

Implementación y Verificación de VxLAN EVPN Solo BGP en Catalyst 9000

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Función de Uso de BGP-only EVPN](#)

[Comparaciones y Consideraciones de BGP-Only EVPN](#)

[Comparaciones EBGp](#)

[Consideración del Ruteo IPv4 de BGP Subyacente](#)

[BGP IPv4 subyacente permitido como en](#)

[Trayectorias Máximas BGP IPv4 Subyacentes](#)

[Consideración del Ruteo EVPN BGP de Superposición](#)

[EVPN BGP superpuesto permitido AS IN](#)

[Overlay BGP EVPN Do no cambia el salto siguiente](#)

[Filtro RT de EVPN Desactivable de BGP superpuesto](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Routing IPv4 BGP subyacente](#)

[Configuración del routing BGP IPv4](#)

[Configuración de BGP IPv4 Allowed AS In](#)

[Configuración de rutas máximas BGP](#)

[Multidifusión subyacente](#)

[BGP superpuesto](#)

[Configuración de BGP L2VPN EVPN](#)

[Configuración de BGP EVPN Allowed AS In](#)

[Configure BGP EVPN do not Change Next-Hop](#)

[Configuración del Filtro RT de Desactivación de BGP EVPN](#)

[Configuración de VRF en Hoja](#)

[EVPN L2](#)

[EVPN L3](#)

[Verificación](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo implementar y verificar Virtual Extensible LAN (VXLAN) Ethernet VPN (EVPN) solamente en los Cisco Catalyst 9000 Series Switches con Border Gateway Protocol

(BGP).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- EVPN BGP
- Superposición de VXLAN
- Guía de configuración de software, Cisco IOS XE

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Catalyst 9600X
- Catalyst 9500X
- Cisco IOS XE 17.12 y posterior

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

El diseño de una red de campus de última generación implica la adopción de tecnologías y arquitecturas modernas para satisfacer las demandas cambiantes de los usuarios, las aplicaciones y los dispositivos. VXLAN con la solución BGP EVPN puede proporcionar una arquitectura basada en fabric para lograr simplicidad, escalabilidad y facilidad de gestión. Este documento describe la solución BGP EVPN para los usuarios que prefieren utilizar BGP para el ruteo IPv4 y EVPN por cualquier motivo.

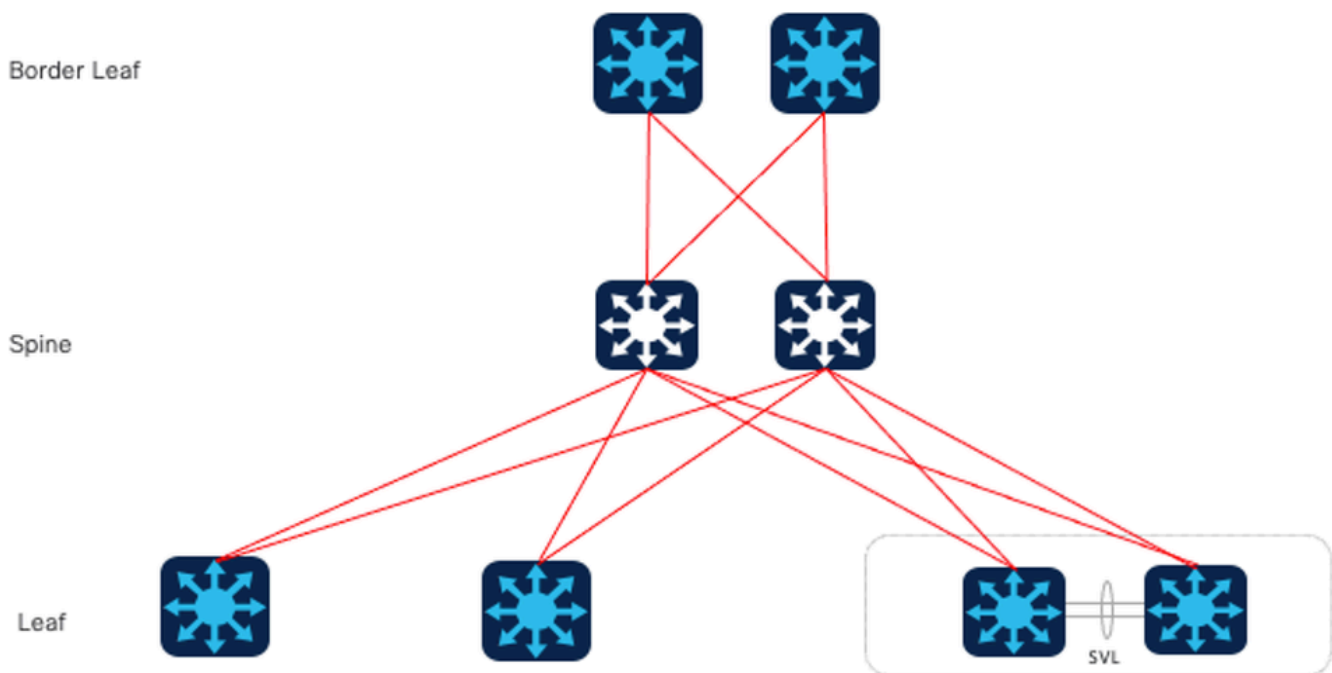
Función de Uso de BGP-only EVPN

VXLAN con BGP EVPN utiliza una arquitectura de columna y hoja en lugar del modelo de red tradicional de 3 niveles. Con una arquitectura de columna y hoja, la columna actúa como un conducto de alta velocidad entre los switches de acceso. El modelo de columna permite un modelo de escalabilidad horizontal en el que se puede aumentar el ancho de banda entre las hojas añadiendo columnas adicionales o se puede aumentar la capacidad del terminal añadiendo más hojas.

Para los usuarios que prefieren utilizar BGP para la información de ruteo IPv4 y EVPN, incluya estas consideraciones:

- Configuración simplificada: con una sola sesión BGP, la configuración y la gestión de la información de routing se simplifican. No es necesario implementar y mantener protocolos de routing independientes para IPv4 y EVPN, lo que reduce la complejidad.
- Plano de control unificado: al utilizar BGP como único protocolo de routing, existe un plano de control unificado para las rutas IPv4 y EVPN. Esto facilita la propagación eficaz de rutas, la convergencia y la publicidad de rutas en toda la red del Data Center.
- Escalabilidad: BGP es idóneo para gestionar redes a gran escala y ofrece una sólida escalabilidad. El uso de una única sesión BGP para la información de routing de IPv4 y EVPN garantiza una escalabilidad eficaz a medida que crece la red, sin necesidad de contar con varias instancias de protocolo de routing. Al mismo tiempo, para el fabric a gran escala, el tiempo de convergencia de BGP es más corto.
- Interoperabilidad: BGP es un protocolo de routing estándar del sector ampliamente adoptado. El uso exclusivo de BGP simplifica la interoperabilidad con diversos equipos de red y proveedores, lo que garantiza la compatibilidad y la integración perfecta en el entorno del Data Center.

Esta topología muestra un diseño de fabric único EVPN C9K común.



Diseño de fabric único EVPN C9K

Comparaciones y Consideraciones de BGP-Only EVPN

Comparaciones EBG

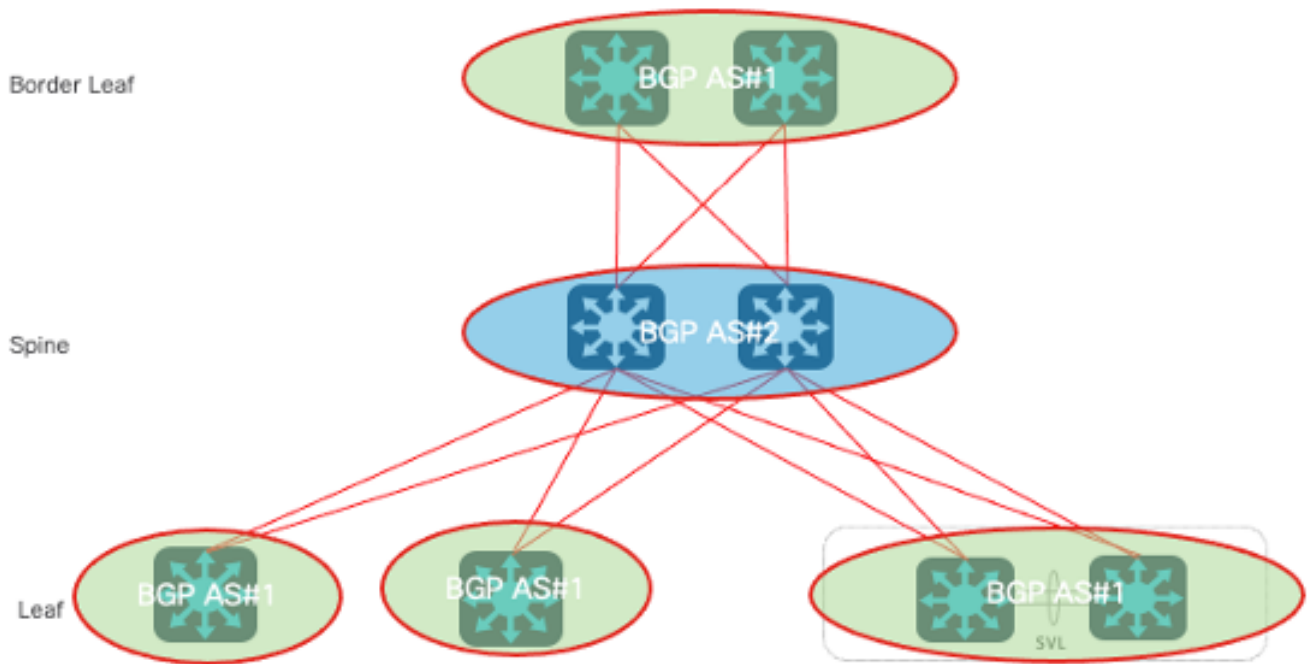
Para el diseño solo de BGP, el primer problema a considerar es si utilizar BGP interno (IBGP) o BGP externo (EBGP). El caso del uso de IBGP, que es común en VxLAN EVPN del DC tradicional. En comparación con el uso de IBGP como subyacente, cuando se utiliza EBG, la columna ya no necesita configurarse como reflector de ruta, sino que funciona como un servidor

de router tradicional para intercambiar rutas. Por lo tanto, el requisito previo para este documento es el caso del uso de EBGP.

Opción 1. Two-AS: La columna utiliza un AS y la hoja y el borde de la hoja utilizan otro AS.

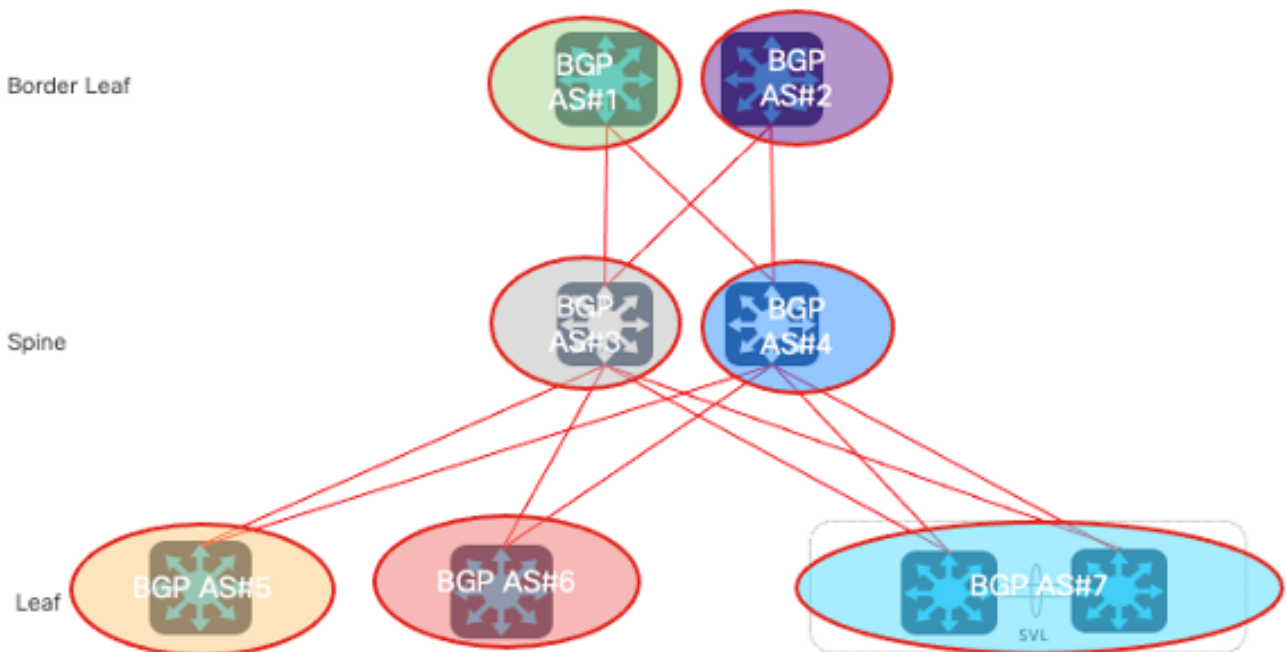
Modelo

de dos AS



Modelo de dos AS

Opción 2. Multi-AS: columna, hoja y hoja de borde cada uno utiliza un AS.



Modelo Multi-AS

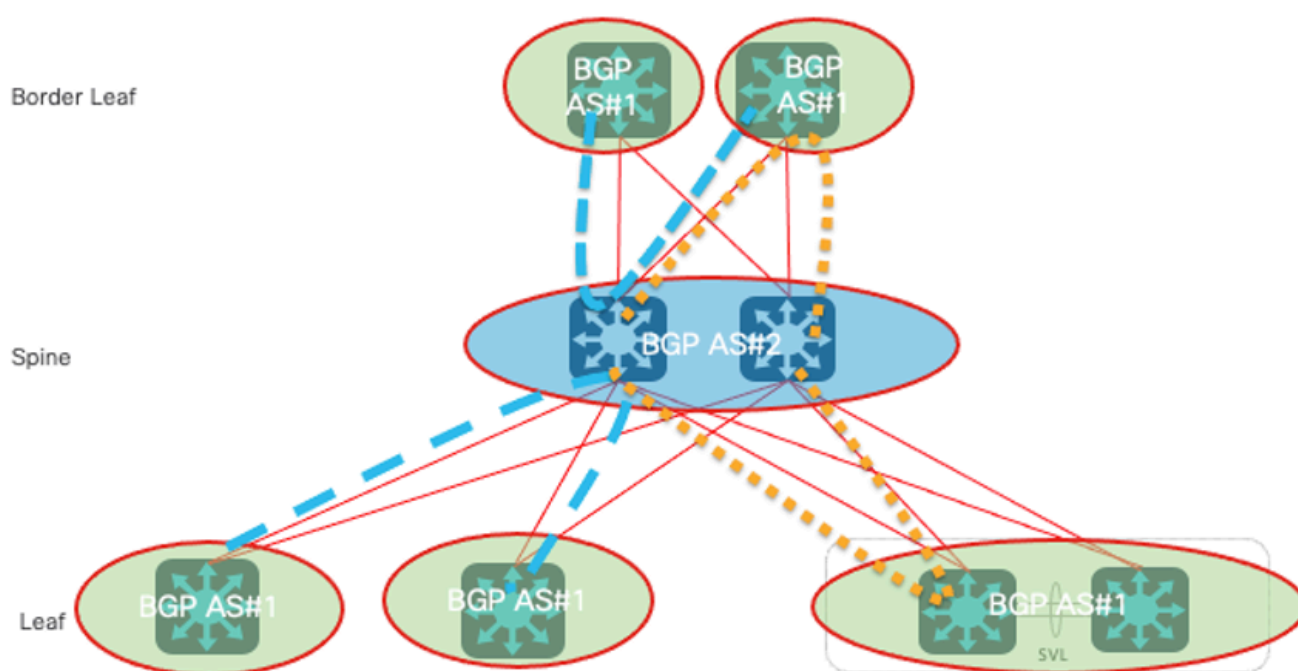
Al comparar los dos diseños, un problema común es la escalabilidad, ya que para la opción 2, cada vez que se agrega una columna o una hoja, es necesario agregar un nuevo número AS, lo que conlleva cambios de configuración más complejos en el futuro, lo que no es propicio para la expansión y el mantenimiento. Por lo tanto, este documento utiliza la opción 1 para la discusión.

En comparación con el uso de IBGP como subyacente, cuando se usa EBGP, la columna ya no necesita configurarse como reflector de ruta, sino que funciona como un servidor de router tradicional para intercambiar rutas.

Consideración del Ruteo IPv4 de BGP Subyacente

Estos son puntos clave que deben tenerse en cuenta en el plano subyacente.

BGP IPv4 subyacente permitido como en



BGP IPv4 subyacente permitido como en

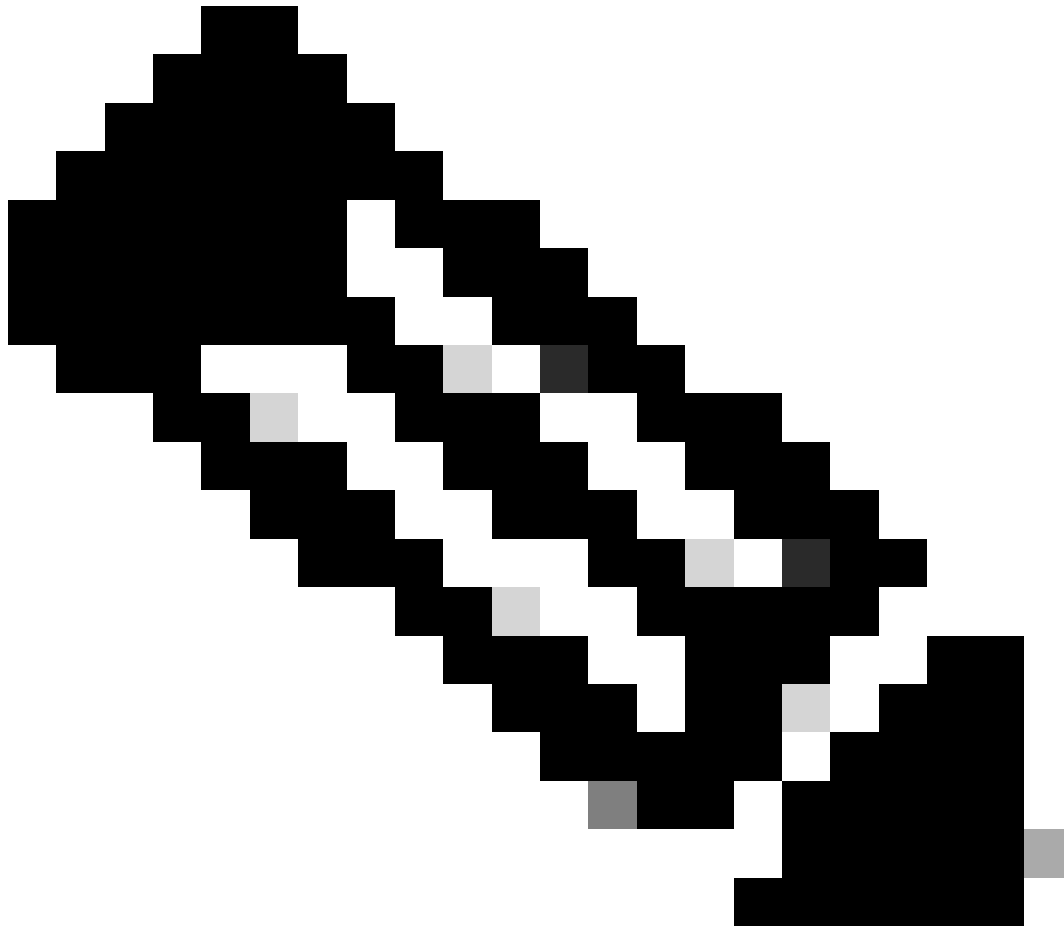
La detección del loop AS se realiza explorando la trayectoria AS completa (como se especifica en el atributo AS_PATH) y verificando que el número del sistema autónomo del sistema local no aparezca en la trayectoria AS.

De acuerdo con el diagrama anterior, se forma el loop AS BGP - el mismo número AS en el as-path en este escenario:

- En los dispositivos de hoja y de hoja de borde, el as-path es {#1, #2, #1}.
- En los dispositivos de columna, el as-path es {#2, #1, #2}.

Para resolver este problema, se configura allow-as-in en la familia de direcciones IPv4 de BGP, con las instrucciones descritas aquí:

- AS In solo puede aparecer una vez en todos los dispositivos de hoja y de hoja de borde (Hoja > Columna > Hoja) ya que todos los switches de hoja se ejecutan en el mismo AS.
 - Se permite que AS In aparezca solo una vez en todos los dispositivos de columna (Columna > BL > Columna) o (Columna > Hoja > Columna) ya que todos los dispositivos de columna se ejecutan en el mismo AS.
-

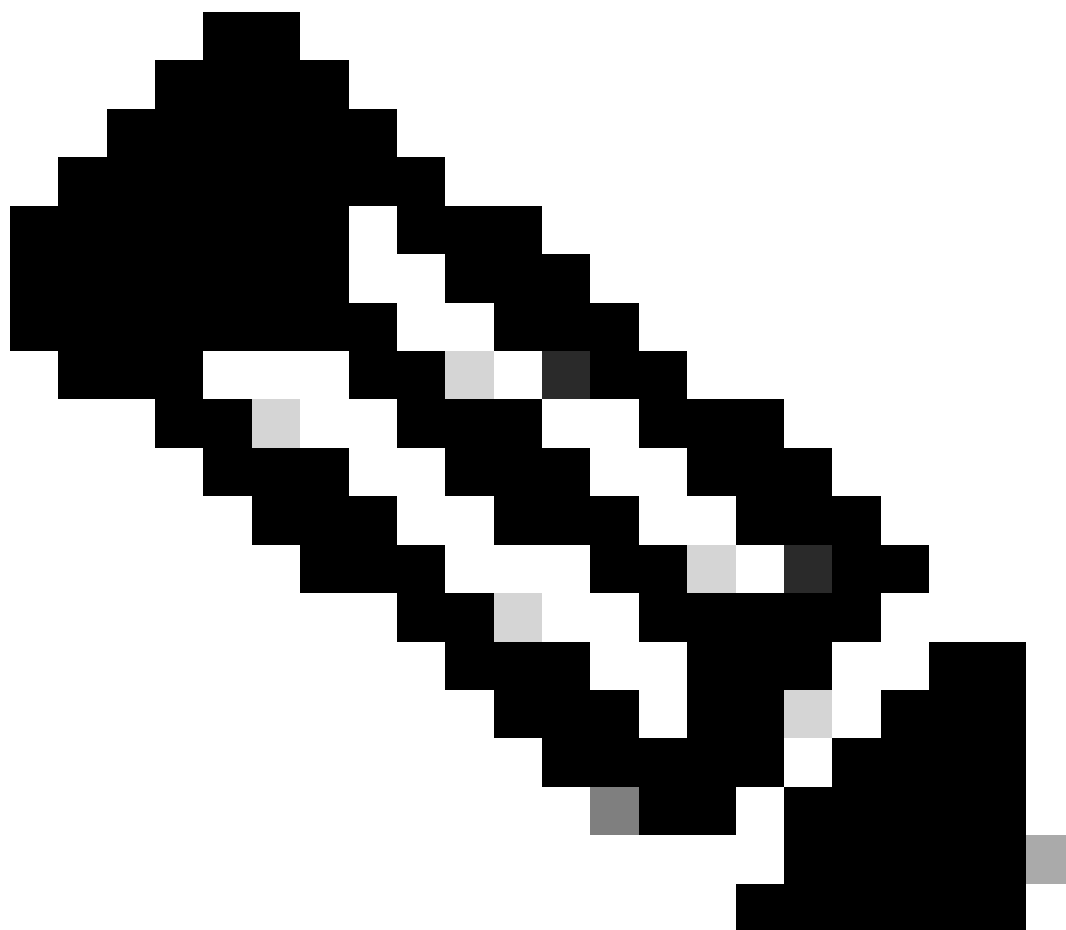


Nota: cuando se utiliza Single-Fabric con DGW, es poco probable que se requiera routing de una columna a otra. Sin embargo, teniendo en cuenta los cambios de topología, como la supercolumna, también se recomienda desactivar la comprobación de AS en los dispositivos de columna.

Trayectorias Máximas BGP IPv4 Subyacentes

BGP elige una ruta en función de sus criterios y es poco probable que aparezcan 2 rutas ECMP en la tabla BGP de forma predeterminada. Para lograr ECMP para la optimización del ancho de banda, 'maximum-paths X' debe configurarse en la familia de direcciones IPv4 de BGP en todos los dispositivos que ejecutan BGP. Mientras tanto, sugerimos mantener el mismo ancho de banda

de link entre la columna y la hoja como práctica recomendada.

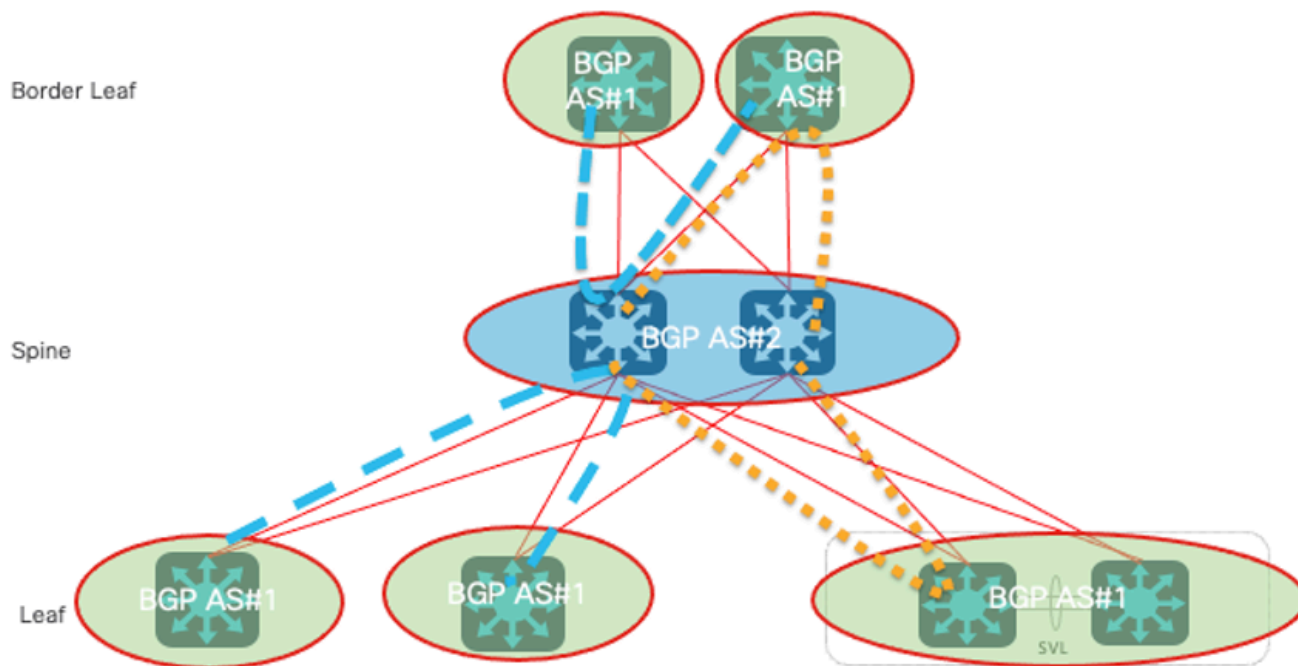


Nota: Las rutas máximas dependen del diseño de la topología. Con dos switches de columna, puede configurar 'maximum-paths 2'.

Consideración del Ruteo EVPN BGP de Superposición

Estos puntos clave deben considerarse en el plano de superposición.

EVPN BGP superpuesto permitido AS IN



Se permite la superposición de BGP IPv4 AS IN

La detección del loop AS se realiza explorando la trayectoria AS completa (como se especifica en el atributo AS_PATH) y verificando que el número del sistema autónomo del sistema local no aparezca en la trayectoria AS.

Según la imagen, se forma el loop AS BGP - el mismo número AS en el as-path en este escenario:

- En los dispositivos de hoja y de hoja de borde, el as-path es {#1, #2, #1}
- En los dispositivos de columna, el as-path es {#2, #1, #2}

Para resolver este problema, se debe configurar allow-as-in en la familia de direcciones IPv4 de BGP, con las instrucciones descritas:

- AS In solo puede aparecer una vez en todos los dispositivos de hoja y de hoja de borde (Hoja > Columna > Hoja) ya que todos los switches de hoja se ejecutan en el mismo AS.
- Se permite que AS In aparezca solo una vez en todos los dispositivos de columna (Columna > BL > Columna) o (Columna > Hoja > Columna) ya que todos los dispositivos de columna se ejecutan en el mismo AS.



Nota: cuando se utiliza Single-Fabric con DGW, es poco probable que se requiera routing de una columna a otra. Sin embargo, teniendo en cuenta los cambios de topología, como la supercolumna, también se recomienda desactivar la comprobación de AS en los dispositivos de columna.

Overlay BGP EVPN Do not Change Next-Hop

BGP cambia el atributo de salto siguiente de la información de alcance de la capa de red (NLRI) anunciada del vecino EBGP de forma predeterminada. El punto final del túnel de hoja/VXLAN (VTEP) utiliza su dirección de origen NVE como atributo de salto siguiente de las rutas EVPN, y esta dirección se utiliza para determinar el destino del túnel VXLAN (interfaz virtual de red/par NVE). Si los nodos de columna cambian el salto siguiente, el túnel VXLAN no se puede establecer correctamente.

Para resolver este problema, se aplican estas instrucciones.

- En todos los nodos de columna, debe configurar route-map con action next-hop sin cambios

Filtro EVPN Disable RT de BGP superpuesto

Las rutas EVPN de los dispositivos de hoja se anuncian con la comunidad de destino de ruta (RT). Los routers sin la configuración RT correspondiente descartan las rutas con la comunidad RT de forma predeterminada. Mientras que todos los dispositivos de columna no tienen ningún Virtual Routing and Forwarding (VRF) configurado. Esto significa que los dispositivos de columna descartan todas las rutas EVPN anunciadas desde los dispositivos de hoja de forma predeterminada.

Para resolver este problema, en todos los nodos Spine, el filtro route-target predeterminado debe estar inhabilitado.

Configurar

Diagrama de la red

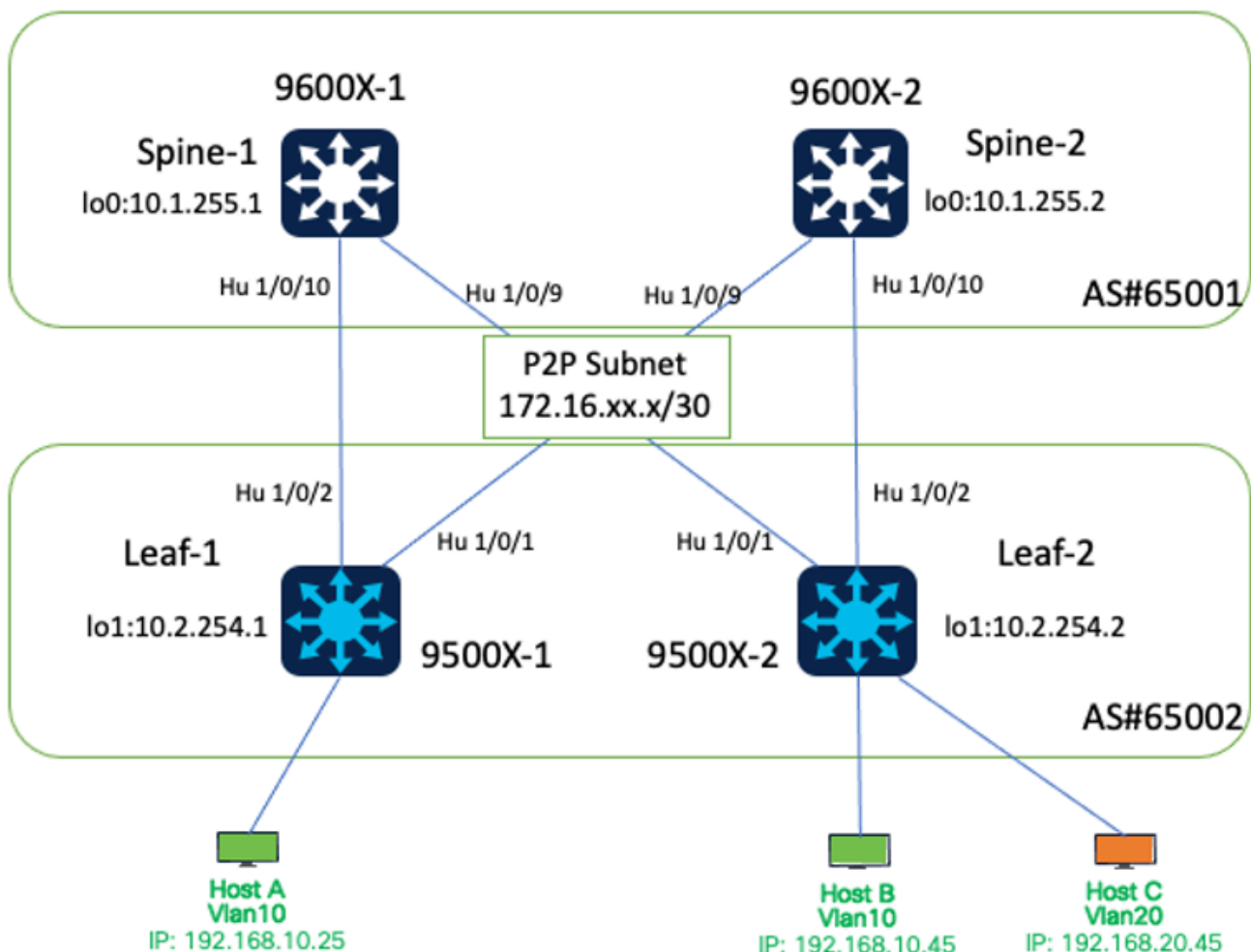


Diagrama de la red

Los detalles de la interfaz para este entorno de laboratorio son los siguientes.

Nombre del dispositivo	Versión del software	Interfaz#	IP Address
Columna-1	IOS-XE 17.12.1	Hu 1/0/9	172.16.12.1/30
		Hu 1/0/10	172.16.11.1/30
		Lo 0	10.1.255.1/32
Columna-2	IOS-XE 17.12.1	Hu 1/0/9	172.16.21.1/30
		Hu 1/0/10	172.16.22.1/30
		Lo 0	10.1.255.2/32
Hoja-1	IOS-XE 17.12.1	Hu 1/0/1	172.16.21.2/30
		Hu 1/0/2	172.16.11.2/30
		Lo 1	10.2.254.1/32
Hoja-2	IOS-XE 17.12.1	Hu 1/0/1	172.16.12.2/30
		Hu 1/0/2	172.16.22.2/30
		Lo 1	10.2.254.2/32



Nota: La asignación de la dirección IP en este laboratorio se realiza sólo con fines de prueba. La máscara de subred (es decir, /30, /31) para las conexiones punto a punto se podría considerar en función de los requisitos de diseño reales.

Configuraciones

Routing IPv4 BGP subyacente

En este ejemplo, las interfaces físicas se utilizan para establecer conexiones BGP.

- Configuración del routing BGP IPv4
- Configuración de BGP IPv4 Allowed AS In
- Configuración de rutas máximas BGP

Configuración del routing BGP IPv4

Configuración en columna:

```
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
```

Configuración en la hoja 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
```

Configuración en la hoja 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
```

Configuración de BGP IPv4 Allowed AS In

Configuración en columna:

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

Configuración en la hoja 1:

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

Configuración en la hoja 2:

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

Configuración de rutas máximas BGP Configuración en columna:

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

Configuración en hoja:

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

Multidifusión subyacente

Para permitir que la replicación de multidifusión (MR) gestione el tráfico de difusión, unidifusión desconocida y multidifusión local de enlaces (BUM), es necesario el routing multidifusión en todos los dispositivos de columna y hoja. Todas las interfaces de conexión de columna y hoja y los loopbacks relacionados deben tener habilitado PIM.

Ejemplo de multidifusión subyacente en columna 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 superpuesto

- Configuración de BGP L2VPN EVPN
- Configuración de BGP EVPN Allowed AS In
- Configuración de BGP EVPN Do not Change Next-Hop
- Configuración del Filtro RT de Desactivación de BGP EVPN

Configuración de BGP L2VPN EVPN

Configuración en columna:

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

Configuración en la hoja 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
```

Configuración en la hoja 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
```

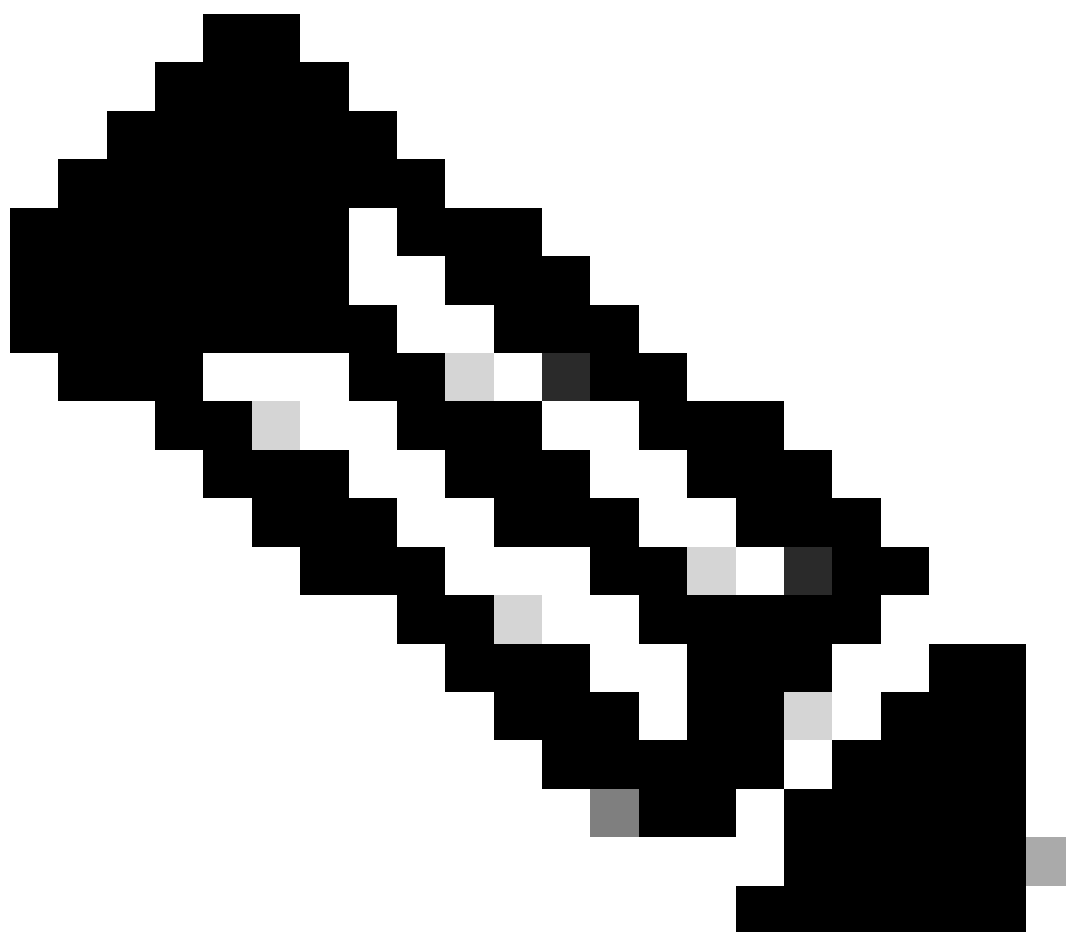
Configuración de BGP EVPN Allowed AS In

Configuración en la hoja 1:

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

Configuración en la hoja 2:

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



Nota: cuando se utiliza Single-Fabric con DGW, es poco probable que se requiera routing de una columna a otra. Sin embargo, teniendo en cuenta los cambios de topología, como la supercolumna, también se recomienda desactivar la comprobación de AS en los dispositivos de columna.

Configure BGP EVPN do not Change Next-Hop

Configuración en columna:

```
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
```

Configuración del Filtro RT de Desactivación de BGP EVPN

Configuración en columna:

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

Configuración de VRF en Hoja

```
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

Habilitar L2VPN EVPN y replicación multidifusión en hoja:

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

Crear instancias de EVPN (EVI) en hoja:

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

Cree VLAN y VNI para el tráfico de usuarios en la hoja:

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

Crear interfaz NVE y coser VNI a mcast grupos en hoja.

```
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

Cree una VLAN para L3VNI en hoja. No se requiere EVI para L3VNI.

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

Configuración de SVI para L2VNI en hoja.

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

Configuración de SVI para L3VNI en hoja. "no autostate" se configura para activar la SVI cuando no se asigna ninguna interfaz activa a esa VLAN.

```
interface Vlan3000
```

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

En Hoja, cose L3VNI al VRF bajo la configuración NVE.

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

Verificación

Verificar que las Sesiones BGP estén Establecidas

```
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: SJCx

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

Verificar 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_RT	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

Verificar 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_RT	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
```

Información Relacionada

- Guía de Configuración de BGP EVPN VXLAN, 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
- [Soporte técnico y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).