Configuring VXLAN BGP EVPN

This chapter contains the following sections:

- Information About VXLAN BGP EVPN, on page 1
- Configuring VXLAN BGP EVPN, on page 12
- Verifying the VXLAN BGP EVPN Configuration, on page 25
- Example of VXLAN BGP EVPN (EBGP), on page 26
- Example of VXLAN BGP EVPN (IBGP), on page 35
- Example Show Commands, on page 43

Information About VXLAN BGP EVPN

Guidelines and Limitations for VXLAN BGP EVPN

VXLAN BGP EVPN has the following guidelines and limitations:

- The following guidelines and limitations apply to VXLAN/VTEP:
  - SPAN source or destination is supported on any port.

  For more information, see the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 7.x.

- When SVI is enabled on a VTEP (flood and learn, or EVPN) regardless of ARP suppression, make sure that ARP-ETHER TCAM is carved using the `hardware access-list tcam region arp-ether 256 double-wide` command. This is not applicable to the Cisco Nexus 9200 and 9300-EX platform switches and Cisco Nexus 9500 platform switches with 9700-EX line cards.

- Beginning with Cisco NX-OS Release 7.0(3)F3(3), VXLAN Layer 2 Gateway is supported only on the 9636C-RX line card. VXLAN and MPLS cannot be enabled on the Cisco Nexus 9508 switch at the same time.

- Beginning with Cisco NX-OS Release 7.0(3)F3(3), if VXLAN is enabled, the Layer 2 Gateway cannot be enabled when there is any line card other than the 9636C-RX.

- Beginning with Cisco NX-OS Release 7.0(3)I6(1), you can configure EVPN over segment routing or MPLS. See the Cisco Nexus 9000 Series NX-OS Label Switching Configuration Guide, Release 7.x for more information.
• Beginning with Cisco NX-OS Release 7.0(3)I6(1), you can use MPLS tunnel encapsulation using the new CLI encapsulation mpls command. You can configure the label allocation mode for the EVPN address family. See the Cisco Nexus 9000 Series NX-OS Label Switching Configuration Guide, Release 7.x for more information.

• In VXLAN EVPN setup that has 2K VNI scale configuration, the control plane down time takes more than 200 seconds. To avoid BGP flap, configure the graceful restart time to 300 seconds.

• SVI and subinterfaces as uplinks are not supported.

• In a VXLAN EVPN setup, border leaves must use unique route distinguishers, preferably using auto rd command. It is not supported to have same route distinguishers in different border leaves.

• ARP suppression is only supported for a VNI if the VTEP hosts the First-Hop Gateway (Distributed Anycast Gateway) for this VNI. The VTEP and the SVI for this VLAN have to be properly configured for the distributed Anycast Gateway operation, for example, global Anycast Gateway MAC address configured and Anycast Gateway feature with the virtual IP address on the SVI.

• The show commands with the internal keyword are not supported.

• DHCP snooping (Dynamic Host Configuration Protocol snooping) is not supported on VXLAN VLANs.

• RACLs are not supported on Layer 3 uplinks for VXLAN traffic. Egress VACLs support is not available for de-capsulated packets in the network to access direction on the inner payload.

As a best practice, use PACLs/VACLs for the access to the network direction.

See the Cisco Nexus 9000 Series NX-OS Security Configuration Guide for other guidelines and limitations for the VXLAN ACL feature.

• QoS classification is not supported for VXLAN traffic in the network to access direction on the Layer 3 uplink interface.

See the Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide for other guidelines and limitations for the VXLAN QoS feature.

• The QoS buffer-boost feature is not applicable for VXLAN traffic.

• VTEP does not support Layer 3 subinterface uplinks that carry VXLAN encapsulated traffic.

• Layer 3 interface uplinks that carry VXLAN encapsulated traffic do not support subinterfaces for non-VXLAN encapsulated traffic.

• For Cisco NX-OS 7.0(3)I2(1) and later, a FEX HIF (FEX host interface port) is supported for a VLAN that is extended with VXLAN.

• For eBGP, it is recommended to use a single overlay eBGP EVPN session between loopbacks.

• EBGP peering from a VXLAN host to local VTEP is supported with loopback in tenant VRF as BGP update-source.

• Bind NVE to a loopback address that is separate from other loopback addresses that are required by Layer 3 protocols. A best practice is to use a dedicated loopback address for VXLAN.

• VXLAN BGP EVPN does not support an NVE interface in a non-default VRF.

• It is recommended to configure a single BGP session over the loopback for an overlay BGP session.

• When configuring VXLAN BGP EVPN, only the "System Routing Mode: Default" is applicable for the following hardware platforms:
- Cisco Nexus 9200, 9300-EX, and 9300-FX/FX2 platform switches
- Cisco Nexus 9300 platform switches
- Cisco Nexus 9500 platform switches with X9500 line cards
- Cisco Nexus 9500 platform switches with -EX and -FX line cards

- The “System Routing Mode: template-vxlan-scale” is not applicable to Cisco NX-OS Release 7.0(3)I5(2) and later.

- When using VXLAN BGP EVPN with Cisco NX-OS Release 7.0(3)I4(x) or 7.0(3)I5(1), the “System Routing Mode: template-vxlan-scale” is required on the following hardware platforms:
  - Cisco Nexus 9300-EX platform switches
  - Cisco Nexus 9500 platform switches with -EX line cards

- Changing the “System Routing Mode” requires a reload of the switch.

- For Cisco NX-OS Release 7.0(3)I2(1) and later, VXLAN is supported on Cisco Nexus 9500 platform switches with the following line cards:
  - 9500-R
  - 9564PX
  - 9564TX
  - 9536PQ
  - 9700-EX
  - 9700-FX

- When Cisco Nexus 9500 platform switches are used as VTEPs (7.0(3)I2(1) and later), 100G line cards are not supported on Cisco Nexus 9500 platform switches. This limitation does not apply to a Cisco Nexus 9500 platform switch with -EX or -FX line cards.

- Cisco Nexus 9300 platform switches with 100G uplinks only support VXLAN switching/bridging. (7.0(3)I2(1) and later)

Cisco Nexus 9200, 9300-EX, and 9300-FX platform switches do not have this restriction.

---

**Note**

For VXLAN routing support, a 40G uplink module is required.

- The VXLAN UDP port number is used for VXLAN encapsulation. For Cisco Nexus NX-OS, the UDP port number is 4789. It complies with IETF standards and is not configurable.

- For Cisco NX-OS Release 7.0(3)I1(2) and earlier, a static route with next-hop reachable over the VXLAN BGP EVPN route is not supported.

- For Cisco Nexus 9200 platform switches that have the Application Spine Engine (ASE2), there exists a Layer 3 VXLAN (SVI) throughput issue. There is a data loss for packets of sizes 99–122. (7.0(3)I3(1) and later).
• For the Cisco NX-OS 7.0(3)I2(3) release, the VXLAN network identifier (VNID) 16777215 is reserved and should not be configured explicitly.

• For Cisco NX-OS Release 7.0(3)I4(1) and later, VXLAN supports In-Service Software Upgrade (ISSU).

• VXLAN does not support co-existence with the GRE tunnel feature or the MPLS (static or segment-routing) feature on Cisco Nexus 9000 Series switches with a Network Forwarding Engine (NFE).

• The `vpc orphan-ports suspend` command must be enabled for orphan ports that are connected to Cisco Nexus 9000 vPC VTEPs.

• VTEP connected to FEX host interface ports is not supported (7.0(3)I2(1) and later).

• In Cisco NX-OS Release 7.0(3)I4(1), resilient hashing (port-channel load-balancing resiliency) and VXLAN configurations are not compatible with VTEPs using ALE uplink ports.

  **Note**  
  Resilient hashing is disabled by default.

  **Note**  
  For information about VXLAN BGP EVPN scalability, see the Verified Scalability Guide for your platform.

### Considerations for VXLAN BGP EVPN Deployment

• A loopback address is required when using the `source-interface config` command. The loopback address represents the local VTEP IP.

• During boot-up of a switch (7.0(3)I2(2) and later), you can use the `source-interface hold-down-time` command to suppress advertisement of the NVE loopback address until the overlay has converged. The range for the `hold-down-time` is 0 - 1000 seconds. The default is 180 seconds.

• To establish IP multicast routing in the core, IP multicast configuration, PIM configuration, and RP configuration is required.

• VTEP to VTEP unicast reachability can be configured through any IGP/BGP protocol.

• If the anycast gateway feature is enabled for a specific VNI, then the anyway gateway feature must be enabled on all VTEPs that have that VNI configured. Having the anycast gateway feature configured on only some of the VTEPs enabled for a specific VNI is not supported.

• It is a requirement when changing the primary or secondary IP address of the NVE source interfaces to shut the NVE interface before changing the IP address.

• As a best practice, the RP for the multicast group should be configured only on the spine layer. Use the anycast RP for RP load balancing and redundancy.

• Every tenant VRF needs a VRF overlay VLAN and SVI for VXLAN routing.

• For scale environments, the VLAN IDs related to the VRF and Layer-3 VNI (L3VNI) must be reserved with the `system vlan nve-overlay id` command.

This is required to optimize the VXLAN resource allocation to scale the following platforms:
• Cisco Nexus 9200 platform switches beginning with Cisco NX-OS Release 7.0(3)I1(2) through 7.0(3)I5(2)

• Cisco Nexus 9300-EX, 9300-FX, and 9300-FX2 platform switches beginning with Cisco NX-OS Release 7.0(3)I1(2) through 7.0(3)I5(2)

• Cisco Nexus 9300 platform switches beginning with Cisco NX-OS Release 7.0(3)I1(2)

Note Beginning with Cisco NX-OS Release 7.0(3)I5(2), the Cisco Nexus 9200, 9300-EX, and 9300-FX/FX2 platform switches do not require this command. Beginning with Cisco NX-OS Release 7.0(3)I5(2), it is strongly recommended to remove the command on Cisco Nexus 9200, 9300-EX, and 9300-FX/FX2 platform switches as it would disable Tenant Routed Multicast functionality on the VRF.

The following example shows how to reserve the VLAN IDs related to the VRF and the Layer-3 VNI:

```
system vlan nve-overlay id 2000
vlan 2000
   vn-segment 50000

interface Vlan2000
   vrf member MYVRF_50000
   ip forward
   ipv6 forward

vrf context MYVRF_50000
   vni 50000
```

Note The `system vlan nve-overlay id` command should be used for a VRF or a Layer-3 VNI (L3VNI) only. Do not use this command for regular VLANs or Layer-2 VNIs (L2VNI).

• When configuring ARP suppression with BGP-EVPN, use the `hardware access-list tcam region arp-ether size double-wide` command to accommodate ARP in this region. (You must decrease the size of an existing TCAM region before using this command.)

vPC Considerations for VXLAN BGP EVPN Deployment

• The loopback address used by NVE needs to be configured to have a primary IP address and a secondary IP address.

The secondary IP address is used for all VxLAN traffic that includes multicast and unicast encapsulated traffic.

• Each vPC peer needs to have separate BGP sessions to the spine.

• vPC peers must have identical configurations.
  • Consistent VLAN to VN-segment mapping.
• Consistent NVE binding to the same loopback interface
  • Using the same secondary IP address.
  • Using different primary IP addresses.

• Consistent VNI to group mapping.
  • The VRF overlay VLAN should be a member of the peer-link port-channel.

• For multicast, the vPC node that receives the (S, G) join from the RP (rendezvous point) becomes the DF (designated forwarder). On the DF node, encap routes are installed for multicast.
  
Decap routes are installed based on the election of a decapper from between the vPC primary node and the vPC secondary node. The winner of the decap election is the node with the least cost to the RP. However, if the cost to the RP is the same for both nodes, the vPC primary node is elected.

The winner of the decap election has the decap mroute installed. The other node does not have a decap route installed.

• On a vPC device, BUM traffic (broadcast, unknown-unicast, and multicast traffic) from hosts is replicated on the peer-link. A copy is made of every native packet and each native packet is sent across the peer-link to service orphan-ports connected to the peer vPC switch.

To prevent traffic loops in VXLAN networks, native packets ingressing the peer-link cannot be sent to an uplink. However, if the peer switch is the encapper, the copied packet traverses the peer-link and is sent to the uplink.

Each copied packet is sent on a special internal VLAN (VLAN 4041).

When peer-link is shut, the loopback interface used by NVE on the vPC secondary is brought down and the status is Admin Shut. This is done so that the route to the loopback is withdrawn on the upstream and that the upstream can divert all traffic to the vPC primary.

Orphans connected to the vPC secondary will experience loss of traffic for the period that the peer-link is shut. This is similar to Layer 2 orphans in a vPC secondary of a traditional vPC setup.

When peer-link is no-shut, the NVE loopback address is brought up again and the route is advertised upstream, attracting traffic.

For vPC, the loopback interface has 2 IP addresses: the primary IP address and the secondary IP address. The primary IP address is unique and is used by Layer 3 protocols.

The secondary IP address on loopback is necessary because the interface NVE uses it for the VTEP IP address. The secondary IP address must be same on both vPC peers.

The vPC peer-gateway feature must be enabled on both peers.

As a best practice, use peer-switch, peer gateway, ip arp sync, ipv6 nd sync configurations for improved convergence in vPC topologies.
In addition, increase the STP hello timer to 4 seconds to avoid unnecessary TCN generations when vPC role changes occur.

The following is an example (best practice) of a vPC configuration:

```
switch# sh ru vpc
version 6.1(2)I3(1)
feature vpc
vpc domain 2
  peer-switch
  peer-keepalive destination 172.29.206.65 source 172.29.206.64
  peer-gateway
  ipv6 nd synchronize
  ip arp synchronize

• On a vPC pair, shutting down NVE or NVE loopback on one of the vPC nodes is not a supported configuration. This means that traffic failover on one-side NVE shut or one-side loopback shut is not supported.

• Redundant anycast RPs configured in the network for multicast load-balancing and RP redundancy are supported on vPC VTEP topologies.

• Enabling vpc peer-gateway configuration is mandatory. For peer-gateway functionality, at least one backup routing SVI is required to be enabled across peer-link and also configured with PIM. This provides a backup routing path in the case when VTEP loses complete connectivity to the spine. Remote peer reachability is re-routed over the peer-link in this case.

The following is an example of SVI with PIM enabled:

```
switch# sh ru int vlan 2
interface Vlan2
  description special_svi_over_peer-link
  no shutdown
  ip address 30.2.1.1/30
  ip pim sparse-mode
```

---

**Note** The SVI must be configured on both vPC peers and requires PIM to be enabled.

• As a best practice when changing the secondary IP address of an anycast vPC VTEP, the NVE interfaces on both the vPC primary and the vPC secondary should be shut before the IP changes are made.

• To provide redundancy and failover of VXLAN traffic when a VTEP loses all of its uplinks to the spine, it is recommended to run a Layer 3 link or an SVI link over the peer-link between vPC peers.

• If DHCP Relay is required in VRF for DHCP clients or if loopback in VRF is required for reachability test on a vPC pair, it is necessary to create a backup SVI per VRF with PIM enabled.

```
switch# sh ru int vlan 20
interface Vlan20
  description backup routing svi for VRF Green
  vrf member GREEN
```
Network Considerations for VXLAN Deployments

• MTU Size in the Transport Network
  Due to the MAC-to-UDP encapsulation, VXLAN introduces 50-byte overhead to the original frames. Therefore, the maximum transmission unit (MTU) in the transport network must be increased by 50 bytes. If the overlays use a 1500-byte MTU, the transport network must be configured to accommodate 1550-byte packets at a minimum. Jumbo-frame support in the transport network is required if the overlay applications tend to use larger frame sizes than 1500 bytes.

• ECMP and LACP Hashing Algorithms in the Transport Network
  As described in a previous section, Cisco Nexus 9000 Series Switches introduce a level of entropy in the source UDP port for ECMP and LACP hashing in the transport network. As a way to augment this implementation, the transport network uses an ECMP or LACP hashing algorithm that takes the UDP source port as input for hashing, which achieves the best load-sharing results for VXLAN encapsulated traffic.

• Multicast Group Scaling
  The VXLAN implementation on Cisco Nexus 9000 Series Switches uses multicast tunnels for broadcast, unknown unicast, and multicast traffic forwarding. Ideally, one VXLAN segment mapping to one IP multicast group is the way to provide the optimal multicast forwarding. It is possible, however, to have multiple VXLAN segments share a single IP multicast group in the core network. VXLAN can support up to 16 million logical Layer 2 segments, using the 24-bit VNID field in the header. With one-to-one mapping between VXLAN segments and IP multicast groups, an increase in the number of VXLAN segments causes a parallel increase in the required multicast address space and the number of forwarding states on the core network devices. At some point, multicast scalability in the transport network can become a concern. In this case, mapping multiple VXLAN segments to a single multicast group can help conserve multicast control plane resources on the core devices and achieve the desired VXLAN scalability. However, this mapping comes at the cost of suboptimal multicast forwarding. Packets forwarded to the multicast group for one tenant are now sent to the VTEPs of other tenants that are sharing the same multicast group. This causes inefficient utilization of multicast data plane resources. Therefore, this solution is a trade-off between control plane scalability and data plane efficiency.

  Despite the suboptimal multicast replication and forwarding, having multitenant VXLAN networks to share a multicast group does not bring any implications to the Layer 2 isolation between the tenant networks. After receiving an encapsulated packet from the multicast group, a VTEP checks and validates the VNID in the VXLAN header of the packet. The VTEP discards the packet if the VNID is unknown to it. Only when the VNID matches one of the VTEP’s local VXLAN VNIDs, does it forward the packet to that VXLAN segment. Other tenant networks will not receive the packet. Thus, the segregation between VXLAN segments is not compromised.

Considerations for the Transport Network

The following are considerations for the configuration of the transport network:

• On the VTEP device:
  • Enable and configure IP multicast.*
  • Create and configure a loopback interface with a /32 IP address.
(For vPC VTEPs, you must configure primary and secondary /32 IP addresses.)

- Enable UP multicast on the loopback interface. *
- Advertise the loopback interface /32 addresses through the routing protocol (static route) that runs in the transport network.
- Enable IP multicast on the uplink outgoing physical interface. *

- Throughout the transport network:
  - Enable and configure IP multicast.*

---

**Note**

* Not required for static ingress replication or BGP EVPN ingress replication.

### Considerations for Tunneling VXLAN

DC Fabrics with VXLAN BGP EVPN are becoming the transport infrastructure for overlays. These overlays, often originated on the server (Host Overlay), require integration or transport over the top of the existing transport infrastructure (Network Overlay).

Nested VXLAN (Host Overlay over Network Overlay) support has been added starting with Cisco NX-OS Release 7.0(3)I7(4) and Cisco NX-OS Release 9.2(2) on the Cisco Nexus 9200, 9300-EX, 9300-FX, and 9300-FX2 platform switches.

*Figure 1: Host Overlay*

To provide Nested VXLAN support, the switch hardware and software must differentiate between two different VXLAN profiles:
• VXLAN originated behind the Hardware VTEP for transport over VXLAN BGP EVPN (nested VXLAN)
• VXLAN originated behind the Hardware VTEP to integrated with VXLAN BGP EVPN (BUD Node)

The detection of the two different VXLAN profiles is automatic and no specific configuration is needed for nested VXLAN. As soon as VXLAN encapsulated traffic arrives in a VXLAN enabled VLAN, the traffic is transported over the VXLAN BGP EVPN enabled DC Fabric.

The following attachment modes are supported for Nested VXLAN:
• Untagged traffic (in native VLAN on a trunk port or on an access port)
• Tagged traffic (tagged VLAN on a IEEE 802.1Q trunk port)
• Untagged and tagged traffic that is attached to a vPC domain
• Untagged traffic on a Layer 3 interface of a Layer 3 port-channel interface

BGP EVPN Considerations for VXLAN Deployment

Commands for BGP EVPN

The following describes commands to support BGP EVPN VXLAN control planes.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>member vni range [associate-vrf]</code></td>
<td>Associate VXLAN VNIs (Virtual Network Identifiers) with the NVE interface</td>
</tr>
<tr>
<td></td>
<td>The attribute <code>associate-vrf</code> is used to identify and separate processing VNIs that are associated with a VRF and used for routing.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The VRF and VNI specified with this command must match the configuration of the VNI under the VRF.</td>
</tr>
<tr>
<td><code>show nve vni</code></td>
<td>Displays information that determine if the VNI is configured for peer and host learning via the control plane or data plane.</td>
</tr>
<tr>
<td><code>show nve vni summary</code></td>
<td>Displays the Layer 2 VPN EVPN address family.</td>
</tr>
<tr>
<td><code>show bgp l2vpn evpn</code></td>
<td>Specifies BGP as the mechanism for host reachability advertisement.</td>
</tr>
<tr>
<td><code>show bgp l2vpn evpn summary</code></td>
<td>Suppresses ARP under Layer 2 VNI.</td>
</tr>
<tr>
<td><code>host-reachability protocol bgp</code></td>
<td>Configures anycast gateway MAC of the switch.</td>
</tr>
<tr>
<td><code>suppress-arp</code></td>
<td>Creates the VRF and enter the VRF mode.</td>
</tr>
<tr>
<td><code>fabric forwarding anycast-gateway-mac</code></td>
<td>Enables/Disables the Ethernet VPN (EVPN).</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>router bgp</code></td>
<td>Configures the Border Gateway Protocol (BGP).</td>
</tr>
<tr>
<td><code>system vlan nve-overlay id range</code></td>
<td>For scale environments, the VLAN IDs related to the VRF and Layer-3 VNI (L3VNI) must be reserved with the <code>system vlan nve-overlay id</code> command. This is required to optimize the VXLAN resource allocation to scale the following platforms:</td>
</tr>
<tr>
<td></td>
<td>• Cisco Nexus 9200 platform switches beginning with the Cisco NX-OS Release 7.0(3)I1(2) through 7.0(3)I5(2)</td>
</tr>
<tr>
<td></td>
<td>• Cisco Nexus 9300-EX, 9300-FX, and 9300-FX2 platforms switches beginning with the Cisco NX-OS Release 7.0(3)I1(2) through 7.0(3)I5(2)</td>
</tr>
<tr>
<td></td>
<td>• Cisco Nexus 9300 platforms switches beginning with the Cisco NX-OS Release 7.0(3)I1(2)</td>
</tr>
<tr>
<td></td>
<td>• Cisco Nexus 9500 platforms switches with -EX and -FX line cards.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Beginning with the Cisco NX-OS Release 7.0(3)I5(2), the Cisco Nexus 9200, Cisco Nexus 9300-EX, 9300-FX, and 9300-FX2 do not require this command. Beginning with Cisco NX-OS Release 7.0(3)I5(2), it is strongly recommended to remove the command on Cisco Nexus 9200, 9300-EX, 9300-FX, and 9300-FX2 platform switches as it would disable Tenant Routed Multicast functionality on the VRF.</td>
</tr>
<tr>
<td></td>
<td>The <code>system vlan nve-overlay id</code> command should be used for a VRF or a Layer-3 VNI (L3VNI) only. Do not use this command for regular VLANs or Layer-2 VNIs (L2VNI).</td>
</tr>
</tbody>
</table>
Configuring VXLAN BGP EVPN

Enabling VXLAN

Enable VXLAN and the EVPN.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 feature vn-segment</td>
<td>Enable VLAN-based VXLAN</td>
</tr>
<tr>
<td>Step 2 feature nv overlay</td>
<td>Enable VXLAN</td>
</tr>
<tr>
<td>Step 3 nv overlay evpn</td>
<td>Enable the EVPN control plane for VXLAN.</td>
</tr>
</tbody>
</table>

Command Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>suppress mac-route</td>
<td>Suppresses the BGP MAC route so that BGP only sends the MAC/IP route for a host. Under NVE, the MAC updates for all VNIs are suppressed.</td>
</tr>
</tbody>
</table>

Note

- Receive-side — Suppressing the MAC route depends upon the capability of the remote EVPN peer to derive a MAC route from the MAC/IP route (7.0(3)I2(2) and later). Avoid using the “suppress mac-route” command if devices in the network are running an earlier NX-OS release.
- Send-side — Suppressing the MAC route means that the sender has a MAC/IP route. If your configuration has pure-Layer 2 VNIs (such as no corresponding VRF or Layer3-VNI), then there is no corresponding MAC/IP and you should avoid using the “suppress mac-route” command.
Configuring VLAN and VXLAN VNI

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 vlan number</td>
<td>Specify VLAN.</td>
</tr>
<tr>
<td>Step 2 vn-segment number</td>
<td>Map VLAN to VXLAN VNI to configure Layer 2 VNI under VXLAN VLAN.</td>
</tr>
</tbody>
</table>

Configuring VRF for VXLAN Routing

Configure the tenant VRF.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 vrf context vxlan</td>
<td>Configure the VRF.</td>
</tr>
<tr>
<td>Step 2 vni number</td>
<td>Specify VNI.</td>
</tr>
<tr>
<td>Step 3 rd auto</td>
<td>Specify VRF RD (route distinguisher).</td>
</tr>
<tr>
<td>Step 4 address-family ipv4 unicast</td>
<td>Configure address family for IPv4.</td>
</tr>
<tr>
<td>Step 5 route-target both auto</td>
<td><strong>Note</strong> Specifying the auto option is applicable only for IBGP. Manually configured route targets are required for EBGP.</td>
</tr>
<tr>
<td>Step 6 route-target both auto evpn</td>
<td><strong>Note</strong> Specifying the auto option is applicable only for IBGP. The auto option is available beginning with Cisco NX-OS Release 7.0(3)I7(1). Manually configured route targets are required for EBGP.</td>
</tr>
<tr>
<td>Step 7 address-family ipv6 unicast</td>
<td>Configure address family for IPv6.</td>
</tr>
<tr>
<td>Step 8 route-target both auto</td>
<td><strong>Note</strong> Specifying the auto option is applicable only for IBGP. The auto option is available beginning with Cisco NX-OS Release 7.0(3)I7(1). Manually configured route targets are required for EBGP.</td>
</tr>
</tbody>
</table>
### About RD Auto

The auto-derived Route Distinguisher (rd auto) is based on the Type 1 encoding format as described in IETF RFC 4364 section 4.2 [https://tools.ietf.org/html/rfc4364#section-4.2](https://tools.ietf.org/html/rfc4364#section-4.2). The Type 1 encoding allows a 4-byte administrative field and a 2-byte numbering field. Within Cisco NX-OS, the auto derived RD is constructed with the IP address of the BGP Router ID as the 4-byte administrative field (RID) and the internal VRF identifier for the 2-byte numbering field (VRF ID).

The 2-byte numbering field is always derived from the VRF, but results in a different numbering scheme depending on its use for the IP-VRF or the MAC-VRF:

- The 2-byte numbering field for the IP-VRF uses the internal VRF ID starting at 1 and increments. VRF IDs 1 and 2 are reserved for the default VRF and the management VRF respectively. The first custom defined IP VRF uses VRF ID 3.
- The 2-byte numbering field for the MAC-VRF uses the VLAN ID + 32767, which results in 32768 for VLAN ID 1 and incrementing.

Example auto-derived Route Distinguisher (RD)

- IP-VRF with BGP Router ID 192.0.2.1 and VRF ID 6 - RD 192.0.2.1:6
- MAC-VRF with BGP Router ID 192.0.2.1 and VLAN 20 - RD 192.0.2.1:32787

### About Route-Target Auto

The auto-derived Route-Target (route-target import/export/both auto) is based on the Type 0 encoding format as described in IETF RFC 4364 section 4.2 [https://tools.ietf.org/html/rfc4364#section-4.2](https://tools.ietf.org/html/rfc4364#section-4.2). IETF RFC 4364 section 4.2 describes the Route Distinguisher format and IETF RFC 4364 section 4.3.1 refers that it is desirable to use a similar format for the Route-Targets. The Type 0 encoding allows a 2-byte administrative field and a 4-byte numbering field. Within Cisco NX-OS, the auto derived Route-Target is constructed with the Autonomous System Number (ASN) as the 2-byte administrative field and the Service Identifier (VNI) for the 4-byte numbering field.

Examples of an auto derived Route-Target (RT):

- IP-VRF within ASN 65001 and L3VNI 50001 - Route-Target 65001:50001
- MAC-VRF within ASN 65001 and L2VNI 30001 - Route-Target 65001:30001

For Multi-AS environments, the Route-Targets must either be statically defined or rewritten to match the ASN portion of the Route-Targets.
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/command_references/configuration_commands/b_N9K_Config_Commands_703i7x/b_N9K_Config_Commands_703i7x_chapter_010010.html#wp4498893710

---

**Note**

Auto derived Route-Targets for a 4-byte ASN are not supported.

---

## Configuring SVI for Hosts for VXLAN Routing

Configure the SVI for hosts.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: <code>vlan number</code></td>
<td>Specify VLAN</td>
</tr>
<tr>
<td>Step 2: <code>interface vlan-number</code></td>
<td>Specify VLAN interface.</td>
</tr>
<tr>
<td>Step 3: <code>vrf member vxlan-number</code></td>
<td>Configure SVI for host.</td>
</tr>
<tr>
<td>Step 4: <code>ip address address</code></td>
<td>Specify IP address.</td>
</tr>
</tbody>
</table>

---

## Configuring VRF Overlay VLAN for VXLAN Routing

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: <code>vlan number</code></td>
<td>Specify VLAN</td>
</tr>
<tr>
<td>Step 2: <code>vn-segment number</code></td>
<td>Specify vn-segment.</td>
</tr>
</tbody>
</table>

---

## Configuring VNI Under VRF for VXLAN Routing

Configures a Layer 3 VNI under a VRF overlay VLAN. (A VRF overlay VLAN is a VLAN that is not associated with any server facing ports. All VXLAN VNIs that are mapped to a VRF, need to have their own internal VLANs allocated to it.)

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: <code>vrf context vxlan</code></td>
<td>Create a VXLAN Tenant VRF</td>
</tr>
<tr>
<td>Step 2: <code>vni number</code></td>
<td>Configure Layer 3 VNI under VRF.</td>
</tr>
</tbody>
</table>
Configuring Anycast Gateway for VXLAN Routing

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>fabric forwarding anycast-gateway-mac address</strong></td>
</tr>
<tr>
<td></td>
<td>Configure distributed gateway virtual MAC address.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>One virtual MAC per VTEP</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>All VTEPs must have the same virtual MAC address.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>fabric forwarding mode anycast-gateway</strong></td>
</tr>
<tr>
<td></td>
<td>Associate SVI with Anycast Gateway under VLAN configuration mode.</td>
</tr>
</tbody>
</table>

### Configuring the NVE Interface and VNIs

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>interface nve-interface</strong></td>
</tr>
<tr>
<td></td>
<td>Configure the NVE interface.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>host-reachability protocol bgp</strong></td>
</tr>
<tr>
<td></td>
<td>This defines BGP as the mechanism for host reachability advertisement</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>member vni vni associate-vrf</strong></td>
</tr>
<tr>
<td></td>
<td>Add Layer-3 VNIs, one per tenant VRF, to the overlay.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Required for VXLAN routing only.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>member vni vni</strong></td>
</tr>
<tr>
<td></td>
<td>Add Layer 2 VNI s to the tunnel interface.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>mcast-group address</strong></td>
</tr>
<tr>
<td></td>
<td>Configure the mcast group on a per-VNI basis</td>
</tr>
</tbody>
</table>

### Configuring BGP on the VTEP

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>router bgp number</strong></td>
</tr>
<tr>
<td></td>
<td>Configure BGP.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>router-id address</strong></td>
</tr>
<tr>
<td></td>
<td>Specify router address.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>neighbor address remote-as number</strong></td>
</tr>
<tr>
<td></td>
<td>Define MP-BGP neighbors. Under each neighbor define l2vpn evpn.</td>
</tr>
</tbody>
</table>
### Configuring VXLAN BGP EVPN

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>evpn</code></td>
<td>Configure VRF.</td>
</tr>
<tr>
<td><code>vni number 12</code></td>
<td>Note Only Layer 2 VNI need to be specified.</td>
</tr>
<tr>
<td><code>rd auto</code></td>
<td>Define VRF RD (route distinguisher) to configure VRF context.</td>
</tr>
<tr>
<td><code>route-target import auto</code></td>
<td>Define VRF Route Target and import policies.</td>
</tr>
<tr>
<td><code>route-target export auto</code></td>
<td>Define VRF Route Target and export policies.</td>
</tr>
</tbody>
</table>
About RD Auto

The auto-derived Route Distinguisher (rd auto) is based on the Type 1 encoding format as described in IETF RFC 4364 section 4.2. The Type 1 encoding allows a 4-byte administrative field and a 2-byte numbering field. Within Cisco NX-OS, the auto derived RD is constructed with the IP address of the BGP Router ID as the 4-byte administrative field (RID) and the internal VRF identifier for the 2-byte numbering field (VRF ID).

The 2-byte numbering field is always derived from the VRF, but results in a different numbering scheme depending on its use for the IP-VRF or the MAC-VRF:

- The 2-byte numbering field for the IP-VRF uses the internal VRF ID starting at 1 and increments. VRF IDs 1 and 2 are reserved for the default VRF and the management VRF respectively. The first custom defined IP VRF uses VRF ID 3.
- The 2-byte numbering field for the MAC-VRF uses the VLAN ID + 32767, which results in 32768 for VLAN ID 1 and incrementing.

Example auto-derived Route Distinguisher (RD)

- IP-VRF with BGP Router ID 192.0.2.1 and VRF ID 6 - RD 192.0.2.1:6
- MAC-VRF with BGP Router ID 192.0.2.1 and VLAN 20 - RD 192.0.2.1:32787

About Route-Target Auto

The auto-derived Route-Target (route-target import/export/both auto) is based on the Type 0 encoding format as described in IETF RFC 4364 section 4.2. IETF RFC 4364 section 4.2 describes the Route Distinguisher format and IETF RFC 4364 section 4.3.1 refers that it is desirable to use a similar format for the Route-Targets. The Type 0 encoding allows a 2-byte administrative field and a 4-byte numbering field. Within Cisco NX-OS, the auto derived Route-Target is constructed with the Autonomous System Number (ASN) as the 2-byte administrative field and the Service Identifier (VNI) for the 4-byte numbering field.

Examples of an auto derived Route-Target (RT):

- IP-VRF within ASN 65001 and L3VNI 50001 - Route-Target 65001:50001
- MAC-VRF within ASN 65001 and L2VNI 30001 - Route-Target 65001:30001

For Multi-AS environments, the Route-Targets must either be statically defined or rewritten to match the ASN portion of the Route-Targets.

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/command_references/configuration_commands/b_N9K_Config_Commands_703i7x/b_N9K_Config_Commands_703i7x_chapter_010010.html#wp4498893710

Note

Auto derived Route-Targets for a 4-byte ASN are not supported.
Configuring VXLAN EVPN Ingress Replication

For VXLAN EVPN ingress replication, the VXLAN VTEP uses a list of IP addresses of other VTEPS in the network to send BUM (broadcast, unknown unicast and multicast) traffic. These IP addresses are exchanged between VTEPs through the BGP EVPN control plane.

VXLAN EVPN ingress replication is supported on:

- Cisco Nexus Series 9300 Series switches (7.0(3)I1(2) and later).
- Cisco Nexus Series 9500 Series switches (7.0(3)I2(1) and later).

Before you begin

The following are required before configuring VXLAN EVPN ingress replication (7.0(3)I1(2) and later):

- Enable VXLAN
- Configure VLAN and VXLAN VNI
- Configure BGP on the VTEP
- Configure RD and Route Targets for VXLAN Bridging

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>interface nve-interface</td>
<td>Configure the NVE interface.</td>
</tr>
<tr>
<td>Step 2</td>
<td>host-reachability protocol bgp</td>
<td>This defines BGP as the mechanism for host reachability advertisement</td>
</tr>
<tr>
<td>Step 3</td>
<td>member vni vni associate-vrf</td>
<td>Add Layer-3 VNIs, one per tenant VRF, to the overlay.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note Required for VXLAN routing only.</td>
</tr>
<tr>
<td>Step 4</td>
<td>member vni vni</td>
<td>Add Layer 2 VNIs to the tunnel interface.</td>
</tr>
<tr>
<td>Step 5</td>
<td>ingress-replication protocol bgp</td>
<td>Enables the VTEP to exchange local and remote VTEP IP addresses on the VNI in order to create the ingress replication list. This enables sending and receiving BUM traffic for the VNI.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note Using ingress-replication protocol bgp avoids the need for any multicast configurations that might have been required for configuring the underlay.</td>
</tr>
</tbody>
</table>
# Configuring BGP for EVPN on the Spine

## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>route-map permit all permit 10</code></td>
<td>Configure route-map.</td>
<td>The route-map keeps the next-hop unchanged for EVPN routes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Required for eBGP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Optional for iBGP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Note When two next hops are enabled, next hop ordering is not maintained.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If one of the next hops is a VXLAN next hop and the other next hop is local reachable via FIB/AM/Hmm, the local next hop reachable via FIB/AM/Hmm is always taken irrespective of the order. Directly/locally connected next hops are always given priority over remotely connected next hops.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>set ip next-hop unchanged</code></td>
<td>Set next-hop address.</td>
<td>The route-map keeps the next-hop unchanged for EVPN routes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Required for eBGP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Optional for iBGP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Note Define neighbor.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>router bgp autonomous system number</code></td>
<td>Specify BGP.</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>address-family l2vpn evpn</code></td>
<td>Configure address family Layer 2 VPN EVPN under the BGP neighbor.</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>retain route-target all</code></td>
<td>Configure retain route-target all under address-family Layer 2 VPN EVPN [global].</td>
<td>Required for eBGP. Allows the spine to retain and advertise all EVPN routes when there are no local VNI configured with matching import route targets.</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>neighbor address remote-as number</code></td>
<td>Define neighbor.</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 7</strong> address-family l2vpn evpn</td>
<td>Configure address family Layer 2 VPN EVPN under the BGP neighbor.</td>
</tr>
<tr>
<td><strong>Step 8</strong> disable-peer-as-check</td>
<td>Disables checking the peer AS number during route advertisement. Configure this parameter on the spine for eBGP when all leafs are using the same AS but the spines have a different AS than leafs.</td>
</tr>
<tr>
<td><strong>Step 9</strong> send-community extended</td>
<td>Configures community for BGP neighbors.</td>
</tr>
<tr>
<td><strong>Step 10</strong> route-map permit all out</td>
<td>Applies route-map to keep the next-hop unchanged.</td>
</tr>
</tbody>
</table>

### Suppressing ARP

Suppressing ARP includes changing the size of the ACL ternary content addressable memory (TCAM) regions in the hardware.

**Note**

For information on configuring ACL TCAM regions, see the *Configuring IP ACLs* chapter of the *Cisco Nexus 9000 Series NX-OS Security Configuration Guide*.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> hardware access-list tcam region arp-ether size double-wide</td>
<td>Configure TCAM region to suppress ARP.</td>
</tr>
<tr>
<td></td>
<td><em>tcam-size</em>—TCAM size. The size has to be a multiple of 256. If the size is more than 256, it has to be a multiple of 512.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Reload is required for the TCAM configuration to be in effect.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Configuring the <em>hardware access-list tcam region arp-ether size double-wide</em> is not required on Cisco Nexus 9200 Series switches.</td>
</tr>
<tr>
<td><strong>Step 2</strong> interface nve 1</td>
<td>Create the network virtualization endpoint (NVE) interface.</td>
</tr>
<tr>
<td><strong>Step 3</strong> member vni vni-id</td>
<td>Specify VNI ID.</td>
</tr>
</tbody>
</table>
### Disabling VXLANs

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>no nv overlay evpn</td>
<td>Disables EVPN control plane.</td>
</tr>
<tr>
<td>Step 3</td>
<td>no feature vn-segment-vlan-based</td>
<td>Disables the global mode for all VXLAN bridge domains.</td>
</tr>
<tr>
<td>Step 4</td>
<td>no feature nv overlay</td>
<td>Disables the VXLAN feature.</td>
</tr>
<tr>
<td>Step 5</td>
<td>(Optional) copy running-config start-up-config</td>
<td>Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

### Duplicate Detection for IP and MAC Addresses

Cisco NX-OS supports duplicate detection for IP and MAC addresses. This enables the detection of duplicate IP or MAC addresses based on the number of moves in a given time-interval (seconds).

The default is 5 moves in 180 seconds. (Default number of moves is 5 moves. Default time-interval is 180 seconds.)

- For IP addresses:
  - After the 5th move within 180 seconds, the switch starts a 30 second lock (hold down timer) before checking to see if the duplication still exists (an effort to prevent an increment of the sequence bit). This 30 second lock can occur 5 times within 24 hours (this means 5 moves in 180 seconds for 5 times) before the switch permanently locks or freezes the duplicate entry. *(show fabric forwarding ip local-host-db vrf abc)*

- For MAC addresses:
  - After the 5th move within 180 seconds, the switch starts a 30 second lock (hold down timer) before checking to see if the duplication still exists (an effort to prevent an increment of the sequence bit). This 30 second lock can occur 3 times within 24 hours (this means 5 moves in 180 seconds for 3 times) before the switch permanently locks or freezes the duplicate entry. *(show l2rib internal permanently-frozen-list)*

- Wherever a MAC address is permanently frozen, a syslog message with written by L2RIB.
The following are example commands to help the configuration of the number of VM moves in a specific time interval (seconds) for duplicate IP-detection:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch(config)# fabric forwarding ?</td>
<td>Available sub-commands:</td>
</tr>
<tr>
<td>anycast-gateway-mac</td>
<td>• Anycast gateway MAC of the switch.</td>
</tr>
<tr>
<td>dup-host-ip-addr-detection</td>
<td>• To detect duplicate host addresses in n seconds.</td>
</tr>
<tr>
<td>switch(config)# fabric forwarding dup-host-ip-addr-detection ?</td>
<td>The number of host moves allowed in n seconds. The range is 1 to 1000 moves; default is 5 moves.</td>
</tr>
<tr>
<td>&lt;1-1000&gt;</td>
<td></td>
</tr>
<tr>
<td>switch(config)# fabric forwarding dup-host-ip-addr-detection 100 ?</td>
<td>The duplicate detection timeout in seconds for the number of host moves. The range is 2 to 36000 seconds; default is 180 seconds.</td>
</tr>
<tr>
<td>&lt;2-36000&gt;</td>
<td></td>
</tr>
<tr>
<td>switch(config)# fabric forwarding dup-host-ip-addr-detection 100 10</td>
<td>Detects duplicate host addresses (limited to 100 moves) in a period of 10 seconds.</td>
</tr>
</tbody>
</table>

The following are example commands to help the configuration of the number of VM moves in a specific time interval (seconds) for duplicate MAC-detection:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch(config)# l2rib dup-host-mac-detection ?</td>
<td>Available sub-commands for L2RIB:</td>
</tr>
<tr>
<td>&lt;1-1000&gt;</td>
<td>• The number of host moves allowed in n seconds. The range is 1 to 1000 moves.</td>
</tr>
<tr>
<td>default</td>
<td>• Default setting (5 moves in 180 in seconds).</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>switch(config)# l2rib dup-host-mac-detection 100 ?</td>
<td>The duplicate detection timeout in seconds for the number of host moves. The range is 2 to 36000 seconds; default is 180 seconds.</td>
</tr>
<tr>
<td>&lt;2-36000&gt;</td>
<td></td>
</tr>
</tbody>
</table>
Enabling Nuage Controller Interoperability

The following steps enable Nuage controller interoperability.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>nuage controller interop</code></td>
<td>Global command to enable interoperability mode.</td>
</tr>
<tr>
<td>2</td>
<td><code>router bgp number</code></td>
<td>Configure BGP.</td>
</tr>
<tr>
<td>3</td>
<td><code>address-family l2vpn evpn</code></td>
<td>Configure address family Layer 2 VPN EVPN under the BGP neighbor.</td>
</tr>
<tr>
<td>4</td>
<td><code>advertise-system-mac</code></td>
<td>Enable Nuage interoperability mode for BGP.</td>
</tr>
<tr>
<td>5</td>
<td><code>allow-vni-in-ethertag</code></td>
<td>Enable Nuage interoperability mode for BGP.</td>
</tr>
<tr>
<td>6</td>
<td><code>route-map permitall permit 10</code></td>
<td>Configure route-map to permit all.</td>
</tr>
<tr>
<td>7</td>
<td><code>router bgp number</code></td>
<td>Configure BGP.</td>
</tr>
<tr>
<td>8</td>
<td><code>vrf vrf-name</code></td>
<td>Specify tenant VRF.</td>
</tr>
<tr>
<td>9</td>
<td><code>address-family ipv4 unicast</code></td>
<td>Configure address family for IPv4.</td>
</tr>
<tr>
<td>10</td>
<td><code>advertise l2vpn evpn</code></td>
<td>Enable advertising EVPN routes.</td>
</tr>
<tr>
<td>11</td>
<td><code>redistribute hmm route-map permitall</code></td>
<td>Enables advertise host tenant routes as evpn type-5 routes for interoperability.</td>
</tr>
</tbody>
</table>

**Example**

The following is an example to enable Nuage controller interoperability:

```bash
/*** Enable interoperability mode at global level. ***/
switch(config)# nuage controller interop

/*** Configure BGP to enable interoperability mode. ***/
switch(config)# router bgp 1001
switch(config-router)# address-family l2vpn evpn
switch(config-router-af)# advertise-system-mac
switch(config-router-af)# allow-vni-in-ethertag

/*** Advertise host tenant routes as evpn type-5 routes for interoperability. ***/
switch(config)# route-map permitall permit 10
switch(config)# router bgp 1001
```
### Verifying the VXLAN BGP EVPN Configuration

To display the VXLAN BGP EVPN configuration information, enter one of the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show nve vrf</code></td>
<td>Displays VRFs and associated VNIs</td>
</tr>
<tr>
<td><code>show bgp l2vpn evpn</code></td>
<td>Displays routing table information.</td>
</tr>
<tr>
<td>`show ip arp suppression-cache [detail</td>
<td>summary</td>
</tr>
<tr>
<td><code>show vxlan interface</code></td>
<td>Displays VXLAN interface status.</td>
</tr>
<tr>
<td>`show vxlan interface</td>
<td>count`</td>
</tr>
<tr>
<td>`show l2route evpn mac [all</td>
<td>evi</td>
</tr>
<tr>
<td><code>show l2route evpn fl all</code></td>
<td>Displays all fl routes.</td>
</tr>
<tr>
<td><code>show l2route evpn imet all</code></td>
<td>Displays all imet routes.</td>
</tr>
<tr>
<td><code>show l2route evpn mac-ip all</code></td>
<td>Displays all MAC IP routes.</td>
</tr>
<tr>
<td><code>show l2route evpn mac-ip all detail</code></td>
<td>Displays all MAC IP routes.</td>
</tr>
<tr>
<td><code>show l2route topology</code></td>
<td>Displays Layer 2 route topology.</td>
</tr>
</tbody>
</table>

**Note** Although the `show ip bgp` command is available for verifying a BGP configuration, as a best practice, it is preferable to use the `show bgp` command instead.
Example of VXLAN BGP EVPN (EBGP)

An example of a VXLAN BGP EVPN (EBGP):

Figure 2: VXLAN BGP EVPN Topology (EBGP)

EBGP between Spine and Leaf

- Spine (9504-A)
  - Enable the EVPN control plane
    `nv overlay evpn`
  - Enable the relevant protocols
    `feature bgp`
    `feature pim`
- Configure Loopback for BGP

`interface loopback0`
  `ip address 10.1.1.1/32`
  `ip pim sparse-mode`
- Configure Loopback for Anycast RP

`interface loopback1`
ip address 100.1.1.1/32
ip pim sparse-mode

• Configure Anycast RP

ip pim rp-address 100.1.1.1 group-list 224.0.0.0/4
ip pim ssm range 232.0.0.0/8
ip pim anycast-rp 100.1.1.1 10.1.1.1
ip pim anycast-rp 100.1.1.1 20.1.1.1

• Configure route-map used by EBGP for Spine

route-map permitall permit 10
set ip next-hop unchanged

• Configure interfaces for Spine-leaf interconnect

interface Ethernet4/2
ip address 192.168.1.42/24
ip pim sparse-mode
no shutdown

interface Ethernet4/3
ip address 192.168.2.43/24
ip pim sparse-mode
no shutdown

• Configure the BGP overlay for the EVPN address family.

router bgp 100
router-id 10.1.1.1
address-family l2vpn evpn
    nexthop route-map permitall
    retain route-target all
neighbor 30.1.1.1 remote-as 200
    update-source loopback0
ebgp-multihop 3
    address-family l2vpn evpn
disable-peer-as-check
    send-community extended
    route-map permitall out
neighbor 40.1.1.1 remote-as 200
    update-source loopback0
ebgp-multihop 3
    address-family l2vpn evpn
disable-peer-as-check
    send-community extended
    route-map permitall out

• Configure the BGP underlay.

neighbor 192.168.1.43 remote-as 200
    address-family ipv4 unicast
    allowas-in
disable-peer-as-check

• Spine (9504-B)
• Enable the EVPN control plane and the relevant protocols

```bash
nv overlay evpn
feature bgp
feature pim
```

• Configure Anycast RP

```bash
ip pim rp-address 100.1.1.1 group-list 224.0.0.0/4
ip pim ssm range 232.0.0.0/8
ip pim anycast-rp 100.1.1.1 10.1.1.1
ip pim anycast-rp 100.1.1.1 20.1.1.1
```

• Configure route-map used by EBGP for Spine

```bash
route-map permitall permit 10
set ip next-hop unchanged
```

• Configure interfaces for Spine-leaf interconnect

```bash
interface Ethernet4/2
  ip address 192.168.4.42/24
  ip pim sparse-mode
  no shutdown

interface Ethernet4/3
  ip address 192.168.3.43/24
  ip pim sparse-mode
  no shutdown
```

• Configure Loopback for BGP

```bash
interface loopback0
  ip address 20.1.1.1/32
  ip pim sparse-mode
```

• Configure Loopback for Anycast RP

```bash
interface loopback1
  ip address 100.1.1.1/32
  ip pim sparse-mode
```

• Configure the BGP overlay for the EVPN address family.

```bash
router bgp 100
  router-id 20.1.1.1
  address-family l2vpn evpn
    retain route-target all
  neighbor 30.1.1.1 remote-as 200
    update-source loopback0
    ebgp-multihop 3
    address-family l2vpn evpn
      disable-peer-as-check
      send-community extended
    route-map permitall out
  neighbor 40.1.1.1 remote-as 200
```
- Configure the BGP underlay.

  neighbor 192.168.1.43 remote-as 200
  address-family ipv4 unicast
      allowas-in
      disable-peer-as-check

- Leaf (9396-A)

  - Enable the EVPN control plane
    nv overlay evpn

  - Enable the relevant protocols
    feature bgp
    feature pim
    feature interface-vlan

  - Enable VXLAN with distributed anycast-gateway using BGP EVPN
    feature vn-segment-vlan-based
    feature nv overlay
    fabric forwarding anycast-gateway-mac 0000.2222.3333

  - Enable PIM RP
    ip pim rp-address 100.1.1.1 group-list 224.0.0.0/4
    ip pim ssm range 232.0.0.0/8

- Create VLANs

  vlan 1-1002

- Configure Loopback for BGP

  interface loopback0
      ip address 30.1.1.1/32
      ip pim sparse-mode

- Configure Loopback for local VTEP IP

  interface loopback1
      ip address 50.1.1.1/32
      ip pim sparse-mode

- Configure interfaces for Spine-leaf interconnect
interface Ethernet2/2
  ip address 192.168.1.22/24
  ip pim sparse-mode
  no shutdown

interface Ethernet2/3
  ip address 192.168.3.23/24
  ip pim sparse-mode
  no shutdown

• Create the VRF overlay VLAN and configure the vn-segment.

  vlan 101
  vn-segment 900001

• Configure VRF overlay VLAN/SVI for the VRF

  interface Vlan101
    no shutdown
    vrf member vxlan-900001
    ip forward

• Create VLAN and provide mapping to VXLAN

  vlan 1001
  vn-segment 2001001
  vlan 1002
  vn-segment 2001002

• Create VRF and configure VNI

  vrf context vxlan-900001
  vni 900001
  rd auto
  address-family ipv4 unicast
    route-target import 65535:101 evpn
    route-target export 65535:101 evpn
    route-target import 65535:101
    route-target export 65535:101
  address-family ipv6 unicast
    route-target import 65535:101 evpn
    route-target export 65535:101 evpn
    route-target import 65535:101
    route-target export 65535:101

• Create server facing SVI and enable distributed anycast-gateway

  interface Vlan1001
    no shutdown
    vrf member vxlan-900001
    ip address 4.1.1.1/24
    ipv6 address 4::1:0:1::1/64
    fabric forwarding mode anycast-gateway

  interface Vlan1002
no shutdown
vrf member vxlan-900001
ip address 4.2.2.1/24
ipv6 address 4:2:0:1::1/64
fabric forwarding mode anycast-gateway

• Configure ACL TCAM region for ARP suppression

Note  The **hardware access-list tcam region arp-ether 256 double-wide** command is not needed for Cisco Nexus 9300-EX, 9300-FX, and 9300-FX2 platform switches.

hardware access-list tcam region arp-ether 256 double-wide

• Create the network virtualization endpoint (NVE) interface

interface nve1
  no shutdown
  source-interface loopback1
  host-reachability protocol bgp
  member vni 9000001 associate-vrf
  member vni 2001001
  mcast-group 239.0.0.1
  member vni 2001002
  mcast-group 239.0.0.1

• Configure interfaces for hosts/servers.

interface Ethernet1/47
  switchport
  switchport access vlan 1002

interface Ethernet1/48
  switchport
  switchport access vlan 1001

• Configure BGP

router bgp 200
router-id 30.1.1.1
neighbor 10.1.1.1 remote-as 100
  update-source loopback0
  ebgp-multihop 3
  allowas-in
  send-community extended
  address-family l2vpn evpn
  allowas-in
  send-community extended
neighbor 20.1.1.1 remote-as 100
  update-source loopback0
  ebgp-multihop 3
  allowas-in
  send-community extended
  address-family l2vpn evpn
  allowas-in
  send-community extended
vrf vxlan-900001
  advertise l2vpn evpn
evnp
  vni 2001001 12
  vni 2001002 12
  rd auto
  route-target import auto
  route-target export auto

- Leaf (9396-B)
- Enable the EVPN control plane functionality and the relevant protocols
  nv overlay evpn
  feature bgp
  feature pim
  feature interface-vlan
  feature vn-segment-vlan-based
  feature nv overlay

- Enable PIM RP
  ip pim rp-address 100.1.1.1 group-list 224.0.0.0/4
  ip pim ssm range 232.0.0.0/8

- Enable VXLAN with distributed anycast-gateway using BGP EVPN
  fabric forwarding anycast-gateway-mac 0000.2222.3333

- Create VLANs
  vlan 1-1002

- Create the VRF overlay VLAN and configure the vn-segment
  vlan 101
    vn-segment 900001

- Create VLAN and provide mapping to VXLAN
  vlan 1001
    vn-segment 2001001
  vlan 1002
    vn-segment 2001002

- Create VRF and configure VNI
  vrf context vxlan-900001
    vni 900001
rd auto
address-family ipv4 unicast
  route-target import 65535:101 evpn
  route-target export 65535:101 evpn
  route-target import 65535:101
  route-target export 65535:101
address-family ipv6 unicast
  route-target import 65535:101 evpn
  route-target export 65535:101 evpn
  route-target import 65535:101 evpn
  route-target export 65535:101 evpn

• Configure ACL TCAM region for ARP suppression

Note: The **hardware access-list tcam region arp-ether 256 double-wide** command is not needed for Cisco Nexus 9300-EX, 9300-FX, and 9300-FX2 platform switches.

hardware access-list tcam region arp-ether 256 double-wide

• Configure internal control VLAN/SVI for the VRF

interface Vlan101
  no shutdown
  vrf member vxlan-900001
  ip forward

• Create server facing SVI and enable distributed anycast-gateway

interface Vlan1001
  no shutdown
  vrf member vxlan-900001
  ip address 4.1.1.1/24
  ipv6 address 4:1:0:1::1/64
  fabric forwarding mode anycast-gateway

interface Vlan1002
  no shutdown
  vrf member vxlan-900001
  ip address 4.2.2.1/24
  ipv6 address 4:2:0:1::1/64
  fabric forwarding mode anycast-gateway

• Create the network virtualization endpoint (NVE) interface

interface nve1
  no shutdown
  source-interface loopback1
  host-reachability protocol bgp
  member vni 900001 associate-vrf
  member vni 2001001
  mcast-group 239.0.0.1
  member vni 2001002
mcast-group 239.0.0.1

• Configure interfaces for hosts/servers

interface Ethernet1/47
  switchport
  switchport access vlan 1002

interface Ethernet1/48
  switchport
  switchport access vlan 1001

• Configure interfaces for Spine-leaf interconnect

interface Ethernet2/2
  ip address 192.168.4.22/24
  ip pim sparse-mode
  no shutdown

interface Ethernet2/3
  ip address 192.168.2.23/24
  ip pim sparse-mode
  no shutdown

• Configure Loopback for BGP

interface loopback0
  ip address 40.1.1.1/32
  ip pim sparse-mode

• Configure Loopback for local VTEP IP

interface loopback1
  ip address 51.1.1.1/32
  ip pim sparse-mode

• Configure BGP

router bgp 200
  router-id 40.1.1.1
  neighbor 10.1.1.1 remote-as 100
  update-source loopback0
  ebgp-multihop 3
  allowas-in
  send-community extended
  address-family l2vpn
  allowas-in
  send-community extended
  neighbor 20.1.1.1 remote-as 100
  update-source loopback0
  ebgp-multihop 3
  allowas-in
  send-community extended
  address-family l2vpn
  allowas-in
  send-community extended
  vrf vxlan-900001
  advertise l2vpn evpn
**Example of VXLAN BGP EVPN (IBGP)**

An example of a VXLAN BGP EVPN (IBGP):

*Figure 3: VXLAN BGP EVPN Topology (IBGP)*

IBGP between Spine and Leaf

- Spine (9504-A)
  - Enable the EVPN control plane
    
    `nv overlay evpn`
  - Enable the relevant protocols
    
    `feature ospf`
    `feature bgp`
    `feature pim`
  - Configure Loopback for local VTEP IP, and BGP
    
    `interface loopback0`
    `ip address 10.1.1.1/32`
    `ip router ospf 1 area 0.0.0.0`
    `ip pim sparse-mode`
  - Configure Loopback for Anycast RP
interface loopback1
  ip address 100.1.1.1/32
  ip router ospf 1 area 0.0.0.0
  ip pim sparse-mode

• Configure Anycast RP

  ip pim rp-address 100.1.1.1 group-list 224.0.0.0/4
  ip pim ssm range 232.0.0.0/8
  ip pim anycast-rp 100.1.1.1 10.1.1.1
  ip pim anycast-rp 100.1.1.1 20.1.1.1

• Enable OSPF for underlay routing

  router ospf 1

• Configure interfaces for Spine-leaf interconnect

  interface Ethernet4/2
    ip address 192.168.1.42/24
    ip router ospf 1 area 0.0.0.0
    ip pim sparse-mode
    no shutdown

  interface Ethernet4/3
    ip address 192.168.2.43/24
    ip router ospf 1 area 0.0.0.0
    ip pim sparse-mode
    no shutdown

• Configure BGP

  router bgp 65535
  router-id 10.1.1.1
  neighbor 30.1.1.1 remote-as 65535
  update-source loopback0
  address-family l2vpn evpn
  send-community both
  route-reflector-client
  neighbor 40.1.1.1 remote-as 65535
  update-source loopback0
  address-family l2vpn evpn
  send-community both
  route-reflector-client

• Spine (9504-B)
  • Enable the EVVPN control plane and the relevant protocols

    nv overlay evpn
    feature ospf
    feature bgp
    feature pim

• Configure Anycast RP

    ip pim rp-address 100.1.1.1 group-list 224.0.0.0/4
ip pim ssm range 232.0.0.0/8
ip pim anycast-rp 100.1.1.1 10.1.1.1
ip pim anycast-rp 100.1.1.1 20.1.1.1

• Configure interfaces for Spine-leaf interconnect

interface Ethernet4/2
  ip address 192.168.4.42/24
  ip router ospf 1 area 0.0.0.0
  ip pim sparse-mode
  no shutdown

interface Ethernet4/3
  ip address 192.168.3.43/24
  ip router ospf 1 area 0.0.0.0
  ip pim sparse-mode
  no shutdown

• Configure Loopback for local VTEP IP, and BGP

interface loopback0
  ip address 20.1.1.1/32
  ip router ospf 1 area 0.0.0.0
  ip pim sparse-mode

• Configure Loopback for Anycast RP

interface loopback1
  ip address 100.1.1.1/32
  ip router ospf 1 area 0.0.0.0
  ip pim sparse-mode

• Enable OSPF for underlay routing

router ospf 1

• Configure BGP

router bgp 65535
router-id 20.1.1.1
  neighbor 30.1.1.1 remote-as 65535
  update-source loopback0
  address-family l2vpn evpn
    send-community both
    route-reflector-client
  neighbor 40.1.1.1 remote-as 65535
  update-source loopback0
  address-family l2vpn evpn
    send-community both
    route-reflector-client

• Leaf (9396-A)

  • Enable the EVPN control plane

    nv overlay evpn

  • Enable the relevant protocols
feature ospf
feature bgp
feature pim
feature interface-vlan

• Enable VxLAN with distributed anycast-gateway using BGP EVPN

  feature vn-segment-vlan-based
  feature nv overlay
  fabric forwarding anycast-gateway-mac 0000.2222.3333

• Enabling OSPF for underlay routing

    router ospf 1

• Configure Loopback for local VTEP IP, and BGP

    interface loopback0
    ip address 30.1.1.1/32
    ip router ospf 1 area 0.0.0.0
    ip pim sparse-mode

• Configure interfaces for Spine-leaf interconnect

    interface Ethernet2/2
    no switchport
    ip address 192.168.1.22/24
    ip router ospf 1 area 0.0.0.0
    ip pim sparse-mode
    no shutdown

    interface Ethernet2/3
    no switchport
    ip address 192.168.3.23/24
    ip router ospf 1 area 0.0.0.0
    ip pim sparse-mode
    no shutdown

• Configure PIM RP

    ip pim rp-address 100.1.1.1 group-list 224.0.0.0/4
    ip pim ssm range 232.0.0.0/8

• Create VLANs

    vlan 1-1002

• Create overlay VRF VLAN and configure vn-segment

    vlan 101
    vn-segment 900001

• Configure VRF overlay VLAN/SVI for the VRF

    interface Vlan101
    no shutdown
vrf member vxlan-900001
ip forward

• Create VLAN and provide mapping to VXLAN

vlan 1001
  vn-segment 2001001
vlan 1002
  vn-segment 2001002

• Create VRF and configure VNI

vrf context vxlan-900001
  vni 900001
  rd auto
    address-family ipv4 unicast
    route-target both auto
data-family ipv6 unicast
    route-target both auto
data-family ipv6 unicast
data-family ipv6 unicast
    route-target both auto
data-family ipv6 unicast

• Create server facing SVI and enable distributed anycast-gateway

interface Vlan1001
  no shutdown
  vrf member vxlan-900001
  ip address 4.1.1.1/24
  ipv6 address 4:1:0:1::1/64
  fabric forwarding mode anycast-gateway

interface Vlan1002
  no shutdown
  vrf member vxlan-900001
  ip address 4.2.2.1/24
  ipv6 address 4:2:0:1::1/64
  fabric forwarding mode anycast-gateway

• Configure ACL TCAM region for ARP suppression

Note
The hardware access-list tcam region arp-ether 256 double-wide command is not needed for Cisco Nexus 9300-EX, 9300-FX, and 9300-FX2 platform switches.

hardware access-list tcam region arp-ether 256 double-wide

• Create the network virtualization endpoint (NVE) interface

interface nve1
  no shutdown
  source-interface loopback0
  host-reachability protocol bgp
  member vni 900001 associate-vrf
member vni 2001001
   mcast-group 239.0.0.1
member vni 2001002
   mcast-group 239.0.0.1

- Configure interfaces for hosts/servers

   interface Ethernet1/47
   switchport
   switchport access vlan 1002

   interface Ethernet1/48
   switchport
   switchport access vlan 1001

- Configure BGP

   router bgp 65535
   router-id 30.1.1.1
   neighbor 10.1.1.1 remote-as 65535
   update-source loopback0
   address-family l2vpn evpn
   send-community both
   neighbor 20.1.1.1 remote-as 65535
   update-source loopback0
   address-family l2vpn evpn
   send-community both
   vrf vxlan-900001
   address-family ipv4 unicast
   advertise l2vpn evpn

   evpn
   vni 2001001 12
   vni 2001002 12
   rd auto
   route-target import auto
   route-target export auto

- Leaf (9396-B)

  - Enable the EVPN control plane functionality and the relevant protocols

     nv overlay evpn
     feature ospf
     feature bgp
     feature pim
     feature interface-vlan
     feature vn-segment-vlan-based
     feature nv overlay

  - Enable VxLAN with distributed anycast-gateway using BGP EVPN

     fabric forwarding anycast-gateway-mac 0000.2222.3333

  - Configure PIM RP

     ip pim rp-address 100.1.1.1 group-list 224.0.0.0/4
ip pim ssm range 232.0.0.0/8

• Create VLANs
  vlan 1-1002

• Create overlay VRF VLAN and configure vn-segment
  vlan 101
  vn-segment 900001

• Create VLAN and provide mapping to VXLAN
  vlan 1001
  vn-segment 2001001
  vlan 1002
  vn-segment 2001002

• Create VRF and configure VNI
  vrf context vxlan-900001
  vni 900001
  rd auto
  address-family ipv4 unicast
  route-target both auto
  route-target both auto evpn
  address-family ipv6 unicast
  route-target both auto
  route-target both auto evpn

• Configure ACL TCAM region for ARP suppression

  Note  The hardware access-list tcam region arp-ether 256 double-wide command is not needed for Cisco Nexus 9300-EX, 9300-FX, and 9300-FX2 platform switches.

hardware access-list tcam region arp-ether 256 double-wide

• Configure internal control VLAN/SVI for the VRF

  interface Vlan101
  no shutdown
  vrf member vxlan-900001
  ip forward

• Create server facing SVI and enable distributed anycast-gateway

  interface Vlan1001
  no shutdown
  vrf member vxlan-900001
  ip address 4.1.1.1/24
  ipv6 address 4:1:0:1::1/64
fabric forwarding mode anycast-gateway

interface Vlan1002
  no shutdown
  vrf member vxlan-900001
  ip address 4.2.2.1/24
  ipv6 address 4:2:0:1::1/64
  fabric forwarding mode anycast-gateway

• Create the network virtualization endpoint (NVE) interface

interface nve1
  no shutdown
  source-interface loopback0
  host-reachability protocol bgp
  member vni 900001 associate-vrf
  member vni 2001001
  mcast-group 239.0.0.1
  member vni 2001002
  mcast-group 239.0.0.1

• Configure interfaces for hosts/servers

interface Ethernet1/47
  switchport
  switchport access vlan 1002

interface Ethernet1/48
  switchport
  switchport access vlan 1001

• Configure interfaces for Spine-leaf interconnect

interface Ethernet2/2
  no switchport
  ip address 192.168.4.22/24
  ip router ospf 1 area 0.0.0.0
  ip pim sparse-mode
  no shutdown

interface Ethernet2/3
  no switchport
  ip address 192.168.2.23/24
  ip router ospf 1 area 0.0.0.0
  ip pim sparse-mode
  no shutdown

• Configure Loopback for local VTEP IP, and BGP

interface loopback0
  ip address 40.1.1.1/32
  ip router ospf 1 area 0.0.0.0
  ip pim sparse-mode

• Enabling OSPF for underlay routing

router ospf 1
• Configure BGP

```
router bgp 65535
router-id 40.1.1.1
   neighbor 10.1.1.1 remote-as 65535
      update-source loopback0
      address-family l2vpn evpn
         send-community both
   neighbor 20.1.1.1 remote-as 65535
      update-source loopback0
      address-family l2vpn evpn
         send-community both
vrf vxlan-900001
   address-family ipv4 unicast
      advertise l2vpn evpn
evpn
   vni 2001001 l2
      rd auto
      route-target import auto
      route-target export auto
   vni 2001002 l2
      rd auto
      route-target import auto
      route-target export auto
```

Example Show Commands

• show nve peers

```
9396-B# show nve peers
Interface Peer-IP Peer-State
--------- --------------- ----------
nve1 30.1.1.1 Up
```

• show nve vni

```
9396-B# show nve vni
Codes: CP - Control Plane  DP - Data Plane
       UC - Unconfigured  SA - Suppress ARP
Interface VNI Multicast-group State Mode Type [BD/VRF] Flags
--------- --------- ----------------- ----- ---- ------------------ -----
nve1 900001 n/a             Up CP L3 [vxlan-900001] SA
nve1 2001001 225.4.0.1       Up CP L2 [1001] SA
```
• show ip arp suppression-cache detail

Flags: + - Adjacencies synced via CFSoE
    L - Local Adjacency
    R - Remote Adjacency
    L2 - Learnt over L2 interface

<table>
<thead>
<tr>
<th>Ip Address</th>
<th>Age</th>
<th>Mac Address</th>
<th>Vlan</th>
<th>Physical-ifindex</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.1.54</td>
<td>00:06:41</td>
<td>0054.000.000.0000</td>
<td>1001</td>
<td>Ethernet1/48</td>
<td>L</td>
</tr>
<tr>
<td>4.1.1.51</td>
<td>00:20:33</td>
<td>0051.000.000.0000</td>
<td>1001</td>
<td>(null)</td>
<td>R</td>
</tr>
<tr>
<td>4.2.2.53</td>
<td>00:06:41</td>
<td>0053.000.000.0000</td>
<td>1002</td>
<td>Ethernet1/47</td>
<td>L</td>
</tr>
<tr>
<td>4.2.2.52</td>
<td>00:20:33</td>
<td>0052.000.000.0000</td>
<td>1002</td>
<td>(null)</td>
<td>R</td>
</tr>
</tbody>
</table>

• show vxlan interface

<table>
<thead>
<tr>
<th>Interface</th>
<th>Vlan</th>
<th>VPL Ifindex</th>
<th>LTL</th>
<th>HW VP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth1/47</td>
<td>1002</td>
<td>0x4c07d22e</td>
<td></td>
<td>5697</td>
</tr>
<tr>
<td>Eth1/48</td>
<td>1001</td>
<td>0x4c07d02f</td>
<td></td>
<td>5698</td>
</tr>
</tbody>
</table>

• show bgp l2vpn evpn summary

BGP summary information for VRF default, address family L2VPN EVPN
BGP router identifier 40.1.1.1, local AS number 65535
BGP table version is 27, L2VPN EVPN config peers 2, capable peers 2
14 network entries and 18 paths using 2984 bytes of memory
BGP attribute entries [14/2240], BGP AS path entries [0/0]
BGP community entries [0/0], BGP clusterlist entries [2/8]

<table>
<thead>
<tr>
<th>Neighbor</th>
<th>V</th>
<th>AS</th>
<th>MsgRcvd</th>
<th>MsgSent</th>
<th>TblVer</th>
<th>InQ</th>
<th>OutQ</th>
<th>Up/Down</th>
<th>State/PfxRcd</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.1.1</td>
<td>4</td>
<td>65535</td>
<td>30199</td>
<td>30194</td>
<td>27</td>
<td>0</td>
<td>0</td>
<td>2w6d</td>
<td>4</td>
</tr>
<tr>
<td>20.1.1.1</td>
<td>4</td>
<td>65535</td>
<td>30199</td>
<td>30194</td>
<td>27</td>
<td>0</td>
<td>0</td>
<td>2w6d</td>
<td>4</td>
</tr>
</tbody>
</table>

• show bgp l2vpn evpn

BGP routing table information for VRF default, address family L2VPN EVPN
BGP table version is 27, Local Router ID is 40.1.1.1
Status: s-suppressed, x-deleted, S-stale, d-dampened, h-history, *-valid, >-best
Path type: i-internal, e-external, c-confed, l-local, a-aggregate, r-redist, I-injected
Origin codes: i - IGP, e - EGP, ? - incomplete, | - multipath, & - backup

<table>
<thead>
<tr>
<th>Network</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route Distinguisher: 30.1.1.1:33768</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*i&gt;1:2]:[0]:[0]:[48]:[d8b1.9071.e903]:[0]:[0.0.0.0]:216</td>
<td>100</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>*i 30.1.1.1</td>
<td>100</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>*i&gt;1:2]:[0]:[0]:[48]:[d8b1.9071.e903]:[32]:[4.1.1.12]:272</td>
<td>100</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>*i 30.1.1.1</td>
<td>100</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>
Route Distinguisher: 30.1.1.1:33769
*>i[2]:[0]:[0]:[48]:[d8b1.9071.e903]:[0]:[0.0.0.0]/216
  30.1.1.1 100  0 i
*>i[2]:[0]:[0]:[48]:[d8b1.9071.e903]:[32]:[4.2.2.11]/272
  30.1.1.1 100  0 i

Route Distinguisher: 40.1.1.1:33768 (L2VNI 2001001)
*>i[2]:[0]:[0]:[48]:[d8b1.9071.e903]:[0]:[0.0.0.0]/216
  30.1.1.1 100  0 i
*>i[2]:[0]:[0]:[48]:[d8b1.9071.e903]:[32]:[4.2.2.11]/272
  30.1.1.1 100  0 i

Route Distinguisher: 40.1.1.1:33769 (L2VNI 2001002)
*>i[2]:[0]:[0]:[48]:[d8b1.9071.e903]:[0]:[0.0.0.0]/216
  30.1.1.1 100  0 i
*>i[2]:[0]:[0]:[48]:[d8b1.9071.e903]:[32]:[4.2.2.11]/272
  30.1.1.1 100  0 i

Route Distinguisher: 40.1.1.1:3 (L3VNI 900001)
*>i[2]:[0]:[0]:[48]:[d8b1.9071.e903]:[32]:[4.1.1.12]/272
  30.1.1.1 100  0 i
*>i[2]:[0]:[0]:[48]:[d8b1.9071.e903]:[32]:[4.2.2.11]/272
  30.1.1.1 100  0 i

• show l2route evpn mac all

9396-B# show l2route evpn mac all

<table>
<thead>
<tr>
<th>Topology</th>
<th>Mac Address</th>
<th>Prod</th>
<th>Flags</th>
<th>Seq No</th>
<th>Next-Hops</th>
</tr>
</thead>
<tbody>
<tr>
<td>101</td>
<td>6412.2574.9f27 VXLAN</td>
<td>Rmac</td>
<td>0</td>
<td>30.1.1.1</td>
<td></td>
</tr>
<tr>
<td>1001</td>
<td>d8b1.9071.e903 BGF</td>
<td>SpIRcv</td>
<td>0</td>
<td>30.1.1.1</td>
<td></td>
</tr>
<tr>
<td>1001</td>
<td>f8c2.8890.2a45 Local L</td>
<td></td>
<td>0</td>
<td>Eth1/48</td>
<td></td>
</tr>
<tr>
<td>1002</td>
<td>d8b1.9071.e903 BGF</td>
<td>SpIRcv</td>
<td>0</td>
<td>30.1.1.1</td>
<td></td>
</tr>
<tr>
<td>1002</td>
<td>f8c2.8890.2a45 Local L</td>
<td></td>
<td>0</td>
<td>Eth1/47</td>
<td></td>
</tr>
</tbody>
</table>

• show l2route evpn mac-ip all

9396-B# show l2route evpn mac-ip all

<table>
<thead>
<tr>
<th>Topology</th>
<th>Mac Address</th>
<th>Prod</th>
<th>Flags</th>
<th>Seq No</th>
<th>Host IP</th>
<th>Next-Hops</th>
</tr>
</thead>
<tbody>
<tr>
<td>1001</td>
<td>d8b1.9071.e903 BGF</td>
<td></td>
<td>0</td>
<td>4.1.1.12</td>
<td>30.1.1.1</td>
<td></td>
</tr>
<tr>
<td>1001</td>
<td>f8c2.8890.2a45 HMM</td>
<td></td>
<td>0</td>
<td>4.1.1.122</td>
<td>Local</td>
<td></td>
</tr>
<tr>
<td>1002</td>
<td>d8b1.9071.e903 BGF</td>
<td></td>
<td>0</td>
<td>4.2.2.11</td>
<td>30.1.1.1</td>
<td></td>
</tr>
</tbody>
</table>
Example Show Commands

| 1002 | f8c2.8890.2a45 | -- | 0 | 4.2.2.111 | Local |