Configure EVPN VXLAN for ZT-LAN

For supported software information, click here.

You can configure virtual extensible LAN (VXLAN) on Versa Operating System™ (VOS™) devices. VXLAN is a data plane encapsulation protocol that allows you to run Layer 2 Ethernet VPN (EVPN) over a Layer 3 IP network using standard VXLAN encapsulation over UDP. In multitenant and cloud environments, VXLAN allows a network to handle much larger traffic loads than traditional VLANs while providing the same traffic isolation and segmentation as classic VLANs.

For more information about EVPN, see RFC 7432, BGP MPLS-Based Ethernet VPN.

For more information about EVPN VXLAN, see RFC 8365, A Network Virtualization Overlay Solution Using Ethernet VPN (EVPN).

Note: The terminology in this document aligns with that used in the RFCs. The RFCs define EVPNs that are provided as part of a service with provider edge (PE) routers and customer edge (CE) devices. For ZT-LAN, EVPN is defined as an overlay that exists between leaf and spine devices that have VXLAN tunnel endpoints (VTEPs).

Overview

VXLAN works in both the control plane and the data plane.

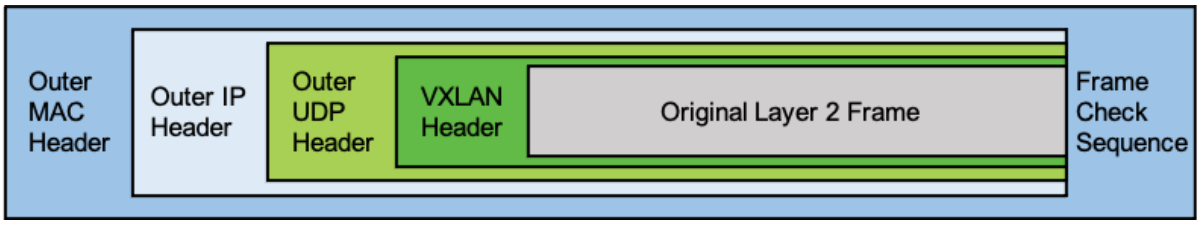
In the control plane, Multiprotocol BGP (MP-BGP), which supports the Layer 2 VPN Address Family Identifier (AFI) and the EVPN Subsequent Address Family Identifier (SAFI), allows a ZT-LAN controller to distribute MAC addresses and IP routing information to another ZT-LAN device.

In the data plane, the Layer 2 MAC frame is encapsulated in an 8-byte VXLAN header with a 24-bit VXLAN network identifier (VNI) that designates the individual VXLAN overlay network, the UDP protocol (port 4789), and the outer IP address (destination/source IP addresses of the tunnel endpoint), thus providing a way to reach the destination MAC address.

VXLAN encapsulation and decapsulation is performed at VTEPs. There is one VTEP at the origin of a VXLAN tunnel and a second VTEP at the termination point of the tunnel. A VTEP can be a physical or virtual end host or a network device, such as a router or switch.

A VXLAN packet has the following format, which is illustrated in the following figure:

- Outer MAC header—14 bytes (4 optional)
- Outer IP header—20 bytes
- Outer UDP header—8 bytes
- VXLAN header—8 bytes



VLAN-to-VXLAN Mapping

To map a VLAN to a VXLAN, a regular VLAN is mapped to a unique 24-bit VXLAN network identifier (VNI) ID so that it can be used throughout a network. The VNI ID is specified as part of the bridge domain configuration. In addition to the regular BGP control plane information, such as the route distinguisher (RD) and the route target (RT), the local MAC addresses that belong to a bridge domain on a ZT-LAN device are distributed to other ZT-LAN devices by attaching the VNI to the MAC routes in the control plane. Using the route distinguisher, VNI, and route target, the MAC addresses are imported into the correct MAC-VRF (routing instance) and bridge domain. A MAC-VRF is a VRF table for installing MAC addresses on a ZT-LAN device for a tenant.

Note: For EVPN multihoming, the BGP EVPN route distinguisher should be different for VTEP endpoints that have the same ESI values.

When a MAC frame is destined to a remote MAC address in a MAC-VRF and bridge domain, it is encapsulated with the correct VNI ID in the VXLAN header. The receiving ZT-LAN device uses the VNI ID to look up the correct MAC-VRF and bridge domain, and then the MAC address is forwarded to the correct local interface in the MAC-VRF.

Although published standards allow you to use different VNI IDs for the same VLAN on different ZT-LAN devices, the VOS implementation maps the VLANs and VNI IDs consistently across all ZT-LAN devices.

EVPN Service Types

EVPN service types specify how a VNIs are mapped to an EVPN instances (EVIs).

The VOS software supports the following EVPN service types:

- VLAN based—A VLAN-based EVPN service does the following:
  - Maps a single VNI to a single EVI.
  - Maintains a MAC table for that VNI.
  - Sets the Ethernet tag ID in all EVPN routes to 0. In the data plane, the ingress device does not include an inner VLAN tag in the encapsulated frame, and the egress device discards frames that have an inner VLAN tag.
- VLAN-aware bundle—A VLAN-aware bundle EVPN service does the following:

- Maps multiple VNIs to a single EVI.
- Maintains a separate bridge table for each VNI.
- Sets the Ethernet tag ID in all EVPN routes to the VNI (the global VNI). In the data plane, the VNI is used to identify the bridge table, the ingress device does not include an inner VLAN tag in the encapsulated frame, and the egress device discards frames that have an inner VLAN tag.

EVPN Route Types

The VOS software supports the following EVPN route types, as specified in RFC 7432:

- Type 1—Ethernet autodiscovery (AD) routes. These routes are advertised only if the Ethernet segment identifier (ESI) is set to a nonzero value, which means that Type 1 routes originate from ZT-LAN devices that have multihomed hosts only. If a customer host device is single-homed to a single ZT-LAN device, the ESI value is 0.
- Type 2—MAC/IP advertisement routes. EVPN allows an end host's IP and MAC addresses to be advertised in the EVPN network layer reachability information (NLRI), which allows the control plane to learn an end system's MAC address. VOS devices support MAC route advertisement.
- Type 3—Inclusive multicast Ethernet tag routes. These routes set up a path for broadcast, unknown, and multicast (BUM) traffic from a local ZT-LAN device to a remote ZT-LAN device on a per-VLAN, per-ESI basis. The information in Type 3 advertisements allows an ingress router to deliver BUM traffic to the other ZT-LAN devices that are part of an EVPN instance. VOS devices support ingress replication.
- Type 4—Ethernet segment routes. These routes are used in multihoming scenarios to elect the designated forwarder (DF) and to allow a customer host device to be multihomed to two or more ZT-LAN devices in either single-active or active–active mode. ZT-LAN devices that are connected to the same Ethernet segment discover each other by using Ethernet segment routes.
- Type 5—IP prefix route. These routes are used to advertise EVPN routes using IP prefixes and to decouple the IP prefix advertisements from the MAC/IP advertisement routes in EVPN (as specified in RFC 9136).

BUM Traffic Handling

BUM traffic is handled using ingress replication on the ingress ZT-LAN device. The flood tag, which is the VNI used to reach a remote ZT-LAN device for BUM traffic, is essentially the same as the VNI used for unicast traffic. The receiving ZT-LAN device uses the VNI to identify the virtual switch (MAC-VRF) and bridge domain so that it can flood BUM traffic into that bridge domain.

Note: For BUM traffic handling, an ingress replication list can have a maximum of 64 EVPN neighbors.

Configure EVPN VXLAN

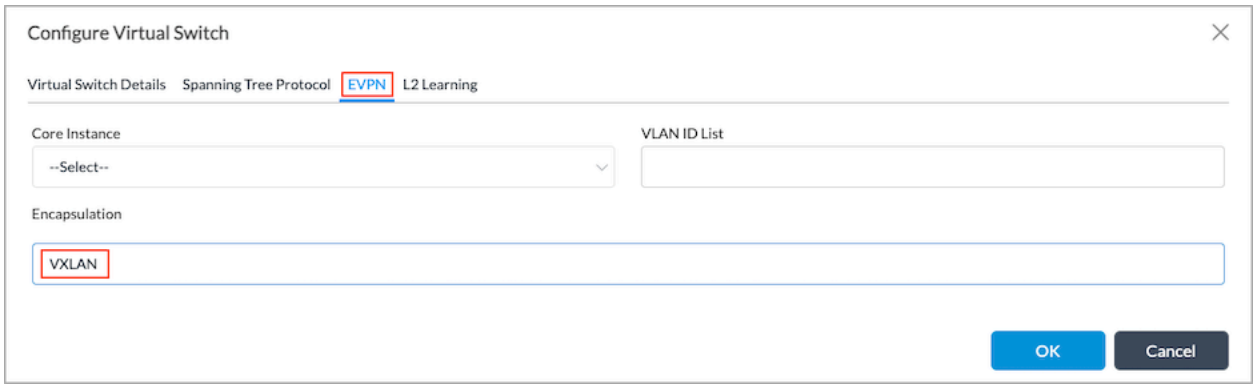
To configure EVPN VXLAN, you do the following:

- Configure a virtual switch (MAC-VRF) with a VNI.
- Configure the EVPN service.

Configure a Virtual Switch with a VNI

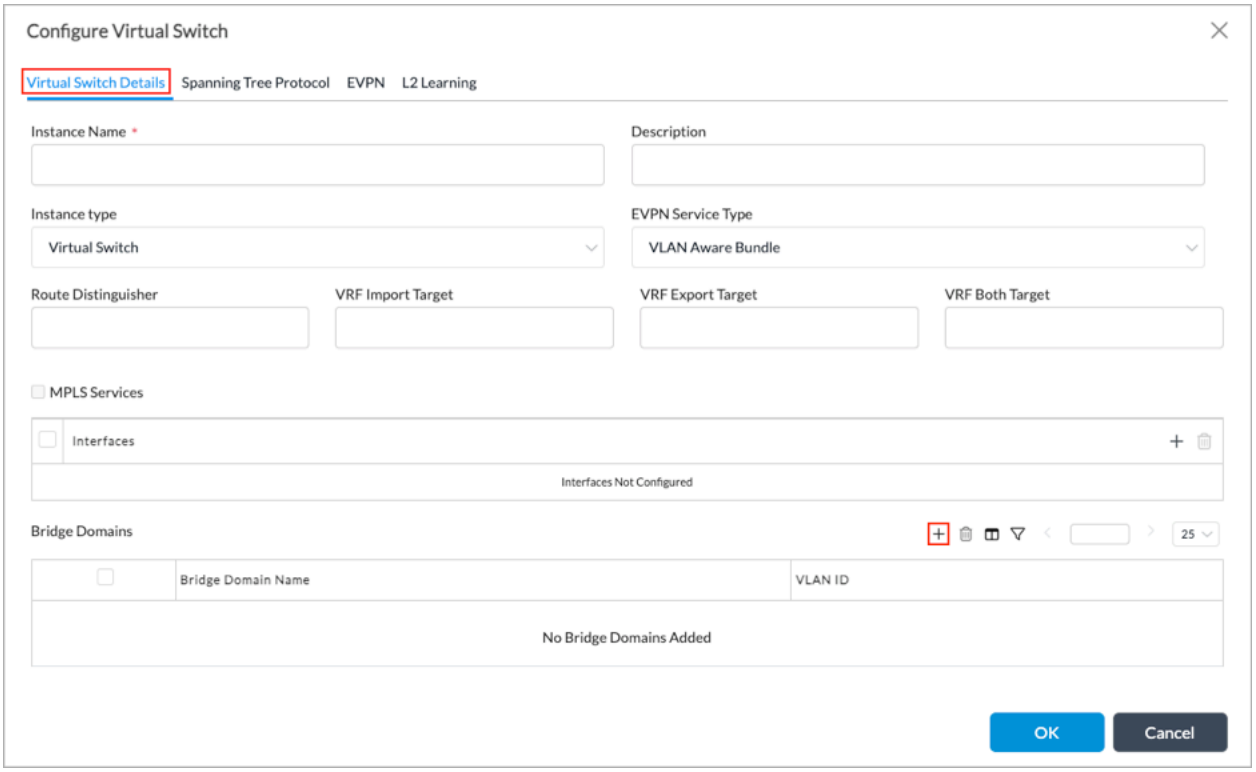
To configure a virtual switch (MAC-VRF) with a VNI:

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select a device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > Virtual Switches in the left menu bar. The main pane displays a list of the virtual switches that are already configured.
4. Click the + Add icon. In the Configure Virtual Switch popup window, select then Virtual Switch Details tab, and then enter a name in the Instance Name field.
5. Select the EVPN tab.
6. Click the Encapsulation field, and then select VXLAN.

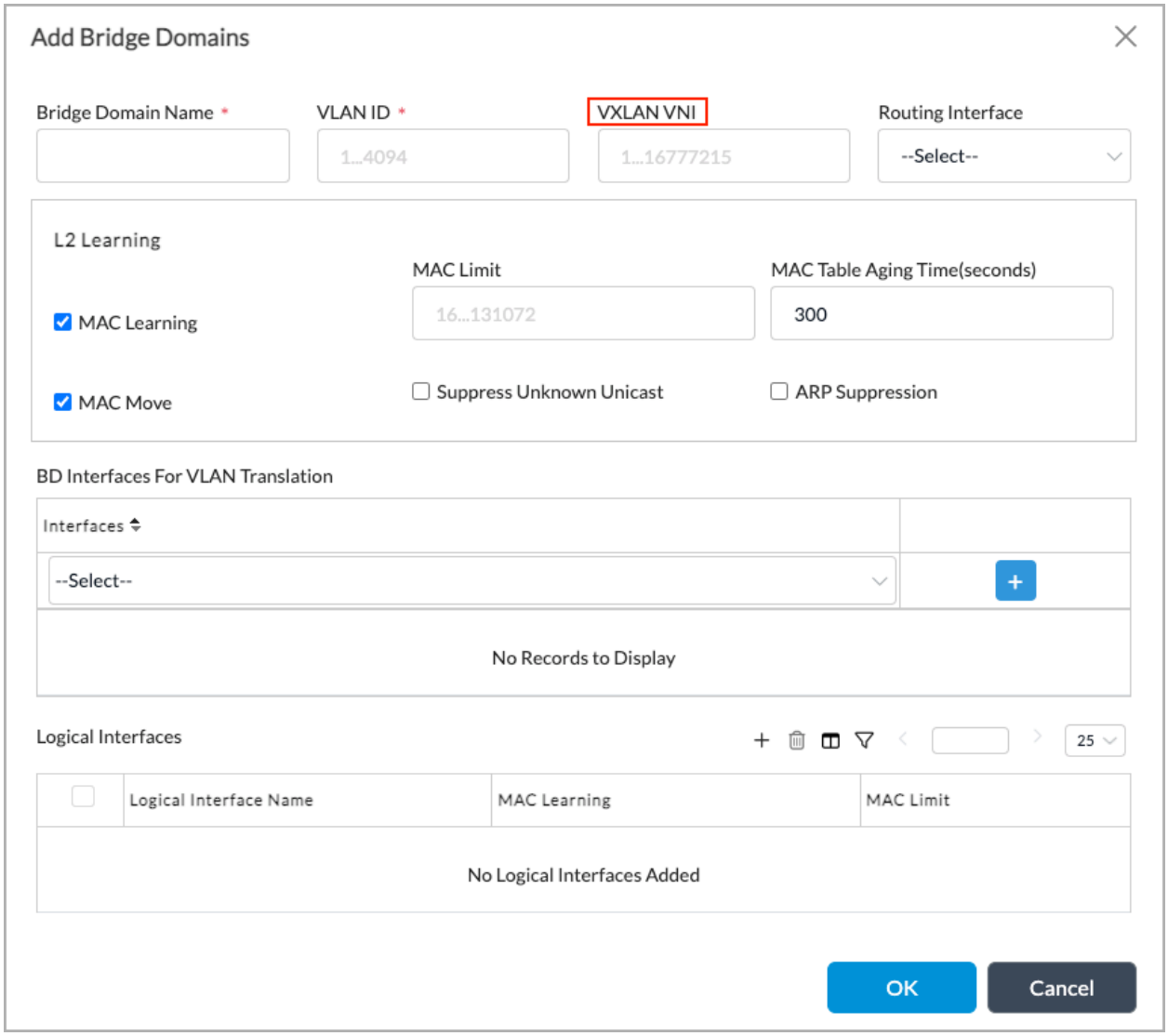


7. Select Virtual Switch Details tab to configure the VXLAN VNI.

Updated: Wed, 23 Oct 2024 08:45:45 GMT



8. In the Bridge Domains group of fields, click the + Add icon. In the Add Bridge Domains popup window, enter information for the following fields.

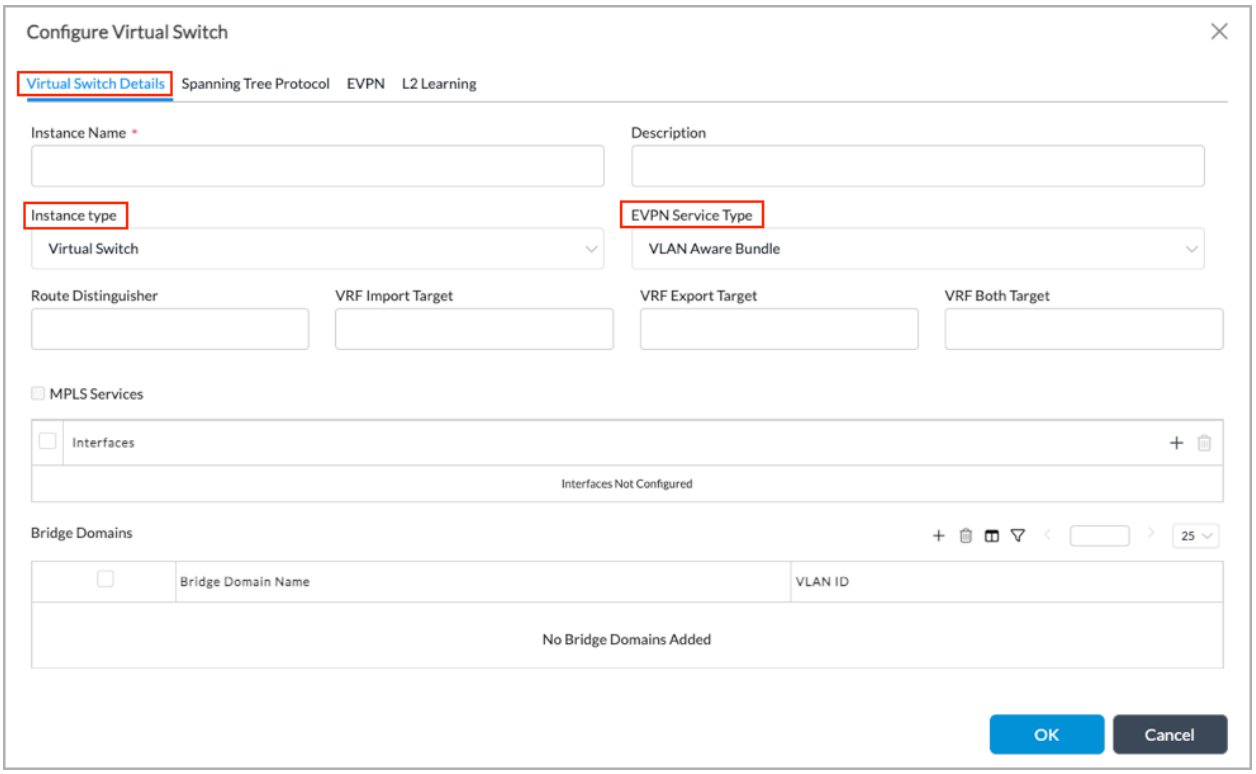


Field	Description
Bridge Domain Name (Required)	Enter a name for the bridge domain.
VLAN ID (Required)	Enter a VLAN ID for the bridge domain.
VXLAN VNI	Enter a number for the VXLAN VNI ID. *Range*: 1 through 16777215 *Default*: None

9. Click OK in the Add Bridge Domains popup window.
10. Click OK in the Configure Virtual Switch popup window.

Configure the EVPN Service

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select a device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > Virtual Switches in the left menu bar. The main pane displays a list of the virtual switches that are already configured.
4. Click the + Add icon. In the Configure Virtual Switch popup window, select the Virtual Switch Details tab, and then enter information for the following fields.



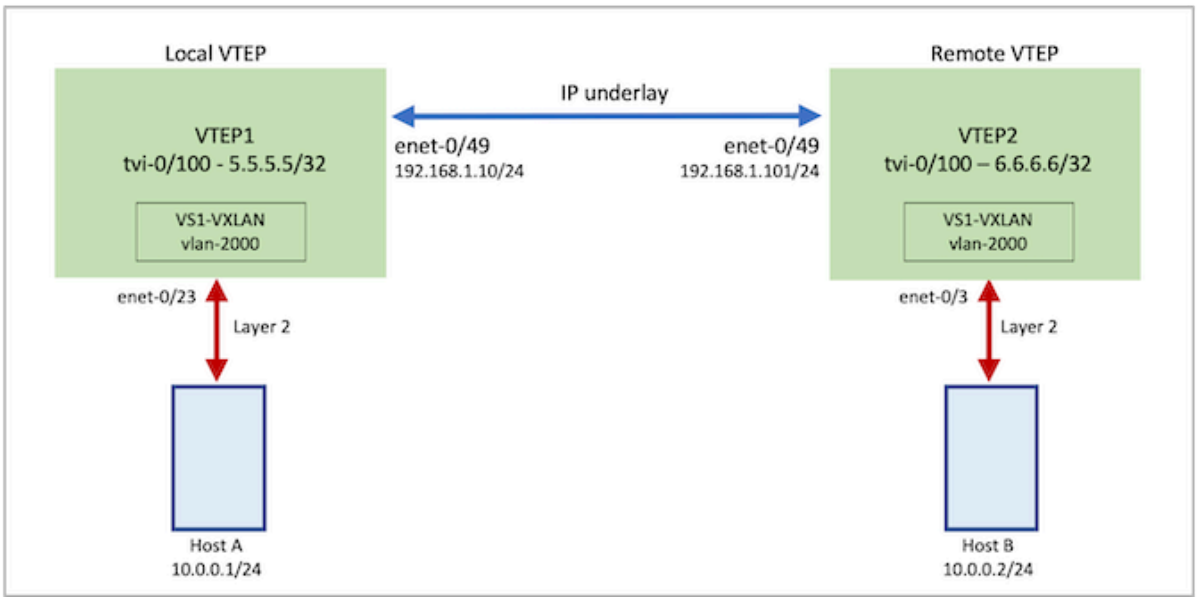
Field	Description
Instance Name (Required)	Enter a name for the virtual switch instance.
Instance Type	Select Virtual Switch.
EVPN Service Type	Select the service type: ◦ VLAN—Map a single VLAN to an EVI.

Field	Description
	◦ VLAN-Aware Bundle—Map multiple VLANs to an EVI.

5. Click OK.

Example Configuration

This section provides an example of configuring EVPN VXLAN using the topology illustrated in the following figure. In this example, Host A connects to the local virtual switch VS1-VXLAN, which is VTEP1 and has an IP address of 5.5.5.5/32. Host B connects to the remote virtual switch VS1-VXLAN, which is VTEP2 and has an IP address of 6.6.6.6/32. Host A and Host B both belong to VLAN 2000. For Host A to communicate with Host B, VTEP1 needs to connect to VTEP2 over the IP underlay network.



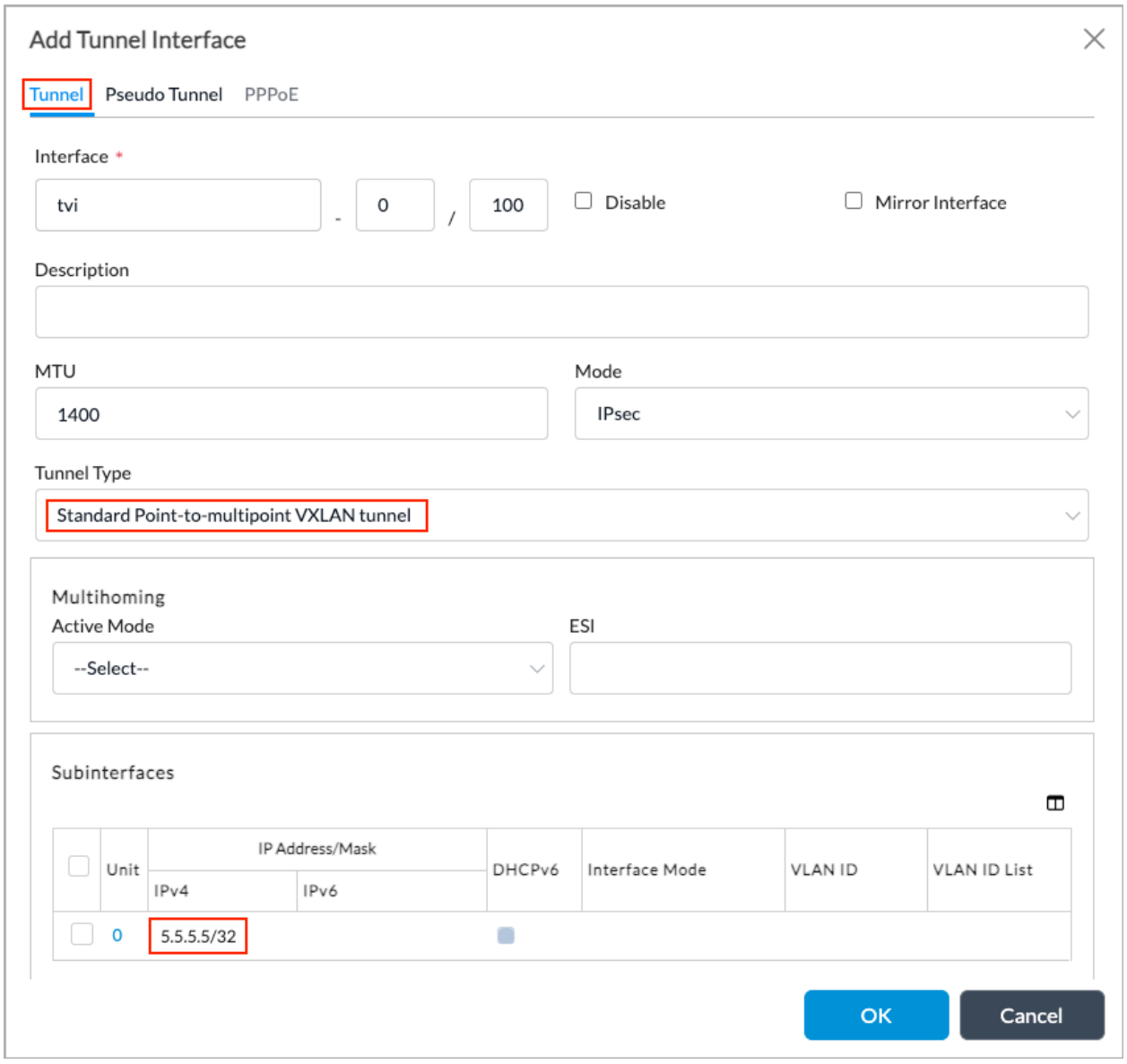
Configure Tunnel Virtual Interfaces on VTEP1 and VTEP2

First, you configure the transport network (underlay) virtual router and its neighbor ZT-LAN devices (5.5.5.5 and 6.6.6.6). These ZT-LAN devices are the remote virtual tunnel endpoint (VTEP) addresses for the EVPN VXLAN network. The EVPN local router address represents the local VTEP address for the EVPN VXLAN network. The transport virtual router also needs a tunnel virtual interface (TVI) to represent the local VTEP with the appropriate tunnel type. (For more information about configuring interfaces, see Configure Interfaces).

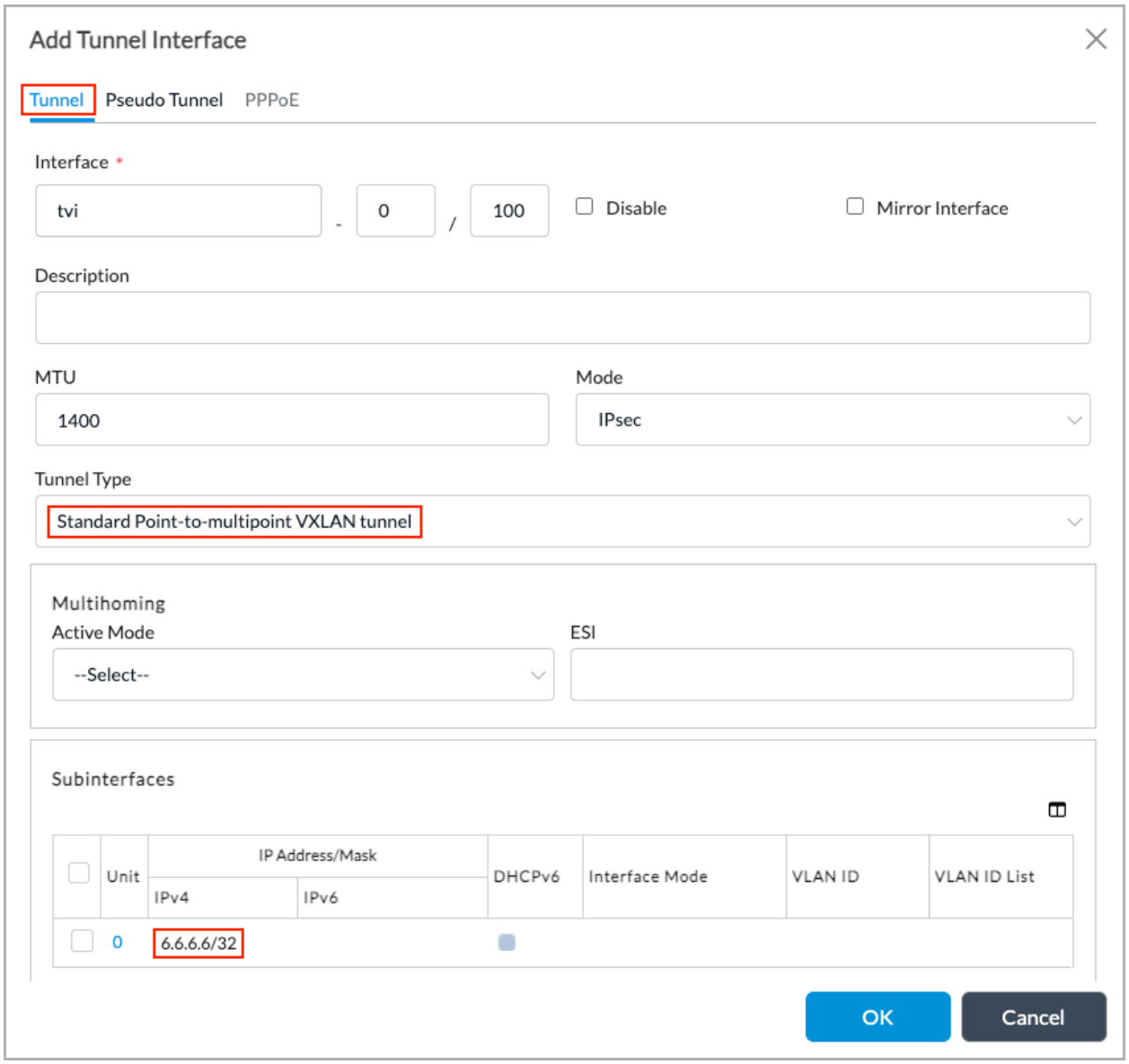
In this example topology, tvi-0/100 on local VTEP1 peers with tvi-0/100 on remote VTEP2. The tunnel is a standard point-to-multipoint IP underlay tunnel. You configure the static routes on the subinterfaces and provide the reachability

information for the neighboring VTEP.

The following screenshot shows the configuration for tvi-0/100 on local VTEP1, whose IP address is 5.5.5.5/32:



The following screenshots show the configuration for tvi-0/100 on remote VTEP2, whose IP address is 6.6.6.6/32:

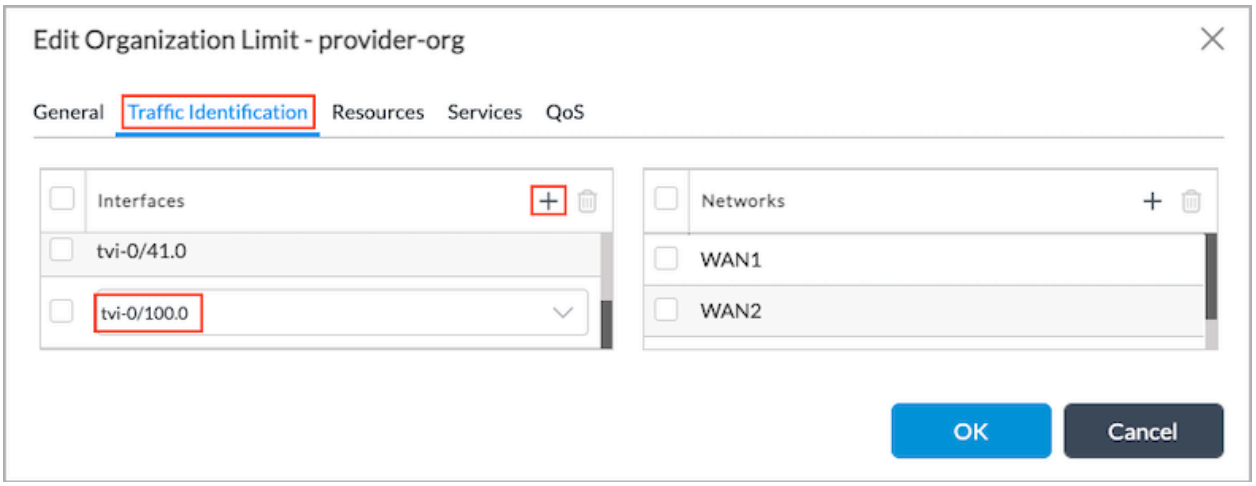


Add TVI Interfaces To Identify Organization Traffic

To properly identify tenant traffic, you include the VXLAN TVI in the organization (tenant) configuration. Without the tenant identification, traffic forwarding does not work on the TVI.

To add the VXLAN TVI interface to the organization:

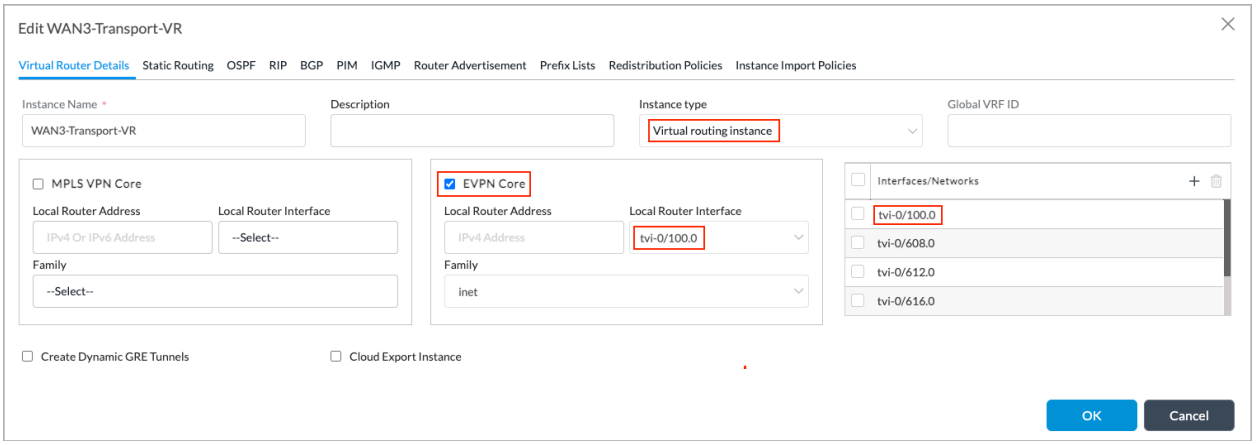
1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select a device in the main pane. The view changes to Appliance view.
2. Select Others > Organization > Limits in the left menu bar.
3. Select an organization in the main pane.
4. In the Edit Organization Limit popup window, select the Traffic Identification tab.
5. In the Interfaces table, click the + Add icon, and then select tvi-0/100.0.



6. Click OK.

Enable the EVPN Core and Add the TVI Interface to the Transport Virtual Router

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select a device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > Virtual Routers in the left menu bar.
4. Click the + Add icon. In the Edit WAN3-Transport-VR popup window, select the Virtual Router Details tab.
5. Enter the information shown in the following screenshot.



6. Click OK.

Configure BGP

Next, you configure BGP on the local router (VTEP1) and the remote router (VTEP2).

Configure BGP on the Local Router

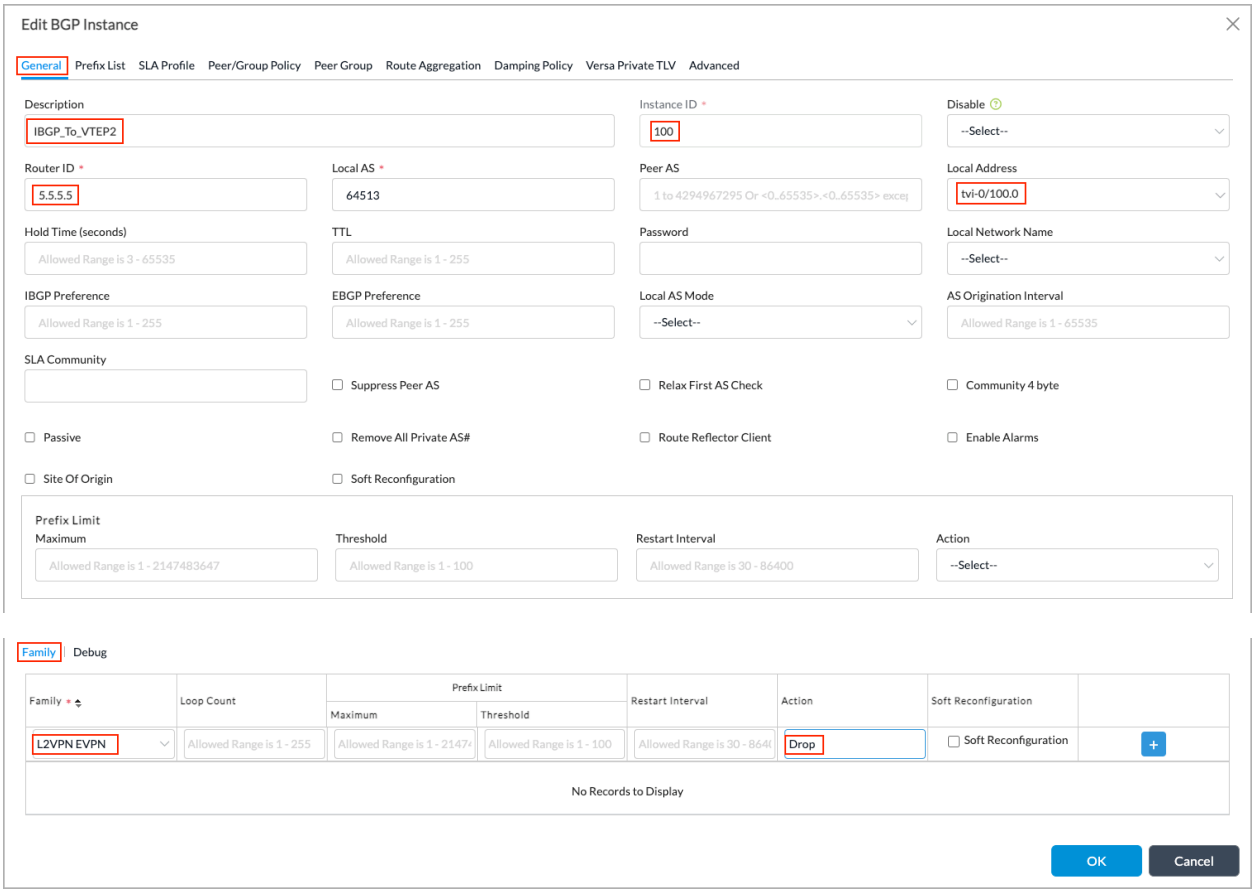
On the local router (VTEP1), you configure a BGP peering relationship between the local loopback interface (tvi-0/100) and the remote loopback interface (tvi-0/100) on the remote router (VTEP2).

To configure a BGP peering on the local router:

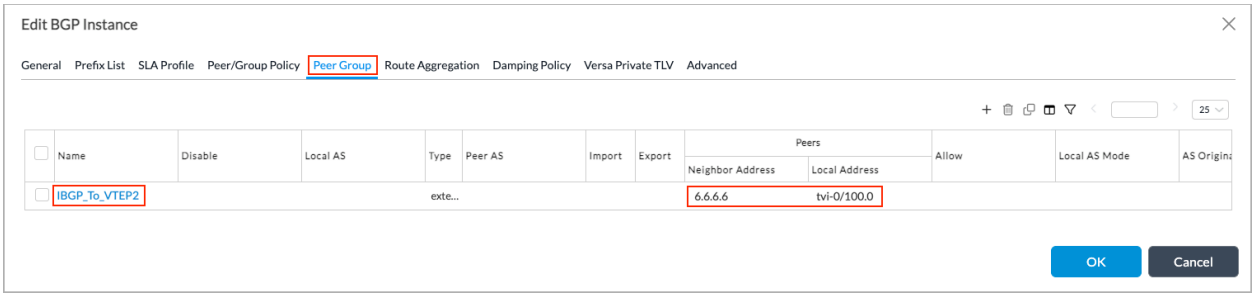
1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select a device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > Virtual Routers in the left menu bar.
4. Click the + Add icon. In the Edit WAN3-Transport-VR popup window, select the BGP tab.

5. Select the instance ID that corresponds to the local router. The Edit BGP Instance popup window displays.
6. Select the General tab, and then configure the following information.

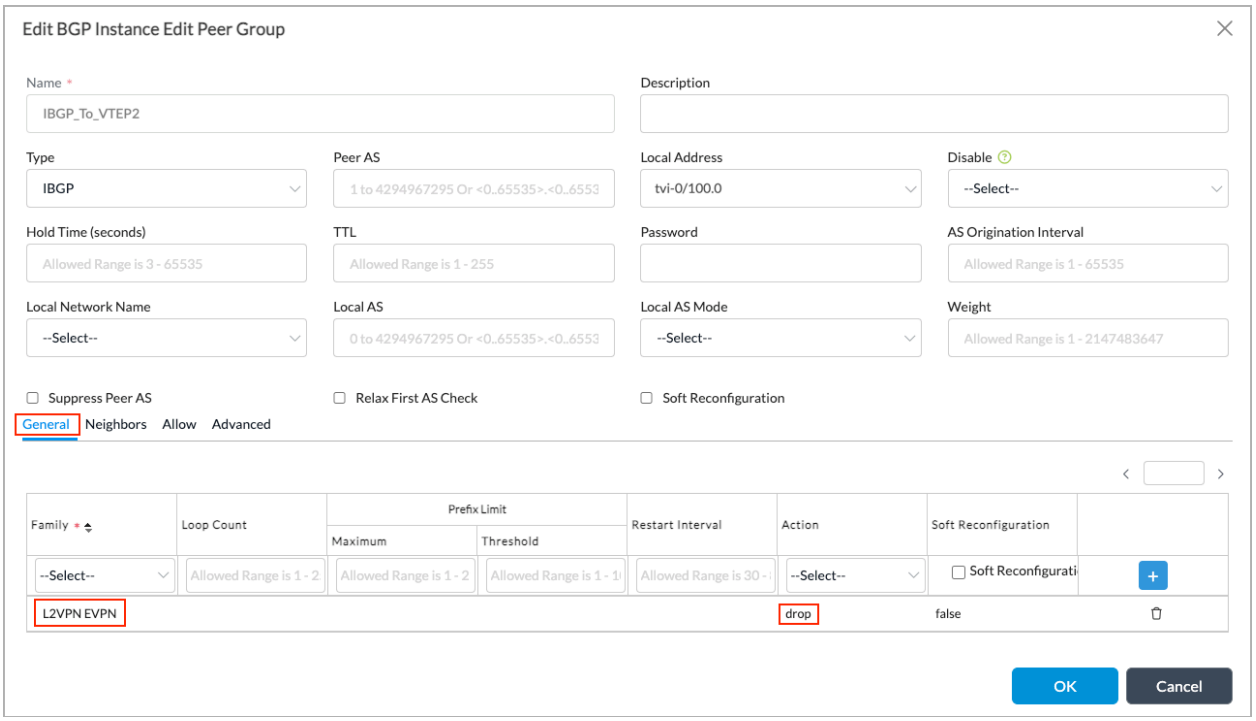
Updated: Wed, 23 Oct 2024 08:45:45 GMT



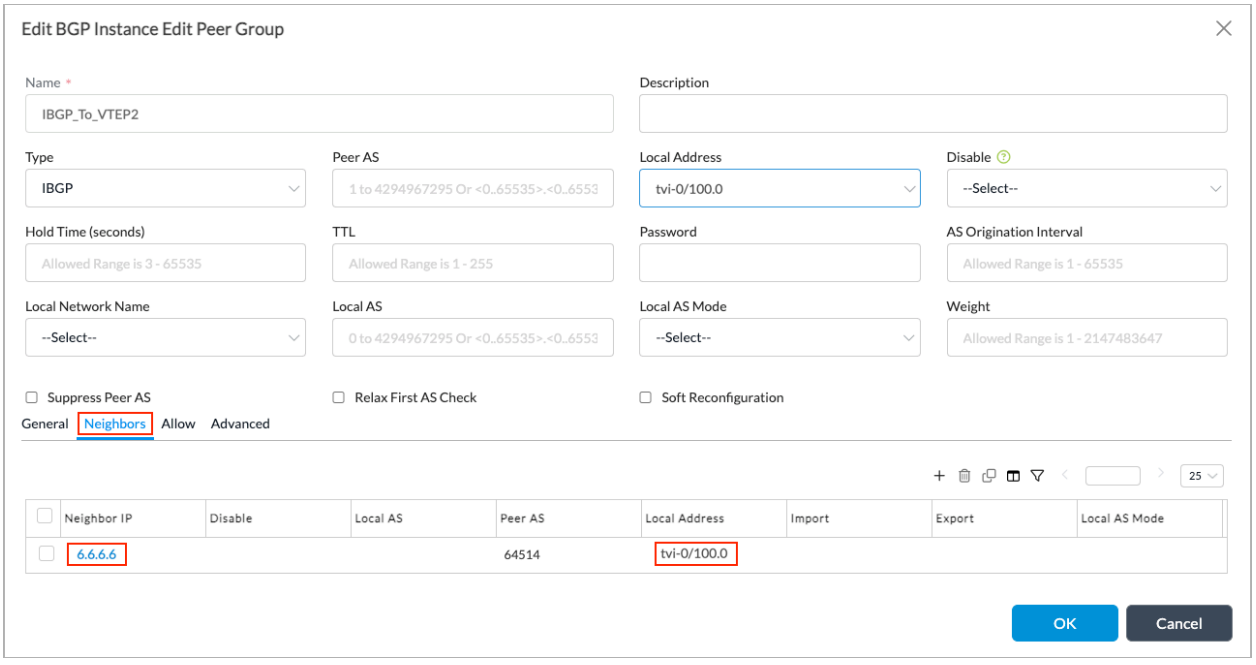
7. Select the Peer Group tab, and then select the peer group instance name that corresponds to the remote router.



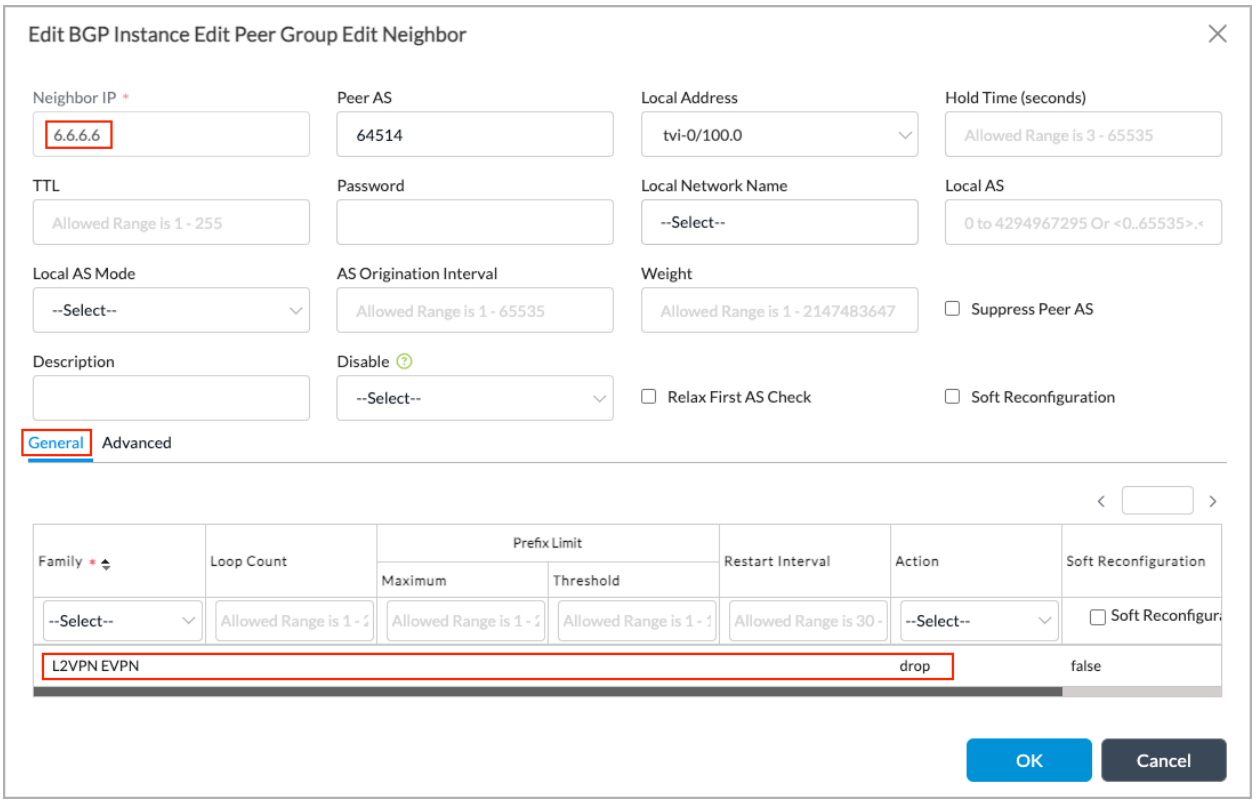
8. In the Edit BGP Instance Edit Peer Group popup window, select the General tab, and then configure the following information.



9. In the Edit BGP Instance Edit Peer Group popup window, select the Neighbors tab, and then configure the following information.



10. Select the neighbor, and in the Edit BGP Instance Edit Peer Group Edit Neighbor popup window, select the General tab, and then configure the following information.



11. Click OK twice.

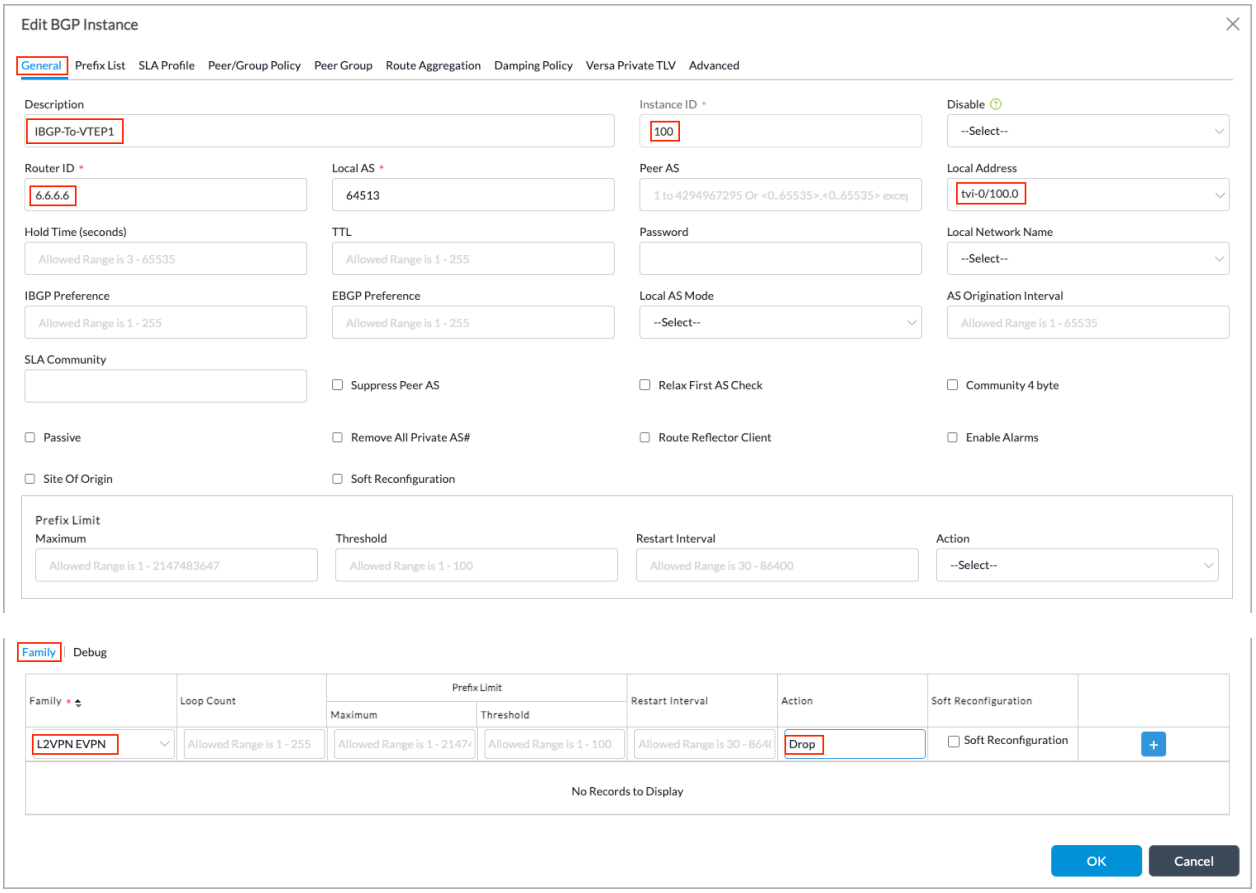
Configure BGP on the Remote Router (VTEP2)

On the remote router (VTEP2), you configure a BGP peering relationship between the remote loopback interface (tvi-0/100) and the loopback interface (tvi-0/100) on the local router (VTEP2).

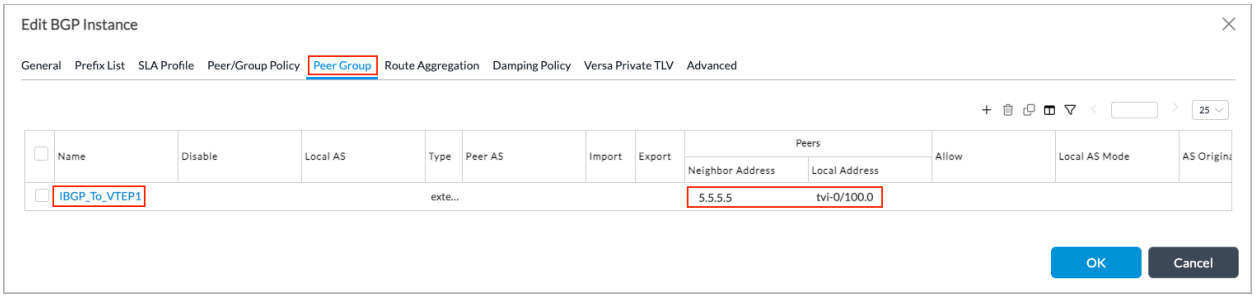
To configure a BGP peering on the remote router:

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select a device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > Virtual Routers in the left menu bar.
4. Click the + Add icon. In the Edit WAN3-Transport-VR popup window, select the BGP tab.

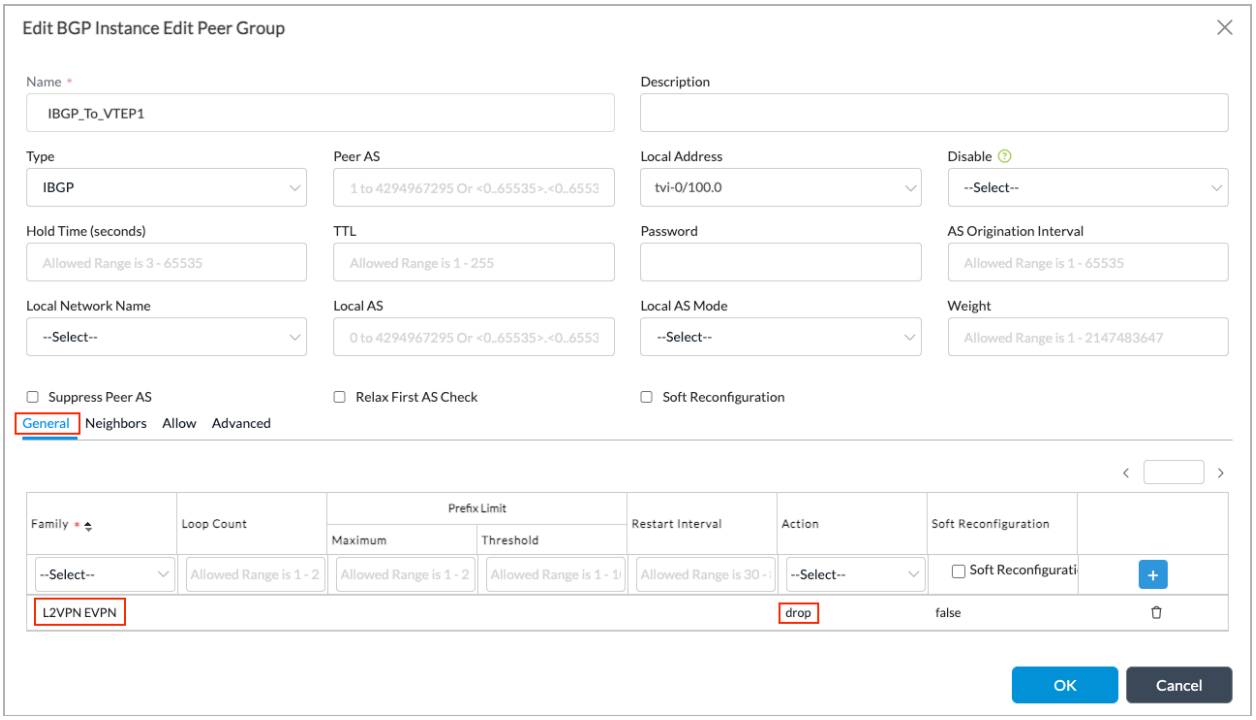
5. Select the instance ID that corresponds to the local router. The Edit BGP Instance popup window displays.
6. Select the General tab, and then configure the following information.



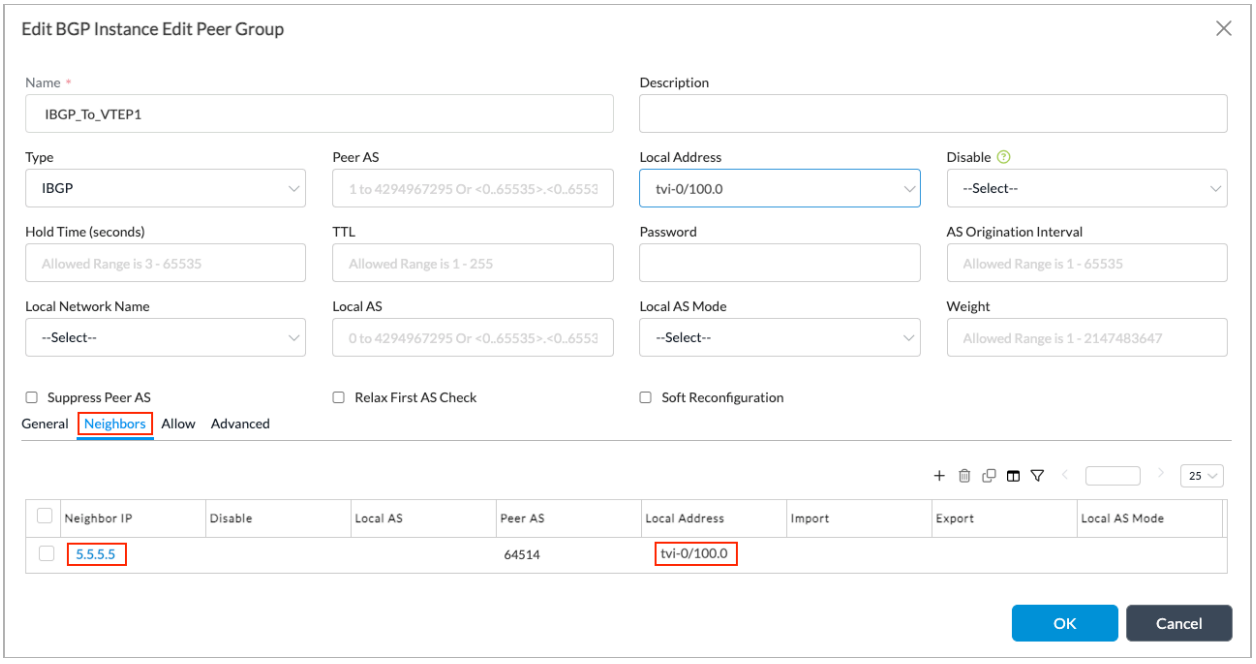
7. Select the Peer Group tab, and then select the peer group instance name that corresponds to the local router.



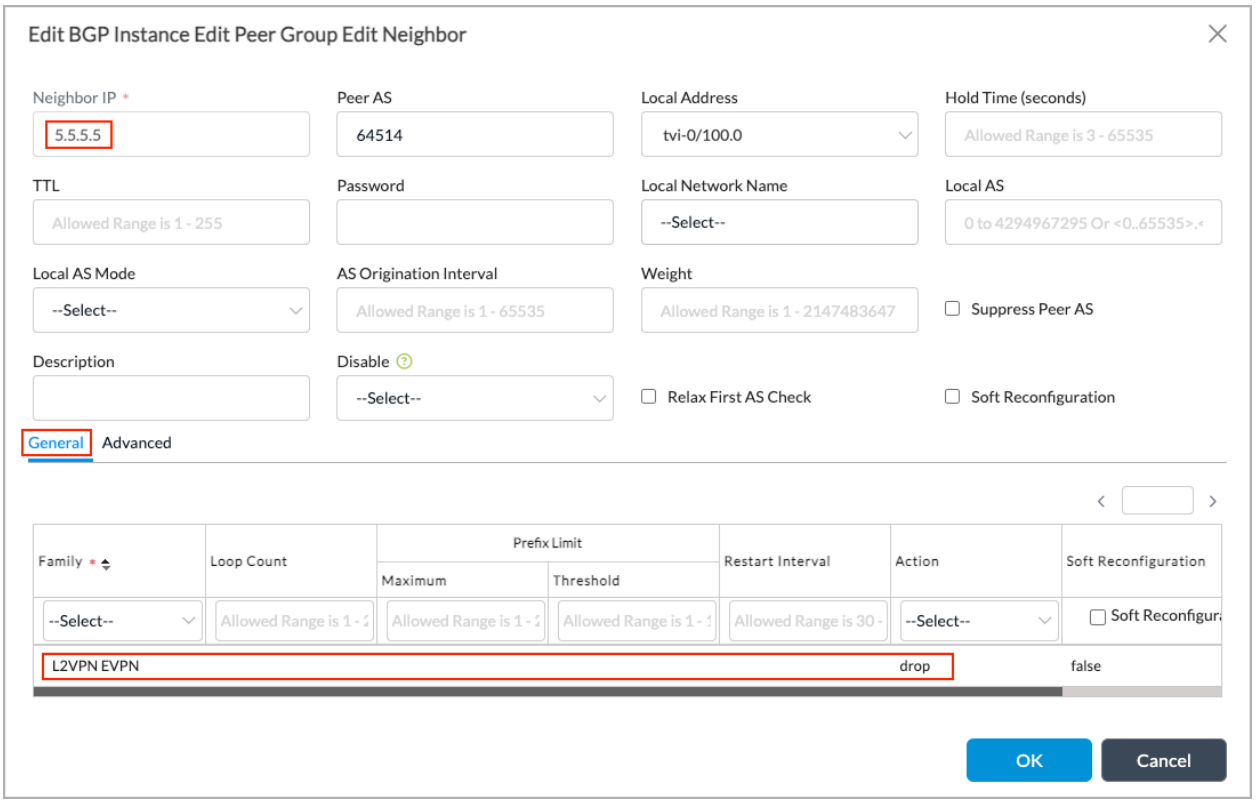
8. In the Edit BGP Instance Edit Peer Group popup window, select the General tab, and then configure the following information.



9. Select the Neighbors tab, and then configure the following information.



10. Select the neighbor, and in the Edit BGP Instance Edit Peer Group Edit Neighbor popup window, select the General tab, and then configure the following information.



11. Click OK twice.

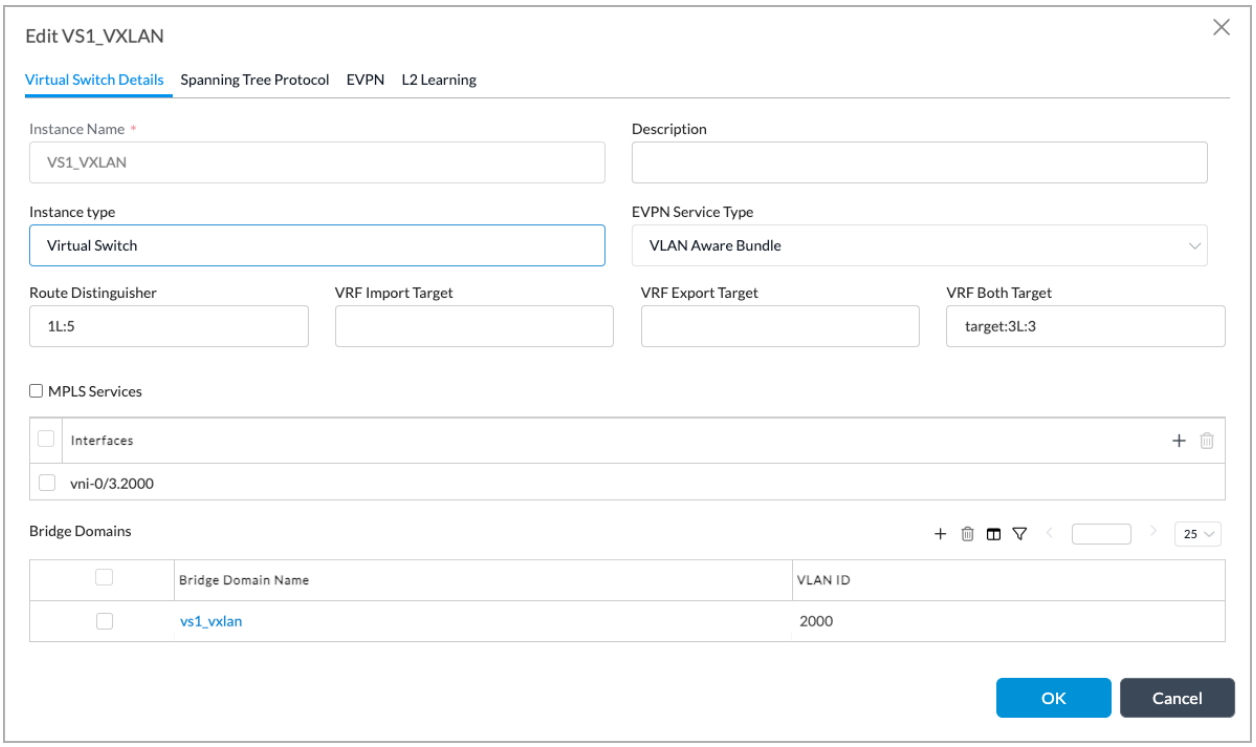
Configure Virtual Switch Instances VTEP1 and VTEP2

Finally, you configure the virtual switch instances VTEP1 and VTEP2.

Configure VS1_VXLAN (VTEP1)

Configure the local virtual switch VS1_VXLAN VTEP1, whose IP address is 5.5.5.5:

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select a device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > Virtual Switches in the left menu bar.
4. Click the + Add icon. In the Edit VS1_VXLAN popup window, select the Virtual Switch Details tab, and then enter the following information.

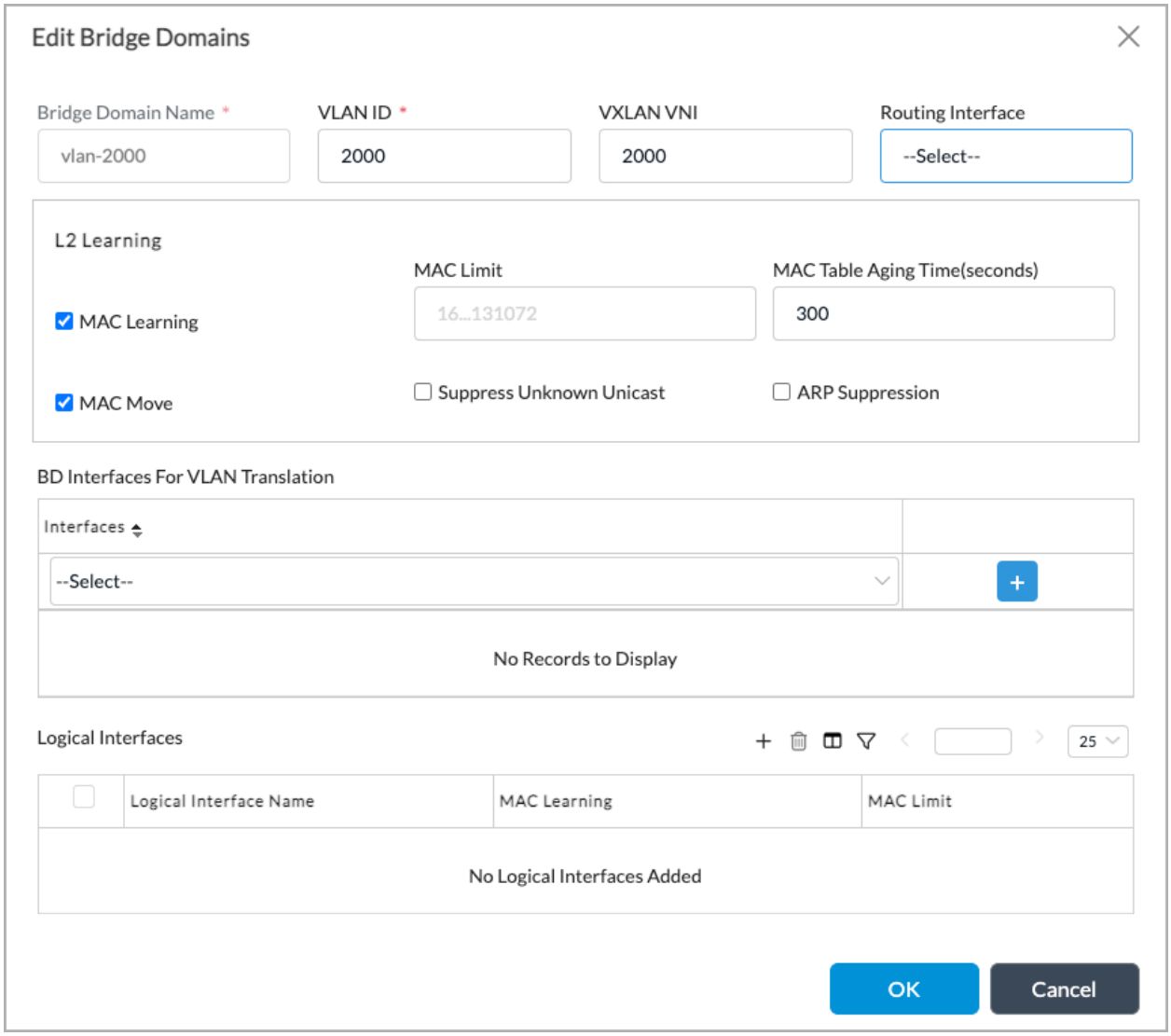


5. Click OK.

Configure the VLAN-to-VXLAN VNI Mapping for VTEP1

Configure the VLAN-to-VXLAN VNI mapping for VTEP1:

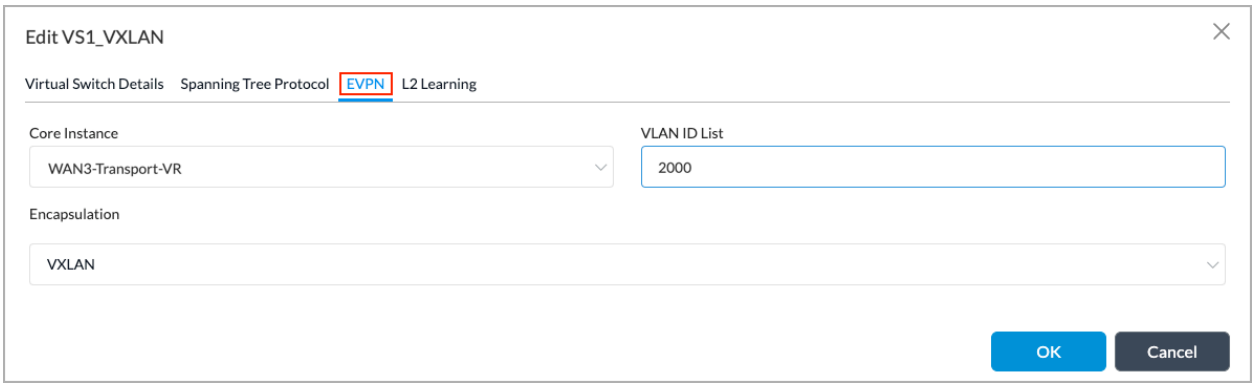
1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select a device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > Virtual Switches in the left menu bar.
4. Select a virtual switch, and edit it. In the Edit Bridge Domains popup window, enter the following information.



5. Click OK.

Map VS1-VXLAN to the the EVPN Core Instance for VTEP1

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select a device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar
3. Select Networking > Virtual Switches in the left menu bar.
4. Select the VS1_VXLAN, and then in the Edit VS1-VXLAN popup window, select EVPN in the left menu bar. Enter the following information.

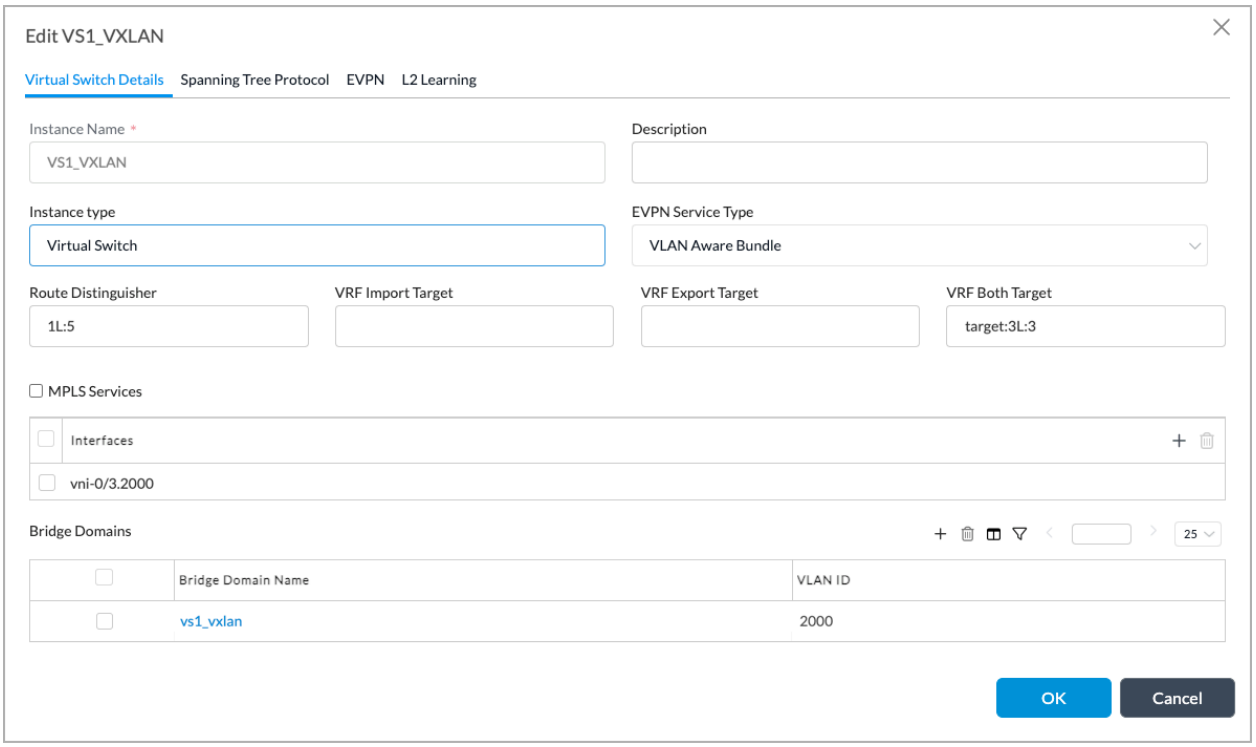


5. Click OK.

Configure VS1_VXLAN (VTEP2)

Configure the remote virtual switch VS1_VXLAN VTEP2, whose IP address is 6.6.6.6:

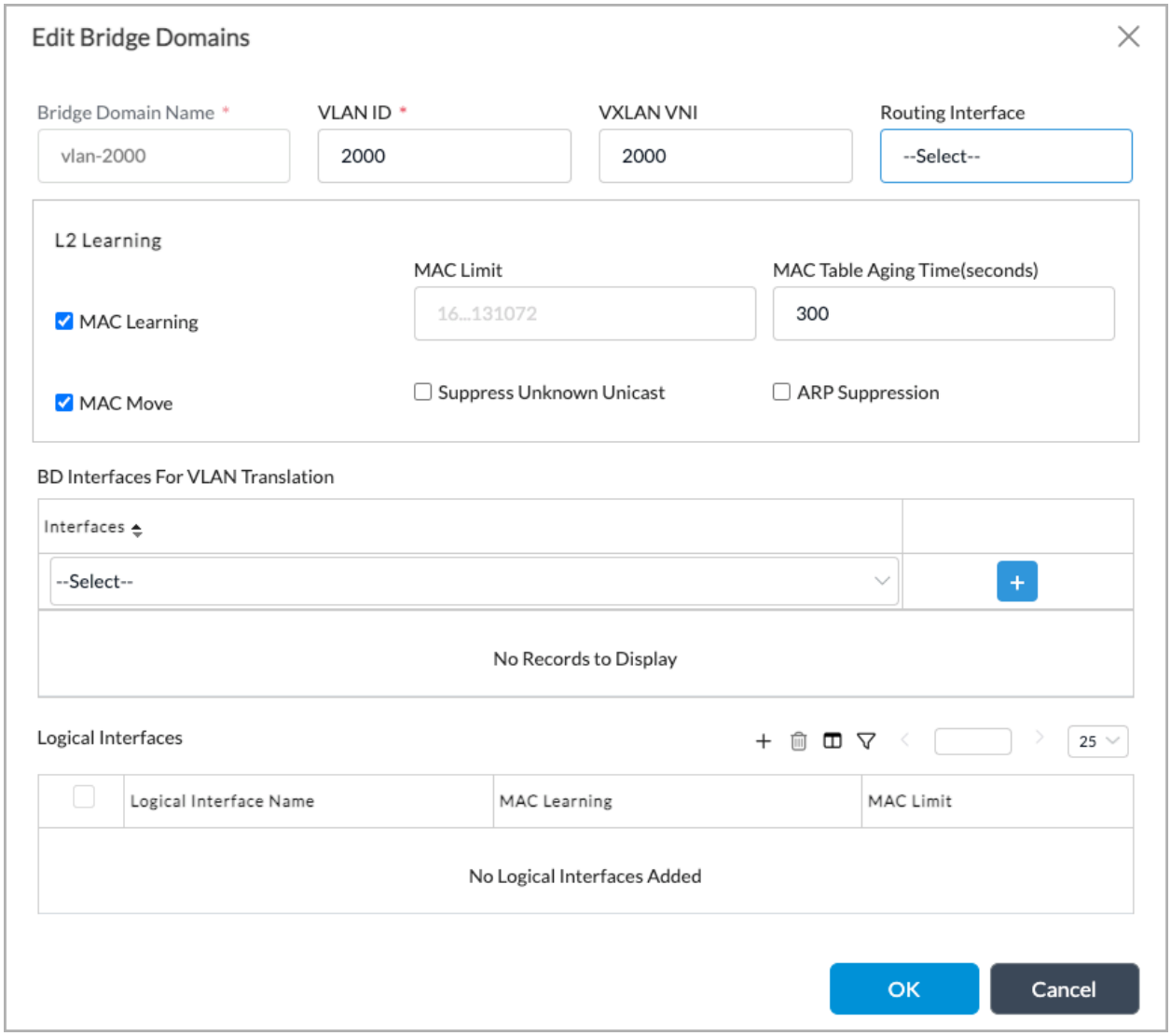
1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select a device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > Virtual Switches in the left menu bar.
4. In Transport-WAN-VR, select VS1_VXLAN.
5. In the Edit VS1_VXLAN popup window, select the Virtual Switch Details tab, and then enter the following information:



6. Click OK.

Configure the VLAN-to-VXLAN VNI Mapping for VTEP2

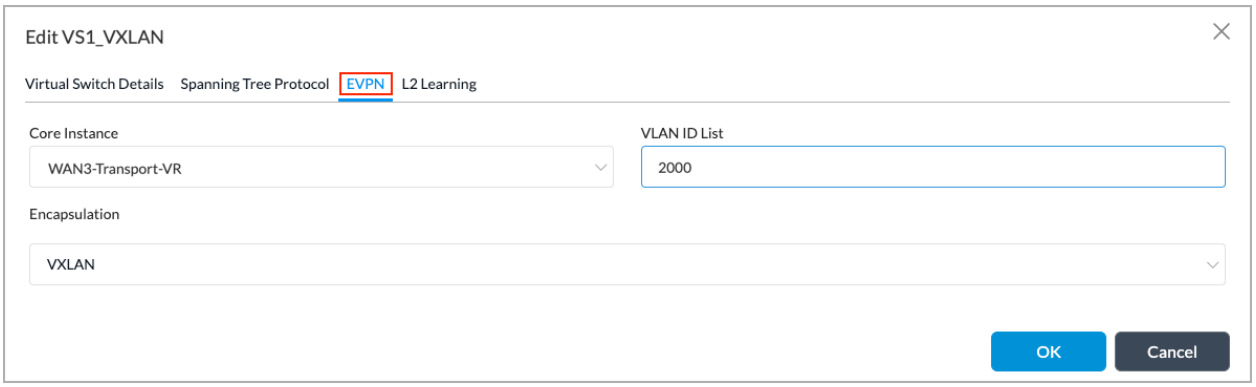
1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select a device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > Virtual Switches in the left menu bar.
4. Select a virtual switch, and edit it. In the Edit Bridge Domains popup window, enter the following information.



5. Click OK.

Map VS1-VXLAN to the EVPN Core Instance (VTEP2)

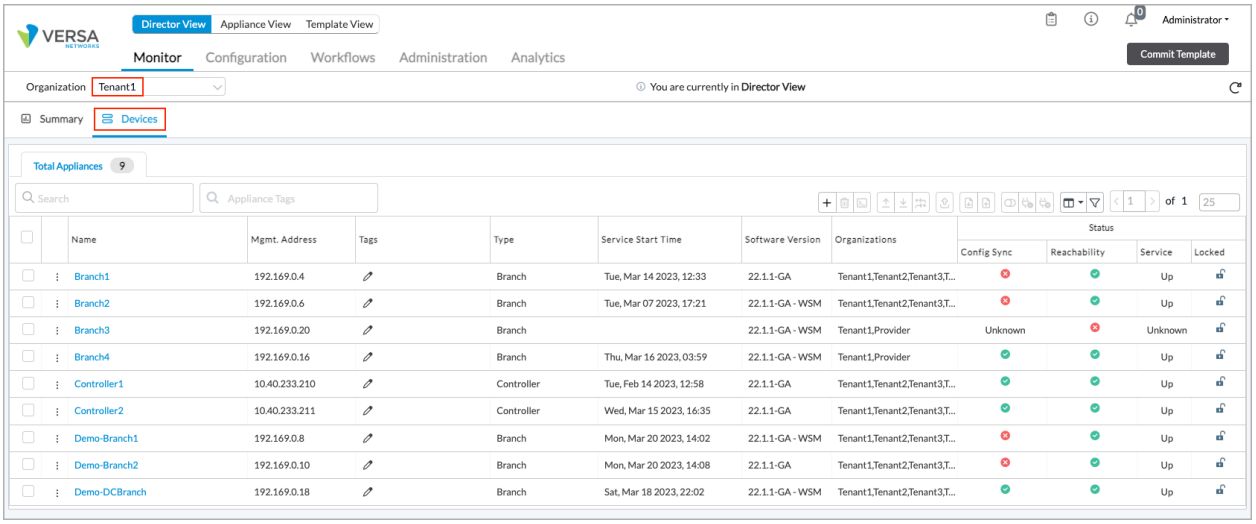
1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select a device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > Virtual Switches in the left menu bar.
4. Select the VS1_VXLAN, and in the Edit VS1-VXLAN popup window, select EVPN in the left menu bar. Enter the following information.



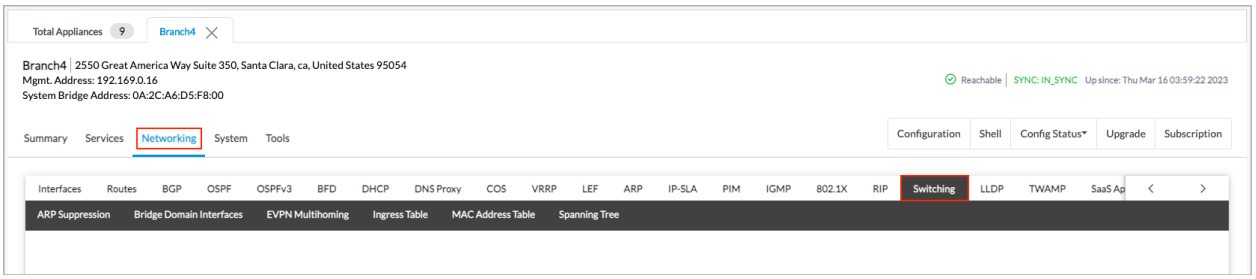
5. Click OK.

Verify the EVPN VXLAN Configuration

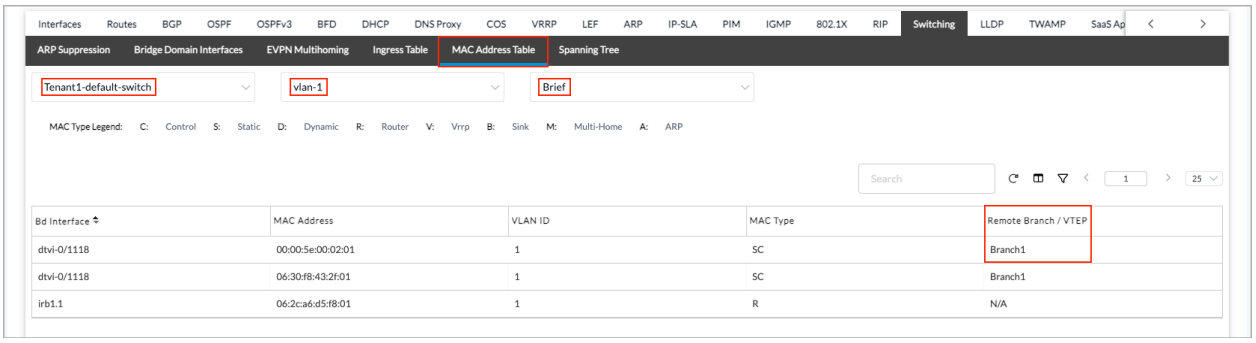
1. In Director view, select the Monitor tab in the top menu bar.
2. In the Organization field, select an organization.
3. Select the Devices tab in the horizontal menu bar.



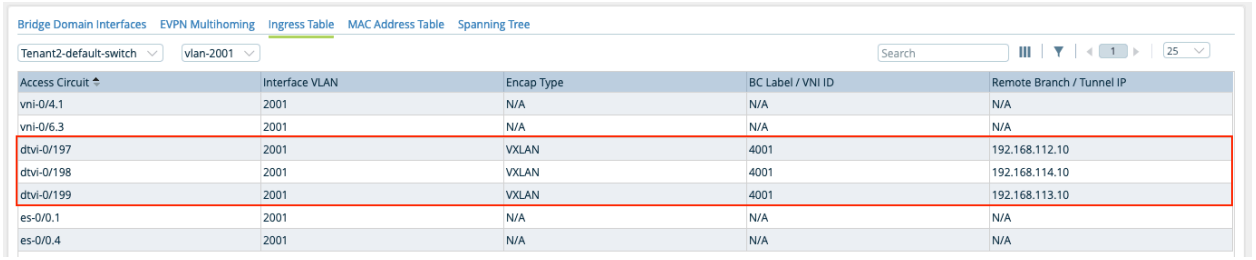
4. Select a device in the main pane. The screen displays information for the selected device.
5. Select the Networking tab, and then select Switching.



6. Select the MAC Address Table in the horizontal menu bar.
7. Select a switch name in the first drop-down list.
8. Select a VLAN in the second drop-down list.
9. Select the type of output to display in the third drop-down list, either Brief (default) or Statistics. The screen displays bridge MAC table information for VXLAN. The following screenshot shows the dtvi-0/213 bridge domain interface connected to the remote branch/VTEP at 192.168.112.10.



10. Select the Ingress Table tab to display the remote VXLAN tunnel endpoints. The following screenshot shows the endpoints for interface VLA 2001.



Supported Software Information

Releases 22.1.1 and later support all content described in this article.

Additional Information

Configure EVPN Multihoming for SD-WAN
Configure EVPN for Hosts Using ZT-LAN
Configure Interfaces
Configure Layer 2 Forwarding
RFC 7432, BGP MPLS-Based Ethernet VPN
RFC 8365, A Network Virtualization Overlay Solution Using Ethernet VPN (EVPN)