# Configuration du routeur Fusion dans SDA

## Table des matières


- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Fonctionnalité d'un périphérique Fusion dans la solution Cisco DNA SD-Access
- Configurer
  - Diagramme du réseau
  - Configurations
    - Étape 1 : configuration de la liaison de transfert
    - Étape 2 : vérification des configurations transmises sur les routeurs périphériques
    - Étape 3 : configuration des routeurs Fusion
    - Étape 4 : configuration de la fuite VRF sur le routeur Fusion
- Vérifier
  - Étape 1 : vérification de l'appairage eBGP entre les routeurs Fusion et Border
  - Étape 2 : vérification de l'appairage iBGP entre les deux routeurs Fusion
  - Étape 3. Vérification des préfixes dans la table BGP et la table de routage
- Configuration manuelle de la redondance en périphérie
  - SDA-Border-1
  - SDA-Border-2
- Simplifier la configuration de Fusion avec l'utilisation de modèles
  - Définition de variable
  - Exemple de modèle
    - Fusion 1
    - Fusion 2


## Introduction

Ce document décrit comment configurer les routeurs Fusion dans une solution Cisco Software-Defined Access (SDA).

## Conditions préalables

### Exigences

Aucune exigence spécifique n'est associée à ce document.

> Remarque : La configuration est requise selon les périphériques pris en charge, disponibles sur le lien vers les notes de version

### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions matérielles suivantes :

- Contrôleur Cisco Digital Network Architecture - Version 1.2.1
- Périphérie et périphérie - Commutateur Cisco Cat3k
- Fusion - Routeur Cisco avec prise en charge des fuites inter-VRF

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Informations générales

Dans la solution Cisco SD-Access, les périphériques sont gérés et configurés par Cisco Catalyst Center. En général, toutes les parties du fabric SD-Access peuvent être, et sont normalement, configurées et gérées par Cisco Catalyst Center. Cependant, le périphérique Fusion se trouve à l'extérieur du fabric et est donc configuré manuellement. L'automatisation des frontières, présentée ci-après, est une fonctionnalité de Cisco Catalyst Center qui permet d'automatiser la configuration des frontières pour le transfert des VRF aux périphériques Fusion.

Parfois, pour des raisons généralement liées à la compatibilité avec la configuration actuelle, l'automatisation des frontières n'est pas appropriée, et donc le transfert de la frontière au périphérique Fusion peut également être configuré manuellement. La compréhension de la configuration utilisée permet d'illustrer les détails importants relatifs à la configuration et au fonctionnement optimaux du système dans son ensemble.

## Fonctionnalité d'un périphérique Fusion dans la solution Cisco DNA SD-Access

Un périphérique Fusion active les fuites VRF (Virtual Routing and Forwarding) sur les domaines de fabric SD-Access et permet la connectivité des hôtes aux services partagés, tels que DHCP, DNS, NTP, ISE, Cisco Catalyst Center, les contrôleurs LAN sans fil (WLC), etc. Bien que ce rôle puisse être exécuté par d'autres périphériques que les routeurs, ce document se concentre sur les routeurs en tant que périphériques Fusion.

Comme mentionné précédemment, les services partagés doivent être mis à la disposition de tous les réseaux virtuels (VPN) du campus. Ceci est réalisé avec la création d'appairages BGP (Border Gateway Protocol) des routeurs périphériques aux routeurs de fusion. Sur le routeur Fusion, les sous-réseaux du VRF de fabric qui ont besoin d'accéder à ces services partagés sont filtrés dans le GRT, ou un VRF de services partagés, et vice-versa. Les cartes de routage peuvent être utilisées pour contenir des tables de routage vers des sous-réseaux spécifiques au fabric SD-Access.

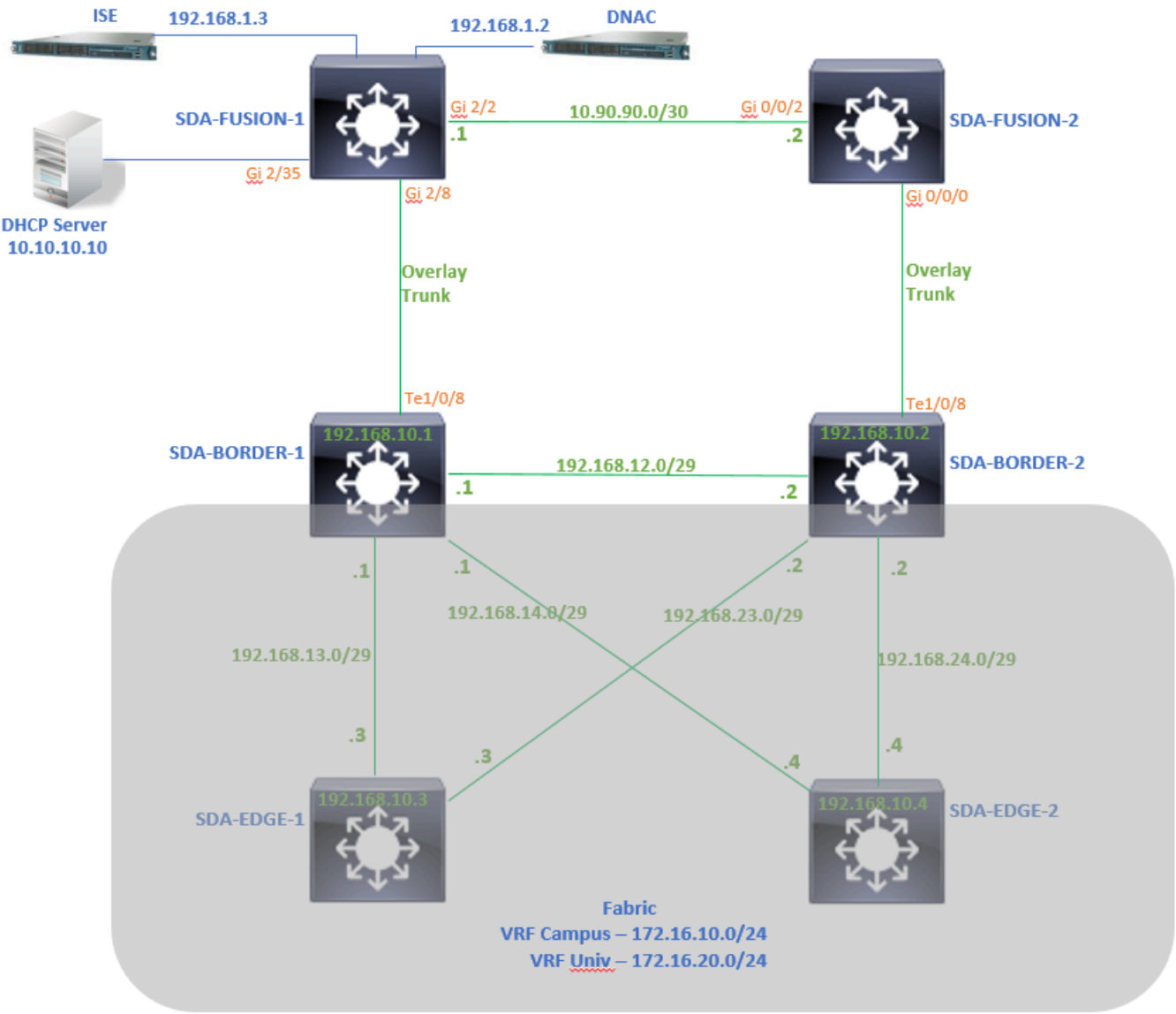
Remarque : Les noeuds de périphérie SD-Access ne prennent pas en charge les routes récapitulatives qui chevauchent les pools IP SD-Access. Les résumés de routage qui chevauchent les pools d'adresses IP doivent être filtrés dans les annonces de routage des périphériques Fusion vers les noeuds périphériques.

# Configurer

Les détails de configuration fournis ici concernent la topologie de réseau présentée ci-dessous. Cette topologie de réseau n'est pas recommandée pour les déploiements. Il est utilisé ici uniquement pour faciliter la présentation des exemples de configuration fournis. Pour connaître les conceptions de déploiement recommandées, reportez-vous à la section Zone de conception pour l'architecture de réseau numérique Cisco.

## Diagramme du réseau

La topologie utilisée pour cet article se compose de deux routeurs de périphérie configurés en tant que frontières externes et de deux routeurs de fusion avec une connexion à chaque routeur de périphérie respectif.



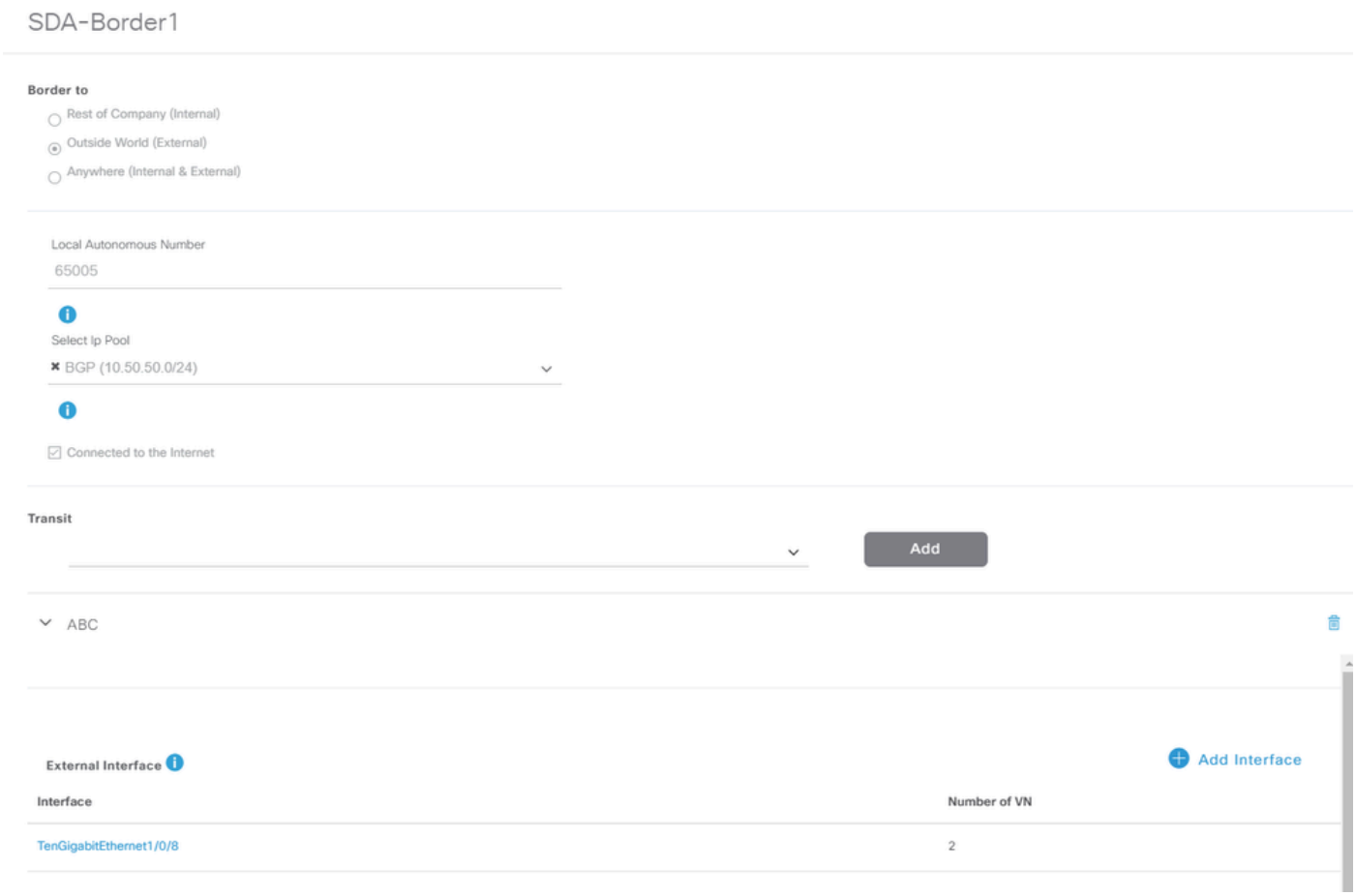

## Configurations

Étape 1 : configuration de la liaison de transfert

Lors de l'étape d'attribution d'un rôle de routeur périphérique lors de son ajout au fabric, une liaison de transfert peut être créée. Au niveau de la couche 2, il s'agit d'une liaison agrégée connectée au routeur Fusion. Les étapes suivantes sont nécessaires :

1. Configurez le numéro de système autonome local pour BGP. Ce numéro de système autonome (AS) est utilisé pour configurer le processus BGP sur les routeurs périphériques.

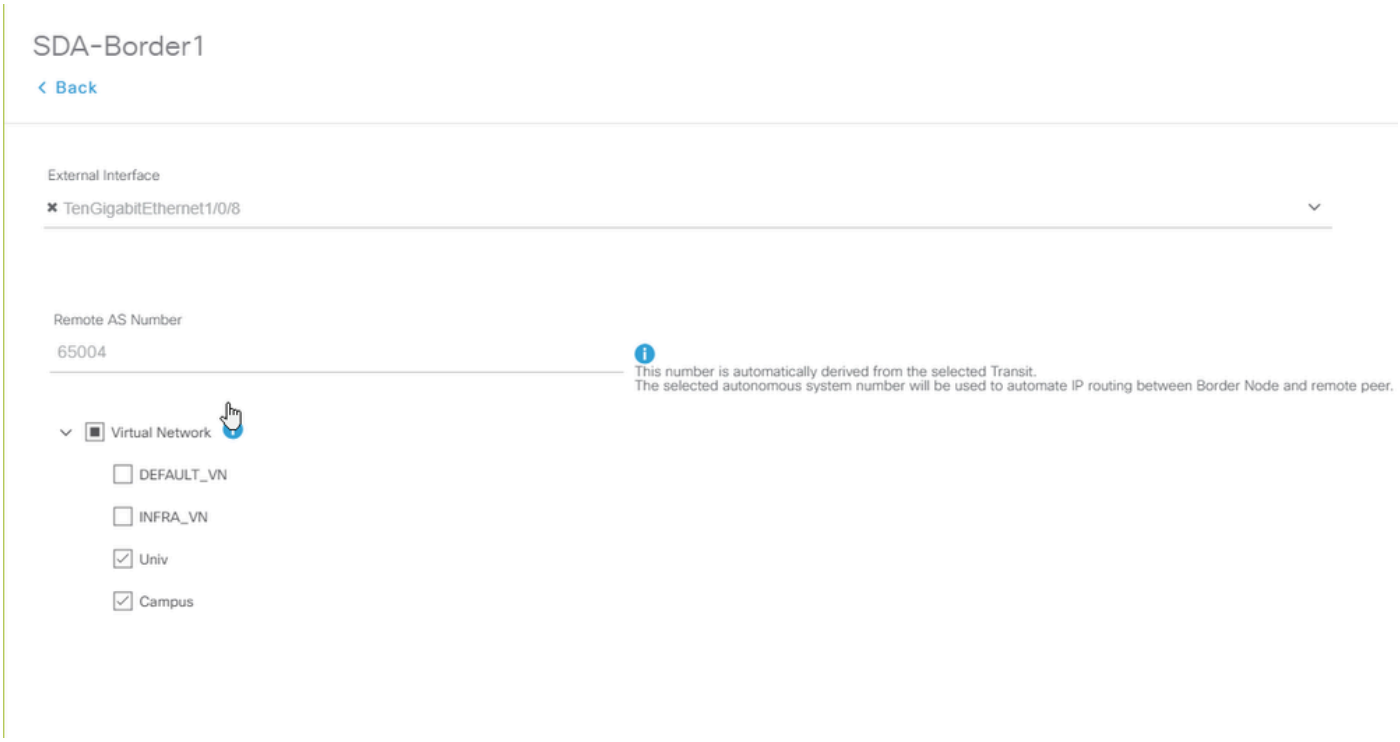
2. Ajoutez une interface sous Transit. Cette interface est la connexion directe entre le routeur Border et le routeur Fusion. (Le 1/0/8 sur la frontière dans cet exemple.)




3. Configurez le numéro de système autonome distant. Ce numéro de système autonome est utilisé sur les routeurs périphériques pour les instructions de voisinage vers le routeur Fusion afin de configurer des homologues BGP externes (eBGP).

4. Sélectionnez tous les réseaux virtuels (VRF) pour lesquels une fuite de VRF est requise sur le routeur Fusion.

5. Déployez la configuration de Cisco Catalyst Center vers les périphériques.




Suivez les mêmes étapes pour le périphérique SDA-Border-2.

Étape 2 : vérification des configurations transmises sur les routeurs périphériques

Cette section traite de la vérification de la configuration sur les routeurs périphériques en relation avec le protocole BGP.

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
```

Étape 3 : configuration des routeurs Fusion

Cette section illustre la configuration manuelle des routeurs Fusion.

SDA-Fusion-1

Configurez la liaison vers le routeur Border Router en tant qu'agrégation pour correspondre à la configuration de VLAN sur le routeur Border-1 :

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

Configurez les VRF requis :

```
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
```

Configurez les interfaces SVI :

```
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
```

Configurez l'appairage BGP externe (eBGP) avec 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
```

Configurez l'appairage BGP interne (iBGP) avec 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
 !
```

Annoncez le sous-réseau du serveur DHCP sous la famille d'adresses globale où l'adresse IP du

serveur DHCP est 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

Configurez la liaison vers le routeur périphérique. Si une interface sur Fusion est de couche 3 au lieu d'une agrégation, configurez les sous-interfaces :

```
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
```

Configurez les VRF correspondants :

```
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
```

```
!
```

Configurez l'appairage eBGP avec 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
```

Configurez l'appairage iBGP avec 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
```

Étape 4 : configuration de la fuite VRF sur le routeur Fusion

La configuration des fuites VRF est identique pour les routeurs Fusion SDA-Fusion-1 et SDA-Fusion-2.

Tout d'abord, configurez la fuite VRF entre les deux VRF (Campus et Univ), utilisez route-target 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
 !
```

Configurez ensuite les fuites de route entre la table de routage globale (GRT) et les VRF, et des VRF à la GRT, utilisez import ... map et 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
 !
```

# Vérifier

Cette section contient les étapes de vérification permettant de s'assurer que la configuration précédente a pris effet correctement.

Étape 1 : vérification de l’appairage eBGP entre les routeurs Fusion et Border

SDA-Border-1 ------Homologue--------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 ------Homologue--------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
```

Étape 2 : vérification de l'appairage iBGP entre les deux routeurs Fusion

SDA-Fusion-1 ------Homologue--------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
```

Étape 3. Vérification des préfixes dans la table BGP et la table de routage

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
```

# Configuration manuelle de la redondance en périphérie

Pour la redondance entre les PETR lorsqu'une liaison externe de frontière échoue, pour les frontières externes et externes + internes, vous devez construire manuellement des sessions iBGP entre les deux frontières pour chacun des VLAN. En outre, dans le cas d'une frontière externe + interne où BGP est importé dans LISP et LISP est redistribué dans BGP, des balises sont nécessaires pour empêcher les importations de routes iBGP vers LISP et ainsi éviter les boucles potentielles.

## 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
!
```

# Simplifier la configuration de Fusion avec l'utilisation de modèles

Cette section contient des exemples de configuration de modèle Fusion pour simplifier la configuration.

Ensuite, vous trouverez les variables à définir en fonction de votre conception de déploiement. Dans cet exemple, les configurations et les réseaux virtuels sont basés sur la topologie précédente qui comporte deux réseaux virtuels, Campus et Univ.

## Définition de variable

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

Global_prefixes = 10.10.10.8/30

FUSION_BGP_AS = 65004
BORDER_BGP_AS = 65005
```

Pour 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
```

Pour 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
```

## Exemple de modèle

### 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
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.