Nexus 9000雲擴展ASIC NX-OS SPAN到CPU過程

目錄

簡介

本檔案介紹在一系列Cisco Nexus 9000雲規模ASIC模組上執行交換連線埠分析器(SPAN)到CPU封包擷取所使用的步驟。本文還介紹使用SPAN到CPU資料包捕獲對通過Cisco Nexus 9000 Cloud Scale系列交換機的資料包流進行故障排除時遇到的常見警告。

背景資訊

SPAN到CPU的封包擷取允許網路管理員快速且輕鬆地驗證特定封包是否輸入和輸出Cisco Nexus 9000 Cloud Scale系列交換器。與普通SPAN或封裝遠端SPAN(ERSPAN)作業階段類似，SPAN到CPU的監控作業階段涉及一個或多個來源介面和流量方向的定義。與源介面上定義的方向（TX、RX或雙向）匹配的任何流量都會複製到Cisco Nexus 9000裝置的控制平面。可以使用Ethanalyzer控制平面資料包捕獲實用程式過濾和分析此複製流量，也可以將其儲存到本地儲存裝置以供日後檢視。

此功能用於在排除通過Cisco Nexus 9000系列交換機的資料包流故障時臨時使用。Cisco強烈建議管理性關閉SPAN到CPU的監控會話，或在未主動用於解決資料包流問題時將其刪除。否則可能會導致網路中複製流量的效能降低，並增加Cisco Nexus 9000系列交換機的CPU利用率。

適用硬體

本文檔中涉及的步驟僅適用於此硬體：

- **Nexus 9200/9300固定交換器** 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-C93600CD-GXN9K-C9364C-GXN9K-C9364D-GX2AN9K-C9332D-GX2B
- **Nexus 9500模組化交換線路卡** N9K-X97160YC-EXN9K-X9732C-EXN9K-X9736C-EXN9K-X97284YC-FXN9K-X9732C-FXN9K-X9788TC-FXN9K-X9716D-GX

必要條件

需求

思科建議您瞭解Cisco Nexus 9000系列交換器上的乙太網路交換連線埠分析器(SPAN)功能的基礎知識。有關此功能的資訊，請參閱以下文檔：

- Cisco Nexus 9000系列NX-OS系統管理配置指南9.3(x)版
- Cisco Nexus 9000系列NX-OS系統管理配置指南9.2(x)版
- Cisco Nexus 9000系列NX-OS系統管理配置指南7.0(3)I7(x)版

採用元件

本檔案中的資訊是根據執行NX-OS軟體版本9.3(3)的Cloud Scale ASIC的Cisco Nexus 9000系列交換器。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

注意事項和限制

在排除資料包流故障時，SPAN到CPU的監控會話需要注意一些警告和限制。本文檔將介紹一些常見警告。有關准則和限制的完整清單，請參閱以下文檔：

- Cisco Nexus 9000系列NX-OS系統管理配置指南9.3(x)版
- Cisco Nexus 9000系列NX-OS系統管理配置指南9.2(x)版
- Cisco Nexus 9000系列NX-OS系統管理配置指南7.0(3)I7(x)版

50 kbps預設硬體速率限制器

預設情況下，Cisco Nexus 9000系列交換機將通過SPAN到CPU監控會話複製到控制平面的流量限製為50 kbps。此速率限制在雲規模ASIC/轉發引擎上執行，是一種自我保護機制，用於確保裝置的控制平面不會因複製流量過多。

show hardware rate-limiter span命令可用於檢視SPAN到CPU監控器會話速率限制器的當前設定。

```
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
```

如果複製的流量被硬體速率限制器丟棄，則Dropped列將是非零值，如下面的輸出所示：

```
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
```

可以使用**hardware rate-limiter span {kbps}全域性配置命令更改SPAN到CPU監控會話硬體速率限制器**，如下面輸出所示。

```
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
```

> **注意**：思科建議不要修改SPAN到CPU監控作業階段硬體速率限制器，使其偏離預設值50 kbps，除非思科TAC明確指示。將此速率限制器增大為高值會導致Cisco Nexus 9000系列交換機上的CPU使用率增加和控制平面不穩定，這可能會對生產流量產生重大影響。

不支援SPAN到CPU硬體速率限制器允許計數器

show hardware rate-limiter span命令的輸出包含允許計數器。在其他硬體速率限制器上，此計數器指示已成功通過硬體速率限制器的位元組數。但是，由於軟體限制，SPAN到CPU硬體速率限制器的Allowed計數器不會增加。以下輸出中顯示了此問題的示例：

```
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
```

此軟體限制會影響所有NX-OS軟體版本，並通過CSCva37512進行記錄。

要確定有多少流量被複製到配置了活動SPAN到CPU監控會話的Nexus 9000裝置的控制平面，請使用**show system internal access-list tcam ingress region span**命令。顯示相關資料包和位元組計數器的上述命令的過濾輸出示例如下所示。

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

控制平面生成的資料包不會顯示在TX SPAN到CPU的監控會話中

SPAN到CPU監控作業階段不會擷取由控制平面建立且從來源介面傳輸出去的封包。這些封包將正確輸出介面，但無法透過產生封包的同一裝置上的SPAN到CPU監控作業階段擷取。

例如，考慮一台Cisco Nexus 9000系列裝置，其中Ethernet1/1是連線到另一台路由器的L3/路由介面。OSPF進程1在Ethernet1/1上啟用，Ethernet1/1是Cisco Nexus 9000裝置上唯一由OSPF啟用的介面。

```
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
```

EtherAnalyzer控制平面封包擷取公用程式顯示裝置的控制平面每10秒產生一次OSPF Hello訊息。

```
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
```

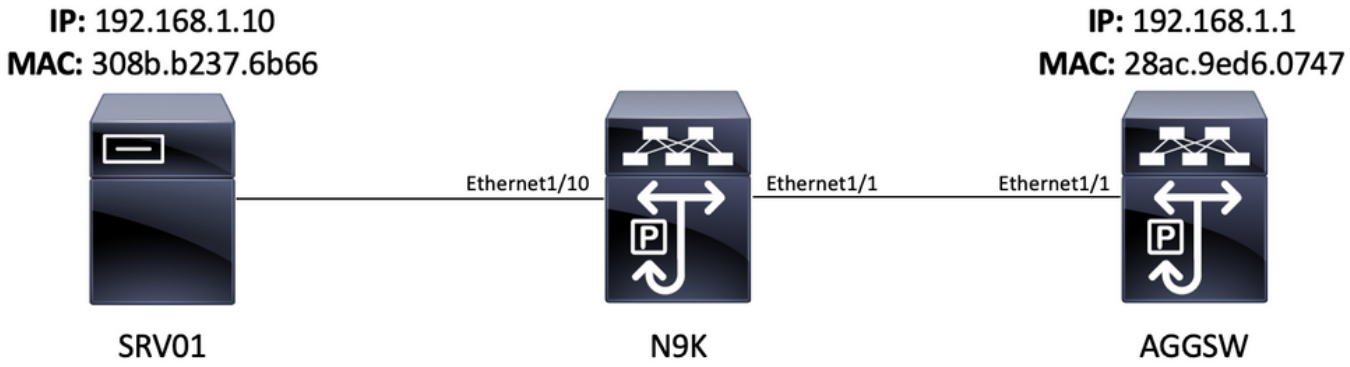
但是，Ethernet1/1介面上的輸出/TX SPAN到CPU不會顯示這些在60秒後在此介面上傳輸的開放最短路徑優先(OSPF)Hello封包。

```
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
```

為了驗證Cisco Nexus 9000裝置的控制平面生成的資料包是否從特定介面傳輸，思科建議在連線到該介面的遠端裝置上使用資料包捕獲實用程式。

Cisco Nexus 9000雲端規模SPAN到CPU的程式

請考慮以下拓撲：



源自VLAN 10中伺服器SRV01(192.168.10.10)的網際網路控制消息協定(ICMP)資料包將發往VLAN 10網關192.168.10.1。將使用SPAN到CPU的監控會話確認此ICMP資料包流經裝置N9K(運行NX-OS軟體版本9.3(3)的Cisco Nexus 93180YC-EX，充當連線第2層交換機SRV01到VLAN 10中的AGGSW。

步驟1.確認新的SPAN作業階段是否有足夠的資源

具有雲規模ASIC且運行NX-OS軟體的Cisco Nexus 9000系列交換機最多支援每個ASIC/轉發引擎四個活動SPAN或ERSPAN會話。此外，如果前三個SPAN或ERSPAN作業階段設定為雙向（TX和RX）來源介面，則第四個SPAN或ERSPAN作業階段的來源介面必須為輸入/RX來源。

設定SPAN到CPU的監控作業階段之前，請確認裝置上目前設定的其他SPAN或ERSPAN作業階段數量。可以使用**show running-config monitor**和**show monitor**命令來完成此操作。以下範例顯示裝置上未設定其他SPAN或ERSPAN作業階段時兩個命令的輸出。

```
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
```

> **附註**：有關SPAN/ERSPAN作業階段最大數量和其他限制的其他資訊，請參閱Cisco Nexus 9000系列NX-OS驗證的NX-OS軟體版本9.3(3)可擴充性指南。

步驟2.配置SPAN到CPU的監控器會話

定義SPAN到CPU監控作業階段的關鍵組態元素是「sup-eth0」的目的地介面，即Supervisor的頻內介面。以下範例顯示將Ethernet1/10的輸入/RX封包複製到Cisco Nexus 9000系列交換器的Supervisor的SPAN到CPU監控作業階段的組態。

```
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#
```

步驟3.驗證SPAN到CPU的監控器作業階段是否啟動

使用**show running-config monitor**和**show monitor**命令以驗證SPAN到CPU的監控作業階段是否已設定和運作。SPAN到CPU的監控器作業階段的設定可以透過**show running-config monitor**命令的輸出進行驗證，如下例所示。

```
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
```

可以通過**show monitor**命令的輸出驗證SPAN到CPU的監控作業階段的操作狀態。輸出應報告SPAN到CPU監控作業階段的狀態為「up」，原因為「The session is up」，如下例所示。

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

步驟4.在控制平面中檢視複製的資料包

EtherAnalyzer控制平面封包擷取公用程式可用於檢視複製到Cisco Nexus 9000裝置控制平面的流量。Ethanalyzer命令中的**mirror**關鍵字過濾流量，以便僅顯示由SPAN到CPU監控器會話複製的流量。Ethanalyzer捕獲和顯示過濾器可用於進一步限制顯示的流量。有關有用的Ethanalyzer捕獲和顯示篩選器的其他資訊，請參閱Ethanalyzer on Nexus 7000故障排除指南。請注意，雖然本文檔是針對

Cisco Nexus 7000平台編寫的，但它主要適用於Cisco Nexus 9000平台。

下面顯示使用Ethanalyzer控制平面資料包捕獲實用程式過濾由SPAN到CPU監控器會話複製的流量的示例。請注意，會使用**mirror**關鍵字以及定義源自或目的地為192.168.10.10（上述拓撲中SRV01的IP地址）的ICMP資料包的顯示過濾器。

```
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
```

附註：使用Control-C組合鍵退出Ethanalyzer控制平面資料包捕獲實用程式。

通過在Ethanalyzer命令中包含**detail**關鍵字，可以檢視有關此流量的詳細資訊。以下舉例說明單個ICMP回應請求資料包。

```
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
```

步驟5.管理性關閉SPAN到CPU的監控器會話

在SPAN到CPU監控器作業階段的上下文中使用**shut**組態命令，以正常關閉SPAN到CPU監控器作業階段，並停止將流量複製到Cisco Nexus 9000裝置的控制平面。

```
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#
```

使用**show monitor**命令驗證SPAN到CPU的監控作業階段的作業狀態。SPAN到CPU的監控作業階段的作業狀態應顯示為「down」，且原因為「Session admin shut」，如下例所示：

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

步驟6.刪除SPAN到CPU監控器會話配置（可選）

如果需要，請使用**no monitor session {id}配置命令刪除SPAN到CPU的監控**會話配置。以下輸出中顯示了此問題的示例。

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

使用**show running-config monitor**命令驗證是否已成功刪除SPAN到CPU的監控作業階段組態，如下例所示。

```
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#
```

分析SPAN到CPU的封包擷取結果

此程式的上述範例顯示，來源為192.168.10.10(SRV01)且目的地為192.168.10.1(AGGSW)的ICMP回應請求封包會進入主機名為N9K的Cisco Nexus 9000裝置的Ethernet1/10介面。這證明SRV01將此流量從其網路介面卡傳送出去。這也證明ICMP回應請求資料包在Cisco Cloud Scale ASIC轉發管道中的進展程度足以將其複製到裝置的控制平面。

但是，這並不能證明Cisco Nexus 9000裝置將ICMP回應請求資料包從Ethernet1/1轉發到AGGSW。需要執行進一步的疑難排解，以驗證封包是否從Ethernet1/1轉送到AGGSW。按可信度排序：

1.如果預期輸出介面（示例中為N9K的Ethernet1/1）的遠端裝置是帶有雲級ASIC的Cisco Nexus 9000系列裝置，則可以在遠端裝置上執行輸入/RX SPAN到CPU的監控會話（示例中為AGGSW的Eth1/1）。 如果預期輸出介面的遠端裝置不是具有雲規模ASIC的Cisco Nexus 9000系列裝置，則遠端裝置上的SPAN、埠映象或其他類似資料包捕獲是等效的。

2.在Cisco Nexus 9000裝置的輸入介面（上面的示例中為N9K的Ethernet1/10）上執行輸入/RX ELAM。有關此過程的更多資訊，請參閱Nexus 9000 Cloud Scale ASIC NX-OS ELAM故障排除技術說明。

3.在Cisco Nexus 9000裝置的輸出介面（上述示例中的N9K的Ethernet1/1）上執行輸出/TX SPAN到CPU。

相關資訊

- Cisco Nexus 9000系列NX-OS故障排除指南9.3(x)版
- Cisco Nexus 9000系列NX-OS故障排除指南9.2(x)版

- Cisco Nexus 9000系列NX-OS故障排除指南7.0(3)I7(x)版
- Nexus 7000上的Ethanalyzer故障排除指南
- Nexus 9000雲端規模ASIC(Tahoe)NX-OS ELAM