

Risoluzione dei problemi di inoltro intra-fabric ACI - Inoltro di layer 2

Sommario

[Introduzione](#)

[Premesse](#)

[Panoramica](#)

[Topologia](#)

[Controllo GUI](#)

[Flusso di lavoro di risoluzione dei problemi per il traffico unicast di layer 2 noto](#)

[Apprendimento MAC EP di origine foglia in ingresso](#)

[Ricerca endpoint MAC di destinazione foglia in ingresso](#)

[Interruttore foglia in ingresso invio a interruttore dorso](#)

[Inoltro dorso](#)

[Esci da leaf remote EP MAC learning](#)

[Ricerca MAC destinazione foglia in uscita](#)

[Verificare che entrambi gli endpoint siano stati appresi correttamente nel repository EP COOP switch spine](#)

[Output ELAM con ELAM Assistant](#)

[ELAM foglia in ingresso con CLI](#)

[Utilizzo di Triage per seguire il flusso](#)

[Flusso di lavoro di risoluzione dei problemi per il traffico unicast di layer 2 sconosciuto - BD in modalità flood](#)

[Ricerca di GIPo BD](#)

[ELAM — foglia in entrata — traffico allagato](#)

[Disegno della topologia FTAG](#)

[ELAM — Foglia di uscita — traffico allagato](#)

[Flusso di lavoro di risoluzione dei problemi per il traffico unicast di layer 2 sconosciuto - BD in proxy hardware](#)

[Riepilogo inoltro Layer 2](#)

[Comportamento inoltro ACI fabric Layer 2](#)

Introduzione

In questo documento viene descritto come comprendere e risolvere i problemi relativi all'inoltro di livello 2 in ACI

Premesse

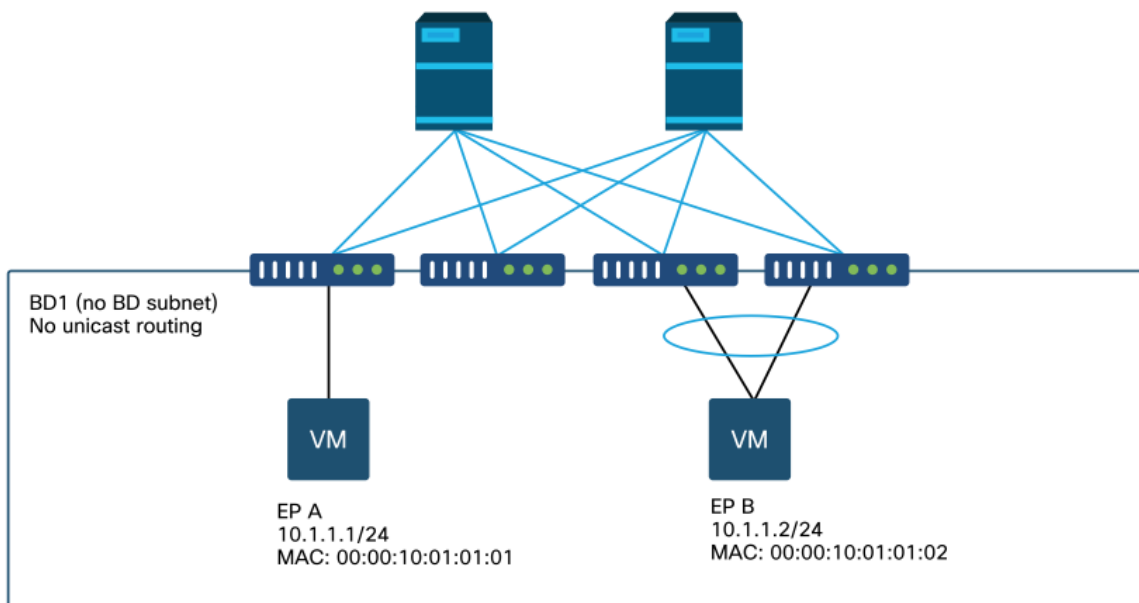
Il materiale tratto da questo documento è stato [Risoluzione dei problemi di Cisco Application Centric Infrastructure, Second Edition](#) libro, in particolare **Inoltro intra-fabric - L2: due endpoint nello stesso BD - nessun routing unicast** capitolo.

Panoramica

In questa sezione viene illustrato un esempio di risoluzione dei problemi in cui gli endpoint nello stesso dominio bridge e nella stessa subnet non possono comunicare tra loro. Nella figura seguente viene illustrata la topologia in cui BD non dispone di subnet e il routing unicast è disabilitato.

In genere, per risolvere i problemi relativi ai flussi di traffico con connettività degli endpoint, si consiglia di iniziare a identificare una coppia di endpoint. Fare riferimento alla topologia riportata di seguito con gli EP A e B. Questi avranno rispettivamente gli indirizzi IP 10.1.1.1/24 e 10.1.1.2/24. Gli indirizzi MAC saranno rispettivamente 00:00:10:01:01:01 e 00:00:10:01:01:02.

Topologia



In questa sezione sono disponibili tre scenari:

1. Flusso unicast di livello 2 noto.
2. Flusso unicast di livello 2 sconosciuto con BD in modalità flood.
3. Flusso unicast di livello 2 sconosciuto con BD in modalità proxy hardware.

I flussi di risoluzione dei problemi che verranno seguiti possono essere riepilogati con il seguente schema:

- Verifica livello 1: Convalida GUI della configurazione, errori ed endpoint appresi.
- Controllo livello 2: CLI sugli switch foglia: Verificare che gli switch foglia di origine e di destinazione abbiano familiarità con gli endpoint. Controllate se i nodi della spine apprendono l'endpoint in COOP.
- Verifica livello 3: Acquisizione pacchetti: ELAM (ELAM Assistant o CLI) per verificare che il frame sia presente. Ftrace per tenere traccia del flusso.

Controllo GUI

Il primo livello di risoluzione dei problemi consiste nel verificare dalla GUI che l'indirizzo MAC dell'endpoint sia stato appreso correttamente. A tale scopo, è possibile utilizzare la scheda operativa dell'EPG in cui si trova l'endpoint.

'Scheda operativa EPG > Endpoint client'

Client End-Points							
MAC	IP	Learning Source	Hosting Server	Report Name	Interface	Multicast Address	Encap
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

In questo scenario, gli endpoint A e B vengono mostrati nella GUI. La GUI mostra i loro indirizzi MAC, l'interfaccia a cui sono connessi al fabric e l'incapsulamento - in questo caso entrambi sono nella VLAN 2501 dell'encap.

È previsto che l'indirizzo IP non venga appreso dalla struttura ACI poiché il routing unicast è stato disabilitato a livello BD.

Fare riferimento alla colonna delle fonti di apprendimento nello screenshot precedente. Se il messaggio indica che l'operazione è stata completata, lo switch foglia ACI ha ricevuto almeno un pacchetto dall'endpoint.

Poiché in questo caso gli endpoint vengono appresi dalla struttura ACI, passare alla successiva richiesta di risoluzione dei problemi per il traffico unicast di layer 2 noto.

Flusso di lavoro di risoluzione dei problemi per il traffico unicast di layer 2 noto

Apprendimento MAC EP di origine foglia in ingresso

In caso di inoltro di livello 2 nello stesso BD, ACI apprenderà solo l'indirizzo MAC di origine e lo inoltrerà in base all'indirizzo MAC di destinazione. Gli indirizzi MAC vengono appresi nell'ambito di BD.

Verificare innanzitutto se l'endpoint è stato appreso:

```
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
```

L'output precedente fornisce le seguenti informazioni:

- L'indirizzo MAC 0000.1001.0101 viene appreso localmente (il flag è L per local) sulla porta ethernet 1/3 con incapsulamento vlan-2501 nel vrf Prod:VRF1.
- Fare riferimento alla colonna 'VLAN/Domain' nell'output precedente. L'ID VLAN elencato è la VLAN interna.

Ricerca endpoint MAC di destinazione foglia in ingresso

Si supponga che l'indirizzo MAC di destinazione sia noto (unicast noto).

```
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
```

L'output precedente fornisce le seguenti informazioni:

- L'indirizzo MAC 0000.1001.0102 non viene appreso localmente.
- Viene appreso dall'interfaccia tunnel 4.
- Viene appreso nell'incapsulamento VXLAN-16351141 che corrisponde al BD_VNID (VXLAN Network ID) del dominio bridge.

Quindi, controllare la destinazione dell'interfaccia del tunnel con il 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 ipvlan
  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
```

In questo modo, il pacchetto verrà incapsulato nella VXLAN con il TEP di origine IP 10.0.88.95 (assegnato al loopback0) e inviato alla destinazione TEP IP 10.0.96.66.

Confermare l'indirizzo IP di origine:

```
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
```

La destinazione TEP IP 10.0.96.66 può essere una delle seguenti:

- Indirizzo PTEP di un'altra foglia (può essere controllato utilizzando `aciddiag fmvread`)
- VIP VPC (può essere visto in 'GUI > Fabric > Access Policies > Policies > Switch > Virtual Port Channel default' (vedi screenshot qui sotto))
- Un IP di loopback su uno switch dorso. Per verificare questa condizione, usare il comando 'show ip interface vrf overlay-1' sullo switch con dorso.

Gruppi di protezione VPC espliciti

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

Interruttore foglia in ingresso invio a interruttore dorso

La foglia in entrata incapsula il frame nella VXLAN con l'IP di destinazione esterno impostato su 10.0.96.66, ossia l'IP di destinazione del tunnel elencato nel precedente comando "show interface tunnel 4". e lo incapsula nella VXLAN con il VNID del dominio bridge (vxlan-16351141), come mostrato nell'output del comando 'show endpoint mac 000.1001.0102' precedente.

In base al percorso IS-IS in VRF overlay-1 determinare dove inviarlo:

```
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
```

Pertanto, esiste un routing ECMP (Equal Cost Multipath) verso la destinazione che utilizza eth1/49 e 1/50, ovvero gli uplink della struttura agli switch con dorsa.

Inoltro dorso

La tabella di routing VRF overlay-1 sul dorso mostra che la route host 10.0.96.66 è raggiungibile tramite verso foglia3 o foglia4. Il valore previsto è 10.0.96.66 e corrisponde all'indirizzo VIP VPC degli switch foglia 103 e 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

Esci da leaf remote EP MAC learning

In questo caso, il TEP di destinazione è una coppia VPC, quindi il pacchetto arriverà su foglia3 o foglia4. Fare riferimento agli output del comando di seguito. Leaf4 dovrebbe mostrare un output simile. Poiché fanno parte della stessa coppia VPC, tutti gli endpoint sono sincronizzati tra i due switch foglia.

L'apprendimento dell'endpoint per il traffico di layer 2 sulla foglia di uscita si basa sull'indirizzo MAC di origine che viene appreso in BD corrispondente al VNID nel pacchetto ricevuto. È possibile verificare questa condizione nella tabella degli endpoint.

L'indirizzo MAC di origine si trova dietro il tunnel 26 nella VXLAN-16351141.

Il tunnel 26 va al TEP IP 10.0.88.95 che è foglia1:

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

```

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 vxlan
  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

```

Ricerca MAC destinazione foglia in uscita

Il comando "show endpoint" conferma che l'MAC di destinazione è stato acquisito dietro il canale porta 1 e usa l'incapsulamento 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/                Encap          MAC Address      MAC Info/        Interface
      Domain                VLAN          IP Address      IP Info
+-----+-----+-----+-----+-----+
---+
135/Prod:VRF1                vlan-2501      0000.1001.0102  LpV
pol

```

Vale a dire che il frame lascia il fabric ACI su canale porta interfaccia foglia3 1 con ID VLAN 2501 di accesso. Il codice VNID di BD si trova nella scheda Tenant Operational (Operativo tenant) nell'interfaccia utente.

Verificare che entrambi gli endpoint siano stati appresi correttamente nel repository EP COOP switch spine

Il repository COOP EP deve essere sincronizzato tra tutti i nodi della spine. il repository EP COOP può essere controllato utilizzando il VNID BD come chiave e immettendo l'indirizzo MAC EP.

L'indirizzo MAC di origine di questo flusso viene imparato dall'hop successivo del tunnel 10.0.88.95 che è l'IP TEP di foglia1. Inoltre, l'output del comando mostra il VNID 16351141 che corrisponde al dominio bridge corretto.

```
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
```

L'indirizzo MAC di destinazione di questo flusso viene individuato in base al VPC VIP 10.0.96.66 di foglia3 e foglia4. Viene inoltre elencato il VNID BD EP 16351141, che corrisponde al BD corretto.

```
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
```

Output ELAM con ELAM Assistant

ELAM Assistant è una potente applicazione ACI che può semplificare l'esecuzione di acquisizioni ELAM su un fabric ACI.

I trigger ELAM Assistant possono essere avviati contemporaneamente su più nodi foglia. Di conseguenza, pacchetti specifici possono essere controllati in parallelo in foglia1, foglia3 e foglia4.

L'acquisizione ELAM configurata viene visualizzata come illustrato di seguito. Come osservato, il pacchetto viene visto su foglia1 (nodo-101) e foglia3 (nodo-103).

ELAM Assistant — parametri

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	

Il report di foglia1 (nodo-101) mostra quanto segue:

- L'output delle informazioni sul pacchetto acquisito conferma l'ingresso del pacchetto su eth1/3 e dispone delle informazioni corrette sull'indirizzo MAC e IP.
- Le informazioni di inoltrato mostrano che il pacchetto viene inoltrato il 1°/49 al TEP IP 10.0.96.66.

ELAM Assistant — leaf1 (node-101) — Informazioni sul pacchetto acquisito

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) — Informazioni inoltrato pacchetti

Packet Forwarding Information	
Forward Result	
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
Contract	
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)
Drop	

In foglia3 (nodo-103) sulla foglia in uscita si osserva quanto segue:

Nelle informazioni sul pacchetto acquisito su foglia3, entra da eth1/49. L'indirizzo IP esterno conferma quanto segue:

- PASSAGGIO origine: 10.0.88.95
- TEP destinazione: 10.0.96.66
- ID: 16351141 (BD VNID)

ELAM Assistant — foglia3 (nodo-103) — Informazioni sul pacchetto acquisito

Captured Packet Information	
Basic Information	
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)

Le informazioni sull'inoltro di pacchetti mostrano che il traffico viene inoltrato sulla porta 1 e in particolare su Ethernet 1/12.

Packet Forwarding Information	
Forward Result	
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
Contract	
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)
Drop	
Drop Code	no drop

ELAM foglia in ingresso con CLI

Si consiglia di utilizzare ELAM Assistant poiché semplifica il funzionamento delle acquisizioni ELAM. Tuttavia, è possibile anche usare i comandi CLI sugli switch ACI per generare un report ELAM. Di seguito è riportato un esempio di come ciò avverrà.

Usare la sequenza di trigger mostrata per acquisire il pacchetto sulla foglia in entrata. Fare riferimento alla sezione "Strumenti" per ulteriori informazioni sulle opzioni ELAM.

- Nell'esempio, l'ASIC è 'tah' come foglia (numero di parte che termina con '-EX').
- Il comando "in-select 6" viene usato per acquisire un pacchetto proveniente da una porta downlink senza un'interfaccia VXLAN.
- 'out-select 1' visualizza anche il vettore di caduta (in caso di perdita di pacchetto).
- Il comando 'reset' è necessario per assicurarsi che tutti i trigger precedenti siano stati puliti.
- Anche se si tratta di un ELAM a flusso collegato, ha visibilità nell'intestazione IP. Di conseguenza, è possibile utilizzare 'ipv4 src_ip' e 'dst_ip' per impostare il trigger.

```
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
```

Per verificare se il pacchetto è stato ricevuto, controllare lo stato ELAM. Se è presente un trigger, significa che è stato intercettato un pacchetto che soddisfa le condizioni.

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

Nell'output successivo il report viene visualizzato utilizzando il comando 'report'. L'output è molto lungo, quindi viene incollato solo l'inizio. Si noti tuttavia che il report completo viene salvato per un'analisi successiva in una posizione nel file system foglia. Il nome del file contiene anche i timestamp dell'acquisizione di 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
```

Il 'report' convalida il pacchetto ricevuto e le informazioni sono come previsto (indirizzo MAC di origine e destinazione, indirizzo IP di origine e destinazione, ecc.)

```
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 : OPCODE_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)  
.....
```

Utilizzo di Triage per seguire il flusso

fTriage viene eseguito da una CLI APIC e può essere utilizzato per seguire il percorso completo attraverso l'infrastruttura ACI. Specificare almeno la foglia in entrata (nodo 101), l'IP di origine e l'IP di destinazione. In questo caso specifico si tratta di un flusso con bridging (livello 2), quindi deve essere utilizzata l'opzione del bridge fTriage.

Si noti che fTriage genera un file log nella directory corrente. Questo file di log conterrà tutti i log e i report ELAM raccolti. In questo modo, il pacchetto può essere acquisito in ogni hop. La versione breve dell'output è la seguente:

```
apic1# ftriage 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/ftriage 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 ftrriage: node:643 spine1: Extracted Internal-port GPD Info  
for lc: 1  
2019-10-01 18:56:21,348 INFO ftrriage: 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

```

Flusso di lavoro di risoluzione dei problemi per il traffico unicast di layer 2 sconosciuto - BD in modalità flood

In questo esempio, l'indirizzo MAC di destinazione è sconosciuto. La ricerca MAC di destinazione nella foglia in entrata non visualizza alcun output.

```
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
-----------------	---------------	---------------------------	----------------------	-----------

Dato che il BD è impostato su "Flood" (Inondazione) per l'unicast L2 sconosciuto, di seguito viene riportato ciò che accadrà ad alto livello:

1. La foglia in ingresso eseguirà l'hash dell'intestazione del pacchetto per assegnarla a uno dei FTAG (da 0 a 15).
2. Il foglio in ingresso incapsula il frame in un pacchetto VXLAN con il VNID BD. L'indirizzo IP di destinazione esterno sarà BD GIPo + FTAG.
3. Verrà inondato nel fabric seguendo una topologia ad albero e dovrebbe raggiungere ogni nodo foglia in cui è installato BD.

In questa sezione vengono evidenziati gli elementi che è possibile controllare.

Ricerca di GIPo BD

La GUI identifica il gruppo multicast 25.1.5.48 usato da BD per il traffico tra più destinazioni.

GIPo BD

Bridge Domain - BD1

Summary Policy Operational Stats Health Faults History

General L3 Configurations Advanced/Troubleshooting

100

Properties

Unknown Unicast Traffic Class ID: 16386
Segment: 15302583
Multicast Address: 225.1.5.48
Monitoring Policy: select a value
First Hop Security Policy: select a value
Optimize WAN Bandwidth:
NetFlow Monitor Policies:

NetFlow IP Filter Type	NetFlow Monitor Policy
No items have been found. Select Actions to create a new item.	

ELAM — foglia in entrata — traffico allagato

Utilizzando ELAM Assistant, viene controllato il report ELAM sulla foglia in entrata. Ciò dimostra che il telaio è stato allagato nel BD ed è in movimento su tutti gli uplink fabric (qui eth1/49, 1/50, 1/51 e 1/52).

ELAM Assistant - foglia in entrata - Informazioni sull'inoltro di pacchetti

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

Per trovare il valore FTAG selezionato dalla foglia in entrata, passare al report non elaborato di ELAM Assistant.

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

Quando si converte il valore esadecimale di 0xC in decimale, si ottiene FTAG 12.

Disegno della topologia FTAG

La topologia FTAG viene calcolata da IS-IS. Per ogni valore FTAG viene creata una topologia ad albero, con un elenco di interfacce radice e di output che consente una topologia di distribuzione del carico ottimale.

Visualizzare la topologia FTAG locale utilizzando il comando seguente. Nell'esempio seguente viene utilizzata la topologia FTAG ID 12 su 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
```

Disegnare la topologia FTAG completa in un fabric ACI di grandi dimensioni può rivelarsi un'attività lunga e complessa. Lo script Python 'aci-ftag-viewer' (<https://github.com/agccie/aci-ftag-viewer>) può essere copiato su un APIC. Genera la topologia FTAG completa della struttura in un singolo passaggio.

L'output seguente mostra la struttura FTAG 12 in Pod1 di un fabric Multi-Pod e include la topologia FTAG sui dispositivi IPN.

Ciò mostra che se il traffico entra nell'infrastruttura ACI da leaf101, attraverserà i seguenti percorsi, come elencato nell'output dello script riportato di seguito.

```
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 — Foglia di uscita — traffico allagato

In questo caso, il traffico inondato raggiunge ogni foglia del tessuto ACI. Così, raggiungerà sia foglia3 che foglia4 che sono la coppia VPC. Entrambi i nodi foglia hanno un VPC verso la destinazione. Per evitare la duplicazione dei pacchetti, la coppia di VPC seleziona solo una foglia per inoltrare il traffico a destinazione. La foglia selezionata è denominata foglia VPC DF (foglia VPC designata mittente).

È possibile eseguire il check-in di ELAM utilizzando il seguente trigger su entrambi i nodi foglia.

```
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-insel14)# set inner ipv4 src_ip 10.1.1.1 dst_ip 10.1.1.2  
module-1(DBG-elam-insel14)# start
```

uscita foglia3:

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

uscita foglia4:

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

Nell'output precedente, il valore di leaf3 '0x1' è impostato per il campo 'vpc_df', mentre il valore di leaf4 '0x0' è impostato per il campo 'vpc_df'. Pertanto, il server d'inoltro designato sarà foglia3. Leaf3 inoltrerà il pacchetto allagato sul suo collegamento VPC all'EP di destinazione.

Flusso di lavoro di risoluzione dei problemi per il traffico unicast di layer 2 sconosciuto - BD in proxy hardware

Lo scenario corrente elencato è quello relativo al traffico unicast di layer 2 con BD in modalità proxy hardware. In questo scenario, poiché la foglia in entrata non conosce l'indirizzo MAC di destinazione, il pacchetto viene inoltrato all'indirizzo proxy-mac della spine anycast. Il dorso eseguirà una ricerca COOP per l'indirizzo MAC di destinazione.

Se la ricerca ha esito positivo come mostrato di seguito, il dorso riscriverà l'IP di destinazione esterna alla destinazione del tunnel (qui 10.0.96.66) e lo invierà alla coppia VPC foglia3-foglia4.

```
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
```

Se la ricerca ha esito negativo (endpoint sconosciuto nell'infrastruttura ACI), il dorso eliminerà l'unicast sconosciuto.

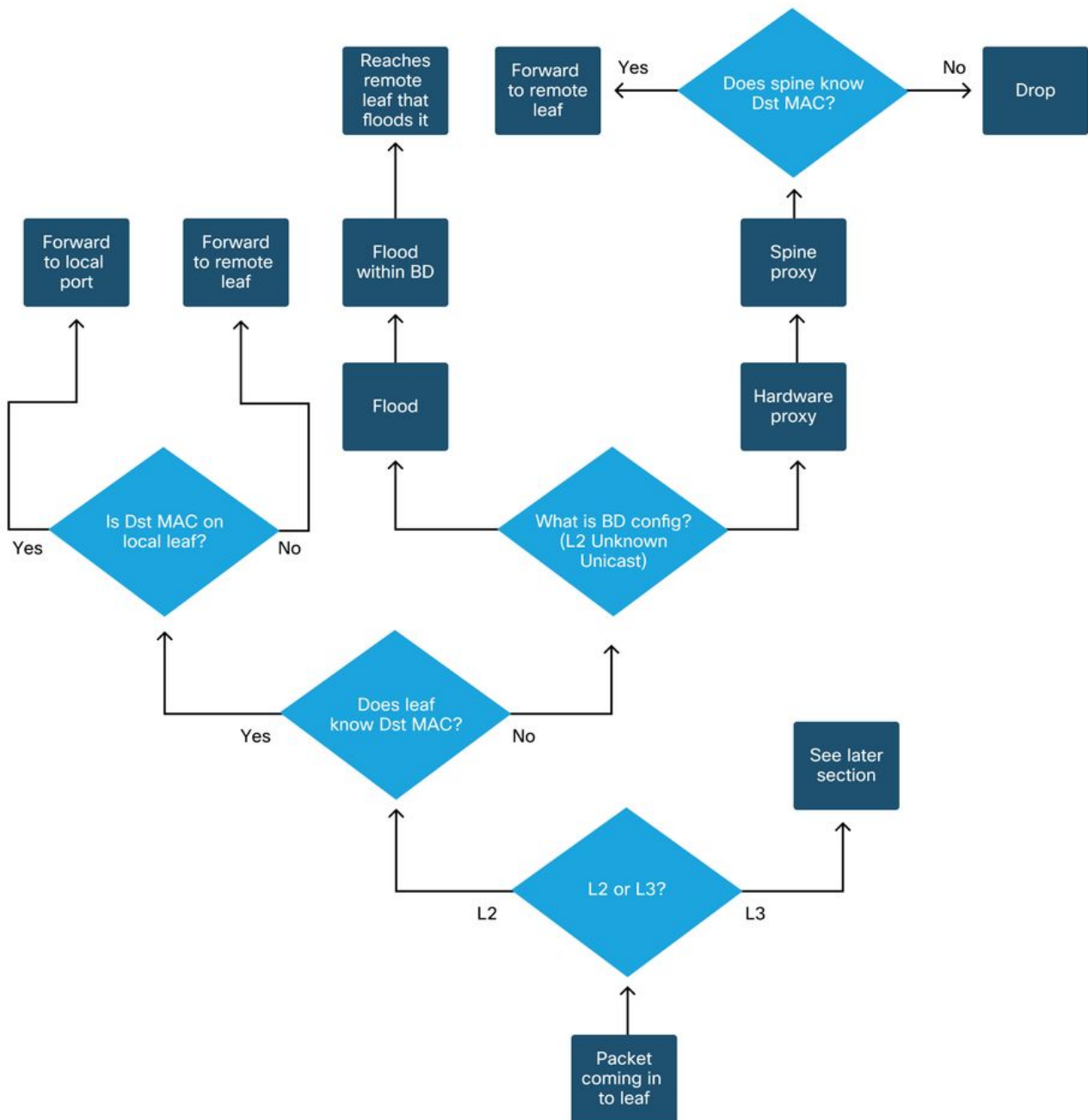
```
spinel# show coop internal info repo ep key 15302583 00:00:10:01:01:02  
Key not found in repo
```

Riepilogo inoltro Layer 2

Il diagramma seguente riepiloga il possibile comportamento di inoltro per il traffico di layer 2

nell'infrastruttura ACI.

Comportamento inoltro ACI fabric Layer 2



Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).