	your computer
Computer <u>d</u> escr	iption:			
		For example: "H Computer".	Kitchen Computer'')	or ''Mary's
Full computer n	ame:	Client1.Wireles	s.com	
Domain:		Wireless.com		
domain and cre ID. _	ate a loc	cai user account, i		
To rename this	compute	er or join a domain	, click Change.	<u>C</u> hange
🚹 Changes	will take	effect after you re	estart this computer.	
		Contract of		

15. 下一步是驗證使用者端是否從伺服器收到CA憑證(信任)。

- 16. 按一下Start;按一下Run;鍵入mmc,然後按一下OK。
- 17. 按一下**檔案**,然後按一下**新增/刪除**管理單元。

o		
Standalone Extensi	ons	
Use this page to ad	d or remove a standalone Snap-in from) the console.
Snap-ins added to:	🔄 Console Root	v
Description		
- Description		
Description		
- Description		
- Description Add	Remove About.	

- 18. 按一下「**Add**」。
- 19. 選擇「**Certificate**」,然後按一下「**Add**」。

Add Standalone Snap-in

Snap-in	Vendor	
🏡 .NET Framework 1.1 Configuration	Microsoft Corporation	
🖆 ActiveX Control	Microsoft Corporation	-
Certificates	Microsoft Corporation	
Component Services	Microsoft Corporation	000
🛃 Computer Management	Microsoft Corporation	
💐 Device Manager	Microsoft Corporation	
🔮 Disk Defragmenter	Microsoft Corp, Executi	20000
👹 Disk Management	Microsoft and VERITAS	
🔟 Event Viewer	Microsoft Corporation	
Folder	Microsoft Corporation	
Description The Certificates snap-in allows you to bro ertificate stores for yourself, a service, o	wse the contents of the r a computer.	
		<u></u>

6

20. 選擇「Computer Account」,然後按一下「Next」。

This snap-in will always	manage certificates for:	
O My user account		
 Service account 		
 Computer account 		
	< Back Next >	Canc
ᆕᄅᇃᇃᇉᇇᅝᅻᅑᅑᇘ	. 수 너 쿡 때	
- トFINISN以接支預設	ž	
elect Computer		
	ww.want this span-in to manage	
Select the computer vo		
Select the computer yo	us manage:	
Select the computer yo This snap-in will alway	(the computer this console is running on)	
Select the computer yo This snap-in will alway O Local computer:	(the computer this console is running on)	
Select the computer yo This snap-in will alway O Local computer: Another compute	ys manage: (the computer this console is running on) ar:	:e,
Select the computer yo This snap-in will alway Local computer: Another compute Allow the selected	(the computer this console is running on) er: Brows ed computer to be changed when launching from the command line.	e This

22. 按一下「Close」,然後按一下「OK」。 23. 展開Cortificates(Level Computer):展開Trusted Post Cortification

23. 展開Certificates(Local Computer);展開Trusted Root Certification Authorities;然後按一下

< Back

Finish

Cancel

Certificates。在清單中查詢Wireless。

h File Action View Favorites Windo	w Help					_160
- → ⓑ छ ४ № × ₫ ₿	R.					
Console Root	Issued To - /	Issued By	Espiration Date	Intended Purposes	Friendly Name	Stat
🗇 Certificates (Local Computer)	SERVICIOS DE CERTIFICACION	SERVICIOS DE CERTIFICACION - A	3/10/2009	Secure Email, Server	SERVICIOS DE CERT	
E Personal	SIA Secure Client CA	51A Secure Client CA	7/9/2019	Secure Enail, Server	Societa Interbancari	
E - Trusted Root Certification Author	SIA Secure Server CA	SIA Secure Server CA	7/9/2019	Secure Email, Server	Societa Interbancari	
Certificates	Swisskey Root CA	Swisskey Root CA	1/1/2016	Secure Email, Server	Swisskey Root CA	
H Enterprise Trust	Symantec Root CA	Symantec Root CA	5/1/2011	<ab< td=""><td><none></none></td><td></td></ab<>	<none></none>	
H M Intermediate Certrication Author	TC TrustCenter Class I CA	TC TrustCenter Class 1 CA	1/1/2011	Secure Email, Server	TC TrustCenter Clas	
H M Insteel Publishers	TC TrustCenter Class 2 CA	TC TrustCenter Class 2 CA	1/1/2011	Secure Email, Server	TC TrustCenter Clas	
H	TC TrustCenter Class 3 CA	TC TrustCenter Class 3 CA	1/1/2011	Secure Email, Server	TC TrustCenter Clas	
E M Trusted People	TC TrustCenter Class 4 CA	TC TrustCenter Class 4 CA	1/1/2011	Secure Email, Server	TC TrustCenter Clas	
in the sec	TC TrustCenter Time Stamping CA	TC TrustCenter Time Staniping CA	1/1/2011	Time Stamping	TC TrustCenter Time	
	Thavte Personal Basic CA	Thavite Personal Basic CA	1/1/2021	Client Authentication	Thavte Personal Bas.	
15	Thavte Personal Freemal CA	Thawte Personal Freemail CA	1/1/2021	Client Authentication	Thavte Personal Fre	
	Theyte Personal Prenium CA	Theeste Personal Premium CA	1/1/2021	Client Authentication	Thanks Personal Pre	_
5	Thaute Premium Server CA	Thoute Prenium Server CA	1/1/2021	Server Authenticatio	Thanke Premium Ser	
	Thavta Server CA	Theaste Server CA	1/1/2021	Server Authenticatio	Thanks Server CA	
15	Thaute Timestampion CA	Thaute Trestanning CA	1/1/2021	Time Stamping	Thanke Timestannin	
	UTN - DATACom SSC	UTN - DATACore SGC	6/25/2019	Server Authentication	UTN - DATACom SGC	
15	The Second Second Sector Sectors	UTM SEDERA Class Authentication	7/9/2019	Server Final	UTN - USED East - Cle	
	The International Manhattan	UTBLI STD Dark March and	7/9/2019	Secure Creat	UTN - USER Proc. dec.	i.
	Contraction of the second section of the second seco	UTILI ISED East Maturely Applications	7/9/2019	Server Auchentication	UTN - USER First And	1
	The second secon	UTN-USERPISE-Network Applications	7/10/2019	Secure chail, Server	UTN - USERPHYC-WRC	
	Diversities of the second of the second second	UIN-USERHIST-ODJect	//10/2019	Time scamping, Code	UTW-USERPHISC-ODJec	Ľ
	Wensign Commercial Software Publ	Verbign Commercial Software Publis	12/31/1999	Secure Enail, Code S	VenSign Commercial	
	MyeriSign Commercial Software Publ	Vertsign Commercial Software Publis	1/8/2004	Secure Email, Code 5	VeriSign Commercial	í
	Wentsign Individual Software Publis	Verbign Individual Software Publishe	15/31/1999	Secure Enal, Code 5	VeriSign Individual 5	
	WeriSign Individual Software Publis	VeriSign Individual Software Publishe	1/8/2004	Secure Email, Code S	VeriSign Individual S	
19	22 Veri5ign Trust Network	VeriSign Trust Network	5/19/2018	Secure Enail, Clent	Veri5ign Class 2 Prim	
	VeriSign Trust Network	VeriSign Trust Network	8/2/2028	Secure Email, Client	VeriSign Class 2 Prim	
10	VeriSign Trust Network	VeriSign Trust Network	5/19/2018	Secure Enail, Clent	Veri5ign Class 3 Prim	,
5	VeriSign Trust Network	VeriSign Trust Network	8/2/2028	Secure Enail, Client	VeriSign Class 3 Prim	
6	VeriSign Trust Network	VertSign Trust Network	5/19/2018	Secure Email, Client	Veri5ign Class 4 Prim	
6	VeriSign Trust Network	VeriSign Trust Network	8/2/2028	Secure Enail, Client	VeriSign Class 1 Prim	
6	VeriSign Trust Network	VertSign Trust Network.	8/2/2028	Secure Email, Client	VeriSign Class 4 Prim	
6	VeriSign Trust Network	VeriSign Trust Network	5/19/2018	Secure Enail, Client	VeriSign Class 1 Prim	
	Wreless-CA	Wireless-CA	12/17/2012	<al></al>	<hione></hione>	
6	Dicert EZ by DST	Xcert EZ by DST	7/11/2009	Secure Enail, Server	Xcert EZ by DST	
	{					>
sted Root Certification Authorities store cont	ains 109 certificates.	araraa ka k	0.00.00.00.00.00.	Constant and the second second		
Start Te Consolet - [Console				03		

24. 重複此過程, 向域中新增更多客戶端。

在Microsoft Windows 2003 Server上安裝Internet身份驗證服務並請求證書

在此設定中,Internet身份驗證服務(IAS)用作RADIUS伺服器,通過PEAP身份驗證對無線客戶端進 行身份驗證。

完成以下步驟,在伺服器上安裝和配置IAS。

- 1. 在「Control Panel(控制面板)」中按一下Add or Remove Programs。
- 2. 按一下Add/Remove Windows Components。
- 3. 選擇Networking Services,然後按一下Details。
- 4. 選擇Internet Authentication Service;按一下OK;然後按一下Next。

of the compo	nent will be insta	illed. To see what's i	ncluded in a compo	nent, click Deta	ils.
ub <u>c</u> ompone	nts of Networkin	ng Services:			
🗹 🚚 Doma	ain Name System	n (DNS)		1.7 MB	
🗹 🦲 Dyna	mic Host Config	uration Protocol (DH	CP)	0.0 MB	
🗹 📙 Interr	net Authenticatio	n Service		0.0 MB	
🗆 🚚 Remo	ote Access Quar	antine Service		0.1 MB	
RPC over HTTP Proxy					
🗆 🚚 Simple TCP/IP Services					
🗆 🚚 Wind	lows Internet Na	me Service (WINS)		0.9 MB	-
escription:	Enables authe users, IAS sup	ntication, authorizati ports the RADIUS p	on and accounting o rotocol.	f dial-up and VI	PN
otal disk spa	ace required:	3.4 MB		Details	
nace availa	ble on disk:	7208.2 MB		2.01000	

5. 按一下Finish完成IAS安裝。



6. 下一步是安裝Internet身份驗證服務(IAS)的電腦證書。

7. 按一下Start;按一下Run;鍵入mmc;然後按一下OK。

diction year Favorit	sec Miluqevi Relb		
vaale Root	Nowe		
		There are no items to shave in this view.	
	1		
	1		
			0. N. O. N.
	Network Connections	A dramant - IDE(212400). Stremet & therefore the Tensalet - Freesalet -	

- 8. 在「檔案」選單中按一下Console,然後選擇Add/Remove管理單元。
- 9. 按一下Add以新增管理單元。

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

10. 從管理單元清單中選擇Certificates,然後按一下Add。

vailable standalone snap-ins:		
Snap-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	-
[「Computer account」,然後按一下	<u>A</u> dd <u>⊂</u> lo:	se
「Computer account」,然後按一下 tificates snap-in	Add Clos	se
「Computer account」,然後按一下 tificates snap-in This snap-in will always manage certificates	Add ⊆los 「Next」。 for:	se
「Computer account」,然後按一下 tificates snap-in This snap-in will always manage certificates ① <u>My</u> user account	Add ⊆los 「Next」 。 for:	se
【 「Computer account」,然後按一下 tificates snap-in This snap-in will always manage certificates 〇 <u>My</u> user account 〇 Service account	<u>A</u> dd <u>C</u> los ⁻ 「Next」 。 for:	se
「Computer account」,然後按一下 tificates snap-in This snap-in will always manage certificates ① <u>My</u> user account ② <u>Service account</u> ② Computer account	Add ⊆los 「Next」 。 for:	5e
「Computer account」,然後按一下 tificates snap-in This snap-in will always manage certificates ① My user account ② Service account ④ Computer account	Add ⊆los Next 」 。 for:	5e
「Computer account」,然後按一下 tificates snap-in This snap-in will always manage certificates ① My user account ② Service account ④ Computer account	Add ⊆los Next 」 。	se
「Computer account」,然後按一下 tificates snap-in This snap-in will always manage certificates	Add ⊆los Next 」 。 for:	se
「Computer account」,然後按一下 tificates snap-in This snap-in will always manage certificates ① My user account ② Service account ④ Computer account	Add ⊆los Next 」 ₀ for:	se
「Computer account」,然後按一下 tificates snap-in This snap-in will always manage certificates ○ My user account ○ Service account ● Computer account	Add ⊆lo: 「Next」 。 for:	se
「Computer account」,然後按一下 tificates snap-in This snap-in will always manage certificates ① My user account ② Service account ③ Computer account	Add ⊆lo: 「Next」 。 for:	se
Computer account」,然後按一下 tificates snap-in This snap-in will always manage certificates My user account Service account Computer account	Add ⊆los Next 」 。 for:	se
「Computer account」,然後按一下 tificates snap-in This snap-in will always manage certificates	Add Close Next」。	se
【 「Computer account」,然後按一下 tificates snap-in This snap-in will always manage certificates ○ My user account ○ Service account ● Computer account	Add Close Next」。	se

Cancel

×

12. 選擇「Local computer」,然後按一下「Finish」。

ect Computer	
Select the computer you wa	ant this snap-in to manage
This span-in will always m	anade:
local computer: (the	computer this console is running on
C Another computer:	Bjowse
Allo <u>w</u> the selected co only applies if you sa	omputer to be changed when launching from the command line. This we the console.
	should be also be also be also be also be also be also be an

- 13. 按一下「Close」,然後按一下「OK」。
- 14. 展開**證書(本地電腦)**;按一下右鍵Personal資料夾;選擇All tasks,然後選擇Request New Certificate。



15. 在「Welcome to the Certificate Request Wizard」上按一下Next。



16. 選擇Domain Controller certificate模板(如果您請求非DC伺服器上的電腦證書,請選擇 Computer證書模板),然後按一下Next。

A certificate type contains preset properties for certificates. Select a certificate type for your request. You can access only certificate types you have permissions for and that are available from a trusted CA. Certificate types: Directory Email Replication Domain Controller	
Select a certificate type for your request. You can access only certificate types you have permissions for and that are available from a trusted CA. Certificate types: Directory Email Replication Domain Controller	
Certificate types: Directory Email Replication Domain Controller	that
Directory Email Replication Domain Controller	
Domain Controller Authentication	
To select a cryptographic service provider and a CA, select Advanced.	
I Advanced	
< Back Next >	

Vou can provide a name an	d description the	at belo you quid	Vlu identifu e checific
certificate.	a acscription the	ic neip you quic	Ny lachary a specific
Tupe a friendly pame and d	lessription for th	o pow cortificat	_
Friendly name	escription for th	e new cerunicat	с,
PEAP-Wireless			
Description:			
IAS Server Certificate - 80)2.1× Authentica	ation	

18. 按一下完成完成認證請求嚮導。

Certificate Request Wizard		×
	Completing the Certificate Leaves Wizard Suppose the successfully completed the Certificate Leaves wizard. Dual non-specified the following settings: Computer Name PEAP-Wireless Certificate Template Domain Controller	
Certificate Request Wizard	< <u>B</u> ack Finish Cancel Image: St was successful.	
OK		

為PEAP-MS-CHAP v2身份驗證配置Internet身份驗證服務

現在您已安裝並請求了IAS的證書,請配置IAS進行身份驗證。

請完成以下步驟:

- 1. 按一下Start > Programs > Administrative Tools,然後按一下Internet Authentication Service管理單元。
- 2. 按一下右鍵Internet身份驗證服務(IAS),然後按一下Register Service in Active Directory。

🐓 Internet Authentication S	Service.	的复数复数使用		
Ele Artion Yev Lelp				
* > 🔟 🗗 🔮 🖾				
Perrote Access Logging Perrote Access Logging	Constraint Start Service Start Service September September Papenties Bala Service	dave Denotors s opundo S to read stan ab	Internet Authentikation Service iton Service (IAS) to authenticate, authentics, and account for dai-up, VPA, evideor and Drhwnet corner to any access server that is compatible with Remote Authentication Disk-In User Service (RADCUS). d the remote access properties of user accounts in Active Directory, on the Action meru, club Register Ser not setting up IAS, deployment scenarios, and troubleshooting, see Help.	tions to your network. You can also configure 1KG to Forward rver in Active Directory.
Register Server in Active Director	7			
2 Start 16	Network Connections	Parce	🙏 drangest - [DH2],19400 🐤 Internet Authentikats	🖉 🕈 🐻 🕅 🖏 🕅 🕅 🕅

3. 出現「**Register Internet Authentication Service in Active Directory**(在**Active Directory中註冊 Internet身份驗證服務**)」對話方塊;按一下「OK(確定)」。這使得IAS能夠對Active Directory中的使用者進行身份驗證。

X

To enable IAS to authenticate users in the Active	Directory, the computers running IAS must be autho	rized to read users' dial-in properties from the domain.
Do you wish to authorize this computer to read us	ers' dial-in properties from the Wireless.com domain	?
	OK Cancel	

4. 在下一個對話方塊中按一下OK。

Server r	registered: 🔀
	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.

- 5. 將無線區域網控制器新增為MS IAS伺服器上的AAA客戶端。
- 6. 按一下右鍵RADIUS Clients,然後選擇New RADIUS Client。

	🖓 Internet Authentication Service		US AND A CONTRACT OF A CONTRACT	×
Image: Constant	Elle Artion Yerr Help			
Were Order Order Order				
New Gerst 2015 Start 2010 Start Connections 2016 Annual - [DH2] (SAID) Sternet Authentication 2016 Start	Internet Autoritation Service (Laca) Premate Acc MarkAdd (Laca) Premate Acc Mark	Maree Connectians to Microsoft Routing and Remote - Connectians to other access servers	order	
🐮 Start 🖉 🔨 Network Connections 🔯 DH-3 🕹 drampst - (DH2) (SAED 🗣 Internet Authenticats. 🖉 🖉 🕄 🕄 🖓 👯 🏹 7.13 PM	New Clerit			
	🏄 Start 🖉 👘 Ketwork Connections	Diric Adress	t-[DHS]15WID	

7. 輸入使用者端的名稱(在此案例中為WLC),並輸入WLC的IP位址。按「**Next**」(下一步)。

Type a friendly name and e	either an IP Address or DNS n	ame for the client.
Eriendly name:	WLC	
Client address (IP or DNS):	:	
10.77.244.210		⊻erify

8. 在下一頁的Client-Vendor下,選擇**RADIUS Standard**;輸入共用金鑰;然後點選**Finish**。 9. 請注意,WLC作為AAA客戶端新增到IAS中。

🖓 Internet Authentication Service			「自然を長く		그리프
Elle girtion Yern Help					Oese
◆ → 1 1 1 1 1 1 1					
Internet Authentication Service (Local)	Priendly Name /	Address	Protocol	Client/Vendor	
Internet Authentication Service (Local) Reguest Sciences Periode Access Logging Periode Access Policies Connection Request Processing	Triendy Name /	863103	Protocol RADIUS	Clerd Wendor RADRUS Standard	
Present A	[Dava	1 A doore	of - IDM215WD	The Internet Authority at	
			Personal and and	II . manuel manonecore	

- 10. 為客戶端建立遠端訪問策略。
- 11. <u>為</u>此,請按一下右鍵**遠端訪問策略**,然後選擇**新建遠端訪問策略**。

🐓 Internet Authent	ication Service				
Elle girtion View	HMp				
+ + 🗈 🗉 (3 R 😥 🖪				
Prismet Aufhetik Boger Access Prismet Aufhetik Boger Access Prismet Access Connection Ba	Image: Service (Local) Logging March Remate Access Bolicy Strin Strin	Connections to Morocoft Rev Connections to other access	Order drag and Resolute t arrver: 2		
a. 11 a		1.0	()		
a start 2	Retwork Connections	The	Tarandar - (nex) towns	P Internet Authoriticali.	• • • • • • • • • • • • • • • • • • •

12. 鍵入遠端訪問策略的名稱。在本示例中,使用名稱PEAP。然後點選下一步。

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

13. 根據您的需求選擇策略屬性。在本例中,選擇Wireless。

Kemote Access Policy mizara	
Access Method Policy conditions are based on the meth	iod used to gain access to the network.
Select the method of access for which you	u want to create a policy.
Use for all VPN connections. To cre previous page, and select Set up a	eate a policy for a specific VPN type, go back to the custom policy.
C <u>D</u> ial-up	
Use for dial-up connections that use Digital Network (ISDN) line.	e a traditional phone line or an Integrated Services
Wireless	
Use for wireless LAN connections of	only.
C Ethernet	
Use for Ethernet connections, such	as connections that use a switch.

14. 在下一頁上,選擇**User**,將此遠端訪問策略應用到使用者清單。

w Remote Access Policy Wizard	
User or Group Access You can grant access to individual users, or you can grant access to select groups.	ed 🕅
Grant access based on the following:	
 User User access permissions are specified in the user account. 	
 <u>Group</u> Individual user permissions override group permissions. Group name: 	
	A <u>d</u> d
	<u>R</u> emove
Z Baale Maria	Comort
< <u>Dack</u> <u>INext</u> >	

15. 在Authentication Methods下,選擇**Protected EAP(PEAP)**,然後按一下**Configure**。

New Remote Access Policy Wizard			×
Authentication Methods EAP uses different types of security devices t	o authenticate user	S.	Ŷ
Select the EAP type for this policy.			
<u>T</u> ype:			
Protected EAP (PEAP)		•	Configure
	< <u>B</u> ack	<u>N</u> ext >	Cancel

16. 在**Protected EAP Properties**頁面上,從Certificate Issued下拉選單中選擇適當的證書,然後 按一下**OK**。

Protected EAP Propertie	es	<u>? ×</u>
This server identifies itsel Select the certificate that	f to callers before the connection is comple you want it to use as proof of identity.	ted.
Certificate issued	tsweb-lapt.Wireless.com	
Friendly name:	PEAP-Wireless	
Issuer:	Wireless-CA	
Expiration date:	12/16/2008 5:53:02 PM	
🔲 Enable Fast Reconner	ct	
E <u>a</u> p Types		
Secured password (EAP-	MSCHAP v2)	Move Up
		Move <u>D</u> own
	it <u>R</u> emove OK	Cancel

17. 驗證遠端訪問策略的詳細資訊,然後按一下**Finish**。

New Remote Access Policy W	'izard	×
S	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 Finish Cancel	

18. 遠端訪問策略已新增到清單中。



19. 按一下右鍵該策略,然後按一下**Properties**。在「如果連**接請求與指定**條件匹配**」下選擇「授 予遠端訪問許可權**」。

AF Fropercies				? >
Settings				
Specify the cond	itions that conne	ction request	ts must match.	
Policy conditions	:			
NAS-Port-Type	matches "Wirele:	ss - Other OR	Wireless - IEE	EE 802.11"
•				F
Add	Edit	Remove	,	
If connection red	uests match the	conditions sr	ecified in this	nolicu the
associated profile	will be applied t	o the connec	stion.	
Edit Profile				
Edit Profile	access permissio	ons are speci	ified in the use	r profile, this
Edit <u>Profile</u> Unless individual policy controls ad	access permissio cess to the netw	ons are speci Jork.	ified in the use	r profile, this
Edit Profile Unless individual policy controls ad	access permissi cess to the netw quest matches t	ons are speci vork. he specified	ified in the use conditions:	r profile, this
Edit Profile Unless individual policy controls ad If a connection re O Deny remote	access permission cess to the netwo equest matches t access permission	ons are speci vork. he specified on	ified in the use conditions:	r profile, this
Edit Profile Unless individual policy controls ad If a connection re O Deny remote O Grant remote	access permission cess to the netwo equest matches t access permission access permission	ons are speci vork. he specified on	ified in the use conditions:	r profile, this
Edit Profile Unless individual policy controls ad If a connection re Deny remote Grant remote	access permissi cess to the netw equest matches t access permissio access permissio	ons are spec vork. he specified on on	ified in the use	r profile, this

將使用者新增到Active Directory

在此設定中,使用者資料庫在Active Directory上維護。

若要將使用者新增到Active Directory資料庫,請完成以下步驟:

1. 在「Active Directory使用者和電腦」控制檯樹中,按一下右鍵**使用者**;按一下**新建**;然後按一 下**使用者**。



2. 在「新建對象 — 使用者」對話方塊中,鍵入無線使用者的名稱。此示例在「名字」欄位中使 用名稱WirelessUser,在「使用者登入名」欄位中使用名稱WirelessUser。按「Next」(下一

-	Crow 4			
First name:	Ulient 1		Initials:	
Last name:				
Full name:	Client 1			
	,			
User logon name Client1		@Wirele	ess.com	-
User logon name	: (pre-Windows	@Wirele	ess.com	•

3. 在「新建對象 — 使用者」對話方塊中,在「密碼」和「確認密碼」欄位中鍵入您選擇的密碼 。清除User must change password at next logon覈取方塊,然後按一下Next。

步)

Passwor	d:	••••	••••		
<u>C</u> onfirm (password:	••••	••••		
🗖 User	must change	password at	next logon		
🔲 U <u>s</u> er	cannot chan	ge password			
Pass	word never e	xpires			
	junt is disable	a			
					1
			< <u>B</u> ack	<u>N</u> ext>	Cance
新建對象	录 — 使用者 _	」對話方塊「	中,按一下 完成	0	
新建對創 v Object	象 — 使用者 ₋ : - User	」對話方塊「	中,按一下 完成	•	
新建對象 v Object	象 — 使用者. - User Create in:	」對話方塊 Wireless.cr	中,按一下 完成 om/Users	ō	
新建對氰 v Object	象 — 使用者. : - User Create in: ou click Finish	」對話方塊(Wireless.co , the following	中,按一下 完成 om/Users g object will be cr	° eated:	
新建對氢 v Object	象 — 使用者. : - User Create in: pu click Finish ie: Client 1	」對話方塊(Wireless.co , the following	中,按一下 完成 om/Users g object will be cr	° eated:	
新建對 Object When you Full nam User log	象 — 使用者. - User Create in: ou click Finish ie: Client 1 jon name: Clie	」對話方塊 Wireless.co , the following :nt1@Wireles	中,按一下 完成 om/Users g object will be cr ss.com	• eated:	
新建對 Object When yo Full nam User log	象 — 使用者. - User Create in: bu click Finish he: Client 1 jon name: Clie	」對話方塊(Wireless.co , the following ent1@Wireles	中,按一下 完成 om/Users g object will be cr ss.com	• eated:	
新建對新 Object When you Full nam User log	象 — 使用者. - User Create in: ou click Finish ie: Client 1 jon name: Clie	」對話方塊(Wireless.co , the following ent1@Wireles	中,按一下 完成 om/Users g object will be cr ss.com	∘ eated:	

5. 重複步驟2至4以建立其他使用者帳戶。

<u>允許對使用者進行無線訪問</u>

請完成以下步驟:

- 1. 在Active Directory使用者和電腦控制檯樹中,按一下**Users**資料夾;按一下右鍵 **WirelessUser**;單擊**Properties**;然後轉到Dial-in頁籤。
- 2. 選擇Allow access,然後按一下OK。

Client 1 Properties	×
Remote controlTerminal Services ProfileCOM+GeneralAddressAccountProfileTelephonesOrganizationMember OfDial-inEnvironmentSessions	
Remote Access Permission (Dial-in or VPN)	
© Deny access	
C Control access through Remote Access <u>Policy</u>	
Callback Options	
No <u>C</u> allback	
Set by Caller (Routing and Remote Access Service only)	
C Always Callback to:	
Assign a Static IP Address	
Apply Static Boutes	
Define routes to enable for this Dial-in Static Routes	
UK Cancel <u>Apply</u>	

配置無線區域網控制器和輕量AP

現在為此設定配置無線裝置。其中包括無線LAN控制器、輕量AP和無線客戶端的配置。

通過MS IAS RADIUS伺服器配置WLC進行RADIUS身份驗證

首先配置WLC以使用MS IAS作為身份驗證伺服器。需要設定WLC,才能將使用者認證轉送到外部

RADIUS伺服器。外部RADIUS伺服器接著驗證使用者認證並提供對無線使用者端的存取許可權。為此,請在Security > RADIUS Authentication頁中將MS IAS伺服器新增為RADIUS伺服器。

請完成以下步驟:

1. 從控制器GUI中選擇**Security**和**RADIUS Authentication**,以顯示「RADIUS Authentication Servers」頁面。然後按一下**New**以定義RADIUS伺服器。

ICO SPOTENO					Save C	onfiguration Ping	Logout
A. A.	MONITOR WLANS CONTR	OLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
ecurity	RADIUS Authentication Ser	vers > New				< Back	App
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 💌					
AP Policies	Shared Secret	•••••					
Access Control Lists	Confirm Shared Secret	•••••					
ID Certificate	Key Wrap						
Web Auth Certificate		(manual)					
Wireless Protection Policies Trusted AP Policies	Server Status	1812 Enabled					
Rogue Policies Standard Signatures Custom Signatures Client Exclusion Policies	Support for RFC 3576	Enabled 💌					
AP Authentication	Retransmit Timeout	2 seconds					
	Network User	Enable					
	Management	Enable					
	IPSec	🔝 Enable					

 在RADIUS Authentication Servers > New 頁中定義RADIUS伺服器引數。這些引數包括 RADIUS伺服器IP地址、共用金鑰、埠號和伺服器狀態。Network User和Management覈取方 塊確定基於RADIUS的身份驗證是否適用於管理和網路使用者。此示例使用MS IAS作為IP地址 為10.77.244.198的RADIUS伺服器。

ises Spectrum	MONITOR	WLANS O	ONTROLLER	WIRELESS 5	ECURITY	MANAGEMENT CC	Save Configurat MMANDS HELP	ion Ping Logo	jt R€
Security	RADIUS A	uthenticatio	n Servers					Apply New	
AA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	Call Stati Credentia Use AES Network	on ID Type als Caching Key Wrap	IP Address	Server Address	Port	IPSec	Admin Statu		
ccess Control Lists	User		Index					-	-
PSec Certificates CA Certificate ID Certificate	M	M	1	10.77.244.198	1812	Disabled	Enabled	Edt Remove	Pina
Veb Auth Certificate									
Vireless Protection volicies Trusted AP Policies Rogue Policies Standard Signatures Custom Signatures Client Exclusion Policies AP Authentication									

3. 按一下「Apply」。

4. MS IAS伺服器已作為Radius伺服器新增到WLC,可用於驗證無線客戶端。

<u>為客戶端配置WLAN</u>

配置無線客戶端連線的SSID(WLAN)。在本示例中,建立SSID並將其命名為PEAP。

將第2層身份驗證定義為WPA2,以便客戶端執行基於EAP的身份驗證(本例中為PEAP-MSCHAPv2)並使用AES作為加密機制。將所有其他值保留為預設值。

注意:本檔案將WLAN與管理介面繫結。當網路中有多個VLAN時,您可以建立一個單獨的VLAN並 將其繫結到SSID。有關如何在WLC上設定VLAN的資訊,請參閱<u>無線LAN控制器上的VLAN組態範</u> <u>例</u>。

若要在WLC上設定WLAN,請完成以下步驟:

- 1. 從控制器的GUI中按一下「**WLANs**」,以顯示「WLANs」頁面。此頁面列出控制器上存在的 WLAN。
- 2. 選擇New以建立一個新的WLAN。輸入WLAN的WLAN ID和WLAN SSID,然後按一下Apply。

3 · 0 · E	6 P 🛠 🛛	3· 🕹 🖂 🦓					🥂 – 8 ×
Cisco Sestems					Save C	onfiguration Ping	Logout Refresh
Alexandra	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
WLANS	WLANs > New					< Back	Apply
WLANS WLANS	WLAN ID	1					
AP Groups VLAN	WLAN SSID	PEAP					

3. 建立新的WLAN後,系統會顯示新WLAN的**WLAN > Edit**頁面。在此頁面上,您可以定義特定 於此WLAN的各種引數,包括一般策略、RADIUS伺服器、安全策略和802.1x引數。

CIRCO STATENO					Save Go	infiguration Pini	g Logout Kerry
de de	MONITOR WLANS	CONTROLLER WIRE	LESS SECURITY	MANAGEMENT	COMMANDS	HELP	
WLANs	WLANs > Edit					< Back	Apply
WLANS	WLAN ID	1					
WLANS AP Groups VLAN	Profile Name	PEAP					
	WLAN SSID	PEAP					
	General Policies				Security Polic	ies	
	Radio Policy	All			IPv6 Enable		
	Admin Status	R Enabled					
	Session Timeout (s	ecs) 0			Layer 2 Securi	ty WPA1+V	NPA2
	Quality of Service	(QoS) Silver (best effort)) Silver (best effort)			□ MAC P	Rering
	WMM Policy	Disabled 💌			Layer 3 Securi	ty None	1
	7920 Phone Suppo	rt 🗌 Client CAC Limit	AP CAC Limit			Web Pr	olicy *
	Broadcast SSID	Enabled					
	Aironet IE	P Enabled	Enabled				
	Allow AAA Override	Enabled				* Web Policy cannot be used in combination w IPsec.	
	Client Exclusion	Enabled ** 60	and the formal		** When client	exclusion is enabl	led, a timeout
	DHCP Server	⊡0verride	cout Value (secs)		value of zero n administrative	neans infinity(will override to reset (require excluded clients)
	DHCP Addr. Assign	ment ERequired			*** CKIP is no	t supported by 10	xx APs
	Interface Name	management 💌					
	MFP Version Requir	red 1					
	MFP Signature Generation	Global MFP Dist	(beld				
	H-REAP Local Switz	hing 🗖					
	* H-REAP Local Sw authentications.	itching not supported with I	PSEC, CRANITE and	FORTRESS			

4. 檢查General Policies底下的Admin Status,以啟用WLAN。如果您希望AP在其信標幀中廣播 SSID,請選中Broadcast SSID。 5. 在Layer 2 Security下,選擇WPA1+WPA2。這會在WLAN上啟用WPA。向下滾動頁面並選擇 WPA策略。此示例使用WPA2和AES加密。從RADIUS Servers下的下拉選單中選擇適當的 RADIUS伺服器。在本示例中,使用10.77.244.198(MS IAS伺服器的IP地址)。其它引數可 以根據WLAN網路的要求進行修改。

	Gince Statem							Save Co	onfiguration Ping	Logout Refresh
	And	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
	WLANS	WPA1+W Paramete	PA2			_				*
	WLANS WLANS AP Groups VLAN	WPA1 Po WPA2 Po WPA2 En Auth Key	icy icy cryption Mgmt	₩ ₩ AES 802.1×	Пткјр					
_		10	*							
6.	按一ト「Apply」	0						Save C	onhauration Rina	Lonout Refresh
		MONITOR	MR ANE	CONTROLLER	WIDELECC	SECI PITY	MANAGEMENT	COMMANDS		Luguar Herress
	WLANs	WLANS								
	WLANS WLANS	Profile Na	inte	W	MAN WLAN S	SID	Adr Sta	nin Secur tus	ity Policies	
	AP Groups VLAN	PEAP		1	PEAP		Ena	bled [WPA	2][Auth(802.1×)]	Edit Rem
		* WLAN ID:	: 9-16 wil I	not be pushed to 1	1130,1200 and	1240 AP mode	k.			



為PEAP-MS CHAPv2身份驗證配置無線客戶端

本示例提供有關如何使用Cisco Aironet Desktop Utility配置無線客戶端的資訊。配置客戶端介面卡 之前,請確保使用韌體和實用程式的最新版本。在Cisco.com上的Wireless downloads(無線下載)頁面中查詢韌體和實用程式的最新版本。

要使用ADU配置Cisco Aironet 802.11 a/b/g無線客戶端介面卡,請完成以下步驟:

- 1. 開啟Aironet案頭實用程式。
- 2. 按一下Profile Management, 然後按一下New以定義配置檔案。
- 3. 在「General(常規)」頁籤下,輸入配置檔名稱和SSID。在本範例中,使用您在WLC(PEAP)上設定的SSID。

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

4. 選擇「安全」頁籤;選擇**WPA/WPA2/CCKM**;在「WPA/WPA2/CCKM EAP」下,鍵入**PEAP** [EAP-MSCHAPv2],然後按一下「配置」。

Profile Management		? 🗙
General Security Advanced		
Set Security Options		x
⊙ wPa/wPa2/CCKM	WPA/WPA2/CCKM EAP Type: PEAP (EAP-MSCHAP V2)	✓
○ WPA/WPA2 Passphrase		
O 802.1x	802.1× EAP Type: EAP-FAST	
Pre-Shared Key (Static WEP)		
○ None		
Configure	Allow Association to Mixed Cells Profile Locked	
	Limit Time for Finding Domain Controller To: 0 sec	
Group Policy Delay:	60 🗢 sec	
	OK	Cancel

5. 選擇Validate Server Certificate,然後在Trusted Root Certificate Authorities下拉選單中選擇 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:	
🔘 Certificate	
 User Name and Password 	
Select a Certificate	
☑ Use Windows User Name and Password	
User Information for PEAP (EAP-MSCHAP V2) Authentication	
User Name: Administrator	
Password	
Confirm Password:	
Advanced. OK Cancel	

6. 按一下OK,然後啟用配置檔案。注意:在Microsoft XP SP2中使用受保護的EAP-Microsoft質 詢握手身份驗證協定版本2(PEAP-MSCHAPv2)時,無線卡由Microsoft無線零配置(WZC)管理 ,必須應用Microsoft修補程式KB885453。這可防止與PEAP快速恢復相關的身份驗證出現多 個問題。

驗證和疑難排解

為了驗證配置是否按預期工作,請在無線客戶端Client1上啟用配置檔案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

一旦在ADU上啟用配置檔案PEAP-MSCHAPv2,客戶端將執行802.11開放式身份驗證,然後執行 PEAP-MSCHAPv2身份驗證。以下是成功的PEAP-MSCHAPv2身份驗證的示例。

使用debug命令瞭解發生的事件的順序。

<u>輸出直譯器工具</u>(僅供<u>已註冊</u>客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析 。

無線LAN控制器上的以下debug命令很有用。

- debug dot1x events enable 用於配置802.1x事件的調試
- debug aaa events enable 要配置AAA事件的調試
- debug mac addr <mac address> 要配置MAC調試,請使用debug mac命令
- debug dhcp message enable 要配置DHCP錯誤消息的調試

以下是debug dot1x events enable命令和debug client <mac address> 命令的示例輸出。

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 Address>:

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 = 0x00000000, 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客戶端通過Cisco Secure ACS進行PEAP身份驗證,則客戶端 可能無法成功進行身份驗證。有時,初始連線可以成功進行身份驗證,但隨後的快速連線身份驗證 嘗試無法成功連線。這是一個已知問題。此問題的詳細資訊和解決方法可從此處獲<u>取</u>。

<u>相關資訊</u>

- 採用ACS 4.0和Windows 2003的統一無線網路下的PEAP
- 使用WLAN控制器(WLC)的EAP驗證組態範例
- •無線區域網路控制器(WLC)軟體升級到3.2、4.0和4.1版
- Cisco 4400系列無線LAN控制器組態設定指南
- 技術支援與文件 Cisco Systems

關於此翻譯

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