

Wireless-Fehlerbehebungen und Protokollierung auf Catalyst 9800 Wireless LAN Controllern

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Paketfluss im 9800 WLC](#)

[Verfolgung auf Kontrollebene](#)

[Syslog](#)

[Stets verfügbare Ablaufverfolgung](#)

[Trace-on-Failure](#)

[Bedingtes Debuggen und RadioActive-Ablaufverfolgung](#)

[Radioaktive Spuren über Web-UI](#)

[Radioaktive Spuren über CLI](#)

[Nicht bedingtes prozessbasiertes Debuggen](#)

[Paketverfolgung auf Datenebene](#)

[Integrierte Paketerfassung](#)

[Alarm-LED und Alarm bei kritischer Plattform](#)

Einleitung

In diesem Dokument werden alle Funktionen und Leistungsmerkmale von Cisco IOS® XE zur Fehlerbehebung bei Catalyst 9800 beschrieben und beschrieben.

Voraussetzungen

Anforderungen

- Grundkenntnisse der Wireless LAN Controller (WLC).
- Grundkenntnisse der an der Nutzung eines WLC beteiligten Anwendungsfälle

Verwendete Komponenten

Dieses Dokument umfasst die Controller 9800-CL, 9800-L, 9800-40 und 9800-80. Es basiert hauptsächlich auf der Version 17.3 von Cisco IOS® XE.

Hintergrundinformationen

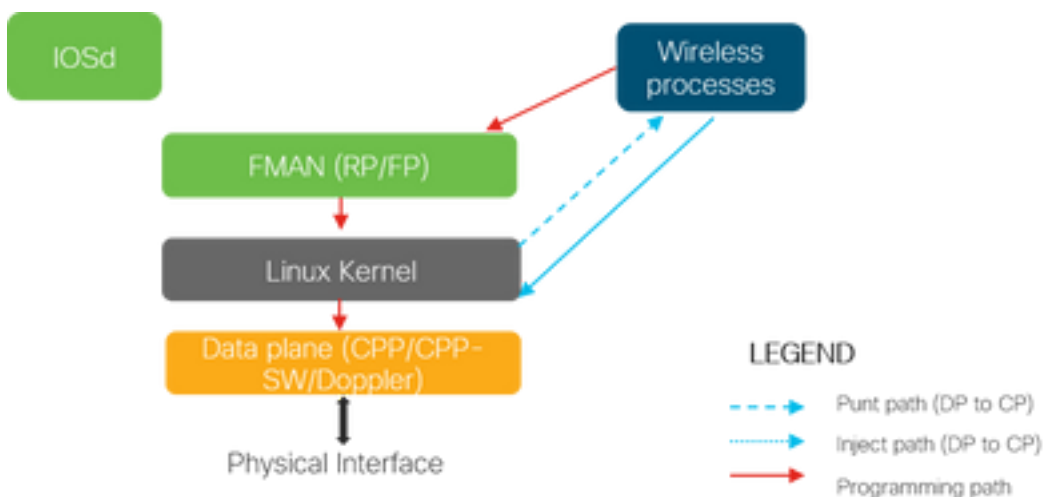
Cisco IOS® XE auf 9800 WLCs besteht im Wesentlichen aus einem Linux-Kernel (binOS) mit

Cisco IOS® und allen Wireless-Prozessen, die als Daemons implementiert sind. Alle Prozess-Daemons können unter dem Oberbegriff Control Plane (CP) gebündelt werden und sind für Control and Provisioning of Access Points (CAPWAP), Mobility, Radio Resource Management (RRM) zuständig. Rogue Management, Network Mobility Service Protocol (NMSRP), die für und vom 9800 WLC bestimmt sind.

Datenebene (DP) bezieht sich auf die Komponenten, die Daten des 9800 WLC weiterleiten.

Bei allen Iterationen von 9800 (9800-40, 9800-80, 9800-CL, 9800-SW, 9800-L) bleibt die Kontrollebene recht häufig. Die Datenebene variiert jedoch je nach den Standards 9800-40 und 9800-80, die einen Hardware-Quantum Flow-Prozessor (QFP) verwenden, der dem ASR1k ähnlich ist, während 9800-CL und 9800-L die Implementierung von Cisco Packet Processor (CPP) verwenden. 9800-SW nutzt einfach den Doppler Chipsatz auf Catalyst Switches der Serie 9k für die Datenweiterleitung.

Paketfluss im 9800 WLC



Wenn ein Paket über physische Ports in den 9800 WLC eingeht und als Kontrolldatenverkehr erkannt wird, wird es an die entsprechenden Kontrollebenenprozesse gesendet. Bei einem AP-Beitritt sind dies alle vom AP stammenden CAPWAP- und DTLS-Austauschvorgänge. Im Fall einer Client-Verbindung entspricht dies dem gesamten Datenverkehr, der vom Client stammt, bis der Client in den RUN-Status wechselt und dem PUNT-Pfad folgt.

Während die verschiedenen Daemons den eingehenden Datenverkehr verarbeiten, wird der resultierende Rückverkehr (Capwap-Antwort, dot11, dot1x, dcp-Antwort) von 9800 WLC, der an den Client gesendet werden soll, zurück in die Datenebene injiziert, um vom physischen Port gesendet zu werden. Bei der Verarbeitung von AP-Joins, Client-Joins, Mobilitätsaustauschs muss die Datenebene programmiert werden, damit sie die Weiterleitung des Datenverkehrs verarbeiten kann. Dies geschieht, indem mehrere Komponenten sequenziell über den im Bild angegebenen Programmierpfad programmiert werden.

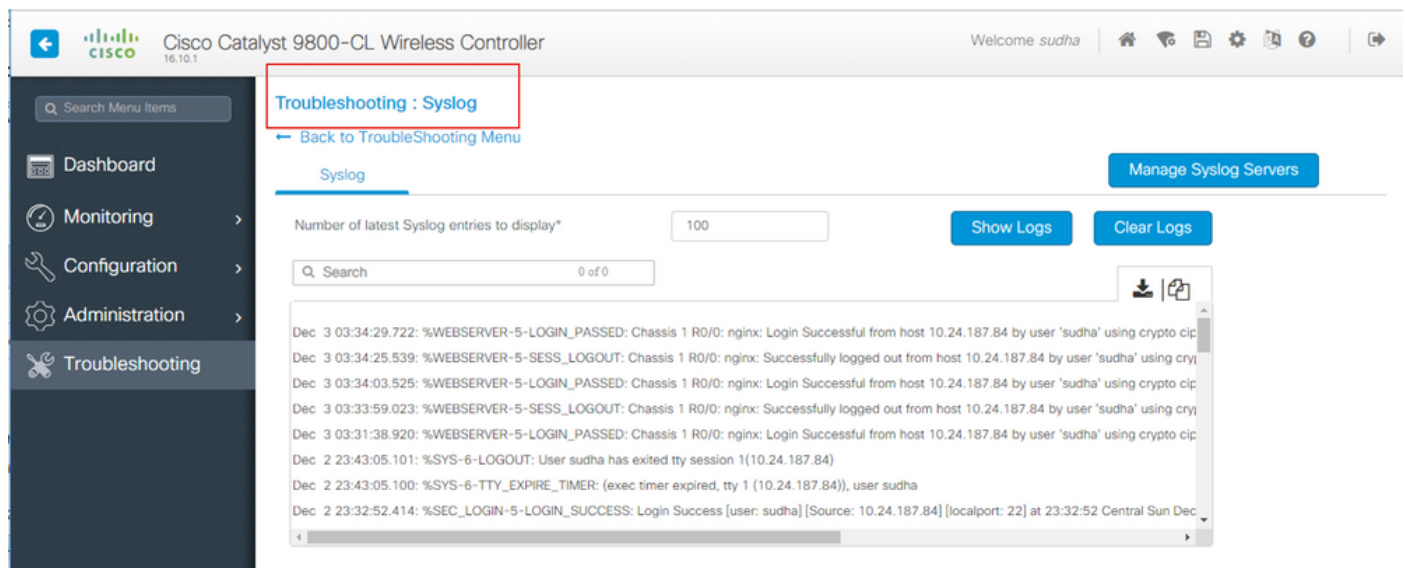
Cisco IOS® XE bietet ein vielseitiges Tool-Set, mit dem das Paket vom Eingang beim 9800 WLC bis zum Verlassen des Pakets verfolgt werden kann. Im nächsten Abschnitt werden diese Tools zusammen mit den Befehlen vorgestellt, die zum Aufrufen dieser Tools über die Kommandozeile (CLI) verwendet werden.

Verfolgung auf Kontrollebene

In diesem Abschnitt werden die verfügbaren Befehle und Tools beschrieben, mit denen die Verarbeitung durch die Prozesse auf der Steuerungsebene angezeigt werden kann, nachdem das für den 9800 WLC bestimmte Paket vom DP durchsucht wurde oder bevor das Antwortpaket vom 9800 WLC zum DP eingespeist wird, um die physische Schnittstelle zu senden.

Syslog

Die vom 9800 WLC generierten Protokolle sind das erste Mittel zur Überprüfung des allgemeinen Systemzustands. Jeder Verstoß gegen den vordefinierten Grenzwert für Systemressourcen wie CPU, Speicher und Puffer wird in das Protokoll aufgenommen. Außerdem werden alle Fehler, die von Subsystemen generiert werden, in Protokolle geschrieben. Um die Protokolle anzuzeigen, navigieren Sie zu **Troubleshooting > Syslog (Fehlerbehebung > Syslog)**.



oder führen Sie den CLI-Befehl aus:

```
# show logging
```

Diese Ausgabe zeigt allgemeine Protokolle sowie einige Wireless-spezifische Protokolle an. Im Gegensatz zu Cisco IOS® wird bei der Protokollierung jedoch in der Regel kein Wireless-Debugging durchgeführt.

Anmerkung: Wenn der WLC9800 so konfiguriert ist, dass diese Protokolle an einen externen Syslog-Server umgeleitet werden, müssen Sie auch die Protokolle auf dem externen Syslog-Server überprüfen.

Stets verfügbare Ablaufverfolgung

Jeder Prozess auf der Kontrollebene des WLC9800 protokolliert fortlaufend die Protokollierungsebene von **Notice** an seinen eigenen dedizierten Puffer. Dies wird als Always-On-Tracing bezeichnet. Dies ist eine einzigartige Funktion, mit der Sie kontextbezogene Daten zu einem aufgetretenen Fehler abrufen können, ohne dass die Fehlerbedingung reproduziert werden muss.

Wenn Sie z. B. mit AireOS vertraut sind, müssen Sie für die Behebung von Client-Verbindungsproblemen Debugs aktivieren und den Client-Verbindungsproblemstatus

reproduzieren, um die Ursache zu identifizieren. Mit der stets verfügbaren Ablaufverfolgung können Sie auf bereits erfasste Ablaufverfolgungen zurückblicken und feststellen, ob es sich um eine gemeinsame Ursache handelt. Je nach Umfang der generierten Protokolle können wir mehrere Stunden bis mehrere Tage zurückblicken.

Nun, während die Traces pro individuellem Prozess protokolliert werden, ist es möglich, sie ganzheitlich für einen bestimmten Kontext von Interesse wie Client-MAC oder AP-MAC oder AP-IP-Adresse zu betrachten. Führen Sie dazu den Befehl

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

Standardmäßig geht dieser Befehl nur 10 Minuten zurück, um die Protokolle zu generieren und zu dekodieren. Sie können wählen, weiter zurück in der Zeit mit:

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

Führen Sie den folgenden Befehl aus, um prozessspezifische Protokolle anzuzeigen:

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

Anmerkung: Für diese CLIs stehen mehrere Filteroptionen zur Verfügung, darunter Modul, Protokollierungsebene, Start-Zeitstempel usw. Um diese Optionen anzuzeigen und zu erkunden, führen Sie den Befehl

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

```
# show logging process ?
```

Trace-on-Failure

Um eine schnelle Momentaufnahme der bekannten Fehlerbedingungen zu erhalten, steht eine Funktion zum Nachverfolgen bei Fehlern zur Verfügung. Dadurch werden alle Traces im System zu einem bestimmten Zeitpunkt analysiert, um die vordefinierten Fehlerbedingungen zu erfüllen. Außerdem werden eine Übersicht sowie Statistiken angezeigt.

Führen Sie den Befehl

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

Führen Sie den Befehl aus, um die vordefinierten Fehlerbedingungen sowie Statistiken zu diesen Bedingungen anzuzeigen.

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

Wenn Sie den Fehler kennen und spezifische Ablaufverfolgungen für den Kontext des Fehlers sammeln möchten, führen Sie den Befehl

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

Diese können in einer Terminalsitzung angezeigt oder zur Offline-Analyse mithilfe der Befehle exportiert werden.

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

Bedingtes Debuggen und RadioActive-Ablaufverfolgung

Bedingtes Debuggen ermöglicht es, die Protokollierung der Debugebene für bestimmte Features für die gewünschten Bedingungen zu aktivieren. Die RadioActive-Ablaufverfolgung geht noch einen Schritt weiter, indem sie die Möglichkeit hinzufügt, Debuginformationen bedingt über Prozesse und Threads hinweg für die interessierende Bedingung zu drucken. Die zugrunde liegende Architektur ist also vollständig abstrahiert.

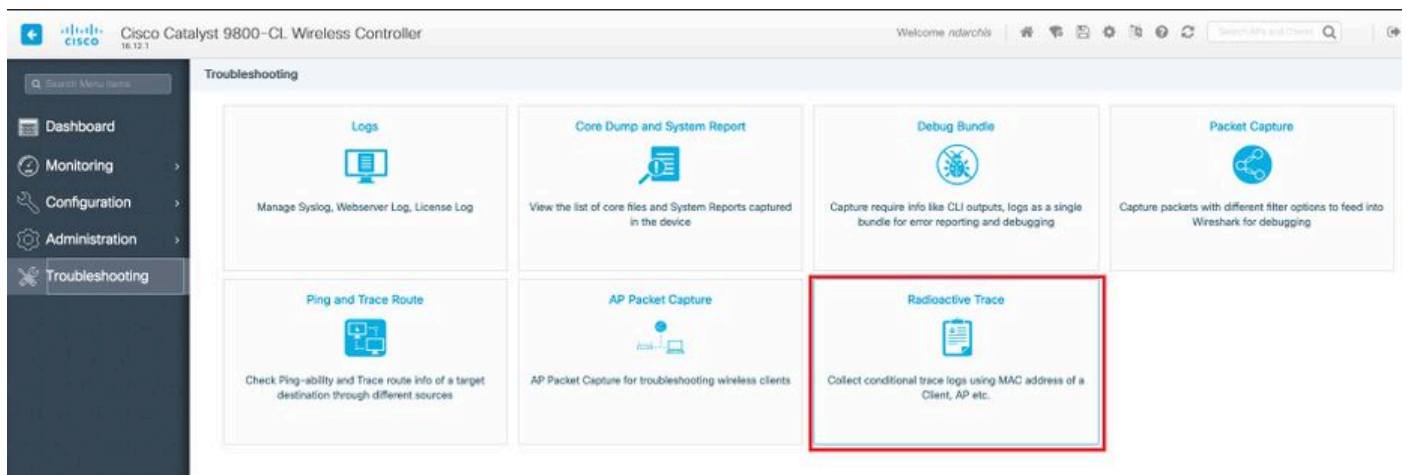
Anmerkung: Am 16.12.2012 wird die radioaktive Nachverfolgung nur für die Fehlerbehebung von AP-Joins mit AP-Funk- und Ethernet-MAC-Adressen, Client-Joins mit Client-MAC-Adressen sowie von Mobilitätsproblemen mit Mobility-Peer-IP- und CMX-Verbindungen mit der CMX-IP-Adresse implementiert.

Anmerkung: Die MAC-Adresse und die IP-Adresse als Bedingung liefern unterschiedliche Ausgänge, da verschiedene Prozesse unterschiedliche Bezeichner für dieselbe Netzwerkeinheit (Access Point, Client oder Mobility Peer) erkennen.

Bei der Client-Konnektivität als Beispiel für die Fehlerbehebung wird bedingtes Debugging ausgeführt, damit die Client-MAC eine End-to-End-Ansicht auf der Kontrollebene erhält.

Radioaktive Spuren über Web-UI

Öffnen Sie das Menü **Fehlerbehebung**, und wählen Sie **Radioactive Tracing** aus.



Klicken Sie auf **Hinzufügen**, und geben Sie eine Client- oder AP-MAC-Adresse ein, die Sie beheben möchten. Ab 16.12 können über die GUI nur noch MAC-Adressen hinzugefügt werden. Sie können die IP-Adresse über die CLI hinzufügen.

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

10 items per page 1 - 1 of 1 items

Sie können mehrere MAC-Adressen zum Verfolgen hinzufügen. Wenn Sie bereit sind, die radioaktive Verfolgung zu starten, klicken Sie auf **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

10 items per page 1 - 1 of 1 items

Nach dem Start werden die Debug-Protokolle über die Verarbeitung der verfolgten MAC-Adressen auf die Festplatte geschrieben.

Wenn Sie das Problem reproduziert haben, das Sie beheben möchten, klicken Sie auf **Beenden**.

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

10 items per page 1 - 1 of 1 items

Für jede debuggte MAC-Adresse können Sie eine Protokolldatei erstellen, in der alle Protokolle zu dieser MAC-Adresse aufgelistet sind. Klicken Sie dazu auf **Generate (Generieren)**.

← 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

Wählen Sie aus, wie lange die sortierte Protokolldatei zurückgehen soll, und klicken Sie auf **Auf Gerät anwenden**.

Enter time interval ✕


Generate logs for last

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

Sie können die Datei jetzt herunterladen, indem Sie auf das kleine Symbol neben dem Dateinamen klicken. Diese Datei befindet sich im Bootflash-Laufwerk des Controllers und kann auch über die CLI kopiert werden.

← 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

Radioaktive Spuren über CLI

Um das bedingte Debuggen zu aktivieren, führen Sie den Befehl

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

Um die aktuell aktivierten Bedingungen anzuzeigen, führen Sie den Befehl

```
# show debugging
```

Bei diesen Debugs wird keine Ausgabe in einer Terminalsitzung ausgegeben, sondern die Debugausgabedatei wird als Flash-Datei gespeichert, die anschließend abgerufen und analysiert werden kann. Die Datei wird mit der Namenskonvention ra_trace_* gespeichert

Für die MAC-Adresse aaaa.bbb.cccc lautet der generierte Dateiname z. B.
ra_trace_MAC_aaabbccccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

Ein Vorteil besteht darin, dass der gleiche Befehl zur Behebung von AP-Join-Problemen (Input-AP-Funk-MAC und Ethernet-MAC), Client-Verbindungsproblemen (Input-Client-MAC), Mobility-Tunnel-Problemen (Input-Peer-IP) und Client-Roaming-Problemen (Input-Client-MAC) verwendet werden kann. Mit anderen Worten, Sie müssen sich nicht mehrere Befehle wie debug capwap, debug client, debug mobility und so weiter merken.

Anmerkung: debug wireless ermöglicht auch den Verweis auf einen FTP-Server und die Ausführung noch ausführlicherer Protokollierung mit internem Schlüsselwort. Wir empfehlen diese derzeit nicht, da einige Probleme ausgeräumt werden müssen.

Um die Ausgabedatei in einer Terminalsitzung zu debuggen, führen Sie den Befehl

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

Um die Debugausgabe zur Offlineanalyse an einen externen Server umzuleiten, führen Sie den Befehl

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


Es gibt eine viel ausführlichere Ansicht derselben Debug-Protokollstufen. Um diese ausführliche Ansicht anzuzeigen, führen Sie den Befehl

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

Führen Sie den Befehl aus, um das Debuggen für bestimmte Kontexte oder vor Ablauf der konfigurierten oder standardmäßigen Überwachungszeit zu deaktivieren.

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

Vorsicht: Das bedingte Debugging ermöglicht die Protokollierung des Debugging-Levels, wodurch sich wiederum die Menge der generierten Protokolle erhöht. Wenn Sie diese Option nicht ausführen, wird der Zeitaufwand für das Anzeigen von Protokollen reduziert. Daher wird empfohlen, das Debuggen immer am Ende der Fehlerbehebungssitzung zu deaktivieren.

Um das Debuggen vollständig zu deaktivieren, führen Sie diese Befehle aus

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

Nicht bedingtes prozessbasiertes Debuggen

Für die Anwendungsfälle und Prozesse, die nicht für die radioaktive Nachverfolgung implementiert sind, können Sie Ablaufverfolgungen auf Debugebene abrufen. Um die Debugging-Ebene für einen bestimmten Prozess festzulegen, verwenden Sie den Befehl

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

Führen Sie den Befehl aus, um die Ablaufverfolgungsebenen der verschiedenen Module zu überprüfen.

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

Um die gesammelten Ablaufverfolgungen anzuzeigen, führen Sie den Befehl

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

Paketverfolgung auf Datenebene

Wenn ein Paket erstmals über den 9800 WLC eingeht, findet eine Verarbeitung auf Datenebene statt, um zu identifizieren, ob es sich bei dem Datenverkehr um die Kontroll- oder Datenebene handelt. Die Packet-Trace-Funktion bietet eine detaillierte Ansicht dieser Cisco IOS® XE-Verarbeitung auf dem Datenflugzeug sowie der Entscheidung, ob ein Paket gelenkt, weitergeleitet, verworfen oder verbraucht werden soll. Diese Funktion auf dem WLC 9800 funktioniert genauso wie die Implementierung auf dem ASR!k.

Packet Tracer auf dem 9800 WLC bietet drei Prüfungsebenen, die mit ASR1K identisch sind.

- Statistik - Zählt Pakete, die in den Netzwerkprozessor eintreten und diesen verlassen

- Zusammenfassung- Diese wird für eine begrenzte Anzahl von Paketen gesammelt, die spezifischen Bedingungen von Interesse entsprechen. Die zusammengefasste Ausgabe zeigt die Eingangs- und Ausgangsschnittstellen, die auf Datenebene getroffenen Nachschlageentscheidungen sowie die Verfolgung von Punt-, Drop- und Injection-Paketen an, falls vorhanden. Diese Ausgabe bietet eine prägnante Ansicht der Datenebenenverarbeitung.
- Path Data (Pfaddaten) - Diese Funktion bietet die detaillierteste Ansicht der DP-Paketverarbeitung. Sie wird für eine begrenzte Anzahl von Paketen gesammelt und enthält eine bedingte Debugging-ID, die verwendet werden kann, um DP-Pakete mit Debugging-Prozessen auf der Kontrollebene, Zeitstempel und funktionspezifische Pfadverfolgungsdaten zu korrelieren. Diese Detailansicht verfügt über zwei optionale Funktionen Paketkopie ermöglicht das Kopieren von Eingangs- und Ausgangspaketen auf verschiedenen Paketschichten (Layer 2, Layer 3 und Layer 4). Feature Invocation Array (FIA) ist die sequenzielle Liste von Funktionen, die auf dem Paket von der Datenebene ausgeführt werden. Diese Funktionen stammen aus der standardmäßigen und benutzerdefinierten Konfiguration des WLC 9800.

Eine detaillierte Beschreibung der Funktion und der Unteroptionen finden Sie unter Cisco [IOS XE Datapath Packet Trace Feature](#)

Bei Wireless-Workflows wie der AP-Verbindung, der Client-Verbindung usw. wird der Uplink bidirektional verfolgt.

Vorsicht: Der dataplane Packet-Tracer parst nur den äußeren CAPWAP-Header. Bedingungen wie Wireless-Client-Mac liefern also keine nützliche Leistung.

Schritt 1: Definieren Sie die Zinsbedingung.

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

Warnung: Beide Befehle - debug platform condition feature sowie debug platform condition mac aaa.bbb.cccc - sind für die Ablaufverfolgung von Datenpaketen auf der Kontrollebene vorgesehen und geben keine Ablaufverfolgungen von Datenplänen zurück.

Schritt 2: Um die aktuell aktivierten Bedingungen anzuzeigen, führen Sie den Befehl

```
# show platform conditions
```

Schritt 3: Aktivieren Sie die Paketverfolgung für eine begrenzte Anzahl von Paketen. Diese Paketnummer wird als eine Potenz von 2 im Bereich von 16-8192 definiert. Standardmäßig werden sowohl die Zusammenfassung als auch die Funktionsdaten erfasst. Optional können Sie festlegen, dass nur eine Sammelansicht angezeigt wird, wenn Sie die Unteroption "Nur Zusammenfassung" verwenden. Sie haben auch Unteroptionen zum Abrufen von Fia Trace, zum Definieren der Paketgröße in Byte, zum Durchsuchen, Einschleusen oder Verwerfen von Paketen. usw.

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

Schritt 4: (Optional) Sie können die verfolgten Pakete kopieren und auslesen

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

Schritt 5: Aktivieren Sie das bedingte Debuggen.

```
# debug platform condition start
```

Schritt 6: Überprüfen Sie die Statistiken, um festzustellen, ob die Paketverfolgung eine Ausgabe erfasst.

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

Schritt 7: Führen Sie den Befehl aus, um die Ausgabe der Paketverfolgung anzuzeigen.

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

Schritt 8: (Optional) Sie können Packet Dump zur Offline-Analyse durch das Cisco TAC exportieren.

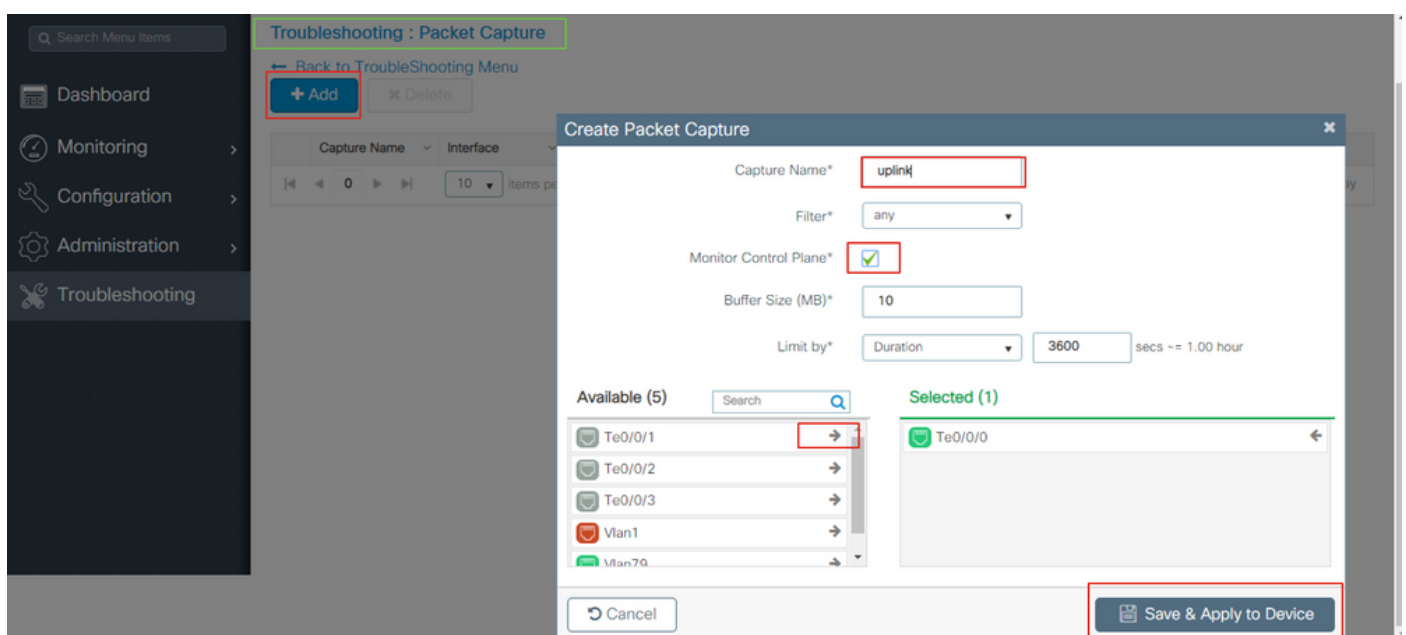
```
# show platform packet-trace packet all | redirect { bootflash: | tftp: | ftp: } pactrac.txt
```

Integrierte Paketerfassung

Embedded Packet Capture (EPC) ist eine Funktion zur Paketerfassung, mit der Pakete erfasst werden können, die an die Catalyst 9800 WLCs gerichtet sind, von diesen stammen und diese durchlaufen. Diese Aufzeichnungen können zur Offline-Analyse mit Wireshark exportiert werden. Weitere Einzelheiten zu dieser Funktion finden Sie im [EPC-Konfigurationsleitfaden](#).

Im Vergleich zu AireOS ermöglicht der 9800 WLC die Erfassung von Paketen und die Spiegelung des Datenverkehrs auf dem Uplink-Switch und nicht auf dem Gerät selbst. Auf dem 9800 kann diese Erfassung sowohl über die Befehlszeilenschnittstelle (CLI) als auch über die grafische Benutzeroberfläche (GUI) eingerichtet werden.

Um die Konfiguration über die GUI vorzunehmen, navigieren Sie zu **Troubleshooting > Packet Capture > +Add**.



Schritt 1: Definieren Sie den Namen der Paketerfassung. Es sind maximal 8 Zeichen zulässig.

Schritt 2. Definieren Sie ggf. Filter

Schritt 3: Aktivieren Sie das Kontrollkästchen Kontrollverkehr überwachen, wenn der Datenverkehr zur System-CPU geleitet und zurück in die Datenebene geleitet werden soll.

Schritt 4: Puffergröße definieren. Es sind maximal 100 MB zulässig.

Schritt 5. Definieren Sie eine Grenze, entweder nach Dauer, die einen Bereich von 1 - 1000000 Sekunden erlaubt, oder nach Anzahl der Pakete, die einen Bereich von 1 - 100000 Paketen erlauben, wie gewünscht

Schritt 6. Wählen Sie die Schnittstelle aus der Liste der Schnittstellen in der linken Spalte und wählen Sie den Pfeil, um sie in die rechte Spalte zu verschieben

Schritt 7: **Speichern und auf Gerät anwenden**

Schritt 8: Um die Erfassung zu starten, wählen Sie **Start**

Schritt 9: Sie können die Erfassung bis zum definierten Limit laufen lassen. Um die Erfassung manuell zu beenden, wählen Sie **Beenden**.

Schritt 10. Nach dem Beenden wird eine **Export**-Schaltfläche verfügbar, auf die Sie klicken können, um die Erfassungsdatei (.pcap) über den HTTPS- oder TFTP-Server oder den FTP-Server oder die Festplatte oder den Flash des lokalen Systems auf den lokalen Desktop herunterzuladen.



Anmerkung: Die CLI bietet eine etwas detailliertere Auswahl an Optionen, z. B. "Limit by". Die GUI ist ausreichend, um Pakete für allgemeine Anwendungsfälle zu erfassen.

So konfigurieren Sie über CLI:

Erstellen Sie die Monitorerfassung:

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

Zuordnen eines Filters Der Filter kann inline angegeben werden, oder es kann auf eine ACL oder Klassenzuordnung verwiesen werden.

In diesem Beispiel entspricht die ACL dem Datenverkehr zwischen den zwei IP-Adressen des 9800 und einem anderen WLC 5520. Typisches Szenario für die Fehlerbehebung von Mobilitätsproblemen:

```
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
```

Wenn Sie die Erfassung in einem Zirkelpuffer ausführen möchten, haben Sie einige Zeit, um das Problem zu bemerken. Anschließend können Sie die Erfassung beenden und speichern.

Wenn Sie es beispielsweise auf 50MB Puffer einstellen. Es dauert maximal 50MB Festplatte auf dem 9800 und seine ziemlich groß, um mehrere Minuten von Daten in der Hoffnung, dass Sie das Auftreten des Problems zu erfassen.

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

Erfassung starten. Sie können ihn über die GUI oder CLI anrufen:

```
monitor capture uplink start
```

Die Erfassung ist jetzt aktiv.

Erlauben Sie die Erfassung der erforderlichen Daten.

Erfassung beenden. Dies ist über die grafische Benutzeroberfläche oder die Kommandozeile möglich:

```
monitor capture uplink stop
```

Sie können die Aufzeichnung aus der Benutzeroberfläche abrufen > Problembehandlung > Paketerfassung > Exportieren.

Oder von CLI auf einen Server hochladen. Beispiel via ftp:

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

Sobald die erforderlichen Daten erfasst wurden, entfernen Sie die Erfassung:

```
no monitor capture uplink
```

Alarm-LED und Alarm bei kritischer Plattform

Alle Geräte der Serie 9800 (9800-L, 9800-40 und 9800-80) verfügen über eine ALM-LED auf der Vorderseite. Wenn die LED rot leuchtet, bedeutet dies, dass auf der Plattform ein kritischer Alarm ausgelöst wird.

Mit dem Befehl **show facility-alarm status (Gebäudealarmstatus anzeigen)** können Sie die Alarme überprüfen, die eine rote LED auslösen

```
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]

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.