Nexus 플랫폼의 ACL로 패킷 삭제 트러블슈팅

목차

소개

이 문서에서는 Nexus 플랫폼에서 ACL(Access Control List)을 사용하여 패킷 손실을 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대해 알고 있는 것이 좋습니다.

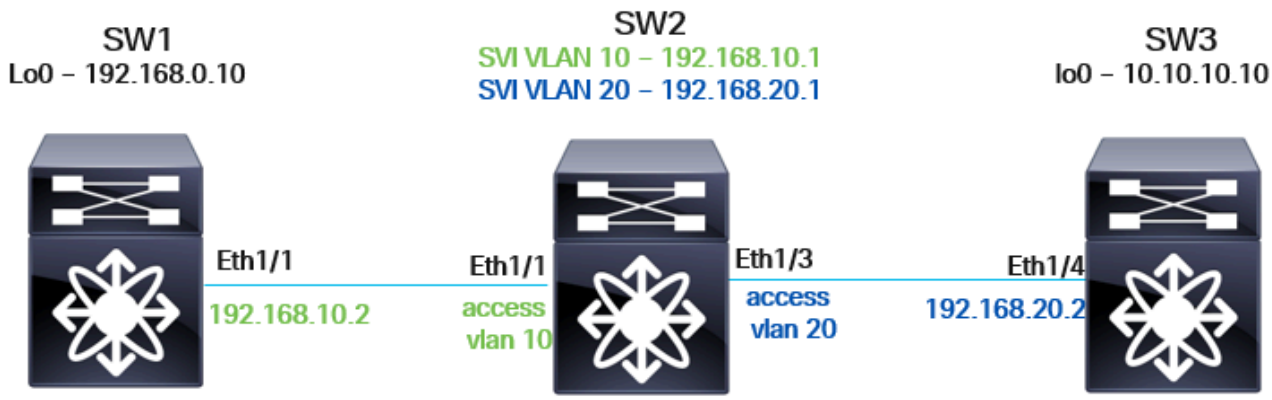
- NXOS 플랫폼
- 액세스 제어 목록

사용된 구성 요소

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

이 문서의 정보는 랩 환경의 Nexus 디바이스에서 생성되었습니다. 이 문서에 사용된 모든 디바이스는 기존 컨피그레이션 없이 시작되었습니다. 라이브 네트워크를 사용하는 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

토폴로지



ACL(Access Control List) 및 기능에 대한 간략한 개요

ACL은 기본적으로 일련의 순서가 지정된 규칙 및 기준에 따라 트래픽을 필터링하는 데 사용됩니다(예: 소스/대상 IP 주소에 따라 필터링). 이러한 규칙은 패킷이 허용 또는 거부될 것인지 여부를 결정하기 위해 특정 조건과 일치하는지 여부를 결정합니다. 더 간단한 관점에서 ACL은 네트워크 패킷이 통과하는 것을 허용할지 또는 네트워크 패킷 내에 설정된 규칙을 기반으로 거부할지를 정의합니다. 패킷이 허용 규칙의 조건을 충족하는 경우 Nexus 스위치에서 처리됩니다. 반대로, 패킷이 거부 조건과 일치하면 패킷을 버립니다.

ACL의 한 가지 주요 기능은 패킷 흐름에 대한 통계 카운터를 제공하는 기능입니다. 이러한 카운터는 ACL 규칙과 일치하는 패킷의 수를 추적하며, 이는 패킷 손실 시나리오를 트러블슈팅할 때 매우 유용할 수 있습니다.

예를 들어 디바이스에서 특정 수의 패킷을 전송하지만 예상보다 적은 패킷을 수신하는 경우, ACL의 통계 카운터는 네트워크 내에서 패킷이 삭제되는 지점을 격리하는 데 도움이 될 수 있습니다.

PACL 및 RACL

ACL의 구현은 PACL(Layer 2 Interface), RACL(Layer 3 Interface) 또는 VACL(VLAN)에 적용되는지 여부에 따라 달라질 수 있습니다. 다음은 이러한 방법을 간단하게 비교한 것입니다.

- PACL(Port Access Control List): ACL은 L2(Layer 2) 스위치포트 인터페이스에 적용됩니다.
- RACL(Router Access Control List): ACL은 L3(Layer 3) 라우팅 인터페이스에 적용됩니다.

ACL 유형	인터페이스	작업	적용된 방향
PACL	L2	Switchport 인터페이스 ACL이 트렁크 인터페이스에 적용되는 경우, 트렁크에서 허용되는 모든 VLAN에 대한 트래픽을 필터링합니다.	인바운드 전용 - 인터페이스로 들어오는 트래픽.
라클	L3	SVI, 물리적 L3 및 L3 하위 인터페이스	인바운드 및 아웃바운드 모두 - 인바운드는 인터페이스로 들어오는 트래픽을 필터링하는 반면, 아웃바운드는 인터페이스를 나가는 트래픽을 필터링합니다.

목표

전송되는 모든 패킷이 제대로 수신되는지 확인해야 합니다.

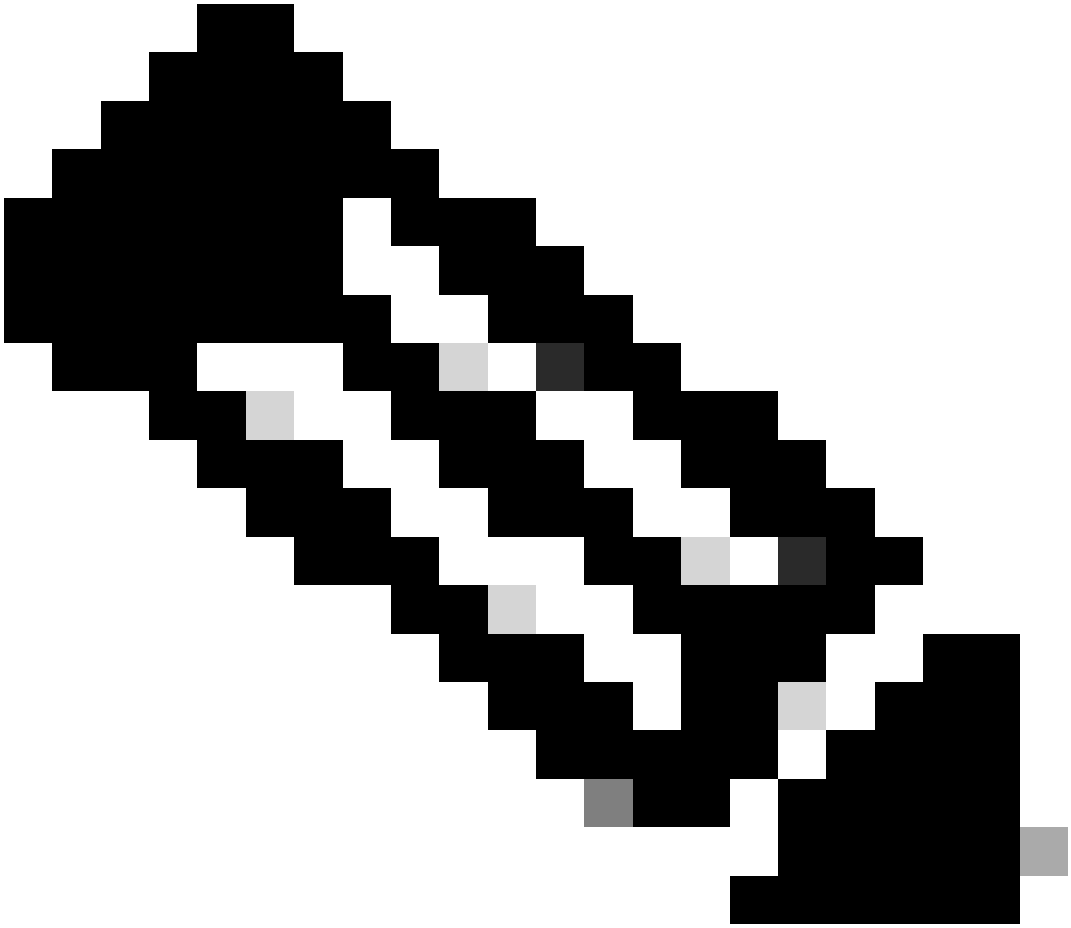
토폴로지 설명

- N9K-1은 N9K-2와 L3 연결을 가집니다. N9K-1의 Eth1/1 인터페이스는 L3 라우티드 인터페이스로 구성된 반면 N9K-2의 Eth1/1은 VLAN 10으로 태그가 지정된 L2 스위치포트 인터페이스입니다.
- N9K-2는 N9K-3과의 L3 연결도 갖습니다. N9K-2의 Eth1/3 인터페이스는 VLAN 20으로 태그가 지정된 L2 스위치포트 인터페이스이며, N9K-3의 Eth1/4는 L3 라우티드 인터페이스로 구성됩니다.
- 루프백 구성: N9K-1 및 N9K-2 모두 Lo0 인터페이스가 구성되어 있습니다. 이러한 Lo0 인터페이스는 두 디바이스 간에 ICMP ping 패킷을 전송하는 데 사용됩니다.

문제 해결

N9K 디바이스에서 RACL 및 PACL을 구성 및 확인하기 위한 자세한 프로세스 단계를 찾으십시오. 이 프로세스 중에 포트 액세스 제어 목록 및 라우터 액세스 제어 목록을 검토하여 패킷 흐름을 분석하고 모든 패킷이 올바르게 전송 및 수신되는지 확인합니다.

1단계. N9K-1(Eth1/1), N9K-2(SVI 10, SVI 20) 및 N9K-3(Eth1/14)의 L3 인터페이스에서 RACL을 구성합니다



참고: 아웃바운드 패킷 흐름을 관찰하려면 N9K-2에서 추가 ACL 컨피그레이션이 필요합니다. N9K-2에는 L3 물리적 라우티드 인터페이스가 없으므로(대신 SVI 및 L2 스위치포트 인터페이스가 있음) PACL은 인바운드 트래픽만 지원합니다.

아웃바운드 패킷 일치를 캡처하기 위해 새 ACL을 생성하여 L3 인터페이스에 적용할 수 있습니다.

ACL은 N9K-1, N9K-2 및 N9K-3에 적용됩니다.

```
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
```

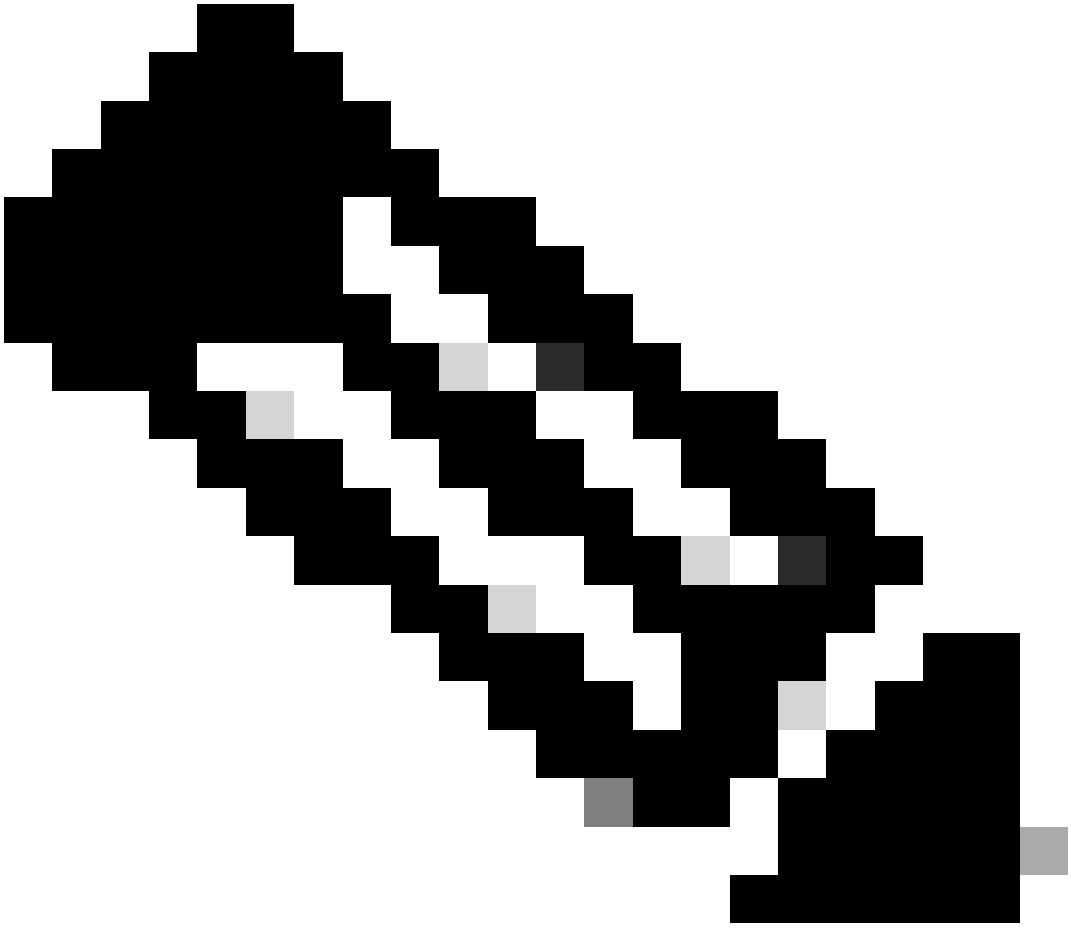
2단계. N9K-2의 L2 스위치포트 인터페이스에서 PACL 구성

TCAM 카빙

ACL 유형에 따라 TCAM 조각이 필요할 수 있습니다. 자세한 내용은 다음을 참조하십시오.

Nexus 9000 TCAM Space를 조각하는 방법 이해

PACL을 L2 물리적 인터페이스에 적용하려면 ip 포트 액세스 그룹을 구성해야 합니다..
그러나 TCAM 영역을 구성하는 것도 필요합니다.



참고: 출력을 깔끔하게 유지하기 위해 특정 행이 제거되었습니다.

```
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)#
```

TCAM 영역 구성 절차

1단계. TCAM 영역 수정

각 환경에 따라 다를 수 있으므로 어느 지역에서 여유 공간을 제공할 수 있는지 평가해 주십시오.

```
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
```

확인을 위한 대체 방법입니다.

```
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#
```

2단계. 지역 규모 축소

ing-l3-vlan-qos에 할당된 영역의 크기를 줄입니다. (이는 각 환경에 따라 다릅니다.)

N9K-C93180YC-2(config)# hardware access-list tcam region ing-l3-vlan-qos 256 >> 512에서 256으로 할당 축소
구성을 저장하고 시스템을 다시 로드하여 구성을 적용하십시오.

3단계. IFACL을 위해 TCAM 영역 늘리기

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

컨피그레이션을 저장하고 시스템을 다시 로드하여 컨피그레이션을 적용합니다.

N9K-C93180YC-2(config)#

4단계. 구성 저장

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

5단계. Reload

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

다시 로드 후 확인

다시 로드한 후 변경 사항이 적용되었는지 확인합니다.

```
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
```

확인을 위한 대체 방법입니다.

```
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 포트 액세스 그룹 구성

L2 물리적 인터페이스에서 ip 포트 access-group을 구성합니다.

```
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)#
```

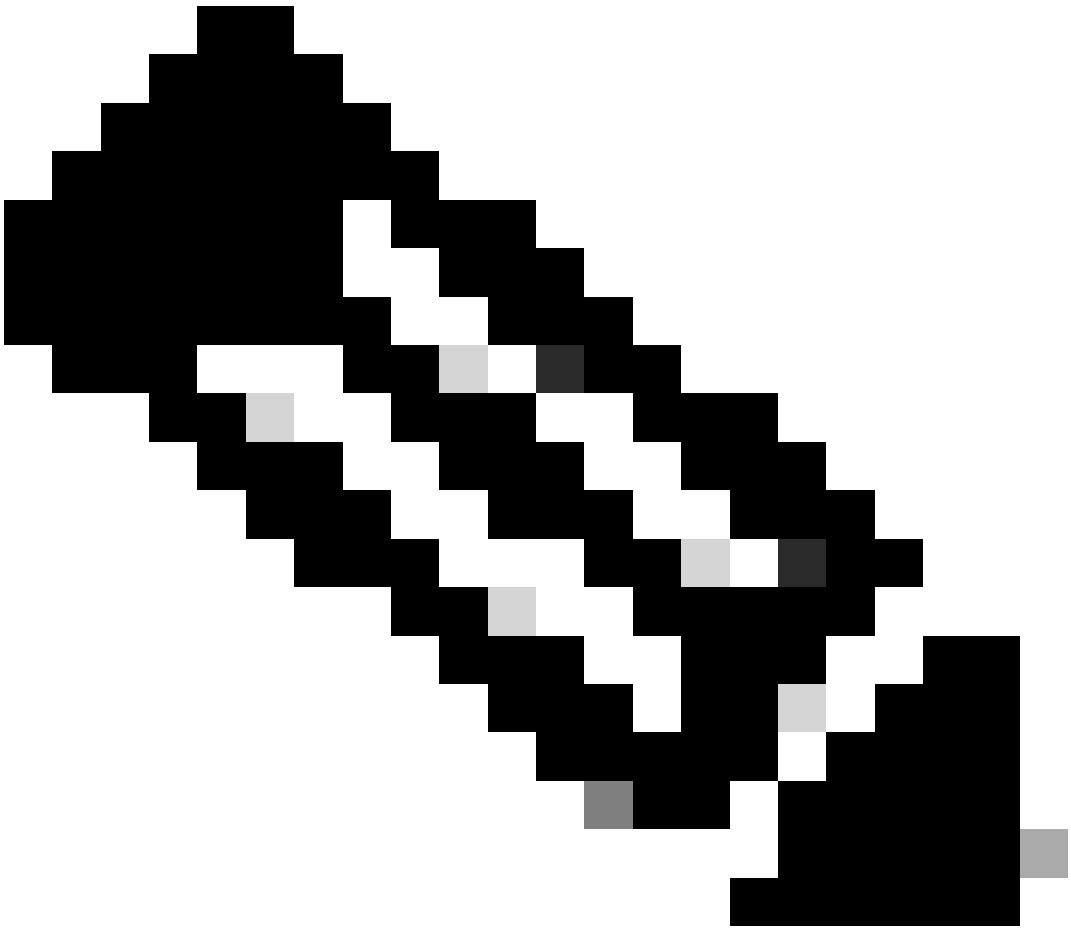
```
interface Ethernet1/1
description ***Link-to-N9K-1***
switchport
switchport access vlan 10
ip port access-group TAC-IN in >>> Inboud only
no shutdown
```

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

3단계. 루프백

N9K-1은 Loopback0(Lo0)을 소스로 사용하지만 N9K-3은 Loopback0(Lo0)을 대상으로 사용할 수 있습니다.
테스트용으로 사용하는 루프백 인터페이스의 실행 중인 컨피그레이션은 다음과 같이 자세히 설명

되어 있습니다.



참고: 라우팅 프로토콜과의 레이어 3 연결은 이전에 구성되었습니다.

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


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

4단계. 소스 IP 192.168.20.2를 사용하여 N9K-3에서 N9K-1의 Lo0 192.168.0.10으로 트래픽을 생성하고 Ping을 보냅니다.

```
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#
```

5단계. N9K-1, N9K-2 및 N9K-3에 대한 PACL 및 RACL 통계 정보 확인

- ICMP 패킷은 N9K-3에서 시작되므로 5개의 ICMP 요청 패킷이 N9K-2에 의해 수신되었는지 확인해야 합니다.
- N9K-2에 대한 PACL 확인: 192.168.20.2(N9K-3의 Eth1/4)에서 시작되는 5개의 패킷이 수신되며 대상은 N9K-1의 Lo0(192.168.0.10)입니다.

```
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-2의 Eth1/3에 대한 관련 컨피그레이션.

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

- N9K-2에서 RACL은 N9K-2를 떠나 N9K-1로 전달되는 5개의 ICMP 요청 패킷을 보고합니다.
- PACL은 아웃바운드 방향을 지원하지 않으므로 RACL로 구성된 VLAN 10용 SVI에 구성된 다른 ACL(TAC-OUT-SVI)을 확인해야 합니다(아웃바운드 방향은 RACL에서 지원됨). VLAN 10은 N9K-2와 N9K-1 간의 연결을 제공합니다.

```
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
```

이전 결과를 기반으로 N9K-3에서 보낸 ICMP 요청 패킷에서는 패킷 손실이 없음을 확인합니다.

- 다음 단계는 다음 디바이스(대상 N9K-1)로 진행하여 N9K-3에서 동일한 수의 ICMP 요청 패킷이 수신되는지 확인하는 것입니다.
- RACL 통계는 N9K-2가 N9K-3에서 시작되는 5개의 ICMP 요청 패킷을 전송 중임을 나타냅니다.

```
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-1의 Eth1/1에 대한 관련 컨피그레이션.

```
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
```

- 이 정보에 따라 N9K-2에서 N9K-3에서 Lo0 192.168.0.10으로 패킷 손실(ICMP 요청)이 없음을 확인합니다.
- 다음 단계는 N9K-1 Lo0 192.168.0.10에서 시작되고 192.168.20.2에서 N9K-3으로 향하는 ICMP 응답 패킷을 추적하는 것입니다.
- 그런 다음 N9K-2로 진행하여 192.168.0.10에서 192.168.20.2로 5개의 ICMP 응답 패킷을 수

신하는지 확인해야 합니다.
- N9K-1에서 ICMP 응답 패킷을 추적하려면 Eth1/1에 구성된 PACL(TAC-IN)을 확인해야 합니다.

```
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
```

- 이전에 제공된 정보를 기반으로 N9K-1에서 N9K-2로의 트래픽에 패킷 손실이 없음을 확인합니다.
- 다음 단계는 N9K-2가 ICMP 응답 패킷을 N9K-3에 올바르게 보내고 있는지 확인하는 것입니다. PACL은 아웃바운드 방향을 지원하지 않으므로 RACL로 구성된 VLAN 20용 SVI에 구성된 다른 ACL(TAC-OUT-SVI)을 확인해야 합니다(아웃바운드 방향은 RACL에서 지원됨). VLAN 20은 N9K-2와 N9K-3 간의 연결을 제공합니다.

```
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
```

관련 구성:

```
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
```

위 출력의 ACL 카운터를 기반으로 N9K-1이 5개의 ICMP 응답 패킷을 N9K-2에 올바르게 보내고 있음을 확인합니다.

- N9K-2에서 N9K-3으로 패킷이 손실되지 않습니다.

- 마지막 단계는 트래픽의 소스인 N9K-3으로 진행하여 5개의 ICMP 응답 패킷을 수신하는지 확인하는 것입니다.
- 5개의 ICMP 패킷이 N9K-1 Lo0(192.168.0.10)에서 오는 ICMP 회신에 대한 ACL TAC-IN에 도달하는 것이 확인되었습니다.
  더 자세히 알아보려면 Eth1/4에 구성된 RACL(TAC-IN)을 검토해야 합니다.

```
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]
```

관련 구성:

```
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
```

- 앞서 설명한 트러블슈팅 단계를 사용하여, 패킷의 수신 및 발신 경로가 소스와 대상 간에 홉별로 검증되었습니다.

이 예에서는 5개의 ICMP 패킷이 모두 각 디바이스에서 제대로 수신되고 전달되었기 때문에 패킷 손실이 없음을 확인했습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.