Verfahren für die Cloud-Skalierung von Nexus 9000 mit ASIC NX-OS SPAN-to-CPU

Einführung

In diesem Dokument werden die Schritte zum Durchführen einer SPAN-zu-CPU-Paketerfassung (Switched Port Analyzer) für eine Reihe von Cisco Nexus 9000 Cloud Scale ASIC-Modulen beschrieben. In diesem Dokument werden auch die häufigsten Probleme beschrieben, die bei der Verwendung einer SPAN-zu-CPU-Paketerfassung zur Fehlerbehebung beim Paketfluss über einen Cisco Nexus Switch der Serie 9000 zur Cloud-Skalierung auftreten.

Hintergrundinformationen

Mit einer SPAN-CPU-Paketerfassung können Netzwerkadministratoren schnell und einfach überprüfen, ob bestimmte Pakete einen Cisco Nexus Switch der Serie 9000 zur Cloud-Skalierung ein- und ausgehen. Ähnlich wie bei einer normalen SPAN- oder Encapsulated Remote SPAN (ERSPAN)-Sitzung umfasst eine SPAN-zu-CPU-Überwachungssitzung die Definition einer oder mehrerer Quellschnittstellen und Datenverkehrsrichtungen. Datenverkehr, der der Richtung (TX, RX oder beide) entspricht, die an einer Quellschnittstelle definiert ist, wird auf der Steuerungsebene des Cisco Nexus 9000 repliziert. Dieser replizierte Datenverkehr kann mithilfe des Paketerfassungs-Utilitys der Ethanalyzer-Kontrollebene gefiltert und analysiert oder zur späteren Überprüfung auf einem lokalen Speichergerät gespeichert werden.

Diese Funktion ist für die temporäre Verwendung bei der Fehlerbehebung des Paketflusses über die Cisco Nexus Switches der Serie 9000 vorgesehen. Cisco empfiehlt nachdrücklich, dass SPAN-to-CPU-Überwachungssitzungen administrativ geschlossen oder entfernt werden, wenn sie nicht aktiv zur Behebung eines Problems mit dem Paketfluss verwendet werden. Andernfalls kann die Leistung für replizierten Datenverkehr im Netzwerk beeinträchtigt und die CPU-Auslastung des Cisco Nexus Switches der Serie 9000 erhöht werden.

Anwendbare Hardware

Das in diesem Dokument beschriebene Verfahren gilt nur für diese Hardware:

N9K-C93180YC-EX	N9K-C92304QC
N9K-X9736C-EX	N9K-C92300YC
N9K-C93108TC-EX	N9K-X9788TC-FX
N9K-X9732C-EX	N9K-X97284YC-FX
N9K-X97160YC-EX	N9K-C93180YC-FX
N9K-C93180LC-EX	N9K-C93108TC-FX
N9K-C92160YC-X	N9K-C9348GC-FXP

N9K-C9272Q	N9K-X9732C-FX
N9K-C9236C	N9K-C9336C-FX2
N9K-C93240YC-FX2	N9K-C93300YC-FX2
N9K-C9364C	N9K-C9332C

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie sich mit den Grundlagen der SPAN-Funktion (Ethernet Switched Port Analyzer) für Switches der Cisco Nexus Serie 9000 vertraut machen. Weitere Informationen zu dieser Funktion finden Sie in den folgenden Dokumenten:

- Cisco Nexus 9000 NX-OS-Systemverwaltungskonfigurationsleitfaden, Version 9.3(x)
- Cisco Nexus 9000 NX-OS-Systemverwaltungskonfigurationsleitfaden, Version 9.2(x)
- Cisco Nexus 9000 NX-OS-Systemverwaltungskonfigurationsleitfaden, Version 7.0(3)I7(x)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Nexus Switches der Serie 9000 mit dem Cloud Scale ASIC mit NX-OS-Softwareversion 9.3(3).

Die Informationen in diesem Dokument wurden von Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Vorbehalte und Einschränkungen

SPAN-to-CPU-Überwachungssitzungen haben einige Vorbehalte und Einschränkungen, die bei der Fehlerbehebung von Paketflüssen beachtet werden müssen. In diesem Dokument werden einige häufig auftretende Probleme behandelt. Eine vollständige Liste der Richtlinien und Einschränkungen finden Sie in den folgenden Dokumenten:

- Cisco Nexus 9000 NX-OS-Systemverwaltungskonfigurationsleitfaden, Version 9.3(x)
- Cisco Nexus 9000 NX-OS-Systemverwaltungskonfigurationsleitfaden, Version 9.2(x)
- Cisco Nexus 9000 NX-OS-Systemverwaltungskonfigurationsleitfaden, Version 7.0(3)I7(x)

Durchsatzbegrenzer für 50 Kbit/s Standard-Hardware

Standardmäßig beschränken die Switches der Cisco Nexus Serie 9000 die Datenverkehrsrate, die über eine SPAN-CPU-Überwachungssitzung auf die Kontrollebene repliziert wird, auf 50 Kbit/s. Diese Ratenbegrenzung wird in der Cloud-Skalierungs-ASIC/Forwarding-Engine durchgeführt und stellt einen Selbstschutzmechanismus dar, der sicherstellt, dass die Kontrollebene des Geräts nicht durch replizierten Datenverkehr überlastet wird.

Mit dem Befehl **show hardware rate-limiter span** kann die aktuelle Einstellung des Durchsatzbegrenzers für SPAN-zu-CPU-Überwachungssitzungen angezeigt werden.

```
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
```

Wenn der replizierte Datenverkehr durch den Hardware-Ratenlimitierer verworfen wird, ist die Spalte "Verworfen" ein Wert ungleich null, wie in der folgenden Ausgabe gezeigt:

```
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
```

Der Hardware-Ratenlimitierer für die SPAN-zu-CPU-Sitzung kann mit dem globalen Konfigurationsbefehl **Hardware-Ratenlimitierung span {kbps}** geändert werden, wie in der unten stehenden Ausgabe gezeigt.

```
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
```

> **Vorsicht**: Cisco empfiehlt, den Hardware-Ratenlimitierer für die SPAN-zu-CPU-Sitzung nicht von seinem Standardwert von 50 Kbit/s zu verändern, es sei denn, dies wird ausdrücklich vom Cisco TAC angewiesen. Die Erhöhung dieses Durchsatzbegrenzers auf einen hohen Wert kann zu einer erhöhten CPU-Auslastung und Instabilität auf Kontrollebene auf dem Switch der Cisco Nexus Serie 9000 führen, was erhebliche Auswirkungen auf den Produktionsdatenverkehr haben kann.

Der zugelassene Zähler für die Hardware von SPAN zu CPU wird nicht unterstützt.

Die Ausgabe des Befehls **show hardware rate-limiter span** enthält einen zugelassenen Zähler. Bei anderen Hardware-Ratenlimitierungen gibt dieser Zähler an, wie viele Bytes erfolgreich durch den Hardware-Ratenbegrenzer geleitet werden. Der zulässige Leistungsindikator für den Hardware-Ratenlimitierer SPAN-zu-CPU erhöht sich jedoch nicht aufgrund einer Softwarebeschränkung. Ein Beispiel hierfür ist die folgende Ausgabe:

```
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
```

Diese Softwarebeschränkung betrifft alle NX-OS-Softwareversionen und wird durch CSCva37512 dokumentiert.

Um zu bestimmen, wie viel Datenverkehr auf die Steuerungsebene eines Nexus 9000-Geräts repliziert wurde, das mit einer aktiven SPAN-zu-CPU-Überwachungssitzung konfiguriert wurde, verwenden Sie den Befehl **show system internal access-list tcam ingress region span**. Nachfolgend wird ein Beispiel für die gefilterte Ausgabe des oben genannten Befehls gezeigt, die relevante Paket- und Bytezähler anzeigt.

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

Von der Kontrollebene generierte Pakete werden in den TX SPAN-to-CPU-Überwachungssitzungen nicht angezeigt.

Pakete, die von der Steuerungsebene erstellt und über eine Quellschnittstelle für eine SPAN-CPU-Überwachungssitzung übertragen werden, werden von der SPAN-to-CPU-Überwachungssitzung nicht erfasst. Diese Pakete senden die Schnittstelle korrekt aus, können jedoch nicht über eine SPAN-CPU-Überwachungssitzung auf demselben Gerät erfasst werden, auf dem das Paket generiert wird.

Betrachten Sie beispielsweise ein Gerät der Cisco Nexus Serie 9000, bei dem Ethernet1/1 eine L3-/geroutete Schnittstelle ist, die mit einem anderen Router verbunden ist. Der OSPF-Prozess 1 wird auf Ethernet1/1 aktiviert, der einzigen OSPF-aktivierten Schnittstelle auf dem 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
```

Das Paketerfassungs-Utility für die Kontrollebene von Ethanalyer zeigt, dass die OSPF Hello-Nachrichten einmal alle 10 Sekunden von der Kontrollebene des Geräts generiert werden.

```
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
```

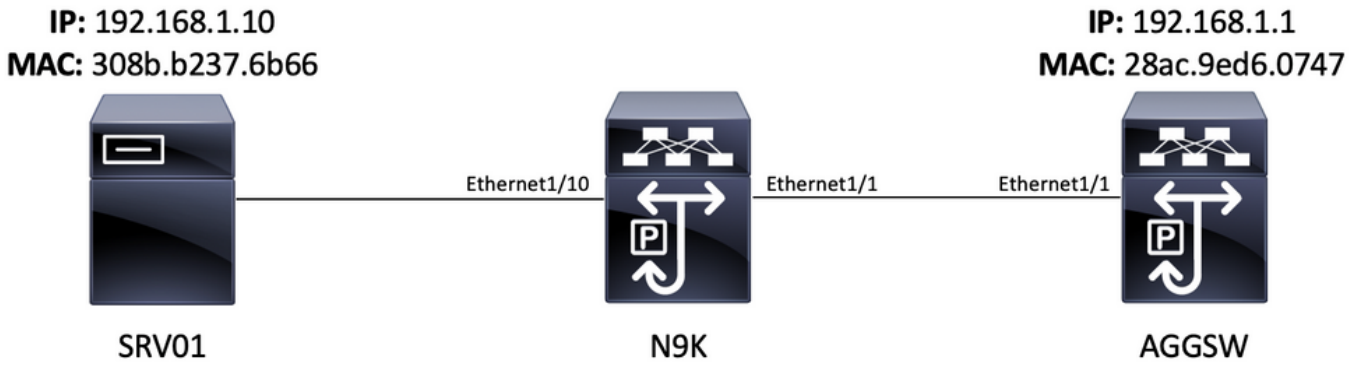
Ein Ausgangs-/TX-SPAN-zu-CPU an der Ethernet1/1-Schnittstelle zeigt diese OSPF-Hello-Pakete (Open Shortest Path First) jedoch nicht an, die nach 60 Sekunden auf dieser Schnittstelle übertragen wurden.

```
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
```

Um zu überprüfen, ob Pakete, die von der Steuerungsebene eines Cisco Nexus 9000-Geräts generiert wurden, über eine bestimmte Schnittstelle übertragen werden, empfiehlt Cisco die Verwendung eines Paketerfassungs-Dienstprogramms auf dem an die Schnittstelle angeschlossenen Remote-Gerät.

Verfahren zur Cloud-Skalierung von Cisco Nexus 9000 von SPAN zu CPU

Betrachten Sie die folgende Topologie:



Für das VLAN 10-Gateway 192.168.10.10 ist ein ICMP-Paket (Internet Control Message Protocol) bestimmt, das vom Server SRV01 in VLAN 10 (192.168.10.1) bezogen wird. Es wird eine SPAN-CPU-Überwachungssitzung verwendet, um zu bestätigen, dass dieses ICMP-Paket das Gerät N9K durchläuft (ein Cisco Nexus 93180YC-EX mit NX-OS-Softwareversion 9.3(3)), das als Layer-2-Switch fungiert, der SRV01 mit AGGSW in VLAN 10 verbindet.

Schritt 1: Ausreichende Ressourcen für die neue SPAN-Sitzung bestätigen

Die Cisco Nexus Switches der Serie 9000 mit dem Cloud Scale ASIC, die NX-OS-Software ausführen, unterstützen maximal vier aktive SPAN- oder ERSPAN-Sitzungen pro ASIC-/Forwarding-Engine. Wenn die ersten drei SPAN- oder ERSPAN-Sitzungen mit bidirektionalen (TX und RX) Quellschnittstellen konfiguriert sind, muss die Quellschnittstelle der vierten SPAN- oder ERSPAN-Sitzung eine Eingangs-/RX-Quelle sein.

Bevor Sie eine SPAN-zu-CPU-Überwachungssitzung konfigurieren, überprüfen Sie die Anzahl der anderen derzeit auf dem Gerät konfigurierten SPAN- oder ERSPAN-Sitzungen. Dies kann mithilfe des **Bildschirms show running-config monitor** und der Befehle **show monitor** erfolgen. Das nachfolgende Beispiel zeigt die Ausgabe beider Befehle, wenn auf dem Gerät keine anderen SPAN- oder ERSPAN-Sitzungen konfiguriert sind.

```
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
```

> **Hinweis**: Weitere Informationen zur maximalen Anzahl von SPAN/ERSPAN-Sitzungen und anderen Einschränkungen finden Sie im Cisco Nexus 9000 NX-OS Verified Scalability Guide für NX-OS Software Version 9.3(3).

Schritt 2: Konfigurieren der Überwachungssitzung von SPAN zu CPU

Das zentrale Konfigurationselement, das eine SPAN-zu-CPU-Überwachungssitzung definiert, ist die Zielschnittstelle "sup-eth0", die die In-Band-Schnittstelle des Supervisors darstellt. Das nachfolgende Beispiel zeigt die Konfiguration einer SPAN-zu-CPU-Überwachungssitzung, in der

die ein-/ausgehenden RX-Pakete von Ethernet1/10 auf den Supervisor des Switches der Cisco Nexus Serie 9000 repliziert werden.

```
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#
```

Schritt 3: Überprüfen Sie, ob die Überwachungssitzung von SPAN zu CPU aktiv ist.

Verwenden Sie die Befehle **show running-config monitor** und **show monitor**, um zu überprüfen, ob die SPAN-to-CPU-Überwachungssitzung konfiguriert und betriebsbereit ist. Die Konfiguration der SPAN-to-CPU-Überwachungssitzung kann mithilfe des Befehls **show running-config monitor** überprüft werden, wie im folgenden Beispiel gezeigt.

```
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
```

Der Betriebsstatus der SPAN-to-CPU-Überwachungssitzung kann durch die Ausgabe des Befehls **show monitor** überprüft werden. Die Ausgabe sollte melden, dass der Status der SPAN-to-CPU-Überwachungssitzung "aktiv" ist, und zwar aus dem Grund "Die Sitzung ist aktiv", wie im folgenden Beispiel gezeigt.

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

Schritt 4: Anzeigen replizierter Pakete auf der Kontrollebene

Mit dem Paketerfassungs-Dienstprogramm der Kontrollebene kann der auf der Kontrollebene des Cisco Nexus 9000 replizierte Datenverkehr angezeigt werden. Das **spiegel**-Schlüsselwort im Ethanalyzer-Befehl filtert Datenverkehr so, dass nur Datenverkehr angezeigt wird, der von einer SPAN-zu-CPU-Überwachungssitzung repliziert wurde. Mithilfe von Ethanalyzer-Erfassungs- und Anzeigefiltern kann der angezeigte Datenverkehr weiter eingeschränkt werden. Weitere Informationen zu nützlichen EtherAnalyzer-Erfassungs- und Anzeigefiltern finden Sie im Ethanalyzer-Leitfaden zur Fehlerbehebung für den Nexus 7000. Beachten Sie, dass dieses Dokument zwar für die Cisco Nexus 7000-Plattform geschrieben wurde, jedoch hauptsächlich auch für die Cisco Nexus 9000-Plattform gilt.

Ein Beispiel für die Verwendung des Paketerfassungs-Utilitys der Ethanalyzer-Kontrollebene zum Filtern von Datenverkehr, der von einer SPAN-zu-CPU-Überwachungssitzung repliziert wird, ist unten dargestellt. Beachten Sie, dass das **spiegel-**Schlüsselwort verwendet wird, sowie ein Anzeigefilter, der ICMP-Pakete definiert, die von 192.168.10.10 stammen oder für diese bestimmt sind (die IP-Adresse von SRV01 in der oben genannten 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
```

Hinweis: Verwenden Sie die Tastenkombination Control-C, um das Paket-Erfassungsprogramm der Ethernet-Analyzer-Kontrollebene zu beenden.

Detaillierte Informationen zu diesem Datenverkehr können Sie anzeigen, indem Sie das **detail**-Schlüsselwort in den Ethanalyzer-Befehl einfügen. Ein Beispiel hierfür ist unten für ein einzelnes ICMP-Echo-Request-Paket dargestellt.

```
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 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
```

Schritt 5: Schließen Sie die Überwachungssitzung von SPAN zu CPU administrativ.

Verwenden Sie den **shutdown**-Konfigurationsbefehl im Kontext der SPAN-to-CPU-Überwachungssitzung, um die SPAN-zu-CPU-Überwachungssitzung ordnungsgemäß herunterzufahren und die Datenreplikation auf die Steuerungsebene des Cisco Nexus 9000-Geräts zu beenden.

```
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#
```

Überprüfen Sie den Betriebsstatus der SPAN-zu-CPU-Überwachungssitzung mit dem Befehl **show monitor**. Der Betriebsstatus der SPAN-to-CPU-Überwachungssitzung sollte unter dem Motto "Session admin shutdown" als "down" angezeigt werden, wie im folgenden Beispiel gezeigt:

```
N9K# show monitor  Session State Reason Description - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

```
- - 1 down Session admin shut
```

Schritt 6: Entfernen Sie die Konfiguration der Überwachungssitzung vom SPAN zur CPU (optional).

Entfernen Sie bei Bedarf die Konfiguration der SPAN-to-CPU-Überwachungssitzung mit dem Konfigurationsbefehl **no monitor session {id}**. Ein Beispiel hierfür ist in der Ausgabe unten dargestellt.

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

Vergewissern Sie sich, dass die Konfiguration der SPAN-to-CPU-Überwachungssitzung erfolgreich mit dem Befehl **show running-config monitor** entfernt wurde, wie im Beispiel unten gezeigt.

```
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#
```

Analysieren der Ergebnisse einer Paketerfassung von SPAN zu CPU

Das obige Beispiel dieses Verfahrens zeigt, dass ICMP-Echo-Anforderungspakete, die von 192.168.10.10 (SRV01) stammen und für 192.168.10.1 (AGGSW) bestimmt sind, die Ethernet1/10-Schnittstelle des Cisco Nexus 900-Geräts mit dem Hostnamen N empfangen. 9000 Dies belegt, dass die SRV01 diesen Datenverkehr von der Netzwerkschnittstellenkarte sendet. Dies beweist auch, dass das ICMP-Echo-Request-Paket weit genug in die Weiterleitungspipeline des Cisco Cloud Scale ASICs fortschreitet, damit es auf die Kontrollebene des Geräts repliziert werden kann.

Dies beweist jedoch nicht, dass das Cisco Nexus 9000-Gerät das ICMP-Echo Request-Paket aus Ethernet1/1 an AGGSW weiterleitet. Es muss eine weitere Fehlerbehebung durchgeführt werden, um zu überprüfen, ob das Paket aus Ethernet1/1 an AGGSW weitergeleitet wird. In der Reihenfolge der Vertrauenswürdigkeit:

1. Wenn das Remote-Gerät der erwarteten Ausgangsschnittstelle (im Beispiel Ethernet1/1 von N9K) ein Gerät der Cisco Nexus Serie 9000 mit einem Cloud-fähigen ASIC ist, können Sie eine Eingangs-/RX-SPAN-zu-CPU-Überwachungssitzung auf dem Remote-Gerät ausführen (im vorherigen Beispiel Eth1/1 von AGGSW). Wenn das Remote-Gerät der erwarteten Ausgangsschnittstelle kein Gerät der Cisco Nexus Serie 9000 mit einem Cloud-Scale-ASIC ist, ist eine SPAN-, Port-Mirror- oder andere ähnliche Paketerfassung auf dem Remote-Gerät gleichwertig.

2. Führen Sie an der Eingangsschnittstelle (Ethernet1/10 von N9K im obigen Beispiel) des Cisco Nexus 9000 ein Eingangs-/RX-ELAM aus. Weitere Informationen zu diesem Verfahren finden Sie im Nexus 9000 Cloud Scale ASIC NX-OS ELAM Troubleshooting TechNote.

3. Führen Sie an der Ausgangsschnittstelle des Cisco Nexus 9000 eine Ausgangs-/TX-SPAN-zu-CPU aus (im obigen Beispiel Ethernet1/1 von N9K).

Zugehörige Informationen

- NX-OS-Fehlerbehebungsleitfaden für die Cisco Nexus Serie 9000, Version 9.3(x)
- NX-OS-Fehlerbehebungsleitfaden für die Cisco Nexus Serie 9000, Version 9.2(x)
- Cisco Nexus NX-OS-Fehlerbehebungsleitfaden für die Serie 9000, Version 7.0(3)I7(x)
- Ethanalyzer für Nexus 7000 - Leitfaden zur Fehlerbehebung
- Nexus 9000 Cloud Scale ASIC (Tahoe) NX-OS ELAM