Procedura SPAN-to-CPU Nexus 9000 Cloud Scale ASIC NX-OS

Sommario

Introduzione

Questo documento descrive i passaggi utilizzati per eseguire un'acquisizione di pacchetti da SPAN (Switched Port Analyzer) a CPU su una serie di moduli Cisco Nexus 9000 Cloud Scale ASIC. Questo documento descrive anche gli avvertimenti comuni riscontrati quando si usa l'acquisizione di pacchetti da SPAN a CPU per risolvere i problemi di flusso dei pacchetti attraverso uno switch Cisco Nexus serie 9000 Cloud Scale.

Premesse

L'acquisizione di pacchetti da SPAN a CPU consente agli amministratori di rete di convalidare in modo rapido e semplice se pacchetti specifici entrano ed escono da uno switch Cisco Nexus serie 9000 Cloud Scale. Analogamente a una normale sessione SPAN o ERSPAN (Encapsulated Remote SPAN), una sessione di monitoraggio SPAN-CPU implica la definizione di una o più interfacce di origine e direzioni del traffico. Tutto il traffico che corrisponde alla direzione (TX, RX o entrambe) definita su un'interfaccia di origine viene replicato sul piano di controllo del dispositivo Cisco Nexus 9000. Questo traffico replicato può essere filtrato e analizzato usando l'utilità di acquisizione pacchetti del control plane Ethanalyzer o salvato su un dispositivo di archiviazione

locale per una revisione successiva.

Questa funzionalità è destinata all'utilizzo temporaneo durante la risoluzione dei problemi di flusso dei pacchetti attraverso gli switch Cisco Nexus serie 9000. Cisco consiglia vivamente di arrestare o rimuovere le sessioni di monitoraggio da SPAN a CPU quando non vengono usate attivamente per la risoluzione di un problema di flusso di pacchetti. In caso contrario, si potrebbe verificare un calo delle prestazioni per il traffico replicato nella rete e un maggiore utilizzo della CPU degli switch Cisco Nexus serie 9000.

Dispositivi interessati

La procedura illustrata in questo documento è applicabile solo a questo hardware:

- **Nexus 9200/9300 Fixed Switch** N9K-C92160YC-XN9K-C92300YCN9K-C92304QCN9K-C92348GC-XN9K-C9236CN9K-C9272QN9K-C932CN9K-C9364CN9K-C93108TC-EXN9K-C93108TC-EX-24N9K-C93180LC-EXN9K-C93180YC-EXN9K-C93180YC-EX-24N9K-C93108TC-FXN9K-C93108TC-FX-24N9K-C93180YC-FXN9K-C93180YC-FX-24N9K-C9348GC-FXPN9K-C93240YC-FX2N9K-C93216TC-FX2N9K-C9336C-FX2N9K-C9336C-FX2-EN9K-C93360YC-FX2N9K-C93180YC-FX3N9K-C93108TC-FX3PN9K-C93180YC-FX3SN9K-C9316D-GXN9K-C93600CD-GXN9K-C9364C-GXN9K-C9364D-GX2AN9K-C932D-GX2B
- **Schede di linea per switch modulari Nexus 9500** N9K-X97160YC-EXN9K-X9732C-EXN9K-X9736C-EXN9K-X97284YC-FXN9K-X9732C-FXN9K-X9788TC-FXN9K-X9716D-GX

Prerequisiti

Requisiti

Cisco consiglia di comprendere le nozioni di base della funzionalità Ethernet Switched Port Analyzer (SPAN) sugli switch Cisco Nexus serie 9000. Per informazioni su questa funzione, consultare i seguenti documenti:

- Guida alla configurazione di Cisco Nexus serie 9000 NX-OS System Management, versione 9.3(x)
- Guida alla configurazione di Cisco Nexus serie 9000 NX-OS System Management, versione 9.2(x)
- Guida alla configurazione di Cisco Nexus serie 9000 NX-OS System Management, versione 7.0(3)I7(x)

Componenti usati

Per la stesura del documento, sono stati usati switch Cisco Nexus serie 9000 con Cloud Scale ASIC con software NX-OS versione 9.3(3).

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.

Avvertenze e limitazioni

Le sessioni di monitoraggio SPAN-CPU presentano alcune avvertenze e limitazioni di cui tenere conto quando si risolvono i flussi di pacchetti. In questo documento vengono illustrati alcuni avvertimenti di uso comune. Per un elenco completo delle linee guida e delle limitazioni, consultare i seguenti documenti:

- Guida alla configurazione di Cisco Nexus serie 9000 NX-OS System Management, versione 9.3(x)
- Guida alla configurazione di Cisco Nexus serie 9000 NX-OS System Management, versione 9.2(x)
- Guida alla configurazione di Cisco Nexus serie 9000 NX-OS System Management, versione 7.0(3)I7(x)

50 kbps Limitatore di velocità hardware predefinito

Per impostazione predefinita, gli switch Cisco Nexus serie 9000 limitano a 50 kbps la velocità del traffico replicato sul control plane tramite una sessione di monitoraggio SPAN-CPU. Questa limitazione della velocità viene eseguita sul motore di inoltro/ASIC Cloud Scale ed è un meccanismo di autoprotezione per garantire che il control plane del dispositivo non sia sovraccaricato dal traffico replicato.

Il comando **show hardware rate-limiter span** può essere usato per visualizzare l'impostazione corrente del limitatore di velocità della sessione di monitoraggio SPAN-CPU.

```
N9K# show hardware rate-limiter span Units for Config: kilo bits per second Allowed, Dropped &
Total: aggregated bytes since last clear counters Module: 1 R-L Class Config Allowed Dropped
Total +----------------+----------+--------------------+--------------------+------------------
-+  span 50  0 0 0
```

Se il traffico replicato viene eliminato dal limitatore di velocità hardware, la colonna Eliminato sarà un valore diverso da zero, come mostrato nell'output seguente:

```
N9K# show hardware rate-limiter span Units for Config: kilo bits per second Allowed, Dropped &
Total: aggregated bytes since last clear counters Module: 1 R-L Class Config Allowed Dropped
Total +----------------+----------+--------------------+--------------------+------------------
-+  span 50 0 499136  499136
```

Il limitatore di velocità dell'hardware della sessione di monitoraggio SPAN-CPU può essere modificato con il comando di configurazione globale **hardware rate-limiter span {kbps}**, come mostrato nell'output seguente.

```
N9K# configure terminal Enter configuration commands, one per line. End with CNTL/Z. N9K-
1(config)# hardware rate-limiter span 250 N9K-1(config)# end N9K# show running-config | inc
rate-limiter hardware rate-limiter span 250 N9K# show hardware rate-limiter span Units for
Config: kilo bits per second Allowed, Dropped & Total: aggregated bytes since last clear
counters Module: 1 R-L Class Config Allowed Dropped Total +----------------+----------+---------
----------+--------------------+--------------------+  span 250  0 0 0
```

> **Attenzione:** Cisco sconsiglia di modificare il limitatore di velocità dell'hardware della sessione SPAN-CPU monitor rispetto al valore predefinito di 50 kbps, a meno che non sia stato esplicitamente richiesto da Cisco TAC. Aumentare questo limitatore di velocità a un valore

elevato può causare un maggiore utilizzo della CPU e l'instabilità del control plane sugli switch Cisco Nexus serie 9000, con un conseguente impatto significativo sul traffico di produzione.

Il contatore consentito per il limite di velocità hardware SPAN-CPU non è supportato

L'output del comando **show hardware rate-limiter span** contiene un contatore Allowed. Su altri limitatori di velocità hardware, questo contatore indica quanti byte passano correttamente attraverso il limitatore di velocità hardware. Tuttavia, il contatore Consentito per il limitatore di velocità hardware SPAN-CPU non aumenta a causa di una limitazione software. Di seguito è riportato un esempio:

```
N9K# show hardware rate-limiter span

Units for Config: kilo bits per second
Allowed, Dropped & Total: aggregated bytes since last clear counters


Module: 1
R-L Class Config Allowed              Dropped                Total
+----------------+----------+--------------------+--------------------+--------------------+
span 50 0               499136               499136
```

Questa limitazione riguarda tutte le versioni del software NX-OS ed è documentata tramite CSCva37512.

Per determinare la quantità di traffico replicata sul control plane di un dispositivo Nexus 9000 configurato con una sessione di monitoraggio SPAN-CPU attiva, usare il comando **show system internal access-list tcam ingress region span**. Di seguito è riportato un esempio dell'output filtrato del comando summenzionato che mostra i contatori di pacchetti e byte rilevanti.

```
N9K# show system internal access-list tcam ingress region span | include pkts:
<snip>
pkts: 56582127, bytes: 4119668263
```

I pacchetti generati dal Control Plane non vengono visualizzati nelle sessioni di monitoraggio SPAN-CPU TX

I pacchetti creati dal control plane e trasmessi da un'interfaccia di origine per una sessione di monitoraggio SPAN-CPU non verranno acquisiti dalla sessione di monitoraggio SPAN-CPU. Questi pacchetti usciranno dall'interfaccia correttamente, ma non possono essere acquisiti tramite una sessione di monitoraggio SPAN-CPU sullo stesso dispositivo su cui sono stati generati.

Ad esempio, si consideri un dispositivo Cisco Nexus serie 9000 dove Ethernet1/1 è un'interfaccia L3/1 connessa a un altro router. Il processo OSPF 1 è attivato su Ethernet1/1, l'unica interfaccia attivata da OSPF sul dispositivo Cisco Nexus 9000.

```
N9K# show running-config ospf  !Command: show running-config ospf !Running configuration last
done at: Wed Feb 26 16:16:30 2020 !Time: Wed Feb 26 16:16:37 2020 version 9.3(3) Bios:version
05.39 feature ospf router ospf 1 interface Ethernet1/1 ip router ospf 1 area 0.0.0.0 N9K# show
ip ospf interface brief  OSPF Process ID 1 VRF default Total number of interface: 1 Interface ID
Area Cost State Neighbors Status Eth1/1 1 0.0.0.0 4 DR 0 up
```

L'utilità di acquisizione pacchetti Ethernet Control Plane mostra che i messaggi OSPF Hello vengono generati dal control plane del dispositivo una volta ogni 10 secondi.

```
N9K# ethanalyzer local interface inband display-filter ospf limit-captured-frames 0 Capturing on
inband 2020-02-26 16:19:13.041255 192.168.1.1 -> 224.0.0.5 OSPF Hello Packet  2020-02-26
16:19:22.334692 192.168.1.1 -> 224.0.0.5 OSPF Hello Packet  2020-02-26 16:19:31.568034
192.168.1.1 -> 224.0.0.5 OSPF Hello Packet  ^C 3 packets captured
```

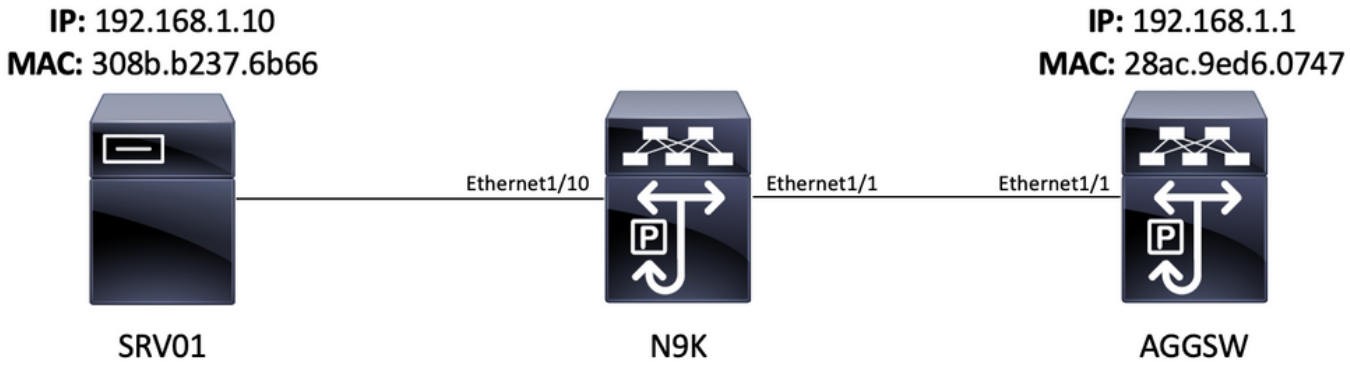
Tuttavia, un SPAN in uscita/TX sulla CPU dell'interfaccia Ethernet1/1 non visualizza questi pacchetti Open Shortest Path First (OSPF) Hello trasmessi su questa interfaccia dopo 60 secondi.

```
N9K# show running-config monitor  !Command: show running-configmonitor !Running configuration
last done at: Wed Feb 26 16:20:48 2020 !Time: Wed Feb 26 16:20:51 2020 version 9.3(3)
Bios:version 05.39 monitor session 1 source interface Ethernet1/1 tx destination interface sup-
eth0 no shut N9K# show monitor  Session State Reason Description ------- ----------- -----------
----------- ------------------------------- 1 up The session is up N9K# ethanalyzer local
interface inband mirror display-filter ospf autostop duration 60 Capturing on inband 0 packets
captured
```

Per verificare se i pacchetti generati dal control plane di un dispositivo Cisco Nexus 9000 vengono trasmessi da un'interfaccia specifica, Cisco consiglia di utilizzare un'utilità di acquisizione pacchetti sul dispositivo remoto connesso all'interfaccia.

Procedura SPAN-to-CPU Cisco Nexus 9000 Cloud Scale

Considerare la topologia seguente:



Un pacchetto Internet Control Message Protocol (ICMP) proveniente dal server SRV01 nella VLAN 10 (192.168.10.10) è destinato al gateway VLAN 10 192.168.10.1. Verrà utilizzata una sessione di monitoraggio SPAN-CPU per confermare che il pacchetto ICMP attraversa il dispositivo N9K (un Cisco Nexus 93180YC-EX con software NX-OS versione 9.3(3)), che agisce come switch di layer 2 che si connette da SRV01 a AGSW nella VLAN 10.

Passaggio 1. Confermare le risorse sufficienti per la nuova sessione SPAN

Gli switch Cisco Nexus serie 9000 con Cloud Scale ASIC con software NX-OS supportano un massimo di quattro sessioni SPAN o ERSPAN attive per motore di inoltro/ASIC. Inoltre, se le prime tre sessioni SPAN o ERSPAN sono configurate con interfacce di origine bidirezionali (TX e RX), l'interfaccia di origine della quarta sessione SPAN o ERSPAN deve essere una sorgente in ingresso/RX.

Prima di configurare una sessione di monitoraggio SPAN-CPU, verificare la quantità di altre

sessioni SPAN o ERSPAN attualmente configurate sul dispositivo. A tale scopo, è possibile usare i comandi **show running-config monitor** e **show monitor**. L'esempio seguente mostra l'output di entrambi i comandi quando sul dispositivo non sono configurate altre sessioni SPAN o ERSPAN.

```
N9K# show running-config monitor  !Command: show running-configmonitor !Running configuration
last done at: Tue Feb 25 20:34:04 2020 !Time: Tue Feb 25 20:34:06 2020 version 9.3(3)
Bios:version 07.66 N9K# show monitor  Note: No sessions configured
```

> **Nota:** Per ulteriori informazioni sul numero massimo di sessioni SPAN/ERSPAN e su altre limitazioni, consultare la Cisco Nexus 9000 NX-OS Verified Scalability Guide for NX-OS Software release 9.3(3).

Passaggio 2. Configurare la sessione di monitoraggio SPAN-CPU

L'elemento di configurazione chiave che definisce una sessione di monitoraggio SPAN-CPU è un'interfaccia di destinazione di "sup-eth0", che è l'interfaccia in banda del supervisore. L'esempio seguente mostra la configurazione di una sessione di monitoraggio SPAN-CPU in cui i pacchetti in entrata/RX di Ethernet 1/10 vengono replicati sul supervisore dello switch Cisco Nexus serie 9000.

```
N9K# configure terminal Enter configuration commands, one per line. End with CNTL/Z. N9K-
1(config)# monitor session 1 N9K-1(config-monitor)# source interface Ethernet1/10 rx N9K-
1(config-monitor)# destination interface sup-eth0 N9K-1(config-monitor)# no shut N9K-1(config-
monitor)# end N9K#
```

Passaggio 3. Verificare che la sessione di monitoraggio SPAN-CPU sia attiva

Per verificare che la sessione di monitoraggio SPAN-CPU sia configurata e operativa, usare i comandi **show running-config monitor** e **show monitor**. La configurazione della sessione di monitoraggio SPAN-CPU può essere verificata tramite l'output del comando **show running-config monitor**, come mostrato nell'esempio che segue.

```
N9K# show running-config monitor  !Command: show running-configmonitor !Running configuration
last done at: Tue Feb 25 20:47:50 2020 !Time: Tue Feb 25 20:49:35 2020 version 9.3(3)
Bios:version 07.66 monitor session 1 source interface Ethernet1/10 rx destination interface sup-
eth0 no shut
```

Lo stato operativo della sessione di monitoraggio SPAN-CPU può essere verificato con l'output del comando **show monitor**. L'output deve riportare che lo stato della sessione del monitor SPAN-CPU è "attivo" con il motivo "La sessione è attiva", come mostrato nell'esempio seguente.

```
N9K# show monitor  Session State Reason Description - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - 1 up The session is up
```

Passaggio 4. Visualizzare i pacchetti replicati nel Control Plane

L'utility di acquisizione dei pacchetti del control plane Ethernet può essere utilizzata per visualizzare il traffico replicato sul control plane del dispositivo Cisco Nexus 9000. La parola chiave **mirror** nel comando Ethanalyzer filtra il traffico in modo che venga mostrato solo il traffico replicato da una sessione di monitoraggio SPAN-CPU. I filtri di acquisizione e visualizzazione di Ethanalyzer possono essere utilizzati per limitare ulteriormente il traffico visualizzato. Ulteriori informazioni sui filtri di acquisizione e visualizzazione di Ethanalyzer sono disponibili nella guida

alla risoluzione dei problemi di Ethanalyzer su Nexus 7000. Questo documento è stato redatto per la piattaforma Cisco Nexus 7000, ma è applicabile anche per la piattaforma Cisco Nexus 9000.

Di seguito è riportato un esempio dell'uso dell'utility di acquisizione dei pacchetti del control plane Ethanalyzer per filtrare il traffico replicato da una sessione di monitoraggio SPAN-CPU. Si noti che vengono usate la parola chiave **mirror** e un filtro di visualizzazione che definisce i pacchetti ICMP provenienti da o destinati a 192.168.10.10 (l'indirizzo IP di SRV01 nella topologia sopra menzionata).

```
N9K# ethanalyzer local interface inband mirror display-filter "icmp && ip.addr==192.168.10.10"
limit-captured-frames 0
Capturing on inband
2020-02-25 21:01:07.592838 192.168.10.10 -> 192.168.10.1 ICMP Echo (ping) request 2020-02-25
21:01:08.046682 192.168.10.10 -> 192.168.10.1 ICMP Echo (ping) request 2020-02-25
21:01:08.047720 192.168.10.10 -> 192.168.10.1 ICMP Echo (ping) request 2020-02-25
21:01:08.527646 192.168.10.10 -> 192.168.10.1 ICMP Echo (ping) request 2020-02-25
21:01:08.528659 192.168.10.10 -> 192.168.10.1 ICMP Echo (ping) request 2020-02-25
21:01:08.529500 192.168.10.10 -> 192.168.10.1 ICMP Echo (ping) request 2020-02-25
21:01:08.530082 192.168.10.10 -> 192.168.10.1 ICMP Echo (ping) request 2020-02-25
21:01:08.530659 192.168.10.10 -> 192.168.10.1 ICMP Echo (ping) request 2020-02-25
21:01:08.531244 192.168.10.10 -> 192.168.10.1 ICMP Echo (ping) request ^C 9 packets captured
```

> **Nota:** Usare la combinazione di tasti Control-C per uscire dall'utilità di acquisizione pacchetti del control plane dell'etanalizzatore.

Èpossibile visualizzare informazioni dettagliate su questo traffico includendo la parola chiave **detail** nel comando Ethanalyzer. Di seguito è riportato un esempio di ciò per un pacchetto di richiesta echo ICMP.

```
N9K# ethanalyzer local interface inband mirror display-filter "icmp && ip.addr==192.168.10.10"
limit-captured-frames 0 detail
Capturing on inband Frame 2 (114 bytes on wire, 114 bytes captured) Arrival Time: Feb 25, 2020
21:56:40.497381000 [Time delta from previous captured frame: 1.874113000 seconds] [Time delta
from previous displayed frame: 1.874113000 seconds] [Time since reference or first frame:
1.874113000 seconds] Frame Number: 2 Frame Length: 114 bytes Capture Length: 114 bytes [Frame is
marked: False] [Protocols in frame: eth:ip:icmp:data] Ethernet II, Src: 30:8b:b2:37:6b:66
(30:8b:b2:37:6b:66), Dst: 28:ac:9e:d6:07:47 (28:ac:9e:d6:07:47) Destination: 28:ac:9e:d6:07:47
(28:ac:9e:d6:07:47) Address: 28:ac:9e:d6:07:47 (28:ac:9e:d6:07:47) .... ...0 .... .... .... ....
= IG bit: Individual address (unicast) .... ..0. .... .... .... .... = LG bit: Globally unique
address (factory default) Source: 30:8b:b2:37:6b:66 (30:8b:b2:37:6b:66) Address:
30:8b:b2:37:6b:66 (30:8b:b2:37:6b:66) .... ...0 .... .... .... .... = IG bit: Individual address
(unicast) .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default) Type
: IP (0x0800) Internet Protocol, Src: 192.168.10.10 (192.168.10.10), Dst: 192.168.10.1
(192.168.10.1) Version : 4 Header length: 20 bytes Differentiated Services Field: 0x00 (DSCP
0x00: Default; ECN: 0x00) 0000 00.. = Differentiated Services Codepoint: Default (0x00) ....
..0. = ECN-Capable Transport (ECT): 0 .... ...0 = ECN-CE: 0 Total Length: 100 Identification:
0x00e1 (225) Flags: 0x00 0.. = Reserved bit: Not Set .0. = Don't fragment: Not Set ..0 = More
fragments: Not Set Fragment offset: 0 Time to live: 254 Protocol: ICMP (0x01) Header checksum :
0x265c [correct] [Good: True] [Bad : False] Source: 192.168.10.10 (192.168.10.10) Destination:
192.168.10.1 (192.168.10.1) Internet Control Message Protocol Type : 8 (Echo (ping) request)
Code: 0 () Checksum : 0xf1ed [correct] Identifier: 0x0004 Sequence number: 0 (0x0000) Data (72
bytes) 0000 00 00 00 00 ed 9e 9e b9 ab cd ab cd ab cd ab cd ..... 0010 ab cd ab cd ab
cd ab cd ab cd ab cd ab cd ..... 0020 ab cd ab cd ab cd ab cd ab cd ab cd ab cd
ab cd ..... 0030 ab cd ab cd ab cd ab cd ab cd ab cd ab cd .....
0040 ab cd ab cd ab cd ab cd ..... Data: 00000000ED9E9EB9ABCDABCDABCDABCDABCDABCDABCD...
[Length: 72] ^C 1 packet captured
```

Passaggio 5. Chiusura amministrativa della sessione di monitoraggio SPAN-CPU

Usare il comando **shutdown** configuration nel contesto della sessione di monitoraggio SPAN-CPU per arrestare normalmente la sessione di monitoraggio SPAN-CPU e interrompere la replica del traffico sul control plane del dispositivo Cisco Nexus 9000.

```
N9K# configure terminal Enter configuration commands, one per line. End with CNTL/Z. N9K-
1(config)# monitor session 1 N9K-1(config-monitor)# shut N9K-1(config-monitor)# end N9K#
```

Verificare lo stato operativo della sessione di monitoraggio SPAN-CPU con il comando **show monitor**. Lo stato operativo della sessione di monitoraggio SPAN-CPU deve essere indicato come "inattivo" con il motivo "Amministrazione sessione chiusa", come mostrato nell'esempio seguente:

```
N9K# show monitor  Session State Reason Description - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - 1 down Session admin shut
```

Passaggio 6. Rimozione della configurazione della sessione di monitoraggio SPAN-CPU (facoltativo)

Se lo si desidera, rimuovere la configurazione della sessione di monitoraggio SPAN-CPU con il comando di configurazione **no monitor session {id}**. Di seguito è riportato un esempio.

```
N9K# configure terminal Enter configuration commands, one per line . End with CNTL/Z. N9K-
1(config)# no monitor session 1 N9K-1(config)# end
```

Verificare che la configurazione della sessione di monitoraggio SPAN-CPU sia stata rimossa correttamente con il comando **show running-config monitor**, come mostrato nell'esempio che segue.

```
N9K# show running-config monitor  !Command: show running-configmonitor !Running configuration
last done at: Tue Feb 25 21:46:25 2020 !Time: Tue Feb 25 21:46:29 2020 version 9.3(3)
Bios:version 07.66 N9K#
```

Analisi dei risultati di un'acquisizione di pacchetti da SPAN a CPU

L'esempio di questa procedura mostra che i pacchetti di richiesta echo ICMP provenienti da 192.168.10.10 (SRV01) e destinati a 192.168.10.1 (AGGSW) entrano nell'interfaccia Ethernet1/10 del dispositivo Cisco Nexus 9000 con nome host N9K. Ciò dimostra che SRV01 invia questo traffico dalla scheda di interfaccia di rete. Ciò dimostra anche che il pacchetto di richiesta echo ICMP avanza in misura sufficiente nella pipeline di inoltro di Cisco Cloud Scale ASIC per essere replicato sul control plane del dispositivo.

Tuttavia, questo non prova che il dispositivo Cisco Nexus 9000 inoltri il pacchetto ICMP Echo Request da Ethernet1/1 al software GASW. È necessario eseguire ulteriori procedure di risoluzione dei problemi per verificare se il pacchetto viene inoltrato fuori dalla rete Ethernet1/1 verso il software GASW. In ordine di affidabilità:

1. Se il dispositivo remoto dell'interfaccia in uscita prevista (Ethernet1/1 di N9K nell'esempio) è un dispositivo Cisco Nexus serie 9000 con ASIC a scala cloud, è possibile eseguire una sessione di monitoraggio in entrata/RX SPAN-CPU sul dispositivo remoto (Eth1/1 di AGGSW nell'esempio precedente). Se il dispositivo remoto dell'interfaccia in uscita prevista non è un dispositivo Cisco Nexus serie 9000 con un ASIC a scala cloud, un SPAN, un mirroring della porta o un'altra

acquisizione di pacchetti simile sul dispositivo remoto è equivalente.

2. Eseguire un ELAM in entrata/RX sull'interfaccia in entrata (Ethernet 1/10 di N9K nell'esempio precedente) del dispositivo Cisco Nexus 9000. Per ulteriori informazioni su questa procedura, fare riferimento alla nota tecnica sulla risoluzione dei problemi relativi a Nexus 9000 Cloud Scale ASIC NX-OS ELAM.

3. Eseguire un'operazione SPAN-CPU uscita/TX sull'interfaccia in uscita del dispositivo Cisco Nexus 9000 (Ethernet1/1 di N9K nell'esempio riportato sopra).

Informazioni correlate

- Guida alla risoluzione dei problemi di Cisco Nexus serie 9000 NX-OS, versione 9.3(x)
- Guida alla risoluzione dei problemi di Cisco Nexus serie 9000 NX-OS, versione 9.2(x)
- Guida alla risoluzione dei problemi di Cisco Nexus serie 9000 NX-OS, versione 7.0(3)I7(x)
- Guida alla risoluzione dei problemi di Ethanalyzer su Nexus 7000
- Nexus 9000 Cloud Scale ASIC (Tahoe) NX-OS ELAM