

# Solução de problemas com o recurso IOS-XE Datapath Packet Trace

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Topologia de referência](#)

[Rastreamento de pacote em uso](#)

[Guia de início rápido](#)

[Habilitar depurações condicionais da plataforma](#)

[Ativar o Packet Trace](#)

[Limitação da condição de saída com rastreamentos de pacotes](#)

[Exibir os resultados do Packet Trace](#)

[Rastreamento FIA](#)

[Exibir os resultados do Packet Trace](#)

[Verifique o FIA associado a uma interface](#)

[Descartar os pacotes rastreados](#)

[Descartar Rastreamento](#)

[Exemplo de Cenário de Rastreamento de Eliminação](#)

[Injetar e Puncionar Rastreamentos](#)

[Rastreamento de queda IOSd](#)

[Rastreamento de caminho de saída IOSd](#)

[Rastreamento de pacotes LFTS](#)

[Correspondência de padrão de rastreamento de pacote com base no filtro definido pelo usuário \(somente plataforma ASR1000\)](#)

[Exemplos de rastreamento de pacote](#)

[Exemplo de Packet Trace - NAT](#)

[Exemplo de Packet Trace - VPN](#)

[Impacto de desempenho](#)

---

## Introdução

Este documento descreve como executar o rastreamento de pacote de caminho de dados para o software Cisco IOS-XE® através do recurso Packet Trace.

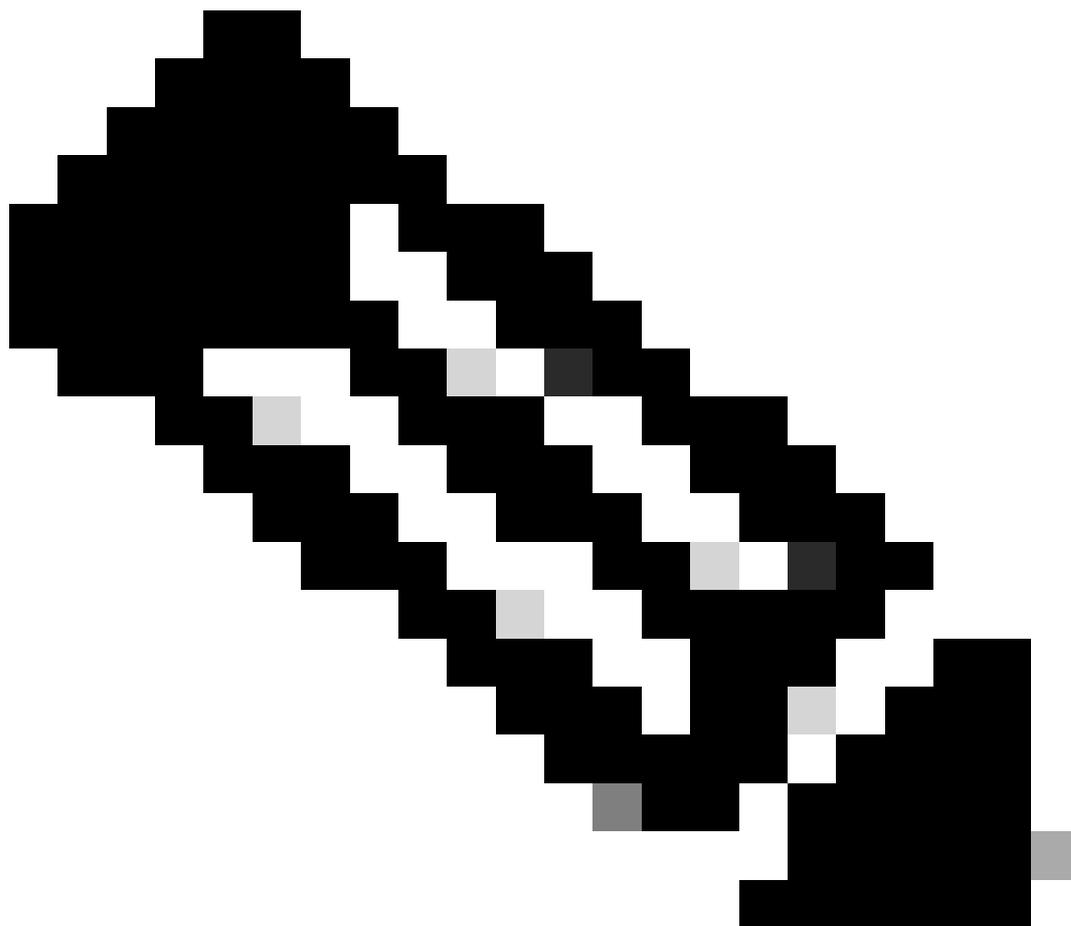
## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento dessas informações:

O recurso de rastreamento de pacotes está disponível no Cisco IOS-XE versão 3.10 e versões posteriores nas plataformas de roteamento baseadas em QFP (Quantum Flow Processor), que incluem os roteadores das séries ASR1000, ISR4000, ISR1000, Catalyst 1000, Catalyst 8000, CSR1000v e Catalyst 8000v. Este recurso não é suportado nos roteadores de serviços de agregação da série ASR900 ou nos switches da série Catalyst que executam o software Cisco IOS-XE.

---



Observação: o recurso de rastreamento de pacotes não funciona na interface de gerenciamento dedicada, GigabitEthernet0 nos roteadores da série ASR1000, já que os pacotes encaminhados nessa interface não são processados pelo QFP.

---

## Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Software Cisco IOS-XE versão 3.10S (15.3(3)S) e posterior
- Roteador ASR1000 Series

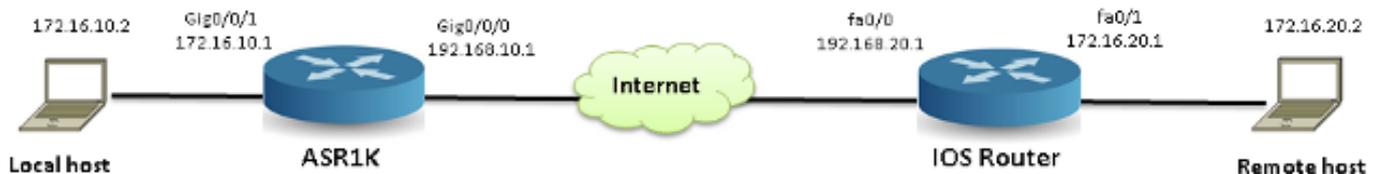
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

Para identificar problemas como configuração incorreta, sobrecarga de capacidade ou até mesmo o bug comum de software durante o Troubleshooting, é necessário entender o que acontece com um pacote dentro de um sistema. O recurso Packet Trace do Cisco IOS-XE atende a essa necessidade. Ele fornece um método seguro para campo que é usado para contabilidade e para capturar os detalhes do processo por pacote com base em uma classe de condições definidas pelo usuário.

## Topologia de referência

Este diagrama ilustra a topologia usada para os exemplos descritos neste documento:



## Rastreamento de pacote em uso

Para ilustrar o uso do recurso de rastreamento de pacotes, o exemplo usado nesta seção descreve um rastreamento do tráfego do Internet Control Message Protocol (ICMP) da estação de trabalho local 172.16.10.2 (atrás do ASR1K) para o host remoto 172.16.20.2 na direção de entrada na interface GigabitEthernet0/0/1 no ASR1K.

Você pode rastrear pacotes no ASR1K com estas duas etapas:

1. Ative as depurações condicionais da plataforma para selecionar os pacotes ou o tráfego que você deseja rastrear no ASR1K.
2. Ative o rastreamento de pacote da plataforma com a opção de rastreamento path-trace ou Feature Invocation Array (FIA).

## Guia de início rápido

Este é um guia de início rápido se você já está familiarizado com o conteúdo deste documento e

deseja uma seção para uma visão rápida da CLI. Estes são apenas alguns exemplos para ilustrar o uso da ferramenta. Consulte as seções posteriores que discutem as sintaxes em detalhes e certifique-se de usar a configuração apropriada a seu requisito.

## 1. Configure as condições da 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)
```

Depois que uma condição de plataforma for configurada, inicie as condições da plataforma com este comando CLI:

```
<#root>
```

```
debug platform condition start
```

## 2. Configurar o rastreamento de pacotes:

```
<#root>
```

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

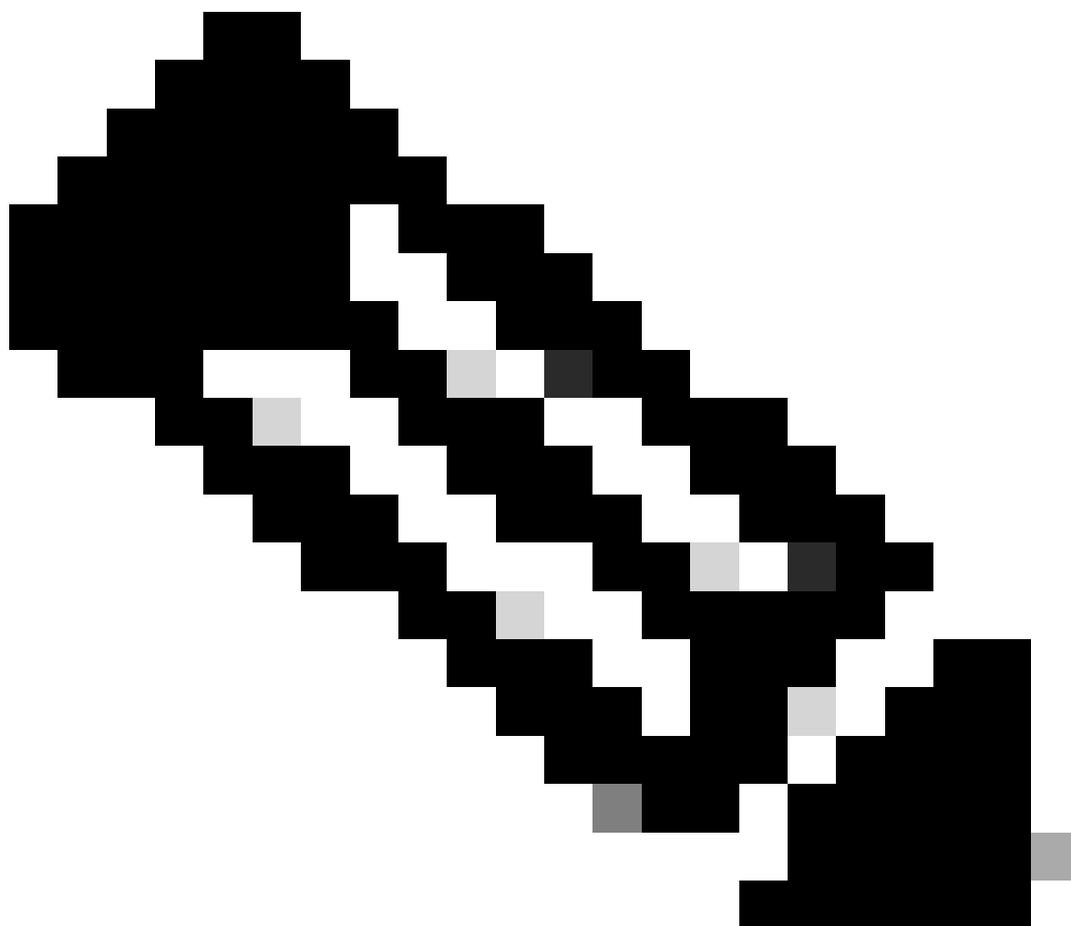
-> basic path-trace, and automatically stops tracing packets after 1024 packets. You can use "circular" option if needed

```
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.



Observação: em versões anteriores do Cisco IOS-XE 3.x, o comando debug platform packet-trace enable também é necessário para iniciar o recurso de rastreamento de pacotes. Isso não é mais necessário nas versões 16.x do Cisco IOS-XE.

---

Insira este comando para limpar o buffer de rastreamento e redefinir o packet-trace:

```
<#root>
```

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

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

O comando para limpar as condições da plataforma e a configuração do rastreamento de pacotes é:

```
<#root>
```

```
clear platform condition all
```

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

comandos show

Verifique a condição da plataforma e a configuração de rastreamento de pacotes depois de aplicar os comandos anteriores para garantir que você tenha o que precisa.

```
<#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
```

Aqui estão os comandos para verificar os pacotes 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 depurações condicionais da plataforma

O recurso Packet Trace conta com a infraestrutura de depuração condicional para determinar os pacotes a serem rastreados. A infraestrutura de depuração condicional oferece a capacidade de filtrar o tráfego com base em:

- Protocolo
- Endereço IP e máscara
- Lista de controle de acesso (ACL)
- Interface
- Direção do tráfego (entrada ou saída)

Essas condições definem onde e quando os filtros são aplicados a um pacote.

Para o tráfego usado neste exemplo, ative depurações condicionais de plataforma na direção de entrada para pacotes ICMP de 172.16.10.2 a 172.16.20.2. Em outras palavras, selecione o tráfego que deseja rastrear. Há várias opções que você pode usar para selecionar esse tráfego.

```
<#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
```

Neste exemplo, uma lista de acesso é usada para definir a condição, como mostrado aqui:

```
<#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
```

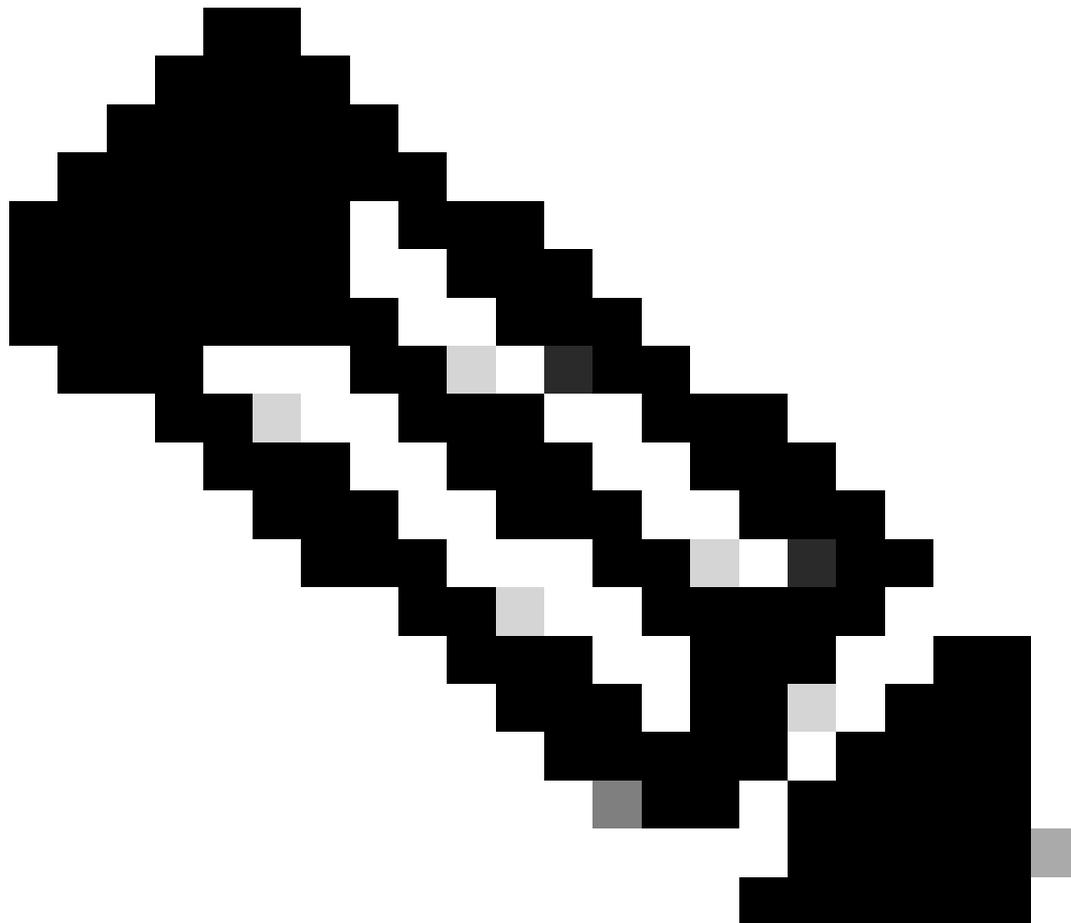
Para iniciar a depuração condicional, insira este comando:

```
<#root>
```

```
ASR1000#
```

```
debug platform condition start
```

---



Observação: para interromper ou desativar a infraestrutura de depuração condicional, insira o comando `debug platform condition stop`.

---

Para visualizar os filtros de depuração condicional configurados, insira este comando:

```
<#root>
```

```
ASR1000#
```

```
show platform conditions
```

Conditional Debug Global State:

```
start
```

Conditions	Direction
GigabitEthernet0/0/1	ingress
& IPV4 ACL [150]	

Feature Condition	Format	Value

```
ASR1000#
```

Em resumo, essa configuração foi aplicada até agora:

```
<#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
```

## Ativar o Packet Trace



Observação: esta seção descreve as opções de pacote e cópia em detalhes, e as outras opções são descritas mais adiante neste documento.

---

Os rastreamentos de pacotes são suportados nas interfaces física e lógica, como interfaces de túnel ou de acesso virtual.

Aqui está a sintaxe CLI do packet trace:

```
<#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>]
```

Aqui estão as descrições das palavras-chave desse comando:

- pkt-num - O número do pacote especifica o número máximo de pacotes que são mantidos ao mesmo tempo.
- summary-only - Especifica que somente os dados de resumo são capturados. O padrão é capturar dados de resumo e dados de caminho de recurso.
- fia-trace - Executa opcionalmente um rastreamento FIA, além das informações de dados do caminho.
- data-size - Permite especificar o tamanho do buffer de dados do caminho, de 2.048 a 16.384 bytes. O padrão é 2.048 bytes.

<#root>

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

Aqui estão as descrições das palavras-chave desse comando:

- in/out - Especifica a direção do fluxo do pacote a ser copiado - entrada e/ou saída.
- L2/L3/L4 - Isso permite que você especifique o local em que a cópia do pacote começa. A camada 2 (L2) é o local padrão.
- size - (tamanho) Permite especificar o número máximo de octetos que são copiados. O padrão é 64 octetos.

Para este exemplo, este é o comando usado para habilitar o rastreamento de pacotes para o tráfego que é selecionado com a infraestrutura de depuração condicional:

<#root>

ASR1000#

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

Para revisar a configuração de rastreamento de pacotes, insira este comando:

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

Você também pode inserir o comando show debugging para visualizar as depurações condicionais da plataforma e as configurações de rastreamento de pacotes:

```
<#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
```



Observação: insira o comando `clear platform condition all` para limpar todas as condições de depuração da plataforma e as configurações e dados de rastreamento de pacotes.

---

Em resumo, esses dados de configuração foram usados até agora para ativar o rastreamento de pacotes:

```
<#root>
```

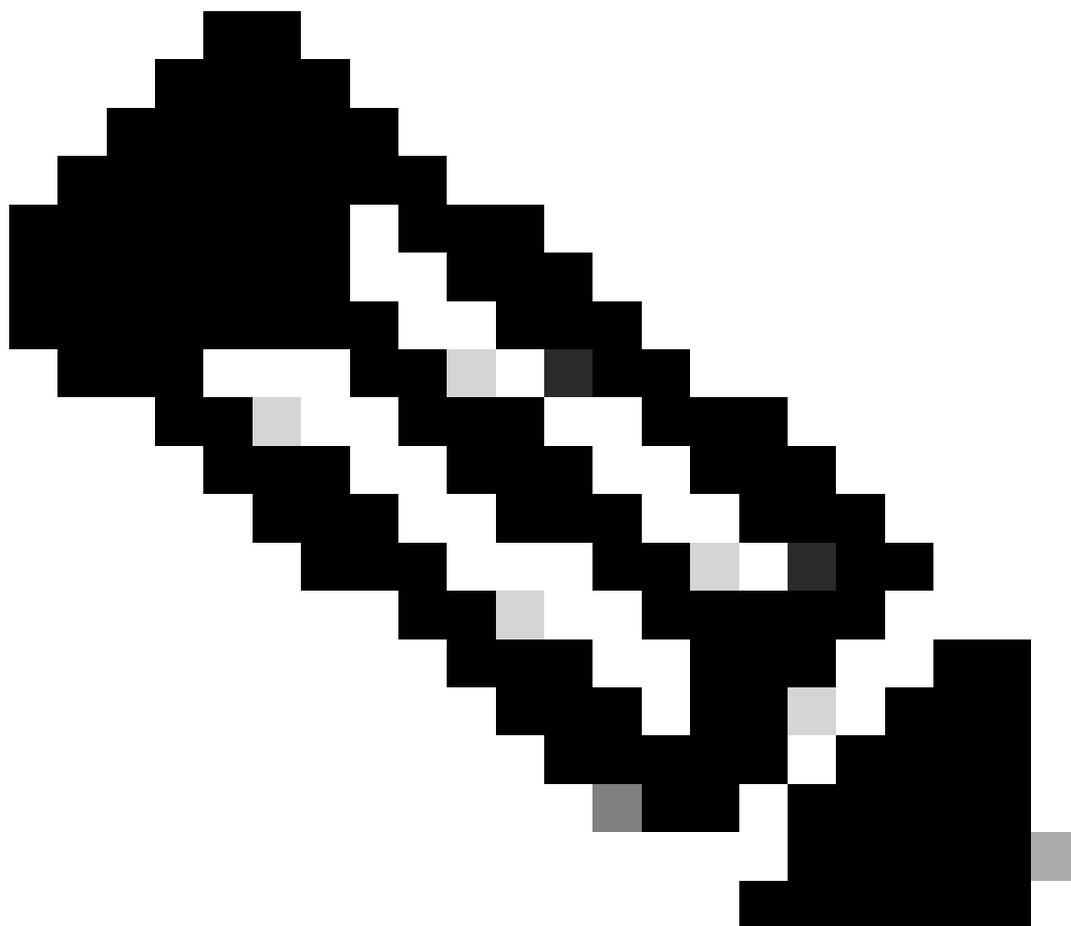
```
debug platform packet-trace packet 16
```

Limitação da condição de saída com rastreamentos de pacotes

As condições definem os filtros condicionais e quando eles são aplicados a um pacote. Por exemplo, `debug platform condition interface g0/0/0 egress` significa que um pacote é identificado como uma correspondência quando alcança o FIA de saída na interface `g0/0/0`, portanto qualquer

processamento de pacote que ocorre desde o ingresso até esse ponto é perdido.

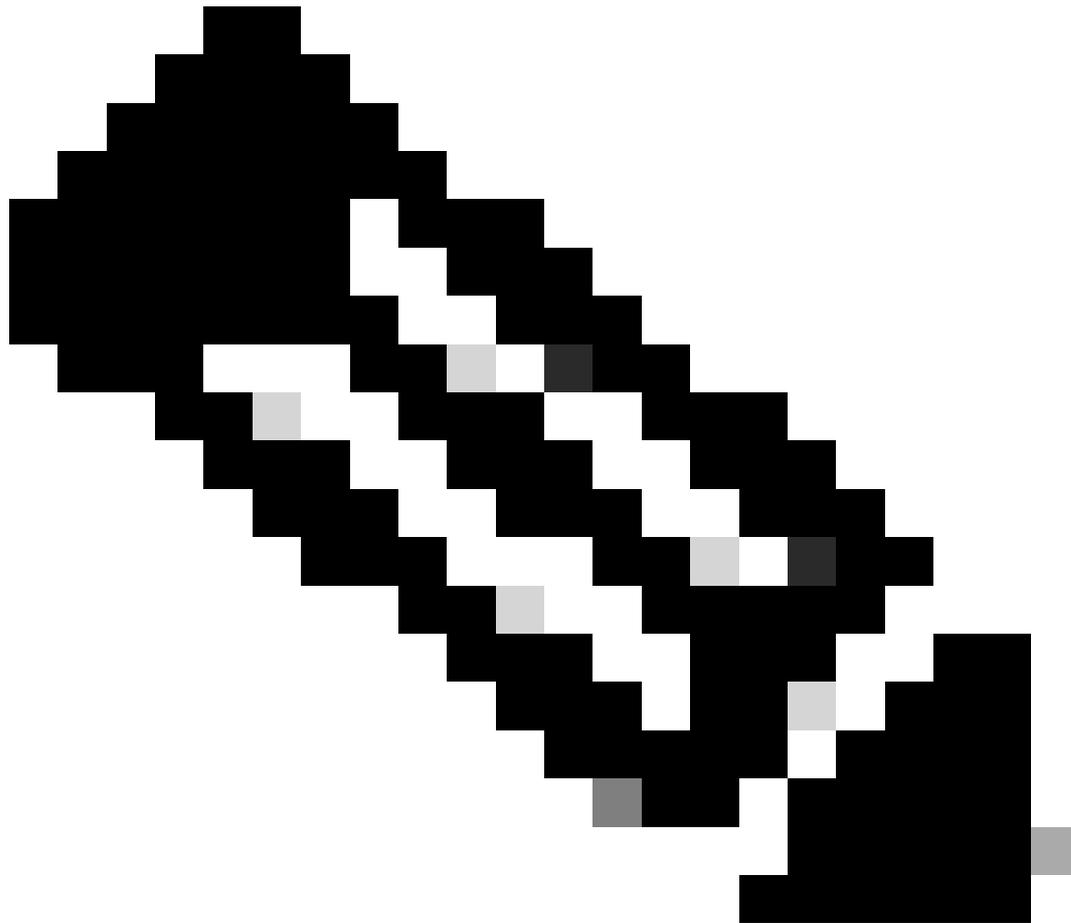
---



Observação: a Cisco recomenda que você use condições de ingresso para rastreamentos de pacotes para obter os dados mais completos e significativos possíveis. As condições de saída podem ser usadas, mas esteja ciente das limitações.

---

Exibir os resultados do Packet Trace



Observação: esta seção pressupõe que o rastreamento de caminho esteja habilitado.

---

Três níveis específicos de inspeção são fornecidos pelo rastreamento de pacotes:

- Relatório
- Resumo por pacote
- Dados de caminho por pacote

Quando cinco pacotes de solicitação ICMP são enviados de 172.16.10.2 para 172.16.20.2, estes comandos podem ser usados para visualizar os resultados do rastreamento de pacotes:

```
<#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

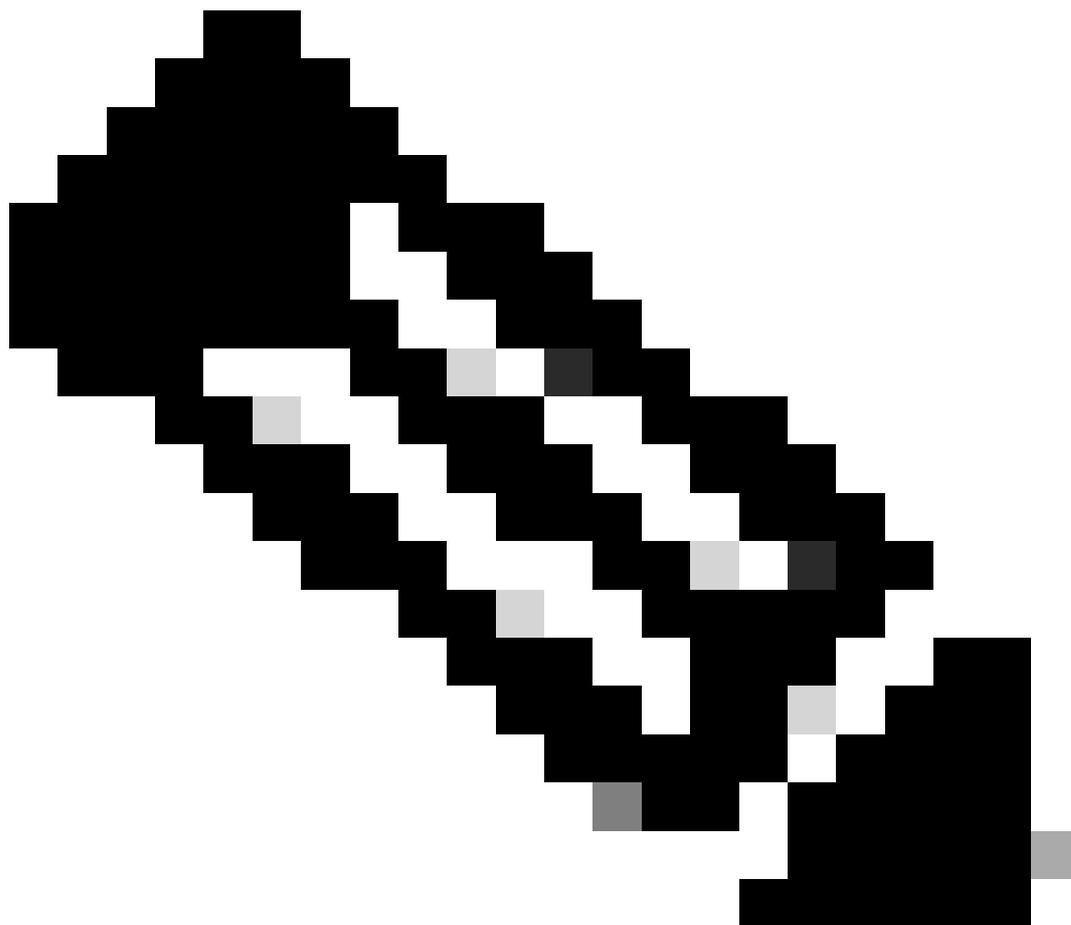
Feature: IPV4

Source : 172.16.10.2

Destination : 172.16.20.2

Protocol : 1 (ICMP)

ASR1000#



Observação: o terceiro comando fornece um exemplo que ilustra como exibir o rastreamento de pacotes para cada pacote. Neste exemplo, o primeiro pacote rastreado é mostrado.

Nessas saídas, você pode ver que cinco pacotes são rastreados e que é possível exibir a interface de entrada, a interface de saída, o estado e o rastreamento de caminho.

Estado	Lembrete
FWD	O pacote é programado/enfileirado para entrega, para ser encaminhado ao próximo salto através de uma interface de saída.
PUNT	O pacote é direcionado do processador de encaminhamento (FP) para o processador de rotas (RP) (plano de controle).
SOLTAR	O pacote é descartado no FP. Execute o rastreamento FIA, use contadores de descarte globais ou use depurações de caminho de dados para encontrar mais detalhes por motivos de descarte.
CONS	O pacote é consumido durante um processo de pacote, como durante a solicitação de

	ping ICMP ou os pacotes de criptografia.
--	--

Os contadores ingress e inject na saída de estatísticas de rastreamento de pacote correspondem aos pacotes que entram por meio de uma interface externa e pacotes que são vistos como injetados do plano de controle, respectivamente.

## Rastreamento FIA

O FIA mantém a lista de recursos que são executados sequencialmente pelos Packet Processor Engines (PPE) no Quantum Flow Processor (QFP) quando um pacote é encaminhado de entrada ou de saída. Os recursos são baseados nos dados de configuração que são aplicados na máquina. Assim, um rastreamento FIA ajuda a entender o fluxo do pacote pelo sistema à medida que o pacote é processado.

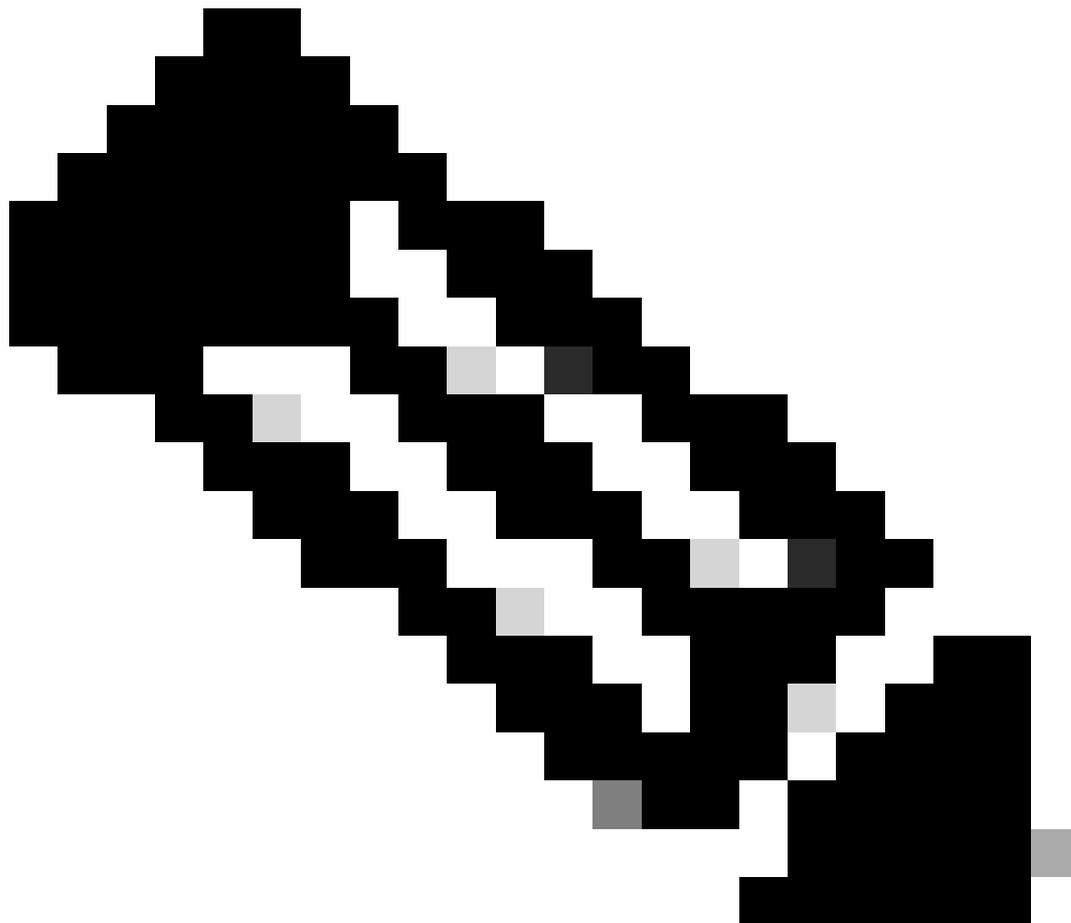
Você deve aplicar estes dados de configuração para habilitar o rastreamento de pacotes com o FIA:

```
<#root>
```

```
ASR1000#
```

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

## Exibir os resultados do Packet Trace



Observação: esta seção pressupõe que o rastreamento FIA esteja habilitado. Além disso, quando você adiciona ou modifica os comandos atuais de rastreamento de pacotes, os detalhes de rastreamento de pacotes armazenados no buffer são limpos, portanto, você deve enviar algum tráfego novamente para que possa rastreá-lo.

Envie cinco pacotes ICMP de 172.16.10.2 para 172.16.20.2 depois de inserir o comando usado para ativar o rastreamento FIA, conforme descrito na seção 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 o FIA associado a uma interface

Quando você habilita as depurações condicionais da plataforma, a depuração condicional é adicionada ao FIA como um recurso. Com base na ordem do recurso de processamento na interface, o filtro condicional precisa ser definido de acordo, por exemplo, se o endereço pré ou pós-NAT deve ser usado no filtro condicional.

Esta saída mostra a ordem dos recursos no FIA para a depuração condicional da plataforma que está habilitada na direção de entrada:

```
<#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)
```

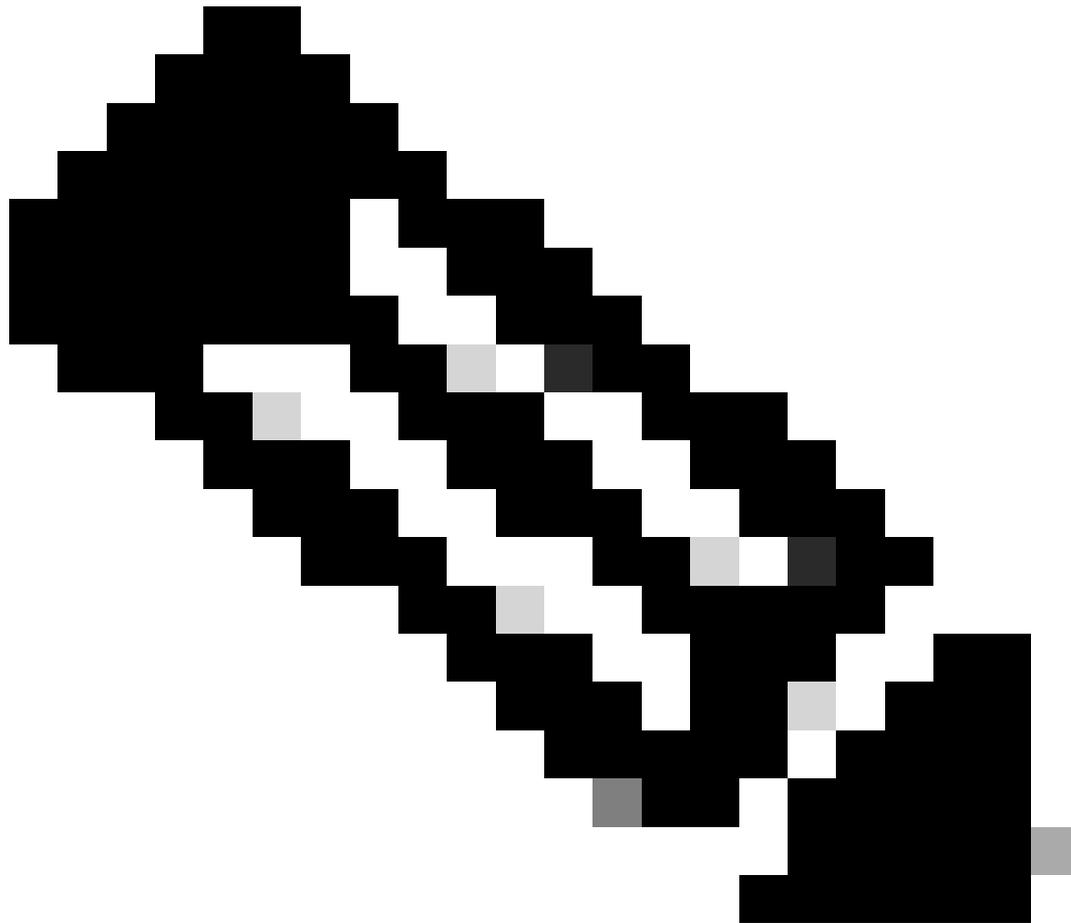
```
CBUG_INPUT_FIA
```

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#



Observação: CBUG\_INPUT\_FIA e DEBUG\_COND\_INPUT\_PKT correspondem aos recursos de depuração condicional configurados no roteador.

---

## Descartar os pacotes rastreados

Você pode copiar e despejar os pacotes à medida que são rastreados, conforme descrito nesta seção. Este exemplo mostra como copiar um máximo de 2.048 bytes dos pacotes na direção de entrada (172.16.10.2 a 172.16.20.2).

Aqui está o comando adicional necessário:

```
<#root>
```

```
ASR1000#
```

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

---

Observação: o tamanho do pacote copiado está no intervalo de 16 a 2.048 bytes.

---

Insira este comando para despejar os pacotes 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#

## Descartar Rastreamento

O rastreamento de queda está disponível no Cisco IOS-XE Software Release 3.11 e posterior. Ativa o rastreamento de pacotes somente para pacotes descartados. Aqui estão alguns destaques do recurso:

- Opcionalmente, permite especificar a retenção de pacotes para um código de queda específico.
- Ele pode ser usado sem condições globais ou de interface para capturar eventos de queda.
- Uma captura de evento de queda significa que somente a queda em si é rastreada, não a vida útil do pacote. No entanto, ele ainda permite capturar dados de resumo, dados de tupla e o pacote para ajudar a refinar as condições ou fornecer pistas para a próxima etapa de depuração.

Aqui está a sintaxe de comando que é usada para habilitar rastreamentos de pacote tipo queda:

```
<#root>
```

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

O código drop é o mesmo que o ID drop, conforme relatado na saída do comando `show platform hardware qfp active statistics drop detail`:

```
<#root>
```

ASR1000#

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

```
-----
```

ID			
Global Drop Stats		Packets	Octets
60			
IpTtlExceeded		3	126
8			
Ipv4Acl		32	3432

```
-----
```

### Exemplo de Cenário de Rastreamento de Eliminação

Aplique essa ACL na interface Gig 0/0/0 do ASR1K para descartar o tráfego de 172.16.10.2 para 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
```

Com a ACL estabelecida, que descarta o tráfego do host local para o host remoto, aplique esta configuração de drop-trace:

```
<#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
```

Envie cinco pacotes de solicitação ICMP de 172.16.10.2 para 172.16.20.2. O rastreamento de queda captura esses pacotes que são descartados pela ACL, como mostrado:

```
<#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

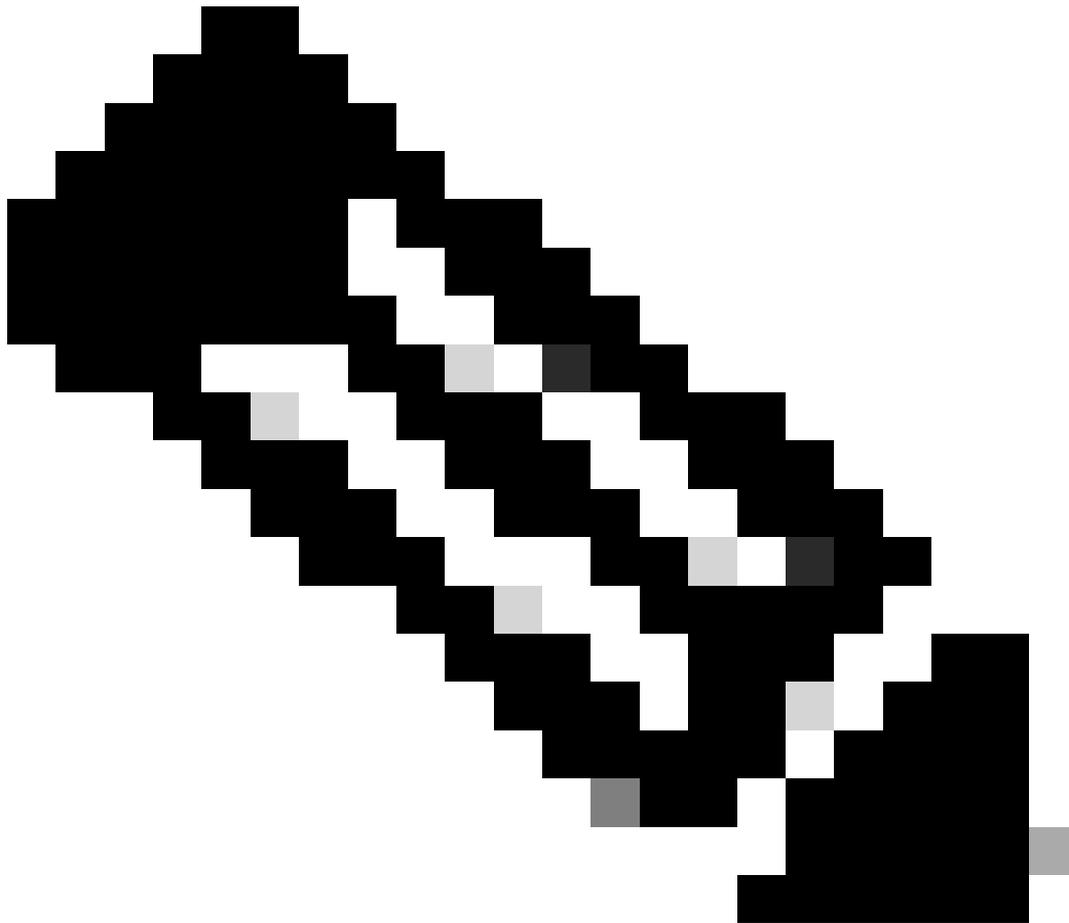
Protocol : 1 (ICMP)

```
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#

## Injetar e Puncionar Rastreamentos

O recurso de rastreamento de pacote de inserção e punt foi adicionado no Cisco IOS-XE Software Release 3.12 e posterior para rastrear pacotes punt (pacotes que são recebidos no FP que são apontados para o plano de controle) e inject (pacotes que são injetados no FP a partir do plano de controle).



Observação: o rastreamento de punt pode funcionar sem as condições globais ou de interface, assim como um rastreamento de queda. No entanto, as condições devem ser definidas para que um traçado de injeção funcione.

---

Aqui está um exemplo de um `punt` e `inject packet trace` quando você efetua ping do ASR1K para um roteador adjacente:

```
<#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#

Agora você pode verificar os resultados de punt e nject trace rdo:

<#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)
```

### Aprimoramento de Rastreamento de Pacotes com IOSd e Rastreamento de Punt/Injeção LFTS e Correspondência de UDF (Novo em 17.3.1)

O recurso de rastreamento de pacotes é aprimorado para fornecer informações adicionais de rastreamento para pacotes originados ou destinados ao IOSd ou outros processos BinOS no Cisco IOS-XE versão 17.3.1.

### Rastreamento de queda IOSd

Com esse aprimoramento, o rastreamento de pacotes é estendido para o IOSd e pode fornecer informações sobre qualquer queda de pacote dentro do IOSd, que são geralmente relatadas na saída do comando *show ip traffic*. Não há nenhuma configuração adicional necessária para ativar o rastreamento de queda IOSd. Aqui está um exemplo de um pacote UDP descartado pelo IOSd devido a um erro de checksum incorreto:

<#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)

### Rastreamento de caminho de saída IOSd

O rastreamento de pacotes é aprimorado para mostrar as informações de rastreamento de caminho e processamento de protocolo à medida que o pacote é originado do IOSd e enviado na direção de saída em direção à rede. Não há nenhuma configuração adicional necessária para capturar as informações de rastreamento de caminho de saída do IOSd. Aqui está um exemplo de rastreamento de caminho de saída para um pacote SSH que sai do roteador:

<#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
```

### Rastreamento de pacotes LFTS

O LFTS (Linux Forwarding Transport Service) é um mecanismo de transporte para encaminhar pacotes lançados do CPP para aplicativos diferentes do IOSd. O aprimoramento de rastreamento de pacotes LFTS adicionou informações de rastreamento para esses pacotes na saída do rastreamento de caminho. Não há necessidade de configuração adicional para obter as informações de rastreamento de LFTS. Aqui está um exemplo de saída do rastreamento de LFTS para o pacote apontado para a aplicação 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
```

### **Correspondência de padrão de rastreamento de pacote com base no filtro definido pelo usuário (somente plataforma ASR1000)**

No Cisco IOS-XE versão 17.3.1, um novo mecanismo de correspondência de pacotes também é adicionado às famílias de produtos ASR1000 para corresponder em campo arbitrário em um pacote baseado na infraestrutura do filtro definido pelo usuário (UDF). Isso permite a correspondência flexível de pacotes com base em campos que não fazem parte da estrutura de cabeçalho L2/L3/L4 padrão. O próximo exemplo mostra uma definição de UDF que corresponde a 2 bytes de padrão definido pelo usuário de 0x4D2 que começa a partir de um deslocamento de 26 bytes do cabeçalho do protocolo externo de 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
```

## **Exemplos de rastreamento de pacote**

Esta seção fornece alguns exemplos em que o recurso de rastreamento de pacotes é útil para fins de solução de problemas.

### **Exemplo de Packet Trace - NAT**

Neste exemplo, uma conversão de endereço de rede (NAT) de origem da interface é configurada na interface WAN de um ASR1K (Gig0/0/0) para a sub-rede local (172.16.10.0/24).

Esta é a condição da plataforma e a configuração de rastreamento de pacote usada para rastrear o tráfego de 172.16.10.2 a 172.16.20.2, que se torna convertido (NAT) na interface Gig0/0/0:

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

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

Quando cinco pacotes ICMP são enviados de 172.16.10.2 para 172.16.20.2 com uma configuração NAT de origem de interface, estes são os resultados do rastreamento de pacotes:

```
<#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#
```

## Exemplo de Packet Trace - VPN

Com este exemplo, um túnel VPN site a site é usado entre o ASR1K e o roteador Cisco IOS para proteger o tráfego que flui entre 172.16.10.0/24 e 172.16.20.0/24 (sub-redes locais e remotas).

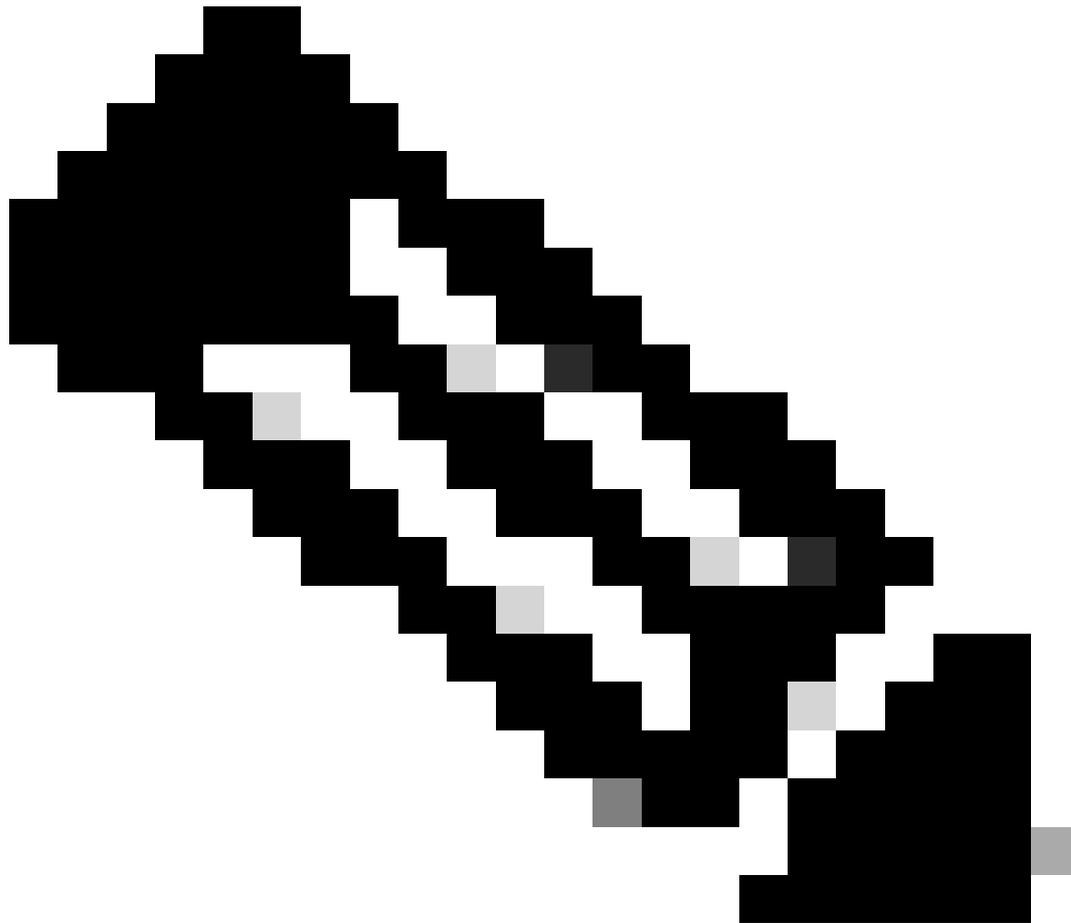
Esta é a condição da plataforma e a configuração de rastreamento de pacotes usada para rastrear o tráfego de VPN que flui de 172.16.10.2 para 172.16.20.2 na interface Gig 0/0/1:

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

Quando cinco pacotes ICMP são enviados de 172.16.10.2 para 172.16.20.2, que são criptografados pelo túnel VPN entre o ASR1K e o roteador Cisco IOS neste exemplo, estas são as saídas de rastreamento de pacote:

---

---



**Observação:** os rastreamentos de pacotes mostram o identificador da Associação de Segurança (SA) QFP no rastreamento que é usado para criptografar o pacote, o que é útil quando você soluciona problemas de VPN IPsec para verificar se a SA correta é usada para criptografia.

---

<#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 de desempenho

Os buffers de rastreamento de pacotes consomem a QFP DRAM; portanto, tenha em mente a quantidade de memória necessária para uma configuração e a quantidade de memória disponível.

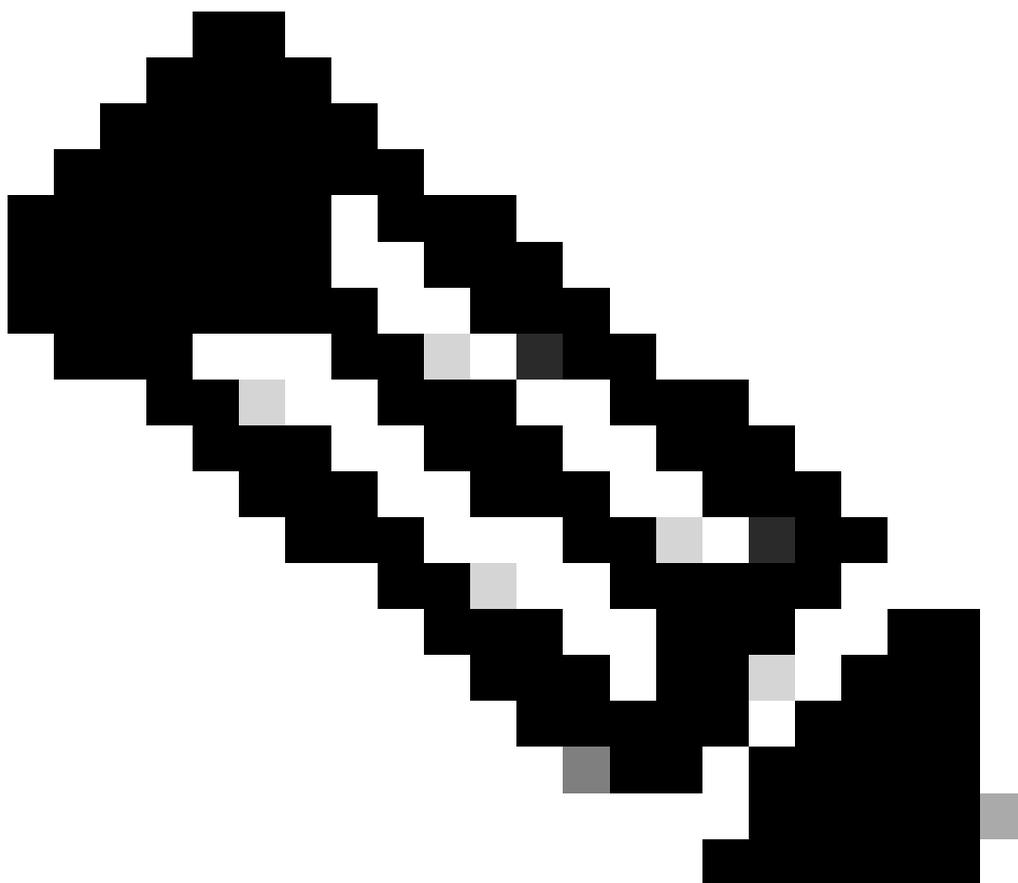
O impacto no desempenho varia, dependendo das opções de rastreamento de pacotes que estão ativadas. O rastreamento de pacotes afeta apenas o desempenho de encaminhamento dos pacotes rastreados, como os pacotes que correspondem às condições configuradas pelo usuário. Quanto mais granular e detalhada for a informação que você configura o rastreamento de pacotes para capturar, maior será o impacto nos recursos.

Como em qualquer solução de problemas, é melhor adotar uma abordagem iterativa e ativar somente as opções de rastreamento mais detalhadas quando uma situação de depuração o justificar.

O uso da DRAM QFP pode ser estimado com esta fórmula:

**memória necessária = (sobrecarga de stats) + número de pcts \* (tamanho de resumo + tamanho de dados de caminho + tamanho de cópia)**

---



---

**Observação:** onde o **overhead de estatísticas** e o **tamanho do resumo** são fixados em 2 KB e 128 B, respectivamente, o **tamanho dos dados do caminho** e o **tamanho da cópia** são configuráveis pelo usuário.

---

## Informações Relacionadas

- [Guia de configuração de software dos Cisco ASR1000 Series Aggregation Series Routers - Packet Trace](#)
- [Quedas de pacotes nos roteadores de serviço da série Cisco ASR1000](#)
- [Suporte técnico e downloads da Cisco](#)

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.