排除Catalyst 9800网状Wifi故障

目录

简介

本文档介绍对9800网状网络环境进行故障排除的不同方法。

先决条件

要求

思科建议您了解无线控制器和网状网部署知识。

1.范围和适用性

适用于：这些问题是发生在海港和采矿环境的。

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

*室外网状部署(RAP-MAP)

*双频(2.4 GHz/5 GHz)无线局域网

*具有以下功能的环境：

*长距离网状链路

*高射频噪音/工业区域（端口、终端、码场）

2.客户报告的常见症状

网状/AP症状

1.网状AP显示在WLC上已连接，但没有客户端连接

*无客户端或上游流量

*在AP重新启动之前，Ping失败。

2. RAP-MAP链路

*断断续续地摆动。

*MAP意外漫游到另一个RAP/MAP。

*网状AP从WLC断开并需要手动重新启动。

3.客户端连通性症状

*客户端无限期停滞在“身份验证”状态。

*客户端在AP之间漫游，但仍未进行身份验证。

*客户端仅在以下时间连接：

*强制从WLC或AP重新启动中删除

*在2.4 GHz频段频繁发生客户端丢弃

3.高概率根本原因存储桶

分类	典型问题
RF/设计	信道重叠、宽信道宽度、天线未对齐
网状控制	父路由选择不稳定，回传SNR较弱
配置	混合数据速率、多个BGN、静态电源
软件	wncd进程停止，客户端状态过时
扩展/加载	超额身份验证呼叫，EAPOL计时器不匹配

4.强制性设计和配置验证

4.1网状回传（严重）

根AP(RAP)

- 信道宽度：仅20 MHz
- 跨RAP的非重叠信道
- 相同的网桥组名称(BGN)
- 静态信道分配
- MAP视线

避免

- 在RAP上混合20/40 MHz
- 所有RAP上的同一信道
- 同一区域内有多个BGN

4.2天线和安装

- 5 GHz全向天线：
- 垂直于地面安装
- 用于网状回传的专用5 GHz无线电
- 长距离MAP首选的定向天线
- 消除障碍物（金属、起重机、容器）

5.射频和无线局域网最佳实践

5.1数据速率（强烈推荐）

2.4 GHz

必需:12 Mbps

禁用:6、9 Mbps

其他:受支持

5 GHz

必需:12 Mbps

禁用:6、9 Mbps

其他:受支持

影响:

- 减少粘性客户端
- 提高漫游和身份验证稳定性

5.2电源和RRM

- 避免AP级静态TX功率
- 使用全局RRM
- 最小发射功率：
- 2.4 GHz:≥ 12 dBm

避免在生产时间进行大规模DCA更改

排除客户端连接故障

问题说明

在网状连接区域中：

- 客户端成功与MAP关联。
- 身份验证开始，但从未完成。
- 客户端在WLC上保持身份验证状态。
- 客户端可以在进行身份验证的同时在AP之间漫游。
- 身份验证仅在以下时间后成功：从WLC中手动删除客户端，或者重新启动MAP。

此行为是间歇性的，难以按需复制，不属于正常身份验证流程的一部分。

观察到的症状

- Show wireless client summary显示客户端卡在身份验证中。
- 客户端生成重复的身份验证尝试。

- 未发现显式身份验证失败或拒绝。
- 客户端即使在发生多个漫游事件后仍保持停滞状态。
- 主要在客户端通过MAP连接时观察到的问题。
- 在运行负载期间发出频率增加。

影响客户端连接问题的网状网部署的主要因素

1.网状回传不稳定性

- 在RAP和MAP之间波动RSSI/SNR。
- MAP在身份验证期间重新选择父节点。
- 网状网延迟导致EAP超时或重新传输。
- MAP临时转发流量，但不一致

影响:

- 身份验证状态机未完成。
- 客户端仍停滞在身份验证中。

2.身份验证期间的漫游

- 客户端在MAP之间或MAP与RAP之间漫游。
- 身份验证上下文未完全传输。
- 客户端继续漫游，同时保持身份验证状态

影响:

- 身份验证重复重新启动。
- 客户端无法到达RUN状态。

3.客户端服务无线电(2.4 GHz)的数据速率较低

- 必须启用6或9 Mbps。
- 重试次数和通话时间消耗过多。
- 身份验证帧延迟或丢弃。

影响:

- EAP交换在网状网中变得不可靠。

- 身份验证显示挂起，没有显式故障。

4.共享相同RF限制的网状回传和客户端流量

- 网状链路利用率高。
- 客户端身份验证流量与：
- 数据流量
- Control Traffic
- 身份验证数据包较小，但时间敏感。

影响:

- 身份验证仅在重试或重置后完成

如何确定问题是否命中（网状身份验证卡住）

当在网状部署中同时观察到所有上述条件时，问题会被视为已命中：

客户端行为指示器

- 客户端保持身份验证状态超过60-120秒。
- 客户端不会自动转换到RUN状态。
- 客户端仅在以下情况下成功连接：
- 从WLC强制删除客户端
- 网状AP重新启动
- 客户端可以在MAP或RAP之间漫游，同时保持身份验证状态。

WLC指示灯

命令:

show wireless client summary

指标：

- 相同的客户端MAC持续列在Authenticating下。
- 客户端条目不会自然过期。

如果客户端已连接10分钟以上，请签入以下命令：

show wireless client mac <client-mac>

网状网特定指示器

命令：

show ap mesh parent

show ap mesh link

指标：

- 客户端身份验证期间的父项更改或不稳定性
- 波动的RSSI/SNR值
- 网状回传中的重试次数或丢包率增加

强制日志收集（在故障期间）

当客户端停滞在“身份验证”状态时，必须收集日志。
重新启动或客户端删除后收集的日志对根本原因没有用。

1.控制器基线日志

show tech wireless

show clock

目的:

- 捕获整体WLC状态
- 跨日志关联时间戳

2.客户端状态验证日志

show wireless client summary

show wireless client summary |包括身份验证

show wireless client mac <client-mac>

3. WNCD内部日志（严重）

启用详细跟踪：

set platform software trace wncd chassis active r0 all verbose

收集日志（最近30分钟）：

show logging process wncd internal last 30分钟

客户端特定的过滤日志：

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

4.无线电活动(RA)跟踪 — 每客户端

从 GUI：

- 监控(Monitor)>无线(Wireless)>客户端(Client)>故障排除(Troubleshooting)
- 添加受影响的客户端MAC。
- 启动RA跟踪。
- 重现问题.

5.网状回传验证日志

show ap mesh link

show ap mesh parent

show ap mesh statistics

6.可选（如果可用）— 身份验证服务器日志

- 受影响客户端的RADIUS身份验证日志
- 身份验证延迟和重传

排除MAP-RAP断开问题

问题说明

在多个IW9167 MAP间断断续续且不可预测的网状回传连接丢失，导致AP断开、网状身份验证失败、AP不可达以及客户端流量黑洞。恢复通常需要AP重新启动或WLC干预。

症状

- MAP与父RAP取消关联
- MAP关联，但无法传递流量
- 无法从WLC、RAP和网关访问MAP
- 客户端已关联，但无上游可达性
- 父级MAP或RAP漫游时的级联故障

错误消息/指示符

ERROR-MeshSecurity:计时器已过期

CRIT-Mesh安全：网状安全无法通过父交换机进行身份验证

CRIT-MeshAwppAdj:作为父项删除

mlme_ext_vap_down:VAP(mon1)关闭

ieee80211_ucfg_mesh_add_client():找不到节点

DTLS关闭警报

CAPWAP心跳超时

如何确定问题已命中（RAP-MAP连接问题）

1.网状控制平面看起来正常

上述命令可能看起来正常，不能单独用于验证流量转发：

show ap summary

show wireless mesh ap tree

show capwap client rcb

这些命令仅确认控制平面状态。

确定网状数据平面故障

MAP：显示网状状态

这是网状转发运行状况的主要指标。

正常输出

父AP MAC:24:D7:9C:04:79:B1

网状链路状态： UP

转发状态：启用

流量黑洞输出

父AP MAC:24:D7:9C:04:79:B1

网状链路状态： UP

转发状态：禁用

解释：
存在网状邻接关系，但AP不转发流量。

2. MAP：显示网状历史记录

如果父交换机重复转换而没有AP重新加载，则表明转发状态不稳定：

CRIT-MeshAwppAdj:作为父项删除

CRIT-MeshAwppAdj:设置为父项

CRIT-MeshAwppAdj:作为父项删除

此模式通常会使AP处于非转发状态。

3. MAP系统日志症状

在流量黑洞期间观察到的常见系统日志消息：

ieee80211_ucfg_mesh_add_client():找不到节点

CLSM:由于null键而跳过键编程

这表明网状安全情景不完整，导致加密流量无法转发。

4. WLC show ap name <AP> mesh path

此命令可确认控制器的数据路径视图。

正常

路径状态：主用

数据路径:完成

流量黑洞

路径状态：主用

数据路径: Incomplete

解释：
存在网状路径，但未建立数据转发。

5.与ARP相关的指示灯

在VLAN SVI驻留在WLC上的部署中：

- 客户端和AP存在ARP条目。
- 客户端流量失败。
- 清除ARP会立即恢复连接。

此行为确认数据平面转发故障，而不是RF或CAPWAP不稳定。

强制日志收集（在故障期间）

第0阶段 — 强制准备（在问题发生之前）

重要信息：重新启动后收集的日志对网格RCA不足。

在RAP和MAP上启用持续调试

在RAP上

terminal length 0

debug map events

debug mesh adjacency child

debug mesh adjacency packet

debug mesh adjacency channel

debug mesh security

debug mesh forwarding packet

debug capwap client events

debug capwap client error

terminal monitor

在地图上

terminal length 0

debug map events

debug mesh adjacency parent

debug mesh adjacency packet

debug mesh adjacency channel

debug mesh security

debug capwap client events

debug capwap client error

terminal monitor

保持调试处于启用状态，直到问题再次出现。

第1阶段 — 问题期间的日志收集（严重）

收集日志前不要重新启动AP

来自受影响映射的日志（发生问题时立即执行）

show mesh status

显示最早的网状历史记录

show mesh history

show flash syslogs

more syslog <date>

来自RAP的日志（上一个和新的父项）

显示最早的网状历史记录

show mesh status

来自WLC的日志（发生故障时）

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

可选（高值）：

show logging process wncd start last 2 days level verbose

客户端与流量关联（推荐）

在出现故障时运行连续ping:

ping -t <网关 — ip>

第2阶段 — RF和配置验证（捕获后）

RF验证(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/转发验证（如果流量黑洞）

如果WLC上托管SVI:

clear arp-cache

如果流量恢→到ARP处理是促成因素。

第3阶段 — 稳定措施（已验证）

网状拓扑控制

- 在MAP上启用Block Child（如果适用）。
- 强制MAP连接到最近的RAP。
- 减少网状网跳数。

射频优化

- 降低RAP传输功率。
- 锁定5 GHz回传信道。
- 标准化2.4 GHz信道(1/6/11)。

在网状网部署中，上述所有问题都非常间歇性且难以获得，因此部署快速脚本捕获日志可以更快地获得解决方案。

以下是可以在WLC上运行的示例EEM脚本，用于解决客户端身份验证问题：

完整EEM脚本（通过WLC CLI应用）

```
::cisco::eem::event_register_timer watchdog time 900 maxrun 240
命名空间导入：:cisco::eem::*
命名空间导入：:cisco::lib::*
# ---------------------------
处理器数量：将WLC时间字符串转换为秒
#支持：“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+days?\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} $time_str -> s]} {
设置总计$s
}
返回$total
}
# ----------------------------
处理器数量：跟踪日志收集实例总数（最多2个）
# ----------------------------
proc get_log_count {} {
如果{[文件存在/bootflash/auth_log_count.txt]} {
set fd [open /bootflash/auth_log_count.txt r]
set count [读取$fd]
关闭$fd
返回$count
} else {
返回0
}
}
proc set_log_count {count} {
set fd [open /bootflash/auth_log_count.txt w]
置入$fd $count
关闭$fd
}
# ----------------------------
主EEM执行次数
# ----------------------------
如果{[catch {cli_open}结果]} {
退出1
}
阵列集cli $result
set fd $cli(fd)
cli_exec $fd "enable"
cli_exec $fd "terminal length 0"
cli_exec $fd "terminal width 0"
#获取当前日志收集计数
set log_count [get_log_count]
set max_log_instances 2
#拉出所有处于身份验证状态的客户端
set summary [cli_exec $fd "show wireless client summary | Include Authenticating"]
```

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

#提取“Connected For”时间字符串
如果{[regexp {Connected For[[:space:]]*:[[:space:]]*(.+)} $detail -> conn_time]} {
set seconds [time_to_seconds $conn_time]

#检查是否卡住>15分钟（900秒）
如果{$seconds > 900} {
action_syslog消息"EEM:客户端$mac在$conn_time(>$seconds)的身份验证中卡住"

#仅在低于最大实例限制时收集日志
如果{$log_count < $max_log_instances} {
action_syslog消息"EEM:收集WLC +客户端日志（实例[expr {$log_count +
1}]/$max_log_instances）"
set log_file "/bootflash/auth_stuck_eem.log"


set fd_log [open $log_file a]

每个客户端日志数量
置入$fd_log "\n=== [时钟格式[时钟秒数]] |客户端$mac |卡住$conn_time ==="
置入$fd_log "\n— Client Detail —"
置入$fd_log $detail
置入$fd_log "\n— Client Summary —"
放置$fd_log [cli_exec $fd "show wireless client summary | include $mac"]

# WLC范围的日志
放置$fd_log "\n— WLC WNCD日志(30m)—"
放置$fd_log [cli_exec $fd "show logging process wncd start last 30 minutes"]
置入$fd_log "\n— WLC Show Tech Wireless —"
放置$fd_log [cli_exec $fd "show tech wireless"]

关闭$fd_log
set log_count [expr {$log_count + 1}]
set_log_count $log_count
} else {
action_syslog消息"EEM:已达到最大日志实例数($max_log_instances)。正在跳过日志收集。"
}

#始终取消对滞留客户端的身份验证
cli_exec $fd "wireless client mac-address $mac deauthenticate"
action_syslog消息"EEM:已取消身份验证的客户端$mac”
```

```
}
}
}
}
cli_close $fd
退出0
```
—
####脚本的主要功能
1.**15分钟间隔**:监视器计时器设置为请求的900秒（15分钟）
2.**滞留阈值**:仅在客户端卡住超过15分钟（900秒）时触发
3.**日志限制**:收集WLC +每个客户端的日志，**最多2个实例总数**，然后跳过日志收集（仍然取消客户端身份验证）
4.**WLC日志集**:包括：
— 每客户端详细信息/摘要
- WNCD进程日志（30分钟窗口）
— 全“show tech wireless”
5.**持久计数器**:跨EEM脚本运行，通过“/bootflash/auth_log_count.txt”跟踪日志实例

部署和验证
1.将脚本应用于WLC:
```
WLC#配置终端
WLC(config)# event manager applet AuthStuckHandler
WLC(config-applet)# event timer watchdog time 900
WLC(config-applet)# action 1 cli命令“sh bootflash:auth_stuck_eem.tcl”
WLC(config-applet)# end
```
（或将完整的Tcl脚本直接粘贴到WLC EEM配置中。）

2.检查EEM注册：
```
WLC# show event manager policy registered
```

3.检索收集的日志：
```
WLC# copy bootflash:auth_stuck_eem.log ftp:
WLC# copy bootflash:auth_log_count.txt ftp:
```

4.重置日志计数器以重新启用收集（如果需要）：
```
WLC# delete bootflash:auth_log_count.txt
```

结论

本文档整合了经过验证的TAC方法和实际案例研究，以解决最普遍的Catalyst 9800网状WiFi问题：回传不稳定、客户端停滞在“身份验证”状态，且流量无法传输。

核心要点是，90%报告的网状故障不是孤立的硬件或客户端故障，而是控制平面和数据平面状态不匹配、网状拓扑不稳定或射频设计欠佳等症状。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。