Solucione problemas de quedas de pacotes com ACLs na plataforma Nexus

Contents

Introdução

Este documento descreve como solucionar problemas de perda de pacotes usando Listas de Controle de Acesso (ACLs) na plataforma Nexus.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

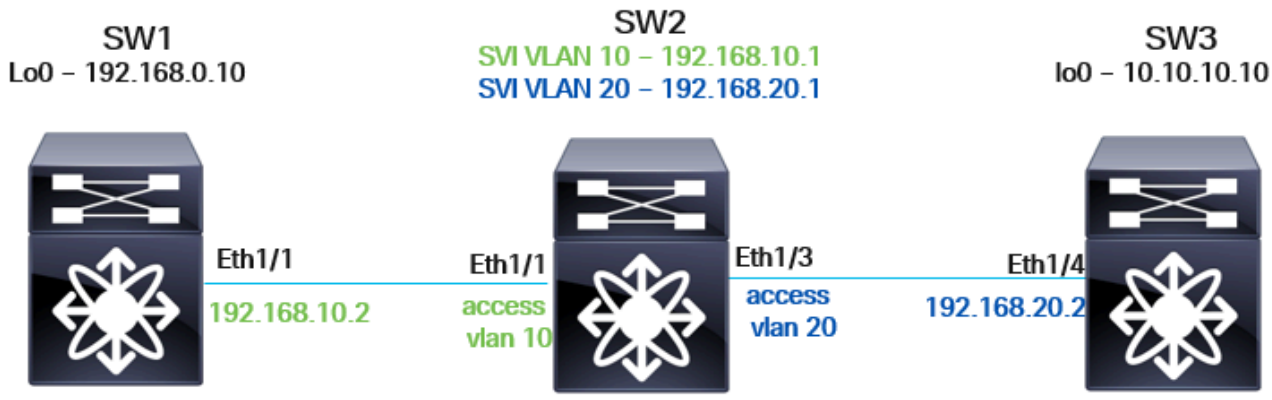
- Plataforma NXOS
- Listas de controle de acesso

Componente usado

N9K1	N9K-C93108TC-EX	9.3(10)
N9K2	N9K-C93108TC-EX	9.3(10)
N9K3	N9K-C93108TC-EX	9.3(10)

As informações neste documento foram criadas a partir de dispositivos Nexus em um ambiente de laboratório. Todos os dispositivos usados neste documento foram iniciados sem nenhuma configuração preexistente. Se você estiver usando uma rede ativa, certifique-se de entender o impacto potencial de qualquer comando.

Topologia



Breve Visão Geral das Listas de Controle de Acesso e suas Funcionalidades

Uma ACL é usada essencialmente para filtrar o tráfego com base em uma série de regras e critérios ordenados (por exemplo, filtragem com base nos endereços IP de origem/destino). Essas regras determinam se os pacotes correspondem a condições específicas para decidir se devem ser permitidos ou recusados. Em termos mais simples, a ACL define se os pacotes de rede podem passar ou ser recusados com base nas regras definidas dentro dela. Se os pacotes atenderem às condições das regras de permissão, serão processados pelo switch Nexus. Por outro lado, se os pacotes corresponderem às condições de negação, eles serão descartados.

Um recurso importante das ACLs é sua capacidade de fornecer contadores estatísticos para o fluxo de pacotes. Esses contadores rastreiam o número de pacotes que correspondem às regras

da ACL, o que pode ser muito útil ao solucionar problemas de cenários de perda de pacotes.

Por exemplo, se um dispositivo estiver enviando um determinado número de pacotes, mas recebendo menos do que o esperado, os contadores estatísticos da ACL podem ajudar a isolar o ponto em que os pacotes estão sendo descartados dentro da rede.

PACL e RACL

A implementação das ACLs pode variar dependendo se elas são aplicadas às interfaces de Camada 2 (PACL), interfaces de Camada 3 (RACL) ou VLANs (VACL). Aqui está uma breve comparação desses métodos:

- Lista de Controle de Acesso à Porta (PACL): A ACL é aplicada a uma interface switchport de Camada 2 (L2).
- Lista de Controle de Acesso (RACL - Access Control List) do Roteador: A ACL é aplicada a uma interface roteada de Camada 3 (L3).

Tipo de ACL	Interface	Ação	Direção Aplicada
PACL	L2	Interfaces de porta de switch Se a ACL for aplicada a uma interface de tronco, ela filtrará o tráfego para todas as VLANs permitidas no tronco.	Somente entrada - o tráfego que entra na interface.
RACL	L3	Subinterfaces SVI, L3 física e L3	Entrada e saída - A entrada filtra o tráfego que entra na interface, enquanto a saída filtra o tráfego que sai da interface.

Objetivo

É necessário confirmar que todos os pacotes que estão sendo enviados foram recebidos corretamente.

Explicação de Topologia

- O N9K-1 tem conectividade L3 com o N9K-2. A interface Eth1/1 no N9K-1 é configurada como uma interface roteada L3, enquanto o Eth1/1 do N9K-2 é uma interface switchport L2,

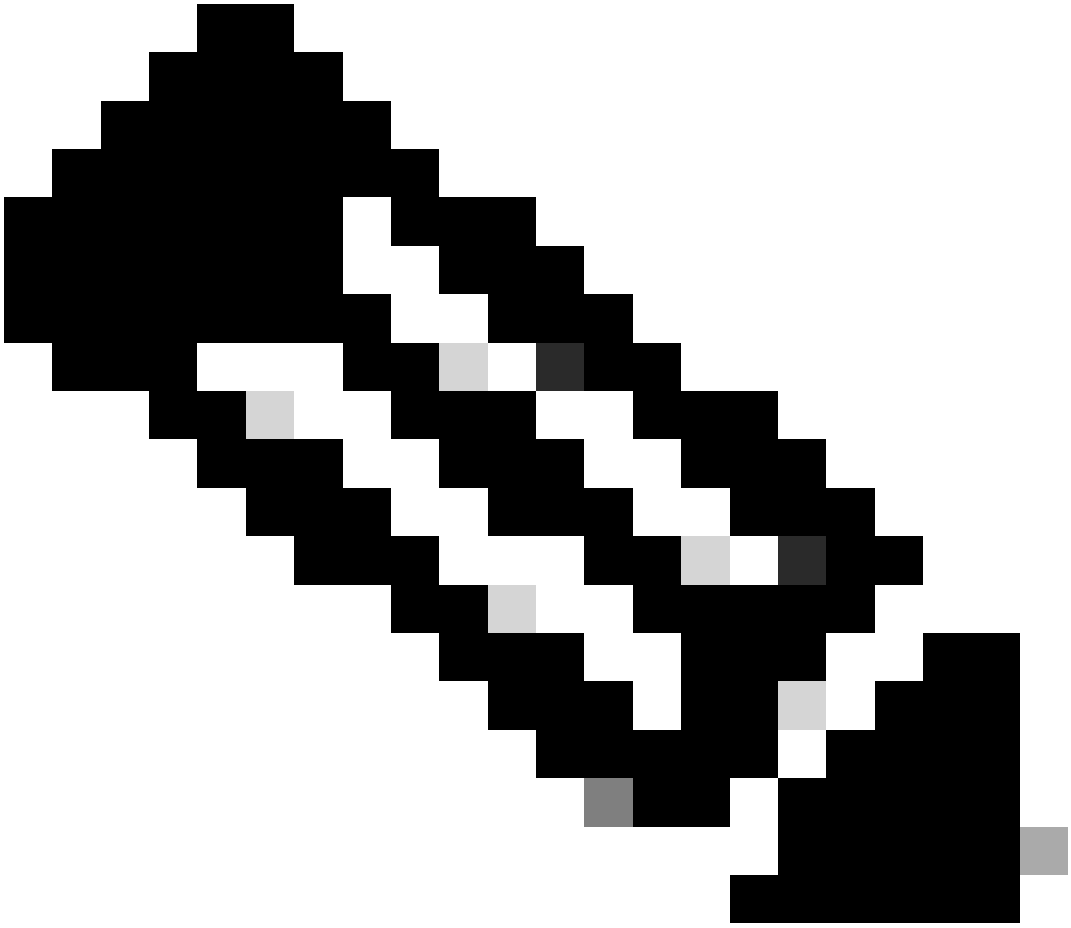
marcada com a VLAN 10.

- O N9K-2 também tem conectividade L3 com o N9K-3. A interface Eth1/3 no N9K-2 é uma interface de switchport L2 marcada com a VLAN 20 e a Eth1/4 do N9K-3 é configurada como uma interface roteada L3.
- Configuração de loopback: Tanto N9K-1 como N9K-2 têm a interface Lo0 configurada. Essas interfaces Lo0 devem ser usadas para enviar pacotes de ping ICMP entre os dois dispositivos.

Troubleshooting

Veja as etapas detalhadas do processo para configurar e verificar o RACL e o PACL nos dispositivos N9K. Durante esse processo, as Listas de Controle de Acesso à Porta e as Listas de Controle de Acesso ao Roteador são analisadas para analisar o fluxo de pacotes e determinar se todos os pacotes estão sendo transmitidos e recebidos corretamente.

Etapa 1. Configurar o RACL nas interfaces L3 de N9K-1 (Eth1/1), N9K-2 (SVI 10, SVI 20) e N9K-3 (Eth1/14)



Note: Para observar o fluxo do pacote de saída, é necessária uma configuração adicional da ACL no N9K-2. Como o N9K-2 não tem interfaces físicas roteadas de L3 (em vez disso, tem interfaces de switchport de SVI e L2), o PACL suporta apenas o tráfego de entrada.

Para capturar correspondências de pacotes de saída, uma nova ACL pode ser criada e aplicada às interfaces L3.

A ACL deve ser aplicada a N9K-1, N9K-2 e N9K-3.

```
ip access-list TAC-IN
statistics per-entry
10 permit ip 192.168.20.2/32 192.168.0.10/32
20 permit ip 192.168.0.10/32 192.168.20.2/32
30 permit ip any any


ip access-list TAC-OUT
```

```
statistics per-entry
10 permit ip 192.168.20.2/32 192.168.0.10/32
20 permit ip 192.168.0.10/32 192.168.20.2/32
30 permit ip any any


***N9K-1***
interface Ethernet1/1
description ***Link-to-N9K-2***
ip access-group TAC-IN in
ip access-group TAC-OUT out
ip address 192.168.10.2/30
no shutdown



***N9K-2***

interface Vlan10
no shutdown
ip access-group TAC-IN-SVI in
ip access-group TAC-OUT-SVI out
ip address 192.168.10.1/30

interface Vlan20
no shutdown
ip access-group TAC-IN-SVI in
ip access-group TAC-OUT-SVI out
ip address 192.168.20.1/30

***N9K-3***

interface Ethernet1/4
description ***Link-to-N9K-2***
ip access-group TAC-IN in
ip access-group TAC-OUT out
ip address 192.168.20.2/30
no shutdown
```

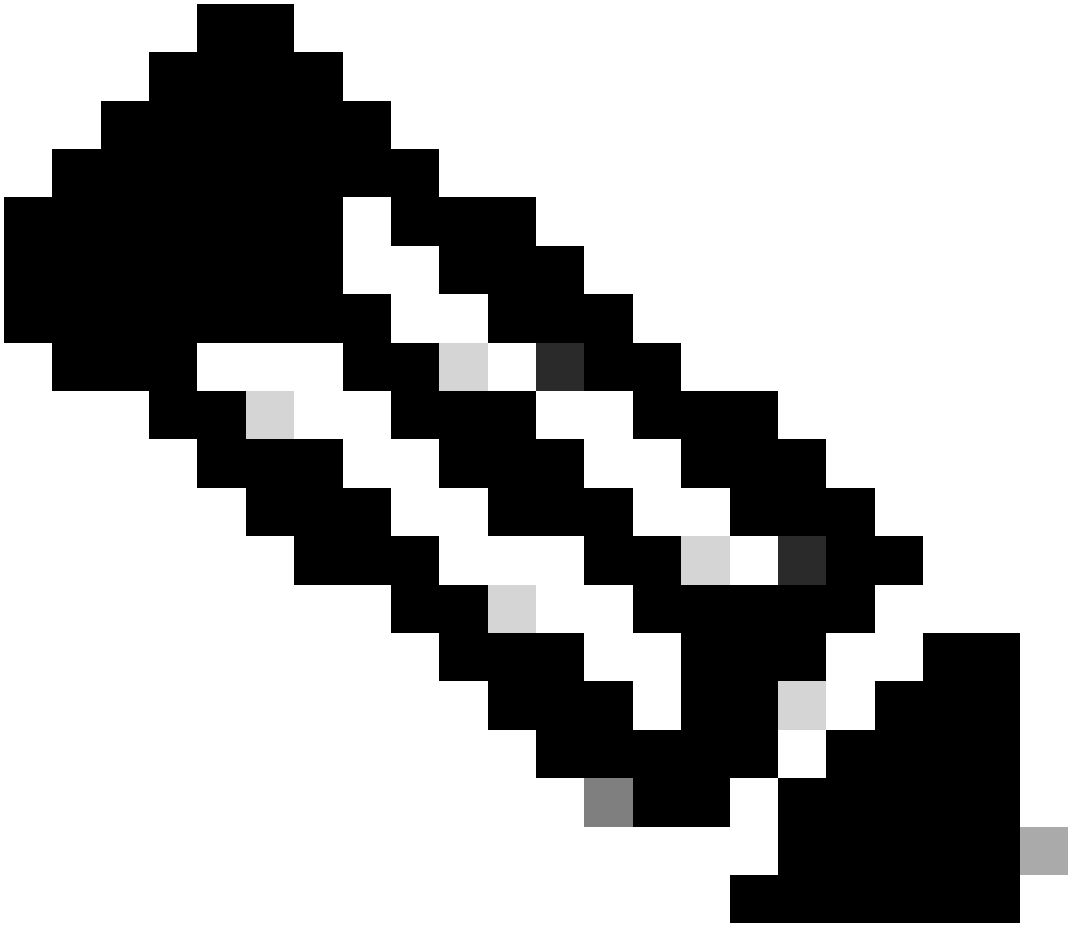
Etapa 2. Configurar PACL nas interfaces L2 Switchport de N9K-2

TCAM Carving

A gravação TCAM pode ser necessária dependendo do tipo de ACL. Para obter mais informações, consulte:

[Entenda como dividir o espaço do TCAM do Nexus 9000]

Para aplicar o PACL às interfaces físicas da L2, é necessário configurar um grupo de acesso de porta ip ....
No entanto, a configuração da região TCAM também é necessária.



Note: Determinadas linhas foram removidas para manter a saída limpa.

```
N9K-C93180YC-2# conf
Enter configuration commands, one per line. End with CNTL/Z.
N9K-C93180YC-2(config)# int e1/2
N9K-C93180YC-2(config-if)# ip port access-group TAC-IN in
ERROR: TCAM region is not configured. Please configure TCAM region Ingress PACL [ing-ifacl] and retry t
N9K-C93180YC-2(config-if)#
```

Procedimento para configurar a região TCAM

Etapa 1. Modificações na Região TCAM

Avalie qual região pode fornecer espaço livre, pois isso pode diferir para cada ambiente.

```
N9K-C93180YC-2# show system internal access-list globals

slot 1
=======




LOU Threshold Value : 5

------------------------------------------------------------------------------------
INSTANCE 0 TCAM Region Information:
------------------------------------------------------------------------------------
Ingress:
--------
Region TID Base Size Width
------------------------------------------------------------------------------------
NAT 13 0 0 1
Ingress PACL 1 0 0 1 >>>>>>> Size of 0
Ingress VACL 2 0 0 1
Ingress RACL 3 0 1792 1
Ingress RBACL 4 0 0 1
Ingress L2 QOS 5 1792 256 1
Ingress L3/VLAN QOS 6 2048 512 1 >>>>>> Size of 512
Ingress SUP 7 2560 512 1
Ingress L2 SPAN ACL 8 3072 256 1
Ingress L3/VLAN SPAN ACL 9 3328 256 1
Ingress FSTAT 10 0 0 1
SPAN 12 3584 512 1
Ingress REDIRECT 14 0 0 1
Ingress NBM 30 0 0 1
Ingress Flow-redirect 39 0 0 1
Ingress RACL Lite 42 0 0 1
Ingress PACL IPv4 Lite 41 0 0 1
Ingress PACL IPv6 Lite 43 0 0 1
Ingress CNTACL 44 0 0 1
Mcast NAT 46 0 0 1
Ingress DACL 47 0 0 1
Ingress PACL Super Bridge 49 0 0 1
Ingress Storm Control 50 0 0 1
Ingress VACL Redirect 51 0 0 1
Egress Netflow L3 56 0 0 1
55 0 0 1
------------------------------------------------------------------------------------
Total configured size: 4096
Remaining free size: 0
Note: Ingress SUP region includes Redirect region
```

Um método alternativo de verificação.

```
N9K-C93180YC-2# sh hardware access-list tcam region
NAT ACL[nat] size = 0
Ingress PACL [ing-ifacl] size = 0 >>>>>>> Size of 0
VACL [vacl] size = 0
Ingress RACL [ing-racl] size = 1792
Ingress L2 QOS [ing-l2-qos] size = 256
Ingress L3/VLAN QOS [ing-l3-vlan-qos] size = 512 >>>>>> Size of 512
Ingress SUP [ing-sup] size = 512
Ingress L2 SPAN filter [ing-l2-span-filter] size = 256
Ingress L3 SPAN filter [ing-l3-span-filter] size = 256
Ingress FSTAT [ing-fstat] size = 0
span [span] size = 512
Egress RACL [egr-racl] size = 1792
Egress SUP [egr-sup] size = 256
Ingress Redirect [ing-redirect] size = 0
Egress L2 QOS [egr-l2-qos] size = 0
Egress L3/VLAN QOS [egr-l3-vlan-qos] size = 0
Ingress Netflow/Analytics [ing-netflow] size = 0
Ingress NBM [ing-nbm] size = 0
TCP NAT ACL[tcp-nat] size = 0
Egress sup control plane[egr-copp] size = 0
Ingress Flow Redirect [ing-flow-redirect] size = 0
Ingress CNTACL [ing-cntacl] size = 0
Egress CNTACL [egr-cntacl] size = 0
MCAST NAT ACL[mcast-nat] size = 0
Ingress DACL [ing-dacl] size = 0
Ingress PACL Super Bridge [ing-pacl-sb] size = 0
Ingress Storm Control [ing-storm-control] size = 0
Ingress VACL redirect [ing-vacl-nh] size = 0
Egress PACL [egr-ifacl] size = 0
Egress Netflow [egr-netflow] size = 0
N9K-C93180YC-2#
```

Etapa 2. Reduzir o Tamanho da Região

Reduza o tamanho da região alocada para ing-l3-vlan-qos. (Isso difere para cada ambiente.)

N9K-C93180YC-2(config)# hardware access-list tcam region ing-l3-vlan-qos 256 **>>>** Reduza a alocação de 512 para 256.
Salve a configuração e recarregue o sistema para que a configuração entre em vigor.

Etapa 3. Aumentar a região TCAM para ing-ifacl

N9K-C93180YC-2(config)# hardware access-list tcam region ing-ifacl 256

Salve a configuração e recarregue o sistema para que a configuração entre em vigor.

N9K-C93180YC-2(config)#

Etapa 4. Salvar configuração

```
N9K-C93180YC-2(config)# copy running-config startup-config
[########################################] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.
N9K-C93180YC-2(config)#
```

Etapa 5. Recarregar

```
N9K-C93180YC-2(config)# reload
This command will reboot the system. (y/n)? [n] y
```

Verificação pós-recarregamento

Após recarregar, verifique se as alterações foram aplicadas.

```
N9K-C93180YC-2# sh system internal access-list globals

slot 1
=======


----------------------------------------------------------------------------------
INSTANCE 0 TCAM Region Information:
----------------------------------------------------------------------------------
Ingress:
--------
Region TID Base Size Width
----------------------------------------------------------------------------------
NAT 13 0 0 1
Ingress PACL 1 0 256 1 >>> The size value is now 256.
Ingress VACL 2 0 0 1
Ingress RACL 3 256 1792 1
Ingress RBACL 4 0 0 1
Ingress L2 QOS 5 2048 256 1
Ingress L3/VLAN QOS 6 2304 256 1 >>> The size value is now 256.
```

```
Ingress SUP 7 2560 512 1
Ingress L2 SPAN ACL 8 3072 256 1
Ingress L3/VLAN SPAN ACL 9 3328 256 1
Ingress FSTAT 10 0 0 1
SPAN 12 3584 512 1
Ingress REDIRECT 14 0 0 1
Ingress NBM 30 0 0 1
Ingress Flow-redirect 39 0 0 1
Ingress RACL Lite 42 0 0 1
Ingress PACL IPv4 Lite 41 0 0 1
Ingress PACL IPv6 Lite 43 0 0 1
Ingress CNTACL 44 0 0 1
Mcast NAT 46 0 0 1
Ingress DACL 47 0 0 1
Ingress PACL Super Bridge 49 0 0 1
Ingress Storm Control 50 0 0 1
Ingress VACL Redirect 51 0 0 1
Egress Netflow L3 56 0 0 1
55 0 0 1
------------------------------------------------------------------------------
Total configured size: 4096
Remaining free size: 0
Note: Ingress SUP region includes Redirect region
```

Um método alternativo de verificação.

```
N9K-C93180YC-2# sh hardware access-list tcam region
NAT ACL[nat] size = 0
Ingress PACL [ing-ifacl] size = 256 >>> The size value is now 256.
VACL [vacl] size = 0
Ingress RACL [ing-racl] size = 1792
Ingress L2 QOS [ing-l2-qos] size = 256
Ingress L3/VLAN QOS [ing-l3-vlan-qos] size = 256 >>> The size value is now 256.
Ingress SUP [ing-sup] size = 512
Ingress L2 SPAN filter [ing-l2-span-filter] size = 256
Ingress L3 SPAN filter [ing-l3-span-filter] size = 256
Ingress FSTAT [ing-fstat] size = 0
span [span] size = 512
Egress RACL [egr-racl] size = 1792
Egress SUP [egr-sup] size = 256
Ingress Redirect [ing-redirect] size = 0
Egress L2 QOS [egr-l2-qos] size = 0
Egress L3/VLAN QOS [egr-l3-vlan-qos] size = 0
Ingress Netflow/Analytics [ing-netflow] size = 0
Ingress NBM [ing-nbm] size = 0
TCP NAT ACL[tcp-nat] size = 0
```

```
Egress sup control plane[egr-copp] size = 0
Ingress Flow Redirect [ing-flow-redirect] size = 0
Ingress CNTACL [ing-cntacl] size = 0
Egress CNTACL [egr-cntacl] size = 0
MCAST NAT ACL[mcast-nat] size = 0
Ingress DACL [ing-dacl] size = 0
Ingress PACL Super Bridge [ing-pacl-sb] size = 0
Ingress Storm Control [ing-storm-control] size = 0
Ingress VACL redirect [ing-vacl-nh] size = 0
Egress PACL [egr-ifacl] size = 0
Egress Netflow [egr-netflow] size = 0
N9K-C9318OYC-2#
```

Configuração do grupo de acesso à porta IP

Configure o grupo de acesso da porta ip nas interfaces físicas L2.

```
N9K-C9318OYC-2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
N9K-C9318OYC-2(config)# int e1/2,e1/51
N9K-C9318OYC-2(config-if-range)# ip port access-group TAC-IN in
N9K-C9318OYC-2(config-if-range)# ip port access-group TAC-OUT out
Port ACL is only supported on ingress direction >>>>>>>>
N9K-C9318OYC-2(config-if-range)#
```

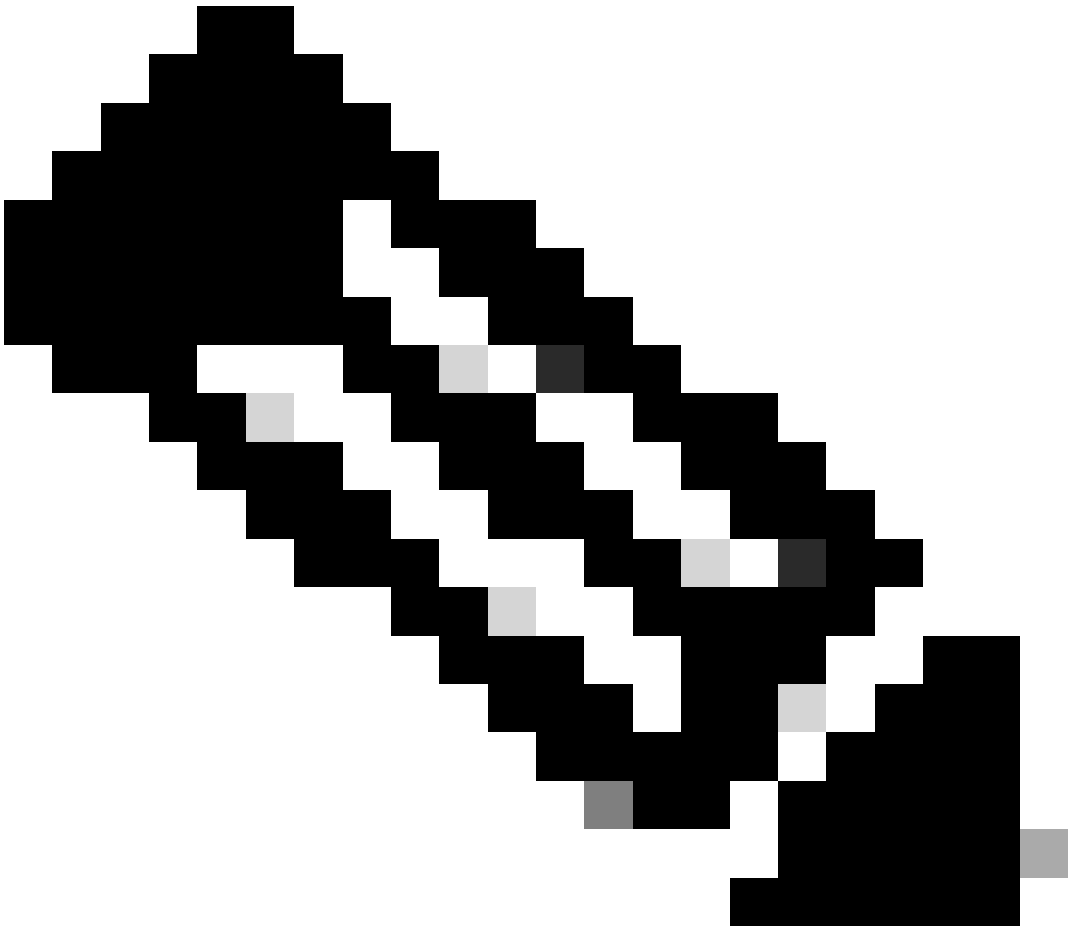
```
interface Ethernet1/1
description ***Link-to-N9K-1***
switchport
switchport access vlan 10
ip port access-group TAC-IN in >>> Inboud only
no shutdown
```

```
interface Ethernet1/3
description ***Link-to-N9K-3***
switchport
switchport access vlan 20
ip port access-group TAC-IN in >>> Inboud only
no shutdown
```

Etapa 3. Loopback

N9K-1 deve utilizar seu Loopback0 (Lo0) como origem, enquanto N9K-3 pode usar seu Loopback0 (Lo0) como destino.
A configuração em execução das interfaces de loopback que você emprega para fins de teste é

detalhada a seguir.



Note: A conectividade da camada 3 com um protocolo de roteamento foi configurada anteriormente.

```
***N9K-1***
interface loopback0
ip address 192.168.0.10/32
```

```
***N9K-3***
interface loopback0
ip address 10.10.10.10/30
```

Etapa 4. Gerar tráfego e enviar um ping de N9K-3 usando o IP de origem 192.168.20.2 para Lo0 192.168.0.10 de N9K-1

```
N9K-3# ping 192.168.0.10 source 192.168.20.2
PING 192.168.0.10 (192.168.0.10) from 192.168.20.2: 56 data bytes
64 bytes from 192.168.0.10: icmp_seq=0 ttl=253 time=1.163 ms
64 bytes from 192.168.0.10: icmp_seq=1 ttl=253 time=0.738 ms
64 bytes from 192.168.0.10: icmp_seq=2 ttl=253 time=0.706 ms
64 bytes from 192.168.0.10: icmp_seq=3 ttl=253 time=0.668 ms
64 bytes from 192.168.0.10: icmp_seq=4 ttl=253 time=0.692 ms

--- 192.168.0.10 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.668/0.793/1.163 ms
N9K-3#
```

Etapa 5. Verificar as Informações de Estatísticas de PACL e RACL em N9K-1, N9K-2 e N9K-3

- Como os pacotes ICMP são originários do N9K-3, é necessário verificar se os cinco pacotes de solicitação ICMP foram recebidos pelo N9K-2.
- Verificação de PACL em N9K-2: Espera-se que cinco pacotes originários de 192.168.20.2 (Eth1/4 de N9K-3) sejam recebidos, com o destino sendo Lo0 de N9K-1 (192.168.0.10).

```
N9K-2# show ip access-lists TAC-IN
IP access list TAC-IN
statistics per-entry
10 permit ip 192.168.20.2/32 192.168.0.10/32 [match=5] >>>
20 permit ip 192.168.0.10/32 192.168.20.2/32 [match=0]
30 permit ip any any [match=0]
```

Configuração relacionada em Eth1/3 de N9K-2.

```
interface Ethernet1/3
description ***Link-to-N9K-3***
switchport
switchport access vlan 20
ip port access-group TAC-IN in >>> PACL
no shutdown
```

- Em N9K-2, o RACL relata 5 pacotes de solicitação ICMP saindo de N9K-2 e sendo encaminhados para N9K-1.
- Como o PACL não suporta a direção de saída, é essencial verificar a outra ACL (TAC-OUT-SVI) configurada no SVI para a VLAN 10, que está configurada como um RACL (já que a direção de saída é suportada em RACLs). A VLAN 10 fornece a conectividade entre N9K-2

e N9K-1.

```
N9K-2# show ip access-lists TAC-OUT-SVI

IP access list TAC-OUT-SVI
statistics per-entry
10 permit ip 192.168.20.2/32 192.168.0.10/32 [match=5] >>>
20 permit ip 192.168.0.10/32 192.168.20.2/32 [match=0]
30 permit ip any any [match=0]



configuration associated:


interface Vlan10
no shutdown
ip access-group TAC-IN-SVI in
ip access-group TAC-OUT-SVI out >>>>
ip address 192.168.10.1/30
```

Com base nos resultados anteriores, confirma-se que não há perda de pacotes com os pacotes de solicitação ICMP enviados de N9K-3.

- A próxima etapa é prosseguir para o próximo dispositivo (destino N9K-1) e verificar se o mesmo número de pacotes de solicitação ICMP está sendo recebido de N9K-3.
- As estatísticas RACL indicam que o N9K-2 está enviando 5 pacotes de solicitação ICMP originados do N9K-3.

```
N9K-1# show ip access-lists TAC-IN
IP access list TAC-IN
statistics per-entry
10 permit ip 192.168.20.2/32 192.168.0.10/32 [match=5] >>>>
20 permit ip 192.168.0.10/32 192.168.20.2/32 [match=0]
30 permit ip any any [match=0]
```

Configuração relacionada em Eth1/1 de N9K-1.

```
interface Ethernet1/1
description ***Link-to-N9K-2***
ip access-group TAC-IN in >>> RACL
ip access-group TAC-OUT out
ip address 192.168.10.2/30
no shutdown
```

- Com base nas informações, confirma-se que não há perda de pacotes (solicitação ICMP) de N9K-3 para Lo0 192.168.0.10 em N9K-2.
- A próxima etapa é rastrear os pacotes de resposta ICMP originados de N9K-1 Lo0 192.168.0.10 e destinados a N9K-3 em 192.168.20.2.
- Em seguida, será necessário prosseguir para N9K-2 e verificar se está recebendo os cinco pacotes de resposta ICMP de 192.168.0.10 a 192.168.20.2.
- Para rastrear os pacotes de resposta ICMP de N9K-1, é necessário verificar o PACL (TAC-IN) configurado em Eth1/1.

```
N9K-2# show ip access-lists TAC-IN
IP access list TAC-IN
statistics per-entry
10 permit ip 192.168.20.2/32 192.168.0.10/32 [match=0]
20 permit ip 192.168.0.10/32 192.168.20.2/32 [match=5] >>> 5 icmp reply comming from 192.168.0.10 to 19
30 permit ip any any [match=0]
```

```
interface Ethernet1/1
description ***Link-to-N9K-1***
switchport
switchport access vlan 10
ip port access-group TAC-IN in >>> PACL (Inboud direction only)
no shutdown
```

- Com base nas informações fornecidas anteriormente, confirma-se que não há perda de pacotes no tráfego de N9K-1 a N9K-2.
- A próxima etapa é confirmar se N9K-2 está enviando corretamente os pacotes de resposta ICMP para N9K-3. Como o PACL não suporta a direção de saída, é necessário verificar a outra ACL (TAC-OUT-SVI) configurada no SVI para a VLAN 20, que está configurada como uma RACL (como a direção de saída é suportada em RACLs). A VLAN 20 fornece a conectividade entre N9K-2 e N9K-3.

```
N9K-2# show ip access-lists TAC-OUT-SVI
IP access list TAC-OUT-SVI
statistics per-entry
10 permit ip 192.168.20.2/32 192.168.0.10/32 [match=0]
20 permit ip 192.168.0.10/32 192.168.20.2/32 [match=5] >>> 5 ICMP reply packets are being sent out to N
```

Configuração relacionada:

```
interface Vlan10
no shutdown
ip access-group TAC-IN-SVI in
ip access-group TAC-OUT-SVI out >>> RACL outboud direccion
ip address 192.168.20.1/30
```

Com base nos contadores de ACL das saídas acima, confirma-se que N9K-1 está enviando corretamente os cinco pacotes de resposta ICMP para N9K-2.

- Não há perda de pacotes entre N9K-2 e N9K-3.

- A etapa final é prosseguir para a origem do tráfego, N9K-3, e verificar se ele está recebendo os cinco pacotes de resposta ICMP.
- Confirma-se que os cinco pacotes ICMP estão atingindo a ACL TAC-IN para as respostas ICMP vindas de N9K-1 Lo0 (192.168.0.10).
  Para investigar mais, é necessário rever o RACL (TAC-IN) configurado em Eth1/4.

```
N9K-3# sh ip access-lists TAC-IN

IP access list TAC-IN
statistics per-entry
10 permit ip 192.168.20.2/32 192.168.0.10/32 [match=0]
20 permit ip 192.168.0.10/32 192.168.20.2/32 [match=5] >>> 5 icmp replies comming from Lo0 N9K-1
30 permit ip any any [match=0]
```

Configuração relacionada:

```
interface Ethernet1/4
description ***Link-to-N9K-2***
ip access-group TAC-IN in >>>
ip access-group TAC-OUT out
ip address 192.168.20.2/30
no shutdown
```

- Usando as etapas de identificação e solução de problemas descritas anteriormente, o caminho de entrada e saída do pacote foi validado em uma base salto a salto entre a origem e o destino.

Neste exemplo, foi confirmado que não há perda de pacotes, pois todos os 5 pacotes ICMP foram recebidos e encaminhados corretamente em cada dispositivo.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.