在升級接入點韌體時保持關聯能力

目錄

簡介

本檔案將說明在下列情況下，使用者端無法與存取點(AP)相關聯的原因：

- 運行輕型可擴展身份驗證協定(LEAP)/非同步通訊伺服器(ACS)。
- AP上的韌體將升級到11.06或更高版本。
- 客戶端上的韌體升級為版本4.25。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- AP340韌體版本11.06和PC340韌體版本4.25.5。
- AP AIR-AP342E2R和客戶端介面卡AIR-PCM342。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

問題1

AP上的韌體版本11.06及更高版本符合IEEE 802.1X Draft 10標準。Draft 8標準在此版本之前使用。客戶端上的韌體版本4.25符合草案10。在執行韌體11.06的AP上，您可以使用任一草案。如果您希望運行韌體4.23及更早版本的客戶端關聯，請使用Draft 8。對於使用Draft 8配置的11.06 AP，4.25客戶端不工作，4.25客戶端不與11.05 AP工作。

AP韌體版本	客戶端韌體版本	IEEE 802.1X草案
11.06（及更高版本）	4.25	10
	4.23或更低版本	8
11.03--11.05	4.25（不適用於11.05）	AP需要8，但客戶端不能與8
	4.23或更低版本	8

解決方案1

有兩種方法可以解決此問題：

1. 在AP上使用Draft 10(11.06)，並將客戶端卡的韌體升級到4.25。
2. 在AP上使用Draft 8，並在客戶端上使用帶有早期韌體的AP。

此表顯示了客戶端介面卡韌體（和工作組橋韌體）的不同版本遵循的IEEE 802.1X草案標準。

使用者端韌體 版本	草案8	草案10
4.13	x	-
4.16	x	-
4.23	x	-
4.25或更高版本	-	x
WGB340/350 8.58	x	-
WGB340/350 8.61	-	x

問題2

已使用RADIUS伺服器的MAC驗證。有幾個Aironet 1231G AP(從Cisco IOS®版本12.3(7)JA1到12.3(7)JA3的AP)存在使用者身份驗證問題。

如果您從較新版本的Cisco IOS升級到12.3(7)JA3，這是一個常見問題。

解決方案2

解決此問題的第一步是使用配置進行測試。請完成以下步驟：

1. 在SECURITY > Encryption Manager處刪除Encryption key。
2. 按一下「**None**」，然後「Apply」。
3. 轉到SSID Manager，選中SSID **SSID_Name**，然後選擇**<NO ADDITION>**。
4. 在Open Authentication選單中，向下滾動並按一下**Apply**。應用這些更改後，可以使用客戶端

介面卡進行測試。如果仍然失敗，即使沒有加密和身份驗證設定，最好將AP重置為預設值並從頭重新配置。

5. 完成以下步驟，將AP重設為預設值：選擇**System Software > System Configuration**。按一下「**Reset to Defaults**（IP除外）」。重新啟動後，您可以重新配置它，並用客戶端介面卡進行測試。
6. 檢查Advanced Security下的MAC Authentication設定並將其設定為Server only。請完成以下步驟：選擇**Security > Advanced Security > MAC Authentication**。按一下「**Server**」。按一下**Save**設定。

相關資訊

- 無線LAN技術提示
- 技術支援與文件 - Cisco Systems