

Nexus 9000 cloudschaal ASIC NX-OS SPAN-to-CPU-procedure

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Toepasselijke hardware](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Voorzorgsmaatregelen en beperkingen](#)

[50 kbps standaard hardwaresnelheidsbeperking](#)

[Beperking aantal SPAN-to-CPU-hardwarevertraging is niet ondersteund](#)

[Packets met besturingsplane worden niet weergegeven in TX SPAN-to-CPU monitorsessies](#)

[Cisco Nexus 9000 cloudschaal SPAN-to-CPU-procedure](#)

[Stap 1. Bevestig voldoende middelen voor de nieuwe SPAN-sessie](#)

[Stap 2. Configuratie van de monitor SPAN-to-CPU](#)

[Stap 3. Controleer of de monitor-sessie SPAN-naar-CPU is omhoog](#)

[Stap 4. Bekijk herhaalde pakketten in het besturingsplane](#)

[Stap 5. Sluit de SPAN-to-CPU-sessie administratief af](#)

[Stap 6. Verwijder de configuratie van de monitor-naar-CPU \(optioneel\)](#)

[De resultaten van een SPAN-to-CPU pakketvastlegging analyseren](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft de stappen die worden gebruikt om een Switched Port Analyzer (SPAN)-to-CPU pakketvastlegging op een reeks Cisco Nexus 9000 Cloud Scale ASIC-modules. Dit document beschrijft ook de gebruikelijke voorbehouden die worden aangetroffen bij het gebruik van een pakketvastlegging met SPAN-naar-CPU's voor het oplossen van problemen door een switch van de Cloud Scale-serie van Cisco Nexus 9000.

Achtergrondinformatie

Met een SPAN-to-CPU pakketvastlegging kunnen netwerkbeheerders snel en eenvoudig valideren of bepaalde pakketten in beslag worden genomen en een Cisco Nexus 9000 Cloud Scale-switch invoeren. Op dezelfde manier als een normale SPAN- of ingekapselde Remote SPAN-sessie (ERSPAN) omvat een SPAN-naar-CPU monitorsessie de definitie van een of meer broninterfaces en verkeersrichtingen. Elk verkeer dat overeenkomt met de richting (TX, RX of beide) die op een broninterface is gedefinieerd, wordt gerepliceerd naar het besturingsplane van het Cisco Nexus 9000-apparaat. Dit gerepliceerde verkeer kan worden gefilterd en geanalyseerd met behulp van het [EtherAnalyzer-besturingsplane voor pakketvastlegging](#) of opgeslagen op een lokaal opslagapparaat om het later te bekijken.

Deze optie is bedoeld voor tijdelijk gebruik bij het oplossen van pakketstromen door Cisco Nexus 9000 Series switches. Cisco raadt sterk aan dat de monitor-sessies SPAN-to-CPU administratief worden afgesloten of verwijderd wanneer ze niet actief worden gebruikt voor het oplossen van een probleem met pakketstromen. Wanneer u dit niet doet, kan dit leiden tot verslechtering van de prestaties voor herhaald verkeer in het netwerk en een verhoogd CPU-gebruik van de Cisco Nexus 9000 Series switch.

Toepasselijke hardware

De procedure die in dit document wordt behandeld, is alleen van toepassing op deze hardware:

- **Nexus 9200/9300 vaste Switches** N9K-C92160YC-XN9K-C92300YCN9K-C92304QCN9K-C92348GC-XN9K-C9236CN9K-C9272QN9K-C9332CN9K-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-C9360D-GXN9K-C9364C-GXN9K-C9364D-GX2AN9K-C9332D-GX2B
- **Nexus 9500 modulaire Switch lijnkaarten** N9K-X97160YC-EXN9K-X9732C-EXN9K-X9736C-EXN9K-X97284YC-FXN9K-X9732C-FXN9K-X9788TC-FXN9K-X9716D-GX

Voorwaarden

Vereisten

Cisco raadt u aan de basis van de Ethernet Switched Port Analyzer (SPAN) optie op de Cisco Nexus 9000 Series switches te begrijpen. Raadpleeg voor meer informatie over deze functie de volgende documenten:

- [Cisco Nexus 9000 Series configuratie-handleiding voor NX-OS systeembeheer, release 9.3\(x\)](#)
- [Cisco Nexus 9000 Series NX-OS systeembeheerdershandleiding, release 9.2\(x\)](#)
- [Cisco Nexus 9000 Series NX-OS systeembeheerdershandleiding, release 7.0\(3\)I7\(x\)](#)

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Nexus 9000 Series switches met de Cloud Scale ASIC met NX-OS software release 9.3(3).

De informatie in dit document is gemaakt van apparatuur in een specifieke labomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Vorzorgsmaatregelen en beperkingen

De monitor-sessies van SPAN-to-CPU hebben bepaalde voorbehouden en beperkingen om u ervan te bewust te zijn wanneer u pakketstromen voor probleemoplossing gebruikt. Dit document

bevat een aantal veelbesproken voorbehouden. Raadpleeg de volgende documenten voor een volledige lijst van richtsnoeren en beperkingen:

- [Cisco Nexus 9000 Series configuratie-handleiding voor NX-OS systeembeheer, release 9.3\(x\)](#)
- [Cisco Nexus 9000 Series NX-OS systeembeheerdershandleiding, release 9.2\(x\)](#)
- [Cisco Nexus 9000 Series NX-OS systeembeheerdershandleiding, release 7.0\(3\)I7\(x\)](#)

50 kbps standaard hardware snelheidsbeperking

Standaard beperken Cisco Nexus 9000 Series switches het aantal verkeer dat naar het besturingsplane is gerepliceerd via een SPAN-to-CPU monitorsessie tot 50 kbps. Deze snelheidsbeperking wordt uitgevoerd op de ASIC/expediteur-motor met cloudschaal en is een zelfbeveiligingsmechanisme dat ervoor zorgt dat het bedieningspaneel van de machine niet overweldigd is door het nagemaakte verkeer.

De opdracht **Show hardware rate-limiter span** kan worden gebruikt om de huidige instelling van de SPAN-to-CPU sessiesessie-limitering te bekijken.

```
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
```

Als het gerepliceerde verkeer door de hardware rate-limiter wordt verbroken, dan is de Dropped kolom een waarde die niet nul is, zoals in de output hieronder wordt weergegeven:

```
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
```

De SPAN-to-CPU de beperking van de de monitor van de hardware snelheid kan worden gewijzigd met de **hardware rate-limiter span {kbps}** globale configuratieopdracht, zoals in de output hieronder getoond.

```
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
```

Voorzichtig: Cisco raadt niet aan de hardware-rate limitering van de SPAN-to-CPU-sessie te wijzigen vanuit de standaardwaarde van 50 kbps, tenzij expliciet opdracht daartoe gegeven door Cisco TAC. Het verhogen van dit snelheidsbeperkingen tot een hoge waarde kan een verhoogd gebruik van CPU's en instabiliteit van besturingsplane veroorzaken op de Cisco Nexus 9000 Series switch, wat een significante impact op het productieverkeer kan veroorzaken.

Beperking aantal SPAN-to-CPU-hardwarevertraging is niet ondersteund

De output van de **show hardware rate-limiter span** opdracht bevat een toegestane teller. Op andere hardware rate limiters geeft deze teller aan hoeveel bytes met succes door de hardware

rate limiter passeren. De toegestane teller voor de SPAN-to-CPU hardwaresnelheidsbeperking is echter niet toegenomen door een softwarebeperking. Een voorbeeld hiervan wordt in de onderstaande uitvoer weergegeven:

```
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
```

Deze softwarebeperking heeft invloed op alle NX-OS software releases en wordt gedocumenteerd via [CSCva37512](#).

Om te bepalen hoeveel verkeer is gerepliceerd naar het bedieningspaneel van een Nexus 9000 apparaat dat met een actieve SPAN-to-CPU monitorsessie is geconfigureerd, gebruikt u de opdracht voor het insluiten van een **stelsel interne toegangslijst** voor het toegangsgebied. Hieronder wordt een voorbeeld weergegeven van de gefilterde uitvoer van de bovengenoemde opdracht, die relevante pakketten en byte-tellers toont.

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

Pakketten met besturingsplane worden niet weergegeven in TX SPAN-to-CPU monitorsessies

Pakketten die door het bedieningspaneel zijn gemaakt en die vanuit een broninterface zijn verzonden voor een SPAN-naar-CPU-monitorsessie, worden niet opgenomen door de SPAN-naar-CPU monitorsessie. Deze pakketten bereiken de interface correct, maar kunnen niet door een SPAN-to-CPU monitorsessie worden opgenomen op hetzelfde apparaat waar het pakket wordt gegenereerd.

Bedenk bijvoorbeeld een Cisco Nexus 9000 Series apparaat waar Ethernet1/1 een L3/routed interface is die op een andere router wordt aangesloten. OSPF-proces 1 is geactiveerd op Ethernet1/1, wat de enige OSPF-geactiveerde interface is op het Cisco Nexus 9000-apparaat.

```
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
```

De [dienst](#) van de [Controle van de Ethanalyzer](#) toont aan dat de OSPF Hello-berichten door het controlevlugtuig van het apparaat eens per 10 seconden worden gegenereerd.

```
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
```

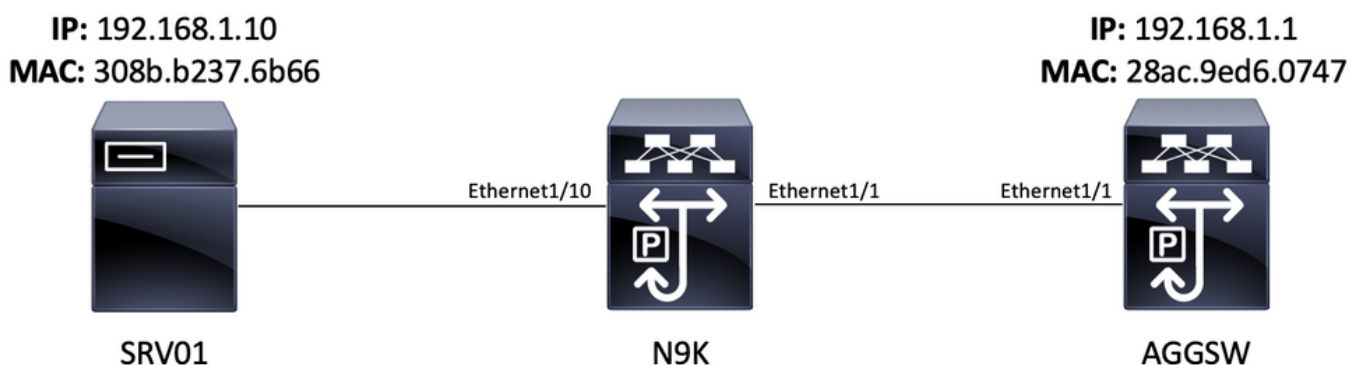
Echter, een uitgang/TX SPAN-to-CPU op de Ethernet1/1 interface toont deze Open Kortste Pad Eerst (OSPF) Hallo pakketten die na 60 seconden op deze interface worden verzonden niet.

```
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# ethalyzer local
interface inband mirror display-filter ospf autostop duration 60 Capturing on inband 0 packets
captured
```

Om te controleren of pakketten die door het bedieningspaneel van een Cisco Nexus 9000-apparaat worden gegenereerd, vanuit een specifieke interface worden verzonden, raadt Cisco het gebruik van een programma voor pakketvastlegging op het externe apparaat dat op de interface is aangesloten.

Cisco Nexus 9000 cloudschaal SPAN-to-CPU-procedure

Overweeg de volgende topologie:



Een ICMP-pakket (Internet Control Message Protocol), afkomstig van server SRV01 in VLAN 10 (192.168.10.10), is bedoeld voor de VLAN 10-gateway 192.168.10.1. Er wordt een SPAN-to-CPU monitorsessie gebruikt om te bevestigen dat dit ICMP-pakket uit een 9K-apparaat bestaat een Cisco Nexus 93180YC-EX die NX-OS software release 9.3(3) draait. Deze functie werkt als een Layer 2-switch die SRV01 verbindt met AGGSW in VLAN 10.

Stap 1. Bevestig voldoende middelen voor de nieuwe SPAN-sessie

Cisco Nexus 9000 Series switches met de Cloud Scale ASIC die NX-OS-software uitvoeren, ondersteunen maximaal vier actieve SPAN- of ERSPAN-sessies per ASIC/verzendmotor. Als de eerste drie SPAN- of ERSPAN-sessies bovendien zijn geconfigureerd met bidirectionele (TX en RX) broninterfaces, moet de broninterface van de vierde SPAN- of ERSPAN-sessie een indringende/RX-bron zijn.

Voordat u een monitor-sessie SPAN-naar-CPU configureren controleert u de hoeveelheid andere SPAN- of ERSPAN-sessies die momenteel op het apparaat worden ingesteld. Dit kan worden gedaan met de **show in werking stellen-in werking stellen-enig monitor** en **monitor** opdrachten **tonen**. Het onderstaande voorbeeld toont de uitvoer van beide opdrachten wanneer er geen andere SPAN- of ERSPAN-sessies op het apparaat zijn ingesteld.

```
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
```

Opmerking: Aanvullende informatie over het maximale aantal SPAN/ERSPAN-sessies en andere beperkingen kan worden gevonden in de [Cisco Nexus 9000 Series NX-OS geverifieerde schaalbaarheidsgids voor NX-OS software release 9.3\(3\)](#).

Stap 2. Configuratie van de monitor SPAN-to-CPU

Het belangrijkste configuratieelement dat een monitor-sessie SPAN-naar-CPU definieert is een doelinterface van "sup-eth0", wat de inband-interface van de toezichhouder is. Het onderstaande voorbeeld toont de configuratie van een monitor-sessie SPAN-naar-CPU waar de ingress/RX-pakketten van Ethernet1/10 worden gerepliceerd naar de supervisor van de Cisco Nexus 9000 Series switch.

```
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#
```

Stap 3. Controleer of de monitor-sessie SPAN-naar-CPU is omhoog

Gebruik de **toonaangevende in werking gestelde-beslist monitor** en **show monitor** opdrachten om te verifiëren dat de SPAN-to-CPU monitor sessie wordt gevormd en operationeel is. De configuratie van de SPAN-to-CPU monitor sessie kan door de uitvoer van het **show in werking stellen-configuratie** controlebevel worden geverifieerd, zoals in het onderstaande voorbeeld wordt getoond.

```
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
```

De operationele status van de monitor SPAN-to-CPU kan worden geverifieerd door de uitvoer van de opdracht **voor de monitor**. De uitvoer moet melden dat de status van de monitor SPAN-to-CPU-sessie "omhoog" is met de reden "De sessie is omhoog", zoals in het onderstaande voorbeeld wordt weergegeven.

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

Stap 4. Bekijk herhaalde pakketten in het besturingsplane

Het [hulpprogramma](#) voor de [pakketvastlegging](#) voor [de](#) scanner kan worden gebruikt om verkeer te bekijken dat naar het besturingsplane van het Cisco Nexus 9000-apparaat is gerepliceerd. Het sleutelwoord van de **spiegel** in het EtherAnalyzer bevel filters verkeer dat slechts door een SPAN-aan-CPU monitorzitting wordt gerepliceerd wordt getoond. Filters voor het opnemen en weergegeven van Ethernet kunnen worden gebruikt om het weergegeven verkeer verder te beperken. Aanvullende informatie over nuttige Ethernet-analyzer-opname en -weergavefilters kan worden gevonden in de [Ethanalyzer op de Nexus 7000 Problemen opsporen en verhelpen Guide](#).

Houd er rekening mee dat dit document is geschreven voor het Cisco Nexus 7000-platform, en dat het bovendien grotendeels van toepassing is op het Cisco Nexus 9000-platform.

Hieronder vindt u een voorbeeld van het gebruik van het pakketopnamestation waarin het apparaat voor de controle van de Ethanalyzer is gebruikt om verkeer te filteren dat is gerepliceerd door een monitor-naar-CPU-sessie. Merk op dat het sleutelwoord van de **spiegel** wordt gebruikt, zowel als een weergavefilter dat ICMP-pakketten definieert die afkomstig zijn van of bestemd zijn voor 192.168.10.10 (het IP-adres van SRV01 in de bovengenoemde topologie).

```
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
```

Opmerking: Gebruik de Control-C-sleutelcombinatie om het beheerprogramma voor de Ethernet-analyzer te beëindigen.

Men kan gedetailleerde informatie over dit verkeer bekijken door het **detail** sleutelwoord in de opdracht van de Ethanalyzer te omvatten. Hieronder vindt u een voorbeeld van één pakket ICMP-Echo-aanvraag.

```
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 ab cd .....
0040 ab cd ab cd ab cd ab cd ..... Data: 00000000ED9E9EB9ABCDABCDABCDABCDABCDABCDABCD...
[Length: 72] ^C 1 packet captured
```

Stap 5. Sluit de SPAN-to-CPU-sessie administratief af

Gebruik de configuratieopdracht in de context van de SPAN-to-CPU-monitorsessie **afsluiten** om de monitor SPAN-to-CPU sessie scherp te sluiten en te stoppen met het kopiëren van verkeer naar het controlevlak van Cisco Nexus 9000-apparaat.

```
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#
```

Controleer de operationele status van de SPAN-to-CPU monitorsessie met de opdracht **monitor**. De operationele status van de monitor SPAN-to-CPU dient als "uitgezet" te worden weergegeven met een reden voor "Sessiebeheer uitgeschakeld", zoals in het onderstaande voorbeeld wordt getoond:

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

Stap 6. Verwijder de configuratie van de monitor-naar-CPU (optioneel)

Indien gewenst, verwijder de SPAN-aan-CPU monitor vergaderconfiguratie met de **geen** configuratieopdracht van de **monitor {id}**. Een voorbeeld hiervan wordt in de onderstaande uitvoer weergegeven.

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

Controleer dat de configuratie van de monitor SPAN-to-CPU met succes is verwijderd met het bevel van de **show in werking stellen**-configuratie, zoals in het onderstaande voorbeeld wordt getoond.

```
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#
```

De resultaten van een SPAN-to-CPU pakketvastlegging analyseren

Het bovenstaande voorbeeld van deze procedure toont aan dat de pakketten ICMP Echo-aanvraag die zijn gebaseerd op 192.168.10.10 (SRV01) en bestemd zijn voor 192.168.10.1 (AGGSW), de Ethernet1/10 interface van het Cisco Nexus 900-apparaat met een hostnaam N9N K. Dit bewijst dat SRV01 dit verkeer vanuit zijn netwerkinterfacekaart verstuurt. Dit bewijst ook dat het pakket ICMP Echo Application ver genoeg gaat in de Cisco Cloud Scale ASIC's verzendpijplijn zodat het naar het besturingsplane van het apparaat kan worden gerepliceerd.

Dit bewijst echter niet dat het Cisco Nexus 9000-apparaat het ICMP Echo Application-pakket vanuit Ethernet1/1 naar AGGSW doorstuurt. Er moet meer worden gedaan voor het opsporen en verhelpen van problemen om te bevestigen of het pakket via Ethernet1/1 naar AGGSW is verzonden. In volgorde van betrouwbaarheid:

1. Als het externe apparaat van de verwachte spanning-interface (Ethernet1/1 van N9K in het voorbeeld) een Cisco Nexus 9000 seriemateriaal met een Cloud-Scale ASIC is, kunt u een IP/RX SPAN-to-CPU monitorsessie op het externe apparaat uitvoeren (Eth1/1 van AGGSW in het voorbeeld eerder). Als het afstandsapparaat van de verwachte rackinterface geen Cisco Nexus

9000 Series-apparaat met een Cloud-Schaal ASIC is, dan is een SPAN, poortspiegel of andere soortgelijke pakketvastlegging op het externe apparaat gelijkwaardig.

2. Voer een indringer/RX-ELAM uit op de IP-interface (Ethernet1/10 van N9K in het bovenstaande voorbeeld) van Cisco Nexus 9000-apparaat. Aanvullende informatie over deze procedure kan worden gevonden in de [technische opmerking](#) van de [Nexus 9000 Cloud Scale ASIC NX-OS ELAM Problemen opsporen en verhelpen](#).

3. Voer een egress/TX SPAN-to-CPU uit op de spanningsinterface van het Cisco Nexus 9000-apparaat (Ethernet1/1 van N9K in het bovenstaande voorbeeld).

Gerelateerde informatie

- [Cisco Nexus 9000 Series Gids voor probleemoplossing in NX-OS, release 9.3\(x\)](#)
- [Cisco Nexus 9000 Series NX-OS handleiding voor probleemoplossing, release 9.2\(x\)](#)
- [Cisco Nexus 9000 Series NX-OS handleiding voor probleemoplossing, release 7.0\(3\)17\(x\)](#)
- [Ethanalyzer op Nexus 7000 Handleiding voor probleemoplossing](#)
- [Nexus 9000 Cloud Scale ASIC \(Tahoe\) NX-OS ELAM](#)