

Inzicht in draadloze debuggen en logbestanden op Catalyst 9800 draadloze LAN-controllers

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Packet flow binnen 9800 WLC](#)

[Controlelampje overtrekken](#)

[Syslog](#)

[Altijd-op-traceren](#)

[Opsporen van fouten](#)

[Voorwaardelijke debugging en RadioActive-tracering](#)

[Radioactieve sporen via web UI](#)

[Radioactieve sporen via CLI](#)

[Niet-voorwaardelijke debugging per proces](#)

[Packet Tracing van datacenters](#)

[Ingesloten pakketvastlegging](#)

[Alarmlampjes en kritische platformalarmen](#)

Inleiding

Dit document beschrijft en biedt een overzicht van alle Cisco IOS® XE-functies en -mogelijkheden die worden benut voor probleemoplossing op Catalyst 9800.

Voorwaarden

Vereisten

- Basiskennis van draadloze LAN-controllers (WLC).
- Basiskennis van de use case flows betrokken bij het gebruik van een WLC.

Gebruikte componenten

Dit document is van toepassing op de 9800-CL, 9800-L, 9800-40 en 9800-80 controllers. Het is voornamelijk gebaseerd op de 17.3 Cisco IOS® XE versie.

Achtergrondinformatie

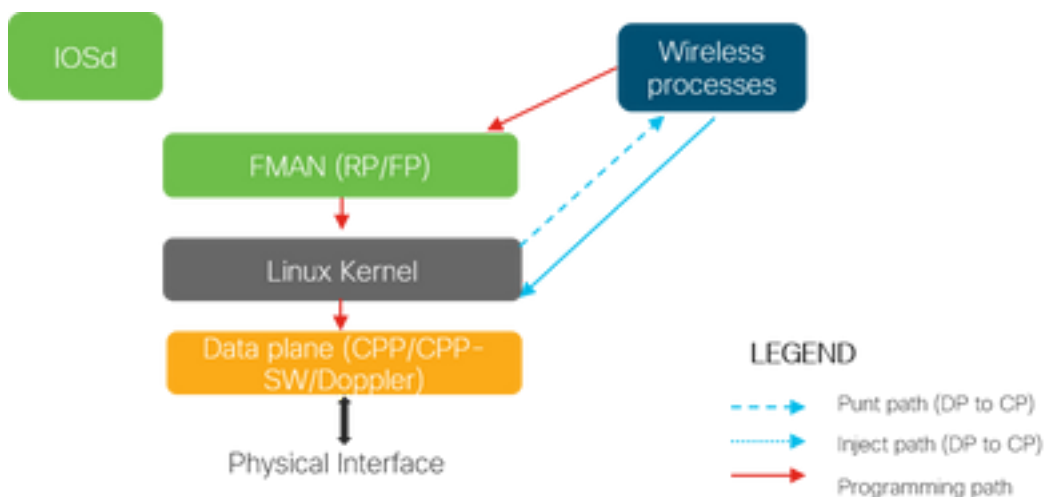
Cisco IOS® XE die op 9800 WLCs wordt uitgevoerd is in wezen samengesteld uit een Linux-

kernel (binOS) met Cisco IOS® en alle draadloze processen die als daemons zijn geïmplementeerd. Alle procesdemonen kunnen worden gebundeld onder de generieke term Control Plane (CP) en zijn verantwoordelijk voor Control and Provisioning of Access points (CAPWAP), Mobility, Radio Resource Management (RRM). Schaduwbeheer, Network Mobility Service Protocol (NMSF) die zijn bestemd voor en vanaf de 9800 WLC.

Data Plane (DP) verwijst naar de componenten die gegevens op 9800 WLC doorsturen.

Op alle iteraties van 9800 (9800-40, 9800-80, 9800-CL, 9800-SW, 9800-L) blijft besturingsplane vrij gewoon. De dataplane varieert echter met de 9800-40 en 9800-80 waarbij gebruik wordt gemaakt van hardware Quantum Flow Processor (QFP) complex vergelijkbaar met ASR1k, terwijl de 9800-CL en 9800-L gebruik maken van software-implementatie van Cisco Packet Processor (CPP). 9800-SW maakt gebruik van de Doppler-chipset op Catalyst 9k Series switches voor data-forward.

Packet flow binnen 9800 WLC



Wanneer een pakket de 9800 WLC van fysieke poorten ingaat, wordt als is vastgesteld dat het controleverkeer is, het doorboord naar de bijbehorende Control Plane Processen. Voor een AP toetreden, zou dit alle capwap en dtls uitwisseling zijn afkomstig van AP. In het geval van client-deelname, zou dit al het verkeer afkomstig van client tot de client gaat naar RUN staat zou volgen PUNT pad.

Terwijl de verschillende daemons het inkomende verkeer verwerken, wordt het resulterende retourverkeer (capwap response, dot11, dot1x, dcp response) afkomstig van 9800 WLC om naar de client te worden gestuurd, weer in het dataplatform geïnjecteerd om naar de fysieke poort te worden verzonden. Terwijl wij AP-verbindingen verwerken, client-toetreden, mobiliteit uitwisselingen, data-vlak moet geprogrammeerd worden zodat het dataverkeer kan verwerken. Dit gebeurt met meerdere componenten die opeenvolgend geprogrammeerd worden over het programmeerpad dat in de afbeelding wordt aangegeven.

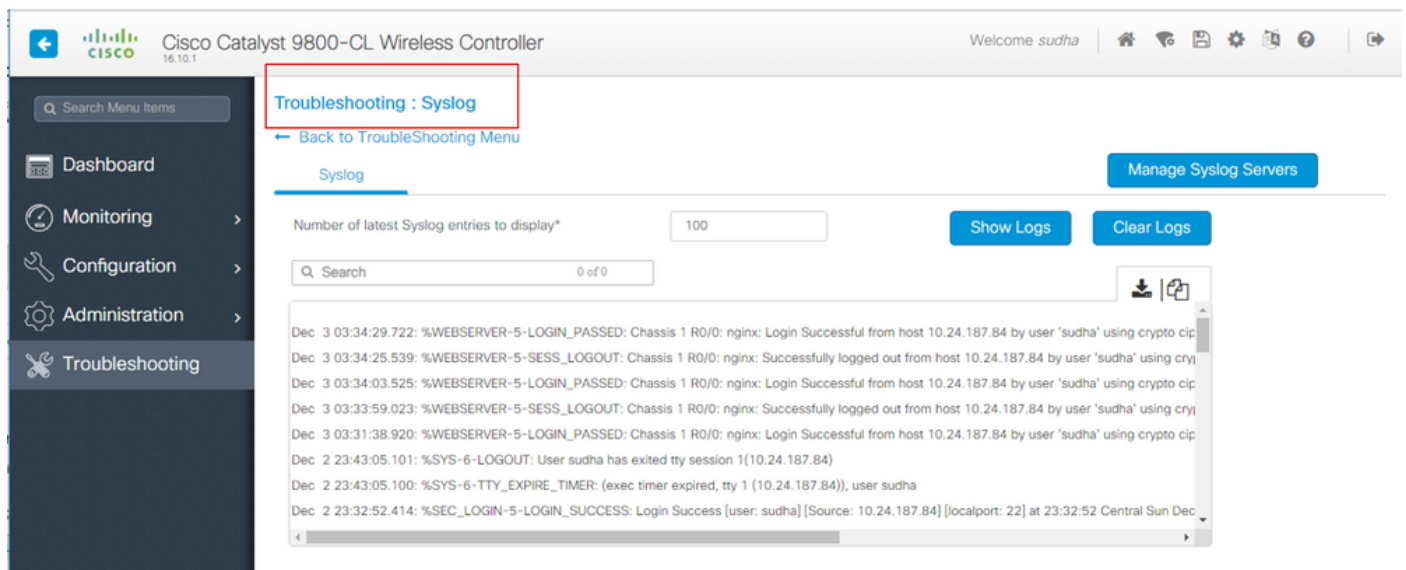
Cisco IOS® XE biedt een veelzijdige tool die is ingesteld om het pakket te overtrekken vanaf het moment dat het 9800 WLC invoert tot het verwerkte verkeer het vakje verlaat. De volgende sectie introduceert deze gereedschappen samen met de opdrachten die worden gebruikt om deze gereedschappen aan te roepen vanuit de opdrachtregelinterface (CLI).

Controlelampje overtrekken

In dit gedeelte worden de opdrachten en gereedschappen beschreven die beschikbaar zijn om de verwerking te bekijken die wordt uitgevoerd door de besturingsplatformprocessen nadat het pakket voor 9800 WLC is geponst van DP of voordat het responspakket dat afkomstig is van 9800 WLC, wordt geïnjecteerd in het DP voor het verzenden van de fysieke interface

Syslog

Logbestanden gegenereerd door de 9800 WLC is het eerste middel om de algemene gezondheid van het systeem te verifiëren. Elke overschrijding van de vooraf gedefinieerde drempel voor systeembronnen zoals CPU, geheugen en buffers wordt in het logbestand gemeld. Ook eventuele fouten die door subsystemen worden gegenereerd, worden in logbestanden geschreven. Als u de logbestanden wilt weergeven, navigeert u naar **Problemen oplossen > 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 name 'Welcome sudha'. The left sidebar contains a search bar and a menu with options: Dashboard, Monitoring, Configuration, Administration, and Troubleshooting. The 'Troubleshooting' menu is expanded, and 'Syslog' is selected. The main content area is titled 'Syslog' and features a 'Manage Syslog Servers' button. Below this, there is a 'Number of latest Syslog entries to display*' field set to 100, and buttons for 'Show Logs' and 'Clear Logs'. A search bar is also present. The log entries displayed include:

- Dec 3 03:34:29.722: %WEBSERVER-5-LOGIN_PASSED: Chassis 1 R0/0: nginx: Login Successful from host 10.24.187.84 by user 'sudha' using crypto cip
- Dec 3 03:34:25.539: %WEBSERVER-5-SESS_LOGOUT: Chassis 1 R0/0: nginx: Successfully logged out from host 10.24.187.84 by user 'sudha' using cryp
- Dec 3 03:34:03.525: %WEBSERVER-5-LOGIN_PASSED: Chassis 1 R0/0: nginx: Login Successful from host 10.24.187.84 by user 'sudha' using crypto cip
- Dec 3 03:33:59.023: %WEBSERVER-5-SESS_LOGOUT: Chassis 1 R0/0: nginx: Successfully logged out from host 10.24.187.84 by user 'sudha' using cryp
- Dec 3 03:31:38.920: %WEBSERVER-5-LOGIN_PASSED: Chassis 1 R0/0: nginx: Login Successful from host 10.24.187.84 by user 'sudha' using crypto cip
- Dec 2 23:43:05.101: %SYS-6-LOGOUT: User sudha has exited tty session 1(10.24.187.84)
- Dec 2 23:43:05.100: %SYS-6-TTY_EXPIRE_TIMER: (exec timer expired, tty 1 (10.24.187.84)), user sudha
- Dec 2 23:32:52.414: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: sudha] [Source: 10.24.187.84] [localport: 22] at 23:32:52 Central Sun Dec

of voer de CLI-opdracht uit:

```
# show logging
```

Deze output toont algemene logboeken evenals sommige draadloos-specifieke logboeken. In tegenstelling tot legacy Cisco IOS® is echter geen draadloze debugging doorgaans een manier om deze logboekuitvoer te bereiken.

Opmerking: Als WLC9800 is geconfigureerd om deze logbestanden om te leiden naar een externe syslog server, dan moet u de logbestanden op externe syslog server ook te controleren.

Altijd-op-traceren

Elk regelvliegtuig proces op de WLC9800 is constant vastleggen op houtkapniveau van **Kennisgeving** aan zijn eigen specifieke buffer. Dit wordt aangeduid als altijd-on-traceren. Dit is een unieke mogelijkheid die u in staat stelt om contextuele gegevens te verkrijgen over een fout die is opgetreden zonder dat de foutvoorwaarde wordt gereproduceerd.

Als u bijvoorbeeld bekend bent met AireOS, voor het oplossen van problemen met clientconnectiviteit, zou u debugs moeten inschakelen en de status van het clientconnectiviteitsprobleem moeten reproduceren om de basisoorzaak te identificeren. Met altijd-

op het vinden, kunt u terugkijken naar reeds gevangen sporen en identificeren als het gemeenschappelijke worteloorzaak is. Afhankelijk van het volume van de gegenereerde logboeken, kunnen we enkele uren tot enkele dagen terugkijken.

Nu, terwijl de sporen per individueel proces worden geregistreerd, is het mogelijk om hen voor een bepaalde context van belang zoals cliënt mac of AP mac of AP ip adres te bekijken. Voer daartoe de opdracht uit

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

Standaard gaat deze opdracht slechts 10 minuten terug om de logbestanden te genereren en te decoderen. Je kunt ervoor kiezen nog verder terug te gaan in de tijd met :

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

Om logbestanden per proces te bekijken, voert u de opdracht uit

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

Opmerking: Er zijn meerdere filteropties op deze CLI's, waaronder module, registratieniveau, start tijdstempel enzovoort. Om deze opties te bekijken en te onderzoeken, voer de opdracht uit

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

```
# show logging process ?
```

Opsporen van fouten

Om een snelle momentopname van algemeen bekende storingsvoorwaarden te krijgen, is de spoorweg-op-mislukkingscapaciteit beschikbaar. Dit parseert alle sporen op het systeem op het gegeven moment om aan de vooraf gedefinieerde storingscondities te voldoen en geeft zowel een overzicht als statistieken.

Om een summier mening te krijgen, stel het bevel in werking

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

Om de vooraf gedefinieerde storingsvoorwaarden te bekijken en statistieken die overeenkomen met deze voorwaarden, voert u de opdracht uit

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

Zodra u de fout kent, om sporen te verzamelen specifiek voor de context van de fout, voer de opdracht uit

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

Deze kunnen op eindzitting worden bekeken of voor off-line analyse met de bevelen worden uitgevoerd

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

OR

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

Voorwaardelijke debugging en RadioActive-tracering

Voorwaardelijke Debugging staat de mogelijkheid toe om debug level logging in te schakelen voor specifieke functies voor de voorwaarden van belang. RadioActive-overtrekken gaat een stap verder door de mogelijkheid toe te voegen om voorwaardelijk af te drukken debug informatie over processen, threads voor de toestand van belang. Dit betekent dat de onderliggende architectuur volledig geabstraheerd is.

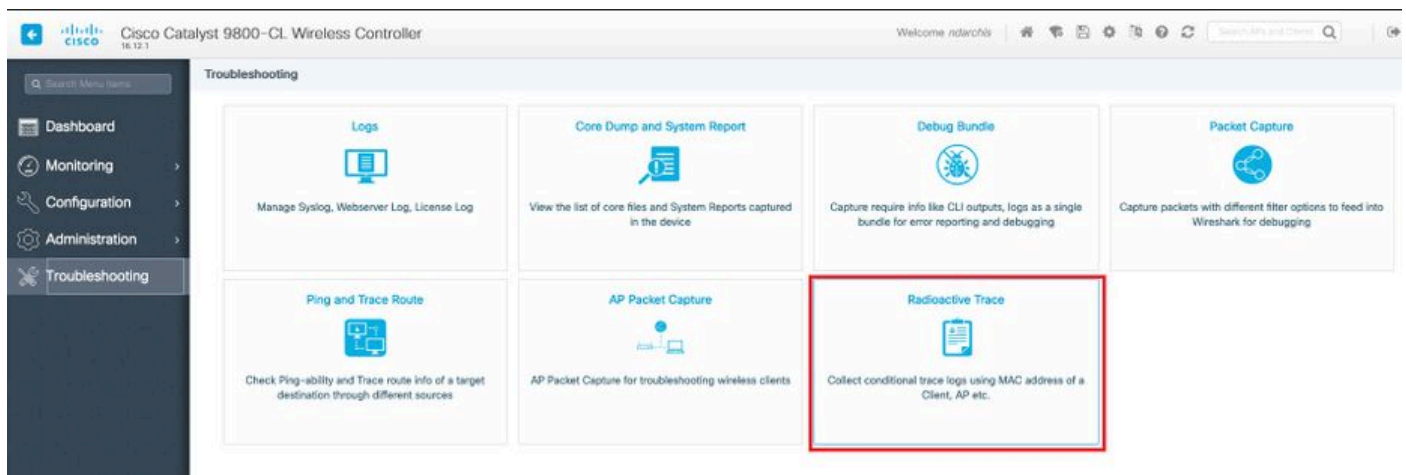
Opmerking: Op 16.12 wordt radioactief traceren alleen geïmplementeerd voor probleemoplossing AP-samenvoeging met AP-radio en Ethernet-mac-adressen, client-samenvoeging met client-mac-adres en mobiliteitsproblemen met mobiele peer-ip en CMX-connectiviteit met het CMX-ip-adres als interessante voorwaarden.

Opmerking: Het adres van MAC versus IP adres als voorwaarde verstrekt verschillende output aangezien de verschillende processen zich van verschillende herkenningstekens voor de zelfde netwerkentiteit (AP of cliënt of mobiliteitspeer) bewust zijn.

Met client connectiviteit, als een voorbeeld om problemen op te lossen, voorwaardelijk debug looppas voor client mac om eind te krijgen om mening op controlevliegtuig te krijgen.

Radioactieve sporen via web UI

Ga naar het menu **Problemen oplossen** en kies **Radioactief overtrekken**



Klik op **Add** en voer een client- of AP-adres in dat u wilt oplossen. Vanaf 16.12 kunnen alleen MAC-adressen worden toegevoegd via de GUI. U kunt IP-adres toevoegen via 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

U kunt meerdere mac-adressen aan de track toevoegen. Wanneer u klaar bent om het radioactieve traceren te starten, klikt u op **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

Zodra begonnen, debug vastlegging worden geschreven aan schijf over om het even welke controle vliegtuig verwerking met betrekking tot de gevolgde mac adressen.

Wanneer u het probleem gereproduceerd hebt dat u wilt oplossen, klikt u op **Stoppen**.

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

Voor elk gedebuggeerd mac-adres kunt u een logbestand genereren door te klikken op **Generate**.

← 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

Geef aan hoe lang u wilt dat uw gesorteerde logbestand gaat en druk op **Toepassen op apparaat**.

Enter time interval ×


Generate logs for last

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

U kunt het bestand nu downloaden door op het pictogram naast de bestandsnaam te klikken. Dit bestand is aanwezig in de bootflash-drive van de controller en kan ook uit het vak worden gekopieerd via 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

Radioactieve sporen via CLI

Om voorwaardelijke debugging mogelijk te maken, voert u de opdracht uit

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

Om de momenteel ingeschakelde voorwaarden te bekijken, voert u de opdracht uit

```
# show debugging
```

Deze debugs drukken geen output op eindscherm maar slaan het debug uitvoerbestand op te flitsen om daarna worden teruggewonnen en geanalyseerd. Het bestand wordt opgeslagen met de naamgevingsconventie ra_trace_*

Bijvoorbeeld, voor mac adres aaaa.bbbb.ccc, bestandsnaam gegenereerd is
ra_trace_MAC_aabbccc_HMMSS.XXX_timezone_DayWeek_Month_Day_year.log

Een voordeel is dat dezelfde opdracht kan worden gebruikt om problemen op te lossen met AP-verbinding (input AP-radio mac en ethernetmac), client connectiviteit problemen (input client mac), mobiliteitstunnel probleem (input peer ip), client roaming problemen (input client mac). Met andere woorden, hoeft u geen meerdere opdrachten te onthouden, zoals debug capwap, debug client, debug mobiliteit enzovoort.

Opmerking: debug Wireless maakt het ook mogelijk om naar een FTP-server te verwijzen en nog meer breedspakige logboekregistratie met een keyword intern. We raden dit op dit moment niet aan, omdat er een aantal kwesties worden opgelost.

Om uitvoerbestand op terminalsessie te debuggen, voert u de opdracht uit

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

Om de debug-uitvoer naar een externe server voor offline analyse te leiden, voert u de opdracht uit

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


Er is een veel ruimere mening van het zelfde zuiveren logboekniveaus. om deze breedsprakige weergave te zien, voert u de opdracht uit

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

Om het zuiveren voor specifieke context of vóór de gevormde of standaardmonitortijd onbruikbaar te maken is omhoog, stel het bevel in werking.

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

Voorzichtig: Het voorwaardelijke zuiveren laat debug niveau het registreren toe die beurtelings volume van de geproduceerde logboeken verhoogt. Als u dit programma laat draaien, vermindert u hoe ver u terug in de tijd kunt kijken. Zo, wordt het geadviseerd om het zuiveren aan het eind van het oplossen van problemen zitting altijd onbruikbaar te maken.

Om alle debugging uit te schakelen, voert u deze opdrachten uit

```
# clear platform condition all
# undebg all
```

Niet-voorwaardelijke debugging per proces

Voor de gebruikscases en processen, niet geïmplementeerd voor radioactief traceren, kunt u debug-niveau traces krijgen. Om debug niveau op specifiek proces te bepalen, gebruik het bevel

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

Om spoor-niveaus van de diverse modules te verifiëren, voer het bevel uit

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

Om de verzamelde sporen te bekijken, voer de opdracht uit

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

Packet Tracing van datacenters

Wanneer een pakket voor het eerst 9800 WLC invoert, vindt enige verwerking plaats op dataplaat om te identificeren als verkeer controlevliegtuig of dataplaat is. Packet-Trace biedt een gedetailleerde weergave van deze Cisco IOS® XE-verwerking op dataplane en de beslissing om het pakket te punteren, doorsturen, neerzetten of te consumeren. Deze functie op WLC 9800 werkt precies hetzelfde als de implementatie op ASR!k.

Packet Tracer op 9800 WLC biedt drie inspectieniveaus hetzelfde als ASR1K.

- Statistieken - Biedt telling van pakketten die de netwerkprocessor invoeren en verlaten
- Samenvatting- Dit wordt verzameld voor een eindig aantal pakketten dat aan specifieke voorwaarde van belang voldoet. De summier output geeft de in- en uitgangen aan, de lookup-beslissing van het gegevensplatform en volgt ook punten-, drop- en injectiepakketten, indien aanwezig. Deze output geeft een beknopt overzicht van de gegevensverwerking

- Path Data - Dit geeft de meest gedetailleerde weergave van DP-pakketverwerking. Verzameld voor eindig aantal pakketten, omvat het voorwaardelijke het zuiveren identiteitskaart die kan worden gebruikt om DP pakket te correleren aan controlevliegtuig zuiveren, timestamp evenals eigenschap-specifieke weg-spoor gegevens. Deze gedetailleerde weergave heeft twee optionele functies Met pakketkopie kunt u in- en uitstappakketten op verschillende lagen van het pakket kopiëren (Layer 2, Layer 3 en Layer 4)De serie van de Invocatie van de eigenschap (FIA) is de opeenvolgende lijst van eigenschappen die op het pakket door het gegevensvliegtuig worden uitgevoerd. Deze functies zijn afgeleid van de standaard- en gebruikersconfiguratie op WLC 9800

Raadpleeg voor een gedetailleerde uitleg van de functie en subopties Cisco [IOS XE Datapath Packet Trace-functie](#)

Voor draadloze workflows zoals AP Josef, client connectiviteit, enzovoort, overtrekken van de uplink bidirectioneel

Voorzichtig: De pakkettracer van het dataplane parseert alleen de kop van de router CAPWAP. Dus, voorwaarden zoals draadloze client mac geen nuttige output.

Stap 1. Bepaal de relevante voorwaarden.

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

Waarschuwing: Zowel de commando's - debug platform voorwaarde functie als debug platform voorwaarde mac aaaa.bbbb.ccc zijn bedoeld voor controle vliegtuig pakket tracing en niet retourneren een dataplane pakket sporen.

Stap 2. Om de momenteel ingeschakelde voorwaarden te bekijken, voert u de opdracht uit

```
# show platform conditions
```

Stap 3. Schakel packet-tracer in voor een eindig aantal pakketten. Dit pakketnummer is gedefinieerd als een voeding van 2 in het bereik van 16 - 8192. In de standaardinstelling worden zowel de samenvatting- als de functiegegevens opgenomen. U kunt er optioneel voor kiezen alleen een overzichtswaergave te krijgen als u de suboptie Alleen overzichtswaergave gebruikt. Je hebt ook sub-opties beschikbaar om fia spoor te krijgen, het bepalen van pakketgrootte in bytes, het spoor punt, injecteren of laat vallen pakketten. en ga zo maar door.

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

Stap 4. (Optioneel) U kunt de pakketten kopiëren en dumpen zoals ze worden overgetrokken

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

Stap 5. Schakel voorwaardelijke debugging in.

```
# debug platform condition start
```

Stap 6. Controleer statistieken om te zien of het pakketspoor uitvoer verzamelt

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

Stap 7. Om de output van het pakketspoor te bekijken, voer het bevel uit

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

Stap 8. (optioneel) U kunt pakketdump exporteren voor offline analyse door Cisco TAC

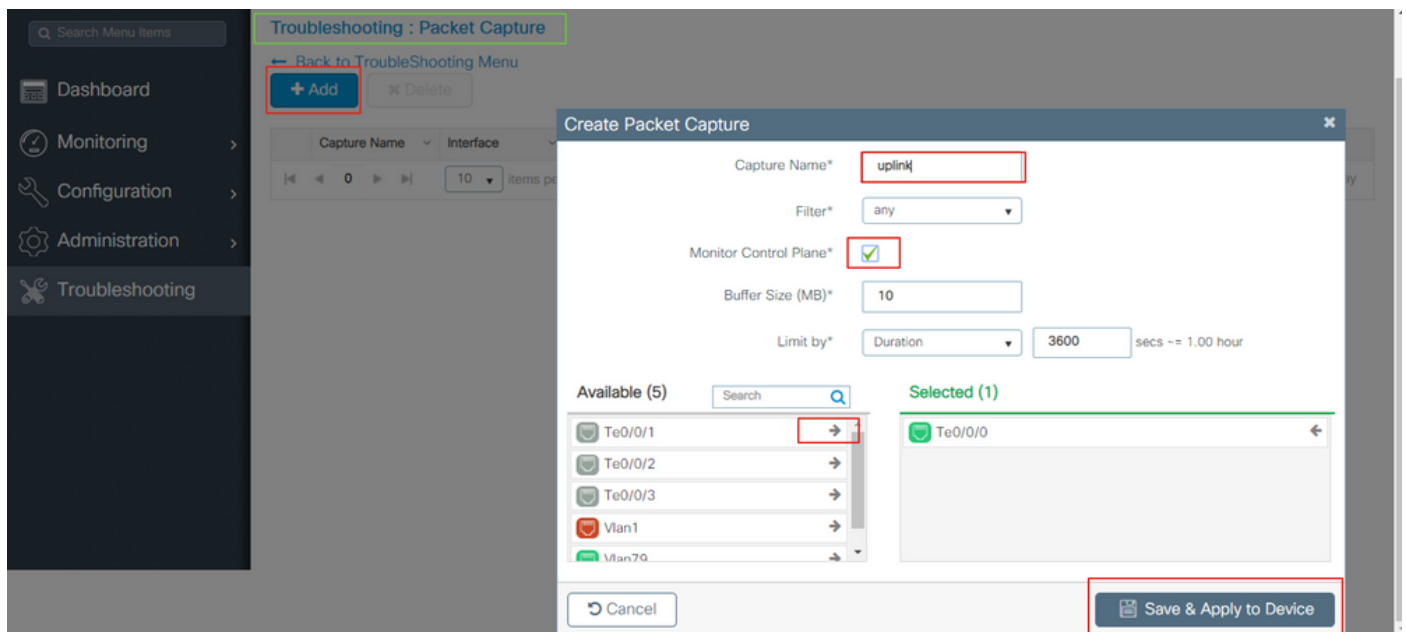
```
# show platform packet-trace packet all | redirect { bootflash: | tftp: | ftp: } pacrac.txt
```

Ingesloten pakketvastlegging

Embedded Packet Capture (EPC) is een pakketopnamevoorziening waarmee gegevens kunnen worden weergegeven in pakketten die bestemd zijn voor, afkomstig zijn van en worden doorgegeven via Catalyst 9800 WLC's. Deze opnamen kunnen worden geëxporteerd voor offline analyse met Wireshark. Zie voor meer informatie over deze functie de [EPC Configuration Guide](#)

Vergeleken met AireOS, kan de 9800 WLC in plaats van te vertrouwen op pakketopname en traffic mirroring mogelijkheden op uplink switch pcap-opname op de doos zelf mogelijk maken. Op 9800 kan deze opname worden ingesteld zowel vanaf een opdrachtregelinterface (CLI) als op een grafische gebruikersinterface (GUI).

Om via GUI te configureren navigeert u naar **Problemen oplossen > Packet Capture > +Add**



Stap 1. Bepaal de naam van de pakketopname. U mag maximaal 8 tekens gebruiken.

Stap 2. Definieer eventuele filters

Stap 3. Vink het vakje aan om het verkeer te controleren als u verkeer wilt zien dat wordt gestraft naar de CPU en vervolgens weer wordt ingespoten in het gegevensvlak

Stap 4. Definieer de buffergrootte. Een maximum van 100 MB is toegestaan

Stap 5. Definieer de grenswaarde, hetzij door de duur die een bereik van 1 - 1000000 seconden toestaat, hetzij door het aantal pakketten dat een bereik van 1 - 100000 pakketten toestaat, zoals

gewenst

Stap 6. Kies de interface uit een lijst met interfaces in de linkerkolom en selecteer de pijl om deze naar de rechterkolom te verplaatsen

Stap 7. Opslaan en toepassen op apparaat

Stap 8. Selecteer **Start** om de opname te starten

Stap 9. U kunt de opname tot de gedefinieerde limiet laten lopen. Selecteer **Stop** om de opname handmatig te stoppen.

Stap 10. Zodra de knop **Exporteren** is gestopt, kan deze knop worden bediend door te klikken op de optie om het opnamebestand (.pcap) op het lokale bureaublad te downloaden via https of TFTP-server of FTP-server of een lokale vaste schijf of flash van het systeem.

Capture Name	Interface	Monitor Control Plane	Buffer Size	Filter by	Limit	Status	Action
<input type="checkbox"/> uplink	TenGigabitEthernet0/0/0	Yes	0%	any	0 secs	Inactive	Start

Opmerking: CLI biedt een beetje meer granulariteit van opties zoals Limit by. GUI is voldoende om pakketten op te nemen voor algemene gevallen van gebruik.

U kunt als volgt via CLI configureren:

Maak de monitoropname:

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

Koppel een filter. Het filter kan inline worden gespecificeerd, of een ACL of een klasse-kaart kan worden verwezen.

In dit voorbeeld is het ACL om het verkeer tussen de 2 IP-adressen van de 9800 en een andere WLC 5520 aan te passen. Typisch scenario voor probleemoplossing bij mobiliteit:

```
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
```

Als u wilt dat de opname in een cirkelbuffer loopt, geeft het wat tijd om het probleem op te merken en dan de opname te stoppen en op te slaan.

Als u de buffer bijvoorbeeld instelt op 50MB. De 9800 heeft maximaal 50 MB schijf nodig en is vrij

groot om enkele minuten gegevens op te nemen, in de hoop dat het probleem zich voordoet.

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

Start de vastlegging. U kunt deze vanuit GUI of CLI bekijken:

```
monitor capture uplink start
```

De vastlegging is nu actief.

Laat de benodigde data verzamelen.

Stop de vastlegging. U kunt dit doen via GUI of CLI:

```
monitor capture uplink stop
```

U kunt de opname ophalen via de GUI > Problemen oplossen > Packet Capture > Exporteren.

Of upload naar een server van CLI. Voorbeeld via ftp:

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

Zodra de benodigde data zijn verzameld, verwijdert u de vastlegging:

```
no monitor capture uplink
```

Alarmlampjes en kritische platformalarmen

Alle 9800 apparaten (9800-L, 9800-40 en 9800-80) hebben een ALM LED op hun voorpaneel. Als die LED rood wordt, betekent dit dat er een kritisch alarm op het platform is.

U kunt het alarm verifiëren dat de LED om rood te gaan met de opdracht **show voorziening-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]

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.