Configure Fusion Router in SDA

Contents

Introduction

This document describes how to configure Fusion Routers in a Cisco Software-Defined Access (SDA) solution.

Prerequisites

Requirements

There are no specific requirements for this document.

Note: Setup is required as per Supported Devices which can be found at Link to Release Notes

Components Used

The information in this document is based on these hardware versions:

- Cisco Digital Network Architecture Controller - Version 1.2.1
- Edge and Border - Cat3k Cisco Switch
- Fusion - Cisco Router with Support for Inter-VRF leaking

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

In the Cisco SD-Access solution, devices are managed and configured by Cisco Catalyst Center. In general, all parts of the SD-Access fabric can be, and normally are, configured and managed by Cisco Catalyst Center. The Fusion device is outside the fabric, though, and so is configured manually. Border Automation, discussed next, is a feature within Cisco Catalyst Center that can automate the Border configuration for handoff of VRFs to the Fusion devices.

On occasion, for reasons typically related to compatibility with current configuration, Border Automation is not suitable, and so the handoff from the Border to the Fusion device can also be configured by hand. An understanding of the configuration that is used helps illustrate important details about the optimal configuration and operation of the overall system.

Functionality of a Fusion Device in Cisco DNA SD-Access Solution

A Fusion device enables Virtual Routing and Forwarding (VRF) leaking across SD-Access Fabric domains, and enables host connectivity to shared services, such as DHCP, DNS, NTP, ISE, Cisco Catalyst Center, Wireless LAN Controllers (WLC), and similar. While this role can be performed by other devices than routers, this document focuses on routers as Fusion devices.

As mentioned previously, the shared services must be made available to all virtual networks (VN’s) on the Campus. This is achieved with the creation of Border Gateway Protocol (BGP) peerings from the Border Routers to the Fusion Routers. On the Fusion Router, the fabric VRF’s subnets that need access to these shared services are leaked into the GRT, or a shared services VRF, and vice-versa. Route maps can be used to help contain routing tables to subnets specific to SD-Access Fabric.

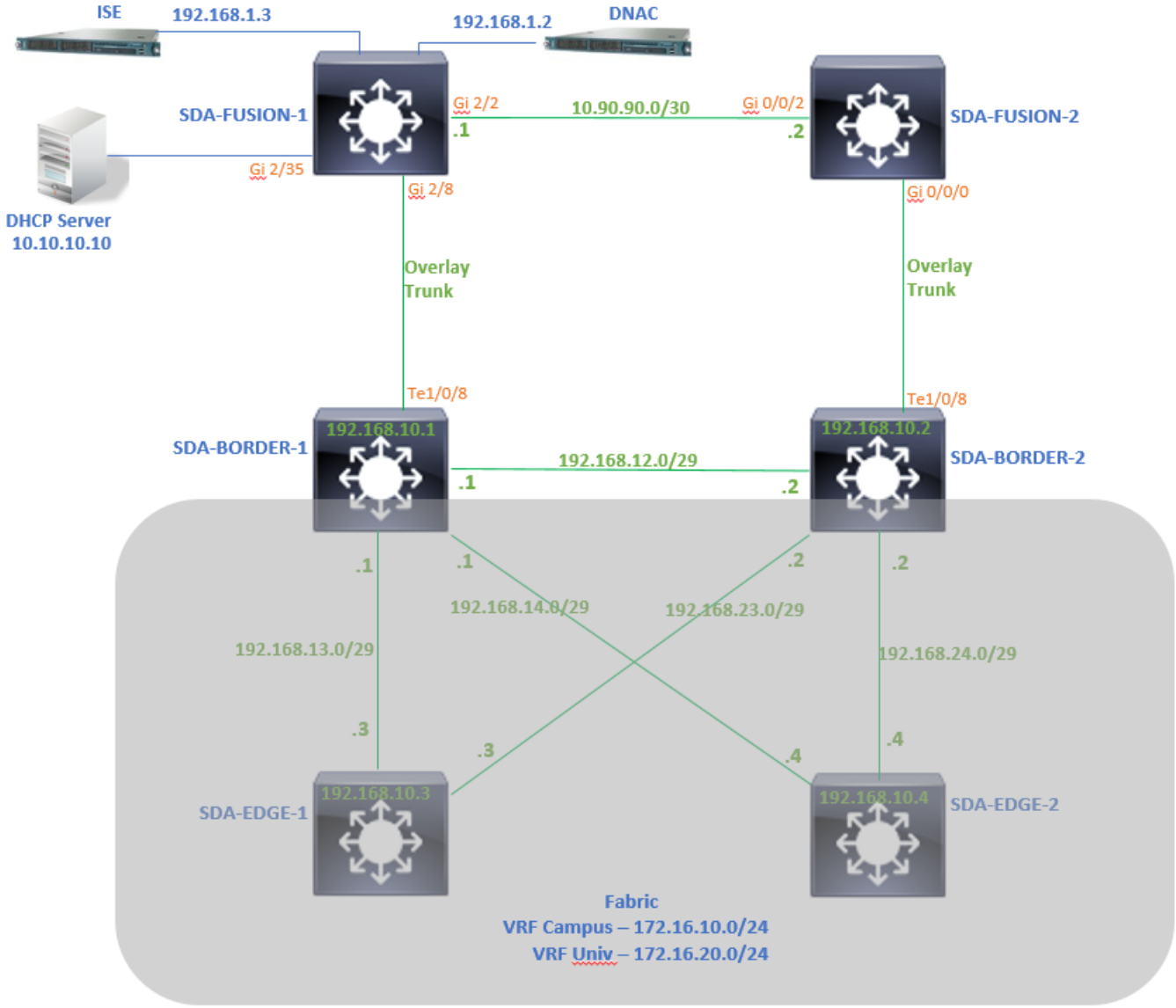
Note: SD-Access Border Nodes do not support summary routes that overlap with SD-Access IP Pools. Summary routes that overlap with IP Pools must be filtered in routing advertisements from Fusion devices to Border Nodes.

Configure

The configuration details given here are with respect to the network topology shown next. This network topology is not a recommended topology for deployments. It is used here solely to facilitate the presentation of the configuration samples provided. For the recommended deployment designs, see the Design Zone for Cisco Digital Network Architecture.

Network Diagram

The topology used for this article consists of two Border Routers both configured as External Borders and two Fusion Routers with a connection to each respective Border Router.



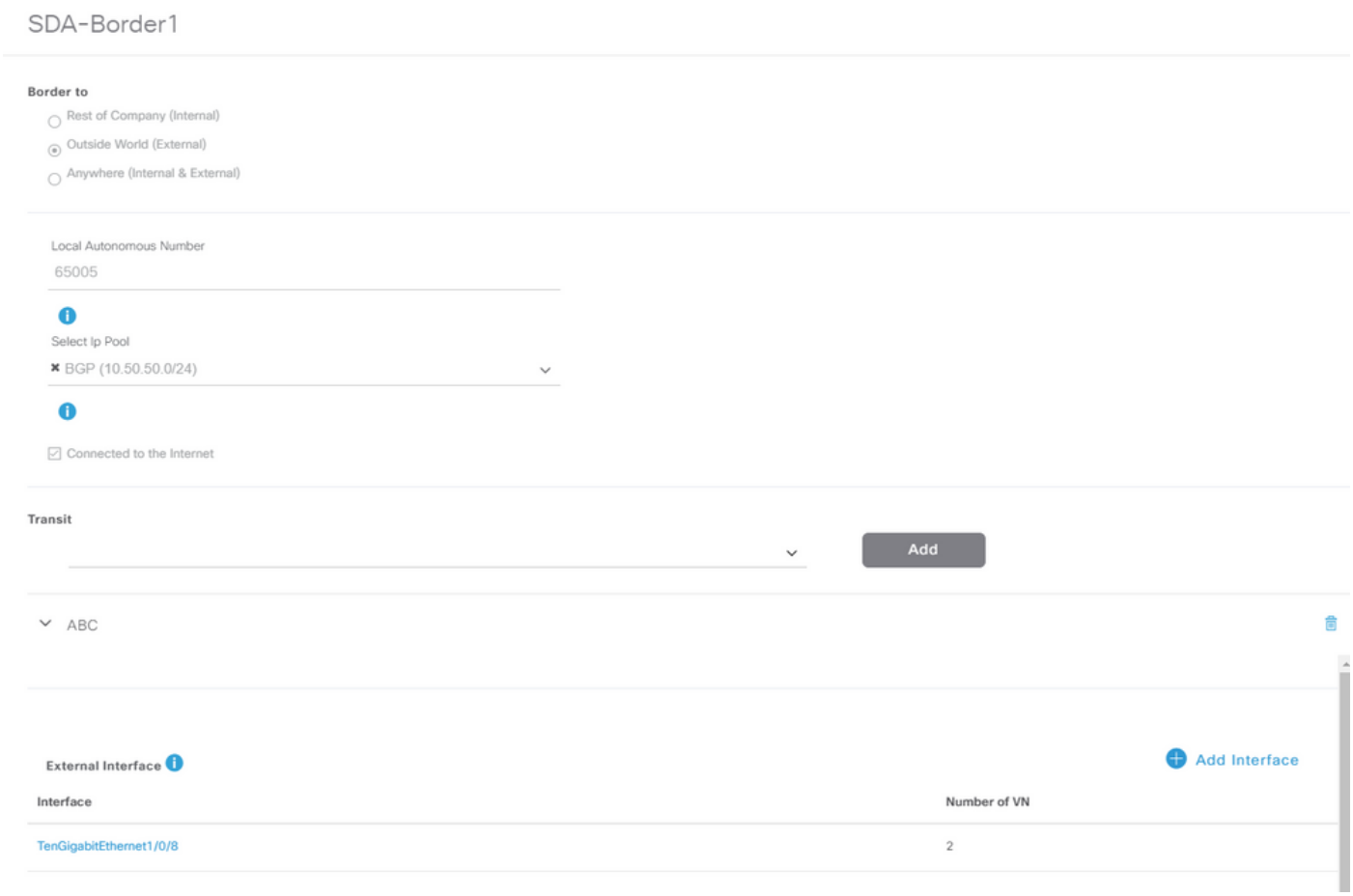
Configurations

Step 1. Configure the Hand-off Link

Within the step of assigning devices a role of Border Router while it is added to the Fabric, a hand-off link can be created. At layer 2 it is a trunk link connected to the Fusion Router. The next steps are needed:

1. Configure Local AS Number for BGP. This Autonomous System (AS) number is used to configure the BGP process on the Border Routers.

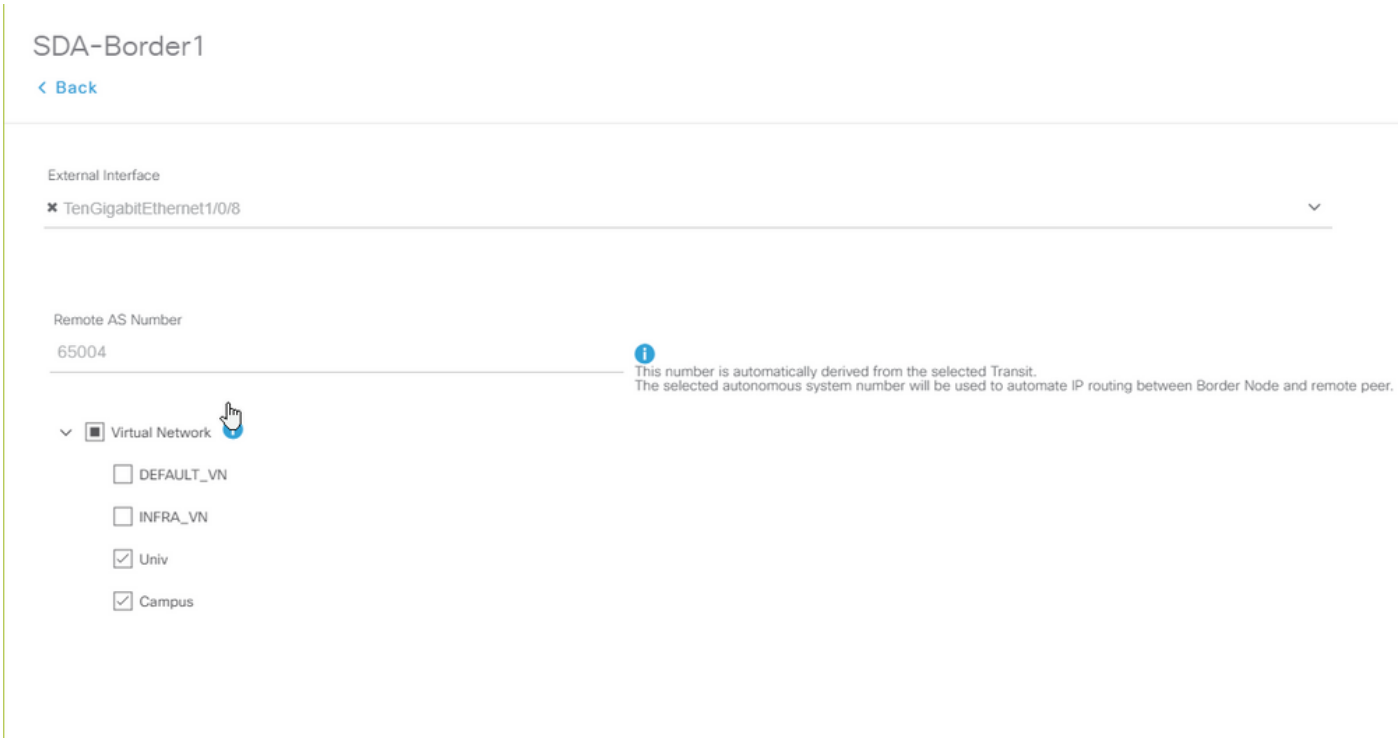
2. Add interface under Transit. This interface is the direct connection between Border and Fusion Router. (Te 1/0/8 on Border in this example.)



3. Configure Remote AS Number. This AS number is used on Border Routers for neighbor statements towards Fusion Router to configure External BGP (eBGP) peers.

4. Select all the Virtual Networks (VRFs) for which VRF leaking is required on Fusion Router.

5. Deploy configuration from Cisco Catalyst Center to Devices.



Use the same steps for the SDA-Border-2 device.

Step 2. Verify Configurations Pushed on Border Routers

This Section covers the verification of configuration on Border Routers related to BGP protocol.

SDA-Border-1

```
SDA-Border1#show run interface loopback 0
!
interface Loopback0
 ip address 192.168.10.1 255.255.255.255
 ip router isis
end


SDA-Border1#show run interface tenGigabitEthernet 1/0/8
!
interface TenGigabitEthernet1/0/8
 switchport mode trunk
end


SDA-Border1#show run interface loopback 1021

interface Loopback1021
 description Loopback Border
 vrf forwarding Campus
 ip address 172.16.10.1 255.255.255.255
end


SDA-Border1#show run interface loopback 1022

interface Loopback1022
 description Loopback Border
 vrf forwarding Univ
 ip address 172.16.20.1 255.255.255.255
end


SDA-Border1#show run | section vrf definition Campus
vrf definition Campus
 rd 1:4099
 !
 address-family ipv4
 route-target export 1:4099
 route-target import 1:4099
 exit-address-family


SDA-Border1#show run | section vrf definition Univ
vrf definition Univ
 rd 1:4100
 !
 address-family ipv4
 route-target export 1:4100
 route-target import 1:4100
```

```
 exit-address-family
SDA-Border1#


SDA-Border1#show run interface vlan 3007
!
interface Vlan3007                                          <<< SVI created for BGP Peering under VRF C
 description vrf interface to External router
 vrf forwarding Campus
 ip address 10.50.50.25 255.255.255.252
 no ip redirects
 ip route-cache same-interface
end

SDA-Border1#show run interface vlan 3006
!
interface Vlan3006                                          <<< SVI created for BGP Peering under VRF U
 description vrf interface to External router
 vrf forwarding Univ
 ip address 10.50.50.21 255.255.255.252
 no ip redirects
 ip route-cache same-interface
end


SDA-Border1#show run | section bgp
router bgp 65005                                           <<< Local AS Number from Cisco Catalyst Cent
 bgp router-id interface Loopback0
 bgp log-neighbor-changes
 bgp graceful-restart
 !
 address-family ipv4
 network 192.168.10.1 mask 255.255.255.255
 redistribute lisp metric 10
 exit-address-family
 !
 address-family ipv4 vrf Campus
 bgp aggregate-timer 0
 network 172.16.10.1 mask 255.255.255.255                  <<< Anycast IP for Pool in VRF Campus
 aggregate-address 172.16.10.0 255.255.255.0 summary-only  <<< Only Summary is Advertised
 redistribute lisp metric 10
 neighbor 10.50.50.26 remote-as 65004                      <<< Peer IP to be used on Fusion for VRF Cam
 neighbor 10.50.50.26 update-source Vlan3007
 neighbor 10.50.50.26 activate
 neighbor 10.50.50.26 weight 65535                         <<< Weight needed for Fusion peering to make
 exit-address-family
 !
 address-family ipv4 vrf Univ
 bgp aggregate-timer 0
 network 172.16.20.1 mask 255.255.255.255                  <<< Anycast IP for Pool in VRF Univ
 aggregate-address 172.16.20.0 255.255.255.0 summary-only
 redistribute lisp metric 10
 neighbor 10.50.50.22 remote-as 65004
 neighbor 10.50.50.22 update-source Vlan3006
 neighbor 10.50.50.22 activate
 neighbor 10.50.50.22 weight 65535
 exit-address-family
```

SDA-Border-2

```
SDA-Border2#show run interface loopback 0
!
interface Loopback0
 ip address 192.168.10.2 255.255.255.255
 ip router isis
end

SDA-Border2#show run interface tenGigabitEthernet 1/0/8
!
interface TenGigabitEthernet1/0/8
 switchport mode trunk
end


SDA-Border2#show run interface loopback 1021
!
interface Loopback1021
 description Loopback Border
 vrf forwarding Campus
 ip address 172.16.10.1 255.255.255.255
end

SDA-Border2#show run interface loopback 1022
!
interface Loopback1022
 description Loopback Border
 vrf forwarding Univ
 ip address 172.16.20.1 255.255.255.255
end


SDA-Border2#show run | section vrf definition Campus
vrf definition Campus
 rd 1:4099
 !
 address-family ipv4
  route-target export 1:4099
  route-target import 1:4099
 exit-address-family


SDA-Border2#show run | section vrf definition Univ
vrf definition Univ
 rd 1:4100
 !
 address-family ipv4
  route-target export 1:4100
  route-target import 1:4100
 exit-address-family


SDA-Border2#show run interface vlan 3001
!
interface Vlan3001
 description vrf interface to External router
 vrf forwarding Campus
 ip address 10.50.50.1 255.255.255.252
 no ip redirects
 ip route-cache same-interface
end
```

```
SDA-Border2#show run interface vlan 3003
!
interface Vlan3003
 description vrf interface to External router
 vrf forwarding Univ
 ip address 10.50.50.9 255.255.255.252
 no ip redirects
 ip route-cache same-interface
end


SDA-Border2#show run | section bgp
router bgp 65005
 bgp router-id interface Loopback0
 bgp log-neighbor-changes
 bgp graceful-restart
 !
 address-family ipv4
  network 192.168.10.2 mask 255.255.255.255
  redistribute lisp metric 10
 exit-address-family
 !
 address-family ipv4 vrf Campus
  bgp aggregate-timer 0
  network 172.16.10.1 mask 255.255.255.255
  aggregate-address 172.16.10.0 255.255.255.0 summary-only
  redistribute lisp metric 10
  neighbor 10.50.50.2 remote-as 65004
  neighbor 10.50.50.2 update-source Vlan3001
  neighbor 10.50.50.2 activate
  neighbor 10.50.50.2 weight 65535
 exit-address-family
 !
 address-family ipv4 vrf Univ
  bgp aggregate-timer 0
  network 172.16.20.1 mask 255.255.255.255
  aggregate-address 172.16.20.0 255.255.255.0 summary-only
  redistribute lisp metric 10
  neighbor 10.50.50.10 remote-as 65004
  neighbor 10.50.50.10 update-source Vlan3003
  neighbor 10.50.50.10 activate
  neighbor 10.50.50.10 weight 65535
 exit-address-family
```

Step 3. Configure Allowas-In on Border Routers

Because of the VRF leaking on the Fusion Router, address-family ipv4 for VRF Campus learns the route originated by VRF Univ (172.16.20.0/24). Both originating and learning router have the same BGP AS number (65005) though. To overcome BGP loop prevention mechanisms, and accept/install the routes on Border Routers, allowas-in must be configured for the peerings with the Fusion Router:

```
SDA-Border1

SDA-Border1(config)#router bgp 65005
SDA-Border1(config-router)#address-family ipv4 vrf Campus
```

```
SDA-Border1(config-router-af)#neighbor 10.50.50.26 allowas-in
SDA-Border1(config-router-af)#exit-address-family
SDA-Border1(config-router)#
SDA-Border1(config-router)#address-family ipv4 vrf Univ
SDA-Border1(config-router-af)#neighbor 10.50.50.22 allowas-in
SDA-Border1(config-router-af)#exit-address-family
SDA-Border1(config-router)#
```

```
SDA-Border2

SDA-Border2(config)#router bgp 65005
SDA-Border2(config-router)#address-family ipv4 vrf Campus
SDA-Border2(config-router-af)#neighbor 10.50.50.2 allowas-in
SDA-Border2(config-router-af)#exit-address-family
SDA-Border2(config-router)#
SDA-Border2(config-router)#address-family ipv4 vrf Univ
SDA-Border2(config-router-af)#neighbor 10.50.50.10 allowas-in
SDA-Border2(config-router-af)#exit-address-family
SDA-Border2(config-router)#
```

Note: Command **allowas-in** must be used with precaution as it can cause loops. When you use only one Fusion device that both Borders peer with, filtering is needed to make sure locally originated routes are not accepted back into the AS from the Fusion peer - within the same VN. If that happens the eBGP path is preferred to the locally originated path due to max weight for eBGP paths.

Step 4. Configure Fusion Routers

This section illustrates the manual configuration for the Fusion routers.

SDA-Fusion-1

Configure the link towards Border Router as a trunk to match the vlan configuration on the Border-1:

```
interface GigabitEthernet2/8
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 3006, 3007
 switchport mode trunk
end
```

Configure the required VRFs:

```
vrf definition Campus
 rd 1:4099
 !
 address-family ipv4
  route-target export 1:4099
  route-target import 1:4099
 exit-address-family
!
```

```
vrf definition Univ
 rd 1:4100
 !
 address-family ipv4
  route-target export 1:4100
  route-target import 1:4100
 exit-address-family
```

Configure SVI interfaces:

```
interface Vlan3007
 vrf forwarding Campus
 ip address 10.50.50.26 255.255.255.252
end

interface Vlan3006
 vrf forwarding Univ
 ip address 10.50.50.22 255.255.255.252
end
```

Configure external BGP (eBGP) peering with SDA-Border-1:

```
router bgp 65004                                    <<< Remote AS from Cisco Catalyst Center
 bgp log-neighbor-changes
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv4 vrf Campus
  neighbor 10.50.50.25 remote-as 65005
  neighbor 10.50.50.25 update-source Vlan3007
  neighbor 10.50.50.25 activate
 exit-address-family
 !
 address-family ipv4 vrf Univ
  neighbor 10.50.50.21 remote-as 65005
  neighbor 10.50.50.21 update-source Vlan3006
  neighbor 10.50.50.21 activate
 exit-address-family
```

Configure internal BGP (iBGP) peering with SDA-Fusion-2:

```
interface GigabitEthernet2/2
 description SDA-Fusion1--->SDA-Fusion2
 ip address 10.90.90.1 255.255.255.252
end

router bgp 65004
```

```
 neighbor 10.90.90.2 remote-as 65004
 !
 address-family ipv4
  neighbor 10.90.90.2 activate
 exit-address-family
 !
```

Advertise DHCP server subnet under global address-family where the DHCP server IP is 10.10.10.10:

```
interface GigabitEthernet2/35
 description connection to DHCP server
 ip address 10.10.10.9 255.255.255.252
end
```

```
router bgp 65004
 !
 address-family ipv4
  network 10.10.10.8 mask 255.255.255.252
 exit-address-family
 !
```

SDA-Fusion-2

Configure the link towards Border Router. If an interface on Fusion is L3 instead of trunk - configure subinterfaces:

```
interface GigabitEthernet0/0/0.3001
 encapsulation dot1Q 3001
 vrf forwarding Campus
 ip address 10.50.50.2 255.255.255.252
end

interface GigabitEthernet0/0/0.3003
 encapsulation dot1Q 3003
 vrf forwarding Univ
 ip address 10.50.50.10 255.255.255.252
end
```

Configure the corresponding VRFs:

```
vrf definition Campus
 rd 1:4099
 !
 address-family ipv4
  route-target export 1:4099
  route-target import 1:4099
 exit-address-family
!
!
```

```
vrf definition Univ
 rd 1:4100
 !
 address-family ipv4
  route-target export 1:4100
  route-target import 1:4100
 exit-address-family
!
```

Configure eBGP Peering with SDA-Border-2:

```
router bgp 65004
 bgp log-neighbor-changes
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv4 vrf Campus
  neighbor 10.50.50.1 remote-as 65005
  neighbor 10.50.50.1 update-source GigabitEthernet0/0/0.3001
  neighbor 10.50.50.1 activate
 exit-address-family
 !
 address-family ipv4 vrf Univ
  neighbor 10.50.50.9 remote-as 65005
  neighbor 10.50.50.9 update-source GigabitEthernet0/0/0.3003
  neighbor 10.50.50.9 activate
 exit-address-family
```

Configure iBGP Peering with SDA-Fusion-1:

```
interface GigabitEthernet0/0/2
 ip address 10.90.90.2 255.255.255.252
 negotiation auto
end

router bgp 65004
 neighbor 10.90.90.1 remote-as 65004
 !
 address-family ipv4
  neighbor 10.90.90.1 activate
 exit-address-family
```

Step 5. Configure VRF Leaking on Fusion Router

The configuration for VRF leaking is identical for both Fusion Routers SDA-Fusion-1 and SDA-Fusion-2.

First, configure VRF leaking between the two VRFs (Campus and Univ), use **route-traget import**:

```
vrf definition Campus
```

```
 !
 address-family ipv4
  route-target export 1:4099
  route-target import 1:4099
  route-target import 1:4100        <<< Import VRF Univ prefixes in VRF Campus
 exit-address-family
 !
vrf definition Univ
 !
 address-family ipv4
  route-target export 1:4100
  route-target import 1:4100
  route-target import 1:4099        <<< Import VRF Campus prefixes in VRF Univ
 exit-address-family
 !
```

Then configure route leaking between the Global Routing Table (GRT) to the VRFs, and from the VRFs to the GRT, use **import ... map** and **export ... map**:

```
ip prefix-list Campus_Prefix seq 5 permit 172.16.10.0/24    <<< Include Prefixes belonging to VRF Campu
ip prefix-list Global_Prefix seq 5 permit 10.10.10.8/30     <<< Include Prefixes belonging to Global (e
ip prefix-list Univ_Prefix seq 5 permit 172.16.20.0/24      <<< Include Prefixes belonging to VRF Univ

route-map Univ_Map permit 10
 match ip address prefix-list Univ_Prefix
route-map Global_Map permit 10
 match ip address prefix-list Global_Prefix
route-map Campus_Map permit 10
 match ip address prefix-list Campus_Prefix


vrf definition Campus
 !
 address-family ipv4
  import ipv4 unicast map Global_Map     <<< Injecting Global into VRF Campus matching route-map Global
  export ipv4 unicast map Campus_Map     <<< Injecting VRF Campus into Global matching route-map Campus
 exit-address-family
 !
vrf definition Univ
 !
 address-family ipv4
  import ipv4 unicast map Global_Map    <<< Injecting Global into VRF Univ matching route-map Global_Ma
  export ipv4 unicast map Univ_Map      <<< Injecting VRF Univ into Global matching route-map Univ_Map
 exit-address-family
 !
```

Verify

This section contains verification steps to ensure that the previous configuration has taken effect correctly.

Step 1. Verify eBGP Peering Between Fusion and Border Routers

SDA-Border-1 ------Peering--------SDA-Fusion-1

```
SDA-Border1#show ip bgp vpnv4 vrf Campus summary

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.50.50.26     4        65004    1294    1295       32    0    0 19:32:22        2



SDA-Border1#show ip bgp vpnv4 vrf Univ summary

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.50.50.22     4        65004    1294    1292       32    0    0 19:32:57        2


-------------------------------------------------


SDA-Fusion1#show ip bgp vpnv4 vrf Campus summary

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.50.50.25     4        65005    1305    1305       31    0    0 19:41:58        1


SDA-Fusion1#show ip bgp vpnv4 vrf Univ summary

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.50.50.21     4        65005    1303    1305       31    0    0 19:42:14        1
```

SDA-Border-2 ------Peering--------SDA-Fusion-2

```
SDA-Border2#show ip bgp vpnv4 vrf Campus summary

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.50.50.2      4        65004       6       6       61    0    0 00:01:37        2


SDA-Border2#show ip bgp vpnv4 vrf Univ summary

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.50.50.10     4        65004       6       6       61    0    0 00:01:39        2

-------------------------------------------------------------------------------

SDA-Fusion2#show ip bgp vpnv4 vrf Campus summary

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.50.50.1      4        65005      17      17        9    0    0 00:11:16        1


SDA-Fusion2#show ip bgp vpnv4 vrf Univ summary

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.50.50.9      4        65005      17      17        9    0    0 00:11:33        1
```

Step 2. Verify iBGP Peering Between both Fusion Routers

SDA-Fusion-1 ------Peering--------SDA-Fusion-2

```
SDA-Fusion1#show ip bgp summary

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.90.90.2      4        65004      10      12        12    0    0 00:04:57        2
```

```
SDA-Fusion2#show ip bgp summary

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.90.90.1      4        65004      19      17         4    0    0 00:11:35        3
```

Step 3. Verify Prefixes in BGP Table and Routing Table

SDA-Border-1

```
SDA-Border1#show ip bgp vpnv4 vrf Campus

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:4099 (default for vrf Campus)
 *>   10.10.10.8/30    10.50.50.26                            65535 65004 i         <<< Prefix leaked from
 *>   172.16.10.0/24   0.0.0.0                                32768 i               <<< VRF Campus originat
 *>   172.16.20.0/24   10.50.50.26                            65535 65004 65005 i   <<< Prefix originated i
```

```
SDA-Border1#show ip route vrf Campus bgp

Routing Table: Campus

B        10.10.10.8/30 [20/0] via 10.50.50.26, 20:30:30          <<< RIB entry for DHCP Server pool pre
B        172.16.10.0/24 [200/0], 20:32:45, Null0                 <<< Null entry created by "aggregate-a
B        172.16.20.0/24 [20/0] via 10.50.50.26, 20:32:45         <<< RIB entry for VRF Univ prefix
```

```
SDA-Border1#show ip bgp vpnv4 vrf Univ

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:4100 (default for vrf Univ)
 *>   10.10.10.8/30    10.50.50.22                            65535 65004 i         <<< Prefix leaked from
 *>   172.16.10.0/24   10.50.50.22                            65535 65004 65005 i   <<< Prefix originated i
 *>   172.16.20.0/24   0.0.0.0                                32768 i               <<< VRF Univ originated
```

```
 SDA-Border1#show ip route vrf Univ bgp

Routing Table: Univ

B        10.10.10.8/30 [20/0] via 10.50.50.22, 20:31:06          <<< RIB entry for DHCP Server pool pre
```

```
B        172.16.10.0/24 [20/0] via 10.50.50.22, 20:33:21         <<< RIB entry for VRF Campus prefix
B        172.16.20.0/24 [200/0], 20:33:21, Null0                 <<< Null entry created by "aggregate-a
```

SDA-Border-2

```
SDA-Border2#show ip bgp vpnv4 vrf Campus

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:4099 (default for vrf Campus)
 *>   10.10.10.8/30    10.50.50.2                             65535 65004 i         <<< Prefix leaked from
 *>   172.16.10.0/24   0.0.0.0                                32768 i               <<< VRF Campus originat
 *>   172.16.20.0/24   10.50.50.2                             65535 65004 65005 i   <<< Prefix originated i


SDA-Border2#show ip route vrf Campus bgp

B        10.10.10.8/30 [20/0] via 10.50.50.2, 01:02:19          <<< RIB entry for DHCP Server pool pref
B        172.16.10.0/24 [200/0], 1w6d, Null0                    <<< Null entry created by "aggregate-ad
B        172.16.20.0/24 [20/0] via 10.50.50.2, 01:02:27         <<< RIB entry for VRF Univ Prefix

------------------------------------------------------------------

SDA-Border2#show ip bgp vpnv4 vrf Univ

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:4100 (default for vrf Univ)
 *>   10.10.10.8/30    10.50.50.10                            65535 65004 i         <<< Prefix leaked from
 *>   172.16.10.0/24   10.50.50.10                            65535 65004 65005 i   <<< Prefix originated i
 *>   172.16.20.0/24   0.0.0.0                                32768 i               <<< VRF Univ originated


SDA-Border2#show ip route vrf Univ bgp

B        10.10.10.8/30 [20/0] via 10.50.50.10, 01:02:29          <<< RIB entry for DHCP Server pool pre
B        172.16.10.0/24 [20/0] via 10.50.50.10, 01:02:34         <<< RIB entry for VRF Campus prefix
B        172.16.20.0/24 [200/0], 1w6d, Null0                     <<< Null entry created by "aggregate-a
```

SDA-Fusion-1

```
SDA-Fusion1#show ip bgp

     Network          Next Hop            Metric LocPrf Weight Path
 *>  10.10.10.8/30    0.0.0.0                  0         32768 i           <<< Locally originated Glob
 * i 172.16.10.0/24   10.50.50.1               0    100      0 65005 i      <<< Prefix imported from VR
 *>                   10.50.50.25              0             0 65005 i
 * i 172.16.20.0/24   10.50.50.9               0    100      0 65005 i      <<< Prefix imported from VR
 *>                   10.50.50.21              0             0 65005 i


SDA-Fusion1#show ip route
```

```
C        10.10.10.8/30 is directly connected, GigabitEthernet2/35            <<< Prefix for DHCP Server
B        172.16.10.0 [20/0] via 10.50.50.25 (Campus), 20:50:21               <<< Prefix imported from V
B        172.16.20.0 [20/0] via 10.50.50.21 (Univ), 20:50:21              <<< Prefix imported from VRF

------------------------------------------------------------------------


SDA-Fusion1#show ip bgp vpnv4 vrf Campus

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:4099 (default for vrf Campus)
Import Map: Global_Map, Address-Family: IPv4 Unicast, Pfx Count/Limit: 1/1000
Export Map: Campus_Map, Address-Family: IPv4 Unicast, Pfx Count/Limit: 1/1000
 *>  10.10.10.8/30    0.0.0.0                  0         32768 i             <<< Prefix imported from G
 *>  172.16.10.0/24   10.50.50.25              0             0 65005 i         <<< Prefix learnt from Bo
 *>  172.16.20.0/24   10.50.50.21              0             0 65005 i         <<< Prefix imported fron


SDA-Fusion1#show ip bgp vpnv4 vrf Campus 172.16.20.0/24
BGP routing table entry for 1:4099:172.16.20.0/24, version 27
Paths: (1 available, best #1, table Campus)
 Advertised to update-groups:
 5
 Refresh Epoch 1
 65005, (aggregated by 65005 192.168.10.1), imported path from 1:4100:172.16.20.0/24 (Univ)
 10.50.50.21 (via vrf Univ) (via Univ) from 10.50.50.21 (192.168.10.1)
 Origin IGP, metric 0, localpref 100, valid, external, atomic-aggregate, best
 Extended Community: RT:1:4100
 rx pathid: 0, tx pathid: 0x0



SDA-Fusion1#show ip route vrf Campus bgp


B        10.10.10.8/30 is directly connected, 20:46:51, GigabitEthernet2/35
B        172.16.10.0 [20/0] via 10.50.50.25, 20:50:07
B        172.16.20.0 [20/0] via 10.50.50.21 (Univ), 20:50:07

------------------------------------------------------------------------


SDA-Fusion1#show ip bgp vpnv4 vrf Univ

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:4100 (default for vrf Univ)
Import Map: Global_Map, Address-Family: IPv4 Unicast, Pfx Count/Limit: 1/1000
Export Map: Univ_Map, Address-Family: IPv4 Unicast, Pfx Count/Limit: 1/1000
 *>  10.10.10.8/30    0.0.0.0                  0         32768 i             <<< Prefix imported from G
 *>  172.16.10.0/24   10.50.50.25              0             0 65005 i         <<< Prefix imported fron
 *>  172.16.20.0/24   10.50.50.21              0             0 65005 i       <<< Prefix learnt from Bor


SDA-Fusion1#show ip bgp vpnv4 vrf Univ 172.16.10.0/24
BGP routing table entry for 1:4100:172.16.10.0/24, version 25
Paths: (1 available, best #1, table Univ)
 Advertised to update-groups:
 4
 Refresh Epoch 1
 65005, (aggregated by 65005 192.168.10.1), imported path from 1:4099:172.16.10.0/24 (Campus)
 10.50.50.25 (via vrf Campus) (via Campus) from 10.50.50.25 (192.168.10.1)
```

```
 Origin IGP, metric 0, localpref 100, valid, external, atomic-aggregate, best
 Extended Community: RT:1:4099
 rx pathid: 0, tx pathid: 0x0



SDA-Fusion1#show ip route vrf Univ bgp

B        10.10.10.8/30 is directly connected, 20:47:01, GigabitEthernet2/35
B        172.16.10.0 [20/0] via 10.50.50.25 (Campus), 20:50:17
B        172.16.20.0 [20/0] via 10.50.50.21, 20:50:17
```

SDA-Fusion-2

```
SDA-Fusion2#show ip bgp

     Network          Next Hop            Metric LocPrf Weight Path
 *>i 10.10.10.8/30    10.90.90.1               0    100      0 i
 *>  172.16.10.0/24   10.50.50.1               0             0 65005 i
 * i                  10.50.50.25              0    100      0 65005 i
 *>  172.16.20.0/24   10.50.50.9               0             0 65005 i
 * i                  10.50.50.21              0    100      0 65005 i


SDA-Fusion2#show ip route

B        10.10.10.8/30 [200/0] via 10.90.90.1, 01:25:56
B        172.16.10.0 [20/0] via 10.50.50.1 (Campus), 01:25:56
B        172.16.20.0 [20/0] via 10.50.50.9 (Univ), 01:25:56

------------------------------------------------------------------------------

SDA-Fusion2#show ip bgp vpnv4 vrf Campus

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:4099 (default for vrf Campus)
Import Map: Global_Map, Address-Family: IPv4 Unicast, Pfx Count/Limit: 1/1000
Export Map: Campus_Map, Address-Family: IPv4 Unicast, Pfx Count/Limit: 1/1000
 *>i 10.10.10.8/30    10.90.90.1               0    100      0 i
 *>  172.16.10.0/24   10.50.50.1               0             0 65005 i
 *>  172.16.20.0/24   10.50.50.9               0             0 65005 i


SDA-Fusion2#show ip route vrf Campus bgp


B        10.10.10.8/30 [200/0] via 10.90.90.1, 01:26:09
B        172.16.10.0 [20/0] via 10.50.50.1, 01:26:13
B        172.16.20.0 [20/0] via 10.50.50.9 (Univ), 01:26:13

------------------------------------------------------------------------------

SDA-Fusion2#show ip bgp vpnv4 vrf Univ

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:4100 (default for vrf Univ)
```

```
Import Map: Global_Map, Address-Family: IPv4 Unicast, Pfx Count/Limit: 1/1000
Export Map: Univ_Map, Address-Family: IPv4 Unicast, Pfx Count/Limit: 1/1000
 *>i 10.10.10.8/30    10.90.90.1               0    100      0 i
 *>  172.16.10.0/24   10.50.50.1               0             0 65005 i
 *>  172.16.20.0/24   10.50.50.9               0             0 65005 i


SDA-Fusion2#show ip route vrf Univ bgp


B        10.10.10.8/30 [200/0] via 10.90.90.1, 01:26:19
B        172.16.10.0 [20/0] via 10.50.50.1 (Campus), 01:26:23
B        172.16.20.0 [20/0] via 10.50.50.9, 01:26:23
```

Manual Configuration for Border Redundancy

For redundancy among the PETRs when a border external link fails, for External and External+Internal borders, you have to manually build iBGP sessions between the two Borders for each of the VNs. Additionally, in case of External+Internal border where BGP is imported into LISP and LISP is redistributed back into BGP, tags are needed to prevent iBGP to LISP route imports and hence avoid potential loops.

SDA-Border-1

<#root>

```
interface Vlan31
 description vrf interface to SDA-Border-2
 vrf forwarding Campus
 ip address 10.31.1.1 255.255.255.252
!
interface Vlan33
 description vrf interface to SDA-Border-2
 vrf forwarding Univ
 ip address 10.33.1.1 255.255.255.252
!

router bgp 65005
!
address-family ipv4 vrf Campus
 redistribute lisp metric 10                        <<< open redistribution pushed by Cisco Catalyst Ce
 neighbor 10.31.1.2 remote-as 65005                 <<< iBGP peering with SDA-Border-2
 neighbor 10.31.1.2 activate
 neighbor 10.31.1.2 send-community                  <<< we need to send community/tag to the neighbor
 neighbor 10.31.1.2 route-map tag_local_eids out    <<< route-map used to tag prefixes sent out
!
address-family ipv4 vrf Univ
 redistribute lisp metric 10



 neighbor 10.33.1.2 remote-as 65005
 neighbor 10.33.1.2 activate
 neighbor 10.33.1.2 send-community
 neighbor 10.33.1.2 route-map tag_local_eids out
!

router lisp
```

```
!
 instance-id 4099
  service ipv4
   eid-table vrf Campus
   route-import database bgp 65005 route-map DENY-Campus locator-set rloc_a0602921-91eb-4e27-a294-f8894
!
 instance-id 4103
  service ipv4
   eid-table vrf Univ
   route-import database bgp 65005 route-map DENY-Univ locator-set rloc_a0602921-91eb-4e27-a294-f88949a
!

ip community-list 1 permit 655370                    <<< community-list matching tag 655370 - pushed by
!

route-map DENY-Campus deny 5                         <<< route-map pushed and used in route-import
 match ip address prefix-list Campus
!
route-map DENY-Campus deny 10
 match ip address prefix-list l3handoff-prefixes
!
route-map DENY-Campus deny 15
 match community 1                                   <<< match on community-list 1 to deny iBGP prefixes
!
route-map DENY-Campus deny 25
 match ip address prefix-list deny_0.0.0.0
!
route-map DENY-Campus permit 30
!

route-map DENY-Univ deny 5                           <<< similar route-map is pushed for Univ VN
 match ip address prefix-list Univ
!
route-map DENY-Univ deny 10
 match ip address prefix-list l3handoff-prefixes
!
route-map DENY-Univ deny 15
 match community 1
!
route-map DENY-Univ deny 25
 match ip address prefix-list deny_0.0.0.0
!
route-map DENY-Univ permit 30
!

route-map tag_local_eids permit 5                   <<< route-map we need to create in order to tag the
set community 655370                                <<< setting community/tag to 655370



!
```

SDA-Border-2

```
interface Vlan31
 description vrf interface to SDA-Border-1
 vrf forwarding Campus
 ip address 10.31.1.2 255.255.255.252
```

```
!
interface Vlan33
 description vrf interface to SDA-Border-1
 vrf forwarding Univ
 ip address 10.33.1.2 255.255.255.252
!

router bgp 65005
!
address-family ipv4 vrf Campus
 neighbor 10.31.1.1 remote-as 65005
 neighbor 10.31.1.1 activate
 neighbor 10.31.1.1 send-community
 neighbor 10.31.1.1 route-map tag_local_eids out
!
 address-family ipv4 vrf Univ
 neighbor 10.33.1.1 remote-as 65005
 neighbor 10.33.1.1 activate
 neighbor 10.33.1.1 send-community
 neighbor 10.33.1.1 route-map tag_local_eids out
!

router lisp
!
 instance-id 4099
  service ipv4
   eid-table vrf Campus
route-import database bgp 65005 route-map DENY-Campus locator-set rloc_677c0a8a-0802-49f9-99cc-f9c6ebda
!

 instance-id 4103
  service ipv4
   eid-table vrf Univ
route-import database bgp 65005 route-map DENY-Univ locator-set rloc_677c0a8a-0802-49f9-99cc-f9c6ebda80
!

ip community-list 1 permit 655370
!

route-map DENY-Campus deny 5
 match ip address prefix-list Campus
!
route-map DENY-Campus deny 10
 match ip address prefix-list l3handoff-prefixes
!
route-map DENY-Campus deny 15
 match community 1
!
route-map DENY-Campus deny 25
 match ip address prefix-list deny_0.0.0.0
!
route-map DENY-Campus permit 30
!

route-map DENY-Univ deny 5
match ip address prefix-list Univ
!
route-map DENY-Univ deny 10
match ip address prefix-list l3handoff-prefixes
!
route-map DENY-Univ deny 15
 match community 1
```

```
!
route-map DENY-Univ deny 25
match ip address prefix-list deny_0.0.0.0
!
route-map DENY-Univ permit 30
!

route-map tag_local_eids permit 5
 set community 655370
!
```

Simplify Fusion Configuration with the Use of Templates

This section contains sample Fusion Template configuration examples to help simplify the configuration.

Next are the Variables the are required to be defined based on your deployment design. In this example, the configurations and VNs are based on the previous topology that have two VNs, Campus and Univ.

Variable Definition

```
interface_Fusion1: GigabitEthernet2/8
interface_Fusion2: GigabitEthernet0/0/0

Global_prefixes = 10.10.10.8/30

FUSION_BGP_AS = 65004
BORDER_BGP_AS = 65005
```

For VN1:

```
VN1 = Campus
Fusion1_VN1_VLAN = 3007
Fusion2_VN1_VLAN = 3001
VN1_prefixes = 172.16.10.0/24

Fusion1_VN1_IP = 10.50.50.26

Fusion1_VN1_MASK = 255.255.255.252

Fusion2_VN1_IP = 10.50.50.2

Fusion2_VN1_MASK = 255.255.255.252
VN1_RD = 4099
VN1_ border1_neighbor_IP = 10.50.50.25
VN1_border2_neighbor_IP = 10.50.50.1
```

For VN2:

```
    VN2 = Univ
    Fusion1_VN2_VLAN = 3006
    Fusion2_VN2_VLAN = 3003
    VN2_prefixes = 172.16.20.0/24

    Fusion1_VN2_IP = 10.50.50.22

    Fusion1_VN2_MASK = 255.255.255.252
    Fusino2_VN2_IP2 = 10.50.50.10

    Fusion2_VN2_MASK = 255.255.255.252
    VN2_RD = 4100
    VN2_border1_neighbor_IP = 10.50.50.21
    VN2_border2_neighbor_IP = 10.50.50.9
```

Template Example

Fusion 1

```
interface $interface_Fusion1
switchport
switchport mode trunk
switchport trunk allowed vlan add $Fusion1_VN1_VLAN, $Fusion1_VN2_VLAN
!
vlan $Fusion1_VN1_VLAN
no shut
!
vlan $Fusion1_VN2_VLAN
no shut
!
vrf definition $VN1
rd 1:$VN1_RD
!
address-family ipv4
route-target export 1:$VN1_RD
route-target import 1:$VN1_RD
route-target import 1:$VN2_RD
exit-address-family
!
vrf definition $VN2
rd 1:$VN2_RD
!
address-family ipv4
route-target export 1:$VN2_RD
route-target import 1:$VN2_RD
route-target import 1:$VN1_RD
exit-address-family
!
interface Vlan $Fusion1_VN1_VLAN
vrf forwarding $VN1
ip address $Fusion1_VN1_IP $Fusion1_VN1_MASK
!
interface Vlan $Fusion1_VN2_VLAN
vrf forwarding $VN2
ip address $Fusion1_VN2_IP $Fusion1_VN2_MASK
!
router bgp $FUSION_BGP_AS
```

```
bgp log-neighbor-changes
!
address-family ipv4
exit-address-family
!
address-family ipv4 vrf $VN1
neighbor $VN1_border1_neighbor_IP remote-as $BORDER_BGP_AS
neighbor $VN1_border1_neighbor_IP update-source Vlan $Fusion1_VN1_VLAN
neighbor $VN1_border1_neighbor_IP activate
exit-address-family
!
address-family ipv4 vrf $VN2
neighbor $VN2_border1_neighbor_IP remote-as $BORDER_BGP_AS
neighbor $VN2_border1_neighbor_IP update-source $Fusion1_VN2_VLAN
neighbor $VN2_border1_neighbor_IP activate
exit-address-family

ip prefix-list ${VN1}_Prefix seq 5 permit $VN1_prefixes
ip prefix-list Global_Prefix seq 5 permit $Global_prefixes
ip prefix-list ${VN2}_Prefix seq 5 permit $VN2_prefixes

route-map ${VN2}_Map permit 10
match ip address prefix-list ${VN2}_Prefix
route-map Global_Map permit 10
match ip address prefix-list Global_Prefix
route-map ${VN1}_Map permit 10
match ip address prefix-list ${VN1}_Prefix

vrf definition $VN1
!
address-family ipv4
import ipv4 unicast map Global_Map
export ipv4 unicast map ${VN1}_Map
exit-address-family
!
vrf definition $VN2
!
address-family ipv4
import ipv4 unicast map Global_Map
export ipv4 unicast map ${VN2}_Map
exit-address-family
!
```

Fusion 2

```
interface $interface_Fusion2.$Fusion2_VN1_VLAN
encapsulation dot1Q $Fusion2_VN1_VLAN
vrf forwarding $VN1
ip address $Fusion2_VN1_IP2 $Fusion2_VN1_MASK
!
interface $interface_Fusion2.$Fusion2_VN2_VLAN
encapsulation dot1Q $Fusion2_VN2_VLAN
vrf forwarding $VN2
ip address $Fusion2_VN2_IP2 $Fusion2_VN2_MASK
!
vlan $Fusion2_VN1_VLAN
no shut
!
```

```
vlan $Fusion2_VN2_VLAN
no shut
!
vrf definition $VN1
rd 1:$VN1_RD
!
address-family ipv4
route-target export 1:$VN1_RD
route-target import 1:$VN1_RD
route-target import 1:$VN2_RD
exit-address-family
!
vrf definition $VN2
rd 1:$VN2_RD
!
address-family ipv4
route-target export 1:$VN2_RD
route-target import 1:$VN2_RD
route-target import 1:$VN1_RD
exit-address-family
!
router bgp $FUSION_BGP_AS
bgp log-neighbor-changes
!
address-family ipv4
exit-address-family
!
address-family ipv4 vrf $VN1
neighbor $VN1_border2_neighbor_IP remote-as $BORDER_BGP_AS
neighbor $VN1_border2_neighbor_IP update-source $interface_Fusion2.$Fusion2_VN1_VLAN
neighbor $VN1_bordre2_neighbor_IP activate
exit-address-family
!
address-family ipv4 vrf $VN2
neighbor $VN2_border2_neighbor_IP remote-as $BORDER_BGP_AS
neighbor $VN2_border2_neighbor_IP update-source $interface_Fusion2.$Fusion2_VN2_VLAN
neighbor $VN2_border2_neighbor_IP activate
exit-address-family

ip prefix-list ${VN1}_Prefix seq 5 permit $VN1_prefixes
ip prefix-list Global_Prefix seq 5 permit $Global_prefixes
ip prefix-list ${VN2}_Prefix seq 5 permit $VN2_prefixes

route-map ${VN2}_Map permit 10
match ip address prefix-list ${VN2}_Prefix
route-map Global_Map permit 10
match ip address prefix-list Global_Prefix
route-map ${VN}_Map permit 10
match ip address prefix-list ${VN1}_Prefix

vrf definition $VN1
!
address-family ipv4
import ipv4 unicast map Global_Map
export ipv4 unicast map ${VN1}_Map
exit-address-family
!
vrf definition $VN2
!
address-family ipv4
import ipv4 unicast map Global_Map
export ipv4 unicast map ${VN2}_Map
```

```
exit-address-family
!
End
```