

عمدخلل ينايبل مسررل نيوكت نيوكت هنم ققحتلالو ASAv مادختساب 2 ةقبطلل

تايوتحمل

[عمدقمل](#)

[قيساسالابلطمل](#)

[تابلطمل](#)

[عمدختسمل تانوكمل](#)

[طخمل](#)

[هجاويف ينالليوتسمل نم عمدخلل ينايبل مسررل مادختساب مللي اذامل
\(ACI\) لوصولي ف مكحتل](#)

[L2 عمدخلل ينايبل مسررل نيوكت](#)

[ASA علىع L2 PBR رورم كرح نم ققحتل](#)

[ققولل علىع L2 PBR نم ققحتل](#)

[L2Ping لاصلتالابلخا لش ف قلاحي ف اهتيؤر متي تل اعاطل](#)

[L2 لاصلت تارابتخا طاقمل](#)

[DST على SRC ةياهن ةطقن نم رورمل كرح قفدت](#)

[ASA نيوكت](#)

عمدقمل

نم ققحتلالو عمدخلل 2 ةقبطلل ينايبل مسرر نيوكت نيوكت ةيفيكدنتسمل اذه فصي
Cisco Application Centric Infrastructure (ACI) في هتحص

قيساسالابلطمل

تابلطمل

ةيلال عيضاوملاب ةفرعم كيديل نوكت ناب Cisco ي صوت

- ةجمرب هجاويف ةثلاثل ةقبطلل نم عمدخلل ينايبل مسررل لمع ةيفيكد مهف
(ACI) تاقيبطلل
- هجاويف دقعلاو رسجل تاقاطنو ةياهنل ةطقن ةسايس ةومجم نيوكت ةيفيكد مهف
(ACI) لوصولي ف مكحتل
- ةيامح رادجك (يرهاظل فيكتلل لبالل نامال قيبطت) ASAv نيوكت ةيفيكد مهف
فافش

عمدختسمل تانوكمل

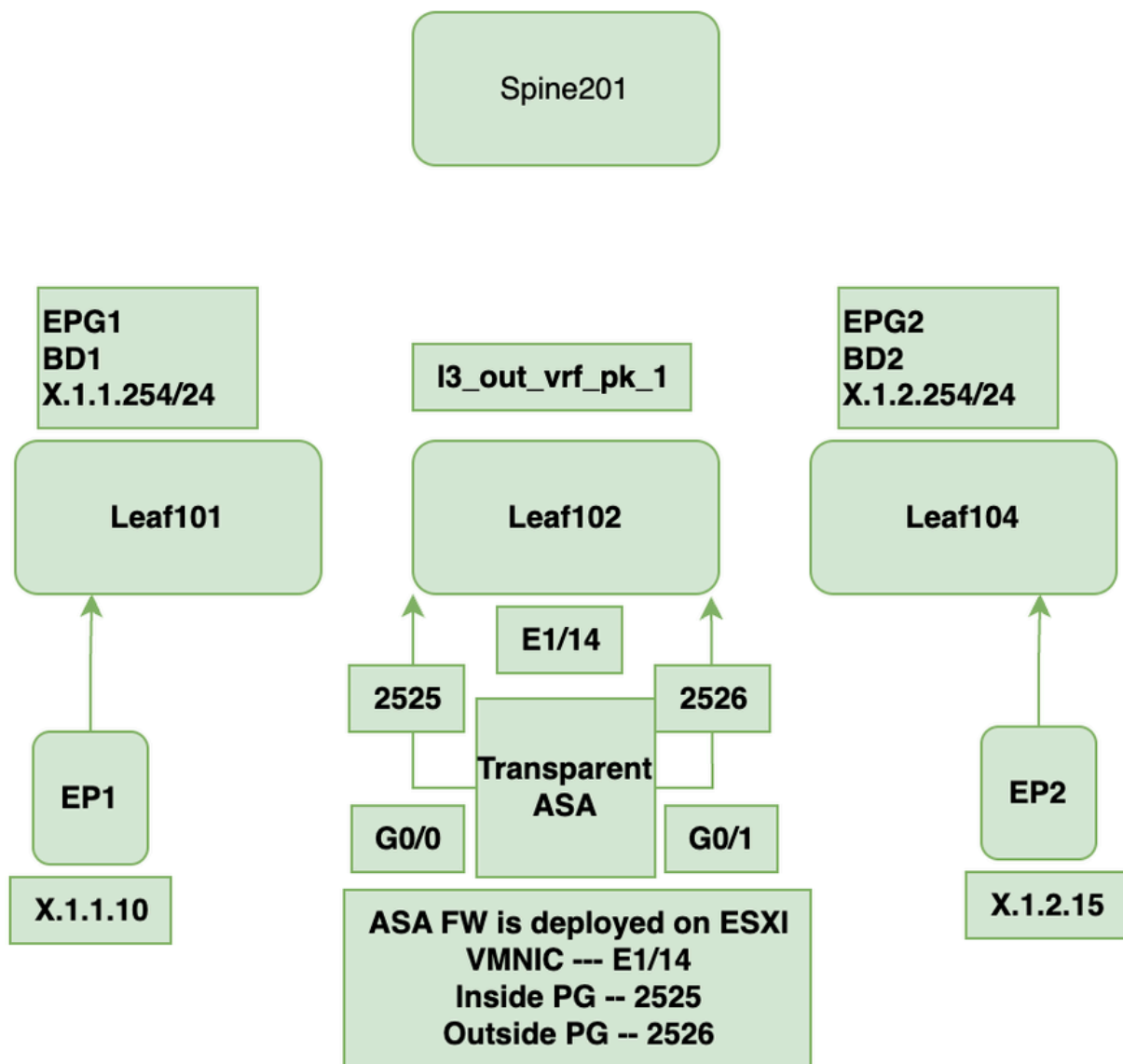
ةيلال ةيدامل تانوكمل او جماربل تارادصل على دنتسمل اذه في ةدراول تامولعمل دنتست

- APIC: 6.0 (3g) رادصل

- H/W: N9K-C93180YC-FX ةيفرطال ةدحول
- S/W: n9000-16.0 (3g) ةيفرطال ةدحول
- 101 و 102 و 103 قرولا ةدقع
- ASAي عل ع رشن

ةصاخ ةيلمعم ةئيبي ف ةدوجوملا ةزهجال نم دنتسملا اذه ي ف ةدراول تامولعمل عاشنإ مت تناك اذا. (يضايرتفا) حوسمم نيوكتب دنتسملا اذه ي ف ةمدختسملا ةزهجال عيمج تادب رما يال لمحتحمل ريثأتلل كمهف نم دكأتف ،ليغشتلا دي ق كتكبش

ططخمل



ططخمل

ةطقنو ديلا ملعت لبقي هنيوكتب بچيو ،دنتسملا اذه ي ف EPG1 و EPG2 نيوكتب ضرع متي ال ةياهنلا.

ةدقعل (اهيلع فرعتلا متي تال x.1.1.10 ةيلعفل EPG1 ةياهن ةطقن ءحص نم ققحتلا 1.

101).

لي م عمل ايهان طاقن

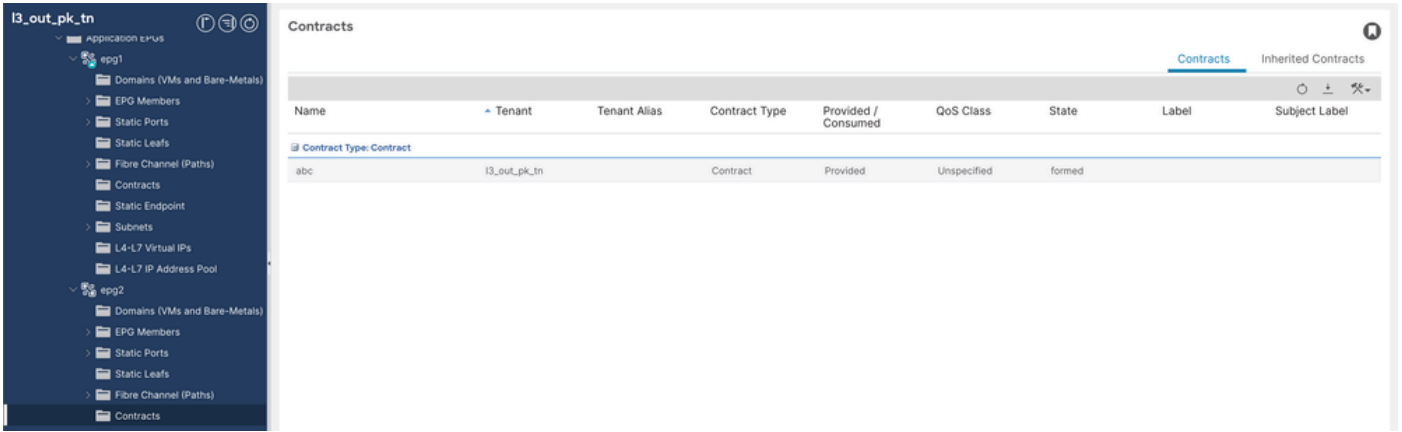
2. ABC دق عمل EPG1 كالهتس | متي .

كلهتس م عمل

3. (104 دق عمل) م عمل ال مت X.1.2.15 ايهان طاقن ي و تحي EPG2 حص نم ققحت ال .

لي م عمل ايهان طاقن

4. EPG2 طساوب دق عمل ABC ري فوت متي .



The screenshot shows the Cisco ACI GUI. On the left is a navigation tree with a highlighted path: Application > epg1 > Domains (VMs and Bare-Metals) > Contracts. The main panel is titled 'Contracts' and has two tabs: 'Contracts' (active) and 'Inherited Contracts'. Below the tabs is a table with the following columns: Name, Tenant, Tenant Alias, Contract Type, Provided / Consumed, QoS Class, State, Label, and Subject Label. A single contract is listed with the name 'abc', tenant 'I3_out_pk_tn', type 'Contract', and state 'formed'.

Name	Tenant	Tenant Alias	Contract Type	Provided / Consumed	QoS Class	State	Label	Subject Label
abc	I3_out_pk_tn		Contract	Provided	Unspecified	formed		

مدقم ال دقعل

يوتسم ال نم ةمدخلل ينابل مسرل مادختسا مزلي اذامل (ACI) لوصول في مكحتل ةهجاو في ينال

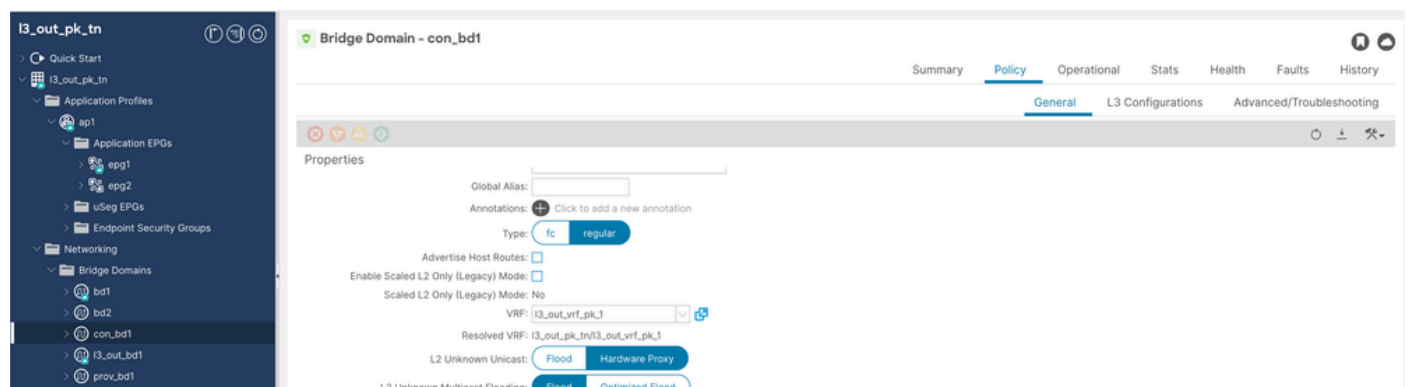
- وأ (L2) ةقبطال، 3 (L3) ةقبطال في L4-L7 ةمدخ ةزهجأ جاردإ نكمي، Cisco ACI في (L1) ةقبطال.
- ةيامل رادج، لاثمل ليبس ىلع) يجرال زاهج موقى: ثلثال يوتسم ال نم ةمدخل لاخدا
تانابل رورم ةكرح هيجوت ةداعإو هيجوتل تارارق ذاختاب (IPS) للستل عنم ماضنو
IP. نيوانع ىلإ ادانتسا
- نيوانع ىلإ ادانتسا رورم ال ةكرح هيجوت ةداعإ متت: ينال يوتسم ال نم ةمدخل لاخدا
IPS. ةزهجأ وأ ةفافشل ةيامل ناردجل اديفم اذه نوكيو. هيجوت ةكراشم نود MAC
- زاهج لاخدا دنع ينال يوتسم ال نم (PBR) ةسايس ىلإ دنتسم ال هيجوتل مادختسا متي
مكحتل ةمئاق في فافش ةيامل رادج وأ IPS لوكتورب لثم، ينال يوتسم ال نم ةمدخ
(ACI) لوصول في
- L2 و L3 نم لكل اهسفن يه رورم ال ةكرح هيجوت ةداعإ ةيلا لظت.
- يسيئرل قرافل:
 - L3 PBR: (هيجوتل في زاهج لكراشي) IP ناونع ىلإ رورم ال ةكرح هيجوت ةداعإ متت
 - L2 PBR: (2) ةقبطال في زاهج لمعي) MAC ناونع ىلإ رورم ال ةكرح هيجوت ةداعإ متت
- ةداعإ نامضل ةيفرطل تاهجاوالب تابث لكشب MAC نيوانع طبر متي، L2 PBR في
ةبسانم رورم ال ةكرح هيجوت

طشنل/طشنل وأ طشنل/لوال يوتسم ال نم PBR مادختسا تالاج لوح تامولعمل نم ديزمل
PBR ل يمسرل ريرقتل عجار، L1/L2

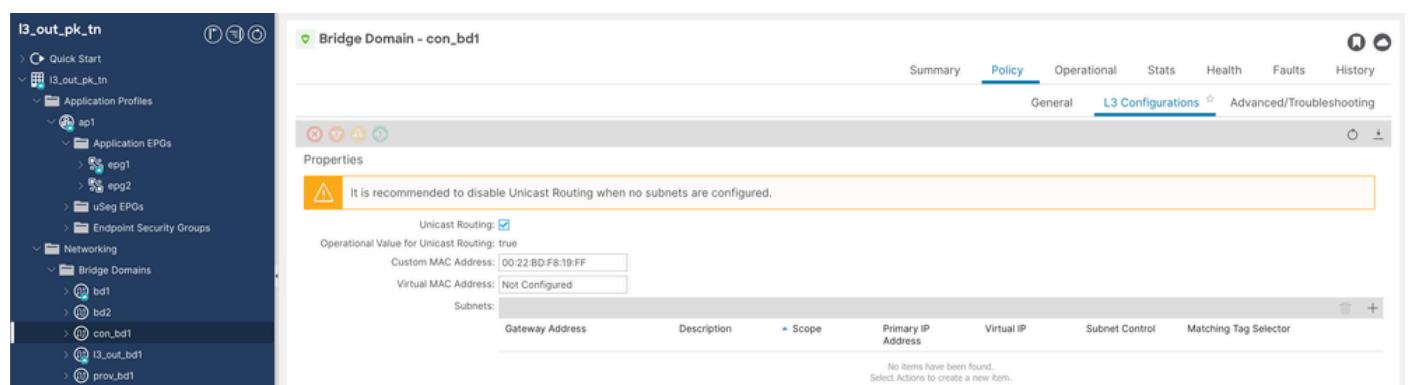
L2 ةمدخل ينابل مسرل نيوكت

con-bd1 ك نيغي bd كلهتسم لكشي. 1 ةوطخ

يُعدّ 2 من صيغ التسمية نم فورعمل ريغ يداخال ثبلا نيي عت بجي ،يداخال ثبلا هي جوت ني كمت بجي
 (BDs) Bridge (BDs) و con تالاجمل ةي عرف ةكبش دوجو مزلي الو ةزهال ليو

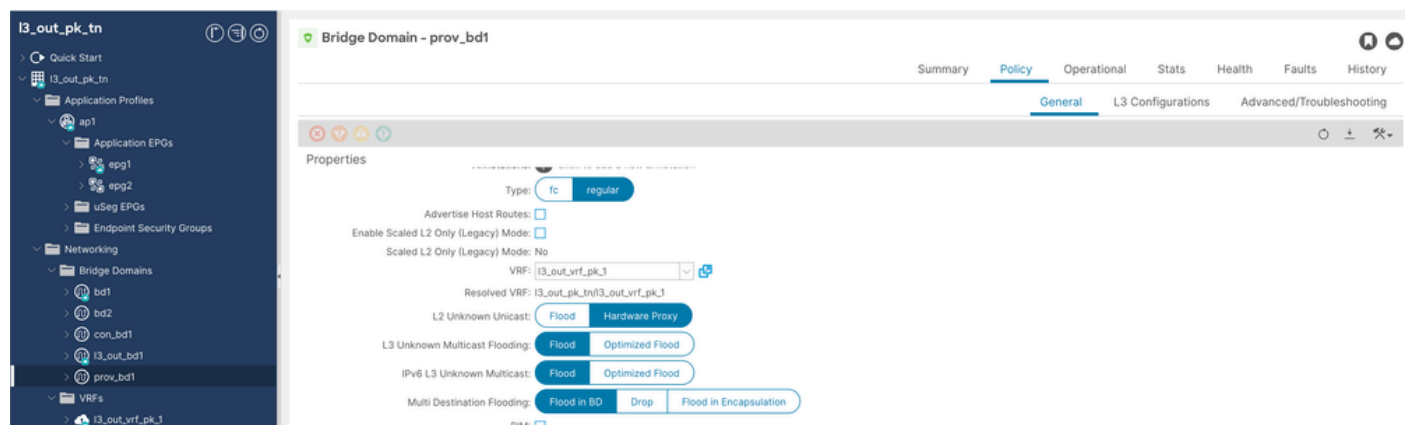


CONS BD نيوكت

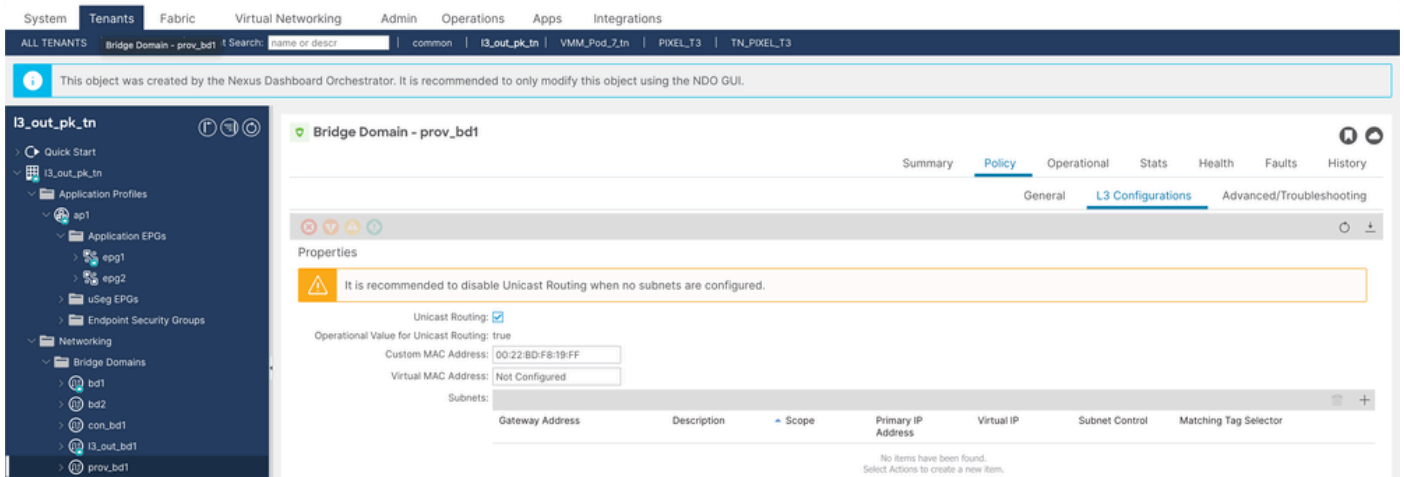


Cons BD ل 2 نيوكتال

prov-bd1. ك يمسمال رفومال نيوكتب مق 2. ةوطخل



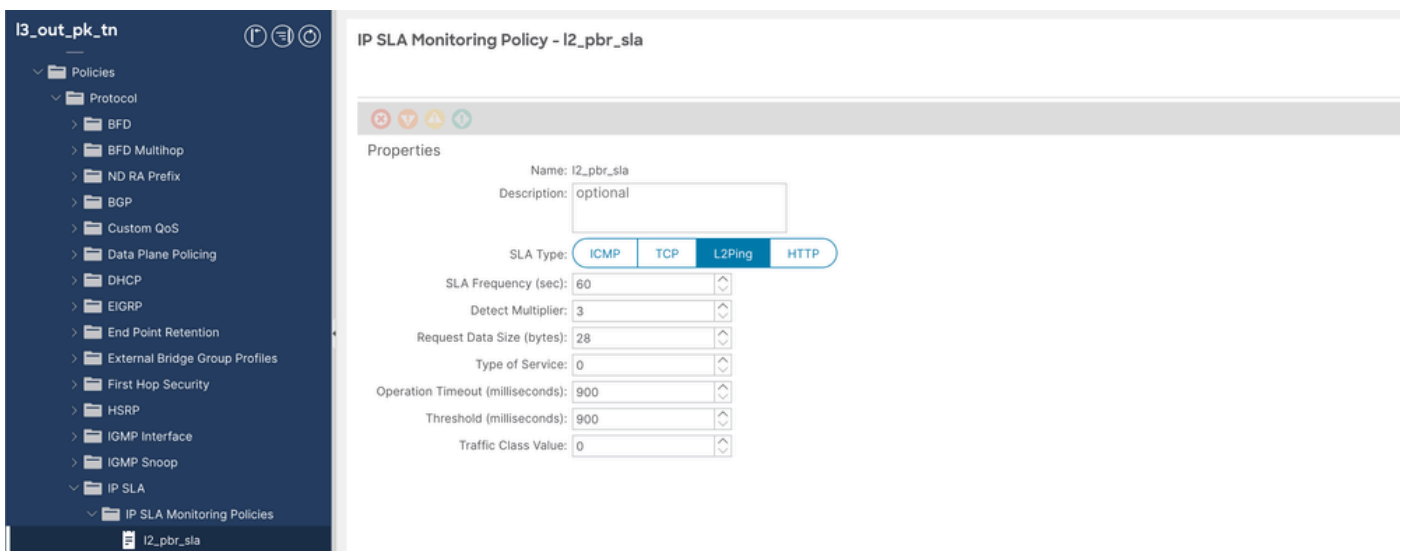
Prov BD نيوكت



PROV BD ل 2 نيوكتال

SLA L2Ping عون مادختساب IP (SLA) ممدخ يوتسم ةيقافاتإ ةسايس نيوكت 3. ةوطخل

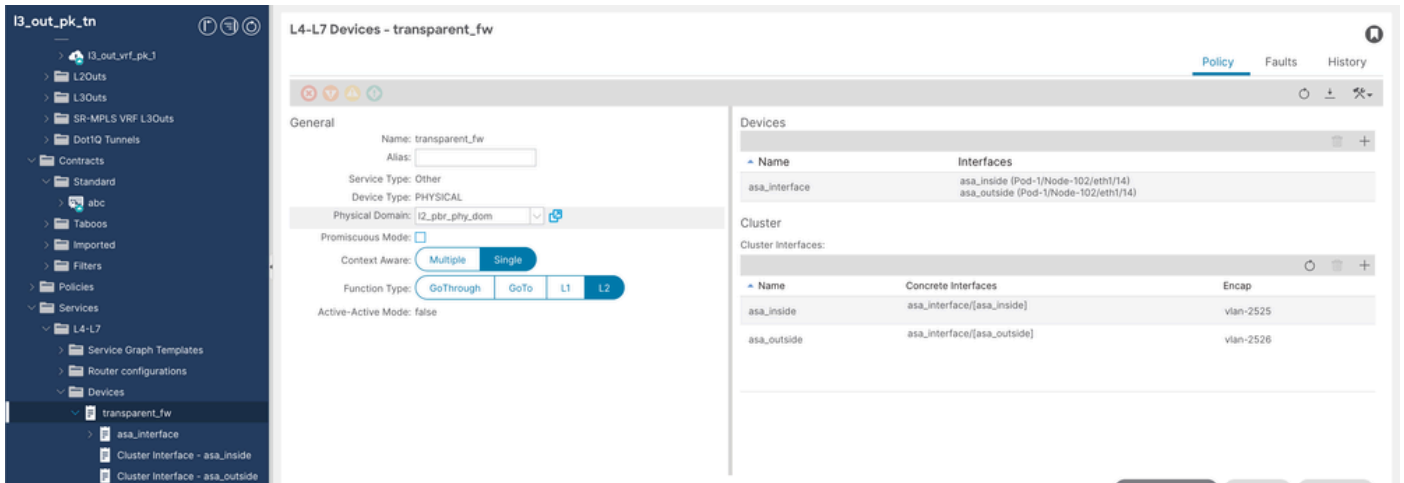
رقنا م، IP SLA ةبقارم تاسايس > IP SLA > لوكوتورب > تاسايس > رجأتسمال ال لقتنا ةسايس عاشنإ قوف نميال سوامال رزب.



IP SLA ةسايس

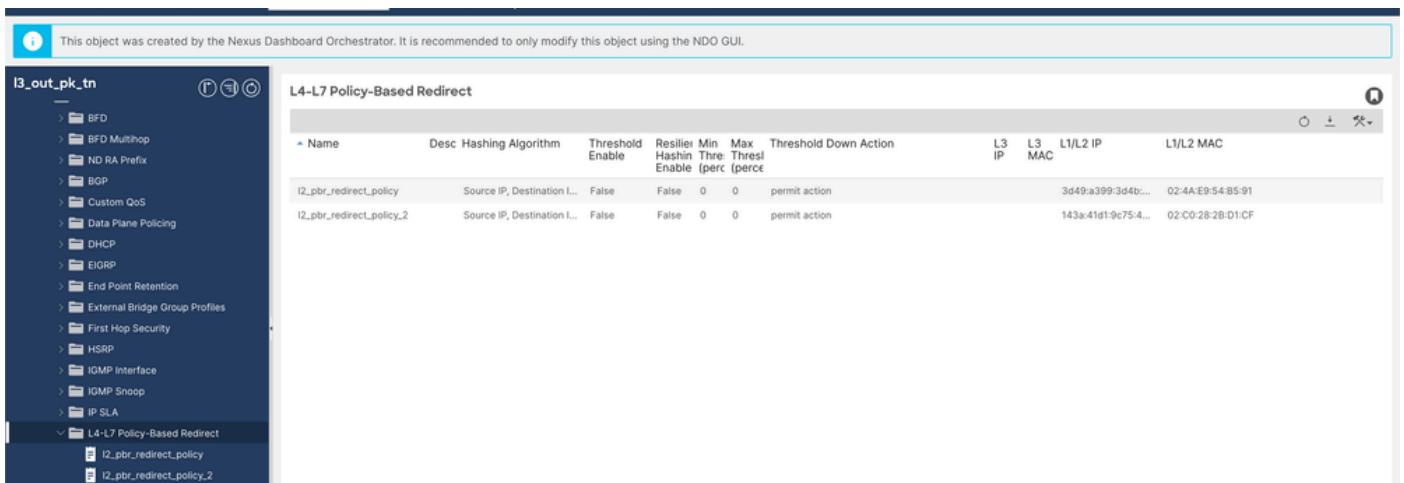
L4/L7 زاخ نيوكت 4. ةوطخل

مقو L4-L7 زاخ قوف نميال سوامال رزب رقنا م، ةزهجال > تامدخال > رجأتسمال ال لقتنا ةسايس عاشنإ.



زاهج L4-L7

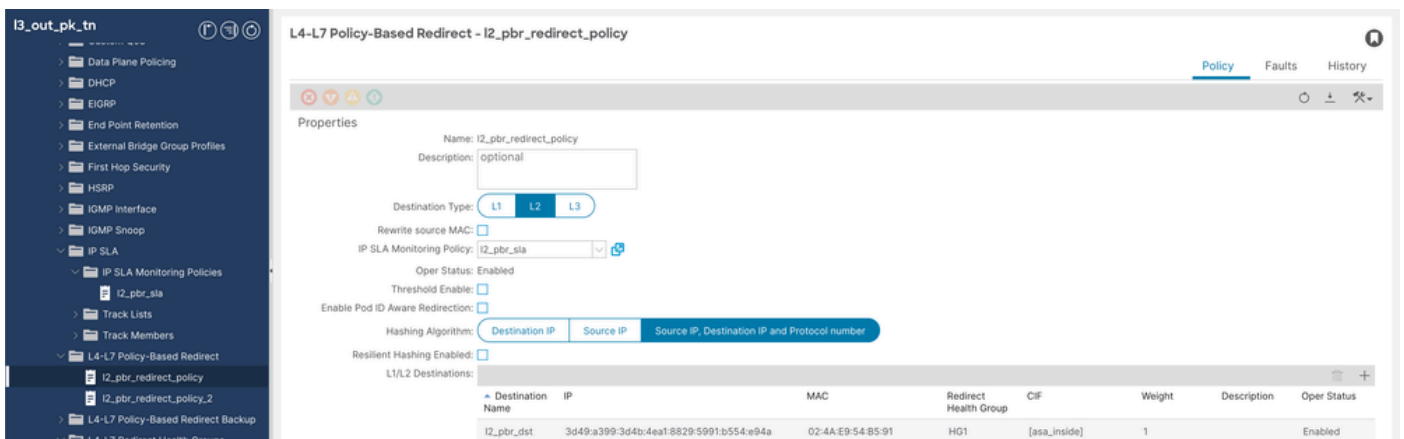
لكنكمي) ةسايسلا لىإ ةدنتسملا هيحوتلا ةداعإ لىل ةماع ةرطن نم ققحتلا 5. ةوطخل (5a و 5b) نيوكت دعب اذه نم ققحتلا.



4-L7 ىوتسملا هيحوت ةداعإ ةسايس

نامأل ةزهجأل L4-L7 ةسايس لىإ ةدنتسملا هيحوتلا ةداعإ ةسايس نيوكت 5.1. ةوطخل (هسفن APIC ةطساوب اهؤلم متي، IP وأ MAC ديدحت لىإ ةجاج ال) ةهجاو لاخاد (ASA) ةلدعمل

مث، L4-L7 ةسايس لىل ةمئاق هيحوت ةداعإ > لوكوتورب > تاسايس > رجأتسم لىإ لقنتنا ةسايس عاشن قوف نميأل سواملا رزب رقنا.



L7-4 يوتسمال هيچوت ةداع| ةسايس نيوكت

هيچراخل ASA ةهجاول L4-L7 ةسايس ىلإ ةدنتسمال هيچوتال ةداع| ةسايس نيوكت 5.2 ةوطخلال (هسفن APIC ةطساوب اهؤلم متي، IP وأ MAC ديحت ىلإ ةجاج ال).

م، L4-L7 ةسايس ىلإ ةمئاق هيچوت ةداع| > لوكوتورب > تاسايس > رجأتسم ىلإ لقتنا ةسايس عاشنإ قوف نميال سوامال رزب رقنا

The screenshot shows the ASA configuration interface for the L4-L7 Policy-Based Redirect configuration. The left sidebar shows the configuration tree with the following structure:

- l3_out_pk_tn
 - Data Plane Policing
 - DHCP
 - EIGRP
 - End Point Retention
 - External Bridge Group Profiles
 - First Hop Security
 - HSRP
 - IGMP Interface
 - IGMP Snoop
 - IP SLA
 - IP SLA Monitoring Policies
 - l2_pbr_sta
 - Track Lists
 - Track Members
 - L4-L7 Policy-Based Redirect
 - l2_pbr_redirect_policy
 - l2_pbr_redirect_policy_2
 - L4-L7 Policy-Based Redirect Backup
 - L4-L7 Redirect Health Groups

The main configuration area shows the L4-L7 Policy-Based Redirect - l2_pbr_redirect_policy_2 configuration. The Properties section includes:

- Name: l2_pbr_redirect_policy_2
- Description: optional
- Destination Type: L1, L2, L3 (L2 is selected)
- Rewrite source MAC: ☐
- IP SLA Monitoring Policy: l2_pbr_sta
- Oper Status: Enabled
- Threshold Enable: ☐
- Enable Pod ID Aware Redirection: ☐
- Hashing Algorithm: Destination IP, Source IP, Source IP, Destination IP and Protocol number
- Resilient Hashing Enabled: ☐
- L1/L2 Destinations:

Destination Name	IP	MAC	Redirect Health Group	CIF	Weight	Description	Oper Status
l2_pbr_dst_o...	143a:41d1:9c75:4973:8501:bcd:d1b:28c0	02:C0:28:2B:D1:CF	H02	[asa_outside]	1		Enabled

L7 2-4 يوتسمال هيچوت ةداع| ةسايس نيوكت

ةمدخلل ينايبل مسرلل بلال نيوكت 6. ةوطخلال

نميال سوامال رزب رقنا م، ةمدخلل ينايبل مسرلل بلال > تامدخ > رجأتسم ىلإ لقتنا ئشنأو L4-L7 ةمدخلل ينايبل مسرلل بلال قوف

The screenshot shows the ASA configuration interface for the L4-L7 Service Graph Template configuration. The left sidebar shows the configuration tree with the following structure:

- l3_out_pk_tn
 - l3_out_vrf_pk_l
 - L2Outs
 - L3Outs
 - SR-MPLS VRF L3Outs
 - Dot1Q Tunnels
 - Contracts
 - Standard
 - abc
 - Taboos
 - Imported
 - Filters
 - Policies
 - Services
 - L4-L7
 - Service Graph Templates
 - transparent_fw
 - Function Node - N1
 - consumer
 - provider

The main configuration area shows the L4-L7 Service Graph Template - transparent_fw configuration. The Topology section includes:

- Consumer (EPG) connected to Provider (EPG) via a central node labeled N1 (transparent_fw).
- transparent_fw Information: Route Redirect: true

ةمدخلل ينايبل مسرلل نيوكت

زاهجل ديحت جهن نيوكت 7. ةوطخلال

ديحت جهن قوف نميال سوامال رزب رقنا م، زاهجل ديحت جهن > تامدخ > رجأتسم ىلإ لقتنا هئاشنأب مقو زاهجل

This object was created by the Nexus Dashboard Orchestrator. It is recommended to only modify this object using the NDO GUI.

l3_out_pk_tn

- Services
 - L4-L7
 - Service Graph Templates
 - transparent_fw
 - Function Node - N1
 - consumer
 - provider
 - Router configurations
 - Devices
 - transparent_fw
 - asa_interface
 - Cluster Interface - asa_inside
 - Cluster Interface - asa_outside
 - Imported Devices
 - Devices Selection Policies
 - abc-transparent_fw-N1
 - consumer
 - provider

Logical Device Context - abc-transparent_fw-N1

Policy Faults History

Properties

Contract Name: abc
Graph Name: transparent_fw
Node Name: N1
Alias:
Context Name:
Devices: transparent_fw
Router Config: select a value

2 مەدخلل يىنايىل م س ر ل نى و ك ت

كلەت س م ل ل ە ي ق ط ن م ل ە ە ج اول ق ا ي س ++

l3_out_pk_tn

- Services
 - L4-L7
 - Service Graph Templates
 - transparent_fw
 - Function Node - N1
 - consumer
 - provider
 - Router configurations
 - Devices
 - transparent_fw
 - asa_interface
 - Cluster Interface - asa_inside
 - Cluster Interface - asa_outside
 - Imported Devices
 - Devices Selection Policies
 - abc-transparent_fw-N1
 - consumer
 - provider

Logical Interface Context - consumer

Policy Faults History

Properties

Connector Name: consumer
Cluster Interface: asa_inside
Associated Network: Bridge Domain L3Out
Bridge Domain: con_bd1
Preferred Contract Group: Exclude
Permit Logging: ☐
L3 Destination (VIP): ☒
L4-L7 Policy-Based Redirect: i2_pbr_redirect_policy
L4-L7 Service EPG Policy: select an option
Custom QoS Policy: select a value
Subnets:

IP/Mask	Scope	Preferred	Subnet Control	Anycast MAC
No items have been found. Select Actions to create a new item.				

زاجال دى د ح ت ج ه ن ل كلەت س م ل نى و ك ت

++ ر ف و م ل ل ە ي ق ط ن م ل ە ە ج اول ق ا ي س

l3_out_pk_tn

- Services
 - L4-L7
 - Service Graph Templates
 - transparent_fw
 - Function Node - N1
 - consumer
 - provider
 - Router configurations
 - Devices
 - transparent_fw
 - asa_interface
 - Cluster Interface - asa_inside
 - Cluster Interface - asa_outside
 - Imported Devices
 - Devices Selection Policies
 - abc-transparent_fw-N1
 - consumer
 - provider

Logical Interface Context - provider

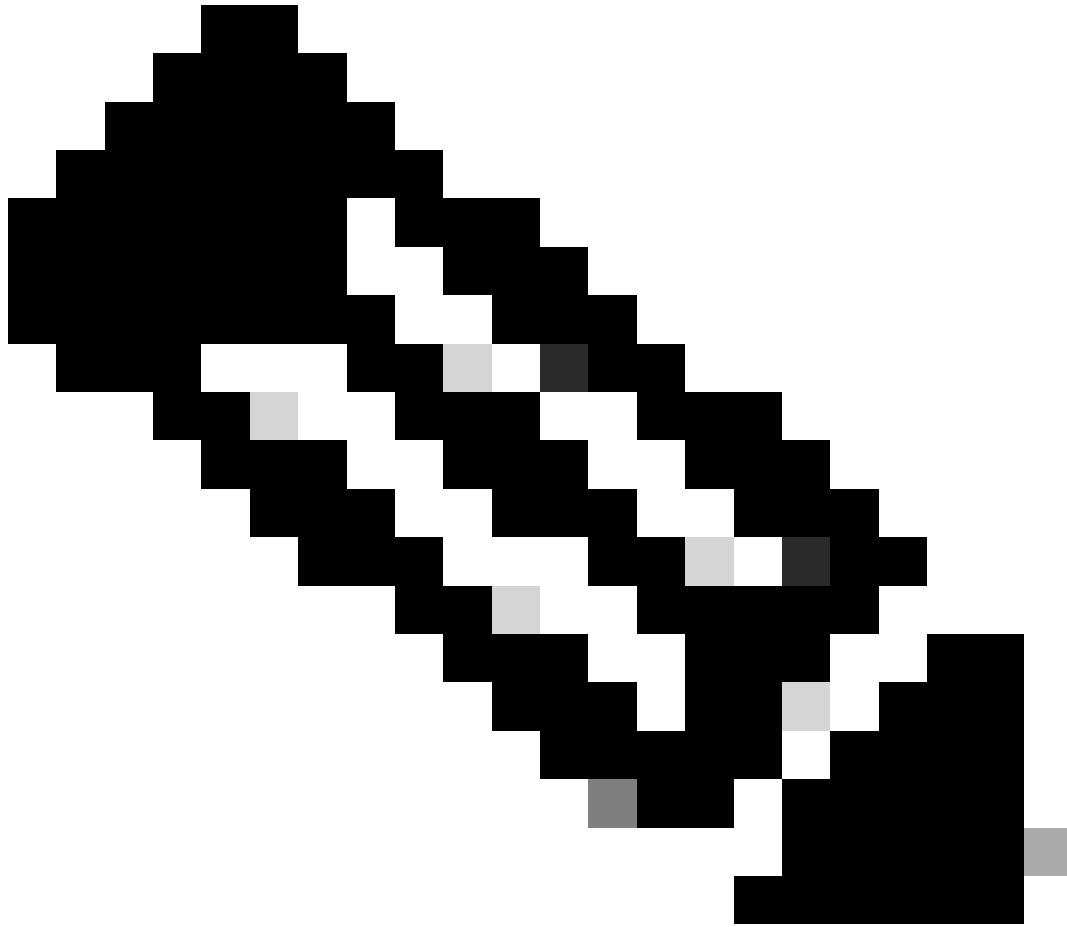
Policy Faults History

Properties

Connector Name: provider
Cluster Interface: asa_outside
Associated Network: Bridge Domain L3Out
Bridge Domain: prov_bd1
Preferred Contract Group: Exclude
Permit Logging: ☐
L3 Destination (VIP): ☒
L4-L7 Policy-Based Redirect: i2_pbr_redirect_policy_2
L4-L7 Service EPG Policy: select an option
Custom QoS Policy: select a value
Subnets:

IP/Mask	Scope	Preferred	Subnet Control	Anycast MAC
No items have been found. Select Actions to create a new item.				

زاجال دى د ح ت ج ه ن ر ف و م نى و ك ت



رايخ مادختسا ةلاح يف ايئاقلت هؤاشنا متيس ناك اذا زاهجال ديدحت جهن :ةظحال م
ةمدخلل ينايبل مسرلا قيبطت

abc. عوضوم ىلع دقاعتلا لجأ نم PBR قيبطت ب مق. 8 ةوطخل

L4-L7 Service Graph > transparent_fw > دقعل عوضوم > دق ع > رجأتسم ىلا لقتنا

نوك

دقعة نيوك

روشنم لاي ثمل يني بال مسرلا تحت ةحصل نم ققحت ،حاج نب رشنل مت اذا 9. ةوطخل (ةلحال نع ثحبا).

The screenshot shows a network management interface. On the left is a sidebar menu with a tree structure under 'I3_out_pk_tn'. It includes 'Endpoint Tags', 'Services', 'L4-L7', 'Service Graph Templates', 'transparent_fw', 'Function Node - N1', 'Router configurations', 'Devices', 'Imported Devices', 'Devices Selection Policies', and 'Deployed Graph Instances'. The main panel is titled 'Deployed Graph Instances' and contains a table with the following data:

Service Graph	Contract	Contained By	State	Description
transparent_fw	abc	Private Networ...	applied	

ةمدخلل يني بال مسرلا ةحص نم ققحتلا

تافرعمو ةجمدمل (VLANs) ةيره اطل ةيلحلم تاكبشلاو ةومجمل ماظن تاهاجو نم ققحتلا ++ فئاطولا لصوم تائف

The screenshot shows the 'Function Node - N1' configuration page. The left sidebar is the same as the previous screenshot. The main panel shows the configuration for 'Function Node - N1'. It includes tabs for 'Policy', 'Faults', and 'History'. The 'Policy' tab is active, showing 'Properties' and 'Function Connectors'.

Properties:

- Name: N1
- Function Type: L2
- Devices: transparent_fw

Cluster Interfaces:

Name	Concrete Interfaces	Encap
asa_inside	asa_interface[asa_inside]	vlan-2525
asa_outside	asa_interface[asa_outside]	vlan-2526

Function Connectors:

Name	Encap	Class ID	L3OutPBR Service pcTag
consumer	vlan-2525	49158	any
provider	vlan-2526	32774	any

2 ةمدخلل يني بال مسرلا ةحص نم ققحتلا

ASA ىلع L2 PBR رورم ةكرح نم ققحتلا

يف اهتيؤر كنكم يتي ال ةدحمل ةياهنل ةطقن ىلإ Src ةياهن ةطقن نم (SSH) نامأل ةقبط ASA ىلع ىوتحمل لودج لاخدا

The screenshot shows a terminal window with the following content:

```
ASA(config)# show conn
1 in use, 3 most used

TCP outside .1.2.15:22 inside 152.1.1.10:58755,
lags 1110

--- 1.2.15 ping statistics ---
1000 packets transmitted, 997 packets received, 0.30% packet loss
round-trip min/avg/max = 0.842/1.118/2.625 ms
bgl-aci07-switch1# ssh .1.2.15 vrf rogue1
User Access Verification
Password:
```

ASA ةحص نم ققحتلا

ةقرولا ىلع L2 PBR نم ققحتلا

1. 102 قرولا ةدقع ىلع (VLAN) ةيره اظلا ةيلحملا ةكبشل ربق ةجم ربل.

```
<#root>

PBR vlan 2525 and 2526 will get programmed on leaf node 102 and mac addresses will be statically tied to
the leaf node.

bgl-aci07-apic100#

fabric 102 show endpoint

-----
Node 102 (bgl-aci07-leaf2)
-----
Legend:
S - static          s - arp          L - local          O - peer-attached
V - vpc-attached   a - local-aged    p - peer-aged      M - span
B - bounce         H - vtep         R - peer-attached-r1 D - bounce-to-proxy
E - shared-service m - svc-mgr

+-----+-----+-----+-----+-----+
| VLAN/ | Encap | MAC Address | MAC Info/ | Interface |
| Domain | VLAN | IP Address | IP Info | |
+-----+-----+-----+-----+-----+
| 28/13_out_pk_tn:13_out_vrf_pk_1 | vlan-2525 | 024a.e954.b591 | LS | eth1/14 |
| 1/13_out_pk_tn:13_out_vrf_pk_1 | vlan-2526 | 02c0.282b.d1cf | LS | eth1/14 |
+-----+-----+-----+-----+-----+
```

2. (104) دوزملاو (101) لك لهت سمل ةدقع ىلع قطانملا ميسقت ةدعاقو ةسايسلا هيحوت ةداع|.

```
<#root>

++ Redirect policy on consumer node

bgl-aci07-apic100#

fabric 101 show service redir info

-----
Node 101 (bgl-aci07-leaf1)
-----
=====
LEGEND
TL: Threshold(Low) | TH: Threshold(High) | HP: HashProfile | HG: HealthGrp | BAC: Backup-Dest |
=====
List of Dest Groups
GrpID Name          destination                                     HG-name
=====
7      destgrp-7        dest-[3d49:a399:3d4b:4ea1:8829:5991:b554:e94a]-[vlan-2228224] 13_out_pk_tn::HG1
8      destgrp-8        dest-[143a:41d1:9c75:4973:8501:bcf:d12b:28c0]-[vlan-2228224] 13_out_pk_tn::HG2

List of destinations
Name                                     bdVnid          vMac          vrf
=====
dest-[3d49:a399:3d4b:4ea1:8829:5991:b554:e94a]-[vlan-2228224] vxlan-16744328 02:4A:E9:54:B5:91 13_
```

dest-[143a:41d1:9c75:4973:8501:bcf:d12b:28c0]-[vlan-2228224] vlan-16056296 02:C0:28:2B:D1:CF 13_

List of Health Groups

HG-Name	HG-OperSt	HG-Dest
=====	=====	=====
13_out_pk_tn::HG1	enabled	dest-[3d49:a399:3d4b:4ea1:8829:5991:b554:e94a]-[v
13_out_pk_tn::HG2	enabled	dest-[143a:41d1:9c75:4973:8501:bcf:d12b:28c0]-[vx

List of Backup Destinations

Name	primaryDestName
=====	=====

List of AclRules

AclRuleVnid	DestGroup	OperSt	OperStQual
=====	=====	=====	=====

++ Zoning rule on consumer Node

bgl-aci07-apic100#

fabric 101 show zoning-rule | grep redir

	4228		32771		49157		default		bi-dir		enabled		2228224	
	4231		49157		32771		default		uni-dir-ignore		enabled		2228224	
	4230		32771		15		default		uni-dir		enabled		2228224	
	4229		16386		32771		default		uni-dir		enabled		2228224	

<#root>

++ Redirect Policy on Provider Node

bgl-aci07-apic100#

fabric 104 show service redir info

Node 104 (bgl-aci07-leaf4)

LEGEND

TL: Threshold(Low) | TH: Threshold(High) | HP: HashProfile | HG: HealthGrp | BAC: Backup-Dest |

List of Dest Groups

GrpID	Name	destination	HG-name
=====	=====	=====	=====
3	destgrp-3	dest-[3d49:a399:3d4b:4ea1:8829:5991:b554:e94a]-[vlan-2228224]	13_out_pk_tn::HG1
4	destgrp-4	dest-[143a:41d1:9c75:4973:8501:bcf:d12b:28c0]-[vlan-2228224]	13_out_pk_tn::HG2

List of destinations

Name	bdVnid	vMac	vrf
=====	=====	=====	=====
dest-[3d49:a399:3d4b:4ea1:8829:5991:b554:e94a]-[vlan-2228224]	vlan-16744328	02:4A:E9:54:B5:91	13_
dest-[143a:41d1:9c75:4973:8501:bcf:d12b:28c0]-[vlan-2228224]	vlan-16056296	02:C0:28:2B:D1:CF	13_

List of Health Groups

HG-Name	HG-OperSt	HG-Dest
=====	=====	=====
13_out_pk_tn::HG1	enabled	dest-[3d49:a399:3d4b:4ea1:8829:5991:b554:e94a]-[v
13_out_pk_tn::HG2	enabled	dest-[143a:41d1:9c75:4973:8501:bcf:d12b:28c0]-[vx

List of Backup Destinations

Name	primaryDestName
=====	=====

```
++ Zoning rule on provider node
bgl-aci07-apid100#
```

```
fabric 104 show zoning-rule | grep redir
```

	4220		32771		49157		default		bi-dir		enabled		2228224	
	4221		49157		32771		default		uni-dir-ignore		enabled		2228224	

لاصتالارابتخإلشف ةلاح في اهتيرؤرمت يتالاعاطخالال L2Ping

ةلاح في لازي ال PBR نأ طحالالتس PBR، زاهج ربع L2Pings لاصتالارابتخإلشف ةلاح في ةومجم/عبتت دوجوإلرشت اهتيرؤرمت يتال F2911 و F2833 و F4203 اعاطخالال نأ ورشنال ةلطم ةيحص.

L2 لاصتالارابتخإلطاقال

إذا ام ةفرعمل رورمل اةجاوإل tcpdump ماذتساب L2Pings لاصتالارابتخإلطاقال كنكمي (CPU) ةيزكرم الةلعمل اةحوالاسرا طقف تيأراذا. حيحص لكشب اهلابلقتساواهلالاسرا مت فاشكتسأ كيلع بجيواقبسم ةروكذمل اعاطخالال ثودح عقوتمال نمف، ةملتسم ريغو ةلسرم (ASA نيوكت مسق إل عجرا) اهطاقساإ بابس ل رثكأ اهلالصإو ASA اعاطخإ.

<#root>

Capturing L2Pings using tcpdump on PBR Node 102

```
bgl-aci07-leaf2#
```

```
tcpdump -i tahoe0 -w /data/techsupport/l2_pbr1.pcap
```

```
tcpdump: listening on tahoe0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C4858 packets captured
4875 packets received by filter
0 packets dropped by kernel
```

In order to deocde the tcpdump

```
cat /data/techsupport/l2_pbr1.pcap | knet_parser.py --decode tahoe --pcap | less
```

```
** Search for mac 00ab.8752.3100
```

```
++ CPU transmit packets
```

```
Frame 505
```

```
Time: 2024-10-29T05:55:28.707136+00:00
```

```
Header: ieth
```

CPU Transmit

sup_tx:1, ttl_bypass:0, opcode:0x0, bd:0x207, outer_bd:0x0, dl:0, span:0, traceroute:0, tclass:5
src_idx:0x0, src_chip:0x0, src_port:0x0, src_is_tunnel:0, src_is_peer:0
dst_idx:0x0, dst_chip:0x0, dst_port:0x0, dst_is_tunnel:0
Len: 72
Eth:

00ab.8752.3100 > 024a.e954.b591

, len/

ethertype:0x721

Frame 506

Time: 2024-10-29T05:55:28.707297+00:00

Header: ieth CPU Transmit

sup_tx:1, ttl_bypass:0, opcode:0x0, bd:0x208, outer_bd:0x0, dl:0, span:0, traceroute:0, tclass:5
src_idx:0x0, src_chip:0x0, src_port:0x0, src_is_tunnel:0, src_is_peer:0
dst_idx:0x0, dst_chip:0x0, dst_port:0x0, dst_is_tunnel:0
Len: 72
Eth:

00ab.8752.3100 > 02c0.282b.d1cf

, len/

ethertype:0x721

++CPU recived packets

Frame 509

Time: 2024-10-10T20:16:37.580855+00:00

Header: ieth_extn

CPU Receive

sup_qnum:0x33, sup_code:0x4d, istack:

ISTACK_SUP_CODE_PBR_TRACK_REFRESH

(0x4d)

Header: ieth

sup_tx:0, ttl_bypass:0, opcode:0x0, bd:0x209, outer_bd:0x2, dl:0, span:0, traceroute:0, tclass:0
src_idx:0x32, src_chip:0x0, src_port:0x6, src_is_tunnel:0, src_is_peer:0
dst_idx:0x1, dst_chip:0x0, dst_port:0x3d, dst_is_tunnel:0
Len: 76
Eth:

00ab.8752.3100 > 024a.e954.b591

, len/ethertype:0x8100(802.1q)

802.1q:

vlan:2526

, cos:0, len/

ethertype:0x721

Frame 510

Time: 2024-10-10T20:16:37.580891+00:00

Header: ieth_extn

CPU Receive

sup_qnum:0x33, sup_code:0x4d, istack:

ISTACK_SUP_CODE_PBR_TRACK_REFRESH(0x4d)

Header: ieth

sup_tx:0, ttl_bypass:0, opcode:0x0, bd:0x20a, outer_bd:0x2, dl:0, span:0, traceroute:0, tclass:0

src_idx:0x32, src_chip:0x0, src_port:0x6, src_is_tunnel:0, src_is_peer:0

dst_idx:0x1, dst_chip:0x0, dst_port:0x3d, dst_is_tunnel:0

Len: 76

Eth:

00ab.8752.3100 > 02c0.282b.d1cf

, len/ethertype:0x8100(802.1q)

802.1q:

vlan:2525

, cos:0, len/

ethertype:0x721

DST إلى SRC ةياهن ةطقن نم رورملا ةكرح قفدت

<#root>

++ Endpoint X.1.1.10 want to send traffic to X.1.2.15

++ If destination is not learned on consumer/source leaf, PBR will be performed on destination leaf

++ For this case we are assuming endpoint X.1.2.15 is learned on Leaf 101 so PBR/Redirection will be performed

bgl-aci07-apic100#

fabric 101 show endpoint

Node 101 (bgl-aci07-leaf1)

Legend:

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

VLAN/ Domain	Encap VLAN	MAC Address IP Address	MAC Info/ IP Info	Interface
13_out_pk_tn:13_out_vrf_pk_1		X.1.2.15		tunnel6 ==>
17	vlan-3516	10b3.d514.3516 L		eth1/5 ==>
13_out_pk_tn:13_out_vrf_pk_1	vlan-3516	X.1.1.10 L		eth1/5

++ EPM entry to get the PC TAG

bgl-aci07-apic100#

fabric 101 show system internal epm endpoint ip X.1.1.10

Node 101 (bgl-aci07-leaf1)

MAC : 10b3.d514.3516 ::: Num IPs : 1
IP# 0 : X.1.1.10 ::: IP# 0 flags : ::: l3-sw-hit: No
Vlan id : 17 ::: Vlan vnid : 11792 ::: VRF name : l3_out_pk_tn:l3_out_vrf_pk_1
BD vnid : 16744307 ::: VRF vnid : 2228224
Phy If : 0x1a004000 ::: Tunnel If : 0
Interface : Ethernet1/5
Flags : 0x80005c04 ::: sclass :

32771

::: Ref count : 5 ==> sclass
EP Create Timestamp : 10/11/2024 09:15:44.430334
EP Update Timestamp : 10/29/2024 10:45:35.458416
EP Flags : local|IP|MAC|host-tracked|sclass|timer|

bgl-aci07-apic100#

fabric 101 show system internal epm endpoint ip X.1.2.15

Node 101 (bgl-aci07-leaf1)

MAC : 0000.0000.0000 ::: Num IPs : 1
IP# 0 : X.1.2.15 ::: IP# 0 flags : ::: l3-sw-hit: No
Vlan id : 0 ::: Vlan vnid : 0 ::: VRF name : l3_out_pk_tn:l3_out_vrf_pk_1
BD vnid : 0 ::: VRF vnid : 2228224
Phy If : 0 ::: Tunnel If : 0x18010006
Interface : Tunnel6
Flags : 0x80004400 ::: sclass :

49157

::: Ref count : 3 ==> sclass
EP Create Timestamp : 10/29/2024 10:38:34.949150
EP Update Timestamp : 10/29/2024 10:45:55.571786
EP Flags : IP|sclass|timer|

++ Traffic will be redirected based on redir(destgrp-7)
bgl-aci07-apic100#

fabric 101 show zoning-rule src-epg 32771 dst-epg 49157

Node 101 (bgl-aci07-leaf1)										

Rule ID	SrcEPG	DstEPG	FilterID	Dir	operSt	Scope	Name	Action	Prio	
4228	32771	49157	default	bi-dir	enabled	2228224		redir(destgrp-7)	src_dst	

++ Based on redirect policy traffic will be redirected to mac

02:4A:E9:54:B5:91

bgl-aci07-apic100#

fabric 101 show service redir info

Node 101 (bgl-aci07-leaf1)

LEGEND

TL: Threshold(Low) | TH: Threshold(High) | HP: HashProfile | HG: HealthGrp | BAC: Backup-Dest |

List of Dest Groups

GrpID Name	destination	HG-name
7 destgrp-7	dest-[3d49:a399:3d4b:4ea1:8829:5991:b554:e94a]-[vxlan-2228224]	l3_out_pk_tn::HG1

List of destinations

Name	bdVnid	vMac	vrf
dest-[3d49:a399:3d4b:4ea1:8829:5991:b554:e94a]-[vxlan-2228224]	vxlan-16744328		

02:4A:E9:54:B5:91

l3_out_pk_tn:l3_out_vrf_pk_1 enabled no-oper-dest l3_out_pk_tn::HG

++ PBR mac addresses are never learnt remotely as IP/MAC learning is disabled for PBR BD
++ PBR mac addresses are statically binded to interfaces where L4/L7 device is connected and reported to
++ Traffic will be forwarded to SPINE PROXY
++ Spine has an COOP entry for 02:4A:E9:54:B5:91

bgl-aci07-apic100#

fabric 201 show coop internal info repo ep key 16744328 02:4A:E9:54:B5:91

Node 201 (bgl-aci07-spine1)

Repo Hdr Checksum : 49503
Repo Hdr record timestamp : 10 29 2024 10:15:07 658496921
Repo Hdr last pub timestamp : 10 29 2024 10:15:07 661679296
Repo Hdr last dampen timestamp : 01 01 1970 00:00:00 0
Repo Hdr dampen penalty : 0
Repo Hdr flags : IN_OBJ ACTIVE
EP bd vnid : 16744328
EP mac :

02:4A:E9:54:B5:91

<<<<===== ASA MAC
flags : 0x480
repo flags : 0x102
Vrf vnid : 2228224
PcTag : 0x100c006
EVPN Seq no : 0
Remote publish timestamp: 01 01 1970 00:00:00 0
Snapshot timestamp: 10 29 2024 10:15:07 658496921
Tunnel nh : 10.0.144.66
MAC Tunnel : 10.0.144.66
IPv4 Tunnel : 10.0.144.66
IPv6 Tunnel : 10.0.144.66
ETEP Tunnel : 0.0.0.0
num of active ipv4 addresses : 0
num of anycast ipv4 addresses : 0
num of ipv4 addresses : 0

num of active ipv6 addresses : 0
num of anycast ipv6 addresses : 0
num of ipv6 addresses : 0
Primary Path:
Current published TEP :

10.0.144.66

Backup Path:
BackupTunnel nh : 0.0.0.0
Current Backup (publisher_id): 0.0.0.0
Anycast_flags : 0
Current citizen (publisher_id): 10.0.144.66
Previous citizen : 10.0.144.66
Prev to Previous citizen : 10.0.144.66
Synthetic Flags : 0x5
Synthetic Vrf : 411
Synthetic IP : X.X.83.223
Tunnel EP entry: 0x7f20900167a8
Backup Tunnel EP entry: (nil)
TX Status: COOP_TX_DONE\
Damp penalty: 0
Damp status: NORMAL
Exp status: 0
Exp timestamp: 01 01 1970 00:00:00 0
Hash: 3209430840 owner: 10.0.144.65

++ Spine will forward this to PBR Leaf Node 102 based on COOP entry
++ PBR Leaf Node will forward this to ASA FW on interface E1/14
++ ASA FW will forward the traffic based on mac address table and send it back to PBR Leaf Node 102
++ PBR Leaf Node will look for Dst IP in the traffic and route it to Leaf 104 if remote endpoint entry
++ Leaf 104 will get this traffic forwarded to actual EP X.1.2.15 (Leaf4 does not learn the client IP a

ASA نیو وکٹ

لیکشت نراق 1. ةوطخ

<#root>

ASA(config)#

show running-config interface

```
!  
interface GigabitEthernet0/0  
  bridge-group 1  
  nameif inside  
  security-level 100  
!  
interface GigabitEthernet0/1  
  bridge-group 1  
  nameif outside  
  security-level 0  
!
```

interface BVI1

ip address 192.168.100.1 255.255.255.0 ==> In case BVI IP is not defined ASA will not switch the packet.

!

قأعم تنك يغبن ي ملعي كام. 2. ةوطخ

<#root>

ASA(config)#

show run mac-learn

mac-learn inside disable

mac-learn outside disable

رآ ي ب ي ب:

MAC ل PBR ل ةتباتل MAC نيوانع لودج. 3. ةوطخل

<#root>

The mac statically binded to inside interface is the PBR mac generated by provider and vice versa
ASA(config)#

show run mac-address-table

mac-address-table static outside 024a.e954.b591

mac-address-table static inside 02c0.282b.d1cf

L2 لاصتا تارابتخا ريرمتل (ACL) لوصولا ي ف مكحتل ةمئاق نيوك ت. 4. ةوطخل

<#root>

ASA(config)#

show access-list

access-list L2_PBR ethertype permit 721

ASA(config)# show run access-group

access-group L2_PBR in interface inside

access-group L2_PBR in interface outside

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا