PEAP sous des réseaux sans fil unifiés avec Microsoft Internet Authentication Service (IAS)

Table des matières

Introduction Conditions préalables Exigences Composants utilisés **Conventions** Présentation de PEAP Configurer Diagramme du réseau Configurations Configurez le serveur de Microsoft Windows 2003 Configurez le serveur de Microsoft Windows 2003 Installez et configurez les services DHCP sur le serveur de Microsoft Windows 2003 Installez et configurez le serveur de Microsoft Windows 2003 en tant que serveur d'Autorité de certification (CA) Connectez les clients de routage au domaine de routage Installez le service d'authentification Internet sur le serveur de Microsoft Windows 2003 et demandez un certificat Configurez le service d'authentification Internet pour l'authentification PEAP-MS-CHAP v2 Ajoutez les utilisateurs à l'Active Directory Permettez l'accès sans fil aux utilisateurs Configurez le contrôleur LAN sans fil et les AP légers Configurez le WLC pour l'authentification RADIUS par le serveur RADIUS de MS IAS Configurez un WLAN pour les clients de routage Configurez les clients sans fil Configurez les clients sans fil pour l'authentification PEAP-MS CHAPv2 Vérifiez et dépannez Informations connexes

Introduction

Ce document fournit un exemple de configuration pour installer Protected Extensible Authentication Protocol (PEAP) avec l'authentification de Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) version 2 dans un réseau sans fil unifié Cisco avec le service d'authentification de routage Internet de Microsoft (IAS) en tant que serveur RADIUS.

Conditions préalables

Exigences

Il existe la supposition que le lecteur a connaissance de l'installation de base de Windows 2003 et de l'installation du contrôleur de routage Cisco puisque ce document couvre seulement les configurations spécifiques pour faciliter les tests.

Remarque : ce document est destiné à donner aux lecteurs un exemple sur la configuration requise sur le serveur MS pour l'authentification PEAP - MS CHAP. La configuration du serveur de Microsoft présentée dans cette section a été testée dans le laboratoire et s'est avérée fonctionner comme prévu. Si vous avez des problèmes pour configurer le serveur de Microsoft, contactez Microsoft pour obtenir de l'aide. TAC de Cisco ne prend pas en charge la configuration du serveur de Microsoft Windows.

Pour obtenir des informations sur l'installation et la configuration initiales des contrôleurs de la gamme Cisco 4400, reportez-vous au <u>Guide de démarrage rapide : Contrôleurs LAN sans fil de la gamme Cisco 4400</u>.

Les guides d'installation et de configuration de Microsoft Windows 2003 peuvent être trouvés sous Installer Windows Server 2003 R2.

Avant de commencer, installez Microsoft Windows Server 2003 avec le système d'exploitation SP sur chacun des serveurs dans le laboratoire de test et mettez à jour tous les Services Pack. Installez les contrôleurs et les points d'accès léger (LAP) et assurez-vous que les dernières mises à jour logicielles sont configurées.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Contrôleur Cisco de la gamme 4400 qui exécute la version 4.0 du microprogramme
- Protocole de point d'accès léger Cisco 1131 (LWAPP) AP
- Serveur Windows 2003 Enterprise (SP1) avec le service d'authentification Internet (IAS), l'autorité de certification (CA), DHCP et les services de système de noms de domaine (DNS) installés
- Windows XP Professional avec SP2 (et les Services Pack mis à jour) et la carte réseau sans fil Cisco Aironet 802.11a/b/g (NIC)
- Utilitaire de bureau Aironet version 4.0
- Commutateur du routage Cisco 3560

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux <u>Conventions relatives aux conseils techniques Cisco.</u>

Présentation de PEAP

PEAP utilise Transport Level Security (TLS) pour créer un canal chiffré crypté entre un client de routage authentifiant PEAP, tel qu'un ordinateur portable sans fil, et un authentificateur PEAP, tel que le Service d'authentification Internet de Microsoft (IAS) ou n'importe quel serveur RADIUS. PEAP ne spécifie pas de méthode d'authentication, mais fournit la sécurité supplémentaire pour d'autres protocoles d'authentification EAP, tels qu'EAP-MSCHAPv2, qui peut fonctionner par le canal crypté par TLS fourni par PEAP. Le processus d'authentification PEAP consiste en deux phases principales :

PEAP phase un : canal chiffré TLS

Le client sans fil s'associe avec l'AP. Une association basée sur IEEE 802.11 fournit un système ouvert ou l'authentification de clé partagée avant qu'une association sécurisée soit créée entre le client de routage et le point d'accès (LAP). Après que l'association basée sur IEEE 802.11 est établie avec succès entre le client de routage et le point d'accès, la session de TLS est négociée avec l'AP. Une fois que l'authentification a abouti avec succès entre le client sans fil et le serveur IAS, la session de TLS est négociée entre eux. La clé qui dérive de cette négociation est utilisée pour crypter toute la communication ultérieure.

Deuxième phase PEAP : communication authentifiée par EAP

La communication d'EAP, qui inclut la négociation d'EAP, se produit à l'intérieur du canal de TLS créé par PEAP dans la première phase du processus d'authentification de PEAP. Le serveur d'IAS authentifie le client sans fil avec EAP-MS-CHAP v2. Le LAP et le contrôleur réachemine seulement les messages entre le client sans fil et le serveur RADIUS. Le WLC et le LAP ne peuvent pas déchiffrer ces messages parce que ce n'est pas le point d'extrémité de TLS.

Une fois que la première phase de PEAP a lieu et que le canal TLS est créé entre le serveur IAS et le client sans fil de 802.1x, pour une tentative réussie d'authentification où l'utilisateur a fourni les identifiants basés sur un mot de passe valide avec PEAP-MS-CHAP v2, l'ordre de message RADIUS est le suivant :

- 1. Le serveur IAS envoie un message de demande d'identité au client : EAP-Request/Identity.
- 2. Le client répond avec un message de réponse d'identité : EAP-Response/Identity.
- 3. Le serveur IAS envoie un message de demande de confirmation MS-CHAP v2 : EAP-Request/EAP-Type=EAP MS-CHAP-V2 (demande).
- 4. Le client répond par un challenge et une réponse MS-CHAP v2 : EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Response).
- 5. Le serveur IAS renvoie un paquet de réussite MS-CHAP v2 lorsque le serveur a correctement authentifié le client : EAP-Request/EAP-Type=EAP-MS-CHAP-V2 (Success).
- 6. Le client répond avec un paquet de réussite MS-CHAP v2 lorsque le client a authentifié avec succès le serveur : EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Success).
- 7. Le serveur d'IAS envoie un EAP-TLV qui indique l'authentification réussie.
- 8. Le client répond avec un message de réussite d'état EAP-TLV.
- 9. Le serveur complète l'authentification et envoie un message de réussite-EAP du texte en clair. Si des VLAN sont déployés pour l'isolation du client, les attributs VLAN sont inclus dans ce message.

<u>Configurer</u>

Ce document fournit un exemple pour la configuration de PEAP MS-CHAP v2.

Remarque : utilisez l'<u>outil de recherche de commandes</u> (clients <u>enregistrés</u> uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Dans cette configuration, un serveur de Microsoft Windows 2003 effectue ces rôles :

- Contrôleur de domaine pour le domaine de routage Wireless.com
- Serveur DHCP/DNS
- Serveur d'Autorité de certification (CA)
- Active Directory pour mettre à jour la base de données utilisateur
- Service d'authentification Internet (IAS) pour authentifier les utilisateurs sans fil

Ce serveur se connecte au réseau câblé par un commutateur de la couche 2 comme montré.

Le contrôleur LAN sans fil (WLC) et le LAP enregistré se connectent également au réseau par le commutateur de la couche 2.

Les clients sans fil C1 et C2 emploieront le Wi-Fi Protected Access 2 (WPA2) - authentification PEAP MSCHAP v2 pour se connecter au réseau sans fil.

L'objectif est de configurer le serveur de Microsoft 2003, le contrôleur LAN sans fil et le poids léger AP pour authentifier les clients sans fil avec l'authentification PEAP MSCHAP v2.

La section suivante explique comment paramétrer les périphériques pour cette configuration.

Configurations

Cette section traite de la configuration requise pour installer l'authentification PEAP MS-CHAP v2 dans ce WLAN :

- Configurez le serveur de Microsoft Windows 2003
- Configurer le contrôleur LAN sans fil (WLC) et les AP de poids léger
- Configurez les clients sans fil

Commencez par la configuration du serveur de Microsoft Windows 2003.

Configurez le serveur de Microsoft Windows 2003

Configurez le serveur de Microsoft Windows 2003

Comme mentionné dans la section de configuration réseau, utilisez le serveur de Microsoft Windows 2003 dans le réseau pour remplir ces fonctions.

- Contrôleur de domaine pour le domaine sans fil
- Serveur DHCP/DNS
- Serveur d'Autorité de certification (CA)
- Service d'authentification Internet (IAS) pour authentifier les utilisateurs sans fil
- Active Directory pour mettre à jour la base de données utilisateur

Configurez le serveur de Microsoft Windows 2003 pour ces services. Commencez par la configuration du serveur de Microsoft Windows 2003 comme contrôleur de domaine.

Configurez le serveur de Microsoft Windows 2003 comme contrôleur de domaine

Afin de configurer le serveur de Microsoft Windows 2003 comme contrôleur de domaine, suivez ces étapes :

 Cliquez sur Start, cliquez sur Run, saisissez dcpromo.exe, puis cliquez sur OK pour démarrer l'assistant d'installation d'Active Directory.



2. Cliquer sur Next to exécute l'assistant d'installation d'Active Directory.

ictive I	Directory Installation Wizard
Ope	erating 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> .
	< <u>B</u> ack <u>Next</u> > Cancel

3. Afin de créer un nouveau domaine, choisissez l'option **Contrôleur de domaine pour un nouveau domaine.**

omain 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 al domain controller for an existing domain?
• Dor	nain 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.
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. Cliquer sur Next to crée une nouvelle forêt d'arborescences de domaine.

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

 Si DNS n'est pas installé dans le système, l'assistant vous fournit des options avec lesquelles configurer DNS. Choisissez No, Just Install and Configure DNS sur cet ordinateur. Cliquez sur Next (Suivant).

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

6. Introduisez le nom DNS complet pour le nouveau domaine de routage. Dans cet exemple Wireless.com est utilisé, puis cliquez sur Next.

ve Directory Installation Wizard			
New Domain Name Specify a name for the new domain.			Se al an
Type the full DNS name for the new do (for example: headquarters.example.mi	main crosoft.com).		
Full DNS name for new domain:			
Wireless.com			
	< Back	Nevts	Cancel

 Écrivez le nom NetBIOS pour le domaine de routage, puis cliquez sur Next. Cet exemple utilise WIRELESS.

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

8. Choisissez la base de données et consignez les emplacements pour le domaine. Cliquez sur Next

(Suivant).

Directory Installation Wizaru			
t abase and Log Folders Specify the folders to contain the Active	Directory database	and log files.	410
For best performance and recoverability, hard disks.	, store the database a	and the log on sep	arate
Where do you want to store the Active [Directory database?		
Database folder:			
C:\WINDOWS\NTDS		Bīo	wse
Where do you want to store the Active [Log folder:	Directory log?		
		Did anonymeter	and a second second

9. Choisissez un emplacement pour le répertoire de Sysvol. Cliquez sur **Next** (Suivant).

stem volume.		A
opy of the domain's I domain controllers	public files. The in the domain.	contents
an NTFS volume.		
	В	Iomse
< <u>B</u> ack	<u>N</u> ext>	Cancel
	opy of the domain's I domain controllers i an NTFS volume. ∠ Back	opy of the domain's public files. The I domain controllers in the domain. an NTFS volume.

10. Choisissez les autorisations par défaut pour les utilisateurs et les groupes. Cliquez sur **Next** (Suivant).

ive Di	rectory Installation Wizard
Permi Se	ssions elect default permissions for user and group objects.
So	ome server programs, such as Windows NT Remote Access Service, read information pred on domain controllers.
G	Permissions compatible with pre-Windows 2000 server operating systems Select this option if you run server programs on pre-Windows 2000 server operating systems or on Windows 2000 or Windows Server 2003 operating systems that are members of pre-Windows 2000 domains.
c	Anonymous users can read information on this domain.
	operating systems Select this option if you run server programs only on Windows 2000 or Windows Server 2003 operating systems that are members of Active Directory domains. Only authenticated users can read information on this domain.
	< <u>B</u> ack <u>N</u> ext > Cancel

11. Définissez le mot de passe administrateur, puis cliquez sur **Next**.

Active Directory Installation Wizard
Directory Services Restore Mode Administrator Password This password is used when you start the computer in Directory Services Restore Mode.
Type and confirm the password you want to assign to the Administrator account used when this server is started in Directory Services Restore Mode.
The restore mode Administrator account is different from the domain Administrator account. The passwords for the accounts might be different, so be sure to remember both.
Restore Mode Password:
Confirm password:
For more information about Directory Services Restore Mode, see <u>Active Directory Help</u> .
< <u>B</u> ack <u>N</u> ext > Cancel

12. Cliquer sur Next pour confirmer les options de domaine définies précédemment.

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	
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 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 NetBIOS name of the domain is WIRELESS Database folder: C:\WINDOWS\NTDS Log file folder: C:\WINDOWS\NTDS SYSVOL folder: C:\WINDOWS\SYSVOL	
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 o the administrator of this computer.	
	~
To change an option, click Back. To begin the operation, click Next.	

13. Cliquez sur Finish pour fermer l'assistant d'installation d'Active Directory.



14. Redémarrez le serveur pour que les modifications prennent

Activ	e Directory Installation W	lizard	
Wir	ndows must be restarted before	the changes made by the Activ	e
Dire	ctory Installation wizard take e	lfect.	
		D. I.D. J. J.	
	<u>Bestart Now</u>	Don't Restart Now	

Au cours de cette étape, vous avez configuré le serveur de Microsoft Windows 2003 comme contrôleur de domaine et avez créé un nouveau domaine de routage **Wireless.com**. Configurez ensuite les services DHCP sur le serveur.

Installez et configurez les services DHCP sur le serveur de Microsoft Windows 2003

Le service DHCP sur le serveur de Microsoft 2003 est utilisé pour fournir des adresses IP aux clients sans fil. Afin d'installer et de configurer des services DHCP sur ce serveur, suivez ces étapes :

- 1. Cliquez sur Add or Remove Programs dans le panneau de configuration.
- 2. Cliquez sur Add/Remove Windows Components.
- 3. Choisissez Networking Services, puis cliquez sur Details.
- 4. Choisissez Dynamic Host Configuration Protocol (DHCP), puis cliquez sur

Networking Services	
To add or remove a component, click the c of the component will be installed. To see w	heck box. A shaded box means that only par what's included in a component, click Details.
Sub <u>c</u> omponents of Networking Services:	
🗹 📇 Domain Name System (DNS)	1.7 MB 🔄
🔽 县 Dynamic Host Configuration Protoc	ol (DHCP) 0.0 MB
🗌 🔲 🌉 Internet Authentication Service	0.0 MB
🗌 🗔 🚚 Remote Access Quarantine Service	e 0.1 MB
🔲 🔜 RPC over HTTP Proxy	0.0 MB
🗌 🗐 Simple TCP/IP Services	0.0 MB
🔲 🗆 🚚 Windows Internet Name Service (W	VINS) 0.9 MB 📘
Description: Sets up a DHCP server that addresses to client computer	automatically assigns temporary IP rs on the same network.
Total disk space required: 3.4 ME	3 Details
Space available on disk: 7224.5 ME	B Contraction
	OK Cancel

5. Cliquer sur **Next pour installer le service DHCP.**

indows Components You can add or remove components of Windows.	Ĩ
To add or remove a component, click the checkbox. A shaded box part of the component will be installed. To see what's included in a Details.	means that only component, click
<u>C</u> omponents:	
🗌 🗔 🥶 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
I 🗆 📾 Bemote Storage	42MB
Description: Contains a variety of specialized, network-related servi	ces and protocols.
Total disk space required: 3.4 MB	Dataila
Space available on disk: 7212.1 MB	

6. Cliquez sur Finish pour terminer l'installation.

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

- 7. Afin de configurer des services DHCP, cliquez sur Start > Programs > Administrative tools , puis cliquez sur le jeu d'outils DHCP.
- 8. Choisissez le serveur DHCP tsweb-lapt.wireless.com (dans cet exemple).
- 9. Cliquez sur Action, puis cliquez sur Authorize pour autoriser le service DHCP.



- 10. Dans l'arborescence de la console, cliquez à droite sur **tsweb-lapt.wireless.com, puis** cliquez sur New Scope pour définir une plage d'adresses IP pour les clients sans fil.
- 11. Sur la page de bienvenue de l'assistant de New Scope, cliquez sur **Next**.



12. Àla page du nom de portée, saisissez le nom de la portée DHCP. Dans cet exemple, utilisez **DHCP-Clients comme nom de portée.** Cliquez sur **Next**

ant). Scope Wizard	
icope Wizard Cope Name You have to pr providing a des	ovide an identifying scope name. You also have the option of scription.
Type a name a how the scope	nd description for this scope. This information helps you quickly identify 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

 Àla page de plage d'adresses IP, saisissez les adresses IP de début et de fin pour la portée, puis cliquez sur Next.

New Scope Wizard	
IP Address Range You define the scop addresses.	e address range by identifying a set of consecutive IP
Enter the range of a	ddresses that the scope distributes.
<u>S</u> tart IP address:	10 . 77 . 244 . 218
End IP address:	10 . 77 . 244 . 219
A subnet mask defin IDs and how many b length or as an IP ac Length:	es how many bits of an IP address to use for the network/subnet its to use for the host ID. You can specify the subnet mask by ddress. 8
S <u>u</u> bnet mask:	255.0.0.0
	< <u>B</u> ack <u>N</u> ext > Cancel

14. Sur la page d'ajout des exclusions, mentionnez l'adresse IP que vous voudriez réserver/exclure de la portée DHCP. Cliquez sur **Next** (Suivant).

Type the IP address r address, type an add	ange that you want to exclu ress in Start IP address only.	ide. If you want to exclude a single
<u>S</u> tart IP address:	End IP address:	
.		Add
Excluded address ran	ige:	
		Remo <u>v</u> e

15. Mentionnez la durée de bail dans la page de durée de bail, puis cliquez sur **Next**.

ew Scope Wizard	
Lease Duration The lease duration specifies how long a clie scope.	nt can use an IP address from this
Lease durations should typically be equal to connected to the same physical network. Fo portable computers or dial-up clients, shorter Likewise, for a stable network that consists r locations, longer lease durations are more ap Set the duration for scope leases when distri	the average time the computer is or mobile networks that consist mainly of lease durations can be useful. mainly of desktop computers at fixed opropriate. ibuted by this server.
Limited to:	
Days: Hours: Minutes:	
	< <u>Back N</u> ext > Cancel

 Sur la page des options de configuration DHCP, choisissez Yes, I want to configure DHCP Option now, puis cliquez sur Next.

Co	onfigure 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
	< Back Next> Cancel

17. S'il existe un routeur de passerelle par défaut, mentionnez l'adresse IP du routeur de passerelle dans la page du routeur (passerelle par défaut), puis cliquez sur **Next**.

IP address:		
	A <u>d</u> d	
10.77.244.220	<u>H</u> emove	
	Цр	
	D <u>o</u> wn	

 Sur la page du nom du domaine et des serveurs DNS, introduisez le nom du domaine qui a été configuré précédemment. Dans l'exemple, utilisez Wireless.com. Saisissez l'adresse IP du serveur. Cliquez sur Add.

use for
A <u>d</u> d
Remove
<u>U</u> р
D <u>o</u> wn

- 19. Cliquez sur Next (Suivant).
- 20. Àla page de serveur WINS, cliquez sur Next.
- 21. Sur la page d'activation du champ, choisissez **Yes, I want to activate the scope now**, puis cliquez sur

Next.

New Scope Wizard			
Activate Scope Clients can obtain address leases only if a s	cope is activate	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			
	< <u>B</u> ack	<u>N</u> ext >	Cancel

22. Lorsque l'assistant de New Scope aura terminé, cliquez sur **Finish**.



23. Dans la fenêtre DHCP Snapin, vérifiez que la portée DHCP qui a été créée est active.

Desco		0.6.0			X	
Elle &dian Yen Help					Close	
◆ → 🗈 🗉 × 🗗 🖻 🖻 🖳 🖵 🥵	2					
Фоно	baseb-lag2-minless.com [th:77.214.217]					
B- C Swee 172 to 0.0 (107/124/217)	Canterits all DHCP Server	3.9.15	Description			
- B Server Optione	Scape [172.16.0.0] DHCP-Clients	** Active **	DHCP Server for Wireless Clients			
	La Server Options					
	1					
🐮 Start 🛛 🎉 Network Connections	 ⊈peor				# 2 B B M M V 60474	

Maintenant que DHCP / DNS est activé sur le serveur, configurez le serveur en tant que serveur d'Autorité de certification (CA) d'entreprise.

Installez et configurez le serveur de Microsoft Windows 2003 en tant que serveur

d'Autorité de certification (CA)

Le PEAP avec EAP-MS-CHAPv2 valide le serveur RADIUS basé sur le certificat actuel sur le serveur. De plus, le certificat du serveur doit être délivré par une autorité publique de certification (CA) que l'ordinateur client considère comme étant de confiance (c'est-à-dire, le certificat public CA existe déjà dans le répertoire Trusted Root Certification Authority dans la mémoire des certificats de l'ordinateur client). Dans cet exemple, configurez le serveur de Microsoft Windows 2003 en tant qu'Autorité de certification (CA) qui fournit le certificat au Service d'authentification Internet (IAS).

Afin d'installer et de configurer les services de certificat sur le serveur, suivez ces étapes :

- 1. Cliquez sur Add or Remove Programs dans le panneau de configuration.
- 2. Cliquez sur Add/Remove Windows Components.
- 3. Cliquez sur Services de certificat.

ows Components Wizard	
/indows Components You can add or remove components of Windows.	
To add or remove a component, click the checkbox. A shaded part of the component will be installed. To see what's included Details.	box means that only 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
	7.9 MB 🔟
Description: Installs a certification authority (CA) to issue certific public key security programs.	cates for use with
Total disk space required: 13.8 MB	Details
Space available on disk: 7310.6 MB	<u></u>
< <u>B</u> ack <u>N</u> ext >	Cancel Hel

 Cliquez sur Yes au message d'avertissement, après avoir installé les services de certificat, l'ordinateur ne peut pas être renommé, se connecter à un domaine ou être supprimé. Voulez-vous continuer

?

Microsof	t Certificate Services			
After installing Certificate Services, the machine name and domain membership may not be changed due to the binding of the machine information stored in the Active Directory. Changing the machine name or domain membership would invalidate the certificates issue Please ensure the proper machine name and domain membership are configured before installing Certificate Services. Do you want				
	<u>Y</u> es <u>No</u>			

5. Sous le type d'autorité de certification, choisissez **Enterprise root CA**, puis cliquez sur **Next**.

lows Components Wizard	_
CA Type Select the type of CA you want to set up.	
Enterprise root CA	
C Enterprise subordinate CA	
C <u>S</u> tand-alone root CA	
C Stand-alone subordinate CA	
The most trusted CA in an enterprise. Should be installed before	any other CA.
Use custom settings to generate the key pair and CA certificat	e

6. Saisissez un nom pour identifier le CA. Cet exemple utilise Wireless-CA. Cliquez sur Next (Suivant).

Common name for this C	Δ <u>.</u>
 Wireless-CA	
, Distinguished name suffi	x:
DC=Wireless,DC=com	
Preview of distinguished	name:
CN=Wireless-CA,DC=W	ireless,DC=com
ļ	
Validity period:	Expiration date:
harmonia harmonia harmonia	

 Un répertoire « journal de certification » est créé pour le stockage de la base de données de certificats. Cliquez sur Next (Suivant).

lows components wizaru	
Certificate Database Settings Enter locations for the certificate database, database log, and co information.	onfiguration
<u>C</u> ertificate database:	
C:\WINDOWS\system32\CertLog	Br <u>o</u> wse
Certificate <u>d</u> atabase log:	
C:\WINDOWS\system32\CertLog	Browse
Shared folder:	Browse
S <u>h</u> ared folder:	Biowse
S <u>h</u> ared folder:	Browse
Shared folder:	Biowse
Shared folder:	Browse

8. Si IIS est activé, il doit être arrêté avant que vous poursuiviez. Cliquez sur **OK au message** d'avertissement qu'IIS doit être arrêté. Il redémarre automatiquement après l'installation du CA.

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

9. Cliquez sur Finish pour terminer l'installation des services d'Autorité de certification (CA).



L'étape suivante consiste à installer et à configurer le Service d'authentification Internet sur le serveur de Microsoft Windows 2003.

Connectez les clients de routage au domaine de routage

L'étape suivante consiste à connecter les clients au réseau câblé et à télécharger les informations spécifiques au domaine depuis le nouveau domaine. En d'autres termes, connectez les clients au domaine. Pour ce faire, suivez ces étapes :

- 1. Connectez les clients au réseau câblé avec une droite par un câble Ethernet.
- 2. Initialisez le client et la connexion avec le nom d'utilisateur/mot de passe du client.
- 3. Cliquez sur Démarrer ; cliquez sur Exécuter ; tapez cmd ; et cliquez sur OK.
- 4. Àl'invite de commande, saisissez **ipconfig**, puis cliquez sur **Enter pour vérifier que le DHCP fonctionne correctement et que le client a reçu une adresse IP du server DHCP.**
- 5. Afin de connecter le client au domaine, cliquez à droite sur My Computer, puis choisissez **Properties**.
- 6. Cliquez sur l'onglet Computer Name.
- 7. Cliquez sur Change.
- 8. Cliquez sur Domain ; tapez wireless.com ; et cliquez sur
| omp | uter Name Chan | ges | |
|-------------------|--|--------------------------------|-------------------------------------|
| You c
compi | an change the name
Iter. Changes may af | and the memb
fect access to | pership of this
network resource |
| Comp | uter name: | | |
| Client | 1 | | |
| Full co
Client | mputer name: | | More. |
| Men | iber of | | |
| 0 | Domain: | | |
| | Wireless | | |
| 0 | Workgroup: | | |
| | WORKGROUP | | |
| ****** | | | |

9. Saisissez Username Administrator et le mot de passe spécifique au domaine auquel le client se connecte. (Il s'agit du compte administrateur dans l'Active Directory sur le





- 10. Click OK.
- 11. Cliquez sur Yes pour redémarrer l'ordinateur.
- 12. Une fois l'ordinateur redémarré, connectez-vous avec ces informations : Username = Administrator; Password = <domain password>; Domain = Wireless.
- 13. Cliquez à droite sur **My Computer**, puis cliquez sur **Properties**.
- 14. Cliquez sur l'onglet **Computer Name pour vérifier que vous êtes sur le domaine Wireless.com.**

ystem Proper	ties			?	
System Restore Automatic Updates			tic Updates	Remote	
General	Com	puter Name	Advanced		
Wind on th	dows uses ne networl	the following inf	ormation to identify	your computer	
Computer desc	ription:				
		For example: " Computer".	(itchen Computer'')	or ''Mary's	
Full computer n	iame:	Client1.Wireles	s.com		
Domain:		Wireless.com			
domain and cre ID.	ate a loca	al user account, (click Network		
To rename this	computer	or join a domain	, click Change.	Change	
🔥 Changes	will take e	effect after you re	start this computer.		
		ОК	Cancel	Apply	

- 15. L'étape suivante consiste à vérifier que le client a reçu le certificat d'authentification (de confiance) du serveur.
- 16. Cliquez sur **Démarrer** ; cliquez sur **Exécuter** ; tapez **mmc**, puis cliquez sur **OK**.

17. Cliquez sur **File**, puis cliquez sur le jeu d'outils **Add/Remove**.

dd/Remove Snap	-in	? ×
Standalone Extensi	ons	
Use this page to add	d or remove a standalone Snap-in from the console.	
Snap-ins added to:	🔄 Console Root 🛛 🔽	
- Description		
Add	Remove About	
	ОК С	ancel

- 18. Cliquez sur Add.
- 19. Choisissez Certificate, puis cliquez sur

Shapin	vendor
Market Revenue 1.1 Configuration	Microsoft Corporation
Control	Microsoft Corporation
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
Description The Certificates snap-in allows you to bro certificate stores for yourself, a service, o	wse the contents of the r a computer.

20. Choisissez **Computer Account**, puis cliquez sur **Next**.

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

21. Cliquez surFinish pour accepter l'ordinateur local par

défaut.

201.	
lect Computer	
Select the computer you want this sn	hap-in to manage.
This snap-in will always manage:	
 Local computer: (the compute 	r this console is running on)
O Another computer:	Province
Allow the selected computer to only applies if you save the co	o be changed when launching from the command line. This photole.
only applies if you save the co	insole.
	Z Rock Einich Concel

22. Cliquez sur **Close**, puis cliquez sur **OK**.

23. Développez Certificates (Local Computer), Trusted Root Certification Authorities et cliquez sur Certificates. Trouvez Wireless dans la

liste.						
🚡 Console1 - [Console Root/Certific	ates (Local Computer)\Trusted R	oot Certification Authorities/Cer	tificates]			6 🛛
🚡 File Action View Favorites Wine	low Help					_ Cose
←→ 🖻 🗷 ¾ 🗡 🛱 🖫	3 😰					
🛄 Console Root	Issued To - A	Issued By	Espiration Date	Intended Purposes	Friendly Name	Statt A
E - 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 Email, Server	Societa Interbancari	
E- In 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	
E Enterprise Trust	Symantec Root CA	Symantec Root CA	5/1/2011	<ab< td=""><td><none></none></td><td></td></ab<>	<none></none>	
E- Intermediate Certification Author	TC TrustCenter Class I CA	TC TrustCenter Class 1 CA	1/1/2011	Secure Email, Server	TC TrustCenter Clas	
E Interested Publishers	TC TrustCenter Class 2 CA	TC TrustCenter Class 2 CA	1/1/2011	Secure Email, Server	TC TrustCenter Clas	
E Third-Party Boot Certification Au	TC TrustCenter Class 3 CA	TC TrustCenter Class 3 CA	1/1/2011	Secure Email, Server	TC TrustCenter Clas	
H- Trusted People	TC TrustCenter Class 4 CA	TC TrustCenter Class 4 CA	1/1/2011	Secure Email, Server	TC TrustCenter Clas	
H-M SPC	TC TrustCenter Time Stamping CA	TC TrustCenter Time Stamping CA	1/1/2011	Time Stamping	TC TrustCenter Time	
	Thavte Personal Basic CA	Thante Personal Basic CA	1/1/2021	Client Authentication	Thavke Personal Bas	
	Thavte Personal Freemail CA	Thavite Personal Freemail CA	1/1/2021	Client Authentication	Thawte Personal Fre	
	Theyte Personal Premium CA	Thante Personal Premium CA	1/1/2021	Client Authentication	Thavke Personal Pre	
	Thavte Premium Server CA	Thavite Premium Server CA	1/1/2021	Server Authenticatio	Thavke Premium Ser	
	Theyte Server CA	Thante Server CA	1/1/2021	Server Authenticatio	Thavke Server CA	
	Thavte Tinestamping CA	Thavite Timestamping CA	1/1/2021	Time Stamping	Thavke Timestampin	
	UTN - DATACorp SGC	UTN - DATACorp SGC	6/25/2019	Server Authentication	UTN - DATACorp SGC	
	UTN-USERFirst-Client Authenticati	UTN-USERFirst-Client Authentication	7/9/2019	Secure Email	UTN - USERFirst-Cle	
	UTN-USERFirst-Hardware	UTN-USER/First-Hardware	7/9/2019	Server Authentication	UTN - USER Pirst-Har	
	UTN-USERFirst-Network Applications	UTN-USERFirst-Network Applications	7/10/2019	Secure Enail, Server	UTN - USERFirst-Net	
	UTN-USERFirst-Object	UTIV-USER/First-Object	7/10/2019	Time Stamping, Code	UTN - USERFirst-Object	
	WeriSign Commercial Software Publ	VeriSign Commercial Software Publis	12/31/1999	Secure Enail, Code 5	VeriSign Commercial	
	VeriSign Commercial Software Publ	VeriSign Commercial Software Publis	1/8/2004	Secure Email, Code S	VeriSign Commercial	
	VeriSign Individual Software Publis	VertSign Individual Software Publishe	12/31/1999	Secure Email, Code 5	VeriSign Individual 5	20
	VeriSign Individual Software Publis	VeriSign Individual Software Publishe	1/8/2004	Secure Email, Code S	VeriSign Individual S	
	Weri5ign Trust Network	Vertign 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	
	VeriSign Trust Network	Vertign Trust Network	5/19/2018	Secure Email, Clent	Veri5ign Class 3 Prim	
	VeriSign Trust Network	VeriSign Trust Network	8/2/2028	Secure Email, Client	VeriSign Class 3 Prim	
	VeriSign Trust Network	VerBign Trust Network	5/19/2018	Secure Email, Client	VeriSign Class 4 Prim	
	VeriSign Trust Network	VeriSign Trust Network	8/2/2028	Secure Enail, Client	VeriSign Class 1 Prim	
	VeriSign Trust Network	VeriSign Trust Network	8/2/2028	Secure Email, Client	VeriSign Class 4 Prim	
	VeriSign Trust Network	VeriSign Trust Network	5/19/2018	Secure Email, Client	VeriSign Class 1 Prim	
	🗮 Wreless-CA	Wireless-CA	12/17/2012	<ai></ai>	<hore></hore>	
	EDicert EZ by DST	Xcert EZ by DST	7/11/2009	Secure Email, Server	Xcert EZ by DST	*
<) >	<	N. C. S.				>
Trusted Root Certification Authorities store co	ntains 109 certificates.					
🐉 start 🁔 🊡 Consolet - [Conso	49			8 3	A U U U U U U U	2:42 PM

24. Répétez cette procédure pour ajouter plus de clients au domaine.

Installez le service d'authentification Internet sur le serveur de Microsoft Windows 2003 et demandez un certificat

Dans cette configuration, le Service d'authentification Internet (IAS) est utilisé en tant que serveur RADIUS pour authentifier des clients sans fil avec l'authentification PEAP.

Suivez ces étapes pour installer et configurer IAS sur le serveur.

- 1. Cliquez sur Add or Remove Programs dans le panneau de configuration.
- 2. Cliquez sur Add/Remove Windows Components.
- 3. Choisissez Networking Services, puis cliquez sur Details.
- 4. Choisissez Internet Authentication Service ; cliquez sur OK ; et cliquez sur

	ns that on
componen	it, click De
	1.7 M
	0.0 M
	0.0 M
	0.1 M
	0.0 M
	0.0 M
	0.9 M
inting of di	ial-up and
	Detai
эк 🚺	Cano
	ОК

5. Cliquez sur Finish pour terminer l'installation IAS.

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

- 6. L'étape suivante consiste à installer le certificat de l'ordinateur pour le Service d'authentification Internet (IAS).
- 7. Cliquez sur **Démarrer** ; cliquez sur **Exécuter** ; tapez **mmc** ; et cliquez sur **OK**.



- 8. Cliquez sur Console dans le menu Fichier, puis choisissez le jeu d'outils Add/Remove.
- 9. Cliquez sur Add pour ajouter un jeu

Standalone				
Use this page to add	i or remove a stand-	alone snap-ir	from the consol	е,
Snap-ins added to:				1
Description				
Description				
Add	Remove At	20ut		
Add	<u>R</u> emove At	<u>pout,</u>	~	

10. Choisissez Certificates dans la liste des jeux d'outil, puis cliquez sur

5nap-in	Vendor
🙀 .NET Framework 1.1 Configuration	Microsoft Corporation
Rective 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
Description The Certificates snap-in allows you to bro certificate stores for yourself, a service,	owse the contents of the or a computer.

11. Choisissez **Computer Account**, puis cliquez sur **Next**.

Certificates snap-in			×
This snap-in will always manage certificates for:			
C <u>My</u> user account			
Service account			
Computer account			
	< <u>B</u> ack	<u>N</u> ext>	Cancel
	l		

12. Choisissez Local computer, puis cliquez sur Finish

rinisn.	
Select Computer	×
Select the computer you want this snap-in to manage. This snap-in will always manage: • Local computer: (the computer this console is running on) • Another computer: [
< <u>B</u> ack Finish Cancel	

13. Cliquez sur **Close**, puis cliquez sur **OK**.

14. Développez Certificats (Ordinateur local); cliquez avec le bouton droit sur Dossier personnel; choisissez Toutes les tâches, puis Demandez un nouveau cortificat

Console I - [Console Reet]		X
🗴 Sle lution year flavgrites yindow yeap		X
Consider Roat Contributer (Local Computer) Contributer (Local C	Piper Certificates (Jucol Computer)	

15. Cliquez sur Next dans Welcome to the Certificate Request Wizard.



16. Choisissez le modèle de certificat du contrôleur de domaine (si vous demandez un certificat

d'ordinateur sur un serveur autre que DC, choisissez un modèle de certificat d'ordinateur), puis cliquez sur

Next.

rtific	ate Request Wizard	×
Cerl	lificate Types	
	A certificate type contains preset properties for certificates.	
	Select a certificate type for your request. You can access only certificate types that you have permissions for and that are available from a trusted CA.	
	Certificate types:	
	Directory Email Replication Domain Controller	
	Domain Controller Authentication	
	To select a cryptographic service provider and a CA, select Advanced.	
	< <u>B</u> ack <u>N</u> ext > Cance	1

17. Saisissez un nom et une description pour le certificat.

cate Request Wizard	
tificate Friendly Name and Description	
You can provide a name and description that help you quickly identify a specific certificate.	
Type a friendly name and description for the new certificate	
Friendly name:	
PEAP-Wireless	
Description:	
IAS Server Certificate - 802.1x Authentication	

18. Cliquez sur **Finish pour terminer avec l'assistant de requête de** certification.



<u>Configurez le service d'authentification Internet pour l'authentification PEAP-MS-</u> <u>CHAP v2</u>

Maintenant que vous avez installé et que vous avez demandé un certificat pour IAS, configurez IAS pour l'authentification.

Procédez comme suit :

- 1. Cliquez sur **Start > Programs > Administrative Tools**, puis cliquez sur le jeu d'outils Internet Authentication Service.
- Cliquez à droite sur Internet Authentication Service (IAS), puis cliquez sur Register Service in Active Directory.

🖓 Internet Authentication Ser	rike		×			
Elle Action Yeve Lalip						
+ → 🔟 🗗 🔮 🔟 () (i)					
Atternet Autococcus in Service Bornet RADBUS Clients Bornet Rocess Logging Bornet Access Policies	Sart Service Sart Service Spp Service Register Server in Adres Directory	rea to Internet Authentication Service Therefore (185) to authenticate, authories, and account for dail-up. VPM, wireless and Diternet connections to your network. You can also configure 186 to forward				
H- Connection wedness hadre	Tian .	quests to any access server that is compatible with Remote Authentication Dial-In User Service (RADIUS).				
	Poperties	I to read the remote access properties of user accounts in Addve Directory, on the Addon menu, click Register Server in Active Directory.				
	H-P	ation about setting up IAS, deployment scenarios, and troubleshooting, see Help.				
Register Server in Active Directory						
🐮 Start 🙆	letwork Connections PDHCP	🚊 drangat - [DH2]15WID 🗣 Internet Authentikats. 🛛 🖉 🕄 🗑 🗑 🕅 👯 💯 7:0719	M			

3. La boîte de dialogue **Register Internet Authentication Service in Active Directory** s'affiche ; cliquez sur **OK**. Ceci permet à IAS d'authentifier des utilisateurs dans Active Directory.

Register Internet Authentication Server in Active Directory:	×
To enable IAS to authenticate users in the Active Directory, the computers r	unning IAS must be authorized to read users' dial-in properties from the domain.
Do you wish to authorize this computer to read users' dial-in-properties from	the Wireless.com domain?
OK	Cancel

4. Cliquez sur **OK dans la boîte de dialogue** suivante.

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.
	OK

- 5. Ajoutez le contrôleur LAN sans fil en tant que client AAA sur le serveur MS IAS.
- 6. Cliquez à droite sur **RADIUS Clients**, puis choisissez **New RADIUS Client**.

🖓 Internet Authentication Service		
Elle Brition Yerk Help		
◆ → 🖪 🗄 🕄 😫 🖪		
Image: Product Acceleration Service (Local) Product	Name Onter Connections to Morosoft Routing and Reacter 1 Connections to other access servers 2	
New Clent	·	
🐮 Shart 🧉 🏀 Network Connection	a Disco Athenticatian 🚯 Internet Authenticatian	😦 😤 🛢 💹 👯 👯 🕅 7.13PM

7. Introduisez le nom du client (WLC, dans ce cas), puis saisissez l'adresse IP du WLC. Cliquez sur **Next**

10	ii.	nnt)
(0	JIVC	anu).

New RADIUS Client		×
Name and Address		
Type a friendly name and	either an IP Address or DNS i	name for the client.
Eriendly name:	WLC	
Client address (IP or DNS)	:	
10.77.244.210		⊻erify
	< <u>B</u> ack	<u>N</u> ext > Cancel

8. Sur la page suivante, sous Client-Vendor, choisissez **RADIUS Standard** ; entrez le secret partagé et cliquez sur **Finish**.

9. Notez que le WLC est ajouté en tant que client AAA sur IAS

🞾 Internet Authentication Servi	KE			104000			×
Elle Buttion Yoleve Hallip	2. 1. 1. 1. 1. 1. 1.	50000	12 12 12 12 12 12 12 12 12 12 12 12 12 1	10000		********	Cleg
* > 1 1 1 1 1 1 1 1 1 1	1 🕫 🗉						
Internet Authentication Service (). 	Local)	Priendly Name /	Address	Protocol	Client Vendor		
Prevote Access Logging Prevote Access Policies Connection Request Process	na	Tarc	0.77.24.210	KALALIS	NACELO SONGARO		
🐮 Start 🛛 🍎 📃 🛍 160	heark Connections	Para	A dran	ght - [DNS],19468	Platemet Authenticals.		🖉 🕈 🖲 🗑 🎆 🍢 🕅 7112PM

- 10. Créez une stratégie d'accès à distance pour les clients.
- 11. Àcette fin, cliquez à droite sur Remote Access Policies, puis choisissez New Remote

그리 ×

And the second sec	ication Service			
ie gation yeen	6Mp			
	3 🗟 📝 🖽			
Internet Authentics Anne Actus Clents Clents	ation Service (Local) Logging	Merrie Connections to Microsoft Routing and Remote Connections to other access servers	Order 1 2	
Connection Re	Meve Remote Access Bolicy	1		
	gev +			
	gen +			
	Rajnah Expertyst			
	Beb]]		

12. Saisissez un nom pour la stratégie d'accès à distance. Dans cet exemple, utilisez le nom PEAP. Cliquez ensuite sur Next.

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?
	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.

 13. Choisissez les attributs de la politique en fonction de vos nécessités. Dans cet exemple, choisissez Wireless.

cy Wizard	×
e based on the method used to gain access to the network.	Ŷ
access for which you want to create a policy.	
connections. To create a policy for a specific VPN type, go and select Set up a custom policy.	back to the
connections that use a traditional phone line or an Integrate (ISDN) line.	d Services
(··)	
LAN connections only.	
t connections, such as connections that use a switch	
	e based on the method used to gain access to the network. access for which you want to create a policy. connections. To create a policy for a specific VPN type, go and select Set up a custom policy. connections that use a traditional phone line or an Integrate (ISDN) line.

14. Sur la page suivante, choisissez User pour appliquer cette stratégie d'accès à distance à la liste des utilisateurs.

User or Group Access You can grant access to individual users, or you can grant access to selec groups.	8
Grant access based on the following:	
Group name:	A <u>d</u> d
	<u>R</u> emove

15. Sous les méthodes d'authentication, choisissez **Protected EAP (PEAP)**, puis cliquez sur **Configure**.

New Remote Access Policy Wizard		×
Authentication Methods EAP uses different types of security device	es to authenticate users.	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. Sur la page Protected EAP Properties , choisissez le certificat approprié du menu déroulant des certificats émis, puis cliquez sur

rotected EAP Prop	erties			1		
This server identifies Select the certificate	itself to ca that you v	allers before the conr want it to use as proc	nection is comp of of identity.	leted.		
Certificate issued		web-lapt.Wireless.co	m			
Friendly name:	PE/	AP-Wireless				
Issuer:	Wir	Wireless-CA				
Expiration date:	12/	12/16/2008 5:53:02 PM				
🔲 Enable Fast Reco	nnect					
E <u>a</u> p Types						
Secured password (B	EAP-MSCH	AP v2)		Move Up		
				Move Dow		
Add	<u>E</u> dit	Remove	ОК	Cancel		

17. Vérifiez les détails de la stratégie d'accès à distance, puis cliquez sur **Finish**.

New Remote Access Policy Wizard



X

18. La stratégie d'accès à distance a été ajoutée à la



19. Cliquez à droite sur la stratégie, puis cliquez **Properties**. Sélectionnez « **Grant remote** access permission » sous « If a connection request matches the specified conditions

AP Properties				<u>۲</u>
Specify the cond	litions that conne	ction reque	ests must match	L.
Policy conditions	:			
NAS-Port-Type	matches "Wirele:	ss - Other C)R Wireless - IE	EE 802.11"
				•
Add	<u>E</u> dit	<u>R</u> emo	ve	
If connection rec associated profile	uests match the e will be applied to	conditions o the conn	specified in this ection.	policy, the
Unless individua policy controls a	access permission	ons are spe vork.	cified in the us	er profile, this
If a connection r	equest matches t access permissio	he specifie on	d conditions:	
Grant remote	access permission	on		
Grant remote	access permissi	on OK	Cancal	1 Aceta

Ajoutez les utilisateurs à l'Active Directory

Dans cette configuration, la base de données de l'utilisateur est mise à jour dans l'Active Directory.

Afin d'ajouter des utilisateurs à la base de données d'Active Directory, suivez ces étapes :

1. Dans l'arborescence de la console Utilisateurs et ordinateurs Active Directory, cliquez avec le bouton droit sur **Utilisateurs** ; cliquez sur **Nouveau** ; puis cliquez sur **Utilisateur**.



2. Dans le nouvel objet - boîte de dialogue de l'utilisateur, introduisez le nom de l'utilisateur sans fil. Cet exemple utilise le nom WirelessUser dans le premier champ d'identification et WirelessUser dans le champ d'identification de connexion d'utilisateur. Cliquez sur Next

Create in:	Wireless.com/Users	
<u>F</u> irst name:	Client 1	
Last name:		
Full name:	Client 1	
<u>U</u> ser logon name:		
Client1	@Wireless.com	1
	Vindows 2000)	
User logon name (pre- <u>V</u>	<u>v</u> indows 2000).	200 C
User logon name (pre- <u>V</u> WIRELESS\	Client1	

(Suivant).

3. Dans le nouvel objet - boîte de dialogue d'utilisateur, saisissez un mot de passe de votre choix dans le champ mot de passe, puis confirmez les champs du mot de passe. Effacez la case à cocher **User must change password at next logon**, puis cliquez sur

Password:		•••••	
<u>C</u> onfirm passwo	rd:		
User <u>m</u> ust c	hange password	l at next logon	
User canno	t change passwo	ord	
Pass <u>w</u> ord n	ever expires		
Account is	disabled		

4. Dans le nouvel objet - boîte de dialogue d'utilisateur, cliquez sur



5. Répétez les étapes 2 à 4 afin de créer des comptes d'utilisateur supplémentaires.

Permettez l'accès sans fil aux utilisateurs

Procédez comme suit :

- 1. Dans l'arborescence de la console Utilisateurs et ordinateurs Active Directory, cliquez sur le dossier **Utilisateurs**, cliquez avec le bouton droit sur **WirelessUser**, cliquez sur **Propriétés**, puis accédez à l'onglet **Accès à distance**.
- 2. Sélectionnez Allow access, puis cliquez sur

Remote control Terminal Servi	ces Profile COM
General Address Account Profile	Telephones Organi:
Member Of Dial-in Env	vironment Sessio
 Remote Access Permission (Dial-in or VPN) 	
Allow access	
C Deny access	
C Control access through Remote Access	Eolicy
☐ Verify Caller-ID:	
- Callback Options	
No <u>C</u> allback	
○ <u>S</u> et by Caller (Routing and Remote Acc	ess Service only)
C Always Callback to:	
Assign a Static IP Address	
Apply Static <u>B</u> outes	
Define routes to enable for this Dial-in connection.	Static Routes

Configurez le contrôleur LAN sans fil et les AP légers

Configurez maintenant les périphériques sans fil pour cette configuration. Ceci inclut la configuration des contrôleurs LAN sans fil, des AP légers et des clients sans fil.

Configurez le WLC pour l'authentification RADIUS par le serveur RADIUS de MS

<u>IAS</u>

Configurez d'abord le WLC pour utiliser MS IAS en tant que serveur d'authentification. WLC doit être configuré afin de transférer les identifiants de l'utilisateur à un serveur RADIUS externe. Le serveur RADIUS externe valide alors les identifiants de l'utilisateur et permet d'accéder aux clients sans fil. À cette fin, ajoutez le serveur MS IAS en tant que serveur RADIUS dans la page **Security > RADIUS Authentication.**

Procédez comme suit :

1. Sélectionnez **Security et RADIUS Authentication** depuis la GUI du contrôleur pour afficher la page des serveurs d'authentification RADIUS. Cliquez alors sur **New afin de définir un serveur**

ADIUS.							
3 · O · 🗷 🖻	🙆 🔎 📩 🥹 🍰	1 🖂 🖏					- <u> </u>
GISCO SPOTEMO					Save Co	infiguration Ping	Logout Refresh
A. A.	MONITOR WUANS CONTR	OLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	RADIUS Authentication Se	rvers > New				< Back	Apply
AAA 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 IPSec Certificates	Confirm Shared Secret	•••••]	
CA Certificate ID Certificate	Key Wrap						
Web Auth Certificate		[
Wireless Protection	Port Number	1812					
Trusted AP Policies Rogue Policies	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. Définissez les paramètres du serveur RADIUS sur la page RADIUS Authentication Servers > New . Ces paramètres incluent l'adresse IP du serveur RADIUS, secret partagé, numéro de port et état du serveur. Les cases à cocher d'utilisateur du réseau et de gestion déterminent si l'authentification basée sur RADIUS s'applique pour la gestion et les utilisateurs du réseau. Cet exemple utilise MS IAS en tant que serveur RADIUS avec l'adresse IP 10.77.244.198.

G · 🕤 🖹 🖻	🚯 🔎 🛠 🛛 🖾·	2	8				4	7 - 8
Cisco Statema	MONITOR WLANS CO	ONTROLLER	WIRELESS 5	ECURITY	MANAGEMENT COA	Save Configurat IMANDS HELP	on Ping Logo	ut Refre
Security	RADIUS Authentication	n Servers					Apply New	
AAA General RADIUS Authentication RADIUS Accolunting Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	Call Station ID Type Credentials Caching Use AES Key Wrap	IP Address	2					
Access Control Lists	User Management	Index	Server Address	Port	1PSec	Admin 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	Edit Remove	Pina

- 3. Cliquez sur Apply.
- 4. Le serveur MS IAS a été ajouté au WLC en tant que serveur RADIUS et peut être utilisé pour authentifier des clients sans fil.

Configurez un WLAN pour les clients de routage

Configurez le SSID (WLAN) auquel les clients sans fil se connectent. Dans cet exemple, créez le SSID, puis nommez-le **PEAP**.

Définissez l'authentification de la couche 2 comme WPA2 de sorte que les clients exécutent l'authentification basée par EAP (PEAP-MSCHAPv2 dans ce cas) et utilise AES comme mécanisme de cryptage. Laissez toutes autres valeurs à leurs paramètres par défaut.

Remarque : ce document lie le WLAN aux interfaces de gestion. Quand vous avez plusieurs VLAN dans votre réseau, vous pouvez créer un VLAN séparé et le relier au SSID. Pour les informations sur la façon de configurer des VLAN sur les WLC, reportez-vous aux <u>VLAN sur</u> <u>l'exemple de configuration de contrôleurs LAN sans fil</u>.

Afin de configurer un WLAN sur le WLC, suivez ces étapes :

- 1. Cliquez sur les WLAN de la GUI du contrôleur afin d'afficher la page des WLAN. Cette page énumère les WLAN qui existent sur le contrôleur.
- Sélectionnez New afin de créer un nouveau WLAN. Saisissez l'ID WLAN et le SSID WLAN pour le WLAN, puis cliquez sur Apply.



3. Une fois que vous avez créé un nouveau WLAN, la page WLAN > Edit du nouveau WLAN apparaît. Sur cette page, vous pouvez définir les divers paramètres spécifiques à ce WLAN qui incluent des stratégies générales, des serveurs RADIUS, des stratégies de sécurisation et des paramètres 802.1x.

Cinco Statune		-					Save Co	onfiguration	Ping	Logout Refre
An de	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP		
WLANs	WLANs > E	dit						< 8-a	ck	Apply
WLANS	WLAN ID		1							
AP Groups VLAN	Profile Nan	ne .	PEAP							
	WLAN SSID		PEAP							
	General Po	licies				Security Policies				
	Radio Polic	T.	All	¥.			1Pv6 Enable			
	Admin Stat	tus	C Enabled					_		
	Session Tir	meaut (sea	cs) 0	0				ky WP	WPA1+WPA2	
	Quality of S	Service (Q	oS) Silver (bes	t effort) 💌				□ M	IAC Filter	ing
	WMM Polic	y	Disabled	-			Laver 3 Securi	ity No.		1
	7920 Phone	e Support	Client CA	C Limit 🗖 AP	CAC Limit		2010 0 00000		Veb Policy	
	Broadcast	SSID	I Enabled						L. Heerenay	
	Aironet IE		Enabled							
	Allow AAA	Override	Enabled				 Web Policy cannot be used in combination w IPsec 			
	Client Excl	usion	Enabled	• 60			** When client	terrelation is	enabled.	a time out
	DHCR Sec		Dowerside	Timeout V	alue (secs)		value of zero r	neans infinity	(nill req	uire hufed clients)
	DHCP SHY	. Assiance					*** CKIP is no	st supported l	by 10xx	APs
	Unice wood	- Assignm	enc Exequired	- 101						
	Interrace w	e De suire	Imanageme	at -						
	MFP Versio MFP Signat	n Required		un rischladt						
	Generation		M (Global	MPP Disabled)						
	H-REAP Lo	cal Switchi	ing 🗋	d with mone	CRAWING and					
	authenticat	tions.	aning not supporte	a with IPSEC,	CRANITE and	FUK IKESS				

- 4. Vérifiez l'état admin sous les stratégies générales afin d'activer le WLAN. Si vous voulez qu'AP diffuse le SSID dans ses trames balises, vérifiez le SSID de diffusion.
- 5. Sous Layer 2 Security, sélectionnez WPA1+WPA2. Ceci active le WPA sur le WLAN. Déroulez la page et choisissez le stratégie WPA. Cet exemple utilise le WPA2 et le cryptage AES. Choisissez le serveur RADIUS approprié du menu déroulant sous serveurs RADIUS. Dans cet exemple, utilisez 10.77.244.198 (adresse IP du serveur MS IAS). Les autres paramètres peuvent être modifiés sur les conditions requises du réseau WLAN.

	fines States						Save C	onfiguration	Ping Logou	ut Refre	sh
	WLANS WLANS AP Groups VLAN	WPA1+WPA2 Parameters WPA1 Policy WPA2 Policy WPA2 Encryption Auth Key Mgmt	F AES	ТКІР	-		000000	HELF			*
6.	Cliquez sur										
		MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT	Save C COMMANDS	onfiguration HELP	Ping Lago	ut Refre	sh
	WLANS WLANS AP Groups VLAN	Profile Name PEAP	1	PEAP	SID	Ad St.	abled [WPA	ity Policies 2][Auth(802.	18)]	Edit	Rem
		* WLAN IDS 9-16 wil	I not be pushed to	1130,1200 and	1240 AP mode	ds.					

Configurez les clients sans fil

Configurez les clients sans fil pour l'authentification PEAP-MS CHAPv2

Cet exemple fournit des informations sur la façon de configurer le client sans fil avec l'utilitaire de bureau Cisco Aironet. Avant de configurer l'adaptateur client, assurez-vous que la dernière version du microprogramme et l'utilitaire sont utilisés. Recherchez la dernière version du microprogramme et les utilitaires dans la page de téléchargements sans fil sur Cisco.com.

Afin de configurer l'adaptateur du client sans fil de Cisco Aironet 802.11 a/b/g avec l'ADU, suivez ces étapes :

- 1. Ouvrez l'utilitaire de bureau d'Aironet.
- 2. Cliquez sur Profile Management, puis cliquez sur New pour définir un profil.
- Sous l'onglet général, saisissez le nom du profil et le SSID. Dans cet exemple, utilisez le SSID que vous avez configuré sur le WLC (PEAP)

Profile M	lanagement	n an	? 🗙
General	Security Advanc	ed	
Profile	e Settings		
	Profile Name:	PEAP-MSCHAPv2	
	Client Name:	CLIENT1	
Netw	ork Names		
	SSID1:	PEAP	
	SSID2:		
	SSID3:		
		na senten en la sector de la sec	
			Cancel

 Sélectionnez l'onglet Security, choisissez WPA/WPA2/CCKM, sous WPA/WPA2/CCKM EAP, tapez PEAP [EAP-MSCHAPv2], puis cliquez sur Configure.

Profile Management	Kaikaikaikai akaikaikaikaikaikaikaikaikaikai akaikaikaikaikaikaikaikaikaikaikaikaikai	? 🗙
General Security Advanced		
- Set Security Options		
⊚ wPa/wPa2/CCKM	WPA/WPA2/CCKM EAP Type: PEAP (EAP-MSCHAP V2)	
○ WPA/WPA2 Passphrase		
O 802.1x	802.1x EAP Type: EAP-FAST	
O Pre-Shared Key (Static WEP)		
O None		
Configure	Allow Association to Mixed Cells	
	Limit Time for Finding Domain Controller To: 0 sec	
Group Policy Delay:	60 🗘 sec	
	ок с	ancel

5. Sélectionnez Validate Server Certificate, puis choisissez Wireless-CA dans le menu déroulant Trusted Root Certificate

 Use Machine Information for Domain Logon Validate Server Identity Trusted Root Certification Authorities Wireless-CA When connecting, use: Certificate User Name and Password 	
 Validate Server Identity Trusted Root Certification Authorities Wireless-CA When connecting, use; Certificate User Name and Password 	
Trusted Root Certification Authorities Wireless-CA When connecting, use: O Certificate O User Name and Password	
Wireless-CA When connecting, use: Certificate User Name and Password	
When connecting, use: Certificate User Name and Password	
 Certificate User Name and Password 	
 User Name and Password 	
Select a Lertificate	
Use Windows User Name and Password	
User Information for PEAP (EAP-MSCHAP V2) Authentication	
User Name: Administrator	
Password.	
Confirm Password:	
Advanced	Cance

 Cliquez sur OK, puis activez le profil.Remarque : lorsque vous utilisez le protocole PEAP-MSCHAPv2 (Protected EAP-Microsoft Challenge Handshake Authentication Protocol Version 2) avec Microsoft XP SP2 et que la carte sans fil est gérée par le système WZC (Microsoft Wireless Zero Configuration), vous devez appliquer le correctif logiciel Microsoft KB885453. Ceci évite plusieurs problèmes d'authentification liés à PEAP Fast Resume.

Vérifiez et dépannez

Afin de vérifier si la configuration fonctionne comme prévu, activez le profil PEAP-MSCHAPv2 sur le client sans fil Client1.

🖻 Cisco Aironet Desktop Utility - Current Profile: PEAP-MSCHAPv2 🛛 🛜 🔀					
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			

Une fois que le profil PEAP-MSCHAPv2 est activé sur l'ADU, le client exécute l'authentification ouverte de 802.11, puis exécute l'authentification PEAP-MSCHAPv2. Voici un exemple d'authentification PEAP-MSCHAPv2 réussie.

Utilisez les commandes de débogage pour comprendre l'ordre des opérations qui se produisent.

L'<u>Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines</u> <u>commandes show.</u> Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show**.

Ces commandes de débogage sur le contrôleur LAN sans fil sont utiles.

- debug dot1x events enable Afin de configurer le débogage des événements de 802.1x
- debug aaa events enable Afin de configurer le débogage des événements AAA
- debug mac addr <mac address> Afin de configurer le débogage MAC, utilisez la commande de débogage mac

• debug dhcp message enable - Afin de configurer le débogage des messages d'erreur DHCP Ce sont les exemples de résultat de la commande debug dot1x events enable et de la commande debug client <mac address>.

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
```
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

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 Reg 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 = 0x0000000,
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
```

Remarque : si vous utilisez le demandeur Microsoft pour vous authentifier auprès d'un Cisco Secure ACS pour l'authentification PEAP, le client risque de ne pas s'authentifier correctement. Parfois la connexion initiale peut authentifier avec succès, mais les tentatives ultérieures d'authentification de connexion rapide ne se connectent pas avec succès. Il s'agit d'un problème identifié. Les détails de ce problème et du respectif correctif sont disponibles <u>ici.</u>

Informations connexes

- PEAP sous des réseaux sans fil unifiés avec ACS 4.0 et Windows 2003
- Exemple de configuration de l'authentification EAP avec des contrôleurs de réseau local sans fil (WLC)
- Mise à niveau logicielle de Wireless LAN Controller (WLC) aux versions 3.2, à 4,0 et 4,1
- Guides de configuration de Wireless LAN Controllers de la gamme Cisco 4400
- Assistance et documentation techniques Cisco Systems

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.