Resolución de problemas de paquetes descartados con ACL en la plataforma Nexus

Contenido

Introducción

Este documento describe cómo resolver problemas de pérdida de paquetes mediante listas de control de acceso (ACL) en la plataforma Nexus.

Prerequisites

Requirements

Cisco recomiendaque tenga conocimientos sobre estos temas:

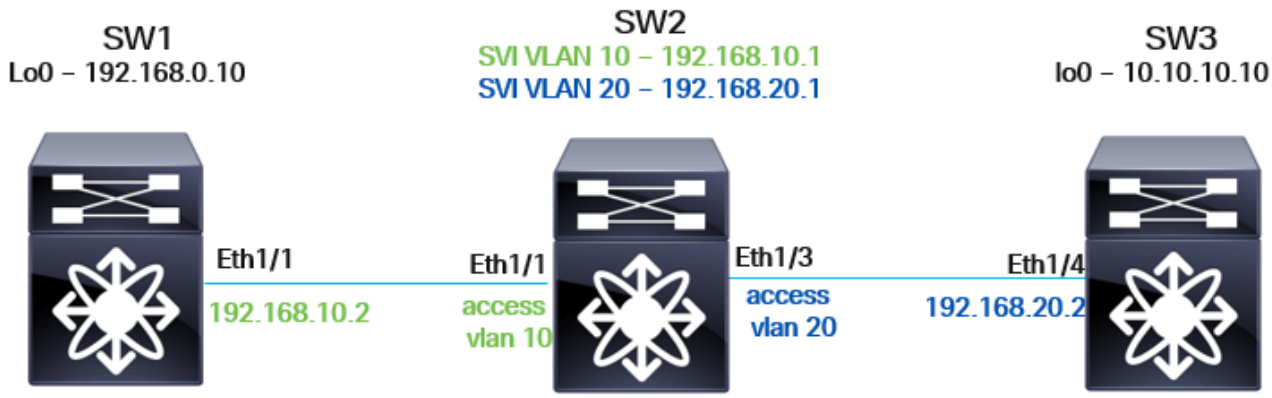
- Plataforma NXOS
- Listas de control de acceso

Componente utilizado

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

La información de este documento se ha creado a partir de dispositivos Nexus en un entorno de laboratorio. Todos los dispositivos utilizados en este documento se iniciaron sin ninguna configuración preexistente. Si utiliza una red activa, asegúrese de comprender el impacto potencial de cualquier comando.

Topología



Breve descripción general de las listas de control de acceso y su funcionalidad

Una ACL se utiliza básicamente para filtrar el tráfico según una serie de reglas y criterios ordenados (por ejemplo, filtrado basado en direcciones IP de origen/destino). Estas reglas determinan si los paquetes cumplen con condiciones específicas para decidir si se les debe permitir o denegar. En términos más sencillos, la ACL define si se puede permitir que los paquetes de red pasen o se les puede denegar en función de las reglas establecidas en ella. Si los paquetes cumplen las condiciones de las normas de autorización, serán procesados por el switch Nexus. Por el contrario, si los paquetes cumplen las condiciones de denegación, se descartarán.

Una característica clave de las ACL es su capacidad de proporcionar contadores estadísticos

para el flujo de paquetes. Estos contadores realizan un seguimiento del número de paquetes que coinciden con las reglas ACL, lo que puede ser muy útil para solucionar problemas de escenarios de pérdida de paquetes.

Por ejemplo, si un dispositivo está enviando un cierto número de paquetes, pero recibiendo menos de lo esperado, los contadores estadísticos de la ACL pueden ayudar a aislar el punto en el que los paquetes se descartan dentro de la red.

PACL y RACL

La implementación de las ACL puede variar en función de si se aplican a interfaces de capa 2 (PACL), interfaces de capa 3 (RACL) o VLAN (VACL). A continuación se ofrece una breve comparación de estos métodos:

- Lista de control de acceso a puertos (PACL): La ACL se aplica a una interfaz de puerto de switch de capa 2 (L2).
- Lista de control de acceso al router (RACL): La ACL se aplica a una interfaz enrutada de capa 3 (L3).

Tipo de ACL	Interfaz	Acción	Dirección aplicada
PACL	L2	Interfaces de puertos de switch Si la ACL se aplica a una interfaz de trunk, filtra el tráfico para todas las VLAN permitidas en el trunk.	Sólo entrante: tráfico entrante en la interfaz.
RACL	L3	Subinterfaces SVI, física L3 y L3	Entrante y saliente: filtra el tráfico entrante que entra en la interfaz y el saliente lo filtra cuando sale de la interfaz.

Objetivo

Es necesario confirmar que todos los paquetes que se envían se reciben correctamente.

Explicación de topología

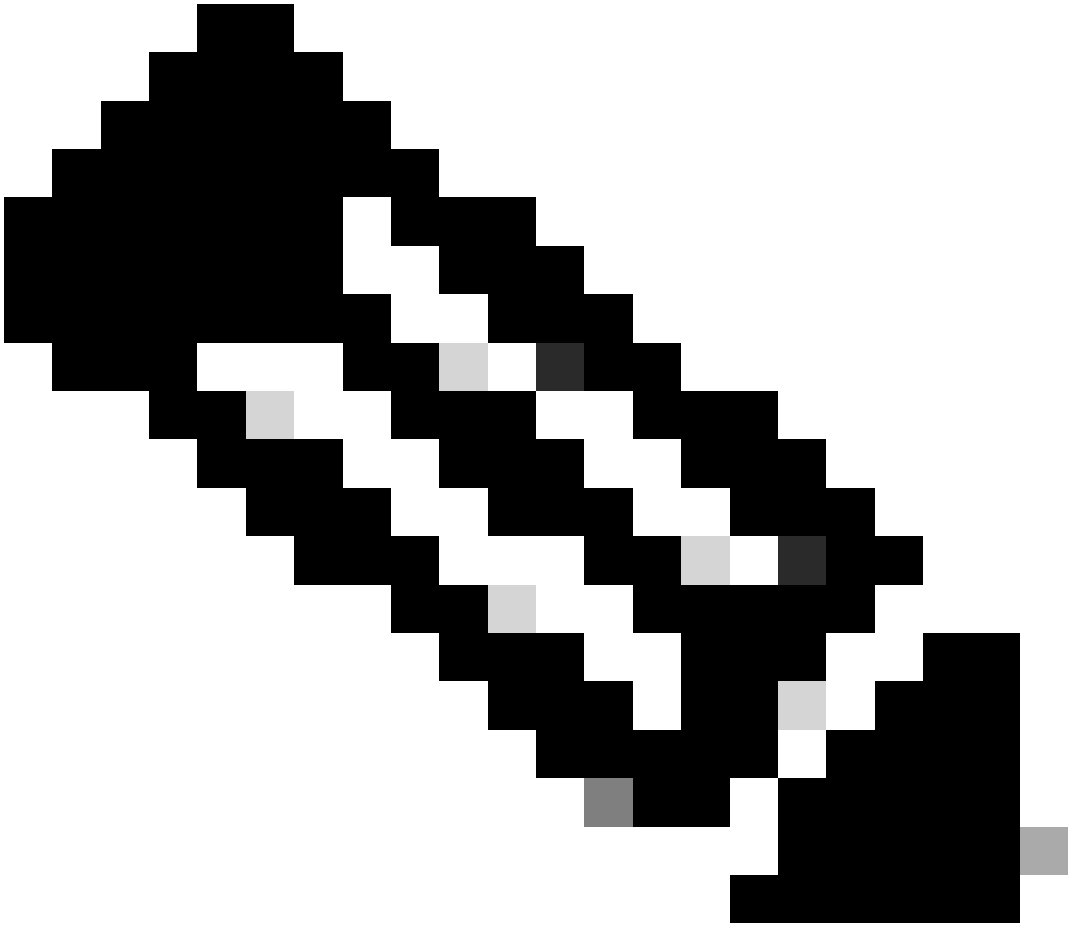
- N9K-1 tiene conectividad L3 con N9K-2. La interfaz Eth1/1 en N9K-1 está configurada como

interfaz enrutada L3, mientras que la Eth1/1 de N9K-2 es una interfaz de puerto de switch L2, etiquetada con VLAN 10.
- N9K-2 también tiene conectividad L3 con N9K-3. La interfaz Eth1/3 en N9K-2 es una interfaz de puerto de switch L2 etiquetada con VLAN 20, y la Eth1/4 de N9K-3 se configura como una interfaz enrutada L3.
- Configuración de loopback: Tanto N9K-1 como N9K-2 tienen configurada la interfaz Lo0. Estas interfaces Lo0 se utilizarán para enviar paquetes ping ICMP entre los dos dispositivos.

Resolución de problemas

Busque los pasos detallados del proceso para configurar y verificar RACL y PACL en los dispositivos N9K. Durante este proceso, se revisan las listas de control de acceso a puertos y las listas de control de acceso a routers para analizar el flujo de paquetes y determinar si todos los paquetes se transmiten y reciben correctamente.

Paso 1. Configure el RACL en las Interfaces L3 de N9K-1 (Eth1/1), N9K-2 (SVI 10, SVI 20) y N9K-3 (Eth1/14)



Nota: Para observar el flujo de paquetes salientes, se necesita una configuración ACL adicional en N9K-2. Dado que N9K-2 carece de interfaces enrutadas físicas L3 (en su lugar, tiene interfaces de puertos de switch SVI y L2), PACL sólo admite tráfico entrante.

Para capturar coincidencias de paquetes salientes, se puede crear una nueva ACL y aplicarla a las interfaces L3.

La ACL se aplicará a N9K-1, N9K-2 y 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
```

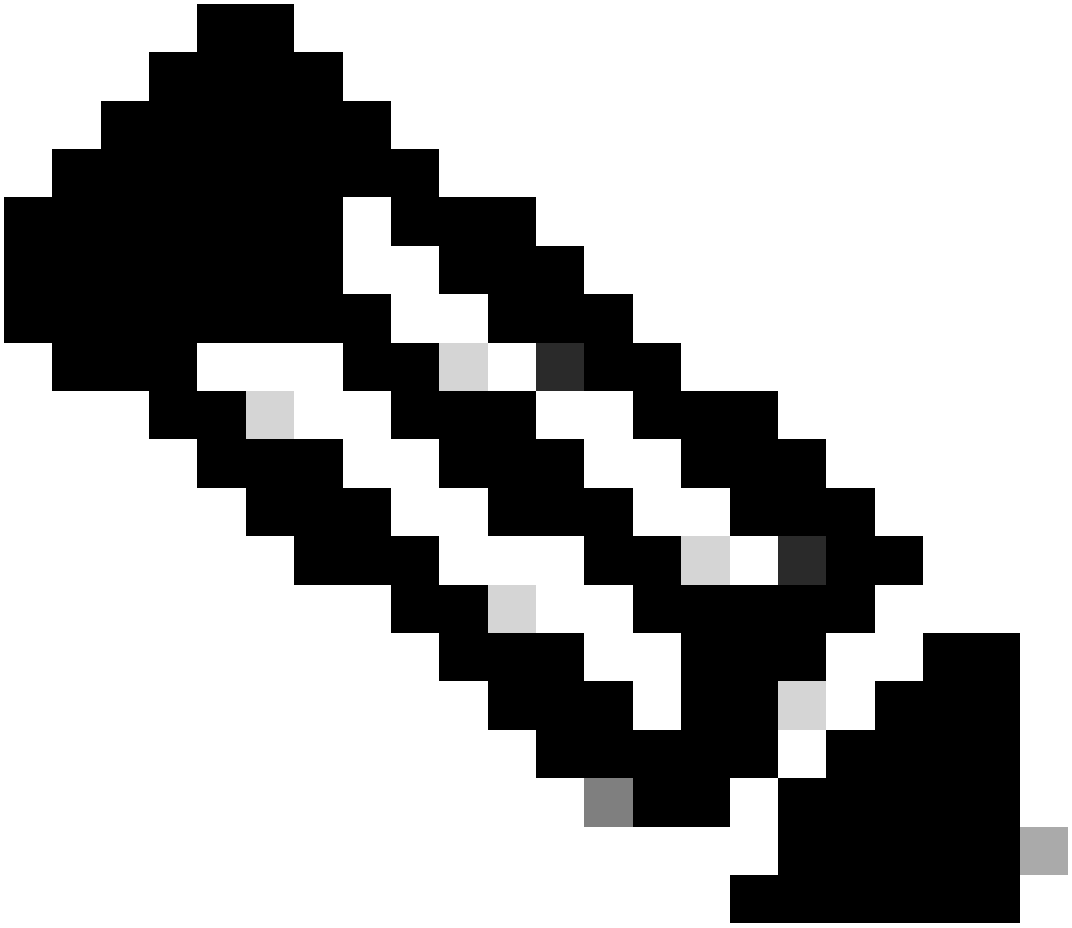
Paso 2. Configuración de PACL en las Interfaces de Switchport L2 de N9K-2

TCAM tallado

Se puede requerir la división TCAM dependiendo del tipo de ACL. Para obtener más información, consulte:

Comprender cómo dividir el espacio TCAM de Nexus 9000

Para aplicar el PACL a las interfaces físicas L2, es necesario configurar un ip port access-group ....
Sin embargo, también es necesario configurar la región TCAM.



Nota: Se han eliminado algunas filas para mantener el resultado limpio.

```
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)#
```

Procedimiento para configurar la región TCAM

Paso 1. Modificaciones de la región TCAM

Por favor, evalúe qué región puede proporcionar espacio libre, ya que esto puede diferir para cada entorno.

```
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
```

Método alternativo de verificación.

```
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#
```

Paso 2. Reduzca el tamaño de la región

Reduzca el tamaño de la región asignada para ing-l3-vlan-qos. (Esto difiere para cada entorno.)

N9K-C93180YC-2(config)# hardware access-list tcam region ing-l3-vlan-qos 256 **>>>** Reduzca la asignación de 512 a 256.
Guarde la configuración y vuelva a cargar el sistema para que la configuración surta efecto.

Paso 3. Aumente la Región TCAM para ing-ifacl

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

Guarde la configuración y vuelva a cargar el sistema para que la configuración surta efecto.

N9K-C93180YC-2(config)#

Paso 4. Guardar configuración

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

Paso 5. Recargar

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

Verificación posterior a la recarga

Después de la recarga, compruebe si los cambios han surtido efecto.

```
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
```

Método alternativo de verificación.

```
N9K-C93180YC-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#
```

Configuración del Grupo de Acceso al Puerto IP

Configure el grupo de acceso al puerto IP en las interfaces físicas L2.

```
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)#
```

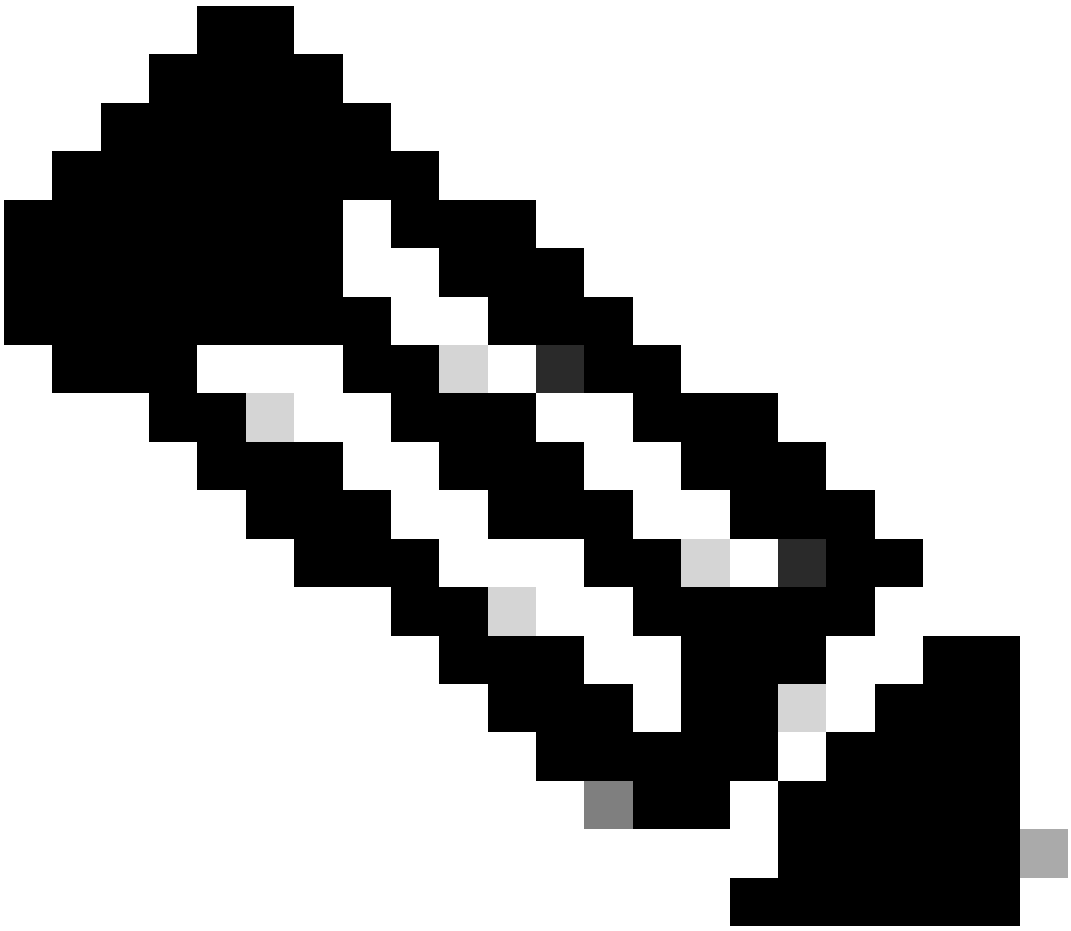
```
interface Ethernet1/1
description ***Link-to-N9K-1***
switchport
switchport access vlan 10
ip port access-group TAC-IN in >>> Inboud only
no shutdown
```

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

Paso 3. Bucle invertido

N9K-1 utilizará su loopback0 (Lo0) como origen, mientras que N9K-3 puede utilizar su loopback0 (Lo0) como destino.
La configuración en ejecución de las interfaces de loopback que utiliza para realizar pruebas se

detalla de la siguiente manera.



Nota: La conectividad de capa 3 con un protocolo de routing se ha configurado previamente.

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

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

Paso 4. Generar tráfico y enviar un ping desde N9K-3 usando la IP de origen 192.168.20.2 a Lo0 192.168.0.10 de 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#
```

Paso 5. Verificar la Información de Estadísticas de PACL y RACL en N9K-1, N9K-2 y N9K-3

- Dado que los paquetes ICMP se originan en N9K-3, es necesario verificar que los cinco paquetes de solicitud ICMP han sido recibidos por N9K-2.
- Verificación de PACL en N9K-2: Se espera que se reciban cinco paquetes que se originan en 192.168.20.2 (Eth1/4 de N9K-3), siendo el destino Lo0 (192.168.0.10) de N9K-1.

```
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]
```

Configuración relacionada en Eth1/3 de 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
```

- En N9K-2, la RACL informa 5 paquetes de solicitud ICMP que salen de N9K-2 y se reenvían a N9K-1.
- Dado que PACL no soporta la dirección saliente, es esencial verificar la otra ACL (TAC-OUT-SVI) configurada en la SVI para VLAN 10, que está configurada como RACL (ya que la dirección saliente es soportada en RACL). VLAN 10 proporciona la conectividad entre N9K-

2 y N9K-1.

```
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
```

Según los resultados anteriores, se confirma que no hay pérdida de paquetes con los paquetes de solicitud ICMP enviados desde N9K-3.

- El siguiente paso es continuar con el siguiente dispositivo (destino N9K-1) y verificar que se reciba el mismo número de paquetes de solicitud ICMP desde N9K-3.
- Las estadísticas de RACL indican que N9K-2 está enviando 5 paquetes de solicitud ICMP que se originan en N9K-3.

```
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]
```

Configuración relacionada en Eth1/1 de 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
```

- Basándose en la información, se confirma que no hay pérdida de paquetes (solicitud ICMP) de N9K-3 a Lo0 192.168.0.10 en N9K-2.
- El siguiente paso es rastrear los paquetes de respuesta ICMP que se originan en N9K-1 Lo0 192.168.0.10 y que están destinados a N9K-3 en 192.168.20.2.
- Luego, es necesario continuar con N9K-2 y verificar si está recibiendo los cinco paquetes de respuesta ICMP de 192.168.0.10 a 192.168.20.2.
- Para rastrear los paquetes de respuesta ICMP de N9K-1, se requiere verificar el PACL (TAC-IN) configurado en Eth1/1.

```
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
```

- Basándose en la información proporcionada anteriormente, se confirma que no hay pérdida de paquetes en el tráfico de N9K-1 a N9K-2.
- El siguiente paso es confirmar que N9K-2 está enviando correctamente los paquetes de respuesta ICMP a N9K-3. Dado que PACL no admite la dirección saliente, es necesario verificar la otra ACL (TAC-OUT-SVI) configurada en la SVI para VLAN 20, que está configurada como RACL (ya que la dirección saliente es compatible con RACL). VLAN 20 proporciona la conectividad entre N9K-2 y N9K-3.

```
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
```

Configuración relacionada:

```
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
```

Según los contadores ACL de las salidas anteriores, se confirma que N9K-1 está enviando correctamente los cinco paquetes de respuesta ICMP a N9K-2.

- No se produce ninguna pérdida de paquetes desde N9K-2 a N9K-3.

- El paso final es continuar con el origen del tráfico, N9K-3, y verificar si está recibiendo los cinco paquetes de respuesta ICMP.
- Se confirma que los cinco paquetes ICMP están alcanzando el TAC-IN de ACL para las respuestas ICMP provenientes de N9K-1 Lo0 (192.168.0.10).
  Para investigar más a fondo, es necesario revisar el RACL (TAC-IN) configurado en Eth1/4.

```
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]
```

Configuración relacionada:

```
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
```

- Mediante los pasos de solución de problemas descritos anteriormente, la ruta entrante y saliente del paquete se validó salto por salto entre el origen y el destino.

Para este ejemplo, se confirmó que no hay pérdida de paquetes ya que los 5 paquetes ICMP se recibieron y reenviaron correctamente en cada dispositivo.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).