

排除Catalyst 9800網狀Wifi故障

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[1.範圍和適用性](#)

[2.客戶報告的常見症狀](#)

[1.網狀AP顯示WLC上已連線，但沒有客戶端連線](#)

[2. RAP-MAP連結](#)

[3.客戶端連線症狀](#)

[3.高概率根本原因儲存桶](#)

[4.強制性設計和配置驗證](#)

[4.1網狀回傳 \(嚴重\)](#)

[4.2天線和安裝](#)

[5.射頻和WLAN最佳實踐](#)

[5.1資料速率 \(強烈建議\)](#)

[5.2電源和RRM](#)

[客戶端連線問題故障排除](#)

[問題描述](#)

[觀察到的症狀](#)

[網格部署中客戶端連線問題的關鍵影響因素](#)

[如何識別出發生的問題 \(網狀驗證卡住\)](#)

[強制日誌收集 \(在故障期間\)](#)

[疑難排解MAP-RAP斷開問題](#)

[問題描述](#)

[症狀](#)

[如何識別發生的問題 \(RAP-MAP連線問題\)](#)

[強制日誌收集 \(在故障期間\)](#)

[結論](#)

簡介

本文描述對9800網狀環境進行故障排除的不同方法。

必要條件

需求

思科建議您瞭解無線控制器和網狀網部署知識。

1.範圍和適用性

適用於：這些問題在海港和採礦環境中已經發生。

* Catalyst 9800-L/9800-CL/9800-40無線LAN控制器

*室外網狀部署(RAP-MAP)

*雙頻(2.4 GHz/5 GHz)WLAN

*具有以下功能的環境：

*長距離網狀鏈路

*高射頻噪音/工業區域 (埠、終端、碼場)

2.客戶報告的常見症狀

網狀/AP症狀

1.網狀AP顯示WLC上已連線，但沒有客戶端連線

*無客戶端或上游流量

* Ping失敗，直到AP重新啟動。

2. RAP-MAP連結

*間歇性擺動。

*意外漫遊到另一個RAP/MAP。

*網狀AP與WLC斷開連線並需要手動重新啟動。

3. 客戶端連線症狀

*客戶端無限期停滯在「身份驗證」狀態。

*客戶端在AP之間漫遊，但仍未進行身份驗證。

*客戶端僅在以下時間連線：

*強制從WLC或AP重新引導中刪除

* 2.4 GHz上的頻繁客戶端丟棄

3. 高概率根本原因儲存桶

類別	典型問題
RF/設計	通道重疊、寬通道寬度、天線失準
網狀控制	父選擇不穩定性，弱回程SNR
組態	混合資料速率、多個BGN、靜態電源
軟體	wncd進程停止，客戶端狀態過時
擴展/載入	身份驗證呼叫過多，EAPOL計時器不匹配

4. 強制性設計和配置驗證

4.1 網狀回傳 (嚴重)

根AP(RAP)

- 通道寬度：僅20 MHz
- 跨RAP的非重疊通道
- 相同橋接器群組名稱(BGN)
- 靜態通道分配
- MAP視線

避免

- 在RAP上混合20/40 MHz
- 所有RAP上的通道相同
- 同一區域中的多個BGN

4.2天線和安裝

- 5 GHz全向天線：
- 垂直於地面安裝
- 網狀回傳專用的5 GHz無線電
- 優選用於長距離MAP的定向天線
- 消除障礙物 (金屬、起重機、容器)

5.射頻和WLAN最佳實踐

5.1資料速率 (強烈建議)

2.4 GHz

必填:12 Mbps

禁用：6,9 Mbps

其他：支援

5 GHz

必填:12 Mbps

禁用：6,9 Mbps

其他：支援

影響：

- 減少粘滯客戶端
- 提高漫遊和身份驗證穩定性

5.2 電源和RRM

- 避免AP級靜態TX功率
- 使用全域性RRM
- 最小TX功率：
- 2.4 GHz: ≥ 12 dBm

避免在生產時間進行大規模DCA更改

客戶端連線問題故障排除

問題描述

在網狀連線區域中：

- 客戶端成功與MAP關聯。
- 身份驗證開始，但從未完成。
- 使用者端在WLC上仍處於驗證狀態。
- 客戶端可以在進行身份驗證時在AP之間漫遊。
- 身份驗證僅在以下時間後成功：手動從WLC移除使用者端，或重新啟動MAP。

此行為是間歇性的，難以按需複製，不屬於正常身份驗證流程。

觀察到的症狀

- Show wireless client summary顯示客戶端停滯在「Authentication (身份驗證)」中。
- 客戶端生成重複的身份驗證嘗試。

- 未發現顯式身份驗證失敗或拒絕。
- 即使在發生多個漫遊事件後，客戶端仍保持停滯狀態。
- 主要在客戶端通過MAP連線時觀察到的問題。
- 在操作負載期間發出頻率增加。

網格部署中客戶端連線問題的關鍵影響因素

1.網狀回程不穩定性

- RAP和MAP之間的RSSI/SNR波動。
- MAP在身份驗證期間重新選擇父項。
- 網狀網路延遲導致EAP超時或重新傳輸。
- MAP臨時轉發流量，但不一致

影響:

- 身份驗證狀態機未完成。
- 客戶端在身份驗證中仍然停滯不前。

2.身份驗證期間的漫遊

- 客戶端在MAP之間或MAP和RAP之間漫遊。
- 身份驗證上下文未完全傳輸。
- 客戶端繼續漫遊，同時保持身份驗證狀態

影響:

- 身份驗證重複重新啟動。
- 客戶端永遠不會達到RUN狀態。

3.客戶端服務無線電(2.4 GHz)的資料速率較低

- 必須啟用6或9 Mbps。
- 過多的重試次數和通話時間消耗。
- 身份驗證幀延遲或丟棄。

影響:

- EAP交換變得不可靠。

- 身份驗證顯示掛起，沒有顯示故障。

4. 共用相同RF限制的網狀回傳和客戶端流量

- 網狀鏈路利用率高。
- 客戶端身份驗證流量與：
 - 資料流量
 - 控制流量
 - 驗證資料包較小，但具有時間敏感性。

影響：

- 身份驗證僅在重試或重置後完成

如何識別出發生的問題（網狀驗證卡住）

當網狀部署中同時觀察到所有上述情況時，問題會視為已解決：

客戶端行為指示器

- 客戶端保持身份驗證狀態的時間超過60-120秒。
- 客戶端不會自動轉換到RUN狀態。
- 客戶端僅在以下時間後成功連線：
 - 強制從WLC移除使用者端
 - 網狀AP重新啟動
 - 客戶端可以在MAP或RAP之間漫遊，同時保持身份驗證狀態。

WLC指標

指令：

顯示無線客戶端摘要

指標：

- 相同的客戶端MAC持續列在Authenticating（身份驗證）下。
- 客戶端條目不會自然過期。

如果客戶端已連線超過10分鐘，請簽入此命令：

show wireless client mac <client-mac>

網狀特定指示器

命令:

show ap mesh parent

show ap mesh link

指標 :

- 客戶端身份驗證期間的父項更改或不穩定性
- 波動的RSSI/SNR值
- 網狀回傳的重試次數或丟包率增加

強制日誌收集 (在故障期間)

當客戶端停滯在「身份驗證」狀態時，必須收集日誌。
重新啟動或客戶端刪除後收集的日誌對根本原因沒有用。

1. 控制器基線日誌

show tech wireless

show clock

目的:

- 擷取整個WLC狀態
- 跨日誌關聯時間戳

2. 客戶端狀態驗證日誌

顯示無線客戶端摘要

顯示無線客戶端摘要 | 包括身份驗證

show wireless client mac <client-mac>

3. WNCN內部日誌 (嚴重)

啟用詳細跟蹤：

```
set platform software trace wncd chassis active r0 all verbose
```

收集日誌 (最近30分鐘)：

```
show logging process wncd internal last 30分鐘
```

客戶端特定的過濾日誌：

```
show logging process wncd start last 30 minutes filter mac <client-mac> to-file  
bootflash:wncd_client.log
```

4.無線電活動(RA)跟蹤 — 每客戶端

在 GUI 上：

- 監控>無線>客戶端>故障排除
- 新增受影響的客戶端MAC。
- 啟動RA跟蹤。
- 重現問題。

5.網狀回程驗證日誌

```
show ap mesh link
```

```
show ap mesh parent
```

```
show ap mesh statistics
```

6.可選 (如果可用) — 身份驗證伺服器日誌

- 受影響客戶端的RADIUS身份驗證日誌
- 身份驗證延遲和重新傳輸

疑難排解MAP-RAP斷開問題

問題描述

在多個IW9167 MAP之間間歇性和不可預測地丟失網狀回傳連線，導致AP中斷、網狀身份驗證失敗、無法訪問的AP和客戶端流量黑洞。恢復通常需要AP重新啟動或WLC干預。

症狀

- MAP與父RAP取消關聯
- MAP關聯，但無法傳遞流量
- 無法從WLC、RAP和網關訪問MAP
- 已關聯但沒有上游可達性的客戶端
- 父級MAP或RAP漫遊時的級聯中斷

錯誤消息/指示符

ERROR-MeshSecurity:計時器已過期

CRIT-Mesh安全：網格安全無法與父節點進行身份驗證

CRIT-MeshAwppAdj:作為父項刪除

mlme_ext_vap_down:VAP(mon1)關閉

ieee80211_ucfg_mesh_add_client():找不到節點

DTLS關閉警報

CAPWAP心跳超時

如何識別發生的問題 (RAP-MAP連線問題)

1.網狀控制平面看起來正常

上述命令可能顯示為正常，且無法單獨用於驗證流量轉發：

show ap summary

show wireless mesh ap tree

show capwap client rcb

這些命令僅確認控制平面狀態。

網狀資料平面故障識別

MAP：顯示網狀狀態

這是網狀轉發運行狀況的主要指標。

正常輸出

父AP MAC:24:D7:9C:04:79:B1

網狀鏈路狀態：UP

轉發狀態：已啟用

流量黑洞輸出

父AP MAC:24:D7:9C:04:79:B1

網狀鏈路狀態：UP

轉發狀態：已停用

解釋：

存在網狀鄰接關係，但AP沒有轉發流量。

2. MAP：顯示網格歷史記錄

不重新載入AP的重複父級轉換表示轉發狀態不穩定：

CRIT-MeshAwppAdj:作為父項刪除

CRIT-MeshAwppAdj:設定為父級

CRIT-MeshAwppAdj:作為父項刪除

這種模式通常會使AP處於非轉發狀態。

3. MAP系統日誌症狀

在流量黑屏期間觀察到的常見系統日誌消息：

ieee80211_ucfg_mesh_add_client():找不到節點

CLSM:由於空鍵而跳過鍵程式設計

這些指示網狀安全上下文不完整，從而阻止了加密流量轉發。

4. WLC show ap name <AP> mesh path

此指令可確認控制器對資料路徑的檢視。

健康

路徑狀態：Active (作用中)

資料路徑：完成

流量黑洞

路徑狀態：Active (作用中)

資料路徑：未完成

解釋：

存在網狀路徑，但未建立資料轉發。

5. ARP相關指標

在VLAN SVI位於WLC上的部署中：

- 客戶端和AP存在ARP條目。
- 客戶端流量失敗。
- 清除ARP會立即恢復連線。

此行為可確認資料平面轉發故障，而不是RF或CAPWAP不穩定。

強制日誌收集（在故障期間）

第0階段 — 強制準備（在問題發生之前）

重要資訊：重新啟動後收集的日誌對網格RCA不足。

在RAP和MAP上啟用持續調試

關於RAP

終端長度0

調試網狀事件

debug mesh adjacency child

調試網狀鄰接資料包

debug mesh adjacency channel

debug map security

debug mesh forwarding packet

偵錯 capwap 用戶端事件

debug capwap client error

終端監視器

在地圖上

終端長度0

調試網狀事件

debug mesh adjacency parent

調試網狀鄰接資料包

debug mesh adjacency channel

debug map security

偵錯 capwap 用戶端事件

debug capwap client error

終端監視器

保持調試處於啟用狀態，直到問題重新出現。

第1階段 — 問題期間的日誌收集 (嚴重)

收集日誌之前不要重新啟動AP

來自受影響對映的日誌 (當問題發生時立即)

顯示網狀狀態

顯示最早的網格歷史記錄

顯示網格歷史記錄

show flash syslogs

more syslog <date>

來自RAP的日誌 (以前父項和新父項)

顯示最早的網格歷史記錄

顯示網狀狀態

來自WLC的日誌 (發生故障時)

show wireless mesh ap tree

show wireless mesh neighbor

show ap name <AP-NAME> mesh path

show ap name <AP-NAME> config general

show tech-support wireless

可選 (高值) :

show logging process wncd start last 2 days level verbose

使用者端與流量關聯 (建議)

在故障期間運行連續ping:

ping -t <gateway-ip>

第2階段 — RF和配置驗證 (捕獲後)

RF驗證(WLC)

show ap dot11 5ghz summary

show ap dot11 24ghz summary

```
show ap name <AP> config dot11 5ghz
```

```
show ap name <AP> config dot11 24ghz
```

ARP/轉發驗證 (如果流量黑洞)

如果SVI託管在WLC上 :

```
clear arp-cache
```

如果流量恢→到ARP處理是起作用的因素。

第3階段 — 穩定措施 (已驗證)

網狀拓撲控制

- 在MAP上啟用Block Child (如果適用)。
- 強制MAP連線到最近的RAP。
- 減少網狀跳數。

RF最佳化

- 降低RAP傳輸功率。
- 鎖定5 GHz回程通道。
- 標準化2.4 GHz通道(1/6/11)。

上述所有問題在網狀部署中都是間歇性且難以獲得，因此部署快速指令碼捕獲日誌可以更快地獲得解決方案。

以下是可以在WLC上執行以解決使用者端驗證問題的EEM指令碼範例：

完整EEM指令碼 (通過WLC CLI應用)

```
::cisco::eem::event_register_timer watchdog time 900 maxrun 240
名稱空間匯入 : :cisco::eem::*
名稱空間匯入 : :cisco::lib::*
# -----
# Proc:將WLC時間串轉換為秒
#支援 : 「X days Xh:Xm:Xs」、 「Xh:Xm:Xs」、 「Xm:Xs」、 「Xs」
# -----
proc time_to_seconds {time_str} {
```

```

set total 0
如果{[regexp {[0-9]+\s+天 ?\s+([0-9]+\s+h:([0-9]+\s+m:([0-9]+\s+s) $time_str -> d h m s]} {
set total [expr {$d*86400 + $h*3600 + $m*60 + $s}]
} elseif {[regexp {[0-9]+\s+h:([0-9]+\s+m:([0-9]+\s+s) $time_str -> h m s]} {
set total [expr {$h*3600 + $m*60 + $s}]
} elseif {[regexp {[0-9]+\s+m:([0-9]+\s+s) $time_str -> m s]} {
set total [expr {$m*60 + $s}]
} elseif {[regexp {[0-9]+\s+s) $time_str -> s]} {
設定總計$s
}
}
返回$total
}
# -----
# Proc:跟蹤日誌收集例項總數 ( 最多2個 )
# -----
proc get_log_count {} {
如果{[檔案存在/bootflash/auth_log_count.txt]} {
set fd [open /bootflash/auth_log_count.txt r]
set count [讀$fd]
關閉$fd
返回$count
} else {
返回0
}
}
proc set_log_count {count} {
set fd [open /bootflash/auth_log_count.txt w]
放置$fd $count
關閉$fd
}
# -----
#主EEM執行
# -----
如果{[catch {cli_open}結果]} {
出口1
}
陣列集cli $result
set fd $cli(fd)
cli_exec $fd "enable"
cli_exec $fd "terminal length 0"
cli_exec $fd "終端寬度0"
#獲取當前日誌收集計數
set log_count [get_log_count]
set max_log_instances 2
#拉出所有處於身份驗證狀態的客戶端
set summary [cli_exec $fd "show wireless client summary | include Authentication"]

```

```
設定行[分割$summary "\n"]
foreach line $lines {
#匹配MAC格式xxxx.xxxx.xxxx
如果{{regex {{([0-9a-fA-F]{4}\.){3}} $line -> mac}} {
set detail [cli_exec $fd "show wireless client mac-address $mac detail"]

#提取「Connected For」時間字串
如果{{regex {Connected For[:space:]*[:space:]*(.+)} $detail -> conn_time}} {
set seconds [time_to_seconds $conn_time]

#檢查是否卡住>15分鐘 ( 900秒 )
如果{$seconds > 900} {
action_syslog消息"EEM:客戶端$mac在$conn_time(>$seconds)的身份驗證中停滯"

#僅在低於最大例項限制時收集日誌
如果{$log_count < $max_log_instances} {
action_syslog消息"EEM:正在收集WLC +客戶端日誌 ( 例項[expr {$log_count +
1}]/$max_log_instances ) "
set log_file "/bootflash/auth_stuck_eem.log"

set fd_log [open $log_file a]
```

每個客戶端日誌數

```
放置$fd_log "\n=== [時鐘格式[時鐘秒]] |客戶端$mac |卡住$conn_time ==="
```

```
放置$fd_log "\n — 客戶端詳細資訊 — "
```

```
放置$fd_log $detail
```

```
放置$fd_log "\n — 客戶端摘要 — "
```

```
放置$fd_log [cli_exec $fd "show wireless client summary | include $mac"]
```

WLC範圍的日誌數量

```
放置$fd_log "\n— WLC WNCD日誌(30m)—"
```

```
放置$fd_log [cli_exec $fd "show logging process wncd start last 30 minutes"]
```

```
放置$fd_log "\n— WLC Show Tech Wireless —"
```

```
放入$fd_log [cli_exec $fd "show tech wireless"]
```

關閉\$fd_log

```
set log_count [expr {$log_count + 1}]
```

```
set_log_count $log_count
```

```
} else {
```

```
action_syslog消息"EEM:已達到最大日誌例項數($max_log_instances)。正在跳過日誌收集。"
```

```
}
```

#始終取消對停滯的客戶端的身分驗證

```
cli_exec $fd "wireless client mac-address $mac deauthenticate"
```

```
action_syslog消息"EEM:已取消身分驗證的客戶端$mac"
```

```
}  
}  
}  
}  
cli_close $fd  
退出0  
—
```

####指令碼的主要功能

1. **15分鐘間隔**：監視程式計時器設定為請求的900秒（15分鐘）
2. **停滯閾**：僅客戶端上的觸發器的停滯時間超過15分鐘（900秒）
3. **日誌限制**：收集WLC +每個客戶端日誌的**最多2個例項**然後跳過日誌收集（仍取消客戶端身份驗證）
4. **WLC日誌集**：包括：
 - 每客戶端詳細資訊/摘要
 - WNCD進程日誌（30分鐘視窗）
 - 全「show tech wireless」
5. **持久計數器**：通過「/bootflash/auth_log_count.txt」跨運行EEM指令碼跟蹤日誌例項

部署與驗證

1. 將指令碼應用於WLC：

```
WLC# configure terminal
```

```
WLC(config)#事件管理器小程序AuthStuckHandler
```

```
WLC(config-applet)# event timer watchdog time 900
```

```
WLC(config-applet)# action 1 cli命令「sh bootflash:auth_stack_eem.tcl」
```

```
WLC(config-applet)# end
```

（或將完整Tcl指令碼直接貼上到WLC EEM配置中。）

2. 檢查EEM註冊：

```
WLC# show event manager policy registered
```

3. 檢索收集的日誌：

```
WLC# copy bootflash:auth_stuck_eem.log ftp:
```

```
WLC# copy bootflash:auth_log_count.txt ftp:
```

4. 重置日誌計數器以重新啟用收集（如果需要）：

```
WLC# delete bootflash:auth_log_count.txt
```

結論

本文整合經驗證的TAC方法和真實案例研究，以解決最普遍的Catalyst 9800網狀WiFi問題：回傳不穩定、客戶端停滯在「身份驗證」狀態，以及流量無法傳輸。

其核心要點是，90%報告的網狀故障不是孤立的硬體或客戶端故障，而是控制平面和資料平面狀態不匹配、網狀拓撲不穩定或射頻設計欠佳等症狀。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。