

Resolución de problemas de controladores de LAN inalámbrica Catalyst 9800

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Flujo de paquetes dentro del WLC 9800](#)

[Seguimiento del plano de control](#)

[Syslog](#)

[Seguimiento siempre activo](#)

[Depuración condicional y seguimiento de RadioActive](#)

[Rastreos radiactivos a través de la interfaz web](#)

[Rastreos radiactivos a través de CLI](#)

[Depuración no condicional por proceso](#)

[Seguimiento de paquetes del plano de datos](#)

[Captura de paquetes integrada](#)

[LED de alarma y alarmas de plataforma crítica](#)

Introducción

Este documento describe y proporciona una descripción general de todas las funciones y capacidades de Cisco IOS® XE aprovechadas para la solución de problemas de Catalyst 9800.

Prerequisites

Requirements

- Conocimiento básico de Wireless LAN Controllers (WLC).
- Conocimiento básico de los flujos de casos de uso involucrados en el uso de un WLC.

Componentes Utilizados

Este documento cubre los controladores 9800-CL, 9800-L, 9800-40 y 9800-80. Se basa principalmente en la versión 17.3 de Cisco IOS® XE.

Antecedentes

Cisco IOS® XE, que se ejecuta en WLC 9800, se compone esencialmente de un núcleo Linux

(binOS) con Cisco IOS® y todos los procesos inalámbricos implementados como demonios.

Todos los demonios de proceso se pueden agrupar bajo el término genérico Plano de control (CP) y son responsables del control y aprovisionamiento de puntos de acceso (CAPWAP), movilidad, gestión de recursos de radio (RRM). Rogue Management, Network Mobility Service Protocol (NMSP) que se destinan hacia y desde el WLC 9800.

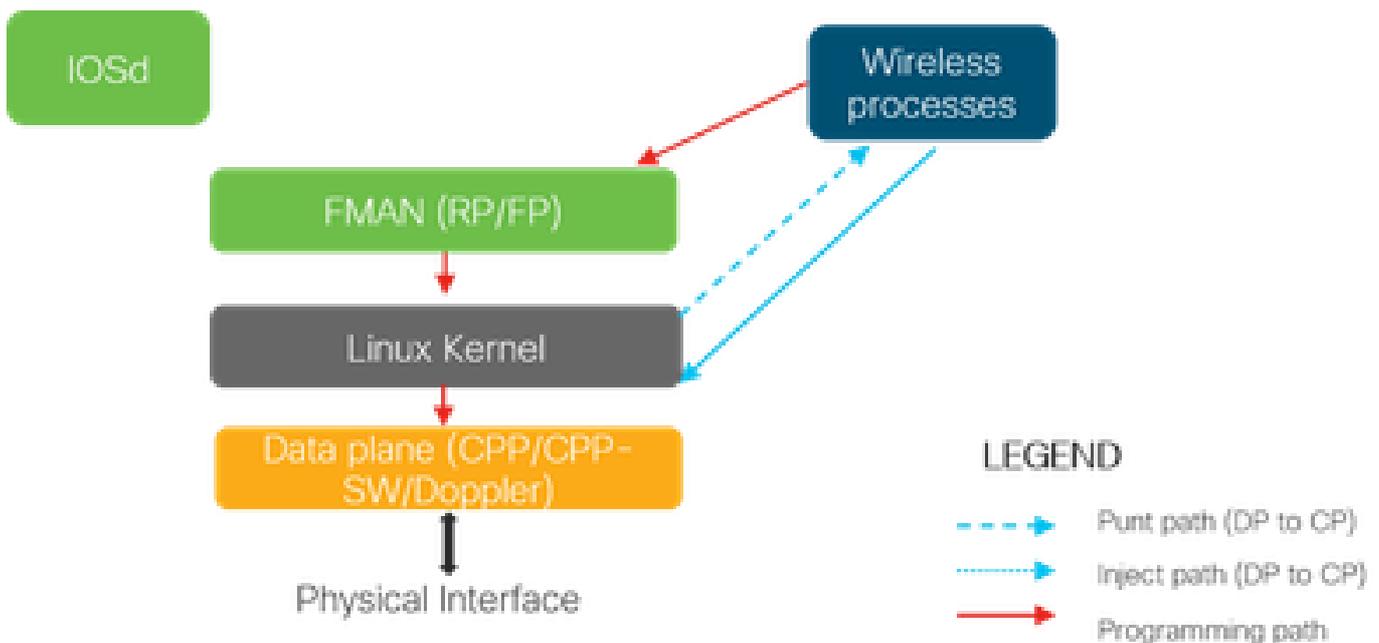
El plano de datos (DP) se refiere a los componentes que reenvían datos en el WLC 9800.

En todas las iteraciones de 9800 (9800-40, 9800-80, 9800-CL, 9800-SW,9800-L), el plano de control sigue siendo bastante común.

Sin embargo, el plano de datos varía según el 9800-40 y el 9800-80 que utilizan el complejo de procesador Quantum Flow (QFP) de hardware similar a ASR1k, mientras que el 9800-CL y el 9800-L utilizan la implementación de software del procesador de paquetes de Cisco (CPP).

9800-SW simplemente aprovecha el conjunto de chips Doppler de los switches Catalyst de la serie 9k para el reenvío de datos.

Flujo de paquetes dentro del WLC 9800



Cuando un paquete ingresa al 9800 WLC desde los puertos físicos, si se determina que es tráfico de control, se lo envía a los procesos del plano de control correspondientes.

Para una unión AP, esto sería todo el intercambio capwap y dtls originado desde AP. En caso de que el cliente se una, esto sería todo el tráfico originado en el cliente hasta que el cliente pase al estado RUN.

A medida que los diversos demonios procesan el tráfico entrante, el tráfico de retorno resultante (respuesta capwap, dot11, dot1x, respuesta dcp) originado en 9800 WLC para ser enviado al cliente se inyecta nuevamente en el plano de datos para ser enviado fuera del puerto físico.

A medida que procesamos las uniones de PA, las uniones de clientes, los intercambios de movilidad y el plano de datos deben programarse para que puedan gestionar el reenvío del tráfico de datos.

Esto ocurre cuando se programan varios componentes secuencialmente en la ruta de programación indicada en la imagen.

Cisco IOS® XE proporciona un conjunto de herramientas versátil para rastrear el paquete desde el momento en que ingresa al WLC 9800 hasta que el tráfico procesado sale de la caja.

En la siguiente sección se presentan estas herramientas junto con los comandos utilizados para invocar estas herramientas desde la interfaz de línea de comandos (CLI).

Seguimiento del plano de control

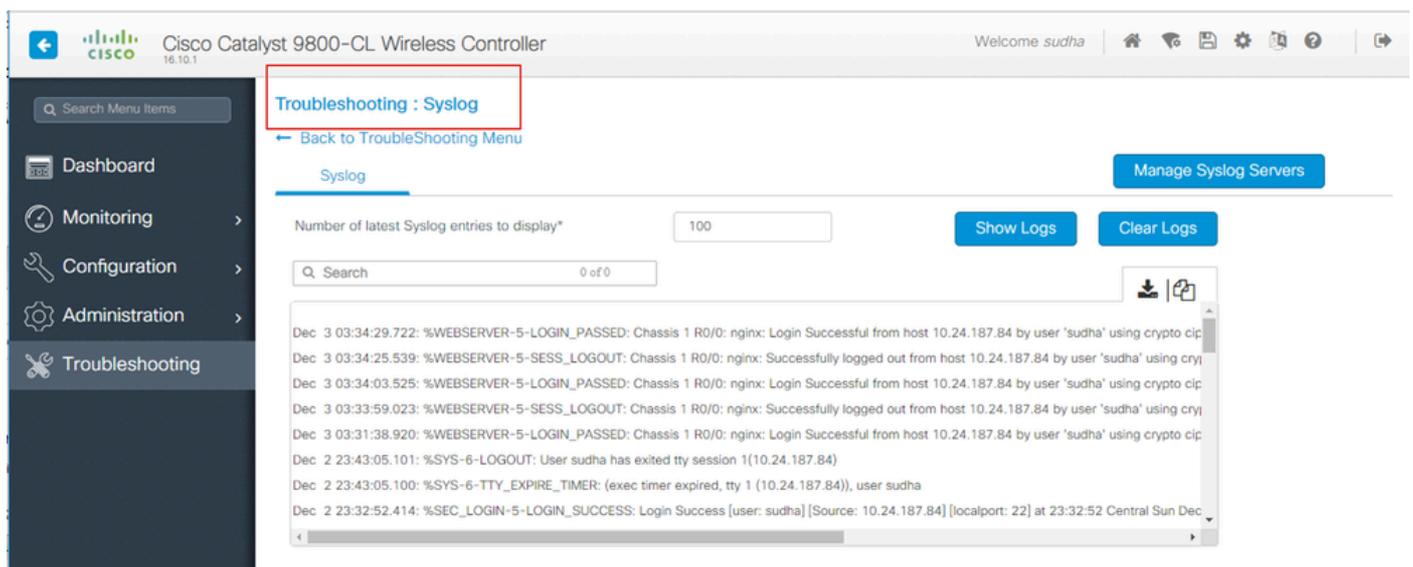
Esta sección describe los comandos y las herramientas disponibles para ver el procesamiento realizado por los procesos del plano de control después de que el paquete destinado para el WLC 9800 haya sido impulsado desde el DP o antes de inyectar el paquete de respuesta originado desde el WLC 9800 al DP para enviar la interfaz física

Syslog

Los registros generados por el WLC 9800 son el primer medio para verificar el estado general del sistema.

Cualquier violación del umbral predefinido para los recursos del sistema como la CPU, la memoria y los búferes se informa en el registro.

Además, cualquier error generado por cualquier subsistema se escribe en los registros. Para ver los registros, navegue hasta Troubleshooting > Syslog



The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller web interface. The top navigation bar includes the Cisco logo, the device name 'Cisco Catalyst 9800-CL Wireless Controller', and the user 'Welcome sudha'. A sidebar on the left contains menu items: Dashboard, Monitoring, Configuration, Administration, and Troubleshooting. The main content area is titled 'Troubleshooting : Syslog' and includes a 'Back to TroubleShooting Menu' link. Below this, there is a 'Syslog' section with a 'Manage Syslog Servers' button. A form allows setting the 'Number of latest Syslog entries to display*' to 100, with 'Show Logs' and 'Clear Logs' buttons. A search bar is present with '0 of 0' results. The Syslog log entries are displayed in a scrollable area, showing various system events such as user logins, logouts, and session expirations.

o ejecute el comando CLI :

```
# show logging
```

Este resultado muestra registros generales así como algunos registros específicos de la red inalámbrica. Sin embargo, a diferencia del IOS® de Cisco heredado, ninguna depuración inalámbrica suele llegar a esta salida de registro.



Nota: Si el WLC9800 está configurado para redirigir estos registros a un servidor syslog externo, también debe verificar los registros en el servidor syslog externo.

Seguimiento siempre activo

Cada proceso del plano de control en el WLC9800 está registrando constantemente en el nivel de registro de Aviso a su propio buffer dedicado. Esto se denomina seguimiento siempre activo.

Se trata de una capacidad exclusiva que le permite obtener datos contextuales sobre un fallo que se ha producido sin exigir que se reproduzca la condición de fallo.

Por ejemplo, si está familiarizado con AireOS, para cualquier solución de problemas de conectividad del cliente, debería habilitar los debugs y reproducir el estado del problema de conectividad del cliente para identificar la causa raíz.

Con el seguimiento siempre activo, puede volver a los seguimientos ya capturados e identificar si es una causa raíz común. Dependiendo del volumen de registros generados, podemos mirar hacia atrás varias horas a varios días.

Ahora, mientras que los seguimientos se registran por proceso individual, es posible verlos integralmente para un contexto particular de interés como mac del cliente o MAC del AP o dirección IP del AP. Para ello, ejecute el comando

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

De forma predeterminada, este comando sólo se remonta a 10 minutos para generar y decodificar los registros. Puede optar por retroceder más en el tiempo con :

```
# show logging profile wireless start last <number> [minutes|hours|days] filter mac to-file bootflash:
```

Para ver los registros por proceso, ejecute el comando

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

 Nota: Hay varias opciones de filtrado en estas CLI, incluidos el módulo, el nivel de registro, la marca de hora de inicio, etc. Para ver y explorar estas opciones, ejecute el comando

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

Depuración condicional y seguimiento de RadioActive

La depuración condicional permite habilitar el registro de nivel de depuración para funciones específicas para las condiciones de interés.

El seguimiento de RadioActive va un paso más allá al agregar la capacidad de imprimir condicionalmente información de depuración en los procesos y subprocesos para la condición de interés.

Esto significa que la arquitectura subyacente es completamente abstracta.

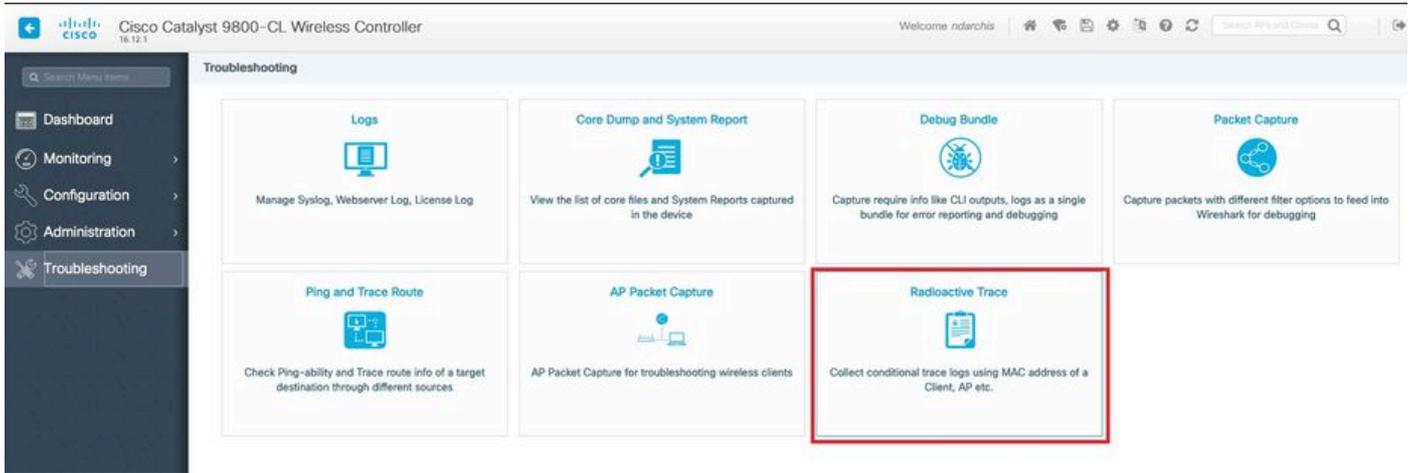
 Nota: En la versión 16.12, el seguimiento radioactivo solo se implementa para solucionar problemas de unión de AP con direcciones MAC de radio y Ethernet de AP, conexión del cliente con dirección MAC del cliente, así como problemas de movilidad con conectividad IP de peer de movilidad y CMX con la dirección IP de CMX como condiciones de interés.

 Nota: la dirección MAC frente a la dirección IP como condición proporciona salidas diferentes, ya que los diferentes procesos son conscientes de los diferentes identificadores para la misma entidad de red (AP o cliente o peer de movilidad).

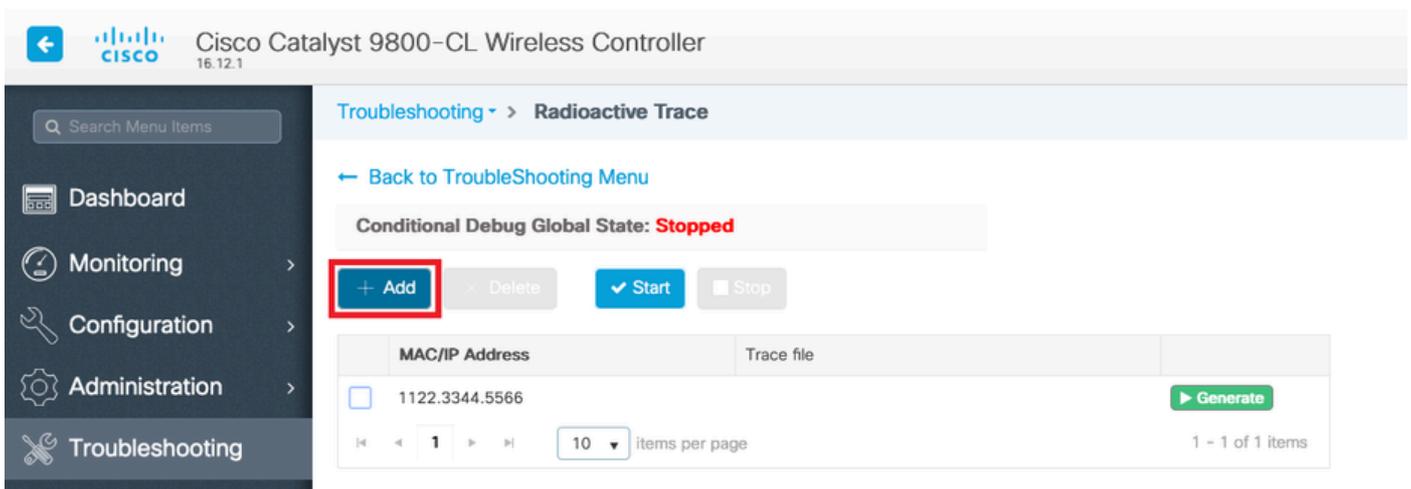
Con la conectividad del cliente, como ejemplo para resolver problemas, se ejecuta el debug condicional para que el mac del cliente obtenga una vista integral en el plano de control.

Rastros radiactivos a través de la interfaz web

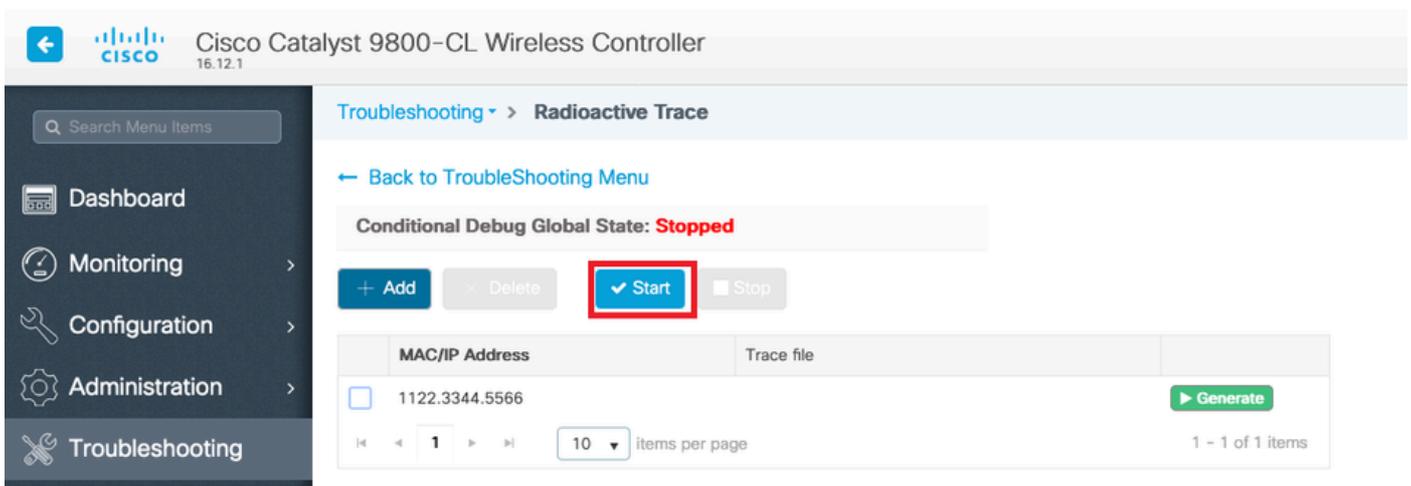
Vaya al menú de la página Troubleshooting y elija Radioactive Tracing



Haga clic en Add e ingrese una dirección MAC de cliente o AP que desee resolver. A partir de la versión 16.12, solo se pueden agregar direcciones MAC a través de la GUI. Puede agregar una dirección IP a través de CLI.

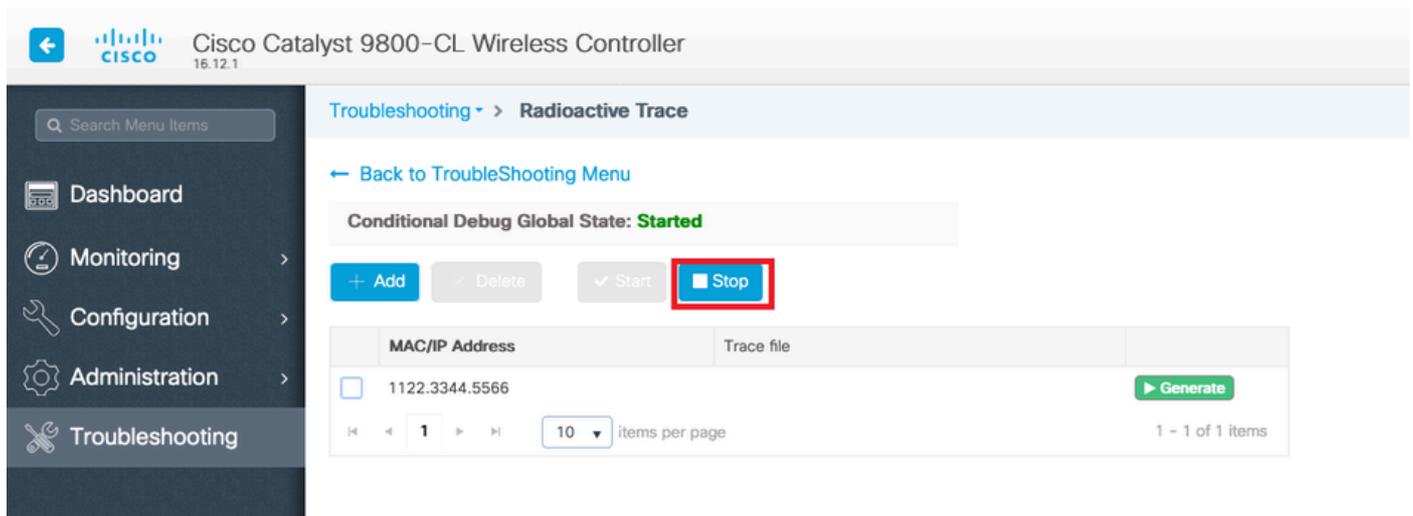


Puede agregar varias direcciones MAC para realizar un seguimiento. Cuando esté listo para iniciar el seguimiento radiactivo, haga clic en inicio.



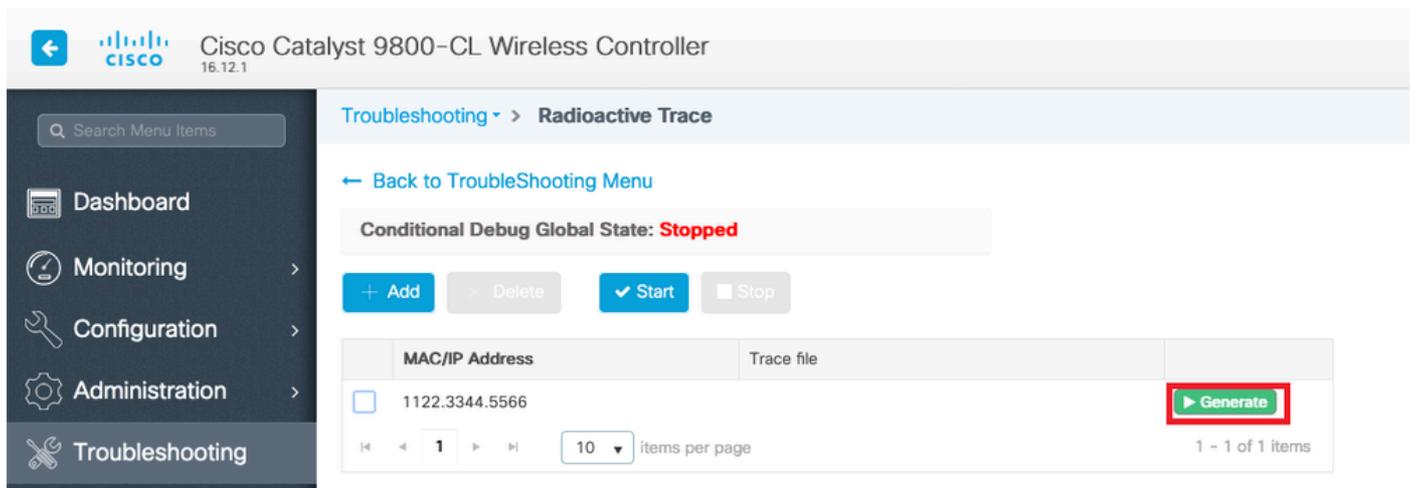
Una vez iniciado, el registro de depuración se escribe en el disco acerca de cualquier procesamiento del plano de control relacionado con las direcciones MAC rastreadas.

Cuando haya reproducido el problema que desea solucionar, haga clic en Detener.



The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. The left sidebar contains navigation options: Dashboard, Monitoring, Configuration, Administration, and Troubleshooting. The main content area is titled "Radioactive Trace" and shows the "Conditional Debug Global State" as "Started". Below this, there are buttons for "+ Add", "Delete", "Start", and "Stop". The "Stop" button is highlighted with a red box. A table below lists MAC/IP addresses, with one entry "1122.3344.5566" and a "Generate" button next to it. The page also shows "10 items per page" and "1 - 1 of 1 items".

Para cada dirección MAC depurada, puede generar un archivo de registro que recopile todos los registros pertenecientes a esa dirección MAC haciendo clic en Generar.



The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. The left sidebar contains navigation options: Dashboard, Monitoring, Configuration, Administration, and Troubleshooting. The main content area is titled "Radioactive Trace" and shows the "Conditional Debug Global State" as "Stopped". Below this, there are buttons for "+ Add", "Delete", "Start", and "Stop". A table below lists MAC/IP addresses, with one entry "1122.3344.5566" and a "Generate" button next to it. The "Generate" button is highlighted with a red box. The page also shows "10 items per page" and "1 - 1 of 1 items".

Elija cuánto tiempo atrás desea que transcurra el archivo de registro intercalado y haga clic en Aplicar al dispositivo.

Enter time interval



Generate logs for last 10 minutes

30 minutes

1 hour

since last boot

seconds



Cancel

Apply to Device

Ahora puede descargar el archivo haciendo clic en el pequeño icono situado junto al nombre del archivo. Este archivo está presente en la unidad bootflash del controlador y también se puede copiar desde la caja a través de CLI.

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	debugTrace_1122.3344.5566.txt	Generate

◀ 1 ▶ 10 items per page 1 - 1 of 1 items

Rastros radiactivos a través de CLI

Para habilitar la depuración condicional, ejecute el comando

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

Para ver las condiciones habilitadas actualmente, ejecute el comando

```
# show debugging
```

Estos debugs no imprimen ningún resultado en la sesión de terminal pero almacenan el archivo de salida de debug en flash para recuperarlo y analizarlo después. El archivo se guarda con la convención de nomenclatura `ra_trace_*`

Por ejemplo, para la dirección mac `aaaa.bbbb.cccc`, el nombre de archivo generado es `ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log`

Una ventaja es que el mismo comando se puede utilizar para resolver problemas de unión de AP (MAC de radio AP de entrada y MAC de Ethernet), problemas de conectividad del cliente (MAC de cliente de entrada), problema del túnel de movilidad (IP de peer de entrada), problemas de itinerancia del cliente (MAC de cliente de entrada).

En otras palabras, no tiene que recordar varios comandos como `debug capwap`, `debug client`, `debug mobility`, etc.

 Nota: `debug wireless` también permite apuntar a un servidor FTP y ejecutar un registro aún más detallado con la palabra clave `internal`. No se recomienda por el momento, ya que hay algunos problemas que se están solucionando.

Para depurar el archivo de salida en la sesión de terminal, ejecute el comando

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

Para redirigir el resultado de la depuración a un servidor externo para el análisis sin conexión, ejecute el comando

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

Existe una vista mucho más detallada de los mismos niveles de registro de depuración. Para ver esta vista detallada, ejecute el comando

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

Para inhabilitar la depuración para un contexto específico o antes de que se active el tiempo de supervisión configurado o predeterminado, ejecute el comando.

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

 **Precaución:** la depuración condicional habilita el registro de nivel de depuración que, a su vez, aumenta el volumen de los registros generados. Si deja esta opción en ejecución, reducirá la cantidad de tiempo desde el que puede ver los registros. Por lo tanto, se recomienda desactivar siempre la depuración al final de la sesión de solución de problemas.

Para inhabilitar toda la depuración, ejecute estos comandos

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

Depuración no condicional por proceso

Para los casos prácticos y procesos, no implementados para el seguimiento radiactivo, puede obtener seguimientos de nivel de depuración. Para establecer el nivel de depuración en un proceso específico, utilice el comando

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

Para comprobar los niveles de seguimiento de los distintos módulos, ejecute el comando

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

Para ver los seguimientos recopilados, ejecute el comando

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

Seguimiento de paquetes del plano de datos

Cuando un paquete ingresa por primera vez al WLC 9800, se produce algún procesamiento en el plano de datos para identificar si el tráfico es el plano de control o el plano de datos.

La función Packet-Trace proporciona una vista detallada de este procesamiento de Cisco IOS® XE realizado en el plano de datos y de la decisión tomada sobre si se debe perforar, reenviar, descartar o consumir el paquete.

Esta función en el WLC 9800 funciona exactamente igual que la implementación en ASR!k.

Packet Tracer en el WLC 9800 proporciona tres niveles de inspección iguales que ASR1K.

- Estadísticas: proporciona la cuenta de paquetes que entran y salen del procesador de red
- Summary-
 - Esto se recopila para un número finito de paquetes que coinciden con una condición específica de interés.
 - La salida de resumen indica las interfaces de ingreso y egreso, la decisión de búsqueda tomada por el plano de datos y también rastrea los paquetes de punt, drop e inject, si los hay.
 - Este resultado proporciona una vista sucinta del procesamiento del plano de datos
- Path Data (Datos de ruta): proporciona la vista más detallada de la gestión de paquetes DP. Recolectado para un número finito de paquetes, incluye una ID de depuración condicional que se puede utilizar para correlacionar el paquete DP con las depuraciones del plano de control, la marca de tiempo y los datos de seguimiento de trayectoria específicos de la función. Esta vista detallada tiene dos funciones opcionales
 - La copia de paquetes permite copiar paquetes de entrada y salida en varias capas del paquete (capa 2, capa 3 y capa 4)
 - La matriz de invocación de funciones (FIA) es la lista secuencial de funciones que ejecuta el plano de datos en el paquete. Estas características se derivan de la configuración predeterminada y habilitada por el usuario en el WLC 9800

Para obtener una explicación detallada de la función y las subopciones, refiérase a la [Función de Seguimiento de Paquetes de Ruta de Datos de Cisco IOS XE](#)

Para flujos de trabajo inalámbricos como la unión de puntos de acceso, la conectividad del cliente, etc., se realiza un seguimiento bidireccional del enlace ascendente

 Precaución: El rastreador de paquetes del plano de datos sólo analiza el encabezado CAPWAP externo. Por lo tanto, condiciones como el cliente inalámbrico mac no producen resultados útiles.

Paso 1. Defina la condición de interés.

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

 Advertencia: Tanto los comandos - debug platform condition feature como debug platform condition mac aaaa.bbbb.cccc están diseñados para el seguimiento de paquetes del plano de control y no devuelven ningún seguimiento de paquetes del plano de datos.

Paso 2. Para ver las condiciones habilitadas actualmente, ejecute el comando

```
# show platform conditions
```

Paso 3. Habilite packet-tracer para un número finito de paquetes. Este número de paquete se define como una potencia de 2 en el intervalo de 16 a 8192. De forma predeterminada, se capturan los datos de resumen y de función. Opcionalmente, puede optar por obtener sólo una vista de resumen si utiliza la subopción sólo resumen. También tiene subopciones disponibles para obtener el seguimiento de fia, definiendo el tamaño del paquete en bytes, rastrear punt, inyectar o descartar paquetes, etc.

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

Paso 4. (Opcionalmente) Puede copiar y volcar los paquetes a medida que se realiza el seguimiento

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

Paso 5. Habilitar depuración condicional.

```
# debug platform condition start
```

Paso 6. Para ver si el seguimiento de paquetes está recopilando algún resultado, verifique las estadísticas

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

Paso 7. Para ver la salida de packet-trace, ejecute el comando

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

Paso 8. (Opcional) Puede exportar el volcado de paquetes para que Cisco TAC lo analice sin conexión

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

Captura de paquetes integrada

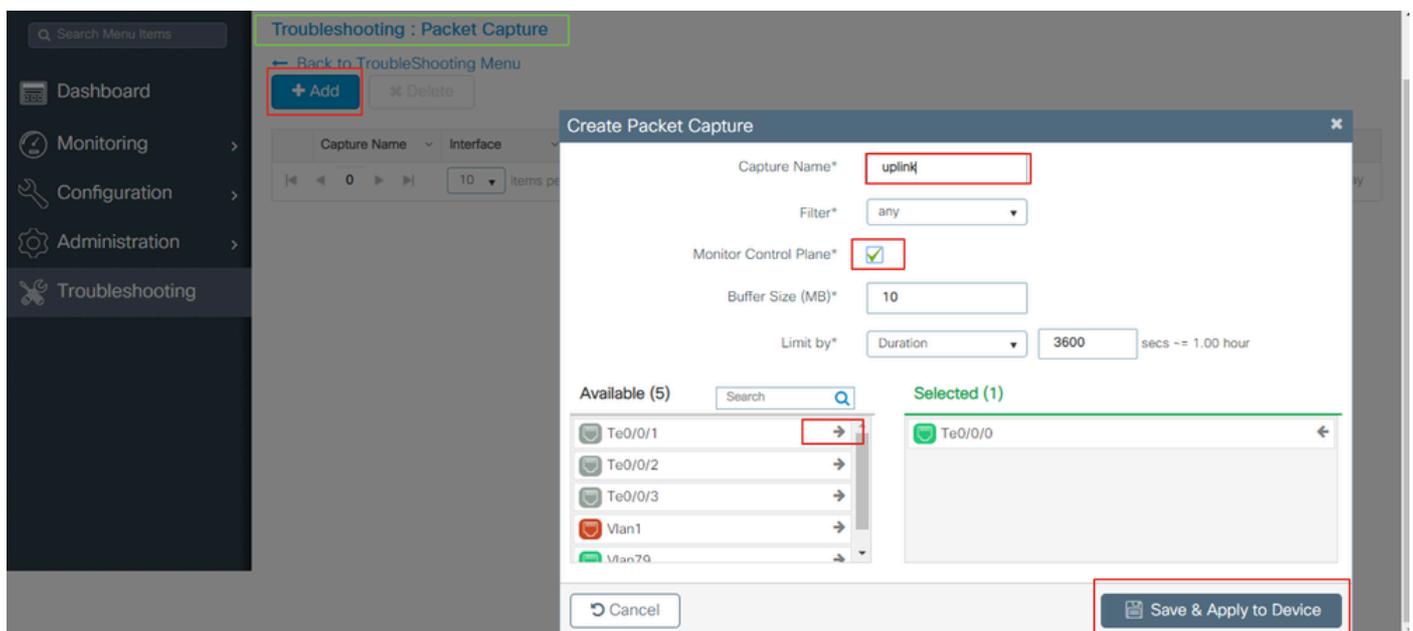
La captura de paquetes integrados (EPC) es una función de captura de paquetes que permite ver los paquetes destinados a los WLC Catalyst 9800, que se originan en ellos y que pasan por ellos. Estas capturas se pueden exportar para analizarlas sin conexión con Wireshark.

Para obtener más detalles sobre la función, consulte la [Guía de configuración de EPC](#)

En comparación con AireOS, en lugar de depender de la captura de paquetes y las capacidades de duplicación de tráfico en el switch de enlace ascendente, el WLC 9800 permite la captura de pcap en la propia caja.

En 9800, esta captura se puede configurar tanto desde la interfaz de línea de comandos (CLI) como desde la interfaz gráfica de usuario (GUI).

Para configurar mediante la GUI, navegue hasta Troubleshooting > Packet Capture > +Add



Paso 1. Defina el nombre de la captura de paquetes. Se permite un máximo de 8 caracteres.

Paso 2. Definir filtros, si los hubiera

Paso 3. Marque la casilla Monitor Control Traffic (Controlar el tráfico) si desea ver el tráfico dirigido a la CPU del sistema e inyectado de nuevo en el plano de datos

Paso 4. Defina el tamaño del búfer. Se permite un máximo de 100 MB

Paso 5. Defina el límite, ya sea por la duración que permite un rango de 1 a 1000000 segundos o por el número de paquetes que permite un rango de 1 a 100000 paquetes, según lo deseado

Paso 6. Elija la interfaz de la lista de interfaces de la columna izquierda y seleccione la flecha para moverla a la columna derecha

Paso 7. Guardar y aplicar al dispositivo

Paso 8. Para iniciar la captura, seleccione Iniciar

Paso 9. Puede dejar que la captura se ejecute hasta el límite definido. Para detener manualmente la captura, seleccione Detener.

Paso 10. Una vez detenido, un botón Exportar se encuentra disponible para hacer clic con la opción de descargar el archivo de captura (.pcap) en el escritorio local a través de https o servidor TFTP o servidor FTP o disco duro o flash del sistema local.

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

 Nota: CLI proporciona un poco más de granularidad de las opciones, como Limitar por. GUI es suficiente para capturar paquetes para casos prácticos comunes.

Para configurar mediante CLI:

Cree la captura de monitor:

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

Asocie un filtro. El filtro se puede especificar en línea o se puede hacer referencia a una ACL o a un mapa de clase.

En este ejemplo, es la ACL para hacer coincidir el tráfico entre las 2 direcciones IP del 9800 y otro WLC 5520. Situación típica para la resolución de problemas de movilidad:

```
conf t
```

```
ip access-list extended mobilitywlcs  
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 mobilitywlcs
```

Si desea que la captura se ejecute en un búfer circular, le dará tiempo para darse cuenta del problema y, a continuación, detener la captura y guardarla.

Si lo configura en 50MB buffer por ejemplo. Se necesitan como máximo 50 MB de disco en el 9800 y es bastante grande para capturar varios minutos de datos con la esperanza de que se produzca el problema.

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

Comience la captura. Puede modificarlo desde la GUI o la CLI:

```
monitor capture uplink start
```

La captura está ahora activa.

Permita que recopile los datos necesarios.

Detenga la captura. Puede hacerlo a través de la GUI o la CLI:

```
monitor capture uplink stop
```

Puede recuperar la captura desde la GUI > Troubleshooting > Packet Capture > Export.

O bien, cárguela en un servidor desde CLI. Ejemplo vía ftp:

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

Una vez recopilados los datos necesarios, elimine la captura:

no monitor capture uplink

LED de alarma y alarmas de plataforma crítica

Todos los appliances de la serie 9800 (9800-L, 9800-40 y 9800-80) tienen un LED ALM en el panel frontal. Si ese LED se pone rojo, significa que hay una alarma crítica en la plataforma.

Puede verificar las alarmas que hacen que el LED se vuelva rojo con el 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]

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).