

# Risoluzione Dei Problemi Di Catalyst 9800 Mesh Wifi

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[1. Campo di applicazione e applicabilità](#)

[2. Sintomi comuni segnalati dal cliente](#)

[1. L'access point Mesh mostra unito sul WLC ma non sui client che si connettono](#)

[2. Collegamento RAP-MAP](#)

[3. Sintomi della connettività dei client](#)

[3. Bucket causa principale alta probabilità](#)

[4. Convalida obbligatoria della progettazione e della configurazione](#)

[4.1 Backhaul di rete \(critico\)](#)

[4.2 Antenna e montaggio](#)

[5. Best practice per RF e WLAN](#)

[5.1 Velocità di trasferimento dati \(consigliata\)](#)

[5.2 Alimentazione e RRM](#)

[Risoluzione dei problemi di connettività client](#)

[Descrizione del problema](#)

[Sintomi osservati](#)

[Fattori principali che contribuiscono alle distribuzioni di Mesh per i problemi di connessione del client](#)

[Come identificare il problema riscontrato \(autenticazione Mesh bloccata\)](#)

[Raccolta obbligatoria log \(durante la finestra di errore\)](#)

[Risoluzione dei problemi di disconnessione MAP-RAP](#)

[Descrizione del problema](#)

[Sintomi](#)

[Come identificare il problema riscontrato \(problema di connessione RAP-MAP\)](#)

[Raccolta obbligatoria log \(durante la finestra di errore\)](#)

[Conclusioni](#)

---

## Introduzione

In questo documento vengono descritti diversi metodi per risolvere i problemi degli ambienti 9800 Mesh.

# Prerequisiti

## Requisiti

Cisco raccomanda la conoscenza di Wireless Controller insieme alla conoscenza dell'installazione di Mesh.

## 1. Campo di applicazione e applicabilità

Si applica a: Questi problemi sono stati riscontrati per l'ambiente minerario e del porto marittimo.

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

- \* Implementazioni Mesh all'esterno (RAP-MAP)

- \* WLAN dual-band (2,4 GHz / 5 GHz)

- \* Ambienti con:

- \* Collegamenti mesh a lunga distanza

- \* Disturbo RF elevato / aree industriali (porte, terminali, iarde)

## 2. Sintomi comuni segnalati dal cliente

Sintomi di Mesh/AP

1. L'access point Mesh mostra unito sul WLC ma non sui client che si connettono

- \* Nessun traffico client o upstream

- \* Il ping ha esito negativo fino al riavvio del punto di accesso.

## 2. Collegamento RAP-MAP

- \* Lampeggia in modo intermittente.
- \* MAP esegue il roaming a un altro RAP/MAP in modo imprevisto.
- \* Mesh AP si disconnette dal WLC e richiede il riavvio manuale.

## 3. Sintomi della connettività dei client

- \* Client bloccato in stato di autenticazione per un periodo di tempo indefinito.
- \* Il client esegue il roaming tra i punti di accesso, ma rimane non autenticato.
- \* Il client si connette solo dopo:
  - \* Imponi rimozione dal riavvio del WLC o del punto di accesso
  - \* Frequenti cadute del client su 2,4 GHz

## 3. Bucket ad alta probabilità della causa principale

Categoria	Problemi tipici
RF/Progettazione	Sovrapposizione dei canali, larghezza del canale ampia, disallineamento dell'antenna
Controllo mesh	Instabilità della selezione padre, SNR backhaul debole
Configurazione	Velocità di trasmissione dati miste, più BGN, alimentazione statica
Software	processo wncd bloccato, stato client non aggiornato
Scala/Carica	Numero eccessivo di chiamate di autenticazione, timer EAPOL non corrispondente

## 4. Convalida obbligatoria della progettazione e della configurazione

### 4.1 Backhaul di rete (critico)

Root AP (RAP)

- Larghezza del canale: solo 20 MHz
- Canali non sovrapposti nei punti di autorizzazione risorse
- Stesso nome gruppo bridge (BGN)
- Assegnazione canale statico
- Linea di visibilità verso MAP

Evitare

- Mixaggio 20/40 MHz su RAP
- Stesso canale su tutti i RAP
- Più BGN nella stessa area

### 4.2 Antenna e montaggio

- 5 GHz antenna omni:
- Montato perpendicolarmente al suolo
- Radio a 5 GHz dedicata per backhaul mesh
- Antenna direzionale preferita per MAPPE a lungo raggio
- Eliminare gli ostacoli (metallo, gru, contenitori)

## 5. Best practice per RF e WLAN

### 5.1 Velocità di trasferimento dati (consigliata)

2,4 GHz

Obbligatorio: 12 Mbps

Disabilita: 6, 9 Mbps

Altri: Supportato

5 GHz

Obbligatorio: 12 Mbps

Disabilita: 6, 9 Mbps

Altri: Supportato

Conseguenze:

- Riduce i client permanenti
- Migliora la stabilità di roaming e autenticazione

## 5.2 Alimentazione e RRM

- Evitare l'alimentazione TX statica a livello AP
- Usa RRM globale
- Alimentazione TX minima:
  - 2,4 GHz:  $\geq 12$  dBm

Evitare modifiche aggressive del DCA nelle ore di produzione

## Risoluzione dei problemi di connettività client

### Descrizione del problema

Nelle aree collegate alla rete:

- Associazione dei client alle mappe completata.
- L'autenticazione ha inizio ma non viene mai completata.
- Il client rimane nello stato di autenticazione sul WLC.
- Il client può spostarsi tra i punti di accesso durante l'autenticazione.
- L'autenticazione ha esito positivo solo dopo: Il client viene rimosso manualmente dal WLC o MAP viene riavviato.

Questo comportamento è intermittente, difficile da riprodurre su richiesta e non fa parte del normale flusso di autenticazione.

## Sintomi osservati

- Mostra riepilogo client wireless visualizza i client bloccati nell'autenticazione.
- I client generano tentativi di autenticazione ripetuti.
- Non sono stati rilevati errori o rifiuti di autenticazione espliciti.
- Il client rimane bloccato anche dopo più eventi di roaming.
- Problema osservato principalmente quando i client sono connessi tramite MAP.
- La frequenza di emissione aumenta durante il carico operativo.

## Fattori principali che contribuiscono alle distribuzioni di Mesh per i problemi di connessione del client

### 1. Instabilità del backhaul della rete

- Fluttuazione di RSSI/SNR tra RAP e MAP.
- MAP: rielezione del padre durante l'autenticazione.
- Latenza mesh che causa timeout o ritrasmissione EAP.
- Mapping per l'inoltro temporaneo del traffico ma non coerente

#### Conseguenze:

- Il computer dello stato di autenticazione non è stato completato.
- Il client rimane bloccato nell'autenticazione.

### 2. Roaming durante l'autenticazione

- I client eseguono il roaming tra MAP o tra MAP e RAP.
- Il contesto di autenticazione non viene trasferito completamente.
- Il client continua il roaming mentre è in stato di autenticazione

#### Conseguenze:

- L'autenticazione viene riavviata ripetutamente.
- Il client non raggiunge mai lo stato RUN.

### 3. Basse velocità di trasmissione dati su client radio (2,4 GHz)

- 6 o 9 Mbps obbligatorio abilitato.
- Tentativi eccessivi e consumo di tempo di trasmissione.
- Frame di autenticazione ritardati o eliminati.

#### Conseguenze:

- Lo scambio EAP diventa inaffidabile sulla rete.
- L'autenticazione sembra bloccata senza errori espliciti.

### 4. Backhaul mesh e traffico client che condividono gli stessi vincoli RF

- Utilizzo elevato sui collegamenti mesh.
- Il traffico di autenticazione client è in concorrenza con:
  - Traffico dati
  - Controllo del traffico
- I pacchetti di autenticazione sono piccoli, ma richiedono un intervallo di tempo.

#### Conseguenze:

- L'autenticazione viene completata solo dopo nuovi tentativi o reimpostazioni

### Come identificare il problema riscontrato (autenticazione Mesh bloccata)

Il problema è considerato risolto quando tutte le condizioni menzionate sono osservate contemporaneamente in una distribuzione mesh:

#### Indicatori di comportamento client

- Il client rimane nello stato di autenticazione per più di 60-120 secondi.
- Il client non passa automaticamente allo stato RUN.
- Il client si connette correttamente solo dopo:
  - Rimozione forzata del client dal WLC
  - Riavvio Mesh AP
- Il client può spostarsi tra MAP o RAP pur rimanendo nello stato di autenticazione.

#### Indicatori WLC

Comando:

mostra riepilogo client wireless

Indicatori:

- Stesso MAC client elencato in modo permanente in Autenticazione.
- L'ingresso del cliente non invecchia naturalmente.

Archiviare questo comando se il client è connesso da più di 10 minuti:

show wireless client mac <mac-client>

Indicatori specifici della rete

Comandi:

mostra elemento padre mesh ap

mostra collegamento a rete ap

Indicatori:

- Modifica o instabilità padre durante l'autenticazione del client
- Valori RSSI/SNR variabili
- Aumento dei tentativi o perdita di pacchetti in caso di backhaul mesh

Raccolta obbligatoria log (durante la finestra di errore)

I registri devono essere raccolti mentre il client è bloccato nello stato di autenticazione.

I registri raccolti dopo il riavvio o l'eliminazione del client non sono utili per la causa principale.

1. Log di base controller

show tech wireless

show clock

Scopo:

- Acquisisci stato WLC generale
- Correlazione di timestamp tra registri

## 2. Registri di convalida dello stato del client

mostra riepilogo client wireless

mostra riepilogo client wireless | include l'autenticazione

show wireless client mac <mac-client>

## 3. Registri interni WNCD (critici)

Abilita traccia dettagliata:

set platform software trace wncd chassis active r0 all verbose

Raccogli registri (ultimi 30 minuti):

show logging process wncd internal ultimi 30 minuti

Registri filtrati specifici del client:

show logging processo wncd avvio ultimi 30 minuti filtro mac <client-mac> to-file  
bootflash:wncd\_client.log

## 4. Traccia RSA (Radio Active) - Per client

Dalla GUI:

- Monitor > Wireless > Client > Risoluzione dei problemi
- Aggiungi MAC client interessato.
- Avviare la traccia dell'Autorità registrazione.
- Riprodurre il problema.

## 5. Log di convalida backhaul Mesh

mostra collegamento a rete ap

mostra elemento padre mesh ap

mostra statistiche mesh ap

## 6. Facoltativo (Se Disponibile) - Log Del Server Di Autenticazione

- Log di autenticazione RADIUS per il client interessato
- Latenza di autenticazione e ritrasmissioni

# Risoluzione dei problemi di disconnessione MAP-RAP

## Descrizione del problema

Perdita intermittente e imprevedibile della connettività backhaul mesh su più MAP IW9167, con conseguenti disjoin degli AP, errori di autenticazione mesh, punti di accesso non raggiungibili e blocchi del traffico client. Il ripristino spesso richiedeva il riavvio dell'access point o l'intervento del WLC.

## Sintomi

- MAP dissocia da RAP padre
- Mapping associato, ma impossibile passare il traffico
- MAP non raggiungibile da WLC, RAP e gateway
- Client associati ma non raggiungibili a monte
- Interruzioni a cascata durante il roaming di MAP o RAP padre

## Messaggi di errore / Indicatori

ERROR-MeshSecurity: Timer scaduto

CRIT-MeshSecurity Autenticazione di Mesh Security con il padre non riuscita

CRIT-MeshAwppAdj: Rimuovi come padre

mlme\_ext\_vap\_down: VAP (mon1) non attivo

ieee80211\_ucfg\_mesh\_add\_client(): Nodo non trovato

Avvisi di chiusura DTLS

Timeout heartbeat CAPWAP

Come identificare il problema riscontrato (problema di connessione RAP-MAP)

1. Il piano di controllo della rete è integro

I comandi indicati possono apparire normali e non possono essere utilizzati da soli per convalidare l'inoltro del traffico:

mostra riepilogo app

mostra albero wireless mesh ap

show capwap client rcb

Questi comandi confermano solo lo stato del piano di controllo.

Identificazione dell'errore del piano dati della rete

MAP: mostra lo stato mesh

Questo è l'indicatore primario dello stato di inoltro della rete.

Output integro

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

Stato collegamento mesh: ATTIVO

Stato inoltro: ATTIVATO

Output Traffic Blackholing

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

Stato collegamento mesh: ATTIVO

Stato inoltro: DISABLED

Interpretazione

Il protocollo Mesh adiacente esiste, ma il punto di accesso non sta inoltrando il traffico.

2. MAP: show mesh history

Le transizioni padre ripetute senza ricaricamento AP indicano uno stato di inoltro instabile:

CRIT-MeshAwppAdj: Rimuovi come padre

CRIT-MeshAwppAdj: Imposta come padre

CRIT-MeshAwppAdj: Rimuovi come padre

Questo modello spesso lascia l'access point in uno stato di non inoltro.

3. Sintomi dei sintomi di MAP

Messaggi syslog comuni osservati durante le interruzioni del traffico:

ieee80211\_ucfg\_mesh\_add\_client(): Nodo non trovato

CLSM: Ignora la programmazione della chiave a causa della chiave Null

Ciò indica che il contesto di sicurezza della rete è incompleto e impedisce l'inoltro del traffico crittografato.

4. Percorso mesh <AP>show ap name WLC

Questo comando conferma la visualizzazione del percorso dati da parte del controller.

Integro

Stato percorso: Active

Percorso dati: Completa

Traffic Blackholing

Stato percorso: Active

Percorso dati: Incompleto

interpretazione:

Il percorso mesh esiste, ma l'inoltro dei dati non è definito.

## 5. Indicatori relativi alla politica di vicinato (ARP)

Nelle implementazioni in cui la VLAN SVI risiede sul WLC:

- Sono presenti voci ARP per client e access point.
- Il traffico del client non riesce.
- Se si cancella ARP, la connettività viene ripristinata immediatamente.

Questo comportamento conferma un errore di inoltro del piano dati, non l'instabilità RF o CAPWAP.

## Raccolta obbligatoria log (durante la finestra di errore)

Fase 0 - Preparazione obbligatoria (prima del rilascio)

**IMPORTANTE:** i log raccolti dopo il riavvio non sono sufficienti per RCA mesh.

Abilita debug permanenti su RAP e MAP

Su RAP

lunghezza terminale 0

debug mesh events

figlio adiacenza mesh di debug

debug mesh adjacency packet

debug mesh adjacency channel

debug mesh security

debug mesh forwarding packet

debug capwap client events

debug capwap client error

monitor del terminale

Sulla mappa

lunghezza terminale 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

monitor del terminale

Mantenere abilitati i debug fino alla riproduzione del problema.

Fase 1 - Raccolta dei log durante il problema (CRITICAL)

NON RIAVVIARE GLI ACCESS POINT PRIMA DI RACCOGLIERE I LOG

Registri dal MAP interessato (immediatamente in caso di problemi)

show mesh status

mostra cronologia mesh meno recente

mostra cronologia mesh

mostra syslog flash

more syslog <data>

Registri da RAP (padre precedente e nuovo)

mostra cronologia mesh meno recente

show mesh status

Log da WLC (al momento dell'errore)

mostra albero wireless mesh ap

mostra router adiacente mesh wireless

show ap name <AP-NAME> mesh path

show ap name <AP-NAME> config general

show tech-support wireless

Facoltativo (valore elevato):

show logging process wncd start last 2 days livello verbose

Correlazione traffico e client (scelta consigliata)

Esegui ping continuo durante la finestra di errore:

```
ping -t <gateway-ip>
```

Fase 2 - Convalida RF e configurazione (post-acquisizione)

Convalida RF (WLC)

```
mostra riepilogo ap dot11 5ghz
```

```
mostra riepilogo ap dot11 24ghz
```

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

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

Convalida ARP/Inoltro (in caso di blocco del traffico)

Se la SVI è ospitata sul WLC:

```
cancella arp-cache
```

Se il traffico ripristina → la gestione ARP è un fattore che contribuisce.

Fase 3 - Azioni di stabilizzazione (convalidate)

Controlli della topologia della rete

- Abilitare Blocca figlio nelle mappe, se applicabile.
- Forza la connessione delle mappe al punto di accesso più vicino.
- Ridurre il numero di hop mesh.

Ottimizzazione RF

- Riduzione della potenza di trasmissione RAP.
- Bloccare i canali backhaul da 5 GHz.
- Canali standard a 2,4 GHz (1/6/11).

Tutti i problemi citati sono molto intermittenti nella distribuzione mesh e difficile da ottenere, quindi la distribuzione di script rapido per acquisire i log può ottenere la risoluzione più veloce.

Di seguito è riportato un esempio di script EEM che può essere eseguito sul WLC per un problema di autenticazione del client:

Script EEM completo (applicazione tramite CLI WLC)

```
::cisco::eem::event_register_timer tempo di watchdog 900 maxrun 240
importazione spazio dei nomi ::cisco::eem::*
importazione spazio dei nomi ::cisco::lib::*
N. —
N. proc.: Converti stringa temporale WLC in secondi
# Supporti: "X giorni Xh:Xm:Xs", "Xh:Xm:Xs", "Xm:Xs", "Xs"
N. —
proc_time_to_seconds {time_str} {
imposta totale 0
if {[regexp {[0-9]+\s+giorni?\s+([0-9]+\s+h:([0-9]+\s+m:([0-9]+\s+s)} $time_str -> d h m s]} {
set total [espr {$d*86400 + $h*3600 + $m*60 + $s}]
} elseif {[regexp {[0-9]+\s+h:([0-9]+\s+m:([0-9]+\s+s)} $time_str -> h m s]} {
set total [espr {$h*3600 + $m*60 + $s}]
} elseif {[regexp {[0-9]+\s+m:([0-9]+\s+s)} $time_str -> m s]} {
set total [espr {$m*60 + $s}]
} elseif {[regexp {[0-9]+\s+s} $time_str -> s]} {
imposta totale $s
}
restituisce $total
}
N. —
N. proc.: Registra il totale delle istanze della raccolta di log (massimo 2)
N. —
proc_get_log_count {} {
if {[file esiste /bootflash/auth_log_count.txt]} {
set fd [open /bootflash/auth_log_count.txt r]
set count [lettura $fd]
chiudi $fd
restituisce $count
} else {
valore restituito 0
}
}
```

```

proc set_log_count {count} {
set fd [open /bootflash/auth_log_count.txt w]
put $fd $count
chiudi $fd
}
N. —
# Esecuzione EEM principale
N. —
if {[catch {cli_open} risultato]} {
uscita 1
}
set di array cli $result
set fd $cli(fd)
cli_exec $fd "abilita"
cli_exec $fd "lunghezza terminale 0"
cli_exec $fd "larghezza terminale 0"
# Recupero del conteggio della raccolta di log corrente
set log_count [get_log_count]
set max_log_instance 2
# Pull di tutti i client in stato di autenticazione
set summary [cli_exec $fd "show wireless client summary" | include Authenticating"]
set lines [split $summary "\n"]
foreach line $lines {
# Formato MAC 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"]

# Estrazione della stringa temporale "Connesso per"
if {[regexp {Connected For[:space:]]*:[[:space:]]*(.+)} $detail -> conn_time]} {
set seconds [time_to_seconds $conn_time]

# Verifica se bloccato >15 minuti (900 secondi)
se {$seconds > 900} {
action_syslog msg "EEM: $mac client bloccato in Autenticazione per $conn_time (>$seconds)"

# Raccolta dei registri solo se il limite massimo di istanze è inferiore a
if {$log_count < $max_log_instance} {
action_syslog msg "EEM: Raccolta dei log WLC + client (Instance [expr {$log_count +
1}]/$max_log_instance)"
set log_file "/bootflash/auth_stuck_eem.log"

set fd_log [open $file_log a]

N. registri per client
puts $fd_log "\n=== [formato orologio [secondi]] | Client $mac | $conn_time bloccato =="

```

```
puts $fd_log "\n— Dettagli client —"
inserisce $fd_log $detail
puts $fd_log "\n— Riepilogo client —"
puts $fd_log [cli_exec $fd "show wireless client summary" | include $mac"]
```

N. registri a livello WLC

```
puts $fd_log "\n— WLC Registri WNCD (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"]
```

```
chiudi $fd_log
set log_count [espr {$log_count + 1}]
set_log_count $conteggio
} else {
action_syslog msg "EEM: È stato raggiunto il numero massimo di istanze del log
($max_log_instance). La raccolta dei log verrà ignorata."
}
```

# Disautentica sempre il client bloccato

```
cli_exec $fd "indirizzo-mac client wireless $mac deauthentication"
action_syslog msg "EEM: Client deautenticato $mac"
}
}
}
```

```
cli_chiudi $fd
uscita 0
```

##### Caratteristiche principali dello script

1. **intervallo di 15 minuti**: Timer di watchdog impostato su 900 secondi (15 minuti) come richiesto
2. **Soglia autocentrante**: Attiva solo sui client bloccati per oltre 15 minuti (900 secondi)
3. **Limite log**: Raccoglie i log WLC + per client per **max 2 istanze totali**, quindi ignora la raccolta dei log (disautentica ancora i client)
4. **Raccolta registri WLC**: Include:
  - Riepilogo/dettaglio per client
  - Registri di processo WNCD (finestra di 30 minuti)
  - `show tech wireless` completo
5. **Contatore permanente**: Rileva le istanze del log tramite `/bootflash/auth\_log\_count.txt` tra le esecuzioni dello script EEM

Distribuzione e verifica

1. Applicare lo script al WLC:

```
WLC# configure terminal
```

```
Applet gestione eventi WLC(config)# AuthStuckHandler
```

```
WLC(config-applet)# ora watchdog timer evento 900
```

```
WLC(config-applet)# azione 1 comando cli "sh bootflash:auth_stuck_eem.tcl"
```

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

In alternativa, incollare lo script Tcl completo direttamente nella configurazione EEM del WLC.

2. Controllare la registrazione EEM:

```
WLC# mostra criteri di gestione eventi registrati
```

3. Recuperare i registri raccolti:

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

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

4. Reimpostare il contatore di log per riabilitare la raccolta (se necessario):

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

## Conclusioni

Questo documento consolida metodologie TAC convalidate e case study reali per risolvere i problemi più diffusi di Catalyst 9800 Mesh WiFi: backhaul instabile, client bloccati nello stato di autenticazione e traffico non trasmesso.

Un punto chiave è che il 90% degli errori mesh segnalati non sono guasti hardware o client isolati, ma sintomi di mancata corrispondenza tra lo stato del control-plane e del data-plane, topologia mesh instabile o progettazione RF non ottimale.

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).