# Trusted AP-beleid op een draadloze LANcontroller

## Inhoud

Inleiding Voorwaarden Vereisten Conventies Trusted AP-beleid Wat is een Trusted AP? Hoe te om AP als Betrouwbare AP te configureren vanuit de WLC GUI? De betekenis van Trusted AP-beleidsinstellingen Hoe moet u het vertrouwde AP-beleid op de WLC configureren? Trusted AP-waarschuwingsbericht Gerelateerde informatie

## Inleiding

Dit document beschrijft het *vertrouwde AP* draadloze beschermingsbeleid op een Draadloze LAN controller (WLC), definieert een betrouwbaar AP-beleid en biedt een korte beschrijving van al het vertrouwde AP-beleid.

## Voorwaarden

## **Vereisten**

Zorg ervoor dat u een basisbegrip van de draadloze LAN veiligheidsparameters (zoals SSID, encryptie, authenticatie, etc.) hebt.

## **Conventies**

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

## **Trusted AP-beleid**

Trusted AP-beleid is een beveiligingsfunctie in de controller die ontworpen is om te worden gebruikt in scenario's waar klanten naast de controller een parallel autonoom AP-netwerk hebben. In dat scenario kan de autonome AP als vertrouwde AP op de controller worden gemarkeerd en kan de gebruiker beleid voor deze vertrouwde AP's definiëren (die alleen EVN of WAP, onze eigen

SSID, korte preambule enzovoort zouden moeten gebruiken). Als een van deze AP er niet in slaagt aan dit beleid te voldoen, heft de controller een alarm in het netwerkbeheerapparaat (Wireless Control System) dat stelt dat een vertrouwde AP een geconfigureerd beleid heeft overtreden.

## Wat is een Trusted AP?

Betrouwbare AP's zijn AP's die geen deel uitmaken van een organisatie. Ze veroorzaken echter geen veiligheidsbedreiging voor het netwerk. Deze AP's worden ook vriendelijke AP's genoemd. Er zijn meerdere scenario's waar u een AP als een vertrouwde AP zou willen configureren.

U kunt bijvoorbeeld verschillende categorieën AP's in uw netwerk hebben zoals:

- APs u die niet LWAPP (wellicht lopen zij IOS of VxWorks) uitvoeren
- LWAPP AP's die werknemers inbrengen (met kennis van de beheerder)
- LWAPP APs die worden gebruikt om het bestaande netwerk te testen
- LWAPP APs die buren bezitten

Normaal gesproken zijn vertrouwde APs APs die in **categorie 1** vallen, die APs zijn die u bezit die geen LWAPP lopen. Het kunnen oude APs zijn die VxWorks of IOS runnen. Om ervoor te zorgen dat deze APs het netwerk niet beschadigen, kunnen bepaalde eigenschappen worden afgedwongen, zoals correcte SSIDs en authenticatie-types. Configureer het vertrouwde AP-beleid op de WLC en zorg ervoor dat de vertrouwde APs aan dit beleid voldoen. Als dit niet het geval is, kunt u de controller configureren om verschillende handelingen uit te voeren, zoals een alarm afslaan naar het netwerkbeheerapparaat (WCS).

Bekende AP's die tot de buren behoren kunnen als vertrouwde APs worden gevormd.

Normaal gesproken zou MFP (Management Frame Protection) AP's die geen legitieme LWAPP AP's zijn moeten verhinderen om zich bij de WLC aan te sluiten. Als NIC-kaarten MFP ondersteunen, mogen zij geen afwijkingen van andere apparaten dan de echte AP's accepteren. Raadpleeg <u>MFP</u> (Infrastructuur Management Frame Protection<u>) met WLC en LAP Configuration</u> <u>Voorbeeld</u> voor meer informatie over MFP.

Als u AP's hebt die VxWorks of IOS (zoals in categorie 1) lopen, zullen zij zich nooit bij de LWAPP groep aansluiten of MFP doen, maar u zou het beleid kunnen willen afdwingen dat op die pagina vermeld staat. In dergelijke gevallen moet het vertrouwde AP-beleid op de controller worden ingesteld voor de AP's van belang.

In het algemeen, als je weet over een schurkenpas en identificeert dat het geen bedreiging voor je netwerk is, kun je dat AP als bekend vertrouwde AP identificeren.

## Hoe te om AP als Betrouwbare AP te configureren vanuit de WLC GUI?

Voltooi deze stappen om een AP als vertrouwde AP te configureren:

- 1. Log in op de GUI van de WLC via HTTP of https inloggen.
- 2. Klik in het hoofdmenu van de controller op Draadloos.
- Klik in het menu aan de linkerkant van de draadloze pagina op AP's van de Roep.

isco - Microsoft Internet Expl	lorer provided by Cisco Systems, Inc.		<u> </u>			_ 0
ne gan gew rigwannes g	loos Reb			Save Configurati	on Ping L	ogout Refres
6	MONITOR WLANS CONTROLLER	WIRELESS SECURITY MAN	AGEMENT COM	MANDS HELP		
lireless	All APs					
ccess Points	Search by Ethernet MAC	Search				
All APs 802.11a Radios						
802.11b/g Radios Third Party APs	AP Name	AP ID Ethernet MAC	Admin Status	Operational Status	Port	
ridging	ap:Sb:fb:d0	34 00:0b:85:5b:fb:d0	Enable	REG	2	Detail
Rogue APs	ap:51:Sa:e0	35 00:0b:85:51:5a:e0	Enable	REG	2	Detail
Rogue Clients						
Adhoc Rogues ients						
obal RF						
802.11a Network 802.11b/g Network 802.11h						
ountry						
mers						
Discussions • 🎲 🞲 🗐	3 3 1 E ØDiscussions not available on htt	p://10.77.244.204/			1	

De pagina Verkennende APs maakt een lijst van alle APs die als schurk APs op het netwerk worden gedetecteerd.

- 4. Van deze lijst van schurkenAP's, plaats AP die u als vertrouwde AP wilt configureren dat onder categorie 1 valt (zoals uitgelegd in de vorige sectie). U kunt APs met de MAC adressen vinden die op de pagina van Rogue APs worden vermeld. Als het gewenste AP niet in deze pagina staat, klik op Volgende om het AP van de volgende pagina te identificeren.
- 5. Zodra het gewenste AP van de lijst van AP van de Rogue is gevestigd, klik de knop **Bewerken** die aan AP correspondeert, wat u aan de detailpagina van AP neemt.

Rogue APs			Item	s 1 to 20 of 26	Next
MAC Address	SSID	# Detecting Radios	Number of Clients	Status	
00:02:8a:0e:33:f5	Unknown	1	0	Pending	Edit
00:07:50:d5:cf:b9	Unknown	1	0	Pending	Edit
00:0b:85:51:5a:ee	Unknown	0	0	Containment Pending	Edit
00:0c:85:eb:de:62	Unknown	1	0	Alert	Edit
00:0d:ed:be:f6:70	Unknown	2	0	Alert	Edit
00:12:01:a1:f5:10	auto-2	1	0	Pending	Edit

In de pagina met informatie over Rogue AP kunt u gedetailleerde informatie over deze AP vinden (zoals of die AP verbonden met verbonden netwerk, zowel als de huidige status van AP etc.).

6. Om deze AP als vertrouwde AP te configureren selecteert u **Bekende Interne** van de vervolgkeuzelijst Stand van de Update Status en klikt u op **Toepassen**.Wanneer u de AP status aan *gekend intern* bijwerken, wordt deze AP gevormd als vertrouwde AP van dit

#### netwerk.

A A	MONITOR WI ANE			SECURITY	MANAGEMEN	л сом		uration F	ing Logou	rt   Refres
Wireless	Roque AP Detail	CONTROLLER	TINECESS	Secondin	MAN BROCHTER			< Back		volv
Access Points All APs 802.11a Radios	MAC Address			00:12:01:01:f	5:10			- BUCK		
Third Party APs	Is Poque On Wired N	etwork?		No						
Rogues Rogue APs Known Rogue APs	First Time Reported On	ietholki		Wed Dec 12 1	2:27:28 2007					
Rogue Clients Adhoc Rogues	Last Time Reported On			Wed Dec 12 1	3:13:09 2007					
Clients Global RF	Current Status			Known						
802.11b/g Network 802.11h	Update Status			Choose I	New Status ] Iew Status	3				
Country Timers				Contain Rogu Alert Unknown Known Intern Acknowledge	e n Sil					
	APs that detected t	his Rogue		Hechowieoge	C. A. OPTITUDE					
	Base Radio MAC	AP Name	\$\$1	D	Channel	Radio Type	WEP	WPA	Pre- Amble	RSSI
	00:0b:85:51:5a:e0	ap:51:5a:e0	auto	i+2	1	802.11g	Enabled	Enabled	Short	-71
	Clients associated t MAC Address	o this Rogue Last	AP Time Heard							
	al.						1			
Discussions * 1 87 Dr. E	1 E1 #1 #1 [1] Menut	or out multiple on	Marchine TT 244	204/						

7. Herhaal deze stappen voor alle AP's die u als vertrouwde APs wilt configureren.

### Controleer de Trusted AP-configuratie

Voltooi deze stappen om te controleren of de AP correct is ingesteld als vertrouwde AP van de controller GUI:

- 1. Klik op Draadloos.
- 2. Klik in het menu aan de linkerkant van de draadloze pagina op Known Rogue AP's.



Het gewenste AP moet op de Known Rogue APs pagina met de status weergegeven zoals *bekend*.

Eisco - Microsoft Internet Ex	splorer provided by Cisco	Systems, Inc.					@_×
Ele Edit Yew Fgvorites	Iools Help						
Cinco Statema						ve Configuration	Ping   Logout   Refresh
A. A.	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY MAN	AGEMENT COMMA	NDS HELP	
Wireless	Known Rogue AP	s			Items 1	to 4 of 4	New
Access Points All APs	MAC Address	SSID		# Detecting Radios	Number of Clients	Status	
802.11a Radios 802.11b/g Radios	00:02:8a:0e:33:f5	Unknown		2	0	Known	Edit Remove
Third Party APs	00:07:85:92:4d:c9	Unknown		2	0	Known	Edit Remove
Bridging	00:0b:fc:fc:15:00	Unknown		1	0	Known	Edit Remove
Rogues	00:12:01:a1:f5:10	auto-2		2	0	Known	Edit Remove
Rogue Clients Adhoc Rogues Clients Global RF 802.11a Network 802.11b/g Network 802.11b/ Country Timers							
× Decussions • 🗊 🕑 🗐	9999 19 19 ØDec	ussions not available on	http://10.77.244	204/			all Internet

## De betekenis van Trusted AP-beleidsinstellingen

De WLC heeft dit vertrouwde AP beleid:

- <u>Geavanceerd encryptiebeleid</u>
- <u>Afdwingbaar beleid</u>
- Afgedwongen beleid op het gebied van radio
- <u>SSID valideren</u>
- Waarschuwing als vertrouwde AP ontbreekt
- Time-out bij overschrijding voor Trusted AP-vermeldingen (seconden)

#### Geavanceerd encryptiebeleid

Dit beleid wordt gebruikt om het coderingstype te definiëren dat de vertrouwde AP zou moeten gebruiken. U kunt een van deze coderingstypen configureren onder Afgedwongen coderingsbeleid:

- None
- Open (Openstaand)
- medegebruik
- WAP/802.11i

De WLC verifieert of het coderingstype dat op de vertrouwde AP wordt ingesteld overeenkomt met het coderingstype dat is ingesteld op "**Enforced Encryption Policy**". Indien het vertrouwde AP het aangewezen coderingstype niet gebruikt, werpt de WLC een alarm naar het beheersysteem om

passende maatregelen te nemen.

### Afdwingbaar beleid

De radio preamble (soms een header genoemd) is een gedeelte van gegevens aan het hoofd van een pakket dat informatie bevat die draadloze apparaten nodig hebben wanneer ze pakketten verzenden en ontvangen. **Korte** preambule verbeteren de doorvoerprestaties, zodat ze standaard ingeschakeld zijn. Voor sommige draadloze apparaten, zoals SpectraLink NetLink-telefoons, zijn echter **lange** preambule nodig. U kunt een van deze voorvoegselopties configureren onder Afdwingbaar voorvoegsel-beleid:

- None
- Kort
- lang

De WLC verifieert of het Preamble-type dat op de vertrouwde AP is geconfigureerd overeenkomt met het preambule-type dat is ingesteld in de instelling "Afdwingbaar beleid". Indien de vertrouwde AP het gespecificeerde preambule type niet gebruikt, roept de WLC een alarm op in het beheersysteem om passende maatregelen te nemen.

### Afgedwongen beleid op het gebied van radio

Dit beleid wordt gebruikt om het radiotype te definiëren dat de vertrouwde AP zou moeten gebruiken. U kunt een van deze radiotypen configureren onder Afgedwongen radiotypebeleid:

- None
- alleen 802.11b
- alleen 802.11a
- Alleen 802.11b/g

De WLC verifieert of het radiotype dat op de vertrouwde AP is geconfigureerd overeenkomt met het radiatype dat is ingesteld in de instelling **"Afgedwongen radiotype beleid"**. Indien de vertrouwde AP de gespecificeerde radio's niet gebruikt, werpt de WLC een alarm in het beheersysteem op om passende maatregelen te nemen.

#### **SSID** valideren

U kunt de controller configureren om een vertrouwde APs SSID te valideren tegen de SSID's die zijn ingesteld op de controller. Als de vertrouwde APs SSID's één van de controller SSID's aanpast, roept de controller een alarm op.

#### Waarschuwing als Trusted AP ontbreekt

Als dit beleid is geactiveerd, waarschuwt de WLC het beheersysteem als de vertrouwde AP van de bekende AP van de Rogue APs lijst ontbreekt.

#### Time-out bij overschrijding voor betrouwbare AP-vermeldingen (seconden)

Deze Time-outwaarde voor beëindiging van het programma specificeert het aantal seconden voordat de vertrouwde AP wordt beschouwd als verlopen en wordt gespoeld vanaf de WLC-ingang. U kunt deze waarde in seconden specificeren (120-3600 seconden).

### Hoe moet u het vertrouwde AP-beleid op de WLC configureren?

Voltooi deze stappen om een betrouwbaar AP-beleid op de WLC te configureren via de GUI:

Opmerking: al het vertrouwde AP beleid zit op dezelfde WLC pagina.

- 1. Klik in het hoofdmenu van de WLC GUI op Beveiliging.
- 2. Klik in het menu aan de linkerkant van de Security pagina op **Trusted AP-beleid** dat onder de rubriek Draadloos beschermingsbeleid



 Selecteer in de pagina Betrouwbaar AP-beleid het gewenste coderingstype (Geen, Open, EVN, WAP/802.11i) in de vervolgkeuzelijst Afdwingingsbeleid.



 Selecteer het gewenste type preambule (Geen, Kort, Lang) in de vervolgkeuzelijst Afdruktype onderdeel Afbeeldingsbeleid uitvoeren.



 Selecteer het gewenste radiatype (alleen geen, 802.11b, 802.11a alleen, 802.11b/g alleen) in de vervolgkeuzelijst Toegedwongen radiobeleid.

Cisco - Microsoft Internet E	xplorer provide	d by Cisco S	ystems, Inc.	286.0		in the		<u>013/0</u>	2
Ele Edit Yew Favorites	Ioois Help								10
Cases Systems							Save Co	nfiguration   Ping	Logout   Refresh
A. A.	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	Trusted A	P Policies						< Back	Apply
AAA General RADIUS Authentication RADIUS Accounting	Enforced	encryptic	on policy		W 5	rep .			
Local Net Users MAC Filtering Disabled Clients User Login Policies AR Policies	Enforced	radio typ	e policy		N Ni	one			
Access Control Lists	Validate	SSID			8	2.11a Only 2.11b/g Only			
1PSec Certificates CA Certificate	Alert if T	rusted AP	is missing			Enabled			
Web Auth Certificate	Expiratio	n Timeou	t for Trusted /	AP Entries (s	econds)	20			
Wireless Protection Policies Trusted AP Policies Rogue Policies Standard Signatures Custom Signatures Client Exclusion Policies AP Authentication									
× Discussions • 🎲 🕃 🕄	0111	Discuss	ions not available or	http://10.77.244	.204/				
0									Internet

- 6. Schakel het aanvinkvakje **SSID valideren** of uit om de instelling SSID valideren in of uit te schakelen.
- 7. Schakel de **waarschuwing** uit **als vertrouwde AP ontbreekt.** Schakel **het** aanvinkvakje **in** om de waarschuwing in te schakelen of uit te schakelen als vertrouwde AP ontbreekt.
- 8. Voer een waarde (in seconden) in voor de optie **Time-out bij** beëindiging **voor Trusted AP-items**.



9. Klik op Apply (Toepassen).

**Opmerking:** om deze instellingen te configureren vanuit de WLC CLI kunt u de **configuratie** van **de** WLC **vertrouwde-ap** opdracht gebruiken met de juiste beleidsoptie.

Cisco Controlle	er) > <b>config</b>	wps	trusted-ap	?
encryption	Configures	the	trusted AP	encryption policy to be enforced.
missing-ap	Configures	aler	t of missir	ng trusted AP.
preamble	Configures	the	trusted AP	preamble policy to be enforced.
radio	Configures	the	trusted AP	radio policy to be enforced.
timeout	Configures	the	expiration	time for trusted APs, in seconds.

### Trusted AP-waarschuwingsbericht

beleidsinstelling.

Hier is een voorbeeld van een betrouwbaar waarschuwingsbericht van AP-beleidsschending dat door de controller wordt getoond.

```
Thu Nov 16 12:39:12 2006 [WARNING] apf_rogue.c 1905: Possible AP
impersonation of xx:xx:xx:xx:xx, using source address of
00:16:35:9e:6f:3a, detected by 00:17:df:7d:e1:70 on slot 0
Thu Nov 16 12:39:12 2006 [SECURITY] apf_rogue.c 1490: Trusted AP Policy
failed for AP xx:xx:xx:xx:xx - invalid SSID 'SSID1'
Thu Nov 16 12:39:12 2006 [SECURITY] apf_rogue.c 1457: Trusted AP Policy
failed for AP xx:xx:xx:xx:xx - invalid encryption type
Thu Nov 16 12:39:12 2006 Previous message occurred 6 times
Let hier op de gemarkeerde foutmeldingen. Deze foutmeldingen geven aan dat SSID en het
coderingstype dat op de vertrouwde AP is ingesteld, niet overeenkomen met de Trusted AP-
```

Hetzelfde waarschuwingsbericht kan worden gezien vanaf de WLC GUI. Ga naar het hoofdmenu van de WLC GUI en klik op **Monitor** om dit bericht te bekijken. In het gedeelte Recentste trappen van de pagina Monitor klikt u op **Alles bekijken** om alle recente waarschuwingen op de WLC te bekijken.

						Same Contra	water I firm	a la constata d	
L L						Save Comig	uración Ping	Logout	
D. 20. anterestation	MONITOR WLAN	s CONTR	OLLER	WIRELE	SS SECURITY	MANAGEMENT COMMANDS H	ED		
lonitor ummary tatistics	tenterer Andrea	-	:# :*	•	🏮 :=: 🧕	Cisce 4400 Serie Cisce 4400 Serie 3 4 MODEL 440	5 2 4		
Controller Ports	Controller Summ	hary			Rogue Summary				
/ireless	Management IP Add	dress	10.77.2	44.204		Active Roque APs	25	Detail	
Kogue APs Known Rogue APs	Service Port IP Add	ress	0.0.0.0			Active Roque Clients	0	Detail	
Rogue Clients	Software Version		3.2.150	0.10		Adhoc Rogues	0	Detail	
802.11a Radios	System Name		WLC-4	400-TSW	EB	Rogues on Wired Network	0		
802.11b/g Radios	Up Time		16 day	s, 8 hour	s, 42 minutes				
RADIUS Servers	System Time		Wed D	ec 12 12:	40:03 2007	Top WLANS			
	Internal Temperatu	re	+38 C			top tieres			
	802.118 Network St	Chate	Enable	4		WLAN	# of (	lients	
	OD5-110/g Network	51808	chable	9		WCS	0	Detai	
	Loopes Dalat Cur					WCS123	0	Detai	
	Access Point au	ninary							
		Total	Up	D	own	Most Recent Traps			
	802.11a Radios	2	• 2	• 0	Datail	Dec	70 data at d		
	802.11b/g Radios	2	• 2	• 0	Detail	Rogue AP : 00:13:19:49:08:	70 detected or	Base Radio	
	All APs	2	• 2	• 0	Detail	Roque AP : 00:11:21:54:60	0 detected on	Base Radio I	
						Trusted AP 00:07:85:92:4did	9 has invalid r	adio policy. I	
	Client Summary					Trusted AP 00:07:85:92:4d:c9 has invalid encryption on			
	Current Clients	6			Detail			View Al	
	Excluded Clients	Excluded Clients 0			Detail				
						This page refreshes every 20 s	accords		
	Disabled Clients	0	)		Detail	this page retresties every ou s	PE CONTINUES :		

Op de pagina Recentste overgangen kunt u de controller identificeren die het vertrouwde waarschuwingsbericht voor AP-beleidsschending genereert zoals in deze afbeelding:

Cisco - Microsoft Internet Ex	plorer provided by Cisco Sys	tems, Inc.	<u>iiiinee</u>					_@×
Ele Edit Yew Favorites	Tools Fleib							- <b>1</b>
Cases Systems						Save Co	nfiguration Ping	Logout   Refresh
A.A.	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Monitor	Trap Logs							Clear Log
Summary	Number of Traps sinc	e last reset	12516					
Statistics Controller	Number of Traps sinc	e log last view	ed 3					
Ports	Log System Time	Trap						
Rogue APs	0 Wed Dec 12 12:40:32 2007	Rogue : 00:0 Interface no	f:f8:58:a8:5c :1(802.11b/	removed fro	om Base Radio M	IAC : 00:0b:85:	5b:fb:d0	
Known Rogue APs Rogue Clients	1 Wed Dec 12 12:40:32 2007	Rogue : 00:1 Interface no	3:19:ab:99:00 :1(802.11b/	) removed fr	rom Base Radio	MAC: 00:0b:85	:5b:fb:d0	
Adhoc Rogues 802.11a Radios	2 Wed Dec 12 Rogue : 00:13:19:ab:99:00 removed from Base Radio MAC : 00:0b:85:51:5a:e0 12:40:32 2007 Interface no:1(802.11b/g)							
802.11b/g Radios Clients	3 Wed Dec 12 12:39:31 2007	Rogue AP : 0 Interface no	0:13:19:49:0	8:70 detecte ) with RSSI:	d on Base Radio -47 and SNR: 48	MAC:00:0b:8	5:51:5a:e0	
RADIUS Servers	4 Wed Dec 12 12:39:31 2007	Rogue AP : 0 Interface no	0:13:19:49:0 :1(802.11b/	8:70 detecte ) with RSSI:	d on Base Radio -55 and SNR: 4-	MAC:00:0b:8	5:5b:fb:d0	
	5 Wed Dec 12 12:39:31 2007	Rogue AP : 0 Interface no	0:11:21:b4:ff	:00 detected	on Base Radio	MAC : 00:0b:85	:Sb:fb:d0	
	6 Wed Dec 12 12:39:29 2007	Trusted AP 0 802.11b/g	0:07:85:92:4	d:c9 has inv	alid radio policy	. It's using 802	2.11a instead of	
	7 Wed Dec 12 12:39:29 2007	Trusted AP 0	0:07:85:92:4 EP	d:c9 has inv	alid encryption	configuration.	It's using Open	
	8 Wed Dec 12 12:39:29 2007	Trusted AP 0 802.11b/g	0:02:8a:0e:3	3:f5 has inv	alid radio policy	. It's using 802	.11a instead of	
	9 Wed Dec 12 12:39:29 2007	Trusted AP 0	0:02:8a:0e:3	3:fS has inv	alid encryption (	configuration.	It's using Open	
	10 Wed Dec 12 12:39:29 2007	Trusted AP 00:12:01:a1:f5:10 is advertising an invalid SSID.						
	11 Wed Dec 12	Regue : 00:1	1-5c:93:d3:bi	removed fr	om Base Radio	HAC: 00:06:85	:51:5a:e0	
	12:30:12 2007	Rogue : 00:1	4:f1:ae:9d:70	removed fr	om Base Radio !	MAC : 00:0b:85:	51:Sa:e0	
	12:38:10 2007	Interface no	:1(802.11b/	)	en Baca Badia I	war . no.ob.er.	FI-F	
	13 Wed Dec 12 12:38:10 2007	Interface no						
	14 Wed Dec 12 12:38:10 2007	Rogue : 00:1 Interface no						
	15 Wed Dec 12 12:37:32 2007	Rogue : 00:1 Interface no	4:1b:b6:23:60 :1(802.11b/c	) removed fr	rom Base Radio	MAC : 00:0b:85	:5b:fb:d0	
	16 Wed Dec 12 12:37:18 2007	Rogue AP : 0 Interface no	0:12:d9:e2:b :0(802.11a)	9:20 detecte with RSSI: -8	d on Base Radio 3 and SNR: 8	MAC : 00:0b:8	5:51:5a:e0	
× Discussions • 🎲 🕑 🕄	0 10 10 🖭 🖉 Discussion	ns not available on h	etp://10.77.244.	204/				9
Done								Internet

## Gerelateerde informatie

- <u>Cisco-configuratiegids voor draadloze LAN-controllers, release 5.2 Routedetectie in RF-</u> groepen mogelijk
- <u>Cisco-configuratiegids voor draadloze LAN-controllers, release 4.0 Beveiligingsoplossingen</u> <u>configureren</u>
- Ruggendetectie onder Unified draadloze netwerken
- Ontwerphandleiding en implementatiehandleiding voor SpectraLink-telefoon
- <u>Configuratievoorbeeld van draadloze LAN-verbinding</u>
- <u>Connectiviteit met probleemoplossing in een draadloos LAN-netwerk</u>
- Verificatie van configuratievoorbeelden voor draadloze LAN-controllers
- <u>Technische ondersteuning en documentatie Cisco Systems</u>