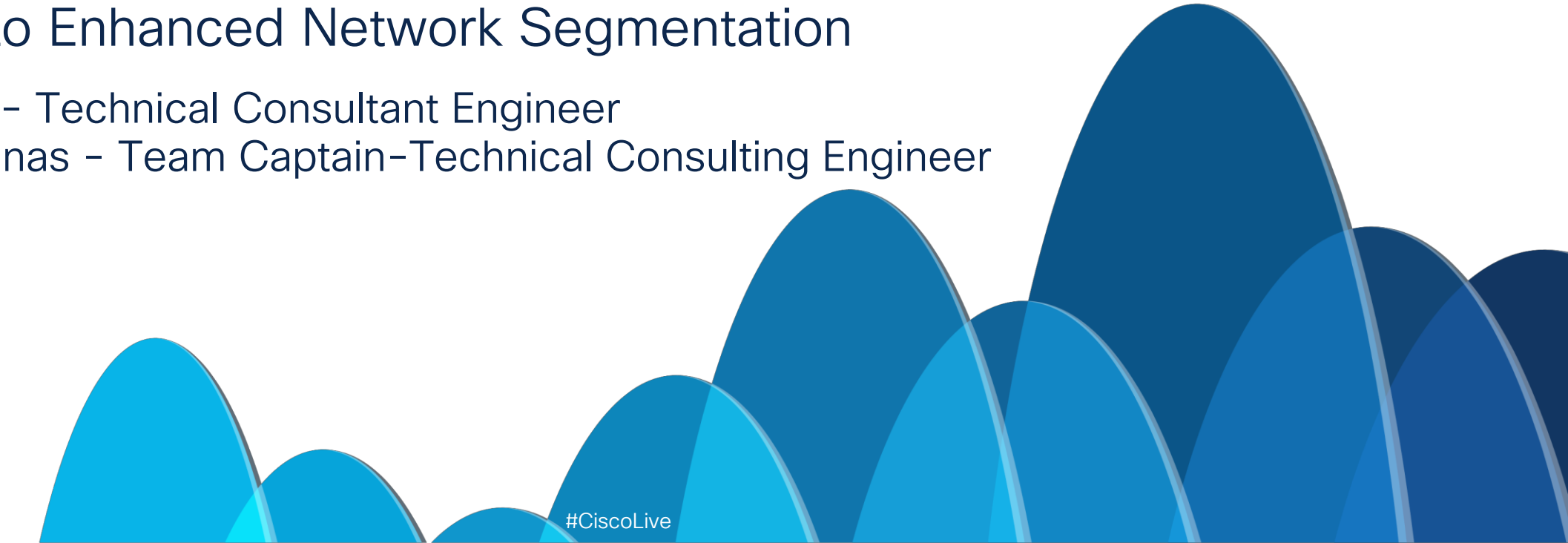
The bridge to possible

SDA: Deploying and Troubleshooting LISP Extranet (Single Site)

A Guide to Enhanced Network Segmentation

Marcus Hill – Technical Consultant Engineer
Diego Cabanas – Team Captain-Technical Consulting Engineer

TACENT-2010



cisco Live!

#CiscoLive

Agenda

- Overview of LISP Extranet in SDA
- Deploying LISP Extranet Step-by-Step
- Troubleshooting Tips
  - South-North
  - North-South
- Configuration Guidelines
- Summary and Q&A

The bridge to possible

Overview of LISP Extranet in SDA

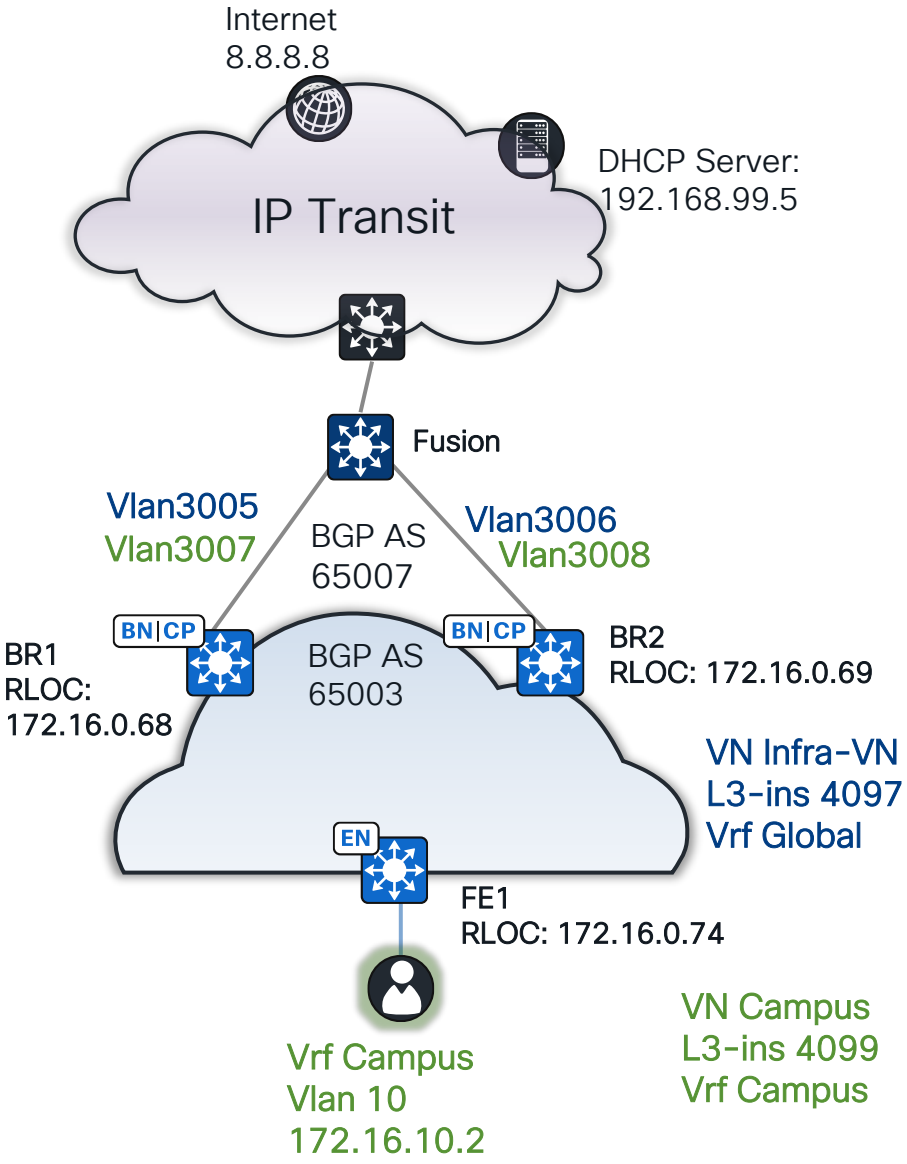
cisco Live!

#CiscoLive

Introduction to LISP Extranet

Current Deployment Challenges

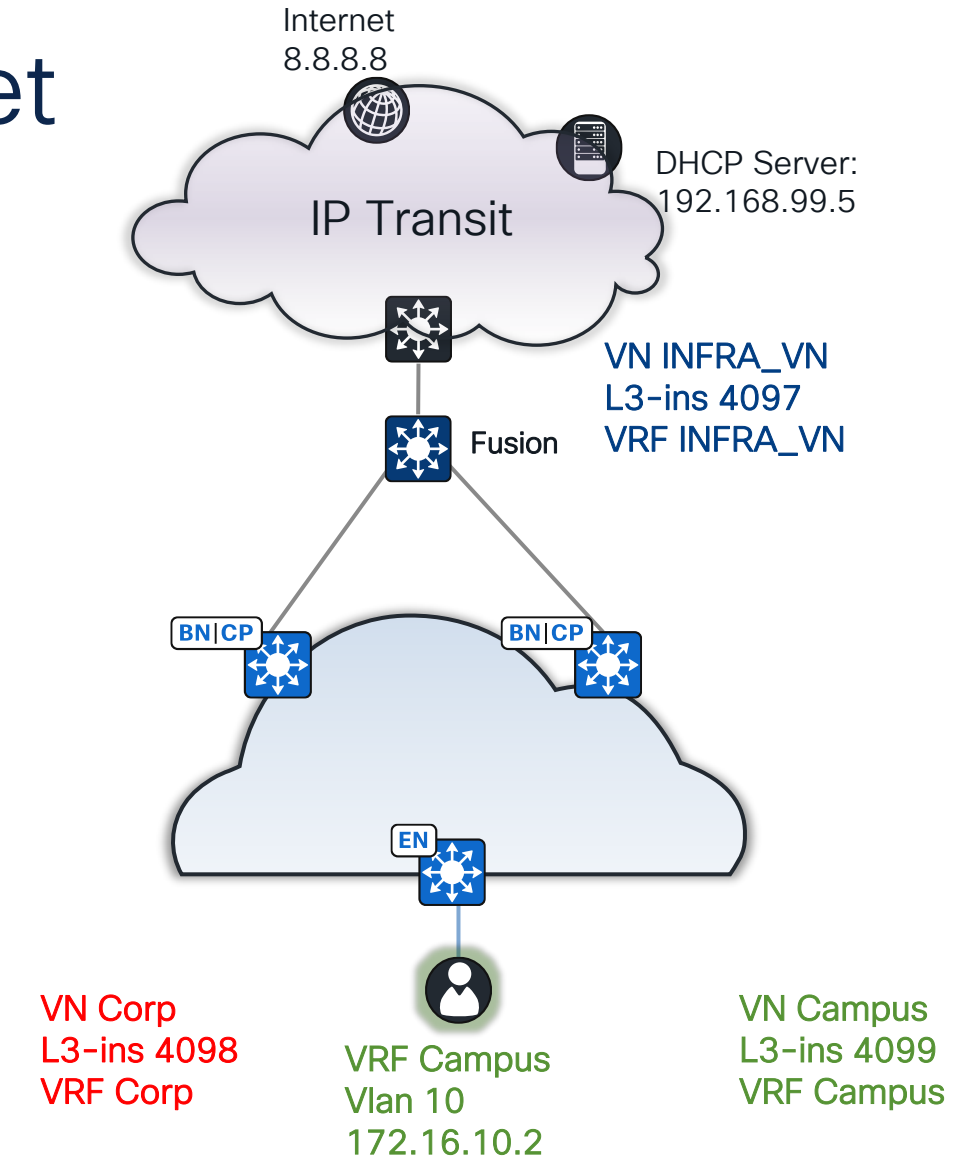
- For configurations involving Route Leaking, a fusion router is required; this component can add a layer of complexity to the setup.
- Peer devices may be subject to constraints in available resources.
- Fusion router is an additionally MANUAL configuration that needs to be maintained.



Introduction to LISP Extranet

How does LISP Extranet enhance SDA Fabric?

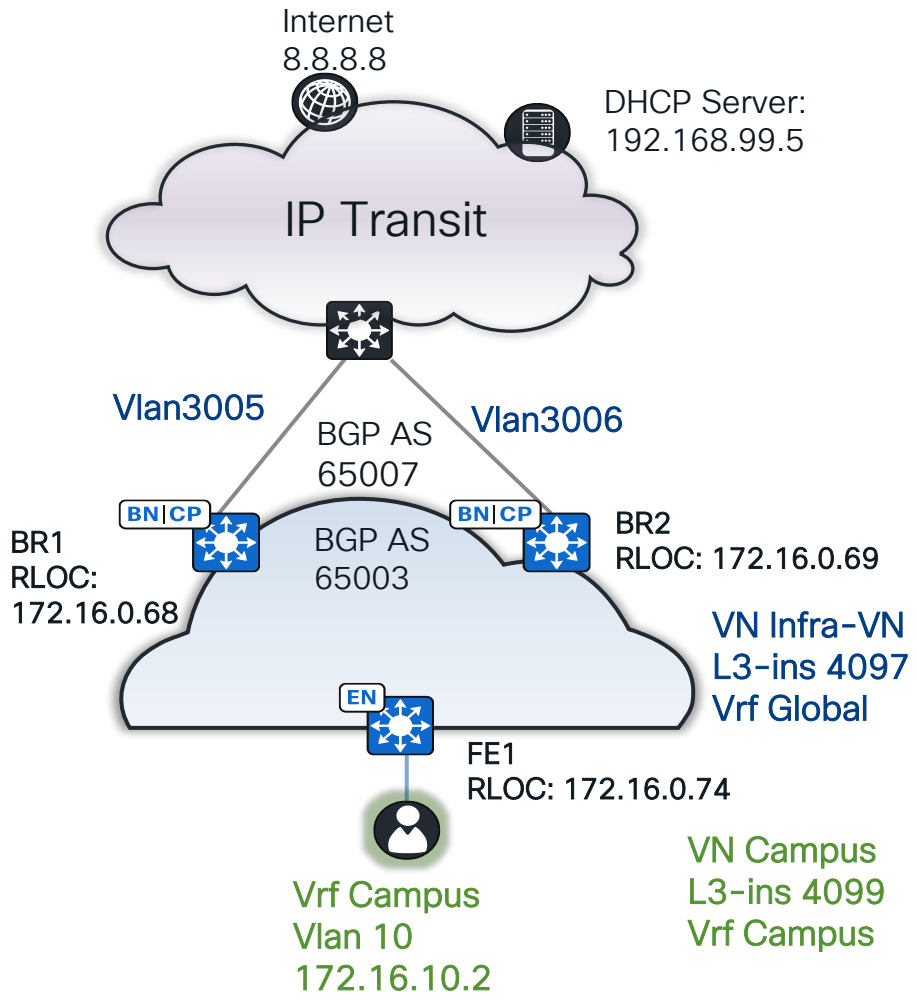
- Provider VN:
  - Target VN for Route-Leaking (INFRA_VN)
  - Policy-driven connection of INFRA_VN (GRT) to Fabric VNs.
- Subscriber VN:
  - VN that subscribes to the provider for shared services
  - Subscriber VN: Tenants to the Provider VN (CAMPUS_VN, CORP_VN)

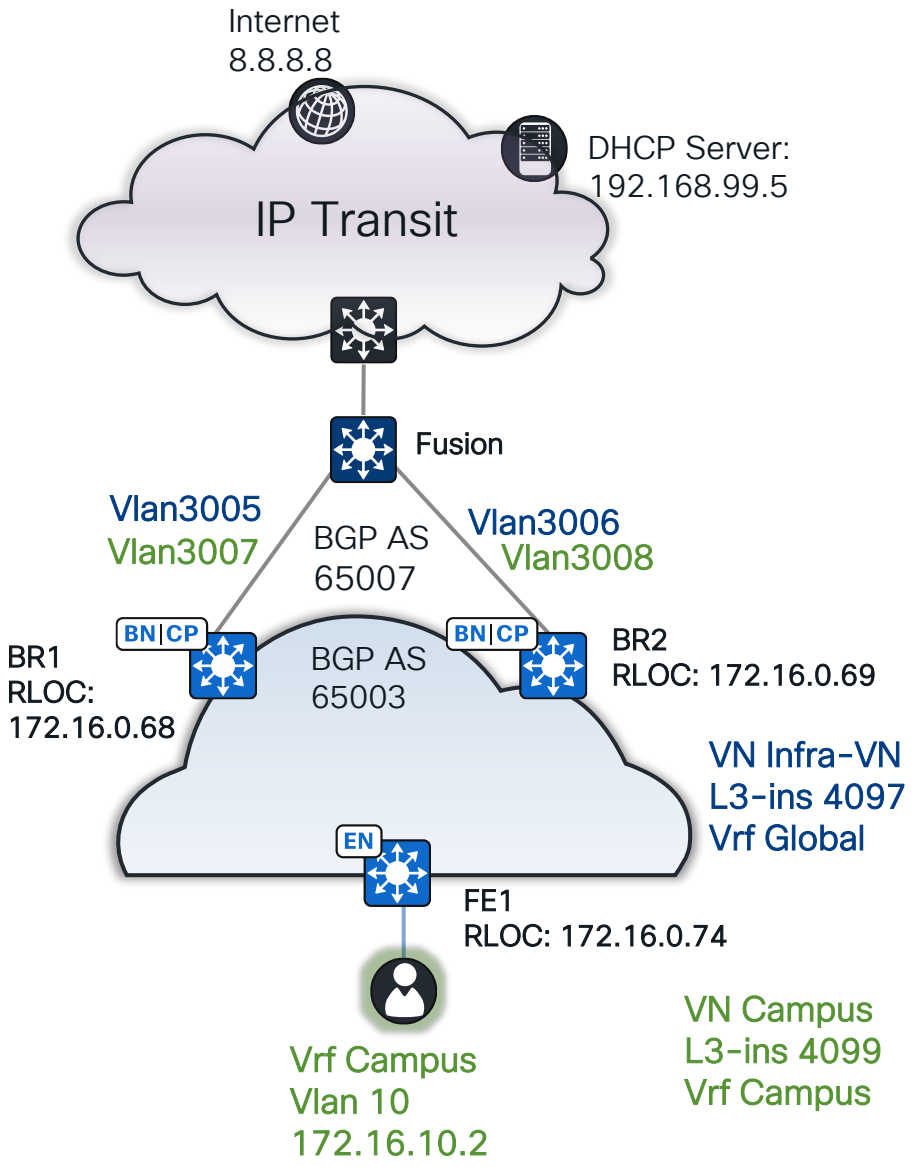


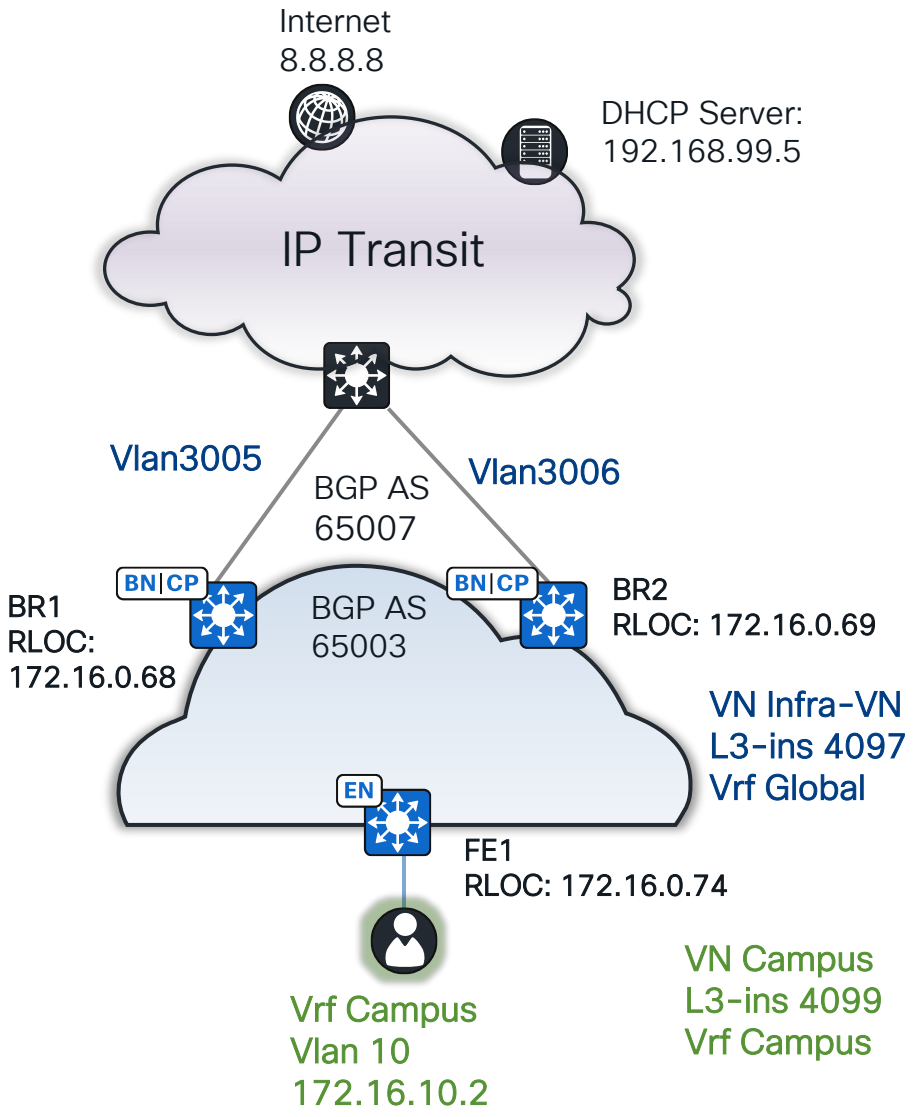
Introduction to LISP Extranet

Enhanced Network Management with Policy-Based Routing in SDA Extranet

- **Traditional LISP:**
  - Route Leaking performed outside of the fabric (Fusion)
- **Extranet LISP:**
  - Route Leaking Performed inside the Fabric (LISP CP)
- **SDA Extranet Benefits**
  - CatC pushed configurations for Route Leaking
  - Less complex configurations to maintain







The bridge to possible

Deploying LISP Extranet

cisco Live!

#CiscoLive

Deploying LISP Extranet

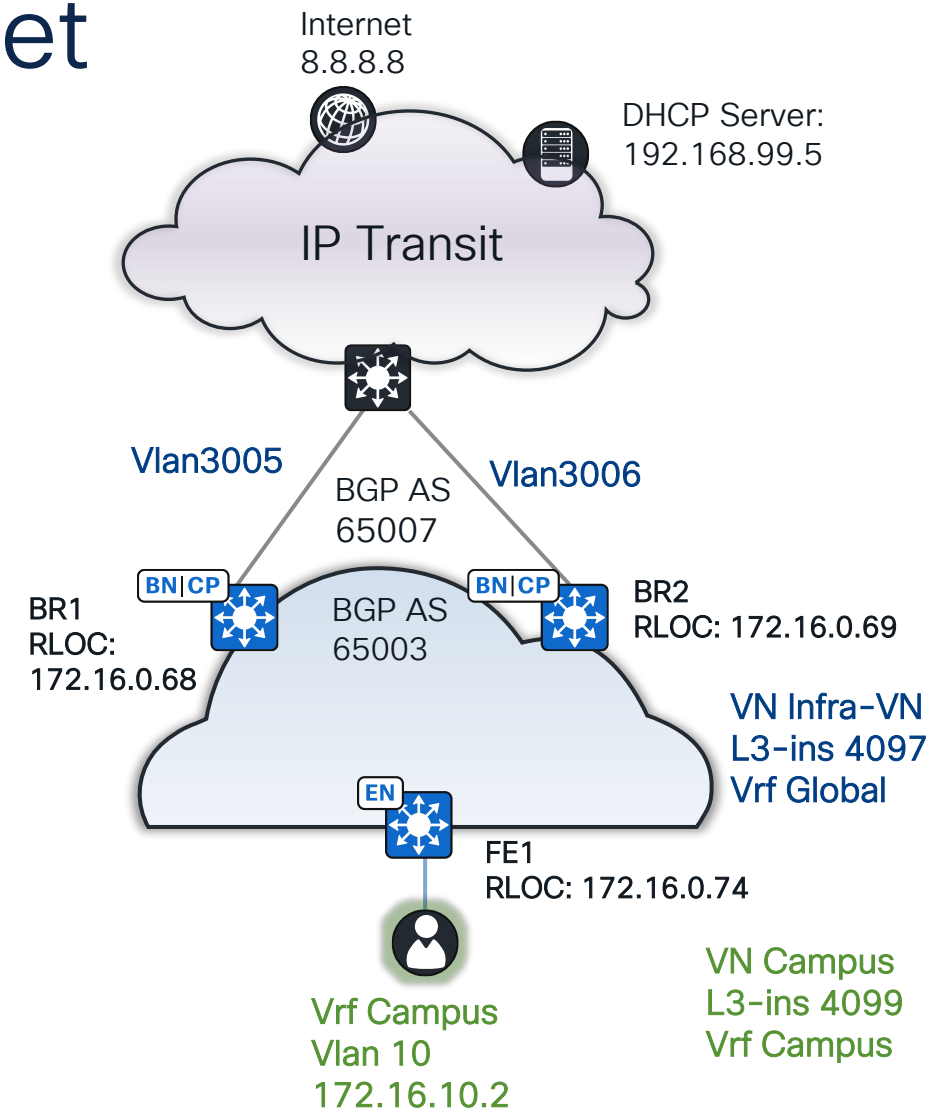
Topology:

- Provider VN

Infra-VN

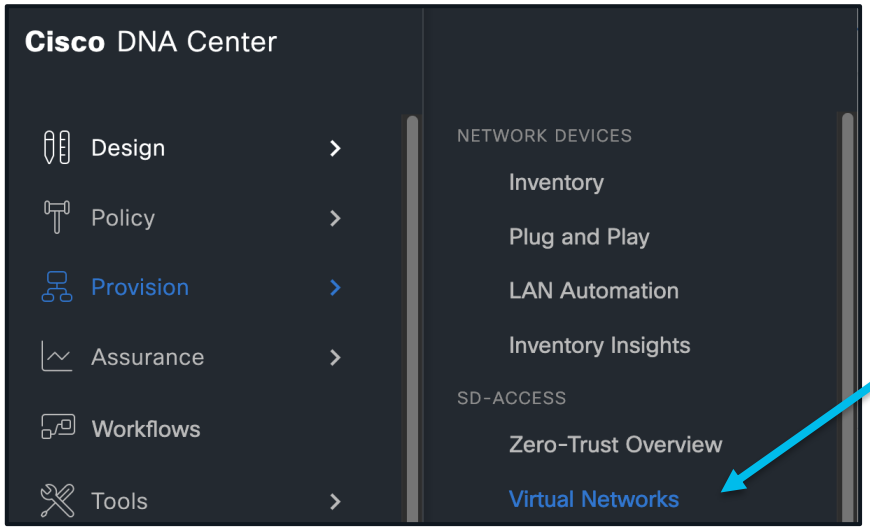
- Subscriber VN

Campus



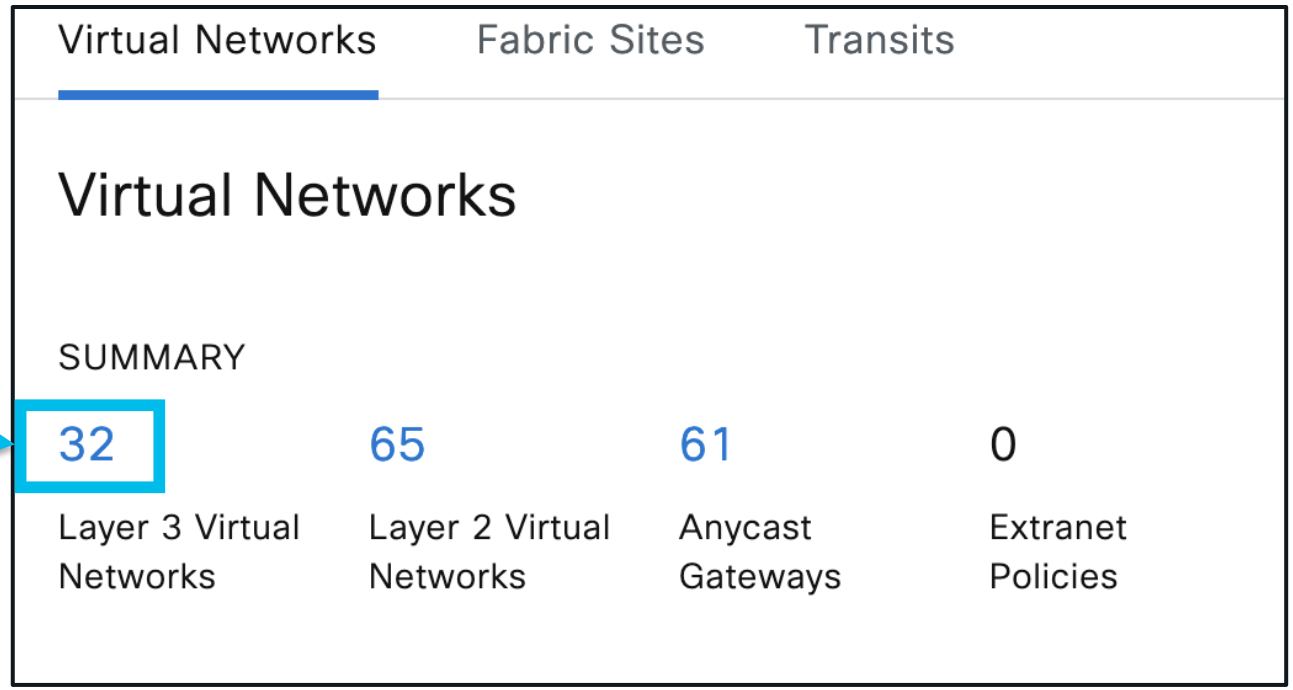
Deploying LISP Extranet Step-by-Step

1. Start the Extranet policy flow



- After you have already created your Virtual network and prerequisites for the Fabric. In the Cisco Catalyst Center, navigate to Provision > Virtual network.

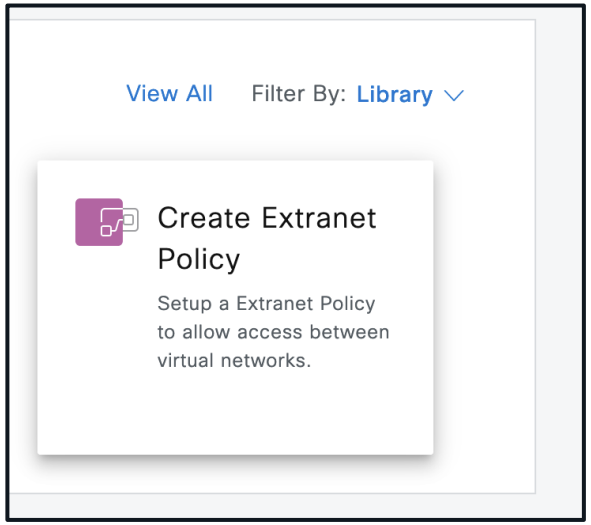
- Click on the blue number for your current Layer 3 Virtual Networks.

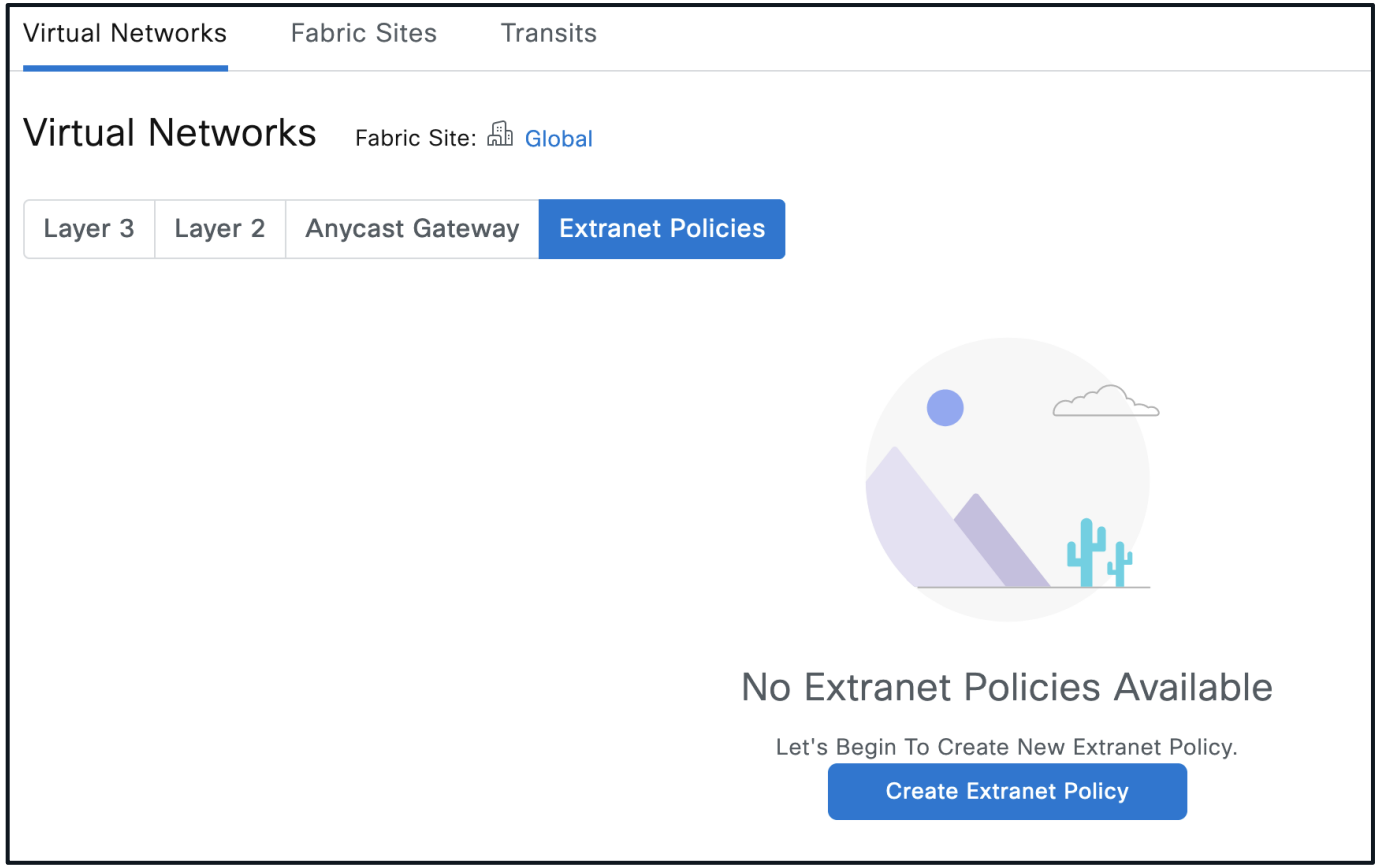


Deploying LISP Extranet Step-by-Step

1. Start the Extranet policy flow

- Go to the Extranet Policies Tab and click on Create Extranet Policy

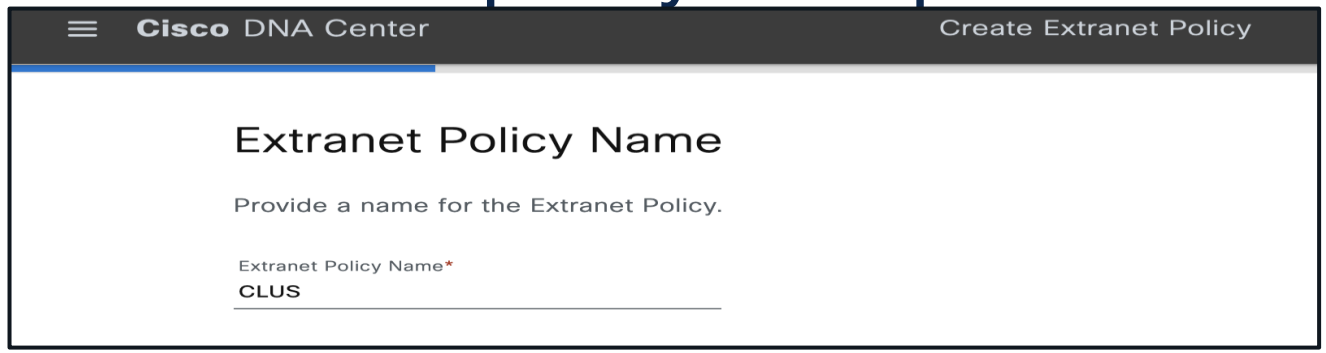


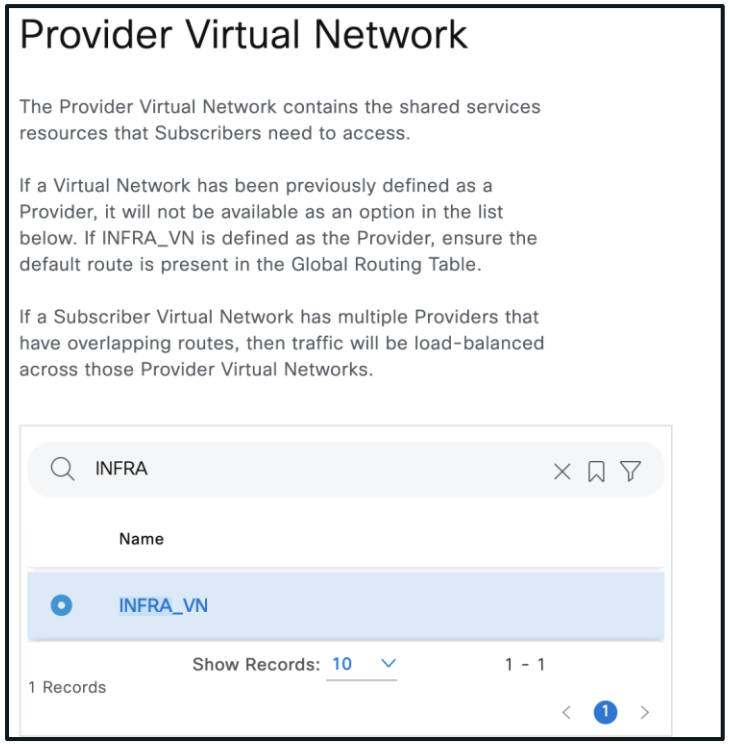


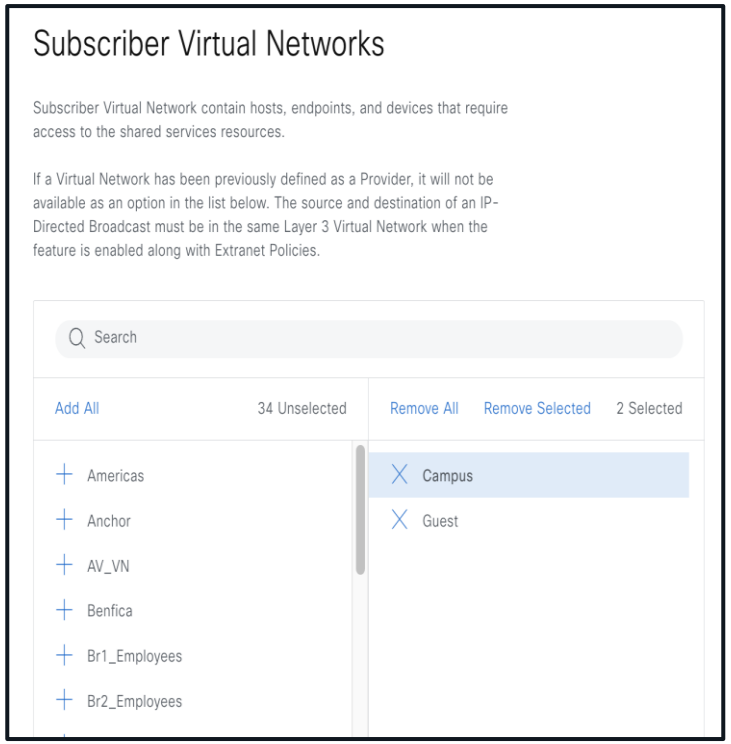
Deploying LISP Extranet Step-by-Step

2. Virtual Network definition type

1. Add the name to identify your policy
2. Select the Provider Network, in our case we are using the global routing table as the provider VN and we select the INFRA_VN.
3. Then select the Subscriber Virtual Networks that we want to communicate with the provider Campus.



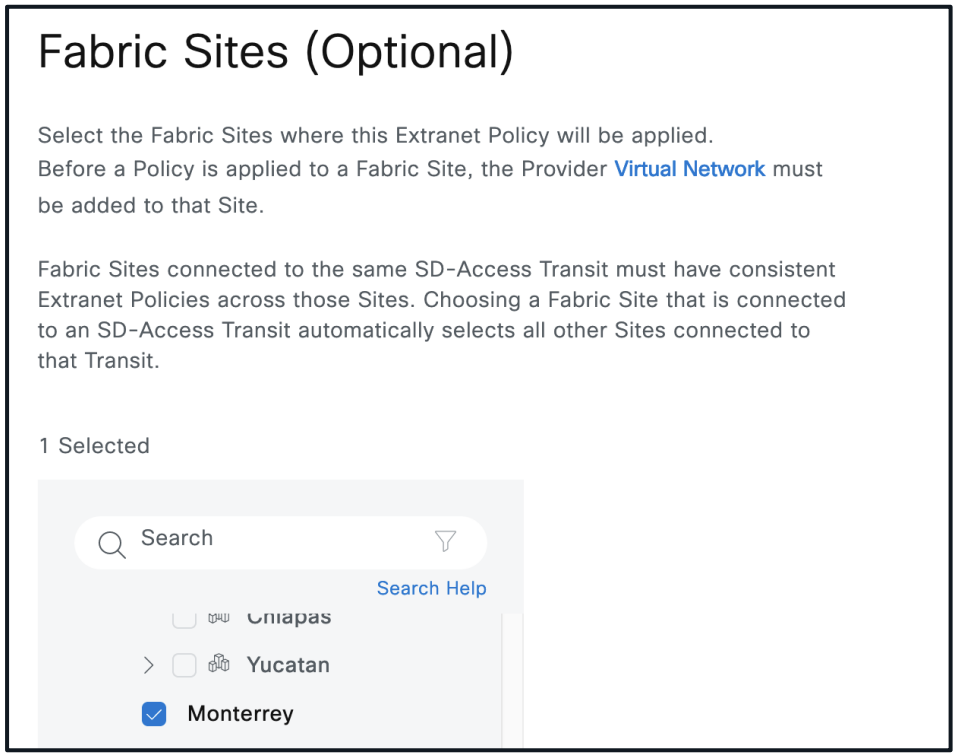


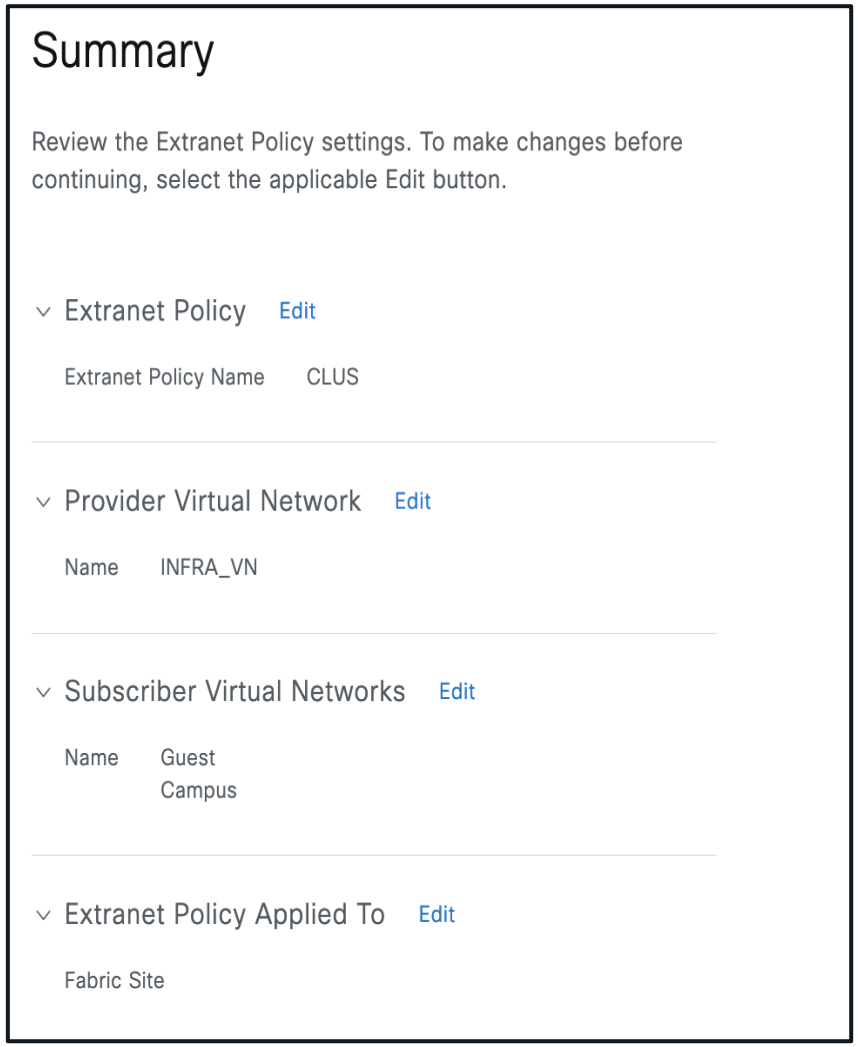


Deploying LISP Extranet Step-by-Step

3. Assign the Extranet Policy and verify the summary

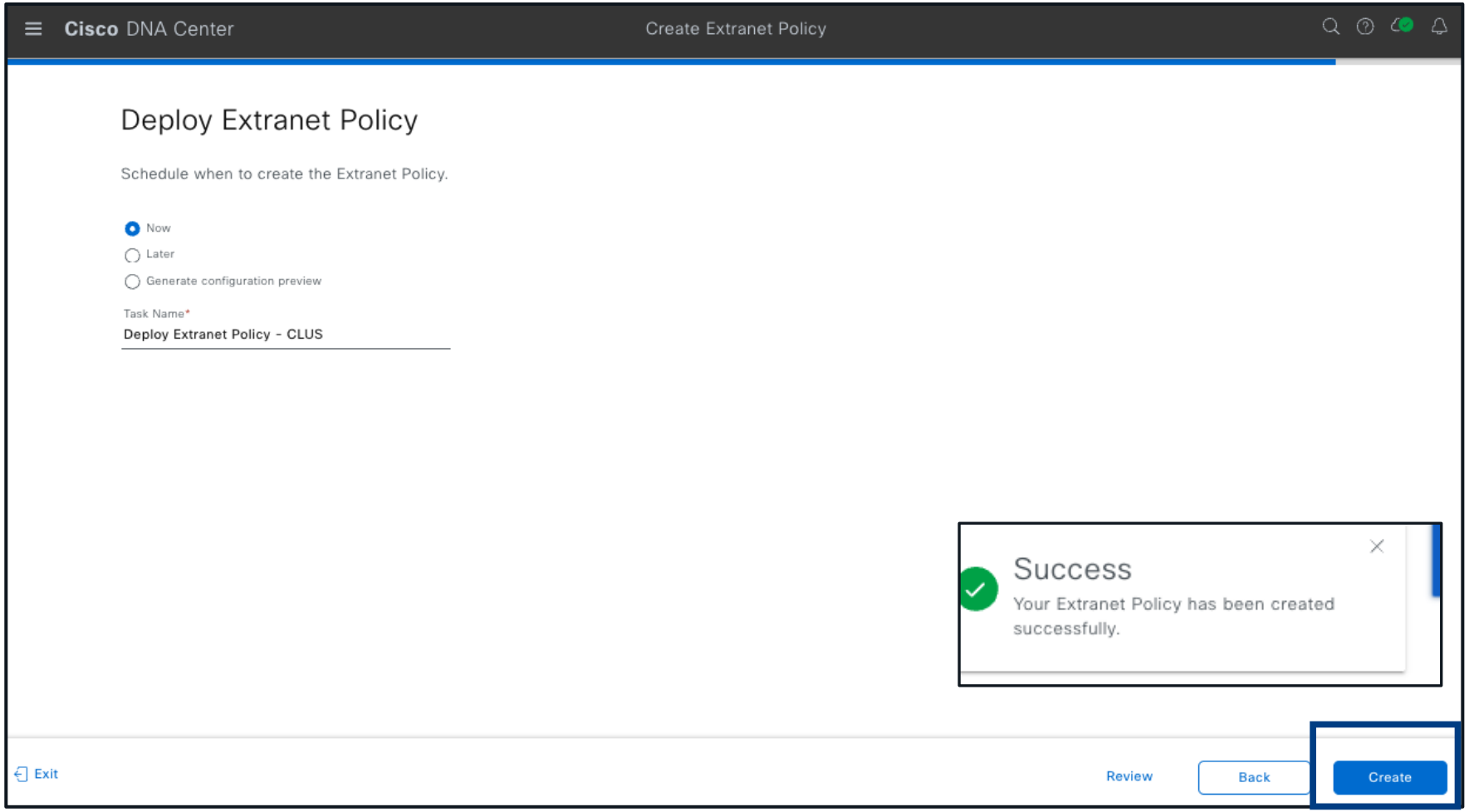
3. Select the Fabric Sites where the Extranet policy is going to be applied.





Deploying LISP Extranet Step-by-Step

4. Create the Extranet Policy



Deploying LISP Extranet

What is configured with the previous flow in the Border nodes?

1. Policy map attached to the Provider VN L3 handoff Vlan and LISP interface:

```
interface vlan3005
 ip policy route-map EXTRANET_MATCH_SUBSCRIBER_V4
interface LISP0.4097
 ip policy route-map EXTRANET_MATCH_SUBSCRIBER_V4
```

2. Create loopbacks for the anycast gateway for the Subscriber VNs in the Provider VN.

```
interface Loopback4990
 description Loopback Border
 ip address 172.16.10.1 255.255.255.255 ← Anycast Gateway
```

3. ACL to match the Fabric subnets for the Subscriber VN.

```
ip access-list extended EXTRANET_Campus_IPV4_ACL
 10 deny ip any host 172.16.10.1 ← Anycast Gateway for Campus
 20 permit ip any 172.16.10.0 0.0.0.255 ← VN Campus subnets
exit
```

Deploying LISP Extranet

What is configured with the previous flow in the Border nodes?

4. Route-maps are used to set the proper vrf according to the routing required.

```
route-map EXTRANET_MATCH_SUBSCRIBER_V4 permit 30
 description Match IPV4 ACL and set Vrf
 match ip address EXTRANET_Campus_IPV4_ACL
 set vrf Campus
```

5. Include the summarization for the Subscriber VN subnets in the provider VN BGP section.

```
router bgp 65003
 address-family ipv4 ←Infra_VN vrf global
 aggregate-address 172.16.10.0 255.255.255.0 summary-only ← vrf Campus subnet
<snipped>
 network 172.16.10.1 mask 255.255.255.255 ← Campus anycast Gateway
```

Deploying LISP Extranet

What is configured with the previous flow in the Control Plane?

6. Include the router lisp configuration for extranet.

```
router lisp
site site_uci
 [omitted]
  extranet CLUS
 eid-record-provider instance-id 4097 <- INFRA_VN
  172.16.4.0/24 <- Extended Node Pool
  172.16.5.0/24 <- AP Pool
  ip-any
  exit-eid-record-provider
 eid-record-subscriber instance-id 4099 <- CAMPUS_VN
  172.16.10.0/24
  ip-any
  exit-eid-record-subscriber
```

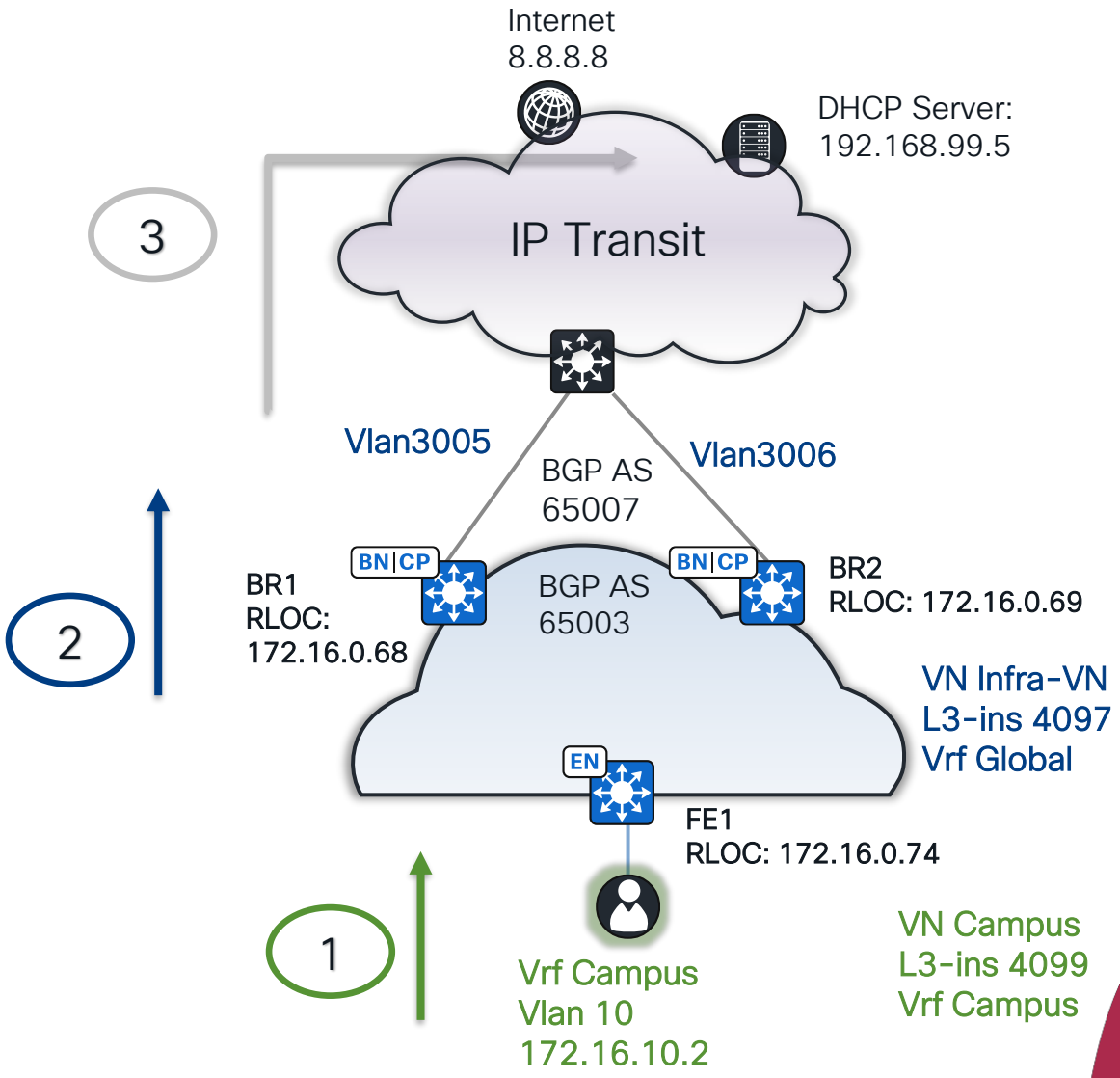
The bridge to possible

Troubleshooting LISP Extranet

cisco Live!

#CiscoLive

South-North flow



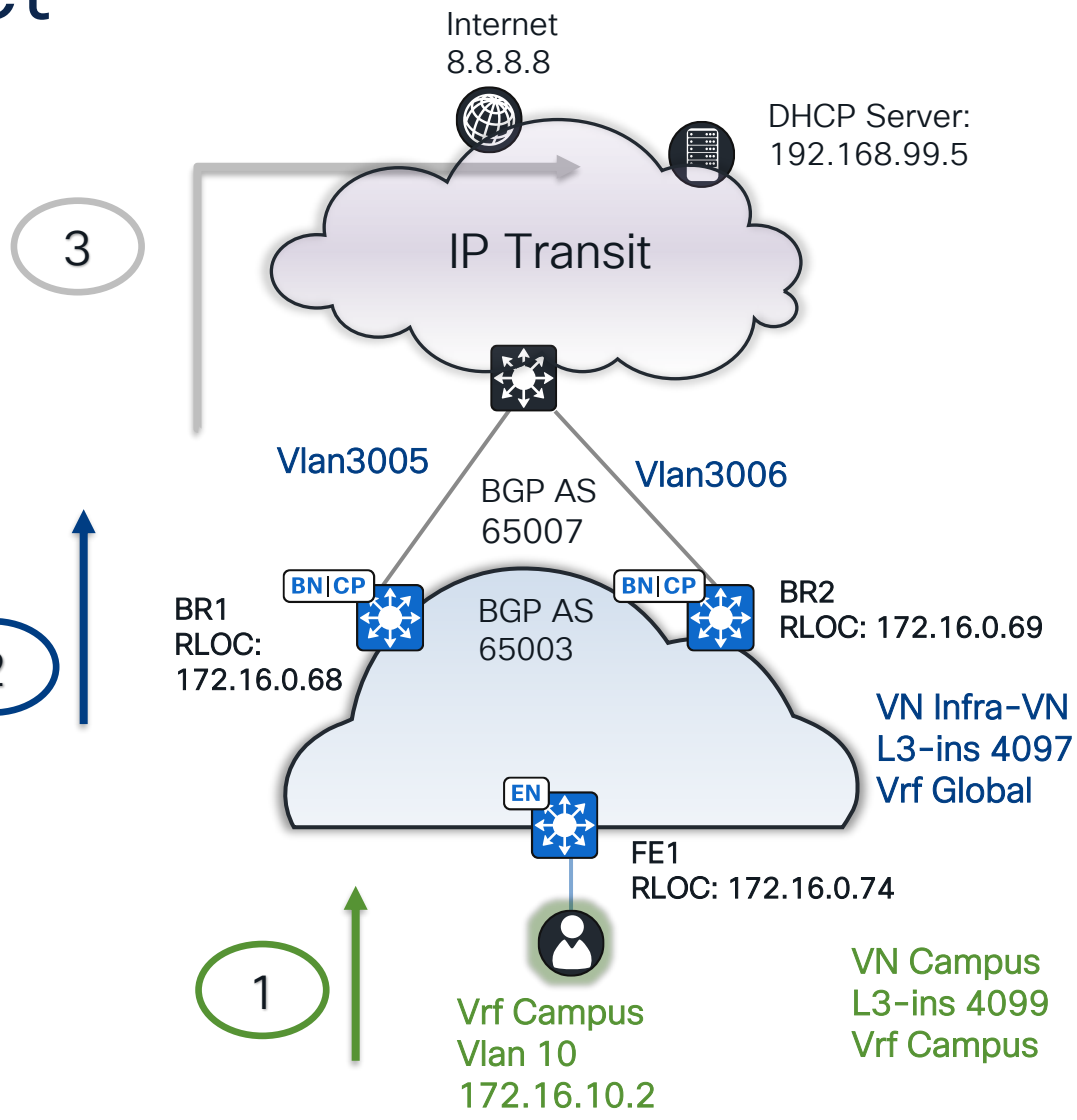
Troubleshooting LISP Extranet

South-North 172.16.10.2 to 192.168.99.5

```
02.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 3005
nternet Protocol Version 4, Src: 172.16.10.2, Dst: 192.168.99.5
nternet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
```

```
nternet Protocol Version 4, Src: 172.16.0.74, Dst: 172.16.0.68
rtual eXtensible Local Area Network
 Flags: 0x8800, GBP Extension, VXLAN Network ID (VNI)
 Group Policy ID: 0
 VXLAN Network Identifier (VNI): 4097
 Reserved: 0
nternet Protocol Version 4, Src: 172.16.10.2, Dst: 192.168.99.5
nternet Control Message Protocol
 Type: 8 (Echo (ping) request)
 Code: 0
```

```
> Internet Protocol Version 4, Src: 172.16.10.2, Dst: 192.168.99.5
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
```



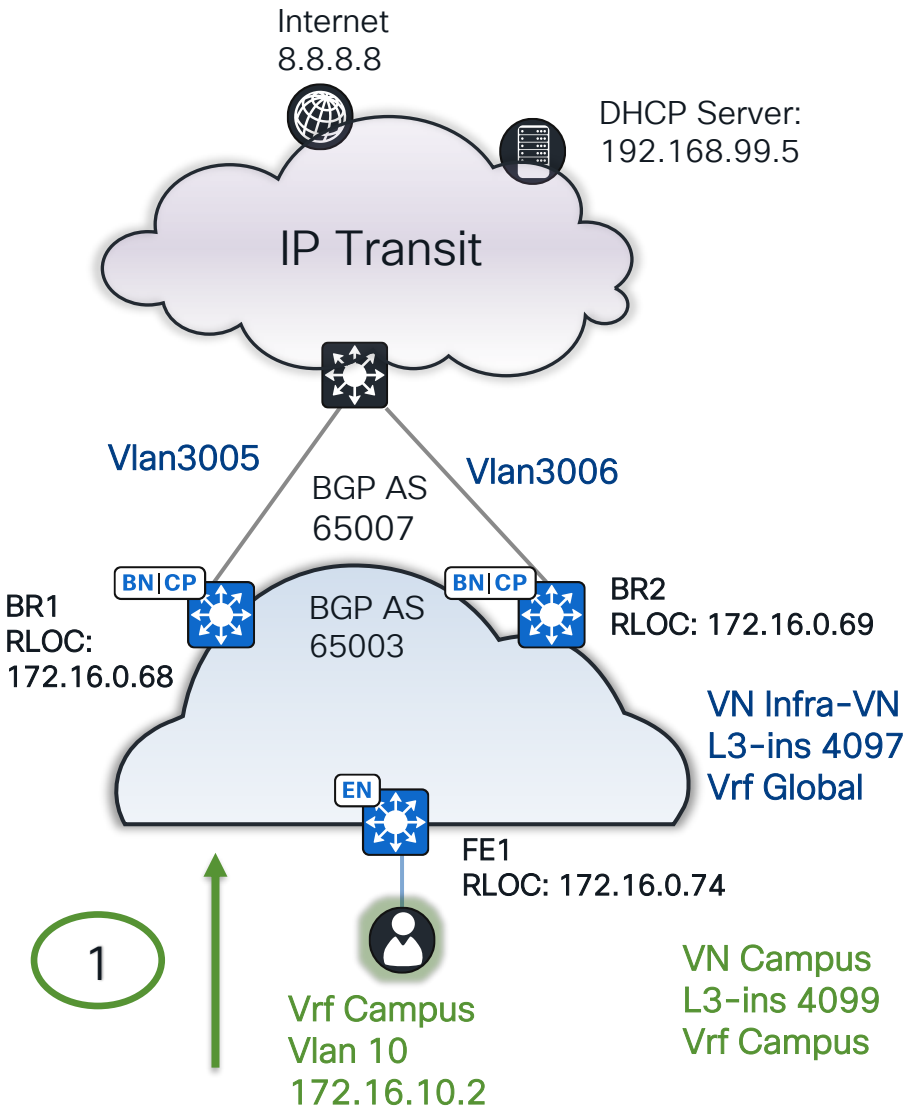
Troubleshooting LISP Extranet

South-North 172.16.10.2 to 192.168.99.5

```
Edge#show device-tracking database address 172.16.10.2
[snipped]
Network Layer Address Link Layer Address Interface vlan prlvl age state    Time
left
DH4 172.16.10.2       7c4d.8f0c.f102     Gi1/0/3   10   0024  1s REACHABLE  250
s try 0(170155 s)

Edge#show ip vrf
  Name                              Default RD            Interfaces
  Campus                            <not set>             LI0.4099
                                                          Vl10


Edge#show lisp instance-id 4099 ipv4 database 172.16.10.2/32
LISP ETR IPv4 Mapping Database for LISP 0 EID-table vrf Campus (IID 4099),
<snipped>
172.16.10.2/32, dynamic-eid Data-IPV4, inherited from default locator-set
rloc_94ab4c50-688c-45fc-892a-cd7ca60c0dae
<snipped>
  Locator       Pri/Wgt  Source     State
  172.16.0.74    10/10   cfg-intf   site-self, reachable
  Map-server        Uptime          ACK  Domain-ID
  172.16.0.68       00:49:23        Yes  0
  172.16.0.69       00:49:23        Yes  0
```



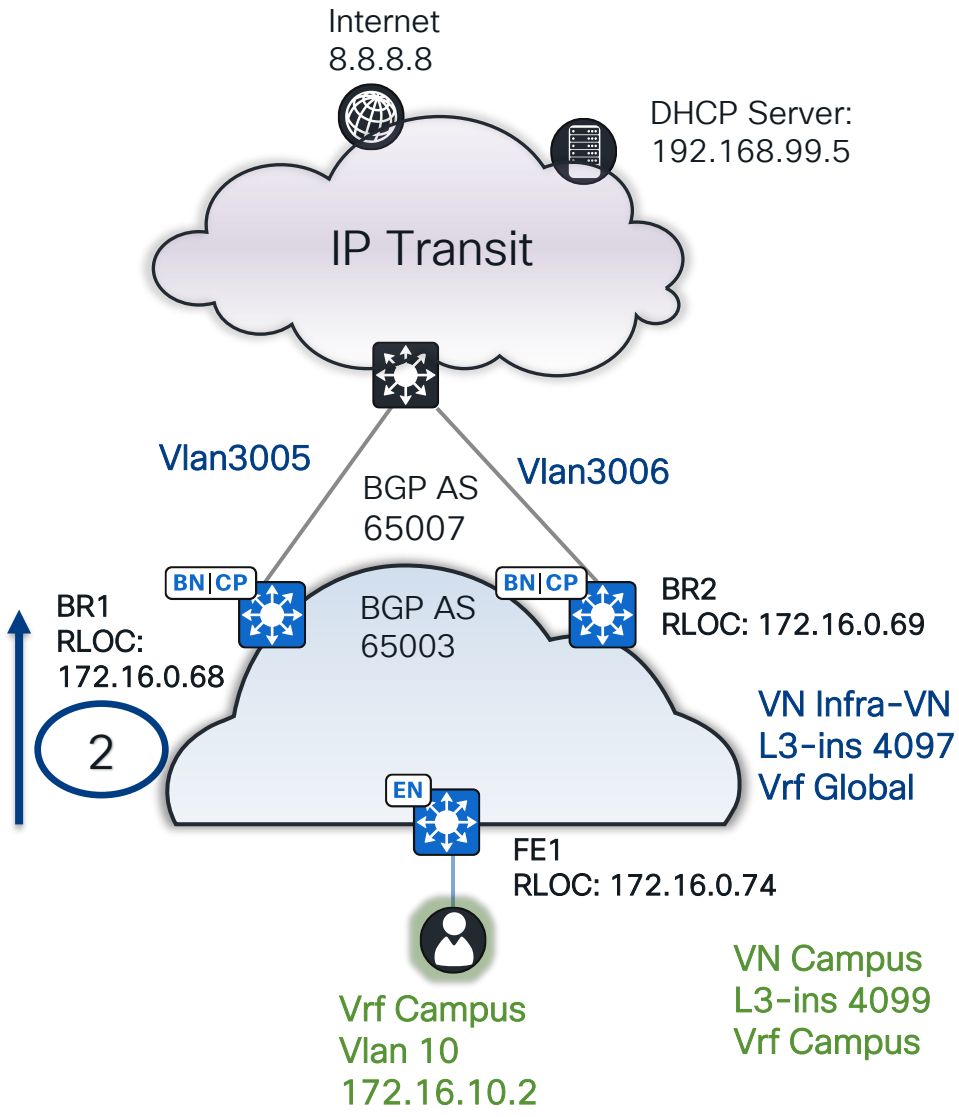
Troubleshooting LISP Extranet

South-North 172.16.10.2 to 192.168.99.5

```
Edge# show ip route vrf Campus 192.168.99.5
Routing Table: Campus
% Network not in table

Edge# show ip cef vrf Campus 192.168.99.5
192.0.0.0/2
  nexthop 172.16.0.68 LISP0.4099
  nexthop 172.16.0.69 LISP0.4099

Edge# show lisp instance-id 4099 ipv4 map-cache 192.168.99.5
LISP IPv4 Mapping Cache for LISP 0 EID-table vrf Campus (IID 4099), 1 entries
192.0.0.0/2, uptime: 01:14:06, expires: 00:13:41, via map-reply, unknown-eid-
forward
  Sources: map-reply
  State: unknown-eid-forward, last modified: 01:03:17, map-source:
172.16.0.68
  Active, Packets out: 791(264398 bytes), counters are not accurate (~
00:00:06 ago)
  PETR         Uptime    State      Pri/Wgt  Encap-IID   Domain-ID/MH-ID
Metric
  172.16.0.68  01:03:17  admin-down 255/10   -           2136580547/41411  -
  172.16.0.68  01:03:17  up          10/10   4097        2136580547/41411  0
  172.16.0.69  01:03:17  admin-down 255/10   -           2136580547/41411  -
  172.16.0.69  01:03:17  up          10/10   4097        2136580547/41411  0
```

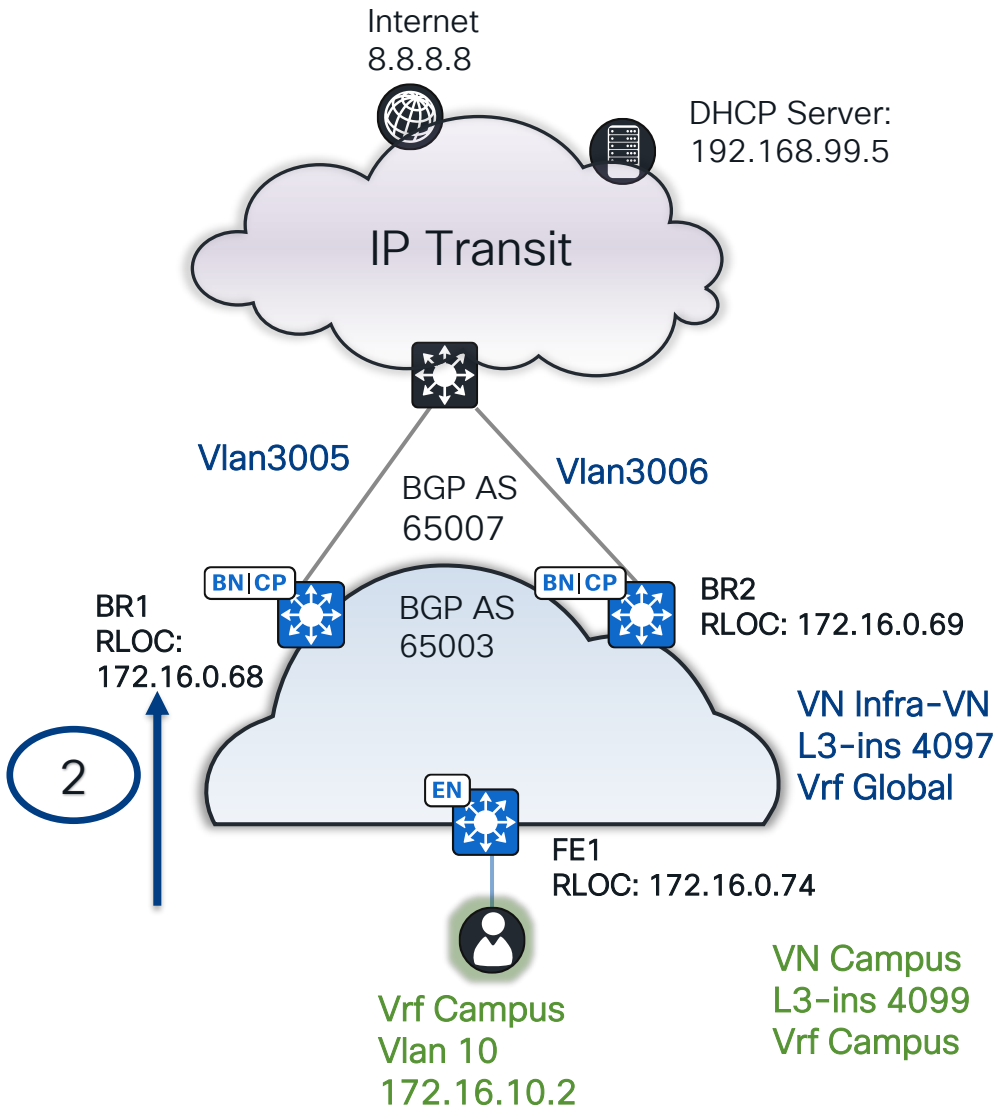


Troubleshooting LISP Extranet

South-North 172.16.10.2 to 192.168.99.5

```
Edge#show ip lisp instance-id 4099 forwarding eid remote 192.168.99.5
Prefix                 Fwd action  Locator status bits   encap_iid
192.0.0.0/2            encap       0x00000000            4097
ifnums:
      LISP0.4099(79): 172.16.0.68, 172.16.0.69

Edge# show ip cef vrf Campus 192.168.99.5 internal
192.0.0.0/2, epoch 1, flags [sc, lisp elig], refcnt 6, per-destination
sharing
  sources: LISP, IPL
<snipped>
    SC owned,sourced: LISP remote EID - locator status bits
0x00000000, encap_iid 4097
    LISP remote EID: 948 packets 363452 bytes fwd action encap,
encap_iid 4097
[ommited]
```



Troubleshooting LISP Extranet

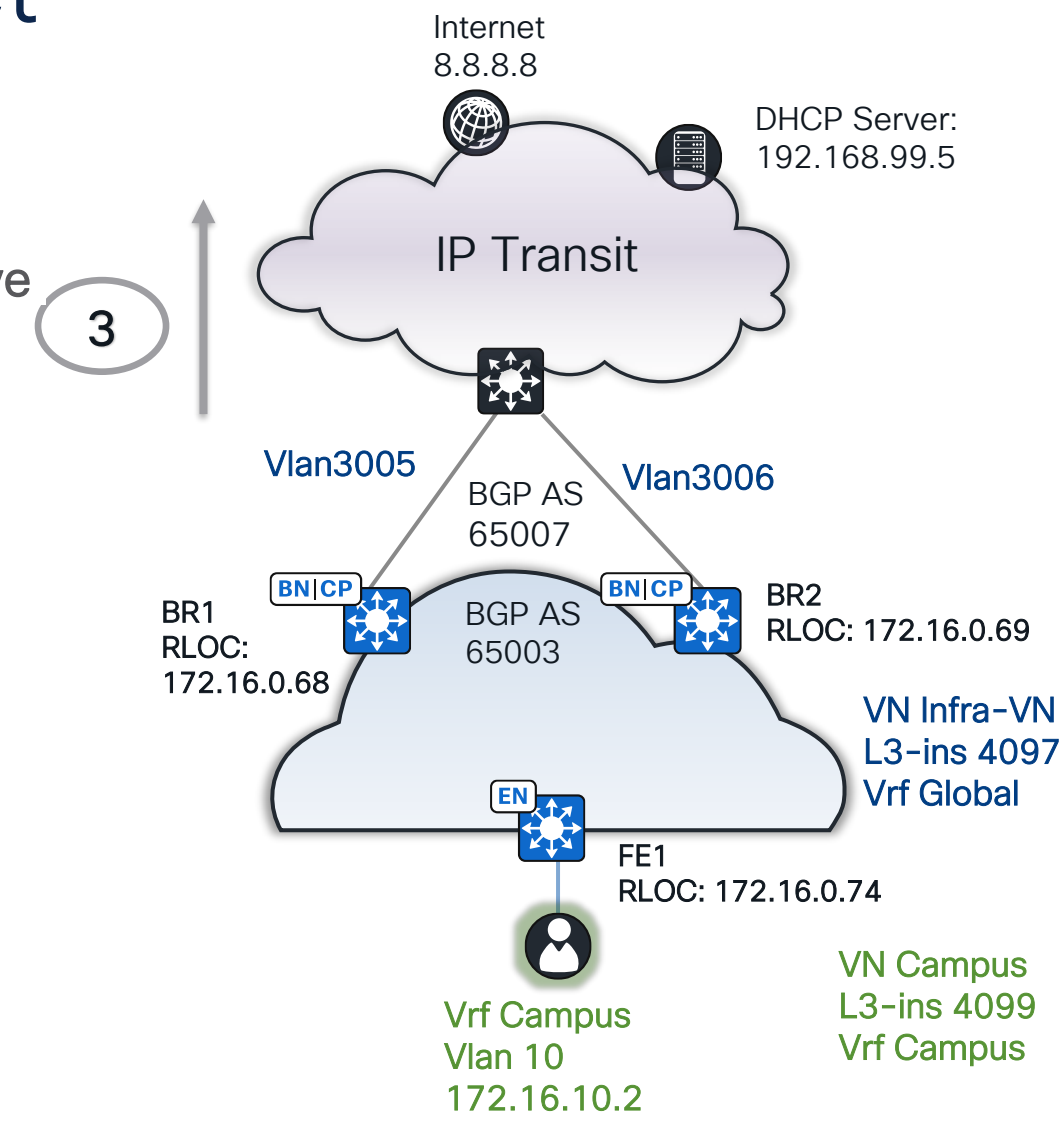
South-North 172.16.10.2 to 192.168.99.5

TAC Tip

For a Border to advertise a default route into LISP PUBSUB; it must first have a default route in its Routing Table for each VRF; **in extranet, we do not expect to have a default route in the subscriber VN.**

```
Border# show ip route vrf Campus 0.0.0.0
Routing Table: Campus
% Network not in table

Border# show ip route 0.0.0.0
Routing entry for 0.0.0.0/0, supernet
  Known via "bgp 65003", distance 20, metric 0, candidate default
path
  Tag 65007, type external
  Last update from 172.16.1.18 01:24:39 ago
  Routing Descriptor Blocks:
  * 172.16.1.18, from 172.16.1.18, 01:24:39 ago
      opaque_ptr 0x7F9B81F33678
      Route metric is 0, traffic share count is 1
      AS Hops 1
      Route tag 65007
      MPLS label: none
      MPLS Flags: NSF
```



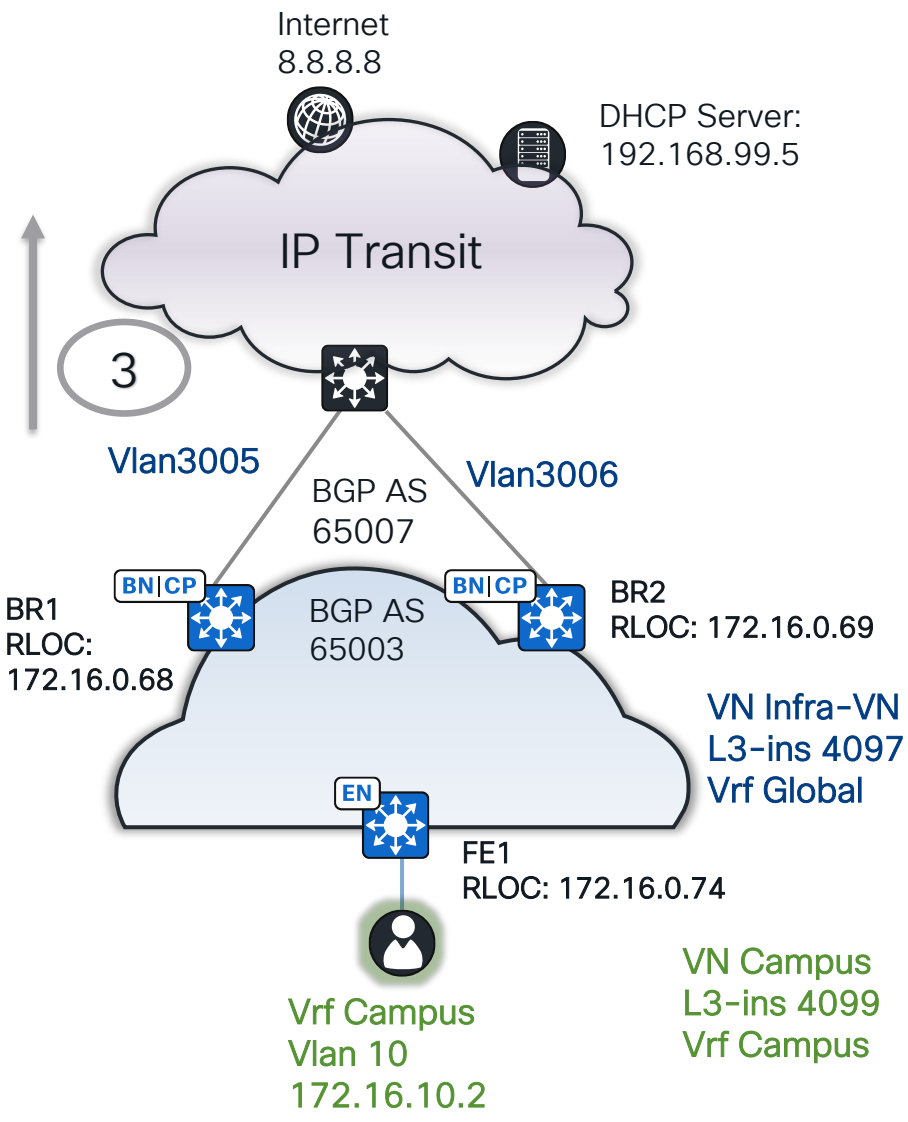
Troubleshooting LISP Extranet

South-North 172.16.10.2 to 192.168.99.5

With a default route only in the provider VN (INFRA/GRT), we only announce a default route into LISP for that VRF alone.

```
Border#show lisp instance-id 4097 ipv4 database 0.0.0.0/0
0.0.0.0/0, locator-set DEFAULT_ETR_LOCATOR, default-ETR
  Uptime: 01:58:48, Last-change: 01:29:10
<snipped>
  Locator       Pri/Wgt  Source     State
  172.16.0.69    10/10   cfg-intf   site-self, reachable
  Map-server        Uptime         ACK  Domain-ID
  172.16.0.68       01:29:10       Yes  2136580547
  172.16.0.69       01:29:10       Yes  2136580547

Border#show lisp instance-id 4099 ipv4 database 0.0.0.0/0
<snipped>
0.0.0.0/0, locator-set DEFAULT_ETR_LOCATOR *** NO ROUTE TO EID PREFIX ***,
default-ETR
  Uptime: 01:58:40, Last-change: 01:58:40
<snipped>
  Map-server        Uptime         ACK  Domain-ID
  172.16.0.68       01:58:24       Yes  2136580547
  172.16.0.69       01:58:33       Yes  2136580547
```



Troubleshooting LISP Extranet

South-North 172.16.10.2 to 192.168.99.5

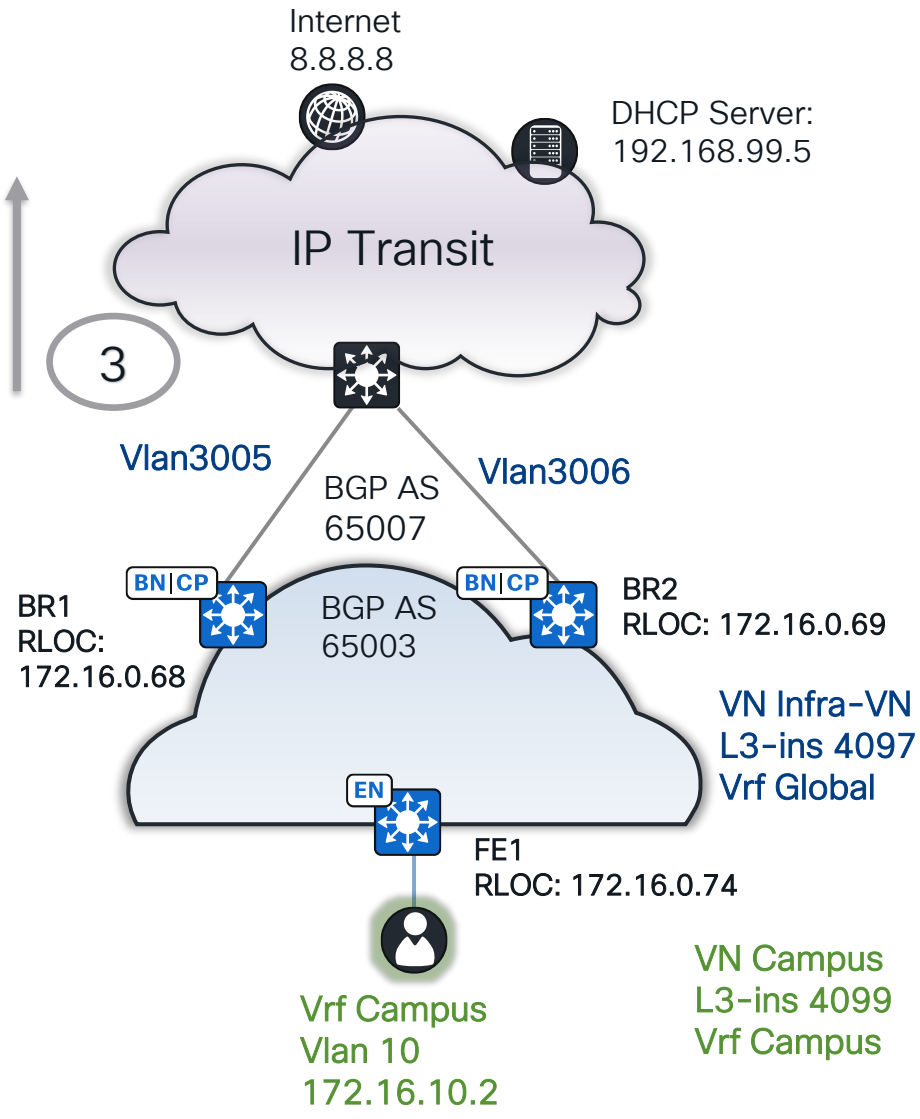
With the remote-locator-set command (**in CP nodes**) we can confirm that this External Border is being considered a default-ETR **only in INFRA_VN as intended**.

```
Border#show lisp remote-locator-set default-etrs | be LISP
LISP remote-locator-set default-etr-locator-set-ipv4 Information

 RLOC           Pri/Wgt/Metric      Inst        Domain-ID/MH-ID  ETR      SI/ID
 172.16.0.68     10/10 /0           4097        2136580547/41411  Default PB/-
 172.16.0.68    255/10 /-           4099        2136580547/41411  Default
 172.16.0.69     10/10 /0           4097        2136580547/41411  Default PB/-
 172.16.0.69    255/10 /-           4099        2136580547/41411  Default
```

TAC Tip

The rest of the RLOCs are marked with a priority of 255 which is considered **administratively down**, any Edge will not use these.

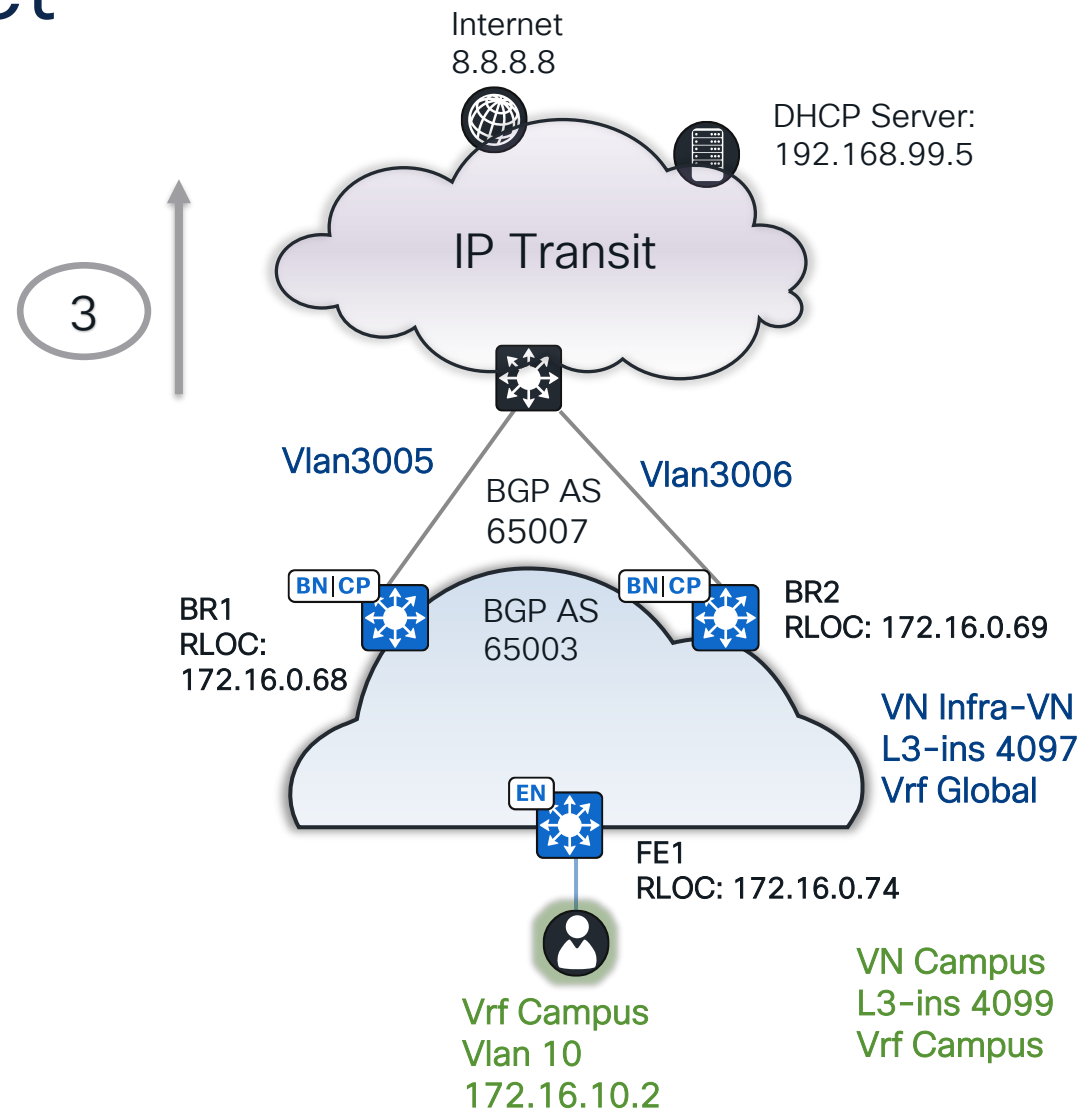


Troubleshooting LISP Extranet

South-North 172.16.10.2 to 192.168.99.5

If we check the extranet prefixes for the subscriber VN, we can see the list of "leaked" routes that this CP can resolve:

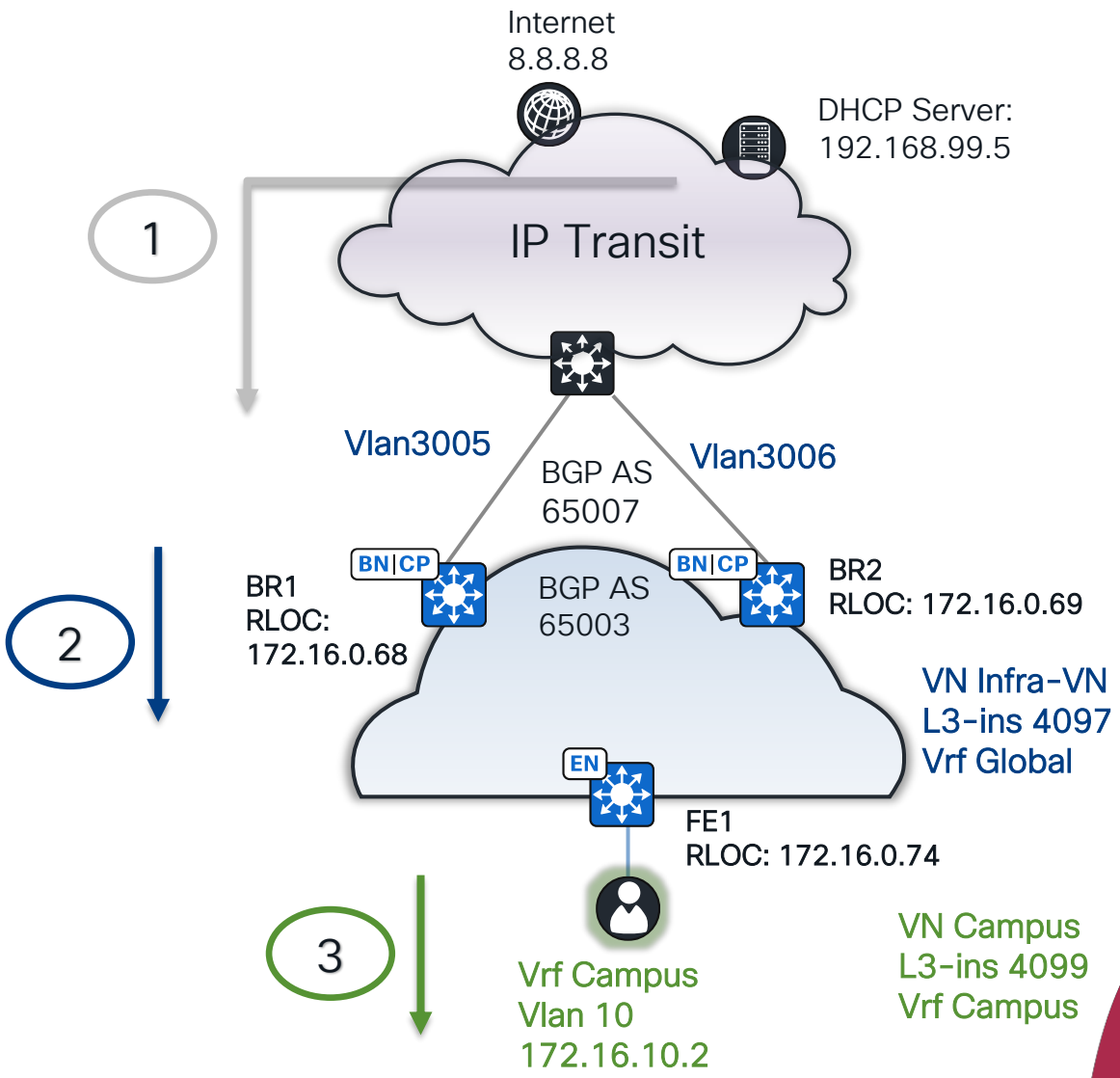
```
Border# show lisp instance-id 4099 extranet CLUS
LISP Extranet policy table
Home Instance ID: 4099
Prov/Sub     Source              InstID      EID prefix
Provider     Default ETR Reg V4  4097
Provider     Config              4097        172.16.4.0/24
Provider     Config              4097        172.16.5.0/24
Subscriber   Config              4099        172.16.10.0/24
Subscriber   Config              4099        172.16.11.0/24
Total entries: 4
```



TAC Tip

When using LISP Extranet, make sure that **neither the default route nor any specific route exists in the Subscriber VRF**, if a path from the subscriber VRF exists, it will win over the Extranet one.

North-South flow



Troubleshooting LISP Extranet

North-South 192.168.99.5 to 172.16.10.2

```
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 3006
Cisco MetaData
Internet Protocol Version 4, Src: 192.168.99.5, Dst: 172.16.10.2
Internet Control Message Protocol
   Type: 0 (Echo (ping) reply)
   Code: 0
   Checksum: 0x403a [correct]
```

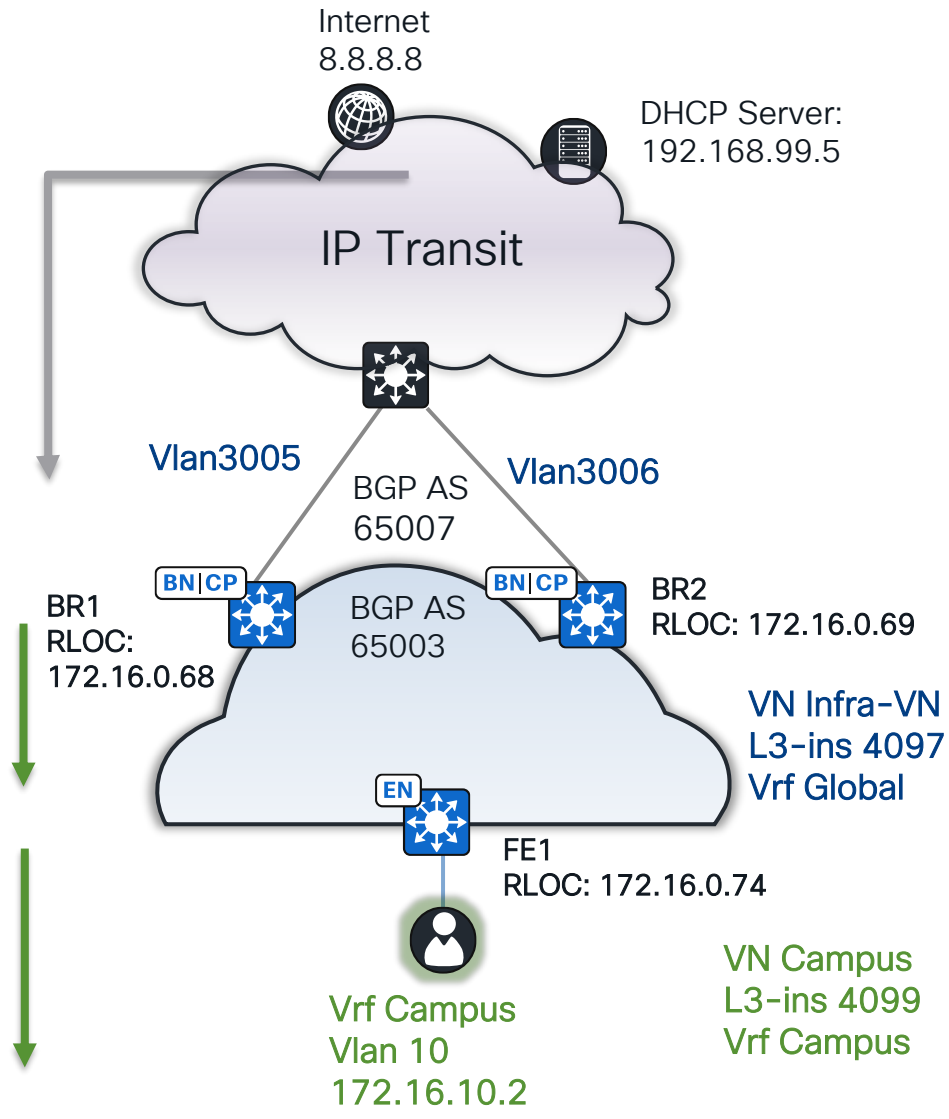
1

```
ernet Protocol Version 4, Src: 172.16.0.69, Dst: 172.16.0.74
r Datagram Protocol, Src Port: 65349, Dst Port: 4789
tual eXtensible Local Area Network
Flags: 0x8800, GBP Extension, VXLAN Network ID (VNI)
Group Policy ID: 0
VXLAN Network Identifier (VNI): 4099
Reserved: 0
ernet II, Src: 00:00:00_00:80:63 (00:00:00:00:80:63), Dst: ba:25:cd:f4:ad:38 (ba:25:cd:f4:ad:38)
ernet Protocol Version 4, Src: 192.168.99.5, Dst: 172.16.10.2
ernet Control Message Protocol
Type: 0 (Echo (ping) reply)
Code: 0
Checksum: 0x4eb7 [correct]
```

2

```
> Internet Protocol Version 4, Src: 192.168.99.5, Dst: 172.16.10.2
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x4eb7 [correct]
```

3

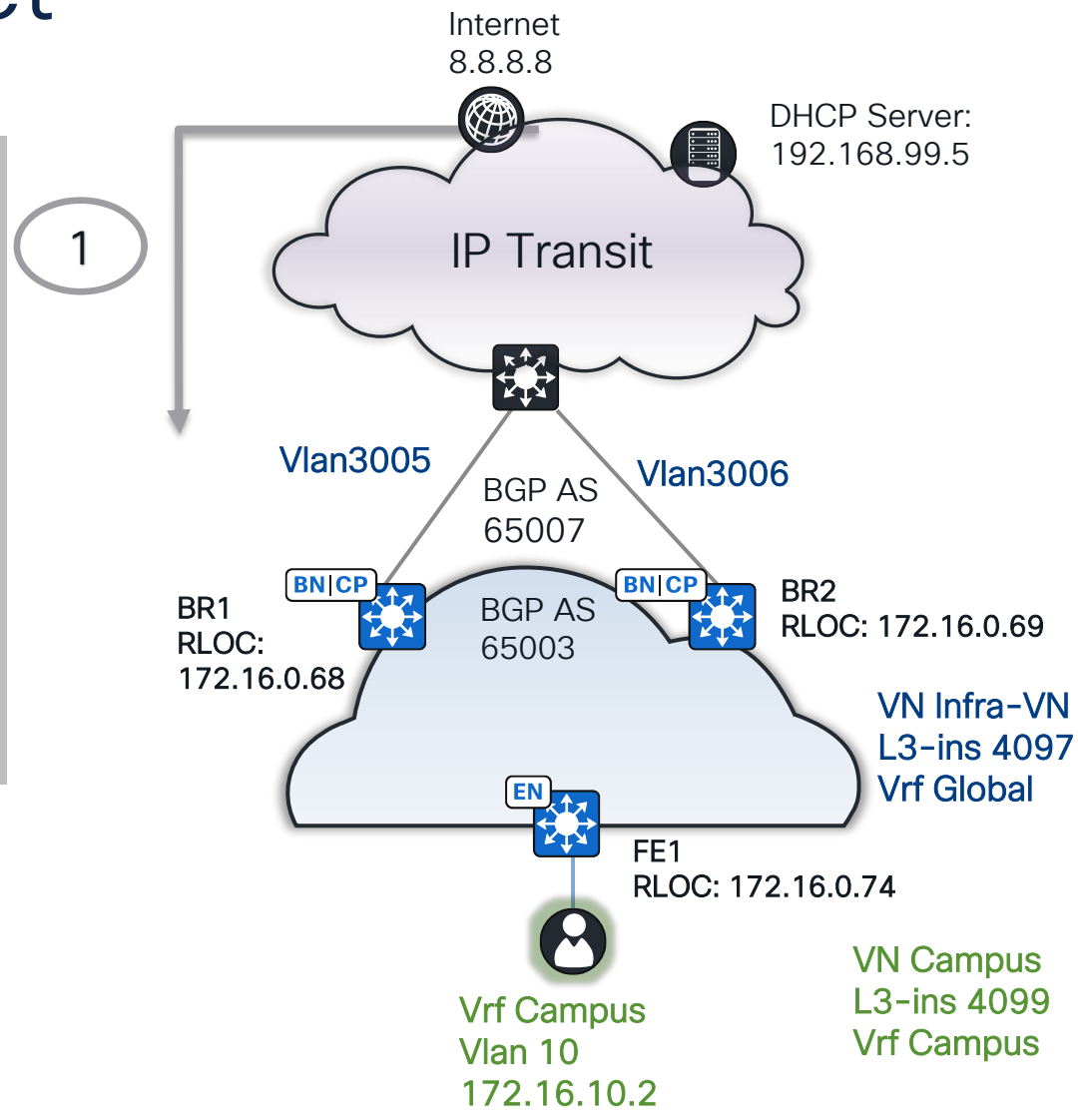


Troubleshooting LISP Extranet

North-South 192.168.99.5 to 172.16.10.2

```
Border#show ip route 172.16.10.1
Routing entry for 172.16.10.1/32
  Known via "connected", distance 0, metric 0 (connected, via
interface)
  Advertised by bgp 65003
  Routing Descriptor Blocks:
  * directly connected, via Loopback4990
      Route metric is 0, traffic share count is 1

Border#show ip bgp neighbors 172.16.1.22 advertised-routes | inc
Network|172.16.10.0/24
   Network          Next Hop            Metric LocPrf Weight Path
*> 172.16.10.0/24   0.0.0.0                  10         32768 ?
```



Troubleshooting LISP Extranet

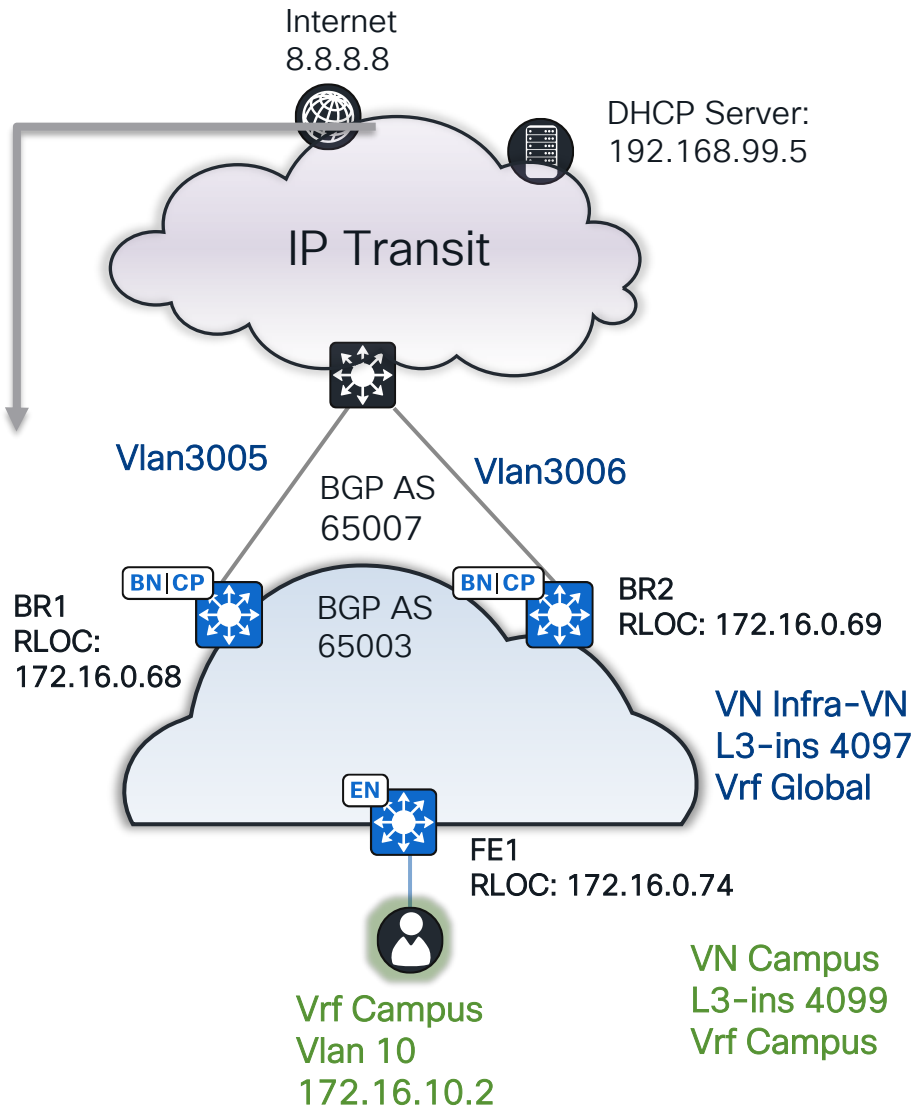
North-South 192.168.99.5 to 172.16.10.2

How is VRF Leaking happening in North to South flow?

```
Ethernet II, Src: Cisco_1f:48:51 (d4:e8:80:1f:48:51), Dst: Cisco_53:7f:ff (4c:5d:3c:53:7f:ff)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 3006
Cisco MetaData
Internet Protocol Version 4, Src: 192.168.99.5, Dst: 172.16.10.2
Internet Control Message Protocol
   Type: 0 (Echo (ping) reply)
   Code: 0
   Checksum: 0x403a [correct]
```

```
Border#show ip policy
Interface             Route map
Vlan3006              EXTRANET_MATCH_SUBSCRIBER_V4
LISP0.4097            EXTRANET_MATCH_SUBSCRIBER_V4
```

```
route-map EXTRANET_MATCH_SUBSCRIBER_V4 permit 30
 description Match IPV4 ACL and set Vrf
 match ip address EXTRANET_Campus_IPV4_ACL
 set vrf Campus
```

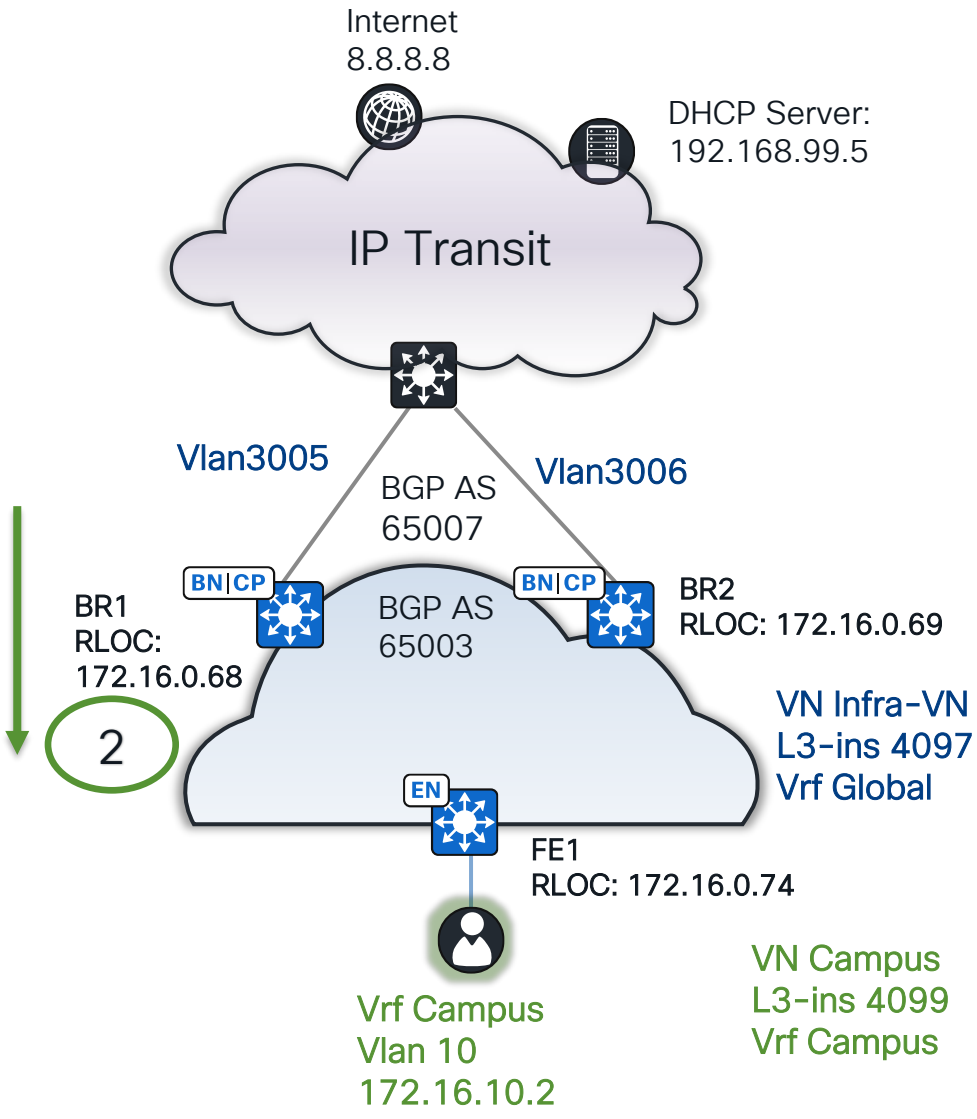


Troubleshooting LISP Extranet

North-South 192.168.99.5 to 172.16.10.2

```
Border# show lisp instance-id 4099 ipv4 map-cache 172.16.10.2
LISP IPv4 Mapping Cache for LISP 0 EID-table vrf Campus (IID 4099), 1
entries

172.16.10.2/32, uptime: 00:00:24, expires: never, via pub-sub,
complete, local-to-site
  Sources: pub-sub
  State: complete, last modified: 00:00:24, map-source: 172.16.0.69
  Exempt, Packets out: 3(1728 bytes), counters are not accurate (~
00:00:00 ago)
  Configured as EID address space
  Locator      Uptime    State  Pri/Wgt     Encap-IID
  172.16.0.74  00:00:24  up      10/10        -
    Last up-down state change:          00:00:24, state change count: 1
    Last route reachability change:     03:01:40, state change count: 1
    Last priority / weight change:      never/never
    RLOC-probing loc-status algorithm:
      Last RLOC-probe sent:             never
```

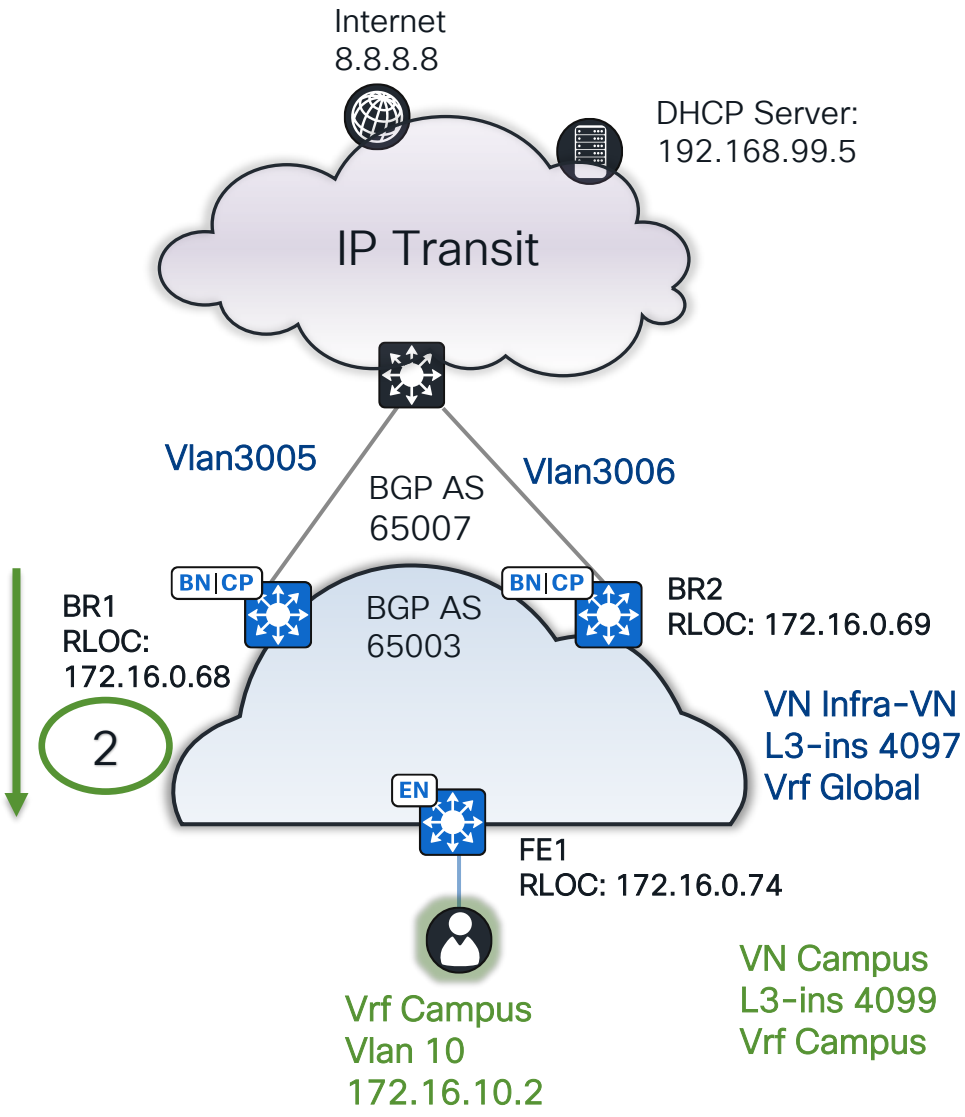


Troubleshooting LISP Extranet

North-South 192.168.99.5 to 172.16.10.2

```
Border#show ip cef  vrf Campus 172.16.10.2
172.16.10.2/32
  nexthop 172.16.0.74 LISP0.4099

Border#show ip cef vrf Campus 172.16.10.2 internal
          172.16.10.2/32, epoch 0, flags [sc, lisp elig], RIB[l],
refcnt 6, per-destination sharing
            sources: LISP, RIB, IPL
 LISP remote EID: 9 packets 2804 bytes fwd action encap, cfg as EID
space
              SC inherited: LISP generalised SMR - [disabled, not
inheriting, 0x7F491A6D6820 locks: 4]<snipped>
              LISP source path list
<snipped>
                      nexthop 172.16.0.74 LISP0.4099, IP midchain out
of LISP0.4099, addr 172.16.0.74 7F491C30EF68
                  1 output chain
                    chain[0]: IP midchain out of LISP0.4099, addr
172.16.0.74 7F491C30EF68
IP adj out of GigabitEthernet1/0/47, addr 172.16.0.73 7F491C311268
```

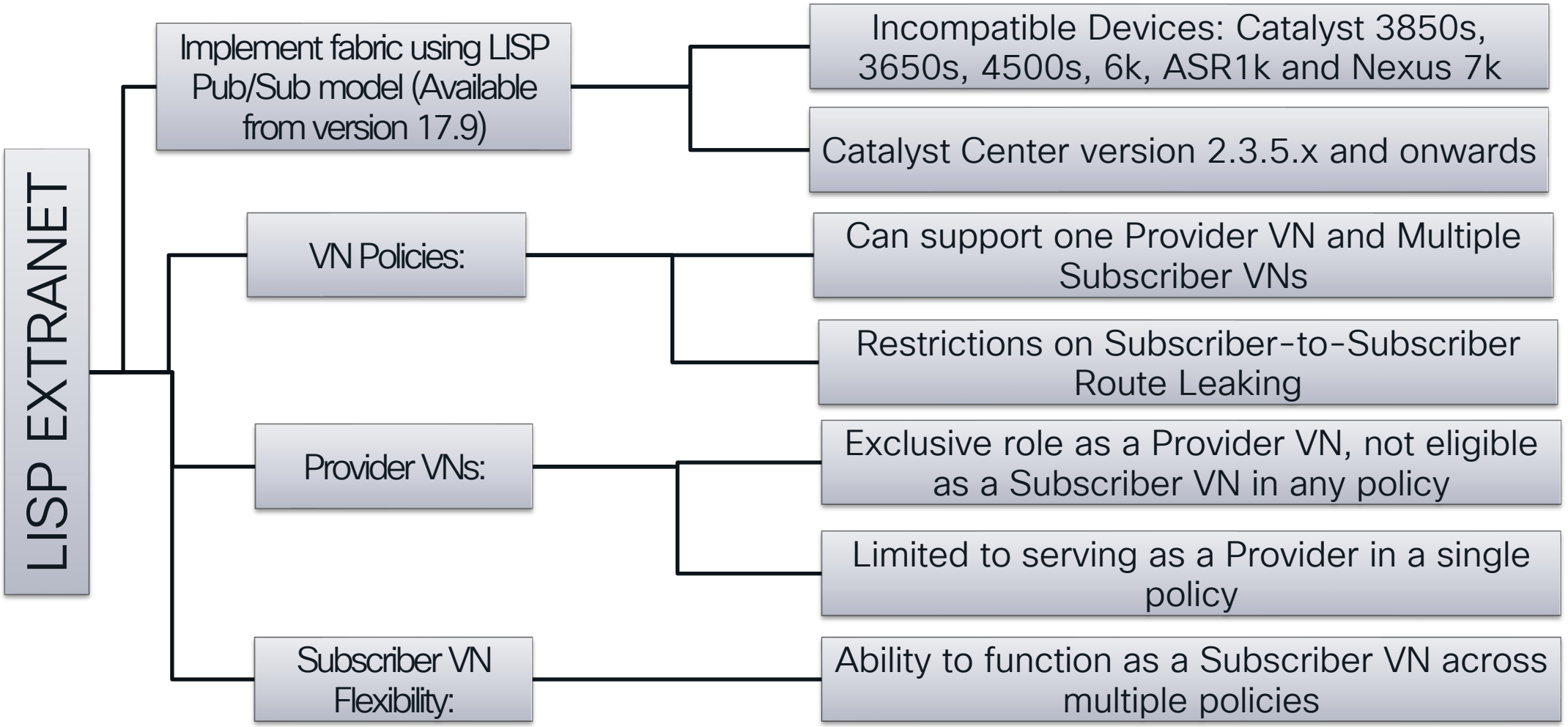


The bridge to possible

Configuration Guidelines

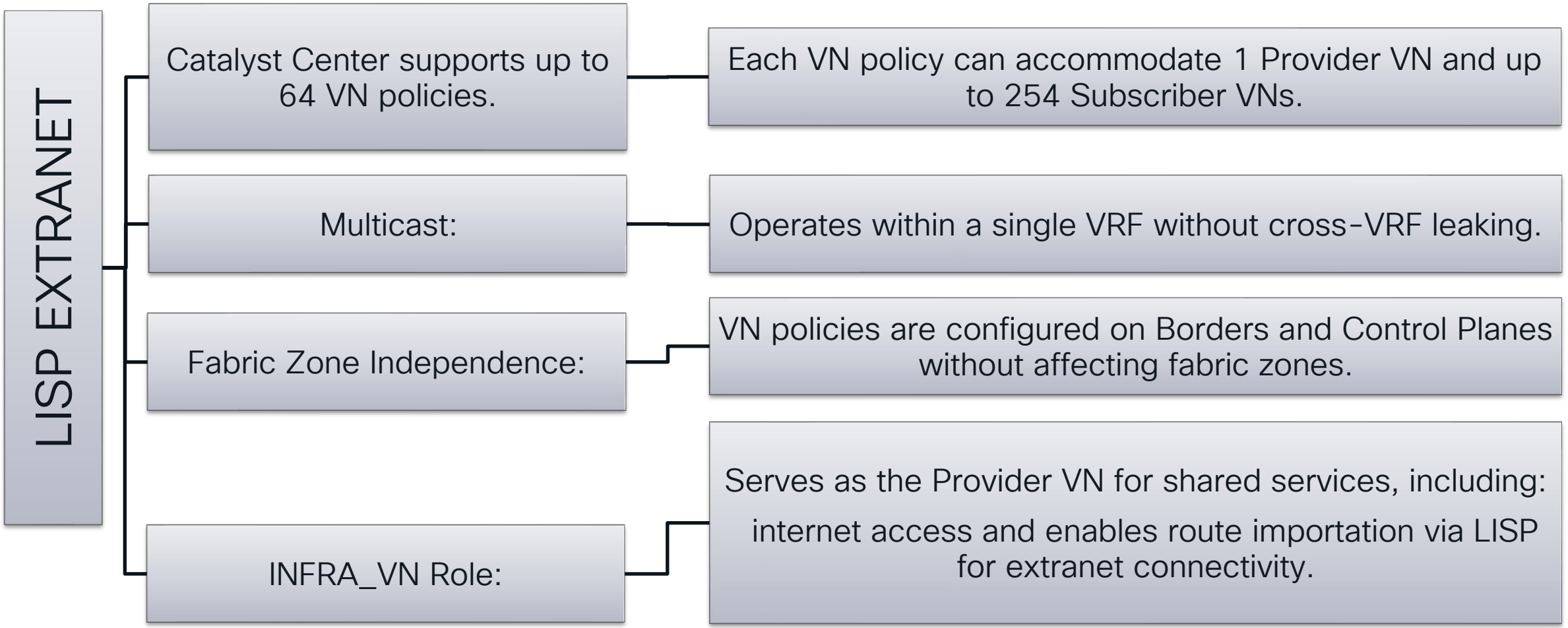
Configuration Guidelines

Considerations and Limitations

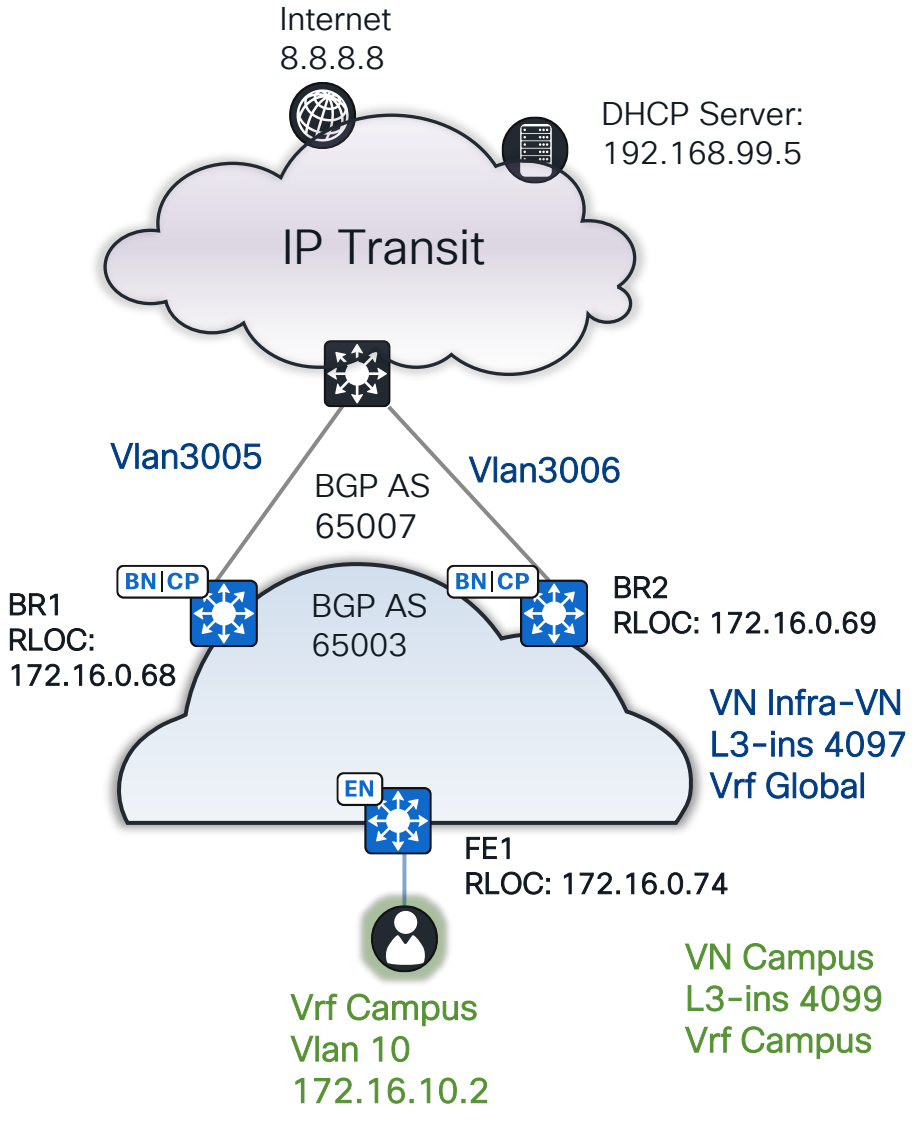


Configuration Guidelines

Considerations and Limitations



Summary and Q&A EXTRANET



Catalyst Center

SDA

Learn how Cisco Catalyst Center and SDA will help you implement your Fabric Network.

Start

Monday, June 3rd | 11:00 a.m.
BRKSEC-2845
Cisco Secure Firewall and SDA integration Deep Dive

Monday, June 3rd | 12:50 p.m.
CNCCSS-2000
Catalyst Center – An SDA Customer Case Study with TTI Consumer Power Tool Inc. and SHI

Monday, June 3rd | 2:00 p.m.
VILSEC-1045
Hit the Accelerator on Cisco ISE/SDA for Zero Trust with Ordr

Monday, June 3rd to Thursday, June 6th | 8:00 a.m.
LABENS-2664
Building the SD-Access Fabric with Ansible Playbooks: DIY SDA

Tuesday, June 4th | 4:00 p.m.
BRKENS-1801
SD-Access Success Stories: Concept to Reality by Stanford Health and Yale University

End

More .....

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2025.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live mobile app.

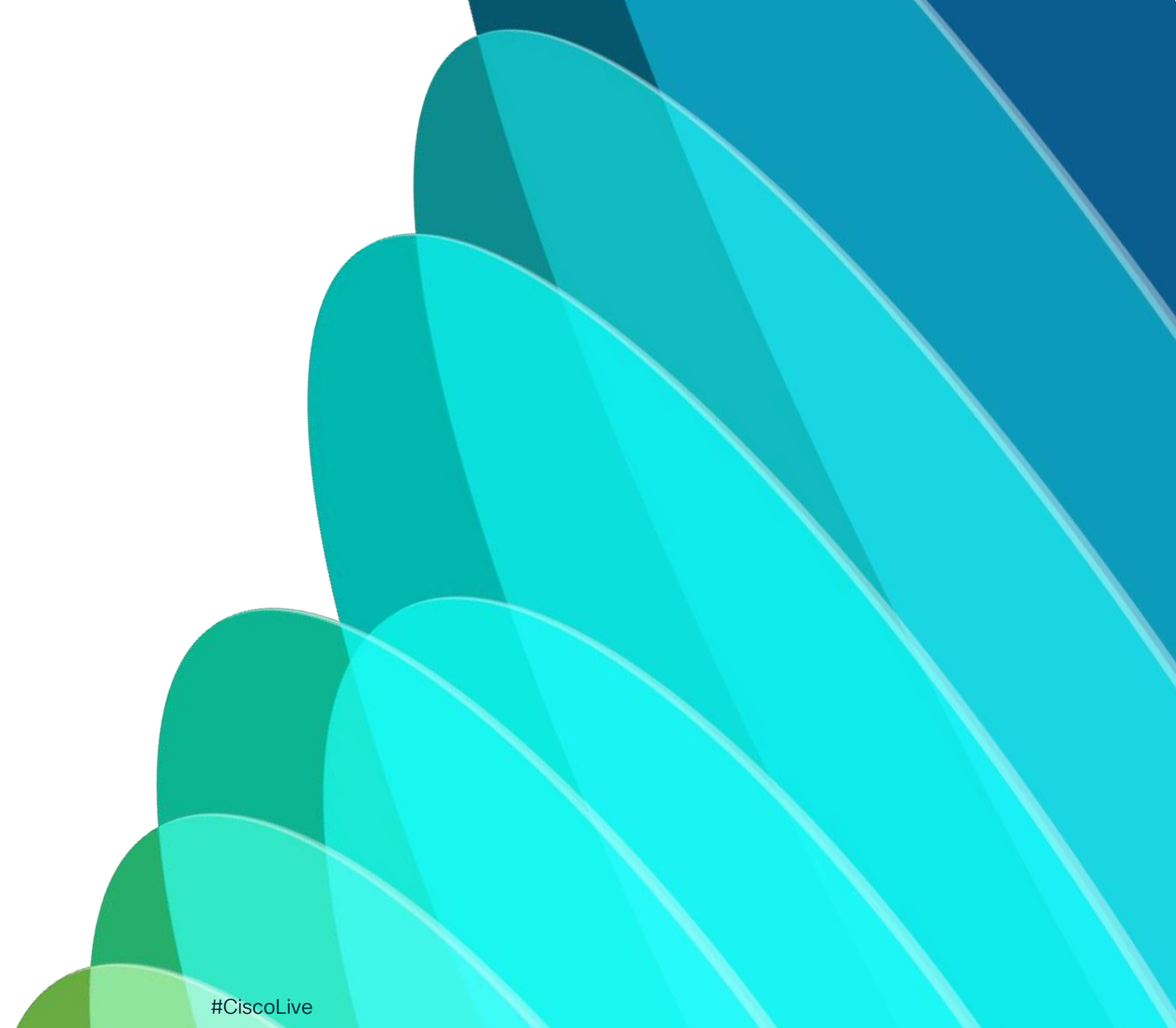
Continue your education

- 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

Contact me at: marhill2@cisco.com, dcabanas@cisco.com

The bridge to possible

Thank you



cisco Live!