Implémenter et vérifier le VPN VxLAN BGP-Only sur Catalyst 9000

Table des matières

Introduction

Ce document décrit comment implémenter et vérifier Virtual Extensible LAN (VXLAN) Ethernet VPN (EVPN) sur les commutateurs de la gamme Cisco Catalyst 9000 avec Border Gateway

Protocol (BGP) uniquement.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- EVPN BGP
- Superposition VXLAN
- Guide de configuration du logiciel, Cisco IOS XE

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Catalyst 9600X
- Catalyst 9500X
- Cisco IOS XE 17.12 et versions ultérieures

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

La conception d'un réseau de campus de nouvelle génération implique l'adoption de technologies et d'architectures modernes pour répondre à l'évolution des demandes des utilisateurs, des applications et des périphériques. La solution VXLAN avec BGP EVPN peut fournir une architecture basée sur le fabric pour plus de simplicité, d'évolutivité et de facilité de gestion. Ce document décrit la solution EVPN BGP pour les utilisateurs qui préfèrent utiliser BGP pour le routage IPv4 et EVPN pour n'importe quelle raison.

Fonction d'utilisation EVPN BGP uniquement

VXLAN avec BGP EVPN utilise une architecture spine-leaf au lieu du modèle de réseau traditionnel à 3 niveaux. Avec une architecture spine-leaf, la spine agit comme un conduit à haut débit entre les commutateurs d'accès. Le modèle spine permet un modèle évolutif dans lequel la bande passante entre les leafs peut être augmentée par l'ajout de spines supplémentaires ou la capacité des terminaux peut être augmentée par l'ajout de leafs.

Pour les utilisateurs qui préfèrent utiliser le protocole BGP pour les informations de routage IPv4 et EVPN, incluez les considérations suivantes :

- Configuration simplifiée : avec une seule session BGP, la configuration et la gestion des informations de routage sont simplifiées. Il n'est pas nécessaire de déployer et de gérer des

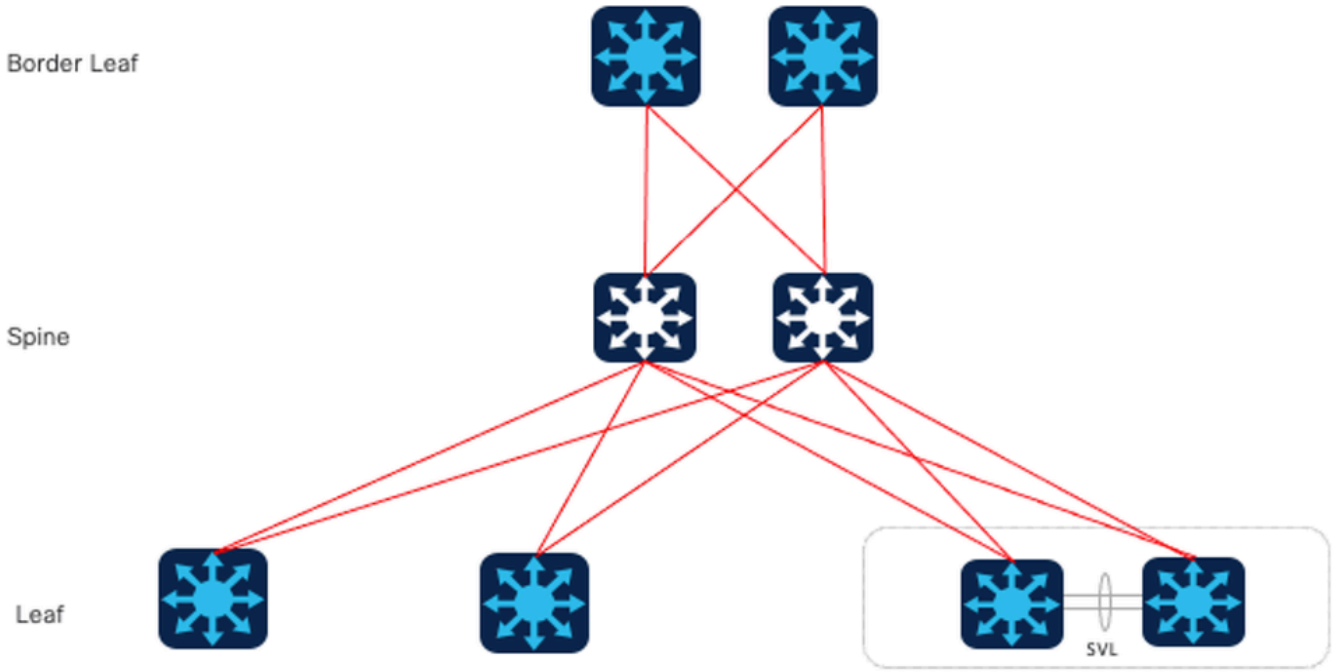
protocoles de routage distincts pour IPv4 et EVPN, ce qui réduit la complexité.

- Plan de contrôle unifié : en utilisant BGP comme protocole de routage unique, il existe un plan de contrôle unifié pour les routes IPv4 et EVPN. Cela facilite la propagation, la convergence et l'annonce de routage efficaces sur l'ensemble du réseau du data center.

- Évolutivité : le protocole BGP est parfaitement adapté à la gestion de réseaux à grande échelle et offre une évolutivité robuste. L'utilisation d'une seule session BGP pour les informations de routage IPv4 et EVPN garantit une évolutivité efficace au fur et à mesure de la croissance du réseau, sans nécessiter plusieurs instances de protocole de routage. En même temps, pour un fabric à grande échelle, le temps de convergence BGP est plus court.

- Interopérabilité : le protocole BGP est un protocole de routage standard largement adopté. L'utilisation de BGP simplifie exclusivement l'interopérabilité avec divers équipements et fournisseurs de réseau, garantissant la compatibilité et l'intégration transparente dans l'environnement du data center.

Cette topologie présente une conception de fabric unique C9K EVPN commune.



Conception de fabric unique C9K EVPN

Comparaisons et considérations EVPN BGP uniquement

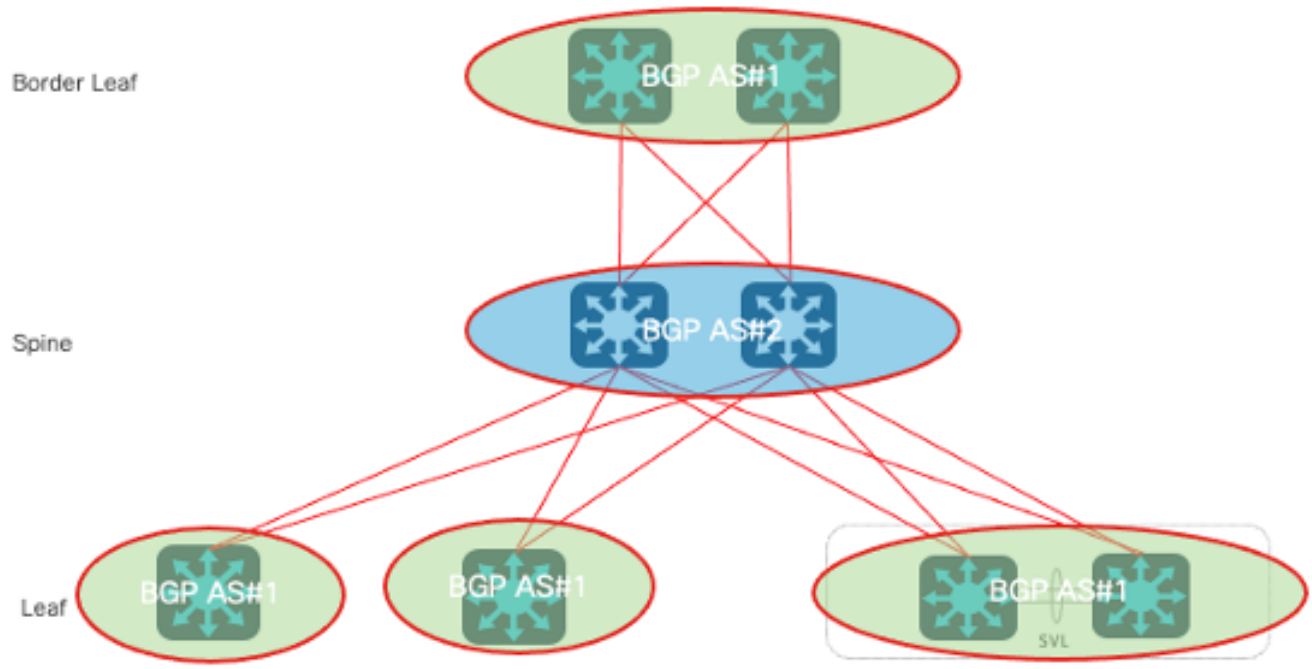
Comparaisons EBGP

Pour la conception BGP uniquement, la première question à considérer est de savoir s'il faut utiliser le BGP interne (IBGP) ou le BGP externe (EBGP). Cas d'utilisation d'IBGP, qui est courant dans le VPN VxLAN EVPN du DC traditionnel. Comparé à l'utilisation d'IBGP comme sous-couche, lors de l'utilisation d'EBGP, Spine n'a plus besoin d'être configuré comme réflecteur de route, mais fonctionne comme un serveur de routeur traditionnel pour échanger des routes. La condition préalable à ce document est donc l'utilisation du protocole EBGP.

Option 1.Deux AS : la colonne vertébrale utilise un AS, et la feuille et la feuille de bordure en utilisent un autre.

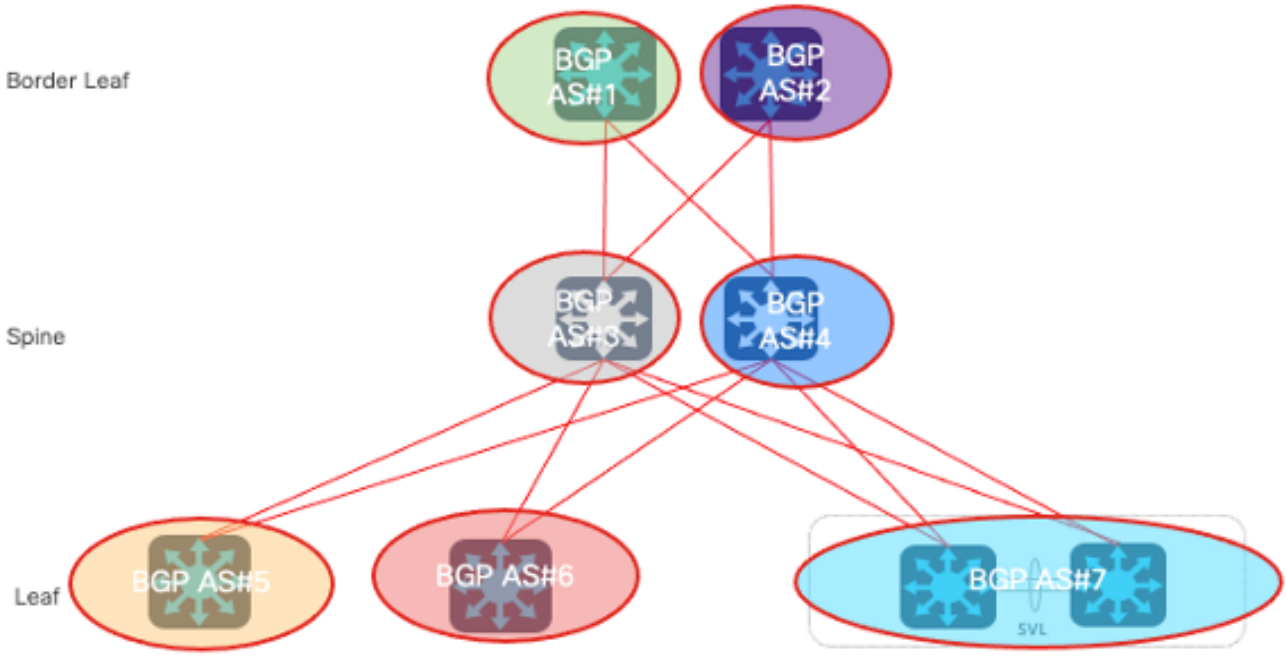
Modèle

Two-AS



Modèle Two-AS

Option 2. Multi-AS : Spine, Leaf et Border Leaf utilisent chacun un AS.



Modèle multi-AS

En comparant les deux conceptions, un problème commun est l'évolutivité, car pour l'option 2,

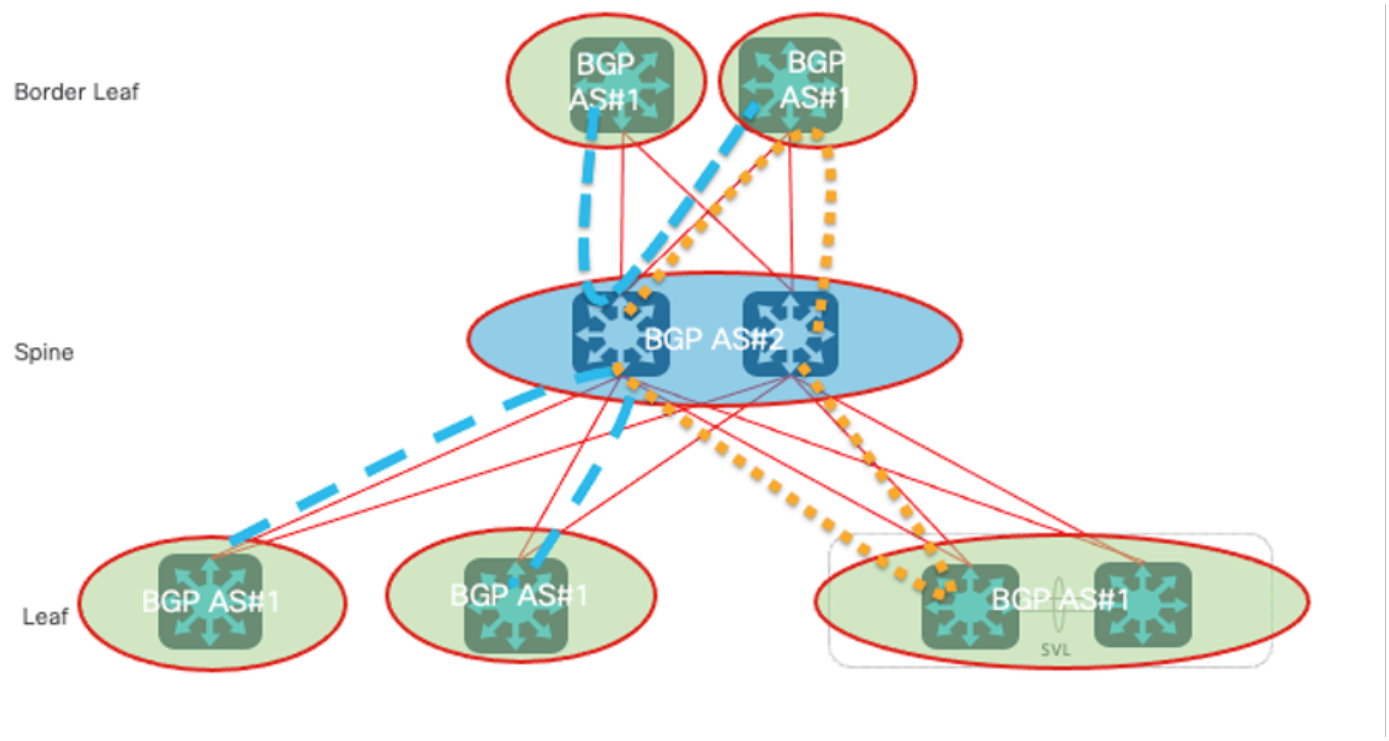
chaque fois qu'une colonne vertébrale ou une feuille est ajoutée, un nouveau numéro de système autonome doit être ajouté, ce qui entraîne des modifications de configuration plus complexes à l'avenir, ce qui n'est pas favorable à l'expansion et à la maintenance. Par conséquent, ce document utilise l'option 1. pour la discussion.

Par rapport à l'utilisation d'IBGP comme sous-couche, lors de l'utilisation d'EBGP, Spine n'a plus besoin d'être configuré comme réflecteur de route, mais fonctionne comme un serveur de routeur traditionnel pour échanger des routes.

Considération du routage IPv4 BGP sous-jacent

Ce sont des points clés qui doivent être pris en compte dans le plan sous-jacent.

Sous-jacent BGP IPv4 autorisé AS IN



Sous-jacent BGP IPv4 autorisé AS IN

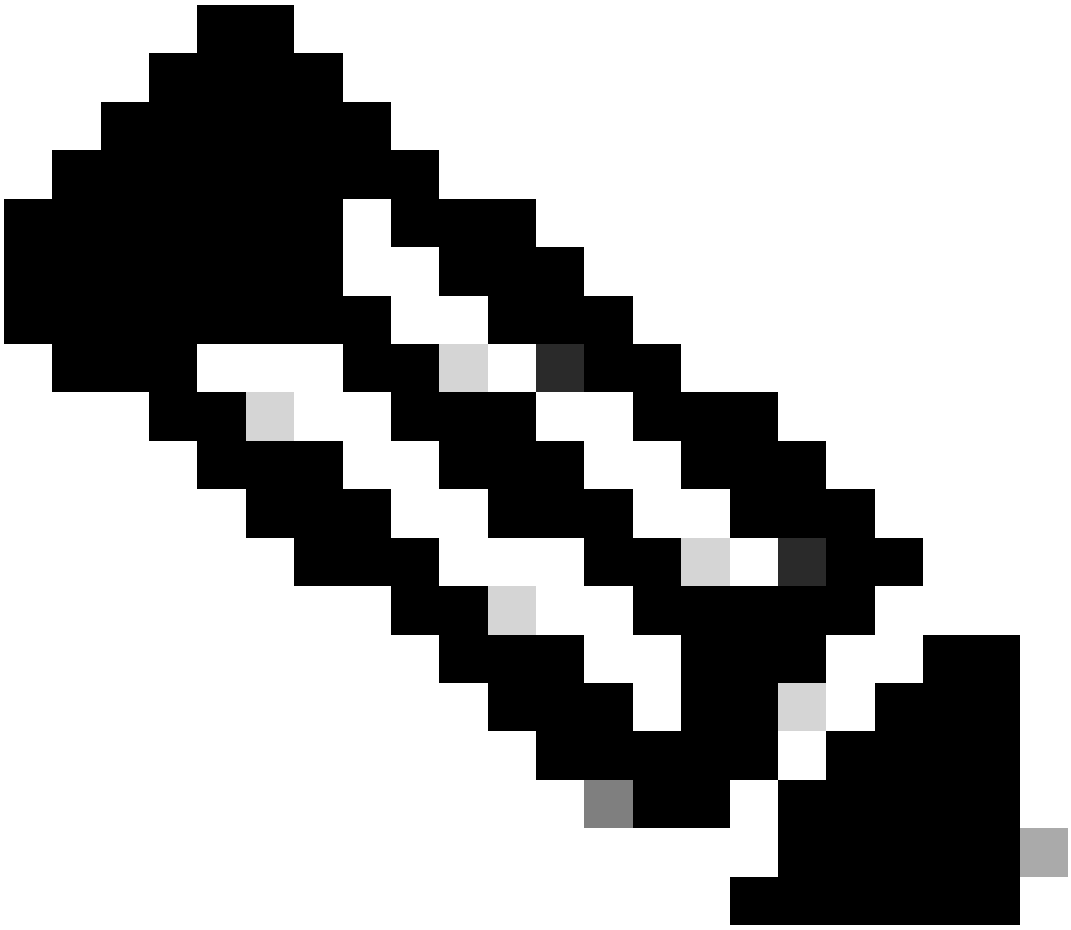
La détection de boucle AS s'effectue en analysant le chemin AS complet (comme spécifié dans l'attribut AS_PATH) et en vérifiant que le numéro de système autonome du système local n'apparaît pas dans le chemin AS.

Selon le schéma ci-dessus, la boucle AS BGP est formée - le même numéro AS dans l'as-path dans ce scénario :

- Sur les périphériques Leaf et Border Leaf, le chemin as est {#1, #2, #1}.
- Sur les périphériques Spine, le chemin as-path est {#2, #1, #2}.

Pour résoudre ce problème, allow-as-in est configuré dans la famille d'adresses IPv4 BGP, avec les instructions décrites ici :

- Autorisé AS In à n'apparaître qu'une seule fois sur tous les périphériques Leaf et Border Leaf (Leaf > Spine > Leaf), car tous les commutateurs Leaf fonctionnent dans le même AS.
- Autorisé AS In à n'apparaître qu'une seule fois sur tous les périphériques Spine (Spine > BL > Spine) ou (Spine > Leaf > Spine) car tous les périphériques Spine s'exécutent dans le même AS.

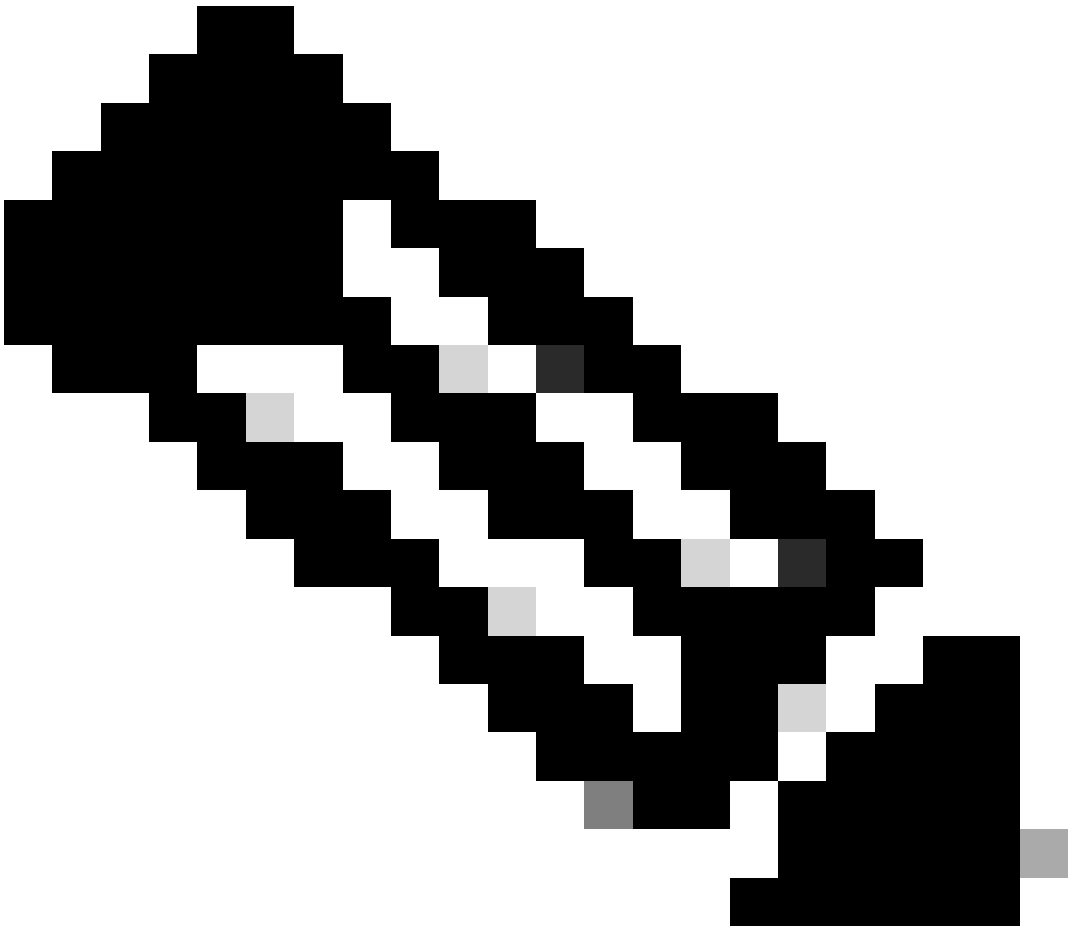


> Remarque : lorsque le fabric unique est utilisé avec DGW, il est peu probable que le routage soit nécessaire d'un spine à un autre. Cependant, compte tenu des modifications de topologie, telles que super-spine, il est recommandé de désactiver également la vérification AS sur les périphériques Spine.

Chemins maximum sous-jacents BGP IPv4

BGP choisit une route en fonction de ses critères, et il est peu probable qu'il apparaisse 2 routes ECMP dans la table BGP par défaut. Pour obtenir le protocole ECMP pour l'optimisation de la bande passante, 'maximum-paths X' doit être configuré dans la famille d'adresses IPv4 BGP dans tous les périphériques BGP en cours d'exécution. En attendant, nous vous suggérons de

conserver la même bande passante de liaison entre spine et leaf comme meilleure pratique.

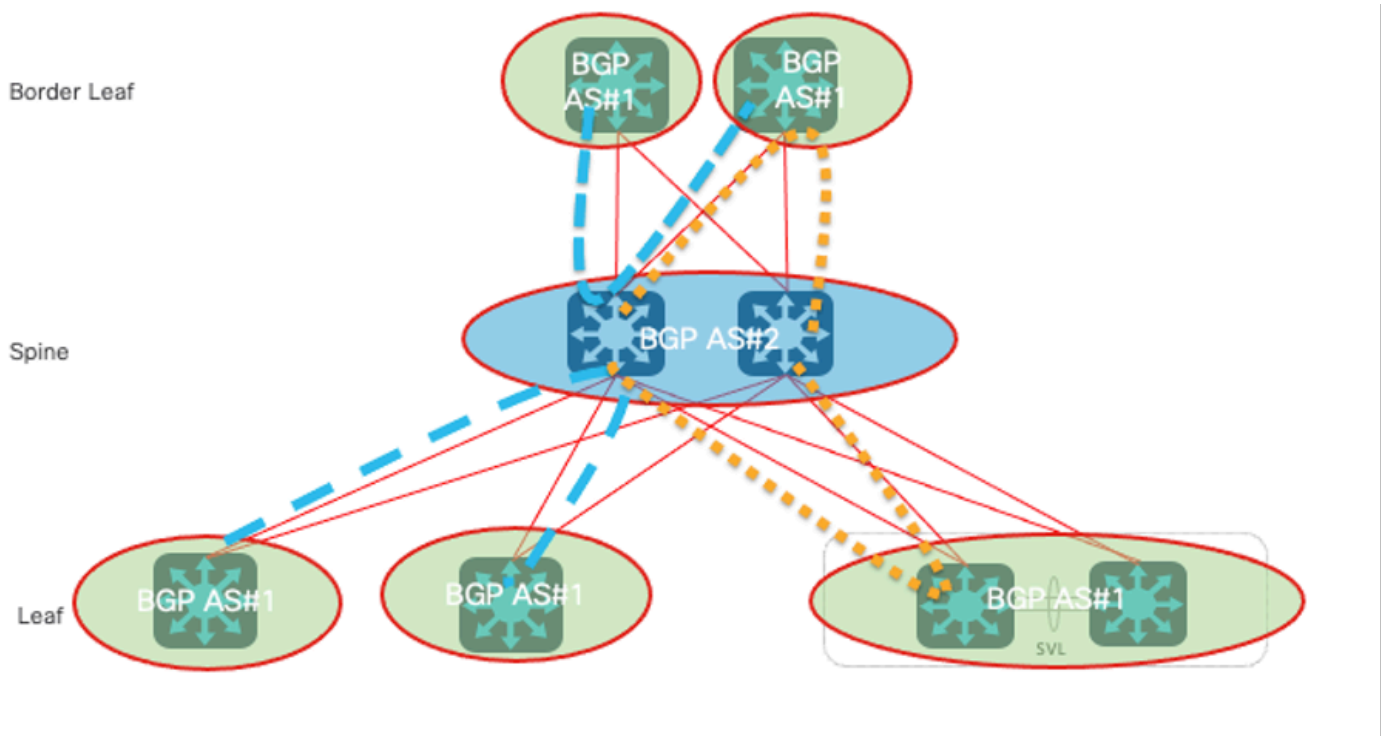


Remarque : les chemins maximum dépendent de la conception de la topologie. Avec deux commutateurs spine, vous pouvez configurer « maximum-paths 2 ».

Considération du routage EVPN BGP de superposition

Ces points clés doivent être considérés dans le plan de superposition.

EVPN BGP de superposition autorisé AS IN



Superposition BGP IPv4 autorisée AS IN

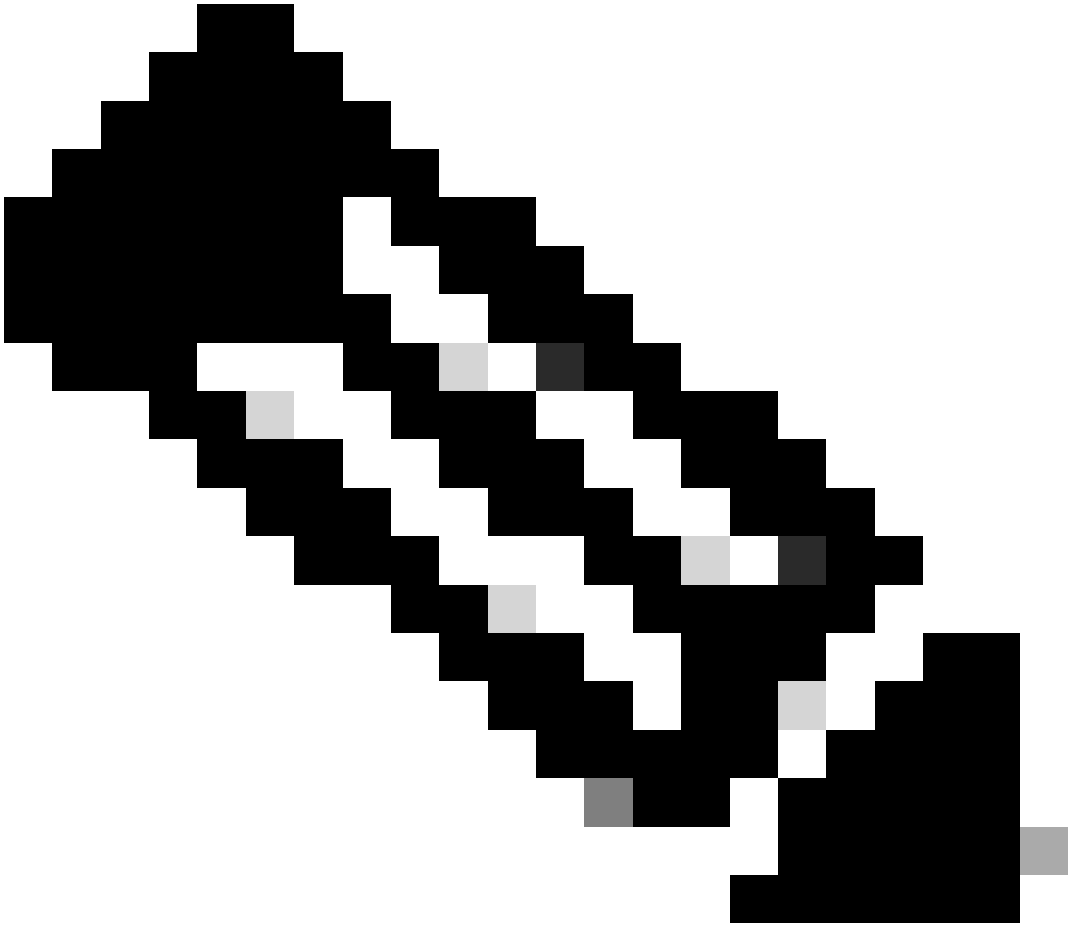
La détection de boucle AS s'effectue en analysant le chemin AS complet (comme spécifié dans l'attribut AS_PATH) et en vérifiant que le numéro de système autonome du système local n'apparaît pas dans le chemin AS.

Selon l'image, la boucle AS BGP est formée - le même numéro AS dans l'as-path dans ce scénario :

- Sur les périphériques Leaf et Border Leaf, le chemin as est {#1, #2, #1}
- Sur les périphériques Spine, le chemin as est {#2, #1, #2}

Pour résoudre ce problème, l'autorisation d'accès en entrée doit être configurée dans la famille d'adresses IPv4 BGP, avec les instructions suivantes :

- Autorisé AS In à n'apparaître qu'une seule fois sur tous les périphériques Leaf et Border Leaf (Leaf > Spine > Leaf), car tous les commutateurs Leaf fonctionnent dans le même AS.
- Autorisé AS In à n'apparaître qu'une seule fois sur tous les périphériques Spine (Spine > BL > Spine) ou (Spine > Leaf > Spine) car tous les périphériques Spine s'exécutent dans le même AS.



Remarque : lorsque le fabric unique est utilisé avec DGW, il est peu probable que le routage soit nécessaire d'un spine à un autre. Cependant, compte tenu des modifications de topologie, telles que super-spine, il est recommandé de désactiver également la vérification AS sur les périphériques Spine.

Overlay BGP EVPN Ne pas modifier le tronçon suivant

Le protocole BGP modifie l'attribut de tronçon suivant des informations d'accessibilité de couche réseau (NLRI) annoncées à partir du voisin EBGP par défaut. Le point d'extrémité de tunnel leaf/VXLAN (VTEP) utilise son adresse source NVE comme attribut de tronçon suivant des routes EVPN, et cette adresse est utilisée pour déterminer la destination du tunnel VXLAN (Network Virtual Interface/NVE peer). Si les noeuds spine changent le tronçon suivant, le tunnel VXLAN ne peut pas être correctement établi.

Pour résoudre ce problème, ces instructions sont appliquées.

- Sur tous les noeuds Spine, vous devez configurer route-map avec action next-hop inchangé

Filtre RT de désactivation EVPN BGP de superposition

Les routes EVPN à partir des périphériques Leaf sont annoncées avec la communauté Route Target (RT). Les routeurs sans la configuration RT correspondante abandonnent les routes avec la communauté RT par défaut. En revanche, aucun VRF (Virtual Routing and Forwarding) n'est configuré sur tous les périphériques dorsaux. Cela signifie que les périphériques dorsaux abandonnent toutes les routes EVPN annoncées à partir des périphériques Leaf par défaut.

Pour résoudre ce problème, sur tous les noeuds Spine, le filtre route-cible par défaut doit être désactivé.

Configurer

Diagramme du réseau

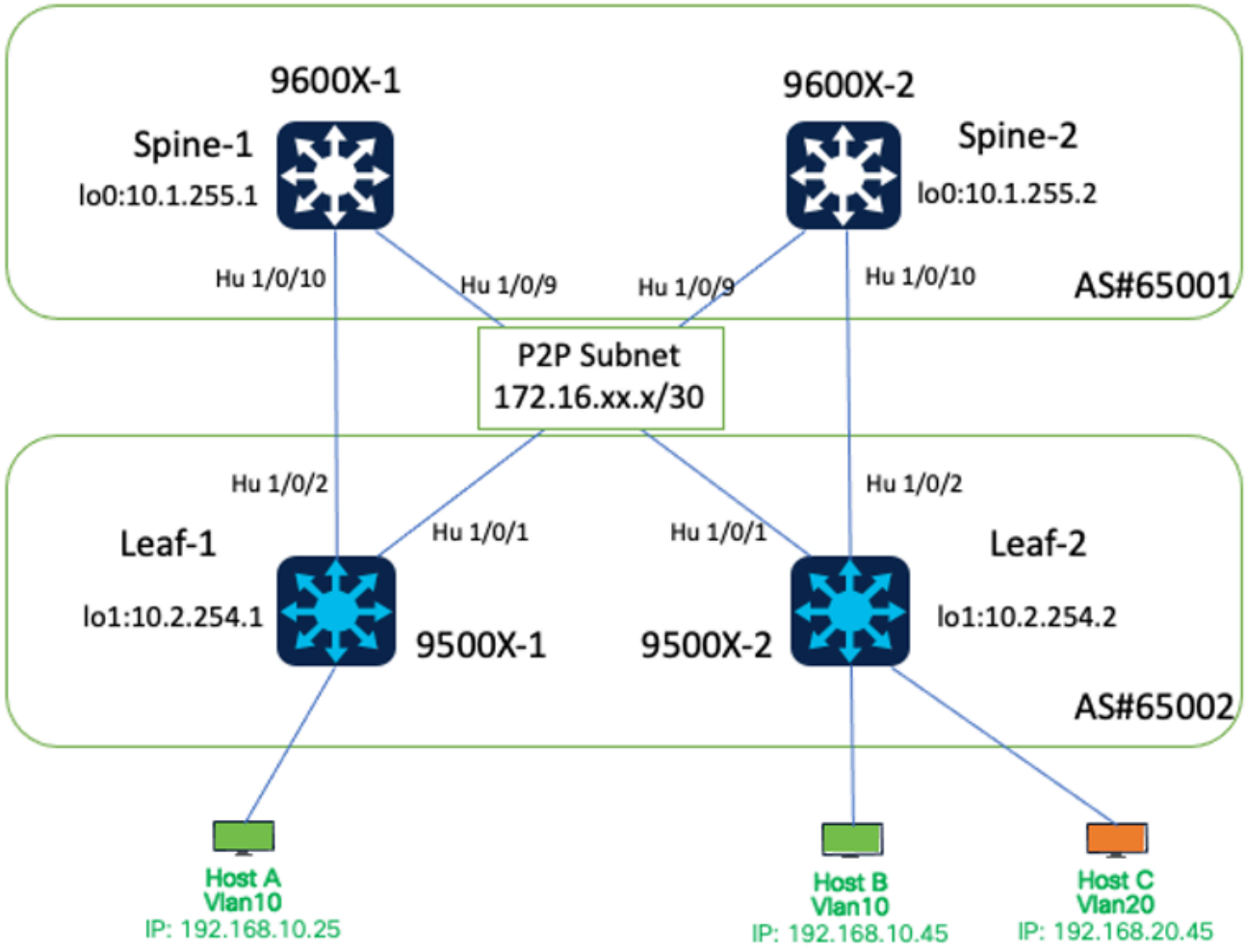
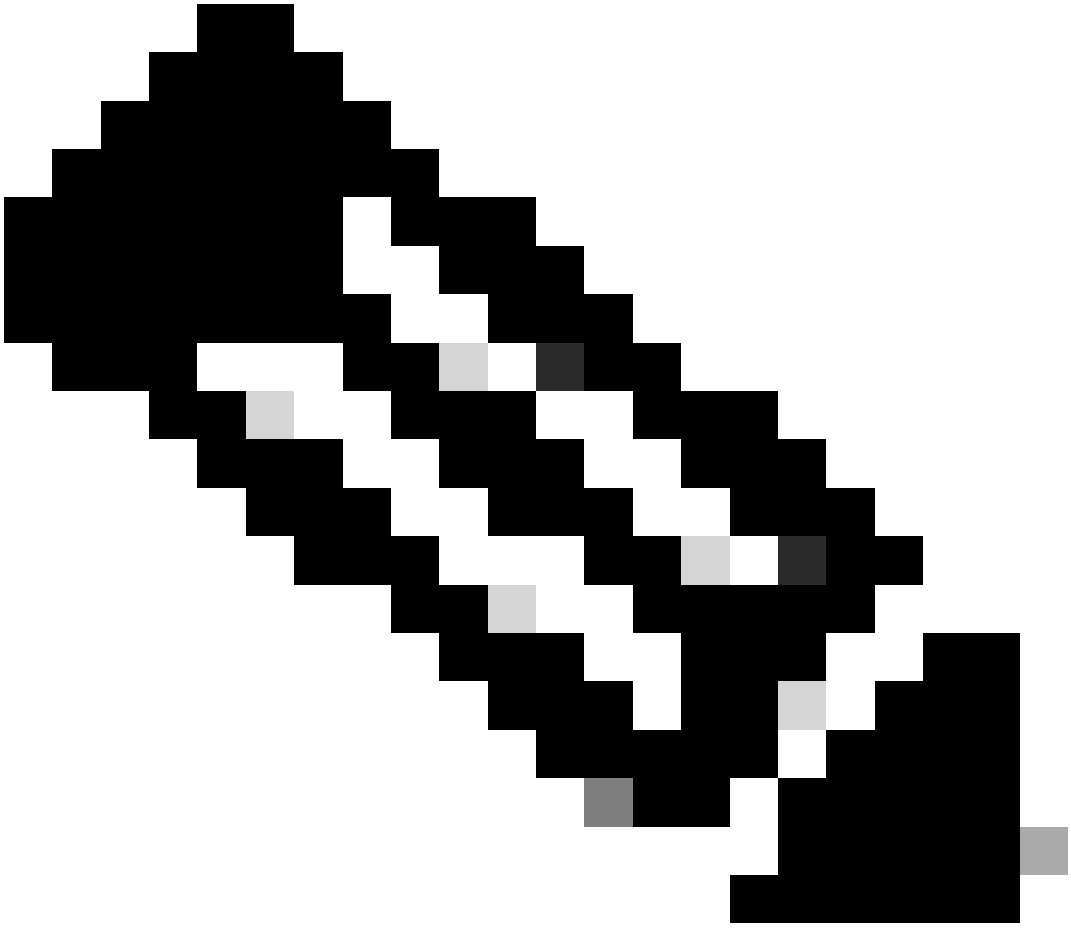


Diagramme du réseau

Les détails de l'interface de cet environnement de travaux pratiques sont les suivants.

Nom du périphérique	Version du logiciel	Interface#	Adresse IP
Spine-1	IOS-XE 17.12.1	Hu 01/01/9	172.16.12.1/30
		Hu 01/01/10	172.16.11.1/30
		Lo 0	10.1.255.1/32
Spine-2	IOS-XE 17.12.1	Hu 01/01/9	172.16.21.1/30
		Hu 01/01/10	172.16.22.1/30
		Lo 0	10.1.255.2/32
Feuille 1	IOS-XE 17.12.1	Hu 0/1/1	172.16.21.2/30
		Hu 0/1/2	172.16.11.2/30
		Niveau 1	10.2.254.1/32
Feuille 2	IOS-XE 17.12.1	Hu 0/1/1	172.16.12.2/30
		Hu 0/1/2	172.16.22.2/30
		Niveau 1	10.2.254.2/32



Remarque : l'affectation d'adresses IP dans ces travaux pratiques est uniquement à des fins de test. Le masque de sous-réseau (c'est-à-dire /30, /31) pour les connexions point à point peut être considéré en fonction de vos exigences de conception réelles.

Configurations

Routage IPv4 BGP sous-jacent

Dans cet exemple, les interfaces physiques sont utilisées pour établir des connexions BGP.

- Configuration du routage IPv4 BGP
- Configurer BGP IPv4 autorisé AS In
- Configurez les chemins d'accès maximum BGP

Configuration du routage IPv4 BGP

Configuration sur le Spine :

```
router bgp 65001
bgp log-neighbor-changes
bgp listen range 172.16.0.0/16 peer-group Leaf-Peers
no bgp default ipv4-unicast
neighbor Leaf-Peers peer-group
neighbor Leaf-Peers remote-as 65002
!
address-family ipv4
redistribute connected
neighbor Leaf-Peers activate
neighbor Leaf-Peers allowas-in 1
maximum-paths 2
exit-address-family
```

Configuration sur Leaf-1 :

```
router bgp 65002
bgp log-neighbor-changes
no bgp default ipv4-unicast
neighbor 172.16.11.1 remote-as 65001
neighbor 172.16.21.1 remote-as 65001
!
address-family ipv4
redistribute connected
neighbor 172.16.11.1 activate
neighbor 172.16.21.1 activate
exit-address-family
```

Configuration sur Leaf-2 :

```
router bgp 65002
bgp log-neighbor-changes
no bgp default ipv4-unicast
neighbor 172.16.12.1 remote-as 65001
neighbor 172.16.22.1 remote-as 65001
!
address-family ipv4
redistribute connected
neighbor 172.16.12.1 activate
neighbor 172.16.22.1 activate
exit-address-family
```

Configurer BGP IPv4 autorisé AS In

Configuration sur le Spine :

```
router bgp 65001
address-family ipv4
neighbor Leaf-Peers allowas-in 1
```

Configuration sur Leaf-1 :

```
router bgp 65002
address-family ipv4
neighbor 172.16.11.1 allowas-in 1
neighbor 172.16.21.1 allowas-in 1
```

Configuration sur Leaf-2 :

```
router bgp 65002
address-family ipv4
neighbor 172.16.12.1 allowas-in 1
neighbor 172.16.22.1 allowas-in 1
```

Configuration des chemins d'accès maximaux BGP
Configuration sur le Spine :

```
router bgp 65001
address-family ipv4
maximum-paths 2
```

Configuration sur leaf :

```
router bgp 65002
address-family ipv4
maximum-paths 2
```

Multidiffusion Sous-Jacente

Pour permettre à la réplication multidiffusion (MR) de gérer le trafic de diffusion, de monodiffusion inconnue et de multidiffusion link-local (BUM), le routage multidiffusion est requis sur tous les périphériques Spine et Leaf. PIM doit être activé sur toutes les interfaces de connexion Spine et Leaf et sur les boucles associées.

Exemple de multidiffusion sous-jacente sur Spine 1 :

```
ip multicast-routing
ip pim rp-address 10.1.255.1 //configure Spine loopback as RP
interface Loopback0
ip pim sparse-mode
interface HundredGigE1/0/9
ip pim sparse-mode
```

```
interface HundredGigE1/0/10
ip pim sparse-mode
```

BGP superposé

- Configurer le EVPN L2VPN BGP
- Configurer le EVPN BGP autorisé AS dans
- Configuration du protocole EVPN BGP Ne pas modifier le tronçon suivant
- Configurer le filtre RT de désactivation EVPN BGP

Configurer BGP L2VPN EVPN

Configuration sur le Spine :

```
router bgp 65001
neighbor Leaf-Peers ebgp-multihop 255
address-family l2vpn evpn
neighbor Leaf-Peers activate
neighbor Leaf-Peers send-community both
```

Configuration sur Leaf-1 :

```
router bgp 65002
neighbor 172.16.11.1 ebgp-multihop 255
neighbor 172.16.21.1 ebgp-multihop 255
address-family l2vpn evpn
neighbor 172.16.11.1 activate
neighbor 172.16.11.1 send-community both
neighbor 172.16.21.1 activate
neighbor 172.16.21.1 send-community both
```

Configuration sur Leaf-2 :

```
router bgp 65002
neighbor 172.16.12.1 ebgp-multihop 255
neighbor 172.16.22.1 ebgp-multihop 255
address-family l2vpn evpn
neighbor 172.16.12.1 activate
neighbor 172.16.12.1 send-community both
neighbor 172.16.22.1 activate
neighbor 172.16.22.1 send-community both
```

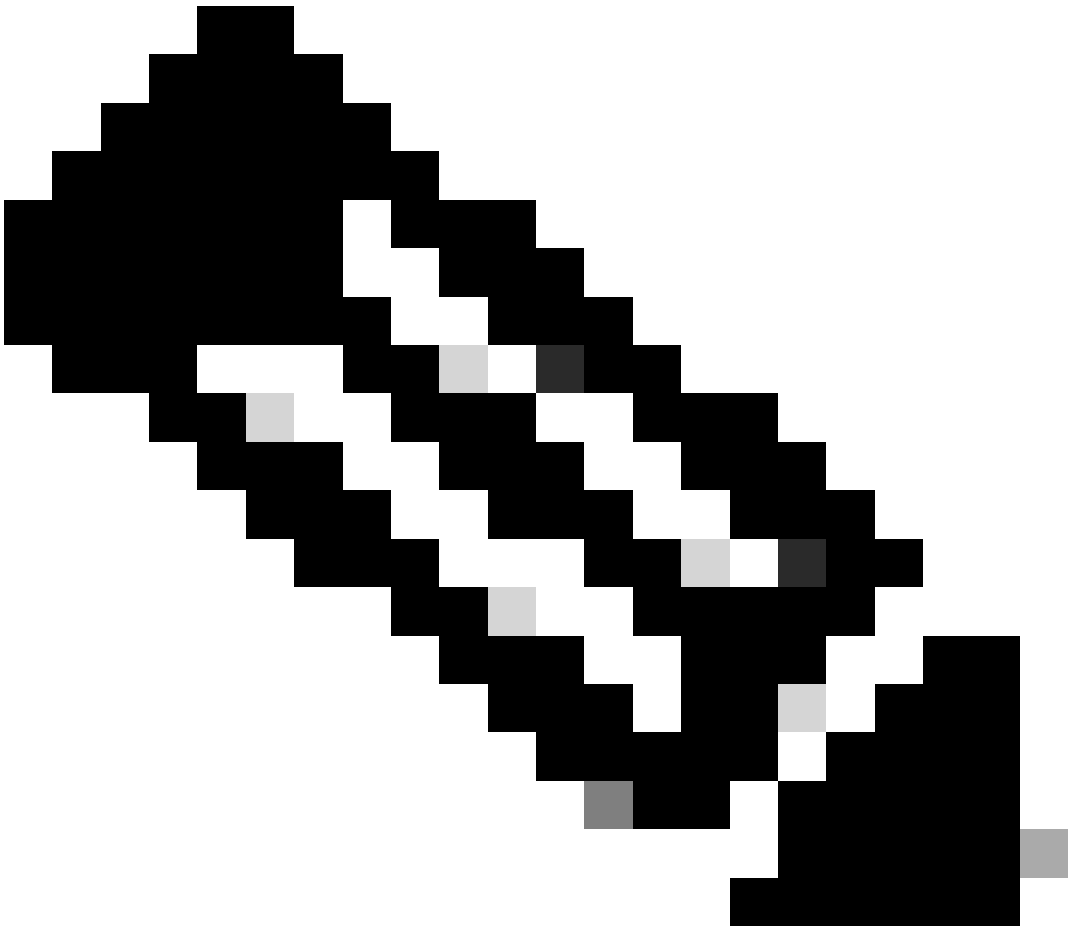
Configurer le EVPN BGP autorisé AS dans

Configuration sur Leaf-1 :

```
router bgp 65002
address-family l2vpn evpn
neighbor 172.16.11.1 allowas-in 1
neighbor 172.16.21.1 allowas-in 1
```

Configuration sur Leaf-2 :

```
router bgp 65002
address-family l2vpn evpn
neighbor 172.16.12.1 allowas-in 1
neighbor 172.16.22.1 allowas-in 1
```



Remarque : lorsque le fabric unique est utilisé avec DGW, il est peu probable que le routage soit nécessaire d'un spine à un autre. Cependant, compte tenu des modifications de topologie, telles que super-spine, il est recommandé de désactiver également la vérification AS sur les périphériques Spine.

Configurer BGP EVPN ne pas modifier le tronçon suivant

Configuration sur le Spine :

```
route-map BGP-NHU permit 10
set ip next-hop unchanged
!
router bgp 65001
address-family l2vpn evpn
neighbor Leaf-Peers route-map BGP-NHU out
```

Configurer le filtre RT de désactivation EVPN BGP

Configuration sur le Spine :

```
router bgp 65001
no bgp default route-target filter
```

Configuration VRF sur leaf

```
vrf definition S1-EVPN
rd 1:1
!
address-family ipv4
route-target export 1:1
route-target import 1:1
route-target export 1:1 stitching
route-target import 1:1 stitching
exit-address-family
router bgp 65002
address-family ipv4 vrf S1-EVPN
advertise l2vpn evpn
redistribute connected
maximum-paths 2
exit-address-family
```

EVPN L2

Activez la réplication EVPN L2VPN et multicast sur Leaf :

```
l2vpn evpn
replication-type static
```

Créer des instances EVPN (EVI) sur le leaf :

```
l2vpn evpn instance 10 vlan-based
encapsulation vxlan
l2vpn evpn instance 20 vlan-based
encapsulation vxlan
```

Créez des VLAN et des VNI pour le trafic utilisateur sur Leaf :

```
vlan configuration 10
member evpn-instance 10 vni 10010
vlan configuration 20
member evpn-instance 20 vni 10020
```

Créez une interface NVE et cousez VNI sur des groupes de moulage sur Leaf.

```
interface nve1
no ip address
source-interface Loopback1
host-reachability protocol bgp
member vni 10010 mcast-group 225.0.0.10
member vni 10020 mcast-group 225.0.0.20
```

EVPN L3

Créez un VLAN pour L3VNI sur Leaf. EVI n'est pas requis pour L3VNI.

```
vlan configuration 3000
member vni 33000
```

Configurez SVI pour L2VNI sur Leaf.

```
interface Vlan10
mac-address 0010.0010.0010
vrf forwarding S1-EVPN
ip address 192.168.10.254 255.255.255.0
```

Configurez l'interface SVI pour L3VNI sur leaf. « no autostate » est configuré pour activer l'interface SVI lorsqu'aucune interface active n'est attribuée à ce VLAN.

```
interface Vlan3000
```

```
vrf forwarding S1-EVPN
ip unnumbered Loopback1
no autostate
```

Sur Leaf, cousez L3VNI sur le VRF en configuration NVE.

```
interface nve1
member vni 33000 vrf S1-EVPN
```

Vérifier

Vérification de l'établissement des sessions BGP

```
C9600X-SPINE-1#show ip bgp all summary
For address family: IPv4 Unicast
BGP router identifier 10.1.255.1, local AS number 65001
BGP table version is 23, main routing table version 23
12 network entries using 2976 bytes of memory
22 path entries using 2992 bytes of memory
2 multipath network entries and 4 multipath paths
4/3 BGP path/bestpath attribute entries using 1184 bytes of memory
3 BGP AS-PATH entries using 104 bytes of memory
8 BGP extended community entries using 400 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 7656 total bytes of memory
BGP activity 7259/7235 prefixes, 13926/13892 paths, scan interval 60 secs
12 networks peaked at 07:06:41 Dec 5 2023 UTC (2w1d ago)

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
*172.16.11.2    4        65002     138     130       23    0    0 01:38:17        9
*172.16.12.2    4        65002     138     130       23    0    0 01:38:11        9
* Dynamically created based on a listen range command
Dynamically created neighbors: 2, Subnet ranges: 1

BGP peergroup Leaf-Peers listen range group members:
  172.16.0.0/16

For address family: L2VPN E-VPN
BGP router identifier 10.1.255.1, local AS number 65001
BGP table version is 27, main routing table version 27
10 network entries using 3840 bytes of memory
12 path entries using 2784 bytes of memory
8/6 BGP path/bestpath attribute entries using 2368 bytes of memory
3 BGP AS-PATH entries using 104 bytes of memory
8 BGP extended community entries using 400 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 9496 total bytes of memory
BGP activity 7259/7235 prefixes, 13926/13892 paths, scan interval 60 secs
12 networks peaked at 07:38:03 Dec 6 2023 UTC (2w0d ago)
```

```
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
*172.16.11.2    4        65002     138     130       27    0    0 01:38:17        6
*172.16.12.2    4        65002     138     130       27    0    0 01:38:11        6
* Dynamically created based on a listen range command
Dynamically created neighbors: 2, Subnet ranges: 1

BGP peergroup Leaf-Peers listen range group members:
  172.16.0.0/16

Total dynamically created neighbors: 2/(100 max), Subnet ranges: 1


C9500X-LEAF-1#show ip bgp all summary
For address family: IPv4 Unicast
BGP router identifier 10.2.255.1, local AS number 65002
BGP table version is 19, main routing table version 19
12 network entries using 2976 bytes of memory
22 path entries using 2992 bytes of memory
2 multipath network entries and 4 multipath paths
4/3 BGP path/bestpath attribute entries using 1184 bytes of memory
3 BGP AS-PATH entries using 104 bytes of memory
8 BGP extended community entries using 384 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 7640 total bytes of memory
BGP activity 577/545 prefixes, 4021/3975 paths, scan interval 60 secs
12 networks peaked at 07:10:16 Dec 5 2023 UTC (1d18h ago)

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.16.11.1     4        65001    2427    3100       19    0    0 20:39:49        9
172.16.21.1     4        65001    2430    3094       19    0    0 20:39:49        9

For address family: L2VPN E-VPN
BGP router identifier 10.2.255.1, local AS number 65002
BGP table version is 5371, main routing table version 5371
16 network entries using 6144 bytes of memory
20 path entries using 4640 bytes of memory
9/9 BGP path/bestpath attribute entries using 2664 bytes of memory
3 BGP AS-PATH entries using 104 bytes of memory
8 BGP extended community entries using 384 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 13936 total bytes of memory
BGP activity 577/545 prefixes, 4021/3975 paths, scan interval 60 secs
16 networks peaked at 07:36:38 Dec 6 2023 UTC (18:16:58.620 ago)

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.16.11.1     4        65001    2427    3100     5371    0    0 20:39:49        4
172.16.21.1     4        65001    2430    3094     5371    0    0 20:39:49        4


Initiate traffic between hosts, verify IP Multicast and PIM configuration, and mroute table.

Please note that on IOS-XE platform, (*, G) entry should always present, and (S, G) entry presents only




C9600X-SPINE-1#show ip mroute
IP Multicast Routing Table
<snip>
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
```

```
                        t - LISP transit group
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 225.0.0.20), 16:51:00/stopped, RP 10.1.255.1, flags: SJCx
  Incoming interface: HundredGigE1/0/2, RPF nbr 172.16.11.1
  Outgoing interface list:
    Tunnel0, Forward/Sparse-Dense, 16:51:00/00:02:58, flags:

(*, 225.0.0.10), 16:51:14/stopped, RP 10.1.255.1, flags: SJCFx
  Incoming interface: HundredGigE1/0/2, RPF nbr 172.16.11.1
  Outgoing interface list:
    Tunnel0, Forward/Sparse-Dense, 16:51:14/00:02:45, flags:

(10.2.254.1, 225.0.0.10), 00:00:01/00:02:57, flags: FTx
  Incoming interface: Loopback1, RPF nbr 0.0.0.0, Registering
  Outgoing interface list:
    HundredGigE1/0/2, Forward/Sparse, 00:00:01/00:03:27, flags:

(*, 224.0.1.40), 1d18h/00:02:42, RP 10.1.255.1, flags: SJCL
  Incoming interface: HundredGigE1/0/2, RPF nbr 172.16.11.1
  Outgoing interface list:
    Loopback0, Forward/Sparse, 1d18h/00:02:42, flags
```

Vérifier EVPN L2

```
C9500X-LEAF-1#show l2vpn evpn evi 10 detail
EVPN instance:       10 (VLAN Based)
  RD:                10.2.254.1:10 (auto)
  Import-RTs:        65002:10
  Export-RTs:        65002:10
<snip>

C9500X-LEAF-1#show nve peers
'M' - MAC entry download flag  'A' - Adjacency download flag
'4' - IPv4 flag  '6' - IPv6 flag

Interface  VNI      Type Peer-IP          RMAC/Num_RTs   eVNI     state flags UP time
nve1       33000    L3CP 10.2.254.2       242a.0412.0102 33000      UP  A/M/4 18:11:35
nve1       10010    L2CP 10.2.254.2       2              10010      UP   N/A  00:36:00
nve1       10020    L2CP 10.2.254.2       2              10020      UP   N/A  00:01:17

C9500X-LEAF-1#show bgp l2vpn evpn
BGP table version is 5475, local router ID is 10.2.254.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path, L long-lived-stale,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 10.2.254.1:10
 *>   [2][10.2.254.1:10][0][48][683B78FC8C9F][0][*]/20
                       10.2.254.2                             0 65001 65002 ?
 *>   [2][10.2.254.1:10][0][48][683B78FC8C9F][32][192.168.10.45]/24
                       10.2.254.2                             0 65001 65002 ?
```

```
<snip>

C9500X-LEAF-1#show bgp l2vpn evpn detail [2][10.2.254.1:10][0][48][683B78FC8C9F][32][192.168.10.45]/24
BGP routing table entry for [2][10.2.254.1:10][0][48][683B78FC8C9F][32][192.168.10.45]/24, version 5371
Paths: (1 available, best #1, table evi_10)
  Not advertised to any peer
  Refresh Epoch 12
  65001 65002, imported path from [2][10.2.254.2:10][0][48][683B78FC8C9F][32][192.168.10.45]/24 (global)
    10.2.254.2 (via default) from 172.16.21.1 (10.1.255.2)
      Origin incomplete, localpref 100, valid, external, best
      EVPN ESI: 00000000000000000000, Label1 10010, Label2 33000
      Extended Community: RT:1:1 RT:65002:10 ENCAP:8
        Router MAC:242A.0412.0102
      rx pathid: 0, tx pathid: 0x0
      Updated on Dec 7 2023 01:52:33 UTC

C9500X-LEAF-1#show device-tracking database
<snip>

    Network Layer Address                  Link Layer Address     Interface  vlan       prlvl      ag
ARP 192.168.20.25                          3c13.cc01.a7df         Hu1/0/7    20         0005       3m
ARP 192.168.10.25                          3c13.cc01.a7df         Hu1/0/7    10         0005       20

C9500X-LEAF-1#show l2vpn evpn mac ip
IP Address                            EVI   VLAN  MAC Address    Next Hop(s)
------------------------------------- ----- ----- -------------- -----------
192.168.10.25                         10    10    3c13.cc01.a7df Hu1/0/7:10
192.168.10.45                         10    10    683b.78fc.8c9f 10.2.254.2
```

Vérifier EVPN L3

```
C9500X-LEAF-1#show nve peers
'M' - MAC entry download flag  'A' - Adjacency download flag
'4' - IPv4 flag  '6' - IPv6 flag

Interface  VNI      Type Peer-IP          RMAC/Num_RTs   eVNI     state flags UP time
nve1       33000    L3CP 10.2.254.2       242a.0412.0102 33000      UP  A/M/4 18:50:51
nve1       10010    L2CP 10.2.254.2       2              10010      UP   N/A  01:15:16
nve1       10020    L2CP 10.2.254.2       2              10020      UP   N/A  00:31:39

9500X-LEAF-1#sh bgp l2vpn evpn
BGP table version is 5523, local router ID is 10.2.255.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path, L long-lived-stale,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
<snip>
Route Distinguisher: 1:1 (default for vrf S1-EVPN)
 *>   [5][1:1][0][24][192.168.10.0]/17
                       0.0.0.0                  0         32768 ?
 *>   [5][1:1][0][24][192.168.20.0]/17
```

```
                    0.0.0.0                  0         32768 ?

C9500X-LEAF-1#sh ip ro vrf S1-EVPN

Routing Table: S1-EVPN
<snip>
      192.168.10.0/24 is variably subnetted, 4 subnets, 2 masks
C        192.168.10.0/24 is directly connected, Vlan10
S        192.168.10.25/32 is directly connected, Vlan10
B        192.168.10.45/32 [20/0] via 10.2.254.2, 00:00:56, Vlan3000
L        192.168.10.254/32 is directly connected, Vlan10
      192.168.20.0/24 is variably subnetted, 4 subnets, 2 masks
C        192.168.20.0/24 is directly connected, Vlan20
S        192.168.20.25/32 is directly connected, Vlan20
B        192.168.20.45/32 [20/0] via 10.2.254.2, 00:49:54, Vlan3000
L        192.168.20.254/32 is directly connected, Vlan20
```

Informations connexes

- Guide de configuration de VXLAN EVPN BGP, Cisco IOS XE Dublin 17.12.x : https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/17-12/configuration_guide/vxlan/b_1712_bgp_evpn_vxlan_9500_cg/bgp_evpn_vxlan_overview.html
- Assistance technique de Cisco et téléchargements

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.