Risoluzione dei problemi con la funzionalità IOS-XE Datapath Packet Trace

Sommario

Introduzione

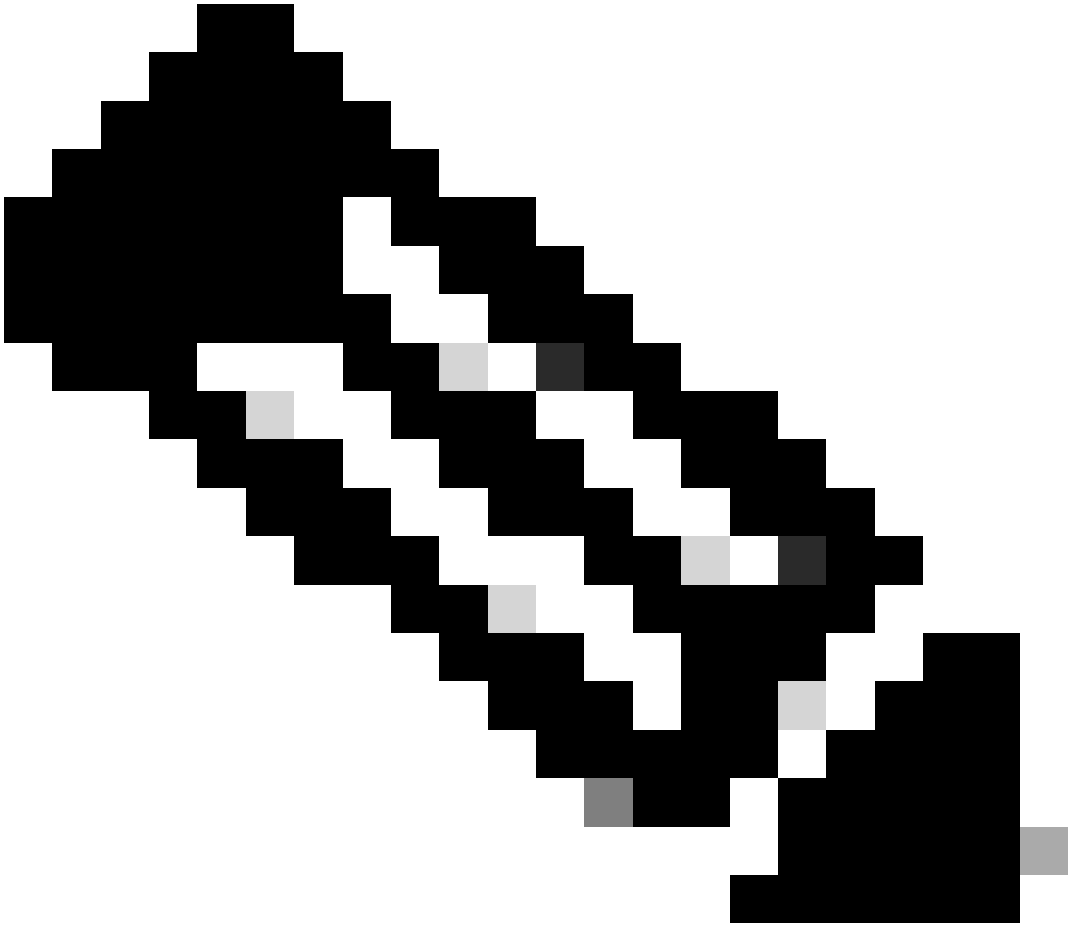
Questo documento descrive come eseguire la traccia dei pacchetti di datapath per il software Cisco IOS-XE® tramite la funzione Packet Trace.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza delle seguenti informazioni:

La funzione packet-trace è disponibile nelle versioni Cisco IOS-XE 3.10 e successive sulle piattaforme di routing basate su QFP (Quantum Flow Processor), che includono i router ASR1000, ISR4000, ISR1000, Catalyst 1000, Catalyst 8000, CSR1000v e Catalyst serie 8000v. Questa funzione non è supportata sui router dei servizi di aggregazione ASR900 o sugli switch Catalyst serie 900 con software Cisco IOS-XE.



> Nota: la funzione packet-trace non funziona sull'interfaccia di gestione dedicata, Gigabit Ethernet0 sui router serie ASR1000, poiché i pacchetti inoltrati su quell'interfaccia non vengono elaborati da QFP.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Software Cisco IOS-XE release 3.10S (15.3(3)S) e successive
- ASR serie 1000 router

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Per identificare problemi come una configurazione errata, un sovraccarico di capacità o anche un normale bug software durante la risoluzione dei problemi, è necessario capire cosa succede a un pacchetto all'interno di un sistema. La funzione Cisco IOS-XE Packet Trace soddisfa questa esigenza. Fornisce un metodo sicuro sul campo utilizzato per l'accounting e per acquisire i dettagli del processo per pacchetto in base a una classe di condizioni definite dall'utente.

Topologia di riferimento

Il diagramma mostra la topologia utilizzata per gli esempi descritti nel presente documento:

Traccia pacchetti in uso

Per illustrare l'uso della funzione packet trace, l'esempio usato in questa sezione descrive una traccia del traffico ICMP (Internet Control Message Protocol) dalla workstation locale 172.16.10.2 (dietro ASR1K) all'host remoto 172.16.20.2 in direzione di entrata sull'interfaccia Gigabit Ethernet0/0/1 sull'ASR1K.

È possibile tracciare i pacchetti sull'ASR1K in due modi:

1. Abilitare i debug condizionali della piattaforma per selezionare i pacchetti o il traffico che si desidera tracciare sull'ASR1K.

2. Abilitare la traccia del pacchetto della piattaforma con l'opzione path-trace o Feature Invocation Array (FIA) trace.

Guida introduttiva

Di seguito è riportata una guida introduttiva se si ha già familiarità con il contenuto di questo documento e si desidera una sezione per una rapida panoramica della CLI. Questi sono solo

alcuni esempi per illustrare l'utilizzo dello strumento. Consultare le sezioni successive in cui vengono descritte in dettaglio le sintassi e assicurarsi di utilizzare la configurazione appropriata alle proprie esigenze.

1. Configurare le condizioni della piattaforma:

<#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)

Dopo aver configurato una condizione della piattaforma, avviare le condizioni della piattaforma con questo comando CLI:

<#root>

debug platform condition start

2. Configura traccia pacchetto:

<#root>

debug platform packet-trace packet 1024

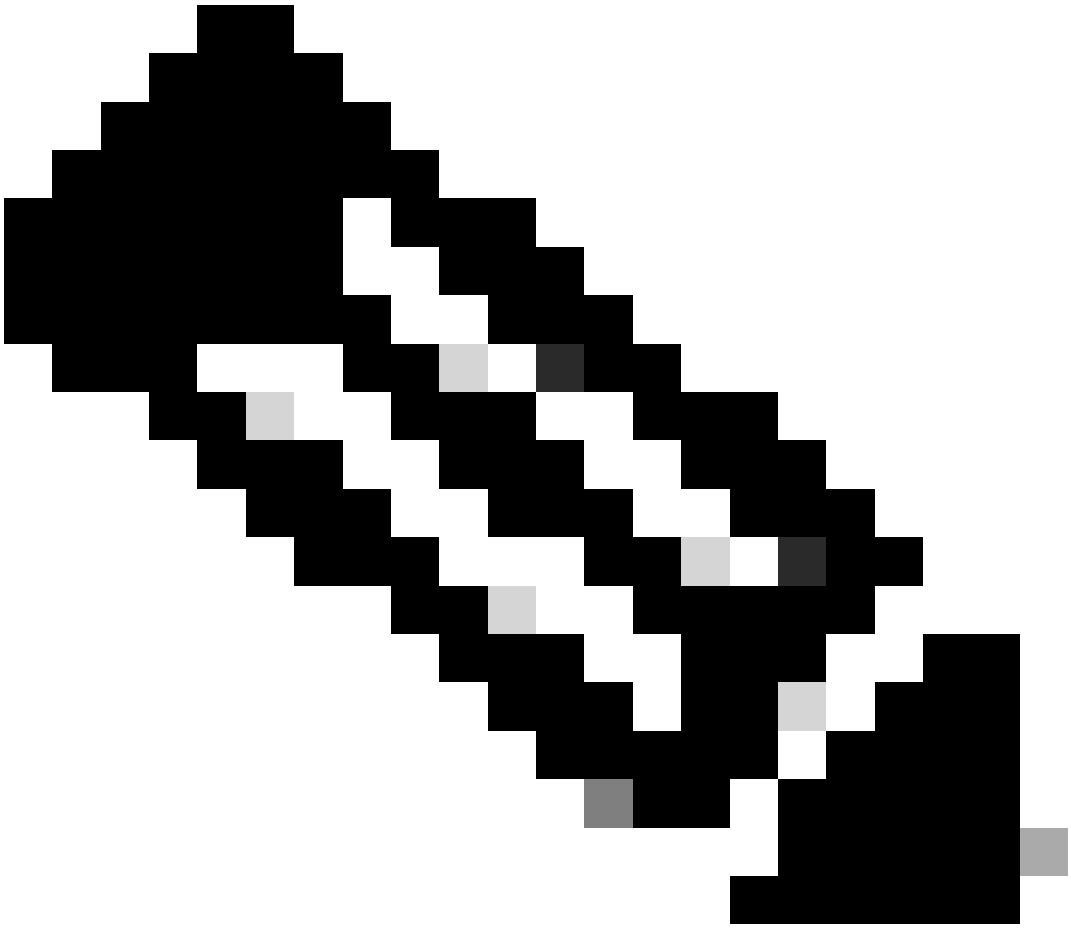
-> basic path-trace, and automatically stops
tracing packets after 1024 packets. You can use "circular" option if needed

debug platform packet-trace packet 1024 fia-trace -

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

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

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



Nota: nelle versioni precedenti di Cisco IOS-XE 3.x, per avviare la funzione packet-trace è necessario anche il comando debug platform packet-trace enable. Questa funzionalità non è più richiesta nelle versioni Cisco IOS-XE 16.x.

Immettere questo comando per cancellare il buffer di traccia e reimpostare packet-trace:

<#root>

clear platform packet-trace statistics

  --> clear the packet trace buffer

Il comando per cancellare le condizioni della piattaforma e la configurazione della traccia del pacchetto è:

<#root>

clear platform condition all

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

Comandi show

Verificare la condizione della piattaforma e la configurazione della traccia dei pacchetti dopo aver applicato i comandi precedenti per assicurarsi di avere i dati necessari.

<#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

Di seguito sono riportati i comandi per controllare i pacchetti tracciati/acquisiti:

<#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
```

Abilita debug condizionali della piattaforma

Per determinare i pacchetti da tracciare, la funzionalità Packet Trace si basa sull'infrastruttura di debug condizionale. L'infrastruttura di debug condizionale consente di filtrare il traffico in base a:

- Protocollo
- Indirizzo IP e maschera
- Access Control List (ACL)
- Interfaccia
- Direzione del traffico (in entrata o in uscita)

Queste condizioni definiscono dove e quando i filtri vengono applicati a un pacchetto.

Per il traffico usato nell'esempio, abilitare i debug condizionali della piattaforma nella direzione in entrata per i pacchetti ICMP da 172.16.10.2 a 172.16.20.2. In altre parole, selezionare il traffico da tracciare. Per selezionare questo traffico, è possibile utilizzare diverse opzioni.

<#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
```

Nell'esempio, viene usato un elenco degli accessi per definire la condizione, come mostrato di seguito:

<#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#
```

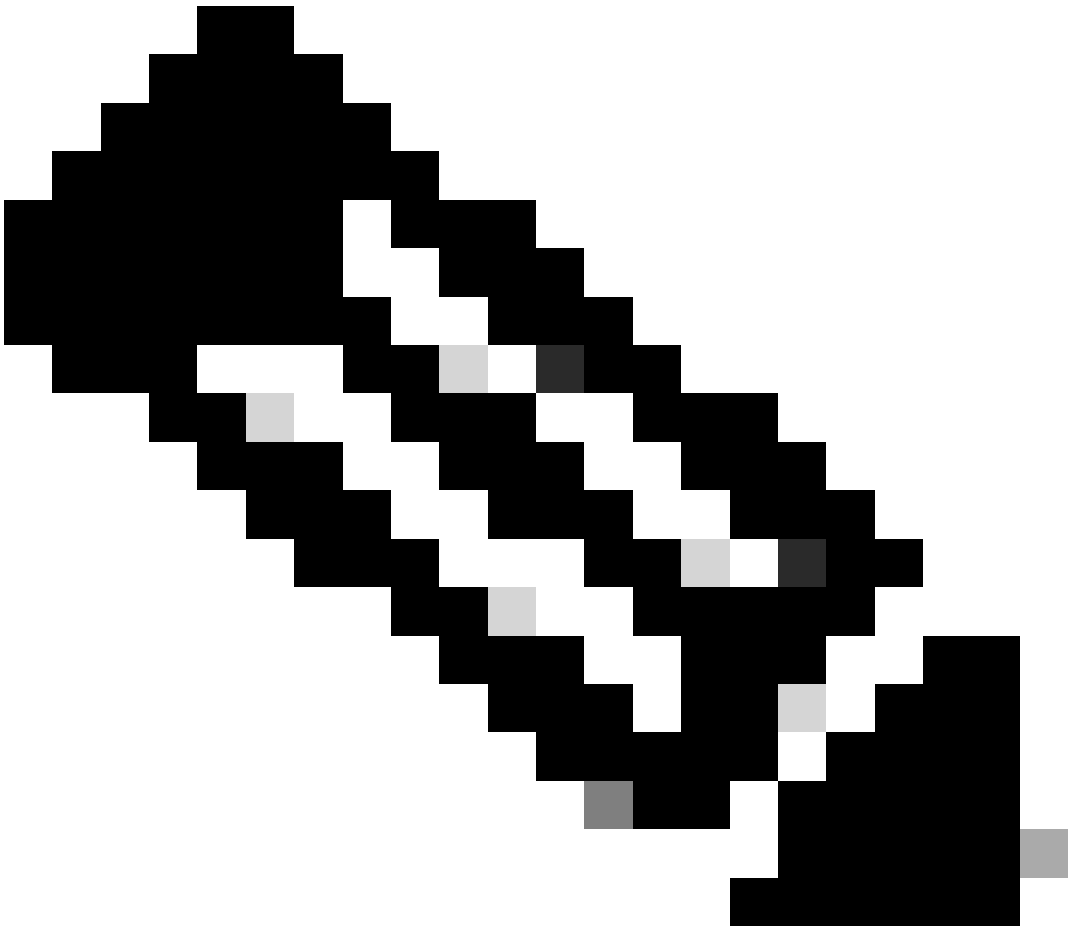
```
debug platform condition interface gig 0/0/1 ipv4
 access-list 150 ingress
```

Per avviare il debug condizionale, immettere questo comando:

<#root>

```
ASR1000#
```

```
debug platform condition start
```



Nota: per arrestare o disabilitare l'infrastruttura di debug condizionale, immettere il comando debug platform condition stop.

Per visualizzare i filtri di debug condizionali configurati, immettere questo comando:

<#root>

```
ASR1000#
```

show platform conditions

```
Conditional Debug Global State:
```

Start

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

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

ASR1000#
```

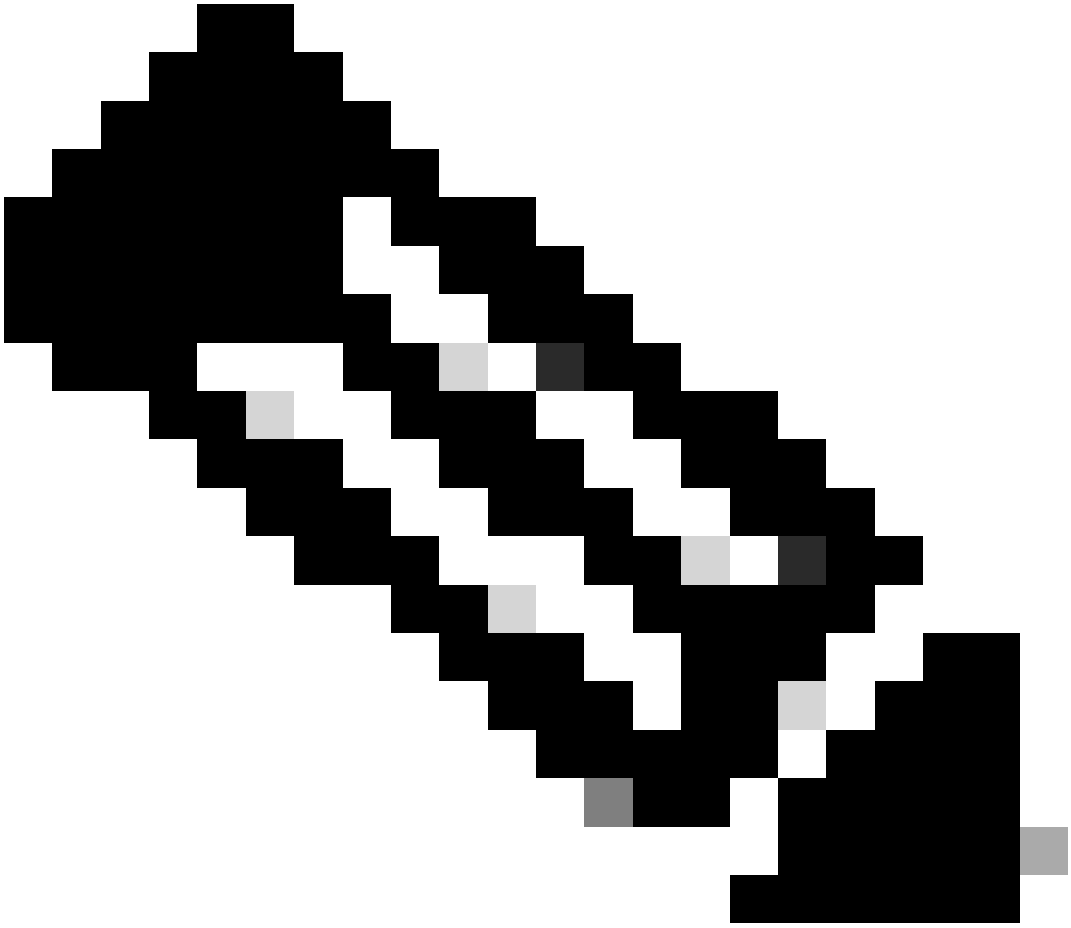
In sintesi, questa configurazione è stata finora applicata:

<#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

Abilita traccia pacchetti



Nota: questa sezione descrive in dettaglio le opzioni relative al pacchetto e alla copia, mentre le altre opzioni sono descritte più avanti nel documento.

Le tracce dei pacchetti sono supportate sia sulle interfacce fisiche che su quelle logiche, ad esempio sulle interfacce tunnel o di accesso virtuale.

Di seguito è riportata la sintassi della CLI di traccia del pacchetto:

<#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>]**

Di seguito vengono descritte le parole chiave di questo comando:

- pkt-num - Il numero di pacchetto specifica il numero massimo di pacchetti che vengono gestiti contemporaneamente.
- summary-only - Specifica che vengono acquisiti solo i dati di riepilogo. Per impostazione predefinita, vengono acquisiti sia i dati di riepilogo che i dati dei percorsi delle funzionalità.
- fia-trace: consente di eseguire facoltativamente una traccia FIA in aggiunta alle informazioni sui dati del percorso.
- data-size: consente di specificare le dimensioni del buffer dei dati del percorso, da 2.048 a 16.384 byte. Il valore predefinito è 2.048 byte.

<#root>

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

Di seguito vengono descritte le parole chiave di questo comando:

- in/out - Specifica la direzione del flusso del pacchetto da copiare: in entrata e/o in uscita.
- L2/L3/L4: consente di specificare la posizione in cui avviare la copia del pacchetto. Il livello 2 (L2) è la posizione predefinita.
- size - Consente di specificare il numero massimo di ottetti copiati. L'impostazione predefinita è 64 ottetti.

Nell'esempio, questo è il comando usato per abilitare la traccia dei pacchetti per il traffico selezionato con l'infrastruttura di debug condizionale:

<#root>

ASR1000#

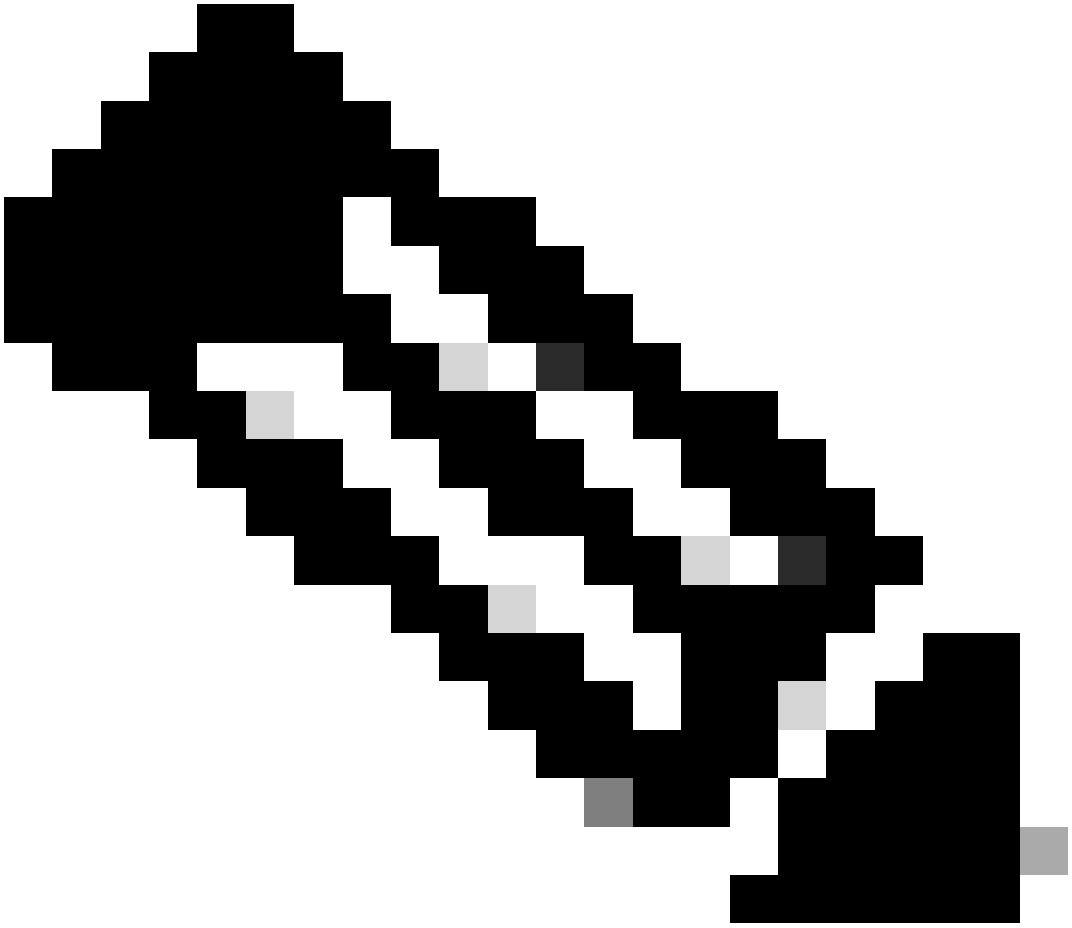
debug platform packet-trace packet 16

Per esaminare la configurazione della traccia del pacchetto, immettere questo comando:

```
<#root>

ASR1000#

show platform packet-trace configuration


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

È inoltre possibile immettere il comando show debugging per visualizzare i debug condizionali della piattaforma e le configurazioni di traccia dei pacchetti:

```
<#root>

ASR1000#

show debugging


IOSXE Conditional Debug Configs:


Conditional Debug Global State: Start

Conditions
                                                                Direction
------------------------------------------------------------------------|---------
GigabitEthernet0/0/1                     & IPV4 ACL [150]              ingress
...
IOSXE Packet Tracing Configs:

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

Feature  Type           Submode                                          Level
-------|--------------|-----------------------------------------------|----------


IOSXE Packet Tracing Configs:


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



Nota: immettere il comando clear platform condition all per cancellare tutte le condizioni di debug della piattaforma, le configurazioni e i dati di traccia del pacchetto.

In breve, questi dati di configurazione sono stati usati fino ad ora per abilitare la traccia dei pacchetti:

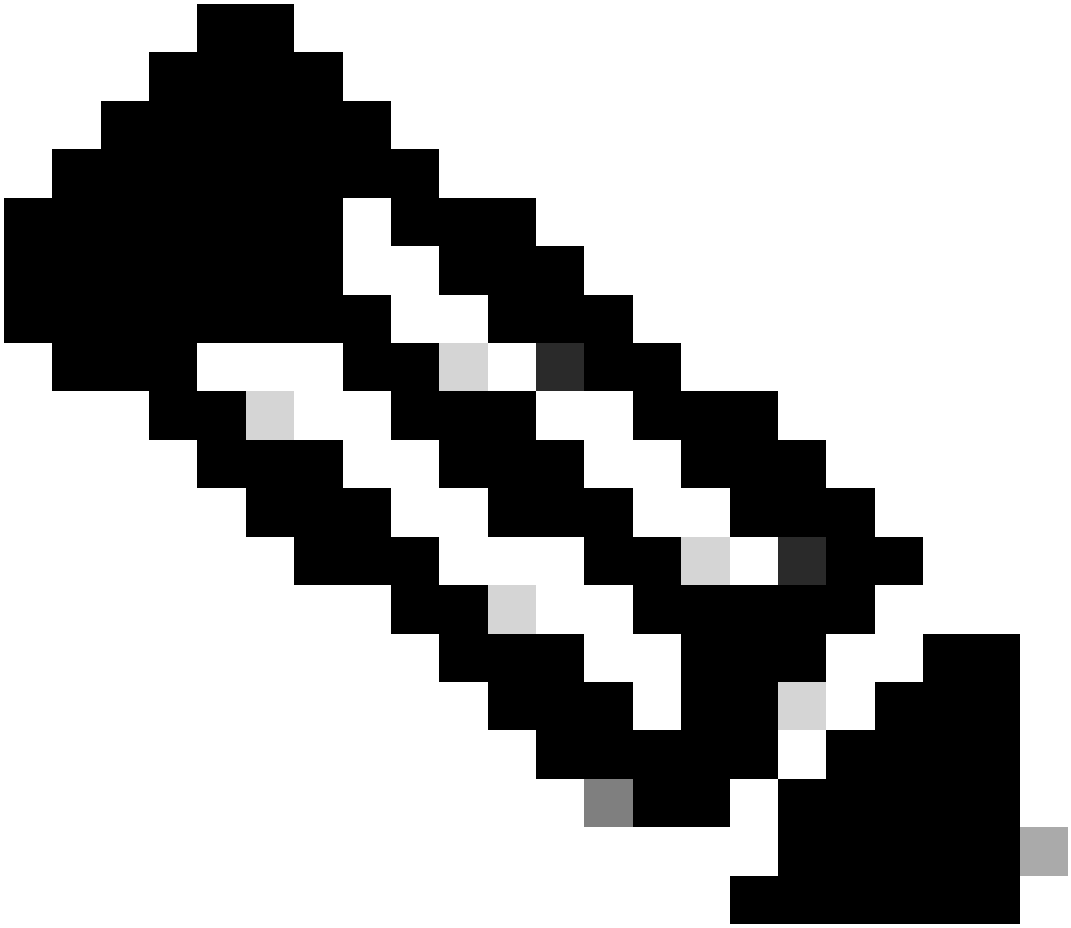
<#root>

debug platform packet-trace packet 16

Limitazione della condizione di uscita con tracce del pacchetto

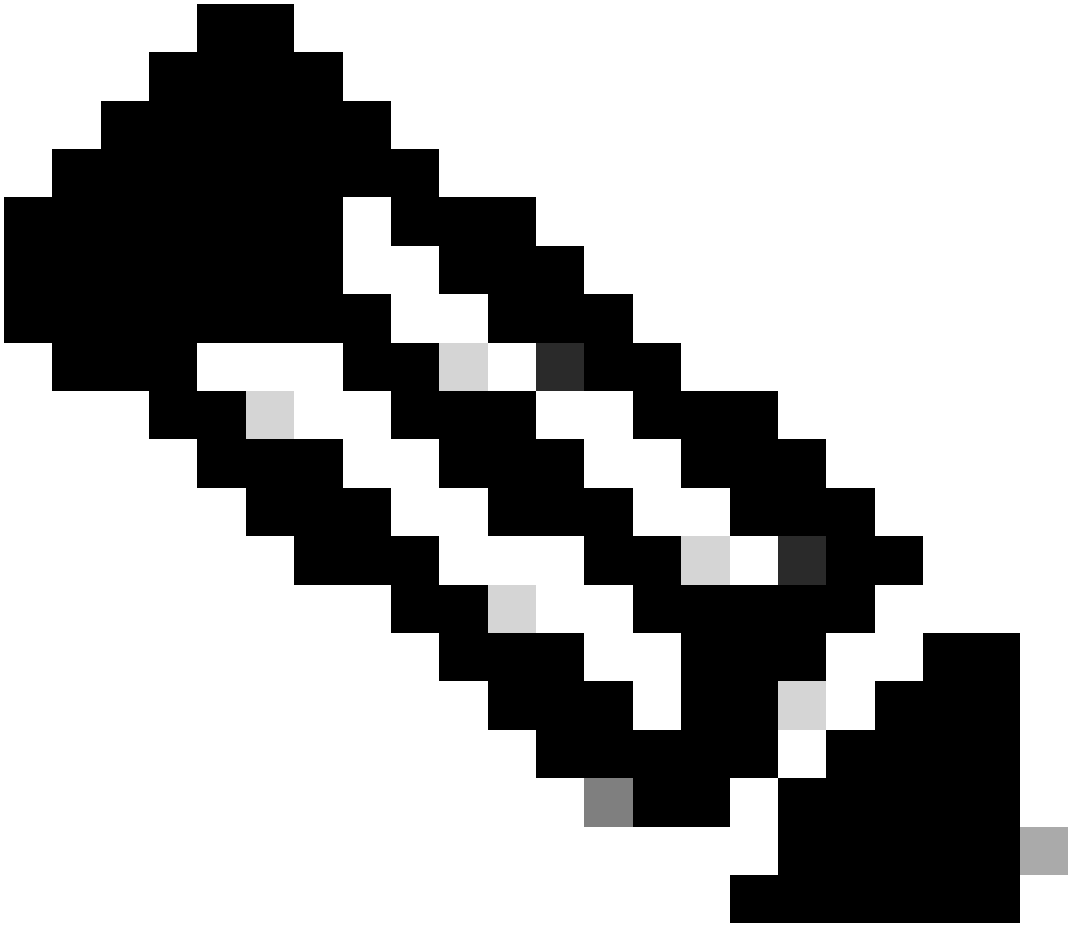
Le condizioni definiscono i filtri condizionali e quando vengono applicati a un pacchetto. Ad esempio, debug platform condition interface g0/0/0 uscita significa che un pacchetto viene identificato come corrispondente quando raggiunge l'output FIA sull'interfaccia g0/0/0, quindi

qualsiasi elaborazione di pacchetto che ha luogo dall'entrata fino a quel punto viene persa.



Nota: Cisco consiglia di usare le condizioni di ingresso per le tracce dei pacchetti al fine di ottenere dati più completi e significativi possibile. È possibile utilizzare le condizioni di uscita, ma occorre essere consapevoli dei limiti.

Visualizzazione dei risultati della traccia del pacchetto



Nota: in questa sezione si presume che la traccia del percorso sia abilitata.

Il tracciato del pacchetto fornisce tre livelli specifici di ispezione:

- Contabilità
- Riepilogo per pacchetto
- Dati percorso per pacchetto

Quando si inviano cinque pacchetti di richiesta ICMP da 172.16.10.2 a 172.16.20.2, è possibile usare questi comandi per visualizzare i risultati della traccia del pacchetto:

<#root>

ASR1000#

show platform packet-trace statistics

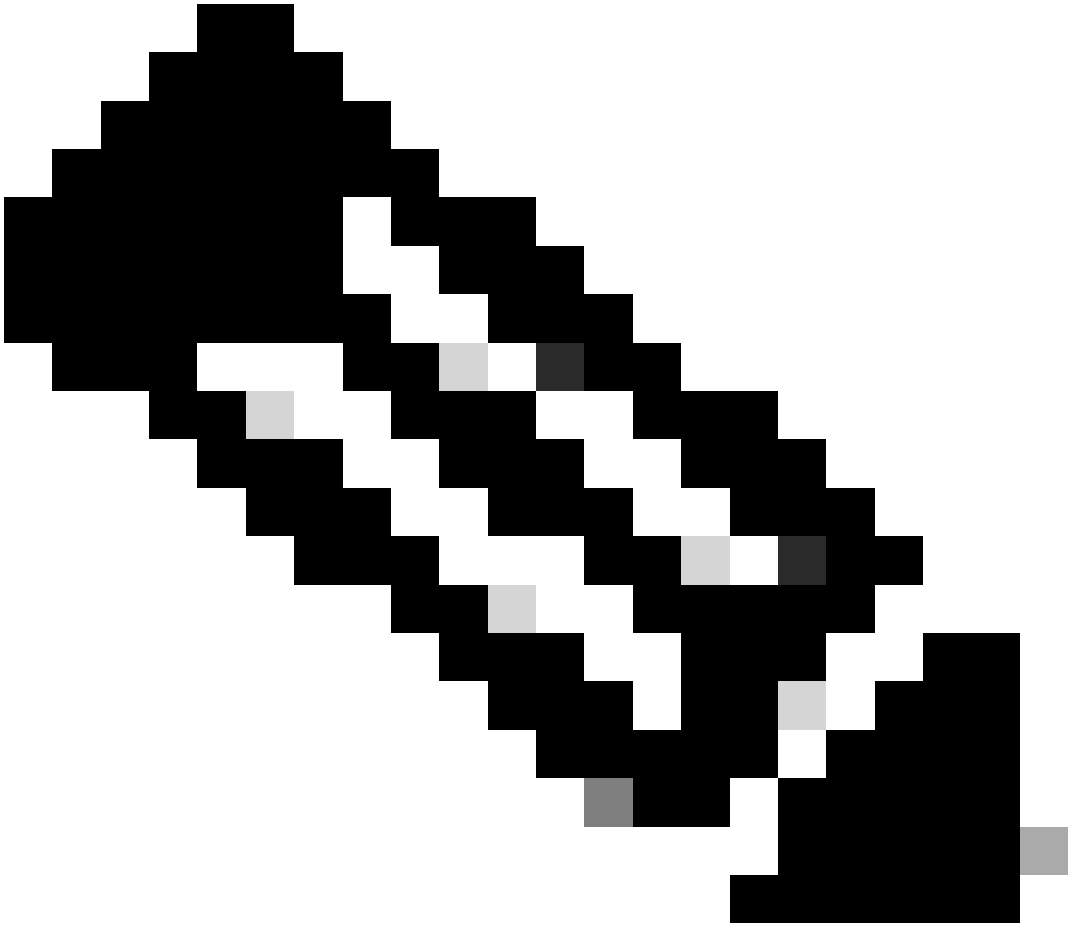
```
Packets Traced: 5


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

 ASR1000#
```

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

```
Pkt

   Input            Output           State  Reason


0

     Gi0/0/1          Gi0/0/0          FWD
 1     Gi0/0/1          Gi0/0/0          FWD
 2     Gi0/0/1          Gi0/0/0          FWD
 3     Gi0/0/1          Gi0/0/0          FWD
 4     Gi0/0/1          Gi0/0/0          FWD

 ASR1000#
```

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

```
 Packet: 0

          CBUG ID: 4
 Summary
 Input     : GigabitEthernet0/0/1
 Output    : GigabitEthernet0/0/0
 State     : FWD
 Timestamp
    Start   : 1819281992118 ns (05/17/2014 06:42:01.207240 UTC)
    Stop    : 1819282095121 ns (05/17/2014 06:42:01.207343 UTC)
 Path Trace
 Feature: IPV4
 Source      : 172.16.10.2
 Destination : 172.16.20.2
 Protocol    : 1 (ICMP)

 ASR1000#
```



Nota: il terzo comando fornisce un esempio che mostra come visualizzare la traccia del pacchetto per ciascun pacchetto. Nell'esempio, viene mostrato il primo pacchetto tracciato.

Da questi output, è possibile vedere che sono stati tracciati cinque pacchetti e che è possibile visualizzare l'interfaccia di input, l'interfaccia di output, lo stato e la traccia del percorso.

State	Osservazioni
FWD	Il pacchetto viene programmato/messo in coda per la consegna, per essere inoltrato all'hop successivo tramite un'interfaccia di uscita.
PUNT	Il pacchetto viene inviato dal processore di inoltro (FP) al processore di routing (RP) (control plane).
DROP	Il pacchetto viene scartato sull'FP. Eseguire la traccia FIA, utilizzare i contatori di rilascio globali o utilizzare i debug datapath per trovare ulteriori dettagli per motivi di rilascio.
SVANTAGGI	Il pacchetto viene consumato durante un processo, ad esempio durante la

	richiesta ping ICMP o i pacchetti crittografici.

I contatori entrata e entrata nell'output delle statistiche di traccia dei pacchetti corrispondono ai pacchetti che entrano rispettivamente tramite un'interfaccia esterna e dai pacchetti che vengono visti come iniettati dal piano di controllo.

Traccia FIA

La FIA contiene l'elenco di funzionalità che vengono eseguite in sequenza dai Packet Processor Engine (PPE) nel Quantum Flow Processor (QFP) quando un pacchetto viene inoltrato in entrata o in uscita. Le feature si basano sui dati di configurazione applicati alla macchina. Pertanto, una traccia FIA aiuta a comprendere il flusso del pacchetto attraverso il sistema mentre il pacchetto viene elaborato.

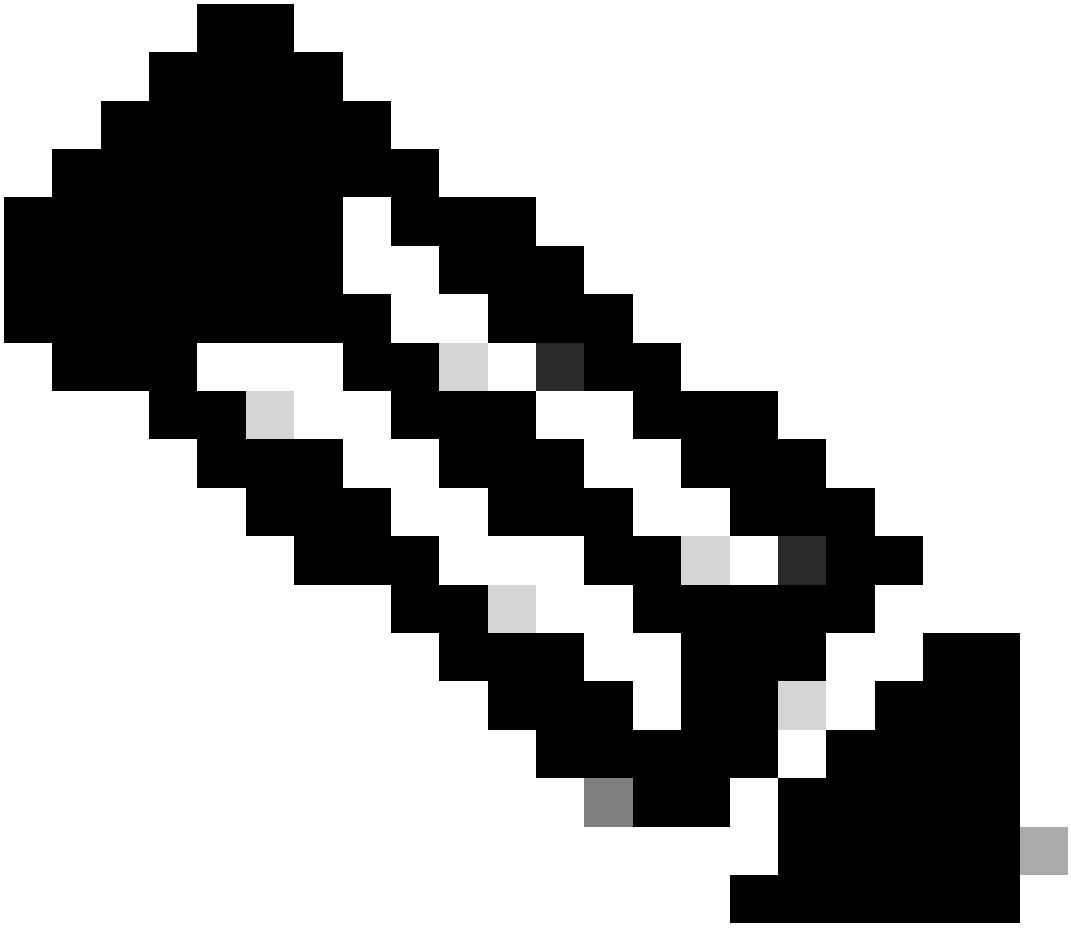
Per abilitare la traccia dei pacchetti con FIA, è necessario applicare questi dati di configurazione:

<#root>

ASR1000#

debug platform packet-trace packet 16 fia-trace

Visualizzazione dei risultati della traccia del pacchetto



Nota: questa sezione presuppone che la traccia FIA sia abilitata. Inoltre, quando si aggiungono o si modificano i comandi di traccia del pacchetto corrente, i dettagli di traccia del pacchetto nel buffer vengono cancellati, quindi è necessario inviare di nuovo del traffico per poterlo tracciare.

Inviare cinque pacchetti ICMP da 172.16.10.2 a 172.16.20.2 dopo aver immesso il comando utilizzato per abilitare la traccia FIA, come descritto nella sezione precedente.

<#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#
```

Controllare la FIA associata a un'interfaccia

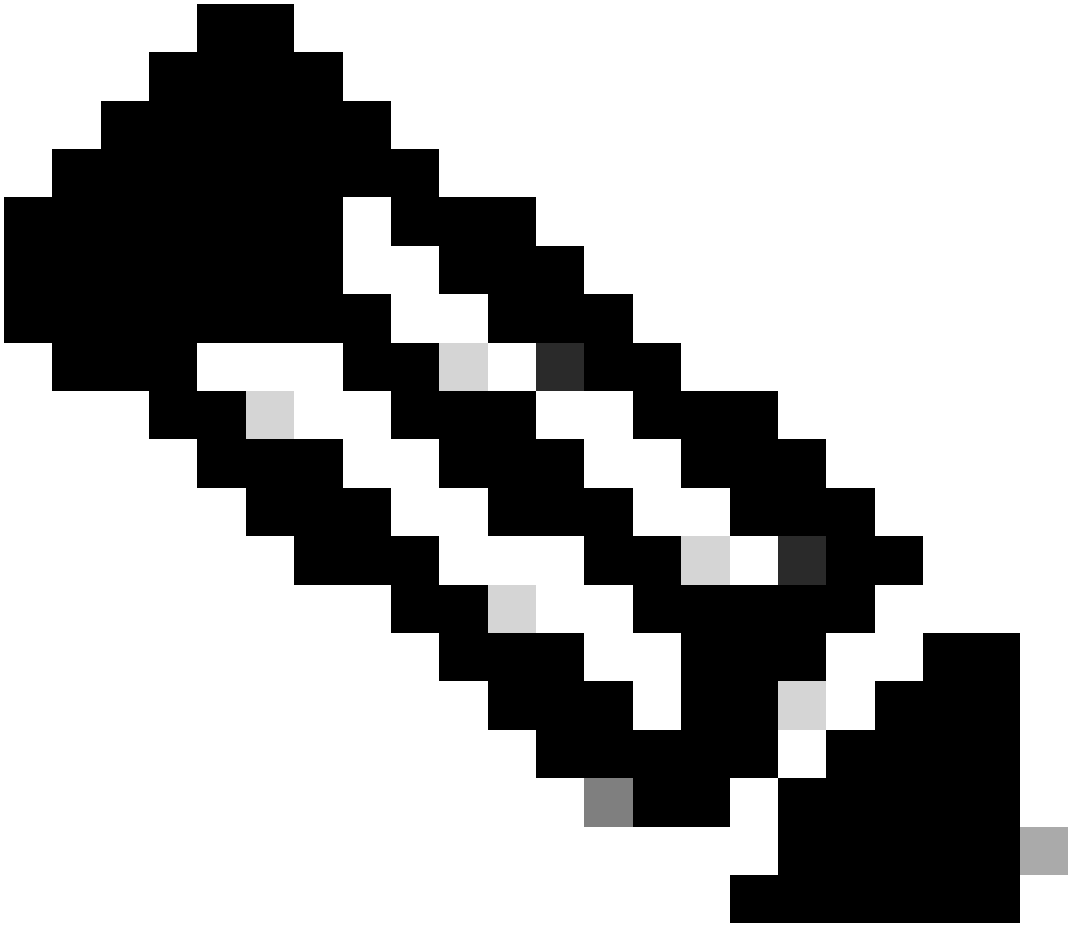
Quando si attivano i debug condizionali della piattaforma, il debug condizionale viene aggiunto alla FIA come funzionalità. In base all'ordine delle funzionalità di elaborazione sull'interfaccia, il filtro condizionale deve essere impostato di conseguenza, ad esempio se l'indirizzo precedente o successivo al NAT deve essere utilizzato nel filtro condizionale.

Questo output mostra l'ordine delle funzionalità nella FIA per il debug condizionale della piattaforma abilitato nella direzione in entrata:

<#root>

```
ASR1000#

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


 General interface information
 Interface Name: GigabitEthernet0/0/1
 Interface state: VALID
 Platform interface handle: 10
 QFP interface handle: 8
 Rx uidb: 1021
 Tx uidb: 131064
 Channel: 16
 Interface Relationships

 BGPPA/QPPB interface configuration information
 Ingress: BGPPA/QPPB not configured. flags: 0000
 Egress : BGPPA not configured. flags: 0000

 ipv4_input enabled.
 ipv4_output enabled.
 layer2_input enabled.
 layer2_output enabled.
 ess_ac_input enabled.

 Features Bound to Interface:
 2 GIC FIA state
 48 PUNT INJECT DB
 39 SPA/Marmot server
 40 ethernet
 1 IFM
 31 icmp_svr
 33 ipfrag_svr
 34 ipreass_svr
 36 ipvfr_svr
 37 ipv6vfr_svr
 12 CPP IPSEC
 Protocol 0 - ipv4_input
 FIA handle - CP:0x108d99cc  DP:0x8070f400
 IPV4_INPUT_DST_LOOKUP_ISSUE (M)
 IPV4_INPUT_ARL_SANITY (M)


  CBUG_INPUT_FIA
```

```
 DEBUG_COND_INPUT_PKT


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

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

ASR1000#
```



Nota: CBUG_INPUT_FIA e DEBUG_COND_INPUT_PKT corrispondono alle funzionalità di debug condizionale configurate sul router.

Scarica i pacchetti tracciati

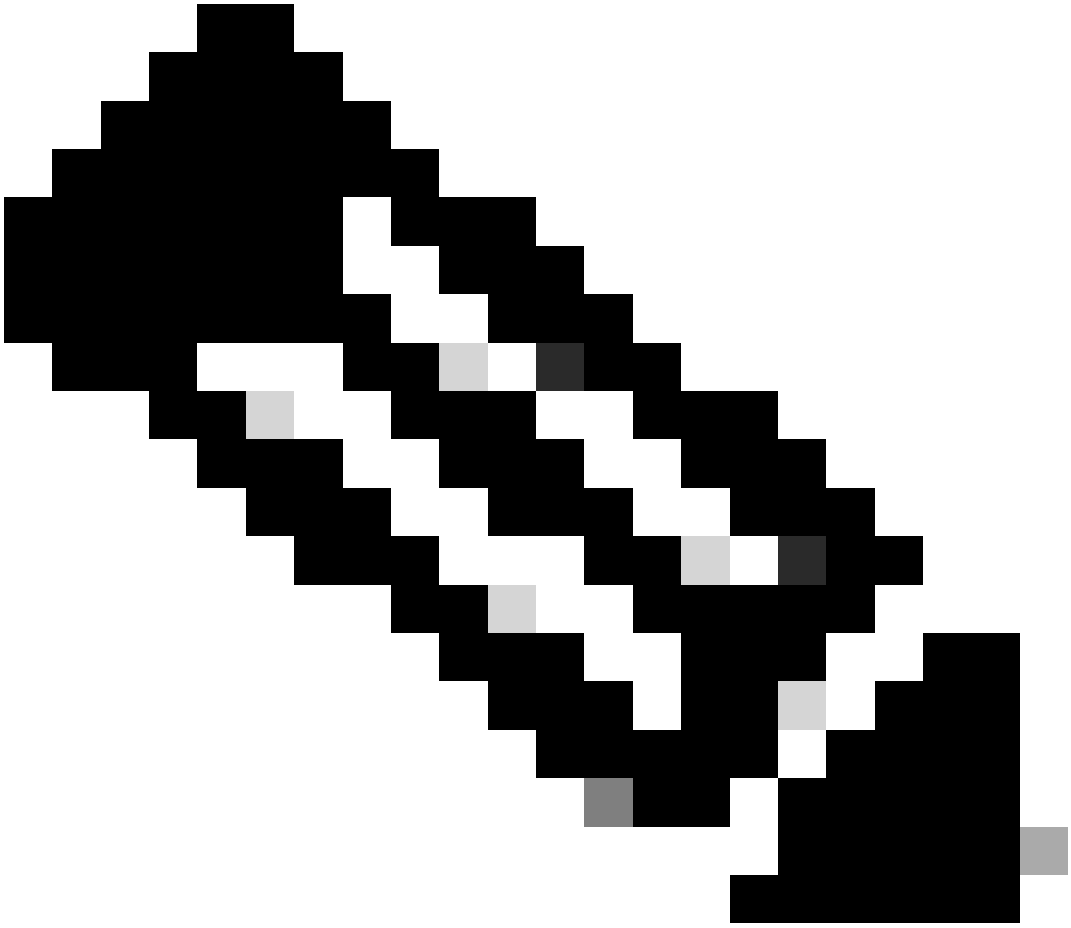
Come descritto in questa sezione, è possibile copiare ed eseguire il dump dei pacchetti man mano che vengono tracciati. Nell'esempio viene mostrato come copiare un massimo di 2.048 byte dei pacchetti in direzione di entrata (da 172.16.10.2 a 172.16.20.2).

Di seguito è riportato il comando aggiuntivo necessario:

<#root>

ASR1000#

debug platform packet-trace copy packet input size 2048



Nota: le dimensioni del pacchetto copiato sono comprese tra 16 e 2.048 byte.

Immettere questo comando per eseguire il dump dei pacchetti copiati:

<#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#
```

Rilascia traccia

Drop trace è disponibile nel software Cisco IOS-XE versione 3.11 e successive. Abilita la traccia dei pacchetti solo per i pacchetti ignorati. Ecco alcune caratteristiche principali:

- Facoltativamente, consente di specificare la conservazione dei pacchetti per un codice a discesa specifico.
- Può essere utilizzato senza condizioni globali o di interfaccia per acquisire gli eventi di rilascio.
- L'acquisizione di un evento di rilascio indica che viene tracciata solo la perdita stessa, non la durata del pacchetto. Tuttavia, consente ancora di acquisire dati di riepilogo, dati di tupla e il pacchetto per migliorare le condizioni o fornire indicazioni per il passaggio successivo del debug.

Di seguito è riportata la sintassi del comando che viene usata per abilitare le tracce dei pacchetti di tipo drop:

<#root>

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

Il codice di rilascio è lo stesso dell'ID di rilascio, come riportato nell'output del 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
```

Scenario di esempio per la traccia di rilascio

Applicare questo ACL sull'interfaccia Gig 0/0/0 di ASR1K per interrompere il traffico tra le versioni 172.16.10.2 e 172.16.20.2:

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

Con l'ACL attivo, che scarta il traffico dall'host locale all'host remoto, applicare la seguente configurazione di 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
```

Inviare cinque pacchetti di richiesta ICMP da 172.16.10.2 a 172.16.20.2. Il comando drop trace acquisisce i pacchetti scartati dall'ACL, come mostrato:

<#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#
```

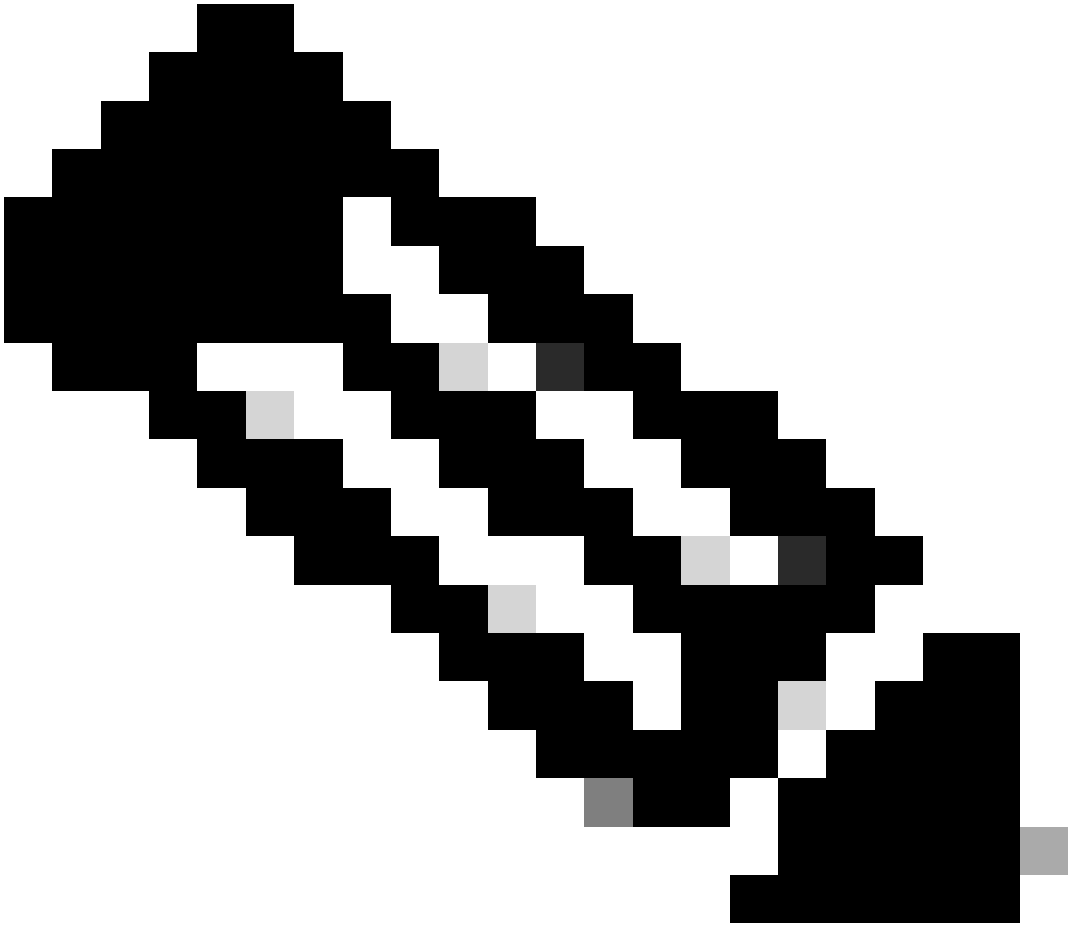
show platform packet-trace packet 0

```
 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#
```

Iniezione e punzonatura

La funzione inject e punt packet trace è stata aggiunta nel software Cisco IOS-XE versione 3.12 e successive per tracciare i pacchetti punt (pacchetti che vengono ricevuti sull'FP e che vengono puntati sul control plane) e inject (pacchetti che vengono iniettati sull'FP dal control plane).



Nota: la traccia della punta può funzionare senza le condizioni globali o di interfaccia, proprio come una traccia di rilascio. Affinché una traccia di inserimento funzioni, è tuttavia necessario definire le condizioni.

Di seguito è riportato un esempio di punt e inject packet trace quando si esegue il ping tra l'ASR1K e un router adiacente:

<#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#
```

A questo punto è possibile verificare i risultati punt e nject trace rrestituiti:

<#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)
```

Miglioramento Packet Trace con IOSd e LFTS Punt/Inject Trace e UDF Corrispondenza (novità della versione 17.3.1)

La funzione di traccia dei pacchetti è stata ulteriormente migliorata per fornire informazioni di traccia aggiuntive per i pacchetti originati o destinati a IOSd o ad altri processi BinOS in Cisco IOS-XE versione 17.3.1.

IOSd Drop Tracing

Con questo miglioramento, il rilevamento dei pacchetti viene esteso a IOSd e può fornire informazioni su qualsiasi perdita di pacchetti all'interno di IOSd, generalmente segnalata nell'output ***show ip traffic***. Non è necessaria alcuna configurazione aggiuntiva per abilitare la traccia di rilascio di IOSd. Di seguito è riportato un esempio di pacchetto UDP scartato da IOSd a causa di un errore di checksum errato:

```
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)
```

Traccia percorso di uscita IOSd

Packet trace è stato migliorato per mostrare le informazioni di trace del percorso e di elaborazione del protocollo quando il pacchetto proviene da IOSd e viene inviato in uscita verso la rete. Non è necessaria alcuna configurazione aggiuntiva per acquisire le informazioni di traccia del percorso di uscita di IOSd. Di seguito è riportato un esempio di traccia del percorso di uscita per un pacchetto SSH in uscita dal router:

```
<#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
```

Traccia pacchetti a sinistra

LFTS (Linux Forwarding Transport Service) è un meccanismo di trasporto per inoltrare i pacchetti puniti dal CPP in applicazioni diverse da IOSd. Il miglioramento della traccia dei pacchetti LFTS ha aggiunto informazioni di traccia per tali pacchetti nell'output di traccia del percorso. Non è necessaria alcuna configurazione aggiuntiva per ottenere le informazioni di traccia LFTS. Di seguito è riportato un esempio di output del comando LFTS tracing per il pacchetto punted all'applicazione 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
```

Corrispondenza pattern di traccia pacchetto in base al filtro definito dall'utente (solo piattaforma ASR1000)

In Cisco IOS-XE versione 17.3.1, alle famiglie di prodotti ASR1000 è stato aggiunto un nuovo meccanismo di corrispondenza del pacchetto che consente di trovare una corrispondenza nel campo arbitrario di un pacchetto basato sull'infrastruttura UDF (User Defined Filter). Ciò consente una corrispondenza flessibile dei pacchetti basata su campi che non fanno parte della struttura standard dell'intestazione L2/L3/L4. Nell'esempio seguente viene mostrata una definizione UDF che corrisponde a 2 byte del pattern definito dall'utente di 0x4D2 e che inizia da un offset di 26 byte dall'intestazione del protocollo esterno L3.

```
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
```

Esempi di traccia dei pacchetti

In questa sezione vengono forniti alcuni esempi in cui la funzione di traccia dei pacchetti è utile per la risoluzione dei problemi.

Esempio di traccia del pacchetto - NAT

Nell'esempio, un'interfaccia di origine Network Address Translation (NAT) viene configurata sull'interfaccia WAN di un ASR1K (Gig0/0/0) per la subnet locale (172.16.10.0/24).

Di seguito vengono riportate le condizioni della piattaforma e la configurazione della traccia dei pacchetti utilizzata per tracciare il traffico tra le versioni 172.16.10.2 e 172.16.20.2, che viene convertito (NAT) sull'interfaccia 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 si inviano cinque pacchetti ICMP da 172.16.10.2 a 172.16.20.2 con una configurazione NAT di origine interfaccia, i risultati della traccia del pacchetto sono i seguenti:

```
<#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#
```

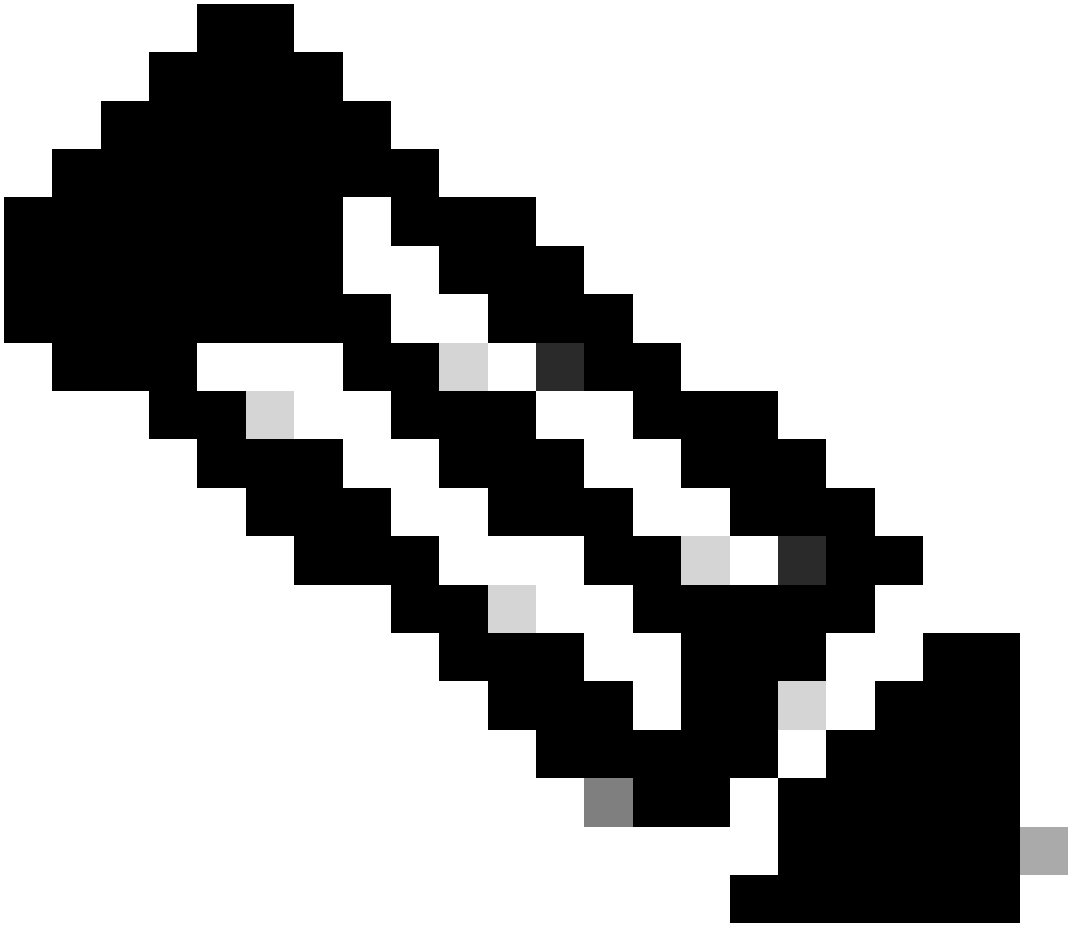
Esempio di traccia del pacchetto - VPN

In questo esempio, viene usato un tunnel VPN da sito a sito tra l'ASR1K e il router Cisco IOS per proteggere il traffico che scorre tra la versione 172.16.10.0/24 e la versione 172.16.20.0/24 (subnet locali e remote).

Di seguito vengono riportate le condizioni della piattaforma e la configurazione della traccia dei pacchetti utilizzata per tracciare il traffico VPN che passa da 172.16.10.2 a 172.16.20.2 sull'interfaccia 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 si inviano cinque pacchetti ICMP da 172.16.10.2 a 172.16.20.2, criptati dal tunnel VPN tra ASR1K e il router Cisco IOS in questo esempio, questi sono gli output di traccia del pacchetto:



Nota: le tracce del pacchetto mostrano l'handle dell'associazione di sicurezza (SA) QFP nella traccia utilizzata per crittografare il pacchetto, utile quando si risolvono i problemi della VPN IPsec per verificare che per la crittografia venga utilizzata l'associazione di sicurezza corretta.

<#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#
```

Conseguenze sulle prestazioni

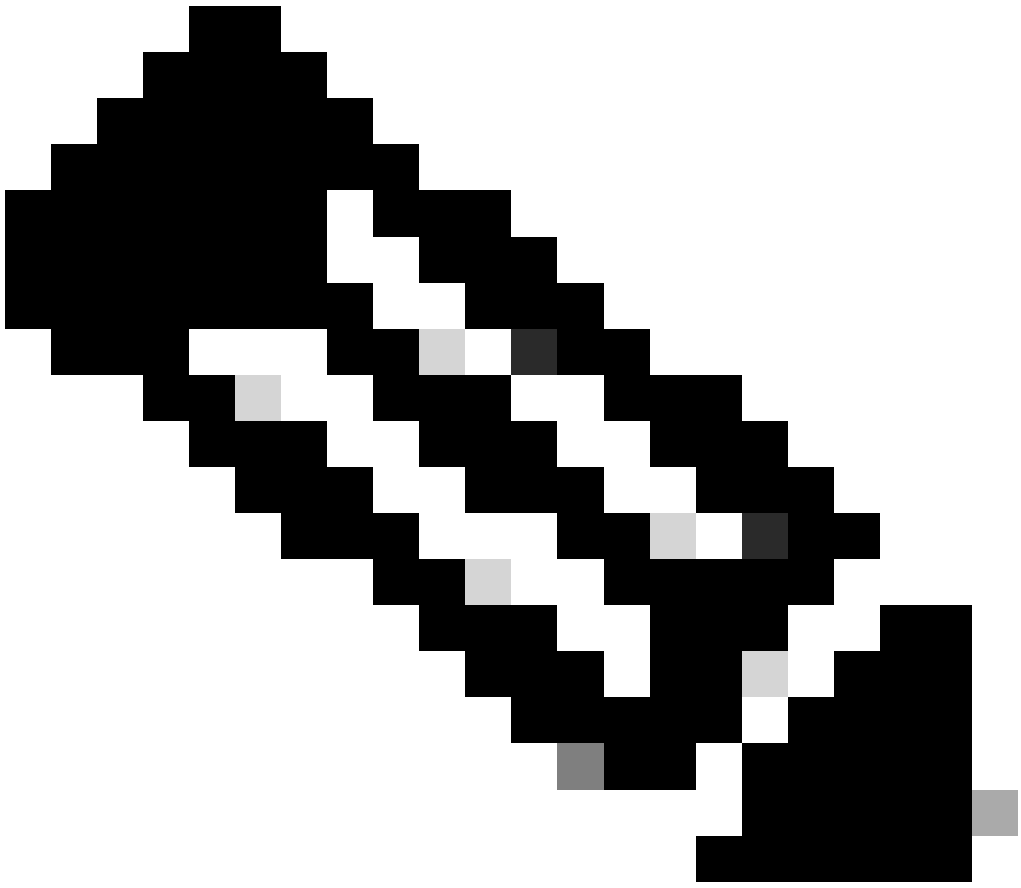
I buffer di traccia dei pacchetti utilizzano la memoria DRAM QFP, quindi è importante tenere presente la quantità di memoria richiesta da una configurazione e la quantità di memoria disponibile.

L'impatto sulle prestazioni varia a seconda delle opzioni di traccia dei pacchetti abilitate. La traccia dei pacchetti influisce solo sulle prestazioni di inoltro dei pacchetti tracciati, ad esempio i pacchetti che soddisfano le condizioni configurate dall'utente. Maggiore è il livello di granularità e di dettaglio delle informazioni che si configura per l'acquisizione della traccia del pacchetto, maggiore sarà l'impatto sulle risorse.

Come per la risoluzione dei problemi, è consigliabile adottare un approccio iterativo e abilitare le opzioni di traccia più dettagliate solo quando la situazione di debug lo richiede.

L'utilizzo di QFP DRAM può essere stimato con la seguente formula:

memoria necessaria = (sovraccarico stato) + numero di pkt * (dimensione riepilogo + dimensione dati percorso + dimensione copia)



Nota: dove il **sovraccarico dello stato** e la **dimensione del riepilogo** sono fissati rispettivamente a 2 KB e 128 MB, la **dimensione**

---

dei dati del percorso e la **dimensione della copia** sono configurabili dall'utente.

Informazioni correlate

- **Guida alla configurazione del software dei router per Cisco ASR serie 1000 Aggregation - Packet Trace**
- **Perdite di pacchetti sui Cisco ASR serie 1000 Service Router**
- **Supporto tecnico Cisco e download**

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).