Implementierung und Überprüfung von BGP-only-VxLAN EVPN auf Catalyst 9000

Inhalt

- Einleitung
- Voraussetzungen
  - Anforderungen
  - Verwendete Komponenten
- Hintergrundinformationen
  - BGP-only-EVPN-Funktion
- Vergleich und Überlegungen zu BGP-only-EVPNs
  - EBGP-Vergleiche
  - Überlegungen zum BGP-IPv4-Routing
    - Underlay-BGP-IPv4 zugelassen AS IN
    - Unterlagern der maximalen BGP-IPv4-Pfade
  - Überlegungen zum Overlay-BGP-EVPN-Routing
    - Overlay-BGP-EVPN zulässig AS IN
    - Overlay-BGP-EVPNNext-Hop nicht ändern
    - Overlay-BGP-EVPNDisable-RT-Filter
- Konfigurieren
  - Netzwerkdiagramm
  - Konfigurationen
  - BGP-IPv4-Routing zugrunde liegen
    - BGP-IPv4-Routing konfigurieren
    - Konfigurieren von BGP IPv4 Zulässige AS in
    - Konfigurieren der maximalen BGP-Pfade
  - Underlay-Multicast
  - Overlay-BGP
    - Konfigurieren von BGP L2VPN EVPN
    - Konfigurieren des zulässigen BGP-EVPNs für AS in
    - Konfigurieren von BGP EVPN Ändern von Next-Hop nicht
    - Konfigurieren des RT-Filters "BGP EVPN Disable"
  - VRF-Konfiguration auf Leaf
  - EVPN L2
  - EVPN L3
- Überprüfung
- Zugehörige Informationen

Einleitung

Dieses Dokument beschreibt die Implementierung und Überprüfung von Virtual Extensible LAN (VXLAN) Ethernet VPN (EVPN) nur bei Cisco Catalyst Switches der Serie 9000 mit Border

Gateway Protocol (BGP).

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- BGP-EVPN
- VXLAN-Overlay
- Software-Konfigurationsleitfaden, Cisco IOS XE

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Catalyst 9600X
- Catalyst 9500X
- Cisco IOS XE 17.12 und höher

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Die Entwicklung eines Campus-Netzwerks der nächsten Generation erfordert die Einführung moderner Technologien und Architekturen, um die wachsenden Anforderungen von Benutzern, Anwendungen und Geräten zu erfüllen. VXLAN mit BGP-EVPN-Lösung bietet eine Fabric-basierte Architektur für Einfachheit, Skalierbarkeit und einfaches Management. In diesem Dokument wird die BGP-EVPN-Lösung für Benutzer beschrieben, die BGP sowohl für das IPv4- als auch für das EVPN-Routing aus irgendeinem Grund verwenden möchten.

BGP-only-EVPN-Funktion

VXLAN mit BGP-EVPN nutzt eine Spine-Leaf-Architektur anstelle des traditionellen 3-Tier-Netzwerkmodells. Bei einer Spine-Leaf-Architektur fungiert das Spine als Hochgeschwindigkeitskanal zwischen den Access Switches. Das Spine-Modell ermöglicht ein Scale-Out-Modell, bei dem die Bandbreite zwischen den Blättern durch Hinzufügen zusätzlicher Spines oder die Endpunktkapazität durch Hinzufügen weiterer Blätter erhöht werden kann.

Wenn Benutzer BGP sowohl für IPv4- als auch für EVPN-Routing-Informationen verwenden möchten, berücksichtigen Sie dabei Folgendes:

- Vereinfachte Konfiguration: Eine einzige BGP-Sitzung optimiert die Konfiguration und

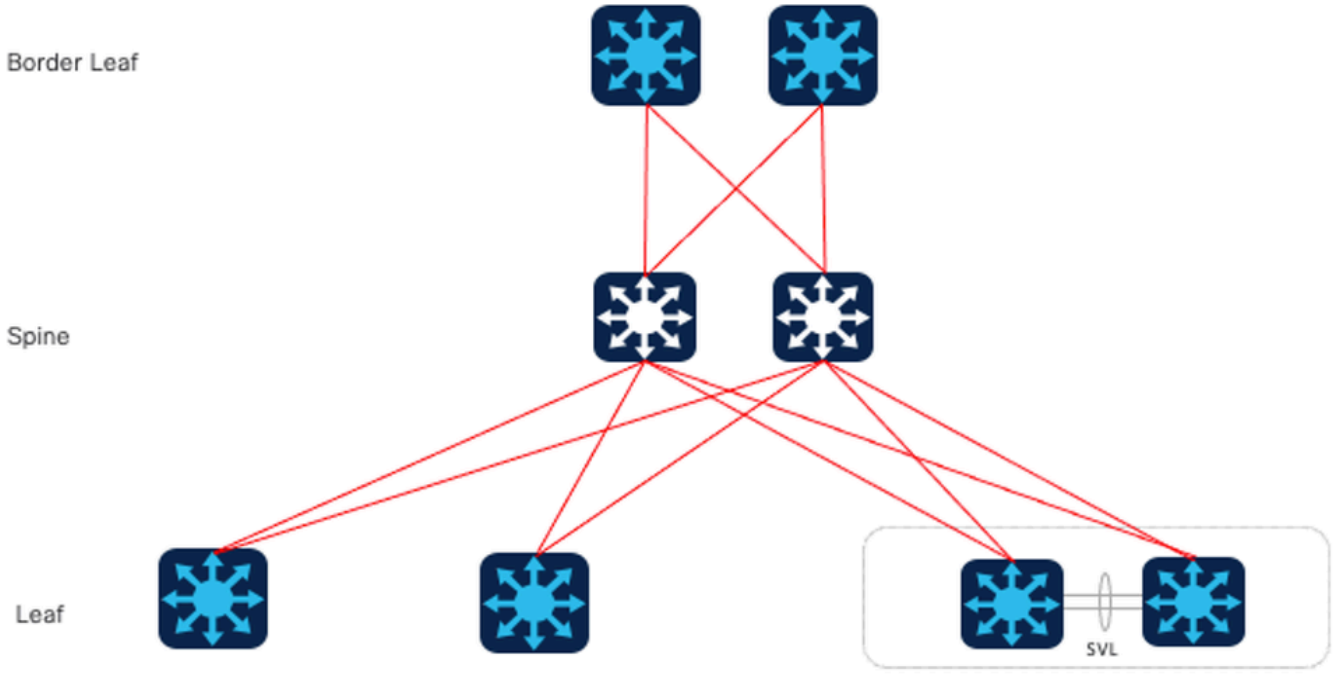
Verwaltung von Routing-Informationen. Es müssen keine separaten Routing-Protokolle für IPv4 und EVPN bereitgestellt und gepflegt werden, wodurch die Komplexität verringert wird.

- Einheitliche Kontrollebene: Durch die Verwendung von BGP als alleinigem Routing-Protokoll entsteht eine einheitliche Kontrollebene für IPv4- und EVPN-Routen. Dies vereinfacht die effiziente Routenpropagierung, Konvergenz und Routenankündigung im gesamten Rechenzentrumsnetzwerk.

- Skalierbarkeit: BGP eignet sich hervorragend für die Verarbeitung großer Netzwerke und bietet eine robuste Skalierbarkeit. Durch die Verwendung einer einzelnen BGP-Sitzung für IPv4- und EVPN-Routing-Informationen wird eine effiziente Skalierung bei wachsendem Netzwerk gewährleistet, ohne dass mehrere Routing-Protokoll-Instanzen erforderlich sind. Gleichzeitig ist die BGP-Konvergenzzeit bei umfangreichen Fabrics kürzer.

- Interoperabilität: BGP ist ein weit verbreitetes Routing-Protokoll nach Branchenstandard. Durch die Verwendung von BGP wird die Interoperabilität mit verschiedenen Netzwerkgeräten und -anbietern vereinfacht, sodass die Kompatibilität und nahtlose Integration in die Rechenzentrumsumgebung gewährleistet ist.

Diese Topologie zeigt ein gemeinsames Design für ein einzelnes C9K-EVPN-Fabric.



C9K EVPN Single Fabric-Design

Vergleich und Überlegungen zu BGP-only-EVPNs

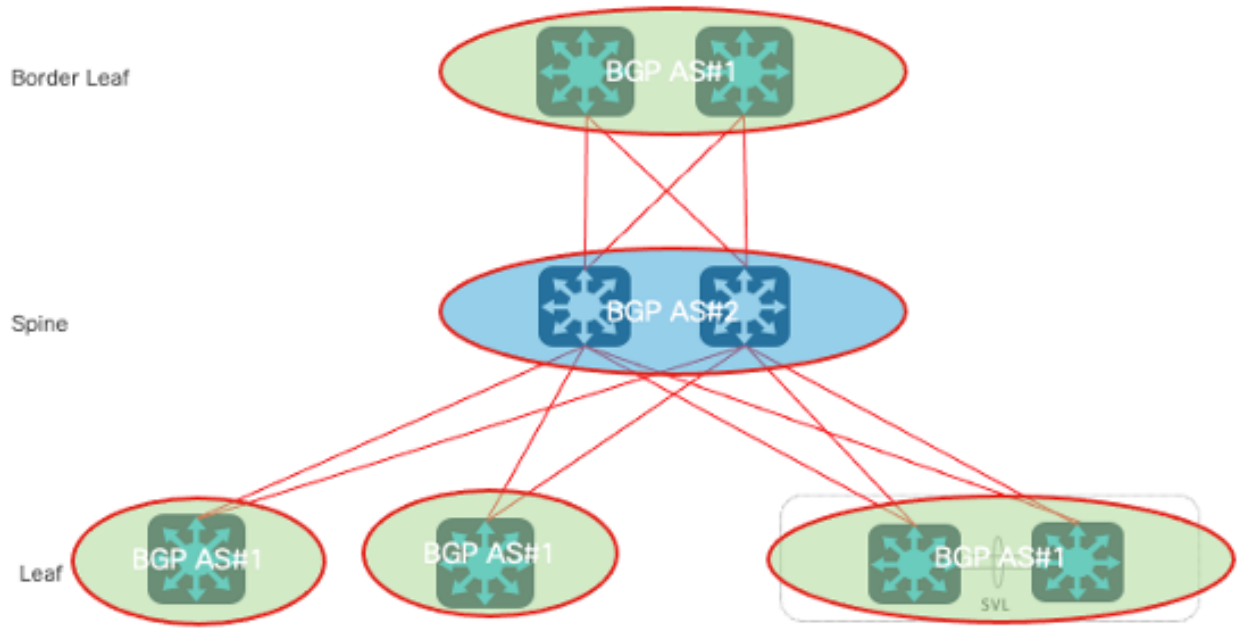
EBGP-Vergleiche

Bei einem reinen BGP-Design muss als Erstes geprüft werden, ob ein internes BGP (IBGP) oder ein externes BGP (EBGP) verwendet werden soll. Der Fall der Verwendung von IBGP, das im VxLAN-EVPN des traditionellen Rechenzentrums üblich ist. Im Vergleich zur Verwendung von IBGP als Underlay muss Spine bei der Verwendung von EBGP nicht mehr als Routen-Reflektor

konfiguriert werden, sondern fungiert als herkömmlicher Router-Server für den Austausch von Routen. Voraussetzung für dieses Dokument ist also die Verwendung von EBGP.

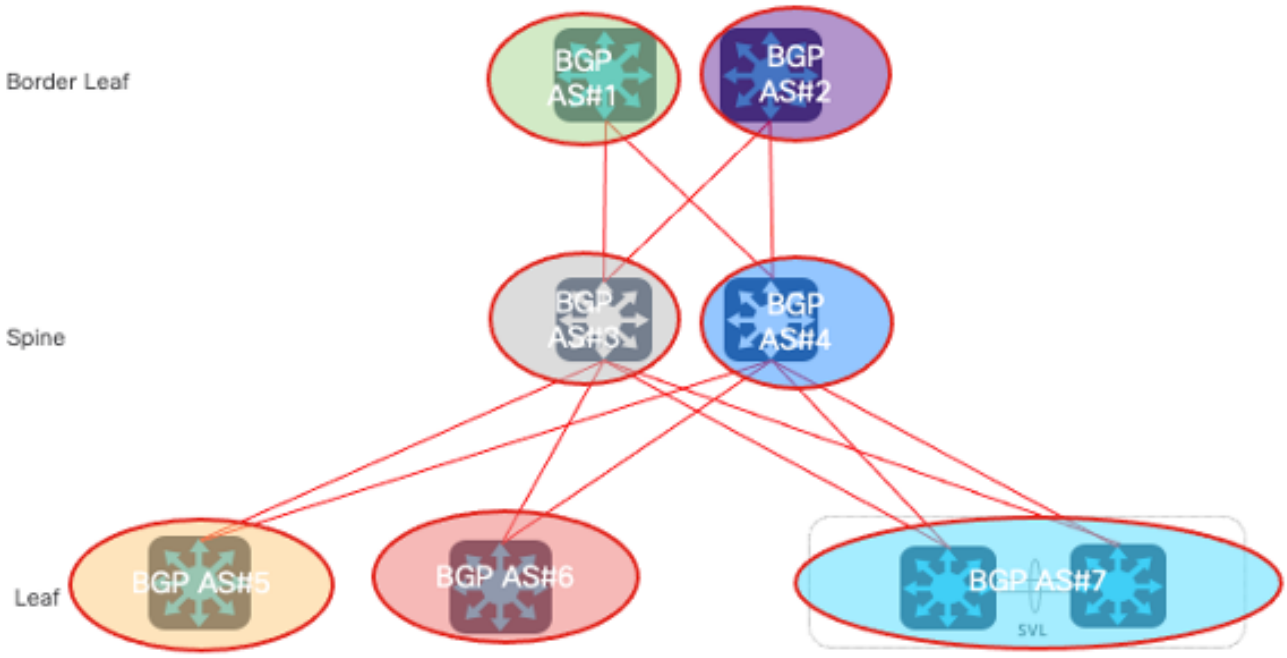
Option 1.Two-AS: Spine verwendet ein AS, Leaf und Border Leaf verwenden ein anderes AS.

Modell mit zwei AS



Modell mit zwei AS

Option 2: Multi-AS: Spine, Leaf und Border Leaf verwenden jeweils ein AS.



Multi-AS-Modell

Beim Vergleich der beiden Designs besteht ein häufiges Problem in der Skalierbarkeit, da für Option 2 jedes Mal, wenn ein Spine oder Leaf hinzugefügt wird, eine neue AS-Nummer

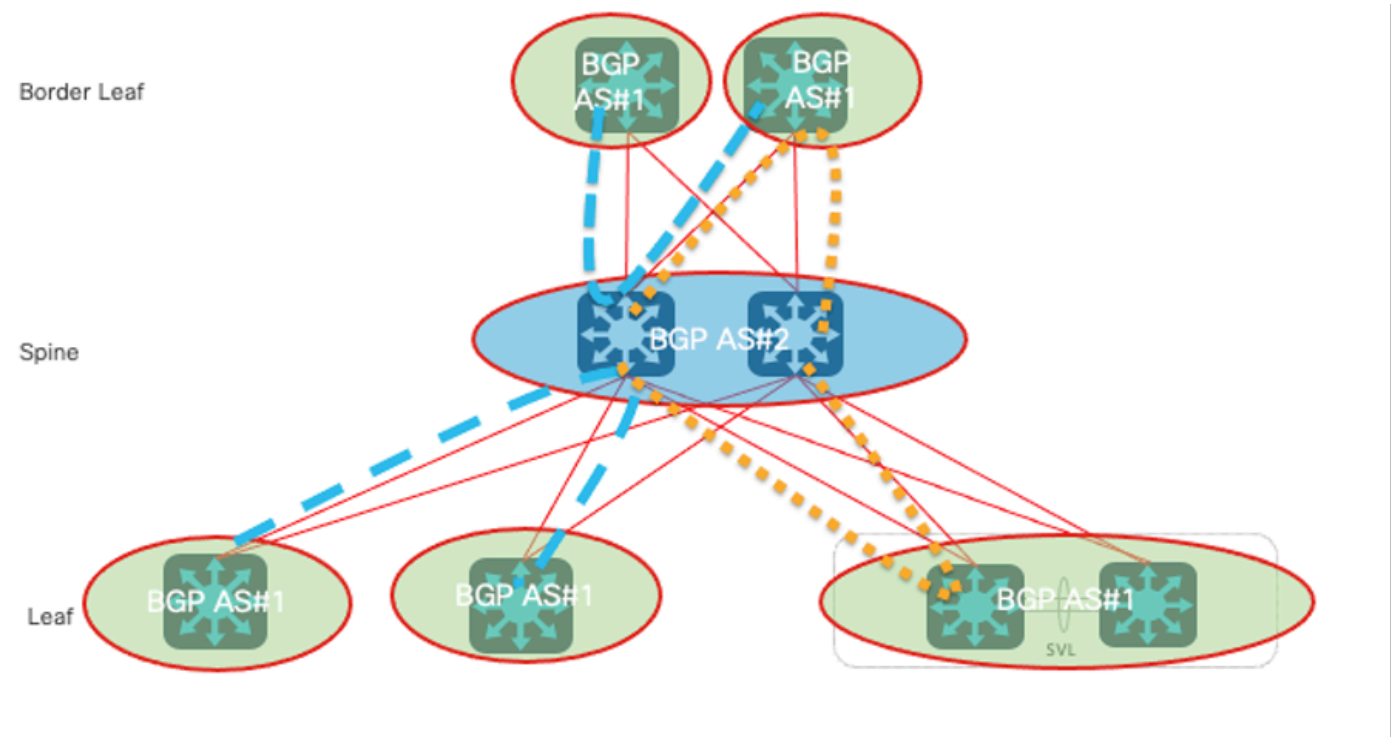
hinzugefügt werden muss, was zu komplexeren Konfigurationsänderungen in der Zukunft führt. Dies ist jedoch nicht der Fall. Sie ist erweiterungs- und wartungsfreundlich. Daher wird in diesem Dokument Option 1. zur Diskussion verwendet.

Im Vergleich zur Verwendung von IBGP als Underlay muss Spine bei der Verwendung von EBGP nicht mehr als Routen-Reflektor konfiguriert werden, sondern fungiert als herkömmlicher Router-Server für den Austausch von Routen.

Überlegungen zum BGP-IPv4-Routing

Dies sind wichtige Punkte, die in der Unterlagsebene berücksichtigt werden müssen.

Underlay-BGP-IPv4 zugelassen AS IN



Underlay-BGP-IPv4 zugelassen AS IN

Die AS-Schleifenerkennung erfolgt durch Scannen des vollständigen AS-Pfads (wie im AS_PATH-Attribut angegeben) und durch Überprüfen, dass die autonome Systemnummer des lokalen Systems nicht im AS-Pfad erscheint.

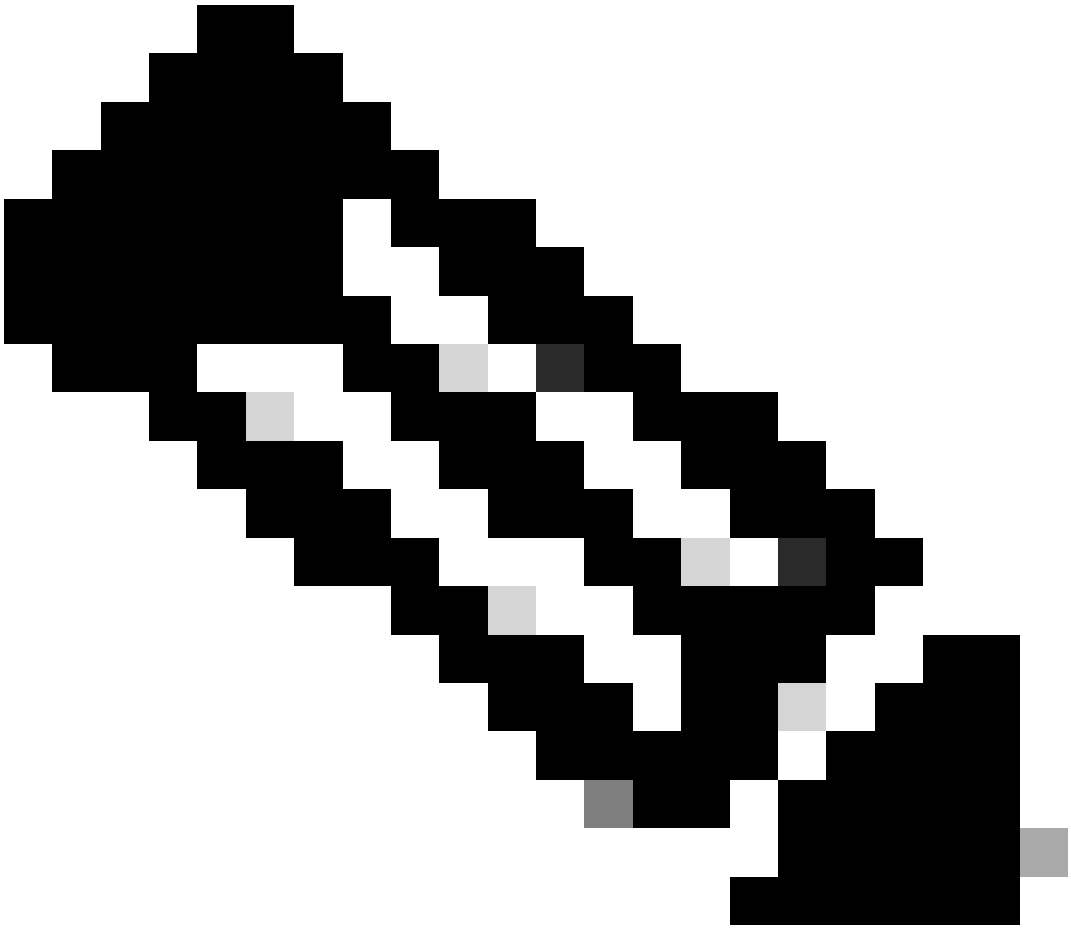
Gemäß obigem Diagramm wird die BGP AS-Schleife gebildet - in diesem Szenario dieselbe AS-Nummer im AS-Pfad:

- Auf Leaf- und Border-Leaf-Geräten lautet der as-path {#1, #2, #1}.
- Auf Spine-Geräten lautet der As-Pfad {#2, #1, #2}.

Um dieses Problem zu beheben, wird "allow-as-in" in der BGP-IPv4-Adressfamilie konfiguriert, und zwar mit den folgenden Anweisungen:

- AS-In darf auf allen Leaf- und Border-Leaf-Geräten nur einmal angezeigt werden (Leaf >

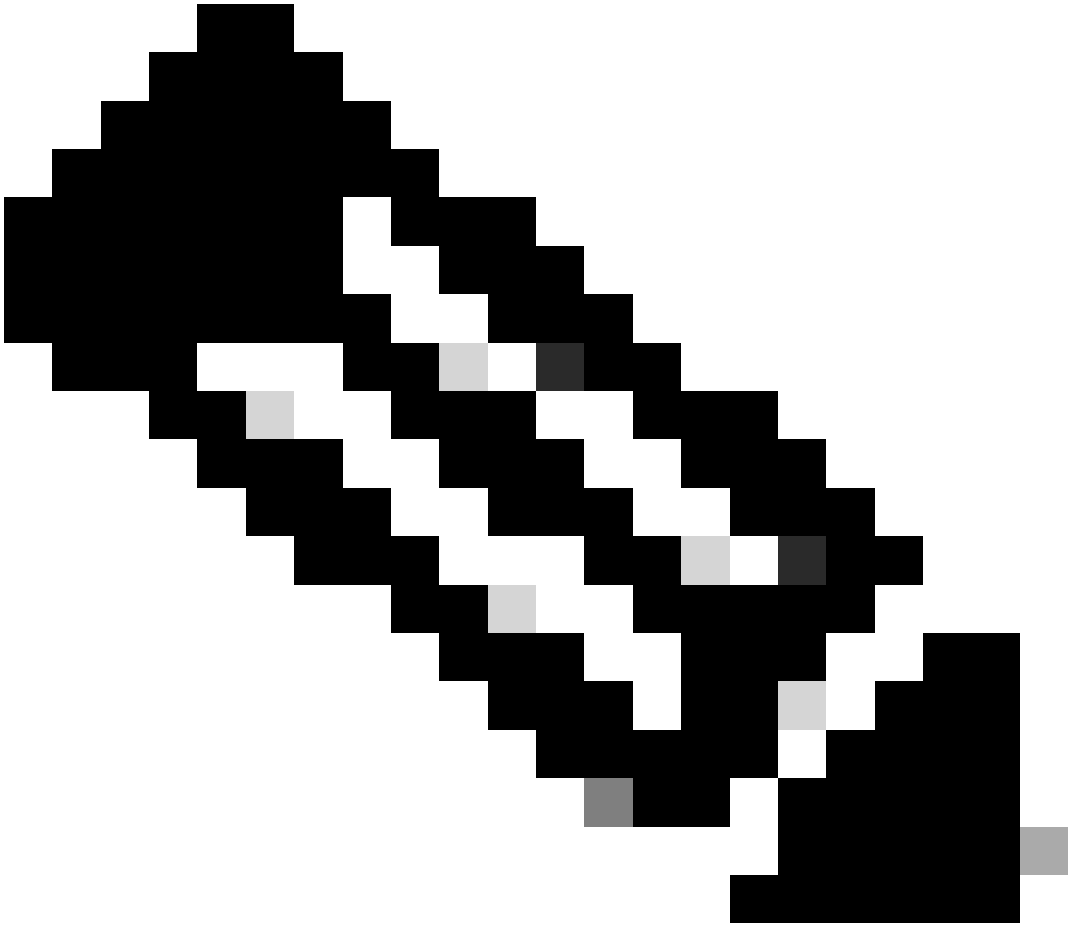
Spine > Leaf), da alle Leaf-Switches im selben AS ausgeführt werden.
- AS In darf nur einmal auf allen Spine-Geräten (Spine > BL > Spine) oder (Spine > Leaf > Spine) angezeigt werden, da alle Spine-Geräte im selben AS ausgeführt werden.



Hinweis: Wenn Single-Fabric mit der DGW verwendet wird, ist es unwahrscheinlich, dass Routing von einem Spine zu einem anderen erforderlich ist. In Anbetracht von Topologieänderungen, z. B. Super-Spine, wird jedoch empfohlen, die AS-Prüfung auch für Spine-Geräte zu deaktivieren.

Unterlagern der maximalen BGP-IPv4-Pfade

BGP wählt eine Route anhand seiner Kriterien aus, und es ist unwahrscheinlich, dass standardmäßig 2 ECMP-Routen in der BGP-Tabelle aufgeführt werden. Um ECMP für die Bandbreitenoptimierung zu erreichen, müssen die maximalen Pfade X in der BGP-IPv4-Adressfamilie auf allen BGP-Geräten konfiguriert werden. In der Zwischenzeit empfehlen wir, die gleiche Verbindungsbandbreite zwischen Spine und Leaf beizubehalten.

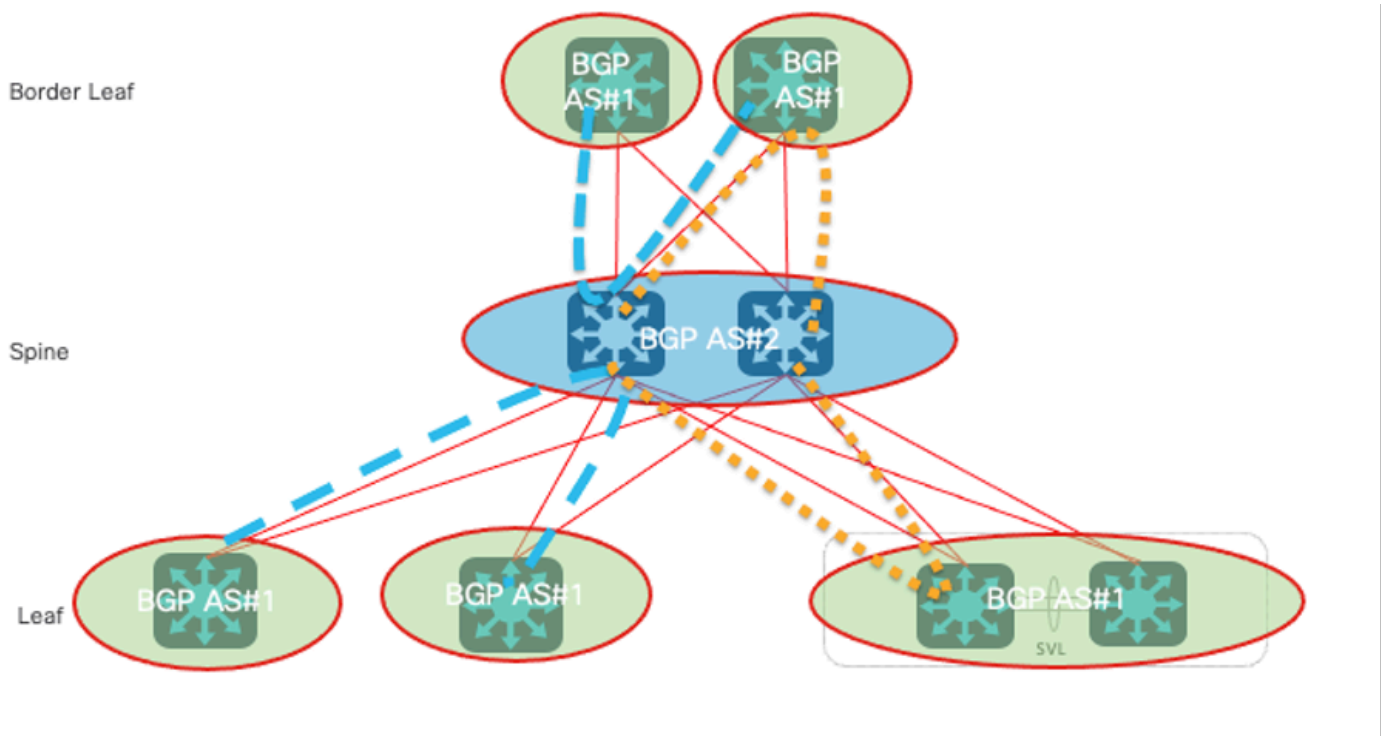


Hinweis: Die maximalen Pfade hängen vom Design der Topologie ab. Mit zwei Spine-Switches können Sie "maximum-paths 2" konfigurieren.

Überlegungen zum Overlay-BGP-EVPN-Routing

Diese Schlüsselpunkte müssen in der Overlay-Ebene berücksichtigt werden.

Overlay-BGP-EVPN zulässig AS IN



Overlay-BGP-IPv4 zugelassen AS IN

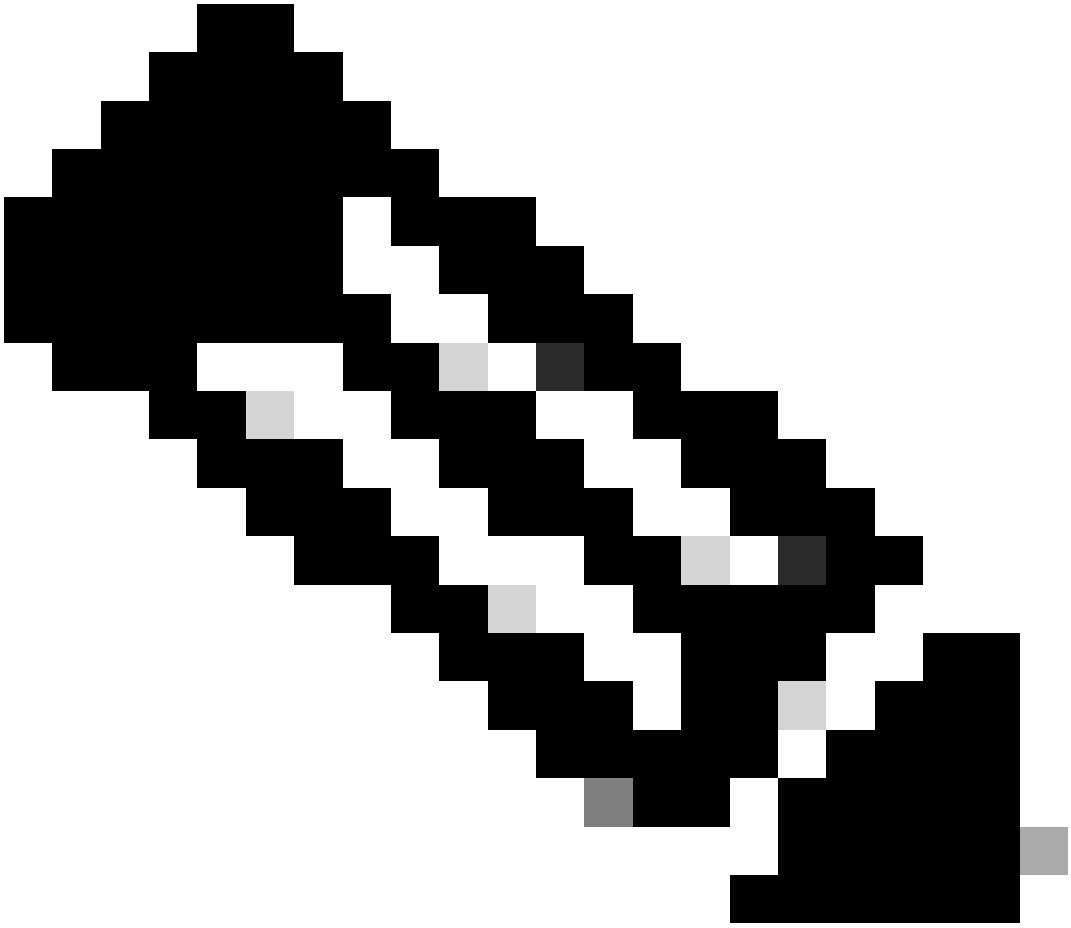
Die AS-Schleifenerkennung erfolgt durch Scannen des vollständigen AS-Pfads (wie im AS_PATH-Attribut angegeben) und durch Überprüfen, dass die autonome Systemnummer des lokalen Systems nicht im AS-Pfad erscheint.

Dem Bild zufolge wird die BGP AS-Schleife gebildet - in diesem Szenario die gleiche AS-Nummer im AS-Pfad:

- Auf Leaf- und Border-Leaf-Geräten lautet der as-path {#1, #2, #1}
- Auf Spine-Geräten lautet der as-Pfad {#2, #1, #2}.

Um dieses Problem zu beheben, muss allow-as-in in der BGP IPv4-Adressfamilie konfiguriert werden, und zwar mit den folgenden Anweisungen:

- AS-In darf auf allen Leaf- und Border-Leaf-Geräten nur einmal angezeigt werden (Leaf > Spine > Leaf), da alle Leaf-Switches im selben AS ausgeführt werden.
- AS In darf nur einmal auf allen Spine-Geräten (Spine > BL > Spine) oder (Spine > Leaf > Spine) angezeigt werden, da alle Spine-Geräte im selben AS ausgeführt werden.



Hinweis: Wenn Single-Fabric mit der DGW verwendet wird, ist es unwahrscheinlich, dass Routing von einem Spine zu einem anderen erforderlich ist. In Anbetracht von Topologieänderungen, z. B. Super-Spine, wird jedoch empfohlen, die AS-Prüfung auch für Spine-Geräte zu deaktivieren.

Overlay BGP EVPN Ändern des Next-Hop nicht

Das BGP ändert das Next-Hop-Attribut der NLRI (Network Layer Reachability Information), das standardmäßig vom EBGP-Nachbarn angekündigt wird. Der Endpunkt des Leaf/VXLAN-Tunnels (VTEP) verwendet seine NVE-Quelladresse als Next-Hop-Attribut der EVPN-Routen. Diese Adresse wird verwendet, um das Ziel des VXLAN-Tunnels (Virtual Interface/NVE Peer für das Netzwerk) zu bestimmen. Wenn Spine-Knoten den Next-Hop ändern, kann der VXLAN-Tunnel nicht richtig eingerichtet werden.

Um dieses Problem zu lösen, werden diese Anweisungen angewendet.

- Auf allen Spine-Knoten muss "route-map" mit der Aktion "next-hop" unverändert konfiguriert

werden.

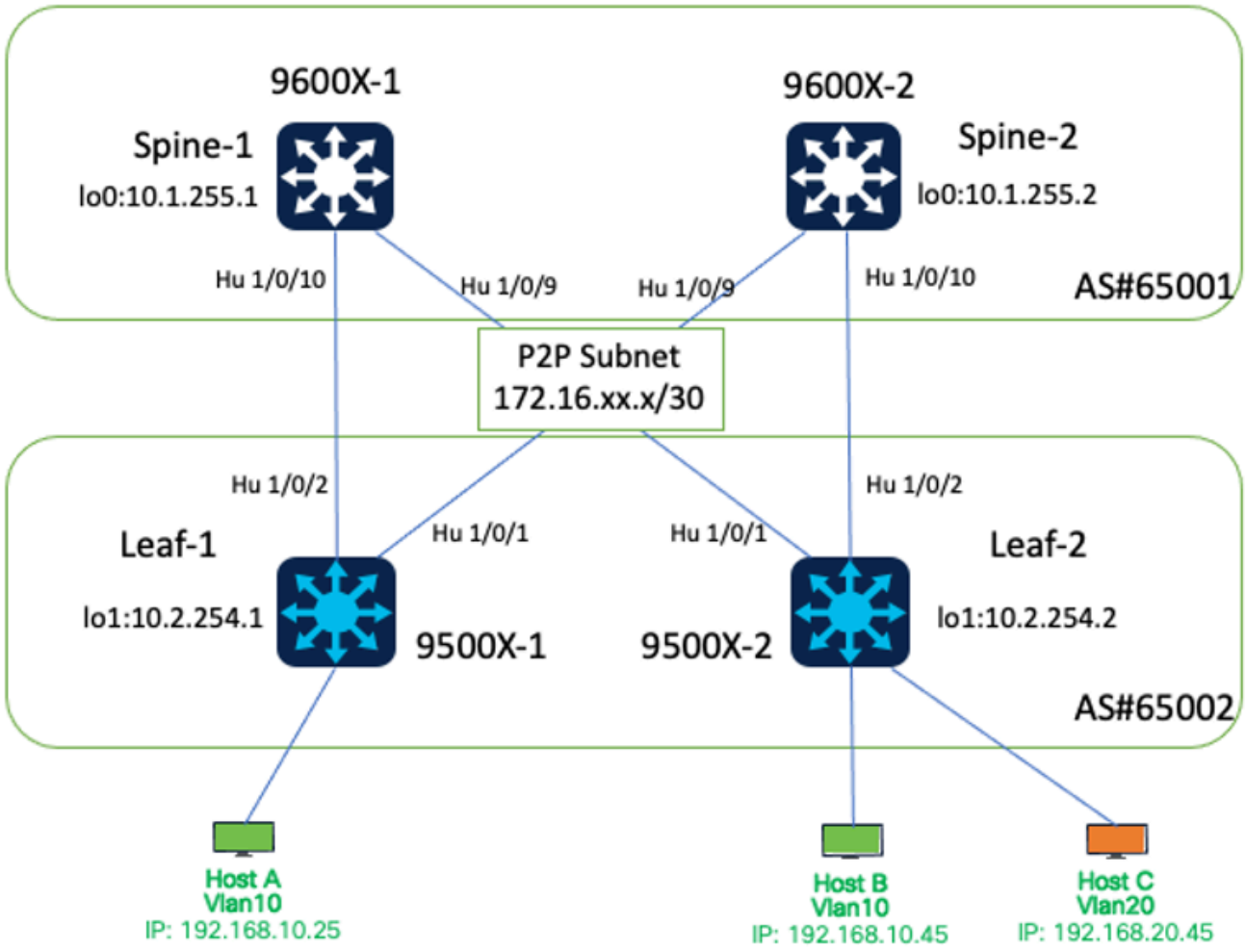
Overlay-BGP-EVPN RT-Filter deaktivieren

Die EVPN-Routen der Leaf-Geräte werden in der RT-Community (Route Target) angekündigt. Router ohne die entsprechende RT-Konfiguration verwerfen die Routen standardmäßig mit der RT-Community. Für alle Spine-Geräte ist dagegen kein Virtual Routing and Forwarding (VRF) konfiguriert. Das bedeutet, dass die Spine-Geräte standardmäßig alle von den Leaf-Geräten gemeldeten EVPN-Routen verwerfen.

Um dieses Problem zu lösen, muss auf allen Spine-Knoten der Standardfilter für route-target deaktiviert werden.

Konfigurieren

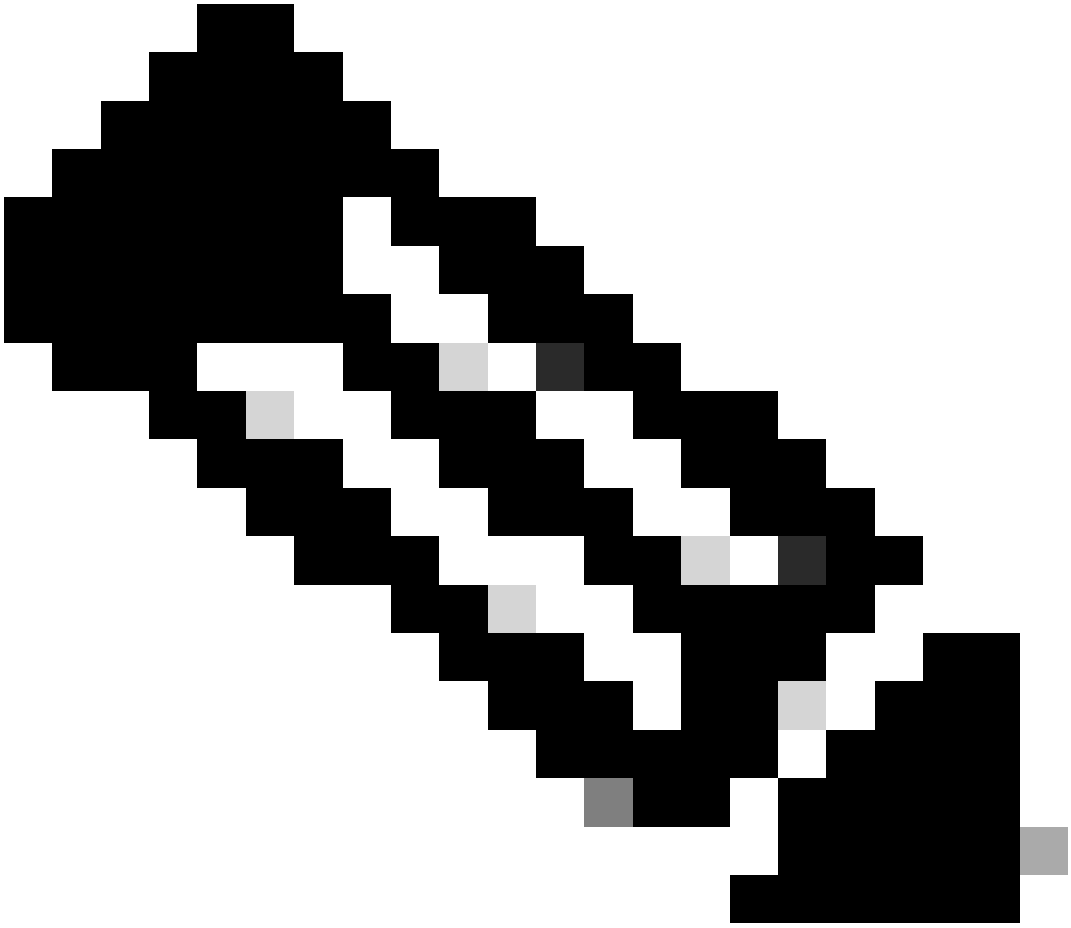
Netzwerkdiagramm



Netzwerkdiagramm

Die Schnittstellen für diese Übungsumgebung sind im Folgenden dargestellt.

Device Name (Gerätename)	Software-Version	Schnittstelle#	IP-Adresse
Spine-1	IOS-XE 17.12.1	Hu 0.0.9	172.16.12.1/30
		Hu 01.01.10	172.16.11.1/30
		Niedrig 0	10.1.255.1/32
Spine-2	IOS-XE 17.12.1	Hu 0.0.9	172.16.21.1/30
		Hu 01.01.10	172.16.22.1/30
		Niedrig 0	10.1.255.2/32
Blatt-1	IOS-XE 17.12.1	Hu 1/0/1	172.16.21.2/30
		Hu 0/1/2	172.16.11.2/30
		01	10.2.254.1/32
Blatt 2	IOS-XE 17.12.1	Hu 1/0/1	172.16.12.2/30
		Hu 0/1/2	172.16.22.2/30
		01	10.2.254.2/32



Hinweis: Die IP-Adresszuweisung in dieser Übung dient nur Testzwecken. Die Subnetzmaske (d. h. /30, /31) für Point-to-Point-Verbindungen kann entsprechend Ihren tatsächlichen Designanforderungen in Betracht gezogen werden.

Konfigurationen

BGP-IPv4-Routing zugrunde liegen

In diesem Beispiel werden die physischen Schnittstellen verwendet, um BGP-Verbindungen herzustellen.

- BGP-IPv4-Routing konfigurieren
- Konfigurieren von BGP IPv4 Zulässige AS in
- Konfigurieren der maximalen BGP-Pfade

BGP-IPv4-Routing konfigurieren

Konfiguration auf 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
```

Konfiguration auf 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
```

Konfiguration auf 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
```

Konfigurieren von BGP IPv4 Zulässige AS in

Konfiguration auf Spine:

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

Konfiguration auf Leaf-1:

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

Konfiguration auf Leaf-2:

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

Konfigurieren der maximalen BGP-Pfade
Konfiguration auf Spine:

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

Konfiguration auf Leaf:

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

Underlay-Multicast

Damit die Multicast-Replikation (MR) Broadcast-, Unknown Unicast- und Link-Local Multicast (BUM)-Datenverkehr verarbeiten kann, ist Multicast-Routing auf allen Spine- und Leaf-Geräten erforderlich. Für alle Spine- und Leaf-Verbindungsschnittstellen und zugehörigen Loopbacks muss PIM aktiviert sein.

Beispiel für Underlay-Multicast auf 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
```

Overlay-BGP

- Konfigurieren von BGP L2VPN EVPN
- Konfigurieren des zulässigen BGP-EVPNs für AS in
- Konfigurieren von BGP EVPN Ändern des Next-Hop nicht
- Konfigurieren des RT-Filters "BGP EVPN Disable"

Konfigurieren von BGP L2VPN EVPN

Konfiguration auf Spine:

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

Konfiguration auf 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
```

Konfiguration auf 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
```

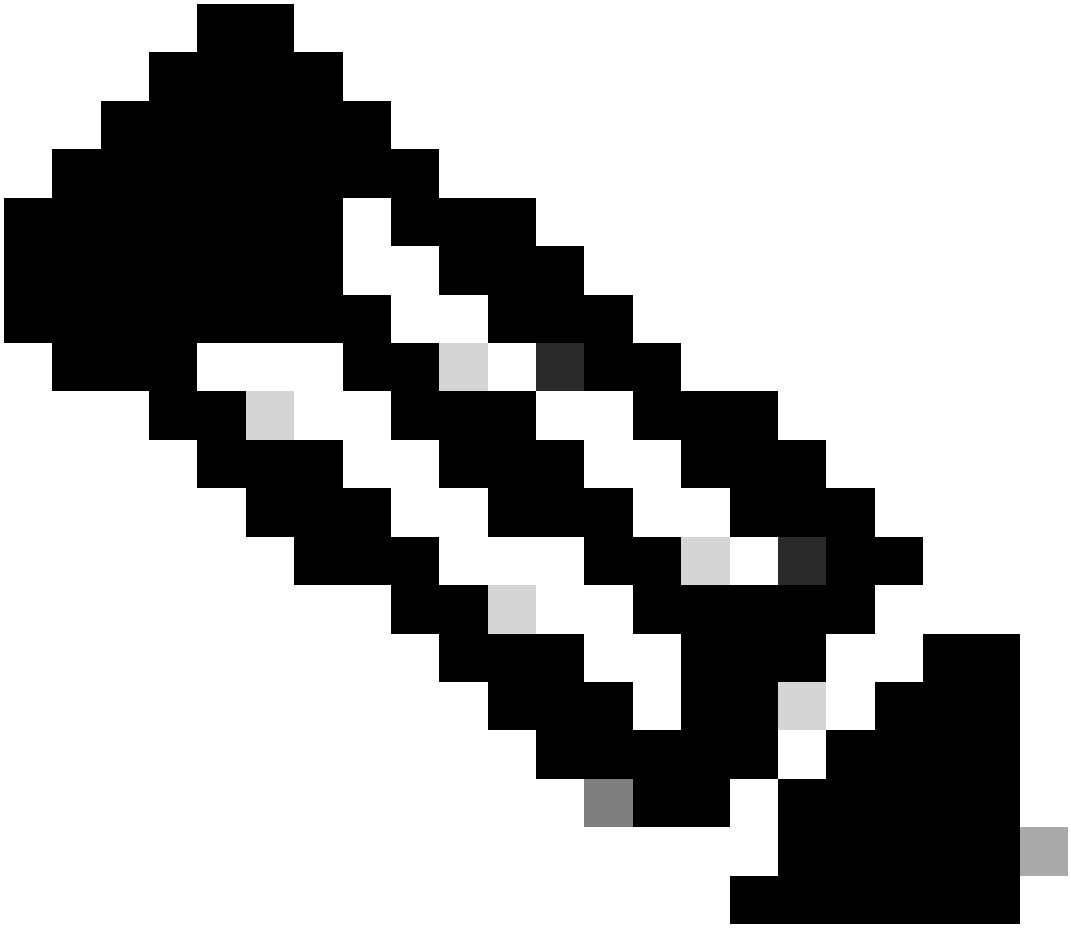
Konfigurieren des zulässigen BGP-EVPNs für AS in

Konfiguration auf 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
```

Konfiguration auf 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
```



Hinweis: Wenn Single-Fabric mit der DGW verwendet wird, ist es unwahrscheinlich, dass Routing von einem Spine zu einem anderen erforderlich ist. In Anbetracht von Topologieänderungen, z. B. Super-Spine, wird jedoch empfohlen, die AS-Prüfung auch für Spine-Geräte zu deaktivieren.

Konfigurieren von BGP EVPN ändern Next-Hop nicht

Konfiguration auf 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
```

Konfigurieren des RT-Filters "BGP EVPN Disable"

Konfiguration auf Spine:

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

VRF-Konfiguration auf 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

Aktivieren Sie L2VPN EVPN und Multicast-Replikation auf Leaf:

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

Erstellen von EVPN-Instanzen (EVI) auf Leaf:

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

Erstellung von VLANs und VNI für Benutzerdatenverkehr auf Leaf:

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

Erstellen Sie eine NVE-Schnittstelle, und nähen Sie den VNI, um Gruppen auf dem Blatt zu vermischen.

```
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

VLAN für L3VNI auf Leaf erstellen. EVI ist für L3VNI nicht erforderlich.

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

Konfigurieren von SVI für L2VNI auf Leaf

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

Konfigurieren von SVI für L3VNI auf Leaf "no autostate" (kein automatischer Status) wird konfiguriert, um die SVI hochzufahren, wenn diesem VLAN keine aktive Schnittstelle zugewiesen ist.

```
interface Vlan3000
vrf forwarding S1-EVPN
ip unnumbered Loopback1
no autostate
```

Auf dem Blatt wird L3VNI unter NVE-Konfiguration in die VRF-Instanz geheftet.

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

Überprüfung

Überprüfung der Einrichtung von BGP-Sitzungen

```
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
```

Überprüfung von 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
```

Überprüfung von 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
```

Zugehörige Informationen

- BGP EVPN VXLAN-Konfigurationsleitfaden, 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
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.