Criteri access point attendibili su un controller LAN wireless

Sommario

Introduzione Prerequisiti Requisiti Convenzioni Criteri Trusted AP Che cos'è un Trusted AP? Come configurare un access point come access point attendibile dall'interfaccia utente grafica del WLC? Informazioni sulle impostazioni dei criteri Trusted AP Come configurare i criteri Trusted AP sul WLC? Messaggio di avviso di violazione dei criteri PA trusted Informazioni correlate

Introduzione

Questo documento descrive i criteri di protezione wireless *Trusted AP* su un controller WLC (Wireless LAN Controller), definisce i criteri Trusted AP e fornisce una breve descrizione di tutti i criteri Trusted AP.

Prerequisiti

Requisiti

Verificare di avere una conoscenza di base dei parametri di sicurezza della LAN wireless (ad esempio SSID, crittografia, autenticazione e così via).

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento <u>Cisco sulle convenzioni</u> <u>nei suggerimenti tecnici.</u>

Criteri Trusted AP

I criteri Trusted AP (Trusted AP Policies) sono una funzione di sicurezza del controller progettata per essere utilizzata in scenari in cui i clienti hanno una rete parallela autonoma AP insieme al controller. In questo scenario, l'access point autonomo può essere contrassegnato come l'access

point attendibile sul controller e l'utente può definire criteri per questi access point attendibili (che dovrebbero utilizzare solo WEP o WPA, il proprio SSID, un breve preambolo e così via). Se uno di questi punti di accesso non rispetta questi criteri, il controller invia un allarme al dispositivo di gestione della rete (Wireless Control System) che indica che un punto di accesso attendibile ha violato un criterio configurato.

Che cos'è un Trusted AP?

I punti di accesso attendibili sono punti di accesso che non fanno parte di un'organizzazione. Tuttavia, non rappresentano una minaccia per la sicurezza della rete. Questi punti di accesso sono anche chiamati punti di accesso amichevoli. Esistono diversi scenari in cui è possibile configurare un punto di accesso come attendibile.

Ad esempio, nella rete potrebbero essere presenti diverse categorie di access point, quali:

- Punti di accesso che non eseguono LWAPP (probabilmente eseguono IOS o VxWorks)
- Punti di accesso LWAPP introdotti dai dipendenti (con l'autorizzazione dell'amministratore)
- AP LWAPP utilizzati per verificare la rete esistente
- Access point LWAPP di proprietà dei vicini

In genere, i punti di accesso attendibili sono punti di accesso che rientrano nella **categoria 1**, ovvero punti di accesso di proprietà dell'utente che non eseguono LWAPP. Potrebbe trattarsi di vecchi access point con VxWorks o IOS. Per garantire che questi access point non danneggino la rete, è possibile applicare alcune funzionalità, ad esempio gli SSID corretti e i tipi di autenticazione. Configurare i criteri degli access point attendibili sul WLC e verificare che gli access point attendibili soddisfino tali criteri. In caso contrario, è possibile configurare il controller in modo che esegua diverse azioni, ad esempio l'invio di un avviso al dispositivo di gestione della rete (WCS).

I punti di accesso noti appartenenti ai punti di accesso adiacenti possono essere configurati come punti di accesso attendibili.

In genere, la funzionalità MFP (Management Frame Protection) deve impedire agli access point non legittimi di unirsi al WLC. Se le schede NIC supportano i dispositivi multifunzione, non è consentito accettare disautenticazioni da dispositivi diversi dai veri access point. Per ulteriori informazioni sull'opzione MFP, fare riferimento agli <u>esempi di configurazione di Infrastructure</u> <u>Management Frame Protection (MFP) con WLC e LAP</u>.

Se sono presenti access point che eseguono VxWorks o IOS (come nella categoria 1), non verranno mai aggiunti al gruppo LWAPP o eseguiranno la funzionalità MFP, ma è possibile che si desideri applicare i criteri elencati in tale pagina. In questi casi, è necessario configurare sul controller i criteri dei punti di accesso attendibili per i punti di accesso desiderati.

In generale, se si è a conoscenza di un punto di accesso non autorizzato e si è certi che non rappresenti una minaccia per la rete, è possibile identificarlo come punto di accesso attendibile.

<u>Come configurare un access point come access point attendibile dall'interfaccia</u> <u>utente grafica del WLC?</u>

Per configurare un access point come access point attendibile, completare la procedura seguente:

1. Accedere alla GUI del WLC tramite HTTP o https.

- 2. Dal menu principale del controller, fare clic su Wireless.
- 3. Nel menu sul lato sinistro della pagina Wireless, fare clic su **Rogue AP** (Punti di accesso non autorizzati)

Fie Edt Vew Favortes	plorer provided by Cisco Systems, Inc. Tools Helo		<u> 85 – 800</u>				
Cases Sveriges	MONITOR WLANS CONTROL		S SECURITY M	NAGEMENT CON	Sava Configurati IMANDS HELP	on Ping	Logout Refres
Wireless Access Points All APs 802.11a Radios	All APs Search by Ethernet MAC		Search				
802.11b/g Radios Third Party APs	AP Name	AP ID	Ethernet MAC	Admin Status	Operational Status	Port	
Bridging	ap:5b:fb:d0	34	00:0b:85:5b:fb:d0	Enable	REG	2	Detail
Rogue APs Rogue APs Roswa Rogue APs	ap:51:5a:e0	35	00:0b:85:51:5a:e0	Enable	REG	2	Detail
Adhoc Rogues							
Global RF 802.11a Network 802.11b/g Network 802.11b/g Network							
ountry							
limers							
Discussions • 🎲 🕃 🗒	🗿 🗊 🐮 🔛 🧭 Discussions not availa	ble on http://10.77.	244.204/				
						inter	net

Nella pagina Access point non autorizzati vengono elencati tutti gli access point rilevati come access point non autorizzati nella rete.

- 4. Da questo elenco di access point anomali, individuare l'access point che si desidera configurare come trusted che rientra nella categoria 1 (come spiegato nella sezione precedente).Èpossibile individuare gli access point con gli indirizzi MAC elencati nella pagina degli access point non autorizzati. Se l'access point desiderato non si trova in questa pagina, fare clic su **Avanti** per identificarlo nella pagina successiva.
- 5. Una volta individuato l'access point desiderato dall'elenco degli access point non autorizzati, fare clic sul pulsante **Modifica** corrispondente all'access point per visualizzare la pagina dei dettagli dell'access point.

Rogue APs			Iten	ns 1 to 20 of 26	Nex
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:beif6:70	Unknown	2	0	Alert	Edit
00:12:01:a1:f5:10	auto-2	1	0	Pending	Edit

Nella pagina dei dettagli dell'access point non autorizzato sono disponibili informazioni

dettagliate sull'access point, ad esempio se è connesso alla rete cablata, lo stato corrente dell'access point e così via.

6. Per configurare questo access point come attendibile, selezionare **Interno noto** dall'elenco a discesa Aggiorna stato e fare clic su **Applica**.Quando lo stato dell'access point viene aggiornato su *Interno noto*, l'access point viene configurato come attendibile nella rete.

Ele Edit Yew Favorites	Iools Help								Ju	inks »	R.
Cases Stateme							Save Config	uration P	ing Logou	rt Refre	sh
A. A.	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMEN	л сом	MANDS H	ELP			
Wireless	Rogue AP Detail							< Back		pply	
Access Points All APs 802-11a Padios	MAC Address			00:12:01:81:	5:10						
002.11b/g Radios Third Party APs	Туре			AP							
Bridging	Is Rogue On Wired N	ietwork?		No							
Rogues Rogue APs Known Rogue APs	Rogue APs On On				2:27:28 2007						
Rogue Clients Adhoc Rogues	Last Time Reported On			Wed Dec 12 1	3:13:09 2007						
Clients	Current Status			Known							
802.11a Network											
802.11b/g Network 802.11h	Update Status			Choose	New Status	-					
Country				Contain Rogu Alert Unknow	¢						
Timers				Known Intern Acknowledge	el External						
	APs that detected t	nis Rogue									
	Base Radio MAC	AP Name	\$\$1	D	Channel	Radio Type	WEP	WPA	Pre- Amble	RSSI	1
	00:0b:85:51:5a:e0	ap:51:5a:e0	auto	i=2	1	802.119	Enabled	Enabled	Short	-71	1
	Clients associated t	o this Roque	AD								
	MAC Address	Last	Time Heard								
	THE HOULESS		Thire free o								
	٠.										2
Discussions • 192 🖓 🕅	🗊 🗊 🗊 🔠 🧭 Discussio	ns not available on i	http://10.77.24	.204/							-

7. Ripetere questa procedura per tutti gli access point che si desidera configurare come trusted.

Verifica la configurazione Trusted AP

Completare questa procedura per verificare che l'access point sia configurato correttamente come attendibile dall'interfaccia utente del controller:

- 1. Fare clic su Wireless.
- 2. Nel menu sul lato sinistro della pagina Wireless, fare clic su **Punti di accesso non autorizzati noti**.



L'access point desiderato dovrebbe essere visualizzato nella pagina Access point non autorizzati con lo stato

Known.

Eisco - Microsoft Internet E	xplorer provided by Cisc	o Systems, Inc.			8000		
Ele Edit Yew Favorites	Iools Help						
Cases Systems					S-1	we Configuration	Ping Logout Refresh
A. A.	MONITOR WLAN	CONTROLLER	WIRELESS	SECURITY MAN	AGEMENT COMMA	NDS HELP	
Wireless	Known Rogue AF	5			Items 1	to 4 of 4	New
Access Points All APs	MAC Address	SSID		# Detecting Radios	Number of Clients	Status	
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 Bemove
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 Country Timers							
X Discussions * 1 🞲 🕞 😳	9998 × Ø®	ussions not available on	http://10.77.244	.204/			(a)
el nove							arcemet

Informazioni sulle impostazioni dei criteri Trusted AP

II WLC ha questi criteri dell'access point attendibile:

- <u>Criterio di crittografia imposto</u>
- <u>Criterio preambolo imposto</u>
- <u>Criterio tipo di radio imposto</u>
- <u>Convalida SSID</u>
- Avvisa se il punto di accesso attendibile è mancante
- Timeout scadenza per voci di access point attendibili (secondi)

Criterio di crittografia imposto

Questo criterio viene utilizzato per definire il tipo di crittografia che l'access point attendibile deve utilizzare. In Criterio di crittografia imposto è possibile configurare uno qualsiasi di questi tipi di crittografia:

- Nessuna
- Open (Aperto)
- WEP
- WPA/802.11i

Il WLC verifica se il tipo di crittografia configurato nell'access point attendibile corrisponde al tipo di crittografia configurato nell'impostazione "**Criteri di crittografia imposti**". Se l'access point attendibile non usa il tipo di crittografia designato, il WLC invia un allarme al sistema di gestione

Criterio preambolo imposto

Il preambolo radio (talvolta chiamato intestazione) è una sezione di dati alla base di un pacchetto che contiene le informazioni di cui i dispositivi wireless hanno bisogno quando inviano e ricevono i pacchetti. I preamboli **brevi** migliorano le prestazioni di throughput, pertanto sono abilitati per impostazione predefinita. Tuttavia, alcuni dispositivi wireless, ad esempio i telefoni SpectraLink NetLink, richiedono preamboli **lunghi**. In Criterio di preambolo imposto è possibile configurare una delle opzioni seguenti:

- Nessuna
- Breve
- Lunga

Il WLC verifica se il tipo di preambolo configurato nell'access point attendibile corrisponde al tipo di preambolo configurato nell'impostazione "**Criterio di preambolo imposto**". Se l'access point attendibile non utilizza il tipo di preambolo specificato, il WLC invia un allarme al sistema di gestione per prendere le misure appropriate.

Criterio tipo di radio imposto

Questo criterio viene utilizzato per definire il tipo di radio che l'access point attendibile deve utilizzare. In Criterio tipo radio imposto è possibile configurare uno qualsiasi di questi tipi di radio:

- Nessuna
- Solo 802.11b
- Solo 802.11a
- Solo 802.11b/g

Il WLC verifica se il tipo di radio configurato nell'access point attendibile corrisponde al tipo di radio configurato nell'impostazione "**Criterio del tipo di radio imposto**". Se l'access point attendibile non utilizza le radio specificate, il WLC invia un allarme al sistema di gestione per prendere le misure appropriate.

Convalida SSID

Èpossibile configurare il controller per convalidare un SSID di punti di accesso trusted rispetto agli SSID configurati nel controller. Se l'SSID degli access point attendibili corrisponde a uno degli SSID dei controller, il controller genera un allarme.

Avvisa se l'access point attendibile è mancante

Se questo criterio è abilitato, il WLC avvisa il sistema di gestione se l'access point attendibile non è presente nell'elenco degli access point non autorizzati noti.

Timeout scadenza voci di access point attendibili (secondi)

Questo valore di timeout di scadenza specifica il numero di secondi prima che l'access point attendibile venga considerato scaduto e scaricato dalla voce WLC. È possibile specificare questo valore di timeout in secondi (120 - 3600 secondi).

Come configurare i criteri Trusted AP sul WLC?

Completare questi passaggi per configurare i criteri Trusted AP sul WLC tramite la GUI:

Nota: tutti i criteri PA trusted si trovano sulla stessa pagina WLC.

- 1. Dal menu principale della GUI del WLC, fare clic su Security (Sicurezza).
- 2. Dal menu visualizzato sul lato sinistro della pagina Sicurezza, fare clic su **Trusted AP policies** (Criteri access point attendibili) elencato sotto l'intestazione Criteri di protezione

wireless.



 Nella pagina Criteri Trusted AP, selezionare il tipo di crittografia desiderato (Nessuno, Aperto, WEP, WPA/802.11i) dall'elenco a discesa Criterio di crittografia applicato.



 Selezionare il tipo di preambolo desiderato (None, Short, Long) dall'elenco a discesa Criterio tipo di preambolo imposto.



 Selezionare il tipo di radio desiderato (Nessuno, solo 802.11b, solo 802.11a, solo 802.11b/g) dall'elenco a discesa Criterio tipo radio imposto.

🗿 Cisco - Microsoft Internet D	oplorer provided	by Cisco Syste	ms, Inc.			de la companya de la			_ @ ×
Ele Edit Yew Favorites	<u>I</u> ools <u>H</u> elp								- 19 19
Cases Sections							Save Co	nfiguration 🗌 Ping	Logout Refresh
A.A.	MONITOR	WLANS CO	NTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	Trusted AP	Policies						< Back	Apply
AAA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Access Control Lists IPSec Certificates CA Certificate ID Certificate Web Auth Certificate Wieless Protection Policies Trusted AP Policies Regue Policies Standard Signatures Client Exclusion Policies AP Authentication	Enforced o Enforced p Validate S Alert if Tru Expiration	encryption p preamble po radio type po SID isted AP is n Timeout for	olicy licy olicy nissing r Trusted A	P Entries (s	econds)	VEP hort hort h			
× Discussions • 🗊 🕃 🕄	9991E	Ø Discussions	not available on	http://10.77.244	.204/				Ø
2									nternet

- 6. Per abilitare o disabilitare l'impostazione Convalida SSID, selezionare o deselezionare la casella di controllo **Convalida SSID abilitato**.
- 7. Per abilitare o disabilitare l'impostazione **Avvisa se** il punto di accesso attendibile è mancante, selezionare o deselezionare la casella di controllo Avvisa se il punto di accesso attendibile è mancante.
- 8. Immettere un valore (in secondi) per l'opzione **Timeout scadenza per voci PA attendibili**.



9. Fare clic su Apply (Applica).

Nota: per configurare queste impostazioni dalla CLI del WLC, è possibile usare il comando config wps trusted-ap con l'opzione di criterio appropriata.

Cisco Controlle	er) >config	wps trusted-ap ?
encryption	Configures	the trusted AP encryption policy to be enforced.
missing-ap	Configures	alert of missing 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.

Messaggio di avviso di violazione dei criteri PA trusted

Di seguito è riportato un esempio di messaggio di avviso di violazione dei criteri del punto di accesso attendibile visualizzato dal controller.

Thu Nov 16 12:39:12 2006 [WARNING] apf_rogue.c 1905: Possible AP impersonation of xx: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: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:xx - invalid encryption type Thu Nov 16 12:39:12 2006 Previous message occurred 6 times Si notino qui i messaggi di errore evidenziati Questi messaggi di errore indication

Si notino qui i messaggi di errore evidenziati. Questi messaggi di errore indicano che il SSID e il tipo di crittografia configurato nell'access point attendibile non corrispondono all'impostazione dei criteri dell'access point attendibile.

Lo stesso messaggio di avviso può essere visualizzato dalla GUI del WLC. Per visualizzare questo messaggio, andare al menu principale dell'interfaccia utente del WLC e fare clic su **Monitor**. Nella sezione Trap più recenti della pagina Monitor, fare clic su **View All** per visualizzare tutti gli alert recenti sul WLC.

an Bernen							Save Confin	ration Disa	L Losout L B		
h. h.									- Logoon - n		
In the second second	MONITOR WDAN	SOUCHIN	OLLER	WIRE	1599	SECORIT	MANAGEMENT COMMANDS H	E D			
lonitor ummary tatistics	ten inner 	-	:=:=	•	-	:=: 0	Cisco 4400 Series Winkes LAN Costrolle 3 4 MODEL 4404				
Controller Ports	Controller Summ	ary			Rogue Summary						
Vireless	Management IP Add	fress	10.77.2	244.20	4		Active Rogue APs	25	Detail		
Known Rogue APs	Service Port IP Add	ress	0.0.0.0				Active Rogue Clients	0	Detail		
Rogue Clients Adhoc Rogues	Software Version	Software Version					Adhoc Rogues	0	Detail		
802.11a Radios	System Name	n Name WLC-44					Rogues on Wired Network	0			
802.11b/g Radios	Up Time		16 day	s, 8 ho	urs, 42	minutes					
RADIUS Servers	System Time	System Time Wed Dec 12 12					10:03 2007 Top WLANS				
	Internal Temperatu	Internal Temperature +38 C									
	802.11a Network St	802.11a Network State Enabled					WLAN	# of (lients		
	opsitteld Hermork	OU2.11D/g Network State Er					WCS	0	Detail		
	Longer Delet Cur						WCS123	0	Detail		
	Access Point Sul	nmary									
		Total	Up		Down		Most Recent Traps				
	802.11a Radios	2	• 2	٠	0	Detail					
	802.11b/g Radios	2	• 2	٠	0	Detail	Rogue AP : 00:13:19:49:08:	70 detected or	Base Radio		
	All APs	2	• 2	٠	0	Detail	Rogue AP : 00:13:19:49:08:	70 detected or	Base Radio		
							Touted AD 00-07-05-02-44-c	0 becected on	base kadio i udio policy 1		
	Client Summary						Trusted AP 00:07:85:92:4d:c9 has invalid radio policy				
	Current Clearty					Dated	114144 11 00.01.02.92.10.0	, 110, 111, 010, 0	View All		
	Evoluded Clients	Evaluated Cleants 0				Detail					
	Disabled Clients	Excluded clients 0				Detail	This page refreshes every 30 s	conds.			
	Distance Cherry		<i>.</i>			PCP/1962					

Nella pagina Trap più recenti è possibile identificare il controller che ha generato il messaggio di avviso di violazione dei criteri del punto di accesso attendibile, come mostrato nell'immagine seguente:

Cisco - Microsoft Internet Ex	plorer provided by Cisco Sy	rstems, Inc. 🤉	<u>Tääree</u>		741			_@×		
Ele Edit View Favorites	Tools Fielb									
Cinco Station						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 sin	ce last reset	12516							
Statistics	Number of Traps sin	ce log last view	ed 3					_		
Controller										
Wireless	Log System Time	Trap								
Rogue APs	0 Wed Dec 12 12:40:32 2007	Rogue : 00:01 Interface no:	:f8:58:a8:5c 1(802.11b/	removed fro	om Base Radio M	IAC : 00:0b:85:	b:fb:d0			
Known Rogue APs Rogue Clients	1 Wed Dec 12 12:40:32 2007	Rogue : 00:12	3:19:ab:99:0	0 removed f	rom Base Radio	MAC: 00:0b:85	:5b:fb:d0			
Adhoc Rogues	2 Wed Dec 12	Rogue : 00:13	3:19:ab:99:0	0 removed f	rom Base Radio	MAC : 00:0b:85	51:5a:e0			
802.118 Kadios 802.11b/g Radios	Wed Dec 12	Rogue AP : 0	0:13:19:49:0	9) 8:70 detecte	d on Base Radio	MAC : 00:0b:8	5:51:5a:e0			
Clients RADIUS Servers	Wed Dec 12	Reque AP : 0	1(802.11b/ 0:13:19:49:0	g) with RSSI: 8:70 detecte	-47 and SNR: 40 d on Base Radio	B MAC : 00:0b:8	s:sb:fb:d0			
NAUSUS SEITEIS	4 12:39:31 2007	Interface no	1(802.11b/	g) with RSSI:	-55 and SNR: 4	1	11.01.10			
	5 Wed Dec 12 12:39:31 2007	Interface no:	1(802.11b/	g) with RSSI:	-95 and SNR: 4	MAC : 00:06:85	Sbirbidu			
	6 Wed Dec 12 12:39:29 2007	Trusted AP 0 802.11b/a	0:07:85:92:4	d:c9 has inv	alid radio policy	. It's using 802	11a instead of			
	7 Wed Dec 12	Trusted AP 0	0:07:85:92:4	d:c9 has inv	alid encryption	configuration.	It's using Open			
	8 Wed Dec 12	Trusted AP 0	0:02:8a:0e:3	3:f5 has inv	alid radio policy	. It's using 802	.11a instead of			
	Wed Dec 12	802.11b/g Trusted AP 0	0:02:8a:0e:3	3:f5 has inv	alid encryption	onfiguration.	it's using Open			
	12:39:29 2007	instead of W	ER							
	10 wed bec 12 12:39:29 2007	Trusted AP 0	>							
	11 Wed Dec 12 12:38:12 2007	Reque : 00-1 Interface no:	Reque : 00:11:5c:93:d3:h0 removed from Base Radio MAC : 00:0b:85:51:5a:e0 Interface po:1(802.11b/o)							
	12 Wed Dec 12	Rogue : 00:1-	4:f1:ae:9d:70	removed fr	om Base Radio !	MAC:00:0b:85	51:5a:e0			
	Wed Dec 12	Roque : 00:02	Interface no:1(802.11b/g) Roque : 00:07:50:d5:cf:b9 removed from Base Radio MAC : 00:0b:85:51:5a:e0							
	13 12:38:10 2007	Interface no								
	14 Wed Dec 12 12:38:10 2007	Interface no								
	15 Wed Dec 12 12:37:32 2007	Rogue : 00:1- Interface no:	4:1b:b6:23:6 :1(802.11b/	0 removed f	rom Base Radio	MAC : 00:0b:85	:5b:fb:d0			
	16 Wed Dec 12	Rogue AP : 0	0:12:d9:e2:b	9:20 detecte	d on Base Radio	MAC: 00:0b:8	5:51:5a:e0			
	12:37:16 2007	interrace no	0(302.113)	with R551: -8	5 and SNR: 8		1 11 1A	-		
× Discussions • 🖏 🕲 🕄	🕽 🗊 🐩 🔛 💋 Discussi	ions not available on h	ttp://10.77.244	204/				9		
Done								Internet		

Informazioni correlate

- Guida alla configurazione di Cisco Wireless LAN Controller, versione 5.2 Abilitazione del rilevamento dei punti di accesso di routing nei gruppi RF
- <u>Guida alla configurazione di Cisco Wireless LAN Controller, versione 4.0 Configurazione</u> delle soluzioni di sicurezza
- <u>Rilevamento di anomalie nelle reti wireless unificate</u>
- Guida alla progettazione e all'installazione dei telefoni SpectraLink
- Esempio di configurazione della connessione base della LAN wireless
- <u>Risoluzione dei problemi di connettività in una rete LAN wireless</u>
- Esempi di configurazione dell'autenticazione sui controller LAN wireless
- Documentazione e supporto tecnico Cisco Systems