Políticas AP de confianza en un controlador LAN inalámbrico

Contenido

Introducción Prerequisites Requirements Convenciones Políticas de AP de confianza ¿Qué es un AP de confianza? ¿Cómo Configurar un AP como AP de Confianza desde la GUI del WLC? Introducción a la configuración de la política AP de confianza ¿Cómo Configurar las Políticas AP de Confianza en el WLC? Mensaje de alerta de violación de política AP de confianza Información Relacionada

Introducción

Este documento describe las políticas de protección inalámbrica *AP* de confianza en un controlador de LAN inalámbrica (WLC), define las políticas AP de confianza y proporciona una breve descripción de todas las políticas AP de confianza.

Prerequisites

Requirements

Asegúrese de tener una comprensión básica de los parámetros de seguridad de LAN inalámbrica (como SSID, cifrado, autenticación, etc.).

Convenciones

Consulte <u>Convenciones de Consejos TécnicosCisco para obtener más información sobre las</u> <u>convenciones del documento.</u>

Políticas de AP de confianza

Las políticas AP de confianza es una función de seguridad en el controlador que está diseñada para ser utilizada en escenarios donde los clientes tienen una red AP autónoma paralela junto con el controlador. En ese escenario, el AP autónomo se puede marcar como el AP confiable en el controlador, y el usuario puede definir políticas para estos AP de confianza (que deberían utilizar

solamente WEP o WPA, nuestro propio SSID, breve preámbulo, etc.). Si alguno de estos AP no cumple con estas políticas, el controlador emite una alarma al dispositivo de administración de red (Wireless Control System) que indica que un AP de confianza violó una política configurada.

¿Qué es un AP de confianza?

Los AP de confianza son AP que no forman parte de una organización. Sin embargo, no suponen una amenaza para la seguridad de la red. Estos AP también se llaman AP amistosos. Existen varios escenarios donde puede que desee configurar un AP como un AP de confianza.

Por ejemplo, puede tener diferentes categorías de AP en su red como:

- AP que posee que no ejecutan LWAPP (tal vez ejecuten IOS o VxWorks)
- AP LWAPP que los empleados aportan (con el conocimiento del administrador)
- AP LWAPP utilizados para probar la red existente
- AP LWAPP que poseen los vecinos

Normalmente, los APs confiables son APs que caen en la **categoría 1**, que son APs que posee que no ejecutan LWAPP. Pueden ser AP antiguos que ejecutan VxWorks o IOS. Para asegurarse de que estos AP no dañen la red, se pueden aplicar ciertas características, como SSID correctos y tipos de autenticación. Configure las políticas AP confiables en el WLC, y asegúrese de que los AP confiables cumplan estas políticas. Si no es así, puede configurar el controlador para realizar varias acciones, como alarmar al dispositivo de administración de red (WCS).

Los AP conocidos que pertenecen a los vecinos se pueden configurar como AP de confianza.

Normalmente, la MFP (protección de tramas de administración) debería evitar que los AP que no son AP LWAPP legítimos se unan al WLC. Si las tarjetas NIC soportan MFP, no se les permite aceptar desautenticaciones de dispositivos que no sean los AP reales. Consulte <u>Ejemplo de</u> <u>Configuración de Protección de Tramas de Administración de Infraestructura (MFP) con WLC y</u> <u>LAP</u> para obtener más información sobre MFP.

Si tiene AP que ejecutan VxWorks o IOS (como en la categoría 1), nunca se unirán al grupo LWAPP ni realizarán MFP, pero es posible que desee aplicar las políticas enumeradas en esa página. En tales casos, las políticas AP confiables deben configurarse en el controlador para los AP de interés.

En general, si conoce un AP no autorizado e identifica que no es una amenaza para su red, puede identificar ese AP como un AP confiable conocido.

¿Cómo Configurar un AP como AP de Confianza desde la GUI del WLC?

Complete estos pasos para configurar un AP como AP confiable:

- 1. Inicie sesión en la GUI del WLC a través del login HTTP o https.
- 2. En el menú principal del controlador, haga clic en Wireless.
- 3. En el menú ubicado en el lado izquierdo de la página Inalámbrica, haga clic en AP rogue.

Cisco - Microsoft Internet Ex	oplorer provided by Cisco Systems, Inc.					- 0
jie Edit Yew Favorites	Tools Refs					
A. A.	MONITOR WLANS CONTROLLER	WIRELESS SECURITY M	NAGEMENT COM	Save Configurati MANDS HELP	on Ping L	ogout Refre
Wireless Access Points All APs 802.11a Radios	All APs Search by Ethernet MAC	Search				
Third Party APs	AP Name	AP ID Ethernet MAC	Admin Status	Operational Status	Port	
ridging	ap:5b:fb:d0	34 00:0b:85:5b:fb:d0	Enable	REG	2	Detail
Rogue APs Known Rogue APs Rogue Clients	ap:51:5a:e0	35 00:0b:85:51:5a:e0	Enable	REG	2	Detail
Adhoc Rogues ients						
obal RF 102.11a Network 102.11b/g Network 102.11b						
untry						
ners						
Discussions • 👘 🕅 🕅	🕘 🐩 🐩 📧 💋 Discussions not available on h	etp://10.77.244.204/				
					intern	et

La página de AP rogue enumera todos los AP que se detectan como AP rogue en la red.

- 4. De esta lista de AP rogue, localice el AP que desea configurar como AP confiable que cae en la categoría 1 (como se explicó en la sección anterior).Puede localizar los AP con las direcciones MAC enumeradas en la página de AP rogue. Si el AP deseado no está en esta página, haga clic en Next para identificar el AP de la siguiente página.
- 5. Una vez que el AP deseado se encuentra desde la lista de AP rogue, haga clic en el botón **Edit** que corresponde al AP, que lo lleva a la página de detalles del AP.

Rogue APs			Iten	ns 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

En la página de detalles de AP rogue, puede encontrar información detallada acerca de este AP (como si ese AP se conectó a la red por cable, así como el estado actual del AP y así sucesivamente).

6. Para configurar este AP como un AP confiable, seleccione Interno Conocido en la lista desplegable Update Status y haga clic en Apply.Cuando usted actualiza el estado de AP a *Interno Conocido*, este AP se configura como el AP confiable de esta red.

Ele Edit Yew Favorit	es Iools Help								Ju	inks 🏁 🧃
Cinco Svoteme							Save Confi	puration P	ing Logo	rt Refrest
A. A.	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEME	ит сом	MANDS H	HELP		
Wireless	Rogue AP Detail							< Back		pply
Access Points All APs 802.11a Radios 802.11b/g Radios	MAC Address			00:12:01:01:	5:10					
Bridging	Is Rogue On Wired	Network?		No						
Rogues Rogue APs Known Rogue APs	First Time Reported On	I		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						
802.11a Network 802.11b/g Network 802.11h	Update Status			Choose	New Status] New Status	3				
Country Timers				Contain Rogu Alert Unknow Known Intern	e n el					
	APs that detected t	his Rogue		Acknowledge	C.Merride					
	Base Radio MAC	AP Name	\$51	D	Channel	Radio Type	WEP	WPA	Pre- Amble	RSSI
	00:0b:85:51:5a:e0	ap:51:5a:e0	auto	i=2	1	802.119	Enabled	Enabled	Short	-71
	Clients associated t MAC Address	o this Rogue Last	AP Time Heard							
	al.						-			
K Discussions * 1871 EA B	n en en en (el) Ørmune	ing and available on	http://iiii.77.24	2047						

7. Repita estos pasos para todos los AP que desee configurar como AP de confianza.

Verificar la configuración de AP de confianza

Complete estos pasos para verificar que el AP esté configurado correctamente como AP confiable desde la GUI del controlador:

- 1. Haga clic en Wireless.
- 2. En el menú ubicado en el lado izquierdo de la página Inalámbrico, haga clic en **AP rogue conocidos**.



El AP deseado debe aparecer en la página AP rogue conocidos con el estado enumerado como

Conocido.

Cisco - Microsoft Internet E	oplorer provided by Cisco Tools Help	o Systems, Inc.	58		1999			- 02
Tore former	1000 (B4)				54	ve CooFourat	on Pina	Logout Refresh
A. A.	MONITOR WLAN	CONTROLLER	WIRELESS	SECURITY MAN	AGEMENT COMMA	NDS HELP		
Wireless	Known Rogue AP	5			Items 1	to 4	d 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	\geq	Edit Remove
Roque Clients Adhoc Roques Clients Global RF 802.11a Network 802.11b/g Network 802.11h Country Timers								
X Discussions * 1 🞲 🕞 🗐	9998000	ussions not evailable on	.http://10.77.244	204/				ternet (

Introducción a la configuración de la política AP de confianza

El WLC tiene estas políticas AP confiables:

- Política de cifrado aplicada
- Política de Preámbulo aplicada
- Política de tipos de radio aplicada
- Validar SSID
- Alerta si falta el AP confiable
- Tiempo de espera de vencimiento para las entradas AP de confianza (segundos)

Política de cifrado aplicada

Esta política se utiliza para definir el tipo de encriptación que el AP confiable debe utilizar. Puede configurar cualquiera de estos tipos de cifrado en Política de cifrado aplicada:

- Ninguno
- Abierto
- WEP
- WPA/802.11i

El WLC verifica si el tipo de encripción configurado en el AP confiable coincide con el tipo de encripción configurado en la configuración de **"Política de encripción forzada"**. Si el AP confiable no utiliza el tipo de encripción designado, el WLC genera una alarma al sistema de administración para tomar las acciones apropiadas.

Política de Preámbulo aplicada

El preámbulo de radio (a veces llamado encabezado) es una sección de datos en la cabeza de un paquete que contiene información que los dispositivos inalámbricos necesitan cuando envían y reciben paquetes. **Los** preámbulos **cortos** mejoran el rendimiento, por lo que están habilitados de forma predeterminada. Sin embargo, algunos dispositivos inalámbricos, como los teléfonos SpectraLink NetLink, requieren preámbulos **largos**. Puede configurar cualquiera de estas opciones de preámbulo en la política de preámbulo implementada:

- Ninguno
- Breve
- Largo

El WLC verifica si el tipo Preamble configurado en el AP confiable coincide con el tipo de preámbulo configurado en la configuración de "**Política de preámbulo forzada**". Si el AP confiable no utiliza el tipo de preámbulo especificado, el WLC genera una alarma al sistema de administración para tomar las acciones apropiadas.

Política de tipos de radio aplicada

Esta política se utiliza para definir el tipo de radio que debe utilizar el AP de confianza. Puede configurar cualquiera de estos tipos de radio en Política de tipo de radio aplicada:

- Ninguno
- Solo 802.11b
- Solo 802.11a
- Solo 802.11b/g

El WLC verifica si el tipo de radio configurado en el AP confiable coincide con el tipo de radio configurado en la configuración "**Política de tipo de radio aplicada**". Si el AP de confianza no utiliza las radios especificadas, el WLC emite una alarma al sistema de administración para tomar las acciones apropiadas.

Validar SSID

Puede configurar el controlador para validar un SSID de APs de confianza contra los SSID configurados en el controlador. Si el SSID de APs confiable coincide con uno de los SSID del controlador, el controlador genera una alarma.

Alerta si falta el AP de confianza

Si se habilita esta política, el WLC alerta al sistema de administración si el AP confiable falta de la lista de AP rogue conocidos.

Tiempo de espera de vencimiento para las entradas AP de confianza (segundos)

Este valor de tiempo de espera de vencimiento especifica el número de segundos antes de que el AP confiable se considere expirado y vaciado de la entrada del WLC. Puede especificar este valor de tiempo de espera en segundos (120 - 3600 segundos).

¿Cómo Configurar las Políticas AP de Confianza en el WLC?

Complete estos pasos para configurar las políticas AP confiables en el WLC a través de la GUI:

Nota: Todas las políticas AP confiables residen en la misma página WLC.

- 1. Desde el menú principal de la GUI del WLC, haga clic en Seguridad.
- 2. En el menú ubicado en el lado izquierdo de la página Seguridad, haga clic en **Trusted AP policies** enumeradas en el encabezado Wireless Protection Policies

Cisco - Microsoft Internet Exp Ele Edit Yew Fgyorites	Norer provided by Cisco Systems, Inc.	x (8) x
Conce Secret	Save Conf MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS	iguration Ping Logout Refresh HELP
Security AAA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Access Control Lists IPSec Certificate UD Certificate Web Auth Certificate Wreless Protection Policies Trusted AP Policies Region Policies Region Policies Standard Signatures Client Exclusion Policies AP Authentication	RADIUS Authentication Servers Call Station ID Type IP Address Credentials Caching Use AES Key Wrap Network User Management Server Index Server Address Port IPSec Admin Status User	Apply New
× Discussions • 🎲 🕑 🕘	Image: Second	🥑 Internet

 En la página Trusted AP policies (Políticas de punto de acceso de confianza), seleccione el tipo de encriptación deseado (Ninguno, Abrir, WEP, WPA/802.11i) en la lista desplegable Enforce Encryption Policy (Política de cifrado aplicada).



 Seleccione el tipo de preámbulo deseado (Ninguno, Corto, Largo) en la lista desplegable Política de tipos de preámbulo aplicada.



 Seleccione el tipo de radio deseado (Ninguno, sólo 802.11b, sólo 802.11a, sólo 802.11b/g) en la lista desplegable Política de tipo de radio aplicada.

Cisco - Microsoft Internet Ex	xplorer provided b	y Cisco Systems, Inc.			in the second		013/4	_ @ ×
Ele Edit View Favorites	Tools Rep							- 10
Cases Statum						Save Co	nfiguration Ping	Logout Refresh
A. A.	MONITOR V	VLANS CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	Trusted AP I	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 D Certificate UC Certificate Web Auth Certificate Wireless Protection Policies Trusted AP Policies Rague Policies Standard Signatures Client Exclusion Policies AP Authentication	Enforced en Enforced pr Enforced ra Validate SS Alert if Trus Expiration T	ecryption policy eamble policy dio type policy ID ted AP is missing fimeout for Trusted /	AP Entries (s	econds)	rEP hort none ne 22.11b Only 22.11b/g Only Enabled 20			
× Discussions • 🎲 🕃 🕄	999121	Ø Discussions not available or	http://10.77.244	.204/				9
 Image: A second s							i in	ternet

- 6. Marque o desmarque la casilla de verificación **Validar SSID habilitado** para habilitar o inhabilitar la configuración Validar SSID.
- 7. Marque o desmarque la casilla de verificación **Alerta si falta el AP confiable habilitado** para habilitar o inhabilitar la Alerta si falta el AP confiable.
- 8. Introduzca un valor (en segundos) para la opción **Expiration Timeout for Trusted AP entries**.



9. Haga clic en Apply (Aplicar).

Nota: Para configurar estos parámetros desde la CLI del WLC, puede utilizar el comando config wps trust-ap con la opción de política apropiada.

Cisco Controlle	r) >config	wps	trusted-ap	?
encryption	Configures	the	trusted AP	encryption policy to be enforced
missing-ap	Configures	aler	rt of missin	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

Mensaje de alerta de violación de política AP de confianza

Este es un ejemplo del mensaje de alerta de violación de política AP confiable que muestra el controlador.

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

Observe los mensajes de error resaltados aquí. Estos mensajes de error indican que el SSID y el tipo de encripción configurados en el AP de confianza no coinciden con la configuración de la política AP de confianza.

Se puede ver el mismo mensaje de alerta desde la GUI del WLC. Para ver este mensaje, vaya al menú principal de la GUI del WLC y haga clic en **Monitor**. En la sección Trampas más recientes de la página Monitor, haga clic en **Ver todo** para ver todas las alertas recientes en el WLC.

co Sratana							Save Config	uration Ping	Logout F			
harananana harananana haranana harana har	MONITOR WLAN	sCONI	ROLLER	WIRE	LESS	SECURITY	MANAGEMENT COMMANDS H	EГЪ				
onitor Immary atistics		· 🔶	:=:=	-	- ,) (#) Q	100 Access Points Supporte Cisco 4400 Serie Wireless LAN Controls 3 4 MODEL 440	6 *				
Controller Forts	Controller Summ	агу					Rogue Summary					
ireless	Management IP Add	óress	10.77.	244.20	Active Roque APs	25	Detail					
Rogue APs Known Rogue APs	Service Port IP Add	ress	0.0.0.0	0			Active Roque Clients	0	Detail			
opue Clients	Software Version		3.2.15	0.10			Adhoc Roques	0	Detail			
dhoc Rogues 02.11a Radios	System Name		WLC-4	400-TS	WEB		Roques on Wired Network	0	NCA1002			
/02.11b/g Radios	Up Time		16 day	rs, 8 ho	ours, 42	minutes						
Clients RADIUS Servers	System Time		Wed D	ec 12 3	12:40:0	3 2007						
	Internal Temperatu	re	+38 C				Top WLANS					
	802.11a Network St	tate	Enabled				WLAN	# of Clients				
	802.11b/g Network	State	Enable	:d				by ss	10			
							WCS	0	Detai			
	Access Point Sur	mmary					WC5123	0 0				
		Total	Up		Down		Most Recent Traps					
	802.11a Radios	2	• 2	٠	0	Dateil						
	802.11b/g Radios	2	• 2	٠	0	Detail	Rogue AP : 00:13:19:49:08:	70 detected on	Base Radio			
	All APs	2	• 2	٠	0	Detail	Rogue AP : 00:13:19:49:08:	70 detected on	Base Radio			
							Rogue AP : 00:11:21:b4:ff:0	0 detected on	Base Radio I			
	Client Summary						Trusted AP 00:07:85:92:4d:0	9 has invalid r	adio policy. I			
							Trusted AP 00:07:85:92:4d:c9 has invalid encryption co					
	Current Clients		6			Detail			View.Al			
	Excluded Clients	Excluded Clients 0				Detail						
	Disabled Clients		0			Detail	This page refreshes every 30 s	econds.				

En la página Trampas más recientes, puede identificar el controlador que genera el mensaje de alerta de violación de la política AP confiable como se muestra en esta imagen:

Cisco - Microsoft Internet Ex	plorer provided by Cisco Systems, Inc.	_10 ×
Ele Edit Yew Favorites	Tools Alab	- 1
Croce Svereme	Save Configuration Ping Log	out Refresh
A. A.	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	
Monitor	Trap Logs Ct	ear Log
Summary	Number of Traps since last reset 12516	
Statistics Controller	Number of Traps since log last viewed 3	
Ports	Log System Time Trap	
Rogue APs	0 Wed Dec 12 Rogue : 00:0f:f0:S0:a0:5c removed from Base Radio MAC : 00:0b:85:5b:fb:d0 12:40:32 2007 Interface no:1(802.11b/g)	
Known Rogue APs Rogue Clients	1 Wed Dec 12 Rogue : 00:13:19:ab:99:00 removed from Base Radio MAC : 00:0b:85:5b:fb:d0 12:40:32 2007 Interface no:1(802.11b/o)	
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 Rogue AP : 00:13:19:49:00:70 detected on Base Radio MAC : 00:0b:85:51:5a:e0 12:39:31 2007 Interface no:1(802.11b/g) with RSSI: -47 and SNR: 48	
RADIUS Servers	4 Wed Dec 12 Rogue AP : 00:13:19:49:08:70 detected on Base Radio MAC : 00:0b:85:5b:fb:d0 12:39:31 2007 Interface no:1(002.11b/o) with BSS1: -55 and SNB: 44	
	5 Wed Dec 12 Rogue AP : 00:11:21:b4:ff:00 detected on Base Radio NAC : 00:0b:85:5b:fb:d0	
	6 Wed Dec 12 Trusted AP 00:07:05:92:4d:c9 has invalid radio policy. It's using 802.11a instead of 12:39:29 2007 802.11b/g	
	7 Wed Dec 12 Trusted AP 00:07:85:92:4d:c9 has invalid encryption configuration. It's using Open 12:39:29 2007 instead of WEP	
	8 Wed Dec 12 Trusted AP 00:02:8a:0e:33:f5 has invalid radio policy. It's using 802.11a instead of 12:39:29 2007 802.11b/o	
	9 Wed Dec 12 Trusted AP 00:02:8a:0e:33:f5 has invalid encryption configuration. It's using Open 12:39:29 2007 instead of WER.	
	10 Wed Dec 12 12:39:29 2007 Trusted AP 00:12:01:a1:f5:10 is advertising an invalid SSID.	
	Wed Dec 12 Regue : 00:11:Sc:93:d3:hB removed from Base Radio MAC : 00:0b:85:S1:Sa:e0 11 12:38:12 2007 Interface no:1(802.11b/e)	
	Wed Dec 12 Rogue : 00:14:f1:ae:9d:70 removed from Base Radio NAC : 00:0b:85:51:5a:e0 12 12:38:10 2007 Interface po:16802 11b (p)	
	Wed Dec 12 Rogue : 00:07:50:d5:cf:b9 removed from Base Radio MAC : 00:0b:85:51:5a:e0 13 12:39:10 2007 Interface part(002)	
	Wed Dec 12 Rogue : 00:19:a9:41:12:b4 removed from Base Radio MAC : 00:0b:85:51:5a:e0 14 12:38:10 2007 Interface no:1(602.11b/g)	
	15 Wed Dec 12 Rogue : 00:14:1b:b6:23:60 removed from Base Radio MAC : 00:0b:85:5b:fb:d0 12:37:32 2007 Interface no:1(802.11b/g)	
	Wed Dec 12 Rogue AP : 00:12:d9:e2:b9:20 detected on Base Radio MAC : 00:0b:85:51:5a:e0 16 12:37:18 2007 Interface no:0(802.11a) with RSSI: -83 and SNR: 8	-
× Discussions • 🞲 🕞 🕄	2 1 1 2 Ciscussions not available on http://10.77.244.204/	0)
Done .	🔮 Internet	

Información Relacionada

- Guía de Configuración del Controlador de LAN Inalámbrica de Cisco, Versión 5.2 -Habilitación de la Detección del Punto de Acceso de Ruteo en Grupos de RF
- Guía de Configuración del Controlador de LAN Inalámbrica de Cisco, Versión 4.0 -Configuración de Soluciones de Seguridad
- Detección no autorizada en redes inalámbricas unificadas
- Guía de diseño e implementación del teléfono SpectraLink
- Ejemplo de Configuración de Conexión LAN de Elementos Básicos de Red Inalámbrica
- Resolución de problemas de conectividad en una red inalámbrica de LAN
- Ejemplos de configuración de autenticación de controladores para redes LAN inalámbricas
- Soporte Técnico y Documentación Cisco Systems