統一無線網路下的惡意檢測

目錄

簡介

無線網路擴展了有線網路，提高了員工的工作效率和資訊訪問能力。然而，未經授權的無線網路帶來了額外的安全隱患。對有線網路的埠安全考慮較少，無線網路很容易擴展到有線網路。因此，將自己的思科接入點(AP)引入安全可靠的無線或有線基礎設施並允許未經授權的使用者訪問此安全網路的員工很容易危及安全網路。

欺詐檢測允許網路管理員監控並消除這種安全問題。思科統一網路架構提供兩種欺詐檢測方法，可實現完整的欺詐識別和遏制解決方案，而無需昂貴且難以驗證的重疊網路和工具。

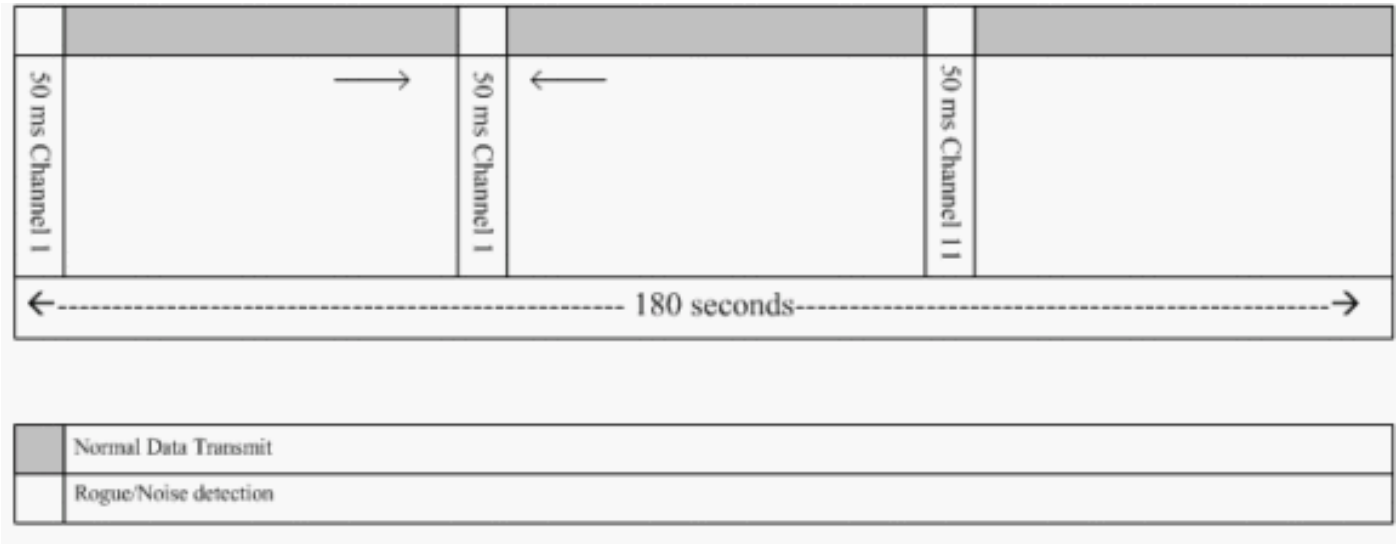
功能概述

欺詐檢測不受任何法規的約束，其操作無需遵守法律。但是，惡意遏制通常會帶來法律問題，如果讓基礎架構提供商自動運行，這些問題可能會使基礎架構提供商處於不利位置。思科對此類問題極為敏感，可提供以下解決方案。每個控制器都配置有RF組名稱。輕量AP向控制器註冊後，會在其所有信標/探測響應幀中嵌入特定於控制器上配置的RF組的身份驗證資訊元件(IE)。當輕量AP從沒有此IE或具有錯誤IE的AP接收到信標/探測響應幀時，輕量AP會報告AP為惡意，將其BSSID記錄在惡意表中，並將表傳送到控制器。其中有兩種方法，即無管理位置發現協定(RLDP)和無源操作，分別進行了詳細的說明；請參閱確定活動欺詐部分。

基礎架構惡意發現

在活動無線環境中進行非法發現可能成本高昂。此過程要求處於服務（或本地模式）中的AP停止服務、偵聽雜訊並執行欺詐檢測。網路管理員配置掃描通道，並配置掃描所有站的時間段。AP偵聽惡意客戶端信標50 ms，然後返回到已配置的通道以再次為客戶端提供服務。此活動掃描與鄰居消息結合使用，可識別哪些接入點是無管理系統，哪些接入點是有效的，哪些是網路的一部分。若要設定掃描的通道和掃描時間段，請瀏覽至Wireless > 802.11b/g Network(視網路要求而定，選擇「b/g」或「a」)，然後選擇瀏覽器視窗右上角的「Auto RF」按鈕。

您可以向下滾動到**雜訊/干擾/無管理系統監控通道**，以配置要掃描的通道以檢測無管理系統或雜訊。可用選項包括：所有通道（1至14）、國家/地區通道（1至11）或動態通道關聯(DCA)通道（預設值為1、6和11）。 經過這些通道的掃描時間段可以在同一視窗、監控間隔（60到3600秒）和雜訊測量間隔(Monitor Intervals)下配置。預設情況下，非通道雜訊和惡意代碼的偵聽間隔為180秒。這意味著每180秒掃描一次每個通道。以下是每180秒掃描的DCA通道範例：



如圖所示，配置要掃描的大量通道與較短的掃描間隔相結合，使AP實際為資料客戶端提供服務的時間更短。

輕量型AP會等待，以將客戶端和AP標籤為惡意程式，因為這些惡意程式可能不會被另一個AP報告，直到另一個週期完成。同一個AP再次移動到同一通道，以監控欺詐AP和客戶端以及噪音和干擾。如果偵測到相同的使用者端和/或AP，則它們會在控制器上再次列為無管理系統。現在，控制器開始確定這些惡意程式是連線到本地網路，還是僅連線到相鄰AP。無論哪種情況，不屬於受管本地無線網路的AP都被視為欺詐接入點。

欺詐詳細資訊

輕量AP在通道外傳輸50毫秒，以偵聽惡意客戶端、監控噪音和通道干擾。檢測到的任何欺詐客戶端或AP都會傳送到控制器，控制器會收集以下資訊：

- 非法AP MAC地址
- 惡意AP名稱
- 惡意連線的客戶端MAC地址
- 幀是使用WPA還是WEP進行保護
- 序言
- 訊雜比
- 接收器訊號強度指示器(RSSI)

惡意檢測器接入點

您可以讓AP作為欺詐檢測器運行，這樣可以將其置於中繼埠上，使其可以偵聽所有有線端連線的VLAN。接下來會在所有VLAN的有線子網中查詢客戶端。欺詐檢測器AP偵聽地址解析協定(ARP)資料包，以確定已識別的欺詐客戶端或控制器傳送的欺詐AP的第2層地址。如果找到匹配的第2層地址，控制器會生成警報，將欺詐AP或客戶端識別為威脅。此警報表示在有線網路上發現惡意。

確定活動欺詐

惡意AP在被控制器新增為惡意接入點之前，必須「看到」兩次。如果非法AP未連線到公司網路的有線網段，則不會將其視為威脅。為了確定無管理系統是否處於活動狀態，可使用各種方法。這些辦法包括區域發展方案。

無管理系統位置探索通訊協定(RLDP)

RLDP是一種主動方法，當欺詐AP未配置身份驗證（開放式身份驗證）時使用。此模式預設處於禁用狀態，它指示活動AP移動到無管理系統通道並作為客戶端連線到無管理系統。在此期間，活動AP將取消身份驗證消息傳送到所有連線的客戶端，然後關閉無線電介面。然後，它將作為客戶端與惡意AP關聯。

然後，AP嘗試從惡意AP獲取IP地址，並通過惡意AP將包含本地AP和惡意連線資訊的使用者資料包協定(UDP)資料包（埠6352）轉發到控制器。如果控制器收到此資料包，警報設定為通知網路管理員，在有線網路上發現具有RLDP功能的欺詐AP。

注意：使用debug dot11 rldp enable命令檢查輕量AP是否關聯並從惡意AP接收DHCP地址。此命令還顯示輕量AP傳送到控制器的UDP資料包。

以下是輕量AP傳送的UDP（目的地連線埠6352）封包的範例：

```
0020 0a 01 01 0d 0a 01 .......(.*....... 0030 01 1e 00 07 85 92 78 01 00 00 00 00 00 00 00 00
00...x......... 0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

資料的前5個位元組包含惡意AP提供給本地模式AP的DHCP地址。接下來的5個位元組是控制器的IP地址，然後是6個位元組，代表非法AP MAC地址。然後是18位元組的零。

被動操作：

當欺詐AP具有某種形式的身份驗證（WEP或WPA）時，使用此方法。在惡意AP上配置身份驗證形式時，輕量AP無法關聯，因為它不知道惡意AP上配置的金鑰。當控制器將惡意客戶端MAC地址清單傳遞給配置為惡意檢測器的AP時，該過程從控制器開始。欺詐檢測器掃描所有連線和配置的子網以查詢ARP請求，ARP搜尋匹配的第2層地址。如果發現匹配項，控制器將通知網路管理員在有線子網中檢測到欺詐行為。

主動欺詐遏制

一旦在有線網路上檢測到欺詐客戶端，網路管理員就能夠同時包含欺詐AP和欺詐客戶端。之所以可以實現這一點，是因為802.11去身份驗證資料包被傳送到與惡意AP關聯的客戶端，從而緩解了此類漏洞造成的威脅。每次嘗試控制非法AP時，將近15%的輕量AP資源被使用。因此，建議在包含欺詐AP後對其進行物理定位和刪除。

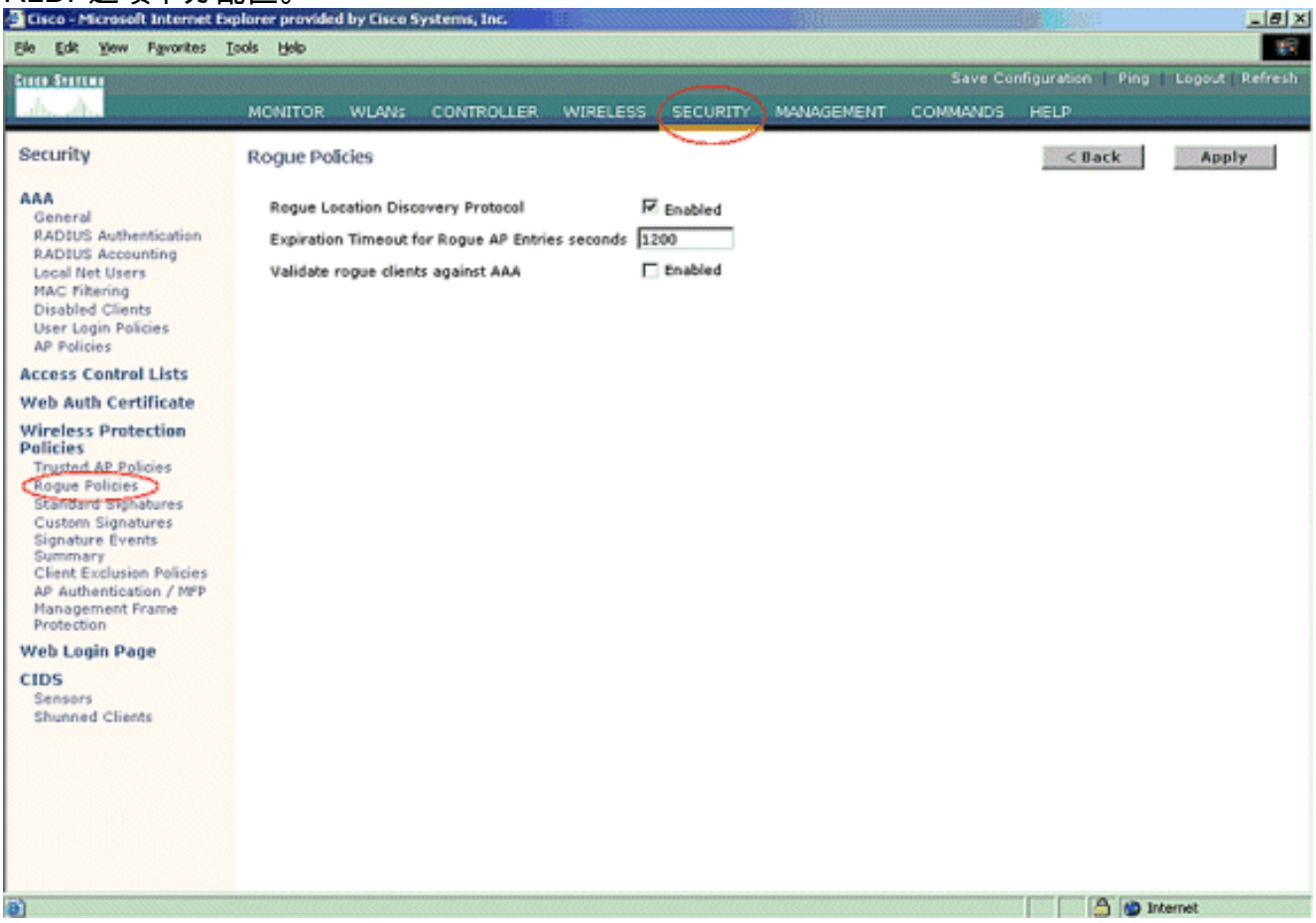
附註： 在WLC 5.2.157.0版中，一旦檢測到假冒，您現在可以選擇手動或自動包含檢測到的假冒。在5.2.157.0之前的控制器軟體版本中，手動遏制是唯一的選項。

欺詐檢測 — 配置步驟

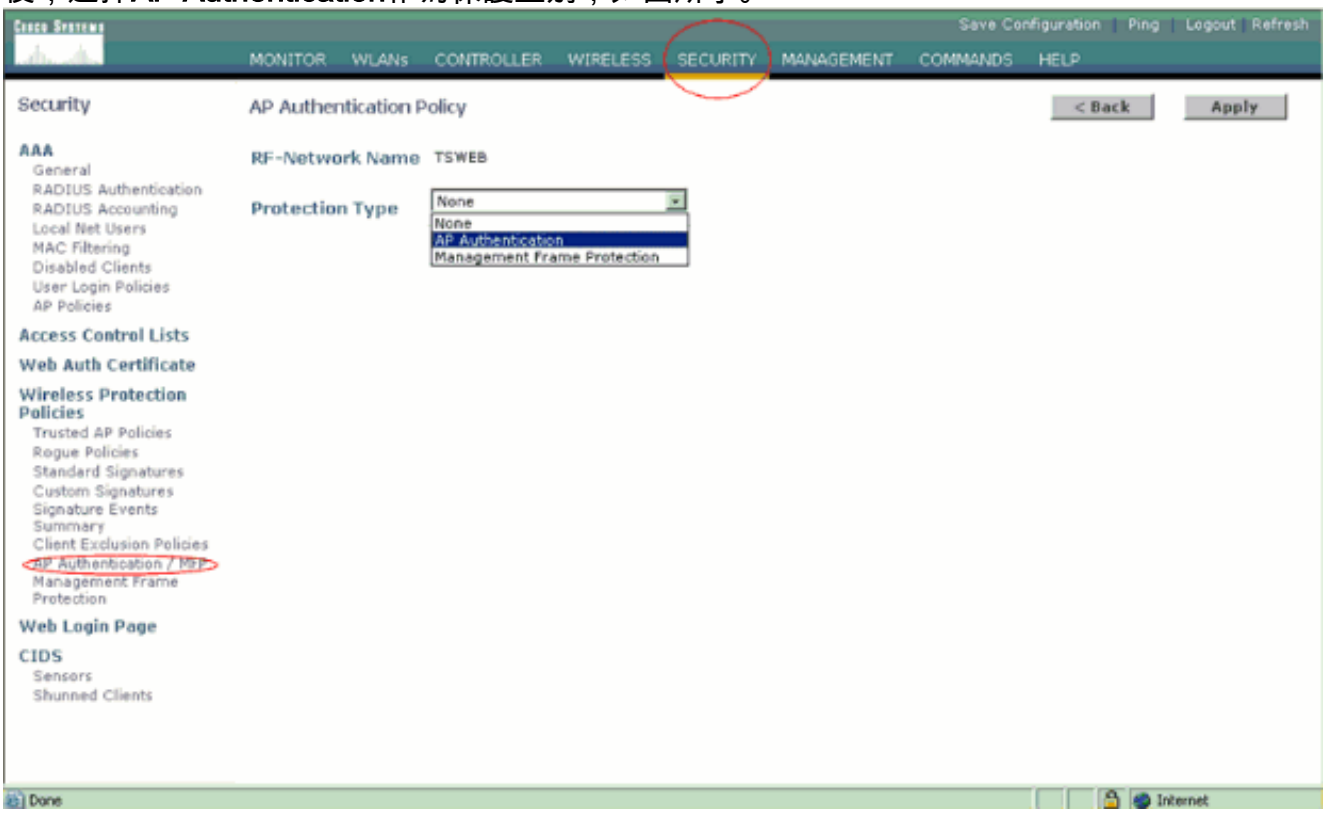
幾乎整個欺詐檢測配置在預設情況下都處於啟用狀態，以實現最大化的開箱即用網路安全。這些配置步驟假設控制器上未設定欺詐檢測，以便澄清重要的欺詐檢測資訊。

要設定欺詐檢測，請完成以下步驟：

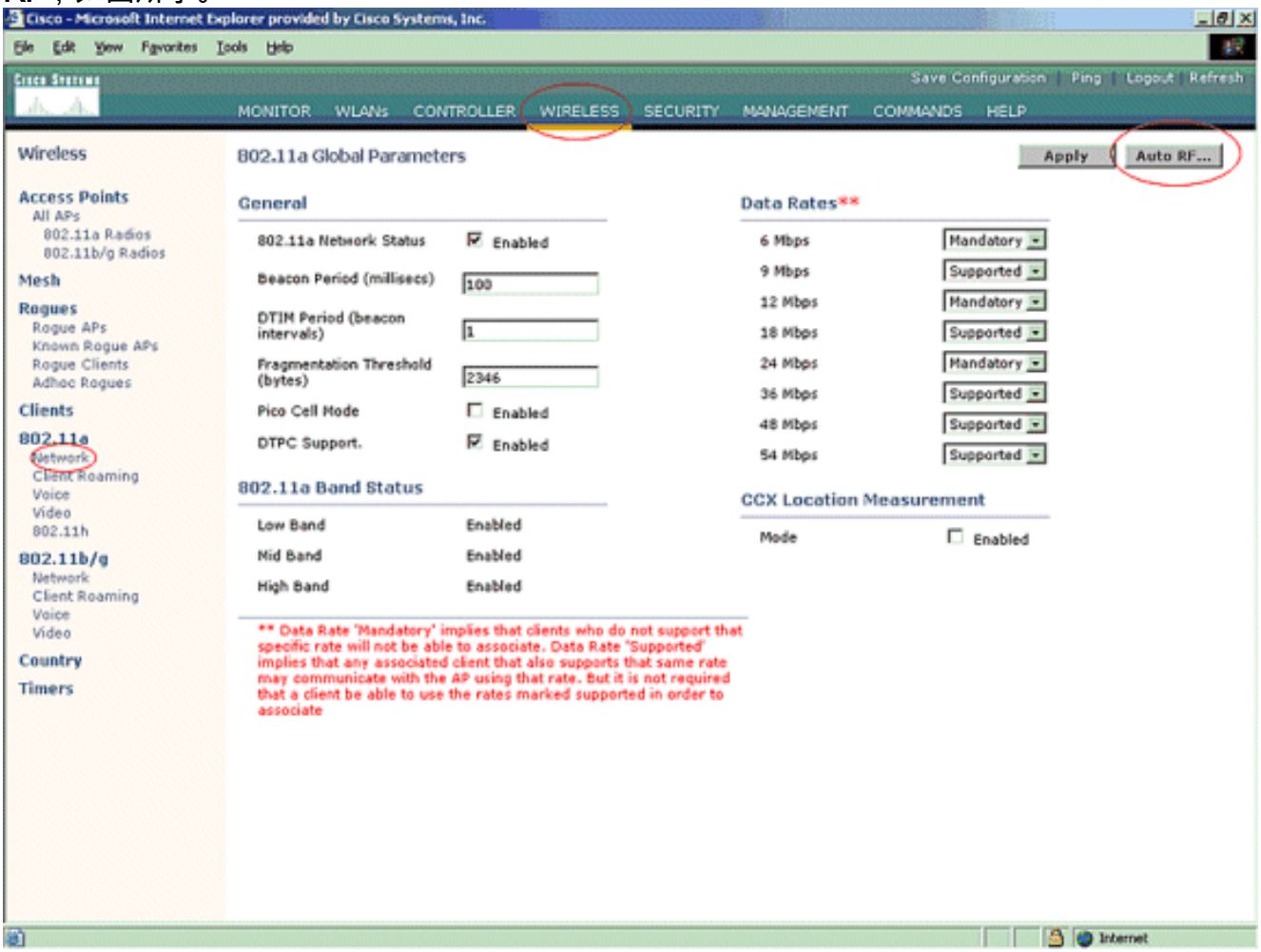
1. 確保已開啟「無管理系統位置發現」協定。若要將其開啟，請選擇**Security > Rogue Policies**，然後在**Rogue Location Discovery Protocol**上按一下**Enabled**，如圖所示。**注意：**如果某個非法AP在一段時間內未被監聽，則它會從控制器中刪除。這是欺詐AP的**過期超時**，在RLDP選項下方配置。



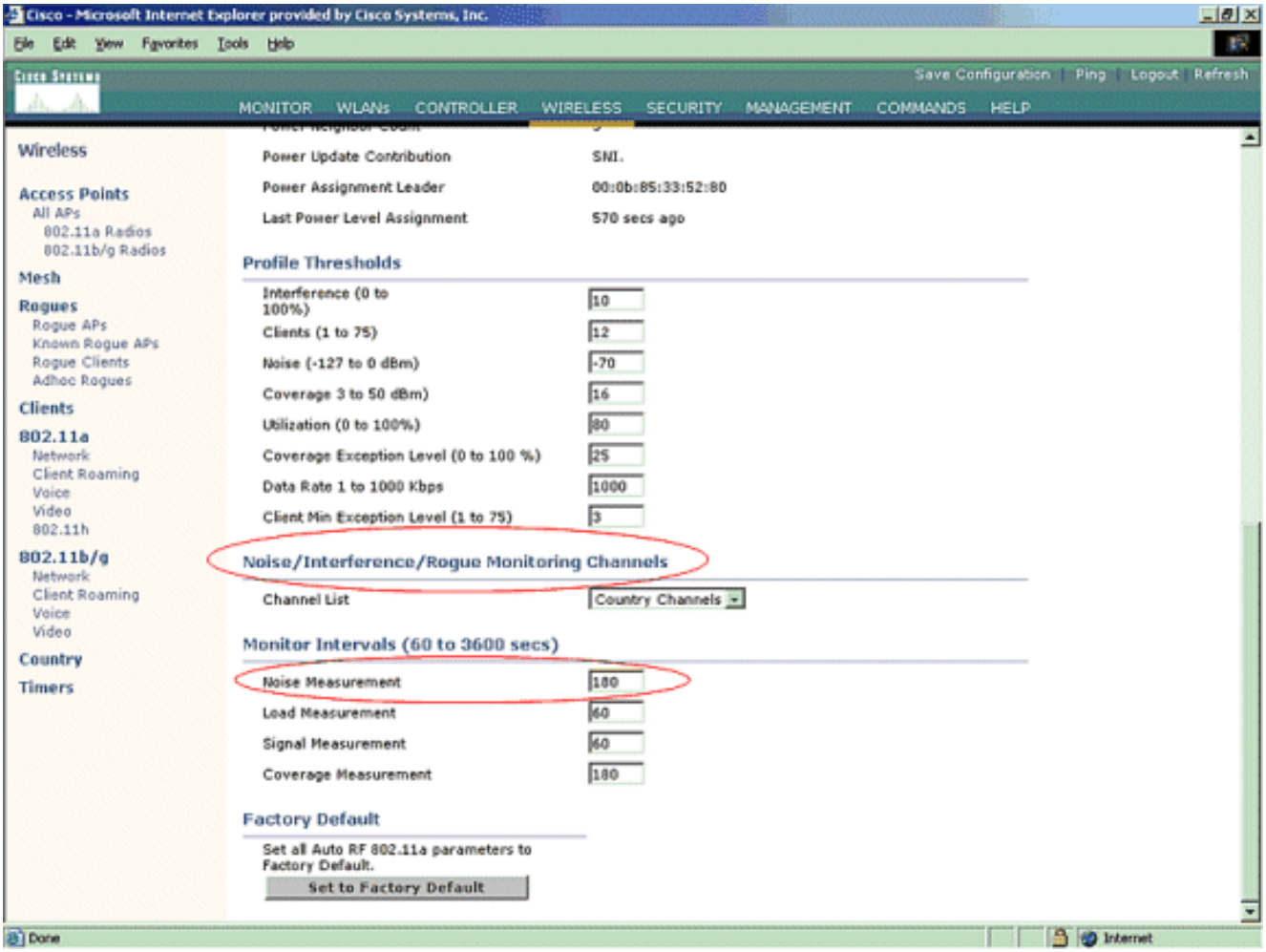
2. 這是選用步驟。啟用此功能後，傳送具有不同RF組名稱的RRM鄰**居資料**包的AP將報告為無管理系統。這將有助於研究您的RF環境。若要啟用它，請選擇**Security-> AP Authentication**。然後，選擇**AP Authentication**作為保護型別，如圖所示。



3. 按以下步驟驗證要掃描的通道：選擇**Wireless > 802.11a Network**，然後在右側選擇**Auto RF**，如圖所示。



在**Auto RF**頁面上，向下滾動並選擇**Noise/Interference/Rogue Monitoring Channels**。

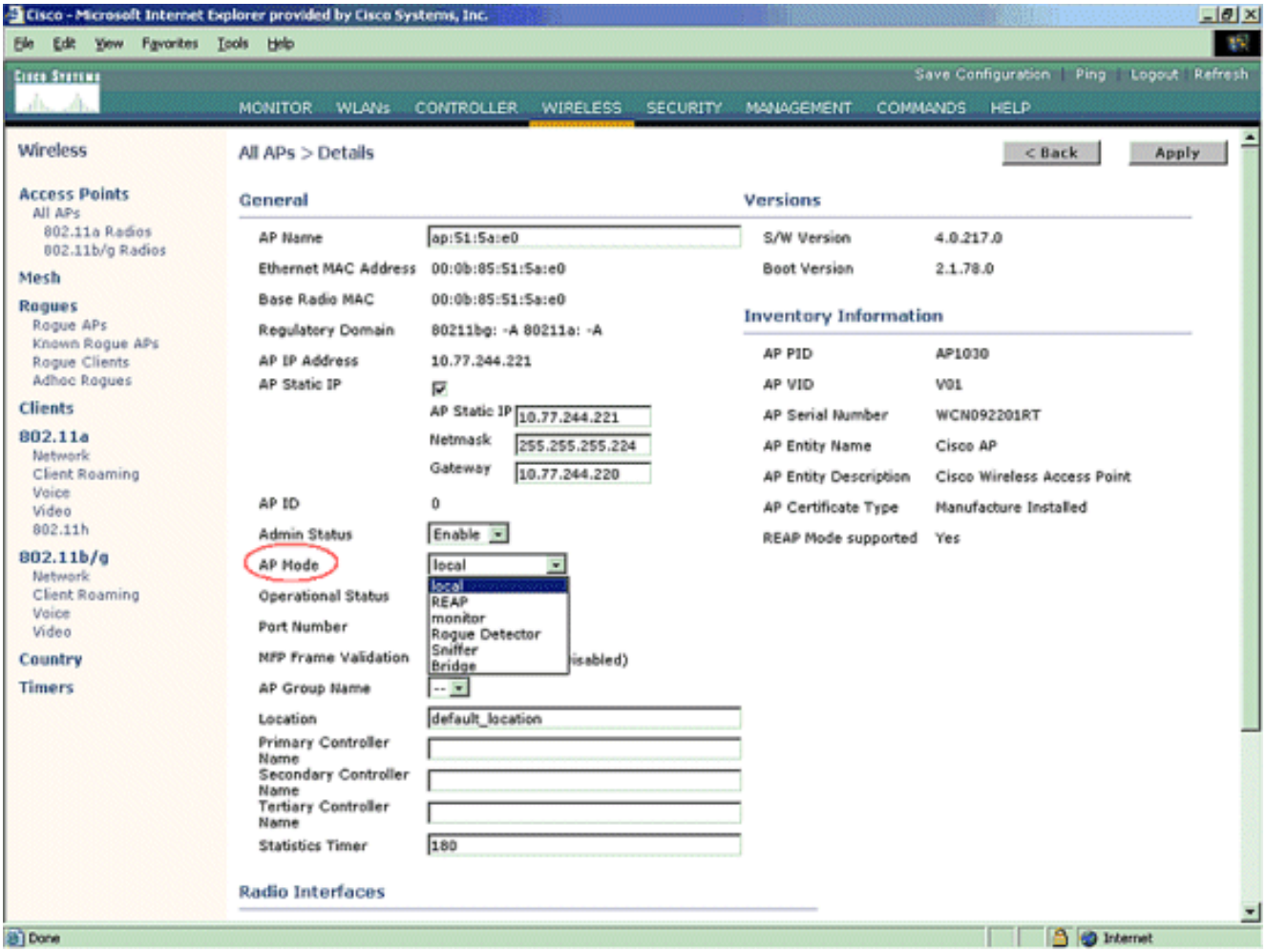


除了其他控制器和AP功能外，「通道清單」還詳細列出了要掃描的用於惡意監控的通道。有關輕量AP的詳細資訊，請參閱輕量型存取點常見問題，有關無線控制器的詳細資訊，請參閱無線LAN控制器(WLC)疑難排解常見問題。

Channel Group Option	Channels Scanned for 802.11b/g	Channels Scanned for 802.11a
All Channels	1 - 14	
Country Channels	1 -11	
DCA Channels (Configurable)	1, 6, 11	36, 40, 44, 48, 52, 56, 60, 64

4. 設定掃描所選通道的時間段：已定義通道組的掃描持續時間在**Monitor Intervals > Noise Measurement**下配置，允許範圍是60到3600秒。如果保留預設值180秒，AP將每180秒掃描一次通道組中的每個通道，持續50毫秒。在此期間，AP無線電從其服務通道改變為指定通道，偵聽並記錄50毫秒期間的值，然後返回到原始通道。跳數時間加上50毫秒的駐留時間，會使AP每次離開通道約60毫秒。這意味著每個AP在總共180秒中花費大約840毫秒來監聽惡意程式。「listen」或「dwell」時間不能修改，並且不能隨雜訊測量值的調整而更改。如果雜訊測量計時器降低，惡意發現過程可能會發現更多惡意程式，並更快地找到它們。但是，這種改進是以犧牲資料完整性和客戶端服務為代價的。另一方面，較高的值可以提高資料完整性，但會降低快速找到惡意代碼的能力。
5. 配置AP操作模式：輕量AP操作模式定義AP的角色。與本文檔中提供的資訊相關的模式有

：**Local** — 這是AP的正常操作。此模式允許在掃描已配置的通道以檢測噪音和欺詐時，為資料客戶端提供服務。在此操作模式下，AP會關閉通道50毫秒，並偵聽惡意程式。在自動RF配置中指定的時間段內，它會逐個循環通過每個通道。**Monitor** — 這是僅無線電接收模式，允許AP每12秒掃描一次所有配置的通道。只有解除驗證資料包才會通過這樣配置的AP在空中傳送。監控模式AP可以檢測惡意程式，但無法作為客戶端連線到可疑惡意程式以傳送RLDP資料包。**注意**：DCA是指可使用預設模式配置的非重疊通道。**欺詐檢**測器 — 在此模式下，AP無線電關閉，並且AP僅偵聽有線流量。控制器會傳送配置為惡意檢測器的AP，以及可疑惡意客戶端和AP MAC地址的清單。欺詐檢測器僅偵聽ARP資料包，如果需要，可以通過TRUNK鏈路連線到所有廣播域。輕量AP連線到控制器後，您可以簡單配置單個AP模式。若要變更AP模式，請連線到控制器Web介面，然後導覽至**Wireless**。按一下所需AP旁邊的**Details**以顯示與以下內容類似的螢幕
：



使用AP模式下拉選單選擇所需的AP操作模式。

疑難排解指令

您也可以使用以下命令來疑難排解AP上的組態：

- **show rogue ap summary** — 此命令顯示輕量AP檢測到的欺詐AP清單。
- **show rogue ap detailed** *<rogue ap的MAC地址>* — 使用此命令可檢視有關單個欺詐AP的詳細資訊。此命令可幫助確定無管理AP是否插入有線網路。

結論

思科集中式控制器解決方案中的欺詐檢測和遏制是業內最有效、干擾最小的方法。為網路管理員提供的靈活性使網路管理員能夠適應任何網路需求，從而更加定製。

相關資訊

- RF組概述
- 技術支援與文件 - Cisco Systems