# 使用Nexus平台上的ACL排除資料包丟棄故障

## 目錄



## 簡介

本檔案介紹如何在Nexus平台上使用存取控制清單(ACL)對封包遺失進行疑難排解。

## 必要條件

### 需求

思科建議您瞭解以下主題：

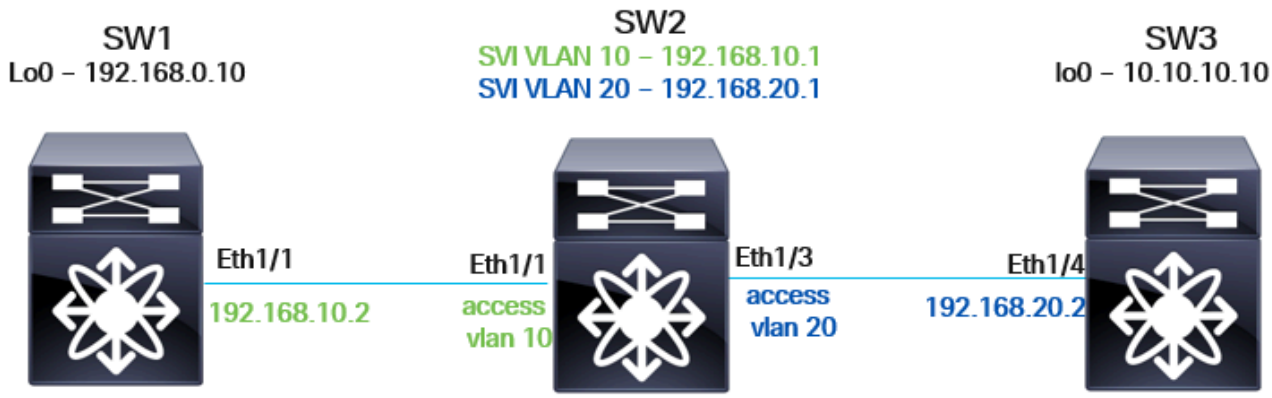
- NXOS平台
- 存取控制清單

### 採用元件

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

本文中的資訊是根據實驗室環境中的Nexus裝置所建立。文中使用到的所有裝置皆已啟動，且未進行任何預先存在的組態。如果您使用的是即時網路，請確保您已瞭解任何命令的潛在影響。

## 拓撲




## 存取控制清單及其功能的簡短概觀

ACL基本上用於根據一系列有序的規則和標準過濾流量（例如，根據源/目標IP地址過濾）。 這些規則確定資料包是否與特定條件匹配，以決定應允許還是拒絕這些資料包。在更簡單的術語中，ACL根據網路資料包內設定的規則來定義是允許通過網路資料包還是拒絕網路資料包。如果資料包滿足許可規則條件，則由Nexus交換機進行處理。反之，如果封包符合deny條件，則應該將其捨棄。

ACL的一個關鍵功能是能夠為封包流量提供統計計數器。這些計數器跟蹤與ACL規則匹配的資料包數量，這在排除資料包丟失情況故障時非常有用。

例如，如果裝置正在傳送一定數量的資料包，但收到的資料包少於預期，則來自ACL的統計計數器有助於隔離網路中丟棄資料包的點。

### PACL和RACL

ACL的實施方式可能會有所差異，這取決於它們是否應用於第2層介面(PACL)、第3層介面(RACL)或VLAN(VACL)。 以下是這些方法的簡短比較：

- 連線埠存取控制清單(PACL):ACL會套用到第2層(L2)交換器連線埠介面。
- 路由器存取控制清單(RACL):ACL會套用到第3層(L3)路由介面。

| ACL型別 | 介面 | 動作 | 應用方向 |
| --- | --- | --- | --- |
| PACL | L2 | 交換機埠介面<br><br>如果將ACL套用到主幹介面，則會過濾主幹上允許的所有VLAN流量。 | 僅傳入 — 進入介面的流量。 |
| RACL | L3 | SVI、物理L3和L3子介面 | 入站和出站 — 入站過濾進入介面的流量，而出站過濾離開介面的流量。 |

## 目標

必須確認已正確接收所有傳送的資料包。

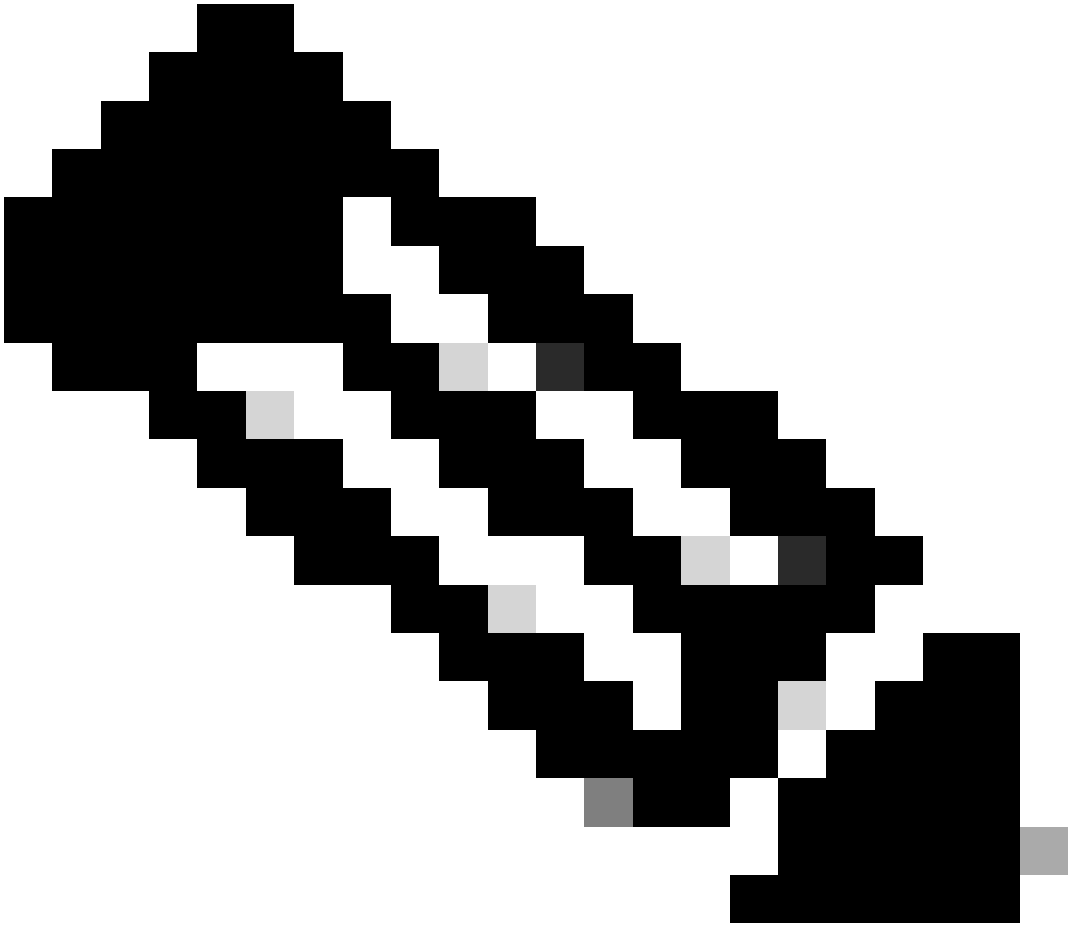
## 拓撲說明

- N9K-1與N9K-2具有L3連線。N9K-1上的Eth1/1介面配置為L3路由介面，而N9K-2的Eth1/1為L2交換機埠介面，標籤有VLAN 10。
- N9K-2也與N9K-3具有L3連線。N9K-2上的Eth1/3介面是使用VLAN 20標籤的L2交換機埠介面，N9K-3的Eth1/4被配置為L3路由介面。
- 環回配置：N9K-1和N9K-2都配置了Lo0介面。應使用這些Lo0介面在兩個裝置之間傳送ICMP ping資料包。

## 疑難排解

請檢視在N9K裝置上配置和驗證RACL和PACL的詳細過程步驟。在此過程中，將檢視埠訪問控制清單和路由器訪問控制清單，以分析資料包流，並確定是否正確傳輸和接收所有資料包。

### 步驟1.在N9K-1(Eth1/1)、N9K-2(SVI 10、SVI 20)和N9K-3(Eth1/14)的L3介面上配置RACL



附註：要觀察出站資料包流，N9K-2上需要額外的ACL配置。由於N9K-2缺少L3物理路由介面（而是SVI和L2交換機埠介面），因此PACL僅支援入站流量。

---

為了捕獲出站資料包匹配項，可以建立一個新的ACL並將其應用到L3介面。

ACL應應用於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
```

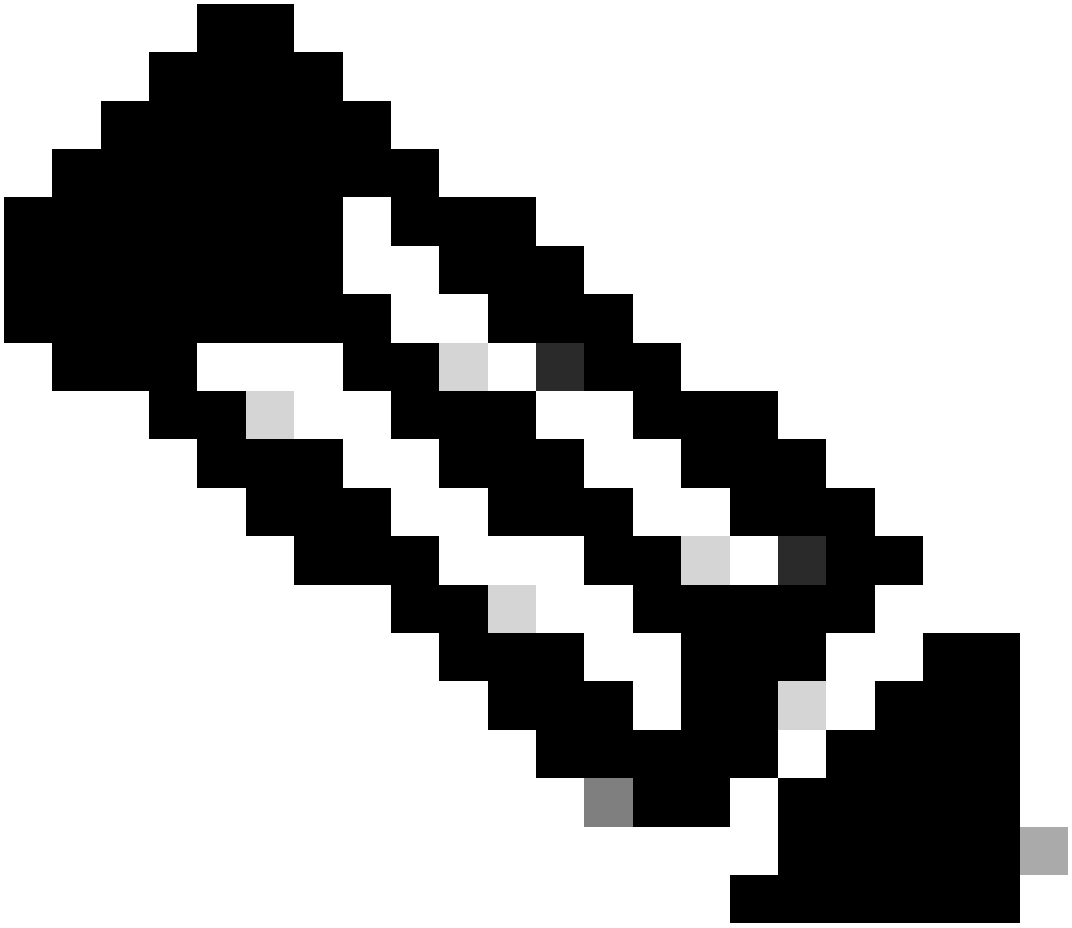
## 步驟2.在N9K-2的L2交換機埠介面上配置PACL

TCAM雕刻

根據ACL型別，可能需要TCAM雕刻，有關詳細資訊，請參閱：

瞭解如何劃分Nexus 9000 TCAM空間

要將PACL應用到L2物理介面，必須配置ip port access-group ....
但是，還需要配置TCAM區域。



附註：已移除某些行以保持輸出清潔。

```
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區域的步驟

### 步驟1. TCAM區域修改

請評估哪個區域可以提供可用空間，因為每個環境的可用空間可能有所不同。

```
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
```

另一種驗證方法。

```
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#
```

步驟2.縮小區域規模

減小分配給ing-l3-vlan-qos的區域大小。（這因環境而異。）

N9K-C93180YC-2(config)# hardware access-list tcam region ing-l3-vlan-qos 256 >>>將分配從512減少到256。
請儲存配置並重新載入系統，以使配置生效。

步驟3.增加面向介面的TCAM區域

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

儲存配置並重新載入系統以使配置生效。

N9K-C93180YC-2(config)#

步驟4.儲存配置

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

步驟 5. 重新載入

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

重新載入後驗證

重新載入後，檢查更改是否已生效。

```
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
```

另一種驗證方法。

```
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-C93180YC-2#
```

IP埠訪問組的配置

在L2物理介面上配置ip port access-group。

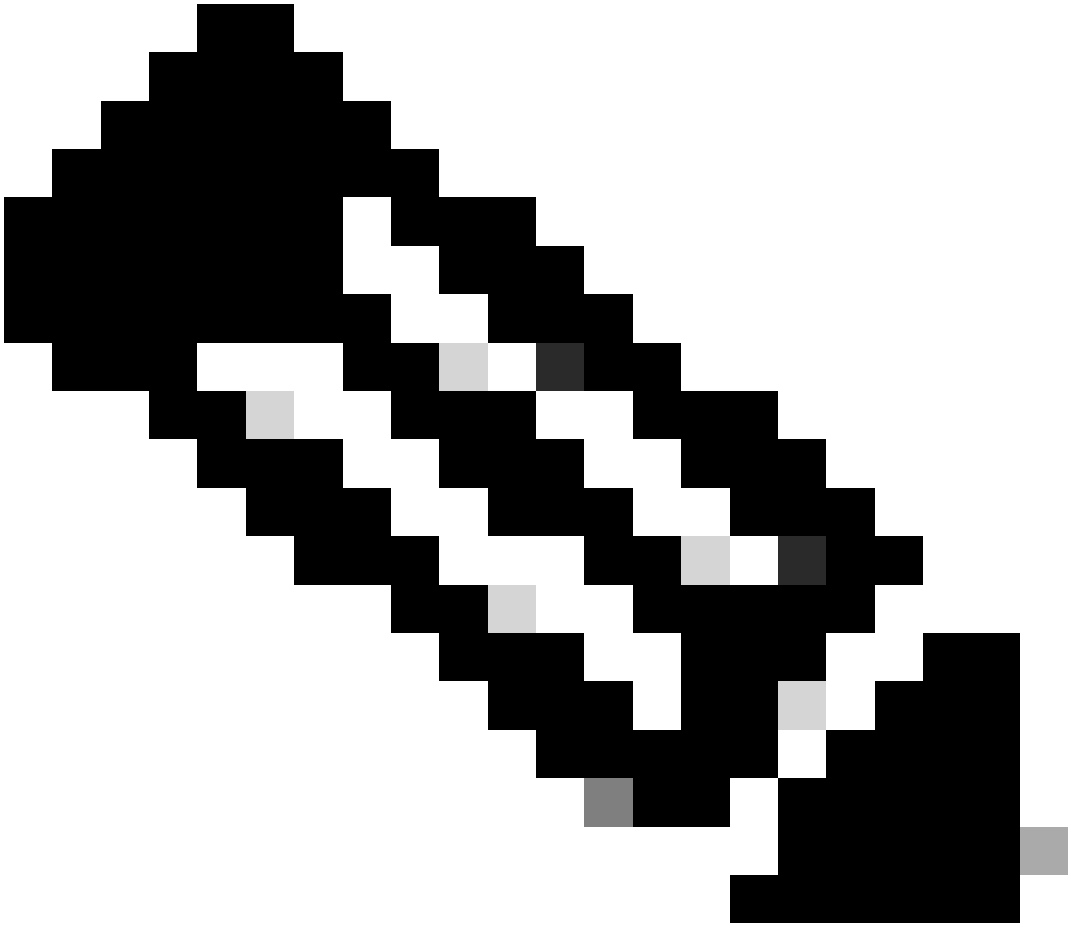
```
N9K-C93180YC-2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
N9K-C93180YC-2(config)# int e1/2,e1/51
N9K-C93180YC-2(config-if-range)# ip port access-group TAC-IN in
N9K-C93180YC-2(config-if-range)# ip port access-group TAC-OUT out
Port ACL is only supported on ingress direction >>>>>>>>
N9K-C93180YC-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
```

## 步驟3.環回

N9K-1使用其Loopback0(Lo0)作為源，而N9K-3使用其Loopback0(Lo0)作為目標。
用於測試目的的環回介面的運行配置如下所述。



附註：先前已配置了與路由協定的第3層連線。

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

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

## 步驟4.使用源IP 192.168.20.2生成流量並從N9K-3傳送Ping N9K-1的Lo0 192.168.0.10

```
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#
```

## 步驟5.驗證N9K-1、N9K-2和N9K-3上的PACL和RACL統計資訊

- 由於ICMP資料包源自N9K-3，因此必須驗證N9K-2是否收到了這五個ICMP請求資料包。
- N9K-2上的PACL驗證：預期收到五個來自192.168.20.2（N9K-3的Eth1/4）的資料包，目的地為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 Eth1/3上的相關配置。

```
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報告5個ICMP請求資料包，這些資料包離開N9K-2並轉發到N9K-1。
- 由於PACL不支援傳出方向，因此驗證在SVI上為VLAN 10設定的其他ACL(TAC-OUT-SVI)是否設定為RACL非常重要（因為RACL支援傳出方向）。VLAN 10提供N9K-2和N9K-1之間的連線。

```
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
```

根據前面的結果，確認從N9K-3傳送的ICMP請求資料包沒有丟包。

- 下一步是進入下一個裝置（目標N9K-1），並檢驗從N9K-3收到的ICMP請求資料包是否相同。
- RACL統計資訊表明N9K-2正在傳送來自N9K-3的5個ICMP請求資料包。

```
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 Eth1/1上的相關配置。

```
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
```

- 根據該資訊，確認從N9K-3到N9K-2上的Lo0 192.168.0.10沒有丟包（ICMP請求）。
- 下一步是跟蹤從N9K-1 Lo0 192.168.0.10到192.168.20.2 N9K-3的ICMP應答資料包。
- 然後，必須進入N9K-2，並驗證它是否收到從192.168.0.10到192.168.20.2的五個ICMP應答資料包。
- 要跟蹤來自N9K-1的ICMP應答資料包，需要驗證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
```

- 根據先前提供的資訊，確認從N9K-1到N9K-2的流量沒有丟包。
- 下一步是確認N9K-2正在正確向N9K-3傳送ICMP應答資料包。由於PACL不支援出站方向，因此必須驗證在SVI上為VLAN 20配置的另一個ACL(TAC-OUT-SVI)，該ACL配置為RACL（因為RACL支援出站方向）。VLAN 20提供N9K-2和N9K-3之間的連線。

```
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
```

相關配置：

```
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
```

根據上述輸出的ACL計數器，確認N9K-1正在將五個ICMP應答資料包正確傳送到N9K-2。

- 從N9K-2到N9K-3，沒有資料包丟失。

- 最後一步是進入流量的來源N9K-3，並驗證它是否收到五個ICMP應答資料包。
- 確認五個ICMP封包正在進入ACL TAC-IN，以取得來自N9K-1 Lo0(192.168.0.10)的ICMP回覆。
  要進一步研究，必須檢視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]
```

相關配置：

```
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
```

- 使用前面介紹的故障排除步驟，源主機和目的主機之間逐跳驗證資料包的傳入和傳出路徑。

在本例中，已確認沒有丟包，因為每台裝置上都已正確接收和轉發所有5個ICMP資料包。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。