Nexus 9000云扩展ASIC NX-OS SPAN到CPU过程

目录

简介

本文档介绍在一系列Cisco Nexus 9000云扩展ASIC模块上执行交换端口分析器(SPAN)到CPU数据包捕获的步骤。本文档还介绍使用SPAN到CPU数据包捕获对通过Cisco Nexus 9000云扩展系列交换机的数据包流进行故障排除时遇到的常见警告。

背景信息

SPAN到CPU的数据包捕获使网络管理员能够快速轻松地验证特定数据包是否进出Cisco Nexus 9000云扩展系列交换机。与普通SPAN或封装远程SPAN(ERSPAN)会话类似，SPAN到CPU监控会话涉及一个或多个源接口和流量方向的定义。与源接口上定义的方向（TX、RX或两者）匹配的任何流量都会复制到Cisco Nexus 9000设备的控制平面。可以使用Ethanalyzer控制平面数据包捕获实用程序过滤和分析此复制的流量，或将其保存到本地存储设备以供以后查看。

此功能用于在排除通过Cisco Nexus 9000系列交换机的数据包流故障时临时使用。思科强烈建议在未主动用于排除数据包流问题时，SPAN到CPU监控会话会管理性关闭或删除。否则可能导致网络中复制流量的性能下降，并增加Cisco Nexus 9000系列交换机的CPU利用率。

适用硬件

本文档中介绍的过程仅适用于此硬件：

- **Nexus 9200/9300固定式交换机** 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模块化交换机线卡** N9K-X97160YC-EXN9K-X9732C-EXN9K-X9736C-EXN9K-X97284YC-FXN9K-X9732C-FXN9K-X9788TC-FXN9K-X9716D-GX

先决条件

要求

思科建议您了解Cisco Nexus 9000系列交换机上以太网交换端口分析器(SPAN)功能的基础知识。有关此功能的信息，请参阅以下文档：

- Cisco Nexus 9000系列NX-OS系统管理配置指南，版本9.3(x)
- Cisco Nexus 9000系列NX-OS系统管理配置指南，版本9.2(x)
- Cisco Nexus 9000系列NX-OS系统管理配置指南，版本7.0(3)I7(x)

使用的组件

本文档中的信息基于运行NX-OS软件版本9.3(3)的云扩展ASIC的Cisco Nexus 9000系列交换机。

本文档中的信息在特定实验室环境设备上创建。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

警告和限制

SPAN到CPU监控会话在排除数据包流故障时需要注意一些警告和限制。本文档将介绍一些常见的警告。有关指南和限制的完整列表，请参阅以下文档：

- Cisco Nexus 9000系列NX-OS系统管理配置指南，版本9.3(x)
- Cisco Nexus 9000系列NX-OS系统管理配置指南，版本9.2(x)
- Cisco Nexus 9000系列NX-OS系统管理配置指南，版本7.0(3)I7(x)

50 kbps默认硬件速率限制器

默认情况下，Cisco Nexus 9000系列交换机将通过SPAN到CPU监控会话复制到控制平面的流量速率限制为50 kbps。此速率限制在云扩展ASIC/转发引擎上执行，是一种自保护机制，可确保设备的控制平面不会被复制的流量所淹没。

show hardware rate-limiter span**命令可用于查看SPAN到CPU监控器会话速率限制器的当前设置。**

```
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
```

如果硬件速率限制器丢弃了复制的流量，则Dropped列将是非零值，如以下输出所示：

```
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
```

SPAN到CPU监控会话硬件速率限制器可以使用**硬件速率限制器span {kbps}全**局配置命令进行更改，如下面的输出所示。

```
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
```

> **警告**：除非Cisco TAC明确指示，否则思科不建议将SPAN到CPU监控器会话硬件速率限制器修改为远离其默认值50 kbps。将此速率限制器增加到高值可能导致Cisco Nexus 9000系列交换机上CPU利用率增加和控制平面不稳定，从而对生产流量产生重大影响。

不支持SPAN到CPU硬件速率限制器允许的计数器

show hardware rate-limiter span命**令的输出包**含“允许”计数器。在其他硬件速率限制器上，此计数器指示成功通过硬件速率限制器的字节数。但是，SPAN到CPU硬件速率限制器的允许计数器不会因软件限制而增加。以下输出中显示了此示例：

```
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
```

此软件限制会影响所有NX-OS软件版本，并且通过CSCva37512进行记录。

要确定已复制到配置有活动SPAN到CPU监控会话的Nexus 9000设备控制平面的流量，请使用**show system internal access-list tcam ingress region span**命令。上述命令的过滤输出示例显示相关数据包和字节计数器，如下所示。

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

控制平面生成的数据包不显示在TX SPAN到CPU监控会话中

由控制平面创建并从源接口为SPAN到CPU监控会话传输的数据包不会被SPAN到CPU监控会话捕获。这些数据包将正确出口接口，但无法通过生成数据包的同一设备上的SPAN到CPU监控会话捕获。

例如，假设Cisco Nexus 9000系列设备中Ethernet1/1是连接到另一台路由器的L3/路由接口。OSPF进程1在Ethernet1/1上激活，Ethernet1/1是Cisco Nexus 9000设备上唯一一个OSPF激活的接口。

```
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
```

Ethanalyer控制平面数据包捕获实用程序显示，OSPF Hello消息由设备的控制平面每10秒生成一次。

```
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
```

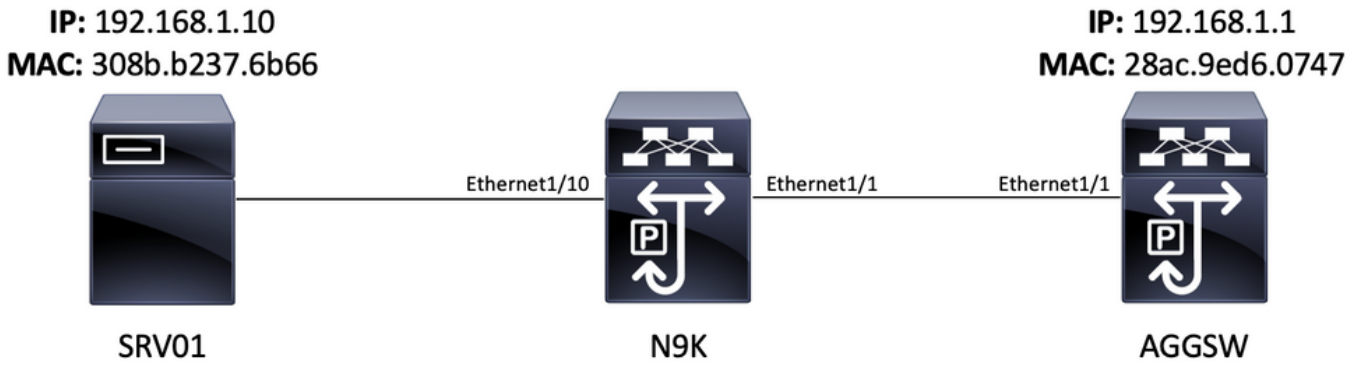
但是，Ethernet1/1接口上的出口/TX SPAN到CPU在60秒后不显示在此接口上传输的这些开放最短路径优先(OSPF)Hello数据包。

```
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
```

为了验证Cisco Nexus 9000设备的控制平面生成的数据包是否从特定接口传输出去，思科建议在连接到该接口的远程设备上使用数据包捕获实用程序。

Cisco Nexus 9000云扩展SPAN到CPU的过程

请考虑以下拓扑：



从VLAN 10(192.168.10.10)中的服务器SRV01发往VLAN 10网关192.168.10.1的Internet控制消息协议(ICMP)数据包。将使用SPAN到CPU监控器会话，以确认此ICMP数据包通过设备N9K(运行NX-OS软件版本9.3(3)的Cisco Nexus 93180YC-EX)，该设备充当将SRV01连接到VLAN 10中

AGGSW的第2层交换机。

步骤1.确认为新SPAN会话有足够的资源

运行NX-OS软件的Cisco Nexus 9000系列交换机具有云扩展ASIC，每个ASIC/转发引擎最多支持四个活动SPAN或ERSPAN会话。此外，如果前三个SPAN或ERSPAN会话配置了双向（TX和RX）源接口，则第四个SPAN或ERSPAN会话的源接口必须是入口/RX源。

在配置SPAN到CPU监控会话之前，请验证设备上当前配置的其他SPAN或ERSPAN会话的数量。这可以通过show running-config monitor**和show monitor命**令**来完**成。以下示例显示当设备上未配置其他SPAN或ERSPAN会话时两个命令的输出。

```
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
```

> **注意**：有关SPAN/ERSPAN会话最大数量和其他限制的其他信息，请参阅Cisco Nexus 9000系列NX-OS经验证的NX-OS软件版本9.3(3)的可扩展性指南。

步骤2.配置SPAN到CPU监控器会话

定义SPAN到CPU监控器会话的关键配置元素是“sup-eth0”的目标接口，该接口是管理引擎的带内接口。以下示例显示SPAN到CPU监控器会话的配置，其中Ethernet1/10的入口/RX数据包被复制到Cisco Nexus 9000系列交换机的管理引擎。

```
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#
```

步骤3.验证SPAN到CPU监控器会话是否启动

使用**show running-config monitor**和**show monitor**命令以验证SPAN到CPU监控器会话是否已配置并运行。SPAN到CPU监控器会话的配置可以通过**show running-config monitor命令**的输出进行验证，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
```

SPAN到CPU监控器会话的运行状态可以通过show monitor命令的输**出来**验证。输出应报告SPAN到CPU监控器会话的状态为“up”，原因为“The session is up”，如以下示例所示。

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

步骤4.在控制平面中查看复制的数据包

Ethanalyer控制平面数据包捕获实用程序可用于查看复制到Cisco Nexus 9000设备控制平面的流量。Ethanalyzer命令中的**mirror**关键字过滤流量，以便仅显示由SPAN到CPU监控器会话复制的流量

。Ethanalyzer捕获和显示过滤器可用于进一步限制显示的流量。有关有用的Ethanalyzer捕获和显示过滤器的其他信息，请参阅Nexus 7000 Ethanalyzer故障排除指南。请注意，本文档是为Cisco Nexus 7000平台编写的，但也大多适用于Cisco Nexus 9000平台。

以下是使用Ethanalyzer控制平面数据包捕获实用程序过滤由SPAN到CPU监控会话复制的流量的示例。请注意，使用**mirror**关键字，以及定义源自或发往192.168.10.10的ICMP数据包（前述拓扑中SRV01的IP地址）的显示过滤器。

```
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
```

注意：使用Control-C组合键退出Ethanalyzer控制平面数据包捕获实用程序。

您可以通过在Ethanalyzer命令中包含**detail**关键字来查看有关此流量的详细信息。下面显示了单个ICMP回应请求数据包的示例。

```
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: 00000000ED9E9EB9ABCDABCDABCDABCDABCDABCDABCDABCD...
[Length: 72] ^C 1 packet captured
```

步骤5.管理性关闭SPAN到CPU监控器会话

在SPAN到CPU监控器会话的上下文中使用**shut** 配置命令以平稳关闭SPAN到CPU监控器会话并停止将流量复制到Cisco Nexus 9000设备的控制平面。

```
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命令验证SPAN到CPU监控器会话的**运行状态**。SPAN到CPU监控器会话的运行状态应显示为“关闭”，原因为“会话管理员关闭”，如下例所示：

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

步骤6.删除SPAN到CPU监控器会话配置（可选）

如果需要，请使用no monitor session {id}配置命令删除SPAN**到CPU监控器会话**配置。以下输出中显示了此示例。

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

如以下示例所示，使用**show running-config monitor**命令验证SPAN到CPU监控器会话配置是否已成功删除。

```
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数据包捕获的结果

此过程的上述示例显示，从192.168.10.10(SRV01)发往192.168.10.1(AGGSW)的ICMP回应请求数据包从Cisco Nexus 9000设备的Ethernet1/10接口进入，主机名为N9K。这证明SRV01将此流量从其网络接口卡发送出去。这也证明ICMP回应请求数据包已经进入思科云扩展ASIC的转发管道，以便其复制到设备的控制平面。

但是，这并不能证明Cisco Nexus 9000设备将ICMP回应请求数据包从Ethernet1/1转发到AGGSW。需要执行进一步的故障排除，以验证数据包是否从Ethernet1/1转发到AGGSW。按可信度排序：

1.如果预期出口接口的远程设备（本例中为N9K的Ethernet1/1）是带云扩展ASIC的Cisco Nexus 9000系列设备，则可以在远程设备上执行入口/RX SPAN到CPU监控会话（本例中为AGGSW的Eth1/1）。 如果预期出口接口的远程设备不是具有云扩展ASIC的Cisco Nexus 9000系列设备，则远程设备上的SPAN、端口镜像或其他类似数据包捕获是等效的。

2.在Cisco Nexus 9000设备的入口接口（上例中为N9K的以太网接口1/10）上执行入口/RX ELAM。有关此过程的其他信息，请参阅Nexus 9000云扩展ASIC NX-OS ELAM故障排除技术说明。

3.在Cisco Nexus 9000设备的出口接口（上例中为N9K的以太网接口1/1）上执行出口/TX SPAN到CPU。

相关信息

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

- Cisco Nexus 9000系列NX-OS故障排除指南，版本7.0(3)I7(x)
- Ethanalyzer on Nexus 7000故障排除指南
- Nexus 9000云扩展ASIC(Tahoe)NX-OS ELAM