

# Risoluzione dei problemi di trasmissione ExtCommunity di EVPN per ACI Fabric

## Sommario

[Introduzione](#)

[Premesse](#)

[Problema](#)

## Introduzione

Questo documento descrive l'impatto di un attributo della community estesa MAC del router non configurato correttamente su un'infrastruttura ACI quando ricevuto da un peer Border Gateway Protocol (BGP) esterno.

## Premesse

Con BGP, è possibile inviare gli attributi della community e della community estesa con i prefissi annunciati ai peer BGP. Questi attributi della community consentono di modificare i criteri di routing e di modificare dinamicamente il modo in cui viene gestito il traffico indirizzato.

## Problema

Quando l'attributo della community estesa MAC del router viene inviato con un prefisso AFI IPv4 da un peer BGP esterno a un'infrastruttura ACI, la programmazione errata di FIB e HAL si verifica su una foglia dell'infrastruttura che riceve la route dalle foglie del bordo tramite il processo MP-BGP interno. Infatti, l'attributo extcommunity dell'indirizzo RMAC appartiene alla famiglia di indirizzi VPN BGP L2VPN e, quando viene inserito nella famiglia di indirizzi IPv4 BGP, viene rifiutato. Ciò è dovuto a una violazione della regola 5.2 (Uniform-Propagation-Mode), descritta nel documento IETF intitolato "EVPN Interworking with IPVPN". A pagina 15, punto 4, lettera c), è indicato il problema specifico:

4. As discussed, Communities, Extended Communities and Large Communities SHOULD be kept by the gateway PE from the originating SAFI route. Exceptions of Extended Communities that SHOULD NOT be kept are:

C. All the extended communities of type EVPN.

The gateway PE SHOULD NOT copy the above extended communities from the originating ISF route to the re-advertised ISF route.

Link al documento: [EVPN Interworking con IPVPN](#)

Ecco un esempio del problema con iBGP, tuttavia, il problema è visto anche con eBGP.

Diagramma topologico:

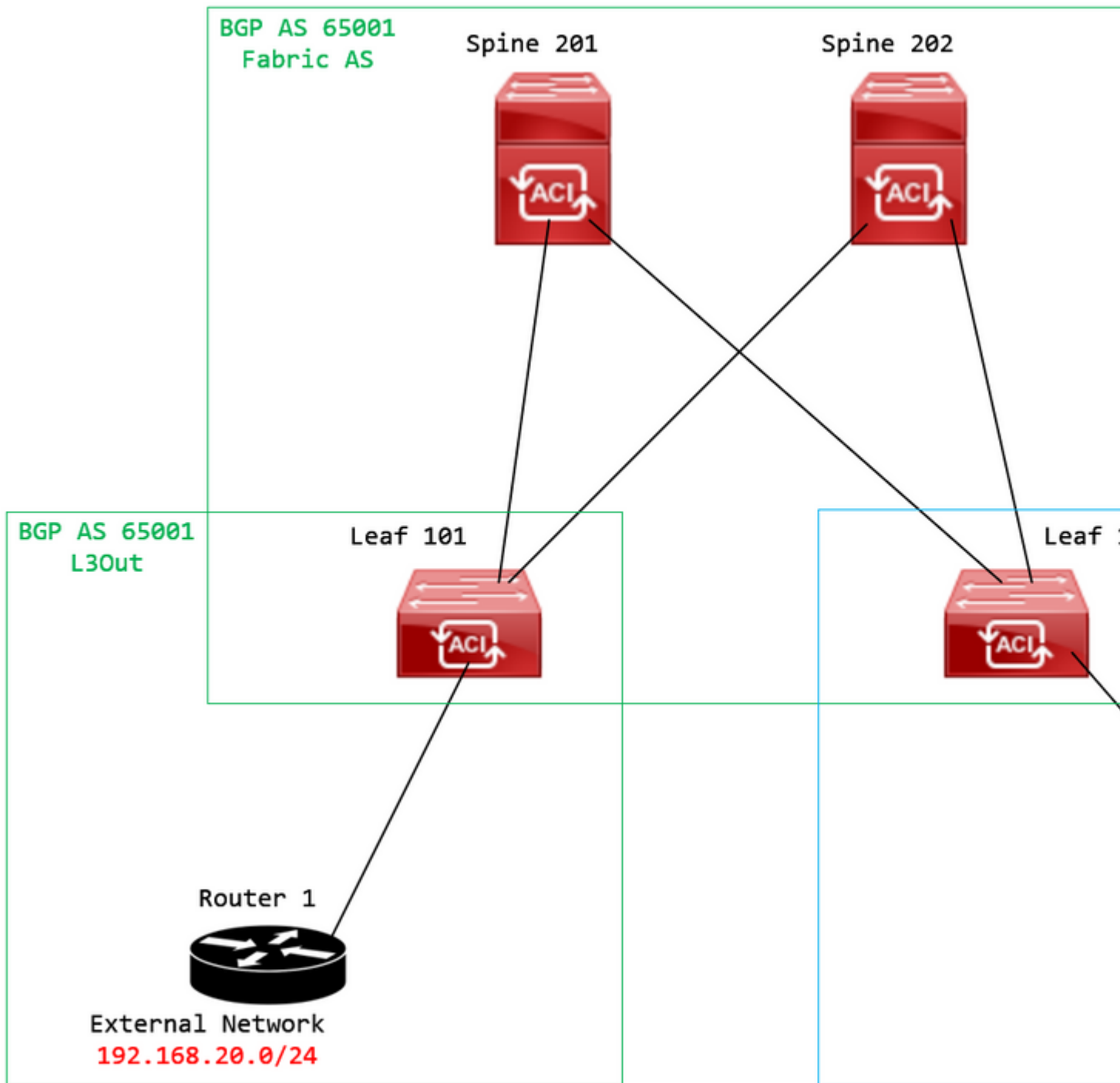


Diagramma topologico

Configurare la mappa delle route sul dispositivo peer BGP esterno (router 1) e impostare l'attributo della community di estensione RMAC EVPN:

```
Router-1# show run | sec route-map
route-map RMAC permit 10
  set extcommunity evpn rmac aaaa.bbbb.cccc
```

In Configurazione famiglia di indirizzi IPv4 dei router adiacenti BGP, configurare le community estese BGP e configurare la mappa delle route nella direzione in uscita:

```
Router-1# show run bgp
```

<output omitted>

feature bgp

router bgp 65001

vrf example

router-id 192.168.20.20

address-family ipv4 unicast

network 192.168.20.0/24

neighbor 192.168.30.30

remote-as 65001

update-source loopback1

address-family ipv4 unicast

send-community extended

route-map RMAC out

Verificare lo stato BGP su BL 101:

<#root>

leaf-101# show ip bgp 192.168.20.0 vrf example:example

BGP routing table information for VRF example:example, address family IPv4 Unicast

BGP routing table entry for 192.168.20.0/24, version 40 dest ptr 0xa0fec840

Paths: (1 available, best #1)

Flags: (0x80c001a 00000000) on xmit-list, is in urib, is best urib route, is in HW, exported

vpn: version 2725, (0x100002) on xmit-list

Multipath: eBGP iBGP

Advertised path-id 1, VPN AF advertised path-id 1

Path type (0xa96485b8): internal 0x18 0x0 ref 0 adv path ref 2, path is valid, is best path

AS-Path: NONE, path sourced internal to AS

192.168.20.20 (metric 5) from 192.168.20.20 (192.168.20.20)

Origin IGP, MED not set, localpref 100, weight 0 tag 0, propagate 0

Extcommunity:

RT:65001:2162688

COST:pre-bestpath:163:1879048192

Router MAC:aaaa.bbbb.cccc

**\*\*\*Notice that the router mac is present here.\*\*\***

VNID:2162688

VRF advertise information:

Path-id 1 not advertised to any peer

VPN AF advertise information:

```
Path-id 1 advertised to peers:
 10.0.216.65      10.0.216.66
```

Controllare RIB su CL 102:

```
<#root>
```

```
leaf-102# show ip route 192.168.20.0 vrf example:example
IP Route Table for VRF "example:example"
 '*' denotes best ucast next-hop
 '**' denotes best mcast next-hop
 '[x/y]' denotes [preference/metric]
 '%<string>' in via output denotes VRF <string>
```

```
192.168.20.0/24
```

```
, ubest/mbest: 1/0
   *via
```

```
10.0.210.70
```

```
%overlay-1, [200/0], 00:00:43, bgp-65001, internal, tag 65001,
```

```
rwVnid: vxlan-2162688
```

```
recursive next hop: 10.0.210.70/32%overlay-1
```

**\*\*\*Notice that we have the route here and our next-hop address is correct (showing the TEP IP of BL 101)**

```
leaf-102# acidiag fvnread | grep 101
 101      1      leaf-101      <output omitted>
```

```
10.0.210.70/32
```

```
leaf      active  0
```

Controllare FIB su CL 102:

```
<#root>
```

```
module-1(DBG-elam-insel6)# show forwarding route 192.168.20.0 vrf example:example
ERROR: no longest match in IPv4 table 0xf5df36b0
```

**\*\*\*No entry is present.\*\*\***

Controllare la tabella HAL su CL 102:

```
<#root>
```

```
module-1(DBG-elam-insel6)# show platform internal hal 13 routes | grep 192.168.20.0
```

```
***No entry is present.***
```

Ping da EP (host 1) all'host nella rete esterna proveniente dal peer BGP esterno (192.168.20.20):

```
<#root>
```

```
Host-1# ping 192.168.20.20 vrf example
PING 192.168.20.20 (192.168.20.20): 56 data bytes
Request 0 timed out
Request 1 timed out
Request 2 timed out
Request 3 timed out
Request 4 timed out
```

```
--- 192.168.20.20 ping statistics ---
5 packets transmitted, 0 packets received, 100.00% packet loss
```

```
***No connectivity.***
```

Controllare ELAM su CL 102:

```
<#root>
```

```
leaf-102# vsh_lc
module-1# debug platform internal roc elam asic 0
module-1(DBG-elam)# trigger reset
module-1(DBG-elam)# trigger init in-select 6 out-select 0
module-1(DBG-elam-insel6)# set outer ipv4 src_ip 192.168.10.10 dst_ip 192.168.20.20
module-1(DBG-elam-insel6)# start
module-1(DBG-elam-insel6)# stat
```

```
ELAM STATUS
=====
Asic 0 Slice 0 Status Armed
Asic 0 Slice 1 Status Triggered
```

```
module-1(DBG-elam-insel6)# ereport
Python available. Continue ELAM decode with LC Pkg
ELAM REPORT
<output omitted>
```

```
-----
Lookup Drop
```

```
-----
LU drop reason :
```

```
UC_PC_CFG_TABLE_DROP
```

```
***Notice the drop vector here.***
```

## Soluzione

La soluzione consiste nell'interrompere l'invio dell'attributo della community estesa MAC del router con un prefisso della famiglia di indirizzi IPv4 da un peer BGP esterno a un'infrastruttura ACI.

Rimuovere la mappa delle route configurata in precedenza e interrompere l'invio delle community estese dal dispositivo peer BGP esterno (router 1). La rimozione di una di queste configurazioni o di entrambe funzionerà:

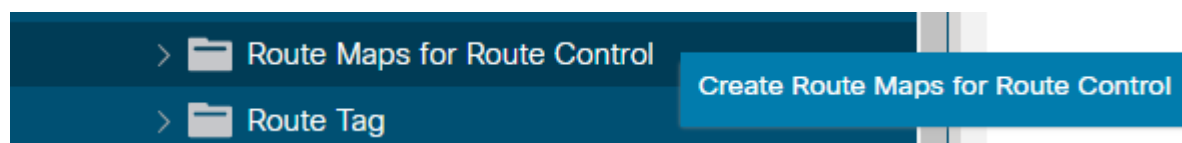
```
Router-1# show run bgp
```

```
feature bgp
```

```
router bgp 65001
  vrf example
    router-id 192.168.20.20
    address-family ipv4 unicast
      network 192.168.20.0/24
    neighbor 192.168.30.30
      remote-as 65001
      update-source loopback1
      address-family ipv4 unicast
```

Un'altra soluzione (meno preferibile) è quella di filtrare semplicemente tutte le community ricevute dal dispositivo peer BGP esterno creando una mappa dei percorsi nella L3Out configurata in ACI.

Passare alla Tenant > Policies > Protocol > Route Maps for Route Control > Create Route Maps for Route Control:



*Selezionare l'opzione Crea route map per il controllo route*

Assegnare un nome alla mappa del percorso, abilitare `Route-Map Continue` e quindi aggiungere un contesto. Selezionare il `+` nella tabella **Contesti**:

# Create Route Maps for Route Control

Name:

Description:

Route-Map Continue:

This action will be applied on all the entries which are part of Per Peer BGP Route-map.

## Contexts

Order	Name	Action	Des
-------	------	--------	-----

*Crea mappa route e crea contesto*

Assegnare un nome al contesto e lasciare l'azione predefinita di `Permit` selezionato, quindi creare una regola di corrispondenza selezionando la `+` icona nella `Associated Matched Rules` e selezionare **Create Match Rule for a Route Map:**

# Create Route Control Context





Order:   

Name:

Action:  Deny  Permit

Description:

Associated Matched Rules:  

Rule Name

**Create Match Rule for a Route Map**

Set Rule:  

**Cancel** 

*Crea contesto di controllo ciclo di lavorazione e seleziona l'opzione Crea regola di corrispondenza per una mappa ciclo di lavorazione*

Assegnare un nome alla regola di corrispondenza, quindi aggiungere un nuovo prefisso selezionando l'icona + nella casella Match Prefix tabella:



# Create Match Rule

Name:

Description:

Match Regex Community Terms:

Name	Regular Expression	Community Type	Description
------	--------------------	----------------	-------------

Match Community Terms:

Name	Description
------	-------------

Match Prefix:

IP	Description	Aggregate	Greater Mask
----	-------------	-----------	--------------

*Crea regola corrispondenza e crea prefisso corrispondenza*

Aggiungere il prefisso desiderato. Nell'esempio viene mostrato come aggiungere un aggregato di tutti i prefissi:

# Create Match Route Destination Rule



IP:

Description:

Aggregate:

Greater Than Mask:

Less Than Mask:

Cancel

OK

*Crea regola di destinazione route corrispondente*

Dopo aver selezionato **OK** nel **Create Match Route Destination Rule** , il prefisso è stato aggiunto alla **Match Prefix** tabella nella **Create Match Rule** finestra:

# Create Match Rule

Name:

Description:

Match Regex Community Terms:

Name	Regular Expression	Community Type	Description
------	--------------------	----------------	-------------

Match Community Terms:

Name	Description
------	-------------

Match Prefix:

IP	Description	Aggregate	Great Mask
0.0.0.0/0		True	0

*Il prefisso di corrispondenza è stato aggiunto alla regola di corrispondenza*

Dopo aver selezionato **Submit** nel **Create Match Rule** finestra, selezionare **Update** nel **Associated Matched Rules** tabella nella **Create Route Control Context** finestra:

# Create Route Control Context



Order:  ^  
v

Name:

Action:  Deny  Permit

Description:

Associated Matched Rules: 🗑️ +

Rule Name

Set Rule:  v

*Aggiungi regola di corrispondenza associata a contesto di controllo route*

La regola di corrispondenza associata verrà aggiunta al contesto:

# Create Route Control Context





Order:   

Name:

Action:  Deny  Permit

Description:

Associated Matched Rules:  

Rule Name

remove-communities-match-rule

Set Rule:  

*La regola di corrispondenza associata è stata aggiunta al contesto di controllo della route*

Selezionare quindi il menu a discesa accanto a Set Rule e selezionare [Create Set Rules for a Route Map](#):

# Create Route Control Context



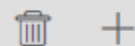
Order:   

Name:

Action:  Deny  Permit

Description:

Associated Matched Rules:



Rule Name

Set Rule:  

[Create Set Rules for a Route Map](#)

Cancel

OK

*Selezionare l'opzione per creare regole per una mappa ciclo di lavorazione*

Assegnare un nome alla regola impostata, quindi selezionare **Set Community** e lasciare invariati i criteri predefiniti di **No community** selezionato:

# Create Set Rules for a Route Map

## STEP 1 > Select

Name:

Description:

Set Community:  Criteria:

Set Route Tag:

Set Dampening:

Set Weight:

Set Next Hop:

Set Preference:

Set Metric:

Set Metric Type:

Additional Communities:

Set AS Path:

Next Hop Propagation:

Multipath:

Set External EPG:

Previous

*Crea regola set per mappa route*

Dopo aver selezionato **Fine** nella casella **Create Set Rules for a Route Map** viene visualizzata la regola impostata selezionata nella finestra **Create Route Control Context** **finestra**:

# Create Route Control Context



Order:

Name:

Action:  Deny  Permit

Description:

Associated Matched Rules:

Rule Name		
remove-communities-match-rule		

Set Rule:

*Imposta regola aggiunta al contesto di controllo route*

Dopo aver selezionato **OK** nel **Create Route Control Context** viene visualizzato il contesto aggiunto alla **Contexts** tabella nella **Create Route Maps for Route Control** finestra. Infine, selezionare **Submit** per completare la configurazione:



# Create Route Maps for Route Control

Name:

Description:

Route-Map Continue:

This action will be applied on all the entries which are part of Per Peer BGP Route-map.

## Contexts

Order	Name	Action	Des
0	remove-communitites-context	Permit	

*Il contesto è stato aggiunto alla mappa route*

Passare al profilo BGP Peer Connectivity in L3Out e selezionare la scheda + icona nella Route Control Profile , quindi aggiungere la mappa dei percorsi con la direzione predefinita Route Import Policy selezionato:

## BGP Peer Connectivity Profile 192.168.20.20

Properties

Send Domain Path

Password:

Confirm Password:

Allowed Self AS Count:

Peer Controls:  Bidirectional Forwarding Detection  
 Disable Connected Check

Address Type Controls:  AF Mcast  
 AF Ucast

Routing Domain ID: 0

EBGP Multihop TTL:

Weight for routes from this neighbor:

Private AS Control:  Remove all private AS  
 Remove private AS  
 Replace private AS with local AS

BGP Peer Prefix Policy:   
Pre-existing BGP session must be reset to apply the Prefix policy

Site of Origin:   
e.g. extended:as2-nn2:1000:65534  
e.g. extended:ipv4-nn2:1.2.3.4:65515  
e.g. extended:as4-nn2:1000:65505  
e.g. extended:as2-nn4:1000:6554387

Local-AS Number Config:

Local-AS Number:   
This value must not match the MP-BGP RR policy

Route Control Profile:

Name	Direction
<input type="text" value="select an option"/>	<input type="text" value="Route Import Policy"/>
<b>remove-communities</b>	
mr	

Aggiungi mappa route al profilo di connettività peer BGP

Dopo aver selezionato **Aggiorna** per la mappa del percorso, verrà visualizzata la mappa del percorso aggiunta al Route Control Profile tabella:

## BGP Peer Connectivity Profile 192.168.20.20

✖ ⚠ ⚡ ⚙

### Properties

Send Domain Path

Password:

Confirm Password:

Allowed Self AS Count:

Peer Controls:  Bidirectional Forwarding Detection  
 Disable Connected Check

Address Type Controls:  AF Mcast  
 AF Ucast

Routing Domain ID: 0

EBGP Multihop TTL:

Weight for routes from this neighbor:

Private AS Control:  Remove all private AS  
 Remove private AS  
 Replace private AS with local AS

BGP Peer Prefix Policy:   
Pre-existing BGP session must be reset to apply the Prefix policy

Site of Origin:   
e.g. extended:as2-nn2:1000:65534  
e.g. extended:ipv4-nn2:1.2.3.4:65515  
e.g. extended:as4-nn2:1000:65505  
e.g. extended:as2-nn4:1000:6554387

Local-AS Number Config:

Local-AS Number:   
This value must not match the MP-BGP RR policy

Route Control Profile:

Name	Direction
remove-communities	Route Import Policy

*La mappa delle route è ora aggiunta al profilo di connettività peer BGP*

\*Per ulteriori informazioni sulle opzioni di configurazione della mappa del percorso in ACI, consultare il [white paper ACI Fabric L3Out](#)

Dopo aver implementato una delle soluzioni precedenti, verificare se il problema è stato risolto.

Verificare lo stato BGP su BL 101:

<#root>

```
leaf-101# show ip bgp 192.168.20.0 vrf example:example
BGP routing table information for VRF example:example, address family IPv4 Unicast
BGP routing table entry for 192.168.20.0/24, version 46 dest ptr 0xa0fec840
Paths: (1 available, best #1)
Flags: (0x80c001a 00000000) on xmit-list, is in urib, is best urib route, is in HW, exported
  vpn: version 2731, (0x100002) on xmit-list
Multipath: eBGP iBGP
```



```
Prefix          | Next-hop      | Interface/VRF | Additional Info
```

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

```
*192.168.20.0/24
```

```
10.0.210.70
```

```
overlay-1
```

```
***Notice that we have the route here and our next-hop address is correct (showing the TEP IP of BL 101)
```

```
Route Class-id:0x0  
Policy Prefix 0.0.0.0/0
```

```
leaf-102# acidiag fmvread | grep 101  
101      1      leaf-101
```

```
10.0.210.70/32
```

```
leaf      active  0
```

Tabella HAL su CL 102:

```
<#root>
```

```
module-1(DBG-elam-insel6)# show platform internal hal l3 routes | grep 192.168.20.0  
|
```

```
4662  
| 192.168.20.0/ 24| UC| 686| 20601| TRIE| a5| 5/ 0| 60a5|A| 8443| 86b6| ef5| 1/ 2|
```

```
***Notice that we have an entry here and it's in the correct VRF.***
```

```
module-1(DBG-elam-insel6)# hex
```

```
4662
```

```
0x
```

```
1236
```

```
module-1(DBG-elam-insel6)# show platform internal hal l3 vrf pi
```

```
=====
```

Vrf	Hw	I	I	Vrf	-- TOR --	- Spine -	ACL							
VrfId	Name	VrfId	I	S	Vnid	SB	NB	Proxy	ACI	Ing	Msk	Lbl	Egr	Msk
						BdId	BdId	Ou	Bd	Enc				

```
=====
```

```
26 example:example
```

```
1236
```

```
0 0 210000 0 0 0 1 0 0 0 0 0 0 0
```

Ping da EP (host 1) all'host nella rete esterna proveniente dal peer BGP esterno (192.168.20.20):

```
<#root>
```

```
Host-1# ping 192.168.20.20 vrf example
PING 192.168.20.20 (192.168.20.20): 56 data bytes
64 bytes from 192.168.20.20: icmp_seq=0 ttl=252 time=1.043 ms
64 bytes from 192.168.20.20: icmp_seq=1 ttl=252 time=1.292 ms
64 bytes from 192.168.20.20: icmp_seq=2 ttl=252 time=1.004 ms
64 bytes from 192.168.20.20: icmp_seq=3 ttl=252 time=0.769 ms
64 bytes from 192.168.20.20: icmp_seq=4 ttl=252 time=1.265 ms
```

```
--- 192.168.20.20 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.769/1.074/1.292 ms
```

```
***Connectivity is there.***
```

ELAM su CL 102:

```
<#root>
```

```
leaf-102# vsh_lc
module-1# debug platform internal roc elam asic 0
module-1(DBG-elam)# trigger reset
module-1(DBG-elam)# trigger init in-select 6 out-select 0
module-1(DBG-elam-insel6)# set outer ipv4 src_ip 192.168.10.10 dst_ip 192.168.20.20
module-1(DBG-elam-insel6)# start
module-1(DBG-elam-insel6)# stat
```

```
ELAM STATUS
```

```
=====
```

```
Asic 0 Slice 0 Status Armed
```

```
Asic 0 Slice 1 Status Triggered
```

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

```
ELAM REPORT
```

```
<output omitted>
```

```
-----
Lookup Drop
-----
```

```
LU drop reason :
```

```
no drop
```

```
***Traffic forwards correctly.***
```

## Informazioni correlate

- Questo comportamento è documentato anche in questo difetto: ID bug Cisco [CSCvx28929](#)
- [Documentazione e supporto tecnico](#) © Cisco Systems

## 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).