

Resolución de problemas con la función de seguimiento de paquetes de ruta de datos IOS-XE

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Topología de referencia](#)

[Seguimiento de paquetes en uso](#)

[Guía de inicio rápido](#)

[Habilitar depuraciones condicionales de plataforma](#)

[Habilitar seguimiento de paquetes](#)

[Limitación de la Condición de Salida con Rastros de Paquetes](#)

[Mostrar los resultados de seguimiento de paquetes](#)

[Seguimiento FIA](#)

[Mostrar los resultados de seguimiento de paquetes](#)

[Verifique el FIA asociado con una interfaz](#)

[Volcar los paquetes rastreados](#)

[Eliminar seguimiento](#)

[Ejemplo de escenario de seguimiento de descarte](#)

[Inyectar y puntear trazas](#)

[Seguimiento de caídas de IOSd](#)

[Seguimiento de ruta de salida IOSd](#)

[seguimiento de paquetes LFTS](#)

[Coincidencia de patrones de seguimiento de paquetes basada en el filtro definido por el usuario \(sólo plataforma ASR1000\)](#)

[Ejemplos de Rastreo de Paquetes](#)

[Ejemplo de Rastreo de Paquetes - NAT](#)

[Ejemplo de Rastreo de Paquetes - VPN](#)

[Impacto en el rendimiento](#)

Introducción

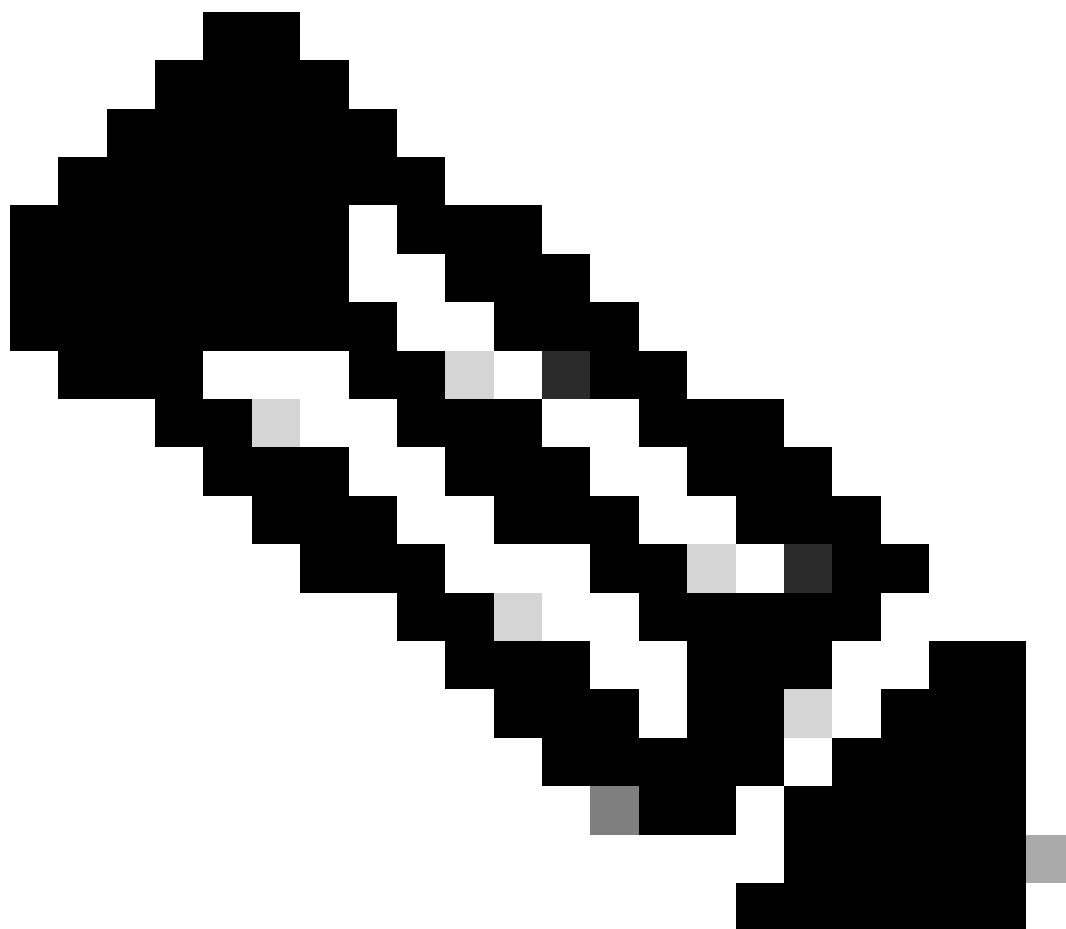
Este documento describe cómo realizar el seguimiento de paquetes de trayectoria de datos para el software Cisco IOS-XE® a través de la función Packet Trace.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento de esta información:

La función packet-trace está disponible en Cisco IOS-XE versión 3.10 y versiones posteriores en las plataformas de routing basadas en el procesador Quantum Flow (QFP), que incluyen los routers de las series ASR1000, ISR4000, ISR1000, Catalyst 1000, Catalyst 8000, CSR1000v y Catalyst 8000v. Esta función no es compatible con los routers de servicios de agregación de la serie ASR900 ni con los switches de la serie Catalyst que ejecutan el software Cisco IOS-XE.



Nota: La función packet-trace no funciona en la interfaz de administración dedicada, GigabitEthernet0, en los routers de la serie ASR1000, ya que los paquetes reenviados en esa interfaz no son procesados por el QFP.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y

hardware.

- Software Cisco IOS-XE versión 3.10S (15.3(3)S) y posteriores
- Router de la serie ASR1000

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Para identificar problemas como la configuración incorrecta, la sobrecarga de capacidad o incluso el error de software normal durante la resolución de problemas, es necesario entender qué le sucede a un paquete dentro de un sistema. La función Cisco IOS-XE Packet Trace responde a esta necesidad. Proporciona un método de seguridad de campo que se utiliza para la contabilidad y para capturar los detalles del proceso por paquete basados en una clase de condiciones definidas por el usuario.

Topología de referencia

Este diagrama ilustra la topología que se utiliza para los ejemplos que se describen en este documento:



Seguimiento de paquetes en uso

Para ilustrar el uso de la función de seguimiento de paquetes, el ejemplo que se utiliza en esta sección describe un seguimiento del tráfico del Protocolo de mensajes de control de Internet (ICMP) desde la estación de trabajo local 172.16.10.2 (detrás de ASR1K) hasta el host remoto 172.16.20.2 en la dirección de ingreso en la interfaz GigabitEthernet0/0/1 en ASR1K.

Puede rastrear paquetes en el ASR1K con estos dos pasos:

1. Habilite los debugs condicionales de la plataforma para seleccionar los paquetes o el tráfico que desea rastrear en el ASR1K.
2. Habilite el seguimiento de paquetes de plataforma con la opción de seguimiento path-trace o Feature Invocation Array (FIA).

Guía de inicio rápido

Aquí tiene una guía de inicio rápido si ya está familiarizado con el contenido de este documento y desea una sección para ver rápidamente la CLI. Estos son solo algunos ejemplos para ilustrar el uso de la herramienta. Consulte las secciones posteriores que tratan la sintaxis en detalle y asegúrese de utilizar la configuración que se ajuste a sus necesidades.

1. Configurar condiciones de plataforma:

```
<#root>
```

```
debug platform condition ipv4 10.0.0.1/32 both
```

```
--> matches in and out packets with source  
or destination as 10.0.0.1/32
```

```
debug platform condition ipv4 access-list 198 egress
```

```
--> (Ensure access-list 198 is  
defined prior to configuring this command) - matches egress packets corresponding  
to access-list 198
```

```
debug platform condition interface gig 0/0/0 ingress
```

```
--> matches all ingress packets  
on interface gig 0/0/0
```

```
debug platform condition mpls 10 1 ingress
```

```
--> matches MPLS packets with top ingress  
label 10
```

```
debug platform condition ingress
```

```
--> matches all ingress packets on all interfaces  
(use cautiously)
```

Después de configurar una condición de plataforma, inicie las condiciones de plataforma con este comando CLI:

```
<#root>
```

```
debug platform condition start
```

2. Configurar seguimiento de paquetes:

<#root>

```
debug platform packet-trace packet 1024
```

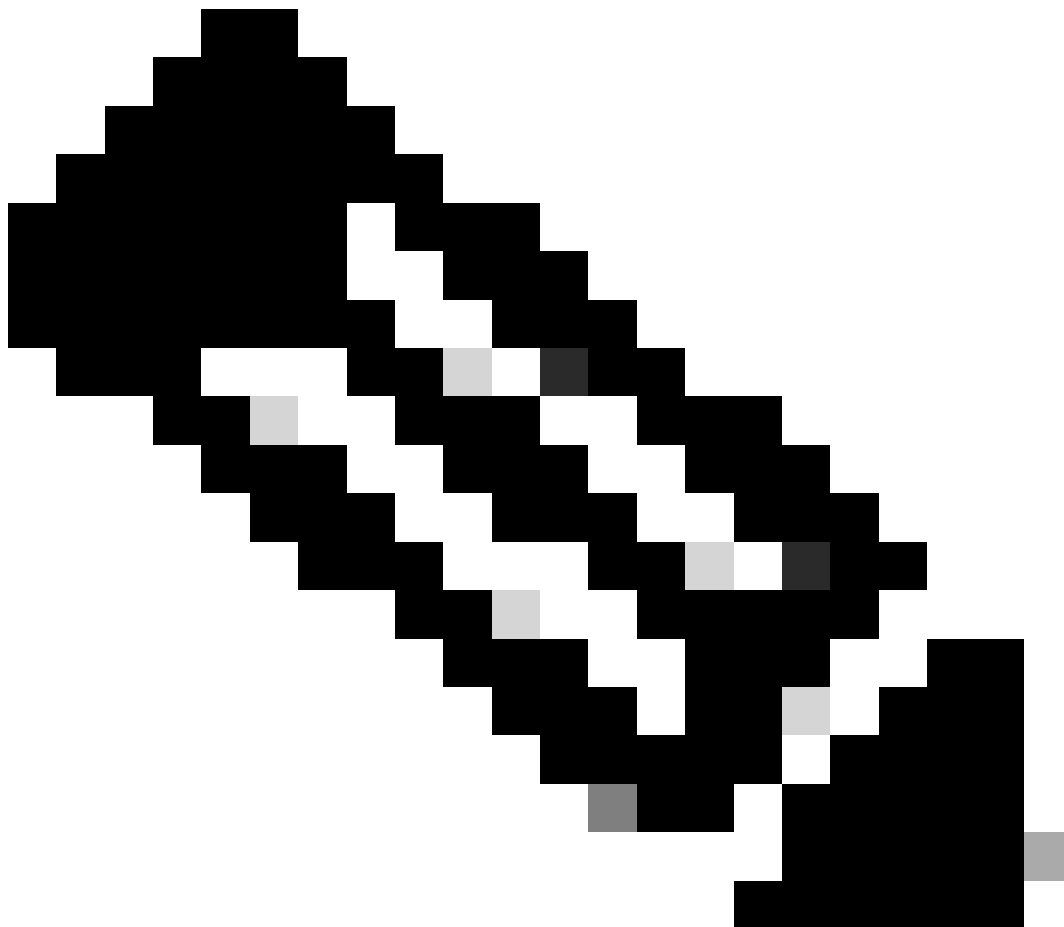
-> basic path-trace, and automatically stops tracing packets after 1024 packets. You can use "circular" option if needed

```
debug platform packet-trace packet 1024 fia-trace -
```

> enables detailed fia trace, stops tracing packets after 1024 packets

```
debug platform packet-trace drop [code <dropcode>]
```

-> if you want to trace/capture only packets that are dropped. Refer to Drop Trace section for more details.



Nota: En versiones anteriores de Cisco IOS-XE 3.x, también se requiere el comando `debug platform packet-trace enable` para iniciar la función `packet-trace`. Esto ya no es necesario en las versiones de Cisco IOS-XE 16.x.

Ingrese este comando para borrar el buffer de seguimiento y restablecer `packet-trace`:

```
<#root>
```

```
clear platform packet-trace statistics
```

```
--> clear the packet trace buffer
```

El comando para borrar las condiciones de la plataforma y la configuración de seguimiento de paquetes es:

```
<#root>
```

```
clear platform condition all
```

```
--> clears both platform conditions and the packet trace configuration
```

Comandos show

Verifique la condición de la plataforma y la configuración de seguimiento de paquetes después de aplicar los comandos anteriores para asegurarse de que tiene lo que necesita.

```
<#root>
```

```
show platform conditions
```

```
--> shows the platform conditions configured
```

```
show platform packet-trace configuration
```

```
--> shows the packet-trace configurations
```

```
show debugging
```

```
--> this can show both platform conditions and platform packet-trace configured
```

Estos son los comandos para verificar los paquetes rastreados/capturados:

```
<#root>
```

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

--> statistics of packets traced

```
show platform packet-trace summary
```

--> summary of all the packets traced, with input and output interfaces, processing result and reason.

```
show platform packet-trace packet 12
```

-> Display path trace of FIA trace details for the 12th packet in the trace buffer

Habilitar depuraciones condicionales de plataforma

La función Packet Trace se basa en la infraestructura de depuración condicional para determinar los paquetes que se rastrearán. La infraestructura de depuración condicional ofrece la capacidad de filtrar el tráfico en función de:

- Protocolo
- Dirección IP y máscara
- Lista de control de acceso (ACL)
- Interfaz
- Dirección del tráfico (entrada o salida)

Estas condiciones definen dónde y cuándo se aplican los filtros a un paquete.

Para el tráfico que se utiliza en este ejemplo, habilite los debugs condicionales de plataforma en la dirección de ingreso para los paquetes ICMP de 172.16.10.2 a 172.16.20.2. En otras palabras, seleccione el tráfico que desea rastrear. Hay varias opciones que puede utilizar para seleccionar este tráfico.

```
<#root>
```

```
ASR1000#
```

```
debug platform condition
```

```
?
```

```
egress      Egress only debug
feature     For a specific feature
ingress     Ingress only debug
interface   Set interface for conditional debug
ipv4       Debug IPv4 conditions
ipv6       Debug IPv6 conditions
start      Start conditional debug
stop       Stop conditional debug
```

En este ejemplo, se utiliza una lista de acceso para definir la condición, como se muestra aquí:

```
<#root>
```

```
ASR1000#
```

```
show access-list 150
```

```
Extended IP access list 150
```

```
10 permit icmp host 172.16.10.2 host 172.16.20.2
```

```
ASR1000#
```

```
debug platform condition interface gig 0/0/1 ipv4  
access-list 150 ingress
```

Para iniciar la depuración condicional, ingrese este comando:

```
<#root>
```

```
ASR1000#
```

```
debug platform condition start
```

Nota: Para detener o inhabilitar la infraestructura de depuración condicional, ingrese el comando `debug platform condition stop`.

Para ver los filtros de depuración condicional que se configuran, ingrese este comando:

```
<#root>
```

```
ASR1000#
```

```
show platform conditions
```

```
Conditional Debug Global State:
```

```
start
```

```
Conditions
```

```
Direction
```

```
-----|-----  
GigabitEthernet0/0/1
```

```
& IPV4 ACL [150]
```

```
ingress
```

Feature Condition	Format	Value
-------------------	--------	-------

```
ASR1000#
```

En resumen, esta configuración se ha aplicado hasta el momento:

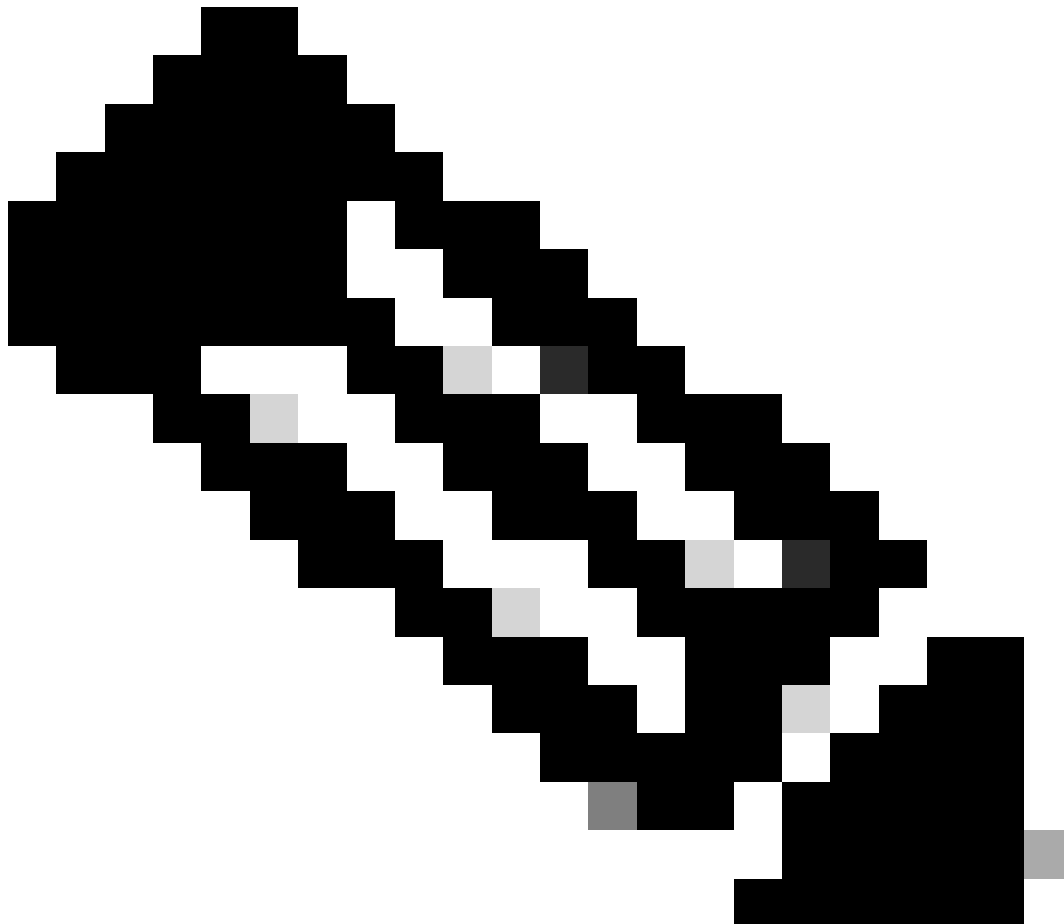
```
<#root>
```

```
access-list 150 permit icmp host 172.16.10.2 host 172.16.20.2
```

```
debug platform condition interface gig 0/0/1 ipv4 access-list 150 ingress
```

```
debug platform condition start
```

Habilitar seguimiento de paquetes



Nota: En esta sección se describen detalladamente las opciones de paquete y copia, y las demás opciones se describen más adelante en el documento.

Los seguimientos de paquetes se soportan tanto en las interfaces físicas como en las lógicas, como las interfaces de túnel o de acceso virtual.

Esta es la sintaxis de la CLI de seguimiento de paquetes:

<#root>

ASR1000#

debug platform packet-trace

?

copy	Copy packet data
drop	Trace drops only
inject	Trace injects only
packet	Packet count
punt	Trace punts only

<#root>

```
debug platform packet-trace packet <pkt-size/pkt-num> [fia-trace | summary-only]
[circular] [data-size <data-size>]
```

A continuación se describen las palabras clave de este comando:

- pkt-num - El número de paquete especifica el número máximo de paquetes que se mantienen a la vez.
- summary-only - Especifica que sólo se capturan los datos de resumen. El valor predeterminado es capturar tanto los datos de resumen como los datos de ruta de característica.
- fia-trace: realiza opcionalmente un seguimiento FIA además de la información de datos de la trayectoria.
- data-size - Esto le permite especificar el tamaño del buffer de datos de la trayectoria, de 2,048 a 16,384 bytes. El valor predeterminado es 2.048 bytes.

<#root>

```
debug platform packet-trace copy packet {in | out | both} [L2 | L3 | L4]
[size <num-bytes>]
```

A continuación se describen las palabras clave de este comando:

- in/out: especifica la dirección del flujo de paquetes que se va a copiar: entrada y/o salida.
- L2/L3/L4 - Esto le permite especificar la ubicación en la que comienza la copia del paquete. La ubicación predeterminada es la capa 2 (L2).
- size - Esto le permite especificar el número máximo de octetos que se copian. El valor predeterminado es 64 octetos.

Para este ejemplo, este es el comando utilizado para habilitar el seguimiento de paquetes para el tráfico que se selecciona con la infraestructura de depuración condicional:

```
<#root>  
ASR1000#  
debug platform packet-trace packet 16
```

Para revisar la configuración de seguimiento de paquetes, ingrese este comando:

```
<#root>  
ASR1000#  
show platform packet-trace configuration  
  
debug platform packet-trace packet 16 data-size 2048
```

También puede ingresar el comando show debugging para ver tanto las depuraciones condicionales de la plataforma como las configuraciones de seguimiento de paquetes:

```
<#root>  
ASR1000#  
show debugging  
  
IOSXE Conditional Debug Configs:  
  
Conditional Debug Global State: Start  
  
Conditions  
  
----- Direction |-----  
GigabitEthernet0/0/1 & IPV4 ACL [150] ingress
```

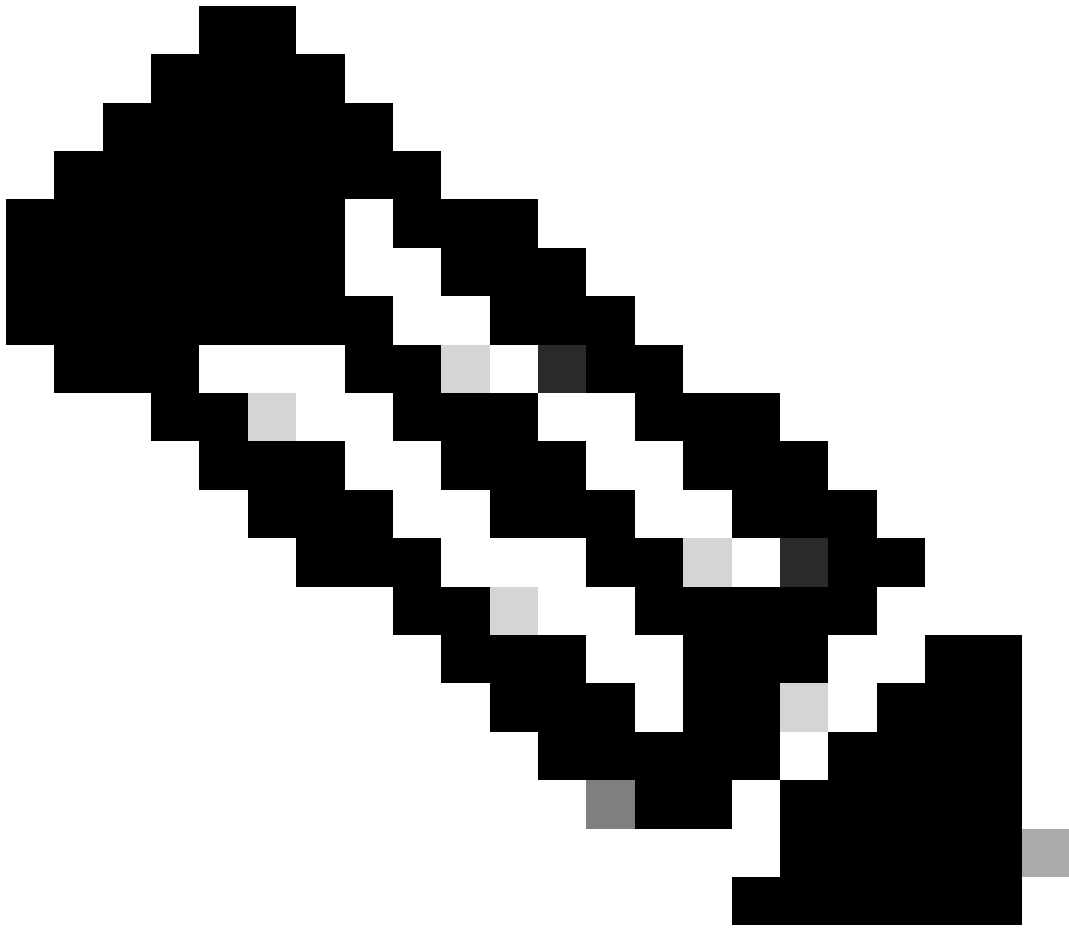
...

IOSXE Packet Tracing Configs:

Feature Condition	Format	Value
----- ----- -----		
Feature Type	Submode	Level
----- ----- -----		

IOSXE Packet Tracing Configs:

debug platform packet-trace packet 16 data-size 2048



Nota: Ingrese el comando clear platform condition all para borrar todas las condiciones de depuración de la plataforma y las configuraciones y datos de seguimiento de paquetes.

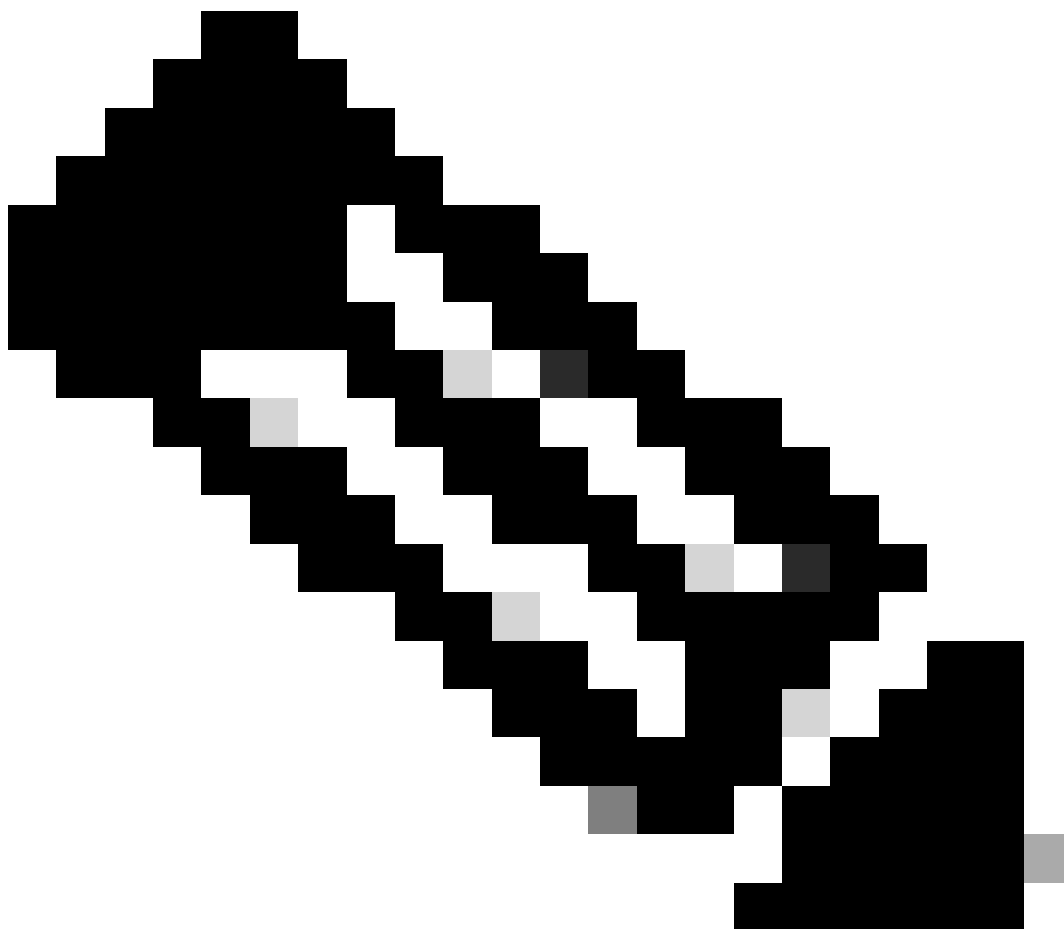
En resumen, estos datos de configuración se han utilizado hasta ahora para habilitar packet-trace:

<#root>

```
debug platform packet-trace packet 16
```

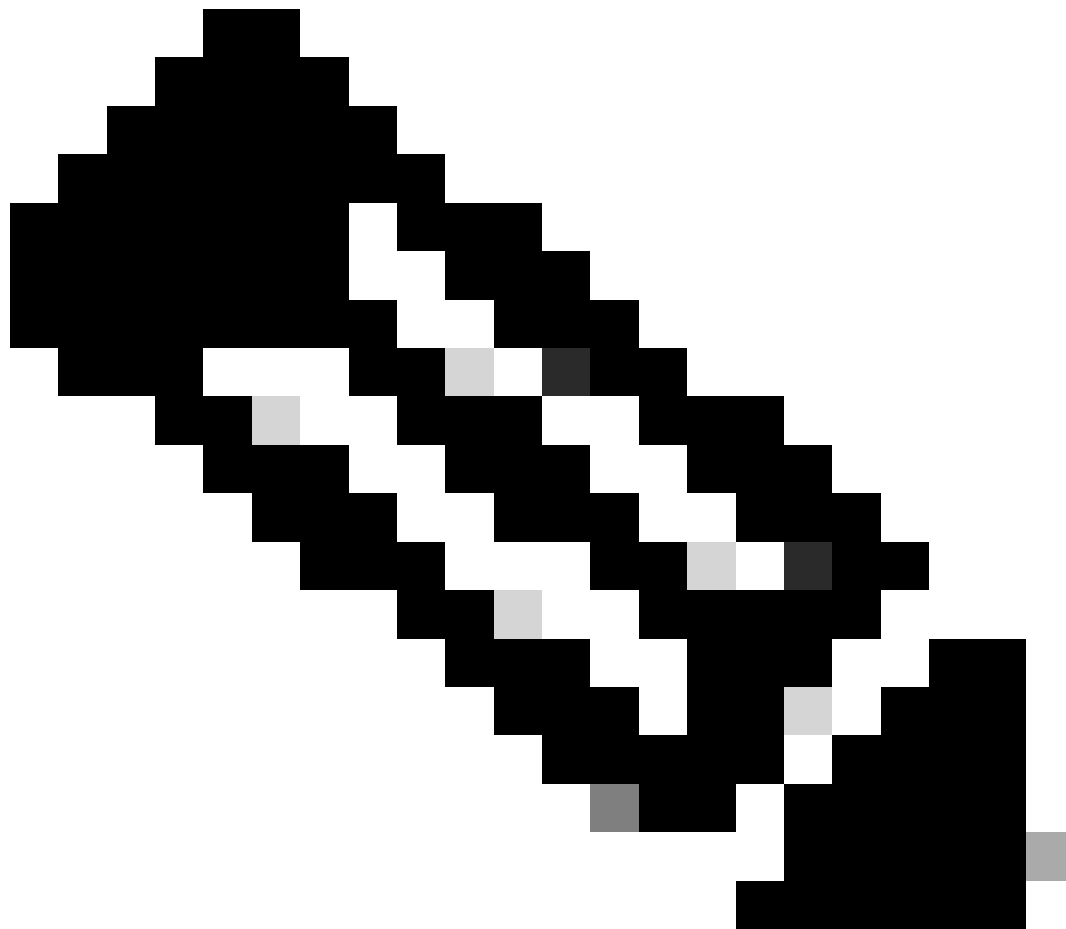
Limitación de la Condición de Salida con Rastreo de Paquetes

Las condiciones definen los filtros condicionales y cuándo se aplican a un paquete. Por ejemplo, `debug platform condition interface g0/0/0 egress` significa que un paquete se identifica como una coincidencia cuando alcanza el FIA de salida en la interfaz g0/0/0, de modo que cualquier procesamiento de paquetes que se lleve a cabo desde el ingreso hasta ese punto se pierde.



Nota: Cisco recomienda encarecidamente que utilice las condiciones de ingreso para los seguimientos de paquetes con el fin de obtener los datos más completos y significativos posibles. Se pueden utilizar las condiciones de salida, pero tenga en cuenta las limitaciones.

Mostrar los resultados de seguimiento de paquetes



Nota: En esta sección se asume que path-trace está habilitado.

El seguimiento de paquetes proporciona tres niveles específicos de inspección:

- Contabilidad
- Resumen por paquete
- Datos de ruta por paquete

Cuando se envían cinco paquetes de solicitud ICMP de 172.16.10.2 a 172.16.20.2, estos comandos se pueden utilizar para ver los resultados de seguimiento de paquetes:

```
<#root>
```

```
ASR1000#
```

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

Packets Traced: 5

Ingress 5
Inject 0
Forward 5
Punt 0
Drop 0
Consume 0

ASR1000#

show platform packet-trace summary

Pkt

	Input	Output	State	Reason
0				
	Gi0/0/1	Gi0/0/0	FWD	
1	Gi0/0/1	Gi0/0/0	FWD	
2	Gi0/0/1	Gi0/0/0	FWD	
3	Gi0/0/1	Gi0/0/0	FWD	
4	Gi0/0/1	Gi0/0/0	FWD	

ASR1000#

show platform packet-trace packet 0

Packet: 0

CBUG ID: 4

Summary

Input : GigabitEthernet0/0/1
Output : GigabitEthernet0/0/0
State : FWD

Timestamp

Start : 1819281992118 ns (05/17/2014 06:42:01.207240 UTC)
Stop : 1819282095121 ns (05/17/2014 06:42:01.207343 UTC)

Path Trace

Feature: IPV4

Source : 172.16.10.2
Destination : 172.16.20.2
Protocol : 1 (ICMP)

ASR1000#



Nota: El tercer comando proporciona un ejemplo que ilustra cómo ver el seguimiento de paquetes para cada paquete. En este ejemplo, se muestra el primer paquete rastreado.

A partir de estos resultados, puede ver que se realiza un seguimiento de cinco paquetes y que puede ver la interfaz de entrada, la interfaz de salida, el estado y el seguimiento de la trayectoria.

Estado	Observación
FWD	El paquete está programado/en cola para su entrega, para ser reenviado al siguiente salto a través de una interfaz de salida.
PUNTO	El paquete se envía desde el procesador de reenvío (FP) al procesador de routing (RP) (plano de control).
DEJAR CAER	El paquete se descarta en el FP. Ejecute el seguimiento FIA, utilice contadores de caídas globales o utilice los debugs de trayectoria de datos para encontrar más detalles por razones de caídas.
CONS	El paquete se consume durante un proceso de paquete, como durante la solicitud de ping ICMP o los paquetes criptográficos.

Los contadores ingress y inject en la salida de las estadísticas de seguimiento de paquetes corresponden a los paquetes que ingresan a través de una interfaz externa y a los paquetes que se consideran inyectados desde el plano de control, respectivamente.

Seguimiento FIA

La FIA contiene la lista de funciones que ejecutan secuencialmente los motores de procesador de paquetes (PPE) en el procesador de flujo cuántico (QFP) cuando un paquete se reenvía ya sea de entrada o de salida. Las funciones se basan en los datos de configuración que se aplican en el equipo. Por lo tanto, un seguimiento FIA ayuda a comprender el flujo del paquete a través del sistema a medida que se procesa el paquete.

Debe aplicar estos datos de configuración para habilitar el seguimiento de paquetes con FIA:

```
<#root>
```

```
ASR1000#
```

```
debug platform packet-trace packet 16 fia-trace
```

Mostrar los resultados de seguimiento de paquetes



Nota: En esta sección se asume que el seguimiento FIA está activado. Además, cuando agrega o modifica los comandos de seguimiento de paquetes actuales, se borran los detalles de seguimiento de paquetes almacenados en búfer, por lo que debe volver a enviar parte del tráfico para poder rastrearlo.

Envíe cinco paquetes ICMP de 172.16.10.2 a 172.16.20.2 después de ingresar el comando que se utiliza para habilitar el seguimiento FIA, como se describe en la sección anterior.

```
<#root>
```

```
ASR1000#
```

```
show platform packet-trace summary
```

Pkt	Input	Output	State	Reason
0	Gi0/0/1	Gi0/0/0	FWD	
1	Gi0/0/1	Gi0/0/0	FWD	
2	Gi0/0/1	Gi0/0/0	FWD	
3	Gi0/0/1	Gi0/0/0	FWD	

4 Gi0/0/1 Gi0/0/0 FWD

ASR1000#

show platform packet-trace packet 0

Packet: 0 CBUG ID: 9

Summary

Input : GigabitEthernet0/0/1
Output : GigabitEthernet0/0/0
State : FWD

Timestamp

Start : 1819281992118 ns (05/17/2014 06:42:01.207240 UTC)
Stop : 1819282095121 ns (05/17/2014 06:42:01.207343 UTC)

Path Trace

Feature: IPV4

Source : 172.16.10.2
Destination : 172.16.20.2
Protocol : 1 (ICMP)

Feature: FIA_TRACE

Entry : 0x8059dbe8 - DEBUG_COND_INPUT_PKT
Timestamp : 3685243309297

Feature: FIA_TRACE

Entry : 0x82011a00 - IPV4_INPUT_DST_LOOKUP_CONSUME
Timestamp : 3685243311450

Feature: FIA_TRACE

Entry : 0x82000170 - IPV4_INPUT_FOR_US_MARTIAN
Timestamp : 3685243312427

Feature: FIA_TRACE

Entry : 0x82004b68 - IPV4_OUTPUT_LOOKUP_PROCESS
Timestamp : 3685243313230

Feature: FIA_TRACE

Entry : 0x8034f210 - IPV4_INPUT_IPOPTIONS_PROCESS
Timestamp : 3685243315033

Feature: FIA_TRACE

Entry : 0x82013200 - IPV4_OUTPUT_GOTO_OUTPUT_FEATURE
Timestamp : 3685243315787

Feature: FIA_TRACE

Entry : 0x80321450 - IPV4_VFR_REFRAG
Timestamp : 3685243316980

Feature: FIA_TRACE

Entry : 0x82014700 - IPV6_INPUT_L2_REWRITE
Timestamp : 3685243317713

Feature: FIA_TRACE

Entry : 0x82000080 - IPV4_OUTPUT_FRAG
Timestamp : 3685243319223

Feature: FIA_TRACE

Entry : 0x8200e500 - IPV4_OUTPUT_DROP_POLICY
Timestamp : 3685243319950

Feature: FIA_TRACE

Entry : 0x8059aff4 - PACTRAC_OUTPUT_STATS
Timestamp : 3685243323603

Feature: FIA_TRACE

Entry : 0x82016100 - MARMOT_SPA_D_TRANSMIT_PKT
Timestamp : 3685243326183

ASR1000#

Verifique el FIA asociado con una interfaz

Cuando se habilitan los debugs condicionales de plataforma, se agrega la depuración condicional al FIA como una función. Según el orden de las funciones de procesamiento en la interfaz, el filtro condicional debe configurarse en consecuencia; por ejemplo, si la dirección anterior o posterior a NAT debe utilizarse en el filtro condicional.

Este resultado muestra el orden de las funciones en el FIA para la depuración condicional de la plataforma que se habilita en la dirección de ingreso:

```
<#root>
```

```
ASR1000#
```

```
show platform hardware qfp active interface if-name GigabitEthernet 0/0/1
```

```
General interface information
```

```
Interface Name: GigabitEthernet0/0/1
```

```
Interface state: VALID
```

```
Platform interface handle: 10
```

```
QFP interface handle: 8
```

```
Rx uidb: 1021
```

```
Tx uidb: 131064
```

```
Channel: 16
```

```
Interface Relationships
```

```
BGPPA/QPPB interface configuration information
```

```
Ingress: BGPPA/QPPB not configured. flags: 0000
```

```
Egress : BGPPA not configured. flags: 0000
```

```
ipv4_input enabled.
```

```
ipv4_output enabled.
```

```
layer2_input enabled.
```

```
layer2_output enabled.
```

```
ess_ac_input enabled.
```

```
Features Bound to Interface:
```

```
2 GIC FIA state
```

```
48 PUNT INJECT DB
```

```
39 SPA/Marmot server
```

```
40 ethernet
```

```
1 IFM
```

```
31 icmp_svr
```

```
33 ipfrag_svr
```

```
34 ipreass_svr
```

```
36 ipvfr_svr
```

```
37 ipv6vfr_svr
```

```
12 CPP IPSEC
```

```
Protocol 0 - ipv4_input
```

```
FIA handle - CP:0x108d99cc DP:0x8070f400
```

```
IPV4_INPUT_DST_LOOKUP_ISSUE (M)
```

```
IPV4_INPUT_ARL_SANITY (M)
```

```
CBUG_INPUT_FIA
```

DEBUG_COND_INPUT_PKT

IPV4_INPUT_DST_LOOKUP_CONSUME (M)
IPV4_INPUT_FOR_US_MARTIAN (M)
IPV4_INPUT_IPSEC_CLASSIFY
IPV4_INPUT_IPSEC_COPROC_PROCESS
IPV4_INPUT_IPSEC_RERUN_JUMP
IPV4_INPUT_LOOKUP_PROCESS (M)
IPV4_INPUT_IPOPTIONS_PROCESS (M)
IPV4_INPUT_GOTO_OUTPUT_FEATURE (M)
Protocol 1 - ipv4_output
FIA handle - CP:0x108d9a34 DP:0x8070eb00
IPV4_OUTPUT_VFR
MC_OUTPUT_GEN_RECYCLE (D)
IPV4_VFR_REFRAG (M)
IPV4_OUTPUT_IPSEC_CLASSIFY
IPV4_OUTPUT_IPSEC_COPROC_PROCESS
IPV4_OUTPUT_IPSEC_RERUN_JUMP
IPV4_OUTPUT_L2_REWRITE (M)
IPV4_OUTPUT_FRAG (M)
IPV4_OUTPUT_DROP_POLICY (M)
PACTRAC_OUTPUT_STATS
MARMOT_SPA_D_TRANSMIT_PKT
DEF_IF_DROP_FIA (M)
Protocol 8 - layer2_input
FIA handle - CP:0x108d9bd4 DP:0x8070c700
LAYER2_INPUT_SIA (M)
CBUG_INPUT_FIA
DEBUG_COND_INPUT_PKT
LAYER2_INPUT_LOOKUP_PROCESS (M)
LAYER2_INPUT_GOTO_OUTPUT_FEATURE (M)
Protocol 9 - layer2_output
FIA handle - CP:0x108d9658 DP:0x80714080
LAYER2_OUTPUT_SERVICEWIRE (M)
LAYER2_OUTPUT_DROP_POLICY (M)
PACTRAC_OUTPUT_STATS
MARMOT_SPA_D_TRANSMIT_PKT
DEF_IF_DROP_FIA (M)
Protocol 14 - ess_ac_input
FIA handle - CP:0x108d9ba0 DP:0x8070cb80
PPPOE_GET_SESSION
ESS_ENTER_SWITCHING
PPPOE_HANDLE_UNCLASSIFIED_SESSION
DEF_IF_DROP_FIA (M)

QfpEth Physical Information
DPS Addr: 0x11215eb8
Submap Table Addr: 0x00000000
VLAN Ethertype: 0x8100
QOS Mode: Per Link

ASR1000#



Nota: CBUG_INPUT_FIA y DEBUG_COND_INPUT_PKT corresponden a las funciones de depuración condicional que se configuran en el router.

Volcar los paquetes rastreados

Puede copiar y volcar los paquetes a medida que se realiza un seguimiento, como se describe en esta sección. Este ejemplo muestra cómo copiar un máximo de 2.048 bytes de los paquetes en la dirección de ingreso (172.16.10.2 a 172.16.20.2).

Este es el comando adicional que se necesita:

```
<#root>
```

```
ASR1000#
```

```
debug platform packet-trace copy packet input size 2048
```



Nota: El tamaño del paquete que se copia está en el rango de 16 a 2.048 bytes.

Ingrese este comando para volcar los paquetes copiados:

```
<#root>
```

```
ASR1000#
```

```
show platform packet-trace packet 0
```

```
Packet: 0          CBUG ID: 14
Summary
Input   : GigabitEthernet0/0/1
Output  : GigabitEthernet0/0/0
State   : FWD
Timestamp
  Start  : 1819281992118 ns (05/17/2014 06:40:01.207240 UTC)
  Stop   : 1819282095121 ns (05/17/2014 06:40:01.207343 UTC)
Path Trace
Feature: IPV4
```



```
Source      : 172.16.10.2
Destination : 172.16.20.2
Protocol    : 1 (ICMP)
Feature: FIA_TRACE
Entry      : 0x8059dbe8 - DEBUG_COND_INPUT_PKT
Timestamp  : 4458180580929
```

<some content excluded>

```
Feature: FIA_TRACE
Entry      : 0x82016100 - MARMOT_SPA_D_TRANSMIT_PKT
Timestamp  : 4458180593896
```

Packet Copy In

```
a4934c8e 33020023 33231379 08004500 00640160 0000ff01 5f16ac10 0201ac10
01010800 1fd40024 00000000 000184d0 d980abcd abcdabcd abcdabcd abcdabcd
abcdabcd abcdabcd abcdabcd abcdabcd abcdabcd abcdabcd abcdabcd abcdabcd
abcdabcd abcdabcd abcdabcd abcdabcd abcd
```

ASR1000#

Eliminar seguimiento

El rastreo de caídas está disponible en la versión 3.11 y posteriores del software Cisco IOS-XE. Habilita el seguimiento de paquetes sólo para paquetes perdidos. A continuación se indican algunos aspectos destacados de esta función:

- Opcionalmente, le permite especificar la retención de paquetes para un código de descarte específico.
- Se puede utilizar sin condiciones globales o de interfaz para capturar eventos de caídas.
- Una captura de evento de descarte significa que sólo se realiza un seguimiento de la propia caída, no de la vida útil del paquete. Sin embargo, todavía le permite capturar datos de resumen, datos de tupla y el paquete para ayudar a refinar las condiciones o proporcionar pistas para el siguiente paso de depuración.

Esta es la sintaxis de comando que se utiliza para habilitar los seguimientos de paquetes de tipo descartado:

<#root>

```
debug platform packet-trace drop [code <code-num>]
```

El código de descarte es el mismo que el ID de descarte, como se informó en el resultado del comando `show platform hardware qfp active statistics drop detail`:

<#root>

```
ASR1000#
```

```
show platform hardware qfp active statistics drop detail
```

```
-----
```

ID		Packets	Octets
Global Drop Stats			

60			
IpTtlExceeded		3	126
8			
Ipv4Ac1		32	3432

```
-----
```

Ejemplo de escenario de seguimiento de descarte

Aplice esta ACL en la interfaz Gig 0/0/0 del ASR1K para descartar el tráfico de 172.16.10.2 a 172.16.20.2:

```
access-list 199 deny ip host 172.16.10.2 host 172.16.20.2
access-list 199 permit ip any any
interface Gig 0/0/0
 ip access-group 199 out
```

Con la ACL en su lugar, que descarta el tráfico del host local al host remoto, aplique esta configuración de rastreo de caídas:

```
<#root>
```

```
debug platform condition interface Gig 0/0/1 ingress
```

```
debug platform condition start
```

```
debug platform packet-trace packet 1024 fia-trace
```

```
debug platform packet-trace drop
```

Envíe cinco paquetes de solicitud ICMP de 172.16.10.2 a 172.16.20.2. El seguimiento de descarte captura estos paquetes que son descartados por la ACL, como se muestra:

<#root>

ASR1000#

show platform packet-trace statistics

Packets Summary
Matched 5
Traced 5
Packets Received
Ingress 5
Inject 0
Packets Processed
Forward 0
Punt 0

Drop 5
Count Code Cause
5 8 Ipv4Acl

Consume 0

ASR1000#

show platform packet-trace summary

Pkt	Input	Output	State	Reason
0	Gi0/0/1	Gi0/0/0	DROP	8 (Ipv4Acl)
1	Gi0/0/1	Gi0/0/0	DROP	8 (Ipv4Acl)
2	Gi0/0/1	Gi0/0/0	DROP	8 (Ipv4Acl)
3	Gi0/0/1	Gi0/0/0	DROP	8 (Ipv4Acl)
4	Gi0/0/1	Gi0/0/0	DROP	8 (Ipv4Acl)

ASR1K#

debug platform condition stop

ASR1K#

show platform packet-trace packet 0

Packet: 0 CBUG ID: 140
Summary
Input : GigabitEthernet0/0/1
Output : GigabitEthernet0/0/0

State : DROP 8 (Ipv4Acl)

Timestamp

Start : 1819281992118 ns (05/17/2014 06:42:01.207240 UTC)
Stop : 1819282095121 ns (05/17/2014 06:42:01.207343 UTC)

Path Trace

Feature: IPV4

Source : 172.16.10.2

Destination : 172.16.20.2

```
Protocol      : 1 (ICMP)
Feature: FIA_TRACE
Entry        : 0x806c7eac - DEBUG_COND_INPUT_PKT
Lapsed time: 1031 ns
Feature: FIA_TRACE
Entry        : 0x82011c00 - IPV4_INPUT_DST_LOOKUP_CONSUME
Lapsed time: 657 ns
Feature: FIA_TRACE
Entry        : 0x806a2698 - IPV4_INPUT_ACL
Lapsed time: 2773 ns
Feature: FIA_TRACE
Entry        : 0x82000170 - IPV4_INPUT_FOR_US_MARTIAN
Lapsed time: 1013 ns
Feature: FIA_TRACE
Entry        : 0x82004500 - IPV4_OUTPUT_LOOKUP_PROCESS
Lapsed time: 2951 ns
Feature: FIA_TRACE
Entry        : 0x8041771c - IPV4_INPUT_IPOPTIONS_PROCESS
Lapsed time: 373 ns
Feature: FIA_TRACE
Entry        : 0x82013400 - MPLS_INPUT_GOTO_OUTPUT_FEATURE
Lapsed time: 2097 ns
Feature: FIA_TRACE
Entry        : 0x803c60b8 - IPV4_MC_OUTPUT_VFR_REFRAG
Lapsed time: 373 ns
Feature: FIA_TRACE
Entry        : 0x806db148 - OUTPUT_DROP
Lapsed time: 1297 ns
Feature: FIA_TRACE
Entry        : 0x806a0c98 - IPV4_OUTPUT_ACL
Lapsed time: 78382 ns
```

ASR1000#

Inyectar y puntear trazas

La función de seguimiento de paquetes de inserción y punt se agregó en la versión 3.12 y posteriores del software Cisco IOS-XE para rastrear paquetes de punt (paquetes recibidos en el FP que se puntean en el plano de control) e inject (paquetes que se inyectan en el FP desde el plano de control).



Nota: El rastreo de punt puede funcionar sin las condiciones globales o de interfaz, al igual que un rastreo de drop. Sin embargo, deben definirse las condiciones para que funcione un seguimiento de inyección.

A continuación se muestra un ejemplo de `a punt` e `inject packet trace` cuando hace ping desde el ASR1K a un router adyacente:

```
<#root>
```

```
ASR1000#
```

```
debug platform condition ipv4 172.16.10.2/32 both
```

ASR1000#

debug platform condition start

ASR1000#

debug platform packet-trace punt

ASR1000#

debug platform packet-trace inject

ASR1000#

debug platform packet-trace packet 16

ASR1000#

ASR1000#ping 172.16.10.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.10.2, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 14/14/15 ms

ASR1000#

Ahora puede verificar los resultados punt y nject trace resultados:

<#root>

ASR1000#

show platform packet-trace summary

Pkt	Input	Output	State	Reason
0	INJ.2	Gi0/0/1	FWD	
1	Gi0/0/1	internal0/0/rp:0	PUNT	11 (For-us data)
2	INJ.2	Gi0/0/1	FWD	
3	Gi0/0/1	internal0/0/rp:0	PUNT	11 (For-us data)
4	INJ.2	Gi0/0/1	FWD	
5	Gi0/0/1	internal0/0/rp:0	PUNT	11 (For-us data)
6	INJ.2	Gi0/0/1	FWD	
7	Gi0/0/1	internal0/0/rp:0	PUNT	11 (For-us data)
8	INJ.2	Gi0/0/1	FWD	
9	Gi0/0/1	internal0/0/rp:0	PUNT	11 (For-us data)

ASR1000#

show platform packet-trace packet 0

Packet: 0 CBUG ID: 120
Summary

Input : INJ.2

Output : GigabitEthernet0/0/1
State : FWD
Timestamp
Start : 115612780360228 ns (05/29/2014 15:02:55.467987 UTC)
Stop : 115612780380931 ns (05/29/2014 15:02:55.468008 UTC)
Path Trace
Feature: IPV4
Source : 172.16.10.1
Destination : 172.16.10.2
Protocol : 1 (ICMP)

```
ASR1000#
ASR1000#
```

```
show platform packet-trace packet 1
```

```
Packet: 1          CBUG ID: 121
Summary
Input   : GigabitEthernet0/0/1
Output  : internal0/0/rp:0
```

```
State      : PUNT 11 (For-us data)
```

```
Timestamp
Start   : 115612781060418 ns (05/29/2014 15:02:55.468687 UTC)
Stop    : 115612781120041 ns (05/29/2014 15:02:55.468747 UTC)
Path Trace
Feature: IPV4
Source   : 172.16.10.2
Destination : 172.16.10.1
Protocol : 1 (ICMP)
```

Mejora de Packet Trace con coincidencia de IOSd y LFTS Punt/Inject Trace y UDF (novedad en 17.3.1)

La función de seguimiento de paquetes se mejora aún más para proporcionar información de seguimiento adicional para los paquetes originados o destinados a IOSd u otros procesos BinOS en la versión 17.3.1 de Cisco IOS-XE.

Seguimiento de caídas de IOSd

Con esta mejora, el seguimiento de paquetes se extiende a IOSd, y puede proporcionar información sobre cualquier caída de paquetes dentro de IOSd, que generalmente se informa en el resultado de *show ip traffic*. No se requiere ninguna configuración adicional para habilitar el seguimiento de caídas IOSd. Este es un ejemplo de un paquete UDP descartado por IOSd debido a un error de checksum incorrecto:

<#root>

```
Router#debug platform condition ipv4 10.118.74.53/32 both
Router#debug platform condition start
Router#debug platform packet-trace packet 200
Packet count rounded up from 200 to 256
```

Router#

```
Router#show plat pack pa 0
Packet: 0          CBUG ID: 674
```

Summary

```
Input       : GigabitEthernet1
Output      : internal0/0/rp:0
State       : PUNT 11 (For-us data)
```

Timestamp

```
Start       : 17756544435656 ns (06/29/2020 18:19:17.326313 UTC)
Stop        : 17756544469451 ns (06/29/2020 18:19:17.326346 UTC)
```

Path Trace

Feature: IPV4(Input)

```
Input       : GigabitEthernet1
Output      : <unknown>
Source      : 10.118.74.53
Destination : 172.18.124.38
Protocol    : 17 (UDP)
  SrcPort   : 2640
  DstPort   : 500
```

IOSd Path Flow: Packet: 0 CBUG ID: 674

Feature: INFRA

Pkt Direction: IN

Packet Rcvd From DATAPLANE

Feature: IP

Pkt Direction: IN

Packet Enqueued in IP layer

```
Source      : 10.118.74.53
Destination : 172.18.124.38
Interface   : GigabitEthernet1
```

Feature: IP

Pkt Direction: IN

FORWARDED To transport layer

```
Source      : 10.118.74.53
Destination : 172.18.124.38
Interface   : GigabitEthernet1
```

Feature: UDP

Pkt Direction: IN

DROPPED

UDP: Checksum error: dropping

Source : 10.118.74.53(2640)

Destination : 172.18.124.38(500)

Seguimiento de ruta de salida IOSd

El seguimiento de paquetes se mejora para mostrar la información de seguimiento de ruta y de procesamiento de protocolos a medida que el paquete se origina desde IOSd y se envía en la dirección de salida hacia la red. No se requiere configuración adicional para capturar la información de seguimiento de trayectoria de salida de IOSd. A continuación se muestra un ejemplo de seguimiento de trayectoria de salida para un paquete SSH que egresa del router:

<#root>

```
Router#show platform packet-trace packet 2
Packet: 2          CBUG ID: 2
```

IOSd Path Flow:

Feature: TCP

Pkt Direction: OUTtcp0: 0 SYNRCVD 172.18.124.38:22 172.18.124.55:52774 seq 3052140910 OPTS 4 ACK 2346

Feature: TCP

Pkt Direction: OUT

FORWARDED

TCP: Connection is in SYNRCVD state

ACK : 2346709419

SEQ : 3052140910

Source : 172.18.124.38(22)

Destination : 172.18.124.55(52774)

Feature: IP

Pkt Direction: OUTRoute out the generated packet.srcaddr: 172.18.124.38, dstaddr: 172.18.124.55

Feature: IP

Pkt Direction: OUTInject and forward successful srcaddr: 172.18.124.38, dstaddr: 172.18.124.55

Feature: TCP

Pkt Direction: OUTtcp0: 0 SYNRCVD 172.18.124.38:22 172.18.124.55:52774 seq 3052140910 OPTS 4 ACK 2346

Summary

Input : INJ.2

Output : GigabitEthernet1

State : FWD

Timestamp

```

Start   : 490928006866 ns (06/29/2020 13:31:30.807879 UTC)
Stop    : 490928038567 ns (06/29/2020 13:31:30.807911 UTC)
Path Trace
Feature: IPV4(Input)
Input   : internal0/0/rp:0
Output  : <unknown>
Source  : 172.18.124.38
Destination : 172.18.124.55
Protocol : 6 (TCP)
  SrcPort : 22
  DstPort : 52774
Feature: IPSec
Result  : IPSEC_RESULT_DENY
Action  : SEND_CLEAR
SA Handle : 0
Peer Addr : 172.18.124.55
Local Addr: 172.18.124.38

```

seguimiento de paquetes LFTS

LFTS (Linux Forwarding Transport Service) es un mecanismo de transporte para reenviar paquetes impulsados desde el CPP a aplicaciones distintas de IOSd. La mejora del seguimiento de paquetes LFTS agregó información de seguimiento para dichos paquetes en la salida de seguimiento de trayectoria. No se requiere ninguna configuración adicional para obtener la información de seguimiento de LFTS. A continuación se presenta un ejemplo de resultado de seguimiento LFTS para paquetes punteados a la aplicación NETCONF:

<#root>

```

Router#show plat packet-trace pac 0
Packet: 0          CBUG ID: 461
Summary
Input   : GigabitEthernet1
Output  : internal0/0/rp:0
State   : PUNT 11 (For-us data)
Timestamp
Start   : 647999618975 ns (06/30/2020 02:18:06.752776 UTC)
Stop    : 647999649168 ns (06/30/2020 02:18:06.752806 UTC)
Path Trace
Feature: IPV4(Input)
Input   : GigabitEthernet1
Output  : <unknown>
Source  : 10.118.74.53
Destination : 172.18.124.38
Protocol : 6 (TCP)
  SrcPort : 65365
  DstPort : 830

```

LFTS Path Flow: Packet: 0 CBUG ID: 461

```
Feature: LFTS
Pkt Direction: IN
  Punt Cause : 11
  subCause : 0
```

Coincidencia de patrones de seguimiento de paquetes basada en el filtro definido por el usuario (sólo plataforma ASR1000)

En la versión 17.3.1 de Cisco IOS-XE, también se agrega un nuevo mecanismo de coincidencia de paquetes a las familias de productos ASR1000 para que coincidan en un campo arbitrario de un paquete basado en la infraestructura de filtro definido por el usuario (UDF). Esto permite una coincidencia flexible de paquetes basada en campos que no forman parte de la estructura de encabezado L2/L3/L4 estándar. El siguiente ejemplo muestra una definición de FDU que coincide en 2 bytes del patrón definido por el usuario de 0x4D2 que comienza desde un desplazamiento de 26 bytes desde el encabezado del protocolo exterior L3.

```
udf grekey header outer 13 26 2
ip access-list extended match-grekey
 10 permit ip any any udf grekey 0x4D2 0xFFFF

debug plat condition ipv4 access-list match-grekey both
debug plat condition start
debug plat packet-trace pack 100
```

Ejemplos de Rastreo de Paquetes

Esta sección proporciona algunos ejemplos en los que la función de seguimiento de paquetes es útil para solucionar problemas.

Ejemplo de Rastreo de Paquetes - NAT

Con este ejemplo, se configura una traducción de direcciones de red (NAT) de origen de interfaz en la interfaz WAN de un ASR1K (Gig0/0/0) para la subred local (172.16.10.0/24).

Esta es la condición de plataforma y la configuración de seguimiento de paquetes que se utiliza para rastrear el tráfico de 172.16.10.2 a 172.16.20.2, que se convierte en traducido (NAT) en la interfaz Gig0/0/0:

```
debug platform condition interface Gig 0/0/1 ingress
debug platform condition start
```

```
debug platform packet-trace packet 1024 fia-trace
```

Cuando se envían cinco paquetes ICMP de 172.16.10.2 a 172.16.20.2 con una configuración NAT de origen de interfaz, estos son los resultados de seguimiento de paquetes:

```
<#root>
```

```
ASR1000#
```

```
show platform packet-trace summary
```

Pkt	Input	Output	State	Reason
0	Gi0/0/1	Gi0/0/0	FWD	
1	Gi0/0/1	Gi0/0/0	FWD	
2	Gi0/0/1	Gi0/0/0	FWD	
3	Gi0/0/1	Gi0/0/0	FWD	
4	Gi0/0/1	Gi0/0/0	FWD	

```
ASR1000#
```

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

```
Packets Summary  
Matched 5  
Traced 5  
Packets Received  
Ingress 5  
Inject 0  
Packets Processed  
Forward 5  
Punt 0  
Drop 0  
Consume 0
```

```
ASR1000#
```

```
show platform packet-trace packet 0
```

Packet: 0 CBUG ID: 146

Summary

Input : GigabitEthernet0/0/1
Output : GigabitEthernet0/0/0
State : FWD

Timestamp

Start : 3010217805313 ns (05/17/2014 07:01:52.227836 UTC)
Stop : 3010217892847 ns (05/17/2014 07:01:52.227923 UTC)

Path Trace

Feature: IPV4

Source : 172.16.10.2
Destination : 172.16.20.2
Protocol : 1 (ICMP)

Feature: FIA_TRACE

Entry : 0x806c7eac - DEBUG_COND_INPUT_PKT

Lapsed time: 1031 ns

Feature: FIA_TRACE

Entry : 0x82011c00 - IPV4_INPUT_DST_LOOKUP_CONSUME

Lapsed time: 462 ns

Feature: FIA_TRACE

Entry : 0x82000170 - IPV4_INPUT_FOR_US_MARTIAN

Lapsed time: 355 ns

Feature: FIA_TRACE

Entry : 0x803c6af4 - IPV4_INPUT_VFR

Lapsed time: 266 ns

Feature: FIA_TRACE

Entry : 0x82004500 - IPV4_OUTPUT_LOOKUP_PROCESS

Lapsed time: 942 ns

Feature: FIA_TRACE

Entry : 0x8041771c - IPV4_INPUT_IPOPTIONS_PROCESS

Lapsed time: 88 ns

Feature: FIA_TRACE

Entry : 0x82013400 - MPLS_INPUT_GOTO_OUTPUT_FEATURE

Lapsed time: 568 ns

Feature: FIA_TRACE

Entry : 0x803c6900 - IPV4_OUTPUT_VFR

Lapsed time: 266 ns

Feature: NAT

Direction : IN to OUT

Action : Translate Source

Old Address : 172.16.10.2 00028

New Address : 192.168.10.1 00002

Feature: FIA_TRACE

Entry : 0x8031c248 - IPV4_NAT_OUTPUT_FIA

Lapsed time: 55697 ns

Feature: FIA_TRACE

Entry : 0x801424f8 - IPV4_OUTPUT_THREAT_DEFENSE

Lapsed time: 693 ns

```
Feature: FIA_TRACE
Entry      : 0x803c60b8 - IPV4_MC_OUTPUT_VFR_REFRAG
Lapsed time: 88 ns
Feature: FIA_TRACE
Entry      : 0x82014900 - IPV6_INPUT_L2_REWRITE
Lapsed time: 444 ns
Feature: FIA_TRACE
Entry      : 0x82000080 - IPV4_OUTPUT_FRAG
Lapsed time: 88 ns
Feature: FIA_TRACE
Entry      : 0x8200e600 - IPV4_OUTPUT_DROP_POLICY
Lapsed time: 1457 ns
Feature: FIA_TRACE
Entry      : 0x82017980 - MARMOT_SPA_D_TRANSMIT_PKT
Lapsed time: 7431 ns
ASR1000#
```

Ejemplo de Rastreo de Paquetes - VPN

Con este ejemplo, se utiliza un túnel VPN de sitio a sitio entre el ASR1K y el router Cisco IOS para proteger el tráfico que fluye entre 172.16.10.0/24 y 172.16.20.0/24 (subredes locales y remotas).

Aquí está la condición de plataforma y la configuración de seguimiento de paquetes que se utiliza para rastrear el tráfico VPN que fluye de 172.16.10.2 a 172.16.20.2 en la interfaz Gig 0/0/1:

```
debug platform condition interface Gig 0/0/1 ingress
debug platform condition start
debug platform packet-trace packet 1024 fia-trace
```

Cuando se envían cinco paquetes ICMP de 172.16.10.2 a 172.16.20.2, que son cifrados por el túnel VPN entre ASR1K y el router Cisco IOS en este ejemplo, estas son las salidas de seguimiento de paquetes:



Nota: Los seguimientos de paquetes muestran el identificador de asociación de seguridad (SA) QFP en el seguimiento que se utiliza para cifrar el paquete, lo que resulta útil cuando se solucionan problemas de VPN IPsec para verificar que se utiliza la SA correcta para el cifrado.

<#root>

ASR1000#

show platform packet-trace summary

Pkt	Input	Output	State	Reason
0	Gi0/0/1	Gi0/0/0	FWD	
1	Gi0/0/1	Gi0/0/0	FWD	
2	Gi0/0/1	Gi0/0/0	FWD	
3	Gi0/0/1	Gi0/0/0	FWD	
4	Gi0/0/1	Gi0/0/0	FWD	

ASR1000#

show platform packet-trace packet 0

```

Packet: 0          CBUG ID: 211
Summary
Input      : GigabitEthernet0/0/1
Output     : GigabitEthernet0/0/0
State      : FWD
Timestamp
Start      : 4636921551459 ns (05/17/2014 07:28:59.211375 UTC)
Stop       : 4636921668739 ns (05/17/2014 07:28:59.211493 UTC)
Path Trace
Feature: IPV4
Source     : 172.16.10.2
Destination : 172.16.20.2
Protocol   : 1 (ICMP)
Feature: FIA_TRACE
Entry      : 0x806c7eac - DEBUG_COND_INPUT_PKT
Lapsed time: 622 ns
Feature: FIA_TRACE
Entry      : 0x82011c00 - IPV4_INPUT_DST_LOOKUP_CONSUME
Lapsed time: 462 ns
Feature: FIA_TRACE
Entry      : 0x82000170 - IPV4_INPUT_FOR_US_MARTIAN
Lapsed time: 320 ns
Feature: FIA_TRACE
Entry      : 0x82004500 - IPV4_OUTPUT_LOOKUP_PROCESS
Lapsed time: 1102 ns
Feature: FIA_TRACE
Entry      : 0x8041771c - IPV4_INPUT_IPOPTIONS_PROCESS
Lapsed time: 88 ns
Feature: FIA_TRACE
Entry      : 0x82013400 - MPLS_INPUT_GOTO_OUTPUT_FEATURE
Lapsed time: 586 ns
Feature: FIA_TRACE
Entry      : 0x803c6900 - IPV4_OUTPUT_VFR
Lapsed time: 266 ns
Feature: FIA_TRACE
Entry      : 0x80757914 - MC_OUTPUT_GEN_RECYCLE
Lapsed time: 195 ns
Feature: FIA_TRACE
Entry      : 0x803c60b8 - IPV4_MC_OUTPUT_VFR_REFRAG
Lapsed time: 88 ns

```

Feature: IPSec

Result : IPSEC_RESULT_SA
Action : ENCRYPT
SA Handle : 6
Peer Addr : 192.168.20.1
Local Addr: 192.168.10.1

Feature: FIA_TRACE

Entry : 0x8043caec - IPV4_OUTPUT_IPSEC_CLASSIFY

Lapsed time: 9528 ns

Feature: FIA_TRACE

Entry : 0x8043915c - IPV4_OUTPUT_IPSEC_DOUBLE_ACL

Lapsed time: 355 ns

Feature: FIA_TRACE

Entry : 0x8043b45c - IPV4_IPSEC_FEATURE_RETURN

Lapsed time: 657 ns

Feature: FIA_TRACE

Entry : 0x8043ae28 - IPV4_OUTPUT_IPSEC_RERUN_JUMP

Lapsed time: 888 ns

Feature: FIA_TRACE

Entry : 0x80436f10 - IPV4_OUTPUT_IPSEC_POST_PROCESS

Lapsed time: 2186 ns

Feature: FIA_TRACE

Entry : 0x8043b45c - IPV4_IPSEC_FEATURE_RETURN

Lapsed time: 675 ns

Feature: FIA_TRACE

Entry : 0x82014900 - IPV6_INPUT_L2_REWRITE

Lapsed time: 1902 ns

Feature: FIA_TRACE

Entry : 0x82000080 - IPV4_OUTPUT_FRAG

Lapsed time: 71 ns

Feature: FIA_TRACE

Entry : 0x8200e600 - IPV4_OUTPUT_DROP_POLICY

Lapsed time: 1582 ns

Feature: FIA_TRACE

Entry : 0x82017980 - MARMOT_SPA_D_TRANSMIT_PKT

Lapsed time: 3964 ns

ASR1000#

Impacto en el rendimiento

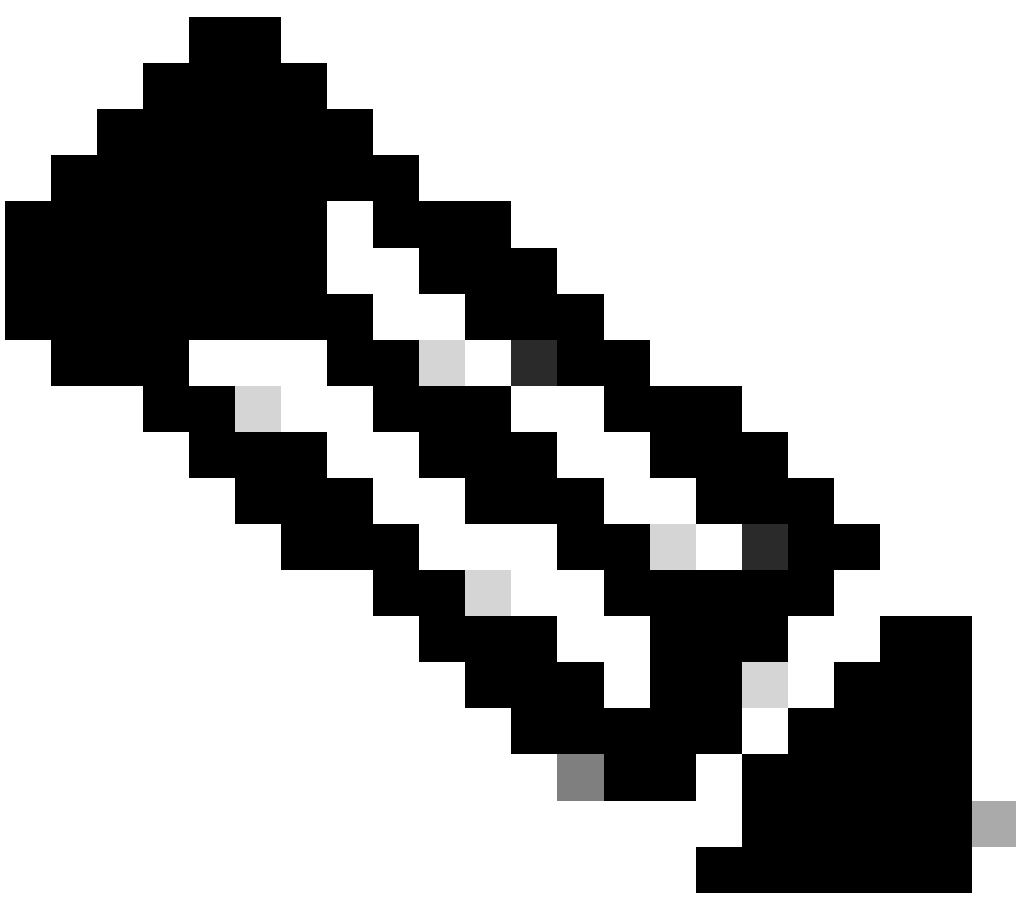
Los búferes de seguimiento de paquetes consumen QFP DRAM, por lo que debe tener en cuenta la cantidad de memoria que requiere una configuración y la cantidad de memoria disponible.

El impacto en el rendimiento varía en función de las opciones de seguimiento de paquetes habilitadas. El seguimiento de paquetes sólo afecta el rendimiento de reenvío de los paquetes que se rastrean, como aquellos paquetes que coinciden con las condiciones configuradas por el usuario. Cuanto más granular y detallada sea la información que configure el seguimiento de paquetes para capturar, mayor será el impacto que pueda tener en los recursos.

Al igual que con cualquier solución de problemas, lo mejor es adoptar un enfoque iterativo y habilitar solamente las opciones de seguimiento más detalladas cuando una situación de depuración lo justifique.

El uso de DRAM QFP se puede estimar con esta fórmula:

memoria necesaria = (sobrecarga de estadísticas) + número de paquetes * (tamaño de resumen + tamaño de datos de ruta + tamaño de copia)



Nota: Cuando la **sobrecarga de estadísticas** y el **tamaño de resumen** se fijan en 2 KB y 128 KB, respectivamente, el usuario puede configurar el **tamaño de los datos de la ruta** y el **tamaño de la copia**.

Información Relacionada

- [Guía de configuración de software de los routers de la serie de agregación Cisco ASR1000 - Seguimiento de paquetes](#)
- [Paquetes rechazados en routers de servicios de la serie ASR1000 de Cisco](#)
- [Soporte técnico y descargas de Cisco](#)

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).