無線LAN控制器上的受信任AP策略

目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>慣例</u> <u>受信任的AP策略</u> <u>什麼是受信任的AP?</u> <u>如何從WLC GUI將AP配置為受信任AP?</u> <u>瞭解受信任的AP策略設定</u> <u>如何在WLC上配置受信任的AP策略?</u> <u>受信任AP策略違規警報消息</u> <u>相關資訊</u>

<u>簡介</u>

本檔案介紹無線LAN控制器(WLC)上的*受信AP*無線保護策略,定義受信AP策略,並提供所有受信 AP策略的簡短說明。

必要條件

<u>需求</u>

確保您已基本瞭解無線LAN安全引數(例如SSID、加密、身份驗證等)。

<u>慣例</u>

如需文件慣例的詳細資訊,請參閱<u>思科技術提示慣例。</u>

<u>受信任的AP策略</u>

受信任AP策略是控制器中的一項安全功能,旨在用於客戶與控制器具有並行自主AP網路的方案。 在這種情況下,自治AP可以在控制器上標籤為可信AP,並且使用者可以定義這些可信AP的策略 (這些策略應僅使用WEP或WPA、我們自己的SSID、短前導碼等)。 如果其中任何AP無法滿足這 些策略,控制器會向網路管理裝置(無線控制系統)發出警報,指出受信任的AP違反了配置的策略 。

什麼是受信任的AP?

受信任的AP是不屬於組織的AP。但是,它們不會對網路造成安全威脅。這些AP也稱為友好AP。存

在多種情況,您可能希望將AP配置為受信任AP。

例如,您的網路中可能有不同類別的AP,例如:

• 您擁有的不運行LWAPP的AP(可能運行IOS或VxWorks)

- 員工引入的LWAPP AP (在管理員知情的情況下)
- •用於測試現有網路的LWAPP AP
- 鄰居擁有的LWAPP AP

通常,受信任的AP是屬於**類別1**的AP,它們是您擁有的不運行LWAPP的AP。它們可能是運行 VxWorks或IOS的舊AP。為了確保這些AP不會損壞網路,可以實施某些功能,如正確的SSID和身 份驗證型別。在WLC上配置受信任AP策略,並確保受信任AP符合這些策略。如果沒有,可以將控 制器配置為採取多種措施,例如向網路管理裝置(WCS)發出警報。

屬於鄰居的已知AP可以配置為受信任AP。

通常,MFP(管理幀保護)應阻止非合法LWAPP AP加入WLC。如果NIC卡支援MFP,則不允許它 們接受來自實際AP以外的裝置的取消身份驗證。有關MFP的詳細資訊,請參閱<u>具有WLC和LAP的基</u> 磁設施管理幀保護(MFP)配置示例。

如果您有運行VxWorks或IOS的AP(如類別1),它們永遠不會加入LWAPP組或執行MFP,但您可 能要強制實施該頁面上列出的策略。在這種情況下,需要在控制器上為感興趣的AP配置受信任的 AP策略。

一般來說,如果您知道某個惡意AP並發現它不會對您的網路構成威脅,您可以將該接入點識別為已 知的受信任AP。

如何從WLC GUI將AP配置為受信任AP?

完成以下步驟,將AP配置為受信任AP:

- 1. 透過HTTP或https登入登入WLC的GUI。
- 2. 在控制器主選單中,按一下Wireless。
- 3. 在Wireless (無線) 頁面左側的選單中,按一下Rogue APs。

Cisco - Microsoft Internet Ex	plorer provided by Cisco Systems, Inc.				×
Circo Sermon	MONITOR WLANS CONTROLLER	WIRELESS SECURITY MAN	Sar IAGEMENT COMMAI	ve Configuration Pi NDS HELP	ng Logout Refresh
Wireless Access Points All APS 802.11a Radios 802.11b/g Radios Third Party APS Bridging Rogue APS Rogue Clients Adhoc Rogues Clients Global RF 802.11a Network 802.11b/g Network 802.11b/	All APs Search by Ethernet MAC AP Name ap:5b:fb:d0 ap:51:5a:e0	WIRELESS SECURITY MAN Search AP ID Ethernet MAC 34 00:0b:85:5b:fb:d0 35 00:0b:85:51:5a:e0	Admin Status Qu Enable Rt Enable Rt	nds HELP Perational EG 2 EG 2	Detail Detail
× Discussions • 🎲 🕃 🕘	🗿 🗊 🧐 🔠 🧭 Discussions not available on ht	ttp://10.77.244.204/			ø
e)					D Internet

Rogue APs頁面列出了網路中檢測到作為欺詐AP的所有接入點。

4. 從非法AP清單中,找到要配置為屬於類別1的受信任AP的AP(如上一節所述)。您可以查詢 Rogue AP頁上列出了MAC地址的AP。如果所需AP未在此頁面中,請按一下**下一步**以從下一 頁面識別該AP。

5. 從Rogue AP清單中找到所需的AP後,點選與AP對應的Edit按鈕,該按鈕將引導您進入AP的 詳細資訊頁面。

Rogue APs			Iter	ms 1 to 20 of 26	\langle
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

在Rogue AP details(無管理AP詳細資訊)頁面中,可以找到有關此AP的詳細資訊(例如 AP是否連線到有線網路,以及AP的當前狀態等)。

6. 若要將此AP配置為受信任AP,請從Update Status下拉選單中選擇**Known Internal**,然後按一下**Apply**。將AP狀態更新為*Known Internal*時,此AP被配置為此網路的受信任AP。

							Save Costs	suration 5	ina 1000	d Defre	db.
	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMEN	л сом	MANDS H	IELP			
Wireless	Rogue AP Detail							< Back		pply	
Access Points All APs 802.11a Radios 802.11b/g Radios Third Party APs	MAC Address			00:12:01:61:f	5:10						
Bridging	Is Rogue On Wired M	vetwork?		No							
Rogues Rogue APs Known Rogue APs	First Time Reported On			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							
802.118 Network 802.11b/g Network 802.11h	Update Status			Choose I	New Status] New Status	3					
Country Timers				Contain Rogu Alert Unknow Known Intern Acknowledge	e n pi						
	APs that detected t	his Rogue		Acknowledge	C. Alfertings						
	Base Radio MAC	AP Name	SSI)	Channel	Radio Type	WEP	WPA	Pre- Amble	RSSI	1
	00:0b:85:51:5a:e0	ap:51:5a:e0	auto	2	1	802.119	Enabled	Enabled	Short	-71	2
	Clients associated t MAC Address	o this Rogue / Last	\P Time Heard								
	.										2
Discussions • 173 🕞	🔄 🔁 🐩 🐩 🔠 💆 Discussio	ns not available on h	ttp://10.77.244	204/							-

7. 對要配置為受信任AP的所有AP重複這些步驟。

<u>驗證受信任的AP配置</u>

完成以下步驟,從控制器GUI驗證AP是否正確配置為受信任AP:

- 1. 按一下「Wireless」。
- 2. 在Wireless(無線)頁面左側的選單中,按一下Known Rogue APs。

Cisco - Microsoft Internet Ex	plorer provided by Cisco Systems, Inc.					
Ele Edt Yew Favorites	Iools Help					
A. A.	MONITOR WLANS CONTROLLER	WIRELESS SECURITY MAI	NAGEMENT COM	Sava Configurati MANDS HELP	on Ping Lo	gout Refresi
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 Known 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						
Country						
Discussions * 🎲 🕃 🗐	🗿 🗊 🐮 🖉 Discussions not available on h	8tp://10.77.244.204/				
					interne	t

所需的AP應顯示在「已知無管理AP」頁面上,其狀態列為*已知*。

Eisco - Microsoft Internet Ex	plorer provided by Cisco	Systems, Inc.						@_×
Bie Edit Yew Fgvorites	Toole Rep							- 1 2K
Cinca Systems						re Configuratio	n Ping L	ogout Refresh
LA, A.	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY MANA	GEMENT COMMAJ	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	Ed	it Remove
Third Party APs	00:07:85:92:4d:c9	Unknown		2	0	Known	Ed	it Bemaxe
Bridging	00:0b:fc:fc:15:00	Unknown		1	0	Known	Ed	it Remove
Rogues	00:12:01:a1:f5:10	auto-2		2	0	Known		it Remove
Rogue Clients Adhoc Rogues Clients Global RF 802.11a Network 802.11b/g Network 802.11h Country Timers								
× Discussions • 💋 🖓 🖏	999 19 19 Ø0	ussions not available on h	R1p:∬10.77.244.	204/				9
2 Done							Dinkerr	set .

<u>瞭解受信任的AP策略設定</u>

WLC具有以下受信任的AP策略:

- <u>強制加密策略</u>
- 實施的無線電型別策略
- <u>驗證SSID</u>
- 缺少受信任的AP時發出警報
- <u>受信任AP條目的過期超時(秒)</u>

此策略用於定義受信任AP應使用的加密型別。您可以在Enforced encryption policy下配置以下任何 加密型別:

- 無
- 未解決
- WEP
- WPA/802.11i

WLC驗證受信任AP上配置的加密型別是否與「強制加密策略」設定中配置**的加密類**型匹配。如果受 信任的AP不使用指定的加密型別,WLC會向管理系統發出警報,以便採取適當的措施。

無線電報頭(有時稱為報頭)是資料包頭部的資料部分,包含無線裝置傳送和接收資料包時所需的 資訊。**短前導**碼可提高吞吐量效能,因此預設情況下啟用短前導碼。但是,某些無線裝置(例如 SpectraLink NetLink電話)需要長**的前**導符。您可以在Enforced preamble(實施前導碼)策略下配 置以下任何前導碼選項:

- 無
- 短
- •長

WLC驗證受信任AP上配置的前導碼型別是否與「強制的前導碼策略」設定**上配置的前**導碼型別。如 果受信任的AP不使用指定的報頭型別,WLC會向管理系統發出警報,以便採取適當的措施。

實施的無線電型別策略

此策略用於定義受信任AP應使用的無線電型別。您可以在Enforced radio type policy下配置以下任 何無線電型別:

- 無
- •僅802.11b
- •僅802.11a
- •僅802.11b/g

WLC驗證受信任AP上配置的無線電型別是否與「強制無線電型別策略」設定**上配置的無線電類**型匹 配。如果受信任的AP不使用指定的無線電,WLC會向管理系統發出警報,以便採取適當的措施。 您可以配置控制器,以根據控制器上配置的SSID驗證受信任的AP SSID。如果受信任的AP SSID與 控制器SSID之一匹配,控制器將發出警報。

<u>缺少受信任的AP時發出警報</u>

如果啟用此策略,則如果已知無管理AP清單中缺少受信任AP,則WLC會向管理系統發出警報。

<u>受信任AP條目的過期超時(秒)</u>

此Expiration Timeout值指定受信任AP被視為已過期並從WLC條目中刷新之前的秒數。可以指定此 超時值(秒)(120 - 3600秒)。

如何在WLC上配置受信任的AP策略?

完成以下步驟,以便透過GUI在WLC上設定受信任AP原則:

注意:所有受信任的AP策略都位於同一WLC頁面上。

- 1. 在WLC GUI主功能表中,按一下「Security」。
- 2. 在「安全」頁面左側的選單中,按一下「無線保護策略」標題下面列出的**受信任AP策略**。



3. 在Trusted AP policies(受信任AP策略)頁上,從Enforced encryption policy(實施加密策略)下拉選單中選擇所需的加密型別(None、Open、WEP、WPA/802.11i)。

Ele Edt Yew Favorites	Jook Help	and the second			1
Case Stations			Save Configura	tion Ping	Logout Ref
A. A.	MONITOR WLANS CONTROLLER WIRELESS SE	CURITY MANAGEMENT	COMMANDS HELF		
Security	Trusted AP Policies			< Back	Apply
General RADIUS Authentication	Enforced encryption policy	WEP .			
Local Net Users	Enforced preamble policy	WEP WPA/802.11i	-		
Disabled Clients User Login Policies AP Policies	Enforced radio type policy	None			
Access Control Lists	Validate SSID	Enabled			
IPSec Certificates CA Certificate	Alert if Trusted AP is missing	Enabled			
Web Auth Certificate	Expiration Timeout for Trusted AP Entries (second	ads) 120			
Policies Trusted AP Policies Rogue Policies Standard Signatures Custom Signatures Client Exclusion Policies AP Authentication	Image: Image: Source of the state of the				
· Decressore · D D O	이 데 데 데 AD becassions not available on http://to.///.244.204/				arreat
ᄡᄃᇥᄹᇹᇪᇹᇹᆋᇥᇪᇹᇂ	·····································	公司的关道理制		Dia ant	
EENTORCED prea	amble type policy下拉进丰中选择) solarer provided by Cisco Systems, Inc.	11 常的 則 导 嗎 空	別(INONe、 3	snort,	Long)。
Ele Edk Yew Favorites	Tools Field				
Cases Sverens			Save Configura	tion Ping	Logout Re
AA	MONITOR WLANS CONTROLLER WIRELESS SE	CURITY MANAGEMENT	COMMANDS HELP	•	
Security	Trusted AP Policies			< Back	Apply
ÁAA General RADIUS Authentication	Enforced encryption policy	WEP			
RADIUS Accounting Local Net Users MAC Filtering	Enforced preamble policy	None 💌			
Disabled Clients User Login Policies	Enforced radio type policy	long			
AP Policies Access Control Lists	Validate SSID	Enabled			
shale of still a still					

 Web Auth Certificate
 Expiration Timeout for Trusted AP Entries (seconds)

 Wireless Protection Policies
 Trusted AP Policies

 Rogue Policies
 Standard Signatures

 Custom Signatures
 Client Exclusion Policies

 AP Authentication
 AP Authentication

× Discussions * 🗊 🕲 🕄 🐩 🐩 🗷 Ø Discussions not available on http://10.77.244.204/

1

5. 從Enforced radio type policy下拉選單中選擇所需的無線電型別(無、僅802.11b、僅 802.11a、僅802.11b/g)。



- 6. 選中或取消選中Validate SSID Enabled 覈取方塊以啟用或禁用Validate SSID 設定。
- 7. 選中或取消選中**Alert if trusted AP is missing Enabled**覈取方塊,以啟用或禁用Alert if trusted AP is missing設定。
- 8. 為Expiration Timeout for Trusted AP entries 選項輸入一個值(以秒為單位)。



9. 按一下「Apply」。

注意:為了從WLC CLI配置這些設定,您可以使用帶有適當策略選項的config wps trusted-ap命令。

Cisco Controller) >config wps trusted-ap ?

encryption	Configures t	he trusted AP encryption policy to be enforced.
missing-ap	Configures a	lert of missing trusted AP.
preamble	Configures t	he trusted AP preamble policy to be enforced.
radio	Configures t	he trusted AP radio policy to be enforced.
timeout	Configures t	he expiration time for trusted APs, in seconds.

受信任AP策略違規警報消息

以下是控制器顯示的受信任AP策略違規警報消息的示例。

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:el: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 請注意此處突出顯示的錯誤消息。這些錯誤消息表示受信任AP上配置的SSID和加密型別與受信任 AP策略設定不匹配。

可從WLC GUI看到相同的警報訊息。若要檢視此訊息,請前往WLC GUI主功能表,然後按一下「 Monitor」。在「監視器」頁的「最新陷阱」部分中,按一下檢視全部以檢視WLC上的所有最新警報

	-		
	r		
1		,	

Edit Yew Favorit	tes Iools Help									
Statum							Save Config	ration Ping	Logout A	
A	HOMITON MILLIN		001150		***	eccupro	HUNDERET CONTINUE IN	210		
	MONITOR WEAK	SCON	NULLER	WINEU	599	SECONTIN	In Access Parks Supported	:0'		
nitor	Core Protons						Cisco 4400 Series			
	A.A. *	-			·		Wheless LAN Controller			
imary			100 10	-	ļ					
istics							· · · · · · · · · · · · · · · · · · ·			
ts	Controller Summ	ary					Rogue Summary			
less	Management IP Add	fress	10.77.2	44.204						
que APs	Service Port IP Add	Service Port IP Address 0.0.0.0					Active Rogue APs	25	Detail	
gue Clients	Software Version		3.2.150	3.2.150.10			Active Rogue Clients	0	Detai	
hoc Rogues	System Name		WLC-4400-TSWEB				Adhoc Rogues	0	Detail	
.11a Kadios .11b/g Radios	Up Time		16 day	16 days, 8 hours, 42 minutes			Rogues on Wired Network	0		
ents	System Time		Wed Dec 12 12:40:03 2007							
DIUS Servers	Internal Temperatu	re	+38 C				Top WLANs			
	802.11a Network St	ate	Enabled					# of C	# of Clients	
	802.11b/g Network	State					WLAN	by SS	ID	
							WCS	0	Detail	
	Access Point Sur	nmary					WC\$123	0	Detail	
	House Found out	initial y								
		Total	Up		Down		Most Recent Traps			
	802.11a Radios	2	• 2	٠	0	Datail	A			
	802.11b/g Radios	2	• 2	•	0	Detail	Rogue AP 1 001131191491081	/U detected on	Base Kadio	
	All APs	2	• 2	•	0	Detail	Rogue AP : 00:13:19:49:00:	o detected on	Base Radio	
							Rogue AP : 00:11:21:04:000	a becievelid of	base kadio i	
	Client Summary						Trusted AD 00:07:85:92:44:0	has invalid ro	adio policy. I	
							Trusted AP 00:07:05:92:40:0	y has invalid e	noryption co	
	Current Clients		6			Detail			VIEW AL	
	Excluded Clients		0			Detail				
	Disabled Clients		0			Detail	inis page refreshes every 30 se	conds.		
	Disabled Cilents		-							

在「最新陷阱」頁面上,您可以標識生成受信任AP策略違規警報消息的控制器,如下圖所示:

🗿 Cisco - Microsoft Internet Ex	lorer provided by Cisco Systems, Inc.	Gillions 672		.ex
Ele Edt Vew Favorites	ook Heb			#
Conce Systems			Save Co	onfiguration Ping Logout Refresh
A.A.	MONITOR WLANS CONTROLLER W	IRELESS SECURITY	MANAGEMENT COMMANDS	HELP
Monitor	Trap Logs			Clear 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:f8 12:40:32 2007 Interface no:1(:58:a8:5c removed from 802.11b/g)	m Base Radio MAC : 00:0b:85:	5b:fb:d0
Known Rogue APs Rogue Clients	1 Wed Dec 12 Rogue : 00:13:1 12:40:32 2007 Interface no:1()	9:ab:99:00 removed fro 802.11b/g)	om Base Radio MAC : 00:0b:85	5:5b:fb:d0
Adhoc Rogues 802.11a Radios	2 Wed Dec 12 Rogue : 00:13:1 12:40:32 2007 Interface no:1()	9:ab:99:00 removed fre 802.11b/g)	om Base Radio MAC : 00:0b:85	5:51:5a:e0
802.11b/g Radios Clients	3 Wed Dec 12 Rogue AP : 00:1 12:39:31 2007 Interface no:1(3:19:49:08:70 detected 802.11b/g) with RSSI:	on Base Radio MAC : 00:0b:8 -47 and SNR: 48	5:51:5a:e0
RADIUS Servers	4 Wed Dec 12 Rogue AP : 00:1 12:39:31 2007 Interface no:10	3:19:49:08:70 detected 802.11b/g) with RSSI:	on Base Radio MAC : 00:0b:8 -55 and SNR: 44	5:5b:fb:d0
	5 Wed Dec 12 Rogue AP : 00:1 12:39:31 2007 Interface no:10	1:21:b4:ff:00 detected 802.11b/a) with RSSI:	on Base Radio MAC : 00:0b:85 -95 and SNR: 4	5:Sb:fb:d0
	6 Wed Dec 12 Trusted AP 00:0 12:39:29 2007 802.11b/o	17:85:92:4d:c9 has inva	lid radio policy. It's using 80	2.11a instead of
	7 Wed Dec 12 Trusted AP 00:0 12:39:29 2007 instead of WEP	17:85:92:4d:c9 has inva	lid encryption configuration.	It's using Open
	8 Wed Dec 12 Trusted AP 00:0 12:39:29 2007 802-11b/o	12:8a:0e:33:f5 has inva	lid radio policy. It's using 80	2.11a instead of
	9 Wed Dec 12 Trusted AP 00:0 12:39:29 2007 instead of WED	12:8a:0e:33:f5 has inva	lid encryption configuration.	It's using Open
	10 Wed Dec 12 12:39:29 2007 Trusted AP 00:1	2:01:a1:f5:10 is advert	ising an invalid SSID.	>
	11 Wed Dec 12 Regue : 00-11-5 12:38:12 2007 Interface no:10	c:93:d3:h0 removed fro 802.11b/g)	am Base Rodio MAC : 00:0b:85	5:51:5a:e0
	12 Wed Dec 12 Rogue : 00:14:f 12:38:10 2007 Interface no:10	1:ae:9d:70 removed fro 802.11b/o)	m Base Radio MAC : 00:0b:85	:51:5a:e0
	13 Wed Dec 12 Rogue : 00:07:5 12:38:10 2007 Interface no:10	0:d5:cf:b9 removed fro 802.11b/a)	m Base Radio MAC : 00:0b:85	:51:5a:e0
	14 Wed Dec 12 Rogue : 00:19:a 12:38:10 2007 Interface po:10	9:41:12:b4 removed fro	om Base Radio MAC : 00:0b:85	5:51:5a:e0
	15 Wed Dec 12 Rogue : 00:14:1 12:37:32 2007 Interface po:10	b:b6:23:60 removed fre 802.11b/a)	om Base Radio MAC : 00:0b:8	5:5b:fb:d0
	16 Wed Dec 12 Rogue AP : 00:1 12:37:18 2007 Interface no:0(2:d9:e2:b9:20 detected 802.11a) with RSSI: -83	on Base Radio MAC : 00:0b:8 3 and SNR: 8	5:51:5a:e0
× Discussions • 🎲 🕃 🕄	📁 🐩 🔝 🧭 Discussions not available on http:	//10.77.244.204/		9
Done				internet

相關資訊

- Cisco無線LAN控制器組態設定指南5.2版 在RF組中啟用Rouge存取點偵測
- 思科無線LAN控制器組態設定指南4.0版 設定安全解決方案
- 統一無線網路下的惡意檢測
- SpectraLink電話設計和部署指南
- 基本無線 LAN 連線的組態範例
- 排除無線LAN網路中的連線故障
- 無線LAN控制器上的驗證組態範例
- 技術支援與文件 Cisco Systems