Configuring VXLAN BGP EVPN

This chapter contains the following sections:

- Information About VXLAN BGP EVPN, on page 1
- Configuring VXLAN BGP EVPN, on page 9
- Verifying the VXLAN BGP EVPN Configuration, on page 19
- Example of VXLAN BGP EVPN (EBGP), on page 20
- Example of VXLAN BGP EVPN (IBGP), on page 31
- Example Show Commands, on page 41
- VXLAN Cross Connect, on page 44

Information About VXLAN BGP EVPN

Guidelines and Limitations for VXLAN BGP EVPN

VXLAN BGP EVPN has the following guidelines and limitations:

- Routing between VXLAN VLANs and non-VXLAN VLANs, and Layer 3 interfaces, is not supported on Cisco Nexus 3100-V. Hence, Cisco Nexus 3100-V cannot be a border leaf VTEP in a VXLAN EVPN setup.

- You can configure EVPN over segment routing or MPLS. See the Cisco Nexus 9000 Series NX-OS Label Switching Configuration Guide, Release 9.x for more information.

- 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 9.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 sub-interfaces as core links are not supported in multisite EVPN.

- 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.

- When Layer 3 EVPN is configured in Cisco Nexus 3000 Series switches that are based on Broadcom ASIC and these switches are added in the topology with Layer 2 EVPN, the routing for this scenario is not supported. When you configure SVI and Layer 3 EVPN in Cisco Nexus 3000 Series switches based on Broadcom ASIC with Anycast Gateway and when you send the ARP requests from a Layer 2 EVPN device (for example, Cisco Nexus 3000 Series switches, based on a Broadcom ASIC), the Cisco Nexus 3000 Series switches can not be used as a gateway for the ARP requests received on the network ports.

- The `show` commands with the `internal` keyword are not supported.

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

- SPAN TX for VXLAN encapsulated traffic is not supported for the Layer 3 uplink interface.

- 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.

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

- 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.

- Non-VXLAN sub-interface VLANs cannot be shared with VXLAN VLANs.

- Subinterfaces on 40G (ALE) uplink ports are not supported on VXLAN VTEPs.

- Point to multipoint Layer 3 and SVI uplinks are not supported. Since both uplink types can only be enabled point-to-point, they cannot span across more than two switches.

- For EBGP, it is recommended to use a single overlay EBGP EVPN session between loopbacks.

- 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.

- 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.

- 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).

- VTEP connected to FEX host interface ports is not supported.

- Resilient hashing (port-channel load-balancing resiliency) and VXLAN configurations are not compatible with VTEPs using ALE uplink ports.
Resilient hashing is disabled by default.

Notes for EVPN Convergence

The following are notes about EVPN Convergence (7.0(3)I3(1) and later):

• As a best practice, the NVE source loopback should be dedicated to NVE, so that NVE can bring the loopback up or down as needed.

• When vPC has been configured, the loopback stays down until the MCT link comes up.

Note

When feature vpc is enabled and there is no VPC configured, the NVE source loopback is in "shutdown" state after an upgrade. In this case, removing feature vpc restores the interface to "up" state.

• The NVE underlay (through the source loopback) is kept down until the overlay has converged.
  • When MCT comes up, the source loopback is kept down for an amount of time that is configurable. This approach prevents north-south traffic from coming in until the overlay has converged.
  • When MCT goes down, NVE is kept up for 30 seconds in the event that there is still south-north traffic from vPC legs which have not yet gone down.

• BGP ignores routes from vPC peer. This reduces the number of routes in BGP.

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 - 2147483647 seconds. The default is 300 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.
• 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 NVE1 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.
  
  **Note** 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:

  ```
  switchch# sh ru int vlan 2
  interface Vlan2
    description special_svi_over_peer-link
    no shutdown
    ip address 30.2.1.1/30
  ```
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.

```bash
switchch# sh ru int vlan 20
interface Vlan20
description backup routing svi for VRF Green
vrf member GREEN
no shutdown
ip address 30.2.10.1/30
```

### 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 needs to be increased by 50 bytes. If the overlays use a 1500-byte MTU, the transport network needs to 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 3000 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 an input for hashing, which achieves the best load-sharing results for VXLAN encapsulated traffic.

- **Multicast Group Scaling**

  The VXLAN implementation on Cisco Nexus 3000 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 amount 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 multiple-tenant 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 IP 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.*

- **When using SVI uplinks with VXLAN enabled on Cisco Nexus 9200 platform switches and Cisco Nexus 9300-EX platform switches, use the `system nve infra-vlans` command to specify the VLANs that are used for uplink SVI. Failing to specify the VLANs results in traffic loss.

---

**Note**

- The `system nve infra-vlans` command specifies VLANs used by all SVI interfaces for uplink and vPC peer-links in VXLAN as infra-VLANs.
- You should not configure certain combinations of infra-VLANs. For example, 2 and 514, 10 and 522, which are 512 apart.

---

**Note**

* Not required for static ingress replication or BGP EVPN ingress replication.
## 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>member vni range [associate-vrf]</td>
<td>Associate VXLAN VNIs (Virtual Network Identifiers) with the NVE interface. The attribute <code>associate-vrf</code> is used to identify and separate processing VNIs that are associated with a VRF and used for routing. <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>show nve vni</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>show nve vni summary</td>
<td></td>
</tr>
<tr>
<td>show bgp l2vpn evpn</td>
<td>Displays the Layer 2 VPN EVPN address family.</td>
</tr>
<tr>
<td>show bgp l2vpn evpn summary</td>
<td></td>
</tr>
<tr>
<td>host-reachability protocol bgp</td>
<td>Specifies BGP as the mechanism for host reachability advertisement.</td>
</tr>
<tr>
<td>suppress-arp</td>
<td>Suppresses ARP under Layer 2 VNI.</td>
</tr>
<tr>
<td>fabric forwarding anycast-gateway-mac</td>
<td>Configures anycast gateway MAC of the switch.</td>
</tr>
<tr>
<td>vrf context</td>
<td>Creates the VRF and enter the VRF mode.</td>
</tr>
<tr>
<td>nv overlay evpn</td>
<td>Enables/Disables the Ethernet VPN (EVPN).</td>
</tr>
<tr>
<td>router bgp</td>
<td>Configures the Border Gateway Protocol (BGP).</td>
</tr>
</tbody>
</table>
Configuring VXLAN BGP EVPN

Enabling VXLAN

Enable VXLAN and the EVPN.

Procedure

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

### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>vlan number</code></td>
<td>Specify VLAN.</td>
</tr>
<tr>
<td></td>
<td><code>vn-segment number</code></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>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>vrf context vxlan</code></td>
<td>Configure the VRF.</td>
</tr>
<tr>
<td></td>
<td><code>vni number</code></td>
<td>Specify VNI.</td>
</tr>
<tr>
<td></td>
<td><code>rd auto</code></td>
<td>Specify VRF RD (route distinguisher).</td>
</tr>
<tr>
<td></td>
<td><code>address-family ipv4 unicast</code></td>
<td>Configure address family for IPv4.</td>
</tr>
</tbody>
</table>

**Step 5** | `route-target both auto` | **Note** Specifying the `auto` option is applicable only for IBGP.

Manually configured route targets are required for EBGP.

**Step 6** | `route-target both auto evpn` | **Note** 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.

**Step 7** | `address-family ipv6 unicast` | Configure address family for IPv6. |

**Step 8** | `route-target both auto` | **Note** 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.
### 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><strong>Step 1</strong></td>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td>vlan number</td>
<td>Specify VLAN</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td>interface vlan-number</td>
<td>Specify VLAN interface.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td>vrf member vxlan-number</td>
<td>Configure SVI for host.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td>ip address address</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><strong>Step 1</strong></td>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td>vlan number</td>
<td>Specify VLAN</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td>vn-segment number</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><strong>Step 1</strong></td>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td>vrf context vxlan</td>
<td>Create a VXLAN Tenant VRF</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td>vni number</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> fabric forwarding anycast-gateway-mac address</td>
<td>Configure distributed gateway virtual MAC address</td>
</tr>
<tr>
<td><strong>Note</strong> One virtual MAC per VTEP</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> All VTEPs should have the same virtual MAC address</td>
<td></td>
</tr>
</tbody>
</table>

**Step 2** fabric forwarding mode anycast-gateway

Associate SVI with anycast gateway under VLAN configuration mode.

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> interface nve-interface</td>
<td>Configure the NVE interface.</td>
</tr>
<tr>
<td><strong>Step 2</strong> host-reachability protocol bgp</td>
<td>This defines BGP as the mechanism for host reachability advertisement</td>
</tr>
<tr>
<td><strong>Step 3</strong> member vni vni associate-vrf</td>
<td>Add Layer-3 VNIs, one per tenant VRF, to the overlay.</td>
</tr>
<tr>
<td><strong>Note</strong> Required for VXLAN routing only.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> global mcast-group ip-address</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> member vni vni</td>
<td>Add Layer 2 VNIs to the tunnel interface.</td>
</tr>
<tr>
<td><strong>Step 6</strong> mcast-group address</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> router bgp number</td>
<td>Configure BGP.</td>
</tr>
<tr>
<td><strong>Step 2</strong> router-id address</td>
<td>Specify router address.</td>
</tr>
</tbody>
</table>
Configuring VXLAN BGP EVPN

Configuring RD and Route Targets for VXLAN Bridging

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>evpn</td>
</tr>
<tr>
<td>Step 2</td>
<td>vni number 12</td>
</tr>
<tr>
<td>Note</td>
<td>Only Layer 2 VNI s need to be specified.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Step 3 rd auto</td>
<td>Define VRF RD (route distinguisher) to configure VRF context.</td>
</tr>
<tr>
<td>Step 4 route-target import auto</td>
<td>Define VRF Route Target and import policies.</td>
</tr>
<tr>
<td>Step 5 route-target export auto</td>
<td>Define VRF Route Target and export policies.</td>
</tr>
</tbody>
</table>

**Configuring BGP for EVPN on the Spine**

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 route-map permit all permit 10 | Configure route-map.  
  **Note** The route-map keeps the next-hop unchanged for EVPN routes.  
  • Required for eBGP.  
  • Optional for iBGP. |
| Step 2 set ip next-hop unchanged | Set next-hop address.  
  **Note** The route-map keeps the next-hop unchanged for EVPN routes.  
  • Required for eBGP.  
  • Optional for iBGP.  
  **Note** When two next hops are enabled, next hop ordering is not maintained.  
  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. |
| Step 3 router bgp autonomous system number | Specify BGP. |
| Step 4 address-family l2vpn evpn | Configure address family Layer 2 VPN EVPN under the BGP neighbor. |
| Step 5 retain route-target all | Configure retain route-target all under address-family Layer 2 VPN EVPN [global]. |
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong> neighbor <em>address remote-as number</em></td>
<td>Define neighbor.</td>
</tr>
<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.

#### 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. <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><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 <em>vni-id</em></td>
<td>Specify VNI ID.</td>
</tr>
<tr>
<td><strong>Step 4</strong> suppress-arp</td>
<td>Configure to suppress ARP under Layer 2 VNI.</td>
</tr>
</tbody>
</table>
Disabling VXLANs

Procedure

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

2017 Jul 5 10:27:34 leaf %$ VDC-1 %$ %USER-2-SYSTEM_MSG: Unfreeze limit (3) hit, MAC
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>
</table>
| switch(config)# fabric forwarding ? dup-host-ip-addr-detection | Available sub-commands:  
  - Anycast gateway MAC of the switch.  
  - To detect duplicate host addresses in n seconds. |
| switch(config)# fabric forwarding dup-host-ip-addr-detection ? <1-1000> | The number of host moves allowed in n seconds. The range is 1 to 1000 moves; default is 5 moves. |
| switch(config)# fabric forwarding dup-host-ip-addr-detection 100 ? <2-36000> | The duplicate detection timeout in seconds for the number of host moves. The range is 2 to 36000 seconds; default is 180 seconds. |
| switch(config)# fabric forwarding dup-host-ip-addr-detection 100 10 | Detects duplicate host addresses (limited to 100 moves) in a period of 10 seconds. |

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>
</table>
| switch(config)# l2rib dup-host-mac-detection ? <1-1000> default | Available sub-commands for L2RIB:  
  - The number of host moves allowed in n seconds. The range is 1 to 1000 moves.  
  - Default setting (5 moves in 180 in seconds). |
| switch(config)# l2rib dup-host-mac-detection 100 ? <2-36000> | The duplicate detection timeout in seconds for the number of host moves. The range is 2 to 36000 seconds; default is 180 seconds. |
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>nuage controller interop</td>
<td>Global command to enable interoperability mode.</td>
</tr>
<tr>
<td>2</td>
<td>router bgp number</td>
<td>Configure BGP.</td>
</tr>
<tr>
<td>3</td>
<td>address-family l2vpn evpn</td>
<td>Configure address family Layer 2 VPN EVPN under the BGP neighbor.</td>
</tr>
<tr>
<td>4</td>
<td>advertise-system-mac</td>
<td>Enable Nuage interoperability mode for BGP.</td>
</tr>
<tr>
<td>5</td>
<td>allow-vni-in-ethertag</td>
<td>Enable Nuage interoperability mode for BGP.</td>
</tr>
<tr>
<td>6</td>
<td>route-map permitall permit 10</td>
<td>Configure route-map to permit all.</td>
</tr>
<tr>
<td>7</td>
<td>router bgp number</td>
<td>Configure BGP.</td>
</tr>
<tr>
<td>8</td>
<td>vrf vrf-name</td>
<td>Specify tenant VRF.</td>
</tr>
<tr>
<td>9</td>
<td>address-family ipv4 unicast</td>
<td>Configure address family for IPv4.</td>
</tr>
<tr>
<td>10</td>
<td>advertise l2vpn evpn</td>
<td>Enable advertising EVPN routes.</td>
</tr>
<tr>
<td>11</td>
<td>redistribute hmm route-map permitall</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)# route-map permitall permit 10
```
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>show nve vrf</td>
<td>Displays VRFs and associated VNIs</td>
</tr>
<tr>
<td>show bgp l2vpn evpn</td>
<td>Displays routing table information.</td>
</tr>
<tr>
<td>show ip arp suppression-cache [detail</td>
<td>summary</td>
</tr>
<tr>
<td>show vxlan interface</td>
<td>Displays VXLAN interface status.</td>
</tr>
<tr>
<td>show vxlan interface</td>
<td>count</td>
</tr>
</tbody>
</table>

**Note**

A VP is allocated on a per-port per-VLAN basis. The sum of all VPs across all VXLAN-enabled Layer 2 ports gives the total logical port VP count. For example, if there are 10 Layer 2 trunk interfaces, each with 10 VXLAN VLANS, then the total VXLAN VLAN logical port VP count is 10*10 = 100.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show l2route evpn mac [all</td>
<td>evi evi [bgp</td>
</tr>
<tr>
<td>show l2route evpn fl all</td>
<td>Displays all fl routes.</td>
</tr>
<tr>
<td>show l2route evpn imet all</td>
<td>Displays all imet routes.</td>
</tr>
<tr>
<td>show l2route evpn mac-ip all</td>
<td>Displays all MAC IP routes.</td>
</tr>
<tr>
<td>show l2route evpn mac-ip all detail</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 1: 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 local VTEP IP, and 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 225.0.0.0/8
ip pim rp-candidate loopback1 group-list 225.0.0.0/8
ip pim log-neighbor-changes
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
    next-hop 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

    feature telnet
    feature nxapi
    feature bash-shell
    feature scp-server
    nv overlay evpn
    feature bgp
    feature pim
    feature lldp

  • Configure Anycast RP

    ip pim rp-address 100.1.1.1 group-list 225.0.0.0/8
    ip pim rp-candidate loopback1 group-list 225.0.0.0/8
    ip pim log-neighbor-changes
    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
    vlan 1-1002
    route-map permitall permit 10
      set ip next-hop unchanged

  • Configure interfaces for Spine-leaf interconnect

    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 local VTEP IP, and BGP

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

  • Configure Loopback for Anycast RP

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

  • Configure the BGP overlay for the EVPN address family.

    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 permit all out
neighbor 40.1.1.1 remote-as 200
ebgp-multihop 3
address-family l2vpn evpn
disable-peer-as-check
send-community extended
route-map permit all out

• 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
  feature dhcp

• Configure DHCP relay for Tenant VRFs

  service dhcp
  ip dhcp relay
  ip dhcp relay information option
  ip dhcp relay sub-option type cisco
  ip dhcp relay information option vpn

• 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 225.0.0.0/8

• 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
  no switchport
  load-interval counter 1 5
  ip address 192.168.1.22/24
  ip pim sparse-mode
  no shutdown

interface Ethernet2/3
  no switchport
  load-interval counter 1 5
  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

Note: The `rd auto` and `route-target` commands are automatically configured unless one or more are entered as overrides.

rd auto
address-family ipv4 unicast
  route-target import 65535:101 evpn
  route-target export 65535:101 evpn
  route-target import 65535:101
deroute-target export 65535:101
daddress-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
ip dhcp relay address 192.168.100.1 use-vrf default

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

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

Note
You can choose either of the following two options for creating the NVE interface. Use the first option for a small number of VNIs. Use the second option to configure a large number of VNIs.

Create the network virtualization endpoint (NVE) interface

Option 1

interface nve1
no shutdown
source-interface loopback1
host-reachability protocol bgp
member vni 900001 associate-vrf
member vni 2001001 suppress-arp
mcast-group 225.4.0.1
member vni 2001002 suppress-arp
mcast-group 225.4.0.1

Option 2

interface nve1
no shutdown
source-interface loopback 1
host-reachability protocol bgp
global suppress-arp
global mcast-group 224.1.1.1 L3
global mcast-group 255.1.1.1 L2
member vni 10000 associate-vrf
member vni 10001 associate-vrf
member vni 10002 associate-vrf
member vni 10003 associate-vrf
member vni 10004 associate-vrf
member vni 10005 associate-vrf
member vni 20000
member vni 20001
member vni 20002
member vni 20003
member vni 20004
member vni 20005

• Configure interfaces for hosts/servers.

interface Ethernet1/47
  switchport access vlan 1002
interface Ethernet1/48
  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

---

**Note**
The following commands in EVPN mode do not need to be entered.

evpn
  vni 2001001 12
  vni 2001002 12

---

**Note**
The *rd auto* and *route-target auto* commands are automatically configured unless one or more are entered as overrides.

rd auto
  route-target import auto
  route-target export auto
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

---

**Note** The following `advertise` command is optional.

advertise l2vpn evpn

evpn
    vni 2001001 12
    vni 2001002 12

---

**Note** The following `rd auto` and `route-target` commands are automatically configured unless one or more are entered as overrides.

**Note** The following EVPN mode commands are optional.

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

  feature telnet
feature nxapi
feature bash-shell
feature scp-server
nv overlay evpn
feature bgp
feature pim
feature interface-vlan
feature vn-segment-vlan-based
feature lldp
feature nv overlay

- Enable VxLAN with distributed anycast-gateway using BGP EVPN

fabric forwarding anycast-gateway-mac 0000.2222.3333

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

  vlan 1-1002
  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


\[\text{Note}\] The following commands are automatically configured unless one or more are entered as overrides.

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

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

- Configure internal control VLAN/SVI for the VRF

  interface Vlan1
• Create server facing SVI and enable distributed anycast-gateway

interface Vlan101
  no shutdown
  vrf member vxlan-900001

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

Note: You can choose either of the following two procedures for creating the NVE interface. Use Option 1 for a small number of VNIs. Use Option 2 to configure a large number of VNIs.

Option 1

interface nve1
  no shutdown
  source-interface loopback1
  host-reachability protocol bgp
  member vni 10000 associate-vrf
  mcast-group 224.1.1.1
  member vni 10001 associate-vrf
  mcast-group 224.1.1.1
  member vni 20000 suppress-arp
  mcast-group 225.1.1.1
  member vni 20001 suppress-arp
  mcast-group 225.1.1.1

Option 2

interface nve1
  no shutdown
  source-interface loopback 1
  host-reachability protocol bgp
global suppress-arp
global mcast-group 224.1.1.1 L3
global mcast-group 255.1.1.1 L2
  member vni 10000 associate-vrf
  member vni 10001 associate-vrf
  member vni 10002 associate-vrf
  member vni 10003 associate-vrf
  member vni 10004 associate-vrf
member vni 10005 associate-vrf
member vni 20000
member vni 20001
member vni 20002
member vni 20003
member vni 20004
member vni 20005

• Configure interfaces for hosts/servers

  interface Ethernet1/47
    switchport access vlan 1002
  interface Ethernet1/48
    switchport access vlan 1001

• Configure interfaces for Spine-leaf interconnect

  interface Ethernet2/1
  interface Ethernet2/2
    no switchport
    load-interval counter 1 5
    ip address 192.168.4.22/24
    ip pim sparse-mode
    no shutdown
  interface Ethernet2/3
    no switchport
    load-interval counter 1 5
    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

---

Note
The following `advertise` command is optional.

`advertise l2vpn evpn`

---

Note
The `rd auto` and `route-target` commands are optional unless you want to use them to override the `import` or `export` options.

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

---

**Example of VXLAN BGP EVPN (IBGP)**

An example of a VXLAN BGP EVPN (IBGP):
IBGP between Spine and Leaf

- Spine (9504-A)
  - Enable the EVPN control plane
    
    \[ \text{nv overlay evpn} \]
  - Enable the relevant protocols
    
    \[
    \begin{align*}
    & \text{feature ospf} \\
    & \text{feature bgp} \\
    & \text{feature pim}
    \end{align*}
    \]
  - Configure Loopback for local VTEP IP, and BGP
    
    \[
    \begin{align*}
    & \text{interface loopback0} \\
    & \quad \text{ip address 10.1.1.1/32} \\
    & \quad \text{ip router ospf 1 area 0.0.0.0} \\
    & \quad \text{ip pim sparse-mode}
    \end{align*}
    \]

- Configure Loopback for Anycast RP
  
  \[
  \begin{align*}
  & \text{interface loopback1} \\
  & \quad \text{ip address 100.1.1.1/32} \\
  & \quad \text{ip router ospf 1 area 0.0.0.0} \\
  & \quad \text{ip pim sparse-mode}
  \end{align*}
  \]
• Configure Anycast RP

  ip pim rp-address 100.1.1.1 group-list 225.0.0.0/8  
ip pim rp-candidate loopback1 group-list 225.0.0.0/8  
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 EVPN control plane and the relevant protocols

  feature telnet  
  feature nxapi  
  feature bash-shell  
  feature scp-server  
  nv overlay evpn  
  feature ospf  
  feature bgp  
  feature pim  
  feature lldp

• Configure Anycast RP

  ip pim rp-address 100.1.1.1 group-list 225.0.0.0/8  
ip pim rp-candidate loopback1 group-list 225.0.0.0/8
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
vlan 1-1002

• 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 225.0.0.0/8
    ip pim ssm range 232.0.0.0/8

• 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

• 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

Note The rd auto and route-target commands are automatically configured unless one or more are entered as overrides.

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

• 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

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

Note You can choose either of the following two procedures for creating the NVE interfaces. Use the first one for a small number of VNIs. Use the second procedure to configure a large number of VNIs.

Create the network virtualization endpoint (NVE) interface

Option 1

interface nve1
  no shutdown
source-interface loopback0
host-reachability protocol bgp
member vni 900001 associate-vrf
member vni 2001001
  suppress-arp
  mcast-group 225.4.0.1
member vni 2001002
  suppress-arp
  mcast-group 225.4.0.1

Option 2

Interface nve1
source-interface loopback 1
host-reachability protocol bgp
global suppress-arp
global mcast-group 255.1.1.1 L2
global mcast-group 255.1.1.2 L3
member vni 10000
member vni 20000
member vni 30000

• Configure interfaces for hosts/servers

  interface Ethernet1/47
    switchport access vlan 1002

  interface Ethernet1/48
    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

---

**Note**  
The following commands in EVPN mode do not need to be entered.

evpn
  vni 2001001 12
  vni 2001002 12

---

**Note**  
The `rd auto` and `route-target auto` commands are automatically configured unless one or more are entered as overrides.
The `rd auto` and `route-target` commands are automatically configured unless you want to use them to override the `import` or `export` options.

The following EVPN mode commands are optional.

evpn
  vni 2001001 12
  rd auto
  route-target import auto
  route-target export auto
  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
    
    feature telnet
    feature nxapi
    feature bash-shell
    feature scp-server
    nv overlay evpn
    feature ospf
    feature bgp
    feature pim
    feature interface-vlan
    feature vn-segment-vlan-based
    feature lldp
    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 225.0.0.0/8
    ip pim ssm range 232.0.0.0/8

  - Create overlay VRF VLAN and configure vn-segment
    
    vlan 1-1002
    vlan 101
    vn-segment 900001

  - Create VLAN and provide mapping to VXLAN
• Create VRF and configure VNI

vrf context vxlan-900001
  vni 900001

**Note** The *rd auto* and *route-target* commands are automatically configured unless you want to use them to override the *import* or *export* options.

```plaintext
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

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

• Configure internal control VLAN/SVI for the VRF

```plaintext
interface Vlan101
  no shutdown
  vrf member vxlan-900001
```

• Create server facing SVI and enable distributed anycast-gateway

```plaintext
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
```

**Note** You can choose either of the following two command procedures for creating the NVE interfaces. Use Option 1 for a small number of VNIs. Use Option 2 to configure a large number of VNIs.
Create the network virtualization endpoint (NVE) interface

Option 1

interface nve1
    no shutdown
    source-interface loopback0
    host-reachability protocol bgp
    member vni 900001 associate-vrf
    member vni 2001001
        suppress-arp
        mcast-group 225.4.0.1
    member vni 2001002
        suppress-arp
        mcast-group 225.4.0.1

Option 2

interface nve1
    source-interface loopback0
    host-reachability protocol bgp
    global suppress-arp
    global mcast-group 255.4.0.1
    member vni 900001
    member vni 2001001

• Configure interfaces for hosts/servers

    interface Ethernet1/47
        switchport access vlan 1002

    interface Ethernet1/48
        switchport access vlan 1001

• Configure interfaces for Spine-leaf interconnect

    interface Ethernet2/1

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

Note
The rd auto and route-target commands are optional unless you want to use them to override the import or export options.

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

<table>
<thead>
<tr>
<th>Interface</th>
<th>VNI</th>
<th>Multicast-group</th>
<th>State</th>
<th>Mode</th>
<th>Type [BD/VRF]</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>nve1</td>
<td>900001</td>
<td>n/a</td>
<td>Up</td>
<td>CP</td>
<td>L3 [vxlan-900001]</td>
<td></td>
</tr>
<tr>
<td>nve1</td>
<td>2001001</td>
<td>225.4.0.1</td>
<td>Up</td>
<td>CP</td>
<td>L2 [1001]</td>
<td>SA</td>
</tr>
<tr>
<td>nve1</td>
<td>2001002</td>
<td>225.4.0.1</td>
<td>Up</td>
<td>CP</td>
<td>L2 [1002]</td>
<td>SA</td>
</tr>
</tbody>
</table>

• show ip arp suppression-cache detail

9396-B# 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>0054.0000.0000</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>0051.0000.0000</td>
<td>1001</td>
<td>(null)</td>
<td>R</td>
</tr>
<tr>
<td>4.2.2.53</td>
<td>00:06:41</td>
<td>0053.0000.0000</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>0052.0000.0000</td>
<td>1002</td>
<td>(null)</td>
<td>R</td>
</tr>
</tbody>
</table>

• show vxlan interface

9396-B# 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>0x10000</td>
<td>5697</td>
</tr>
<tr>
<td>Eth1/48</td>
<td>1001</td>
<td>0x4c07d02f</td>
<td>0x10001</td>
<td>5698</td>
</tr>
</tbody>
</table>

• show bgp l2vpn evpn summary

9396-B# 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
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>A5</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

9396-B# 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-i
jected
Origin codes: i - IGP, e - EGP, ? - incomplete, | - multipath, & - backup

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Route Distinguisher: 30.1.1.1:33768
Route Distinguisher: 30.1.1.1:33769

Route Distinguisher: 40.1.1.1:33768 (L2VNI 2001001)

Route Distinguisher: 40.1.1.1:33769 (L2VNI 2001002)

Route Distinguisher: 40.1.1.1:3 (L3VNI 900001)

**show l2route evpn 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 BGP</td>
<td>SplRcv</td>
<td>0</td>
<td>30.1.1.1</td>
<td></td>
</tr>
<tr>
<td>1001</td>
<td>f8c2.8890.2a45 Local</td>
<td>L</td>
<td>0</td>
<td>Eth1/48</td>
<td></td>
</tr>
<tr>
<td>1002</td>
<td>d8b1.9071.e903 BGP</td>
<td>SplRcv</td>
<td>0</td>
<td>30.1.1.1</td>
<td></td>
</tr>
<tr>
<td>1002</td>
<td>f8c2.8890.2a45 Local</td>
<td>L</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

Flags -(Rmac):Router MAC (Stt):Static (L):Local (R):Remote (V):vPC link
VXLAN Cross Connect

About VXLAN Cross Connect

This feature provides point-to-point tunneling of data and control packet from one VTEP to another. Every attachment circuit will be part of a unique provider VNI. BGP EVPN signaling will discover these end-points based on how the provider VNI is stretched in the fabric. All inner customer.1q tags will be preserved, as is, and packets will be encapsulated in the provider VNI at the encapsulation VTEP. On the decapsulation end-point, the provider VNI will forward the packet to its attachment circuit while preserving all customer.1q tags in the packets.

Note

Cross Connect and xconnect are synonymous.

VXLAN Cross Connect enables VXLAN point-to-point functionality on the following switches:

- Cisco Nexus 9332PQ
- Cisco Nexus 9336C-FX2
- Cisco Nexus 9372PX
- Cisco Nexus 9372PX-E
- Cisco Nexus 9372TX
- Cisco Nexus 9372TX-E
- Cisco Nexus 93120TX
- Cisco Nexus 93108TC-EX
- Cisco Nexus 93108TC-FX
- Cisco Nexus 93180LC-EX
- Cisco Nexus 93180YC-EX
- Cisco Nexus 93180YC-FX
- Cisco Nexus 93240YC-FX2

VXLAN Cross Connect enables tunneling of all control frames (CDP, LLDP, LACP, STP, BFD, and PAGP) and data across the VXLAN cloud.
Guidelines and Limitations for VXLAN Cross Connect

VXLAN Cross Connect has the following guidelines and limitations:

- When an upgrade is performed non-disruptively from Cisco NX-OS Release 7.0(3)I7(4) to Cisco NX-OS Release 9.2(x) code, and if a VLAN is created and configured as xconnect, you must enter the `copy running-config startup-config` command and reload the switch. If the box was upgraded disruptively to Cisco NX-OS Release 9.2(x) code, a reload is not needed on configuring a VLAN as xconnect.

- MAC learning will be disabled on the xconnect VNIs and none of the host MAC will be learned on the tunnel access ports.

- Only supported on a BGP EVPN topology.

- LACP bundling of attachment circuits is not supported.

- Only one attachment circuit can be configured for a provider VNI on a given VTEP.

- A VNI can only be stretched in a point-to-point fashion. Point-to-multipoint is not supported.

- SVI on an xconnect VLAN is not supported.

- ARP suppression is not supported on an xconnect VLAN VNI.

- Xconnect is not supported on the following switches:
  - Cisco Nexus 9504
  - Cisco Nexus 9508
  - Cisco Nexus 9516

- Scale of xconnect VLANs depends on the number of ports available on the switch. Every xconnect VLAN can tunnel all 4k customer VLANs.

- Xconnect or Crossconnect feature on vpc-vtep needs backup-svi as native VLAN on the vPC peer-link.

- Make sure that the NGOAM xconnect hb-interval is set to 5000 milliseconds on all VTEPs before attempting ISSU/patch activation to avoid link flaps.

- Before activating the patch for the cfs process, you must move the NGOAM xconnect hb-interval to the maximum value of 5000 milliseconds. This prevents interface flaps during the patch activation.

- The vPC orphan tunneled port per VNI should be either on the vPC primary switch or secondary switch, but not both.

- Configuring a static MAC on xconnect tunnel interfaces is not supported.

- xconnect is not supported on FEX ports.

- On vpc-vtep, spanning tree must be disabled on both vPC peers for xconnect VLANs.

- Xconnect access ports need to be flapped after disabling NGOAM on all the VTEPs.

- After deleting and adding a VLAN, or removing xconnect from a VLAN, physical ports need to be flapped with NGOAM.
# Configuring VXLAN Cross Connect

This procedure describes how to configure the VXLAN Cross Connect feature.

## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>vlan vlan-id</code></td>
<td>Specifies VLAN.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>switch(config)# vlan 10</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>vn-segment vnid</code></td>
<td>Specifies VXLAN VNID (Virtual Network Identifier).</td>
</tr>
<tr>
<td></td>
<td>Example: <code>switch(config-vlan)# vn-segment 10010</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>xconnect</code></td>
<td>Defines the provider VLAN with the attached VNI to be in cross connect mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>switch(config-vlan)# xconnect</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>exit</code></td>
<td>Exits command mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>switch(config-vlan)# exit</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>interface type port</code></td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>switch(config)# interface ethernet 1/1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><code>switchport mode dot1q-tunnel</code></td>
<td>Creates a 802.1q tunnel on the port. The port will do down and reinitialize (port flap) when the interface mode is changed. BPDU filtering is enabled and CDP is disabled on tunnel interfaces.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>switch(config-if)# switchport mode dot1q-tunnel</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><code>switchport access vlan vlan-id</code></td>
<td>Sets the interface access VLAN.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>switch(config-if)# switchport access vlan 10</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><code>exit</code></td>
<td>Exits command mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>switch(config-vlan)# exit</code></td>
<td></td>
</tr>
</tbody>
</table>
Example

switch# configure terminal
switch(config)# vlan 10
switch(config)# vn-segment 10010
switch(config)# xconnect
switch(config)# vlan 20
switch(config)# vn-segment 10020
switch(config)# xconnect
switch(config)# vlan 30
switch(config)# vn-segment 10030
switch(config)# xconnect

This example shows how to configure access ports:

switch# configure terminal
switch(config)# interface ethernet1/1
switch(config-if)# switchport mode dot1q-tunnel
switch(config-if)# switchport access vlan 10
switch(config-if)# exit
switch(config)# interface ethernet1/2
switch(config-if)# switchport mode dot1q-tunnel
switch(config-if)# switchport access vlan 20
switch(config-if)# exit
switch(config)# interface ethernet1/3
switch(config-if)# switchport mode dot1q-tunnel
switch(config-if)# switchport access vlan 30

Verifying VXLAN Cross Connect Configuration

To display the status for the VXLAN Cross Connect configuration, enter one of the following commands:

Table 1: Display VXLAN Cross Connect Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config vlan session-num</td>
<td>Displays VLAN information.</td>
</tr>
<tr>
<td>show nve vni</td>
<td>Displays VXLAN VNI status.</td>
</tr>
<tr>
<td>show nve vni session-num</td>
<td>Displays VXLAN VNI status per VNI.</td>
</tr>
</tbody>
</table>

Example of the show run vlan 503 command:

switch(config)# sh run vlan 503

!Command: show running-config vlan 503
!Running configuration last done at: Mon Jul 9 13:46:03 2018
!Time: Tue Jul 10 14:12:04 2018

version 9.2(1) Bios:version 07.64
vlan 503
vlan 503
  vn-segment 5503
  xconnect
Example of the `show nve vni 5503` command:

```bash
switch(config)# sh nve vni 5503
Codes: CP - Control Plane  DP - Data Plane 
       UC - Unconfigured  SA - Suppress ARP 
       SU - Suppress Unknown Unicast

<table>
<thead>
<tr>
<th>Interface</th>
<th>VNI</th>
<th>Multicast-group</th>
<th>State</th>
<th>Mode</th>
<th>Type</th>
<th>[BD/VRF]</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>nve1</td>
<td>5503</td>
<td>225.5.0.3</td>
<td>Up</td>
<td>CP</td>
<td>L2</td>
<td>[503]</td>
<td>SA</td>
</tr>
</tbody>
</table>
```

Example of the `show nve vni` command:

```bash
switch(config)# sh nve vni
Codes: CP - Control Plane  DP - Data Plane 
       UC - Unconfigured  SA - Suppress ARP 
       SU - Suppress Unknown Unicast

<table>
<thead>
<tr>
<th>Interface</th>
<th>VNI</th>
<th>Multicast-group</th>
<th>State</th>
<th>Mode</th>
<th>Type</th>
<th>[BD/VRF]</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>nve1</td>
<td>5501</td>
<td>225.5.0.1</td>
<td>Up</td>
<td>CP</td>
<td>L2</td>
<td>[501]</td>
<td>SA</td>
</tr>
<tr>
<td>nve1</td>
<td>5502</td>
<td>225.5.0.2</td>
<td>Up</td>
<td>CP</td>
<td>L2</td>
<td>[502]</td>
<td>SA</td>
</tr>
<tr>
<td>nve1</td>
<td>5503</td>
<td>225.5.0.3</td>
<td>Up</td>
<td>CP</td>
<td>L2</td>
<td>[503]</td>
<td>SA</td>
</tr>
<tr>
<td>nve1</td>
<td>5504</td>
<td>UnicastBGP</td>
<td>Up</td>
<td>CP</td>
<td>L2</td>
<td>[504]</td>
<td>SA</td>
</tr>
<tr>
<td>nve1</td>
<td>5505</td>
<td>225.5.0.5</td>
<td>Up</td>
<td>CP</td>
<td>L2</td>
<td>[505]</td>
<td>SA</td>
</tr>
<tr>
<td>nve1</td>
<td>5506</td>
<td>UnicastBGP</td>
<td>Up</td>
<td>CP</td>
<td>L2</td>
<td>[506]</td>
<td>SA</td>
</tr>
<tr>
<td>nve1</td>
<td>5507</td>
<td>225.5.0.7</td>
<td>Up</td>
<td>CP</td>
<td>L2</td>
<td>[507]</td>
<td>SA</td>
</tr>
<tr>
<td>nve1</td>
<td>5510</td>
<td>225.5.0.10</td>
<td>Up</td>
<td>CP</td>
<td>L2</td>
<td>[510]</td>
<td>SA</td>
</tr>
<tr>
<td>nve1</td>
<td>5511</td>
<td>225.5.0.11</td>
<td>Up</td>
<td>CP</td>
<td>L2</td>
<td>[511]</td>
<td>SA</td>
</tr>
<tr>
<td>nve1</td>
<td>5512</td>
<td>225.5.0.12</td>
<td>Up</td>
<td>CP</td>
<td>L2</td>
<td>[512]</td>
<td>SA</td>
</tr>
<tr>
<td>nve1</td>
<td>5513</td>
<td>UnicastBGP</td>
<td>Up</td>
<td>CP</td>
<td>L2</td>
<td>[513]</td>
<td>SA</td>
</tr>
<tr>
<td>nve1</td>
<td>5514</td>
<td>225.5.0.14</td>
<td>Up</td>
<td>CP</td>
<td>L2</td>
<td>[514]</td>
<td>SA</td>
</tr>
<tr>
<td>nve1</td>
<td>5515</td>
<td>UnicastBGP</td>
<td>Up</td>
<td>CP</td>
<td>L2</td>
<td>[515]</td>
<td>SA</td>
</tr>
<tr>
<td>nve1</td>
<td>5516</td>
<td>UnicastBGP</td>
<td>Up</td>
<td>CP</td>
<td>L2</td>
<td>[516]</td>
<td>SA</td>
</tr>
<tr>
<td>nve1</td>
<td>5517</td>
<td>UnicastBGP</td>
<td>Up</td>
<td>CP</td>
<td>L2</td>
<td>[517]</td>
<td>SA</td>
</tr>
<tr>
<td>nve1</td>
<td>5518</td>
<td>UnicastBGP</td>
<td>Up</td>
<td>CP</td>
<td>L2</td>
<td>[518]</td>
<td>SA</td>
</tr>
</tbody>
</table>
```