Catalyst 9800 Mesh Wifi 문제 해결

목차

소개

이 문서에서는 9800 Mesh 환경의 문제를 해결하는 여러 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Wireless Controller에 대한 지식과 메시 구축 지식을 갖춘 것이 좋습니다.

1. 범위 및 적용 가능성

적용 대상: 에 대한 이러한 문제는 항구 및 채광 환경에 대해 발생했습니다.

* Catalyst 9800-L / 9800-CL / 9800-40 Wireless LAN Controller

* 실외 메시 구축(RAP-MAP)

* 듀얼 밴드(2.4GHz/5GHz) WLAN

* 다음과 같은 환경:

  * 장거리 메시 링크

  * 높은 RF 노이즈/산업 영역(포트, 터미널, 야드)

2. 일반적인 고객이 보고한 증상

메시/AP 증상

1. 메시 AP가 WLC에 조인된 것을 표시하지만 클라이언트 연결은 표시되지 않음

  * 클라이언트 또는 업스트림 트래픽 없음

  * AP를 재부팅할 때까지 Ping이 실패합니다.

2. RAP-MAP 링크

  * 간헐적으로 플랩.

* MAP이 예기치 않게 다른 RAP/MAP으로 로밍합니다.

* 메시 AP는 WLC와의 연결을 끊고 수동 리부팅이 필요합니다.

3. 클라이언트 연결 증상

* 클라이언트가 인증 상태에서 무기한 중단되었습니다.

* 클라이언트가 AP를 통해 로밍하지만 인증되지 않은 상태로 유지됩니다.

* 클라이언트는 다음 이후에만 연결합니다.

* WLC 또는 AP 재부팅 시 강제 제거

* 2.4GHz에서 클라이언트가 자주 끊김

3. 고위험 근본 원인 버켓

카테고리	일반적인 문제
RF/설계	채널 오버랩, 넓은 채널 폭, 안테나 오정렬
메시 제어	상위 선택 불안정성, 약한 백홀 SNR
설정	혼합 데이터 속도, 다중 BGN, 정적 전력
소프트웨어	wncd 프로세스 중지, 오래된 클라이언트 상태
확장/로드	초과 인증 통화, EAPOL 타이머 불일치

4. 필수 설계 및 구성 검증

4.1 메시 백홀(중요)

루트 AP(RAP)

- 채널 폭: 20MHz 전용
- RAP 간에 겹치지 않는 채널
- BGN(Same Bridge Group Name)
- 정적 채널 할당
- 지도에 대한 가시선

회피

- RAP에서 20/40MHz 혼합
- 모든 RAP의 동일한 채널
- 동일한 영역의 여러 BGN

4.2 안테나 및 마운팅

- 5GHz 옴니 안테나:
- 지면에 수직으로 장착된 것
- 메시 백홀용 전용 5GHz 무선 장치
- 장거리 MAP에 선호하는 지향성 안테나
- 장애물 제거(금속, 크레인, 용기)

5. RF 및 WLAN 모범 사례

5.1 데이터 전송률(적극 권장)

2.4기가헤르츠

필수: 12Mbps

비활성화: 6, 9Mbps

기타: 지원

5GHz

필수: 12Mbps

비활성화: 6, 9Mbps

기타: 지원

영향:

- 고착된 클라이언트 감소
- 로밍 및 인증 안정성 향상

5.2 전원 및 RRM

- AP 레벨의 고정 TX 전력 방지
- 전역 RRM 사용
- 최소 TX 전력:
- 2.4GHz: ≥ 12dBm

생산 시간의 적극적인 DCA 변경 방지

클라이언트 연결 문제 해결

문제/장애 설명

메시 연결 영역:

- 클라이언트가 MAP에 연결되었습니다.
- 인증이 시작되지만 완료되지 않습니다.
- 클라이언트는 WLC에서 Authenticating(인증) 상태로 유지됩니다.
- 클라이언트는 계속 인증하는 동안 AP 간에 로밍할 수 있습니다.
- 다음 이후에만 인증 성공: 클라이언트가 WLC에서 수동으로 제거되거나 MAP가 재부팅됩니다.

이 동작은 간헐적이며 온디맨드 방식으로 재현하기가 어렵고 정상적인 인증 흐름의 일부가 아닙니다.

관찰된 증상

- Show wireless client summary(무선 클라이언트 요약 표시)는 인증에서 중단된 클라이언트를 표시합니다.
- 클라이언트는 반복적인 인증 시도를 생성합니다.
- 명시적 인증 실패 또는 거부가 표시되지 않습니다.
- 여러 로밍 이벤트가 발생해도 클라이언트는 정지된 상태로 유지됩니다.
- 주로 클라이언트가 MAP를 통해 연결될 때 발생하는 문제입니다.
- 운영 로드 중 문제 발생 빈도가 증가합니다.

클라이언트 연결 문제에 대한 메시 구축의 주요 기여 요인

1. 메시 백홀 불안정

- RAP와 MAP 간의 변동 RSSI/SNR
- MAP 인증 중에 상위 항목을 다시 선택합니다.
- 메시 지연으로 인해 EAP 시간 초과 또는 재전송이 발생했습니다.
- 트래픽을 일시적으로 전달하지만 일관되지 않은 MAP

영향:

- 인증 상태 컴퓨터가 완료되지 않았습니다.
- 클라이언트는 인증에서 계속 유지됩니다.

2. 인증 중 로밍

- 클라이언트는 MAP 간에 로밍하거나 MAP과 RAP 간에 로밍합니다.
- 인증 컨텍스트가 완전히 전송되지 않습니다.
- 클라이언트가 인증 상태로 남아 있는 동안 로밍을 계속합니다.

영향:

- 인증이 반복적으로 재시작됩니다.
- 클라이언트가 RUN 상태에 도달하지 않습니다.

3. 클라이언트 지원 무선 장치(2.4GHz)의 낮은 데이터 속도

- 필수 6 또는 9Mbps 활성화
- 과도한 재시도 및 통신 시간 소비입니다.
- 인증 프레임이 지연되거나 삭제되었습니다.

영향:

- EAP 교환은 메시를 통해 신뢰할 수 없게 됩니다.
- 명시적 오류 없이 인증이 중단된 것으로 나타납니다.

4. 메시 백홀 및 클라이언트 트래픽이 동일한 RF 제약 조건 공유

- 메시 링크에 대한 높은 사용률.
- 클라이언트 인증 트래픽은 다음과 경쟁합니다.
- 데이터 트래픽
- 제어 트래픽
- 인증 패킷은 작지만 시간에 민감합니다.

영향:

- 재시도 또는 재설정 후에만 인증이 완료됨

문제를 식별하는 방법 적중(메시 인증 고착)

메시 구축에서 언급된 모든 조건이 동시에 관찰되면 문제가 발생한 것으로 간주됩니다.

클라이언트 동작 표시기

- 클라이언트는 60-120초 이상 인증 상태로 유지됩니다.
- 클라이언트는 자동으로 RUN 상태로 전환되지 않습니다.
- 다음 이후에만 클라이언트가 성공적으로 연결됩니다.
- WLC에서 강제 클라이언트 제거
- 메시 AP 재부팅
- 클라이언트는 인증 상태를 유지하면서 MAP 또는 RAP 간에 로밍할 수 있습니다.

WLC 표시기

명령을 사용합니다:

무선 클라이언트 요약 표시

지표:

- 동일한 클라이언트 MAC가 Authenticating(인증) 아래에 지속적으로 나열됩니다.
- 클라이언트 항목이 자연적으로 만료되지 않습니다.

클라이언트가 10분 이상 연결되어 있는 경우 이 명령을 체크 인합니다.

show wireless client mac <client-mac>

메시별 표시기

명령:

ap 메시 상위 표시

ap 메시 링크 표시

지표:

- 클라이언트 인증 중 상위 변경 또는 불안정성
- 변동 RSSI/SNR 값
- 메시 백홀에서의 재시도 또는 패킷 손실 증가

필수 로그 수집(실패 기간 중)

클라이언트가 인증 상태에 있는 동안 로그를 수집해야 합니다.
재부팅 또는 클라이언트 삭제 후에 수집된 로그는 근본 원인에 유용하지 않습니다.

1. 컨트롤러 기준 로그

show tech wireless

시계 표시

목적:

- 전체 WLC 상태 캡처
- 로그 전반에 걸쳐 타임스탬프 상관관계 분석

2. 클라이언트 상태 검증 로그

무선 클라이언트 요약 표시

무선 클라이언트 요약 표시 | 인증 포함

show wireless client mac <client-mac>

3. WNCD 내부 로그(중요)

자세한 정보 추적 사용:

플랫폼 소프트웨어 추적 wwncd 섀시 활성 r0 모두 자세한 정보 표시

로그 수집(최근 30분):

show logging process wncd internal 지난 30분

클라이언트별 필터링된 로그:

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

4. RA(Radio Active) 추적 - 클라이언트당

GUI에서:

- Monitor(모니터링) > Wireless(무선) > Client(클라이언트) > Troubleshooting(문제 해결)
- 영향을 받는 클라이언트 MAC을 추가합니다.
- RA 추적을 시작합니다.
- 문제를 재현합니다.

5. 메시 백홀 검증 로그

ap 메시 링크 표시

ap 메시 상위 표시

ap 메시 통계 표시

6. 선택 사항(사용 가능한 경우) - 인증 서버 로그

- 영향을 받는 클라이언트에 대한 RADIUS 인증 로그
- 인증 지연 및 재전송

MAP-RAP 연결 끊기 문제 해결

문제/장애 설명

여러 IW9167 MAP에서 메시 백홀 연결이 간헐적으로 예기치 않게 손실되어 AP 연결 끊김, 메시 인증 실패, 연결할 수 없는 AP, 클라이언트 트래픽 블랙홀링이 발생합니다. 복구에는 AP 재부팅 또는 WLC 개입이 필요한 경우가 많습니다.

증상

- MAP가 상위 RAP와 연결 해제됨
- MAP가 연결되었지만 트래픽을 전달할 수 없음
- WLC, RAP 및 게이트웨이에서 연결할 수 없는 맵
- 연결된 클라이언트(업스트림 연결 불가)
- 상위 MAP 또는 RAP가 로밍할 때 연속 중단

오류 메시지/표시기

ERROR-Mesh보안: 타이머 만료

CRIT-Mesh보안: 메시 보안이 부모와 인증하지 못했습니다.

CRIT-MeshAwppAdj: 부모로 제거

mlme_ext_vap_down: VAP(mon1)가 다운되었습니다.

ieee80211_ucfg_mesh_add_client(): 노드를 찾을 수 없음

DTLS 닫기 알림

CAPWAP 하트비트 시간 초과

문제를 확인하는 방법(RAP-MAP 연결 문제)

1. 메시 컨트롤 플레인이 정상인 것 같습니다.

위에서 언급한 명령은 정상적으로 나타날 수 있으며 트래픽 전달을 검증하는 데 단독으로 사용할 수 없습니다.

ap 요약 표시

무선 메시 ap 트리 표시

show capwap client rcb

이 명령은 컨트롤 플레인 상태만 확인합니다.

메시 데이터 플레인 오류 식별

MAP: 메시 상태 표시

메시 전달 상태를 나타내는 기본 지표입니다.

정상 출력

상위 AP MAC: 24:D7:9C:04:79:B1

메시 링크 상태: 위로

전달 상태: 활성화됨

트래픽 블랙홀 출력

상위 AP MAC: 24:D7:9C:04:79:B1

메시 링크 상태: 위로

전달 상태: 비활성화됨

해석:
메시 인접성이 존재하지만 AP가 트래픽을 전달하지 않습니다.

2. 지도: 메시 기록 표시

AP 다시 로드 없이 상위 전환이 반복되면 전달 상태가 불안정함을 나타냅니다.

CRIT-MeshAwppAdj: 부모로 제거

CRIT-MeshAwppAdj: 부모로 설정

CRIT-MeshAwppAdj: 부모로 제거

이 패턴은 AP를 비포워딩 상태로 두는 경우가 많습니다.

3. MAP Syslog 증상

트래픽 블랙홀링 중에 관찰된 공통 syslog 메시지:

ieee80211_ucfg_mesh_add_client(): 노드를 찾을 수 없음

CLSM: Null 키로 인해 키 프로그래밍 건너뛰기

이는 메시 보안 컨텍스트가 불완전하여 암호화된 트래픽 포워딩이 불가능함을 나타냅니다.

4. WLC 표시 ap 이름 < AP > 메시 경로

이 명령은 데이터 경로에 대한 컨트롤러의 보기를 확인합니다.

정상

경로 상태: 활성

데이터 경로: 완료

트래픽 블랙홀링

경로 상태: 활성

데이터 경로: 미완료

해석:
메시 경로가 있지만 데이터 전달이 설정되지 않았습니다.

5. ARP 관련 지표

VLAN SVI가 WLC에 상주하는 구축의 경우

- ARP 항목은 클라이언트와 AP에 대해 존재합니다.
- 클라이언트 트래픽이 실패합니다.
- ARP를 지우면 연결이 즉시 복원됩니다.

이 동작은 RF 또는 CAPWAP 불안정성이 아니라 데이터 플레인 포워딩 실패를 확인합니다.

필수 로그 수집(실패 기간 중)

단계 0 - 필수 준비(문제 발생 전)

중요: 재부팅 후 수집된 로그는 메시 RCA에 충분하지 않습니다.

RAP 및 MAP에서 영구 디버깅 사용

RAP

터미널 길이 0

메시 이벤트 디버그

디버그 메시 인접성 하위

디버그 메시 인접 패킷

디버그 메시 인접 채널

메시 보안 디버그

메시 전달 패킷 디버그

debug capwap client events

디버그 capwap 클라이언트 오류

단말기 모니터

지도에서

터미널 길이 0

메시 이벤트 디버그

디버그 메시 인접성 상위

디버그 메시 인접 패킷

디버그 메시 인접 채널

메시 보안 디버그

debug capwap client events

디버그 capwap 클라이언트 오류

단말기 모니터

문제가 재현될 때까지 디버그를 활성화 상태로 둡니다.

1단계 - 문제 발생 시 로그 수집(중요)

로그를 수집하기 전에 AP를 재부팅하지 마십시오.

문제가 발생하면 즉시 영향을 받는 MAP의 로그

메시 상태 표시

가장 오래된 메시 기록 표시

메시 기록 표시

show flash syslogs

추가 syslog <date>

RAP의 로그(이전 및 새 상위)

가장 오래된 메시 기록 표시

메시 상태 표시

WLC에서 로그(오류 시)

무선 메시 ap 트리 표시

무선 메시 네이버 표시

show ap name <AP-NAME> 메시 경로

show ap name <AP-NAME> config general

show tech-support wireless

선택 사항(높은 값):

show logging process wncd start last 2 days level verbose

클라이언트 및 트래픽 상관관계(권장)

실패 기간 동안 연속 ping 실행:

ping -t <gateway-ip>

2단계 - RF 및 컨피그레이션 검증(캡처 후)

RF 검증(WLC)

ap dot11 5ghz 요약 표시

ap dot11 24ghz 요약 표시

show ap name <AP> config dot11 5ghz

show ap name <AP> config dot11 24ghz

ARP/포워딩 검증(트래픽 블랙홀링인 경우)

SVI가 WLC에서 호스팅되는 경우:

arp 캐시 지우기

트래픽이 복구되면 ARP →이 영향을 주는 요인입니다.

3단계 - 안정화 조치(검증됨)

메시 토폴로지 컨트롤

- 해당되는 경우 MAP에서 Block Child를 활성화합니다.
- MAP를 가장 가까운 RAP에 강제로 연결합니다.
- 메시 홉 수 감소.

RF 최적화

- RAP 전송 전력 감소
- 5GHz 백홀 채널 잠금.
- 2.4GHz 채널 표준화(1/6/11).

앞서 언급한 모든 문제는 메시 구축에서 매우 간헐적이기 때문에 로그를 캡처하기 위해 빠른 스크립트를 구축하면 더 빨리 해결할 수 있습니다.

다음은 클라이언트 인증 문제를 위해 WLC에서 실행할 수 있는 샘플 EEM 스크립트입니다.

전체 EEM 스크립트(WLC CLI를 통해 적용)
::cisco::eem::event_register_timer watchdog time 900 maxrun 240
네임스페이스 가져오기 ::cisco::eem::*
네임스페이스 가져오기::cisco::lib::*

```
# ----------------------------
# 프로시저: WLC 시간 문자열을 초로 변환
# 지원: "X일 Xh:Xm:Xs", "Xh:Xm:Xs", "Xm:Xs", "Xs"
# ----------------------------
proc time_to_seconds {time_str} {
집합 합계 0
if {[regexp {([0-9]+)\s+days?\s+([0-9]+)\s+h:([0-9]+)\s+m:([0-9]+)\s+s} $time_str -> d h m]} {
총 설정 [expr {$d*86400 + $h*3600 + $m*60 + $s}]
} elseif {[regexp {([0-9]+)\s+h:([0-9]+)\s+m:([0-9]+)\s+s} $time_str -> h m]} {
총 설정 [expr {$h*3600 + $m*60 + $s}]
} elseif {[regexp {([0-9]+)\s+m:([0-9]+)\s+s} $time_str -> m s]} {
총 설정 [expr {$m*60 + $s}]
} elseif {[regexp {([0-9]+)\s+s} $time_str -> s]} {
총 $s 설정
}
반환 총계
}
# ----------------------------
# 프로시저: 총 로그 수집 인스턴스 추적(최대 2개)
# ----------------------------
proc get_log_count {}
{[file exists /bootflash/auth_log_count.txt]} {
set fd [open /bootflash/auth_log_count.txt r]
set count [읽기 $fd]
닫기 $fd
반환 $count
} 또는 {
반환 0
}
}
proc set_log_count {count} {
set fd [open /bootflash/auth_log_count.txt w]
$fd $count 입력
닫기 $fd
}
# ----------------------------
# 기본 EEM 실행
# ----------------------------
경우 {[catch {cli_open} result]}
출구 1
}
스토리지 세트 cli $result
set fd $cli(fd)
cli_exec $fd "enable"
cli_exec $fd "terminal length 0"
cli_exec $fd "terminal width 0"
```

```
# 현재 로그 수집 수 가져오기
log_count [get_log_count] 설정
max_log_instances 2 설정
# 인증 상태의 모든 클라이언트 끌어오기
set summary [cli_exec $fd "show wireless client summary | 인증 포함"]
행 설정 [분할 $summary "\n"]
foreach 라인 $lines {
# MAC 형식 xxxx.xxxx.xxxx와 일치
if {[regexp {([0-9a-fA-F]{4}\.[0-9a-fA-F]{4}\.[0-9a-fA-F]{4})} $line -> mac]} {
세부 정보 설정 [cli_exec $fd "show wireless client mac-address $mac detail"]

# "Connected For" 시간 문자열 추출
경우 {[regexp {연결 대상 [[:space:]]*:[[:space:]]*(.+)} $detail -> conn_time]} {
초 설정 [time_to_seconds $conn_time]

# >15분(900초)이 걸렸는지 확인
{$seconds > 900} {
action_syslog 메시지 "EEM: $conn_time(>$seconds)에 대한 인증에서 클라이언트 $mac이 중지되었습니다."

# 최대 인스턴스 제한 미만인 경우에만 로그 수집
{$log_count < $max_log_instances} {
action_syslog 메시지 "EEM: WLC + 클라이언트 로그 수집(인스턴스 [expr {$log_count + 1}]/$max_log_instances)"
log_file "/bootflash/auth_stuck_eem.log" 설정


set fd_log [open $log_file a]

클라이언트당 로그 수
$fd_log 입력 "\n=== [clock format [clock seconds]] | 클라이언트 $mac | $conn_time ==="
$fd_log "\n— 클라이언트 세부 정보 —" 넣기
$fd_log $detail 입력
$fd_log "\n— 클라이언트 요약 —" 넣기
$fd_log [cli_exec $fd "show wireless client summary | 포함 $mac"]

# WLC 전체 로그
$fd_log "\n— WLC WNCD 로그(30m) 넣기 —"
puts $fd_log [cli_exec $fd "show logging process wncd start last 30 minutes"]
$fd_log "\n— WLC Show Tech Wireless —" 넣기
$fd_log 입력 [cli_exec $fd "show tech wireless"]

닫기 $fd_log
log_count 설정 [expr {$log_count + 1}]
set_log_count $log_count
} 또는 {
```

action_syslog 메시지 "EEM: 최대 로그 인스턴스($max_log_instances)에 도달했습니다. 로그 수집을 건너뜁니다."
}

중단된 클라이언트 인증 항상 취소
cli_exec $fd "무선 클라이언트 mac-address $mac deauthenticate"
action_syslog 메시지 "EEM: 인증되지 않은 클라이언트 $mac"
}
}
}
}
cli_close $fd
종료 0
—
스크립트의 주요 기능
1. **15분 간격**: Watchdog 타이머가 900초(15분)로 설정됨
2 . **고정 임계값**: 15분(900초) 이상 중단된 클라이언트에 대한 트리거만
3 . **로그 제한**: **최대 2개의 총 인스턴스에 대한 WLC + 클라이언트당 로그** 수집한 다음 로그 수집을 건너뜁니다(여전히 클라이언트 인증 취소).
4. **WLC 로그 수집**: 포함 내용:
- 클라이언트당 세부 정보/요약
- WNCD 프로세스 로그(30분 창)
- 전체 `show tech wireless`
5. **영구 카운터**: EEM 스크립트 실행 전반에 걸쳐 `/bootflash/auth_log_count.txt`를 통해 로그 인스턴스 추적

구축 및 확인
1. WLC에 스크립트 적용:
WLC# 터미널 구성
WLC (config) # 이벤트 관리자 애플릿 AuthStuckHandler
WLC (config-applet) # 이벤트 타이머 watchdog 시간 900
WLC (config-applet)# action 1 cli 명령 "sh bootflash:auth_stuck_eem.tcl"
WLC (config-applet) # 끝
(또는 WLC EEM 컨피그레이션에 전체 Tcl 스크립트를 직접 붙여넣습니다.)

2. EEM 등록 확인:
WLC# show event manager policy registered

3. 수집된 로그를 검색합니다.
WLC# copy bootflash:auth_stuck_eem.log ftp:
WLC# copy bootflash:auth_log_count.txt ftp:

4. 수집을 다시 활성화하려면 로그 카운터를 재설정합니다(필요한 경우).
WLC# 삭제 bootflash:auth_log_count.txt

결론

이 문서에서는 검증된 TAC 방법론과 실제 사례 연구를 통합하여 가장 광범위한 Catalyst 9800 Mesh WiFi 문제를 해결합니다. 불안정한 백홀, 클라이언트가 인증 상태에 머물러 있으며 트래픽이 전송되지 않습니다.

핵심 요지는 보고된 메시 장애의 90%가 격리된 하드웨어 또는 클라이언트 장애가 아니라 컨트롤 플레인 및 데이터 플레인 상태가 일치하지 않거나, 메시 토폴로지가 불안정하거나, 최적화되지 않은 RF 설계의 증상이라는 것입니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.