

Configuración y resolución de problemas de Fabric Peering VXLAN vPC para NXOS

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Diagrama de la red](#)

[Configuración](#)

[Configuración de TCAM](#)

[TCAM tallado](#)

[Configuración para vPC](#)

[Dominio VPC](#)

[Keep-alive](#)

[Interfaz de Capa 3 para el link de par virtual](#)

[VPC Peer-link](#)

[Enlaces ascendentes](#)

[Configuración de SPINES](#)

[Tráfico de difusión, unidifusión desconocida y multidifusión con encapsulación de replicación de entrada](#)

[Tráfico de difusión, unidifusión desconocida y multidifusión con desencapsulamiento de replicación de entrada](#)

[Tráfico de difusión, unidifusión desconocida y multidifusión con encapsulación multidifusión](#)

[Tráfico de difusión, unidifusión desconocida y multidifusión con desencapsulación de multidifusión](#)

[Verificación](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar y verificar el análisis de estructura vPC para el flujo de tráfico de NXOS y BUM.

Prerequisites

Requirements

Cisco recomienda conocer estos temas:

- vPC (canal de puerto virtual)
- LAN extensible virtual (VXLAN)

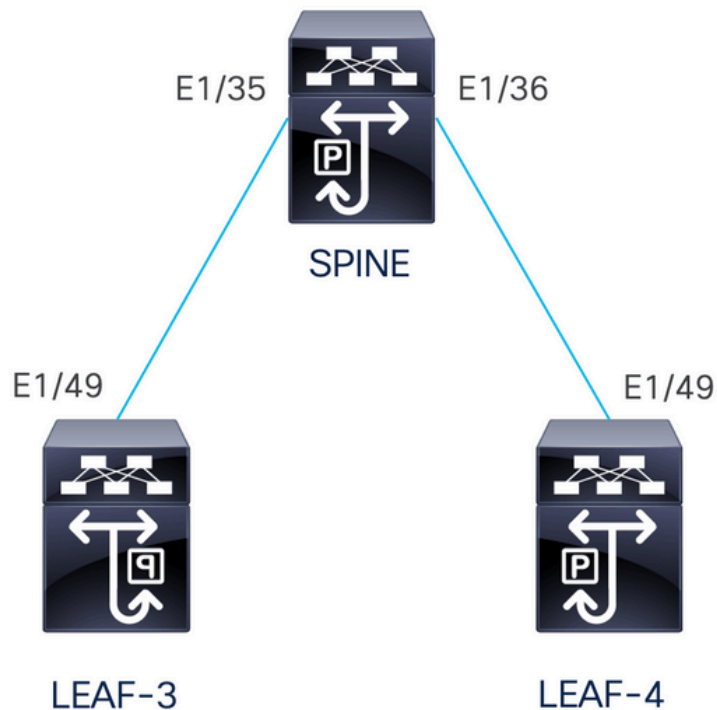
Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- N9K-C93240YC-FX2 para switches Leaf Versión: 10.3(3)
- N9K-C9336C-FX2 para conmutador de columna versión: 10.3(3)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Diagrama de la red



El análisis de estructuras vPC proporciona una solución de acceso de doble reposición mejorada sin la sobrecarga que supone desperdiciar puertos físicos para el enlace de par vPC. Esta función conserva todas las características de un vPC tradicional.

En esta implementación tenemos Leaf-3 y Leaf-4 configurados como vPC con Fabric Peering.

Configuración

Configuración de TCAM

Antes de la configuración, hay una verificación en la memoria TCAM:

```

LEAF-4(config-if)# sh hardware access-list tcam region
    NAT ACL[nat] size = 0
    Ingress PAACL [ing-ifacl] size = 0
        VACL [vac1] size = 0
    Ingress RAACL [ing-racl] size = 2304
    Ingress L2 QOS [ing-l2-qos] size = 256
    Ingress L3/VLAN QOS [ing-l3-vlan-qos] size = 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 RAACL [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 = 512
        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 PAACL IPv4 Lite [ing-ifacl-ipv4-lite] size = 0
    Ingress PAACL IPv6 Lite [ing-ifacl-ipv6-lite] size = 0
        Ingress CNTACL [ing-cntacl] size = 0
        Egress CNTACL [egr-cntacl] size = 0
        MCAST NAT ACL[mcast-nat] size = 0
        Ingress DAACL [ing-dacl] size = 0
    Ingress PAACL Super Bridge [ing-pacl-sb] size = 0
    Ingress Storm Control [ing-storm-control] size = 0
        Ingress VACL redirect [ing-vacl-nh] size = 0
        Egress PAACL [egr-ifacl] size = 0
        Egress Netflow [egr-netflow] size = 0

```

El Fabric Peering vPC requiere la aplicación de la división TCAM de la región ing-flow-redirect. La división TCAM requiere guardar la configuración y volver a cargar el switch antes de utilizar la función.

Este espacio en el TCAM es de ancho doble, por lo que el mínimo que podemos asignar es 512.

TCAM tallado

En este escenario, ing-racl tiene suficiente espacio para tomar 512 y asignar esos 512 a ing-flow-redirect.

```

LEAF-4(config-if)# hardware access-list tcam region ing-racl 1792
Please save config and reload the system for the configuration to take effect

```

```

LEAF-4(config)# hardware access-list tcam region ing-flow-redirect 512
Please save config and reload the system for the configuration to take effect

```

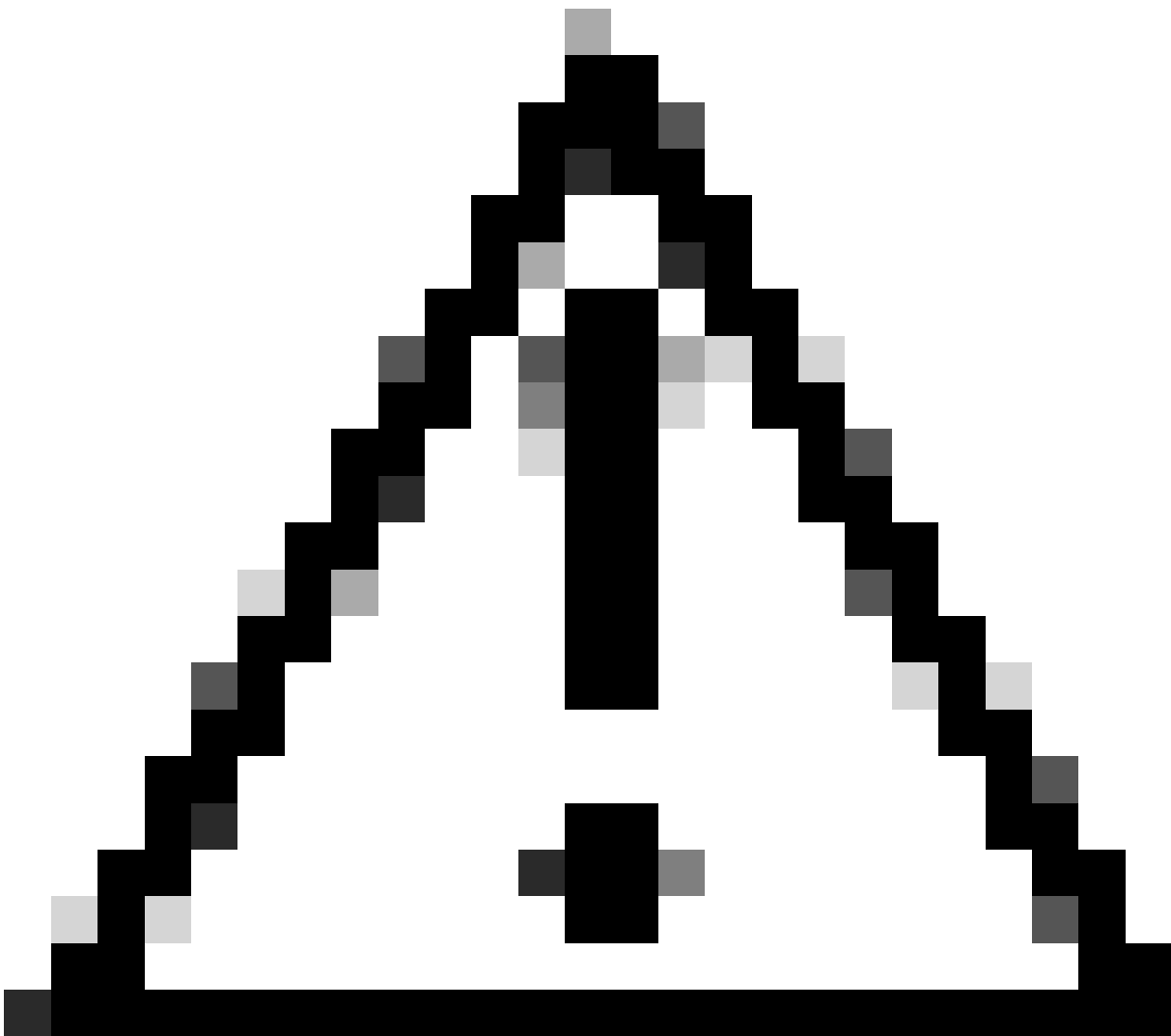


Nota: al configurar el modelo de fabric vPC que se compara a través de DCNM, se realizará el desglose de TCAM, pero se requiere una recarga para que surta efecto

Una vez hecho el cambio, se reflejará en el comando:

```
513E-B-11-N9K-C93240YC-FX2-4# sh hardware access-list tcam region
      NAT ACL[nat] size = 0
      Ingress PACL [ing-ifacl] size = 0
      VACL [vacl] size = 0
      Ingress RAcl [ing-racl] size = 2304
      Ingress L2 QOS [ing-l2-qos] size = 256
      Ingress L3/VLAN QOS [ing-l3-vlan-qos] size = 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 = 512 <<<<<
    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 PACL IPv4 Lite [ing-ifacl-ipv4-lite] size = 0
  Ingress PACL IPv6 Lite [ing-ifacl-ipv6-lite] size = 0
    Ingress CNTACL [ing-cntacl] size = 0
    Egress CNTACL [egr-cntacl] size = 0
    MCAST NAT ACL [mcast-nat] size = 0
    Ingress DAACL [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
```



Precaución: asegúrese de que el dispositivo se recargue después de los cambios en el TCAM; de lo contrario, el VPC no se activará debido a cambios no aplicados en el TCAM.

Configuración para vPC

Dominio VPC

En LEAF-3 y LEAF-4 en el dominio VPC, la configuración consiste en especificar las direcciones IP para el keepalive y el link de peer virtual

```
vpc domain 1
  peer-keepalive destination 192.168.1.1 source 192.168.1.2 vrf management
  virtual peer-link destination 10.10.10.2 source 10.10.10.1 dscp 56

interface port-channel1
  vpc peer-link
```

Keep-alive

Cualquier enlace directo de capa 3 entre pares vPC sólo se debe utilizar para mantener activo el par. Debe estar en un VRF separado dedicado solamente para el keepalive. En esta situación, estamos utilizando la gestión de la interfaz del switch.

```
LEAF-3
interface mgmt0
  vrf member management
  ip address 192.168.1.1/24
```

```
LEAF-4
interface mgmt0
  vrf member management
  ip address 192.168.1.2/24
```

Interfaz de Capa 3 para el link de par virtual

La interfaz de capa 3 utilizada para el enlace de par virtual no debe ser la misma que utilizamos para el keepalive, puede utilizar el mismo loopback utilizado para la capa subyacente o puede ser un loopback dedicado en el Nexus

Aquí el loopback0 es para la capa subyacente y el loopback2 es un loopback dedicado para el link par virtual, mientras que el loopback1 es la interfaz asociada a nuestra interfaz NVE.

```
LEAF-3
interface loopback0
  ip address 10.1.1.1/32
  ip router ospf 1 area 0.0.0.0
  ip pim sparse-mode
```

```
interface loopback1
  ip address 172.16.1.2/32
  ip address 172.16.1.1/32 secondary
  ip router ospf 1 area 0.0.0.0
  ip pim sparse-mode
```

```
interface loopback2
  ip address 10.10.10.2/32
  ip router ospf 1 area 0.0.0.0
```

LEAF-4

```
interface loopback0
  ip address 10.1.1.2/32
  ip router ospf 1 area 0.0.0.0
  ip pim sparse-mode
```

```
interface loopback1
  ip address 172.16.1.3/32
  ip address 172.16.1.1/32 secondary
  ip router ospf 1 area 0.0.0.0
  ip pim sparse-mode
```

```
interface loopback2
  ip address 10.10.10.1/32
  ip router ospf 1 area 0.0.0.0
```

VPC Peer-link

El link de par necesita tener un canal de puerto asignado incluso si no vamos a asignar una interfaz física al canal de puerto.

```
LEAF-3(config-if)# sh run interface port-channel 1 membership
```

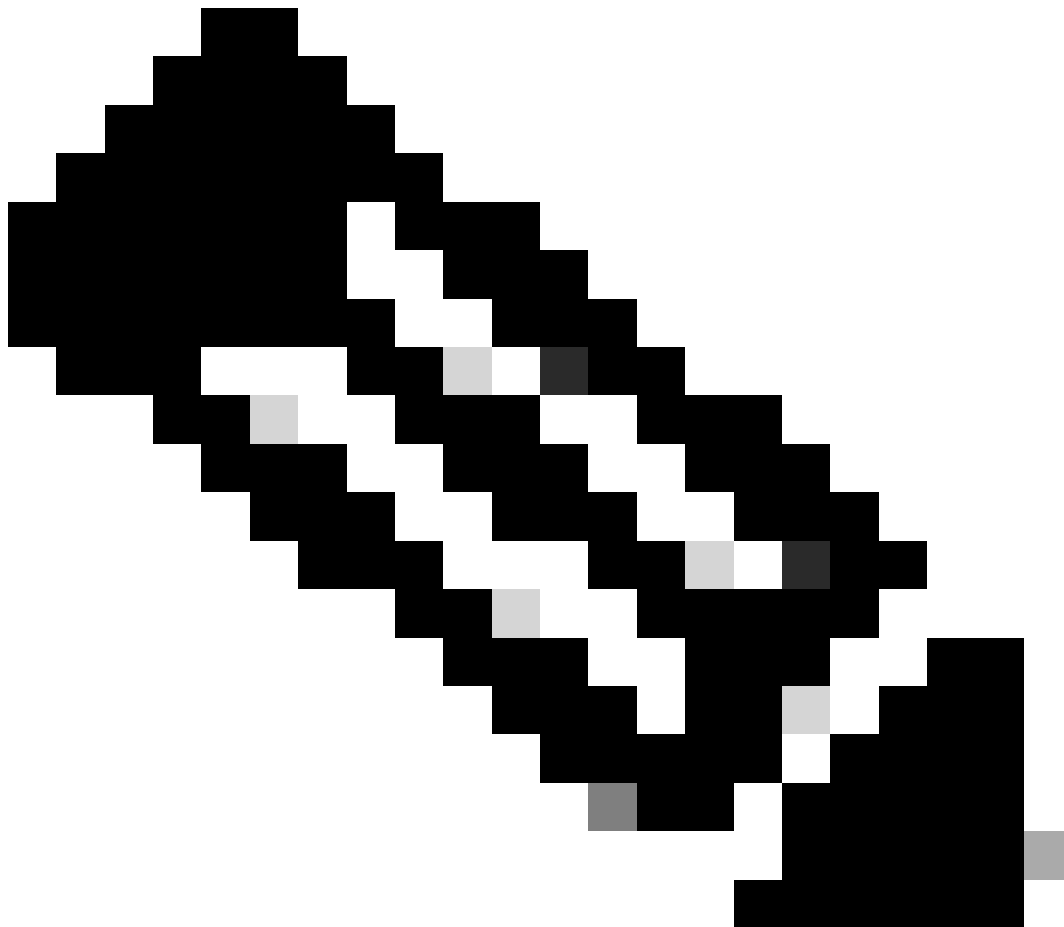
```
interface port-channel1
  switchport
  switchport mode trunk
  spanning-tree port type network
  vpc peer-link
```

Enlaces ascendentes

La última parte de la configuración consiste en configurar los links en ambas hojas hacia el SPINE con el comando port-type fabric.

```
interface Ethernet1/49
  port-type fabric <<<<<<<<
  medium p2p
  ip unnumbered loopback0
  ip router ospf 1 area 0.0.0.0
  ip pim sparse-mode
```

no shutdown



Nota: Si no configura el fabric de tipo de puerto, no podrá ver el keepalive generado por el Nexus

Configuración de SPINES

En las columnas, se recomienda establecer QoS para que coincida con el valor DSCP configurado en el dominio VPC, ya que el enlace de par de iguales del fabric vPC se establece en la red de transporte.

Los mensajes CFS de información del plano de control utilizados para sincronizar la información de estado del puerto, la información de VLAN, la asignación de VLAN a VNI, las direcciones MAC del host y los grupos de indagación IGMP se transmiten a través del fabric. Los mensajes CFS se marcan con el valor DSCP apropiado, que debe protegerse en la red de transporte.


```

class-map type qos match-all CFS
  match dscp 56

policy-map type qos CFS
  class CFS
    Set qos-group 7 <<< Depending on the platform it can be 4

interface Ethernet 1/35-36
  service-policy type qos input CFS

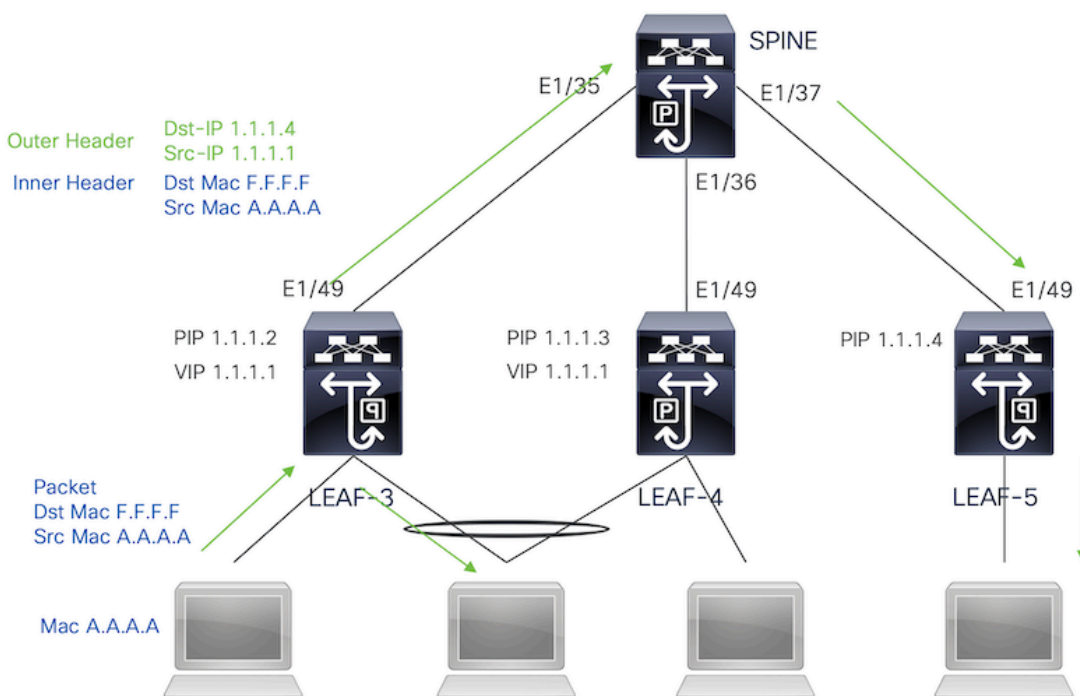
```

Tráfico de difusión, unidifusión desconocida y multidifusión con encapsulación de replicación de entrada

Cuando el nexus recibe un paquete que necesita ser transmitido, genera 2 copias del paquete.

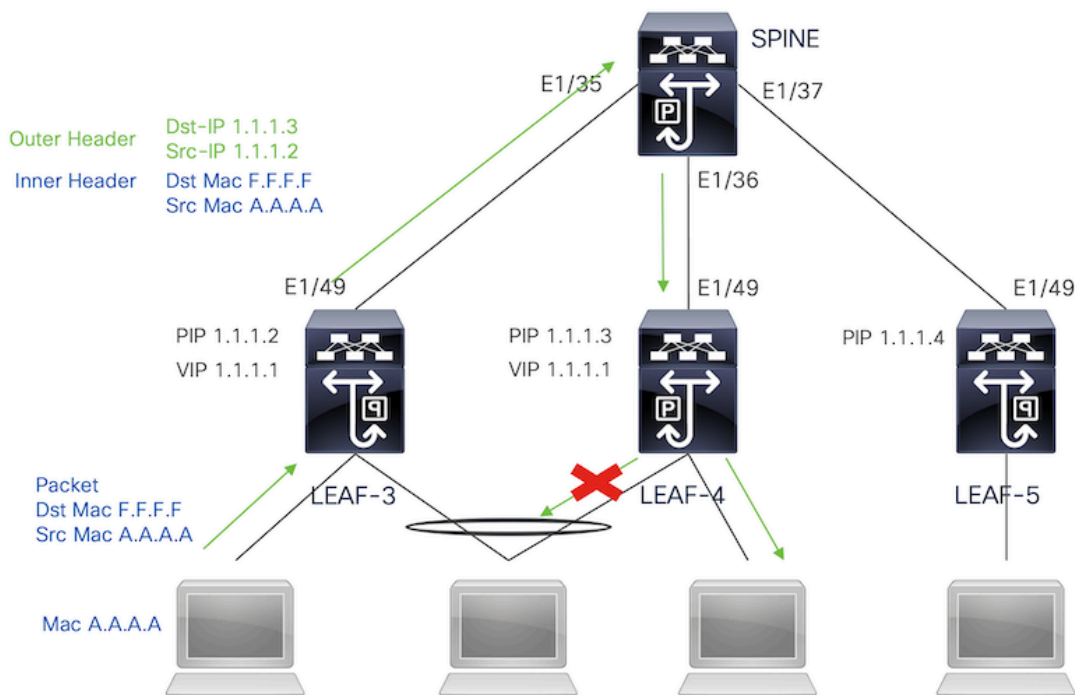
1. A todos los VTEPS remotos de la lista de inundación para el VNI, incluidos los puertos de acceso local
2. Al par VPC remoto

Para la primera copia, Nexus encapsuló el tráfico usando la IP de origen de la dirección IP secundaria y la IP de destino del VTEP remoto y también a los puertos de acceso local.



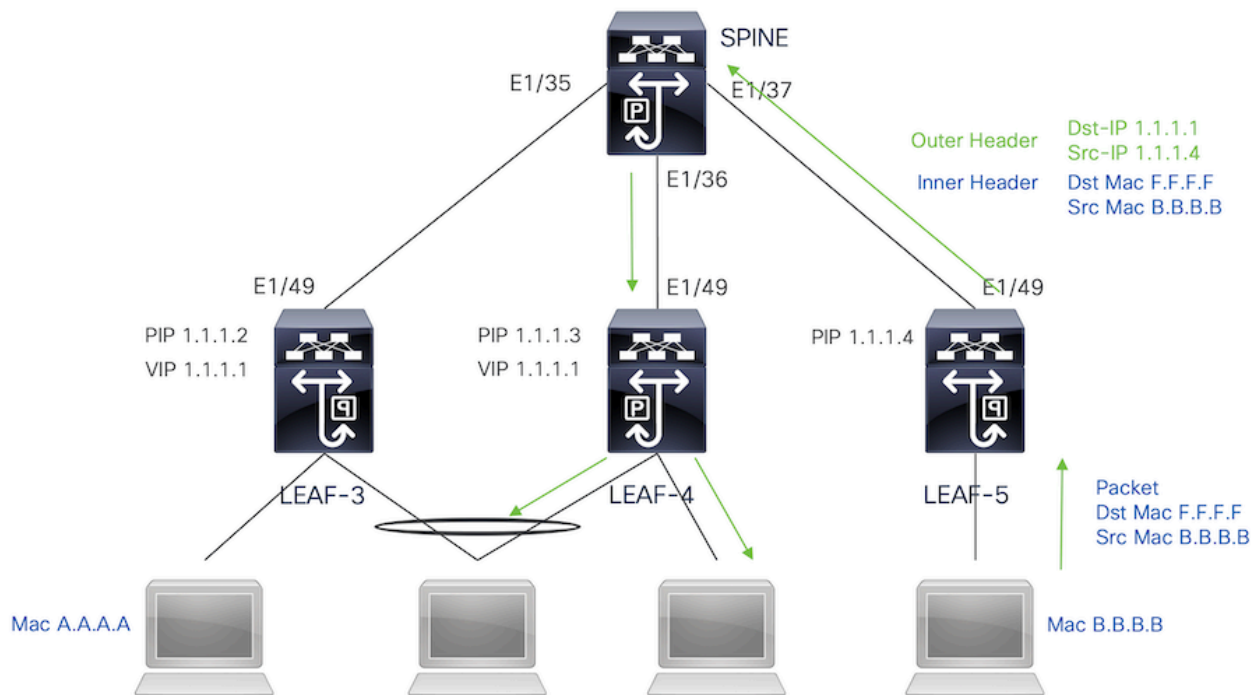
Para la segunda copia, se enviará al par VPC remoto; la IP de origen será la principal del bucle invertido y la IP de destino será la PIP del par VPC remoto.

Una vez recibido el paquete desde la columna, el VTEP remoto sólo reenviará el paquete a los puertos huérfanos.



Tráfico de difusión, unidifusión desconocida y multidifusión con desencapsulamiento de replicación de entrada

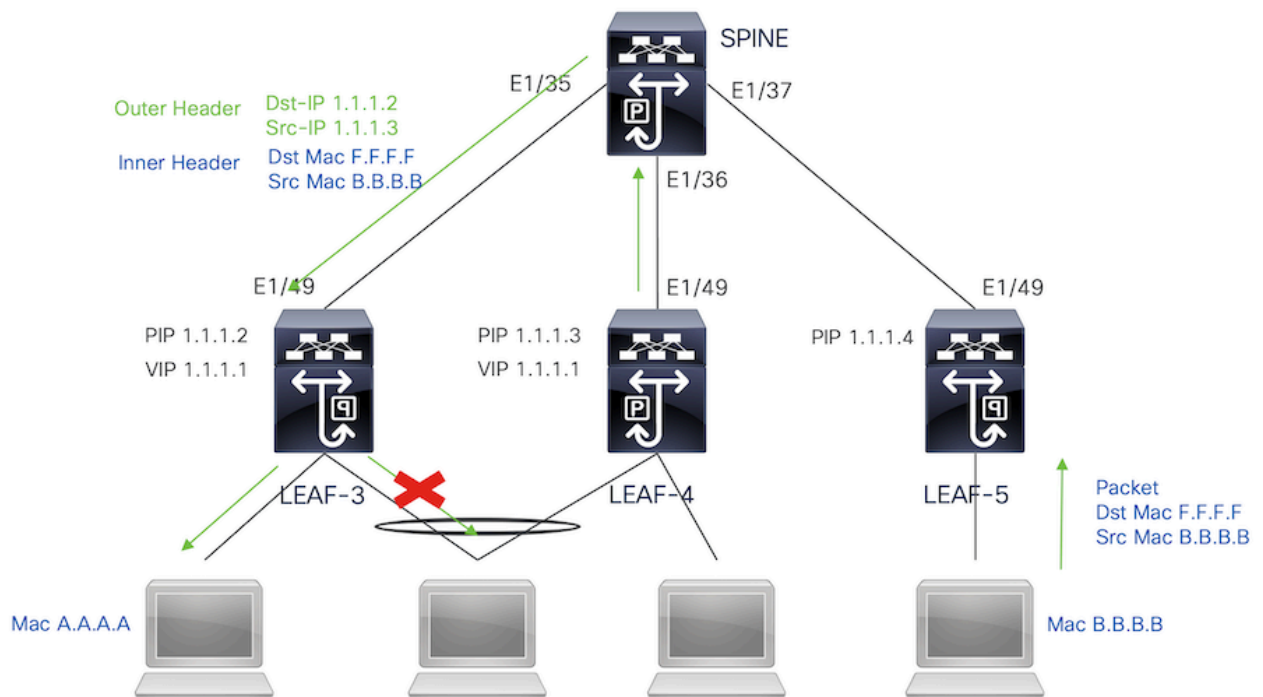
Dado que la IP de destino para el tráfico BUM recibido de otro VTEP es el VIP, el tráfico se transfiere a uno de los dispositivos VPC, desencapsula el paquete y lo envía a los puertos de acceso.



Para que el tráfico llegue a los puertos huérfanos conectados en el par VPC remoto, el nexus genera una copia del paquete y lo enviará solamente al VPC remoto usando la dirección IP

primaria como IP de origen/destino.

Una vez recibido en el par vpc remoto, el nexus desencapsula el tráfico y lo reenvía solamente a los puertos huérfanos.

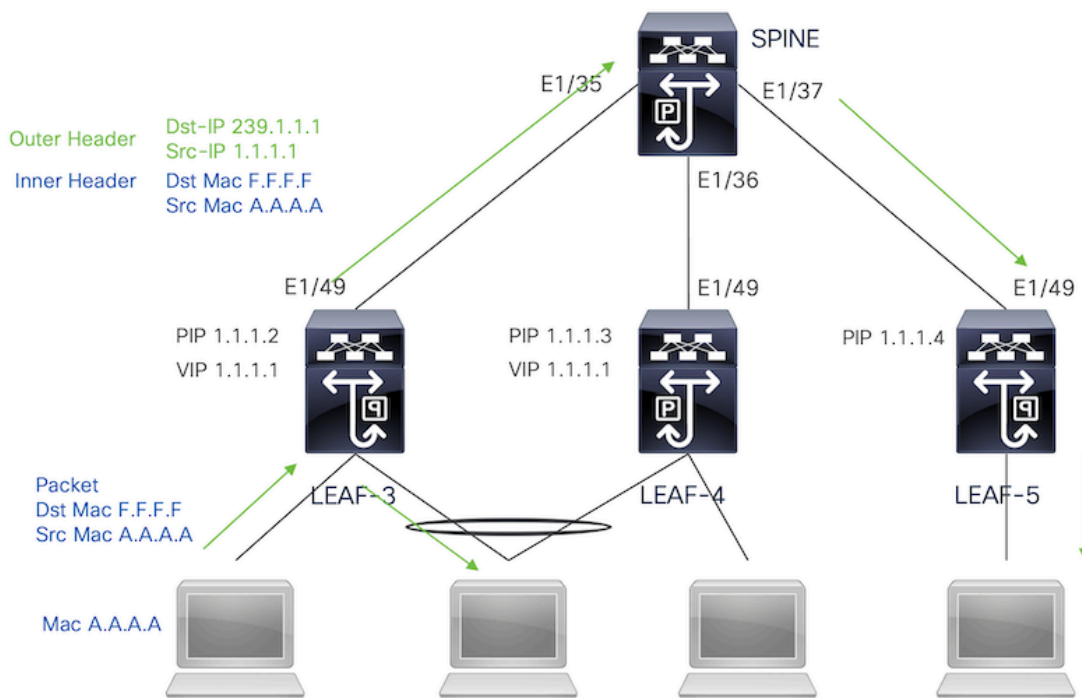


Tráfico de difusión, unidifusión desconocida y multidifusión con encapsulación multidifusión

Cuando el nexus recibe un paquete que necesita ser transmitido, genera 2 copias del paquete.

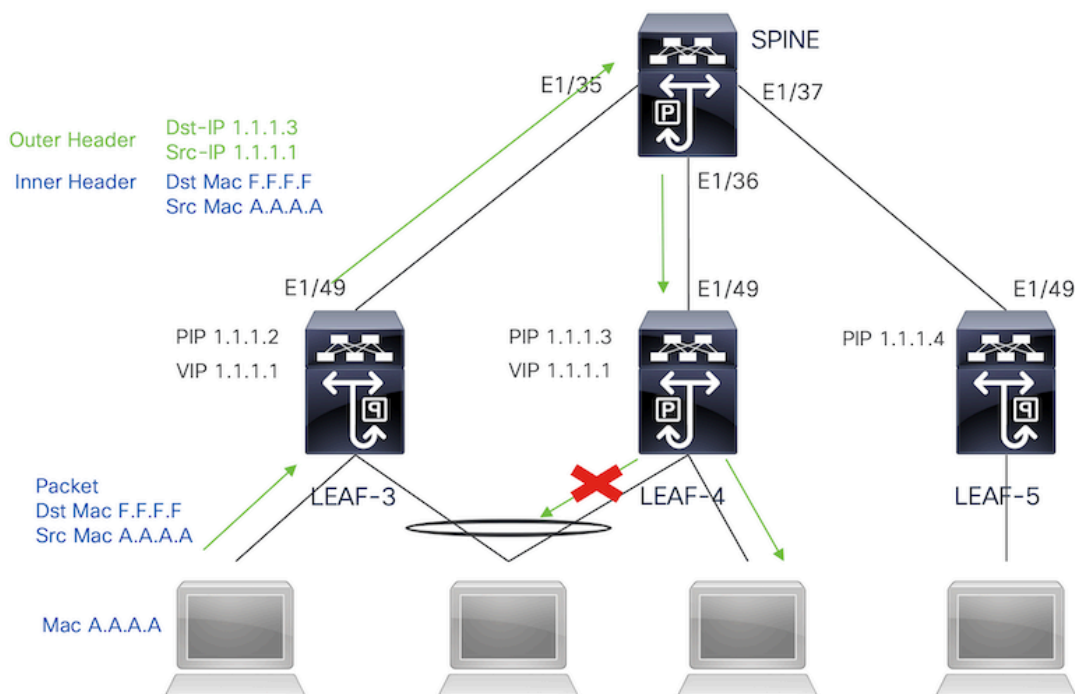
1. El paquete se enviará a todos los OIF de la entrada S,G de multidifusión, incluidos los puertos de acceso local
2. Al par VPC remoto

En la primera copia, Nexus encapsuló el tráfico usando la IP de origen de la dirección IP secundaria y la IP de destino del grupo de multidifusión configurado.



Para la segunda copia, se enviará al par VPC remoto; la IP de origen será la secundaria del bucle invertido y la IP de destino será la PIP del par VPC remoto.

Una vez recibido el paquete desde la columna, el VTEP remoto sólo reenvía el paquete a los puertos huérfanos.



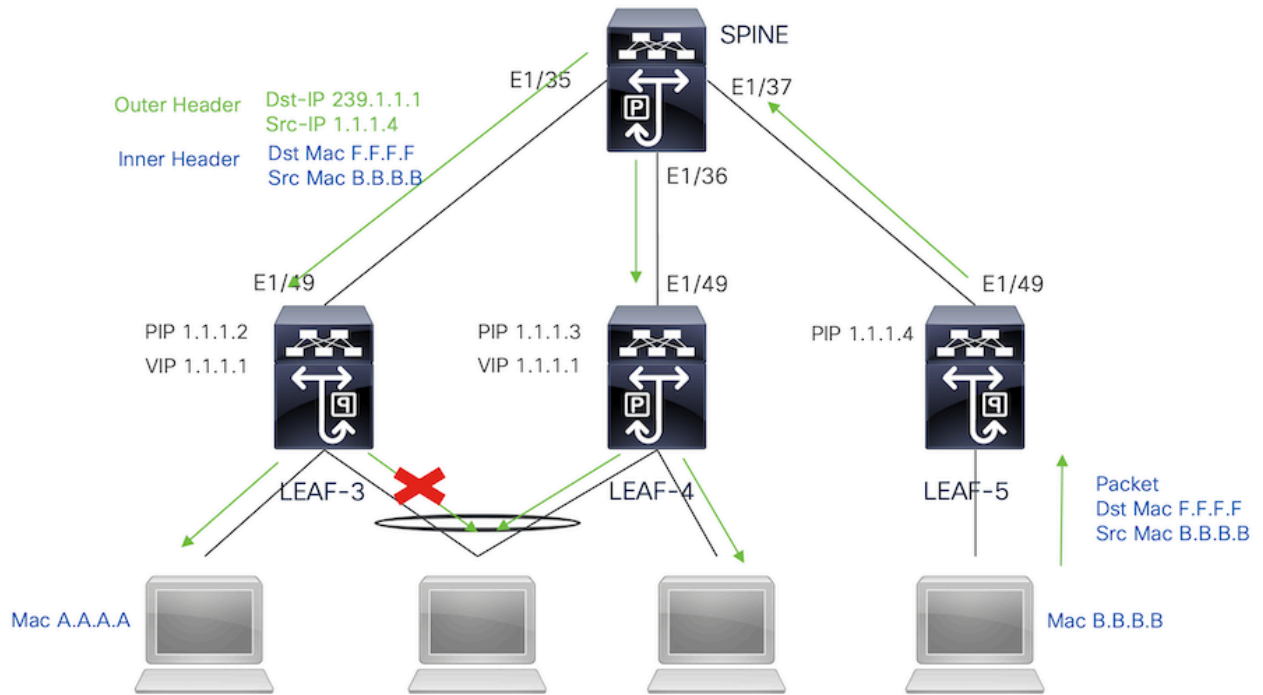
Tráfico de difusión, unidifusión desconocida y multidifusión con desencapsulación de multidifusión

Para el proceso de desencapsulamiento, el paquete va a llegar a ambos pares VPC. Sólo un

dispositivo VPC reenviará el tráfico a través de los canales de puerto VPC. Esto lo decidirá el reenviador mostrado en el comando.

```
module-1# show forwarding internal vpc-df-hash
```

VPC DF: FORWARDER



Verificación

Para asegurarse de que VPC está activo, ejecute los siguientes comandos:

Verifique el alcance de las direcciones IP utilizadas para el link de par virtual.

```
LEAF-3# sh ip route 10.10.10.1
IP Route Table for VRF "default"
'*' denotes best ucast next-hop
'***' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

10.10.10.1/32, ubest/mbest: 1/0
   *via 192.168.120.1, Eth1/49, [110/3], 01:15:01, ospf-1, intra
```

```
LEAF-3# ping 10.10.10.1
PING 10.10.10.1 (10.10.10.1): 56 data bytes
64 bytes from 10.10.10.1: icmp_seq=0 ttl=253 time=0.898 ms
64 bytes from 10.10.10.1: icmp_seq=1 ttl=253 time=0.505 ms
64 bytes from 10.10.10.1: icmp_seq=2 ttl=253 time=0.433 ms
64 bytes from 10.10.10.1: icmp_seq=3 ttl=253 time=0.465 ms
```

64 bytes from 10.10.10.1: icmp_seq=4 ttl=253 time=0.558 ms

LEAF-3(config-if)# show vpc brief

Legend:

(*) - local vPC is down, forwarding via vPC peer-link

```
vPC domain id           : 1
Peer status             : peer adjacency formed ok <<<<
vPC keep-alive status   : peer is alive <<<<
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 consistency status : success
vPC role                : secondary
Number of vPCs configured : 0
Peer Gateway           : Disabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status   : Disabled
Delay-restore status    : Timer is off.(timeout = 30s)
Delay-restore SVI status : Timer is off.(timeout = 10s)
Delay-restore Orphan-port status : Timer is off.(timeout = 0s)
Operational Layer3 Peer-router : Disabled
Virtual-peerlink mode   : Enabled <<<<<<<<
```

vPC Peer-link status

```
-----
id  Port  Status  Active vlans
--  ---  -
1   Po1   up      1,10,50,600-604,608,610-611,614-618,638-639,
        662-663,701-704
```

Para verificar las funciones para el VPC ejecute el comando:

LEAF-3(config-if)# sh vpc role

vPC Role status

```
-----
vPC role                : secondary <<<<
Dual Active Detection Status : 0
vPC system-mac          : 00:23:04:ee:be:01
vPC system-priority     : 32667
vPC local system-mac    : d0:e0:42:e2:09:6f
vPC local role-priority : 32667
vPC local config role-priority : 32667
vPC peer system-mac     : 2c:4f:52:3f:46:df
vPC peer role-priority  : 32667
vPC peer config role-priority : 32667
```

Todas las vlan permitidas en el canal de puerto de link de par deben ser mapeadas a un VNI, en caso de que no lo sean, se mostrarán como inconsistentes

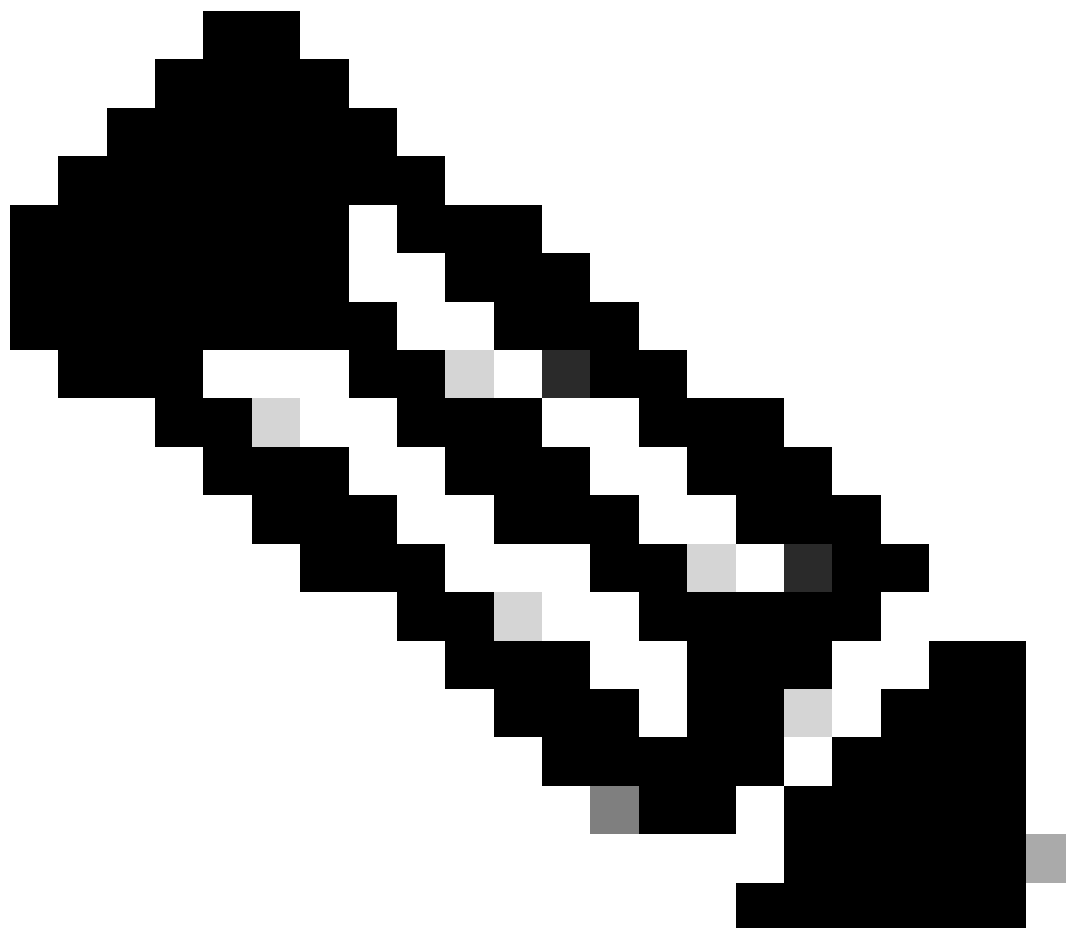
```
LEAF-3(config-if)# show vpc virtual-peerlink vlan consistency
Following vlans are inconsistent
1 608 610 611 614 615 616 617 618 638 639 701 702 703 704
```

Para confirmar que la configuración en los links ascendentes está correctamente programada, ejecute el comando:

```
LEAF-3(config-if)# show vpc fabric-ports
Number of Fabric port : 1
Number of Fabric port active : 1
```

Fabric	Ports	State

Ethernet	1/49	UP



Nota: El NVE y la interfaz de loopback asociada a él se mostrarán a menos que el VPC

esté activo.

Información Relacionada

- [Soporte técnico y descargas de Cisco](#)

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).