cisco Live!

#CiscoLive

The bridge to possible

ACI Troubleshooting – L3Out

Takuya Kishida - Technical Leader @ Cloud Networking

BRKDCN-3569

Cisco Webex App

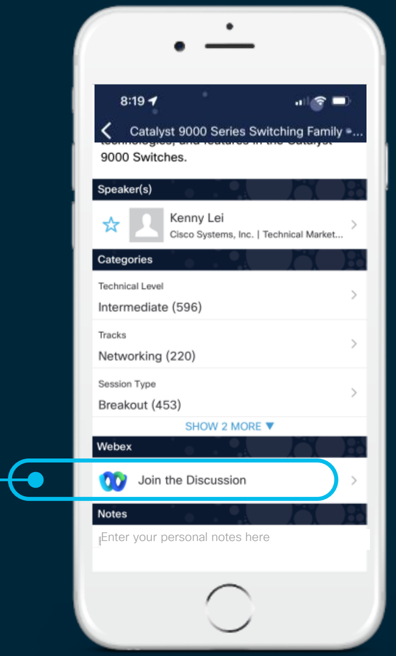
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated
by the speaker until June 17, 2022.



8:19

Catalyst 9000 Series Switching Family ...

9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

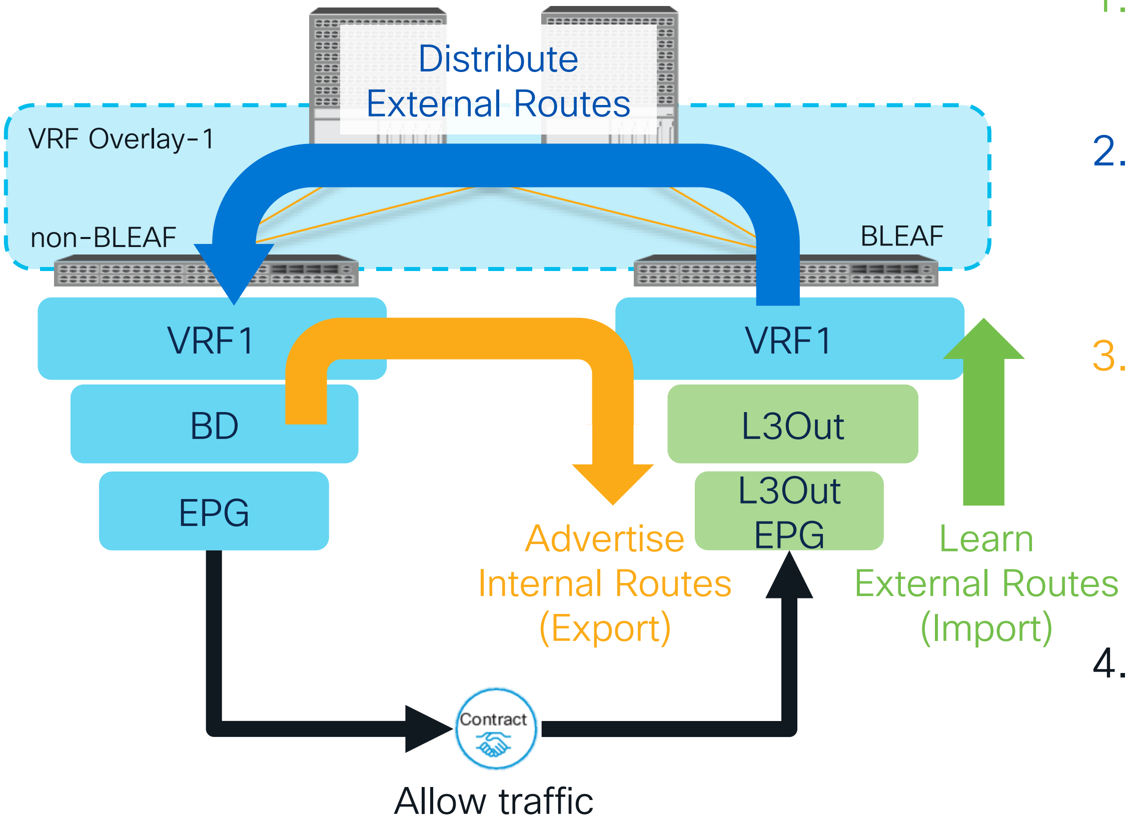
https://ciscolive.ciscoevents.com/ciscolivebot/#BRKDCN-3569

Agenda

- L3Out Key Components
  - Routing protocol deployment
  - Under the hood of infra MP-BGP
  - Under the hood of BD subnet advertisements
- L3Out Internal Route Maps
- L3Out Contract deep dive

L3Out Key Components

L3Out Key Components



1. Learn external routes
   - ➢ Routing Protocol in L3Out
2. Distribute external routes to other leaves
   - ➢ MP-BGP
3. Advertise internal routes (BD subnet) to outside
   - ➢ Redistribution
     and
   - ➢ Contract
4. Allow traffic with contracts
   - ➢ L3Out EPG (External EPG)
     and
   - ➢ Contract

L3Out Key Components

- 1. Learn External Routes = Routing Protocol

Configurations

External Routed Networks (L3Out)

- VRF to deploy a routing protocol
- Routing protocol parameters
  ex. OSPF area 0.0.0.1 nssa

Node Profile

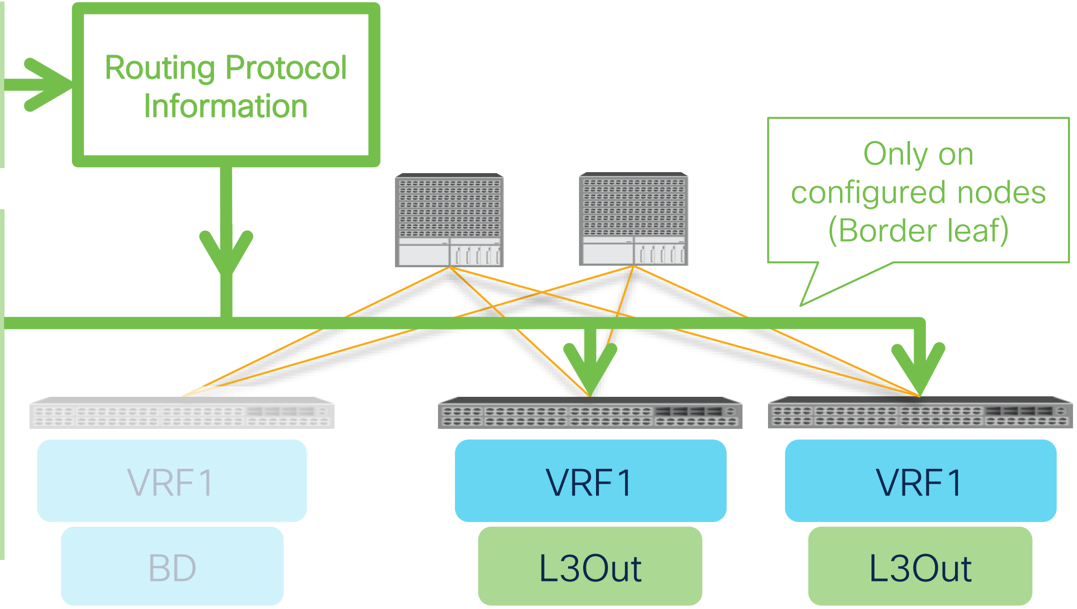
- Node(s) to deploy a routing protocol
- Static route (if any)

Interface Profile

- I/F(s) to deploy a routing protocol
- Routing protocol I/F parameters
  ex. OSPF hello interval

Networks (L3Out EPG)

- Contract
- Advanced Route Control
  ex. route-map


Routing Protocol Information
Only on configured nodes (Border leaf)
VRF1
BD
VRF1
L3Out
VRF1
L3Out

Verification Examples (OSPF)

1. Is OSPF enabled on the correct I/F?

```
border-leaf# show ip ospf int bri vrf TK:VRF1
 Interface                ID     Area            Cost   State    Neighbors Status
 Vlan58                   134    backbone        4      BDR      2         up

border-leaf# show vlan id 58 extended
 VLAN Name                             Encap            Ports
 ---- -------------------------------- ---------------- -----------------------
 58   TK:VRF1:l3out-                   vxlan-15695748,  Eth1/3, Po2
      L3OUT_OSPF:vlan-1425             vlan-1425
```

Same CLI verifications as standalone NX-OS

If anything is not expected, check config or any faults in the APIC GUI.

2. Are OSPF parameters matching with neighbors?

```
border-leaf# show int vlan 58 | grep MTU
  MTU 1500 bytes, BW 10000000 Kbit, DLY 1 usec

border-leaf# show ip ospf int vlan 58 | egrep 'IP|State|Timer|auth'
    IP address 15.0.0.3/24, Process ID default VRF TK:VRF1, area backbone
    State BDR, Network type BROADCAST, cost 4
    Timer intervals: Hello 10, Dead 40, Wait 40, Retransmit 5
    No authentication
```

Is MTU matching?
Is Network Mask matching?
Is Area matching?
Is Timer matching?
Is Network Type expected?
etc.

3. Are OSPF neighbors established correctly?

```
border-leaf# show ip ospf neighbors vrf TK:VRF1
Neighbor ID     Pri State            Up Time  Address         Interface
 4.4.4.4          1 FULL/DR           2d06h    15.0.0.4        Vlan58
 9.9.9.9          1 FULL/DROTHER      2d06h    15.0.0.1        Vlan58
```

Can they ping to each other?
  leaf# iping –V <VRF> <target IP>
  ※OSPF DBD requires unicast reachability
etc.

Verification Examples (EIGRP)

1. Is EIGRP enabled on a correct I/F?

```
border-leaf# show ip eigrp int bri vrf TK:VRF1
                        Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface       Peers   Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
vlan92            2         0/0       1         0/0          50           0

border-leaf# show vlan id 92 extended
 VLAN Name                                Encap            Ports
 ---- ----------------------------------- ---------------- ----------------------
 92   TK:VRF1:l3out-                      vxlan-14712828,  Eth1/3, Po2
      L3OUT_EIGRP:vlan-1426               vlan-1426
```

Same CLI verifications as standalone NX-OS

If anything is not expected, check config or any faults in the APIC GUI.

2. Are EIGRP parameters matching with neighbors?

```
border-leaf# show int vlan 92 | grep MTU
  MTU 1500 bytes, BW 10000000 Kbit, DLY 1 usec

border-leaf# show ip int vlan 92 | grep 'IP addr'
  IP address: 16.0.0.3, IP subnet: 16.0.0.0/24
```

```
border-leaf# show ip eigrp vrf TK:VRF1 | egrep 'AS|K'
IP-EIGRP AS 1 ID 3.3.3.3 VRF TK:VRF1
   Metric weights: K1=1 K2=0 K3=1 K4=0 K5=0
```

Is MTU matching?
Is Network Mask matching?
Is AS matching?
Is K value matching?
etc.

3. Are EIGRP neighbors established correctly?

```
border-leaf# show ip eigrp neighbors vrf TK:VRF1
H   Address                 Interface       Hold  Uptime  SRTT   RTO  Q   Seq
                                            (sec)         (ms)       Cnt  Num
0   16.0.0.4                vlan92          12    2d06h   1      50   0    10
1   16.0.0.1                vlan92          13    2d06h   1      50   0    346
```

Verification Examples (BGP)

1. Is BGP neighbor session configured as expected?

```
border-leaf# show ip bgp neighbors vrf TK:VRF1 | egrep 'BGP nei|Using|Opens|hops'
BGP neighbor is 17.0.0.1,  remote AS 65001, ebgp link,  Peer index 1
  Using Loopback6 as update source for this peer
  External BGP peer might be upto to 2 hops away
  Opens:                         1                   1

border-leaf# show ip int lo6 | grep 'IP addr'
  IP address: 3.3.3.3, IP subnet: 3.3.3.3/32
```

Is it correct remote AS?
Is it using the correct source I/F with the correct IP?
Is enough multi-hop configured for eBGP?
Are Open messages exchanged?

2. Is there IP reachability ?

```
border-leaf# iping -V TK:VRF1 17.0.0.1 -S 3.3.3.3
PING 17.0.0.1 (17.0.0.1) from 3.3.3.3: 56 data bytes
64 bytes from 17.0.0.1: icmp_seq=0 ttl=255 time=0.76 ms
64 bytes from 17.0.0.1: icmp_seq=1 ttl=255 time=0.639 ms
   === snip ===

--- 17.0.0.1 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
```

Is there an IP reachability to the BGP neighbor from the correct source IP?

3. Are BGP neighbors established correctly?

```
border-leaf# show ip bgp summary vrf TK:VRF1
BGP router identifier 3.3.3.3, local AS number 65003

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
17.0.0.1        4 65001    3300    3302       78    0    0   2d06h  2
```

Is it receiving BGP routes?
Is ACI BGP using expected local AS?

L3Out Key Components

- 2. Distribute External Routes = MP-BGP in infra

Configurations

Pod Profile

Pod Policy Group

BGP Route Reflector Policy

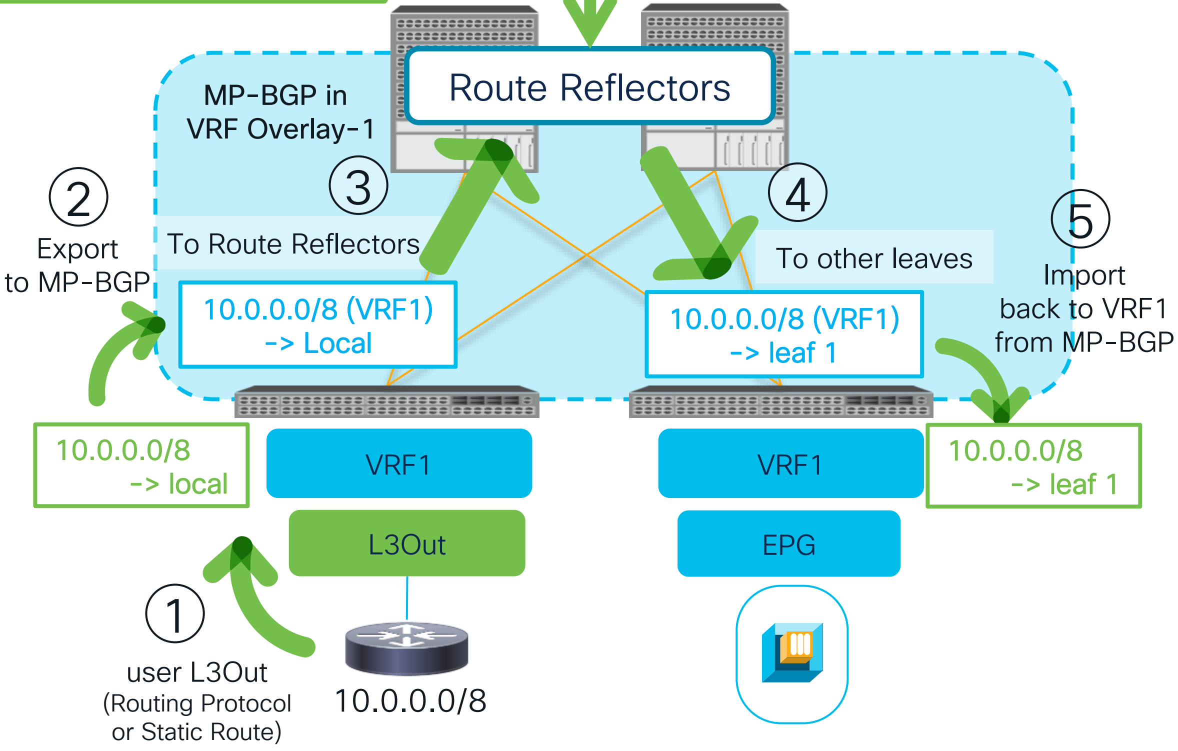
- default

System Settings

BGP Route Reflector

- ACI BGP AS number
  (for both MP-BGP and L3Out BGP)
- MP-BGP Route Reflector Spines

Implement all steps except for step ① (user L3Out)

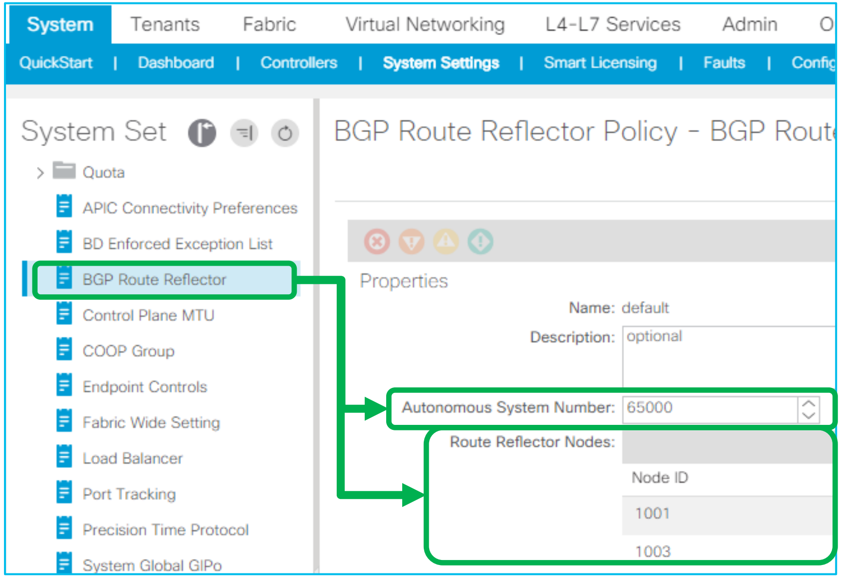


L3Out Key Components

2. Distribute External Routes = MP-BGP in infra

TIP

1. Select ACI BGP AS and Route Reflector spines



Name: default

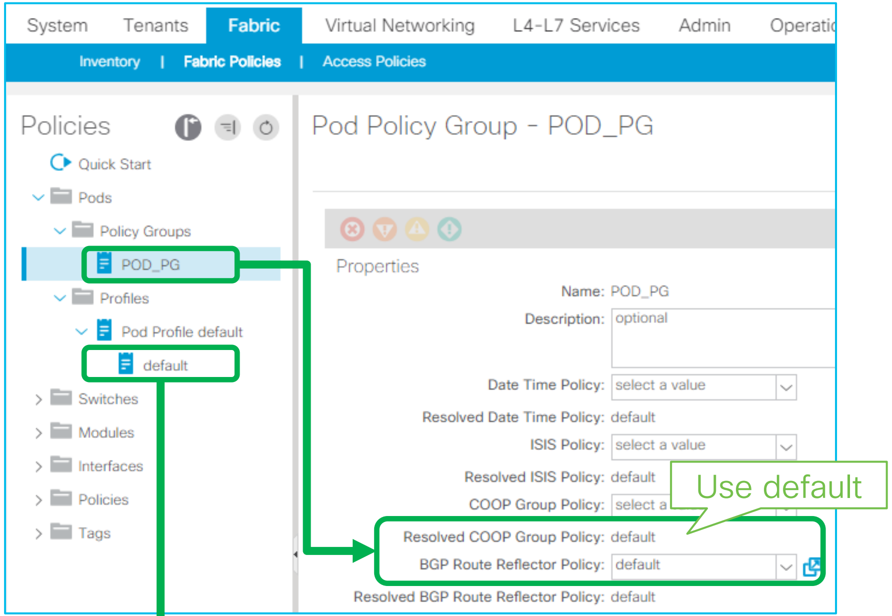
Description: optional

Autonomous System Number: 65000

Route Reflector Nodes:

Node ID
1001
1003

2. Apply Route Reflector policy to Pod Policy Group



Name: POD_PG

Description: optional

Date Time Policy: select a value

Resolved Date Time Policy: default

ISIS Policy: select a value

Resolved ISIS Policy: default

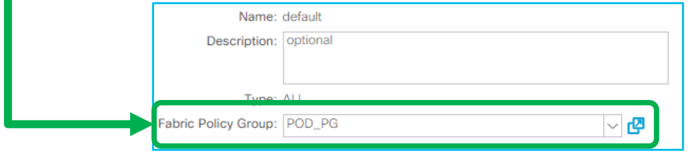
COOP Group Policy: select a

Resolved COOP Group Policy: default

BGP Route Reflector Policy: default

Resolved BGP Route Reflector Policy: default

3. Apply Pod Policy Group to Pod Profile



Name: default

Description: optional

Type: ALL

Fabric Policy Group: POD_PG

※ BGP L3Outs share the same AS with this internal MP-BGP

CLI Verification

1. Do both border leaf and non-border leaf have BGP sessions with RR spines?

```
leaf# show bgp sessions vrf overlay-1
Neighbor         ASN    Flaps LastUpDn|LastRead|LastWrit St Port(L/R)  Notif(S/R)
10.0.184.65      65003 0      2d07h    |never    |never    E  37850/179  0/0
10.0.184.66      65003 0      2d07h    |never    |never    E  45089/179  0/0

leaf# acidiag fnvread | grep spine
    1001         1       spine1       FGE10000000       10.0.184.65/32    spine          active    0
    1002         1       spine2       SAL10000000       10.0.184.66/32    spine          active    0
```

✓ BGP neighbors are RR spines TEP IPs

2. Is the external route learned on a border leaf?

```
border-leaf# show ip route vrf TK:VRF1
10.0.0.0/8, ubest/mbest: 1/0
    *via 15.0.0.1, Vlan58, [110/5], 2d08h, ospf-default, intra
```

3. Does non-border leaf show the expected border leaf as next-hop?

✓ Next-hops are border Leaf TEP IPs
✓ Learned via iBGP in ACI AS# (65003)

```
non-border-leaf# show ip route vrf TK:VRF1
10.0.0.0/8, ubest/mbest: 2/0
    *via 10.0.184.67%overlay-1, [200/5], 2d08h, bgp-65003, internal, tag 65003

non-border-leaf# acidiag fnvread
      ID    Pod ID                 Name     Serial Number         IP Address     Role         State
LastUpdMsgId
-------------------------------------------------------------------------------------------------------
     101         1          border-leaf        SAL10000001      10.0.184.67/32     leaf          active    0
```

L3Out Key Components

- 3. Advertise BD subnets

Configurations

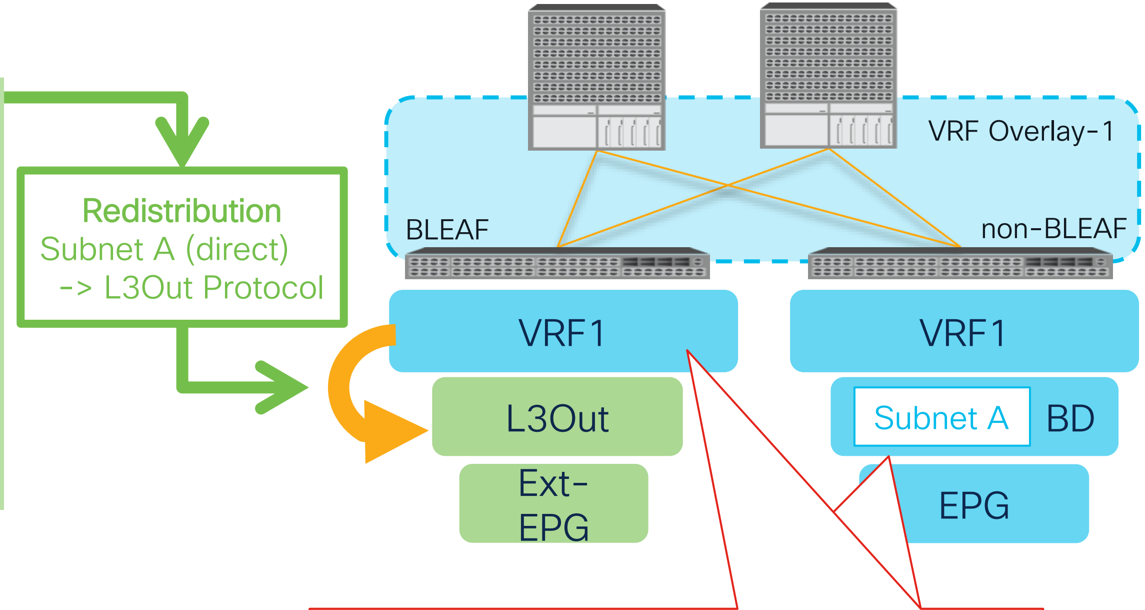
Bridge Domain (BD)

BD Subnet

- Subnet A
  - ✓ "Advertised Externally"

Multiple options to select L3Outs

- L3Out to BD association
- default-export under an L3Out
- ...



No BD Subnet A on BLEAF yet

- ➢ MP-BGP is to distribute only external routes
- ➢ MP-BGP never distributes BD subnets

L3Out Key Components

- 3. Advertise BD subnets

Configurations

Bridge Domain (BD)

BD Subnet

- Subnet A
  - ✓ "Advertised Externally"

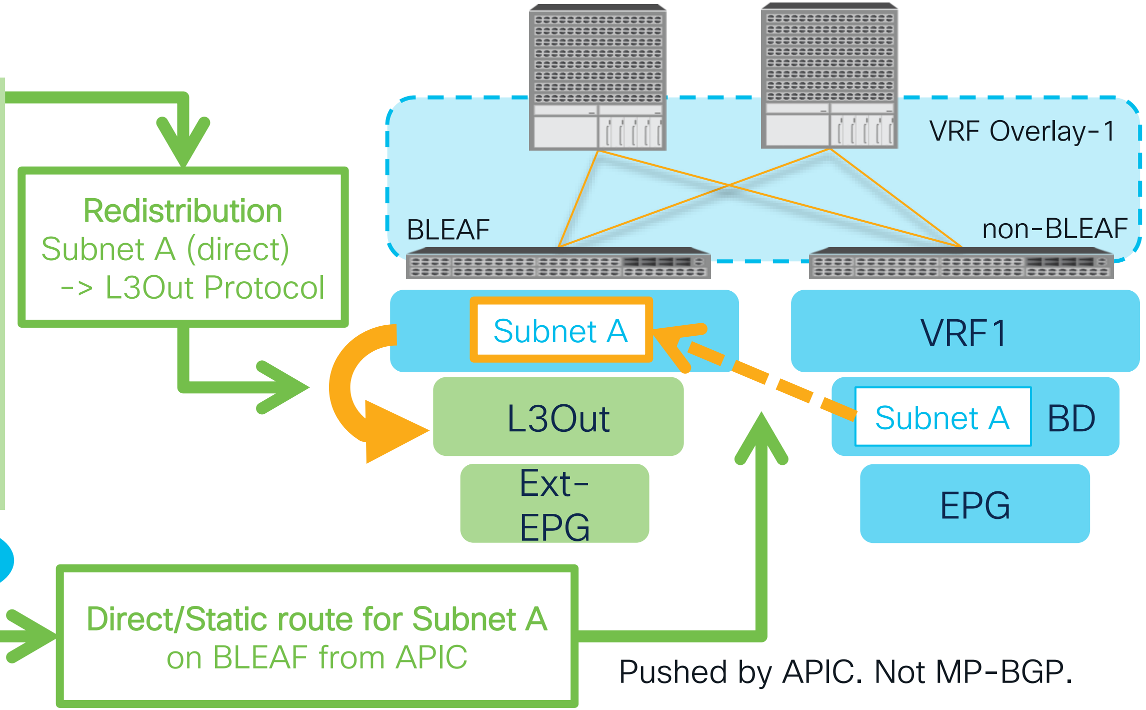
Multiple options to select L3Outs

- L3Out to BD association
- default-export under an L3Out
- …

External Routed Networks (L3Out)

External EPG

- Contracts between Ext-EPG and EPG



Redistribution
Subnet A (direct)
-> L3Out Protocol

Direct/Static route for Subnet A
on BLEAF from APIC

Pushed by APIC. Not MP-BGP.

CLI Verification (OSPF, EIGRP)

1. Does the border leaf have the BD subnet to advertise?

```
border-leaf# show ip route vrf TK:VRF1
192.168.1.0/24, ubest/mbest: 1/0, attached, direct, pervasive
    *via 10.0.184.64%overlay-1, [1/0], 04:32:27, static
```

If not, check the contract between the Ext-EPG and the EPG for the BD.
This should be pushed by APIC. Not via MP-BGP.

2. Check the route-map name used by the routing protocol on the border leaf for static/direct redistribution

```
border-leaf# show ip ospf vrf TK:VRF1

 Redistributing External Routes from
   direct route-map exp-ctx-st-2097152
```

```
border-leaf# show ip eigrp vrf TK:VRF1

  Redistributing:
    direct route-map exp-ctx-st-2097152
```

Check next page for BGP

3. Does the route-map have the expected BD subnet?

```
border-leaf# show route-map exp-ctx-st-2097152
route-map exp-ctx-st-2097152, deny, sequence 1
  Match clauses:
    tag: 4294967295
  Set clauses:
route-map exp-ctx-st-2097152, permit, sequence 15804
  Match clauses:
    ip address prefix-lists: IPv4-st49158-2097152-exc-int-inferred-export-dst
    ipv6 address prefix-lists: IPv6-deny-all
  Set clauses:
```

```
border-leaf# show ip prefix-list IPv4-st49158-2097152-exc-int-inferred-export-dst
ip prefix-list IPv4-st49158-2097152-exc-int-inferred-export-dst: 1 entries
   seq 1 permit 192.168.1.254/24
```

IP prefix-list should have the BD subnet.
If not, check APIC config and any faults.

- ✓ Is "Advertise Externally" on the BD subnet checked?
- ✓ Any missing configurations?

CLI Verification (BGP)

1. Does the border leaf have the BD subnet to advertise?

```
--- snip ---
```

2. Check the route-map name used by BGP outbound rule for each neighbor

```
border-leaf# show bgp process vrf TK:VRF1
 Information for address family IPv4 Unicast in VRF TK:VRF1
    Redistribution
          direct, route-map permit-all
```

BGP redistributes all direct routes first, then limit the routes with an outbound route-map.

```
border-leaf# show ip bgp neighbors vrf TK:VRF1 | egrep '^BGP|Out'
BGP neighbor is 17.0.0.1,  remote AS 65001, ebgp link,  Peer index 1
  Outbound route-map configured is exp-l3out-L3OUT_BGP-peer-2097152, handle obtained
```

3. Does the BGP outbound route-map have the expected BD subnet?

```
border-leaf# show route-map exp-l3out-L3OUT_BGP-peer-2097152
route-map exp-l3out-L3OUT_BGP-peer-2097152, permit, sequence 15801
  Match clauses:
    ip address prefix-lists: IPv4-peer49157-2097152-exc-int-inferred-export-dst
    ipv6 address prefix-lists: IPv6-deny-all
  Set clauses:
route-map exp-l3out-L3OUT_BGP-peer-2097152, deny, sequence 16000
  Match clauses:
    route-type: direct
  Set clauses:
```

IP prefix-list should have the BD subnet.
If not, check APIC config and any faults.

- ✓ Is “Advertise Externally” on the BD subnet checked?
- ✓ Any missing configurations?

```
border-leaf# show ip prefix-list IPv4-peer49157-2097152-exc-int-inferred-export-dst
ip prefix-list IPv4-peer49157-2097152-exc-int-inferred-export-dst: 1 entries
   seq 1 permit 192.168.1.254/24
```

L3Out Internal Route Maps

(OSPF, EIGRP) Two types of route maps

OSPF

```
border-leaf# show ip ospf vrf TK:VRFA | egrep 'direct|static|bgp|eigrp’
   direct route-map exp-ctx-st-2785280
   static route-map exp-ctx-st-2785280
   bgp route-map exp-ctx-proto-2785280
   eigrp route-map exp-ctx-proto-2785280
```

EIGRP

```
border-leaf# show ip eigrp vrf TK:VRFA | egrep 'direct|static|ospf|bgp'
    bgp-65002 route-map exp-ctx-proto-2785280
    direct route-map exp-ctx-st-2785280
    ospf-default route-map exp-ctx-proto-2785280
    static route-map exp-ctx-st-2785280
```

exp-ctx-st-<VRF VNID>

Route maps for direct or static routes

- L3Out association to a BD
- Export Route Control Subnet
- Route map like default-export

exp-ctx-proto-<VRF VNID>

Route maps for routing protocols

- Export Route Control Subnet
- Route map like default-export

(BGP) a route map per L3Out or per peer

```
(when not using a per peer route map)
border-leaf# show bgp ipv4 unicast neighbors vrf TK:VRFA | grep Outbound
  Outbound route-map configured is exp-l3out-BGP-peer-2785280, handle obtained

(when using a per peer route map)
border-leaf# show bgp ipv4 unicast neighbors vrf TK:VRFA | grep Outbound
  Outbound route-map configured is TK-BGP_PEER1-BGP-out, handle obtained
```

Without per-peer route-map

exp-l3out-<L3Out>-peer-<VRF VNID>

- L3Out association to a BD
- Export Route Control Subnet
- Route map like default-export

New in 4.2

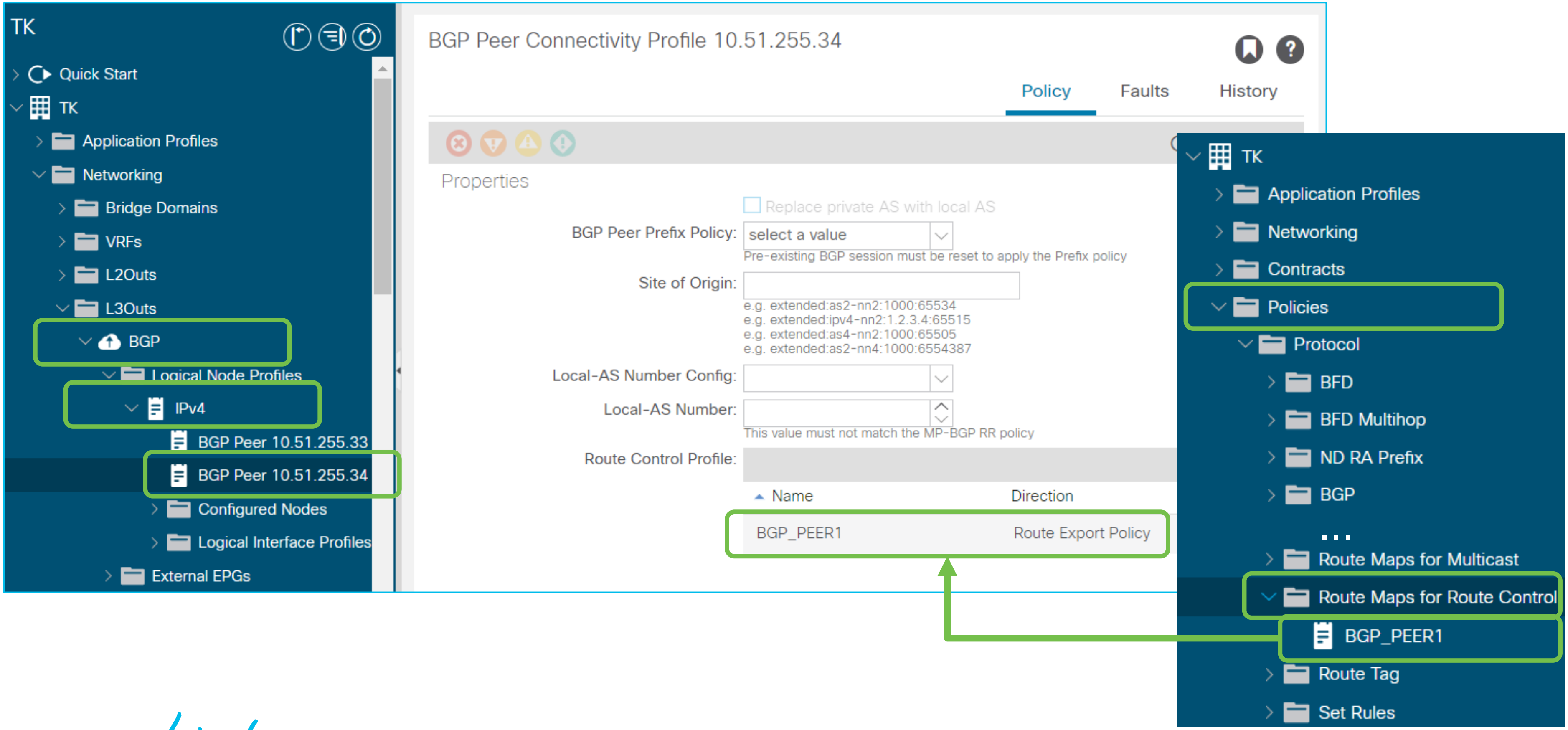
With per-peer route-map

<tenant>-<route_map>-<L3Out>-out

- Non-default route map in BGP peer connectivity profile

BGP per-peer route maps

TIP



BGP Peer Connectivity Profile 10.51.255.34

Policy | Faults | History

Properties

□ 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: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:

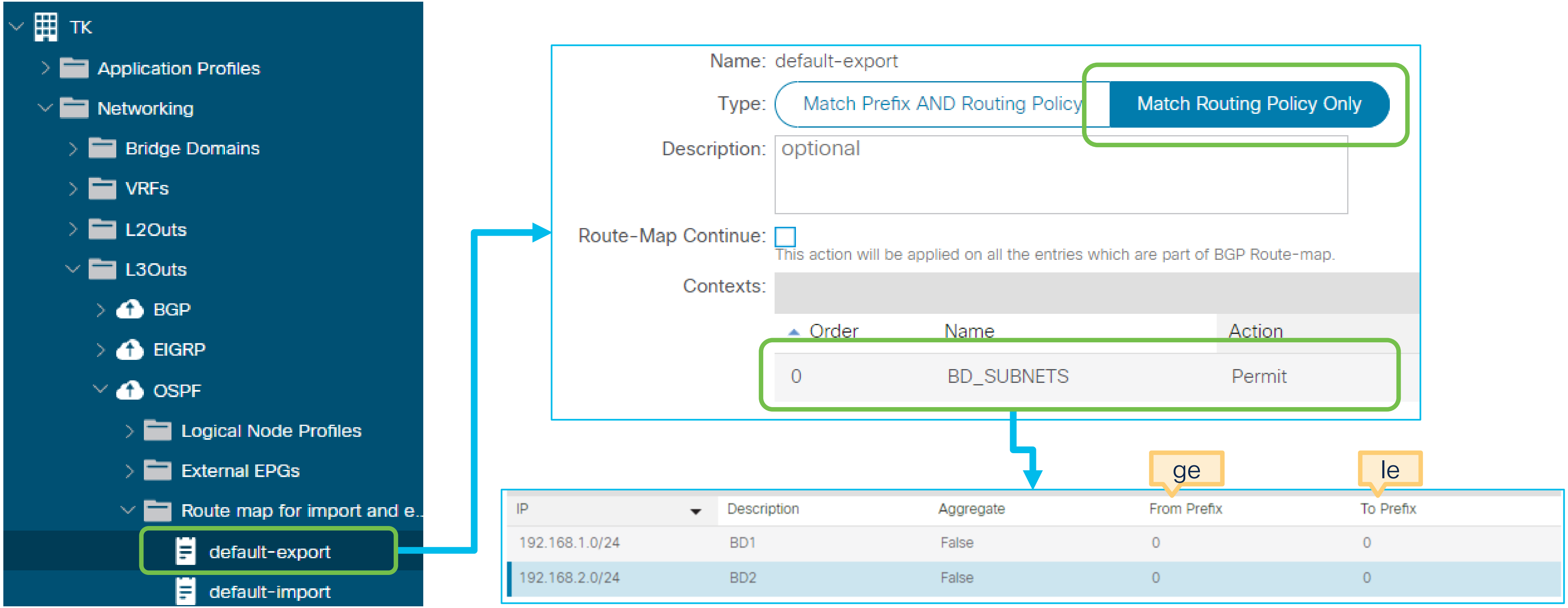
Local-AS Number:
This value must not match the MP-BGP RR policy

Route Control Profile:

Name	Direction
BGP_PEER1	Route Export Policy

default-export route map configuration

All route advertisement (both BD subnets and transit routing) in one single component while L3Out external EPGs are dedicated for security.



Name: default-export

Type: Match Prefix AND Routing Policy | Match Routing Policy Only

Description: optional

Route-Map Continue: □
This action will be applied on all the entries which are part of BGP Route-map.

Contexts:

Order	Name	Action
0	BD_SUBNETS	Permit

IP	Description	Aggregate	From Prefix	To Prefix
192.168.1.0/24	BD1	False	0	0
192.168.2.0/24	BD2	False	0	0

The best way to advertise routes from an L3Out

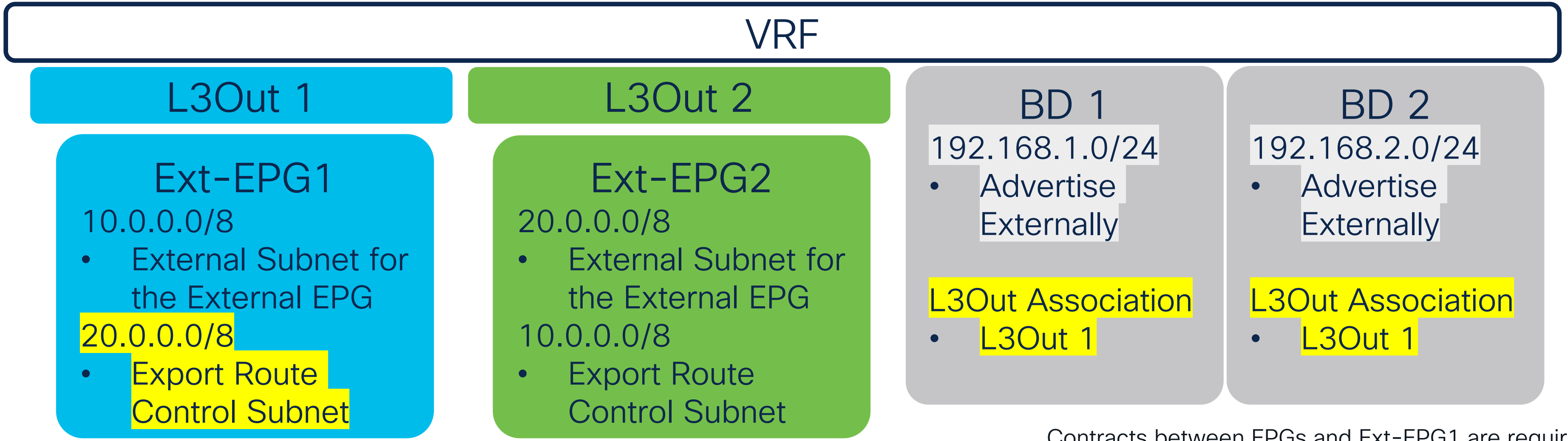
- BD association to an L3Out
- “Export Route Control Subnet” in L3Out EPGs
- Non-default route maps in L3Out EPGs/Subnets
- Non-default route maps (per-peer route maps) in BGP peer connectivity profile
- The default route map (default-export) in an L3Out

Why default-export? Let us compare

How do we advertise BD subnets and Transit routes from L3Out 1?

Route advertisements without default-export:

- BD subnet advertisement via L3Out to BD association
- Transit Routes via Export Route Control Subnet in an external EPG



VRF

L3Out 1

Ext-EPG1

10.0.0.0/8

- External Subnet for the External EPG

20.0.0.0/8

- Export Route Control Subnet

L3Out 2

Ext-EPG2

20.0.0.0/8

- External Subnet for the External EPG

10.0.0.0/8

- Export Route Control Subnet

BD 1

192.168.1.0/24

- Advertise Externally

L3Out Association

- L3Out 1

BD 2

192.168.2.0/24

- Advertise Externally

L3Out Association

- L3Out 1

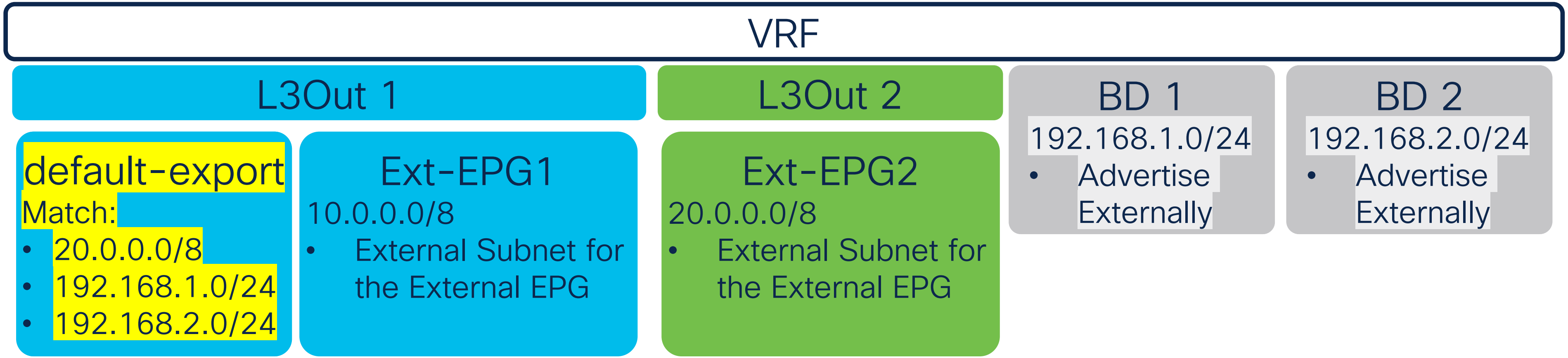
Contracts between EPGs and Ext-EPG1 are required.

Why default-export? Let us compare

How do we advertise BD subnets and Transit routes from L3Out 1?

Route advertisements with default-export:

- IP Prefix List in default-export



VRF

L3Out 1

default-export
Match:
- 20.0.0.0/8
- 192.168.1.0/24
- 192.168.2.0/24

Ext-EPG1
10.0.0.0/8
- External Subnet for the External EPG

L3Out 2

Ext-EPG2
20.0.0.0/8
- External Subnet for the External EPG

BD 1
192.168.1.0/24
- Advertise Externally

BD 2
192.168.2.0/24
- Advertise Externally

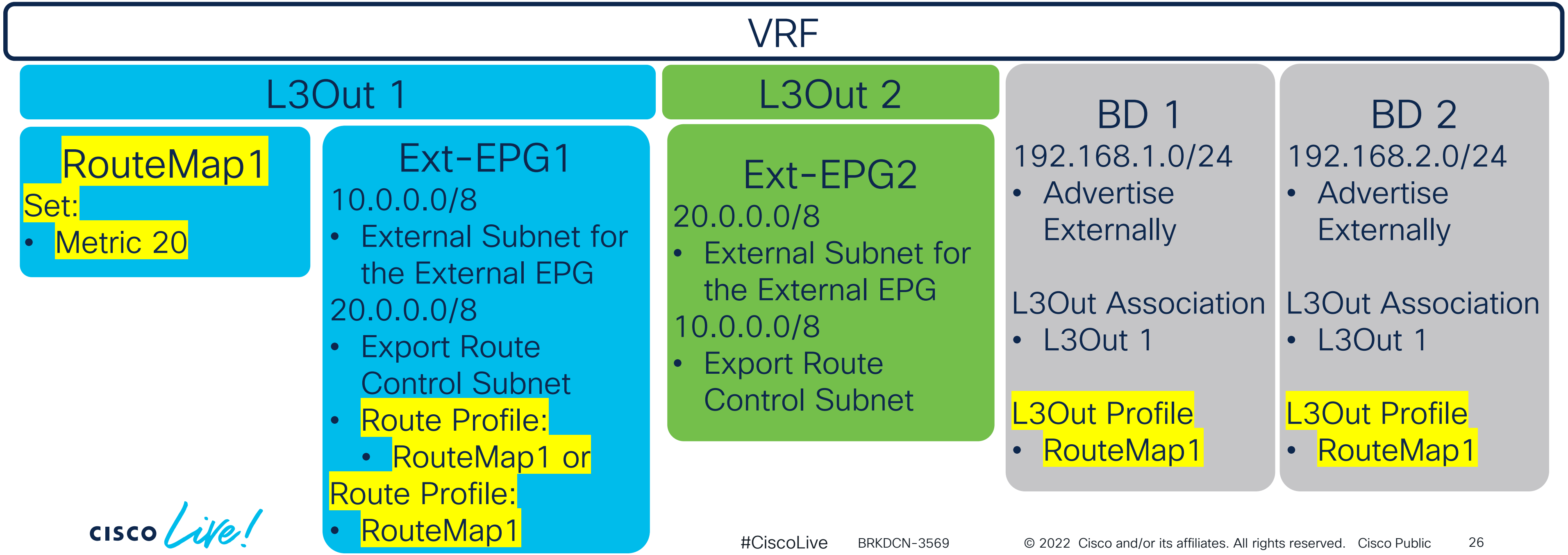
Contracts between EPGs and Ext-EPG1 are required.

Why default-export? Let us compare

How do we set metric to the routes we advertise?

Route advertisements without default-export:

- BD subnet advertisement via L3Out to BD association
- Transit Routes via Export Route Control Subnet in an external EPG



VRF

L3Out 1

RouteMap1
Set:
- Metric 20

Ext-EPG1
10.0.0.0/8
- External Subnet for the External EPG

20.0.0.0/8
- Export Route Control Subnet
- Route Profile:
  - RouteMap1 or

Route Profile:
- RouteMap1

L3Out 2

Ext-EPG2
20.0.0.0/8
- External Subnet for the External EPG

10.0.0.0/8
- Export Route Control Subnet

BD 1
192.168.1.0/24
- Advertise Externally

L3Out Association
- L3Out 1

L3Out Profile
- RouteMap1

BD 2
192.168.2.0/24
- Advertise Externally

L3Out Association
- L3Out 1

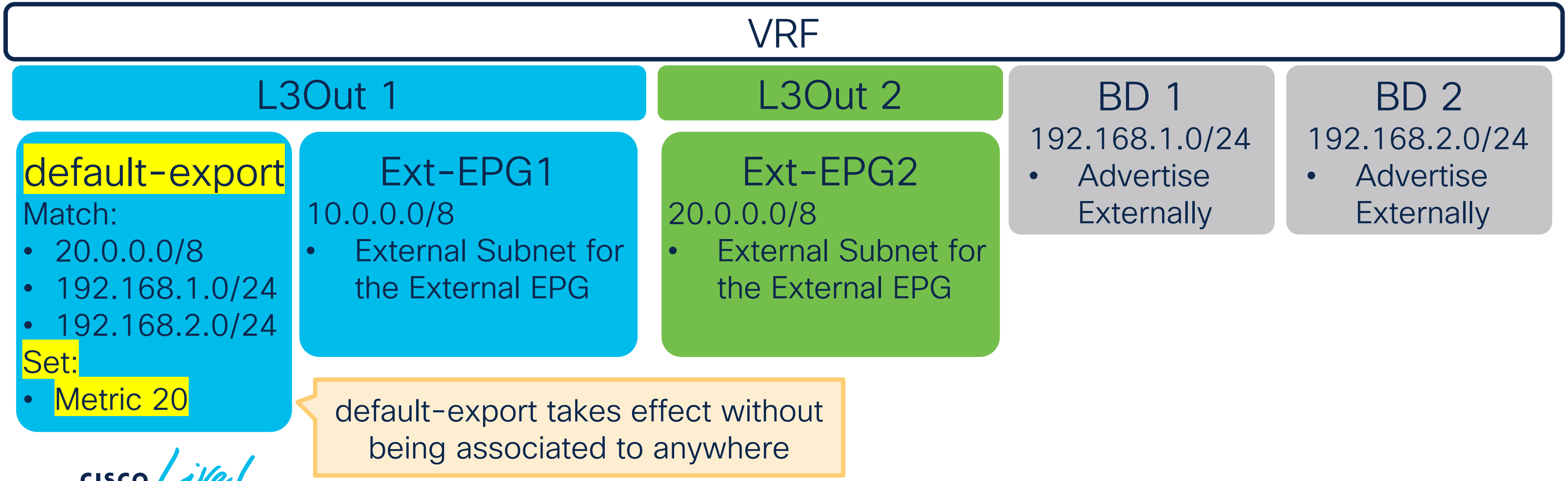
L3Out Profile
- RouteMap1

Why default-export? Let us compare

How do we set metric to the routes we advertise?

Route advertisements with default-export:

- IP Prefix List in default-export



VRF

L3Out 1

default-export

Match:
- 20.0.0.0/8
- 192.168.1.0/24
- 192.168.2.0/24

Set:
- Metric 20

Ext-EPG1

10.0.0.0/8
- External Subnet for the External EPG

L3Out 2

Ext-EPG2

20.0.0.0/8
- External Subnet for the External EPG

BD 1

192.168.1.0/24
- Advertise Externally

BD 2

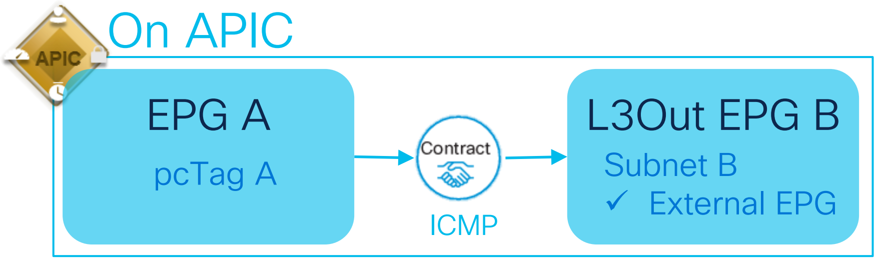
192.168.2.0/24
- Advertise Externally

default-export takes effect without being associated to anywhere

L3Out Contracts

Contracts – EPG to External EPG

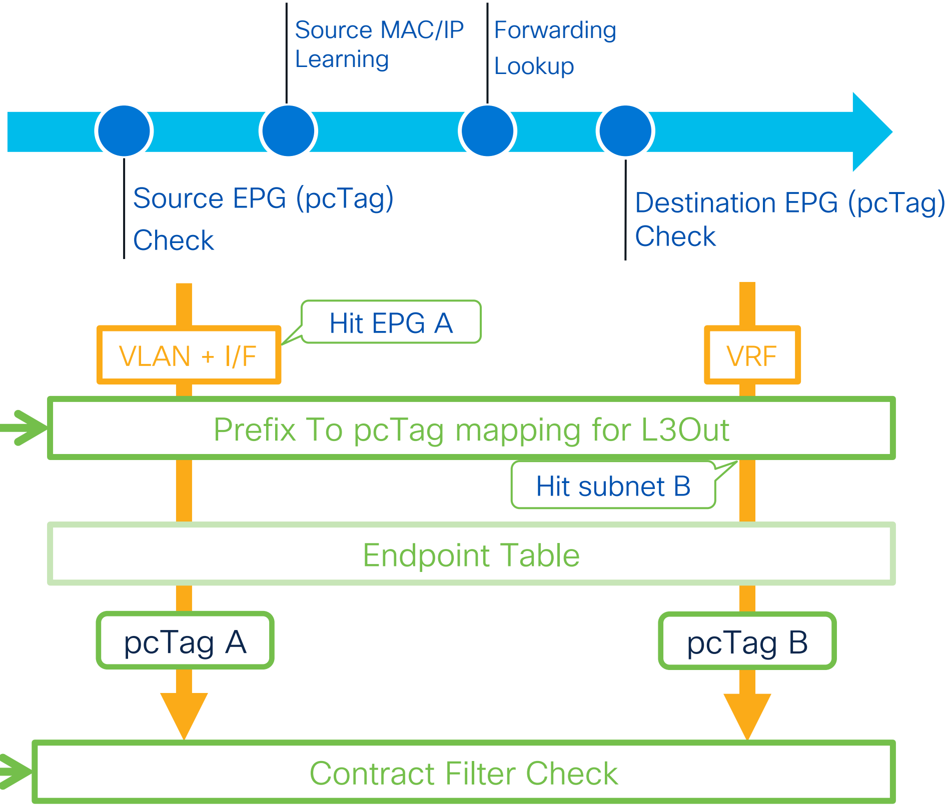
Traffic Flow: Regular EPG A (IP A) -> L3Out EPG B (IP B)



On LEAF

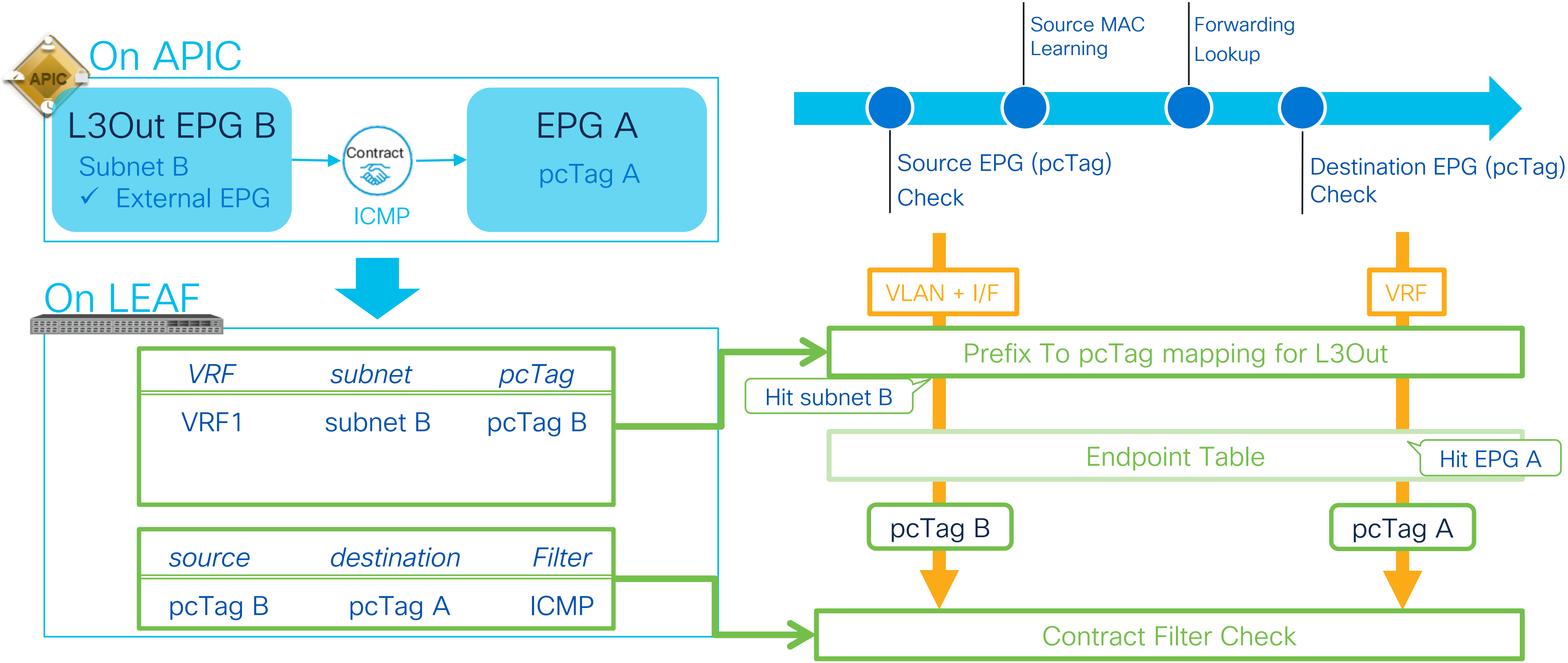
VRF	*subnet*	*pcTag*
VRF1	subnet B	pcTag B

source	*destination*	*Filter*
pcTag A	pcTag B	ICMP



Contracts – External EPG to EPG

Traffic Flow: L3Out EPG B (IP B) -> Regular EPG A (IP A)



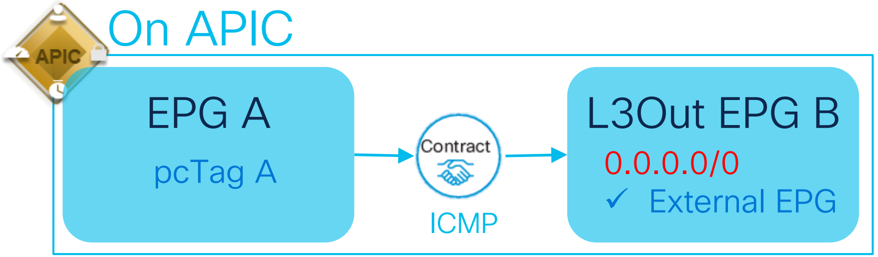
VRF	*subnet*	*pcTag*
VRF1	subnet B	pcTag B

source	*destination*	*Filter*
pcTag B	pcTag A	ICMP

Contracts – EPG to External EPG (0.0.0.0/0)

Traffic Flow: Regular EPG A (IP A) -> L3Out EPG B (IP B)

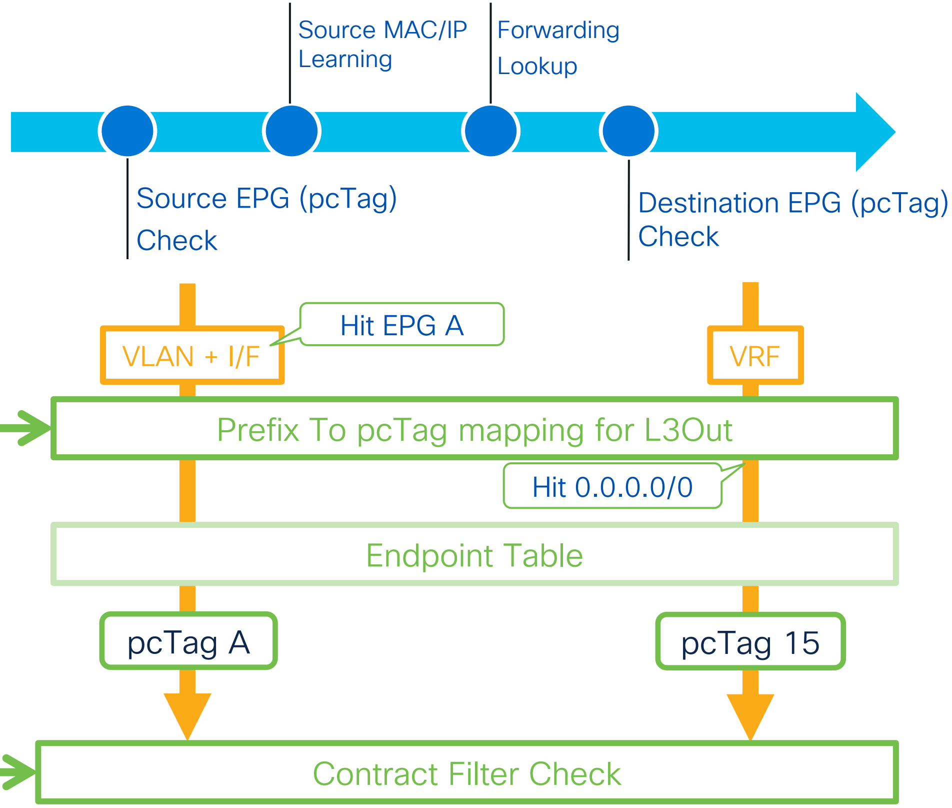
On APIC



On LEAF

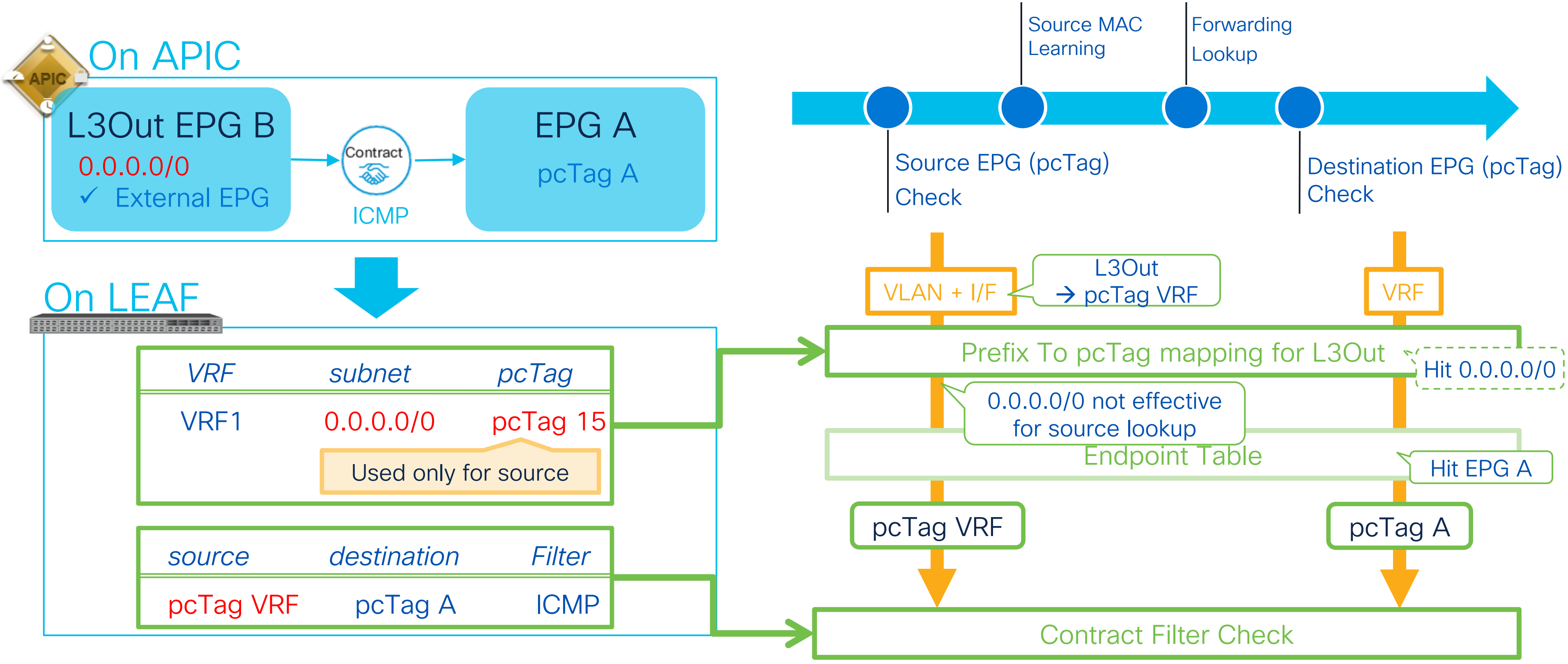
VRF	*subnet*	*pcTag*
VRF1	0.0.0.0/0	pcTag 15

source	*destination*	*Filter*
pcTag A	pcTag 15	ICMP



Contracts – External EPG (0.0.0.0/0) to EPG

Traffic Flow: L3Out EPG B (IP B) -> Regular EPG A (IP A)



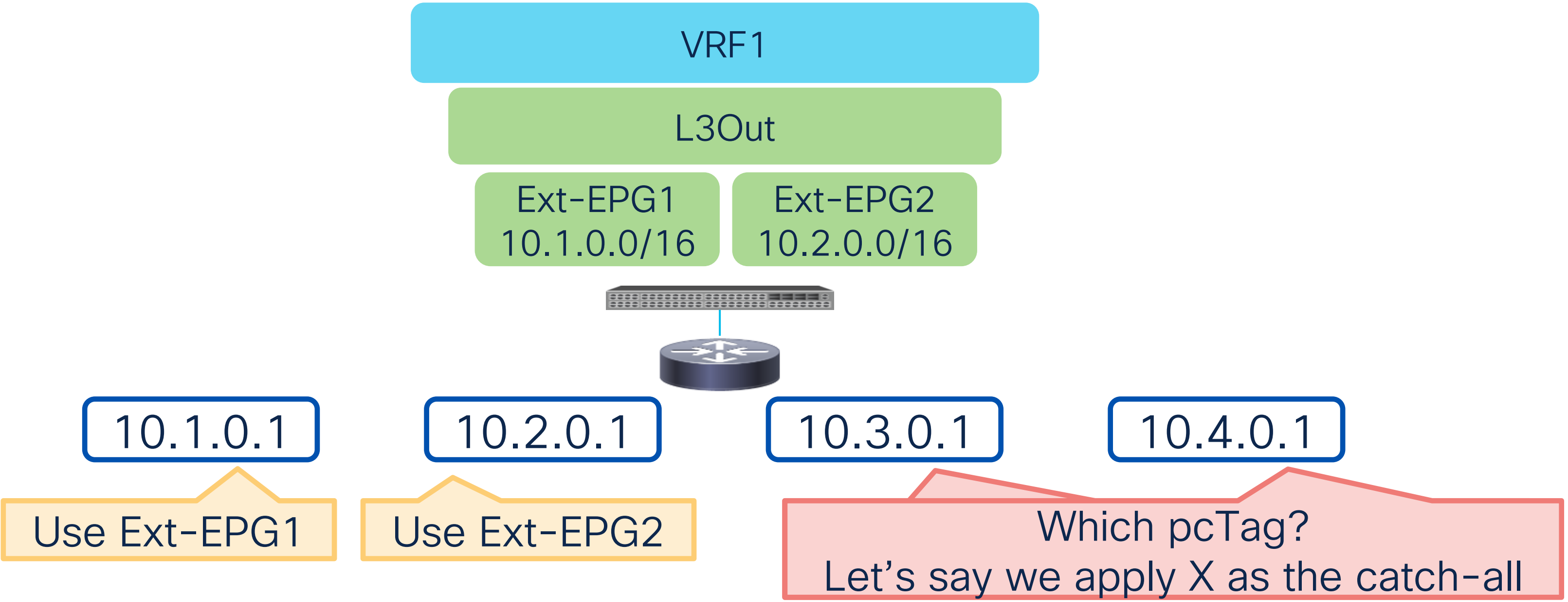
VRF	*subnet*	*pcTag*
VRF1	0.0.0.0/0	pcTag 15

Used only for source

source	*destination*	*Filter*
pcTag VRF	pcTag A	ICMP

Why is 0.0.0/0 so special?

TIP



VRF1

L3Out

Ext-EPG1
10.1.0.0/16

Ext-EPG2
10.2.0.0/16

10.1.0.1

10.2.0.1

10.3.0.1

10.4.0.1

Use Ext-EPG1

Use Ext-EPG2

Which pcTag?
Let’s say we apply X as the catch-all

With the same pcTag X, 10.3.0.1 and 10.4.0.1 can talk to each other without any configurations.

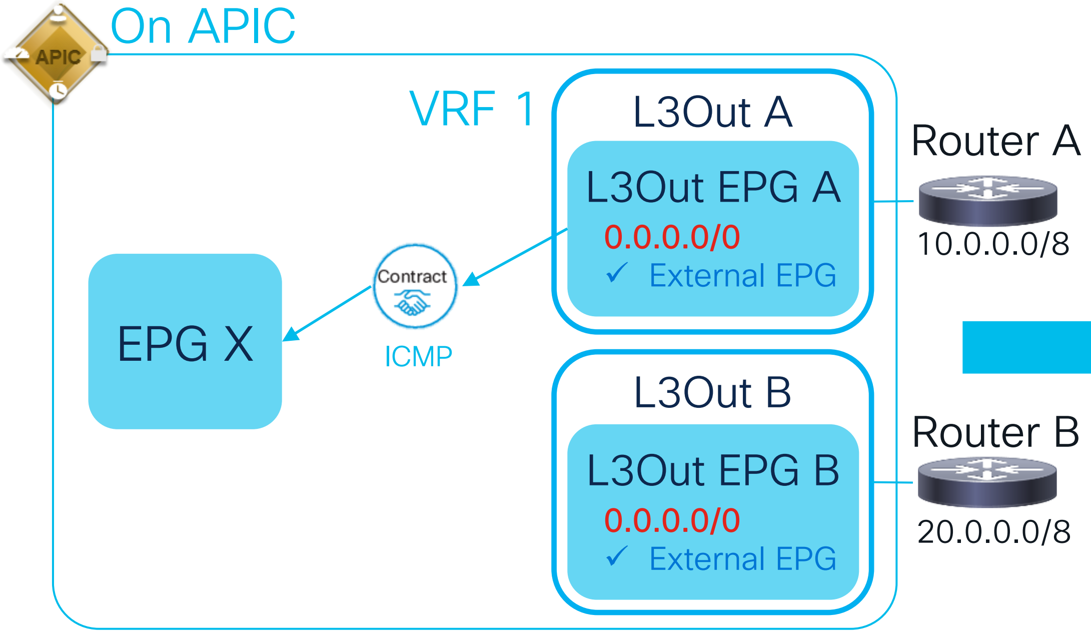
➢ This is against Zero-Trust model of ACI

Assign a different source and destination pcTag for the catch-all

L3Out Contract

Common Issue (L3Out EPGs with 0.0.0.0/0)

On APIC



Prefix-pcTag entry is per VRF. Default catch all (0.0.0.0) is shared with everyone in the VRF.

On Leaf

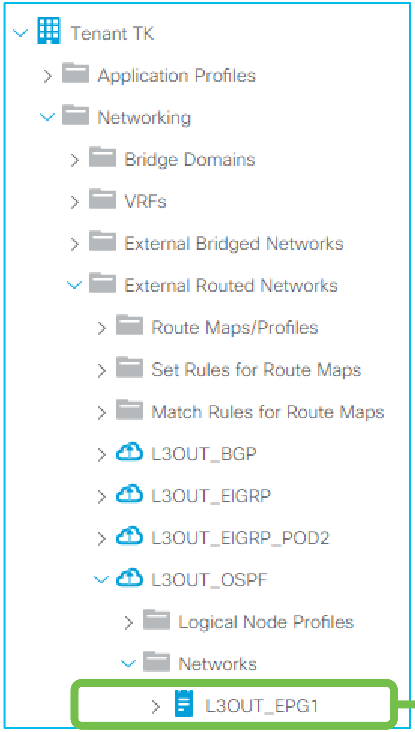
VRF	*subnet*	*pcTag*
VRF1	0.0.0.0/0	pcTag 15

source	*destination*	*Filter*
pcTag X	pcTag 15	ICMP
pcTag VRF	pcTag X	ICMP

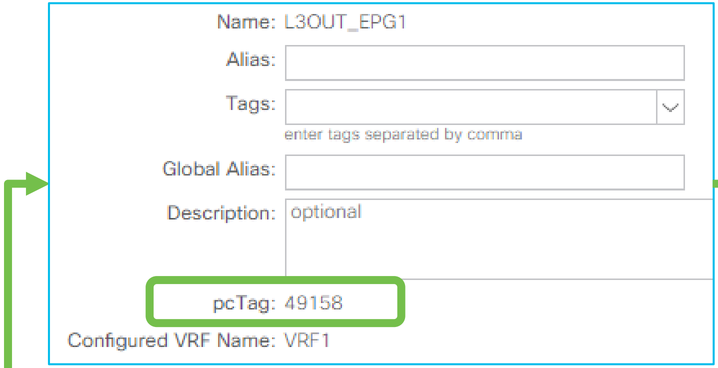
These contracts are from EPG X and L3Out A
However, traffic from/to Router B (20.0.0.0/8) will also hit these.

No duplication of External EPG L3Out subnets in the same VRF
Use 0.0.0.0/0 (External subnet for the external EPG) only for one L3Out EPG per VRF

How to verify prefix to pcTag mapping?



- Tenant TK
  - Application Profiles
  - Networking
    - Bridge Domains
    - VRFs
    - External Bridged Networks
    - External Routed Networks
      - Route Maps/Profiles
      - Set Rules for Route Maps
      - Match Rules for Route Maps
      - L3OUT_BGP
      - L3OUT_EIGRP
      - L3OUT_EIGRP_POD2
      - L3OUT_OSPF
        - Logical Node Profiles
        - Networks
          - L3OUT_EPG1



Name: L3OUT_EPG1

Alias:

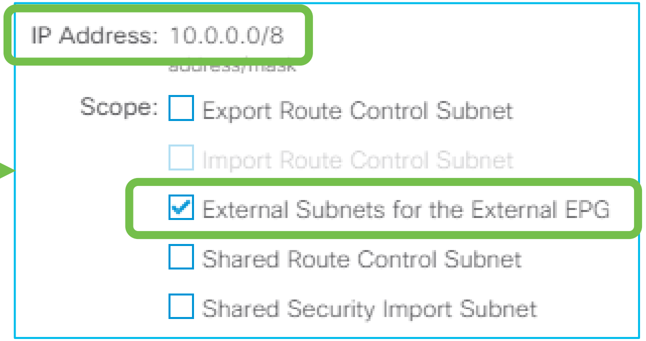
Tags: enter tags separated by comma

Global Alias:

Description: optional

pcTag: 49158

Configured VRF Name: VRF1



IP Address: 10.0.0.0/8 address/mask

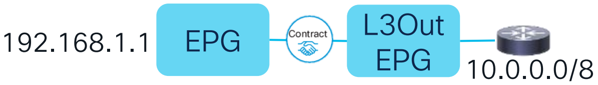
Scope:
- □ Export Route Control Subnet
- □ Import Route Control Subnet
- ☑ External Subnets for the External EPG
- □ Shared Route Control Subnet
- □ Shared Security Import Subnet

VRF1 – 10.0.0.0/8 => pcTag 49158

```
leaf# show zoning-prefixes | egrep 'TK:VRF1|Vrf|--'
+---------+-------------+-----------------+-------+-----------+
| Vrf-Vni |   Vrf-Name  |     Address     | Class | OperState |
+---------+-------------+-----------------+-------+-----------+
| 2097152 |   TK:VRF1   |    10.0.0.0/8   | 49158 |  enabled  |
| 2097152 |   TK:VRF1   |     0.0.0.0/0   |   15  |  enabled  |
+---------+-------------+-----------------+-------+-----------+
```

On older versions

```
leaf# vsh_lc -c 'show system internal aclqos prefix'
leaf# vsh –c ‘show sytem internal policy-mgr prefix’
```



CLI Verifications

1. Check if there are any contract drops

```
leaf# show logging ip access-list internal packet-log deny
[ Wed May  8 18:34:31 2019 155907 usecs]: CName: TK:VRF1(VXLAN: 2719744), VlanType: FD_VLAN, Vlan-Id: 26, SMac: 0x0050569185d1,
DMac:0x0022bdf819ff, SIP: 192.168.1.1, DIP: 10.0.0.1, SPort: 58968, DPort: 80, Src Intf: port-channel1, Proto: 6, PktLen: 74
```

Contract drops on this leaf show up in this command.
Check both ingress/egress leaves just in case,
or check hidden slides for Policy Control Enforcement Direction

2. Check the source (or destination) EPG pcTag

```
leaf# show system internal epm endpoint ip 192.168.1.1 | egrep
Vlan id : 30 ::: Vlan vnid : 9025 ::: VRF name : TK:VRF1
BD vnid : 16318374 ::: VRF vnid : 2097152
Flags : 0x80005c04 ::: sclass : 49100 ::: Ref count : 5
EP Flags : local|IP|MAC|host-tracked|sclass|timer|
```

If your source/destination is an endpoint, it should be in here.
sclass = pcTag = EPG ID for contract

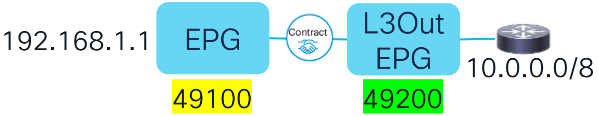
This pcTag takes precedence over “prefix-pcTag mapping table” unless the prefix is /32 or /128.
Make sure the external IP is not here. If it is, check the traffic path that caused ACI to learn the external IP as an endpoint.

3. Check the destination (or source) L3Out external EPG pcTag

```
leaf# show zoning-prefixes | egrep 'TK:VRF1|Vrf|--'
+---------+-------------+-----------------+-------+-----------+
| Vrf-Vni |   Vrf-Name  |     Address     | Class | OperState |
+---------+-------------+-----------------+-------+-----------+
| 2097152 |   TK:VRF1   |   10.0.0.0/8    | 49200 |  enabled  |
| 2097152 |   TK:VRF1   |    0.0.0.0/0    |   15  |  enabled  |
+---------+-------------+-----------------+-------+-----------+
```

“External Subnet for the External EPG” config is reflected here.
This is Longest Prefix Match.

CLI Verifications



4. Check contracts between two pcTags

```
leaf# show zoning-rule scope 2097152 | egrep 'Rule|49100|49200|--'
+---------+---------+---------+----------+----------------+---------+--------------+---------+----------------+
| Rule ID | SrcEPG  | DstEPG  | FilterID |      Dir       |  Scope  |     Name     | Action  |    Priority    |
+---------+---------+---------+----------+----------------+---------+--------------+---------+----------------+
|   4165  |  49100  |  49200  |    5     |     bi-dir     | 2097152 |  common:ICMP |  permit | fully_qual(7)  |
|   4287  |  49200  |  49100  |    5     | uni-dir-ignore | 2097152 |  common:ICMP |  permit | fully_qual(7)  |
+---------+---------+---------+----------+----------------+---------+--------------+---------+----------------+
```

scope = VRF VNID

```
leaf# show zoning-filter filter 5
+----------+----------+----------+-------------+----------+-------------+-------------+-------------+-------------+
| FilterId |   Name   |  EtherT  |   ArpOpc    |   Prot   |  SFromPort  |   SToPort   |  DFromPort  |   DToPort   |
+----------+----------+----------+-------------+----------+-------------+-------------+-------------+-------------+
|    5     |   5_0    |    ip    | unspecified |   icmp   | unspecified | unspecified | unspecified | unspecified |
+----------+----------+----------+-------------+----------+-------------+-------------+-------------+-------------+
```

5. Built-in contract parser for more details with stats

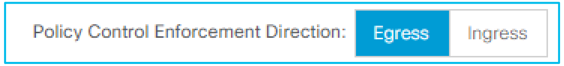
```
leaf# contract_parser.py --vrf TK:VRFA --epg 49100

[7:4165] [vrf:TK:VRFA] permit ipv4 icmp tn-TK/ap-AP1/epg-EPGA(49100) tn-TK/l3out-BGP/instP-EPGB(49200) [contract:uni/tn-TK/brc-
ICMP] [hit=4]
[7:4287] [vrf:TK:VRFA] permit ipv4 icmp tn-TK/l3out-BGP/instP-EPGB(49200) tn-TK/ap-AP1/epg-EPGA(49100) [contract:uni/tn-TK/brc-
ICMP] [hit=1]
```

L3Out Contract

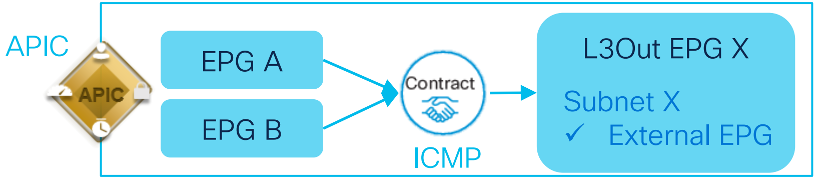
Policy Control Enforcement Direction

Under VRF



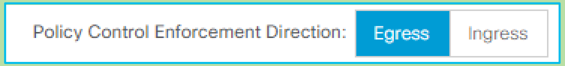
Policy Control Enforcement Direction: [✓ Egress] Ingress

A feature to save contract TCAM usage on border LEAF



No effects on EPG <-> EPG traffic

Egress Policy Enforcement



Policy Control Enforcement Direction: [✓ Egress] Ingress

Non-Border LEAF(s)

with EPG A

source	*destination*	*Filter*
pcTag A	pcTag X	ICMP

with EPG B

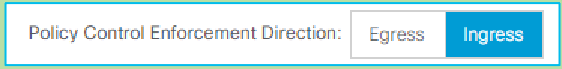
source	*destination*	*Filter*
pcTag B	pcTag X	ICMP

Border LEAF(s)

source	*destination*	*Filter*
pcTag A	pcTag X	ICMP
pcTag B	pcTag X	ICMP

Ingress Policy Enforcement

default from 1.2



Policy Control Enforcement Direction: Egress [✓ Ingress]

Non-Border LEAF(s)

with EPG A

source	*destination*	*Filter*
pcTag A	pcTag X	ICMP

with EPG B

source	*destination*	*Filter*
pcTag B	pcTag X	ICMP

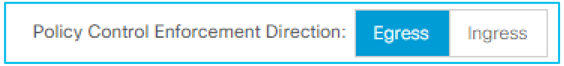
Border LEAF(s)

source	*destination*	*Filter*
- none -		

L3Out Contract

Policy Control Enforcement Direction

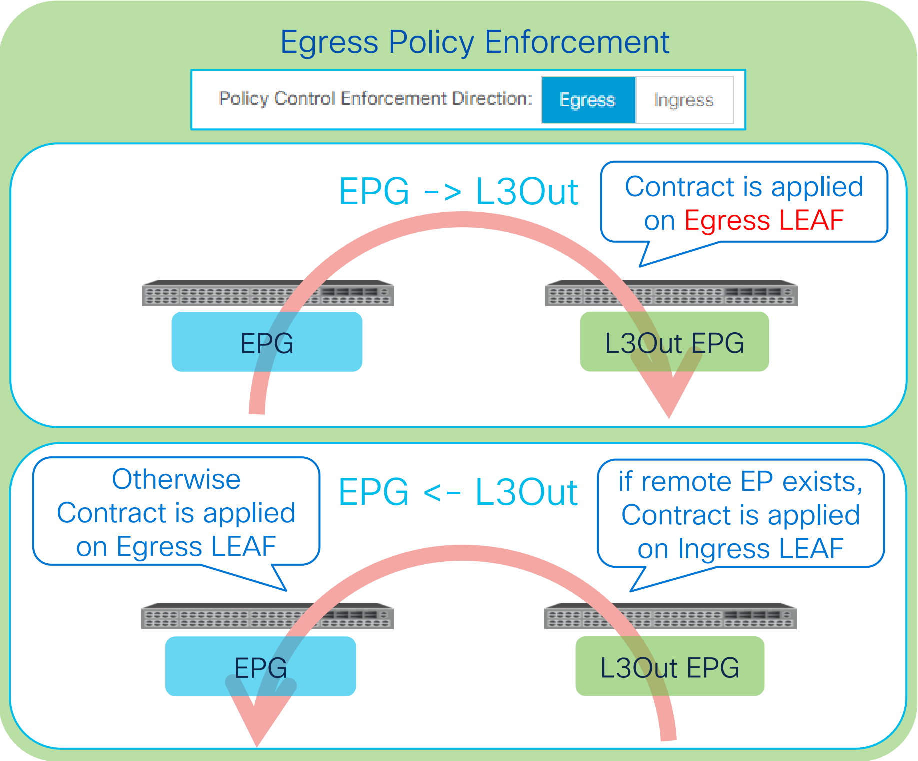
Under VRF



Policy Control Enforcement Direction: [✓ Egress] Ingress

How does it affect traffic flow and contract?

Egress Policy Enforcement



Policy Control Enforcement Direction: [✓ Egress] Ingress

EPG -> L3Out

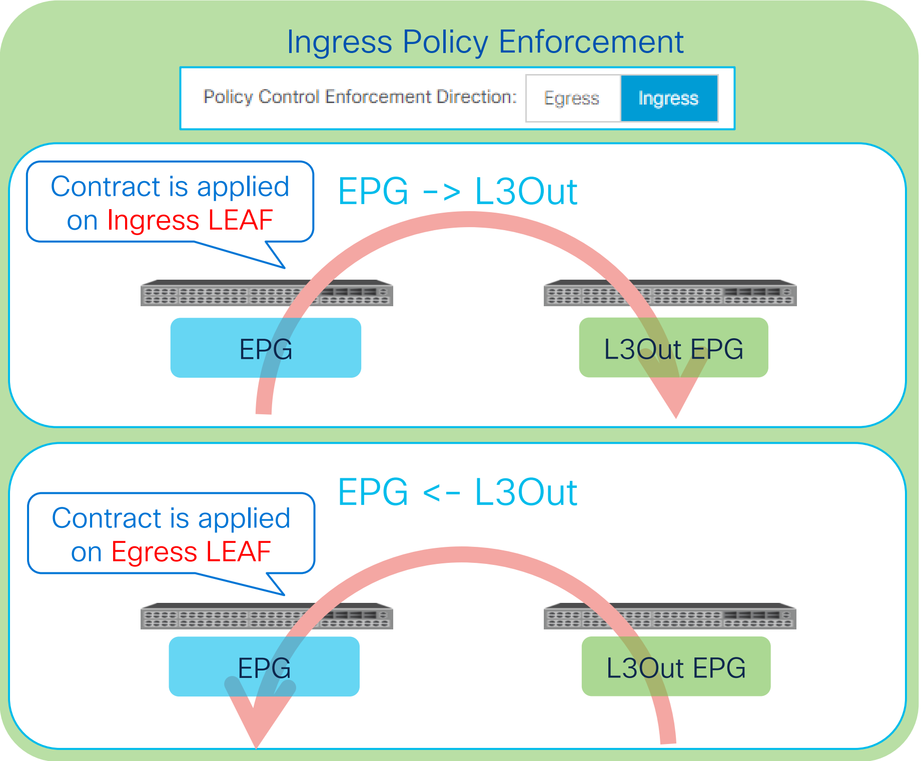
Contract is applied on Egress LEAF

EPG <- L3Out

Otherwise Contract is applied on Egress LEAF

if remote EP exists, Contract is applied on Ingress LEAF

Ingress Policy Enforcement



Policy Control Enforcement Direction: Egress [✓ Ingress]

EPG -> L3Out

Contract is applied on Ingress LEAF

EPG <- L3Out

Contract is applied on Egress LEAF

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

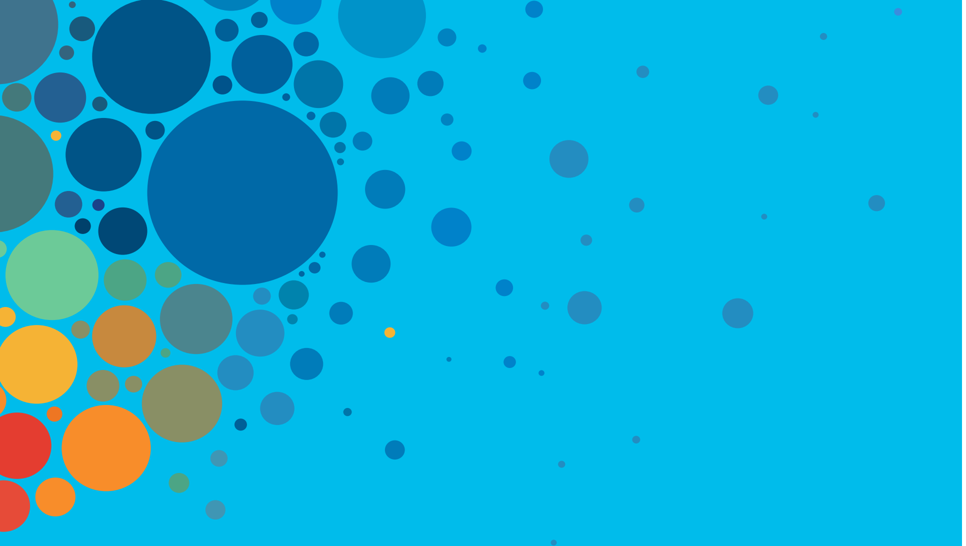
Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**



Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

The bridge to possible

Thank you

cisco Live!

#CiscoLive