Probleemoplossing met de IOS-XE Datapath Packet Trace-functie

Inhoud

Inleiding

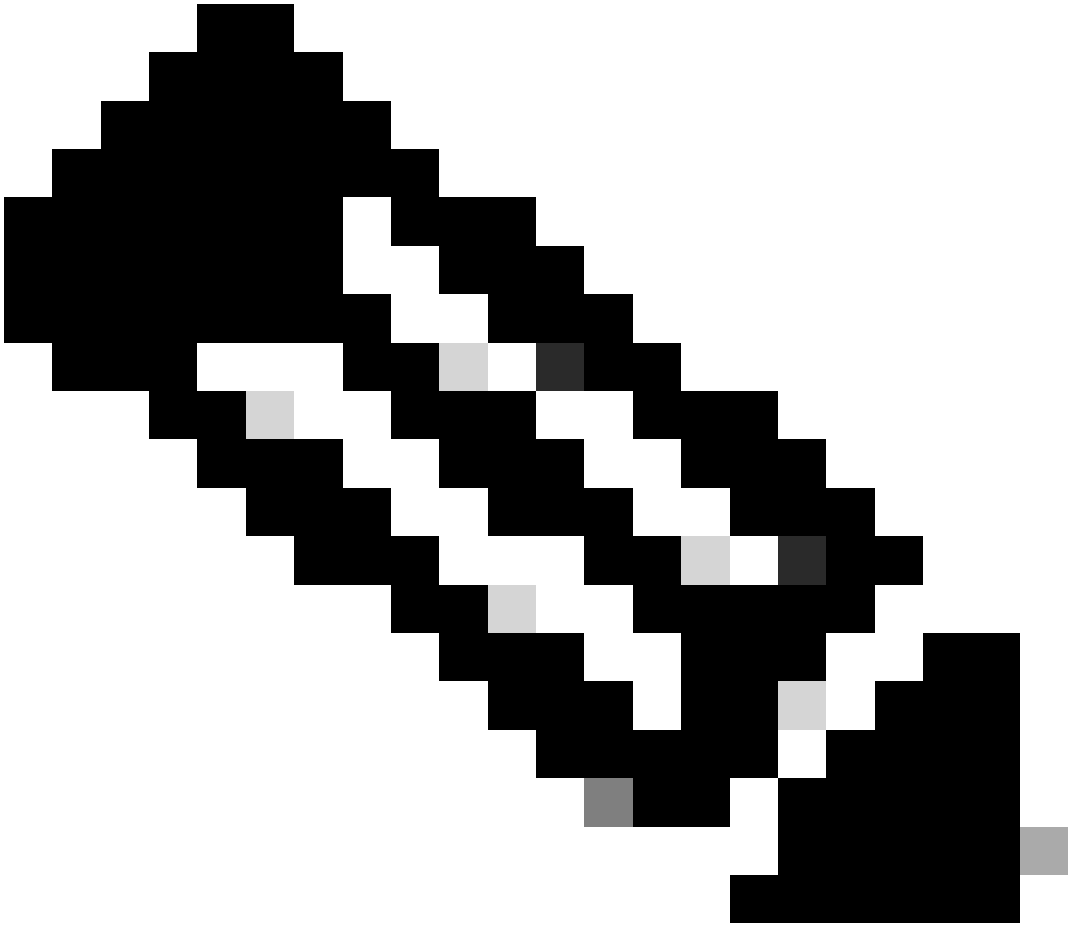
Dit document beschrijft hoe u een datapath-pakketovertrekken voor Cisco IOS-XE®-software kunt uitvoeren via de functie Packet Trace.

Voorwaarden

Vereisten

Cisco raadt u aan bekend te zijn met deze informatie:

De pakketsporenfunctie is beschikbaar in Cisco IOS-XE versie 3.10 en latere releases op de QFP (Quantum Flow Processor) gebaseerde routeringsplatforms, die de ASR 1000, ISR4000, ISR1000, Catalyst 1000, Catalyst 8000, CSR1000v en Catalyst 8000v Series routers omvatten. Deze optie wordt niet ondersteund op de ASR 900 Series aggregatieservices routers of de Catalyst-Series switches waarop Cisco IOS-XE-software wordt uitgevoerd.



> Opmerking: de pakketsporenfunctie werkt niet op de speciale beheerinterface, Gigabit Ethernet0 op de ASR 1000 Series routers, omdat pakketten die op die interface worden doorgestuurd niet worden verwerkt door de QFP.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco IOS-XE softwarerelease 3.10S (15.3(3)S) en hoger

- ASR 1000 Series router

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Om problemen zoals een verkeerde configuratie, overbelasting van de capaciteit of zelfs de gewone softwarebug te identificeren tijdens het oplossen van problemen, is het noodzakelijk om te begrijpen wat er gebeurt met een pakket binnen een systeem. Met de Cisco IOS-XE Packet Trace-functie wordt aan deze behoefte tegemoetgekomen. Het biedt een veldveilige methode die wordt gebruikt voor accounting en om de procesdetails per pakket op te nemen op basis van een klasse van door de gebruiker gedefinieerde voorwaarden.

Referentietopologie

Dit diagram illustreert de topologie die wordt gebruikt voor de voorbeelden die in dit document worden beschreven:

Packet Tracing in gebruik

Om het gebruik van de pakketsporenfunctie te illustreren, beschrijft het voorbeeld dat in deze sectie wordt gebruikt een spoor van het ICMP-verkeer (Internet Control Message Protocol) van het lokale werkstation 172.16.10.2 (achter de ASR1K) naar de externe host 172.16.20.2 in de toegangsrichting op de interface Gigabit Ethernet0/0/1 op de ASR1K.

U kunt pakketten op de ASR1K overtrekken met deze twee stappen:

1. Schakel het platform voorwaardelijke debugs in om de pakketten of het verkeer te selecteren die u op de ASR1K wilt overtrekken.

2. Schakel het platformpakketspoor in met de optie pad-trace of Feature Invocation Array (FIA) voor overtrekken.

Snelstartgids

Hier is een snelstartgids als u al bekend bent met de inhoud van dit document en u een sectie wilt

voor een snelle blik op de CLI. Dit zijn slechts een paar voorbeelden om het gebruik van de tool te illustreren. Verwijs naar de latere secties die de syntaxen in detail bespreken, en zorg ervoor dat u de configuratie gebruikt die aan uw vereiste passend is.

1. Platformvoorwaarden configureren:

<#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)

Nadat een platformvoorwaarde wordt gevormd, begin platformvoorwaarden met dit CLI bevel:

<#root>

debug platform condition start

2. PacketTracker configureren:

<#root>

debug platform packet-trace packet 1024

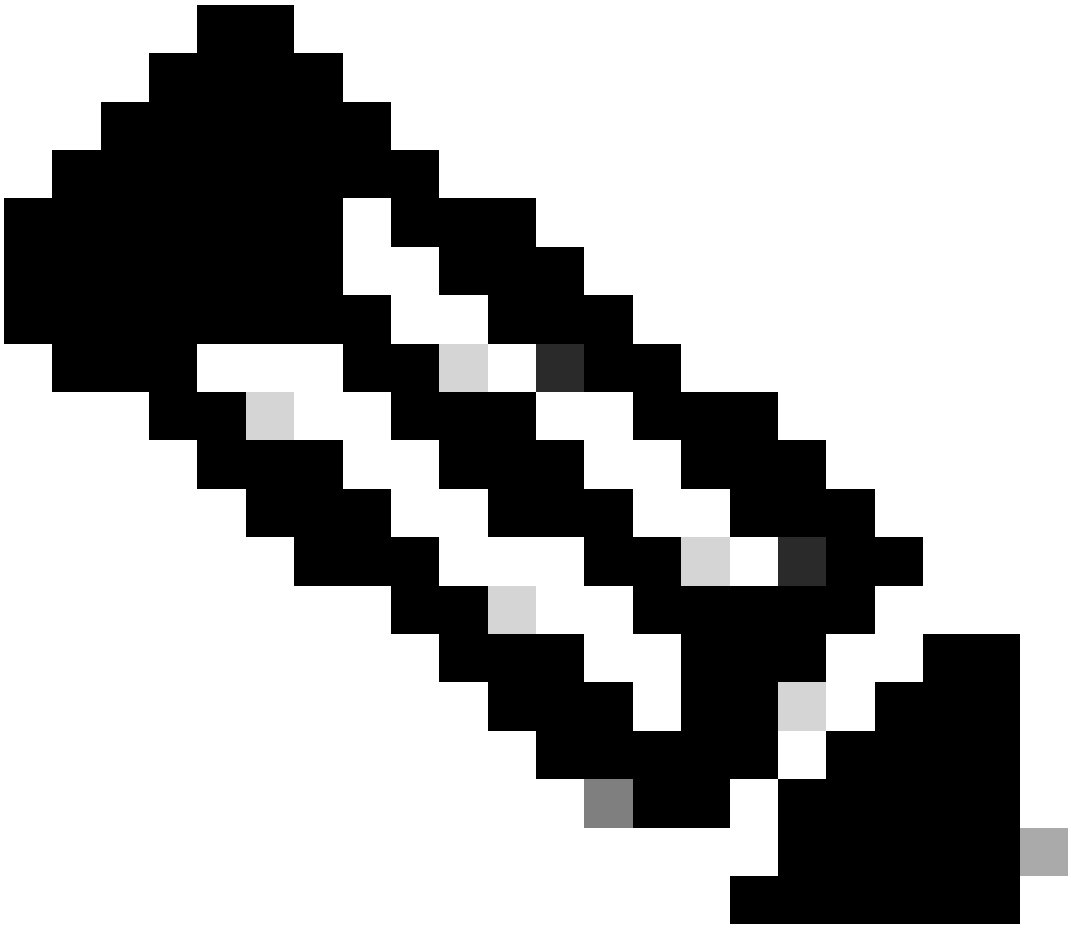
```
  -> basic path-trace, and automatically stops
 tracing packets after 1024 packets. You can use "circular" option if needed
```

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.
```



Opmerking: in eerdere versies van Cisco IOS-XE 3.x is het opdracht debug platform packet-trace enabled ook vereist om de pakketsporenfunctie te starten. Dit is niet langer nodig voor Cisco IOS-XE 16.x releases.

Voer deze opdracht in om de traceerbuffer te wissen en het pakketspoor opnieuw in te stellen:

<#root>

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

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

De opdracht om zowel de platformvoorwaarden als de pakkettraceringsconfiguratie te wissen is:

<#root>

```
clear platform condition all
```

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

Opdrachten weergeven

Controleer de platformvoorwaarde en de configuratie van het pakketspoor nadat u de vorige opdrachten hebt toegepast om er zeker van te zijn dat u hebt wat u nodig hebt.

<#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
```

Hier zijn de opdrachten om de overgetrokken/opgenomen pakketten te controleren:

<#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
```

Platform voorwaardelijke debugs inschakelen

De Packet Trace-functie is afhankelijk van de voorwaardelijke debug-infrastructuur om te bepalen welke pakketten moeten worden overgetrokken. De voorwaardelijke debug-infrastructuur biedt de mogelijkheid om verkeer te filteren op basis van:

- Protocol
- IP-adres en -masker
- Toegangscontrolelijst (ACL)
- Interface
- Verkeersrichting (in- of uitgang)

Deze voorwaarden bepalen waar en wanneer de filters op een pakket worden toegepast.

Voor het verkeer dat in dit voorbeeld wordt gebruikt, laat platform voorwaardelijke debugs in de toegangsrichting voor pakketten ICMP van 172.16.10.2 tot 172.16.20.2 toe. Met andere woorden, selecteer het verkeer dat u wilt overtrekken. Er zijn verschillende opties die u kunt gebruiken om dit verkeer te selecteren.

<#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
```

In dit voorbeeld wordt een toegangslijst gebruikt om de voorwaarde te definiëren, zoals hier wordt getoond:

<#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#
```

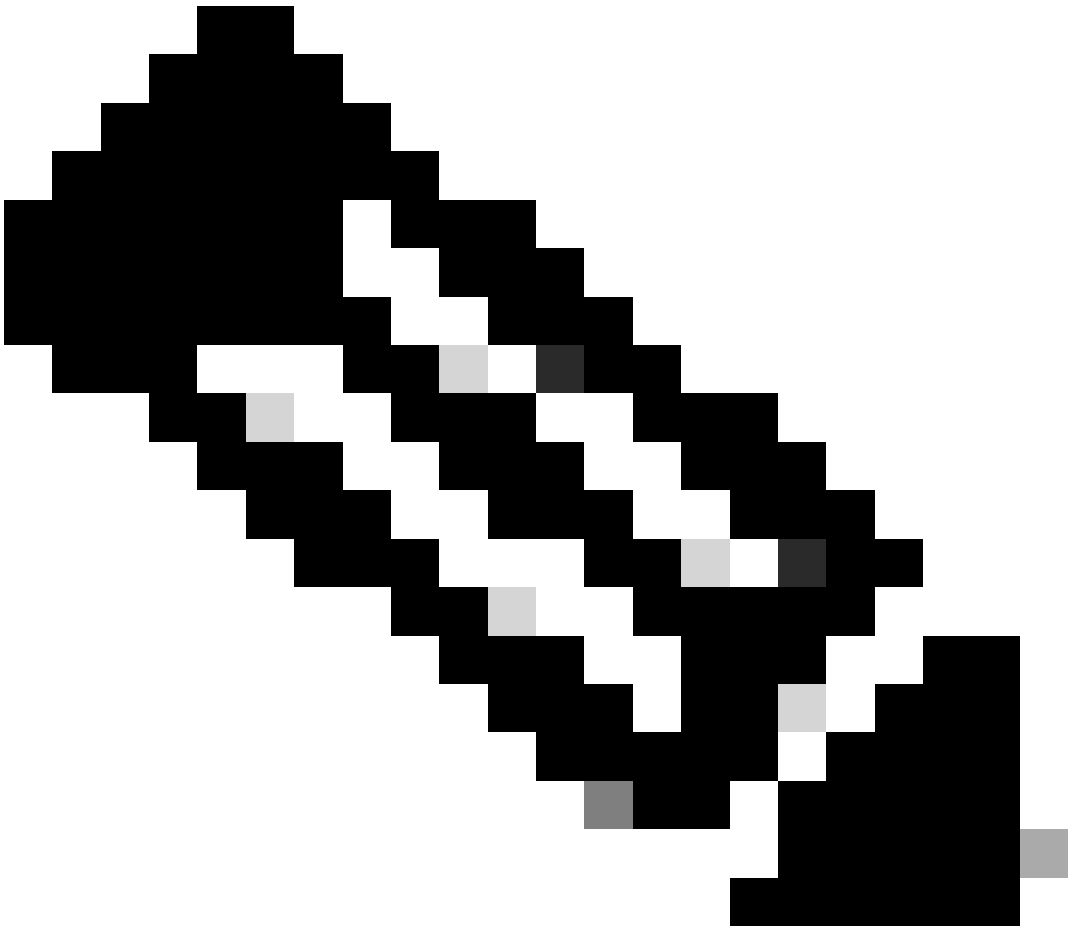
```
debug platform condition interface gig 0/0/1 ipv4
 access-list 150 ingress
```

Als u wilt beginnen met voorwaardelijke debugging, voert u deze opdracht in:

<#root>

```
ASR1000#
```

```
debug platform condition start
```



Opmerking: om de voorwaardelijke debugging-infrastructuur te stoppen of uit te

---

schakelen, voert u de opdracht stopt met de voorwaarde voor het debug-platform in.

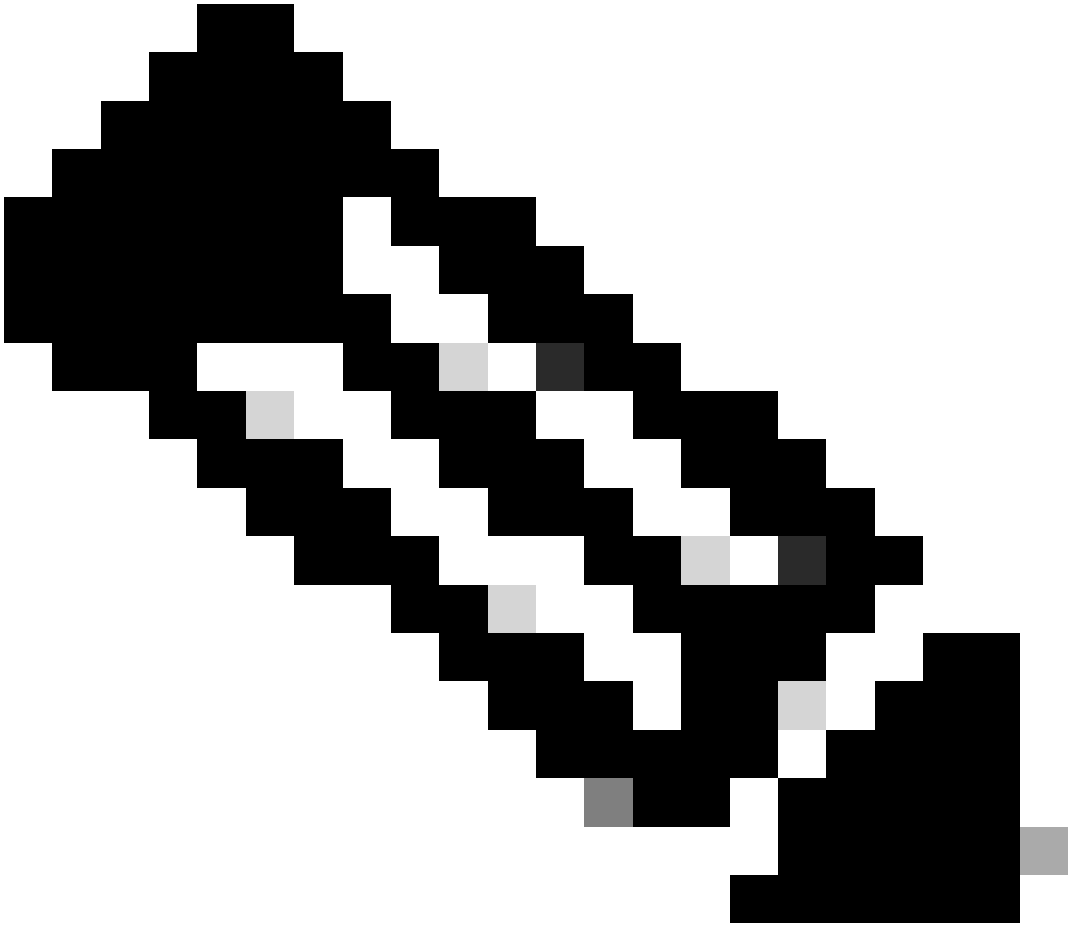
Om de voorwaardelijke debug filters te bekijken die zijn geconfigureerd, voert u deze opdracht in:

```
<#root>

ASR1000#

show platform conditions


Conditional Debug Global State:

Start


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


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

ASR1000#
```

Samengevat is deze configuratie tot nu toe toegepast:

```
<#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
```

PacketTrace inschakelen



N.B.: In deze sectie worden de opties voor pakket en kopiëren gedetailleerd beschreven. De andere opties worden later in het document beschreven.

Packet traces worden ondersteund op zowel de fysieke als de logische interfaces, zoals Tunnel of Virtual-Access interfaces.

Hier is de syntaxis van CLI voor pakkettracering:

<#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>]
```

Hier zijn beschrijvingen van de trefwoorden van deze opdracht:

- pkt-num - Het pakketnummer specificeert het maximale aantal pakketten dat tegelijkertijd wordt onderhouden.
- Alleen-samenvatting - hiermee wordt gespecificeerd dat alleen de samenvattende gegevens worden opgenomen. De standaardinstelling is om zowel overzichtsgegevens als eigenschap-pad gegevens op te nemen.
- fia-trace - Dit voert naar keuze een FIA-track uit naast de padgegevens.
- gegevensgrootte - Hiermee kunt u de grootte van de padgegevensbuffer specificeren, van 2.048 tot 16.384 bytes. De standaardinstelling is 2.048 bytes.

<#root>

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

Hier zijn beschrijvingen van de trefwoorden van deze opdracht:

- in/uit - Dit specificeert de richting van de pakketstroom die moet worden gekopieerd - in- en/of uitgangen.
- L2/L3/L4 - Hiermee kunt u de locatie opgeven waar het pakket moet worden gestart. Layer 2 (L2) is de standaardlocatie.
- grootte - hiermee kunt u het maximale aantal octetten opgeven dat wordt gekopieerd. De standaardinstelling is 64 octetten.

Dit is bijvoorbeeld de opdracht die wordt gebruikt om pakkettracering in te schakelen voor het verkeer dat is geselecteerd met de voorwaardelijke debug-infrastructuur:

<#root>

```
ASR1000#

debug platform packet-trace packet 16
```

Om de configuratie van het pakketspoor te herzien, ga dit bevel in:

<#root>

ASR1000#

show platform packet-trace configuration

```
debug platform packet-trace packet 16 data-size 2048
```

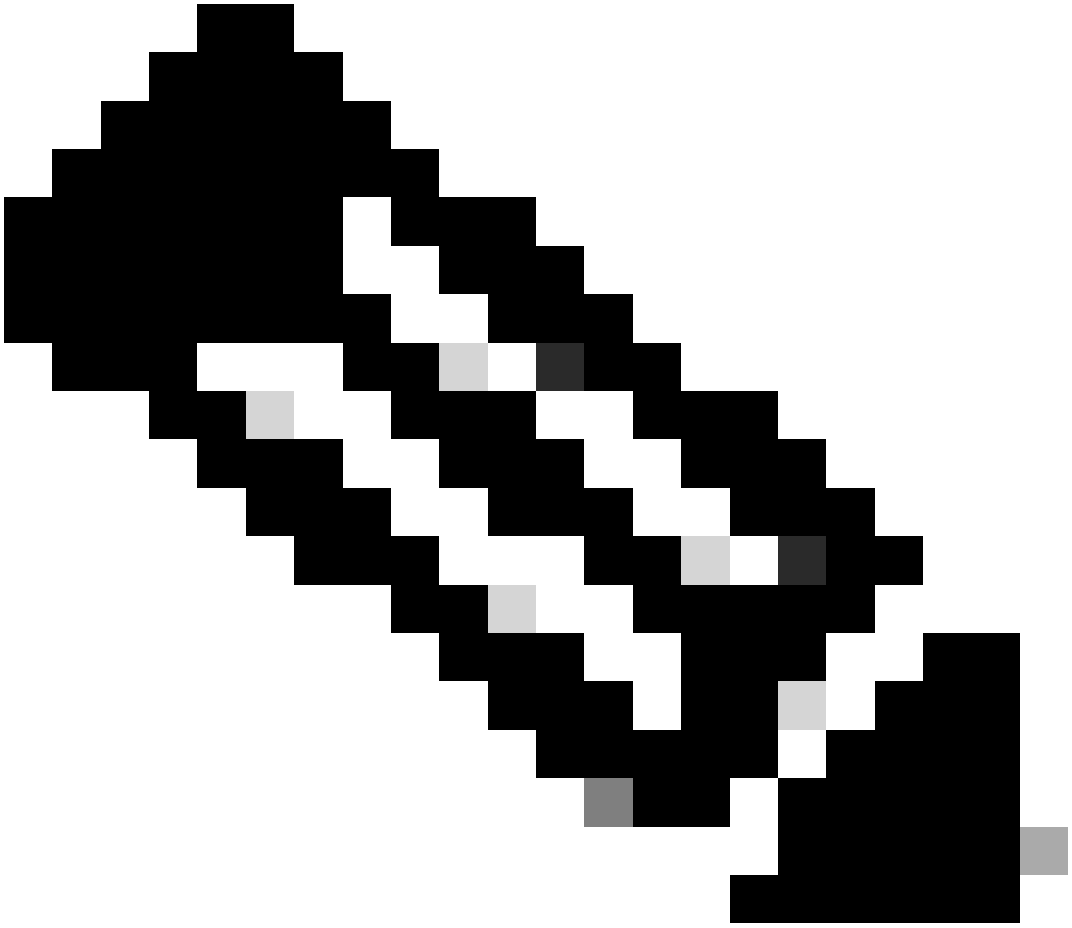
U kunt ook de opdracht voor het debuggen van de show invoeren om zowel de voorwaardelijke debugs van het platform als de configuraties voor pakkettracering te bekijken:

<#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
```



Opmerking: Voer de duidelijke platformvoorwaarde in alle opdracht om alle platformdebug-voorwaarden en de configuraties en gegevens van pakkettracering te wissen.

Samenvattend, zijn deze configuratiegegevens tot nu toe gebruikt om pakkettracering mogelijk te maken:

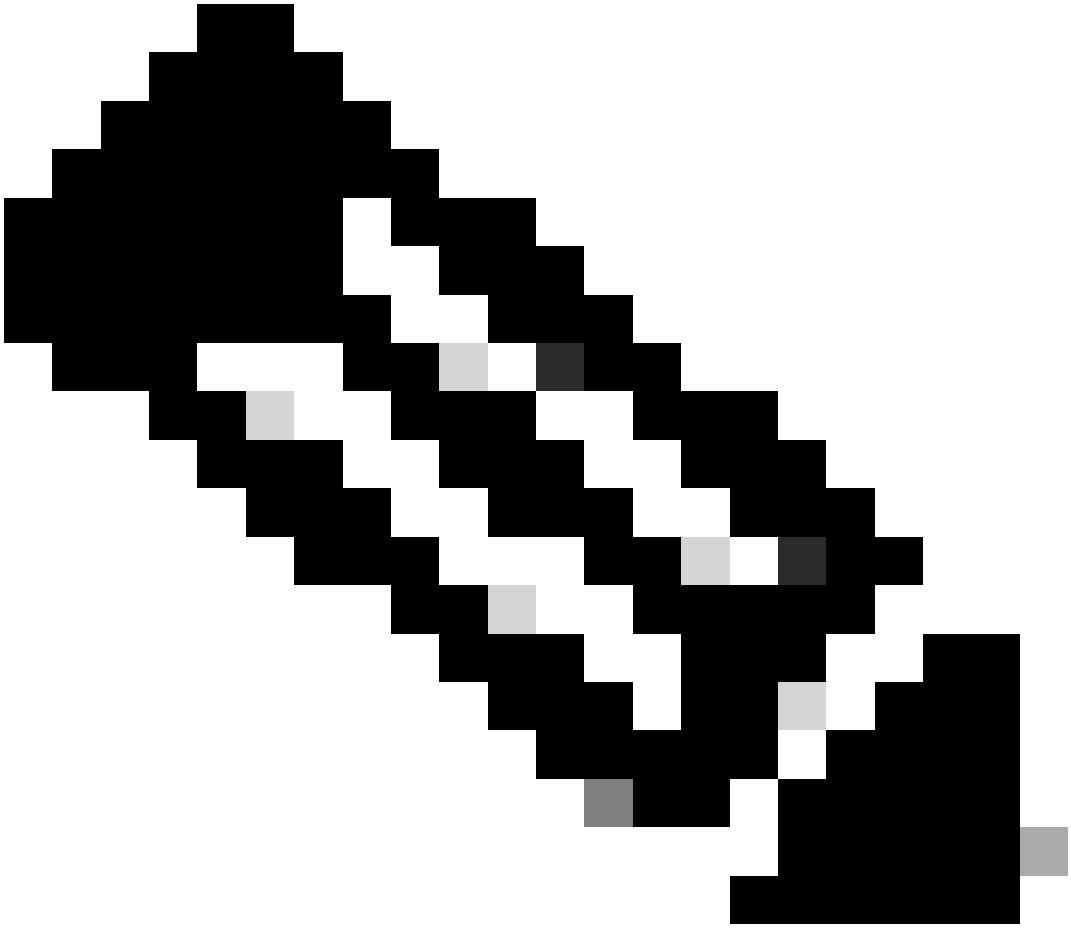
<#root>

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

Uitgangs-conditioneringsbeperking met pakketsporen

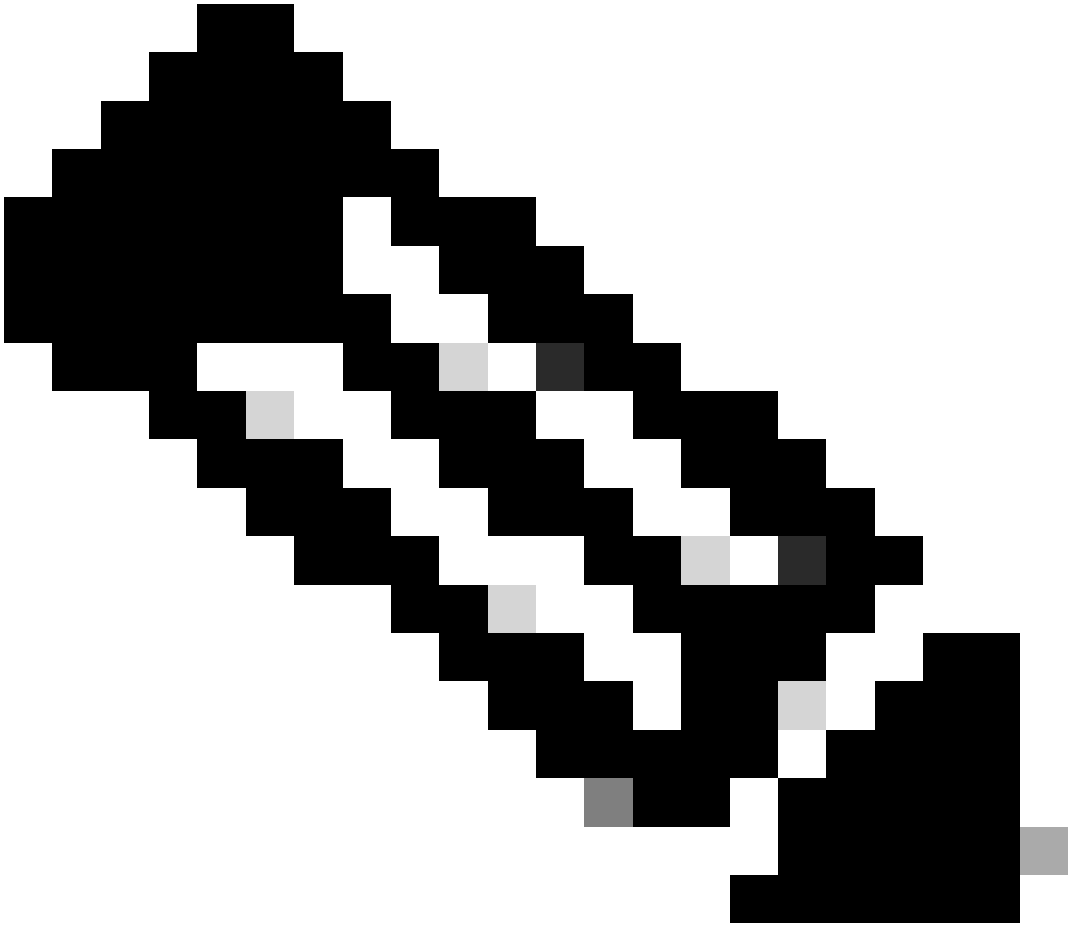
De voorwaarden definiëren de voorwaardelijke filters en wanneer deze worden toegepast op een pakket. Bijvoorbeeld, debug platform voorwaarde interface g0/0/0 uitgang betekent dat een pakket

wordt geïdentificeerd als een gelijke wanneer het de output FIA op interface g0/0/0 bereikt, zodat om het even welke pakketverwerking die van toegang plaatsvindt tot dat punt wordt gemist.



Opmerking: Cisco raadt u ten zeerste aan de toegangsvoorwaarden voor pakketsporen te gebruiken om de meest volledige en betekenisvolle gegevens mogelijk te maken. De uitgangsvoorwaarden kunnen worden gebruikt, maar let op de beperkingen.

De Packet Trace-resultaten weergeven



Opmerking: in deze sectie wordt ervan uitgegaan dat path-trace is ingeschakeld.

Het pakketspoor levert drie specifieke inspectieniveaus:

- Accounting
- Samenvatting per pakket
- Padgegevens per pakket

Wanneer er vijf ICMP-verzoekpakketten worden verzonden van 172.16.10.2 naar 172.16.20.2, kunnen deze opdrachten worden gebruikt om de resultaten van het pakketspoor te bekijken:

<#root>

ASR1000#

show platform packet-trace statistics

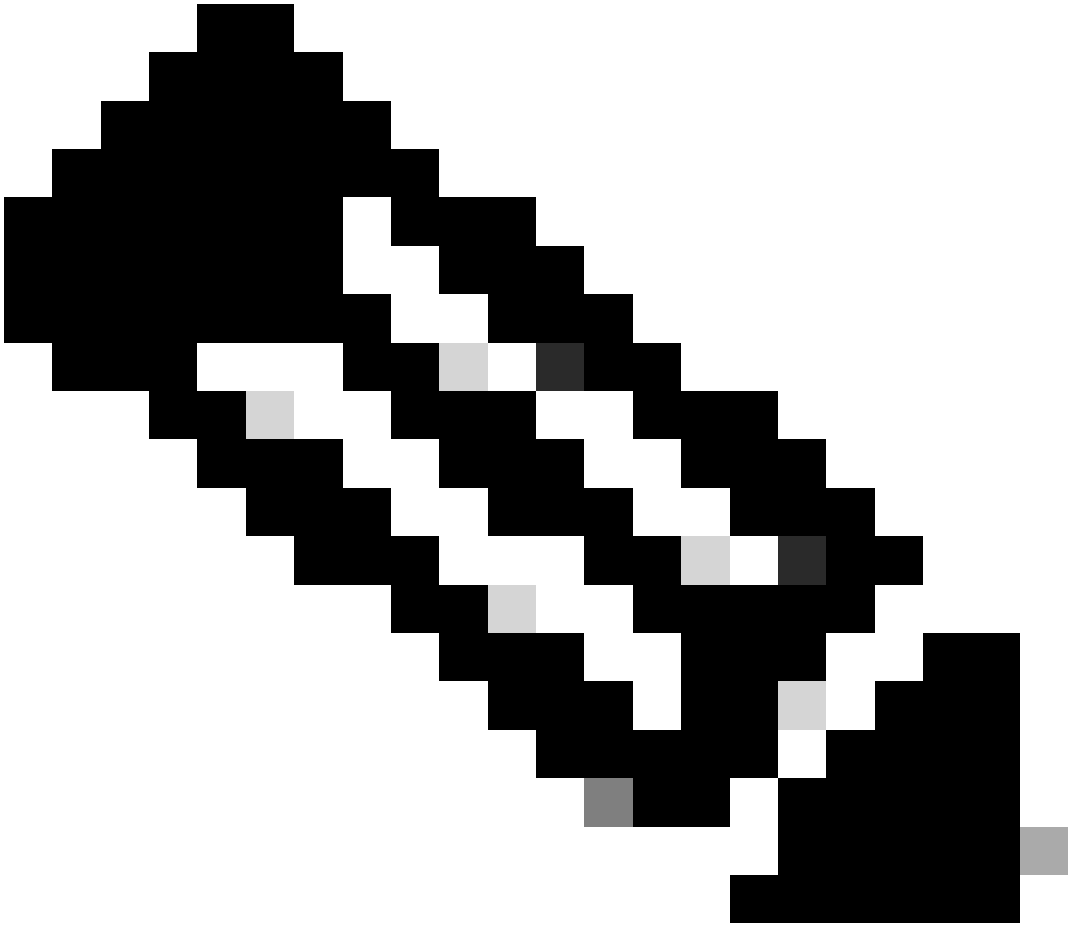
```
Packets Traced: 5


 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#
```



Opmerking: de derde opdracht geeft een voorbeeld van hoe u het pakketspoor voor elk pakket kunt weergeven. In dit voorbeeld wordt het eerste getraceerde pakket weergegeven.

Van deze output, kunt u zien dat vijf pakketten worden overgetrokken en dat u de inputinterface, de outputinterface, de staat, en het wegspoor kunt bekijken.

Toestand	Opmerking
FWD	Het pakket is gepland/in de wachtrij geplaatst voor levering, door te sturen naar volgende hop via een uitgang interface.
PUNT	Het pakket wordt van de het Door:sturen Bewerker (FP) aan de Routeprocessor (RP) (controlevliegtuig) geleefd.
AFWIJZING	Het pakket wordt op FP gevallen. Draai FIA-spoor, gebruik globale drop tellers, of gebruik datapath debugs om meer details te vinden voor drop redenen.
NADELEN	Het pakket wordt tijdens een pakketproces verbruikt, zoals tijdens de ICMP-ping of de crypto-pakketten.

De tellers voor de invoer en injectie in de pakkettraceerstatistieken komen overeen met de pakketten die via een externe interface binnenkomen en pakketten die worden gezien als geïnjecteerd vanuit het bedieningsvlak, respectievelijk.

FIA Trace

De FIA houdt de lijst van functies die sequentieel door de Packet Processor Engines (PPE) in de Quantum Flow Processor (QFP) worden uitgevoerd wanneer een pakket wordt doorgestuurd of ingress of egress. De functies zijn gebaseerd op de configuratiegegevens die op de machine worden toegepast. Zo helpt een FIA-spoor de stroom van het pakket door het systeem te begrijpen als het pakket wordt verwerkt.

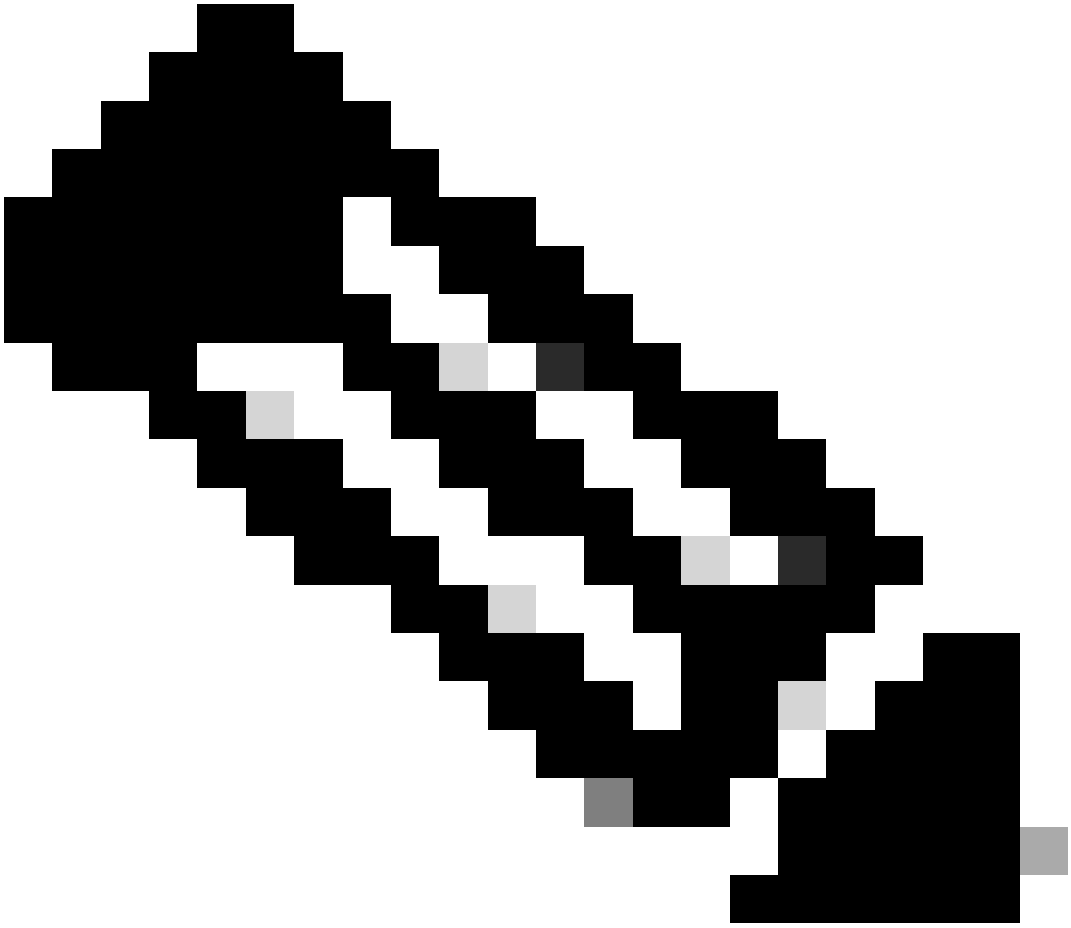
U moet deze configuratiegegevens toepassen om pakkettracering met FIA mogelijk te maken:

<#root>

ASR1000#

debug platform packet-trace packet 16 fia-trace

De Packet Trace-resultaten weergeven



Opmerking: in deze sectie wordt ervan uitgegaan dat FIA-tracering is ingeschakeld. Ook wanneer u de huidige pakkettraceringsopdrachten toevoegt of wijzigt, worden de gegevens van het gebufferde pakketspoor gewist, zodat u opnieuw wat verkeer moet verzenden zodat u het kunt overtrekken.

Verzend vijf ICMP-pakketten van 172.16.10.2 naar 172.16.20.2 nadat u de opdracht hebt ingevoerd die wordt gebruikt om het FIA-spoor in te schakelen, zoals beschreven in de vorige sectie.

<#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#
```

Controleer de FIA die aan een interface is gekoppeld

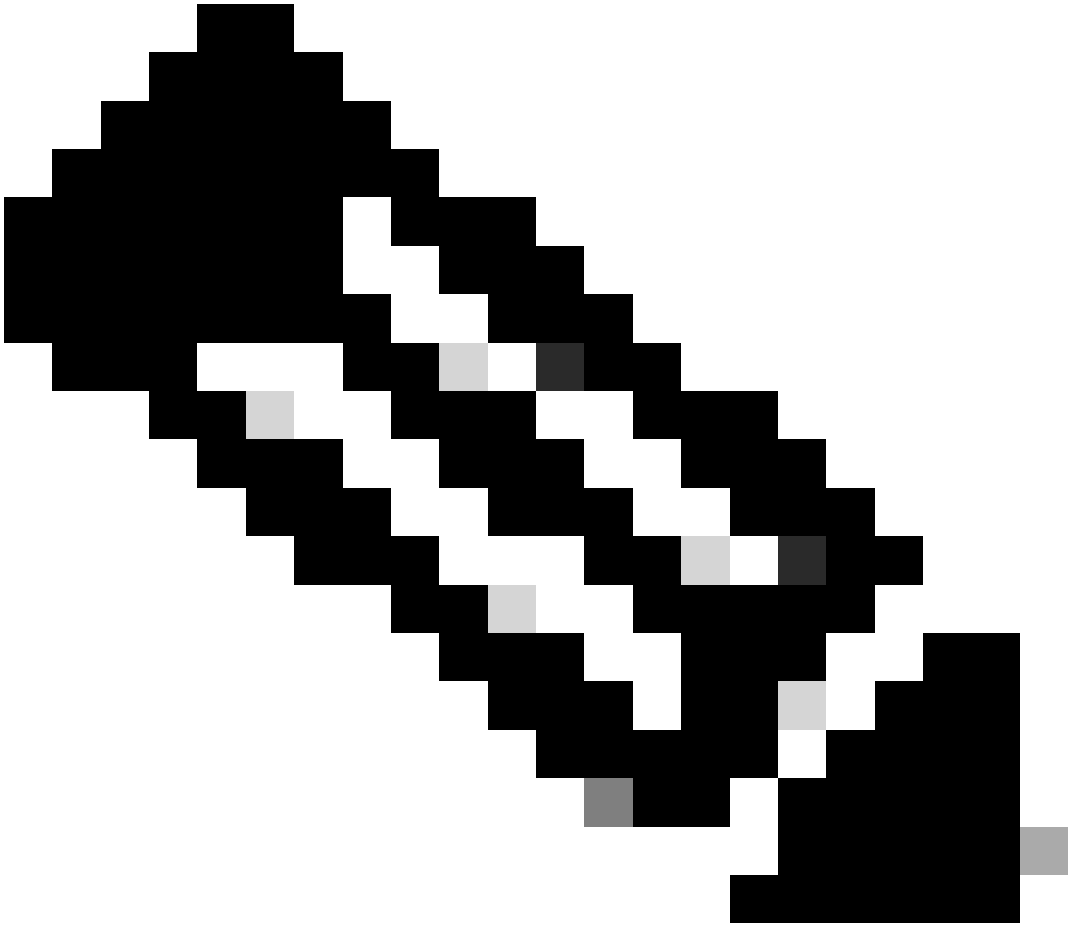
Wanneer u het platform voorwaardelijke debuggen inschakelt, wordt voorwaardelijke debugging als een functie aan de FIA toegevoegd. Gebaseerd op de eigenschaporde van verwerking op de interface, moet het voorwaardelijke filter dienovereenkomstig worden geplaatst, bijvoorbeeld, of het pre- of post-NAT adres in de voorwaardelijke filter moet worden gebruikt.

Deze uitvoer toont de volgorde van de functies in de FIA voor het platform voorwaardelijke debuggen dat is ingeschakeld in de toegangsrichting:

<#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#
```



Opmerking: De CBUG_INPUT_FIA en de DEBUG_COND_INPUT_PKT corresponderen met de voorwaardelijke debug-functies die op de router zijn geconfigureerd.

De overtrek-pakketten dumpen

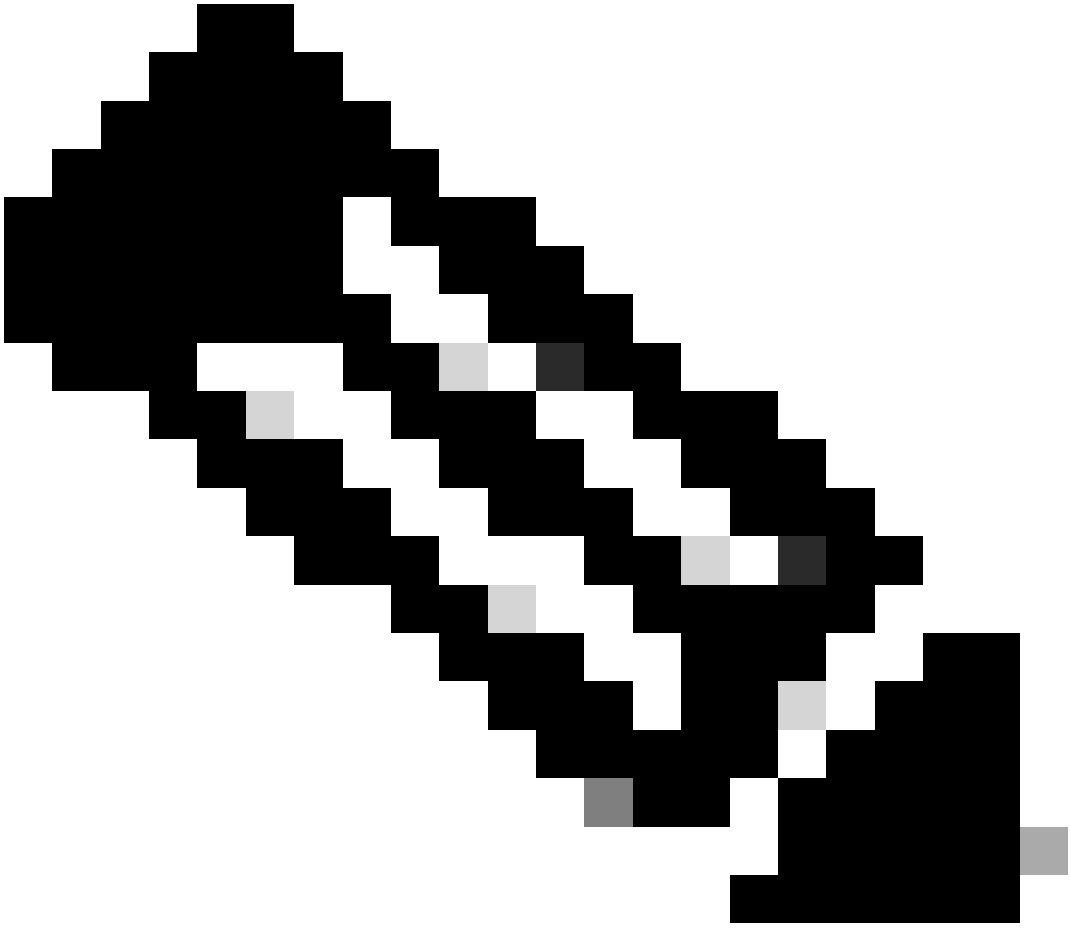
U kunt de pakketten kopiëren en dumpen zoals ze worden overgetrokken, zoals in deze sectie wordt beschreven. Dit voorbeeld laat zien hoe u maximaal 2.048 bytes van de pakketten in de invoerrichting kunt kopiëren (172.16.10.2 tot 172.16.20.2).

Hier is de extra opdracht die nodig is:

<#root>

ASR1000#

debug platform packet-trace copy packet input size 2048



Opmerking: de grootte van het pakket dat wordt gekopieerd, ligt in het bereik van 16 tot 2.048 bytes.

Voer deze opdracht in om de gekopieerde pakketten te dumpen:

<#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#
```

Drop Trace

Drop trace is beschikbaar in Cisco IOS-XE-softwarerelease 3.1 en hoger. Het laat pakketspoor slechts voor gelaten vallen pakketten toe. Hier zijn een paar hoogtepunten van de functie:

- Het staat u toe om het behoud van pakketten voor een specifieke dalingscode te specificeren.
- Het kan zonder globale of interfacevoorwaarden worden gebruikt om dalingsgebeurtenissen te vangen.
- Een drop-gebeurtenis geeft aan dat alleen de drop zelf wordt getraceerd, niet het leven van het pakket. Het staat u echter nog steeds toe om summiere gegevens, tuple gegevens en het pakket op te nemen om de voorwaarden te helpen verfijnen of aanwijzingen te geven voor de volgende debug stap.

Hier is de opdrachtsyntaxis die wordt gebruikt om drop-type pakketsporen in te schakelen:

<#root>

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

De drop code is hetzelfde als de drop-id, zoals gerapporteerd in de show platform hardware qfp actieve statistieken drop detail opdrachtoutput:

<#root>

```
ASR1000#
show platform hardware qfp active statistics drop detail

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

Voorbeeld van Drop Trace Scenario

Pas deze ACL toe op de interface Gig 0/0/0 van de ASR1K om verkeer te laten vallen van 172.16.10.2 naar 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
```

Met ACL op zijn plaats, die het verkeer van de lokale gastheer aan de verre gastheer laat vallen, pas deze drop-trace configuratie toe:

<#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
```

Verzend vijf ICMP verzoekpakketten van 172.16.10.2 tot 172.16.20.2. Het dalingsspoor vangt deze pakketten die door ACL, zoals getoond worden gelaten vallen:

<#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#
```

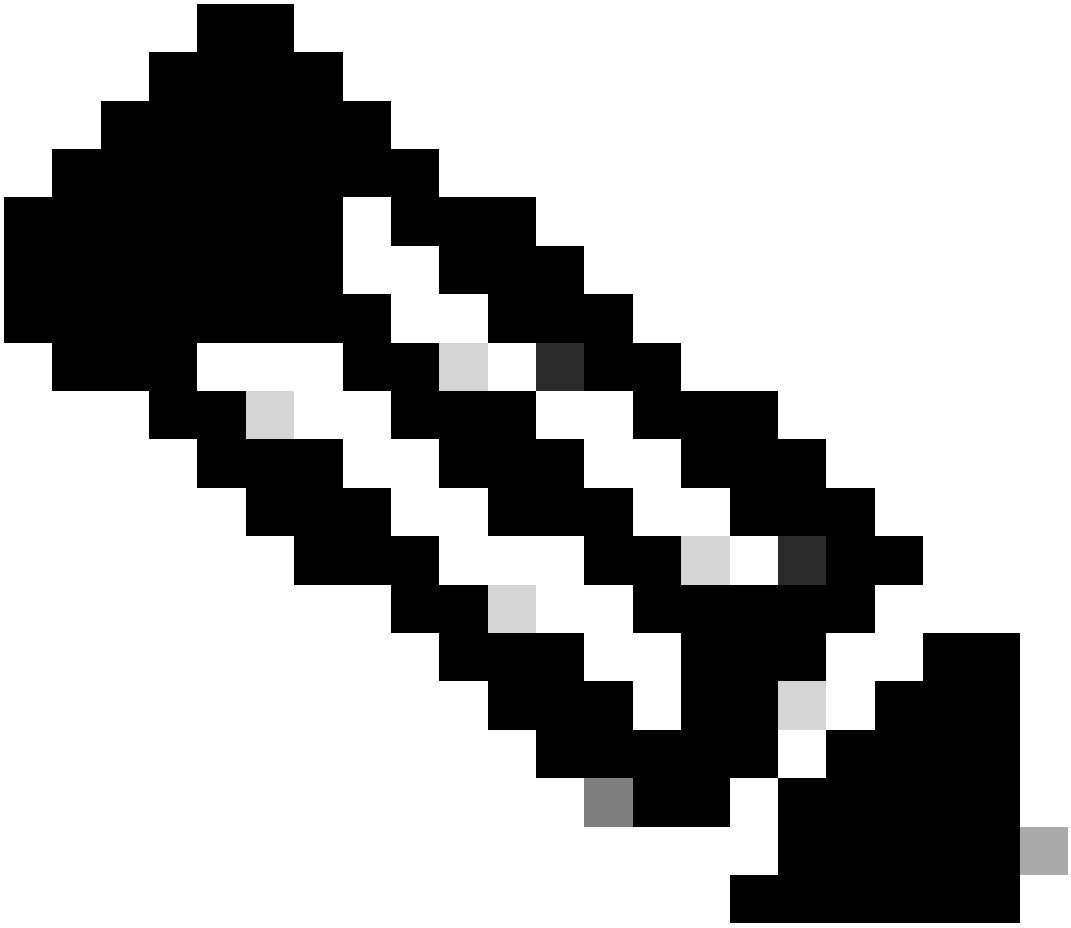
show platform packet-trace packet 0

```
 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#
```

Injecteren en Punt Traces

De optie Injecteren en punt pakketovertrekken is toegevoegd in Cisco IOS-XE softwarerelease 3.12 en hoger om punt (pakketten die op de FP worden ontvangen die naar het besturingsplane worden geprikt) en pakketten (pakketten die van het besturingsplane in het FP worden geïnjecteerd) te kunnen injecteren.



Opmerking: Het punt spoor kan werken zonder de globale of interfacevoorwaarden, net als een drop spoor. De condities dienen echter te worden gedefinieerd voor een injectiesporen tot aan het werk.

Hier is een voorbeeld van een punt en inject packet trace wanneer u van ASR1K aan een aangrenzende router pingelt:

<#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#
```

U kunt nu de resultaten punt en nject trace rresultaten verifiëren:

<#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)
```

Packet Trace-verbetering met IOSd en LFTS Punt/Inject Trace en UDF-matching (nieuw in 17.3.1)

De functie voor pakkettracering is verder verbeterd en biedt aanvullende traceerinformatie voor pakketten die zijn gegenereerd of bestemd zijn voor IOS-D of andere BinOS-processen in Cisco IOS-XE release 17.3.1.

IOS Drop Tracing

Met deze verbetering, pakket wordt het vinden uitgebreid in IOSd, en kan informatie over om het even welke pakketdalingen binnen van IOSd verstrekken, die gewoonlijk in de ***show ip*** verkeersoutput worden gemeld. Er is geen extra configuratie vereist om IOSd drop-tracering in te schakelen. Hier is een voorbeeld van een UDP-pakket dat door IOSd is gedropt vanwege een slechte controlesomfout:

```
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)
```

IOSd uitgaande padtracering

Het pakketspoor wordt verbeterd om de informatie van het wegspoor en van de protocolverwerking te tonen aangezien het pakket uit IOSd voortkomt en in de uitgangsrichting naar het netwerk wordt verzonden. Er is geen extra configuratie vereist om de IOSd informatie van het uitgangspad te vangen. Hier is een voorbeeld van het overtrekken van de uitgangsweg voor een pakket van SSH dat de router egresseert:

<#root>

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

IOSd Path Flow:

```
  Feature: TCP
  Pkt Direction: OUTtcp0: O 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: O 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
```

LFTS-pakkettracering

LFTS (Linux Forwarding Transport Service) is een transportmechanisme om pakketten die van CPP worden gekopieerd door te sturen naar andere toepassingen dan IOSd. LFTS-pakkettraceringsverbetering heeft traceringsinformatie toegevoegd voor dergelijke pakketten in de padtraceringsuitvoer. Er is geen extra configuratie vereist om de LFTS overtredingsinformatie te verkrijgen. Hier is een voorbeelduitvoer van LFTS-overtrekken voor bestraft pakket naar de NETCONF-toepassing:

<#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
```

Packet trace-patroonmatching op basis van door de gebruiker gedefinieerde filter (alleen voor ASR 1000-platform)

In Cisco IOS-XE release 17.3.1 wordt ook een nieuw pakketaanpassingsmechanisme toegevoegd aan de ASR1000-productfamilies zodat deze overeenkomen met een willekeurig veld in een pakket op basis van de UDF-infrastructuur (User Defined Filter). Dit maakt flexibele pakketmatching mogelijk op basis van velden die geen deel uitmaken van de standaard L2/L3/L4-headerstructuur. Het volgende voorbeeld toont een UDF-definitie die overeenkomt met 2 bytes van door de gebruiker gedefinieerd patroon van 0x4D2 dat begint bij een offset van 26 bytes van de L3-routerprotocolkop.

```
udf grekey header outer l3 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
```

Packet Trace-voorbeelden

Deze sectie verschaft een aantal voorbeelden waar de pakkettraceringsfunctie nuttig is voor probleemoplossing.

Packet Trace-voorbeeld - NAT

Bij dit voorbeeld wordt een interface source Network Address Translation (NAT) geconfigureerd op de WAN-interface van een ASR1K (Gig0/0/0) voor het lokale subnet (172.16.10.0/24).

Hier is de platformvoorwaarde en de configuratie van het pakketspoor die worden gebruikt om het verkeer van 172.16.10.2 tot 172.16.20.2 te vinden, dat (NAT) op de interface Gig0/0/0 wordt vertaald:

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

Wanneer vijf ICMP-pakketten worden verzonden van 172.16.10.2 naar 172.16.20.2 met een interfacebron-NAT-configuratie, zijn dit de resultaten van het pakketspoor:

```
      <#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#
```

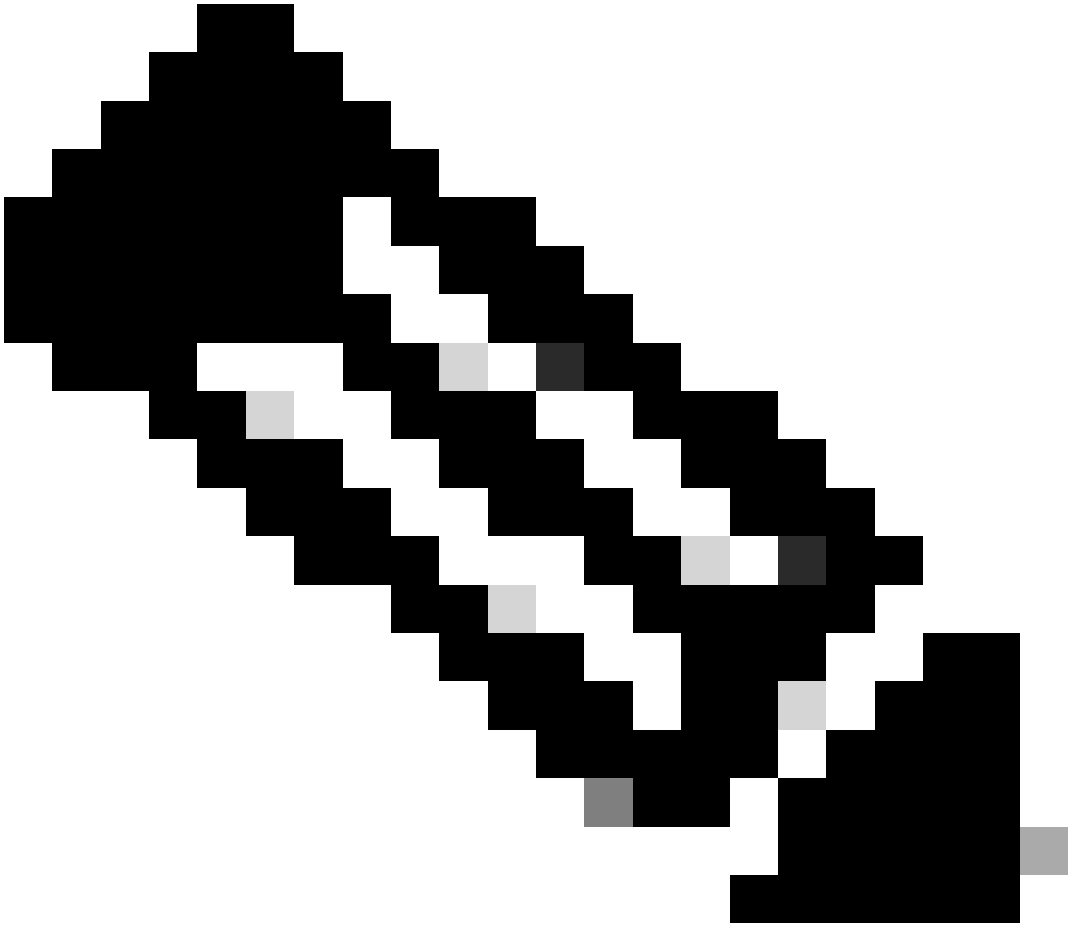
Packet Trace-voorbeeld - VPN

In dit voorbeeld wordt een site-to-site VPN-tunnel gebruikt tussen de ASR1K en de Cisco IOS-router om het verkeer te beschermen dat tussen 172.16.10.0/24 en 172.16.20.0/24 (lokale en externe subnetten) stroomt.

Hier is de platformvoorwaarde en de configuratie van het pakketspoor die worden gebruikt om het VPN-verkeer te traceren dat van 172.16.10.2 tot 172.16.20.2 op de Gig 0/0/1 interface stroomt:

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

Wanneer vijf ICMP-pakketten worden verzonden van 172.16.10.2 naar 172.16.20.2, die in dit voorbeeld zijn versleuteld door de VPN-tunnel tussen de ASR1K en de Cisco IOS-router, zijn dit de resultaten van de pakkettracering:



Opmerking: de pakketsporen tonen de QFP Security Association (SA) handgreep in het spoor dat wordt gebruikt om het pakket te versleutelen. Dit is handig wanneer u IPsec VPN-problemen oplost om te verifiëren dat de juiste SA wordt gebruikt voor de codering.

<#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#
```

Effect op prestaties

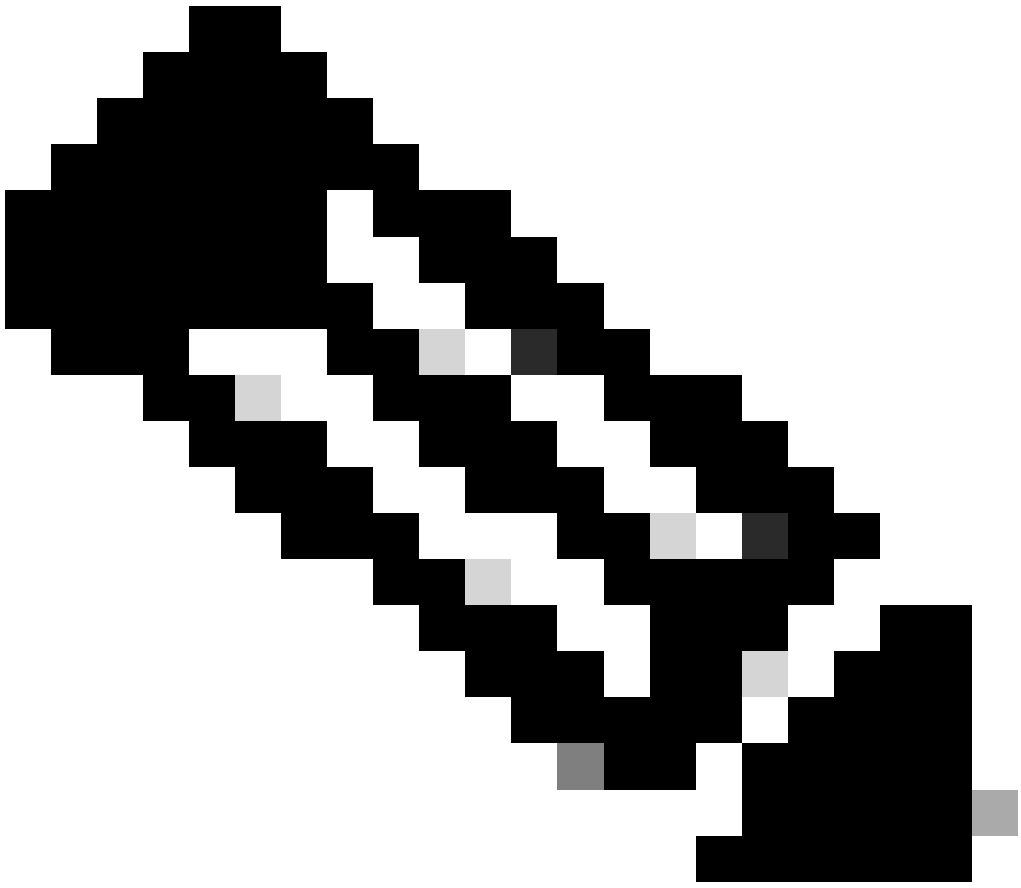
De buffers van het pakketspoor verbruiken QFP DRAM, zo rekening houdend met de hoeveelheid geheugen die een configuratie vereist en de hoeveelheid geheugen die beschikbaar is.

De invloed op de prestaties varieert afhankelijk van de opties voor pakkettracering die zijn ingeschakeld. Het pakketspoor beïnvloedt slechts de het door:sturen prestaties van de pakketten die worden gevonden, zoals die pakketten die de gebruiker-gevormde voorwaarden aanpassen. De gedetailleerdere en gedetailleerdere informatie die u het pakketspoor vormt om op te nemen, hoe groter het middelen kan beïnvloeden.

Zoals met om het even welke het oplossen van problemen, is het best om een herhalende benadering te kiezen en slechts de meer gedetailleerde spooropties toe te laten wanneer een debug situatie het rechtvaardigt.

Het gebruik van QFP DRAM’s kan worden geschat met deze formule:

benodigd geheugen = (stats overhead) + aantal stuks * (summiere grootte + pad gegevensgrootte + kopieergrootte)



Opmerking: waar de **stats overhead** en de **overzichtsgrootte** zijn vastgesteld op respectievelijk 2 KB en 128 B, kunnen de

---

padgegevensgrootte en de **kopieergrootte** door de gebruiker worden geconfigureerd.

Gerelateerde informatie

- **Software voor de configuratiehandleiding voor Cisco ASR 1000 Series routers voor aggregatie - Packet Trace**
- **Packet Drops op Cisco ASR 1000 Series servicerouters**
- **Cisco Technical Support en downloads**

Over deze vertaling

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