

Informazioni sui debug wireless e sulla raccolta di registri sui controller LAN wireless Catalyst 9800

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Flusso di pacchetti all'interno di 9800 WLC](#)

[Control Plane Tracing](#)

[Syslog](#)

[Traccia sempre attiva](#)

[Trace-on-Failure](#)

[Debug condizionale e traccia RadioActive](#)

[Tracce radioattive tramite interfaccia utente Web](#)

[Tracce radioattive tramite CLI](#)

[Debug non condizionale per processo](#)

[Traccia pacchetti Data Plane](#)

[Embedded Packet Capture](#)

[LED di allarme e allarmi della piattaforma critica](#)

Introduzione

Questo documento descrive e fornisce una panoramica di tutte le funzionalità e le caratteristiche di Cisco IOS® XE utilizzate per la risoluzione dei problemi di Catalyst 9800.

Prerequisiti

Requisiti

- Conoscenze base dei Wireless LAN Controller (WLC).
- Conoscenze base dei flussi di casi d'uso coinvolti nell'uso di un WLC.

Componenti usati

Questo documento riguarda i controller 9800-CL, 9800-L, 9800-40 e 9800-80. È basato principalmente sulla versione 17.3 di Cisco IOS® XE.

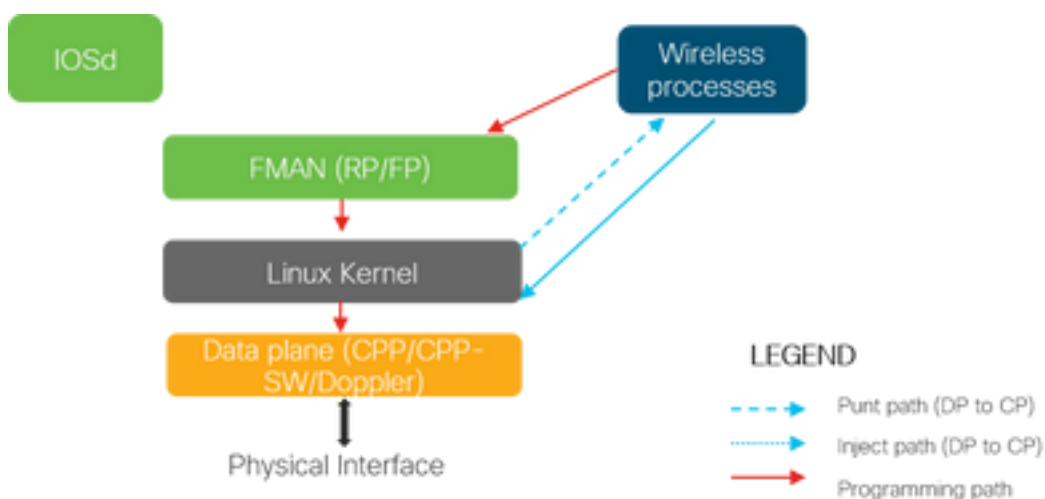
Premesse

Cisco IOS® XE su 9800 WLC è costituito essenzialmente da un kernel Linux (binOS) con Cisco IOS® e da tutti i processi wireless implementati come daemon. Tutti i daemon di processo possono essere raggruppati sotto il termine generico Control Plane (CP) e sono responsabili del controllo e del provisioning dei punti di accesso (CAPWAP), della mobilità, della gestione delle risorse radio (RRM). Rogue Management, Network Mobility Service Protocol (NMSP) destinati a e da 9800 WLC.

Il Data Plane (DP) si riferisce ai componenti che inoltrano i dati su 9800 WLC.

Su tutte le iterazioni di 9800 (9800-40, 9800-80, 9800-CL, 9800-SW,9800-L), Control Plane rimane piuttosto comune. Tuttavia, Data Plane varia con 9800-40 e 9800-80 che utilizzano un complesso QFP (Quantum Flow Processor) hardware simile ad ASR1k, mentre 9800-CL e 9800-L utilizzano l'implementazione software di Cisco Packet Processor (CPP). 9800-SW utilizza semplicemente il chipset Doppler sugli switch Catalyst serie 9k per l'inoltro dei dati.

Flusso di pacchetti all'interno di 9800 WLC



Quando un pacchetto entra nel WLC 9800 da porte fisiche, se viene determinato che controlla il traffico, viene puntato ai corrispondenti processi del Control Plane. Per un join AP, si tratta di tutti gli scambi capwap e dtl originati da AP. In caso di aggiunta client, si tratterebbe di tutto il traffico proveniente dal client fino a quando il client non passa allo stato RUN e seguirebbe il percorso PUNT.

Quando i vari daemon elaborano il traffico in entrata, il traffico di ritorno risultante (risposta capwap, dot11, dot1x, risposta dcp) proveniente dalla rete 9800 WLC e inviato al client viene iniettato nuovamente nel piano dati per essere inviato alla porta fisica. Durante l'elaborazione di join AP, join client, scambi di mobilità, data plane deve essere programmato in modo da gestire l'inoltro del traffico di dati. Ciò si verifica con più componenti programmati in sequenza sul percorso di programmazione indicato nell'immagine.

Cisco IOS® XE fornisce un versatile set di strumenti per tracciare il pacchetto dal momento in cui entra nel WLC del 9800 fino a quando il traffico elaborato non esce dalla scatola. La sezione successiva presenta questi strumenti insieme ai comandi utilizzati per richiamarli dall'interfaccia della riga di comando (CLI).

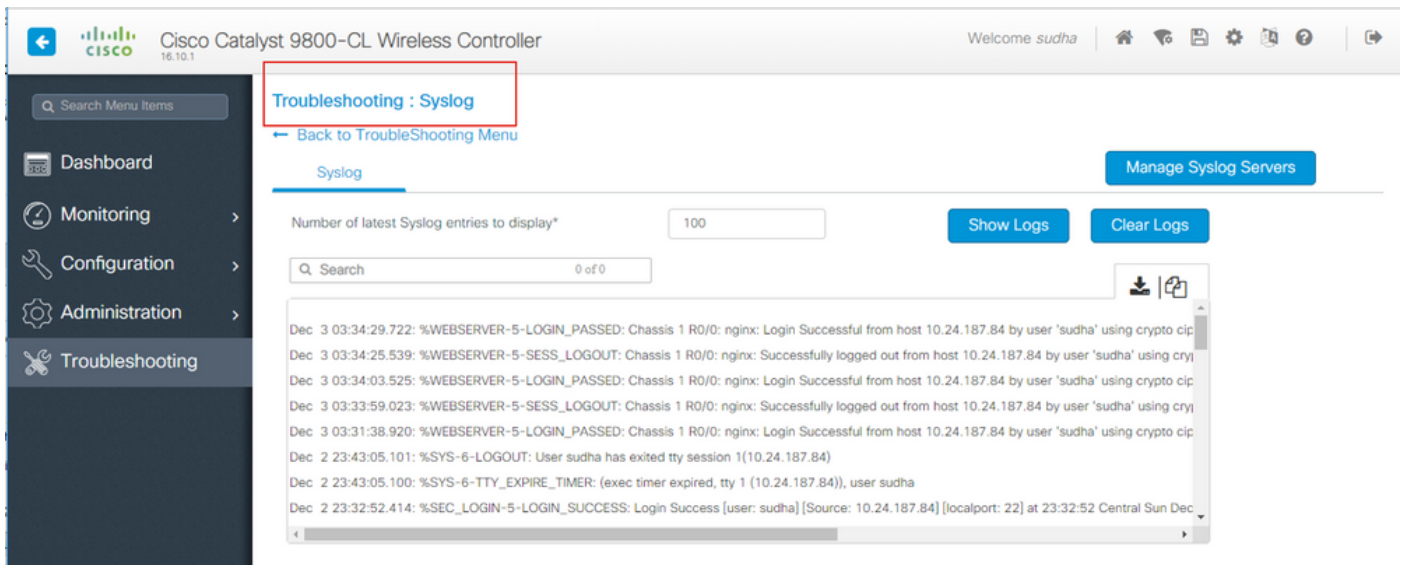
Control Plane Tracing

In questa sezione vengono descritti i comandi e gli strumenti disponibili per visualizzare

l'elaborazione eseguita dai processi del control plane dopo che il pacchetto destinato al WLC 9800 è stato puntato dal DP o prima di inserire il pacchetto di risposta inviato dal WLC 9800 al DP per inviare l'interfaccia fisica

Syslog

I log generati dal WLC 9800 sono il primo mezzo per verificare lo stato generale del sistema. Qualsiasi violazione della soglia predefinita per le risorse di sistema come CPU, memoria e buffer viene segnalata nel registro. Inoltre, qualsiasi errore generato da qualsiasi sottosistema viene scritto nei log. Per visualizzare i log, selezionare **Risoluzione dei problemi > Syslog**



The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. The top navigation bar includes the Cisco logo, the device name 'Cisco Catalyst 9800-CL Wireless Controller', and the user 'Welcome sudha'. The left sidebar contains a search bar and a menu with items: Dashboard, Monitoring, Configuration, Administration, and Troubleshooting. The 'Troubleshooting' menu item is highlighted. The main content area is titled 'Troubleshooting : Syslog' and includes a 'Back to Troubleshooting Menu' link. Below this, there are controls for 'Number of latest Syslog entries to display' (set to 100), 'Show Logs', and 'Clear Logs' buttons. A search bar is also present. The log entries are displayed in a scrollable area, showing various system events such as successful logins and session timeouts for user 'sudha'.

o eseguire il comando CLI:

```
# show logging
```

Questo output mostra i log generali e alcuni log specifici del wireless. Tuttavia, a differenza del precedente Cisco IOS®, in genere nessun debug wireless viene indirizzato a questo output di registrazione.

Nota: Se WLC9800 è configurato per reindirizzare questi log a un server syslog esterno, è necessario controllare anche i log sul server syslog esterno.

Traccia sempre attiva

Ogni processo del control plane sul WLC9800 registra costantemente a livello di log di **Notice** al proprio buffer dedicato. Questo processo viene definito come analisi continua. Questa funzionalità esclusiva consente di ottenere dati contestuali su un errore che si è verificato senza imporre la riproduzione della condizione di errore.

Ad esempio, se si ha familiarità con AireOS, per qualsiasi risoluzione dei problemi di connettività dei client, è necessario abilitare i debug e riprodurre lo stato del problema di connettività dei client per identificare la causa principale. Grazie all'analisi sempre attiva, è possibile tornare alle tracce acquisite e identificare se si tratta della causa principale comune. A seconda del volume di log generati, possiamo guardare indietro da diverse ore a diversi giorni.

Ora, mentre le tracce vengono registrate per singolo processo, è possibile visualizzarle completamente per un particolare contesto di interesse come il mac client o il mac AP o l'indirizzo ip AP. A tale scopo, eseguire il comando

```
# show logging profile wireless filter mac to-file bootflash:
```

Per impostazione predefinita, questo comando torna indietro di soli 10 minuti per generare e decodificare i registri. Puoi scegliere di tornare indietro nel tempo con:

```
# show logging profile wireless start last
```

Per visualizzare i log per processo, eseguire il comando

```
# show logging process to-file bootflash:
```

Nota: Su queste CLI sono disponibili diverse opzioni di filtro, tra cui modulo, livello di log, timestamp di avvio e così via. Per visualizzare ed esplorare queste opzioni, eseguire il comando

```
# show logging profile wireless ?  
# show logging process ?
```

Trace-on-Failure

Per ottenere un'istantanea rapida delle condizioni di errore comunemente note, è disponibile la funzionalità di analisi degli errori. In questo modo vengono analizzate tutte le tracce del sistema in un determinato momento in modo che corrispondano alle condizioni di errore predefinite e vengono presentate la vista di riepilogo e le statistiche.

Per ottenere una visualizzazione di riepilogo, eseguire il comando

```
# show logging profile wireless trace-on-failure summary
```

Per visualizzare le condizioni di errore predefinite e le statistiche corrispondenti, eseguire il comando

```
# show wireless stats trace-on-failure
```

Una volta individuato l'errore, per raccogliere le tracce specifiche del contesto dell'errore, eseguire il comando

```
# show logging profile wireless filter uuid to-file bootflash:tof-FILENAME.txt
```

che possono essere visualizzati nella sessione terminale o esportati per l'analisi offline con i comandi

```
# more bootflash:tof-FILENAME.txt
```

OR

```
# copy bootflash:tof-FILENAME.txt { tftp: | ftp: | scp: | https: } tof-FILENAME.txt
```

Debug condizionale e traccia RadioActive

Il debug condizionale consente di abilitare la registrazione a livello di debug per funzionalità specifiche in base alle condizioni di interesse. RadioActive Trace fa un ulteriore passo avanti aggiungendo la possibilità di stampare in modo condizionale le informazioni di debug tra i processi, thread per le condizioni di interesse. Ciò significa che l'architettura sottostante è completamente astratta.

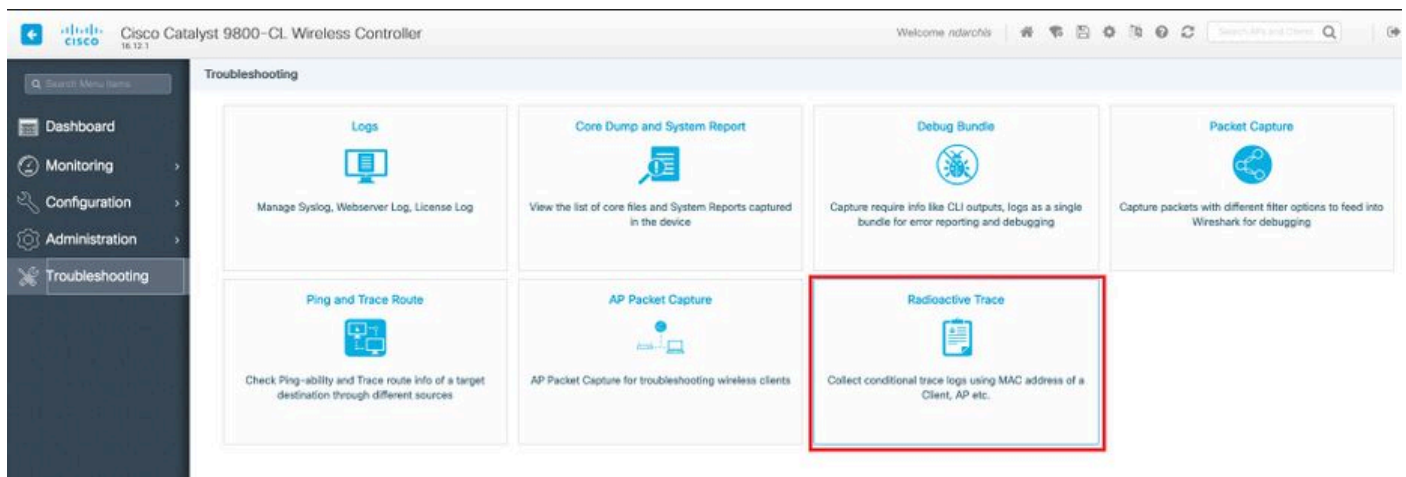
Nota: Nella versione 16.12, il tracciamento radioattivo è implementato solo per la risoluzione dei problemi di aggiunta dell'access point agli indirizzi MAC radio ed Ethernet dell'access point, aggiunta del client all'indirizzo MAC del client e problemi di mobilità con connettività IP peer e CMX mobile con l'indirizzo IP CMX come condizioni di interesse.

Nota: L'indirizzo MAC e l'indirizzo IP come condizione forniscono output diversi, in quanto processi diversi riconoscono identificatori diversi per la stessa entità di rete (punto di accesso o client o peer di mobilità).

Con la connettività del client, come esempio per la risoluzione dei problemi, viene eseguito il debug condizionale affinché la mac del client ottenga la vista end-to-end al control plane.

Tracce radioattive tramite interfaccia utente Web

Andare al menu della pagina **Risoluzione problemi** e scegliere **Traccia radioattiva**



Fare clic su **Add** (Aggiungi) e immettere l'indirizzo MAC del client o del punto di accesso che si desidera risolvere. A partire dalla versione 16.12, solo gli indirizzi mac possono essere aggiunti tramite la GUI. È possibile aggiungere l'indirizzo IP tramite la CLI.

Cisco Catalyst 9800-CL Wireless Controller
16.12.1

Troubleshooting > Radioactive Trace

← Back to Troubleshooting Menu

Conditional Debug Global State: **Stopped**

+ Add Delete Start Stop

MAC/IP Address	Trace file
<input type="checkbox"/> 1122.3344.5566	Generate

1 10 items per page 1 - 1 of 1 items

È possibile aggiungere diversi indirizzi MAC da registrare. Quando si è pronti per avviare la traccia radioattiva, fare clic su **start**.

Cisco Catalyst 9800-CL Wireless Controller
16.12.1

Troubleshooting > Radioactive Trace

← Back to Troubleshooting Menu

Conditional Debug Global State: **Stopped**

+ Add Delete Start Stop

MAC/IP Address	Trace file
<input type="checkbox"/> 1122.3344.5566	Generate

1 10 items per page 1 - 1 of 1 items

Una volta avviato, il log di debug viene scritto su disco in relazione a qualsiasi elaborazione del control plane correlata agli indirizzi MAC rilevati.

Dopo aver riprodotto il problema che si desidera risolvere, fare clic su **Stop**.

Cisco Catalyst 9800-CL Wireless Controller
16.12.1

Troubleshooting > Radioactive Trace

← Back to Troubleshooting Menu

Conditional Debug Global State: **Started**

+ Add Delete Start Stop

MAC/IP Address	Trace file
<input type="checkbox"/> 1122.3344.5566	Generate

1 10 items per page 1 - 1 of 1 items

Per ogni indirizzo MAC sottoposto a debug, è possibile generare un file di log che fascicola tutti i log relativi a tale indirizzo facendo clic su **Genera**.

Cisco Catalyst 9800-CL Wireless Controller
16.12.1

Troubleshooting > Radioactive Trace

← Back to Troubleshooting Menu

Conditional Debug Global State: **Stopped**

+ Add - Delete ✓ Start ■ Stop

MAC/IP Address	Trace file
<input type="checkbox"/> 1122.3344.5566	<input type="button" value="Generate"/>

10 items per page 1 - 1 of 1 items

Scegliere il periodo di tempo che deve trascorrere prima che il file di registro fascicolato passi e fare clic su **Applica al dispositivo**.

Enter time interval ✕


Generate logs for last

- 10 minutes
- 30 minutes
- 1 hour
- since last boot
-

È ora possibile scaricare il file facendo clic sull'icona accanto al nome del file. Questo file è presente nell'unità bootflash del controller e può anche essere copiato dalla CLI.

← Back to TroubleShooting Menu

Conditional Debug Global State: **Stopped**

	MAC/IP Address	Trace file	
<input type="checkbox"/>	1122.3344.5566	debugTrace_1122.3344.5566.txt 	<input type="button" value="▶ Generate"/>

items per page
 1 - 1 of 1 items

Tracce radioattive tramite CLI

Per abilitare il debug condizionale, eseguire il comando

```
# debug wireless {mac | ip} {aaaa.bbbb.cccc | x.x.x.x } {monitor-time} {N seconds}
```

Per visualizzare le condizioni attualmente attivate, eseguire il comando

```
# show debugging
```

Questi debug non stampano alcun output sulla sessione terminale, ma memorizzano il file di output del debug in modo che venga richiamato e analizzato dopo il debug. Il file viene salvato con la convenzione di denominazione `ra_trace_*`

Ad esempio, per l'indirizzo mac `aaaa.bbbb.cccc`, il nome file generato è `ra_trace_MAC_aaaabbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log`

Uno dei vantaggi è che lo stesso comando può essere usato per risolvere i problemi di join AP (input AP radio mac e ethernet mac), problemi di connettività client (input client mac), problemi del tunnel di mobilità (input peer ip), problemi di roaming client (input client mac). In altre parole, non è necessario ricordare più comandi, quali `debug capwap`, `debug client`, `debug mobility` e così via.

Nota: `debug wireless` consente inoltre di puntare a un server FTP e di eseguire una registrazione ancora più dettagliata con la parola chiave `internal`. Non è consigliabile eseguire questa operazione in questo momento, poiché si stanno risolvendo alcuni problemi.

Per eseguire il debug del file di output nella sessione terminal, eseguire il comando

```
# more bootflash:ra_trace_MAC_*.log
```

Per reindirizzare l'output del comando debug a un server esterno per l'analisi offline, eseguire il comando

```
# copy bootflash:ra_trace_MAC_*.log
ftp://username:password@FTPSERVERIP/path/RATRACE_FILENAME.txt
```

È disponibile una visualizzazione molto più dettagliata degli stessi livelli del log di debug. per

visualizzare la visualizzazione dettagliata, eseguire il comando

```
# show logging profile wireless internal filter mac to-file
```

Per disattivare il debug per un contesto specifico o prima che l'ora del monitor configurata o predefinita sia attiva, eseguire il comando.

```
# no debug wireless mac <aaaa.bbbb.cccc>
```

Attenzione: Il debug condizionale abilita la registrazione a livello di debug che a sua volta aumenta il volume dei log generati. Se si lascia attiva questa opzione, si riduce il tempo di visualizzazione dei log. Si consiglia pertanto di disattivare sempre il debug al termine della sessione di risoluzione dei problemi.

Per disabilitare tutte le operazioni di debug, eseguire questi comandi

```
# clear platform condition all  
# undebug all
```

Debug non condizionale per processo

Per i casi di utilizzo e i processi non implementati per la traccia radioattiva, è possibile ottenere le tracce dei livelli di debug. Per impostare il livello di debug su un processo specifico, utilizzare il comando

```
# set platform software trace <PROCESS_NAME> wireless chassis active R0 { module_name | all-modules }
```

Per verificare i livelli di traccia dei vari moduli, eseguire il comando

```
# show platform software trace level <PROCESS_NAME> chassis active R0
```

Per visualizzare le tracce raccolte, eseguire il comando

```
# show logging process to-file
```

Traccia pacchetti Data Plane

Quando un pacchetto entra per la prima volta nel WLC 9800, si verificano alcune elaborazioni sul piano dati per identificare se il traffico è il piano di controllo o il piano dati. La funzione Packet-Trace offre una vista dettagliata dell'elaborazione Cisco IOS® XE eseguita sul piano dati e della decisione presa in merito all'invio, all'inoltro, al rifiuto o al consumo del pacchetto. Questa funzionalità della WLC 9800 funziona esattamente come l'implementazione di ASR1k.

Packet Tracer su 9800 WLC fornisce tre livelli di ispezione uguali a quelli di ASR1K.

- **Statistiche:** fornisce il conteggio dei pacchetti che entrano e escono dal processore di rete
- **Riepilogo-** Questa condizione viene raccolta per un numero finito di pacchetti che soddisfano una condizione di interesse specifica. L'output di riepilogo indica le interfacce in entrata ed in uscita, la decisione di ricerca effettuata dal piano dati e tiene traccia anche dei pacchetti punt, drop e inject, se presenti. Questo output fornisce una visualizzazione succinta

dell'elaborazione del piano dati

- Path Data (Dati di percorso): fornisce una vista più dettagliata della gestione dei pacchetti DP. Raccolto per un numero finito di pacchetti, include l'ID di debug condizionale che può essere utilizzato per correlare il pacchetto DP ai debug del piano di controllo, l'indicatore orario e dati di traccia del percorso specifici della funzionalità. Questa vista dettagliata presenta due funzionalità opzionali La funzione di copia dei pacchetti consente di copiare i pacchetti in entrata ed in uscita a vari livelli (layer 2, layer 3 e layer 4) Feature Invocation array (FIA) è l'elenco sequenziale di funzionalità eseguite sul pacchetto dal piano dati. Queste funzionalità sono derivate dalla configurazione predefinita e abilitata dall'utente sul WLC 9800

Per una spiegazione dettagliata della funzione e delle opzioni secondarie, fare riferimento alla [funzione Cisco IOS XE Datapath Packet Trace](#)

Per flussi di lavoro wireless quali l'aggiunta di un punto di accesso, la connettività dei client e così via, tracciare l'uplink in modo bidirezionale

Attenzione: Il tracer del pacchetto del dataplane analizza solo l'intestazione CAPWAP esterna. Pertanto, condizioni quali la mac client wireless non producono risultati utili.

Passaggio 1. Definire la condizione di interesse.

```
# debug platform condition { interface | mac | ingress | egress | both | ipv4 | ipv6 | mpls | match }
```

Avviso: Entrambi i comandi - debug platform condition e debug platform condition mac aaaa.bbb.ccc sono destinati alla traccia dei pacchetti del control plane e non restituiscono tracce dei pacchetti del dataplane.

Passaggio 2. Per visualizzare le condizioni attualmente attivate, eseguire il comando

```
# show platform conditions
```

Passaggio 3. Abilitare packet-tracer per un numero finito di pacchetti. Questo numero di pacchetto viene definito come una potenza di 2 nell'intervallo da 16 a 8192. Per impostazione predefinita, vengono acquisiti sia i dati di riepilogo che i dati delle funzionalità. Se si utilizza l'opzione secondaria solo riepilogo, è possibile scegliere di ottenere solo una visualizzazione di riepilogo. Sono inoltre disponibili opzioni secondarie per ottenere la traccia via, definire le dimensioni del pacchetto in byte, il puntino di traccia, inserire o rilasciare pacchetti. e così via.

```
# debug platform packet-tracer packet <packet-number> {fia-trace}
```

Passaggio 4. (Facoltativo) È possibile copiare ed eseguire il dump dei pacchetti durante la traccia

```
# debug platform packet-trace copy packet both size 2048 { 12 | 13 | 14 }
```

Passaggio 5. Abilitare il debug condizionale.

```
# debug platform condition start
```

Passaggio 6. Per verificare se il pacchetto di traccia sta raccogliendo output, verificare le

statistiche

```
# show platform packet-trace statistics
```

Passaggio 7. Per visualizzare l'output del comando packet-trace, eseguire il comando

```
# show platform packet-tracer summary
```

Passaggio 8. (Facoltativo) È possibile esportare il dump del pacchetto per l'analisi offline con Cisco TAC

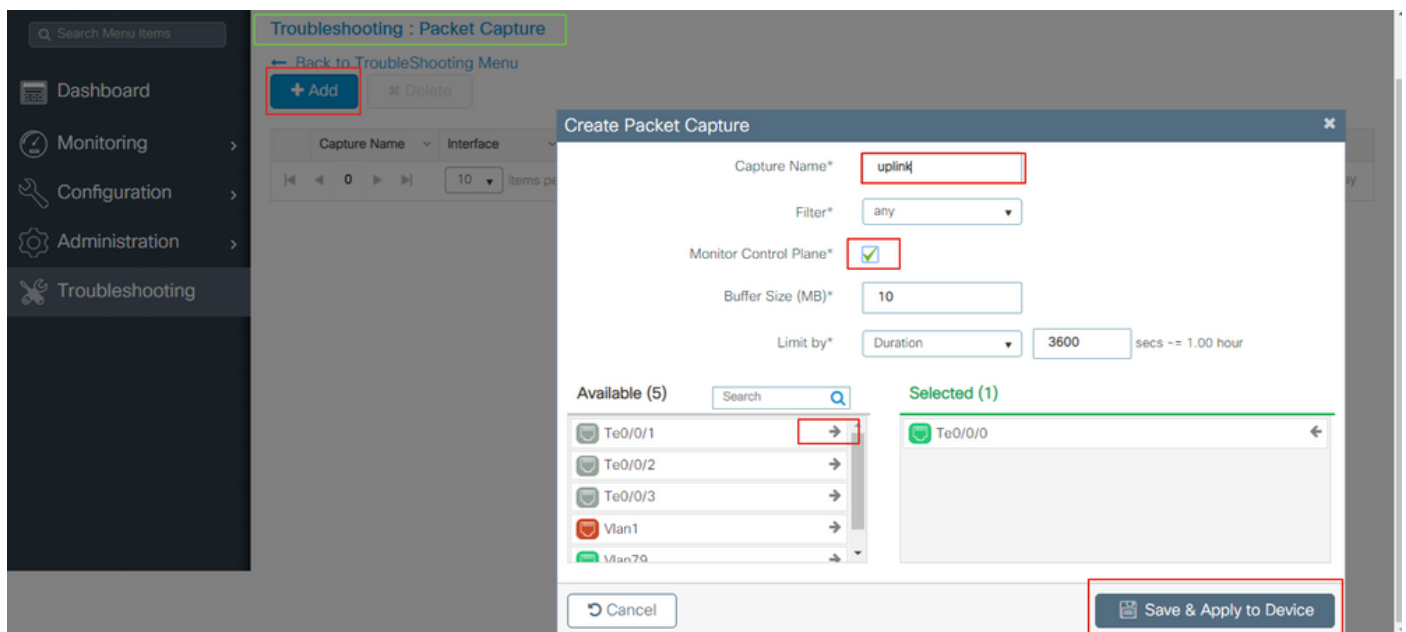
```
# show platform packet-trace packet all | redirect { bootflash: | tftp: | ftp: } pacrac.txt
```

Embedded Packet Capture

Embedded Packet Capture (EPC) è una funzione di acquisizione dei pacchetti che consente di visualizzare i pacchetti destinati a, originati e passanti per i WLC Catalyst 9800. Queste clip possono essere esportate per l'analisi offline con Wireshark. Per ulteriori informazioni su questa funzione, consultare la [guida alla configurazione EPC](#)

Rispetto ad AireOS, invece di affidarsi alle funzionalità di acquisizione dei pacchetti e mirroring del traffico sullo switch uplink, 9800 WLC consente l'acquisizione delle pcap sulla confezione stessa. Sul modello 9800, questa acquisizione può essere configurata sia dall'interfaccia della riga di comando (CLI) sia dall'interfaccia grafica (GUI).

Per eseguire la configurazione tramite GUI, selezionare **Risoluzione dei problemi > Packet Capture > +Add**



Passaggio 1. Definire il nome dell'acquisizione del pacchetto. È consentito un massimo di 8 caratteri.

Passaggio 2. Definire gli eventuali filtri

Passaggio 3. Selezionare la casella per monitorare il traffico se si desidera visualizzare il traffico puntato alla CPU del sistema e inserito nuovamente nel piano dati

Passaggio 4. Definire le dimensioni del buffer. È consentito un massimo di 100 MB

Passaggio 5. Definire il limite, in base alla durata, per un intervallo da 1 a 1000000 secondi, o in base al numero di pacchetti, per un intervallo da 1 a 100000 pacchetti, in base alle esigenze

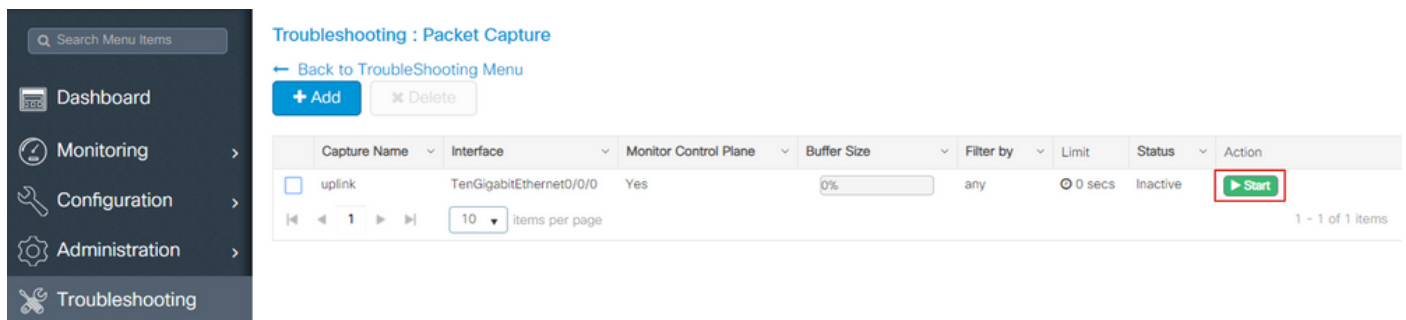
Passaggio 6. Scegliere l'interfaccia dall'elenco di interfacce nella colonna sinistra e selezionare la freccia per spostarla nella colonna destra

Passaggio 7. **Salvataggio e applicazione al dispositivo**

Passaggio 8. Per avviare l'acquisizione, selezionare **Start**

Passaggio 9. È possibile eseguire l'acquisizione fino al limite definito. Per interrompere manualmente la cattura, selezionare **Interrompi**.

Passaggio 10. Una volta arrestato, un pulsante **Esporta** diventa disponibile per fare clic con l'opzione per scaricare il file di acquisizione (.pcap) sul desktop locale tramite server https o TFTP o server FTP o disco rigido o flash del sistema locale.



Nota: CLI offre una maggiore granularità di opzioni quali Limit by. La GUI è sufficiente per acquisire i pacchetti per gli usi più comuni.

Per configurare tramite CLI:

Creare l'acquisizione del monitor:

```
monitor capture uplink interface <uplink_of_the_9800> both
```

Associare un filtro. È possibile specificare il filtro in linea oppure fare riferimento a un ACL o a una mappa di classe.

Nell'esempio, è l'ACL a far corrispondere il traffico tra i due indirizzi ip del router 9800 e un altro WLC 5520. Scenario tipico per la risoluzione dei problemi di mobilità:

```
conf t
```

```
ip access-list extended mobilitywlc  
permit ip host <5520_ip_address> host <9800_ip_address>  
    permit ip host <9800_ip_address> host <5520_ip_address>  
end
```

```
monitor capture uplink access-list mobilitywlc
```

Se si desidera che l'acquisizione venga eseguita in un buffer circolare, si dispone del tempo

necessario per rilevare il problema, quindi arrestare l'acquisizione e salvarla.

Se ad esempio si imposta il buffer a 50 MB. Sono necessari al massimo 50 MB di disco sul modello 9800 e le sue dimensioni relativamente grandi per acquisire diversi minuti di dati nella speranza che il problema si verifichi.

```
monitor capture uplink buffer circular size 50
```

Avviare la cattura. È possibile accedervi dalla GUI o dalla CLI:

```
monitor capture uplink start
```

La cattura è ora attiva.

Consentire la raccolta dei dati necessari.

Interrompere la cattura. È possibile farlo tramite GUI o CLI:

```
monitor capture uplink stop
```

È possibile recuperare l'acquisizione dalla GUI > Risoluzione dei problemi > Acquisizione pacchetto > Esporta.

Oppure caricarlo su un server dalla CLI. Esempio via ftp:

```
monitor capture uplink export ftp://x.x.x.x/MobilityCAP.pcap
```

Una volta raccolti i dati necessari, rimuovere l'acquisizione:

```
no monitor capture uplink
```

LED di allarme e allarmi della piattaforma critica

Tutti gli accessori 9800 (9800-L, 9800-40 e 9800-80) sono dotati di un LED ALM sul pannello anteriore. Se il LED diventa rosso significa che sulla piattaforma è presente un allarme critico.

È possibile verificare gli allarmi che causano il rosso del LED con il comando **show facility-alarm status**

```
WLC#show facility-alarm status
```

```
System Totals Critical: 2 Major: 0 Minor: 0
```

Source	Time	Severity	Description [Index]
-----	-----	-----	-----
TenGigabitEthernet0/1/0	Jul 26 2019 15:14:04	CRITICAL	Physical Port Link Down [1]
TenGigabitEthernet0/1/1	Jul 26 2019 15:14:04	CRITICAL	Physical Port Link Down [1]

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).