

# Solución de problemas de reenvío de ACI dentro del fabric: reenvío de capa 2

## Contenido

[Introducción](#)

[Antecedentes](#)

[Overview](#)

[Topología](#)

[comprobación de GUI](#)

[Flujo de trabajo de resolución de problemas para tráfico unidifusión de capa 2 conocido](#)

[Aprendizaje de MAC de EP de origen de hoja de entrada](#)

[Búsqueda de punto final MAC de destino de hoja de entrada](#)

[Switch de hoja de ingreso que envía al switch de columna](#)

[Reenvío de columna](#)

[Aprendizaje de MAC EP remoto de hoja de salida](#)

[Búsqueda MAC de destino de hoja de salida](#)

[Valide que ambos extremos se han aprendido correctamente en el repositorio COOP EP del conmutador central](#)

[Salida de ELAM mediante ELAM Assistant](#)

[ELAM de hoja de ingreso mediante CLI](#)

[Uso de fTriage para seguir el flujo](#)

[Flujo de trabajo de resolución de problemas para tráfico unidifusión de capa 2 desconocido: BD en modo saturación](#)

[Búsqueda de BD GIPo](#)

[ELAM — hoja de ingreso — tráfico inundado](#)

[Dibujo de la topología FTAG](#)

[ELAM — hoja de salida — tráfico inundado](#)

[Flujo de trabajo de resolución de problemas para tráfico unidifusión de capa 2 desconocido: BD en proxy de hardware](#)

[Resumen de reenvío de capa 2](#)

[Comportamiento de reenvío de capa 2 del fabric ACI](#)

## Introducción

Este documento describe los pasos para comprender y resolver problemas de reenvío de Capa 2 en ACI

## Antecedentes

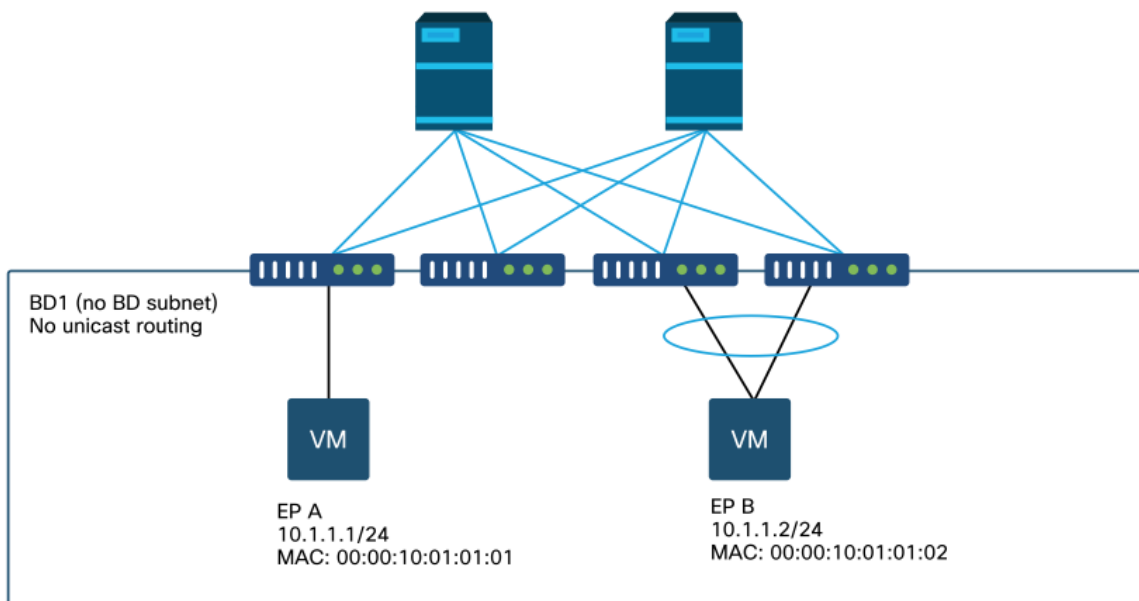
El material de este documento se ha extraído de la [Solución de problemas de Cisco Application Centric Infrastructure, segunda edición](#) libro, específicamente el **Reenvío dentro del fabric: reenvío de L2: dos terminales en el mismo BD: sin routing de unidifusión** capítulo.

# Overview

Esta sección explica un ejemplo de troubleshooting donde los extremos en el mismo dominio de bridge y la misma subred no pueden comunicarse entre sí. La siguiente figura ilustra la topología donde el BD no tiene ninguna subred y tiene el ruteo unicast inhabilitado.

Normalmente, cuando se solucionan problemas de flujos de tráfico con conectividad de terminales, se recomienda comenzar a identificar un par de terminales. Consulte la topología siguiente con los EP A y B. Estos tendrán respectivamente las direcciones IP 10.1.1.1/24 y 10.1.1.2/24. Las direcciones MAC serán 00:00:10:01:01:01 y 00:00:10:01:01:02, respectivamente.

## Topología



En esta sección hay tres escenarios:

1. Flujo de unidifusión de capa 2 conocido.
2. Flujo de unidifusión de capa 2 desconocido con BD en modo de saturación.
3. Flujo de unidifusión de capa 2 desconocido con BD en modo de proxy de hardware.

Los flujos de troubleshooting que se seguirán pueden resumirse mediante el siguiente esquema:

- Comprobación del nivel 1: Validación GUI de la configuración, fallos y terminales aprendidos.
- Comprobación de nivel 2: CLI en los switches de hoja: Verifique si los switches de hoja de origen y destino aprenden los terminales. Verifique si los nodos de columna aprenden el punto final en COOP.
- Comprobación del nivel 3: Captura de paquete: ELAM (ELAM Assistant o CLI) para validar la trama. Triage para rastrear el flujo.

## comprobación de GUI

El primer nivel de solución de problemas consiste en validar desde la GUI que la MAC del

terminal se aprendió correctamente. Esto se puede hacer desde la ficha operativa del EPG donde se encuentra el terminal.

## 'Ficha operativa de EPG > Terminales del cliente'

Client End-Points							
Configured Access Policies							
Contracts							
Controller End-Points							
Deployed Leaves							
MAC	IP	Learning Source	Hosting Server	Reporting Controller Name	Interface	Multicast Address	Encap Address
00:00:10:01:01:01	---	learned	---	---	Pod-1/Node-101/eth1/3 (learned)	---	vlan-2501
00:00:10:01:01:02	---	learned	---	---	Pod-1/Node-103-104/N3k-3-VPC3-4 (learned)	---	vlan-2501

Objects Per Page: 15

En esta situación, ambos extremos A y B se muestran en la GUI. La GUI muestra sus direcciones MAC, la interfaz en la que están conectados al fabric y la encapsulación, en este caso ambas se encuentran en la VLAN 2501 de encapsulación.

Se espera que la dirección IP no se aprenda del fabric de ACI, ya que el routing de unidifusión se ha deshabilitado en el nivel BD.

Consulte la columna de origen de aprendizaje en la captura de pantalla anterior. Si denota "detectado", el switch de hoja ACI recibió al menos un paquete del terminal.

Dado que en este caso los terminales se aprenden del fabric de ACI, pase al siguiente caso de solución de problemas para el tráfico de unidifusión de capa 2 conocido.

## Flujo de trabajo de resolución de problemas para tráfico unidifusión de capa 2 conocido

### Aprendizaje de MAC de EP de origen de hoja de entrada

En el caso del reenvío de Capa 2 en el mismo BD, ACI solo aprenderá el MAC de origen y el reenvío basado en el MAC de destino. Las direcciones MAC se aprenden en el ámbito del BD.

Primero, verifique si se aprende el punto final:

```
leaf1# show endpoint mac 0000.1001.0101
```

Legend:

s - arp

H - vtep

V - vpc-attached

p - peer-aged

```

R - peer-attached-rl B - bounce          S - static          M - span
D - bounce-to-proxy  O - peer-attached   a - local-aged      m - svc-mgr
L - local            E - shared-service

```

```

+-----+-----+-----+-----+-----+
----+
      VLAN/          Encap          MAC Address          MAC Info/          Interface
      Domain          VLAN          IP Address          IP Info
+-----+-----+-----+-----+-----+
----+
4/Prod:VRF1          vlan-2501    0000.1001.0101 L
eth1/3

```

El resultado anterior proporciona la siguiente información:

- La dirección MAC 0000.1001.0101 se aprende localmente (el indicador es L para local) en el puerto Ethernet 1/3 con encapsulación vlan-2501 en vrf Prod:VRF1.
- Consulte la columna 'VLAN/Dominio' en el resultado anterior. La ID de VLAN enumerada es la VLAN interna.

### Búsqueda de punto final MAC de destino de hoja de entrada

Suponga que se conoce el destino MAC (unidifusión conocida).

```

leaf1# show endpoint mac 0000.1001.0102
Legend:
s - arp          H - vtep          V - vpc-attached    p - peer-aged
R - peer-attached-rl B - bounce          S - static          M - span
D - bounce-to-proxy O - peer-attached   a - local-aged      m - svc-mgr
L - local        E - shared-service
+-----+-----+-----+-----+-----+
----+
      VLAN/          Encap          MAC Address          MAC Info/          Interface
      Domain          VLAN          IP Address          IP Info
+-----+-----+-----+-----+-----+
----+
7/Prod:VRF1          vxlan-16351141  0000.1001.0102
tunnel4

```

El resultado anterior proporciona la siguiente información:

- La dirección MAC 0000.1001.0102 no se aprende localmente.
- Se aprende del túnel de interfaz 4.
- Se aprende en la encapsulación VXLAN-16351141 que corresponde al BD\_VNID (ID de red VXLAN) del dominio de bridge.

A continuación, verifique el destino de la interfaz de túnel mediante el comando 'show interface tunnel <x>'

```

leaf1# show interface tunnel 4
Tunnel4 is up
  MTU 9000 bytes, BW 0 Kbit
  Transport protocol is in VRF "overlay-1"
  Tunnel protocol/transport is ivxlan
  Tunnel source 10.0.88.95/32 (lo0)
  Tunnel destination 10.0.96.66
  Last clearing of "show interface" counters never
  Tx
  0 packets output, 1 minute output rate 0 packets/sec

```

Rx

0 packets input, 1 minute input rate 0 packets/sec

Por lo tanto, el paquete será encapsulado en VXLAN con el origen TEP IP 10.0.88.95 (asignado a loopback0) y enviado hacia el destino TEP IP 10.0.96.66.

Confirme la IP de origen:

```
leaf1# show ip interface loopback 0 vrf overlay-1
IP Interface Status for VRF "overlay-1"
lo0, Interface status: protocol-up/link-up/admin-up, iod: 4, mode: ptep
IP address: 10.0.88.95, IP subnet: 10.0.88.95/32
IP broadcast address: 255.255.255.255
IP primary address route-preference: 0, tag: 0
```

El TEP IP 10.0.96.66 de destino puede ser uno de los siguientes:

- Dirección PTEP de otra hoja (se puede comprobar utilizando `aciddiag fnvread`)
- VPC VIP (se puede ver en 'GUI > Fabric > Access Políticas > Políticas > Switch > Virtual Port Channel default' (consulte la captura de pantalla siguiente)
- Alguna IP de loopback en un conmutador central. Utilice el comando 'show ip interface vrf overlay-1' en el conmutador central para verificar esto.

### Grupos de protección VPC explícitos

Name	Domain Policy	Switches	Logical Pair ID	Virtual IP
101-102	default	101, 102	3	10.0.96.67/32
2107-2108		2107, 2108	78	10.2.120.96/32
Pod1-vpc	default	103, 104	1	10.0.96.66/32
pod2-vpc	default	1105, 1106	2	10.1.240.33/32

### Switch de hoja de ingreso que envía al switch de columna

La hoja de ingreso ahora encapsulará la trama en VXLAN con la IP de destino externa establecida en 10.0.96.66 que es la IP de destino del túnel enumerada en el comando 'show interface tunnel 4' anterior. Lo encapsulará en VXLAN con el VNID del dominio de bridge - vxlan-16351141 - como se muestra en el resultado del comando 'show endpoint mac 0000.1001.0102' anterior.

Según la ruta IS-IS en VRF overlay-1, determine dónde enviarla:

```
leaf1# show ip route 10.0.96.66 vrf overlay-1
```

```
IP Route Table for VRF "overlay-1"
'*' denotes best ucast next-hop
'***' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>
```

```
10.0.96.66/32, ubest/mbest: 4/0
  *via 10.0.88.65, Eth1/49.10, [115/3], 2w5d, isis-isis_infra, isis-l1-int
  *via 10.0.88.94, Eth1/50.128, [115/3], 2w5d, isis-isis_infra, isis-l1-int
```

Por lo tanto, existe un routing ECMP (múltiples rutas de igual coste) al destino mediante eth1/49 y 1/50, que son los enlaces ascendentes de fabric a los switches de columna.

## Reenvío de columna

La tabla de ruteo de superposición 1 de VRF en la columna muestra que la ruta del host 10.0.96.66 es alcanzable a través de leaf3 u leaf4. Esto se espera ya que 10.0.96.66 es el VIP de VPC de los switches de hoja 103 y 104:

```
spinel# show ip route 10.0.96.66 vrf overlay-1
IP Route Table for VRF "overlay-1"
'*' denotes best ucast next-hop
'***' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

10.0.96.66/32, ubest/mbest: 2/0
  *via 10.0.88.91, eth1/3.35, [115/2], 02w05d, isis-isis_infra, isis-l1-int
  *via 10.0.88.90, eth1/4.39, [115/2], 02w05d, isis-isis_infra, isis-l1-int
```

```
spinel# show lldp neighbors | egrep "1\3 |1\4 "
leaf3          Eth1/3          120          BR          Eth1/49
leaf4          Eth1/4          120          BR          Eth1/49
```

## Aprendizaje de MAC EP remoto de hoja de salida

En este caso, el TEP de destino es un par VPC por lo que el paquete llegará en la hoja 3 u hoja 4. Consulte los resultados del comando a continuación. Leaf4 debe mostrar un resultado similar. Dado que forman parte del mismo par VPC, todos los terminales están sincronizados entre los dos switches de hoja.

El aprendizaje del terminal para el tráfico de Capa 2 en la hoja de salida se basa en la dirección MAC de origen que se aprende en el BD correspondiente al VNID en el paquete recibido. Esto se puede verificar en la tabla de terminales.

La dirección MAC de origen se encuentra detrás del túnel 26 en VXLAN-16351141.

El túnel 26 va al TEP IP 10.0.88.95 que es leaf1:

```
leaf3# show endpoint mac 0000.1001.0101
Legend:
s - arp          H - vtep          V - vpc-attached  p - peer-aged
R - peer-attached-rl B - bounce        S - static         M - span
D - bounce-to-proxy O - peer-attached a - local-aged    m - svc-mgr
L - local        E - shared-service

+-----+-----+-----+-----+
---+
```

VLAN/ Domain	Encap VLAN	MAC Address IP Address	MAC Info/ IP Info	Interface
136/Prod:VRF1 tunnel26	vxlan-16351141	0000.1001.0101		

```
leaf3# show interface tunnel 26
```

```
Tunnel26 is up
  MTU 9000 bytes, BW 0 Kbit
  Transport protocol is in VRF "overlay-1"
  Tunnel protocol/transport is ipvlan
  Tunnel source 10.0.88.91/32 (lo0)
  Tunnel destination 10.0.88.95
  Last clearing of "show interface" counters never
  Tx
  0 packets output, 1 minute output rate 0 packets/sec
  Rx
  0 packets input, 1 minute input rate 0 packets/sec
```

```
leaf3# acidiag fmvread | egrep "10.0.88.95"
```

```
  101      1          leaf1      FDO20160TPA      10.0.88.95/32      leaf
active    0
```

## Búsqueda MAC de destino de hoja de salida

El comando 'show endpoint' confirma que el MAC de destino se aprende detrás del canal de puerto 1 y utiliza la encapsulación VLAN-2501

```
leaf3# show endpoint mac 0000.1001.0102
```

Legend:

```
s - arp          H - vtep          V - vpc-attached    p - peer-aged
R - peer-attached-rl B - bounce        S - static          M - span
D - bounce-to-proxy O - peer-attached a - local-aged      m - svc-mgr
L - local        E - shared-service
```

VLAN/ Domain	Encap VLAN	MAC Address IP Address	MAC Info/ IP Info	Interface
135/Prod:VRF1 po1	vlan-2501	0000.1001.0102	LpV	

Esto indica que la trama está dejando el fabric ACI en el canal de puerto 1 de la interfaz leaf3 con el ID de VLAN encapsulada 2501. Puede encontrar el VNID BD en la pestaña de funcionamiento del arrendatario en la GUI.

## Valide que ambos extremos se han aprendido correctamente en el repositorio COOP EP del conmutador central

El repo COOP EP debe sincronizarse en todos los nodos de la columna vertebral. el repo de COOP EP se puede comprobar utilizando el VNID BD como clave e introduciendo la dirección MAC EP.

La dirección MAC de origen de este flujo se aprende de tunnel next-hop 10.0.88.95 que es la IP TEP de leaf1. Además, el resultado del comando muestra VNID 16351141 que corresponde al dominio de bridge correcto.

```
spinel# show coop internal info repo ep key 16351141 00:00:10:01:01:01
```

```
Repo Hdr Checksum : 24197
Repo Hdr record timestamp : 10 01 2019 10:16:50 278195866
Repo Hdr last pub timestamp : 10 01 2019 10:16:50 283699467
Repo Hdr last dampen timestamp : 01 01 1970 00:00:00 0
Repo Hdr dampen penalty : 0
Repo Hdr flags : IN_OBJ EXPORT ACTIVE
EP bd vnid : 16351141
EP mac : 00:00:10:01:01:01
flags : 0x80
repo flags : 0x122
Vrf vnid : 2097154
Epg vnid : 0
EVPN Seq no : 0
Remote publish timestamp: 01 01 1970 00:00:00 0
Snapshot timestamp: 10 01 2019 10:16:50 278195866
Tunnel nh : 10.0.88.95
MAC Tunnel : 10.0.88.95
IPv4 Tunnel : 10.0.88.95
IPv6 Tunnel : 10.0.88.95
ETEP Tunnel : 0.0.0.0
```

El MAC de destino de este flujo se aprende contra el VIP VPC 10.0.96.66 de la hoja 3 y la hoja 4. El VNID de BD EP 16351141 también se enumera, que corresponde al BD correcto.

```
spinel# show coop internal info repo ep key 15302583 00:00:10:01:01:02
```

```
Repo Hdr Checksum : 16897
Repo Hdr record timestamp : 10 01 2019 11:05:46 351360334
Repo Hdr last pub timestamp : 10 01 2019 11:05:46 352019546
Repo Hdr last dampen timestamp : 01 01 1970 00:00:00 0
Repo Hdr dampen penalty : 0
Repo Hdr flags : IN_OBJ EXPORT ACTIVE
EP bd vnid : 16351141
EP mac : 00:00:10:01:01:02
flags : 0x90
repo flags : 0x122
Vrf vnid : 2097154
Epg vnid : 0
EVPN Seq no : 0
Remote publish timestamp: 01 01 1970 00:00:00 0
Snapshot timestamp: 10 01 2019 11:05:46 351360334
Tunnel nh : 10.0.96.66
MAC Tunnel : 10.0.96.66
IPv4 Tunnel : 10.0.96.66
IPv6 Tunnel : 10.0.96.66
ETEP Tunnel : 0.0.0.0
```

## Salida de ELAM mediante ELAM Assistant

ELAM Assistant es una potente aplicación de ACI que puede simplificar la ejecución de capturas de ELAM en un fabric de ACI.

Los disparadores de ELAM Assistant se pueden iniciar simultáneamente en múltiples nodos de hoja. Como resultado, se pueden verificar paquetes específicos en paralelo en leaf1, leaf3 y leaf4.

La captura de ELAM configurada aparecerá como se muestra a continuación. Como se ha observado, el paquete se ve en la hoja 1 (nodo 101) y en la hoja 3 (nodo 103).



## ELAM Assistant: parámetros

Capture a packet with ELAM (Embedded Logic Analyzer Module)

ELAM PARAMETERS

Name your capture: L2-only

Status	Node	Direction	Source I/F	Parameters	VxLAN (outer) header
Report Ready	node-101	from frontport	any	src ip 10.1.1.1 dst ip 10.1.1.2	
Report Ready	node-103	from SPINE	any	src ip 10.1.1.1 dst ip 10.1.1.2	
Set	node-104	from SPINE	any	src ip 10.1.1.1 dst ip 10.1.1.2	

El informe de leaf1 (node-101) muestra lo siguiente:

- El resultado de Captured Packet Information confirma que el paquete ingresa en eth1/3 y tiene la información MAC e IP correcta.
- La información de reenvío de paquetes muestra que se reenvió en eth1/49 a TEP IP 10.0.96.66.

### ELAM Assistant — leaf1 (node-101) — Información de paquetes capturados

Basic Information	
Device Type	LEAF
Packet Direction	ingress (front panel port -> leaf)
Incoming I/F	eth1/3

L2 Header	
Destination MAC	0000.1001.0102
Source MAC	0000.1001.0101
Access Encap VLAN	2501
CoS	0

L3 Header	
L3 Type	IPv4
Destination IP	10.1.1.2
Source IP	10.1.1.1
IP Protocol	0x1 (ICMP)
DSCP	0
TTL	255

No Vx

### ELAM Assistant — leaf1 (node-101) — Información de reenvío de paquetes

Packet Forwarding Information	
<b>Forward Result</b>	
Destination Type	To another ACI node (or AVS/AVE)
Destination TEP	10.0.96.66 (vPC (103_104))
Destination Physical Port	eth1/49
Sent to SUP/CPU instead	no
SUP Redirect Reason (SUP code)	NONE
<b>Contract</b>	
Destination EPG pcTag (dclass)	32770 (Prod:App:EPG1)
Source EPG pcTag (sclass)	32770 (Prod:App:EPG1)
Contract was applied	1 (Contract was applied on this node)
<b>Drop</b>	

En la hoja de salida 3 (nodo-103), se observa lo siguiente:

En la información del paquete capturado en leaf3, ingresa desde eth1/49. La dirección IP externa confirma lo siguiente:

- Fuente TEP: 10.0.88.95
- TEP de destino: 10.0.96.66
- VNID: 16351141 (BD VNID)

### ELAM Assistant — leaf3 (node-103) — Información de paquetes capturados

Captured Packet Information	
<b>Basic Information</b>	
Device Type	LEAF
Packet Direction	egress (spine LC -> leaf)
Incoming I/F	eth1/49

L3 Header (Outer VxLAN)	
L3 Type	IPv4
Destination IP	10.0.96.66 (vPC (103_104))
Source IP	10.0.88.95 (bdsol-aci32-leaf1)
IP Protocol	0x11 (UDP)
DSCP	0
TTL	31
Don't Fragment Bit	0x0 (0x0)

L4 Header (Outer VxLAN)	
L4 Type	iVxLAN
DL (Don't Learn) Bit	0 (not set)
Src Policy Applied Bit	1 (Contract was applied on the previous node)
Dst Policy Applied Bit	1 (Contract was applied on the previous node)
Source EPG (sclass / src pcTag)	0x8002 / 32770 (Prod:App:EPG1)
VRF/BD VNID	15302583 (Prod:BD1)

La información de reenvío de paquetes muestra que el tráfico se reenvía en el canal de puerto 1 y específicamente en Ethernet 1/12.

Packet Forwarding Information	
<b>Forward Result</b>	
Destination Type	To a local port
Destination Logical Port	Po1
Destination Physical Port	eth1/12
Sent to SUP/CPU instead	no
SUP Redirect Reason (SUP code)	NONE
<b>Contract</b>	
Destination EPG pcTag (dclass)	32770 (Prod:App:EPG1)
Source EPG pcTag (sclass)	32770 (Prod:App:EPG1)
Contract was applied	1 (Contract was applied on this node)
<b>Drop</b>	
Drop Code	no drop

## ELAM de hoja de ingreso mediante CLI

Se recomienda utilizar ELAM Assistant ya que simplifica la operación de ejecución de capturas de ELAM. Sin embargo, también es posible utilizar comandos CLI en switches ACI para generar un informe ELAM. A continuación se muestra un ejemplo de cómo se haría esto.

Utilice la secuencia de disparo mostrada para capturar el paquete en la hoja de ingreso. Consulte la sección "Herramientas" para obtener más información sobre las opciones de ELAM.

- En este ejemplo, el ASIC es 'tah' como hoja (número de pieza que finaliza en '-EX').
- 'in-select 6' se utiliza para capturar un paquete proveniente de un puerto de link descendente sin un encapsulado VXLAN.
- 'out-select 1' garantiza que también se muestre el vector de descarte (en caso de que se descarte un paquete).
- El comando 'reset' es necesario para asegurarse de que se han limpiado los desencadenadores anteriores.
- Aunque este es un ELAM de flujo en puente tiene visibilidad en el encabezado IP. Como resultado, 'ipv4 src\_ip' y 'dst\_ip' se pueden utilizar para configurar el disparador.

```
module-1# debug platform internal tah elam asic 0
module-1(DBG-elam)# trigger init in-select ?
 10 Outer14-inner14-ieth
 13 Outer(12|13|14)-inner(12|13|14)-noieth
 14 Outer(12(vntag)|13|14)-inner(12|13|14)-ieth
 15 Outer(12|13|14)-inner(12|13|14)-ieth
  6 Outer12-outer13-outer14
  7 Inner12-inner13-inner14
  8 Outer12-inner12-ieth
  9 Outer13-inner13
```

```
module-1(DBG-elam)# trigger init in-select 6 out-select 1
module-1(DBG-elam-insel6)# reset
module-1(DBG-elam-insel6)# set outer ipv4 src_ip 10.1.1.1 dst_ip 10.1.1.2
module-1(DBG-elam-insel6)# start
```

Para ver si se recibió el paquete, verifique el estado de ELAM. Si hay un disparador, significa que se capturó un paquete que coincide con las condiciones.

```
module-1(DBG-elam-insel6)# status
ELAM STATUS
=====
Asic 0 Slice 0 Status Triggered
Asic 0 Slice 1 Status Armed
```

El siguiente resultado muestra que el informe se muestra con el comando 'report'. El resultado es muy largo, por lo que sólo se pega aquí el principio. Pero tenga en cuenta que el informe completo se guarda para su posterior análisis en una ubicación del sistema de archivos hoja. El nombre de archivo también contiene las marcas de tiempo cuando se tomó el ELAM.

```
leaf1# ls -al /var/log/dme/log/elam_2019-09-30-03m-23h-14s.txt
-rw-rw-rw- 1 root root 699106 Sep 30 23:03 /var/log/dme/log/elam_2019-09-30-03m-23h-14s.txt
```

El 'informe' valida que el paquete ha sido recibido y la información es la esperada (MAC de origen y destino, IP de origen y destino, etc.)

module-1(DBG-elam-insel6)# **ereport**  
Python available. Continue ELAM decode with LC Pkg  
ELAM REPORT

=====  
=====  
Trigger/Basic Information  
=====

=====  
ELAM Report File : /tmp/logs/elam\_2019-09-30-03m-23h-14s.txt  
In-Select Trigger : Outerl2-outerl3-outerl4( 6 )  
Out-Select Trigger : Pktrw-sideband-drpvec( 1 )  
ELAM Captured Device : LEAF  
Packet Direction : ingress  
Triggered ASIC type : Sugarbowl  
Triggered ASIC instance : 0  
Triggered Slice : 0  
Incoming Interface : 0x24( 0x24 )  
( Slice Source ID(Ss) in "show plat int hal l2 port gpd" )

=====  
=====  
Captured Packet  
-----

-----  
Outer Packet Attributes  
-----

-----  
Outer Packet Attributes : l2uc ipv4 ip ipuc ipv4uc  
Opcode : OP CODE\_UC  
-----

-----  
Outer L2 Header  
-----

-----  
Destination MAC : 0000.1001.0102  
Source MAC : 0000.1001.0101  
802.1Q tag is valid : yes( 0x1 )  
CoS : 0( 0x0 )  
Access Encap VLAN : 2501( 0x9C5 )  
-----

-----  
Outer L3 Header  
-----

-----  
L3 Type : IPv4  
IP Version : 4  
DSCP : 0  
IP Packet Length : 84 ( = IP header(28 bytes) + IP payload )  
Don't Fragment Bit : not set  
TTL : 255  
IP Protocol Number : ICMP  
IP CheckSum : 51097( 0xC799 )  
Destination IP : 10.1.1.2  
Source IP : 10.1.1.1  
-----

=====  
=====  
Forwarding Lookup ( FPB )

```

=====
-----
Destination MAC (Lookup Key)
-----
-----
Dst MAC Lookup was performed          : yes
Dst MAC Lookup BD                     : 522( 0x20A )
( Hw BDID in "show plat int hal l2 bd pi" )
Dst MAC Address                       : 0000.1001.0102

-----
-----
Destination MAC (Lookup Result)
-----
-----
Dst MAC is Hit                        : yes
Dst MAC is Hit Index                  : 6443( 0x192B )
( phy_id in "show plat int hal objects ep l2 mac (MAC) extensions" )
or ( HIT IDX in "show plat int hal l3 nexthops" for L3OUT/L3 EP)
.....

```

## Uso de fTriage para seguir el flujo

El triaje se ejecuta desde una CLI APIC y se puede utilizar para seguir la ruta completa a través del fabric ACI. Especifique al menos la hoja de ingreso (nodo-101), la IP de origen y la IP de destino. En este caso específico es un flujo puenteado (Capa 2), por lo que se debe utilizar la opción fTriage bridge.

Tenga en cuenta que fTriage genera un archivo de registro en el directorio actual. Este archivo de registro contendrá todos los registros e informes ELAM recopilados. Esto permite que el paquete sea capturado en cada salto. La versión abreviada del resultado es la siguiente:

```

apic1# ftrriage bridge -ii LEAF:101 -sip 10.1.1.1 -dip 10.1.1.2
fTriage Status: {"dbgFtrriage": {"attributes": {"operState": "InProgress", "pid": "12181",
"apicId": "1", "id": "0"}}}
Starting ftrriage
Log file name for the current run is: ftlog_2019-10-01-18-53-24-125.txt
2019-10-01 18:53:24,129 INFO      /controller/bin/ftrriage bridge -ii LEAF:101 -sip 10.1.1.1 -dip
10.1.1.2
2019-10-01 18:53:49,280 INFO      ftrriage:      main:1165 Invoking ftrriage with default password
and default username: apic#fallback\admin
2019-10-01 18:54:10,204 INFO      ftrriage:      main:839 L2 frame Seen on leaf1 Ingress: Eth1/3
Egress: Eth1/49 Vnid: 15302583
2019-10-01 18:54:10,422 INFO      ftrriage:      main:242 ingress encap string vlan-2501
2019-10-01 18:54:10,427 INFO      ftrriage:      main:271 Building ingress BD(s), Ctx
2019-10-01 18:54:12,288 INFO      ftrriage:      main:294 Ingress BD(s) Prod:BD1
2019-10-01 18:54:12,288 INFO      ftrriage:      main:301 Ingress Ctx: Prod:VRF1
2019-10-01 18:54:12,397 INFO      ftrriage:      pktrec:490 leaf1: Collecting transient losses
snapshot for LC module: 1
2019-10-01 18:54:30,079 INFO      ftrriage:      main:933 SMAC 00:00:10:01:01:01 DMAC
00:00:10:01:01:02
2019-10-01 18:54:30,080 INFO      ftrriage:      unicast:973 leaf1: <- is ingress node
2019-10-01 18:54:30,320 INFO      ftrriage:      unicast:1215 leaf1: Dst EP is remote
2019-10-01 18:54:31,155 INFO      ftrriage:      misc:659 leaf1: L2 frame getting bridged in SUG
2019-10-01 18:54:31,380 INFO      ftrriage:      misc:657 leaf1: Dst MAC is present in SUG L2 tbl
2019-10-01 18:54:31,826 INFO      ftrriage:      misc:657 leaf1: RwdMAC DIPo(10.0.96.66) is one of
dst TEPs ['10.0.96.66']
2019-10-01 18:56:16,249 INFO      ftrriage:      main:622 Found peer-node spine1 and IF: Eth1/1 in

```

```

candidate list
2019-10-01 18:56:21,346 INFO      ftriage:      node:643  spine1: Extracted Internal-port GPD Info
for lc: 1
2019-10-01 18:56:21,348 INFO      ftriage:      fcls:4414 spine1: LC trigger ELAM with IFS: Eth1/1
Asic :0 Slice: 0 Srcid: 32
2019-10-01 18:56:54,424 INFO      ftriage:      main:839  L2 frame Seen on spine1 Ingress: Eth1/1
Egress: LC-1/0 FC-24/0 Port-0 Vnid: 15302583
2019-10-01 18:56:54,424 INFO      ftriage:      pktrec:490 spine1: Collecting transient losses
snapshot for LC module: 1
2019-10-01 18:57:15,093 INFO      ftriage:      fib:332  spine1: Transit in spine
2019-10-01 18:57:21,394 INFO      ftriage:      unicast:1252 spine1: Enter dbg_sub_nexthop with
Transit inst: ig infra: False glbs.dipo: 10.0.96.66
2019-10-01 18:57:21,508 INFO      ftriage:      unicast:1417 spine1: EP is known in COOP (DIPO =
10.0.96.66)
2019-10-01 18:57:25,537 INFO      ftriage:      unicast:1458 spine1: Infra route 10.0.96.66 present
in RIB
2019-10-01 18:57:25,537 INFO      ftriage:      node:1331 spine1: Mapped LC interface: LC-1/0 FC-
24/0 Port-0 to FC interface: FC-24/0 LC-1/0 Port-0
2019-10-01 18:57:30,616 INFO      ftriage:      node:460  spine1: Extracted GPD Info for fc: 24
2019-10-01 18:57:30,617 INFO      ftriage:      fcls:5748 spine1: FC trigger ELAM with IFS: FC-
24/0 LC-1/0 Port-0 Asic :0 Slice: 2 Srcid: 0
2019-10-01 18:57:49,611 INFO      ftriage:      unicast:1774 L2 frame Seen on FC of node: spine1
with Ingress: FC-24/0 LC-1/0 Port-0 Egress: FC-24/0 LC-1/0 Port-0 Vnid: 15302583
2019-10-01 18:57:49,611 INFO      ftriage:      pktrec:487 spine1: Collecting transient losses
snapshot for FC module: 24
2019-10-01 18:57:53,110 INFO      ftriage:      node:1339 spine1: Mapped FC interface: FC-24/0 LC-
1/0 Port-0 to LC interface: LC-1/0 FC-24/0 Port-0
2019-10-01 18:57:53,111 INFO      ftriage:      unicast:1474 spine1: Capturing Spine Transit pkt-
type L2 frame on egress LC on Node: spine1 IFS: LC-1/0 FC-24/0 Port-0
2019-10-01 18:57:53,530 INFO      ftriage:      fcls:4414 spine1: LC trigger ELAM with IFS: LC-1/0
FC-24/0 Port-0 Asic :0 Slice: 0 Srcid: 64
2019-10-01 18:58:26,497 INFO      ftriage:      unicast:1510 spine1: L2 frame Spine egress Transit
pkt Seen on spine1 Ingress: LC-1/0 FC-24/0 Port-0 Egress: Eth1/3 Vnid: 15302583
2019-10-01 18:58:26,498 INFO      ftriage:      pktrec:490 spine1: Collecting transient losses
snapshot for LC module: 1
2019-10-01 18:59:28,634 INFO      ftriage:      main:622  Found peer-node leaf3 and IF: Eth1/49 in
candidate list
2019-10-01 18:59:39,235 INFO      ftriage:      main:839  L2 frame Seen on leaf3 Ingress: Eth1/49
Egress: Eth1/12 (Po1) Vnid: 11364
2019-10-01 18:59:39,350 INFO      ftriage:      pktrec:490 leaf3: Collecting transient losses
snapshot for LC module: 1
2019-10-01 18:59:54,373 INFO      ftriage:      main:522  Computed egress encaps string vlan-2501
2019-10-01 18:59:54,379 INFO      ftriage:      main:313  Building egress BD(s), Ctx
2019-10-01 18:59:57,152 INFO      ftriage:      main:331  Egress Ctx Prod:VRF1
2019-10-01 18:59:57,153 INFO      ftriage:      main:332  Egress BD(s): Prod:BD1
2019-10-01 18:59:59,230 INFO      ftriage:      unicast:1252 leaf3: Enter dbg_sub_nexthop with Local
inst: eg infra: False glbs.dipo: 10.0.96.66
2019-10-01 18:59:59,231 INFO      ftriage:      unicast:1257 leaf3: dbg_sub_nexthop invokes
dbg_sub_eg for vip
2019-10-01 18:59:59,231 INFO      ftriage:      unicast:1784 leaf3: <- is egress node
2019-10-01 18:59:59,377 INFO      ftriage:      unicast:1833 leaf3: Dst EP is local
2019-10-01 18:59:59,378 INFO      ftriage:      misc:657  leaf3: EP if(Po1) same as egr if(Po1)
2019-10-01 18:59:59,378 INFO      ftriage:      misc:659  leaf3: L2 frame getting bridged in SUG
2019-10-01 18:59:59,613 INFO      ftriage:      misc:657  leaf3: Dst MAC is present in SUG L2 tbl
2019-10-01 19:00:06,122 INFO      ftriage:      main:961  Packet is Exiting fabric with peer-
device: n3k-3 and peer-port: Ethernet1/16

```

## Flujo de trabajo de resolución de problemas para tráfico unidifusión de capa 2 desconocido: BD en modo saturación

En este ejemplo, el MAC de destino es desconocido. La búsqueda MAC de destino en la hoja de ingreso no muestra resultados.

```
leaf1# show endpoint mac 0000.1001.0102
```

Legend:

s - arp	H - vtep	V - vpc-attached	p - peer-aged
R - peer-attached-rl	B - bounce	S - static	M - span
D - bounce-to-proxy	O - peer-attached	a - local-aged	m - svc-mgr
L - local	E - shared-service		

VLAN/ Domain	Encap VLAN	MAC Address IP Address	MAC Info/ IP Info	Interface
-----------------	---------------	---------------------------	----------------------	-----------

Dado que BD está configurado como 'Inundación' para unidifusión desconocida L2, esto es lo que sucederá a un nivel alto:

1. La hoja de ingreso codificará el encabezado del paquete para asignarlo a uno de los FTAG (de 0 a 15).
2. La hoja de ingreso encapsulará la trama en un paquete VXLAN con el VNID BD. La IP de destino externa será BD GIPO + FTAG.
3. Se inundará en el fabric siguiendo una topología de árbol y debería llegar a cada nodo de hoja que tenga el BD implementado.

Esta sección resaltaré lo que se puede comprobar.

## Búsqueda de BD GIPO

La GUI identifica el grupo multicast 225.1.5.48 utilizado por el BD para el tráfico multidestino.

## BD GIPO

## ELAM — hoja de ingreso — tráfico inundado

Con el asistente de ELAM, se comprueba el informe de ELAM de la hoja de entrada. Esto muestra que la trama se inundó en el BD y está egresando en todos los enlaces ascendentes de fabric (aquí eth1/49, 1/50, 1/51 y 1/52).



## ELAM Assistant - hoja de ingreso - Información de reenvío de paquetes

### Packet Forwarding Information

		Forward Result
Destination Type	Flood in BD	
Destination Ports	eth1/51, eth1/50, eth1/52, eth1/49 (overlay (Fabric uplink))	
vPC Designated Forwarder (DF)	yes	
Sent to SUP/CPU as well	no	
SUP Redirect Reason (SUP code)	NONE	

		Contract
Destination EPG pcTag (dclass)	16386 (null)	
Source EPG pcTag (sclass)	32770 (null)	
Contract was applied	0 (Contract was not applied on this node)	

		Drop
Drop Code		no drop

Para encontrar el valor FTAG seleccionado por la hoja de ingreso, vaya al informe sin procesar del Asistente de ELAM.

```
sug_lu2ba_sb_info.mc_info.mc_info_nopad.ftag: 0xC
```

Al convertir el valor hexadecimal de 0xC a decimal, esto da como resultado FTAG 12.

### Dibujo de la topología FTAG

IS-IS calcula la topología FTAG. Se crea una topología de árbol para cada valor FTAG, con una lista de interfaz raíz y de salida que permite una topología de distribución de carga óptima.

Muestre la topología FTAG local mediante el siguiente comando. En el siguiente ejemplo, estamos usando la topología FTAG ID 12 en spine1.

```
spine1# show isis internal mcast routes ftag
IS-IS process: isis_infra
  VRF : default
FTAG Routes
=====
```

```
FTAG ID: 12 [Enabled] Cost:( 2/ 11/ 0)
```

```
-----
```

```
Root port: Ethernet1/4.39
```

```
OIF List:
```

```
Ethernet1/11.11
```

```
Ethernet1/12.12
```

Dibujar la topología FTAG completa en un fabric ACI de gran tamaño puede resultar una tarea larga y compleja. El script Python 'aci-ftag-viewer' (<https://github.com/agccie/aci-ftag-viewer>) se puede copiar en un APIC. Genera la topología FTAG completa del fabric en una sola pasada.

El siguiente resultado muestra el árbol FTAG 12 en Pod1 de un entramado de varios dispositivos e incluye la topología FTAG en los dispositivos IPN.

Esto muestra que si el tráfico ingresa al fabric ACI desde leaf101, atravesará las siguientes trayectorias según se indica en la salida del script a continuación.

```
admin@apic1:tmp> python aci_ftag_viewer.py --ftag 12 --pod 1
#####
# Pod 1 FTAG 12
# Root spine-204
# active nodes: 8, inactive nodes: 1
#####
spine-204
+- 1/1 ----- 1/52 leaf-101
+- 1/2 ----- 1/52 leaf-102
+- 1/3 ----- 1/52 leaf-103
+- 1/4 ----- 1/52 leaf-104
      +- 1/49 ----- 1/4 spine-201
      |
      |           +- 1/11 ..... (EXT) Eth2/13 n7706-01-Multipod-A1
      |           +- 1/12 ..... (EXT) Eth2/9 n7706-01-Multipod-A2
      |
      +- 1/50 ----- 1/4 spine-202
      |
      |           +- 1/11 ..... (EXT) Eth2/14 n7706-01-Multipod-A1
      |           +- 1/12 ..... (EXT) Eth2/10 n7706-01-Multipod-A2
      |
      +- 1/51 ----- 2/4 spine-203
      |
      |           +- 2/11 ..... (EXT) Eth2/15 n7706-01-Multipod-A1
      |           +- 2/12 ..... (EXT) Eth2/11 n7706-01-Multipod-A2
+- 1/11 ..... (EXT) Eth2/16 n7706-01-Multipod-A1
+- 1/12 ..... (EXT) Eth2/12 n7706-01-Multipod-A2
```

## ELAM — hoja de salida — tráfico inundado

En este caso, el tráfico inundado llega a todas las hojas del fabric de ACI. Por lo tanto, alcanzará tanto la hoja 3 como la hoja 4 que son el par VPC. Ambos nodos de hoja tienen un VPC al destino. Para evitar los paquetes duplicados, el par VPC elige solamente una hoja para reenviar el tráfico inundado al destino. La hoja seleccionada se denomina hoja VPC DF (hoja de reenviador designada VPC).

Esto se puede verificar en ELAM mediante el siguiente disparador en ambos nodos de hoja.

```
module-1# debug platform internal tah elam ASIC 0
module-1(DBG-elam)# trigger reset
module-1(DBG-elam)# trigger init in-select 14 out-select 1
module-1(DBG-elam-insell4)# set inner ipv4 src_ip 10.1.1.1 dst_ip 10.1.1.2
module-1(DBG-elam-insell4)# start
```

salida de leaf3:

```
module-1(DBG-elam-insell14)# ereport | egrep vpc.*df  
sug_lub_latch_results_vec.lub4_1.vpc_df: 0x1
```

salida de hoja4:

```
module-1(DBG-elam-insell14)# ereport | egrep vpc.*df  
sug_lub_latch_results_vec.lub4_1.vpc_df: 0x0
```

En el resultado anterior, leaf3 tiene el valor '0x1' configurado para el campo 'vpc\_df', mientras que leaf4 tiene '0x0' configurado para el campo 'vpc\_df'. Por lo tanto, el reenviador designado será leaf3. leaf3 reenviará el paquete inundado en su link VPC al EP de destino.

## Flujo de trabajo de resolución de problemas para tráfico unidifusión de capa 2 desconocido: BD en proxy de hardware

La situación actual enumerada es la del tráfico unicast desconocido de Capa 2 con el BD en modo proxy de hardware. En este escenario, dado que la hoja de ingreso no conoce la dirección MAC de destino, reenviará el paquete a la dirección MAC de proxy de difusión por proximidad de la columna. La columna realizará una búsqueda COOP para la dirección MAC de destino.

Si la búsqueda se realiza correctamente, como se muestra a continuación, la columna reescribirá la IP de destino externa en el destino del túnel (aquí 10.0.96.66) y la enviará al par VPC hoja3- hoja4.

```
spinel# show coop internal info repo ep key 15302583 00:00:10:01:01:02
```

```
Repo Hdr Checksum : 16897  
Repo Hdr record timestamp : 10 01 2019 11:05:46 351360334  
Repo Hdr last pub timestamp : 10 01 2019 11:05:46 352019546  
Repo Hdr last dampen timestamp : 01 01 1970 00:00:00 0  
Repo Hdr dampen penalty : 0  
Repo Hdr flags : IN_OBJ EXPORT ACTIVE  
EP bd vnid : 16351141  
EP mac : 00:00:10:01:01:02  
flags : 0x90  
repo flags : 0x122  
Vrf vnid : 2097154  
Epg vnid : 0  
EVPN Seq no : 0  
Remote publish timestamp: 01 01 1970 00:00:00 0  
Snapshot timestamp: 10 01 2019 11:05:46 351360334  
Tunnel nh : 10.0.96.66  
MAC Tunnel : 10.0.96.66  
IPv4 Tunnel : 10.0.96.66  
IPv6 Tunnel : 10.0.96.66  
ETEP Tunnel : 0.0.0.0
```

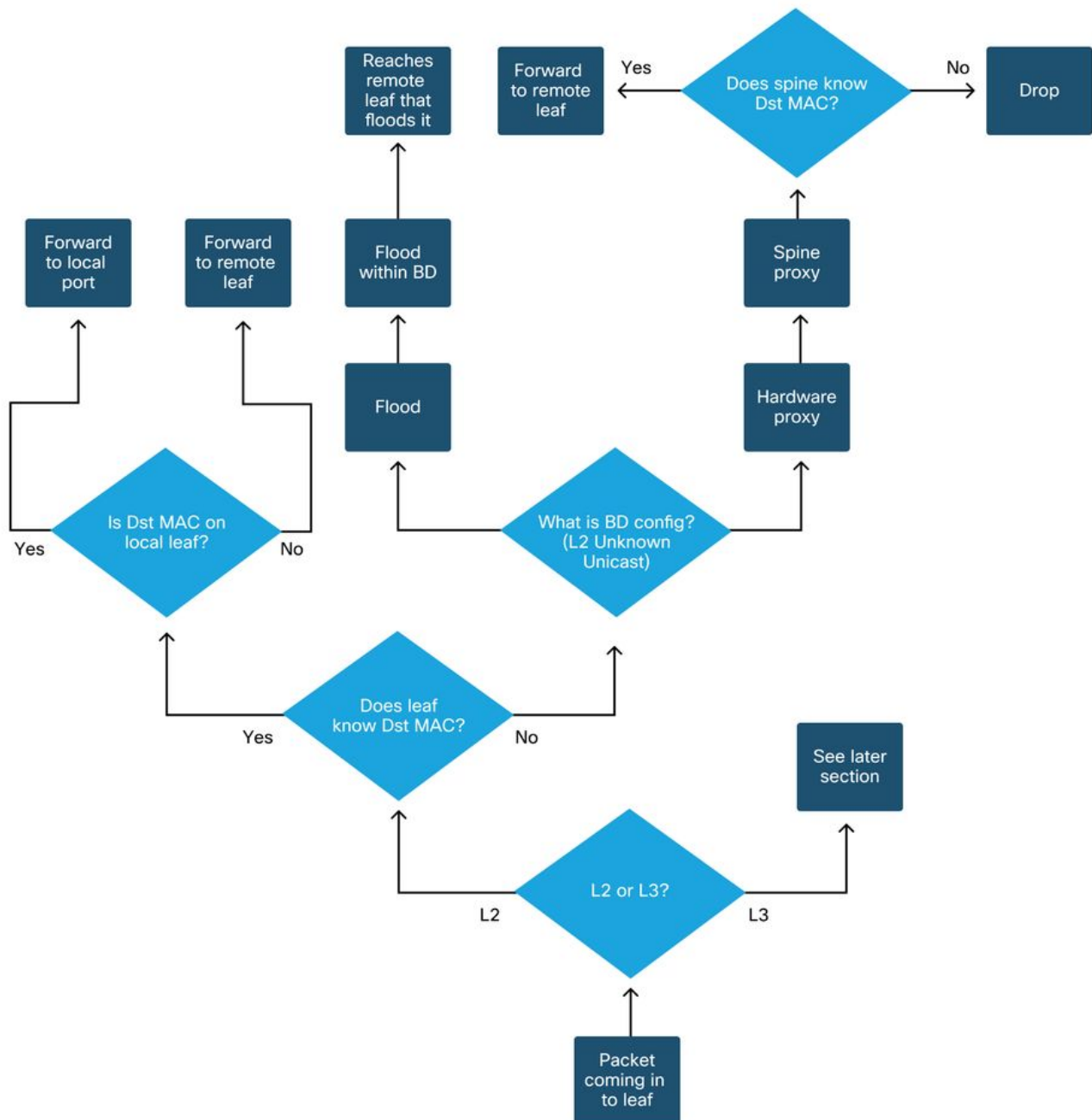
Si la búsqueda falla (el terminal es desconocido en el fabric de ACI), la columna descartará la unidifusión desconocida.

```
spinel# show coop internal info repo ep key 15302583 00:00:10:01:01:02  
Key not found in repo
```

## Resumen de reenvío de capa 2

El siguiente diagrama resume el posible comportamiento de reenvío para el tráfico de capa 2 en el fabric de ACI.

### Comportamiento de reenvío de capa 2 del fabric ACI



## 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).