

Procedimento de SPAN para CPU do Nexus 9000 Cloud Scale ASIC NX-OS

Contents

[Introduction](#)

[Informações de Apoio](#)

[Hardware aplicável](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Caveats e limitações](#)

[Limitador de taxa de hardware padrão de 50 kbps](#)

[O contador permitido de limite de taxa de hardware de SPAN para CPU não é suportado](#)

[Os pacotes gerados pelo plano de controle não aparecem nas sessões do monitor TX SPAN-para-CPU](#)

[Procedimento de SPAN para CPU do Cisco Nexus 9000 Cloud Scale](#)

[Etapa 1. Confirme os recursos suficientes para a nova sessão de SPAN](#)

[Etapa 2. Configurar sessão de monitoramento de SPAN para CPU](#)

[Etapa 3. Verifique se a sessão do monitor de SPAN para CPU está ativa](#)

[Etapa 4. Exibir pacotes replicados no plano de controle](#)

[Etapa 5. Desligar administrativamente a sessão do monitor SPAN-CPU](#)

[Etapa 6. Remova a configuração da sessão do monitor de SPAN para CPU \(opcional\)](#)

[Analisar os resultados de uma captura de pacote de SPAN para CPU](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve as etapas usadas para executar uma captura de pacote SPAN (Switched Port Analyzer) para CPU em uma série de módulos ASIC de escala de nuvem Cisco Nexus 9000. Este documento também descreve as advertências comuns encontradas ao usar uma captura de pacote de SPAN para CPU para solucionar problemas de fluxo de pacotes através de um switch da série Cisco Nexus 9000 Cloud Scale.

Informações de Apoio

Uma captura de pacote de SPAN para CPU permite que os administradores de rede validem rápida e facilmente se pacotes específicos entram e saem de um switch da série Cisco Nexus 9000 Cloud Scale. Da mesma forma que uma sessão normal de SPAN ou de SPAN Remoto Encapsulado (ERSPAN - Encapsulated Remote SPAN), uma sessão de monitoramento de SPAN para CPU envolve a definição de uma ou mais interfaces de origem e direções de tráfego. Qualquer tráfego que corresponda à direção (TX, RX ou ambos) definida em uma interface de origem é replicado para o plano de controle do dispositivo Cisco Nexus 9000. Esse tráfego replicado pode ser filtrado e analisado com o uso do [utilitário de captura de pacotes do plano de controle do Ethalyzer](#) ou salvo em um dispositivo de armazenamento local para revisão

posterior.

Este recurso é destinado ao uso temporário durante a solução de problemas de fluxo de pacotes através dos switches Cisco Nexus 9000 Series. A Cisco recomenda enfaticamente que as sessões de monitoramento de SPAN para CPU sejam desligadas ou removidas administrativamente quando não forem usadas ativamente para solucionar um problema de fluxo de pacote. Se isso não for feito, poderá ocorrer degradação do desempenho do tráfego replicado na rede e maior utilização da CPU do switch Cisco Nexus 9000 Series.

Hardware aplicável

O procedimento abordado neste documento é aplicável somente a este hardware:

- **Switches fixos Nexus 9200/9300** N9K-C92160YC-XN9K-C92300YCN9K-C92304QCN9K-C92348GC-XN9K-C9236CN9K-C9272QN9K-C933CN9K-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-C933C-FX2N9K-C933C-FX2-EN9K-C93360YC-FX2N9K-C93180YC-FX3N9K-C93108TC-FX3PN9K-C93180YC-FX3SN9K-C9316D-GXN9K-C93600CD-GXN9K-C9364C-GXN9K-C9364D-GX2AN9K-C9332D-GX2B
- **Placas de linha de switch modular Nexus 9500** N9K-X97160YC-EXN9K-X9732C-EXN9K-X9736C-EXN9K-X97284YC-FXN9K-X9732C-FXN9K-X9788TC-FXN9K-X9716D-GX

Prerequisites

Requirements

A Cisco recomenda que você compreenda os conceitos básicos do recurso do Analisador de porta comutada Ethernet (SPAN - Ethernet Switched Port Analyzer) nos switches Cisco Nexus 9000 Series. Para obter informações sobre esse recurso, consulte os seguintes documentos:

- [Guia de configuração de gerenciamento do sistema NX-OS do Cisco Nexus 9000 Series, versão 9.3\(x\)](#)
- [Guia de configuração de gerenciamento do sistema NX-OS do Cisco Nexus 9000 Series, versão 9.2\(x\)](#)
- [Guia de configuração de gerenciamento do sistema NX-OS do Cisco Nexus 9000 Series, versão 7.0\(3\)I7\(x\)](#)

Componentes Utilizados

As informações neste documento são baseadas nos switches Cisco Nexus 9000 Series com o ASIC Cloud Scale executando o software NX-OS versão 9.3(3).

As informações apresentadas neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

para um alto valor pode causar maior utilização da CPU e instabilidade do plano de controle no switch Cisco Nexus 9000 Series, o que pode causar um impacto significativo no tráfego de produção.

O contador permitido de limite de taxa de hardware de SPAN para CPU não é suportado

A saída do comando **show hardware rate-limiter span** contém um contador Permitido. Em outros limitadores de taxa de hardware, este contador indica quantos bytes passaram com êxito pelo limitador de taxa de hardware. No entanto, o contador Permitido para o limitador de taxa de hardware SPAN-CPU não aumenta devido a uma limitação de software. Um exemplo disso é mostrado na saída abaixo:

```
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	

Essa limitação de software afeta todas as versões do software NX-OS e é documentada através do [CSCva37512](#).

Para determinar quanto tráfego foi replicado para o plano de controle de um dispositivo Nexus 9000 configurado com uma sessão de monitoramento SPAN-para-CPU ativa, use o comando **show system internal access-list tcam ingress region span**. Um exemplo da saída filtrada do comando acima que mostra contadores de pacotes e bytes relevantes é mostrado abaixo.

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

Os pacotes gerados pelo plano de controle não aparecem nas sessões do monitor TX SPAN-para-CPU

Os pacotes criados pelo plano de controle e transmitidos de uma interface de origem para uma sessão de monitor de SPAN para CPU não serão capturados pela sessão de monitor de SPAN para CPU. Esses pacotes sairão da interface corretamente, mas não podem ser capturados por meio de uma sessão de monitoramento de SPAN para CPU no mesmo dispositivo onde o pacote é gerado.

Por exemplo, considere um dispositivo Cisco Nexus 9000 Series em que Ethernet1/1 é uma interface L3/roteada conectada a outro roteador. O processo 1 do OSPF é ativado na Ethernet1/1, que é a única interface ativada pelo OSPF no 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
```

O [utilitário de captura de pacotes do plano de controle Ethalyzer](#) mostra que as mensagens de saudação do OSPF são geradas pelo plano de controle do dispositivo uma vez a cada 10 segundos.

```
N9K# ethalyzer 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
```

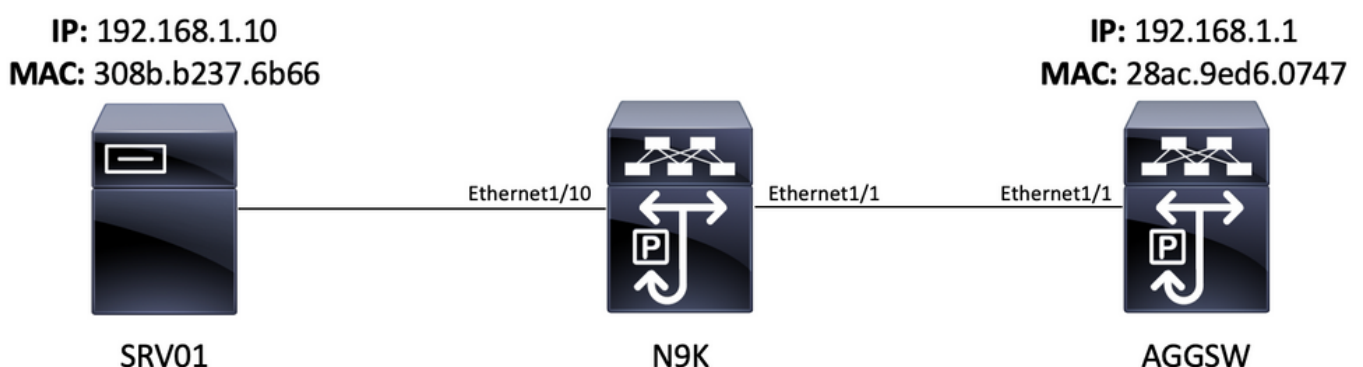
No entanto, um SPAN-para-CPU de saída/TX na interface Ethernet1/1 não mostra esses pacotes Hello do OSPF (Open Shortest Path First) transmitidos nessa interface após 60 segundos de tempo.

```
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
```

Para verificar se os pacotes gerados pelo plano de controle de um dispositivo Cisco Nexus 9000 são transmitidos a partir de uma interface específica, a Cisco recomenda o uso de um utilitário de captura de pacotes no dispositivo remoto conectado à interface.

Procedimento de SPAN para CPU do Cisco Nexus 9000 Cloud Scale

Considere a seguinte topologia:



Um pacote ICMP (Internet Control Message Protocol) originado do servidor SRV01 na VLAN 10 (192.168.10.10) destina-se ao gateway 192.168.10.1 da VLAN 10. Uma sessão de monitor SPAN-CPU será usada para confirmar que esse pacote ICMP atravessa o dispositivo N9K (um Cisco Nexus 93180YC-EX que executa o software NX-OS versão 9.3(3)), que atua como um switch de Camada 2 que conecta o SRV01 ao AGGSW na VLAN 10.

Etapa 1. Confirme os recursos suficientes para a nova sessão de SPAN

Os switches Cisco Nexus 9000 Series com o ASIC de escala de nuvem que executam o software

NX-OS suportam um máximo de quatro sessões de SPAN ou ERSPAN ativas por mecanismo ASIC/forwarding. Além disso, se as três primeiras sessões de SPAN ou ERSPAN forem configuradas com interfaces de origem bidirecional (TX e RX), a interface de origem da quarta sessão de SPAN ou ERSPAN deve ser uma origem de entrada/RX.

Antes de configurar uma sessão de monitoramento de SPAN para CPU, verifique a quantidade de outras sessões de SPAN ou ERSPAN configuradas atualmente no dispositivo. Isso pode ser feito com os comandos **show running-config monitor** e **show monitor**. O exemplo abaixo mostra a saída de ambos os comandos quando nenhuma outra sessão de SPAN ou ERSPAN está configurada no dispositivo.

```
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
```

Note: Informações adicionais sobre o número máximo de sessões de SPAN/ERSPAN e outras limitações podem ser encontradas no [Cisco Nexus 9000 Series NX-OS Verified Scalability Guide for NX-OS Software Release 9.3\(3\)](#).

Etapa 2. Configurar sessão de monitoramento de SPAN para CPU

O elemento-chave de configuração que define uma sessão de monitoramento de SPAN para CPU é uma interface de destino de "sup-eth0", que é a interface inband do supervisor. O exemplo abaixo mostra a configuração de uma sessão de monitoramento de SPAN para CPU onde os pacotes de entrada/RX de Ethernet1/10 são replicados para o supervisor do switch Cisco Nexus 9000 Series.

```
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#
```

Etapa 3. Verifique se a sessão do monitor de SPAN para CPU está ativa

Use os comandos **show running-config monitor** e **show monitor** para verificar se a sessão do monitor SPAN-CPU está configurada e operacional. A configuração da sessão do monitor SPAN-CPU pode ser verificada através da saída do comando **show running-config monitor**, como mostrado no exemplo abaixo.

```
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
```

O estado operacional da sessão de monitoramento de SPAN para CPU pode ser verificado através da saída do comando **show monitor**. A saída deve relatar que o estado da sessão do monitor SPAN-CPU está "ativado" com um motivo de "A sessão está ativa", como mostrado no exemplo abaixo.

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

Etapa 4. Exibir pacotes replicados no plano de controle

O [utilitário de captura de pacotes do plano de controle Ethalyzer](#) pode ser usado para visualizar o tráfego replicado no plano de controle do dispositivo Cisco Nexus 9000. A palavra-chave **mirror** no comando Ethalyzer filtra o tráfego de modo que somente o tráfego replicado por uma sessão de monitoramento de SPAN para CPU é mostrado. Os filtros de captura e exibição do analisador de eventos podem ser usados para limitar ainda mais o tráfego exibido. Informações adicionais sobre filtros úteis de captura e exibição do Ethalyzer podem ser encontradas no [Ethalyzer on Nexus 7000 Troubleshooting Guide](#). Observe que, embora este documento tenha sido escrito para a plataforma Cisco Nexus 7000, ele também se aplica principalmente à plataforma Cisco Nexus 9000.

Um exemplo do uso do utilitário de captura de pacotes do plano de controle do Ethalyzer para filtrar o tráfego replicado por uma sessão de monitoramento de SPAN para CPU é mostrado abaixo. Observe que a palavra-chave **mirror** é usada, assim como um filtro de exibição que define os pacotes ICMP originados ou destinados a 192.168.10.10 (o endereço IP do SRV01 na topologia mencionada acima).

```
N9K# ethalyzer 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
```

Note: Use a combinação de teclas Control-C para sair do utilitário de captura de pacotes do plano de controle do Ethalyzer.

É possível visualizar informações detalhadas sobre esse tráfego incluindo a palavra-chave **detail** no comando Ethalyzer. Um exemplo disso para um único pacote ICMP Echo Request é mostrado abaixo.

```
N9K# ethalyzer 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 : 0xfled [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

```

Etapa 5. Desligar administrativamente a sessão do monitor SPAN-CPU

Use o comando **shut configuration** no contexto da sessão de monitoramento SPAN-CPU para desligar a sessão de monitoramento SPAN-CPU e parar de replicar o tráfego para o plano de controle do 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#

```

Verifique o estado operacional da sessão de monitoramento de SPAN para CPU com o comando **show monitor**. O estado operacional da sessão de monitoramento de SPAN para CPU deve ser mostrado como "inoperante" com um motivo de "administrador da sessão desligado", como mostrado no exemplo abaixo:

```

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

```

Etapa 6. Remova a configuração da sessão do monitor de SPAN para CPU (opcional)

Se desejar, remova a configuração da sessão do monitor SPAN-CPU com o comando de configuração no **monitor session {id}**. Um exemplo disso é mostrado na saída abaixo.

```

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

```

Verifique se a configuração da sessão do monitor SPAN-CPU foi removida com êxito com o comando **show running-config monitor**, como mostrado no exemplo abaixo.

```

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#

```

Analisar os resultados de uma captura de pacote de SPAN para CPU

O exemplo acima deste procedimento mostra que os pacotes ICMP Echo Request originados de 192.168.10.10 (SRV01) destinados a 192.168.10.1 (AGGSW) ingressam na interface Ethernet1/10 do dispositivo Cisco Nexus 9000 com um nome de host N9K. Isso prova que o SRV01 envia esse tráfego para fora da placa de interface de rede. Isso também prova que o pacote ICMP Echo Request progride bastante no pipeline de encaminhamento do Cisco Cloud Scale ASIC para ser replicado no plano de controle do dispositivo.

No entanto, isso não prova que o dispositivo Cisco Nexus 9000 encaminha o pacote ICMP Echo Request da Ethernet1/1 para a AGGSW. É necessário executar mais Troubleshooting para validar se o pacote é encaminhado da Ethernet1/1 para a AGGSW. Por ordem de fiabilidade:

1. Se o dispositivo remoto da interface de saída esperada (Ethernet1/1 de N9K no exemplo) for um dispositivo Cisco Nexus 9000 Series com um ASIC de escala de nuvem, você poderá executar uma sessão de monitoramento de SPAN para CPU de entrada/RX no dispositivo remoto (Eth1/1 de AGGSW no exemplo anterior). Se o dispositivo remoto da interface de saída esperada não for um dispositivo Cisco Nexus 9000 Series com um ASIC de escala de nuvem, então um SPAN, espelho de porta ou outra captura de pacote semelhante no dispositivo remoto é equivalente.
2. Execute um ELAM de entrada/RX na interface de entrada (Ethernet1/10 de N9K no exemplo acima) do dispositivo Cisco Nexus 9000. Informações adicionais sobre esse procedimento podem ser encontradas no [Nexus 9000 Cloud Scale ASIC NX-OS ELAM Troubleshooting TechNote](#).
3. Execute um SPAN para CPU de saída/TX na interface de saída do dispositivo Cisco Nexus 9000 (Ethernet1/1 de N9K no exemplo acima).

Informações Relacionadas

- [Guia de solução de problemas do Cisco Nexus 9000 Series NX-OS, versão 9.3\(x\)](#)
- [Guia de solução de problemas do Cisco Nexus 9000 Series NX-OS, versão 9.2\(x\)](#)
- [Guia de solução de problemas do Cisco Nexus 9000 Series NX-OS, versão 7.0\(3\)I7\(x\)](#)
- [Guia de solução de problemas do Ethalyzer no Nexus 7000](#)
- [Nexus 9000 Cloud Scale ASIC \(Tahoe\) NX-OS ELAM](#)