Fehlerbehebung bei Paketverlusten mit ACLs auf der Nexus-Plattform

Inhalt

- Einleitung
- Voraussetzungen
  - Anforderungen
  - Verwendete Komponente
- Topologie
- Kurzübersicht zu Zugriffskontrolllisten und ihren Funktionen
  - PACL und RACL
- Ziel
- Topologie-Erläuterung
- Fehlerbehebung
  - Schritt 1: Konfigurieren der RACL auf L3-Schnittstellen von N9K-1 (Eth1/1), N9K-2 (SVI 10, SVI 20) und N9K-3 (Eth1/14)
  - Schritt 2: PACL auf L2-Switchport-Schnittstellen von N9K-2 konfigurieren
    - TCAM-Carving
  - Vorgehensweise zum Konfigurieren des TCAM-Bereichs
    - Schritt 1: Änderungen am TCAM-Bereich
    - Schritt 2: Verkleinern der Region
    - Schritt 3: Vergrößern Sie die TCAM-Region für die ING-Fakl.
    - Schritt 4: Konfiguration speichern
    - Schritt 5: Neuladen
    - Überprüfung nach dem Neuladen
    - Konfiguration der IP-Port-Zugriffsgruppe
  - Schritt 3: Loopback
  - Schritt 4: Generieren von Datenverkehr und Senden eines Pings von N9K-3 unter Verwendung der Quell-IP 192.168.20.2 an Lo0 192.168.0.10 von N9K-1
  - Schritt 5: Überprüfen der PACL- und RACL-Statistikinformationen für N9K-1, N9K-2 und N9K-3

Einleitung

In diesem Dokument wird die Fehlerbehebung bei Paketverlusten mithilfe von Zugriffskontrolllisten (Access Control Lists, ACLs) auf der Nexus-Plattform beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in den folgenden Bereichen verfügen:

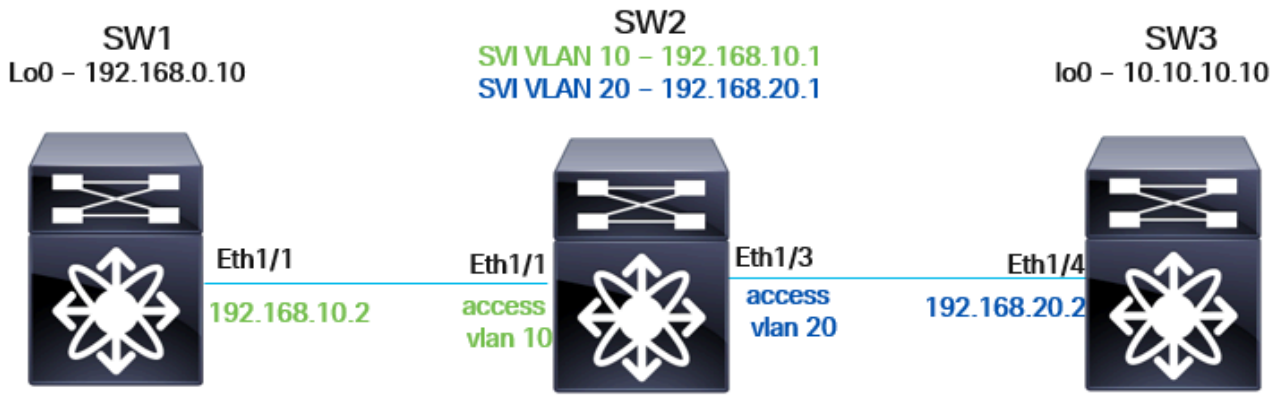
- NXOS-Plattform
- Zugriffskontrolllisten

Verwendete Komponente

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

Die Informationen in diesem Dokument stammen von Nexus-Geräten in einer Laborumgebung. Alle in diesem Dokument verwendeten Geräte wurden ohne vorherige Konfiguration gestartet. Wenn Sie ein Live-Netzwerk verwenden, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Topologie



Kurzübersicht zu Zugriffskontrolllisten und ihren Funktionen

Eine ACL wird im Wesentlichen verwendet, um Datenverkehr auf der Grundlage einer Reihe geordneter Regeln und Kriterien zu filtern (z. B. Filterung nach Quell-/Ziel-IP-Adressen). Anhand dieser Regeln wird bestimmt, ob Pakete bestimmten Bedingungen entsprechen, um zu entscheiden, ob sie zugelassen oder abgelehnt werden. Einfacher ausgedrückt, legt die ACL fest, ob Netzwerkpakete basierend auf den darin festgelegten Regeln passieren dürfen oder abgelehnt werden. Wenn die Pakete die Bedingungen der Genehmigungsregeln erfüllen, werden sie vom Nexus-Switch verarbeitet. Entsprechen die Pakete hingegen den Deny-Bedingungen, werden sie verworfen.

Ein wichtiges Merkmal von ACLs ist die Fähigkeit, statistische Zähler für den Paketfluss bereitzustellen. Diese Zähler verfolgen die Anzahl der Pakete, die mit den ACL-Regeln übereinstimmen. Dies kann bei der Fehlerbehebung von Szenarien mit Paketverlusten sehr

nützlich sein.

Wenn beispielsweise ein Gerät eine bestimmte Anzahl von Paketen sendet, aber weniger als erwartet empfängt, können die statistischen Zähler der ACL dabei helfen, den Punkt zu isolieren, an dem Pakete innerhalb des Netzwerks verworfen werden.

PACL und RACL

Die Implementierung von ACLs kann variieren, je nachdem, ob sie auf Layer-2-Schnittstellen (PACL), Layer-3-Schnittstellen (RACL) oder VLANs (VACL) angewendet werden. Im Folgenden finden Sie einen kurzen Vergleich dieser Methoden:

- Port-Zugriffskontrollliste (PACL): Die ACL wird auf eine Layer 2 (L2)-Switch-Port-Schnittstelle angewendet.
- Router Access Control List (RACL): Die ACL wird auf eine geroutete Layer-3-Schnittstelle (L3) angewendet.

ACL-Typ	Schnittstelle	Aktion	Angewendete Richtung
PACL	L2	Switchport-Schnittstellen Wenn die ACL auf eine Trunk-Schnittstelle angewendet wird, wird der Datenverkehr für alle auf dem Trunk zulässigen VLANs gefiltert.	Eingehend - nur Datenverkehr, der an die Schnittstelle gelangt.
RACL	Anschluss 3	SVI-, physische L3- und L3-Subschnittstellen	Eingehend und ausgehend: Eingehender Datenverkehr filtert den an die Schnittstelle eingehenden Datenverkehr, während der ausgehende Datenverkehr die Schnittstelle verlässt.

Ziel

Es muss sichergestellt werden, dass alle gesendeten Pakete korrekt empfangen wurden.

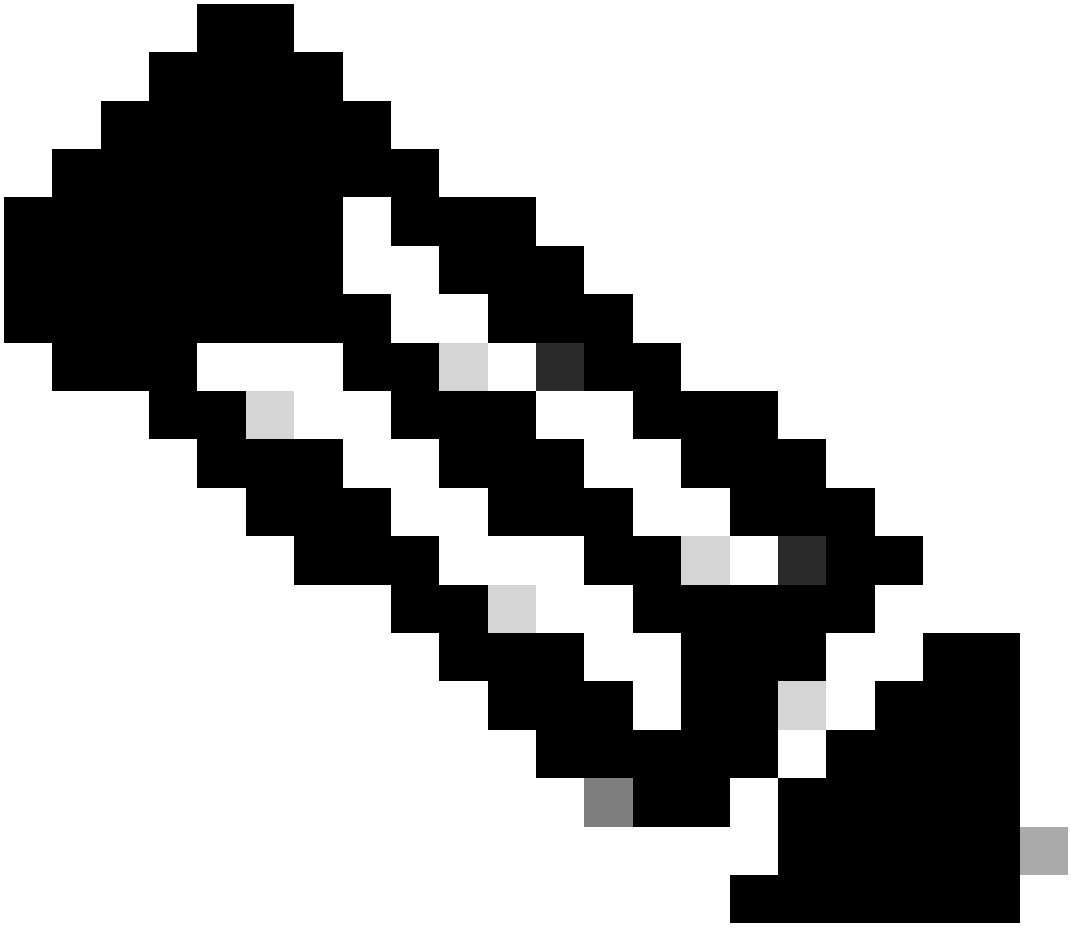
Topologie-Erläuterung

- N9K-1 verfügt über L3-Verbindungen mit N9K-2. Die Eth1/1-Schnittstelle auf N9K-1 ist als L3-Router-Schnittstelle konfiguriert, während die Eth1/1-Schnittstelle von N9K-2 eine L2-Switch-Port-Schnittstelle ist, die mit VLAN 10 gekennzeichnet ist.
- N9K-2 verfügt auch über L3-Verbindungen mit N9K-3. Die Eth1/3-Schnittstelle auf N9K-2 ist eine L2-Switch-Port-Schnittstelle, die mit VLAN 20 gekennzeichnet ist, und die Eth1/4-Schnittstelle von N9K-3 ist als L3-geroutete Schnittstelle konfiguriert.
- Loopback-Konfiguration: Für N9K-1 und N9K-2 ist die Lo0-Schnittstelle konfiguriert. Diese Lo0-Schnittstellen werden zum Senden von ICMP-Ping-Paketen zwischen den beiden Geräten verwendet.

Fehlerbehebung

Hier finden Sie die detaillierten Prozessschritte für die Konfiguration und Verifizierung von RACL und PACL auf den N9K-Geräten. Während dieses Prozesses werden die Portzugriffskontrolllisten und die Router-Zugriffskontrolllisten überprüft, um den Paketfluss zu analysieren und festzustellen, ob alle Pakete korrekt übertragen und empfangen werden.

Schritt 1: Konfigurieren der RACL auf L3-Schnittstellen von N9K-1 (Eth1/1), N9K-2 (SVI 10, SVI 20) und N9K-3 (Eth1/14)



Anmerkung: Zur Überwachung des ausgehenden Paketflusses ist eine zusätzliche ACL-Konfiguration auf N9K-2 erforderlich. Da N9K-2 keine physischen L3-Routing-Schnittstellen aufweist (stattdessen verfügt es über SVI- und L2-Switch-Port-Schnittstellen), unterstützt PACL nur eingehenden Datenverkehr.

Zum Erfassen von Übereinstimmungen mit ausgehenden Paketen kann eine neue ACL erstellt und auf die L3-Schnittstellen angewendet werden.

Die ACL wird auf N9K-1, N9K-2 und N9K-3 angewendet.

```
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
```

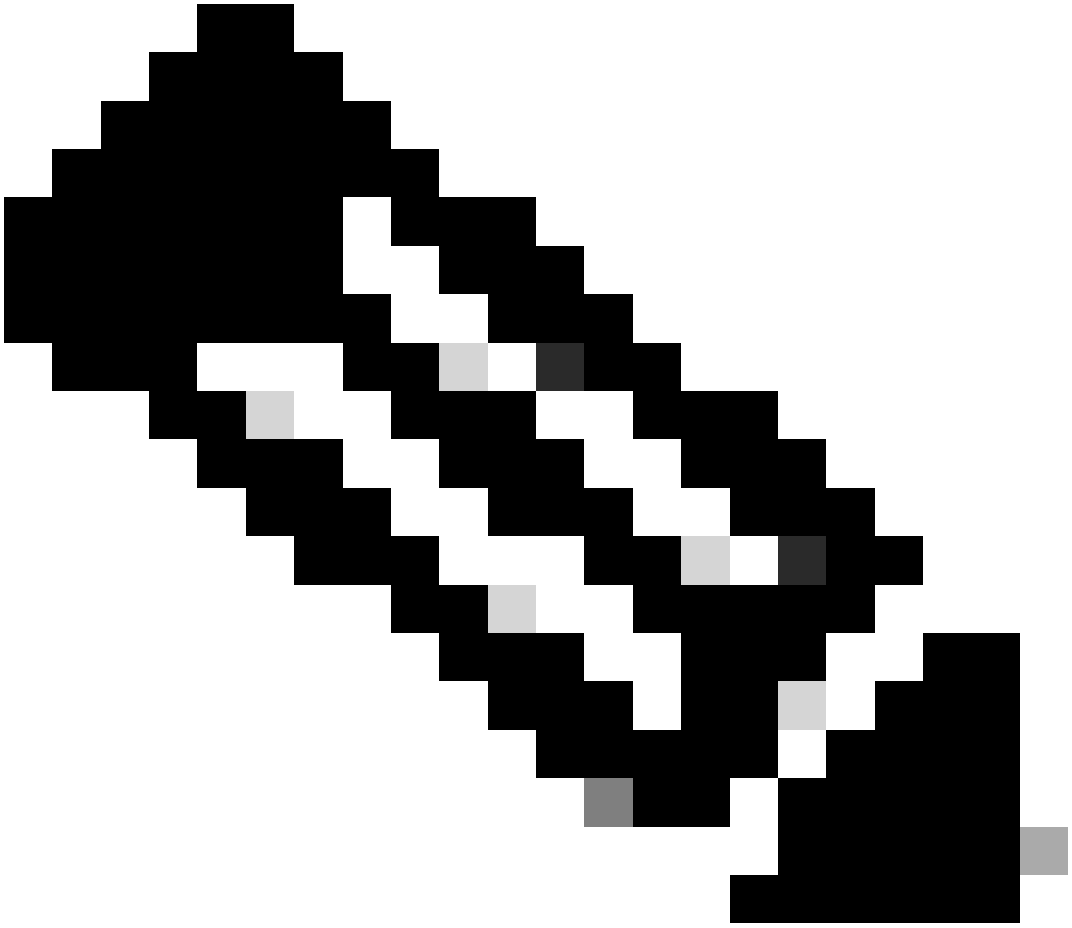
Schritt 2: PACL auf L2-Switchport-Schnittstellen von N9K-2 konfigurieren

TCAM-Carving

Je nach ACL-Typ ist möglicherweise eine TCAM-Partitionierung erforderlich. Weitere Informationen finden Sie unter:

Nexus 9000 TCAM-Platz schaffen

Um die PACL auf physische L2-Schnittstellen anzuwenden, muss eine IP-Port-Zugriffsgruppe konfiguriert werden..
Es ist jedoch auch eine Konfiguration des TCAM-Bereichs erforderlich.



Anmerkung: Einige Zeilen wurden entfernt, um die Ausgabe sauber zu halten.

```
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)#
```

Vorgehensweise zum Konfigurieren des TCAM-Bereichs

Schritt 1: Änderungen am TCAM-Bereich

Bitte bewerten Sie, welche Region freien Speicherplatz bieten kann, da sich dieser je nach Umgebung unterscheiden kann.

```
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
```

Eine alternative Überprüfungsmethode.

```
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#
```

Schritt 2: Verkleinern der Region

Reduzieren Sie die Größe der Region, die für ing-l3-vlan-qos zugewiesen ist. (Dies ist je nach Umgebung unterschiedlich.)

N9K-C93180YC-2(config)# hardware access-list tcam region ing-l3-vlan-qos 256 >>> Reduzieren Sie die Zuweisung von 512 auf 256.
Speichern Sie die Konfiguration, und laden Sie das System neu, damit die Konfiguration wirksam wird.

Schritt 3: Vergrößern Sie die TCAM-Region für die ING-Fakl.

N9K-C93180YC-2(config)# Hardware-Zugriffsliste tcam region ing-ifacl 256

Speichern Sie die Konfiguration, und laden Sie das System neu, damit die Konfiguration wirksam wird.

N9K-C93180YC-2(config)#

Schritt 4: Konfiguration speichern

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

Schritt 5: Neu laden

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

Überprüfung nach dem Neuladen

Überprüfen Sie nach dem Neuladen, ob die Änderungen übernommen wurden.

```
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
```

Eine alternative Überprüfungsmethode.

```
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#
```

Konfiguration der IP-Port-Zugriffsgruppe

Konfigurieren Sie die Zugriffsgruppe "ip port" an den physischen L2-Schnittstellen.

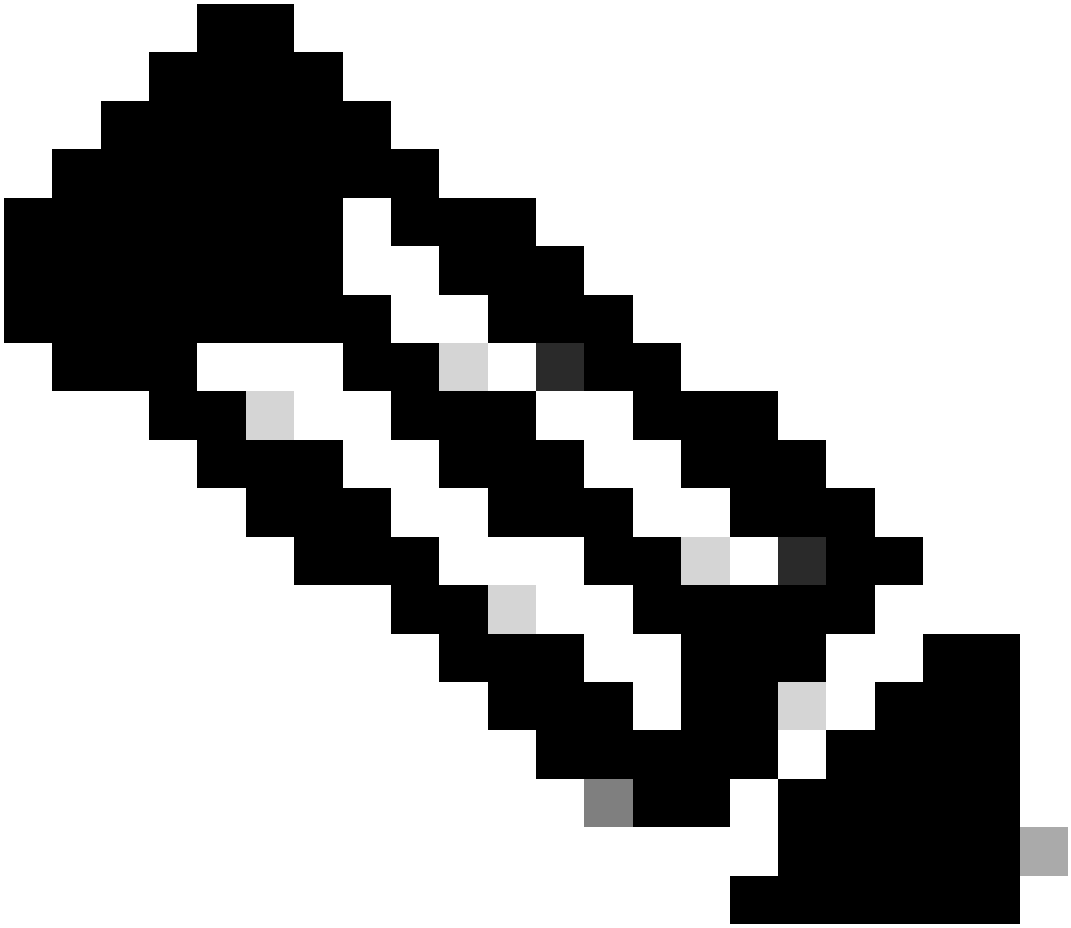
```
N9K-C93180YC-2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
N9K-C93180YC-2(config)# int e1/2,e1/51
N9K-C93180YC-2(config-if-range)# ip port access-group TAC-IN in
N9K-C93180YC-2(config-if-range)# ip port access-group TAC-OUT out
Port ACL is only supported on ingress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

Schritt 3: Loopback

N9K-1 verwendet Loopback0 (Lo0) als Quelle, während N9K-3 Loopback0 (Lo0) als Ziel verwenden kann.
Die Konfiguration der Loopback-Schnittstellen, die Sie zu Testzwecken verwenden, wird im Folgenden ausführlich beschrieben.



Anmerkung: Layer-3-Verbindungen mit einem Routing-Protokoll wurden zuvor konfiguriert.

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

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

Schritt 4: Generieren von Datenverkehr und Senden eines Pings von N9K-3 unter Verwendung der Quell-IP 192.168.20.2 an Lo0 192.168.0.10 von 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#
```

Schritt 5: Überprüfen der PACL- und RACL-Statistikinformationen für N9K-1, N9K-2 und N9K-3

- Da die ICMP-Pakete von N9K-3 stammen, muss überprüft werden, ob die fünf ICMP-Anforderungspakete von N9K-2 empfangen wurden.
- PACL-Verifizierung auf N9K-2: Es wird erwartet, dass fünf Pakete von 192.168.20.2 (Eth1/4 von N9K-3) empfangen werden, wobei das Ziel Lo0 (192.168.0.10) von N9K-1 ist.

```
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]
```

Zugehörige Konfiguration auf Eth1/3 von 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
```

- Auf N9K-2 meldet die RACL 5 ICMP-Anforderungspakete, die N9K-2 verlassen und an N9K-1 weitergeleitet werden.
- Da PACL die ausgehende Richtung nicht unterstützt, muss die andere ACL (TAC-OUT-SVI), die auf der SVI für VLAN 10 konfiguriert ist und als RACL konfiguriert ist, überprüft werden (da die ausgehende Richtung auf RACLs unterstützt wird). VLAN 10 stellt die Verbindung zwischen N9K-2 und N9K-1 her.

```
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
```

Anhand der vorherigen Ergebnisse wird bestätigt, dass bei den von N9K-3 gesendeten ICMP-Anforderungspaketen kein Paketverlust auftritt.

- Der nächste Schritt besteht darin, mit dem nächsten Gerät (Ziel N9K-1) fortzufahren und zu überprüfen, ob die gleiche Anzahl von ICMP-Anforderungspaketen von N9K-3 empfangen wird.
- Die RACL-Statistiken zeigen an, dass N9K-2 5 ICMP-Anforderungspakete von N9K-3 sendet.

```
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]
```

Zugehörige Konfiguration auf Eth1/1 von 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
```

- Anhand der Informationen wird bestätigt, dass auf N9K-2 kein Paketverlust (ICMP-Anforderung) von N9K-3 zu Lo0 192.168.0.10 auftritt.
- Im nächsten Schritt werden die ICMP-Antwortpakete verfolgt, die von N9K-1 Lo0 192.168.0.10 stammen und für N9K-3 unter 192.168.20.2 bestimmt sind.
- Anschließend muss N9K-2 aufgerufen und überprüft werden, ob die fünf ICMP-Antwortpakete von 192.168.0.10 bis 192.168.20.2 empfangen werden.
- Um die ICMP-Antwortpakete von N9K-1 zu verfolgen, muss die für Eth1/1 konfigurierte PACL (TAC-IN) überprüft werden.

```
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
```

- Auf der Grundlage der zuvor bereitgestellten Informationen wird bestätigt, dass beim Datenverkehr von N9K-1 zu N9K-2 kein Paketverlust auftritt.
- Der nächste Schritt besteht darin, zu bestätigen, dass N9K-2 die ICMP-Antwortpakete ordnungsgemäß an N9K-3 sendet. Da PACL die ausgehende Richtung nicht unterstützt, muss die andere ACL (TAC-OUT-SVI) überprüft werden, die auf der SVI für VLAN 20 konfiguriert ist und als RACL konfiguriert ist (da die ausgehende Richtung auf RACLs unterstützt wird). VLAN 20 stellt die Verbindung zwischen N9K-2 und N9K-3 bereit.

```
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
```

Zugehörige Konfiguration:

```
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
```

Basierend auf den ACL-Zählern der oben genannten Ausgaben wird bestätigt, dass N9K-1 die fünf ICMP-Antwortpakete ordnungsgemäß an N9K-2 sendet.

- Zwischen N9K-2 und N9K-3 tritt kein Paketverlust auf.

- Der letzte Schritt besteht darin, zur Quelle des Datenverkehrs, N9K-3, zu gelangen und zu überprüfen, ob die fünf ICMP-Antwortpakete empfangen werden.
- Es wird bestätigt, dass die fünf ICMP-Pakete die ACL-TAC-IN für die ICMP-Antworten von N9K-1 Lo0 (192.168.0.10) erreichen.
  Für weitere Untersuchungen ist es erforderlich, die auf Eth1/4 konfigurierte RACL (TAC-IN) zu überprüfen.

```
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]
```

Zugehörige Konfiguration:

```
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
```

- Mithilfe der oben beschriebenen Schritte zur Fehlerbehebung wurde der ein- und ausgehende Pfad des Pakets auf Hop-by-Hop-Basis zwischen Quelle und Ziel validiert.

Bei diesem Beispiel wurde bestätigt, dass kein Paketverlust auftritt, da alle 5 ICMP-Pakete auf jedem Gerät korrekt empfangen und weitergeleitet wurden.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.