# Troubleshoot Catalyst 9800 Mesh Wifi Issues

## Contents



## Introduction

This document describes different methods to troubleshoot 9800 Mesh environments.

## Prerequisites

**Requirements**

Cisco recommends that you have knowledge of Wireless Controller along with Mesh deployment knowledge.

# 1. Scope & Applicability

Applies to: These issues for have occurred for Sea port and mining environment.

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

* Outdoor Mesh Deployments (RAP–MAP)

* Dual-band (2.4 GHz / 5 GHz) WLANs

* Environments with:

  * Long-distance mesh links

  * High RF noise / industrial areas (ports, terminals, yards)

# 2. Common Customer Reported Symptoms

Mesh / AP Symptoms

### 1. Mesh AP shows Joined on WLC but no Client Connects

  * No client or upstream traffic

  * Ping fails until AP reboot.

### 2. RAP–MAP Link

  * Flaps intermittently.

  * MAP roams to another RAP/MAP unexpectedly.

  * Mesh AP disconnects from WLC and requires manual reboot.

### 3. Client Connectivity Symptoms

* Client stuck in Authenticating state indefinitely.

* Client roams across APs but remains unauthenticated.

* Client connects only after:

  * Force removal from WLC or AP reboot

  * Frequent client drops on 2.4 GHz

## 3. High Probability Root Cause Buckets

| **Category** | **Typical Issues** |
|---|---|
| RF / Design | Channel overlap, wide channel width, antenna misalignment |
| Mesh Control | Parent selection instability, weak backhaul SNR |
| Configuration | Mixed data rates, multiple BGNs, static power |
| Software | wncd process stalls, stale client state |
| Scale / Load | Excess auth calls, EAPOL timer mismatch |

## 4. Mandatory Design and Configuration Validation

### 4.1 Mesh Backhaul (Critical)

Root AP (RAP)

- Channel width: 20 MHz only
- Non-overlapping channels across RAPs
- Same Bridge Group Name (BGN)
- Static channel assignment
- Line of sight to MAP

Avoid

- Mixing 20/40 MHz on RAPs
- Same channel on all RAPs
- Multiple BGNs in same area

### 4.2 Antenna & Mounting

- 5 GHz omni antenna:
- Mounted perpendicular to ground
- Dedicated 5 GHz radio for mesh backhaul
- Directional antenna preferred for long-range MAPs
- Eliminate obstructions (metal, cranes, containers)

## 5. RF & WLAN Best Practices

### 5.1 Data Rates (Highly Recommended)

2.4 GHz

Mandatory: 12 Mbps

Disable: 6, 9 Mbps

Others: Supported

5 GHz

Mandatory: 12 Mbps

Disable: 6, 9 Mbps

Others: Supported

Impact:

- Reduces sticky clients
- Improves roaming & authentication stability

### 5.2 Power & RRM

- Avoid AP-level static TX power
- Use Global RRM
- Minimum TX Power:
- 2.4 GHz: ≥ 12 dBm

Avoid aggressive DCA changes in production hours

# Troubleshooting Client Connectivity Issue

## Problem Description

In mesh-connected areas:

- Clients associate to MAPs successfully.
- Authentication starts but never completes.
- Client remains in Authenticating state on the WLC.
- Client can roam between APs while still authenticating.
- Authentication succeeds only after: Client is manually removed from the WLC, or MAP is rebooted.

This behavior is intermittent, difficult to reproduce on demand, and not part of normal authentication flow.

## Observed Symptoms

- Show wireless client summary displays clients stuck in Authenticating.
- Clients generate repeated authentication attempts.
- No explicit authentication failure or rejection seen.
- Client remains stuck even after multiple roam events.
- Issue primarily observed when clients are connected via MAPs.
- Issue frequency increases during operational load.

## Key Contributing Factors in Mesh Deployments for Client Connection Issue

1. Mesh Backhaul Instability

- Fluctuating RSSI/SNR between RAP and MAP.
- MAP reselecting parent during authentication.
- Mesh latency causing EAP timeout or retransmission.
- MAP temporarily forwarding traffic but not consistently

Impact:

- Authentication state machine does not complete.
- Client remains stuck in Authenticating.

2. Roaming During Authentication

- Clients roam between MAPs or between MAP and RAP.
- Authentication context does not fully transfer.
- Client continues roaming while remaining in Authenticating state

Impact:

- Authentication restarts repeatedly.
- Client never reaches RUN state.

3. Low Data Rates on Client Serving Radio (2.4 GHz)

- Mandatory 6 or 9 Mbps enabled.
- Excessive retries and airtime consumption.
- Authentication frames delayed or dropped.

Impact:

- EAP exchange becomes unreliable over mesh.
- Authentication appears hung without explicit failure.

4. Mesh Backhaul and Client Traffic Sharing the Same RF Constraints

- High utilization on mesh links.
- Client authentication traffic competes with:
- Data traffic
- Control traffic
- Authentication packets are small but time sensitive.

Impact:

- Authentication completes only after retries or resets

## How to Identify the Issue is Hit (Mesh Authentication Stuck)

The issue is considered hit when all the mentioned conditions are observed simultaneously in a mesh deployment:

Client Behavior Indicators

- Client remains in Authenticating state for more than 60–120 seconds.
- Client does not transition to RUN state automatically.
- Client connects successfully only after:
- Forceful client removal from WLC
- Mesh AP reboot
- Client can roam between MAPs or RAPs while remaining in Authenticating state.

WLC Indicators

Command:

**show wireless client summary**

Indicators:

- Same client MAC persistently listed under Authenticating.
- Client entry does not age out naturally.

Check in this command if client is Connected for more than 10 mins:

**show wireless client mac <client-mac>**

Mesh-Specific Indicators

Commands:

**show ap mesh parent**

**show ap mesh link**

Indicators:

- Parent change or instability during client authentication
- Fluctuating RSSI / SNR values
- Increased retries or packet loss on mesh backhaul

## Mandatory Log Collection (During Failure Window)

Logs must be collected while the client is stuck in Authenticating state.
Logs collected after reboot or client deletion are not useful for root cause.

1. Controller Baseline Logs

**show tech wireless**

**show clock**

Purpose:

- Capture overall WLC state
- Correlate timestamps across logs

2. Client State Validation Logs

**show wireless client summary**

**show wireless client summary | include Authenticating**

**show wireless client mac <client-mac>**

3. WNCD Internal Logs (Critical)

Enable verbose tracing:

set platform software trace wncd chassis active r0 all verbose

Collect logs (last 30 minutes):

**show logging process wncd** internal last 30 minutes

Client-specific filtered logs:

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

4. Radio Active (RA) Trace – Per Client

From GUI:

- **Monitor > Wireless > Client > Troubleshooting**
- Add affected client MAC.
- Start RA Trace.
- Reproduce the issue.

5. Mesh Backhaul Validation Logs

**show ap mesh link**

**show ap mesh parent**

**show ap mesh statistics**

6. Optional (If Available) – Authentication Server Logs

- RADIUS authentication logs for the affected client
- Authentication latency and retransmissions

# Troubleshooting MAP-RAP Disconnection Issue

## Problem Description

Intermittent and unpredictable loss of mesh backhaul connectivity across multiple IW9167 MAPs, resulting in AP disjoins, mesh authentication failures, unreachable APs, and client traffic blackholing. Recovery often required AP reboot or WLC intervention.

## Symptoms

- MAP disassociates from parent RAP
- MAP associated but cannot pass traffic
- MAP unreachable from WLC, RAP, and gateway
- Clients associated but no upstream reachability
- Cascading outages when parent MAP or RAP roams

Error Messages / Indicators

ERROR-MeshSecurity: Timer expired

CRIT-MeshSecurity: Mesh Security failed to authenticate with parent

CRIT-MeshAwppAdj: Remove as Parent

mlme_ext_vap_down: VAP (mon1) is down

ieee80211_ucfg_mesh_add_client(): Node not found

DTLS close alerts

CAPWAP heartbeat timeout

## How to Identify the Issue Is Hit (RAP-MAP Connection Issue)

1. Mesh Control Plane Appears Healthy

The mentioned commands can appear normal and cannot be used alone to validate traffic forwarding:

**show ap summary**

**show wireless mesh ap tree**

**show capwap client rcb**

These commands confirm **control-plane state only**.

**Identifying Mesh Data-Plane Failure**

**MAP: show mesh status**

This is the primary indicator of mesh forwarding health.

Healthy Output

Parent AP MAC : 24:D7:9C:04:79:B1

Mesh Link State : UP

Forwarding State : ENABLED

Traffic Blackholing Output

Parent AP MAC : 24:D7:9C:04:79:B1

Mesh Link State : UP

Forwarding State : DISABLED

Interpretation:
Mesh adjacency exists, but the AP is not forwarding traffic.

2. MAP: show mesh history

Repeated parent transitions without AP reload indicate unstable forwarding state:

CRIT-MeshAwppAdj: Remove as Parent

CRIT-MeshAwppAdj: Set as Parent

CRIT-MeshAwppAdj: Remove as Parent

This pattern often leaves the AP in a non-forwarding state.

3. MAP Syslog Symptoms

Common syslog messages observed during traffic blackholing:

ieee80211_ucfg_mesh_add_client(): Node not found

CLSM: Skip key programming due to null key

These indicate that the mesh security context is incomplete, preventing encrypted traffic forwarding.

4. WLC show ap name <AP> mesh path

This command confirms the controller’s view of the data path.

Healthy

Path Status : Active

Data Path : Complete

Traffic Blackholing

Path Status : Active

Data Path : Incomplete

interpretation:
The mesh path exists, but data forwarding is not established.

5. ARP-Related Indicators

In deployments where the VLAN SVI resides on the WLC:

- ARP entries exist for clients and AP.
- Client traffic fails.
- Clearing ARP restores connectivity immediately.

This behavior confirms data-plane forwarding failure, not RF or CAPWAP instability.

## Mandatory Log Collection (During Failure Window)

Phase 0 – Mandatory Preparation (Before Issue Occurs)

IMPORTANT: Logs collected after reboot are insufficient for mesh RCA.

Enable Persistent Debugs on RAP & MAP

On RAP

terminal length 0

debug mesh 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

On MAP

terminal length 0

debug mesh 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

Leave debugs enabled until issue reproduces.

Phase 1 – Log Collection During Issue (CRITICAL)

DO NOT REBOOT APs BEFORE COLLECTING LOGS

Logs from Affected MAP (Immediately When Issue Occurs)

**show mesh status**

**show mesh history oldest**

**show mesh history**

**show flash syslogs**

**more syslog <date>**

Logs from RAP (Previous & New Parent)

**show mesh history oldest**

**show mesh status**

Logs from WLC (At Failure Time)

**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**

Optional (high value):

**show logging process wncd start last 2 days level verbose**

Client & Traffic Correlation (Recommended)

Run continuous ping during failure window:

ping -t <gateway-ip>

Phase 2 – RF & Configuration Validation (Post-Capture)

RF Validation (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 / Forwarding Validation (If Traffic Blackholing)

If SVI hosted on WLC:

clear arp-cache

If traffic restores → ARP handling is a contributing factor.

Phase 3 – Stabilization Actions (Validated)

Mesh Topology Controls

- Enable Block Child on MAPs where applicable.
- Force MAPs to connect to nearest RAP.
- Reduce mesh hop count.

RF Optimization

- Reduce RAP transmit power.
- Lock 5 GHz backhaul channels.
- Standardize 2.4 GHz channels (1/6/11).

All the mentioned issues are very intermittent in mesh deployment and hard to get hence deploying quick script to capture the logs can get the resolution faster.

Here is a sample EEM script which can be run on the WLC for client authentication issue:

Full EEM Script (Apply via WLC CLI)

```
::cisco::eem::event_register_timer watchdog time 900 maxrun 240
namespace import ::cisco::eem::*
namespace import ::cisco::lib::*
# ----------------------------
# Proc: Convert WLC time string to seconds
# Supports: "X days Xh:Xm:Xs", "Xh:Xm:Xs", "Xm:Xs", "Xs"
# ----------------------------
proc time_to_seconds {time_str} {
set total 0
if {[regexp {([0-9]+)\s+days?\s+([0-9]+)\s+h:([0-9]+)\s+m:([0-9]+)\s+s} $time_str -> d h m s]} {
set total [expr {$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]} {
set total $s
}
return $total
}
# ----------------------------
# Proc: Track total log collection instances (max 2)
# ----------------------------
proc get_log_count {} {
if {[file exists /bootflash/auth_log_count.txt]} {
set fd [open /bootflash/auth_log_count.txt r]
set count [read $fd]
close $fd
return $count
} else {
return 0
}
}
proc set_log_count {count} {
set fd [open /bootflash/auth_log_count.txt w]
puts $fd $count
close $fd
}
# ----------------------------
# Main EEM Execution
# ----------------------------
if {[catch {cli_open} result]} {
exit 1
}
array set cli $result
set fd $cli(fd)
cli_exec $fd "enable"
cli_exec $fd "terminal length 0"
cli_exec $fd "terminal width 0"
# Get current log collection count
```

```
set log_count [get_log_count]
set max_log_instances 2
# Pull all clients in Authenticating state
set summary [cli_exec $fd "show wireless client summary | include Authenticating"]
set lines [split $summary "\n"]
foreach line $lines {
# Match MAC format xxxx.xxxx.xxxx
if {[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"]

# Extract "Connected For" time string
if {[regexp {Connected For[[:space:]]*:[[:space:]]*(.+)} $detail -> conn_time]} {
set seconds [time_to_seconds $conn_time]

# Check if stuck >15 minutes (900 seconds)
if {$seconds > 900} {
action_syslog msg "EEM: Client $mac stuck in Authenticating for $conn_time (>$seconds seconds)"

# Collect logs only if under max instance limit
if {$log_count < $max_log_instances} {
action_syslog msg "EEM: Collecting WLC + client logs (Instance [expr {$log_count +
1}]/$max_log_instances)"
set log_file "/bootflash/auth_stuck_eem.log"


set fd_log [open $log_file a]

# Per-client logs
puts $fd_log "\n=== [clock format [clock seconds]] | Client $mac | Stuck $conn_time ==="
puts $fd_log "\n--- Client Detail ---"
puts $fd_log $detail
puts $fd_log "\n--- Client Summary ---"
puts $fd_log [cli_exec $fd "show wireless client summary | include $mac"]

# WLC-wide logs
puts $fd_log "\n--- WLC WNCD Logs (30m) ---"
puts $fd_log [cli_exec $fd "show logging process wncd start last 30 minutes"]
puts $fd_log "\n--- WLC Show Tech Wireless ---"
puts $fd_log [cli_exec $fd "show tech wireless"]

close $fd_log
set log_count [expr {$log_count + 1}]
set_log_count $log_count
} else {
action_syslog msg "EEM: Max log instances ($max_log_instances) reached. Skipping log collection."
}

# Always deauthenticate stuck client
cli_exec $fd "wireless client mac-address $mac deauthenticate"
action_syslog msg "EEM: Deauthenticated client $mac"
}
}
}
}
```

cli_close $fd
exit 0
---
#### Key Features of the script
1. **15-minute interval**: Watchdog timer set to 900 seconds (15 mins) as requested
2. **Stuck threshold**: Only triggers on clients stuck >15 minutes (900 seconds)
3. **Log limit**: Collects WLC + per-client logs for **max 2 total instances**, then skips log collection (still deauthenticates clients)
4. **WLC log collection**: Includes:
- Per-client detail/summary
- WNCD process logs (30 minute window)
- Full `show tech wireless`
5. **Persistent counter**: Tracks log instances via `/bootflash/auth_log_count.txt` across EEM script runs

Deploy & Verify
1. Apply the script to WLC:
WLC# configure terminal
WLC(config)# event manager applet AuthStuckHandler
WLC(config-applet)# event timer watchdog time 900
WLC(config-applet)# action 1 cli command "sh bootflash:auth_stuck_eem.tcl"
WLC(config-applet)# end
(Or paste the full Tcl script directly into the WLC EEM configuration.)

2. Check EEM registration:
WLC# show event manager policy registered

3. Retrieve collected logs:
WLC# copy bootflash:auth_stuck_eem.log ftp:
WLC# copy bootflash:auth_log_count.txt ftp:

4. Reset log counter to re-enable collection (if needed):
WLC# delete bootflash:auth_log_count.txt

# Conclusion

This document consolidates validated TAC methodologies and real-world case studies to resolve the most pervasive Catalyst 9800 Mesh WiFi issues: unstable backhaul, clients stuck in Authenticating state, and traffic not getting transmitted.

A core takeaway is that 90% of reported mesh failures are not isolated hardware or client faults, but symptoms of mismatched control-plane and data-plane state, unstable mesh topology, or suboptimal RF design.