NexusプラットフォームでのACLによるパケットドロップのトラブルシューティング

内容

はじめに

このドキュメントでは、Nexusプラットフォームでアクセスコントロールリスト(ACL)を使用してパケット損失をトラブルシューティングする方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

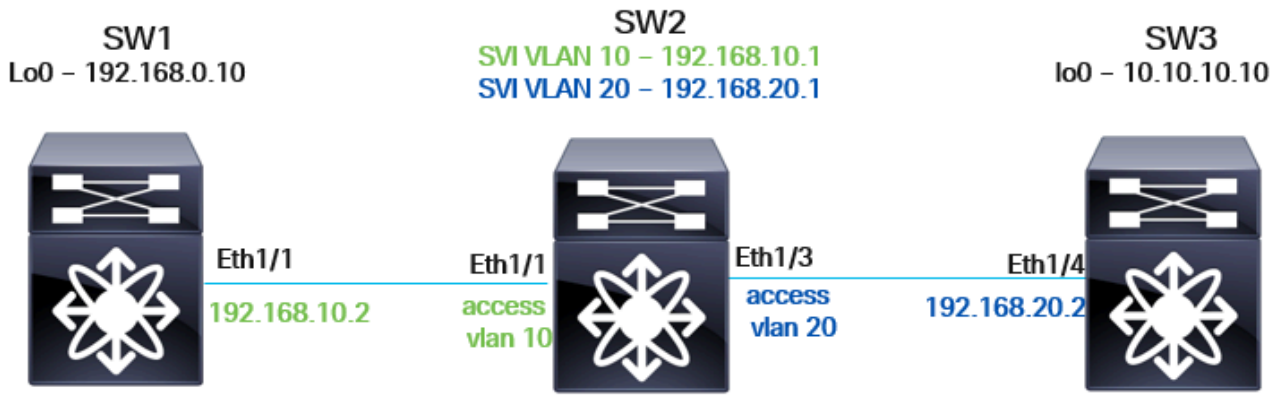
- NXOSプラットフォーム
- アクセス コントロール リスト

使用するコンポーネント

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

このドキュメントの情報は、ラボ環境のNexusデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、既存の設定を使用せずに作業を開始しています。実稼働中のネットワークを使用している場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

トポロジ



アクセスコントロールリストとその機能の概要

ACLは基本的に、一連の順序付けられたルールと基準に基づいてトラフィックをフィルタリングするために使用されます（たとえば、送信元/宛先IPアドレスに基づくフィルタリング）。 これらのルールは、パケットが特定の条件に一致するかどうかを判断し、許可するか拒否するかを決定します。 簡単に説明すると、ACLは、内部で設定されたルールに基づいて、ネットワークパケットの通過を許可するか、拒否するかを定義します。パケットが許可ルールの条件を満たす場合、Nexusスイッチによって処理されます。逆に、パケットがdeny条件に一致する場合、そのパケットは廃棄されます。

ACLの主な機能の1つは、パケットフローの統計カウンタを提供する機能です。これらのカウンタは、ACLルールに一致するパケットの数を追跡します。これは、パケット損失のシナリオをトラブルシューティングする際に非常に便利です。

たとえば、デバイスが特定の数のパケットを送信しているにもかかわらず、予想よりも受信が少ない場合、ACLからの統計カウンタは、ネットワーク内でパケットがドロップされているポイントを特定するのに役立ちます。

PACLおよびRACL

ACLの実装は、ACLがレイヤ2インターフェイス(PACL)、レイヤ3インターフェイス(RACL)、またはVLAN(VACL)に適用されるかによって異なります。 次に、これらの方式の簡単な比較を示します。

- ポートアクセスコントロールリスト(PACL):ACLはレイヤ2(L2)スイッチポートインターフェイスに適用されます。
- ルータアクセスコントロールリスト(RACL):ACLは、レイヤ3(L3)ルーテッドインターフェイスに適用されます。

ACL タイプ	インターフェイス	アクション	適用された方向
PACL	L2	スイッチポートインターフェイス ACLをトランクインターフェイスに適用すると、トランクで許可されるすべてのVLANのトラフィックがフィルタリングされます。	インバウンドのみ：インターフェイスに着信するトラフィック。
RACL	L3	SVI、物理L3、およびL3サブインターフェイス	着信および発信の両方：着信では、インターフェイスに着信するトラフィックがフィルタリングされます。発信では、インターフェイスから発信されるトラフィックがフィルタリングされます。

目的

送信されるすべてのパケットが正しく受信されていることを確認する必要があります。

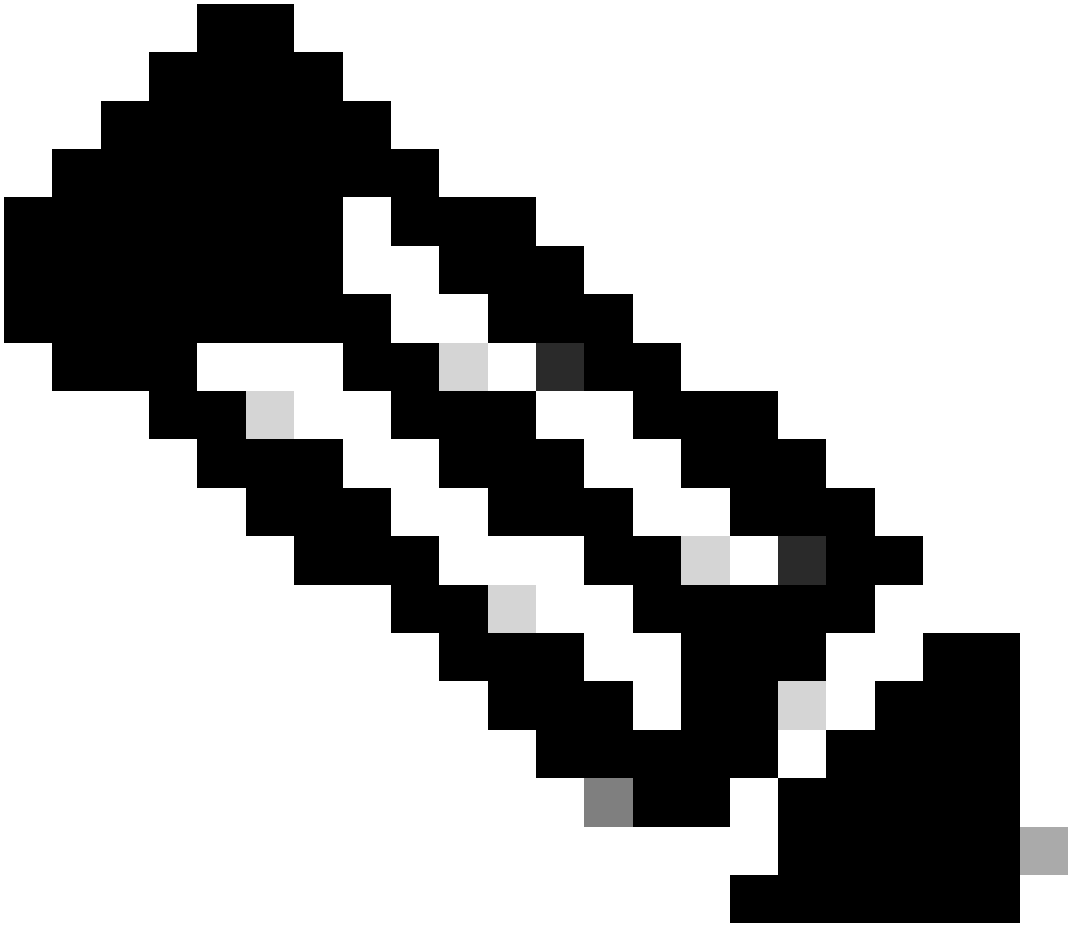
トポロジの説明

- N9K-1はN9K-2とL3接続されています。N9K-1のEth1/1インターフェイスはL3ルーテッドインターフェイスとして設定されていますが、N9K-2のEth1/1はVLAN 10のタグが付けられたL2スイッチポートインターフェイスです。
- N9K-2には、N9K-3とのL3接続もあります。N9K-2のEth1/3インターフェイスは、VLAN 20でタグ付けされたL2スイッチポートインターフェイスであり、N9K-3のEth1/4はL3ルーテッドインターフェイスとして設定されます。
- ループバック設定：N9K-1とN9K-2の両方にLo0インターフェイスが設定されています。これらのLo0インターフェイスは、2つのデバイス間でICMP pingパケットを送信するために使用されます。

トラブルシューティング

N9KデバイスでRACLおよびPACLを設定および検証するための詳細なプロセス手順を確認してください。 このプロセス中に、ポートアクセスコントロールリスト(PACL)とルータアクセスコントロールリストが確認され、パケットフローが分析されて、すべてのパケットが正しく送受信されているかどうかを判別します。

ステップ 1：N9K-1(Eth1/1)、N9K-2(SVI 10、SVI 20)、およびN9K-3(Eth1/14)のL3インターフェイスでのRACLの設定



注：発信パケットフローを確認するには、N9K-2で追加のACL設定が必要です。N9K-2にはL3物理ルーテッドインターフェイスがないため（代わりに、SVIおよびL2スイッチポートインターフェイスを備えています）、PACLは着信トラフィックのみをサポートします。

発信パケットの一致をキャプチャするために、新しいACLを作成してL3インターフェイスに適用できます。

ACLはN9K-1、N9K-2、およびN9K-3に適用する。

```
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
```

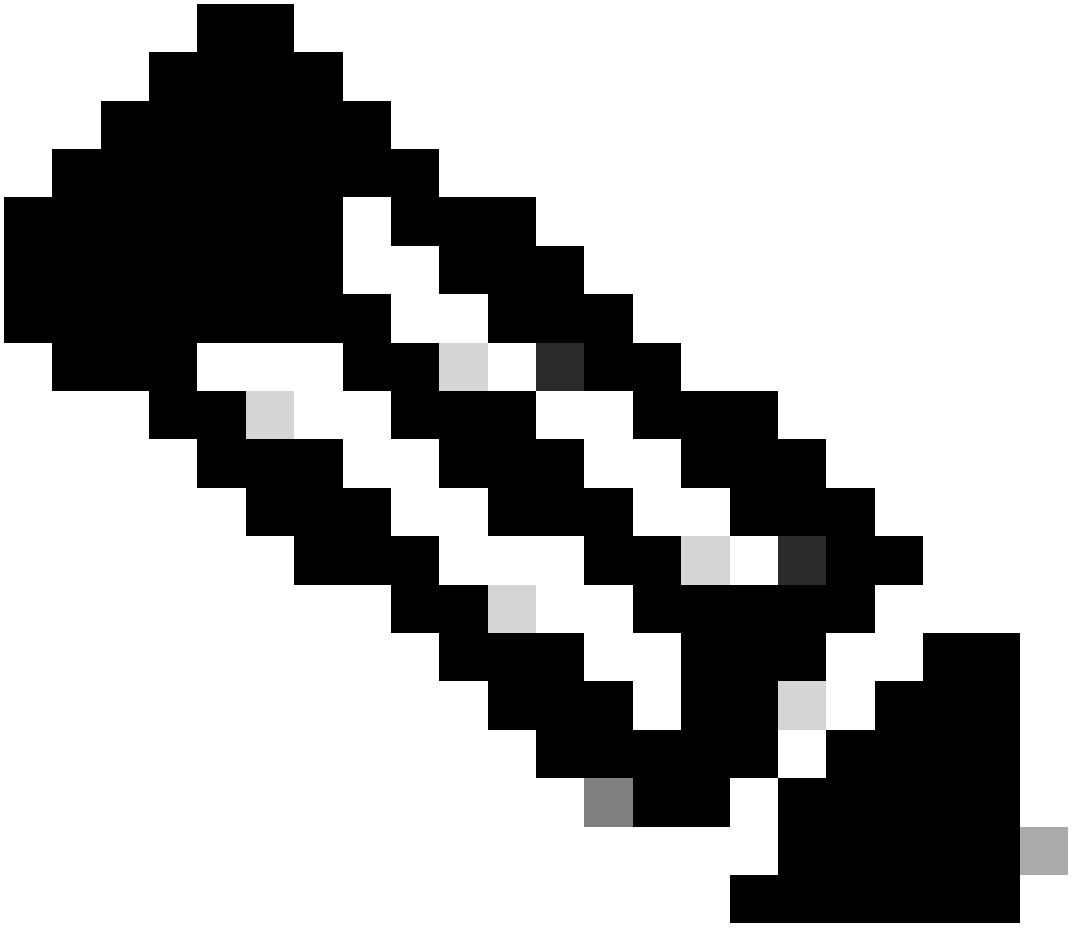
ステップ 2：N9K-2のL2スイッチポートインターフェイスでのPACLの設定

TCAMカービング

ACLタイプによっては、TCAMカービングが必要になる場合があります。詳細については、次を参照してください。

Nexus 9000 TCAMスペースの分割方法の理解

PACLをL2物理インターフェイスに適用するには、ip port access-group ....を設定する必要があります
ただし、TCAMリージョンの設定も必要です。



注：出力をクリーンな状態に保つために、特定の行が削除されています。

```
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リージョンの設定手順

ステップ 1：TCAMリージョンの変更

空き領域を提供できる領域を評価してください。これは、環境によって異なる場合があります。

```
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
```

検証のための代替方法。

```
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#
```

ステップ 2：領域のサイズを小さくする

ing-l3-vlan-qosに割り当てる領域のサイズを小さくします。（これは環境ごとに異なります）。

N9K-C93180YC-2(config)# hardware access-list tcam region ing-l3-vlan-qos 256 >>>割り当てを512から256に減らす。
構成を保存してシステムをリロードし、構成を有効にしてください。

ステップ 3：ing-ifaclのTCAM領域を増やす

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

設定を保存し、システムをリロードして設定を有効にします。

N9K-C93180YC-2(config)#

ステップ 4：save configuration

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

ステップ5：リロード

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

リロード後の検証

リロード後、変更が有効になったかどうかを確認します。

```
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
```

検証のための代替方法。

```
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ポートアクセスグループの設定

L2物理インターフェイスでip port access-groupを設定します。

```
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)#
```

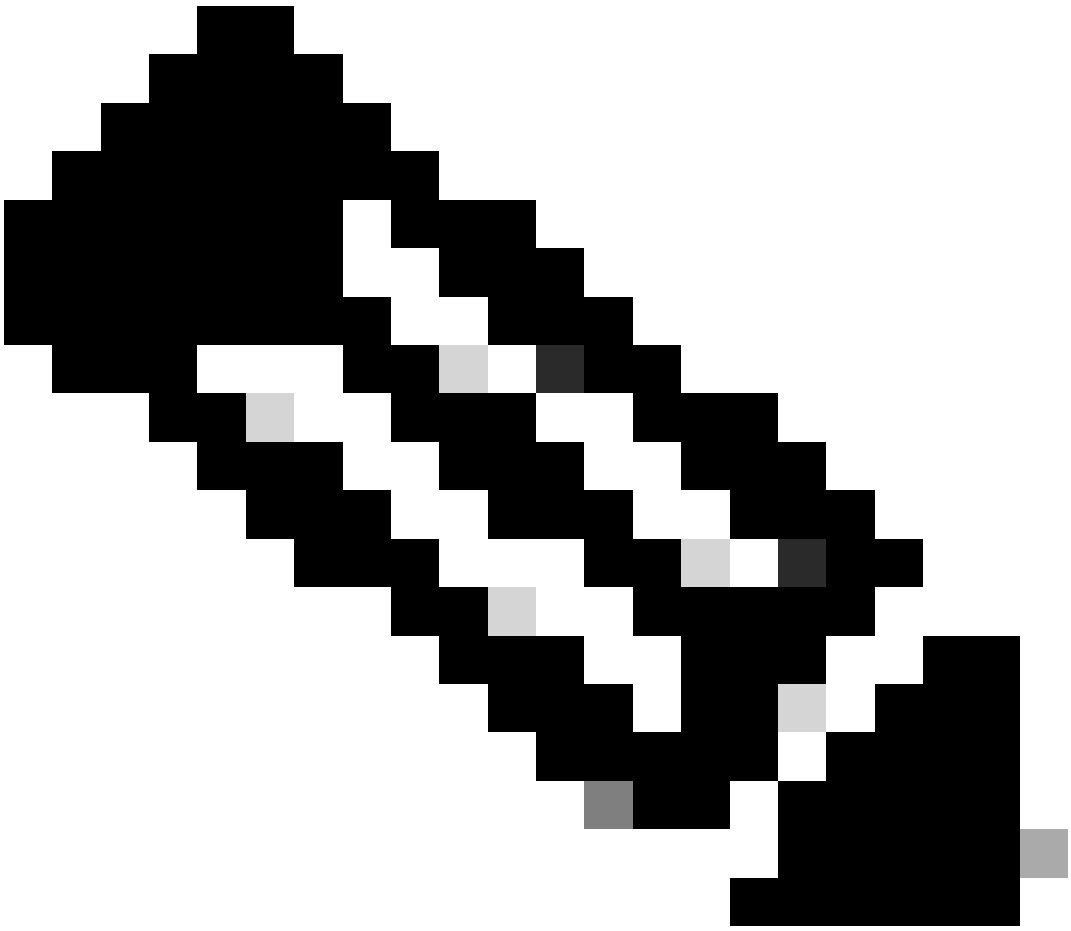
```
interface Ethernet1/1
description ***Link-to-N9K-1***
switchport
switchport access vlan 10
ip port access-group TAC-IN in >>> Inboud only
no shutdown
```

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

ステップ 3：ループバック

N9K-1は送信元としてLoopback0(Lo0)を使用し、N9K-3は宛先としてLoopback0(Lo0)を使用できます。
テスト目的で使用するループバックインターフェイスの実行コンフィギュレーションの詳細を次

に示します。



注：ルーティングプロトコルによるレイヤ3接続は以前に設定されています。

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


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

ステップ 4：トラフィックを生成し、送信元IP 192.168.20.2を使用してN9K-3からN9K-1のLo0 192.168.0.10にpingを送信する

```
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#
```

ステップ 5：N9K-1、N9K-2、およびN9K-3でのPACLおよびRACL統計情報の確認

- ICMPパケットはN9K-3から発信されるため、5つのICMP要求パケットがN9K-2によって受信されたことを確認する必要があります。
- N9K-2でのPACL検証：192.168.20.2（N9K-3のEth1/4）から発信された5つのパケットが受信され、宛先がN9K-1のLo0(192.168.0.10)になることが想定されます。

```
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のEth1/3の関連する設定。

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

- N9K-2で、RACLは5つのICMP要求パケットがN9K-2から送信され、N9K-1に転送されることを報告します。
- PACLはアウトバウンド方向をサポートしないため、VLAN 10のSVIで設定された他のACL(TAC-OUT-SVI)を確認することが不可欠です。これは、RACLとして設定されています（アウトバウンド方向はRACLでサポートされているためです）。 VLAN 10は、N9K-2とN9K-1の間の接続を提供します。

```
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
```

上記の結果から、N9K-3から送信されたICMP要求パケットにパケット損失がないことを確認しました。

- 次の手順では、次のデバイス（宛先N9K-1）に進み、N9K-3から同じ数のICMP要求パケットを受信していることを確認します。
- RACLの統計情報は、N9K-2がN9K-3から発信された5つのICMP要求パケットを送信していることを示しています。

```
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のEth1/1の関連する設定。

```
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
```

- この情報に基づいて、N9K-3からN9K-2上のLo0 192.168.0.10へのパケット損失（ICMP要求）が存在しないことが確認されました。
- 次のステップでは、N9K-1 Lo0 192.168.0.10から発信され、192.168.20.2でN9K-3に宛てら

れたICMP応答パケットを追跡します。
- 次にN9K-2に進み、192.168.0.10 ~ 192.168.20.2の5つのICMP応答パケットを受信しているかどうかを確認します。
- N9K-1からのICMP応答パケットを追跡するには、Eth1/1で設定されたPACL(TAC-IN)を確認する必要があります。

```
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
```

- 前述の情報に基づいて、N9K-1からN9K-2へのトラフィックでパケット損失が発生していないことが確認されました。
- 次の手順では、N9K-2がICMP応答パケットをN9K-3に正しく送信していることを確認します。PACLはアウトバウンド方向をサポートしていないため、（アウトバウンド方向がRACLでサポートされているため）RACLとして設定されているVLAN 20のSVIで設定された他のACL(TAC-OUT-SVI)を確認する必要があります。 VLAN 20は、N9K-2とN9K-3の間の接続を提供します。

```
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
```

関連する設定：

```
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
```

上記の出力からのACLカウンタに基づいて、N9K-1が5つのICMP応答パケットをN9K-2に正しく送信していることを確認できます。

- N9K-2からN9K-3へのパケット損失は発生していません。

- 最後のステップは、トラフィックの送信元N9K-3に進み、5つのICMP応答パケットを受信しているかどうかを確認することです。
- 5つのICMPパケットが、N9K-1 Lo0(192.168.0.10)からのICMP応答に対するACL TAC-INにヒットすることが確認されています。
  さらに調査するには、Eth1/4で設定されたRACL(TAC-IN)を確認する必要があります。

```
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]
```

関連する設定：

```
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
```

- 前に説明したトラブルシューティングの手順を使用して、パケットの着信パスと発信パスが、発信元と宛先の間でホップバイホップで検証されました。

この例では、5つのICMPパケットがすべて受信され、各デバイスで正しく転送されるため、パケット損失は発生しないことが確認されています。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。