使用Nexus平台上的ACL排除丢包故障

目录

简介

本文档介绍如何使用Nexus平台上的访问控制列表(ACL)对数据包丢失进行故障排除。

先决条件

要求

思科建议您了解以下主题：

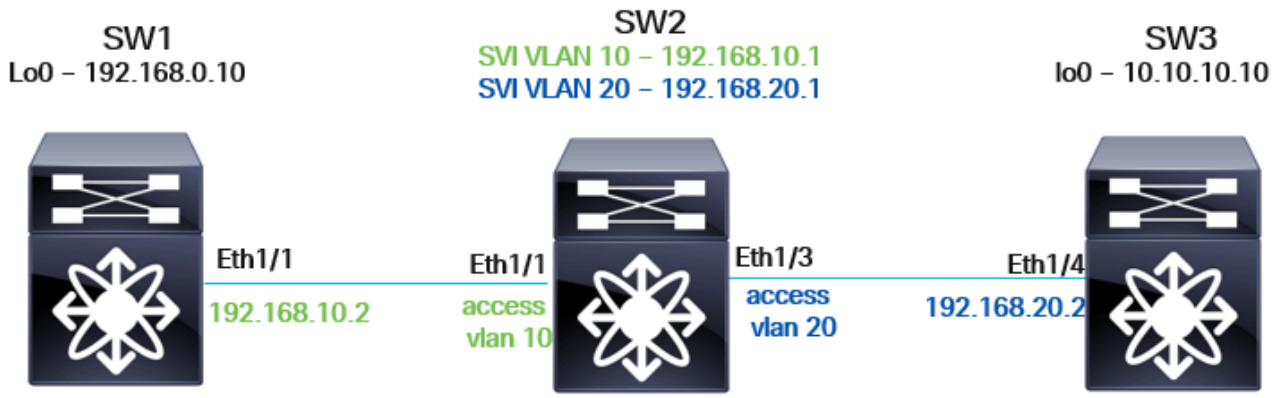
- NXOS平台
- 访问控制列表

使用的组件

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

本文档中的信息是从实验室环境中的Nexus设备创建的。本文档中使用的所有设备均在启动时未进行任何预先存在的配置。如果您使用的是实时网络，请确保您了解任何命令的潜在影响。

拓扑



访问控制列表及其功能的简要概述

ACL实际上用于根据一系列有序的规则和条件过滤流量（例如，根据源/目标IP地址过滤）。 这些规则确定数据包是否与特定条件匹配，以决定是允许还是拒绝这些数据包。用更简单的术语来说，ACL根据网络数据包内设置的规则来定义是允许网络数据包通过还是拒绝网络数据包。如果数据包符合允许规则的条件，则它们将由Nexus交换机处理。反之，如果数据包符合拒绝条件，则这些数据包将被丢弃。

ACL的一个主要功能是能够为数据包流提供统计计数器。这些计数器跟踪与ACL规则匹配的数据包数量，这在排除数据包丢失故障时非常有用。

例如，如果设备正在发送一定数量的数据包，但收到的数据包少于预期，来自ACL的统计计数器可以帮助隔离网络中丢弃数据包的点。

PACL和RACL

ACL的实施方式可能有所不同，具体取决于它们是否应用于第2层接口(PACL)、第3层接口(RACL)或VLAN(VACL)。 以下是对这些方法的简单比较：

- 端口访问控制列表(PACL):ACL应用于第2层(L2)交换机端口接口。
- 路由器访问控制列表(RACL):该ACL应用于第3层(L3)路由接口。

ACL类型	接口	操作	应用方向
PACL	L2	交换机端口接口 如果ACL应用于中继接口，它会过滤中继上允许的所有VLAN的流量。	仅入站 — 进入接口的流量。
RACL	L3	SVI、物理L3和L3子接口	入站和出站 — 入站过滤进入接口的流量，而出站过滤离开接口的流量。

目标

必须确认已正确接收发送的所有数据包。

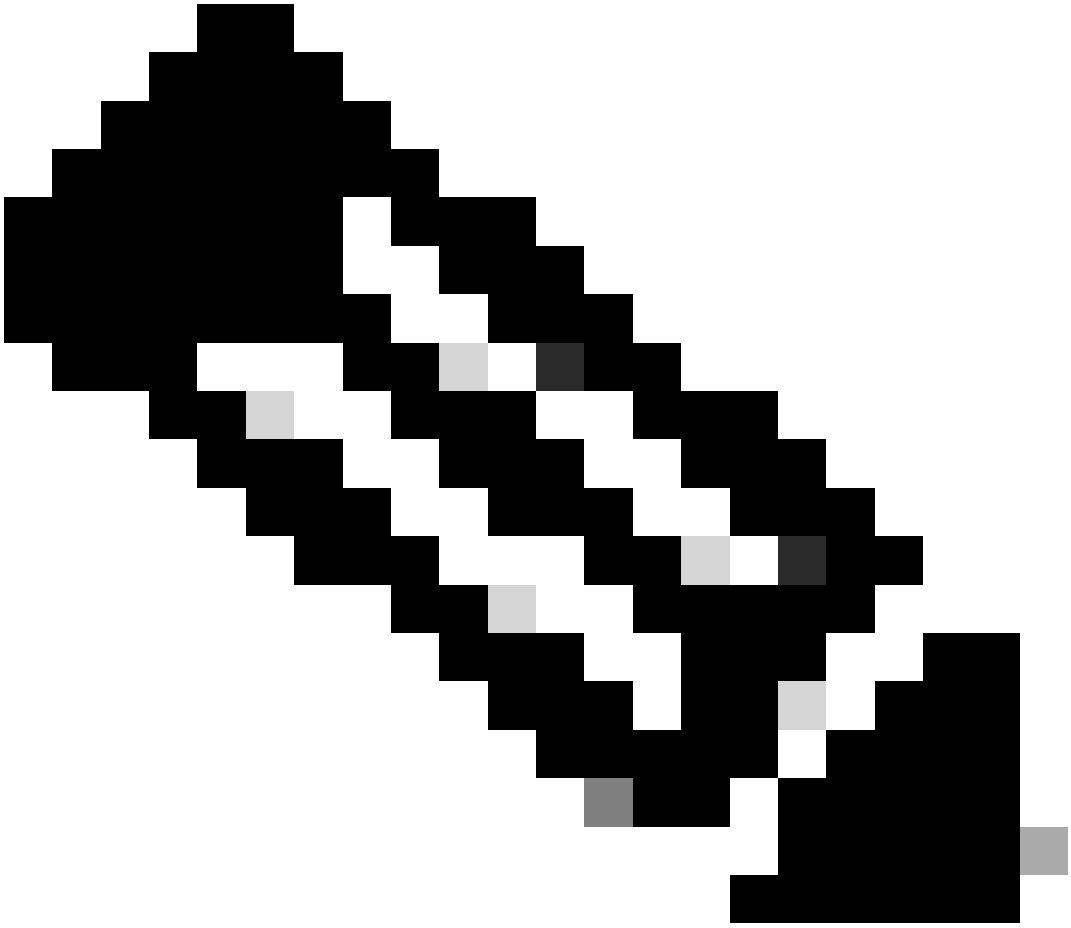
拓扑说明

- N9K-1与N9K-2具有L3连接。N9K-1上的Eth1/1接口配置为L3路由接口，而N9K-2的Eth1/1为L2交换机端口接口，标记为VLAN 10。
- N9K-2也与N9K-3具有L3连接。N9K-2上的Eth1/3接口是标记为VLAN 20的L2交换机端口接口，N9K-3的Eth1/4配置为L3路由接口。
- 环回配置：N9K-1和N9K-2都配置了Lo0接口。应使用这些Lo0接口在两个设备之间发送ICMP ping数据包。

故障排除

请查看在N9K设备上配置和验证RACL和PACL的详细流程步骤。在此流程中，将查看端口访问控制列表和路由器访问控制列表，以分析数据包流，并确定是否正确传输和接收所有数据包。

步骤1.在N9K-1(Eth1/1)、N9K-2(SVI 10、SVI 20)和N9K-3(Eth1/14)的L3接口上配置RACL



注意：要观察出站数据包流，需要在N9K-2上进行额外的ACL配置。由于N9K-2缺少L3物理路由接口（而是SVI和L2交换机端口接口），因此PACL仅支持入站流量。

为了捕获出站数据包匹配项，可以创建新的ACL并将其应用到L3接口。

ACL应应用到N9K-1、N9K-2和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
```

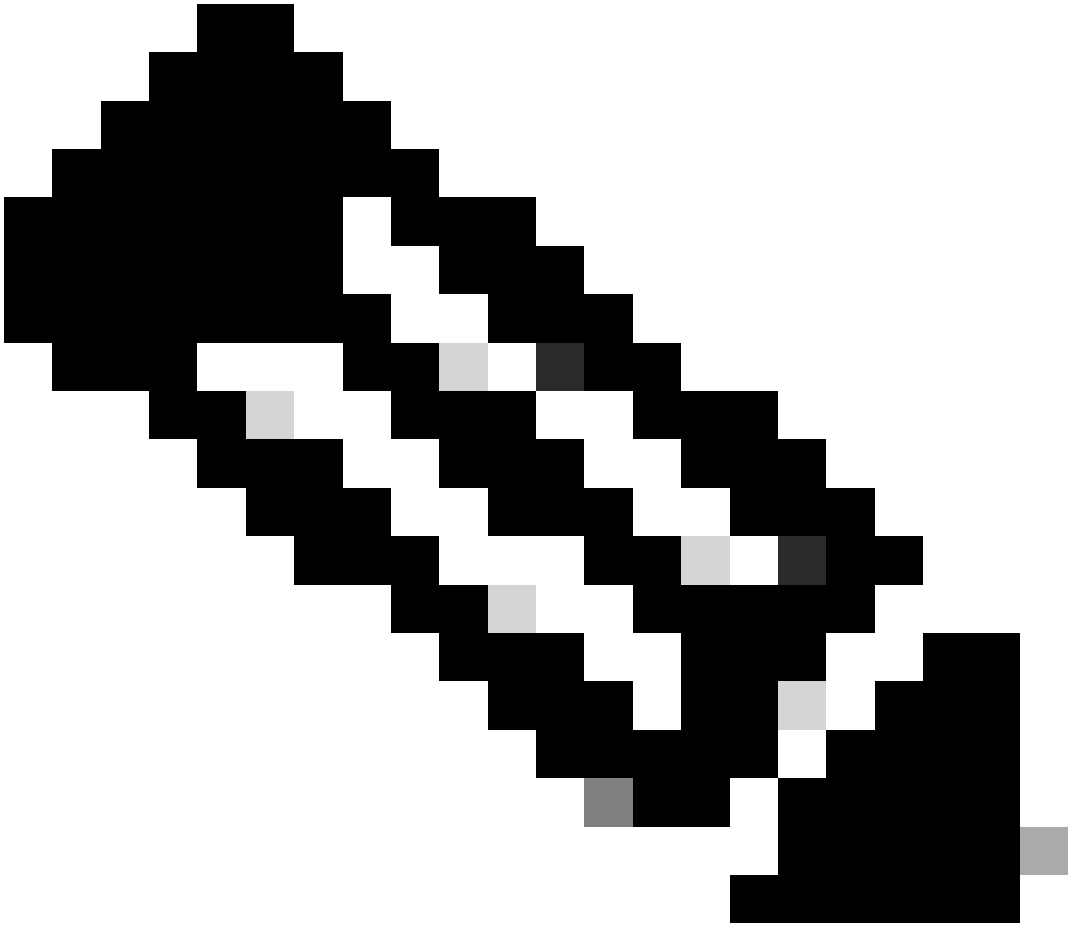
步骤2.在N9K-2的L2交换机端口接口上配置PACL

TCAM雕刻

根据ACL类型，可能需要TCAM切割，有关详细信息，请参阅：

[了解如何划分Nexus 9000 TCAM空间]

要将PACL应用到L2物理接口，必须配置ip port access-group ....
但是，还需要配置TCAM区域。



注意：某些行已被删除，以保持输出正常。

```
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)#
```

配置TCAM区域的步骤

步骤1.修改TCAM区域

请评估哪个区域可以提供可用空间，因为每个环境的可用空间可能有所不同。

```
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
```

另一种验证方法。

```
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#
```

步骤2.缩小区域规模

减小分配给ing-l3-vlan-qos的区域大小。（这因环境而异。）

N9K-C93180YC-2(config)# hardware access-list tcam region ing-l3-vlan-qos 256 >>>将分配从512减少到256。
请保存配置并重新加载系统，以使配置生效。

步骤3.增加接口的TCAM区域

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

保存配置并重新加载系统以使配置生效。

N9K-C93180YC-2(config)#

步骤4.保存配置

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

第 5 步： 重新加载

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

重新加载后验证

重新加载后，检查更改是否已生效。

```
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
```

另一种验证方法。

```
N9K-C9318OYC-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#
```

IP端口访问组的配置

在L2物理接口上配置ip port access-group。

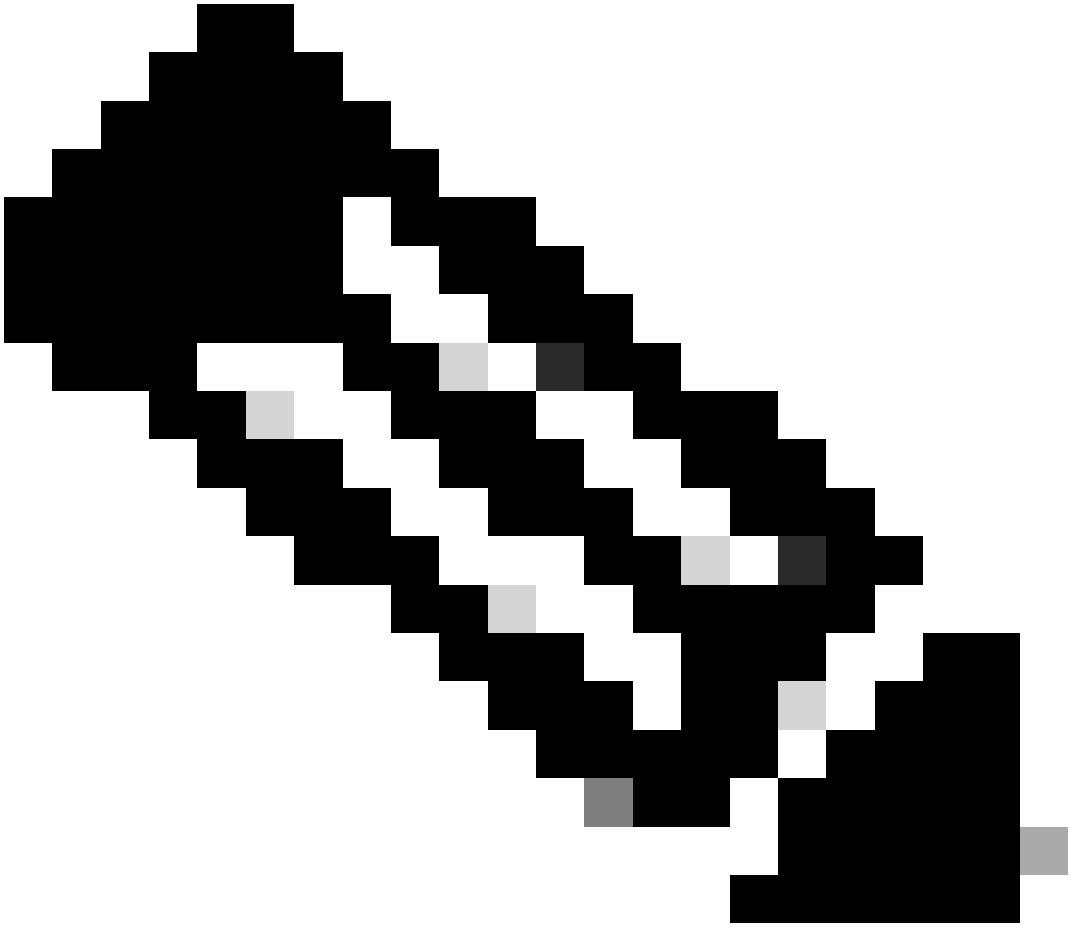
```
N9K-C9318OYC-2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
N9K-C9318OYC-2(config)# int e1/2,e1/51
N9K-C9318OYC-2(config-if-range)# ip port access-group TAC-IN in
N9K-C9318OYC-2(config-if-range)# ip port access-group TAC-OUT out
Port ACL is only supported on ingress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

步骤3.环回

N9K-1将使用其Loopback0(Lo0)作为源，而N9K-3可以使用其Loopback0(Lo0)作为目标。
用于测试目的的环回接口的运行配置详述如下。



注意：之前已配置了使用路由协议的第3层连接。

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

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

步骤4.使用源IP 192.168.20.2生成流量并从N9K-3向N9K-1的Lo0 192.168.0.10发送Ping

```
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#
```

步骤5.检验N9K-1、N9K-2和N9K-3上的PACL和RACL统计信息

- 由于ICMP数据包源自N9K-3，因此有必要验证N9K-2是否收到了这五个ICMP请求数据包。
- N9K-2上的PACL验证：预期收到来自192.168.20.2（N9K-3的Eth1/4）的五个数据包，目的地为N9K-1的Lo0(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]
```

N9K-2的Eth1/3上的相关配置。

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

- 在N9K-2上，RACL报告5个离开N9K-2并被转发到N9K-1的ICMP请求数据包。
- 由于PACL不支持出站方向，因此必须验证在SVI上为VLAN 10配置的另一个ACL(TAC-OUT-SVI)，该VLAN配置为RACL（因为RACL支持出站方向）。VLAN 10提供N9K-2和N9K-1之间的连接。

```
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
```

根据前面的结果，确认从N9K-3发送的ICMP请求数据包没有丢包。

- 下一步是进入下一台设备（目标N9K-1），并检验从N9K-3收到了相同数量的ICMP请求数据包。
- RACL统计信息表明N9K-2正在发送来自N9K-3的5个ICMP请求数据包。

```
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]
```

N9K-1的Eth1/1上的相关配置。

```
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
```

- 根据此信息，确认从N9K-3到N9K-2上的Lo0 192.168.0.10没有数据包丢失（ICMP请求）。
- 下一步是跟踪从N9K-1 Lo0 192.168.0.10发往192.168.20.2处的N9K-3的ICMP应答数据包。
- 然后，需要进入N9K-2，验证它是否接收了从192.168.0.10到192.168.20.2的五个ICMP应答数据包。
- 要跟踪来自N9K-1的ICMP应答数据包，需要验证Eth1/1上配置的PACL(TAC-IN)。

```
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
```

- 根据之前提供的信息，确认从N9K-1到N9K-2的流量没有丢包。
- 下一步是确认N9K-2正在向N9K-3正确发送ICMP应答数据包。由于PACL不支持出站方向，因此有必要验证在SVI上为VLAN 20配置的另一个ACL(TAC-OUT-SVI)，该配置为RACL（因为RACL支持出站方向）。VLAN 20提供N9K-2和N9K-3之间的连接。

```
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
```

相关配置：

```
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
```

根据以上输出中的ACL计数器，确认N9K-1正在向N9K-2正确发送五个ICMP应答数据包。

- 从N9K-2到N9K-3不会发生数据包丢失。

- 最后一步是进入流量源N9K-3，并验证它是否接收了五个ICMP应答数据包。
- 确认五个ICMP数据包进入ACL TAC-IN，获取来自N9K-1 Lo0(192.168.0.10)的ICMP应答。要进一步研究，必须检查Eth1/4上配置的RACL(TAC-IN)。

```
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]
```

相关配置：

```
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
```

- 使用前面介绍的故障排除步骤，源主机和目的主机之间逐跳地验证数据包的传入和传出路径。

在本例中，确认不存在丢包现象，因为所有五个ICMP数据包都是在每台设备上正确接收和转发的。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。