Fix EVPN RMAC ExtCommunity Transmission Issues to ACI Fabric

Contents

Introduction Background Information Problem

Introduction

This document describes the impact of misconfigured Router MAC extended community attribute on an ACI fabric when received from an external Border Gateway Protocol (BGP) peer.

Background Information

With BGP, there is an option to send community and extended community attributes with the prefixes that are advertised to BGP peers. These community attributes allow us to modify routing policies and dynamically alter the way routed traffic is handled.

Problem

When the Router MAC extended community attribute is sent with an IPv4 AFI prefix from an external BGP peer to an ACI fabric, FIB and HAL misprogramming occurs on any leaf in the fabric that receives the route from the border leaf(s) via the internal MP-BGP process. This is because the RMAC extcommunity attribute belongs to the BGP L2VPN EVPN address family, and when it is injected into the BGP IPv4 address family, it gets rejected. This is due to a violation of rule 5.2 (Uniform-Propagation-Mode), which is described in the IETF document entitled, "EVPN Interworking with IPVPN". On page 15, item 4c, the specific issue is called out:

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 to document: EVPN Interworking with IPVPN

Here is an example of the problem with iBGP, however, the problem is also seen with eBGP.

Topology Diagram:



Topology diagram

Configure route map on external BGP peer device (Router 1) and set the EVPN RMAC extcommunity attribute:

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

Under the BGP neighbor IPv4 address family configuration, configure BGP extended communities, and configure the route map in the outbound direction:

<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

Check the BGP status on 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

Check RIB on 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 fnvread | grep 101
 101 1 leaf-101 <output omitted>

10.0.210.70/32

leaf active 0

Check FIB on 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.

Check the HAL table on CL 102:

<#root>

```
module-1(DBG-elam-insel6)# show platform internal hal 13 routes | grep 192.168.20.0
***No entry is present.***
```

Pings from EP (Host 1) to host in external network that comes from external BGP peer (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
--- 192.168.20.20 ping statistics --5 packets transmitted, 0 packets received, 100.00% packet loss
No connectivity.

Check ELAM on 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 Ø 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.

Solution

The solution is to stop sending the Router MAC extended community attribute with an IPv4 address family prefix from an external BGP peer to an ACI fabric.

Remove the previously configured route map and stop sending extended communities from the external BGP peer device (Router 1). Removing either one of these configs, or both, will work:

```
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
```

Another (less preferred) solution is to simply filter out all communities received from the external BGP peer device by creating a route map in the configured L3Out in ACI.

Navigate to your Tenant > Policies > Protocol > Route Maps for Route Control > Create Route Maps for Route Control:



Select the option to Create Route Maps for Route Control

Name your route map, enable the Route-Map Continue option, and then add a context. Select the + icon in the **Contexts** table:

Create Route Maps for Route Control

Name	remove-communities	
Description	: optional	
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

Create Route Map and create Context

Name your context, and leave the default action of Permit selected, then create a match rule by selecting the + icon in the Associated Matched Rules table, and select Create Match Rule for a Route Map:

Order:	0	
Name:	remove-communitites-context	
Action:	Deny Permit	
Description:	optional	
Associated Matched Rules:	1	m +
	Rule Name	
	select an option	~ 9
	Create Match Rule for a Route Map	
Set Rule:	select a value	
Set Rule:	select a value	
Set Rule:	select a value	
Set Rule:	select a value	

Create Route Control Context and select option for Create Match Rule for a Route Map

Name your match rule then add a new prefix by selecting the + icon in the Match Prefix table:

Create Match Rule

Name:	remove-communities	s-match-rule		
Description:	optional			
Match Regex Community Terms:				
	Name	Regular Expression	Community Type	Descr
Match Community Terms:				
	Name	I	Description	
Match Prefix:				
	IP	Description	Aggregate	Great Mask

Create Match Rule and create Match Prefix

Add your desired prefix. This example shows how to add an aggregate of all prefixes:

Create Match Route Destination Rule

IP:	0.0.0/0	
Description:	optional	
Aggregate:		
Greater Than Mask:	0	
Less Than Mask:	0	



Create Match Route Destination Rule

After you select **OK** in the Create Match Route Destination Rule window, you see that your prefix has been added to the Match Prefix table in the Create Match Rule window:



Create Match Rule

Name:	remove-communities	s-match-rule		
Description:	optional			
Match Regex Community Terms:				
	Name	Regular Expression	Community Type	Desc
Match Community Terms:				
	Name		Description	
Match Prefix:				
	IP	Description	Aggregate	Great Mask
	0.0.0/0		True	0

Match Prefix is now added to Match Rule

After you select Submit in the Create Match Rule window, select Update in the Associated Matched Rules table in the Create Route Control Context window:

Order:	0		
Name:	remove-communitites-context		
Action:	Deny Permit		
Description:	optional		
Associated Matched Rules:		1	+
	Rule Name		
	remove-communities-match-rule		\sim
	Update Cancel		
Set Rule:	select a value		

Cancel

Add Associated Match Rule to Route Control Context

Your associated match rule is now added to your context:

Order:	0		
Name:	remove-communitites-context		
Action:	Deny Permit		
Description:	optional		
Associated Matched Rules:		1	+
	Rule Name		
	remove-communities-match-rule		
Set Rule:	select a value		
	Cancel	ОК	

Associated Match Rule is now added to Route Control Context

Next, select the dropdown menu next to Set Rule and select Create Set Rules for a Route Map:

Order:	0		
Name:	remove-communitites-context		
Action:	Deny Permit		
Description:	optional		
Associated Matched Rules:		1	+
	Rule Name		
	remove-communities-match-rule		
Set Rule:	select a value		
	Create Set Rules for a Route Map		
	Cancel	ОК	

Select option to Create Set Rules for a Route Map

Name your set rule, then select the Set Community option and leave the default criteria of No community selected:

Create Set Rules for a Route Map

STEP 1 > Select	
Name:	remove-communities-set-rule
Description:	optional
Set Community:	Criteria: No community
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

Create Set Rule for Route Map

After you select Finish in the Create Set Rules for a Route Map window, you see your set rule selected in the Create Route Control Context window:

Order:	0		
Name:	remove-communitites-context		
Action:	Deny Permit		
Description:	optional		
Associated Matched Rules:		1	+
	Rule Name		
	remove-communities-match-rule		
Set Rule:	remove-communities-set-rule		
	Cancel	OK	

Set Rule is now added to Route Control Context

After you select OK in the Create Route Control Context window, you see your context added to the Contexts table in the Create Route Maps for Route Control window. Finally, select Submit to complete the configuration:

Create Route Maps for Route Control

remove-communitites-context

Name:	remove-communities	
Description:	optional	
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

Permit

Context is now added to Route Map

0

Navigate to the BGP Peer Connectivity Profile in the L3Out and select the + icon in the Route Control Profile table, then add your route map with the default direction of Route Import Policy selected:

BGP Peer Connectivity Profile 192.168.20.20

🔞 👽 📣 🕦			
Properties			
	Send Domain Path		
Password:			
Confirm Password:			
Allowed Self AS Count:	3		
Peer Controls:	 Bidirectional Forwarding Detection Disable Connected Check 		
Address Type Controls:	AF Mcast		
Routing Domain ID:	0		
EBGP Multihop TTL:	3		
Weight for routes from this neighbor:	0		
Private AS Control:	Remove all private AS		
	Remove private AS Replace private AS with local AS		
BGP Peer Prefix Policy:	Select a value		
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
	select an option	~ 0	Route Import Policy
	remove-communities		Cancel
	mr		Cancer

Add Route Map to BGP Peer Connectivity Profile

After you select **Update** for the route map, you see your route map added to the Route Control Profile table:

BGP Peer Connectivity Profile 192.168.20.20

Properties Send Domain Path Password: Confirm	8 👽 🛆 🕔		
Send Domain Path Password: Confirm Password: Allowed Self AS Count Bidirectional Forwarding Detection Desable Connected Check Address Type Controls: Af Weight for routes from this neighbor: Private AS Control: Remove all private AS Replace AD Replace AD Replace AD Replace AD Rep	Properties		
Password: Confirm Password: Allowed Self AS Court: Bidirectional Forwarding Detection Disable Connected Check Address Type Controls: AF Mcast Af Ucast Routing Domain ID: EBGP Multihop TTL: BGP Multihop TTL: Remove all private AS Private AS Control: Remove all private AS Replace Prefix Policy Reversion BBC Policy Route Control Profile Replace private AS Replace Priva		Send Domain Path	
Confirm Passwort:	Password:		
Allowed Self AS Count: 3 Peer Controls: Bidirectional Forwarding Detection Disable Connected Check Address Type Controls: AF Mcast @ AF Ucast Routing Domain ID: 0 EBGP Multihop TTL: 3 @ AF Ucast Routing Domain ID: 0 EBGP Multihop TTL: 3 @ AF Ucast Private AS Control: Remove all private AS Private AS Control: Remove all private AS @ Replace private AS Replace asign BGP Session must be reset to apply the Prefix policy Site of Origin: 0 extended:as2-nn2:1000 65553 @ extended:as2-nn2:1000 65553 Route asign BGP @ extended:as2-nn2:1000 65553 Route asign BGP @ extended:as2-nn2:1000 65553 Route asign BGP @ extended:as2-nn2:1000 65553 Route asig	Confirm Password:		
Peer Controls: Bidirectional Forwarding Detection Disable Connected Check Address Type Controls: AF Mcast AF Ucast Routing Domain ID: EBGP Multihop TTL: 3 O EBGP Multihop TTL: 3 O Private AS Control: Remove all private AS Private AS Control: Remove all private AS Pre-existing BGP session must be reset to apply the Prefix policy Site of Origin: e.g. extended as2-nn2:1000:65534 e.g. e	Allowed Self AS Count:	3	
Address Type Controls: AF Mcast AF Ucast Routing Domain ID: 0 EBGP Multihop TTL: 3 Weight for routes from this neighbor: 0 Private AS Control: Remove all private AS Remove private AS Remove private AS Replace Prefix Policy Site of Origin: Q extended as2-nn2:1000:65534 e 0. extended as2-nn2:1000:6554387 Local-AS Number Config This value must not match the MP-BGP RR policy This value must not match the MP-BGP RR policy And Manter Applicy Prectoin Route Control Profile; A Name Direction	Peer Controls:	 Bidirectional Forwarding Detection Disable Connected Check 	
AF Ucast Routing Domain ID: BGP Multihop TTL: BGP Multihop TTL: BGP Multihop TTL: Remove from this neighbor: Private AS Control: Remove all private AS Replace private AS Replace private AS Replace private AS Replace private AS Replace private AS Replace asign must be reset to apply the Prefix policy Site of Origin: e g extended:as2-nn2:1000:65534 e g extended:as2-nn2:1000:65535 e.g. extended:as2-nn2:1000:6554387 Local-AS Number Config: This value must not match the MP-BGP RR policy Route Control Profile Amme Pre-communities Route Import Policy Route Import Policy	Address Type Controls:	AF Mcast	
Routing Domain ID: 0 EBGP Multihop TTL: 3 Weight for routes from this neighbor: Private AS Control: Remove all private AS Remove private AS Remove private AS Replace private AS R		AF Ucast	
EBGP Multihop TTL: 3 Weight for routes from this neighbor: O Private AS Control: Remove all private AS Remove private AS Replace Prefix Policy Route Of Origin Network and the MP-BGP RR policy Route Control Profile Name Direction Route Import Policy Route Import Policy	Routing Domain ID:	0	
Weight for routes from this neighbor: 0 • Private AS Control: Remove all private AS • Replace private AS • Replace private AS Replace private AS • Replace private AS BGP Peer Prefix Policy: select a value • Pre-existing BGP session must be reset to apply the Prefix policy. select a value • Site of Origin: • • e.g. extended:as2-nn2:1000:65534 e.g. extended:as4-nn2:10:2.3.4:65515 e.g. extended:as4-nn2:1000:65505 •.g. extended:as4-nn2:1000:65505 e.g. extended:as4-nn2:1000:65505 e.g. extended:as4-nn2:1000:65505 e.g. extended:as4-nn2:1000:65505 F.g. extended:as4-nn2:1000:65505 F.g.	EBGP Multihop TTL:	3	
Private AS Control: Remove all private AS Remove private AS Replace private AS with local AS BGP Peer Prefix Policy: Site of Origin: e.g. extended:as2-nn2:1000:65534 e.g. extended:as2-nn2:1000:65534 e.g. extended:as2-nn2:1000:6554387 Local-AS Number Config: Local-AS Number: This value must not match the MP-BGP RR policy Route Control Profile:	Weight for routes from this neighbor:	0	
Remove private AS Replace private AS with local AS BGP Peer Prefix Policy: select a value 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:as2-nn2:1000:6554387 Local-AS Number Config: Local-AS Number: This value must not match the MP-BGP RR policy Route Control Profile ^ Name Direction remove-communities	Private AS Control:	Remove all private AS	
BGP Peer Prefix Policy: select a value 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:as4-nn2:1.2.3.4:65515 e.g. extended:as4-nn2:1000:65505 e.g. extended:as4-nn2:1000:65505 e.g. extended:as2-nn4:1000:65505 e.g. extended:as2-nn4:1000:6554387 Image: Comparison of Comparison		Remove private AS Replace private AS with local AS	
Site of Origin: Image: Pre-existing BGP session must be reset to apply the Prefix policy Site of Origin: Image: Pre-existing BGP session must be reset to apply the Prefix policy e.g. extended:as2-nn2:1000:65534 Image: Pre-existing BGP session must be reset to apply the Prefix policy e.g. extended:as2-nn2:1000:65534 Image: Pre-existing BGP session must be reset to apply the Prefix policy e.g. extended:as2-nn2:1000:65534 Image: Pre-existing BGP session must be reset to apply the Prefix policy Local-AS Number Config: Image: Pre-existing BGP session must be reset to apply the Prefix policy Local-AS Number Image: Pre-existing BGP session must be reset to apply the Prefix policy Route Control Profile: Image: Pre-existing BGP session must be reset to apply the Prefix policy Image: Pre-existing BGP session must be reset to apply the Prefix policy Image: Pre-existing BGP session must be reset to apply the Prefix policy Route Control Profile: Image: Pre-existing BGP session must be reset to apply the Prefix policy Image: Pre-existing BGP session must be reset to apply the Prefix policy Image: Pre-existing BGP session must be reset to apply the Prefix policy Image: Pre-existing BGP session must be reset to apply the Prefix policy Image: Pre-existing BGP session must be reset to apply the Prefix policy Image: Pre-existing BGP session must be reset to apply the Prefix policy Image: Pre-existing BGP ses	BGP Peer Prefix Policy:	select a value	
Site of Origin: e.g. extended:as2-nn2:1000:65534 e.g. extended:isy4-nn2:1.2.3.4:65515 e.g. extended:as4-nn2:1000:65505 e.g. extended:as2-nn4:1000:6554387		Pre-existing BGP session must be reset to apply the Prefix policy	
e.g. extended:as2-nn2:1000:65534 e.g. extended:is94-nn2:1.2.3.4:65515 e.g. extended:as2-nn4:1000:65505 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	Site of Origin:		
Local-AS Number Config: Image: Control Profile: Route Control Profile: Image: Control Profile: Image: Control Profile: Image: Control Profile: <th></th> <th>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</th> <th></th>		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: Image: This value must not match the MP-BGP RR policy Route Control Profile: Image: This value must not match the MP-BGP RR policy Image: Name Direction remove-communities Route Import Policy	Local-AS Number Config:	\sim	
Route Control Profile: Direction	Local-AS Number:	This value must not match the MP-BGP RR policy	
Name Direction remove-communities Route Import Policy	Route Control Profile:		
remove-communities Route Import Policy		 Name 	Direction
		remove-communities	Route Import Policy

Route Map is now added to BGP Peer Connectivity Profile

*For more information on route map configuration options in ACI, refer to the <u>ACI Fabric L3Out White</u> <u>Paper</u>

After implementing one of the above solutions, verify if the problem is solved.

Check the BGP status on 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

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 ***Notice that no 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 Check RIB on 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], 00:00:06, bgp-65001, internal, tag 65001 recursive next hop: 10.0.210.70/32%overlay-1 ***Notice that no rwVnid entry is present here.*** **Note:** The absence or presence of the rwVnid entry alone does not determine whether the issue is

occuring or not. In many cases, the rwVnid entry gets removed from the route in question once the issue is resolved. However, this is not always the case. Always check FIB and HAL tables in order to verify if the issue is resolved or not.

Check FIB on CL 102:

Prefix	(Next	-hop		Interface	/VRF	Ad	ditiona	l Info			
*192.1	168.20.0/2	24										
10.0.2	210.70											
	overlay	/-1										
***Not	ice that	we have t	he route	e here a	nd our ne	xt-hop a	ddress i	s corre	ct (showi	ng the T	EP IP of	BL 101,
Route Policy	Class-id: / Prefix @	0×0 0.0.0.0/0										
leaf-1 1	l02# acidi l01	ag fnvrea 1	d grep le	o 101 eaf-101	<out< td=""><td>put omit</td><td>ted></td><td></td><td></td><td></td><td></td><td></td></out<>	put omit	ted>					
10.0.2	210.70/32											
le	eaf	active	0									
HAL t	able on C	L 102:										
<#root	t>											
module 	e-1(DBG-e]	lam-insel6)# show	platfor	m interna	l hal 13	routes	grep	192.168.2	0.0		
4662												
192.	168.20.0/	24 UC	686	20601	TRIE	a5 5/	0 60a5	A	8443	86b6	ef5 1/	2
Not	ice that	we have a	n entry	here an	d it's in	the cor	rect VRF	'.				
module	e-1(DBG-e]	am-insel6)# hex									
4662												
0 ~												
UX 1236												
module	e-1(DBG-e]	lam-insel6)# show	platfor	m interna	l hal 13	vrf pi =======					
VrfId	Vrf Name	Hw VrfI	I I Vı d I S Vr	f nid	TOR - SB NB BDId BD	- - S Pro Id Ou	pine - xy ACI Bd Enc	 Lbl	Ing Msk	ACL Lbl	Egr Msk	
===== 26	example:	example										
1236												
0 0 21	10000 0	0 0	0	1	0	0	0	0	0			

Pings from EP (Host 1) to host in external network that comes from external BGP peer (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 on 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.

Related Information

- This behavior is also documented in this defect: Cisco bug ID <u>CSCvx28929</u>
- <u>Technical Support & Documentation Cisco Systems</u>