The bridge to possible

Migration to Multi-Region Fabric

Transform and Simplify Middle-mile Based Network Designs for Large Scale, Cloud and Colo based SD-WAN Networks

Hamzah Kardame, Leader, Product Management
Tahir Ali, Technical Leader, Technical Marketing

cisco Live!

BRKENT-2651

Cisco Webex App

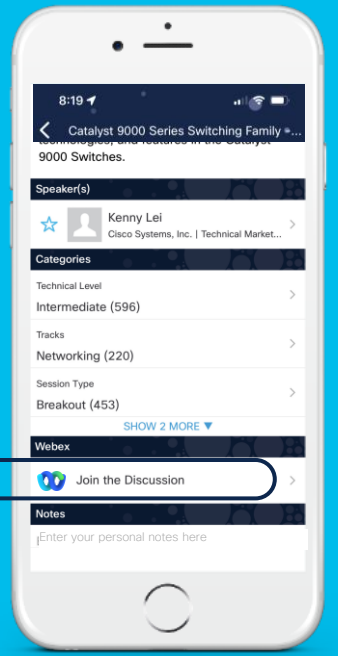
Questions?

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 until February 24, 2023.



Agenda

- Brief overview and why MRF
- MRF – A quick look
- Design considerations
- Migration steps
- Migration from
  - OMP Core
  - BGP Core
- Conclusion

About Me - Hamzah Kardame

Experience

2010-2016
WW TAC Lead
CCIE Security 35596

2017-2020
Technical Leader, TME
Viptela integration
SD-WAN for MSPs

Leader, Product Management, SD-WAN

LinkedIn
www.linkedin.com/in/hamzah-kardame

Expertise

WAN, SD-WAN and Network Security

PKI, TLS, IKEv1/v2/IPsec, DMVPN, GETVPN, FlexVPN, WAAS, Cisco Firewalls, Anyconnect

Featured

CSC Webcast
Ask the Expert
Webinars
Cisco Blogs
Cisco.com Guides
Tech Field Day

About Me -Tahir Ali

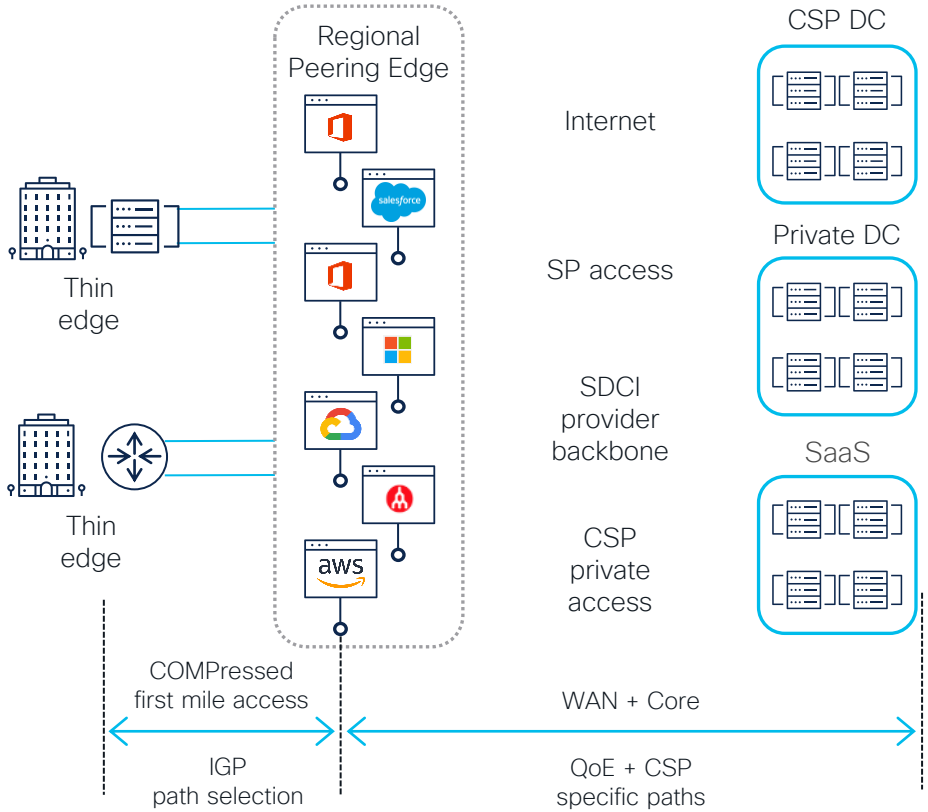
- TME-Technical Leader @Cisco SDWAN BU
  - Since 2018: Part of initial Viptela integration team
  - 2018-2006: MSPs and Partners
- Certifications:
  - CCIE# 26070 (Security | Service Provider |Data Center)
  - AWS | Red-hat Associate
- Area of Expertise: SD-WAN Fabric, Policy, Security, SDCI, Multi-region Fabric
- Interests: Mountains and Beaches
- LinkedIn : https://www.linkedin.com/in/tahiralimarvi/

Overview & Why Multi-Region Fabric (MRF)

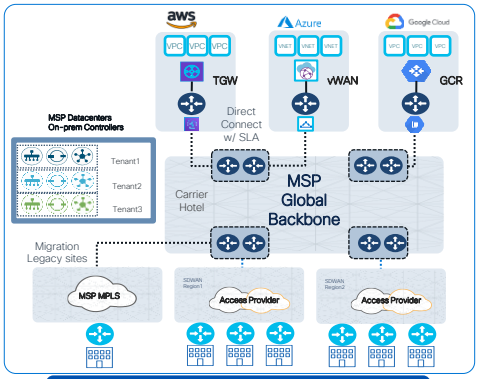
WAN is evolving to a service exchange

- The internet is changing from a network-of-networks to a network of data centers
- SDCI* and multiple provider backbones
- Large POP and Colo footprint
- Short-term contracts, usage-based
- Trending toward single ISP first-mile access
- On demand

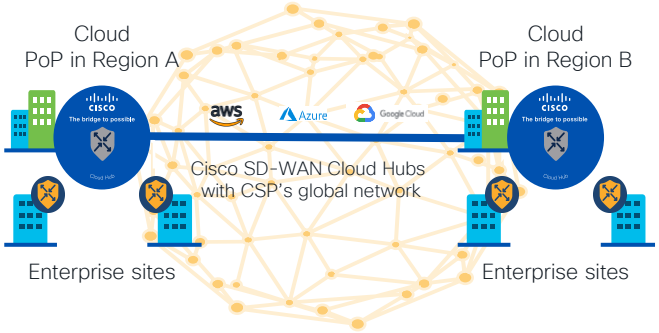
*SDCI – Software Defined Cloud Interconnect



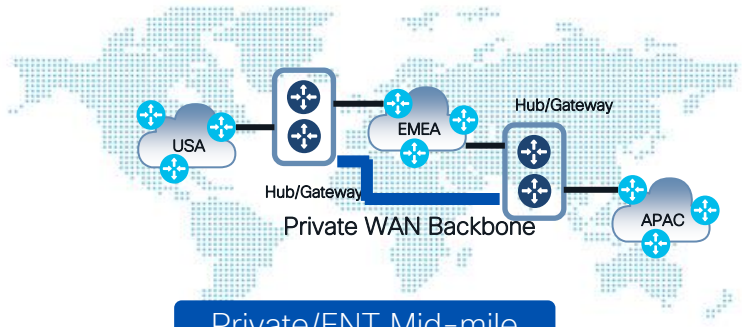
Typical WAN Blueprint



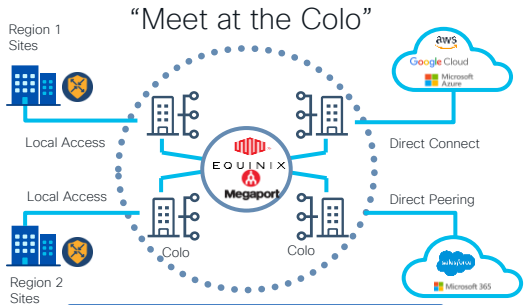
MSP Mid-mile



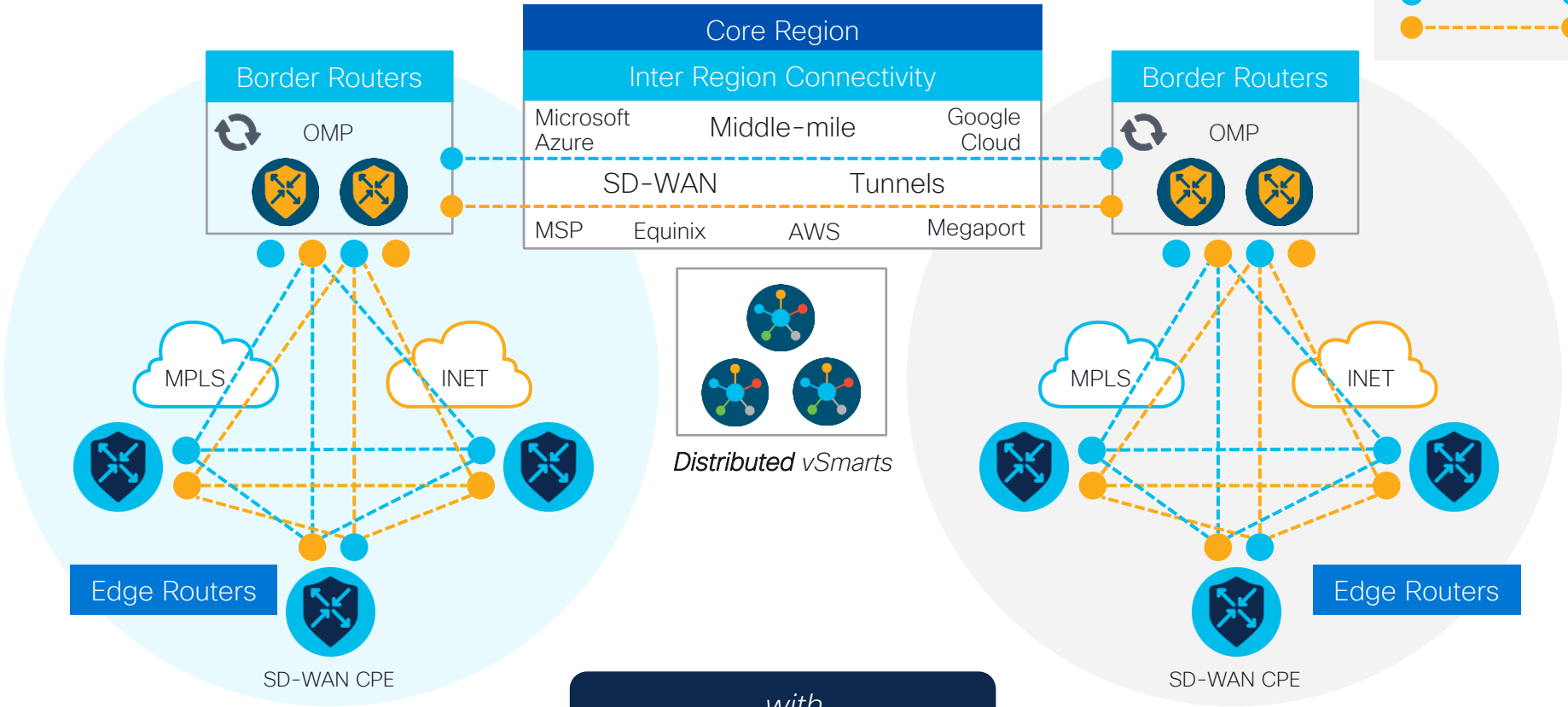
CSP Mid-mile



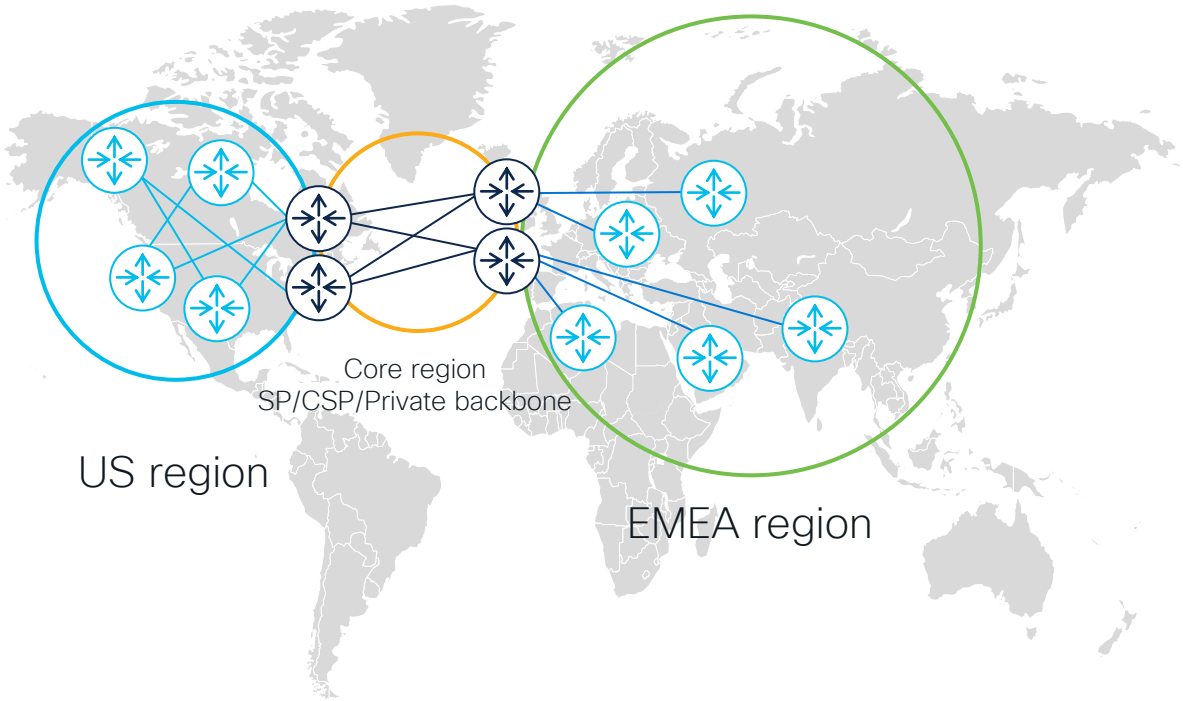
Private/ENT Mid-mile



SDCI Mid-mile



MRF – Key Capabilities



BR/regional hub

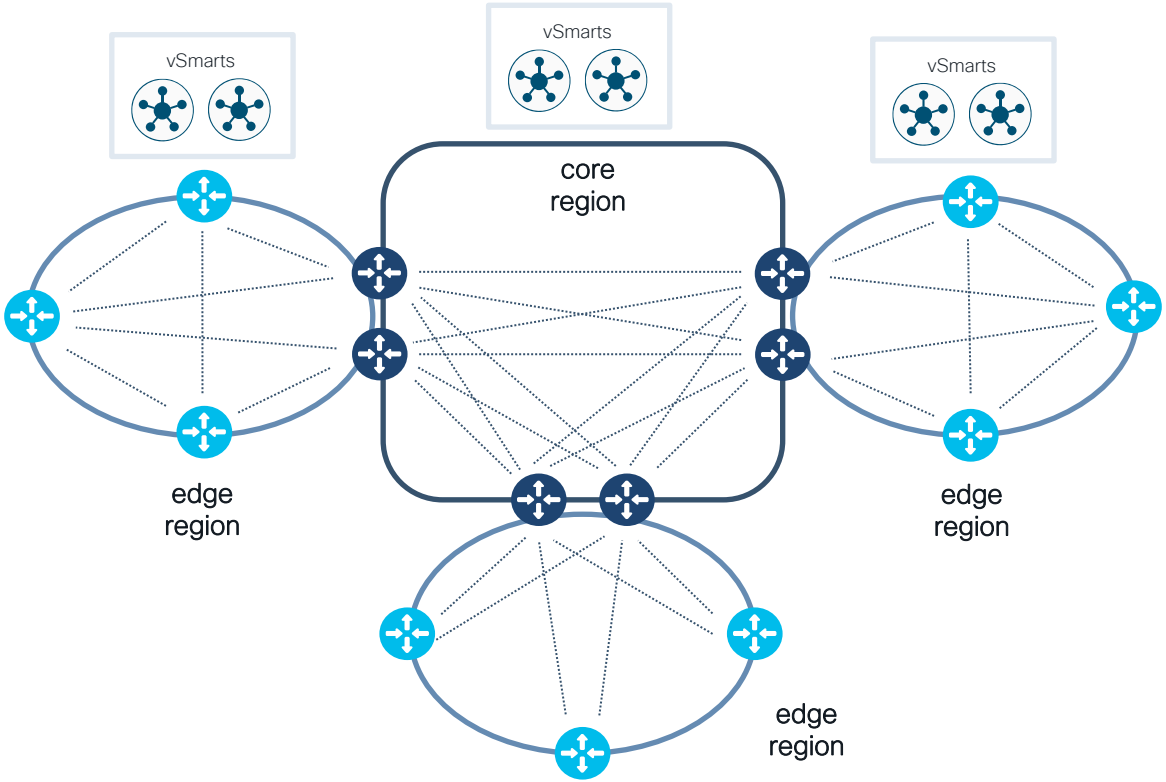
ER/branch

- Intuitive user-defined site grouping. E.g. based on geo
- Finer grouping using sub-regions
- Auto restrict overlay tunnels between regions
- Different topologies per region
- Mix access transports across regions
- Scale up control-plane per region(s)

Multi-Region Fabric

A Quick Look

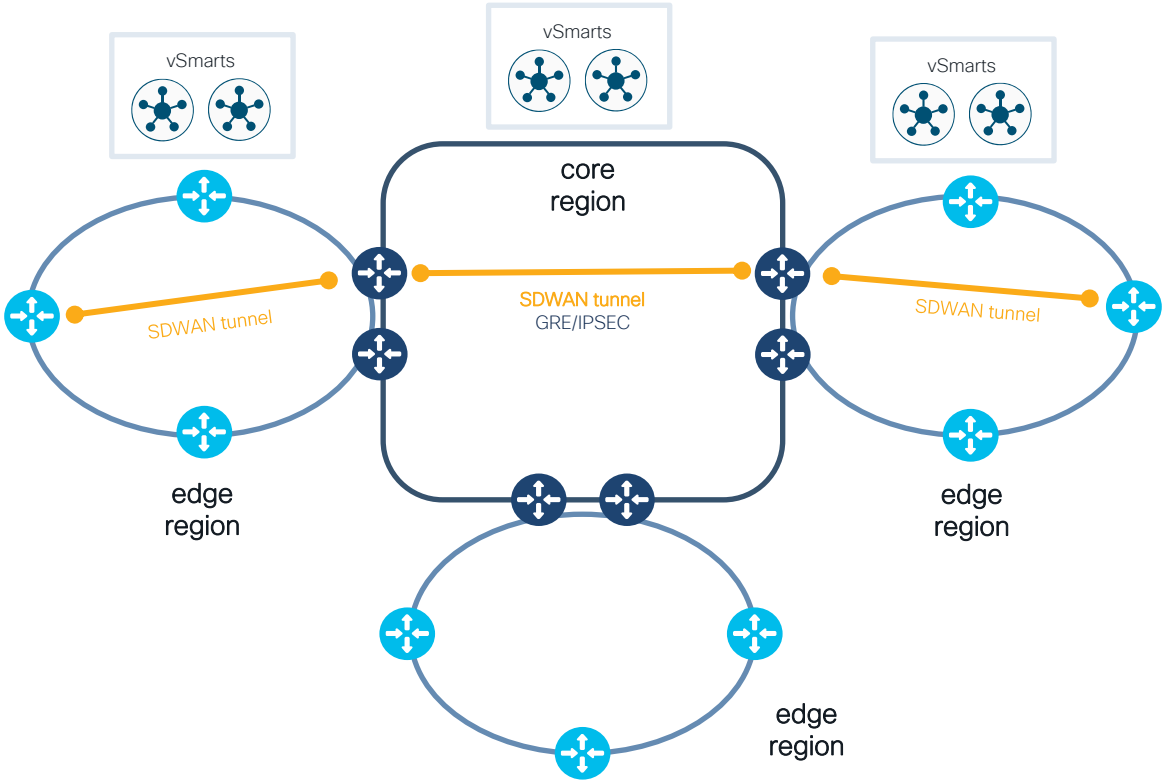
2-Level Topology – Region Aware



Topology

- 2-Layer Architecture
- SD-WAN Fabric organized in Regions
- Regions can be full mesh, partial mesh or hub and spoke
- Core recommended to be full mesh for any to any regional connectivity
- OMP and vSmart region aware
- Regions have Border Nodes in multiple POPs connected to Core
- Global reachability via multiple Border Routers in every Region
- Simplified Configuration (No Control Plane Policy required)

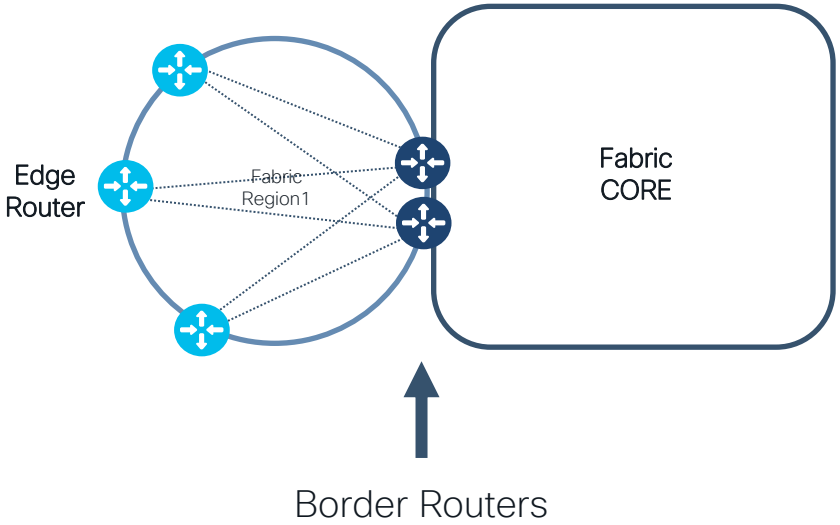
Topology – IP Forwarding



Topology

- SDWAN tunnels restricted by regions
- Hop by Hop tunnels
- Decrypt/Encrypt on all nodes along the path
- IP Lookup and Forwarding per node
- **Requires Service VPN** on intermediate nodes (Border Routers)
- Mix of encapsulation is possible GRE in core/access
  Example: IPsec on access region and GRE on core

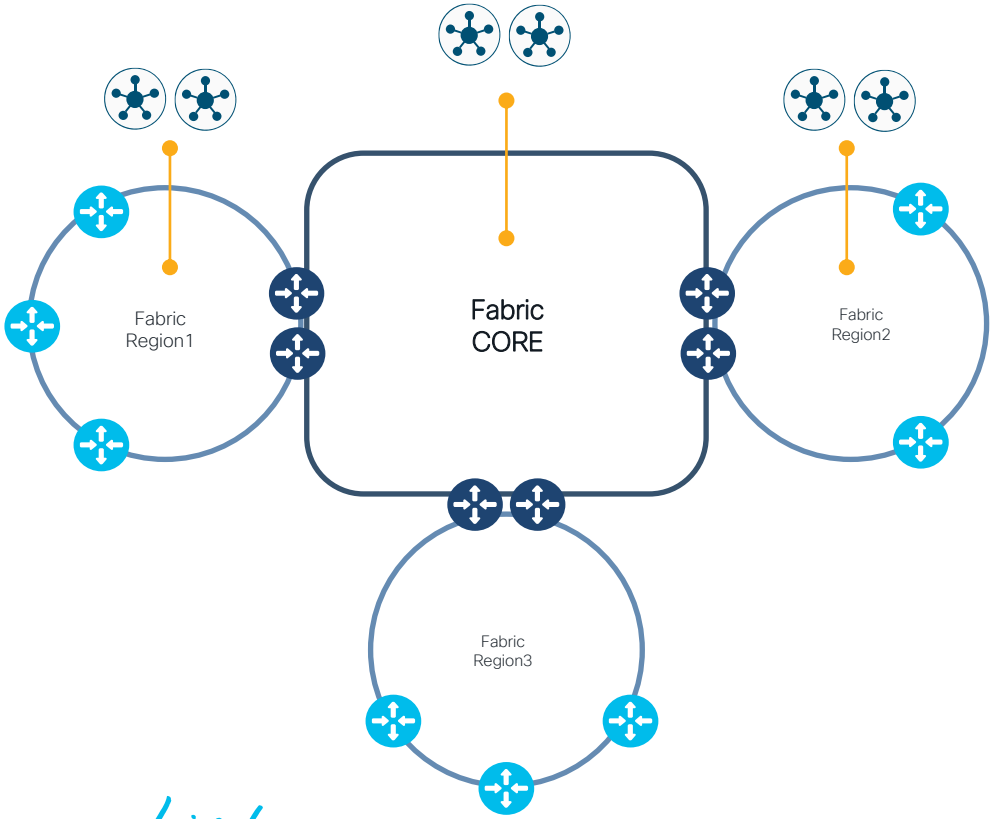
Border Router



What is Border Router?

- Provides inter-region connectivity by connecting regional overlay to a common core or back bone overlay
- Hardware Platform – XE SD-WAN routers
- Virtualized Function - CAT8000v
- Hosted in MSP POP, Cisco POP, CSP, SDCI
- Can be tunnel endpoints for multiple types of connections – SSL VPN (AnyConnect), IPSec
- Horizontally scalable
- Only serves 1 access and 1 core region

Distributed vSmarts



Regional vSmart

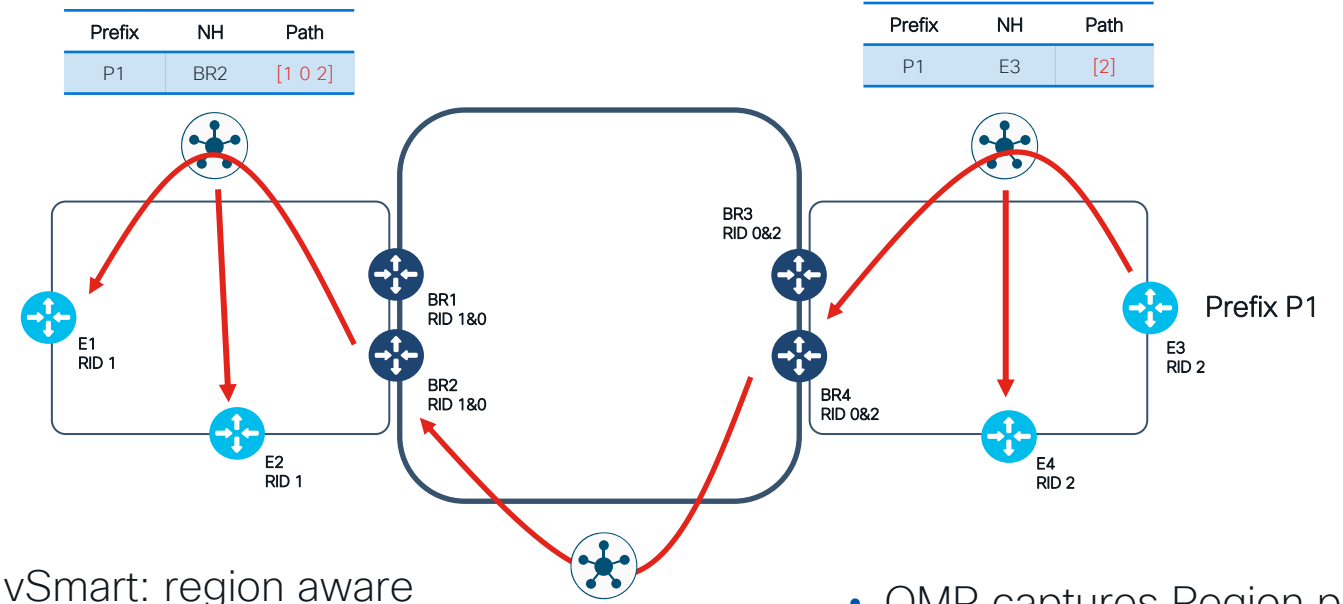
What:

- vSmart controllers become regional

Why:

- To allow for horizontal growth in number of edge routers
- To mitigate the path scale challenges
  - Less OMP peerings
  - Less paths per prefix (BR is the only GW)

Routing in Multi-Region Fabric

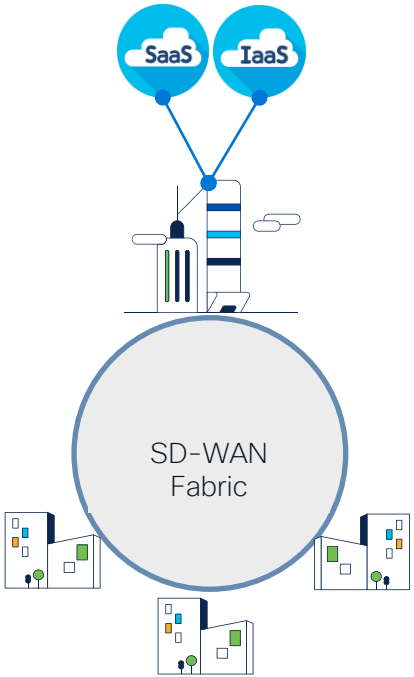


- OMP and vSmart: region aware
- Border routers: vRoute re-origination from one region to another

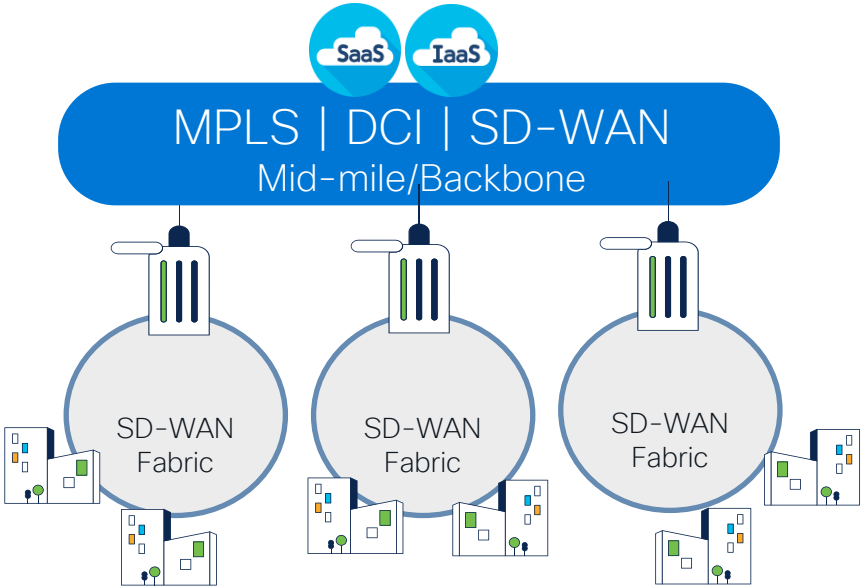
- OMP captures Region path
- Re-originated routes are withdrawn if the connectivity goes down

Design considerations

What does your SD-WAN network look like today?



Flat & Centralized Architecture

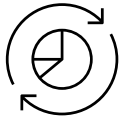


Hierarchical & Semi-centralized Architecture

Migration Considerations

Network topology
Physical and logical layout

Security and compliance needs



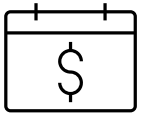
Traffic patterns
Existing and future

Insights into application needs, minimum latency requirements

Reliability and redundancy needs

Cloud connectivity requirements

Scalability needs



Cost

Before the migration

Key design considerations

Identify/update criteria for grouping devices and number of groups needed

- Geography
- Function
- Nature of services/connectivity needed
- Types of applications

Map branch sites to groups

Identify regional aggregation sites for deployment

- Leverage existing sites or new sites required?
- On-prem (HW/CoLo) v. virtual (SDCI/cloud/SP hosted)

Identify WAN transports

For access-regions	For core-region
	DCI / private backbone
	SDCI
	CSP backbone
	SP backbone
	Re-use existing WAN transports

Before the migration

Key design considerations

Understand intra-region and inter-region traffic patterns and future intent

Network scale at day1 v. at day N

Distributed vSmarts

For access-regions
For core-region

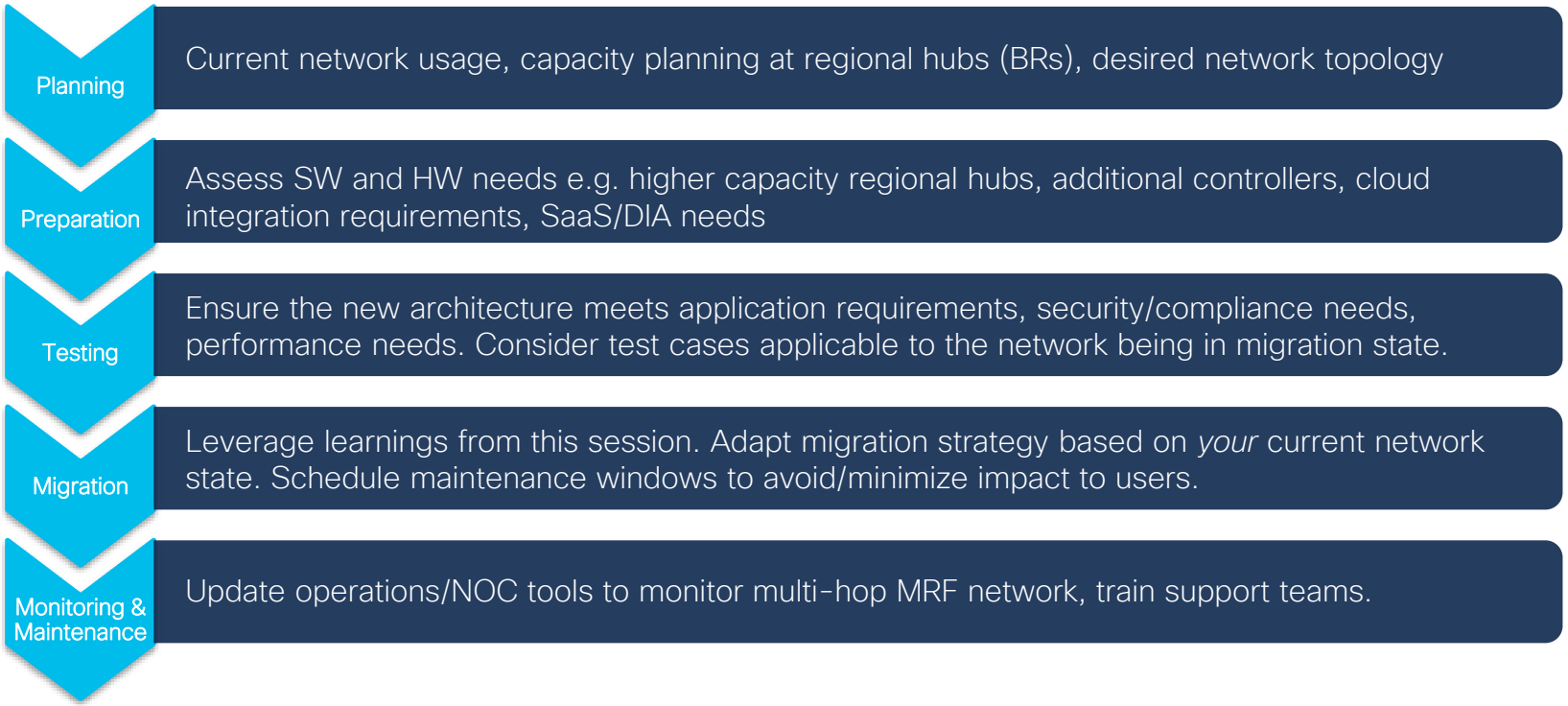
Cloud-hosted
On-prem

Software Versions

For controllers
For Edges

20.9/17.9 or later recommended

Migration Checklist



Migration Steps

What is Migration Mode ?

Aids with migration to MRF

Applied on Edge (branch) and Border (hub) routers only

Minimizes downtime

Keeps existing fabric intact during migration

Existing control policies remain intact

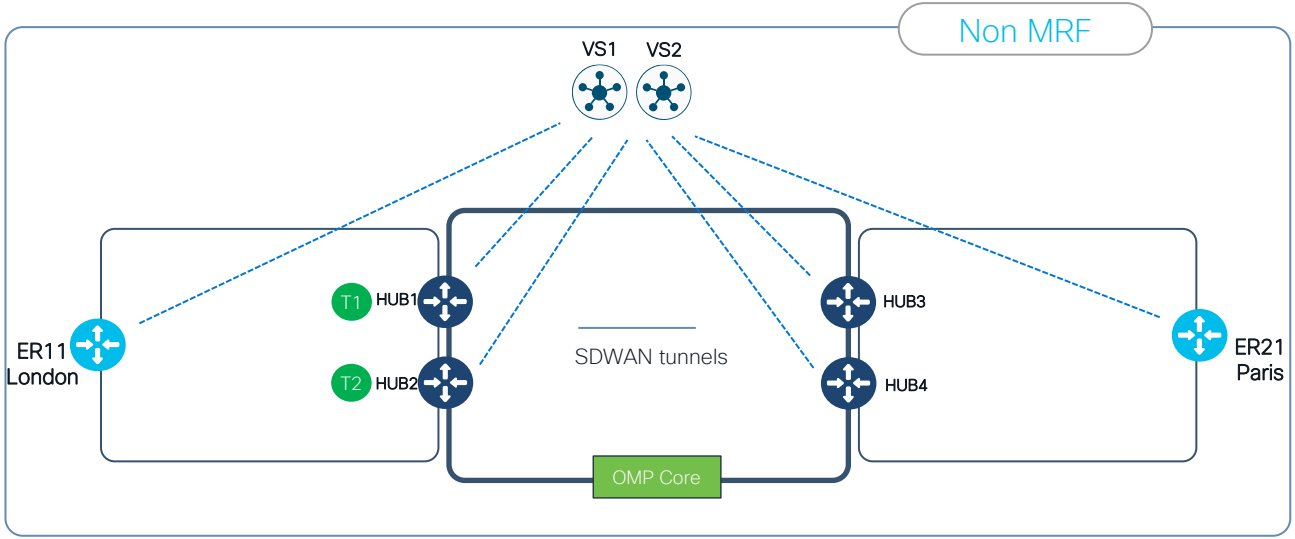
Keeps edge routers' connectivity intact existing vSmarts ('default' region / non-migrated vSmarts)

SDWAN BFD tunnels to non-migrated sites remain intact

Communication from migrated to non-migrated sites is not affected

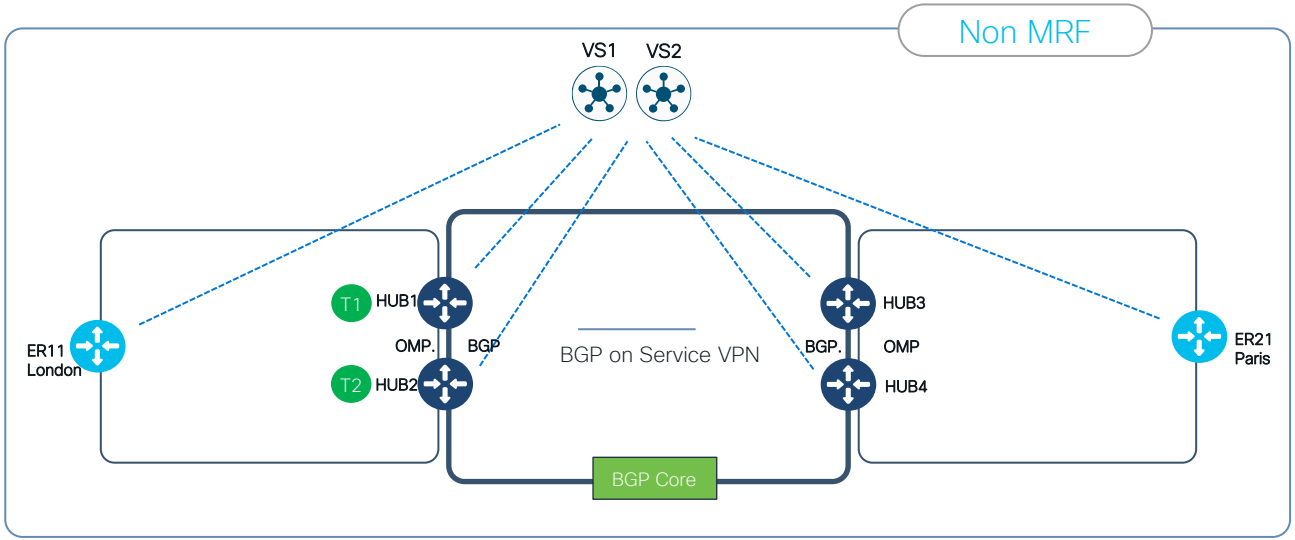
Supported Network Types for brownfield migration

- OMP based Core



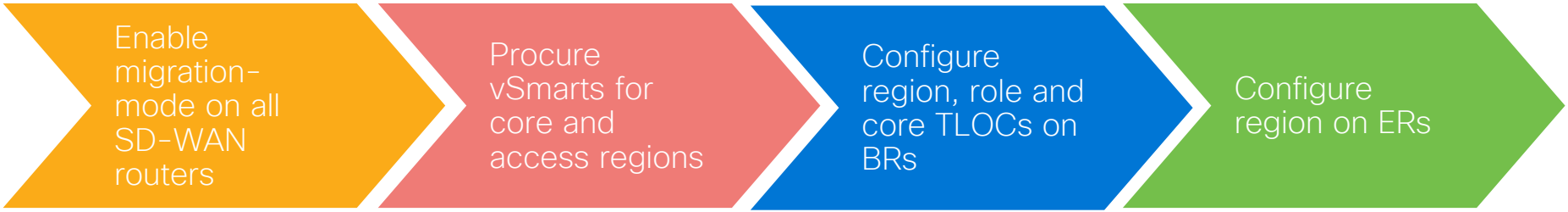
Supported Network Types for brownfield migration

- BGP based Core*



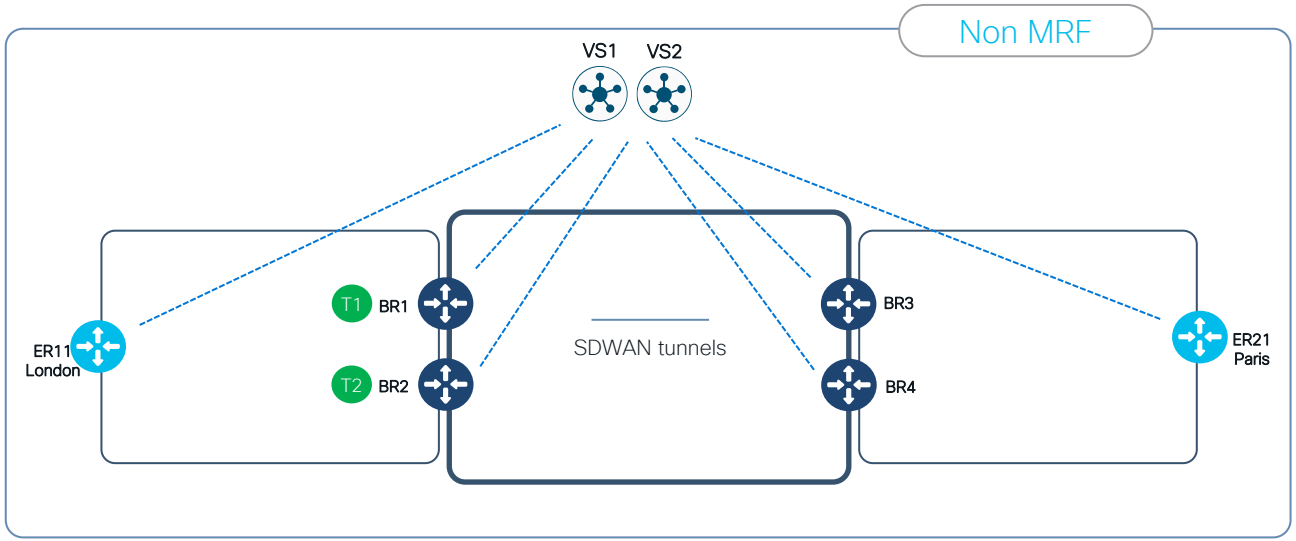
*Starting 20.9.2

Migration Steps High Level



Migration Steps
For OMP Core

Pre-Migration State



- Devices not operating in MRF mode
- Topology built with Control Plane Policies
- SDWAN Tunnels form an ‘OMP core’
- Devices connected to centralized vSmarts (Default Region)

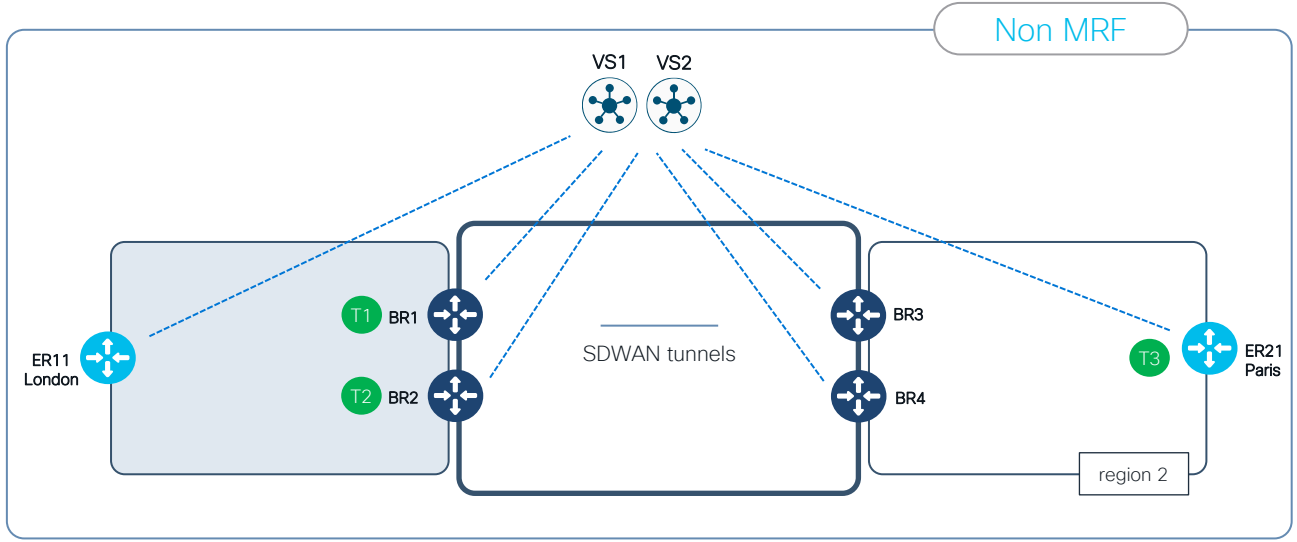
vSmart Connection

Routers connected to default region vSmart

```
ER11#sh sdwan OMP peer region-id
R -> routes received
I -> routes installed
S -> routes sent

TENANT                              DOMAIN    OVERLAY   SITE      REGION
ID        PEER              TYPE    ID        ID        ID        ID        STATE    UPTIME           R/I/S
-------------------------------------------------------------------------------------------------------------
0         10.0.0.30         vsmart  1         1         100       None      up       0:00:00:32       0/0/2


ER11#
```

```
ER21#sh sdwan OMP peer region-id
R -> routes received
I -> routes installed
S -> routes sent

TENANT                              DOMAIN    OVERLAY   SITE      REGION
ID        PEER              TYPE    ID        ID        ID        ID        STATE    UPTIME           R/I/S
-------------------------------------------------------------------------------------------------------------
0         10.0.0.30         vsmart  1         1         100       None      up       0:00:00:22       0/0/2


ER21#
```

Pre-Migration State Routes



ER11 Routing Table

Prefix	NH	Path	From
P1	T1 T2	-	VS1, VS2

- Prefixes advertised from SDWAN routers to centralized vSmart
- Prefixes/next-hop reflected to all devices in the overlay
- In this example, topology is built using advanced Control Plane Policies.
- Prefix P1 next-hop is statically changed from T3 to T1/T2

Logical Control Policy (OMP Core)

Region1 Branch Sites

TLOCs – Outbound Advertisements

Region1 Branches – All Colors
Region1 Gateways – All Colors
Default – reject

ROUTES – Outbound Advertisements

Region1 Branch Sites – Original TLOC
Region1 GW Sites – Original TLOC
Region2 branches – Region1 GW TLOC (mpls/inet)
Default – Reject

- No automatic configuration of Region
- Advanced Control Plane Policies – requires admin to know technical details of TLOCs, Routes and GW

Region1 GW Sites

TLOCs – Outbound Advertisements

Region1 Branches – All Colors
Region1 Gateways – All Colors
Region2 Gateways – private6 color
Default – reject

ROUTES – Outbound Advertisements

Region1 Branch Sites – Original TLOC
Region1 GW Sites – Original TLOC
Region2 branches – Region2 GW TLOC (private6)
Region3 branches – Region3 GW TLOC (private6)
[… etc …]

Default – Reject

Central policy

Pre-migration configuration

```
policy
lists
  tloc-list BR1_CORE_TLOC
   tloc 175.1.11.10 color
green encap ipsec
  !
  tloc-list BR1_TLOCS
   tloc 175.1.11.10 color lte
encap ipsec
   tloc 175.1.11.10 color 3g
encap ipsec
   tloc 175.1.11.10 color red
encap ipsec
   tloc 175.1.11.10 color
green encap ipsec
  !
  tloc-list BR2_CORE_TLOC
   tloc 175.2.13.10 color
green encap ipsec
  !
  tloc-list BR2_TLOCS
   tloc 175.2.13.10 color lte
encap ipsec
   tloc 175.2.13.10 color 3g
encap ipsec
   tloc 175.2.13.10 color
green encap ipsec
  !
  site-list AR1
   site-id 1100
   site-id 1300
  !
  site-list AR1_BR1
   site-id 1100
   site-id 11100
   site-id 1300
  !
```

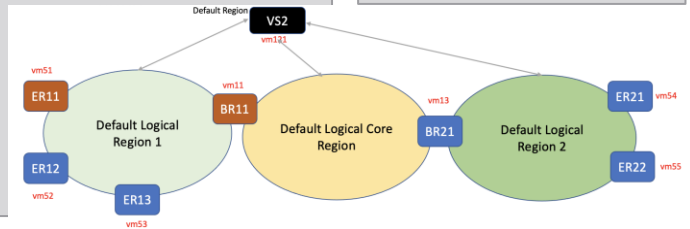
```
site-list AR1_BR2
   site-id 1100
   site-id 1300
   site-id 22100
  !
  site-list AR2
   site-id 2100
  !
  site-list BR1
   site-id 11100
  !
  site-list BR1_AR2
   site-id 11100
   site-id 2100
  !
  site-list BR1_BR2
   site-id 11100
   site-id 22100
  !
  site-list BR1_BR2_AR1
   site-id 1100
   site-id 11100
   site-id 1300
   site-id 22100
  !
  site-list BR1_BR2_AR2
   site-id 11100
   site-id 2100
   site-id 22100
  !
  site-list BR2
   site-id 22100
  !
  site-list BR2_AR2
   site-id 2100
   site-id 22100
  !
!
```

```
control-policy CP1
  sequence 1
   match tloc
    site-list AR1_BR1
   !
   action accept
   !
  !
  sequence 2
   match route
    site-list BR1_BR2_AR2
   !
   action accept
    set
     tloc-list BR1_TLOCS
    !
  !
  sequence 3
   match route
    site-list AR1
   !
   action accept
   !
  !
  default-action reject
!
```

```
control-policy CP2
  sequence 1
   match tloc
    site-list AR1_BR2
   !
   action accept
   !
  !
  sequence 2
   match route
    site-list AR1
   !
   action accept
   !
  !
  sequence 3
   match route
    site-list BR2_AR2
   !
   action accept
    set
     tloc-list BR2_CORE_TLOC
    !
   !
  !
  default-action reject
!
```

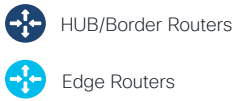
```
control-policy CP3
  sequence 1
   match tloc
    site-list BR1_AR2
   !
   action accept
   !
  !
  sequence 2
   match route
    site-list AR2
   !
   action accept
   !
  !
  sequence 3
   match route
    site-list AR1_BR1
   !
   action accept
    set
     tloc-list BR1_CORE_TLOC
    !
   !
  !
  default-action reject
!
```

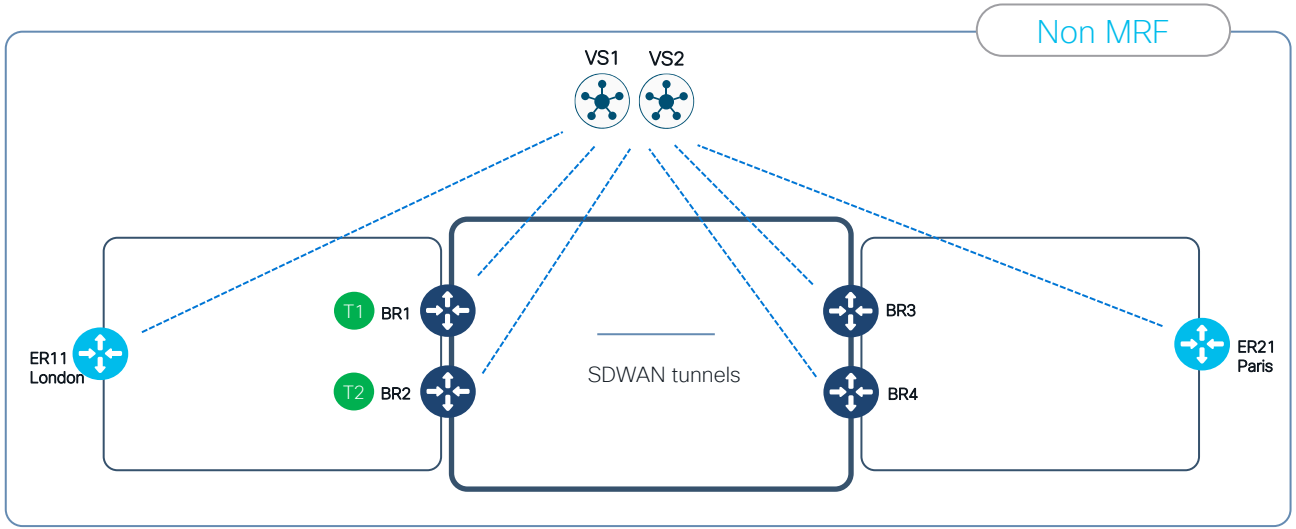
```
control-policy CP4
  sequence 1
   match tloc
    site-list BR2_AR2
   !
   action accept
   !
  !
  sequence 2
   match route
    site-list BR1_BR2_AR1
   !
   action accept
    set
     tloc-list BR2_TLOCS
    !
   !
  !
  sequence 3
   match route
    site-list AR2
   !
   action accept
   !
  !
  default-action reject
!
```



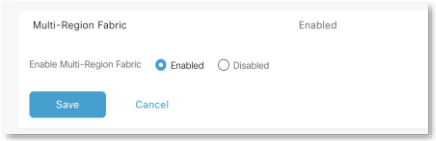

```
apply-policy
site-list AR1
  control-policy CP1 out
!
site-list AR2
  control-policy CP4 out
!
site-list BR1
  control-policy CP2 out
!
site-list BR2
  control-policy CP3 out
!
```

Step 1 : Enable MRF in vManage Settings



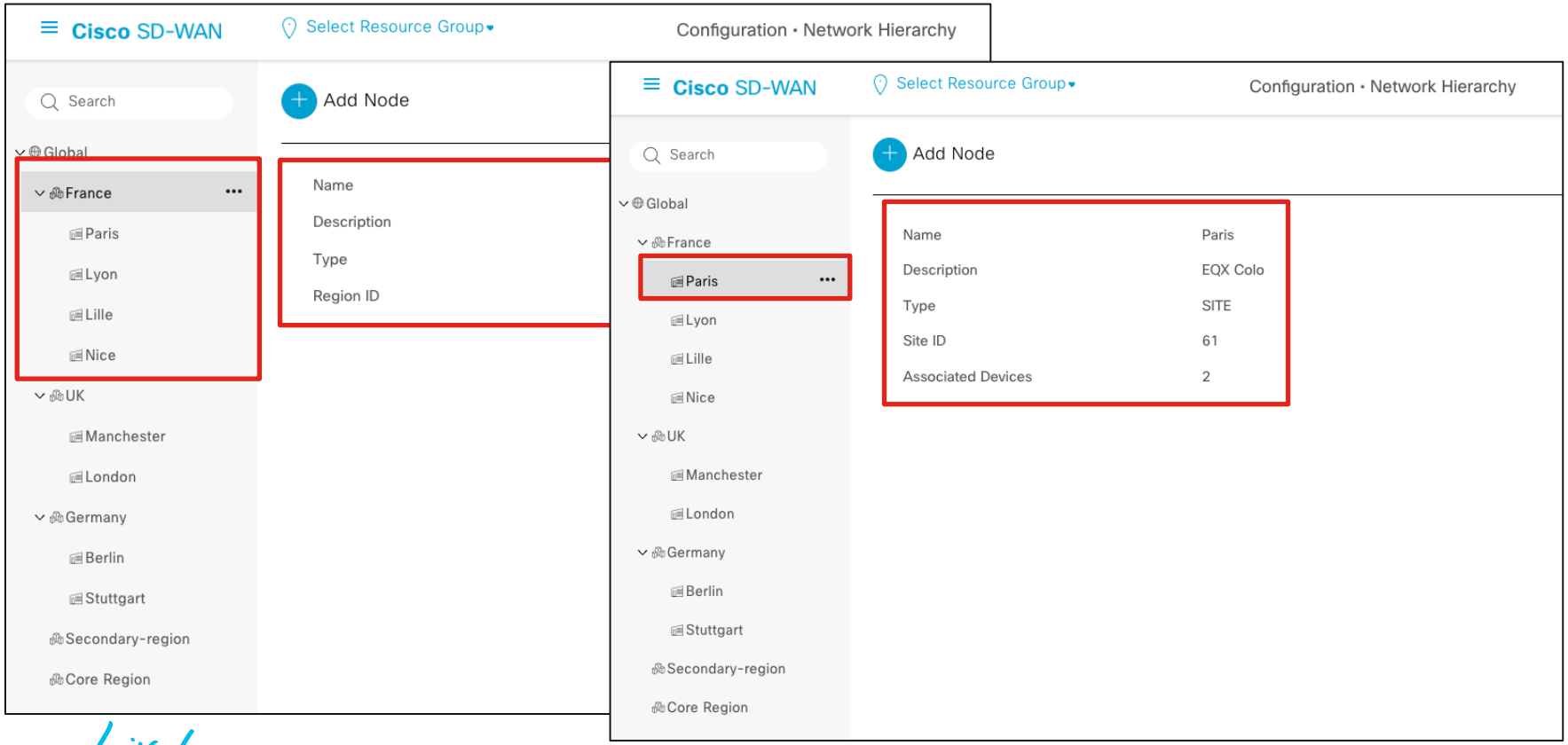


Enable MRF under Admin > Settings

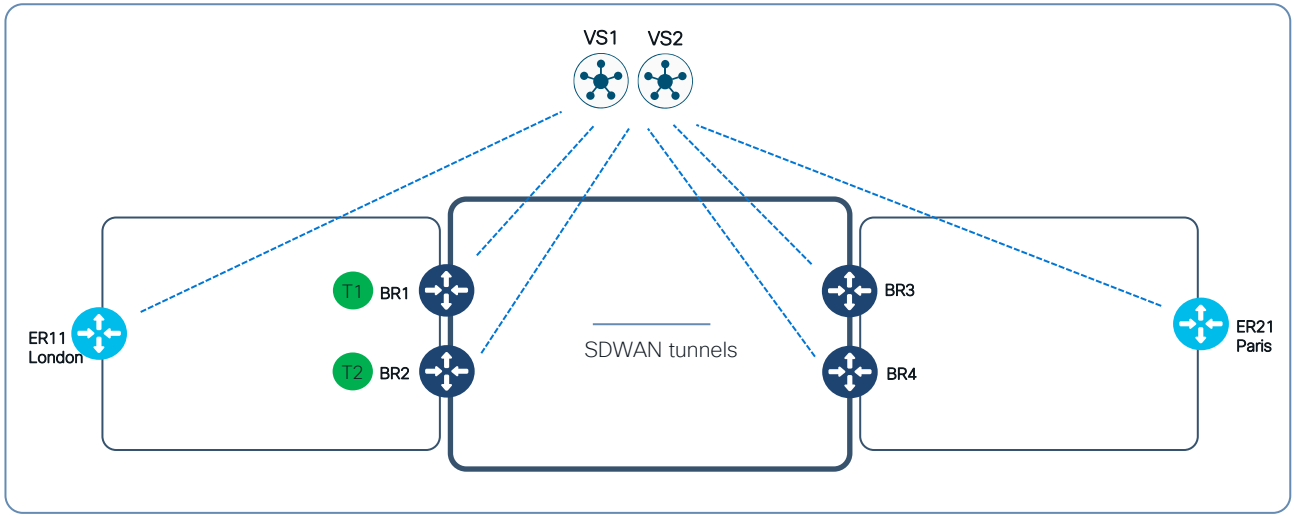


- Enable MRF in vManage Settings.
- This will display MRF parameters like region, roles in device templates
- No change on devices

Step 2 : Configure Regions in Network Hierarchy Manager (NHM)



Step 3 : Enable Migration Mode on BR and ER



Border Routers

Edge Routers

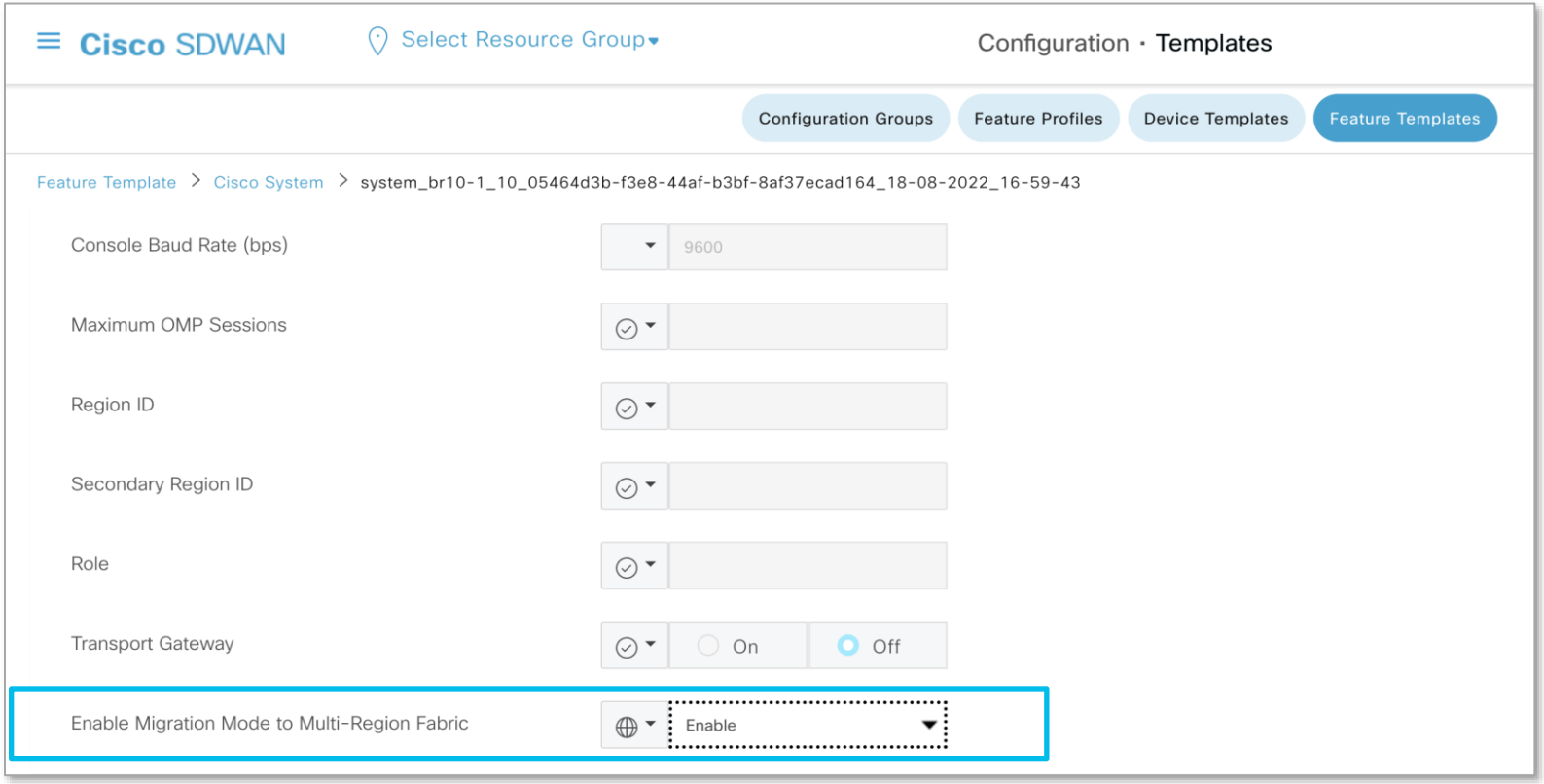
Control Connections

On BRs and ERs

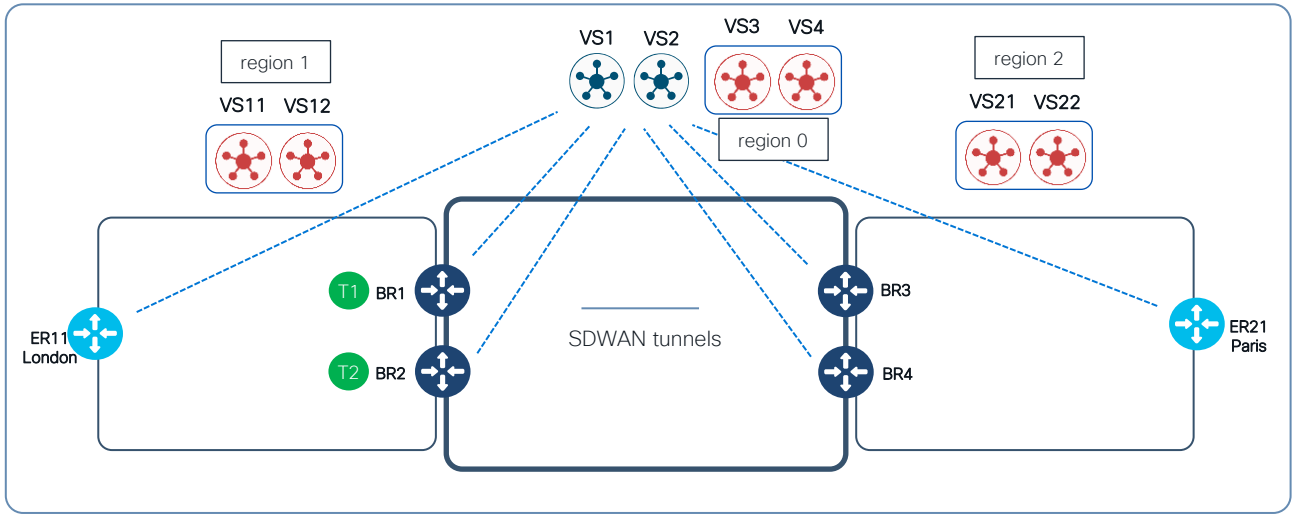
```
system
 multi-region-fabric
  migration-mode enabled
```

- Border Router and Edge Router system feature templates
- Under system - **enable migration-mode enabled**
- There will be no impact on any communication after user configures migration mode

Step 3 : Enable Migration Mode on BR and ER



Step 4 : Add Regional vSmarts



vSmarts

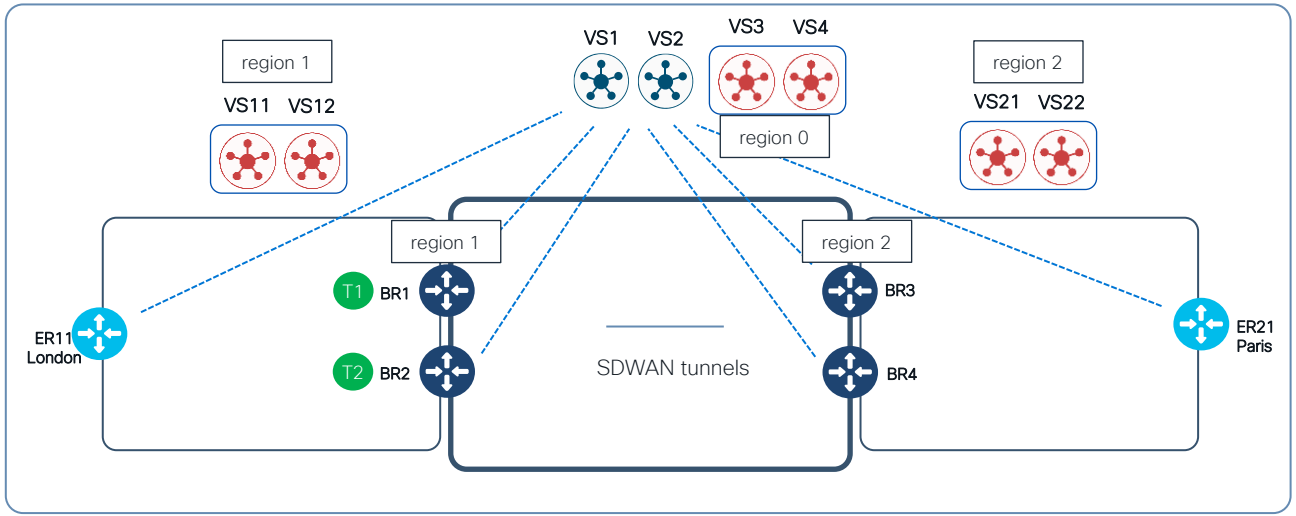
```
system
 host-name              VS3
 system-ip              1.1.0.5
 site-id                1
 region 0

system
 host-name              VS11
 system-ip              1.1.1.5
 site-id                10
 region 1

system
 host-name              VS21
 system-ip              1.1.2.5
 site-id                20
 region 2
```

- Add additional vSmarts for core
- Add vSmarts for access regions depending on network sizing
  - Default vSmarts remain intact (for migration period; can be re-purposed later)
  - Access region vSmart can be shared
- Configure appropriate regions on vSmarts

Distributed vSmart sharing – Examples

vSmart Deployment cases in Regions		Supported ?	Why ?
vSmart Pair A, Region#	vSmart Pair B, Region#		
1,2	1,2	Y	vSmarts can be shared across same set of regions.
0	1,2	Y	vSmart for region 0 is separate from vSmart serving access-regions. A and B will not peer.
1,2	3,4	Y	vSmarts serving different access regions. A and B will not peer.
1,2,3	1,2,4	N	vSmarts have some partial overlapping regions
0,1	0,1	N	Region 0 can't be shared with access region vSmarts
0,1,2	1,2,3	N	• Region 0 can't be shared with access region vSmarts • Both vSmarts have some partial overlapping regions

Step 5 : Configure MRF config on BRs



Configure Transport interface to the core

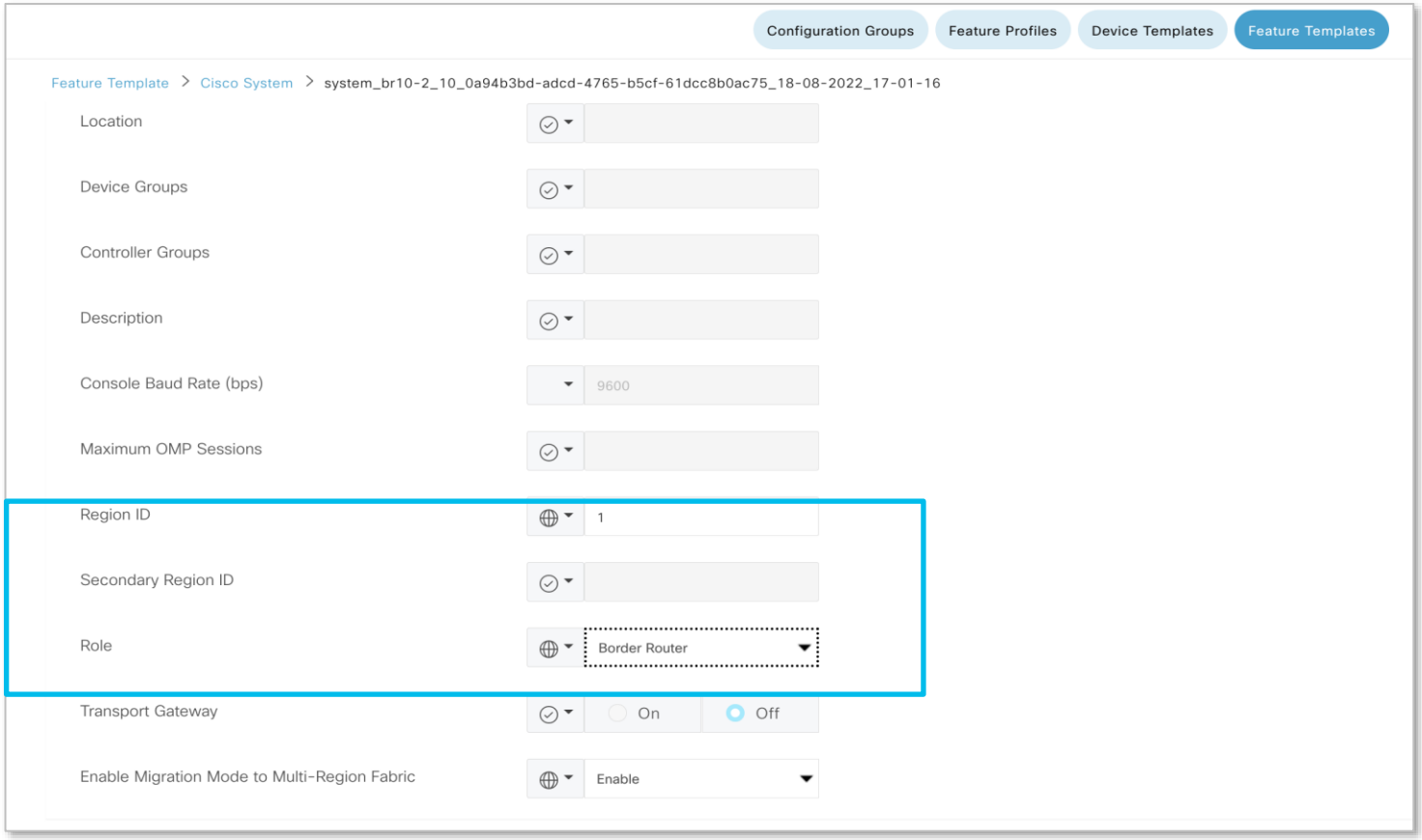
BRx

```
system
 region 1
 role border-router
 multi-region-fabric
  migration-mode enabled
!
sdwan
 interface GigabitEthernet1
  tunnel-interface
   region core
   color private6
!
 interface GigabitEthernet2
  tunnel-interface
   color biz-internet
!
```

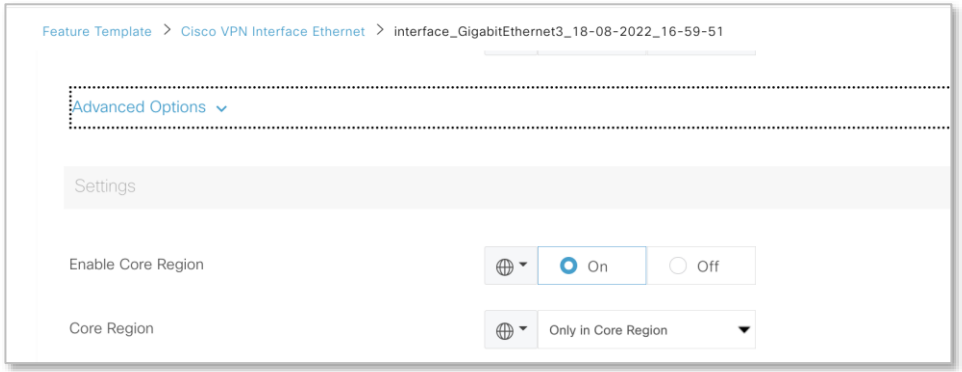
All transport interfaces in Access Region

- Enabling BR and assigning region
  - Core region
- BR now are ready to
  - Interconnect the access-reg to the core and vice-versa (re-origination)
  - Interconnect existing/non-migrated sites to migrated sites
- Optional- core shared

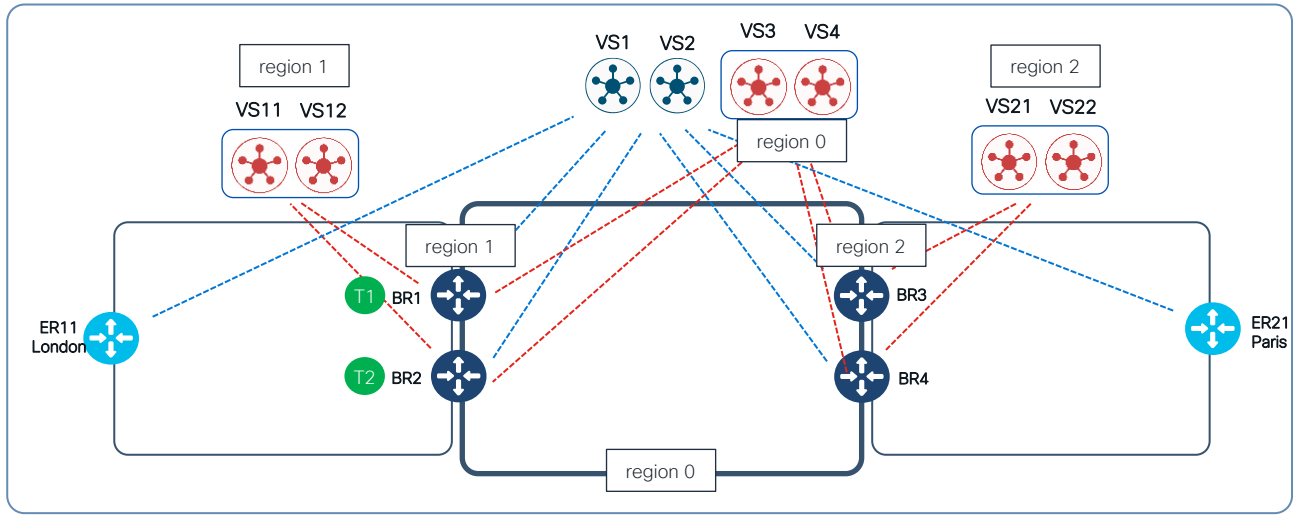
Step 5 : MRF configurations on BRs



Step 5 : MRF config on BRs–role/region



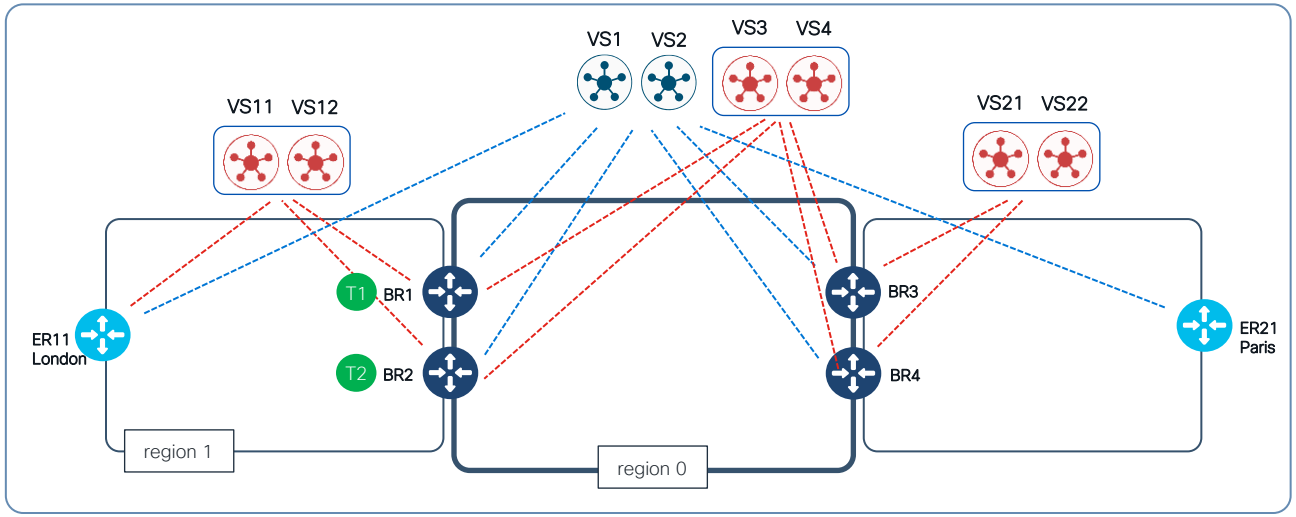
Border Routers connect to new region vSmarts



Border Routers
Edge Routers
Control Connections
Regional Control Connections

- Config change pushed to all BR devices
- Border Routers connect to access and core region vSmart but keep existing connections to default region vSmarts
- Prefixes still advertised from old centralized vSmarts VS1/VS2

Step 6 : Migrate Edge Routers in Region 1 (London)



Border Routers

Edge Routers

Control Connections

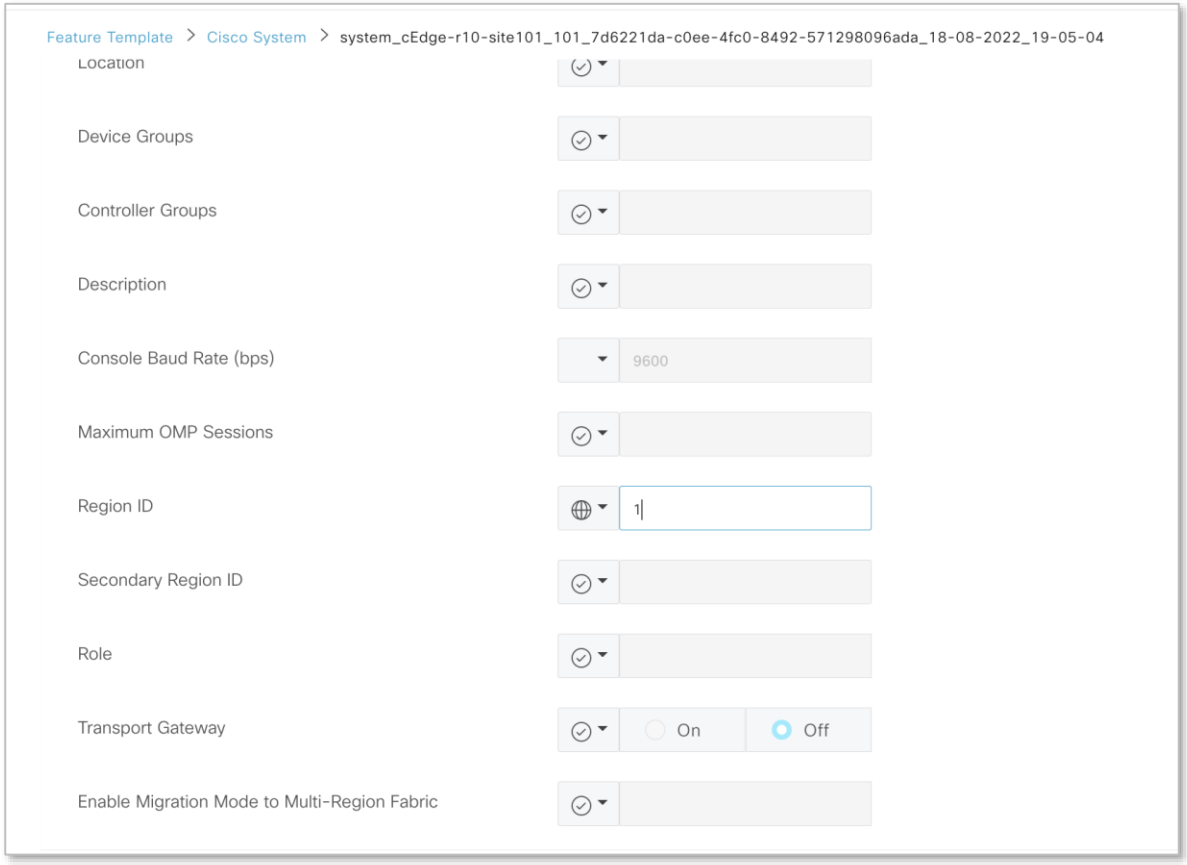
Regional Control Connections

ER

```
system
 region 1
 role edge-router
 multi-region-fabric
  migration-mode
enabled
```

- Config change pushed to devices in region1
- Configure secondary region (if required)
- Devices in region1 connect to region 1 vSmart but keep existing connections to old vSmarts

Step 6 : Migrate Edge Routers in Region1



Region 1 – ER11(London)

```
ER11#sh sdwan OMP peer region-id
R -> routes received
I -> routes installed
S -> routes sent

TENANT                              DOMAIN    OVERLAY   SITE      REGION
ID        PEER             TYPE     ID        ID        ID        ID        STATE    UPTIME           R/I/S
-------------------------------------------------------------------------------------------------------------
0         10.0.0.22        vsmart   1         1         100       1         up       0:00:00:22       24/12/4
0         10.0.0.30        vsmart   1         1         100       None      up       0:00:00:18       2/1/4


ER11#
```

- ER11 migrated to MRF with migration-mode enabled
- Connected to both region-aware vSmart and old vSmart
- Verify connectivity between both regions' edges

Region 2 – ER21(Paris)—still not migrated

```
ER21#sh sdwan OMP peer region-id
R -> routes received
I -> routes installed
S -> routes sent

TENANT                                DOMAIN    OVERLAY   SITE      REGION
ID        PEER            TYPE        ID        ID        ID        ID        STATE    UPTIME           R/I/S
-------------------------------------------------------------------------------------------------------------
0         10.0.0.30       vsmart      1         1         100       None      up       0:00:00:22       0/0/2


ER21#
```

- ER21 not migrated to MRF
- Connected to old vSmart
- Advertises routes to old vSmart

Region 1 – London (ER11) - OMP Route

Routing Table

Prefix	NH	Path	From
P1	T1 T2	-	VS1, VS2


```
ER11#sh sdwan OMP route 10.10.10.105/32
Code:
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid
Stg -> staged
IA  -> On-demand inactive
U   -> TLOC unresolved
BR-R -> border-router reoriginated
TGW-R -> transport-gateway reoriginated

                                                                                                                                  AFFINITY
                                                    PATH                     ATTRIBUTE                                                    GROUP
TENANT    VPN    PREFIX              FROM PEER      ID     LABEL    STATUS    TYPE        TLOC IP        COLOR            ENCAP  PREFERENCE  NUMBER     REGION ID   REGION PATH
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
----
0         10     10.10.10.105/32     10.0.0.30      1      1002     C,I,R     installed   10.0.0.105     mpls             ipsec  -           None       None        -
                                     10.0.0.30      2      1002     R         installed   10.0.0.105     biz-internet     ipsec  -           None       None        -


ER11#
```

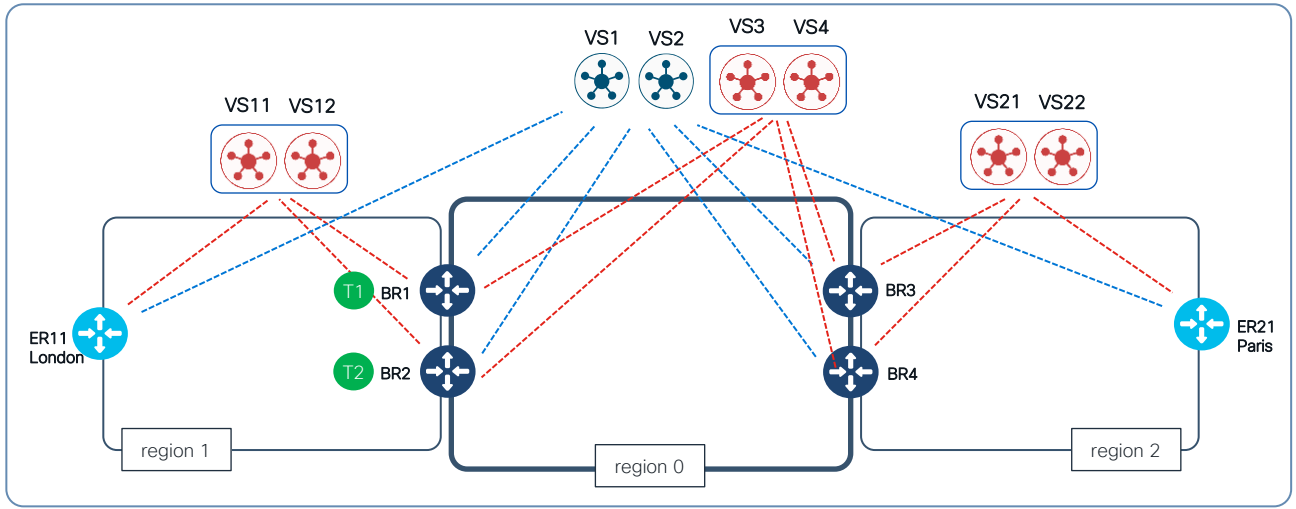
Region2 not migrated - P1 prefix still advertised to/from old vSmarts VS1/VS2 → ER11 learns ER21 route from old vSmart

Step 6b – Migrate Edge Routers in Paris (Region2)

OMP will prefer region aware route vs route from default region

London Routing Table

Prefix	NH	Path	From
P1	T1 T2	1 0 2	VS11 VS12 (C,I,R)
P1	T1 T2	None	VS1 VS2



- Devices in region2 connect to access region2 vSmart but keep existing connections to default vSmarts
- P1 advertised to old vSmarts and new region vSmarts VS21-VS22
- ER11 receives P1 prefix from VS11-VS12 through BR re-origination and also from VS1-VS2

Region 2 – ER21 (Paris)

```
ER21#sh sdwan OMP peer region-id
R -> routes received
I -> routes installed
S -> routes sent

TENANT                              DOMAIN    OVERLAY   SITE      REGION
ID        PEER             TYPE     ID        ID        ID        ID        STATE    UPTIME           R/I/S
-------------------------------------------------------------------------------------------------------------
0         10.0.0.23        vsmart   1         1         100       2         up       0:00:00:05       28/14/2
0         10.0.0.30        vsmart   1         1         100       None      up       0:00:00:05       4/0/2


ER21#
```

- ER21 now migrated to MRF with migration-mode enabled
- Connected to both region vSmart and old vSmart
- Advertises route to both vSmart (region-aware and current/default)

For Reference

Region 2 – ER21

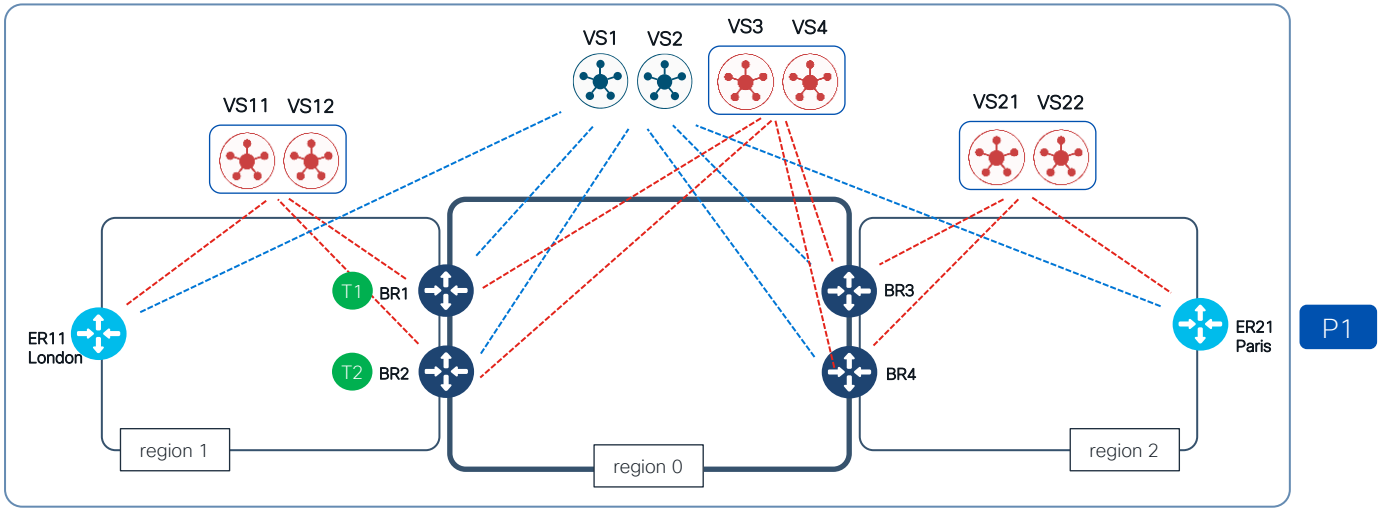
P1 10.10.10.105

```
ER11#sh sdwan OMP route 10.10.10.105/32
Code:
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid
Stg -> staged
IA  -> On-demand inactive
U   -> TLOC unresolved
BR-R -> border-router reoriginated
TGW-R -> transport-gateway reoriginated

                                                                                                                            AFFINITY
                                                 PATH                      ATTRIBUTE                                                GROUP
TENANT    VPN    PREFIX              FROM PEER        ID     LABEL    STATUS    TYPE       TLOC IP          COLOR            ENCAP  PREFERENCE  NUMBER      REGION ID   REGION PATH
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
0         10     10.10.10.105/32     10.0.0.22        9      1003     C,I,R     installed  10.0.0.61        biz-internet     ipsec  -           None        1             1 0 2
                                     10.0.0.30        10     1003     R         installed  10.0.0.61        biz-internet     ipsec  -           None        None          -

ER11#
```

ER11 now learns route from region vSmart with Region path is [1 0 2]

Wrap-up : Clean-up Configs

Remove Migration Mode from the BRs → Remove Migration Mode configs from the ERs. → Decommission or Re-purpose the Default Region vSmart. → De-activate hop-by-hop centralized policies

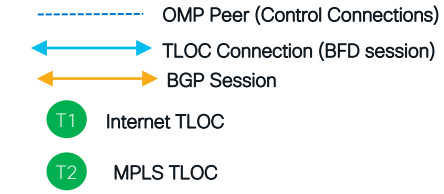


Important

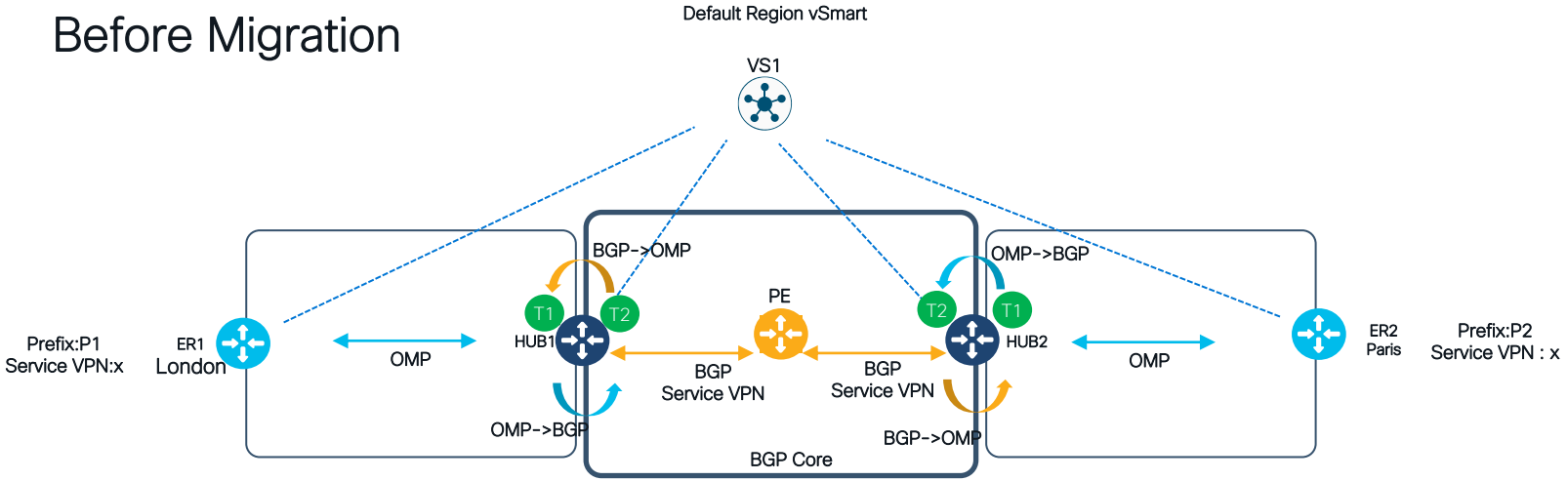
- Pay close attention to your pre-MRF control policies and their intent
- Update control policies during the course of migration to avoid blocking routes/TLOCs originated by Borders
- Test out your migration plan with production configs in your lab

Migration Steps
For BGP Core

Sample Topology



Before Migration



- BGP-based core
- OMP<->BGP redistribution
- Control policy to route traffic

Logical Control Policy (BGP Core)

Region1 Branch Sites

TLOCs – Outbound Advertisements

Region1 Branches – All Colors
Region1 Gateways – All Colors
Default – reject

ROUTES – Outbound Advertisements

Region1 Branch Sites – Original TLOC
Region1 GW Sites – Original TLOC
Region2 branches – Region1 GW TLOC (mpls/inet)
Default – Reject

Region1 GW Sites

TLOCs – Outbound Advertisements

Region1 Branches – All Colors
Region1 Gateways – All Colors
Default – reject

ROUTES – Outbound Advertisements

Region1 Branch Sites – Original TLOC
Region1 GW Sites – Original TLOC
[… etc …]

Default – Reject

- No automatic configuration of Region
- Advanced Control Plane Policies – requires admin to know technical details of TLOCs, Routes and GW

Sample Policy with 2 regions

```
policy
lists
  tloc-list BR1_CORE_TLOC
   tloc 175.1.11.10 color green encap
ipsec
  !
  tloc-list BR1_TLOCS
   tloc 175.1.11.10 color lte encap ipsec
   tloc 175.1.11.10 color 3g encap ipsec
   tloc 175.1.11.10 color red encap ipsec
  !
  tloc-list BR2_CORE_TLOC
   tloc 175.2.13.10 color green encap
ipsec
  !
  tloc-list BR2_TLOCS
   tloc 175.2.13.10 color lte encap ipsec
   tloc 175.2.13.10 color 3g encap ipsec
  !
  site-list AR1
   site-id 1100
   site-id 1300
  !
  site-list AR1_BR1
   site-id 1100
   site-id 11100
   site-id 1300
  !
```

```
site-list AR1_BR2
   site-id 1100
   site-id 1300
   site-id 22100
  !
  site-list AR2
   site-id 2100
  !
  site-list BR1
   site-id 11100
  !
  site-list BR1_AR2
   site-id 11100
   site-id 2100
  !
  site-list BR1_BR2
   site-id 11100
   site-id 22100
  !
  site-list BR1_BR2_AR1
   site-id 1100
   site-id 11100
   site-id 1300
   site-id 22100
  !
  site-list BR1_BR2_AR2
   site-id 11100
   site-id 2100
   site-id 22100
  !
  site-list BR2
   site-id 22100
  !
  site-list BR2_AR2
   site-id 2100
   site-id 22100
  !
!
```

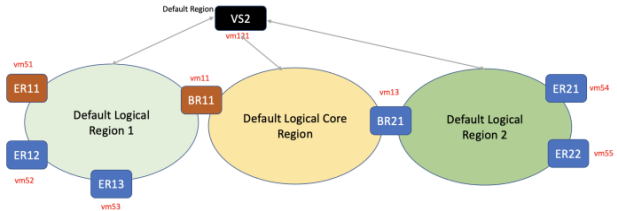
```
control-policy CP1
  sequence 1
   match tloc
    site-list AR1_BR1
   !
   action accept
   !
  !
  sequence 2
   match route
    site-list BR2_AR2
   !
   action accept
    set
     tloc-list BR1_TLOCS
    !
   !
  sequence 3
   match route
    site-list AR1_BR1
   !
   action accept
   !
  !
  default-action reject
!
```

```
control-policy CP2
  sequence 1
   match tloc
    site-list AR1_BR1
   !
   action accept
   !
  !
  sequence 2
   match route
    site-list AR1_BR1
   !
   action accept
   !
  !
  default-action
reject
!
```

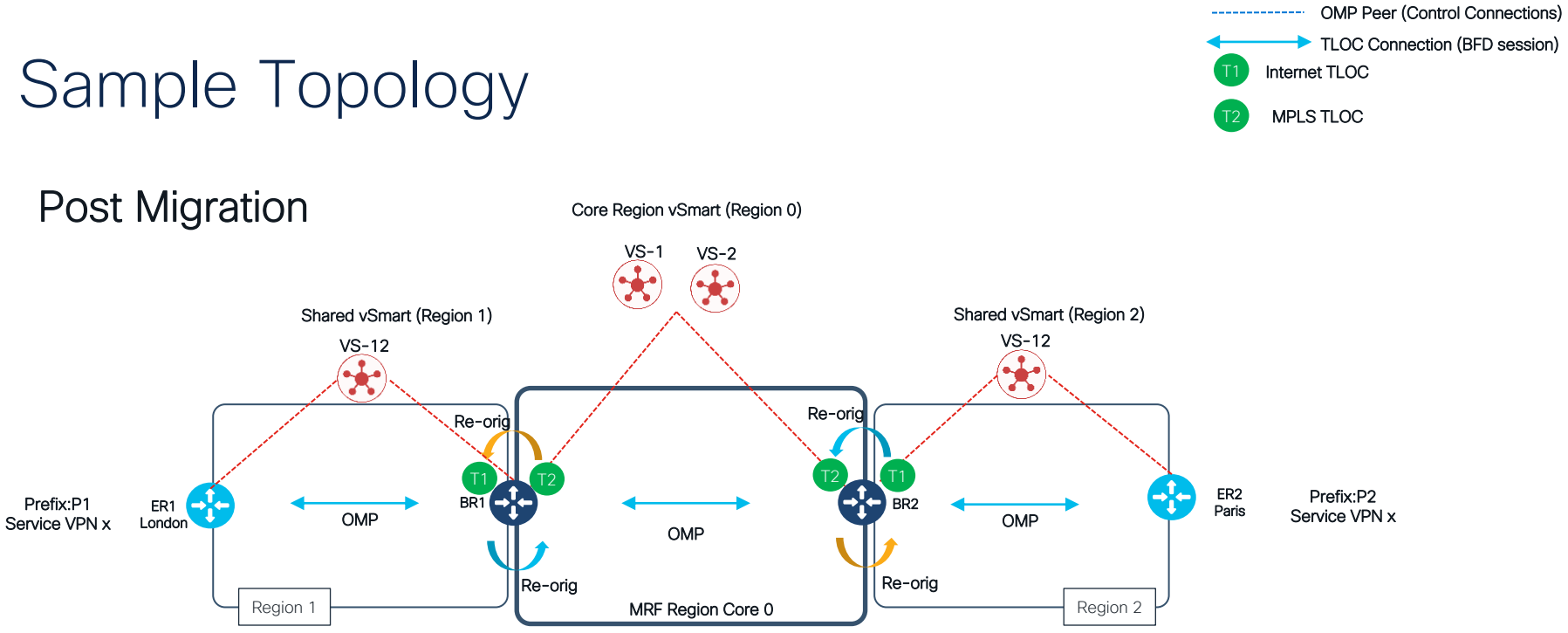
```
control-policy CP3
  sequence 1
   match tloc
    site-list BR2_AR2
   !
   action accept
   !
  !
  sequence 2
   match route
    site-list BR2_AR2
   !
   action accept
   !
  !
  default-action reject
!
```

```
control-policy CP4
  sequence 1
   match tloc
    site-list BR2_AR2
   !
   action accept
   !
  !
  sequence 2
   match route
    site-list AR1_BR1
   !
   action accept
    set
     tloc-list BR2_TLOCS
    !
   !
  !
  sequence 3
   match route
    site-list BR2_AR2
   !
   action accept
   !
  !
  default-action reject
!
!
```

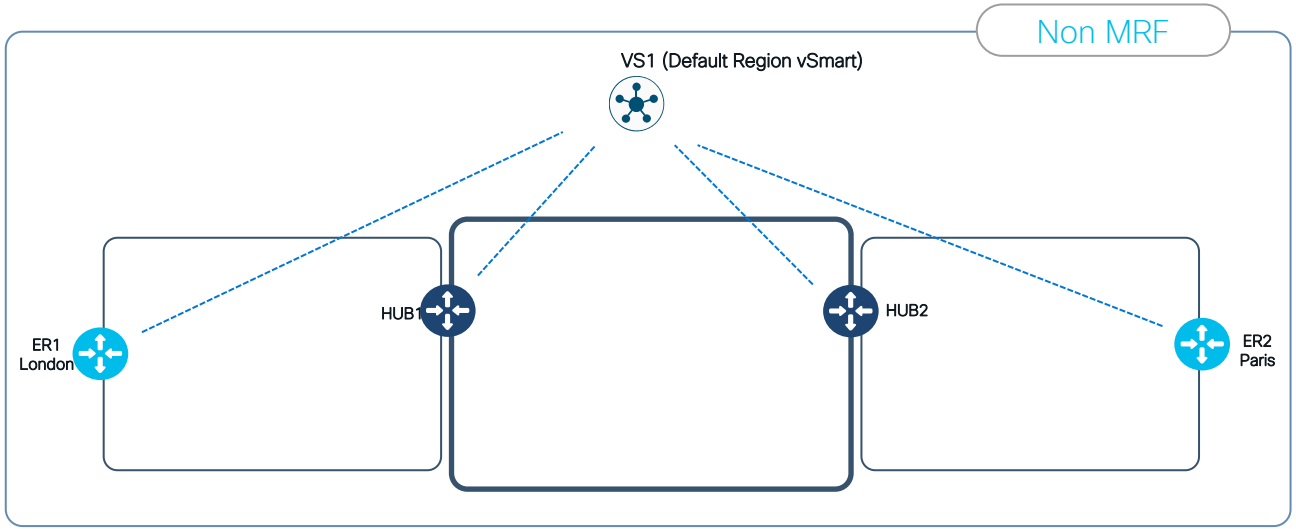
```
apply-policy
site-list AR1
  control-policy CP1 out
!
site-list AR2
  control-policy CP4 out
!
site-list BR1
  control-policy CP2 out
!
site-list BR2
  control-policy CP3 out
!
```

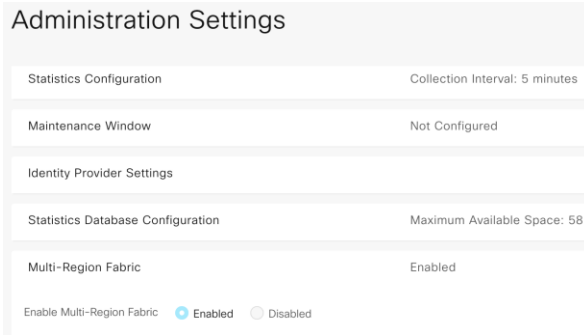


Sample Topology



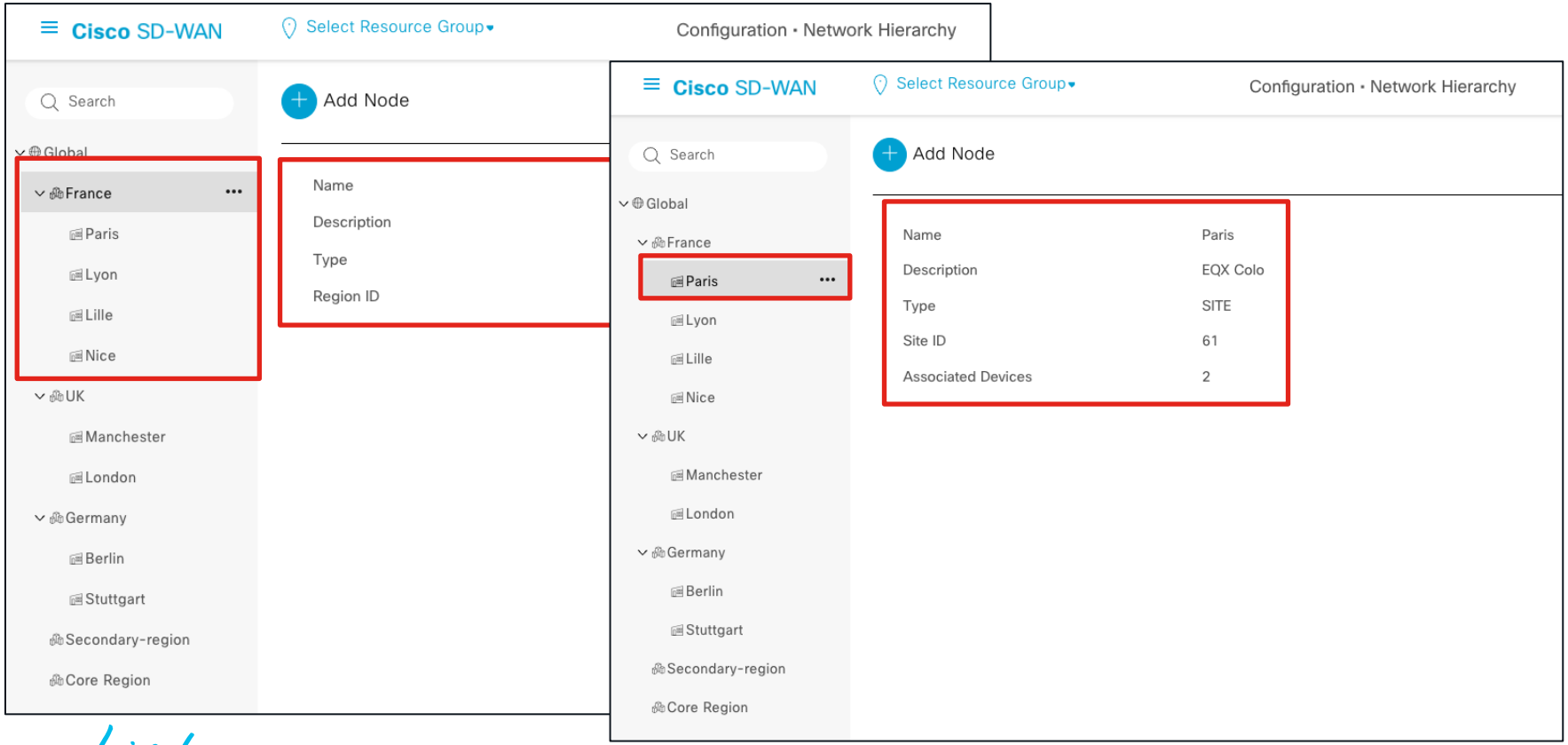
Step 1a – Enable MRF in vManage Settings





- Enable MRF in vManage Settings.
- This will display MRF parameters like region, roles in configuration templates
- No config changes propagated to devices, yet

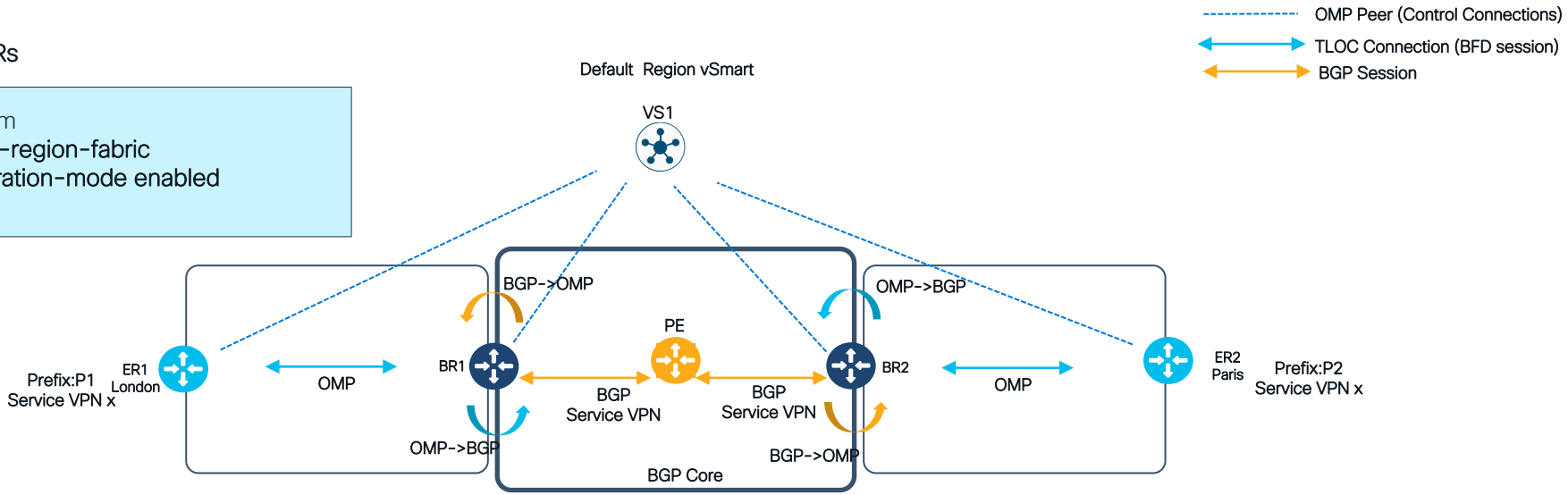
Step 2 : Configure Regions in Network Hierarchy Manager (NHM)



Step3: Enable Migration Mode on all Branches

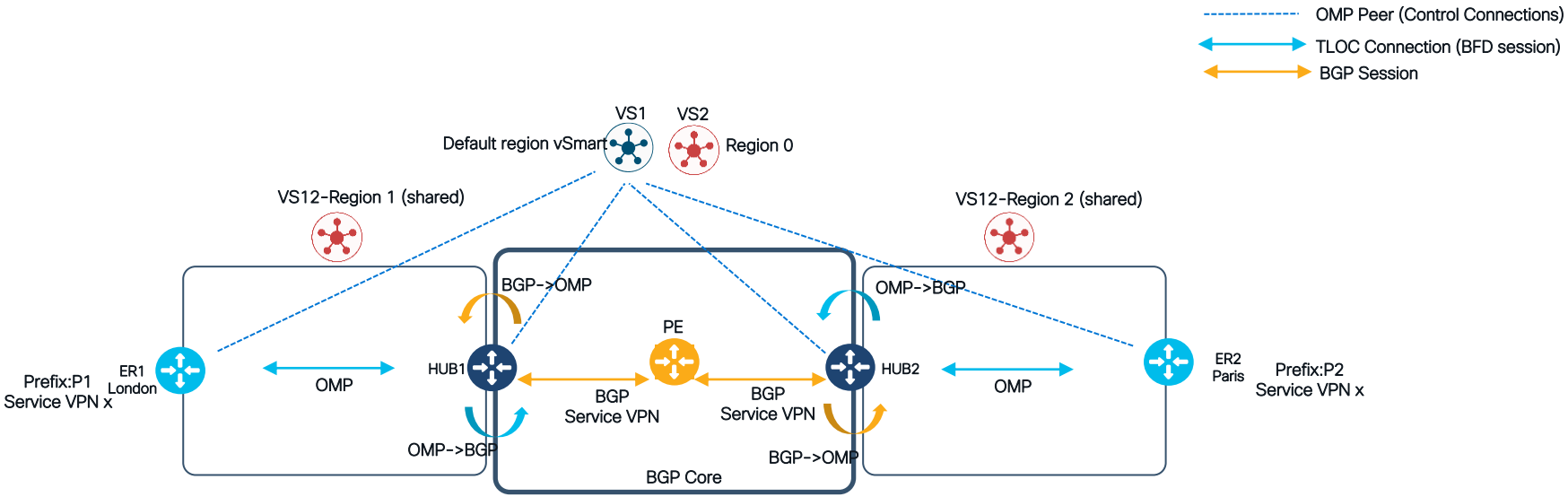
On ERs

```
system
 multi-region-fabric
  migration-mode enabled
```



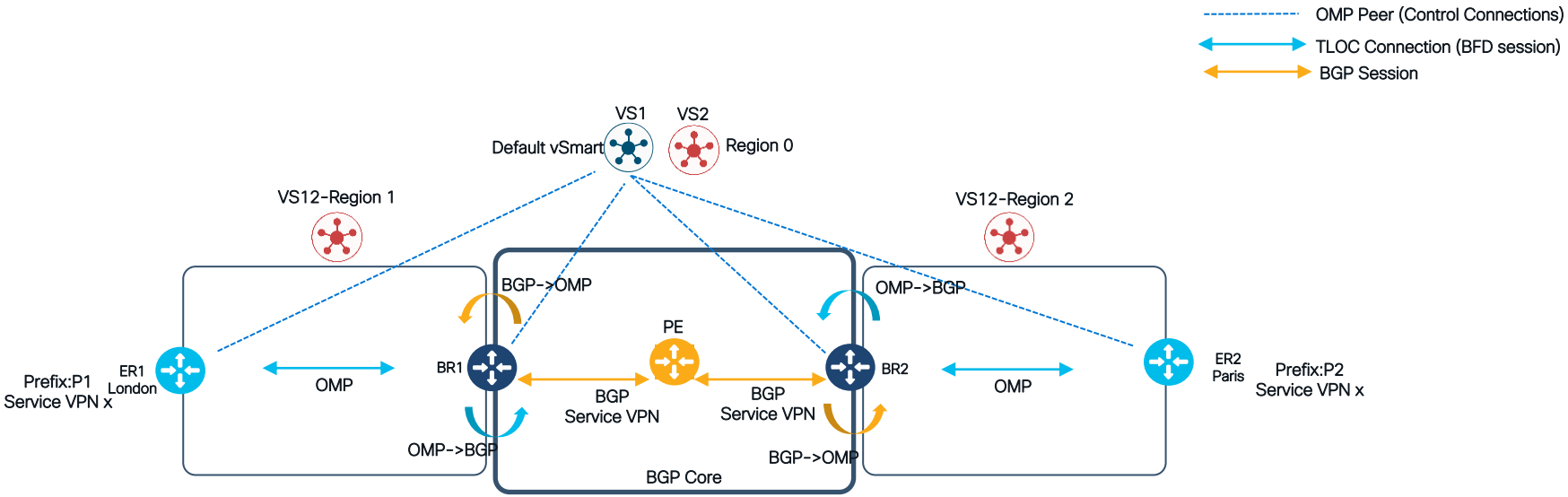
No change to OMP peering

Step3: Provisions vSmarts for Core and Access Regions



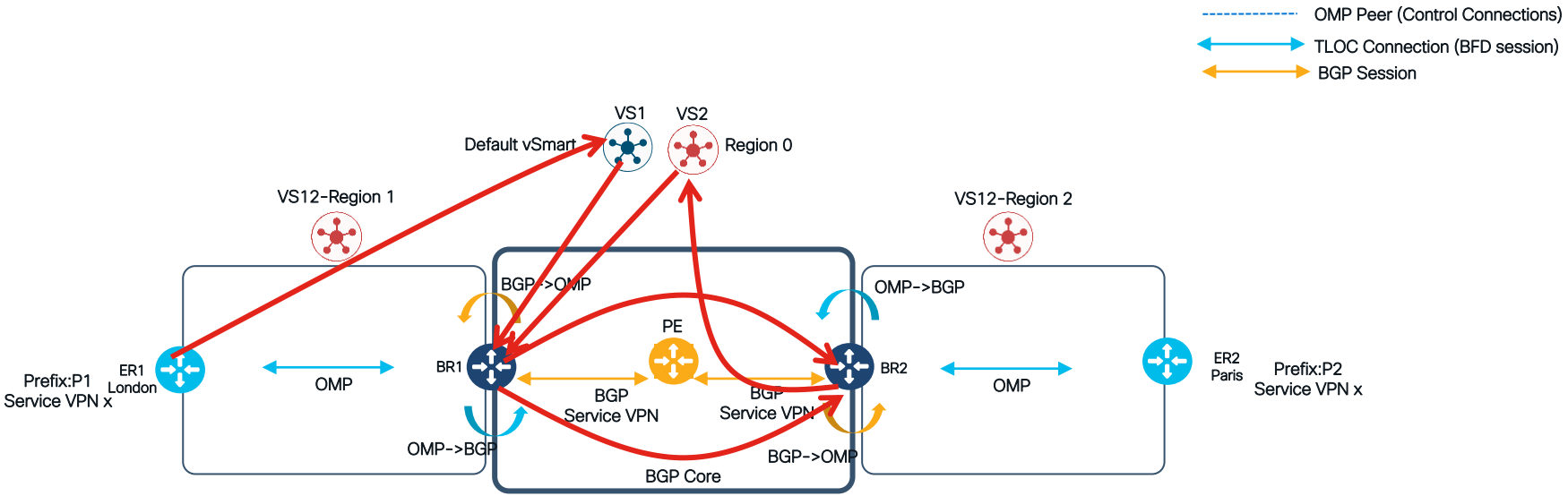
Recommended: Add new vSmarts

Step4: We will now start using Migration Community X



- Unique in the network
- Range:1-4294967295

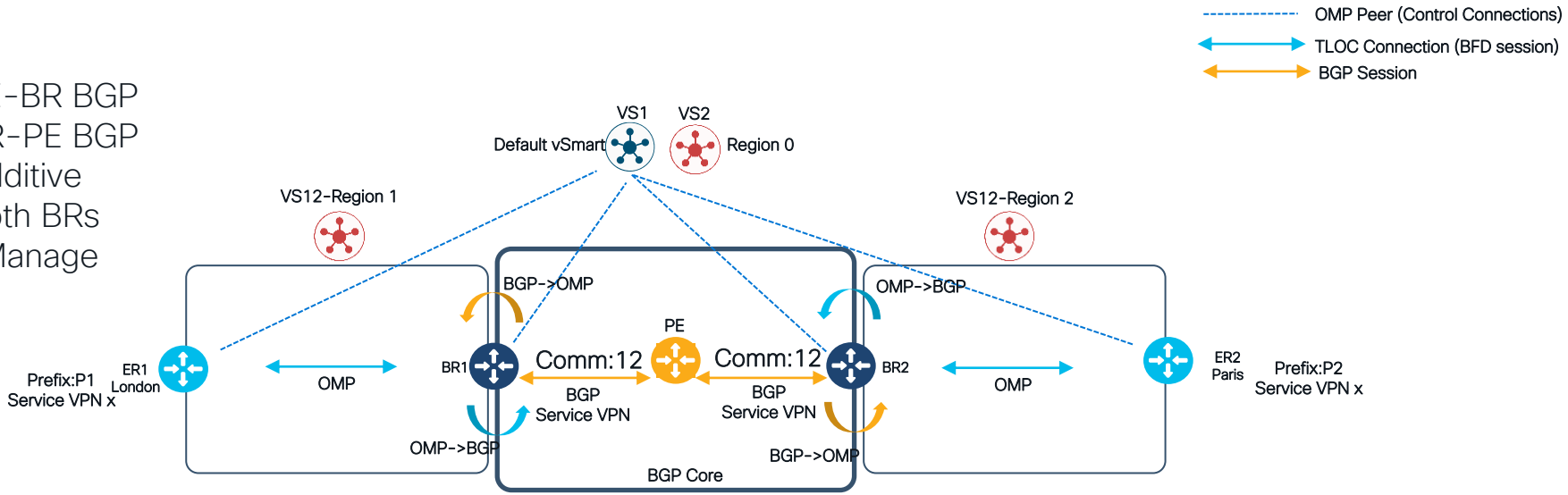
What can go wrong without using Mig Comm-Looping



- Region-aware OMP routes are preferred over default region OMP routes
- BR2 will start advertising routes from London as self-originated

Step5: Set Migration Community between BGP neighbors on BRs and PEs

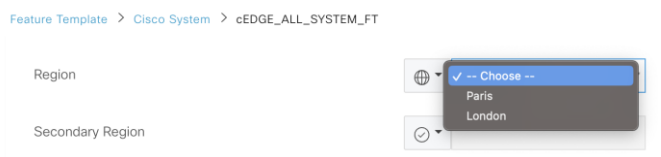
- PE-BR BGP
- BR-PE BGP
- Additive
- Both BRs
- vManage

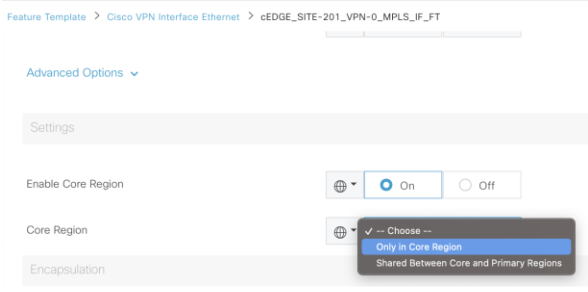


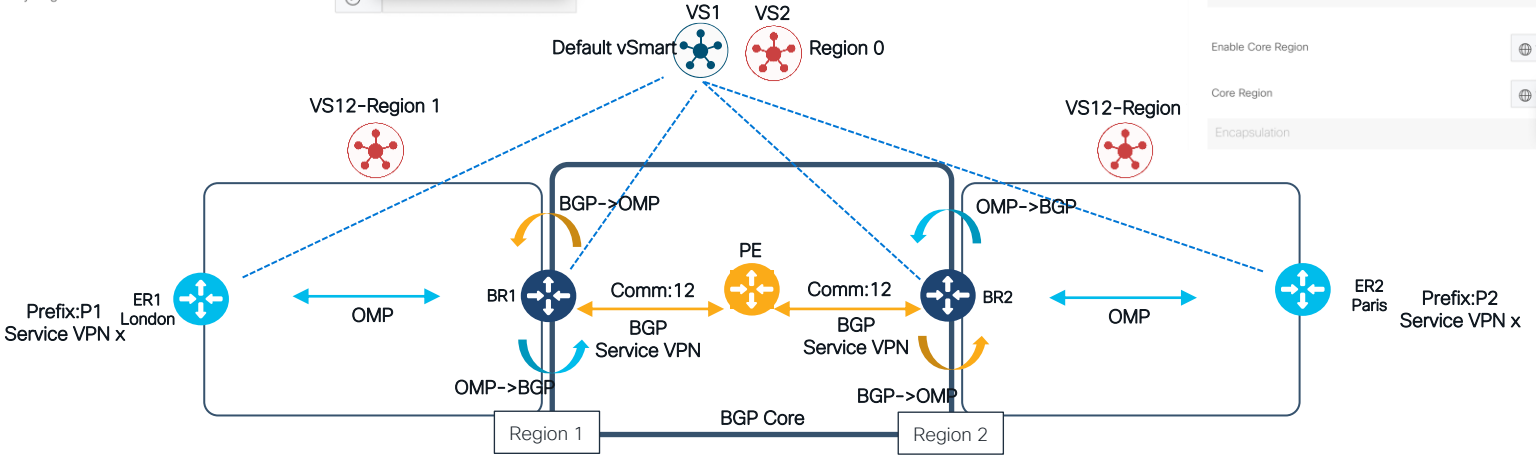

```
route-map APPEND-MIG-COMM permit
1
 set community 12 additive
```

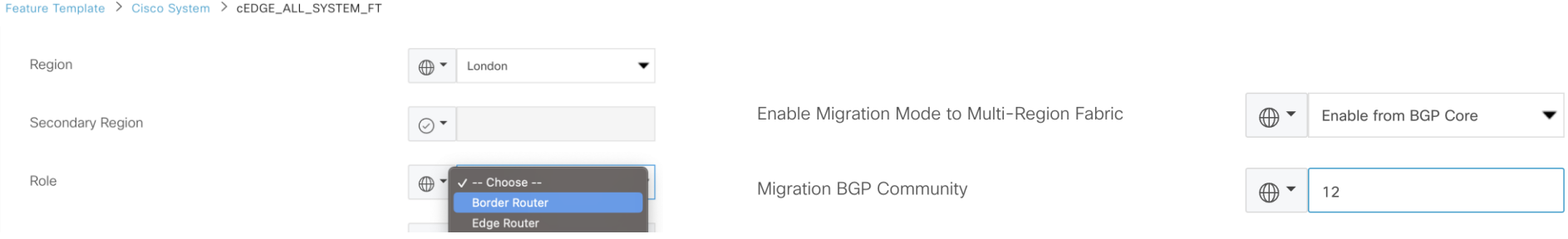
```
router BGP 2
address-family ipv4 vrf 10
propagate-community
neighbor <PE-BR-PE> send-community
neighbor < PE-BR-PE > route-map APPEND-MIG-COMM out
```

Step6: Enable Migration Mode with Comm X on BR

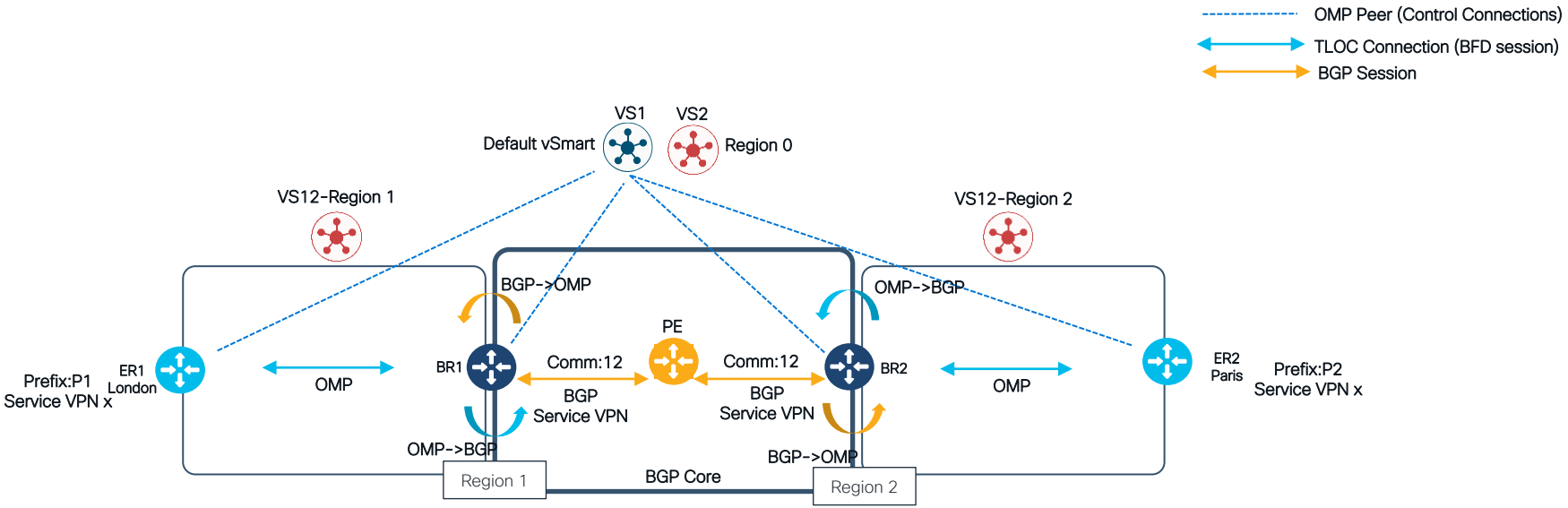








Step6: Match MIG comm and redistribute OMP->BGP

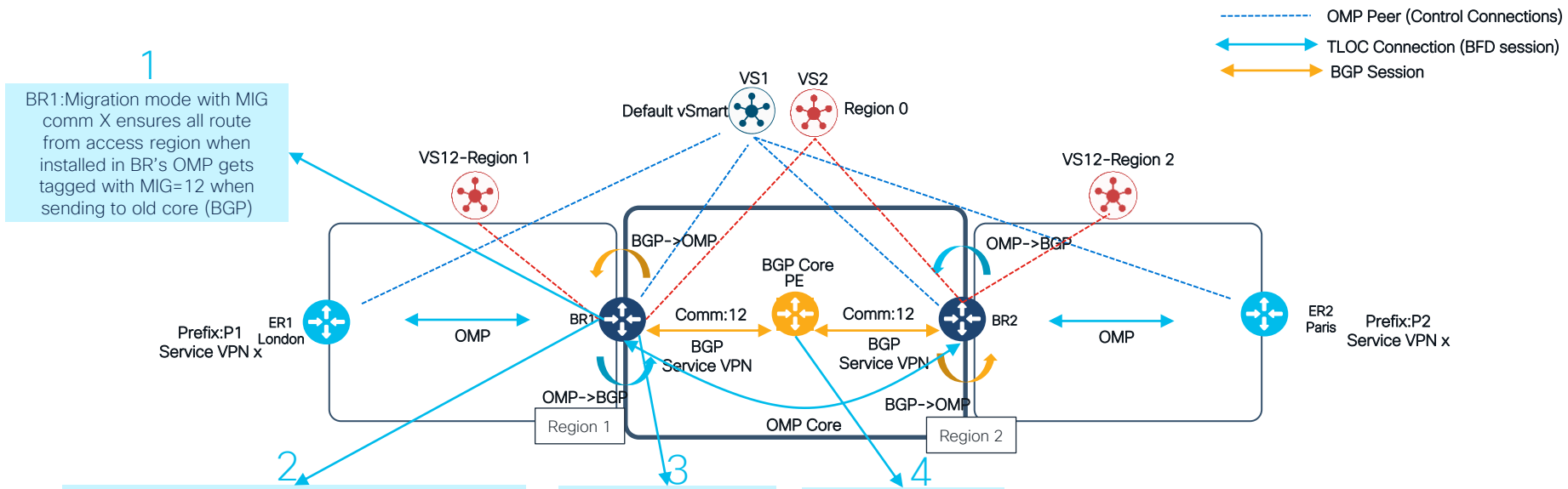



```
ip community-list standard MIG-COMM permit 12
```

```
route-map MATCH-MIG-COMM permit 1
 match community MIG-COMM
```

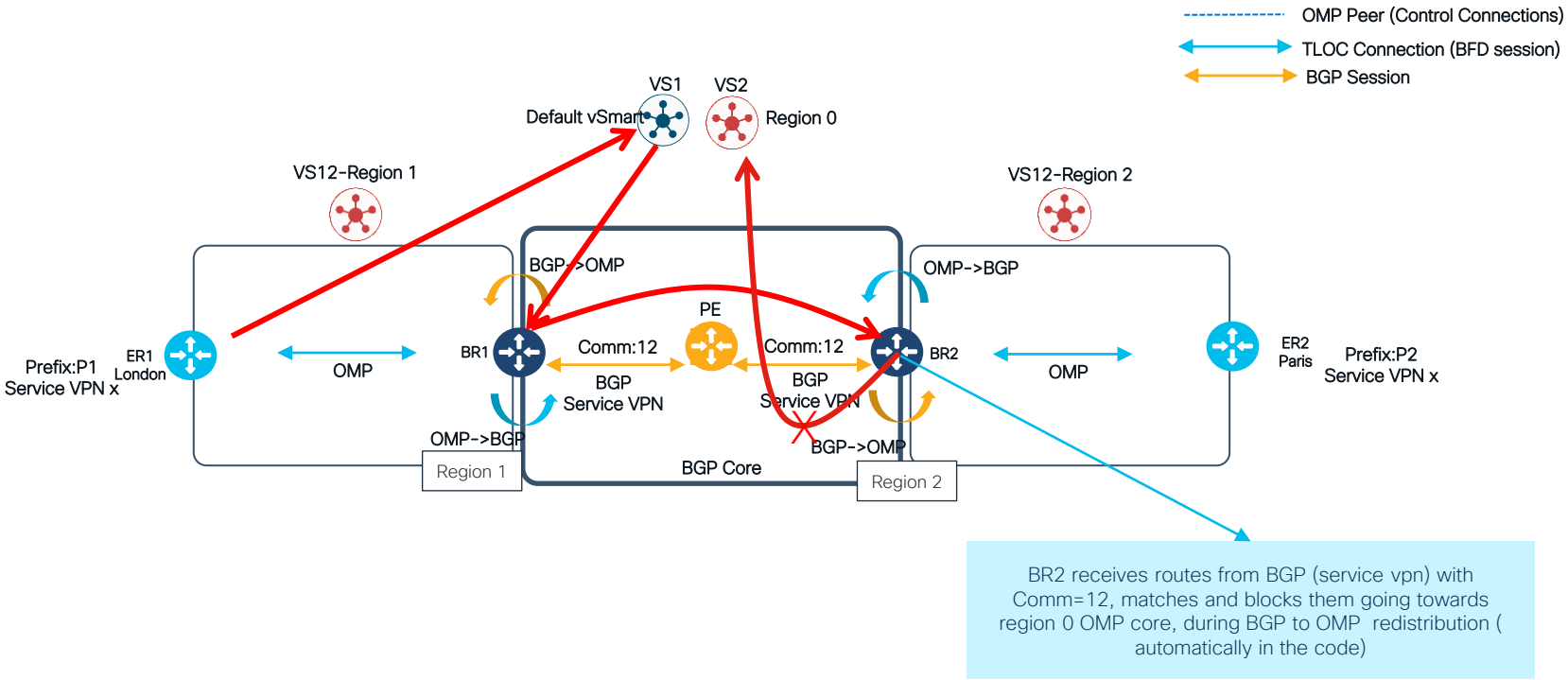
```
router BGP 1 BGP
neighbor <PE> remote-as 12
 address-family ipv4 vrf 10
  redistribute OMP route-map MATCH-MIG-COMM
```

Step6: So, what have we done so far ? ☺

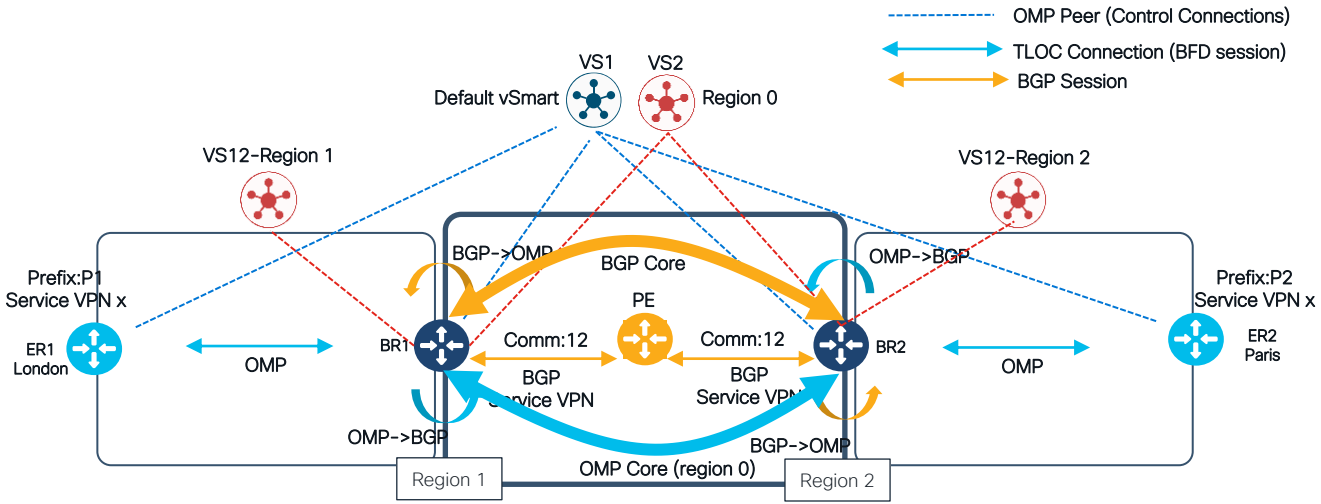


Same will be done on BR2

Step6: So, what have we done till now ? ☺



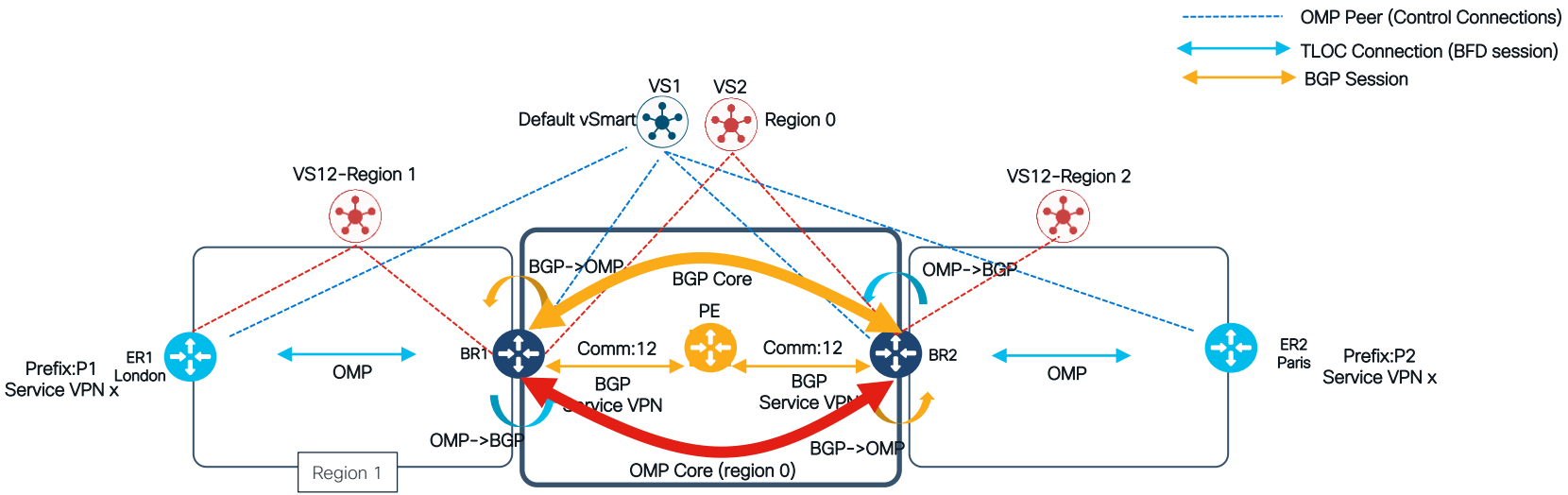
Step7: Modify Control Policies on vSmart to add core TLOCs



- This is required as previously there was no SD-WAN tunnel between BRs and all connectivity was through BGP (service VPN)
- Similar policy for other BR

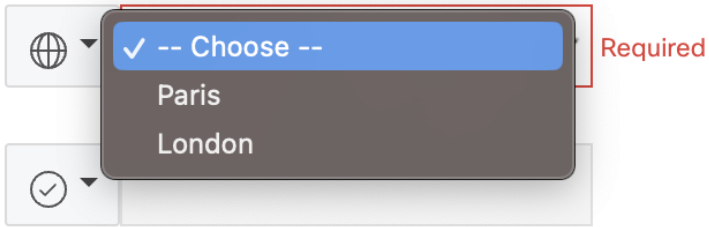
```
control-policy BGP-CORE-EUROPE-HUB-CP
   sequence 1
    match tloc
     site-list EUROPE-ALL-SITES
    !
    action accept
    !
   !
   sequence 11
    match tloc
     site-list AMER-HUB
     tloc-list AMER-HUB-CORE-TLOCS
    !
    action accept
    !
   !
   sequence 21
    match route
     site-list EUROPE-ALL-SITES
     prefix-list _AnyIpv4PrefixList
    !
    action accept
    !
   !
   sequence 31
    match route
     site-list AMER-HUB
     prefix-list _AnyIpv4PrefixList
    !
    action accept
    !
   !
 default-action reject
```

Step8: Now start Migrating Access Regions- on ER

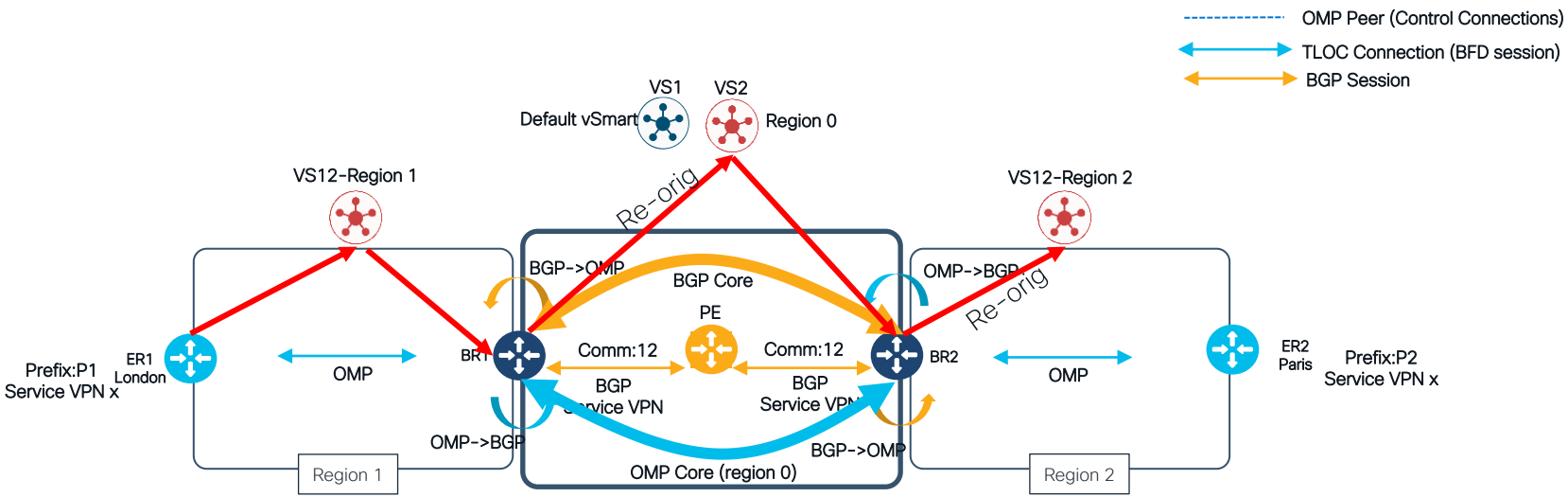


Region

Secondary Region

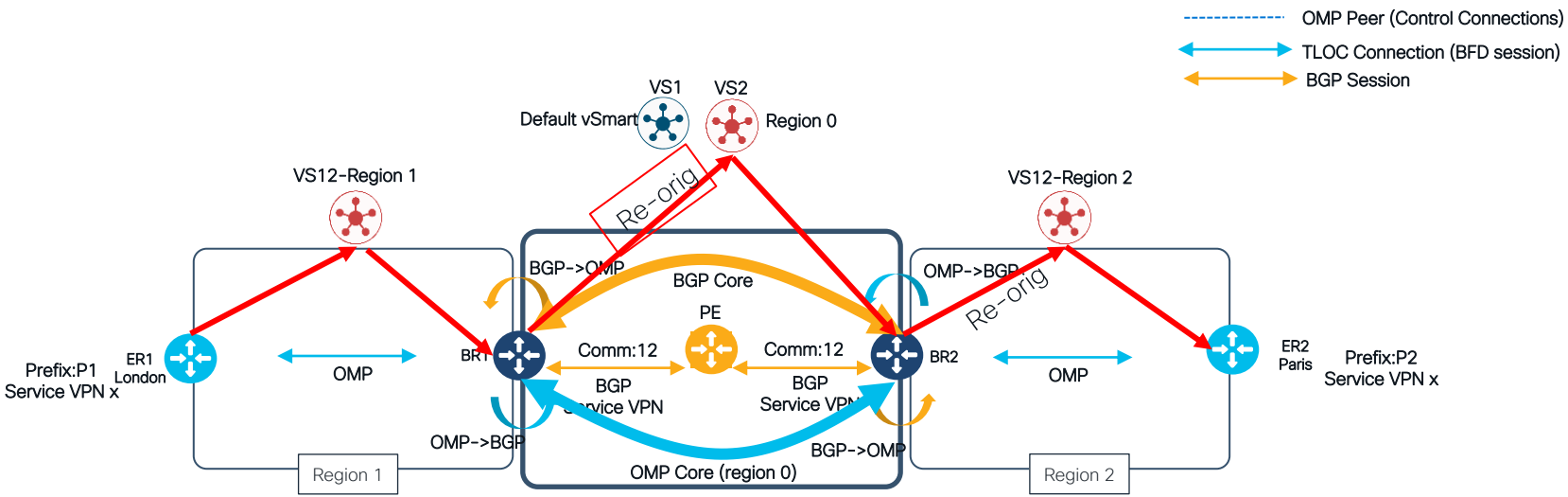


Convergence during ER migration



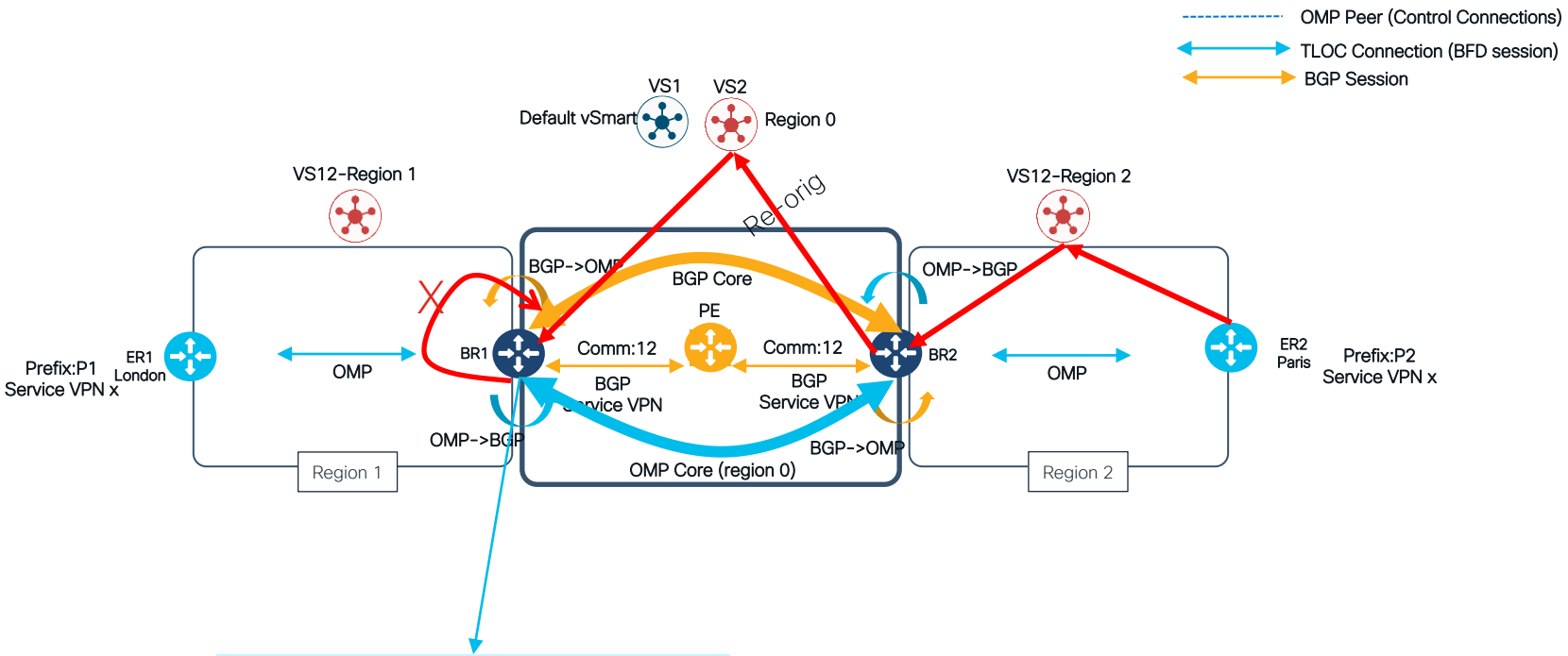
- Now ER1 will also advertise route in region1 along with default region
- BR1 will receive 2 copies of route, from default and region1 vsmart aware. (region aware installed)
- BR1 will send one copy to BGP with mig-x attached, other copy to region0-core without MIG x
- BR2 receives route from BGP and OMP, OMP accepts region 0 route while forwarding wise still BGP is preferred.
- BR2 re-orginates region aware route to region2

Step8: Migrating Other Access Regions- on ER



- Now both domains are fully converged Default and Region aware
- Region-aware routes are preferred, and convergence is done at OMP level. Core still uses BGP for forwarding.

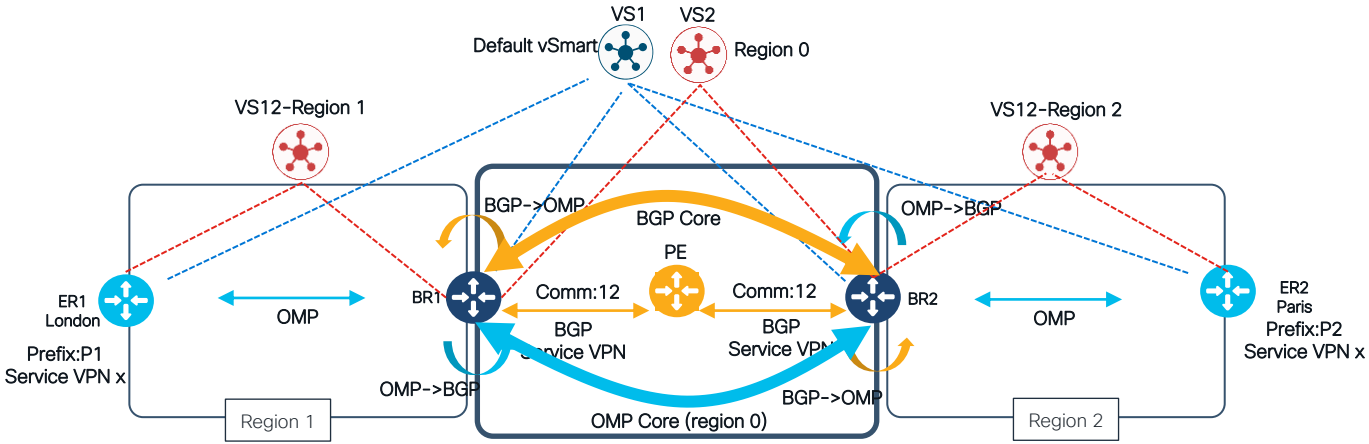
Paris (ER2) now originates the routes



Cleanup

OMP Peer (Control Connections)
TLOC Connection (BFD session)
BGP Session

Remove route-map setting MIG-comm on BGP-BGP → Remove Migration Mode on BR → Remove OMP-BGP redistribution route-map → Remove Migration mode from branches → Remove/Re-purpose Default vSmarts → De-activate control policies



Important

- Cloud on Ramp (CoR) for Multi cloud and SDCI:
  - For brownfield scenarios, leverage this migration sessions' learnings
  - For new setups, CoR automation workflow is available in 20.10/17.10 but can be done manually in 17.9 as well.
- For SDCI Megaport case:
  - Usually, we recommend full-mesh in core, but for Megaport, connectivity is p2p. So, consider cost/feasibility of deploying full-mesh in the core.

Conclusion

Multi-Region Fabric is the core enabler for WAN architectures involving a middle-mile

- For Managed Services SD-WAN
- Large Enterprise deployments using MSP/Cloud/SDCI backbone

Brownfield migration capability available with August ‘22 release (20.9/17.9)!

Eliminate need for lengthy global network policies

Automatic hop-by-hop inter-region routing

Scalable design

Simpler redundancy planning

Flexible architecture to cater to dynamic network needs

Operationally easier to deploy and manage

Cisco SD-WAN multi-region fabric

Complete your Session Survey

- Please complete your session survey after each session. Your feedback is important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from Thursday) to receive your Cisco Live t-shirt.

- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard" at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

Continue Your Education

Visit the Cisco Showcase for related demos.

Book your one-on-one Meet the Engineer meeting.

Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.

Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.


cisco
The bridge to possible
Thank you
cisco Live!


CISCO Live!
ALL IN