# PEAP onder Unified Wireless Networks met Microsoft Internet Verification Service (IAS)

# Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Conventies **PEAP** - Overzicht Configureren Netwerkdiagram Configuraties De Microsoft Windows 2003-server configureren De Microsoft Windows 2003-server configureren DHCP-services installeren en configureren op de Microsoft Windows 2003-server De Microsoft Windows 2003-server installeren en configureren als een certificeringsinstantie (CA)server Clients met domein verbinden Installeer de internetverificatieservice op de Microsoft Windows 2003-server en vraag een certificaat aan De internetverificatieservice configureren voor PEAP-MS-CHAP v2-verificatie Gebruikers toevoegen aan de actieve map Draadloze toegang voor gebruikers toestaan De draadloze LAN-controller en lichtgewicht AP's configureren De WLC voor RADIUS-verificatie configureren via MS IAS RADIUS-server WLAN's voor de clients configureren De draadloze clients configureren De draadloze clients voor PEAP-MS CHAPv2-verificatie configureren Verifiëren en probleemoplossing Gerelateerde informatie

# **Inleiding**

Dit document biedt een configuratievoorbeeld voor het instellen van een Protected Extensible Verification Protocol (PEAP) met Microsoft Challenge Handshake Verification Protocol (MS-CHAP), versie 2-verificatie in een Cisco Unified Wireless-netwerk met de Microsoft Internet Verification Service (IAS) als RADIUS-server.

# Voorwaarden

### **Vereisten**

Er wordt verondersteld dat de lezer kennis heeft van de basisinstallatie van Windows 2003 en de installatie van Cisco-controllers, aangezien dit document alleen betrekking heeft op de specifieke configuraties om de tests te vergemakkelijken.

**Opmerking:** Dit document is bedoeld om de lezers een voorbeeld te geven van de configuratie die vereist is op een MS-server voor PEAP - MS CHAP-verificatie. De Microsoft-serverconfiguratie die in deze sectie wordt gepresenteerd, is getest in het lab en blijkt te werken zoals verwacht. Als u problemen ondervindt bij het configureren van de Microsoft-server, neemt u contact op met Microsoft voor ondersteuning. Cisco TAC ondersteunt Microsoft Windows-serverconfiguratie niet.

Raadpleeg voor installatie- en configuratieinformatie voor Cisco 4400 Series controllers de <u>Quick</u> <u>Start Guide: Cisco 4400 Series draadloze LAN-controllers</u>.

U vindt de installatie- en configuratiehandleidingen voor Microsoft Windows 2003 op <u>Installing</u> <u>Windows Server 2003 R2</u>.

Voordat u begint, installeert u de Microsoft Windows Server 2003 met SP1-besturingssysteem op elk van de servers in het testlaboratorium en werkt u alle servicepakketten bij. Installeer de controllers en lichtgewicht access points en zorg ervoor dat de nieuwste software updates geconfigureerd zijn.

#### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 4400 Series controller voor de firmware versie 4.0
- Cisco 1131 lichtgewicht access point protocol (WAP) access point
- Windows 2003 Enterprise Server (SP1) met internetverificatieservice (IAS), certificeringsinstantie (CA), DHCP en geïnstalleerde DNS-services (Domain Name System)
- Windows XP Professional met SP2 (en bijgewerkte servicepakketten) en Cisco Aironet 802.11a/b/g draadloze netwerkinterfacekaart (NIC)
- Aironet Desktop Utility versie 4.0
- Cisco 3560 Switch

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

### **Conventies**

Raadpleeg <u>Cisco Technical Tips Conventions</u> (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

# PEAP - Overzicht

PEAP maakt gebruik van Transport Level Security (TLS) om een versleuteld kanaal te maken tussen een verificerende PEAP-client, zoals een draadloze laptop, en een PEAP-verificator, zoals Microsoft Internet Verification Service (IAS) of een RADIUS-server. PEAP specificeert geen

verificatiemethode, maar biedt aanvullende beveiliging voor andere EAP-verificatieprotocollen, zoals EAP-MSCHAPv2, die kunnen werken via het met TLS versleutelde kanaal dat door PEAP wordt geboden. Het PEAP-verificatieproces bestaat uit twee hoofdfasen:

#### PEAP fase één: TLS versleuteld kanaal

De draadloze client is gekoppeld aan het toegangspunt. Een op IEEE 802.11 gebaseerde associatie biedt een Open System of Shared Key-verificatie voordat een beveiligde associatie wordt gemaakt tussen de client en het access point (LAP). Nadat de op IEEE 802.11 gebaseerde verbinding tussen de client en het access point met succes is tot stand gebracht, wordt de TLS-sessie met het AP overeengekomen. Nadat de verificatie met succes is voltooid tussen de draadloze client en de IAS-server, wordt de TLS-sessie tussen de client en de IAS-server onderling overeengekomen. De sleutel die binnen deze onderhandeling wordt afgeleid wordt gebruikt om alle verdere communicatie te versleutelen.

#### PEAP fase twee: EAP-geverifieerde communicatie

EAP-communicatie, met inbegrip van EAP-onderhandeling, vindt plaats binnen het TLS-kanaal dat door PEAP in de eerste fase van het PEAP-verificatieproces is gecreëerd. De IAS-server verifieert de draadloze client met EAP-MS-CHAP v2. De LAP en de controller sturen alleen berichten door tussen de draadloze client en de RADIUS-server. De WLC en de LAP kunnen deze berichten niet decrypteren omdat het niet het TLS eindpunt is.

Nadat PEAP-fase één is opgetreden en het TLS-kanaal is gemaakt tussen de IAS-server en de 802.1X Wireless-client, is de RADIUS-berichtsequentie als volgt: voor een succesvolle verificatiepoging waarbij de gebruiker geldige, op een wachtwoord gebaseerde referenties heeft geleverd bij PEAP-MS-CHAP v2:

- 1. De IAS-server stuurt een identiteitsverzoekbericht naar de client: EAP-Verzoek/Identity.
- 2. De client reageert met een identiteitsresponsbericht: EAP-Response/Identity.
- 3. De IAS-server stuurt een MS-CHAP v2-provocatiebericht: EAP-request/EAP-Type=EAP MS-CHAP-V2 (Challenge).
- 4. De client reageert met een uitdaging en antwoord van MS-CHAP v2: EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Response).
- 5. De IAS-server stuurt een MS-CHAP v2-succespakket terug wanneer de server de client met succes heeft geverifieerd: EAP-request/EAP-Type=EAP-MS-CHAP-V2 (Success).
- 6. De client reageert met een succespakket van MS-CHAP v2 wanneer de client de server met succes heeft geverifieerd: EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Success).
- 7. De IAS-server stuurt een EAP-TLV die een geslaagde verificatie aangeeft.
- 8. De client reageert met een EAP-TLV-statusbericht.
- 9. De server voltooit de verificatie en verstuurt een EAP-Success-bericht met behulp van plaintext. Als VLAN's worden geïmplementeerd voor client-isolatie, zijn de VLAN-kenmerken in dit bericht opgenomen.

# **Configureren**

Dit document biedt een voorbeeld voor de configuratie van PEAP MS-CHAP v2.

**Opmerking:** Gebruik de <u>Command Lookup Tool (alleen voor geregistreerde klanten) voor meer</u> informatie over de opdrachten die in deze sectie worden gebruikt.

### **Netwerkdiagram**

Het netwerk in dit document is als volgt opgebouwd:



Wireless Client C1 Wireless Client C2

In deze installatie worden deze rollen uitgevoerd door een Microsoft Windows 2003-server:

- Domeincontroller voor het domein Wireless.com
- DHCP-/DNS-server
- CA-server (Certificate Authority)
- Active Directory voor het onderhouden van de gebruikersdatabase
- Internetverificatieservice (IAS) voor het verifiëren van de draadloze gebruikers

Deze server verbindt met het bekabelde netwerk via een Layer 2 switch zoals getoond.

De draadloze LAN-controller (WLC) en de geregistreerde LAP maken ook verbinding met het netwerk via Layer 2 switch.

Draadloze clients C1 en C2 gebruiken Wi-Fi Protected Access 2 (WPA2) - PEAP MSCHAP v2-verificatie om verbinding te maken met het draadloze netwerk.

Het doel is om de Microsoft 2003-server, draadloze LAN-controller en Light Weight AP te configureren om de draadloze clients te verifiëren met PEAP MSCHAP v2-verificatie.

In het volgende gedeelte wordt uitgelegd hoe u de apparaten voor deze installatie kunt configureren.

#### **Configuraties**

In deze sectie wordt gekeken naar de configuratie die nodig is om PEAP MS-CHAP v2-verificatie in dit WLAN in te stellen:

- De Microsoft Windows 2003-server configureren
- Configureer de draadloze LAN-controller (WLC) en de lichtgewicht AP's
- De draadloze clients configureren

Start met de configuratie van de Microsoft Windows 2003-server.

# De Microsoft Windows 2003-server configureren

### De Microsoft Windows 2003-server configureren

Zoals in het gedeelte Network Setup is vermeld, gebruikt u de Microsoft Windows 2003-server in het netwerk om deze functies uit te voeren.

- Domain Controller voor het domein Wireless
- DHCP-/DNS-server
- CA-server (Certificate Authority)
- Internetverificatieservice (IAS) voor het verifiëren van de draadloze gebruikers
- Active Directory voor het onderhouden van de gebruikersdatabase

Configureer de Microsoft Windows 2003-server voor deze services. Begin met de configuratie van de Microsoft Windows 2003-server als een Domain Controller.

#### De Microsoft Windows 2003-server configureren als domeincontroller

Voltooi de volgende stappen om de Microsoft Windows 2003-server als een domeincontroller te configureren:

 Klik op Start, klik op Uitvoeren, typ dcpromo.exe, en klik vervolgens op OK om de installatiewizard van Active Directory te starten.



2. Klik op **Next** om de installatiewizard van Active Directory uit te voeren.

٥,	perating Sustem 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> .

2

3. Kies de optie **Domeincontroller** voor een nieuw domein om een nieuw domein te maken.

omain C Specify	ontroller Type I the role you want this server to have.
Dio 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.
	( Pack Nouth Canool

4. Klik op **Volgende** om een nieuw bos met domeinbomen te maken.

ctive Directory Installation Wizard	×
Create New Domain Select which type of domain to create.	$\sum_{n}$
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.	
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. Als DNS niet op het systeem is geïnstalleerd, biedt de wizard u opties om DNS te configureren. Kies **Nee, Installeer en configureer DNS** op deze computer. Klik op **Next** (Volgende).

Install or Configure DNS         You can configure or install Domain Naming Service (DNS) on this computer.         Domain Naming Service (DNS) is not configured on this computer. Is DNS already running on this network?         Yes, I will configure the DNS client         No. just install and configure DNS on this computer.	tive Directory Installation Wizard			J
Domain Naming Service (DNS) is not configured on this computer. Is DNS already running on this network? ○ Yes, I will configure the DNS client • No, just install and configure DNS on this computer	Install or Configure DNS You can configure or install Domain Naming	Service (DNS) on this	computer.	
<ul> <li>Yes, I will configure the DNS client</li> <li>No, just install and configure DNS on this computer</li> </ul>	Domain Naming Service (DNS) is not config running on this network?	ured on this computer. I	s DNS already	
No. just install and configure DNS on this computer	○ Yes, I will configure the DNS client			
	No, just install and configure DNS on this	s computer		
< <u>B</u> ack <u>N</u> ext > Cancel		< <u>B</u> ack <u>N</u>	ext >	Cancel

 Typ de volledige DNS-naam voor het nieuwe domein. In dit voorbeeld wordt Wireless.com gebruikt en klikt u op Volgende.

ve Directory Installation Wizard	
<b>Vew Domain Name</b> Specify a name for the new domain.	
Type the full DNS name for the new dom (for example: headquarters.example.mic)	iain rosoft.com).
Eull DNS name for new domain:	
Wireless.com	
	< <u>B</u> ack <u>N</u> ext > Cance

7. Voer de NETBIOS-naam in voor het domein en klik op **Volgende**. In dit voorbeeld wordt **DRAADLOOS** gebruikt.

Active Directory Installation V	Vizard 🔀
<b>NetBIOS Domain Name</b> Specify a NetBIOS name fo	or the new domain.
This is the name that users domain. Click Next to acce	of earlier versions of Windows will use to identify the new pt the name shown, or type a new name.
Domain NetBIOS name:	WIRELESS
	< <u>B</u> ack <u>N</u> ext > Cancel

8. Kies de database en loglocaties voor het domein. Klik op **Next** (Volgende).

Directory Installation Wizaru			
tabase and Log Folders Specify the folders to contain the Active	e Directory database a	and log files.	AN AN
For best performance and recoverability hard disks.	, store the database a	ind the log on sepa	arate
Where do you want to store the Active I	Directory database?		
Database folder:			
C:\WINDOWS\NTDS		Bīow	se
Where do you want to store the Active I	Directory log?		

3

9. Kies een locatie voor de map Sysvol. Klik op Next (Volgende).

Active Directory Installation Wizard	×
<b>Shared System Volume</b> Specify the folder to be shared as t	he system volume.
The SYSVOL folder stores the serv of the SYSVOL folder are replicated	er's copy of the domain's public files. The contents d to all domain controllers in the domain.
The SYSVOL folder must be locate	d on an NTFS volume.
Enter a location for the SYSVOL fo	lder.
Eolder location:	
C:\WINDOWS\SYSVOL	B <u>r</u> owse
	< <u>B</u> ack <u>N</u> ext > Cancel

10. Kies de standaardrechten voor de gebruikers en groepen. Klik op **Next** (Volgende).

Permissions         Select default permissions for user and group objects.         Some server programs, such as Windows NT Remote Access Service, read information stored on domain controllers.            • 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.             M Anonymous users can read information on this domain.             Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems             Select this option if you run server programs only on Windows Server 2003 operating systems	Direc	tory Installation Wizard	
<ul> <li>Some server programs, such as Windows NT Remote Access Service, read information stored on domain controllers.</li> <li>Permissions compatible with pre-Windows 2000 server operating systems</li> <li>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.</li> <li>Anonymous users can read information on this domain.</li> <li>Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems</li> <li>Select this option if you run server programs only on Windows Server 2003 operating systems</li> </ul>	r <b>missi</b> Selec	i <b>ons</b> ct default permissions for user and group objects.	Ś
<ul> <li>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.</li> <li>Anonymous users can read information on this domain.</li> <li>Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems. Select this option if you run server programs only on Windows 2000 or Windows 2003 operating systems.</li> </ul>	Some stored	e server programs, such as Windows NT Remote Access Service, read infor d on domain controllers.	mation
Permissions compatible only with Windows 2000 or Windows Server 2003 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.	• Pe Se sy m	ermissions compatible with pre-Windows 2000 server operating systems elect this option if you run server programs on pre-Windows 2000 server ope ystems or on Windows 2000 or Windows Server 2003 operating systems tha tembers of pre-Windows 2000 domains. Anonymous users can read information on this domain.	erating It are
Server 2003 operating systems that are members of Active Directory domains. Unly authenticated users can read information on this domain.	O P <u>e</u> op Se	ermissions compatible only with Windows 2000 or Windows Server 2003 perating systems elect this option if you run server programs only on Windows 2000 or Windo	ws
	Se au	erver 2003 operating systems that are members of Active Directory domains. uthenticated users can read information on this domain.	. Unly

11. Stel het beheerderwachtwoord in en klik op **Volgende**.

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. Klik op **Volgende** om de eerder ingestelde Domain Options te accepteren.

<b>ummary</b> Beview and confirm the options you sele	ected	6
		×
You chose to:		
Configure this server as the first domain o	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 WI	RELESS	
Database folder: C:\WINDOWS\NTDS		
SYSVOL folder: C:\WINDOWS\NTDS SYSVOL folder: C:\WINDOWS\SYSVO	L	
The password of the new domain admini	istrator will be the same as the password	of
the administrator of this computer.		
		~
To change an option, click Back. To be	gin the operation, click Next.	
	< <u>B</u> ack <u>N</u> ext >	Cancel

13. Klik op **Voltooien** om de installatiewizard van Active Directory te sluiten.



14. Start de server opnieuw om de wijzigingen door te

Activ	e Directory Installation ¥	Vizard	
Win Dire	dows must be restarted before ctory Installation wizard take e	e the changes made by the Activ effect.	e

Met deze stap hebt u de Microsoft Windows 2003-server geconfigureerd als een Domain Controller en een nieuw domein gemaakt voor **Wireless.com**. Configureer vervolgens DHCPservices op de server.

### DHCP-services installeren en configureren op de Microsoft Windows 2003-server

De DHCP-service op de Microsoft 2003-server wordt gebruikt om IP-adressen aan de draadloze clients te leveren. Voltooi de volgende stappen om de DHCP-services op deze server te installeren en te configureren:

- 1. Klik op Software in het Configuratiescherm.
- 2. Klik op Windows-onderdelen toevoegen of verwijderen.
- 3. Kies Netwerkservices en klik op Details.
- 4. Kies Dynamic Host Configuration Protocol (DHCP) en klik op

Networking Services	le se
To add or remove a component, click the of the component will be installed. To see	check box. A shaded box means that only part what's included in a component, click Details.
Subcomponents of Networking Services:	
🗹 🚚 Domain Name System (DNS)	1.7 MB 🔄
🗹 🖳 Dynamic Host Configuration Proto	ocol (DHCP) 0.0 MB
🗌 🔲 📇 Internet Authentication Service	0.0 MB
🔲 🗆 👵 Remote Access Quarantine Servic	ice 0.1 MB
🔲 🗔 🚚 RPC over HTTP Proxy	0.0 MB
🗌 🗔 🚚 Simple TCP/IP Services	0.0 MB
🔲 🗔 🚚 Windows Internet Name Service (*	(WINS) 0.9 MB 🔄
Description: Sets up a DHCP server that addresses to client compute	at automatically assigns temporary IP ters on the same network.
Total disk space required: 3.4 M	MB Details
Space available on disk: 7224.5 M	MB
	OK Cancel

5. Klik op **Next** om de DHCP-service te installeren.

<b>indows Components</b> 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. Klik op **Voltooien** om de installatie te voltooien.



- 7. Om de DHCP-services te configureren klikt u op **Start > Programma's > Systeembeheer** en klikt u op de invoegtoepassing **DHCP**.
- 8. Kies de DHCP-server tsweb-lapt.wireless.com (in dit voorbeeld).
- 9. Klik op **Actie** en klik vervolgens op **Autoriseren** om DHCP-service te autoriseren.



- 10. Klik in de consolestructuur met de rechtermuisknop op **tsweb-lapt.wireless.com** en klik vervolgens op **New Scope** om een IP-adresbereik voor de draadloze clients te definiëren.
- 11. Klik op de pagina Welkom bij de wizard Nieuw bereik van de wizard Nieuw bereik op **Volgende**.



12. Typ op de pagina Naam bereik de naam van de DHCP-scope. In dit voorbeeld, gebruik DHCP-Clients als de scope naam. Klik op Next

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

13. Voer op de pagina IP-adresbereik de begin- en eindadressen voor de scope in en klik op **Volgende**.

New Scope Wizard
IP Address Range You define the scope address range by identifying a set of consecutive IP addresses.
Enter the range of addresses that the scope distributes.
Start IP address: 10 . 77 . 244 . 218
End IP address: 10 . 77 . 244 . 219
A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.
Length: 8
S <u>u</u> bnet mask: 255 . 0 . 0 . 0
< <u>B</u> ack <u>N</u> ext> Cancel

 Vermeld op de pagina Uitsluitingen toevoegen het IP-adres dat u wilt reserveren/uitsluiten van het DHCP-bereik. Klik op Next (Volgende).

exclude. If you want to exclude a single only.
onny.
. A <u>d</u> d
Remo <u>v</u> e
< Back Next > Cancel

15. Vermeld de leaseduur op de pagina Leaseduur en klik op **Volgende**.

w Scope Wizard	
Lease Duration The lease duration specifies how long a c scope.	lient can use an IP address from this
Lease durations should typically be equal to connected to the same physical network, portable computers or dial-up clients, short Likewise, for a stable network that consist locations, longer lease durations are more Set the duration for scope leases when dis	to the average time the computer is For mobile networks that consist mainly of er lease durations can be useful. s mainly of desktop computers at fixed appropriate.
Set the duration for scope leases when dis	stributed by this server.
Days: Hours: Minutes:	
	< Back Next > Cancel

 Kies op de pagina DHCP-opties configureren Ja, ik wil DHCP-optie nu configureren en klik op Volgende.

C	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
	< <u>B</u> ack <u>N</u> ext > Cancel

17. Als er een standaardgatewayrouter is, vermeld dan het IP-adres van de gatewayrouter op de pagina Router (Default Gateway) en klik op **Next**.

IP address:	Tor a roader asea by clients, enter the dutiess bi	
	Add	
10.77.244.220	<u>H</u> emove	
	Цр	
	D <u>o</u> wn	

 Typ op de pagina Domain Name en DNS servers de naam van het domein dat eerder is geconfigureerd. Gebruik in het voorbeeld Wireless.com. Voer het IP-adres van de server in. Klik op Add

(Toevoegen).

Domain Name The Domain clients on y	e <b>and DNS Servers</b> n Name System (DNS) maps a our network.	nd translates domain names	s used by
You can specify DNS name resol	the parent domain you want t ution.	he client computers on your	network to use for
Parent do <u>m</u> ain:	Wireless.com		
servers.			
servers. <u>S</u> erver name:		I <u>P</u> address:	Add
servers. <u>S</u> erver name:	R <u>e</u> solve	I <u>P</u> address:	A <u>d</u> d <u>B</u> emove
servers. <u>S</u> erver name:	R <u>e</u> solve	I <u>P</u> address:	A <u>d</u> d <u>R</u> emove Up
servers. <u>S</u> erver name:	R <u>e</u> solve	I <u>P</u> address:	A <u>d</u> d <u>R</u> emove Up D <u>o</u> wn

19. Klik op Next (Volgende).

20. Klik op de pagina WINS Server op Volgende.

21. Kies Ja op de pagina Werkingsgebied activeren, ik wil het bereik nu activeren en klik op Volgende.

New Scope Wizard	
Activate Scope Clients can obtain address leases only if a	scope is activated.
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. Klik op **Voltooien om** de wizard Nieuw bereik te voltooien.



23. Controleer in het venster DHCP Snapin of het DHCP-bereik dat is gemaakt actief

DHCP		Description of the		_ القاء	
e British Yern Help				De	
	142				
2 CHCP	baseb-lapt.ni-eless.com [10.77.3+1.217]				
10 Scope [172.16.0.0] DHCP-Clerks	Carteris al DHCP Server	3.9.15	Description		
- Server Optione	Scape [172.16.0.0] DHCP-Clients	** Active **	DHCP Server for Wineless Clients		
	and the open of				
	1				
	1				
	1				
	1				
	1				
	1				
	1				
	1				
	1				
	1				
	1				
	1				
	1				
	1				
	1				
	1				
	1				
	1				
	1				
	1				
	1				
	1				

Nu DHCP/ DNS is ingeschakeld op de server, moet u de server configureren als een ECA-server (Enterprise Certificate Authority).

De Microsoft Windows 2003-server installeren en configureren als een

#### certificeringsinstantie (CA)-server

PEAP met EAP-MS-CHAPv2 valideert de RADIUS-server op basis van het certificaat dat op de server aanwezig is. Bovendien moet het servercertificaat worden afgegeven door een openbare certificeringsinstantie (CA) die wordt vertrouwd door de clientcomputer (dat wil zeggen dat het openbare CA-certificaat al bestaat in de map Trusted Root Certification Authority op het certificaatarchief van de clientcomputer). In dit voorbeeld moet u de Microsoft Windows 2003-server configureren als een certificeringsinstantie (CA) die het certificaat afgeeft aan de Internet Verification Service (IAS).

Voltooi de volgende stappen om de certificaatservices op de server te installeren en te configureren:

- 1. Klik op Software in het Configuratiescherm.
- 2. Klik op Windows-onderdelen toevoegen of verwijderen.
- 3. Klik op

Ce	rtifi	caa	tse	rvic	es.

ows Components Wizard	
<b>∀indows Components</b> You can add or remove components of Windows.	ľ
To add or remove a component, click the checkbox. A shade part of the component will be installed. To see what's included Details.	d box means that only I in a component, click
<u>C</u> omponents:	
🖉 📻 Accessories and Utilities	4.9 MB 🔺
🖉 🧃 Application Server	34.4 MB 💻
🗹 😰 Certificate Services	1.8 MB
🗌 🛄 E-mail Services	1.1 MB
Ex Services	7.9 MB 🗾
Description: Installs a certification authority (CA) to issue certif public key security programs.	icates for use with
Total disk space required: 13.8 MB	Detaile
Space available on disk: 7310.6 MB	
< <u>B</u> ack <u>N</u> ext>	Cancel Help

4. Klik op Ja om het waarschuwingsbericht te waarschuwen. Na het installeren van certificaatservices kan de computer niet hernoemd worden en kan de computer niet worden toegevoegd aan of verwijderd worden uit een domein. Wilt u doorgaan?

Microso	ft Certificate Services	×	
	After installing Certificate Services, the machine name and domain membership may not be changed due to the binding of the machine name to CA information stored in the Active Directory. Changing the machine name or domain membership would invalidate the certificates issued from the CA. Please ensure the proper machine name and domain membership are configured before installing Certificate Services. Do you want to continue?		
	<u>No</u>		

5. Kies onder Certificate Authority Type de **Enterprise root CA**, en klik op **Volgende**.

dows components wiza	rd
<b>CA Type</b> Select the type of CA yo	ou want to set up.
Enterprise root CA	
C Enterprise subordinal	te CA
C Stand-alone root CA	
Stand-alone subordir	nate CA
<ul> <li>Description of CA type</li> <li>The most trusted CA in</li> </ul>	an enterprise. Should be installed before any other CA.
🔲 Use custom settings	to generate the key pair and CA certificate

 Voer een naam in om de CA te identificeren. In dit voorbeeld wordt Wireless-AC gebruikt. Klik op Next (Volgende).

Enter information to	dentity this CA.			U
Common name for this C	A:			
Wireless-CA				
Distinguished name suffi	×			
DC=Wireless,DC=com				
Preview of distinguished	name:			
CN=Wireless-CA,DC=W	/ireless,DC=com			
Validity period:		Expiration d	late:	
5 Years 💌		12/12/2012	2 7:01 PM	

7. Er wordt een directory "Cert Log" aangemaakt voor de opslag van de certificaatdatabase. Klik op **Next** 

(Volgende).

ndows Components Wizard	
Certificate Database Settings Enter locations for the certificate database, database log, and co information.	nfiguration
<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
S <u>h</u> ared folder:	
	Blowse
Preserve existing certificate database	
T Liberting Strend Sciences	
< Back Next >	Cancel Help

8. Als IIS is ingeschakeld, moet dit worden gestopt voordat u doorgaat. Klik op **OK** om te waarschuwen dat IIS moet worden gestopt. Het start automatisch opnieuw nadat CA is geïnstalleerd.

Microsof	t Certificate Services	×
	To complete the installation, Certificate Services must temporarily stop the Internet Information Services. Do you want to stop the	e service now?
	Yes No	

9. Klik op **Voltooien** om de installatie van de CA-diensten (Certificate Authority) te voltooien.



De volgende stap is het installeren en configureren van de Internet-verificatieservice op de Microsoft Windows 2003-server.

### Clients met domein verbinden

De volgende stap is om de clients te verbinden met het bekabelde netwerk en de domeinspecifieke informatie van het nieuwe domein te downloaden. Met andere woorden, verbind de cliënten met het domein. Voltooi de volgende stappen om dit te doen:

- 1. Sluit de clients aan op het bekabelde netwerk met een rechtstreekse Ethernet-kabel.
- 2. Start de client op en log in met de gebruikersnaam/ het wachtwoord van de client.
- 3. Klik op Start; klik op Uitvoeren; type cmd; en klik op OK.
- 4. Typ **ipconfig** bij de opdrachtprompt en klik op **Enter** om te verifiëren dat DHCP correct werkt en dat de client een IP-adres van de DHCP-server heeft ontvangen.
- 5. Om zich bij de cliënt aan het domein aan te sluiten, klik **Mijn Computer met de** rechtermuisknop aan, en kies **Eigenschappen**.
- 6. Klik op het tabblad Computer Name.
- 7. Klik op Wijzigen.
- 8. Klik op Domain; typ wireless.com; en klik op
| iompu<br>You ca | i <b>ter Name Chang</b><br>an change the name a | <mark>es</mark><br>and the n | nembership  | of this      |
|-----------------|---|------------------------------|-------------|--------------|
| compu           | iter. Changes may affe                          | ect acce:                    | ss to netwo | ork resource |
|                 |   |                              |             |              |
| Compu           | iter name:                                      |                              |             |              |
| Client          | 1   |                              |             |              |
| Men<br>()       | ber of<br>Domain:                               |                              |             | More         |
|                 | Wireless  |                              |             |              |
| 0               | Workgroup:                                      |                              |             |              |
|                 | WORKGROUP                                       |                              |             |              |
|                 |   |                              |             |              |
|                 |   |                              |             |              |
|                 |   |                              | nk 🔰        | Cance        |

9. Typ **Gebruikersnaam Administrator** en het wachtwoord dat specifiek is voor het domein waartoe de client toetreedt. (Dit is de Administrator-account in de Active Directory op de

Computer Nan	ne Changes	
Enter the name a to join the domai	and password of an account wi in.	th permission
<u>U</u> ser name:	🕵 administrator	<b>~</b>
Password		



- 10. Klik op OK.
- 11. Klik op **Ja** om de computer opnieuw op te starten.
- 12. Log na het opstarten van de computer in met de volgende informatie: Gebruikersnaam = **Beheerder**; Wachtwoord = <**domeinwachtwoord**>; Domein = **Draadloos**.
- 13. Klik met de rechtermuisknop op Deze computer en klik op Eigenschappen.
- 14. Klik op het tabblad **Computer Name** om te controleren of u zich op het Wireless.comdomein \_\_\_\_\_

System Re	store	Automa	atic Updates	Remote
General	Cor	mputer Name	Hardware	Advance
Wind on th	dows use ne netwo	es the following inf rk.	formation to identify	your computer
Computer <u>d</u> esc	ription:			
		For example: "I Computer".	Kitchen Computer''	or "Mary's
Full computer n	iame:	Client1.Wireles	s.com	
Domain:		Wireless.com		
domain and cre ID. To rename this	compute	cal user account, er or join a domain	click Network , click Change.	Network ID
▲ Changes	will take	effect after you re	estart this computer	
Changes	will (ake	errect arter you re	estart this computer	•

- 15. De volgende stap is te verifiëren dat de client het CA-certificaat (vertrouwen) van de server heeft ontvangen.
- 16. Klik op **Start**; klik op **Uitvoeren**; typ **mmc** en klik op **OK**.

17. Klik op **Bestand** en klik op Onverwacht-in **toevoegen/verwijderen**.

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

- 18. Klik op Add (Toevoegen).
- 19. Kies Certificaat en klik op

	Mandar
	Vendor
2. NET Framework 1.1 Configuration	Microsoft Corporation
	Microsoft Corporation
	Microsoft Corporation
	Microsoft Lorporation
Computer Management	Microsoft Lorporation
Borne Manager	Microsoft Corporation
Six Disk Defragmenter	Microsoft Corp, Executi.
Bisk Management	Microsoft and VERITAS
Event Viewer	Microsoft Corporation
E 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.
L	

20. Kies **Computeraccount** en klik op **Volgende**.

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

21. Klik op **Voltooien** om de standaard lokale computer te aanvaarden.

		-
Select Computer		X
Select the computer you wan	it this snap-in to manage.	
This same is will show as a		
i nis snaphn will always mar	lage.	
<ul> <li>Local computer: (the c</li> </ul>	omputer this console is running on)	
O Another computer:	Browse	
Allow the selected com only applies if you save	nputer to be changed when launching from the command line. This a the console.	
		_
	< Back Finish Cancel	

22. Klik op **Sluiten** en klik op **OK**.

23. Breid Certificaten uit (Local Computer); breid Trusted Root-certificeringsinstanties uit en klik op Certificaten. Zoek draadloos in de

IIJST. The Console1 - (Console Root)Certific	ates (Local Computer)\Trusted R	oot Certification Authorities/Cer	tificatesT			6
The Action View Eavorites Win	dow Help					_ IdClose
← → 🖻 🗷 🗞 🗙 🗗 🛱	1					
Console Root	Issued To /	Issued By	Expiration Date	Intended Purposes	Friendly Name	Statt 🔨
Certificates (Local Computer) H- Certificates H- Certif	Services Production Services Product Products Services Product Products Services Pr	SERVICIOS DE CERTIFICACION - A SIA Secure Clerk CA SIA Secure Server CA Sviskey Root CA To TrustCenter Class 1 CA TC TrustCenter Class 1 CA TC TrustCenter Class 2 CA TC TrustCenter Class 3 CA TC TrustCenter Class 3 CA TC TrustCenter Time Stanping CA Thavite Personal Previum CA Thavite Personal Previum CA Thavite Presional Previum CA Thavite Previous Server CA Thavite Previous Server CA Thavite TrustSerPrist-Network Applications UTN-USERPrist-Network Applications UTN-USERPrist-Network Applications UTN-USERPrist-Network Applications UTN-USERPrist-Network Applications UTN-USERPrist-Network VerSign Trust Network VerSign Trust Network	3/10/2009 7/9/2019 7/9/2019 1/1/2016 5/1/2011 1/1/2011 1/1/2011 1/1/2011 1/1/2011 1/1/2011 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2019 7/9/2019 1/8/2004 5/19/2018 8/2/2028 5/19/2018 8/2/2028 5/19/2018	Secure Enal, Server Secure Enal, Server Time Stamping Clerk Authentication Clerk Authentication Server Authentication Secure Enal, Server Time Stamping Server Authentication Secure Enal, Server Time Stamping, Code Secure Enal, Server Secure Enal, Code S Secure Enal, Clent Secure Enal, Clent	SERVICIOS DE CERT Societa Interbancari Societa Interbancari Societa Interbancari Societa Interbancari Societa Interbancari TC TrustCenter Clas TC TrustCenter Clas TC TrustCenter Clas TC TrustCenter Clas TC TrustCenter Time Thavte Personal Pre Thavte Server CA Thavte Server CA Thavte Timestampin UTN - USERFirst-Net UTN - USE	
<	CELDICert EZ by DST	Xcert EZ by DST	7/11/2009	Secure Email, Server	Xcert EZ by DST	> ×
Trusted Root Certification Authorities store co	ntains 109 certificates.					
de etart	Product a survey det de la deve as				****	0.40 PM
Start   Consciet - [Consc				<b>8</b> 9	40000000	2.42 Mi

24. Herhaal deze procedure om meer clients aan het domein toe te voegen.

# Installeer de internetverificatieservice op de Microsoft Windows 2003-server en vraag een certificaat aan

In deze setup wordt de Internet Authenticatieservice (IAS) gebruikt als een RADIUS-server voor het verifiëren van draadloze clients met PEAP-verificatie.

Voltooi deze stappen om IAS op de server te installeren en te configureren.

- 1. Klik op Software in het Configuratiescherm.
- 2. Klik op Windows-onderdelen toevoegen of verwijderen.
- 3. Kies Netwerkservices en klik op Details.
- 4. Kies Internet-verificatieservice; klik op OK; en klik op Volgende.

Networking Services	×
To add or remove a component, click the check box. A shaded box mean of the component will be installed. To see what's included in a componen	ns that only part t, click Details.
Sub <u>c</u> omponents of Networking Services:	
🗹 🛃 Domain Name System (DNS)	1.7 MB 🔺
🗹 🛃 Dynamic Host Configuration Protocol (DHCP)	0.0 MB
🗹 🖳 Internet Authentication Service	0.0 MB
📃 🔲 🚚 Remote Access Quarantine Service	0.1 MB
RPC over HTTP Proxy	0.0 MB
Simple TCP/IP Services	0.0 MB
🔲 🗔 🚚 Windows Internet Name Service (WINS)	0.9 MB 💌
Description: Enables authentication, authorization and accounting of di users. IAS supports the RADIUS protocol.	al-up and VPN
Total disk space required: 3.4 MB	Details.
Space available on disk: 7208.2 MB	
OK	Cancel

5. Klik op **Voltooien** om de IAS-installatie te voltooien.

Windows Components Wizard		×
	Completing the Windows Components Wizard You have successfully completed the Windows Components Wizard.	
	To close this wizard, click Finish.	
	≺ <u>B</u> ack. <b>Finish</b>	Help

- 6. De volgende stap is het installeren van het computercertificaat voor de Internetverificatieservice (IAS).
- 7. Klik op **Start**; klik op **Uitvoeren**; typ **mmc**; en klik op

UK.							
🚡 Console 1 - [Conso	ie Root]		7.0508.2019-2019	A State of the second second			×
🐞 Elle Action View	w Ravgeltes Window Help						_1@ X
* + 1 2	😢 🖾						
Canade Roat	Norec						
				There are no items to	show in this view.		
	1						
the set of the	1 48 Hotel Care	L marca	[ * sums muss				
a start	Reference Connections	1 200	A granger - [Ditts/1	war	Consolci - [Cons	HERE Rain	

- 8. Klik op **Console** in het menu Bestand en kies vervolgens module **toevoegen/verwijderen**.
- 9. Klik op Add om een invoegtoepassing toe te

dd/Remove Snap-	in		?)
Standalone Extens	ions		
Use this page to ad	d or remove a s	tand-alone snap-in	from the console.
Snap-ins added to:	Console P	Root	-
	1		
Description			] =
A <u>d</u> d	<u>R</u> emove	About	
			OK Cancel

10. Kies Certificaten uit de lijst met invoegtoepassingen en klik op

Snap-in	Vendor
🌆 .NET Framework 1.1 Configuration	Microsoft Corporation
Sective Directory Domains and Trusts	Microsoft Corporation
🚟 Active Directory Sites and Services	Microsoft Corporation
Active Directory Users and Compu	Microsoft Corporation
a 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.
[	D bba

11. Kies Computer-account en klik op Volgende.

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

12. Kies Lokale computer en klik op Voltogien

Select Computer			×
Select the computer you want this snap-in to r	manage.		
This snap-in will always manage:			
Local computer: (the computer this control of the computer the computer)	nsole is running on)		
C Another computer:		Biowse.	
Allow the selected computer to be cha only applies if you save the console.	nged when launching from	n the command line. T	his
only applies il you save the console.			
	( Back	Finish C	ancel
	V Eddy		

13. Klik op **Sluiten** en klik op **OK**.

14. Breid Certificaten uit (Local Computer); klik met de rechtermuisknop op Persoonlijke map; kies Alle taken en vraag vervolgens Nieuw certificaat



15. Klik op Volgende in de wizard Certificaataanvraag



16. Kies de **Domain Controller-**certificaatsjabloon (als u een computercertificaat aanvraagt op

een andere server dan de DC, kies een **Computer** certificaatsjabloon) en klik op **Volgende**.

tificate Types	
A certificate type contains preset pro	perties for certificates.
Select a certificate type for your requi you have permissions for and that are	uest. You can access only certificate types that e available from a trusted CA.
<u>C</u> ertificate types:	
Directory Email Replication Domain Controller Domain Controller Authentication	
<u> </u>	vider and a CAL select Advanced
To select a cryptographic service prov	vider and a CA, select Advanced.
To select a cryptographic service pro-	vider and a CA, select Auvanceu.

17. Typ een naam en een beschrijving voor het certificaat.

rtificate Friendly Name and I	Description			
You can provide a name and certificate.	d description that h	ielp you quickl	ly identify a specifi	ic
Type a friendly name and de	escription for the n	ew certificate	<b>4</b>	
Eriendly name:				
PEAP-Wireless				
Description:				
IAS Server Certificate - 80	2.1× Authenticatio	n		
			and the second se	

18. Klik op **Voltooien** om de wizard voor certificeringsaanvragen te voltooien.



### De internetverificatieservice configureren voor PEAP-MS-CHAP v2-verificatie

Nu u een certificaat voor de IAS hebt geïnstalleerd en aangevraagd, moet u de IAS configureren voor verificatie.

Voer de volgende stappen uit:

- 1. Klik op Start > Programma's > Systeembeheer en klik op Inloggen voor internetverificatie.
- 2. Klik met de rechtermuisknop op Internet Authenticatieservice (IAS) en klik vervolgens op Service registreren in Active Directory.

🖓 Internet Authentication Serv	eke		X
Ele ártion Yevi Lelp			
+ → 🗉 🗗 🔮 🖬 🤇	) (ii)		
Althonomet Austendization Service     (c) (c) (c) (c) (c) (c) (c) (c) (c)	Provide Span Lanvide Span Service Register Service in Active to Yew Popperties Belo	reate to Internet Authentication Service      represents to any access envert the is compatible with Renote Authentication Dial-In User Service (RACUE).      to read the remote access properties of user accounts in Advec Directory, on the Addon menu, clob Register Server in Active Directory, at an about setting up 145, deployment scenarios, and troubleshooting, see Help.	ार्ग प्र
Register Server is Active Directory	letwork Connections	Diric2 Advanget - [Dir2/15/400] Statemet Authenticate.	2 🛢 🗟 🕅 🍕 VI. 7.07 PM

3. De internetverificatieservice registreren in actieve map wordt weergegeven. Klik op OK. Hierdoor kan IAS gebruikers in de Active Directory

VERIFIEREN. Register Internet Authentication Server in Active Directory:	×
To enable IAS to authenticate users in the Active Directory, the computers running IAS must be authorized to read use	s' 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	

#### 4. Klik op **OK** in het volgende

dialoo	gvenster.
Server re	egistered: 🔀
1	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. Voeg de draadloze LAN-controller toe als AAA-client op de MS IAS-server.
- 6. Klik met de rechtermuisknop op **RADIUS-clients** en kies **Nieuwe RADIUSclient**.

🖓 Internet Authentication Service		
Elle Brition Yerk Help		
◆ → 🖪 🗄 🕄 😫 🖪		
Image: Product Acceleration Service (Local)       Product	Name Onter Connections to Morosoft Routing and Remote 1 Connections to other access servers 2	
New Clent	·	
🐮 Shart 🧉 🏀 Network Connection	a 🖞 DHCP 🔬 dranget - [DHC] 15 ADD 🗣 Internet Authentikati	😦 😤 🛢 💹 👯 👯 🕅 7.13PM

7. Typ de naam van de client (in dit geval WLC) en voer het IP-adres van de WLC in. Klik op **Next** 

#### (Volgende).

w RADIUS Client		
Name and Address		
Type a friendly name and	d either an IP Address or DNS n	name for the client.
Friendly name:	WLC	
Client address (IP or DN	5):	
10.77.244.210		⊻erify
	< <u>B</u> ack	<u>N</u> ext> Cancel

8. Kies op de volgende pagina onder Client-Verkoper **RADIUS-standaard**, voer het gedeelde geheim in en klik op **Voltooien**.

9. Bericht dat WLC als AAA-client wordt toegevoegd op de IAS.

<i>ii</i> (0.							
🖓 Internet Authentic	etion Service			1.1.1.1.1.1.1			×
Elle dution View I	alle a						Cee
◆ → 🗈 🗉 📾	3 8 3 1						
Internet Authenticati	on Service (Local)	Priendly Name /	Address	Protocol	Client/Vendor		
B 🔤 PAOLIS Clevis		U HLC	10.77.244.210	RADEUS	RADEUS Standard		
10 🤤 Remote Access Li 12 🥙 Demote Access D	20070	1					
E Connection Requ	est Processing						
		1					
		1					
		1					
2 Stat 6	Network Connections	Parce	Ater	gnt - [DHS],19AED	Patemet Authenticata.		🔹 🕄 🛢 🗟 👰 👯 🟹 7.12PM
	1	states of the second second				and the second second second second second	

- 10. Creëer een beleid voor externe toegang voor de clients.
- 11. Om dit te doen, klik je met de rechtermuisknop op **het beleid voor externe toegang** en kies je het **nieuwe beleid voor externe**

Gir Artion Yew Help ← → 100 100 13 12 100 100			
◆ → 1 H 3 B 3			
Internet Authentication Service (Local)     Book Access Looging     Convection Ser     Convection Ser     Convection Ser     Convection Service (Local)     Convection Service (Local)	Mere:	Crebs I 2	
			1

12. Typ een naam voor het beleid voor externe toegang. Gebruik in dit voorbeeld de naam **PEAP**. Klik vervolgens op **Volgende**.

ew 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.
	< <u>B</u> ack <u>N</u> ext> Cancel

13. Kies de beleidskenmerken op basis van uw vereisten. Kies in dit voorbeeld **Draadloos**.

w Remote Access Policy Wizard			×
Access Method Policy conditions are based on the method	used to gain acc	ess to the network	Ŷ
Select the method of access for which you w	ant to create a po	olicy.	
© VPN			
Use for all VPN connections. To create previous page, and select Set up a cu	e a policy for a sp stom policy.	ecific VPN type, g	o back to the
Dial-up			
Use for dial-up connections that use a Digital Network (ISDN) line.	traditional phone	line or an Integrate	ed Services
Use for wireless LAN connections only			
C Ethernet			
Use for Ethernet connections, such as	connections that	t use a switch.	
	< <u>B</u> ack	<u>N</u> ext>	Cancel

14. Kies op de volgende pagina **Gebruiker** om dit beleid voor externe toegang toe te passen op de lijst met gebruikers.

ew Remote Access Policy Wizard	
<b>User or Group Access</b> You can grant access to individual users, or you can grant access to selec groups.	ted
Grant access based on the following:	
<ul> <li><u>G</u>roup Individual user permissions override group permissions.</li> <li>Group name:</li> </ul>	
	A <u>d</u> d
	<u>R</u> emove
< <u>B</u> ack <u>N</u> ext>	Cancel

15. Kies onder Verificatiemethoden de optie **Protected EAP (PEAP)** en klik op **Configureren**.

New Remote Access Policy Wizard			×
Authentication Methods EAP uses different types of security devices	s to authenticate use	rs.	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. Kies op de pagina **Beschermde EAP-eigenschappen** het juiste certificaat in het vervolgkeuzemenu Certificaat afgeven en klik op

rties				
self to ca hat you w	illers before the connection vant it to use as proof of id	n is completed. Jentity.		
5	web-lapt.Wireless.com			
PEA	AP-Wireless			
Wireless-CA				
12/	12/16/2008 5:53:02 PM			
inect				
AP-MSCH	AP v2)	Move L		
		Move Do		
Edit	Remove	OK Cance		
	rties self to ca hat you v Is PE4 Wir 12/ nect AP-MSCH	self to callers before the connection hat you want it to use as proof of ic tsweb-lapt.Wireless.com PEAP-Wireless Wireless-CA 12/16/2008 5:53:02 PM nect AP-MSCHAP v2)		

17. Controleer de details van het beleid voor externe toegang en klik op **Voltooien**.

#### New Remote Access Policy Wizard



X

18. Het beleid voor externe toegang is toegevoegd aan de



19. Klik met de rechtermuisknop op het beleid en klik op Eigenschappen. Kies "Toestemming voor externe toegang verlenen" onder "Als een verbindingsverzoek aan de opgegeven voorwaarden

ettings				
Specify the con	ditions that conne	ction requests	must match.	
Policy <u>c</u> ondition:	s:			
NAS-Port-Type	matches "Wirele	ss - Other OR	Wireless - IEE	E 802.11"
•				
ا بده		Damana	-	
A <u>0</u> 0	<u>E</u> ak	<u>H</u> emove		
If connection re-	quests match the	conditions spe	ecified in this p	olicy, the
BAAAAA BAAAA BAAAA	e will de addileu (			
associated profil		o the connect	1011.	
Edit Profile				
Edit Profile	l access permissi	ons are specif	ied in the user	profile, this
Edit <u>Profile</u> Unless individua policy controls a	l access permissi ccess to the netv	ons are specif	ied in the user	profile, this
Edit <u>Profile</u> Unless individua policy controls a	l access permissi ccess to the netv equest matches I	ons are specif vork.	ied in the user	profile, this
Edit Profile Unless individua policy controls a If a connection i	I access permissi ccess to the netv equest matches I access permissi	ons are specif vork. the specified c	ied in the user	profile, this
Edit Profile Unless individua policy controls a If a connection r Deny remote	I access permissi ccess to the netv equest matches I access permissi	ons are specif vork. the specified c on	ied in the user	profile, this
Edit Profile Unless individua policy controls a If a connection r Deny remote Grant remote	I access permissi ccess to the netv equest matches I access permissi access permissi	ons are specif vork. the specified c on	ied in the user	profile, this
Edit Profile Unless individua policy controls a If a connection r Deny remote Grant remote	I access permissi ccess to the netv equest matches I access permissi access permissi	ons are specif vork. the specified o on	ied in the user	profile, this

#### voldoet".

#### Gebruikers toevoegen aan de actieve map

In deze instelling wordt de gebruikersdatabase onderhouden in de Active Directory.

Voltooi de volgende stappen om gebruikers aan de Active Directory-database toe te voegen:

1. In de Active Directory-console-structuur Gebruikers en Computers klikt u met de rechtermuisknop op **Gebruikers**, klikt u op **Nieuw** en klikt u vervolgens op **Gebruiker**.



 Typ in het dialoogvenster Nieuw object - gebruiker de naam van de draadloze gebruiker. In dit voorbeeld wordt de naam Draadloze gebruiker gebruikt in het veld Voornaam en Draadloze gebruiker in het veld Gebruikersnaam. Klik op Next (Volgende)

Vo	lgende	).

com/Users		
	Initials:	
@Wireless	.com	•
2000):		
Client1		
< Back	Next >	Cancel
	:.com/Users @Wireless 2000): Client1 < <u>B</u> ack	:.com/Users Initials: @Wireless.com 2000): Client1 < Back Next >

3. Typ in het dialoogvenster Nieuw object - gebruiker een wachtwoord naar keuze in de velden Wachtwoord en Wachtwoord bevestigen. Wis het **wachtwoord** van de **gebruiker bij de** 

volgende aanmelding en klik op Volgende.

New Object - User		×
Create in: Wireless.	com/Users	
Password:	•••••	
<ul> <li>User must change password a</li> <li>User cannot change password</li> <li>Password never expires</li> <li>Account is disabled</li> </ul>	at next logon d	
	< <u>B</u> ack <u>N</u> ext > Cancel	

4. Klik in het dialoogvenster Nieuw object - gebruiker op



Voltooien.

5. Herhaal stap 2 tot en met 4 om extra gebruikersaccounts te maken.

#### Draadloze toegang voor gebruikers toestaan

Voer de volgende stappen uit:

- 1. Klik in de structuur van de Active Directory-console op de **gebruikersmap**, klik met de rechtermuisknop op **Draadloze gebruiker**, klik op **Eigenschappen** en ga vervolgens naar het **tabblad Inbellen**.
- 2. Kies Toegang toestaan en klik op

General Address Accou Member Of Dial-in	Terminal Servic Int Profile Envi	es Profile   Telephones   ronment	COM+ Organization Sessions
- Remote Access Permission (I	Dial-in or VPN)		
Allow access			
C Deny access			
C Control access through R	emote Access <u>I</u>	Eolicy	
☐ ⊻erify Caller-ID:	Г		
Callback Options	I		J
No <u>C</u> allback			
C Set by Caller (Routing an	d Remote Acce	ess Service only)	
C Always Callback to:	Γ		
Assign a Static IP Addres	÷ ۲		
Apply Static <u>B</u> outes			
Define routes to enable for t	his Dial-in	Static Ro <u>u</u>	tes
CONNECTION.			
connection.			

# De draadloze LAN-controller en lichtgewicht AP's configureren

Configureer nu de draadloze apparaten voor deze installatie. Dit omvat de configuratie van de draadloze LAN-controllers, lichtgewicht AP's en draadloze clients.

#### De WLC voor RADIUS-verificatie configureren via MS IAS RADIUS-server

Configureer eerst de WLC om de MS IAS als verificatieserver te gebruiken. De WLC moet worden geconfigureerd om de gebruikersreferenties te kunnen doorsturen naar een externe RADIUS-server. De externe RADIUS-server valideert vervolgens de gebruikersreferenties en biedt toegang tot de draadloze clients. Hiertoe voegt u de MS IAS-server als een RADIUS-server toe op de pagina **Security > RADIUS-verificatie**.

Voer de volgende stappen uit:

1. Kies **Beveiliging** en **RADIUS-verificatie** in de GUI van de controller om de pagina RADIUSverificatieservers weer te geven. Klik vervolgens op **Nieuw** om een RADIUS-server te

#### definiëren.

3 · 🔘 🖹 🖻	🚯 🔎 🛧 🚱 🍛 🎍	<b>3</b>					📲 – 8 >
					Save C	onfiguration   Ping	Logout   Refres
A.A.	MONITOR WLANS CONTR	OLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	RADIUS Authentication Ser	vers > New				< Back	Apply
General	Server Index (Priority)	1 💌					
RADIUS Accounting Local Net Users	Server IPAddress	10.77.244.198					
MAC Filtering Disabled Clients	Shared Secret Format	ASCII ¥					
AP Policies	Shared Secret	•••••				]	
ccess Control Lists	Confirm Shared					1	
PSec Certificates CA Certificate	Secret					1	
ID Certificate	Key Wrap						
Wireless Protection Policies	Port Number	1812					
Trusted AP Policies Rogue Policies Standard Signatures	Server Status	Enabled 💌					
Custom Signatures Client Exclusion Policies	Support for RFC 3576	Enabled 💌					
AP Authentication	Retransmit Timeout	2 seconds					
	Network User	Enable					
	Management	Enable					
	IPSec	🔄 Enable					

2. Definieer de RADIUS-serverparameters in de RADIUS-verificatieservers > Nieuwe pagina. Deze parameters omvatten het IP-adres van de RADIUS-server, gedeeld geheim, poortnummer en serverstatus. Met de selectievakjes Netwerkgebruiker en Netwerkbeheer wordt bepaald of de op RADIUS gebaseerde verificatie van toepassing is op beheer- en netwerkgebruikers. In dit voorbeeld wordt de MS IAS gebruikt als de RADIUS-server met IPadres

10.77.244.198.

3 · 0 · 1	6 py	8 8 3.	200	8				4	7 - 8
insce Sentene	MONITOR	WLANS CO	ONTROLLER	WIRELESS 5	ECURITY	MANAGEMENT C	Save Configuratio	m Ping Logo	ut Refre
Security	RADIUS A	Authentication	n Servers				A	pply New	
CAA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Rittering Disabled Clients User Login Policies	Call Stati Credentia Use AES	on ID Type als Caching Key Wrap	IP Address	×					
Access Control Lists	User	Management	Server	Server Address	Port	IPSec	Admin Status		
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	Eina

- 3. Klik op Apply (Toepassen).
- 4. MS IAS server is toegevoegd aan de WLC als een Radius server en kan worden gebruikt om draadloze clients te verifiëren.

#### WLAN's voor de clients configureren

Configureer de SSID (WLAN) waarmee de draadloze clients verbinding maken. Maak in dit voorbeeld de SSID en noem het **PEAP**.

Definieer Layer 2-verificatie als WPA2, zodat de clients EAP-gebaseerde verificatie (in dit geval PEAP-MSCHAPv2) uitvoeren en AES als coderingsmechanisme gebruiken. Laat alle andere waarden op hun defaults staan.

**Opmerking:** dit document bindt het WLAN aan de beheerinterfaces. Wanneer u meerdere VLAN's in uw netwerk hebt, kunt u een afzonderlijk VLAN maken en het aan de SSID binden. Raadpleeg <u>VLAN's op Wireless LAN Controllers</u> Configuration <u>Voorbeeld voor</u> informatie <u>over het</u> configureren <u>van</u> VLAN's <u>op</u> WLC's.

Voltooi de volgende stappen om een WLAN op de WLC te configureren:

- 1. Klik op **WLAN's** vanuit de GUI van de controller om de WLAN-pagina weer te geven. Deze pagina maakt een lijst van de WLAN's die op de controller bestaan.
- Kies Nieuw om een nieuw WLAN te maken. Voer de WLAN-id en de WLAN-SSID voor het WLAN in en klik op Toepassen.



 Zodra u een nieuw WLAN maakt, wordt de pagina WLAN > Bewerken voor het nieuwe WLAN weergegeven. Op deze pagina kunt u verschillende parameters definiëren die specifiek zijn voor dit WLAN, zoals Algemeen beleid, RADIUS-servers, beveiligingsbeleid en 802.1x-

parameters.

Cinco Statun					Save Co	onfiguration Ping	Logout   Refre	
do do	MONITOR WLANS	CONTROLLER WIREL	SS SECURITY	MANAGEMENT	COMMANDS	HELP		
WLANs	WLANs > Edit					< Back	Apply	
WLANS	WLAN ID	1						
WLANS AP Groups VLAN	Profile Name	PEAP						
	WLAN SSID	/LAN SSID PEAP						
	General Policies				Security Polici	ies		
	Radio Policy	All			IPv6 Enable			
	Admin Status	Enabled						
	Session Timeout (see	s) 0			Layer 2 Securi	WPA1+W	PA2 ·	
	Quality of Service (QoS) Silver (best effort)		MAC Fil	tering				
	WMM Policy	Disabled 💌			Lawer 3 Caruri	the liters	100	
	7920 Phone Support	Client CAC Limit	AP CAC Limit		cajer 3 securi	Ly [Wah Ga		
	Broadcast SSID	Enabled				I web Policy		
	Aironet IE	Enabled						
	Allow AAA Override	Enabled			* Web Policy o	annot be used in co	ombination with	
	Client Exclusion	Enabled ** 60			irsec.			
		Time	out Value (secs)		value of zero n	neans infinity(will r	equire	
	DHCP Server	Overnde			*** CKIP is not	supported by 10xx APs		
	DHCP Addr. Assignm	int L Required						
	Interface Name	management 💌						
	MFP Version Required	1						
	MFP Signature Generation	🗹 (Global MFP Disat	led)					
	H-REAP Local Switchi	- D						
	* H-REAP Local Switc authentications.	hing not supported with IP:	EC, CRANITE and	FORTRESS				

- 4. Controleer **Admin Status** onder Algemeen beleid om het WLAN in te schakelen. Als u wilt dat het toegangspunt de SSID uitzendt in zijn beacon-frames, controleer dan **Broadcast SSID**.
- 5. Kies onder Layer 2-beveiliging WPA1+WPA2. Dit schakelt WPA in op het WLAN. Blader naar beneden op de pagina en kies het WPA-beleid. In dit voorbeeld worden WPA2 en AESencryptie gebruikt. Kies de juiste RADIUS-server in het keuzemenu onder RADIUS-servers. Gebruik in dit voorbeeld 10.77.244.198 (IP-adres van de MS IAS-server). De andere parameters kunnen worden aangepast op basis van de behoefte van het WLANnetwerk.

	Cinco Svercon							Save Co	onfiguration	Ping	Logout	Refres	:h
	Andrea	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP				
	WLANS	WPA1+WI Paramete WPA1 Pai	PA2 rs			-							
	AP Groups VLAN	WPA2 En: Auth Key	ryption Mgmt	AES 802.1x	Ткзр								
6.	Klik op <b>Apply</b>												
	(Toepassen).												
	Cinca Srereus							Save C	onfiguration	Ping	Logout	Refres	ιh
	A. A.	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP				
	WLANS	WLANS											
	WLANS	Profile Na	me	W	D WLAN S	SID	Adı Sta	min Secur tus	ity Policies				
	AP Groups VLAN	PEAP		1	PEAP		Eni	abled [WPA	2][Auth(80	2.1x)]		Edit B	em
		* WLAN IDS	: 9-16 will n	iot be pushed to 1	1130,1200 and	1240 AP mode	8.						

## De draadloze clients configureren

#### De draadloze clients voor PEAP-MS CHAPv2-verificatie configureren

Dit voorbeeld bevat informatie over de manier waarop u de draadloze client kunt configureren met het Cisco Aironet Desktop Utility. Zorg ervoor dat de nieuwste versie van de firmware en het hulpprogramma wordt gebruikt voordat u de clientadapter configureert. Vind de nieuwste versie van de firmware en hulpprogramma's op de pagina Draadloze downloads op Cisco.com.

Voltooi de volgende stappen om de Cisco Aironet 802.11 a/b/g draadloze clientadapter met de ADU te configureren:

1. Open het Aironet-desktophulpprogramma.

aeconfigureerd

- 2. Klik op Profielbeheer en klik op Nieuw om een profiel te definiëren.
- 3. Voer op het tabblad Algemeen de naam van het profiel en de SSID in. Gebruik in dit voorbeeld de SSID die u op de WLC (PEAP) hebt

Profile Management	
General Security Advanc	ed
Profile Settings Profile Name: Client Name:	PEAP-MSCHAPv2 CLIENT1
Network Names SSID1:	PEAP
SSID3:	
	OK Cancel

 Kies het tabblad Beveiliging; kies WPA/WPA2/CCKM; typ onder WPA/WPA2/CCKM EAP de optie PEAP [EAP-MSCHAPv2] en klik op Configureren.

Profile Management		? 🗙
General Security Advanced		
- Set Security Options		
⊙ WPA/WPA2/CCKM	WPA/WPA2/CCKM EAP Type: FEAP (EAP-MSCHAP V2)	
O WPA/WPA2 Passphrase		
◯ 802.1x	802.1x EAP Type: EAP-FAST	
O 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	
	ОКССА	ancel

5. Kies **Servercertificaat valideren** en kies **Wireless-AC** onder het vervolgkeuzemenu Trusted Root Certificate

Co	nfigure PEAP (EAP-MSCHAP V2)
	Use Machine Information for Domain Logon
[	Validate Server Identity
	Trusted Root Certification Authorities
	Wireless-CA
ľ	When connecting, use:
	O Certificate
	<ul> <li>User Name and Password</li> </ul>
	Select a Certificate
	Use Windows User Name and Password
	User Information for PEAP (EAP-MSCHAP V2) Authentication
	User Name: Administrator
	Password:
	Caution Descenard
	Contributer datawolida
	Advanced Control Concel

6. Klik op OK en activeer het profiel.Opmerking: wanneer u het Protected EAP-Microsoft Challenge Handshake Verificatieprotocol versie 2 (PEAP-MSCHAPv2) met Microsoft XP SP2 gebruikt en de draadloze kaart wordt beheerd door Microsoft Wireless Zero Configuration (WZC), moet u de Microsoft hotfix KB885453 toepassen. Dit voorkomt verschillende problemen met de verificatie in verband met PEAP Fast Resume.

# Verifiëren en probleemoplossing

Om te controleren of de configuratie werkt zoals verwacht, activeert u het profiel PEAP-MSCHAPv2 op de draadloze client Client1.
😨 Cisco Aironet Desktop Utility - Current Profile: PEAP-MSCHAPv2 🛛 😨 🔀		
<u>Action Options H</u> elp		
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

Nadat het profiel PEAP-MSCHAPv2 op de ADU is geactiveerd, voert de client 802.11 open verificatie uit en voert vervolgens PEAP-MSCHAPv2-verificatie uit. Hier is een voorbeeld van succesvolle PEAP-MSCHAPv2-verificatie.

Gebruik de debug commando's om de volgorde van de gebeurtenissen te begrijpen die voorkomen.

De <u>Output Interpreter Tool</u> (OIT) (alleen voor <u>geregistreerde</u> klanten) ondersteunt bepaalde opdrachten met **show**. Gebruik de OIT om een analyse te bekijken van de output van de opdracht **show**.

Deze debug-opdrachten op de draadloze LAN-controller zijn handig.

- debug dot1x gebeurtenissen inschakelen —om het debuggen van 802.1x gebeurtenissen te configureren
- debug aaa gebeurtenissen enable-om het zuiveren van gebeurtenissen te vormen AAA
- debug mac addr <mac address> —om MAC-debugging te configureren gebruikt u de opdracht debug mac

• debug dhcp bericht inschakelen —om debug van DHCP-foutmeldingen te configureren Dit zijn de voorbeelduitgangen van de debug dot1x gebeurtenissen toelaten bevel en zuiveren client <mac address> bevel.

debug dot1x gebeurtenissen inschakelen:

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 = 0x00000000,
   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
```

**Opmerking:** als u de Microsoft Supplicant gebruikt voor verificatie met een Cisco Secure ACS voor PEAP-verificatie, wordt de client mogelijk niet geverifieerd. Soms kan de eerste verbinding met succes worden geverifieerd, maar latere pogingen voor snelle verificatie maken geen verbinding met succes. Dit is een bekende kwestie. De details van dit probleem en de oplossing voor hetzelfde zijn <u>hier</u> beschikbaar.

## Gerelateerde informatie

- PEAP onder Unified Wireless Networks met ACS 4.0 en Windows 2003
- Configuratie-voorbeeld van EAP-verificatie met WLAN-controllers (WLC)
- Software-upgrade voor draadloze LAN-controllers (WLC) naar versies 3.2, 4.0 en 4.1
- <u>Cisco 4400 Series configuratiehandleidingen voor draadloze LAN-controllers</u>
- Technische ondersteuning en documentatie Cisco Systems

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.