

---

## Configure EVPN VXLAN for SD-WAN

 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 that the terminology in the article aligns with that used in the RFCs, which defines EVPNs in of provider edge (PE) routers. However, the VOS SD-WAN EVPN VXLAN solution is for customer edge (CE) devices for both service providers and enterprises.

---

## Overview

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

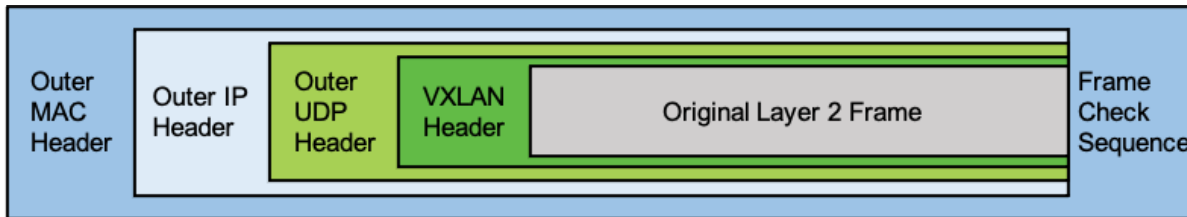
In the control plane, MP-BGP, which supports the Layer 2 VPN Address Family Identifier (AFI) and the EVPN Subsequent Address Family Identifier (SAFI), allows a provider edge (PE) device to distribute MAC addresses and IP routing information to another PE device.

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 VXLAN tunnel endpoints (VTEPs). There is one VTEPs 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 VNI ID so that it can be used throughout a network. You specify the VNI ID 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 PE device are distributed to other PE 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 PE device for a tenant.

Note: In an EVPN multihoming context, 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 PE device uses the VNI ID to look up the correct MAC-VRF and bridge domain, and then the MAC address are 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 PE devices, the VOS implementation maps the VLANs and VNI IDs consistently across all PE devices.

## EVPN Service Types

The VOS software supports the following EVPN service types:

- VLAN based—Map a single VNI to an EVPN instance (EVI), maintain a MAC table for that VNI, and set 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—Map multiple VNIs to an EVI, maintain a separate bridge table for each VNI, and set the Ethernet tag ID in all EVPN routes to the VNI (global VNI case). 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 for multihomed sites only. If a customer edge (CE) device is single-homed, the ESI value is 0.
- Type 2—MAC/IP advertisement routes. EVPN allows an end host's IP and MAC addresses to be advertised within 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 PE device to a remote PE 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 PE 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 CE device to be multihomed to two or more PE devices in either single-active or active-active mode. PE 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 decouple the IP prefix advertisements from the MAC/IP advertisement routes in EVPN (specified in [RFC 9136](#)).

---

## BUM Traffic Handling

BUM traffic is handled using ingress replication on the ingress PE node. The flood tag, which is the VNI used to reach a remote PE device for BUM traffic, is essentially the same as the VNI used for unicast traffic. The receiving PE 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 supports 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.

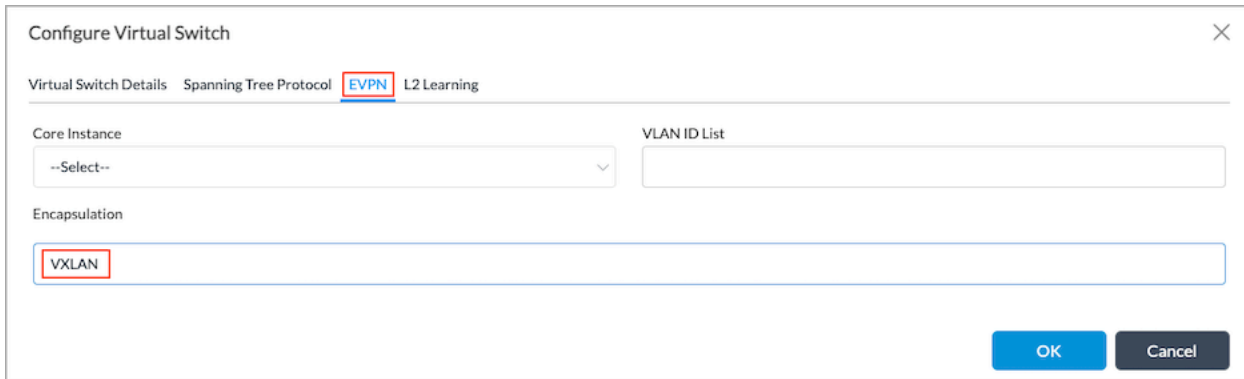
---

### Configure a Virtual Switch with a VNI

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

1. In Director view:
  - a. Select the Configuration tab in the top menu bar.

- b. Select Templates > Device Templates in the horizontal menu bar.
  - c. Select an organization in the left menu bar.
  - d. Select a post-staging template. 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 Virtual Switch Details in the left menu bar, then enter an instance name in the field provided.
5. Select EVPN in the left menu bar.
6. In the Encapsulation field, select VXLAN.



Configure Virtual Switch

Virtual Switch Details   Spanning Tree Protocol   **EVPN**   L2 Learning

Core Instance: --Select--

VLAN ID List:

Encapsulation: **VXLAN**

OK Cancel

7. Select Virtual Switch Details in the left menu bar to configure the VXLAN VNI.

Configure Virtual Switch

Virtual Switch Details

Spanning Tree Protocol

EVPN

L2 Learning

Instance Name \*

Description

Instance type

Virtual Switch

EVPN Service Type

VLAN Aware Bundle

Route Distinguisher

VRF Import Target

VRF Export Target

VRF Both Target

MPLS Services

Interfaces

+

Interfaces Not Configured

Bridge Domains

+

25


Bridge Domain Name

VLAN ID

No Bridge Domains Added

OK

Cancel

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

Add Bridge Domains

Bridge Domain Name \*

VLAN ID \*

VXLAN VNI

Routing Interface

1...4094

1...16777215

--Select--

L2 Learning

☒ MAC Learning

☒ MAC Move

MAC Limit

MAC Table Aging Time(seconds)

16...131072

300

☐ Suppress Unknown Unicast

☐ ARP Suppression

BD Interfaces For VLAN Translation

Interfaces

--Select--

+

No Records to Display

Logical Interfaces

+

<

>

25

☐

Logical Interface Name

MAC Learning

MAC Limit

No Logical Interfaces Added

OK

Cancel

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. <i>Range:</i> 1 through 16777215 <i>Default:</i> None

- Click OK Add Bridge Domains screen, the click OK in the Configure Virtual Switch screen.


## Configure the EVPN Service

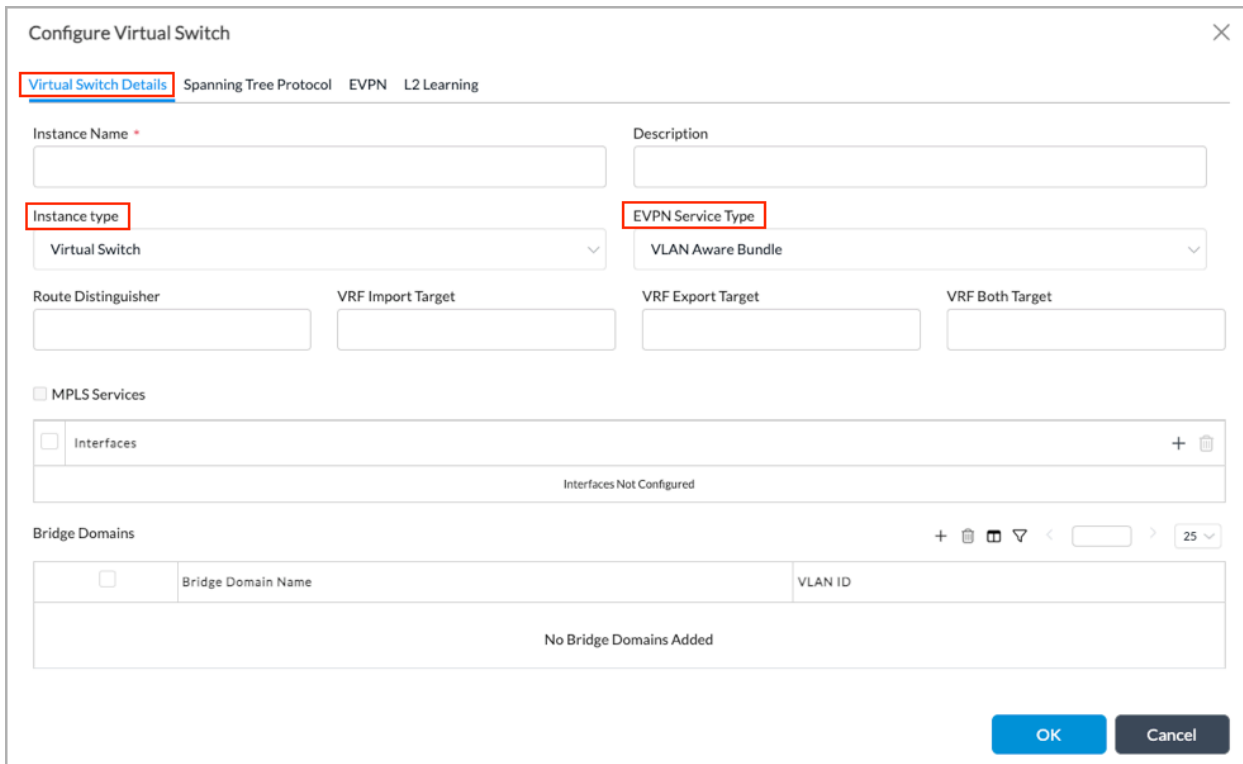
- In Director view:

[https://docs.versa-networks.com/Secure\\_SD-WAN/01\\_Configuration\\_from\\_Director/SD-WAN\\_Configuration/Advanced\\_SD-W...](https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/SD-WAN_Configuration/Advanced_SD-W...)

Updated: Wed, 23 Oct 2024 08:11:12 GMT

Copyright © 2024, Versa Networks, Inc.

- a. Select the Configuration tab in the top menu bar.
  - b. Select Templates > Device Templates in the horizontal menu bar.
  - c. Select an organization in the left menu bar.
  - d. Select a post-staging template. 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 Virtual Switch Details in the left menu bar, and enter information for the following fields.



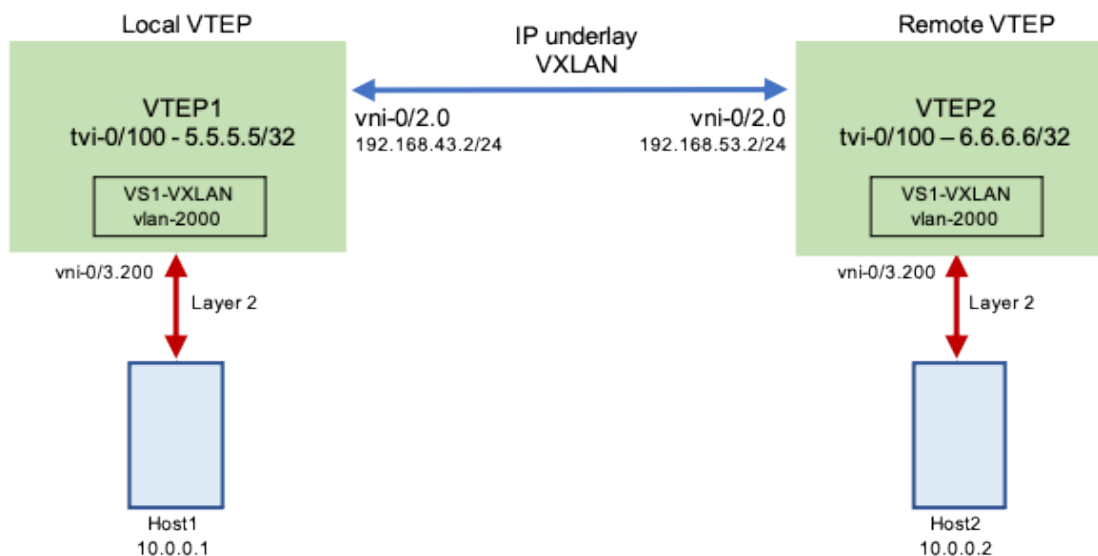
Field	Description
Instance Name (Required)	Enter a name for the virtual switch instance.
Instance Type	Select Virtual Switch.
EVPN Service Type	Select the service type: <ul style="list-style-type: none"> <li>◦ VLAN—Map a single VLAN to an EVI.</li> <li>◦ VLAN-Aware Bundle—Map multiple VLANs to an EVI.</li> </ul>

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, Host1 connects to the local virtual switch VS1-VXLAN, which is VTEP1 and has an IP address of 5.5.5.5/32. Host2 connects to the remote virtual switch VS1-VXLAN, which is VTEP2 and has an IP address of 6.6.6.6/32. Host1 and Host2 both belong to VLAN 2000. For Host1 to communicate with Host2, VTEP1 needs to connect to VTEP2 over a VXLAN tunnel in the IP underlay network.



---

## Configure Tunnel Virtual Interfaces on VTEP1 and VTEP2

First, you configure the transport network (underlay) virtual router and its neighbor PE devices (5.5.5.5 and 6.6.6.6). These PE 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 should also have 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 VXLAN tunnel. You configure the static routes on the subinterfaces and provide the reachability information for the neighboring VTEP.

- Configuration for tvi-0/100 on local VTEP1, whose IP address is 5.5.5.5/32:



Add Tunnel Interface
✕

Tunnel
Pseudo Tunnel
PPPoE

Interface \*

tvi
-
0
/
100

☐ Disable
☐ Mirror Interface

Description

MTU

1400

Mode

IPsec

Tunnel Type

Standard Point-to-multipoint VXLAN tunnel

Multihoming

Active Mode

--Select--

ESI

Subinterfaces

	Unit	IP Address/Mask		DHCPv6	Interface Mode	VLAN ID	VLAN ID List
		IPv4	IPv6				
<input type="checkbox"/>	0	5.5.5.5/32		<input type="checkbox"/>			

OK

Cancel

- Configuration for tvi-0/100 on remote VTEP2, whose IP address is 6.6.6.6/32:

Add Tunnel Interface
✕

Tunnel
Pseudo Tunnel
PPPoE

Interface \*

tvi

-

0

/

100

☐ Disable
☐ Mirror Interface

Description

MTU

1400

Mode

IPsec

Tunnel Type

Standard Point-to-multipoint VXLAN tunnel

Multihoming
Active Mode

--Select--

ESI

Subinterfaces

	Unit	IP Address/Mask		DHCPv6	Interface Mode	VLAN ID	VLAN ID List
		IPv4	IPv6				
<input type="checkbox"/>	0	6.6.6.6/32		<input type="checkbox"/>			

OK

Cancel

**Edit Subinterface**

General **IPv4** IPv6

Static Address

<input type="checkbox"/>	IP Address/Mask	+	🗑️
<input type="checkbox"/>	6.6.6.6/32		

OK Cancel

## 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 Configuration tab in the top menu bar.
  - b. Select Devices > Devices in the horizontal menu bar.
  - c. Select an organization in left navigation panel.
  - d. Select a tenant or Controller node in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Others > Organization > Limits in the left menu bar.
4. Select the tenant or provider organization in the main pane.
5. In the Edit Organization Limit popup window, click the **+** Add icon and add tvl-0/100.0.

**Edit Organization Limit - provider-org**

General **Traffic Identification** Resources Services QoS

Interfaces	Networks
<input type="checkbox"/> tvi-0/41.0	<input type="checkbox"/> WAN1
<input type="checkbox"/> <b>tvi-0/100.0</b>	<input type="checkbox"/> WAN2

OK Cancel

6. Click OK.

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

- In Director view:
  - Select the Configuration tab in the top menu bar.
  - Select Templates > Device Templates in the horizontal menu bar.
  - Select an organization in left navigation panel.
  - Select a post-staging template in the main pane. The view changes to Appliance view.
- Select the Configuration tab in the top menu bar.
- Select Networking > Virtual Routers in the left menu bar.
- Click the **+** Add icon. In the Edit WAN3-Transport-VR popup window, select Virtual Router Details in the left menu bar.

**Edit WAN3-Transport-VR**

Virtual Router Details Static Routing OSPF RIP BGP PIM IGMP Router Advertisement Prefix Lists Redistribution Policies Instance Import Policies

Instance Name: WAN3-Transport-VR Description: Instance type: **Virtual routing instance** Global VRF ID:

MPLS VPN Core	Local Router Interface	Interfaces/Networks
<input checked="" type="checkbox"/> <b>EVPN Core</b>	<input type="text"/> Local Router Address: <input type="text"/> Local Router Interface: <b>tvi-0/100.0</b>	<input type="checkbox"/> <b>tvi-0/100.0</b>
	Family: inet	<input type="checkbox"/> tvi-0/608.0
		<input type="checkbox"/> tvi-0/612.0
		<input type="checkbox"/> tvi-0/616.0

☐ Create Dynamic GRE Tunnels ☐ Cloud Export Instance

OK Cancel


---

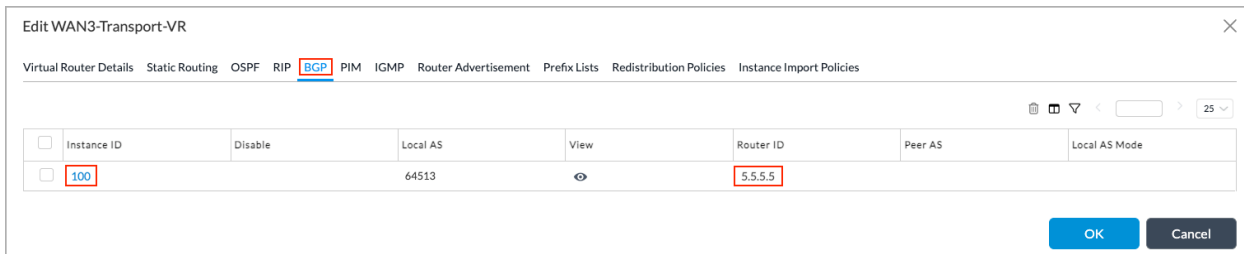
## Configure BGP

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 peer relationship between the local loopback interface (tvi-0/100) and the remote loopback interface (tvi-0/100) on the remote router (VTEP2).

1. In Director view:
  - a. Select the Configuration tab in the top menu bar.
  - b. Select Templates > Device Templates in the horizontal menu bar.
  - c. Select an organization in left navigation panel.
  - d. Select a post-staging template 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 BGP in the left menu bar.



Instance ID	Disable	Local AS	View	Router ID	Peer AS	Local AS Mode
<input type="checkbox"/> 100		64513		5.5.5.5		

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

Edit BGP Instance

General Prefix List SLA Profile Peer/Group Policy Peer Group Route Aggregation Damping Policy Versa Private TLV Advanced

Description: IBGP\_To\_VTEP2

Instance ID: 100

Router ID: 5.5.5.5

Local AS: 64513

Peer AS: 1 to 4294967295 Or <0.65535>.<0.65535> except

Local Address: tvi-0/100.0

Hold Time (seconds): Allowed Range is 3 - 65535

TTL: Allowed Range is 1 - 255

Password:

Local Network Name: --Select--

IBGP Preference: Allowed Range is 1 - 255

EBGP Preference: Allowed Range is 1 - 255

Local AS Mode: --Select--

AS Origination Interval: Allowed Range is 1 - 65535

SLA Community:

☐ Suppress Peer AS

☐ Relax First AS Check

☐ Community 4 byte

☐ Passive

☐ Remove All Private AS#

☐ Route Reflector Client

☐ Enable Alarms

☐ Site Of Origin

☐ Soft Reconfiguration

Prefix Limit Maximum: Allowed Range is 1 - 2147483647

Threshold: Allowed Range is 1 - 100

Restart Interval: Allowed Range is 30 - 86400

Action: --Select--

Family: L2VPN EVPN

Family	Loop Count	Prefix Limit		Restart Interval	Action	Soft Reconfiguration	
		Maximum	Threshold				
L2VPN EVPN	Allowed Range is 1 - 255	Allowed Range is 1 - 21474	Allowed Range is 1 - 100	Allowed Range is 30 - 8640	Drop	<input type="checkbox"/> Soft Reconfiguration	+

No Records to Display

OK Cancel

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

Edit BGP Instance

General Prefix List SLA Profile Peer/Group Policy Peer Group Route Aggregation Damping Policy Versa Private TLV Advanced

Peers

Name	Disable	Local AS	Type	Peer AS	Import	Export	Neighbor Address	Local Address	Allow	Local AS Mode	AS Origination Interval
IBGP_To_VTEP2			exte...				6.6.6.6	tvi-0/100.0			

OK Cancel

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

**Edit BGP Instance Edit Peer Group**

Name: IBGP\_To\_VTEP2

Description:

Type: IBGP

Peer AS: 1 to 4294967295 Or <0.65535>.<0.6553

Local Address: tvi-0/100.0

Disable: --Select--

Hold Time (seconds): Allowed Range is 3 - 65535

TTL: Allowed Range is 1 - 255

Password:

AS Origination Interval: Allowed Range is 1 - 65535

Local Network Name: --Select--

Local AS: 0 to 4294967295 Or <0.65535>.<0.6553

Local AS Mode: --Select--

Weight: Allowed Range is 1 - 2147483647

☐ Suppress Peer AS ☐ Relax First AS Check ☐ Soft Reconfiguration

**General** Neighbors Allow Advanced

Family	Loop Count	Prefix Limit		Restart Interval	Action	Soft Reconfiguration	
		Maximum	Threshold				
--Select--	Allowed Range is 1 - 2	Allowed Range is 1 - 2	Allowed Range is 1 - 1	Allowed Range is 30 -	--Select--	<input type="checkbox"/> Soft Reconfiguration	+
L2VPN EVPN					drop	false	⌵

OK Cancel

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

**Edit BGP Instance Edit Peer Group**

Name: IBGP\_To\_VTEP2

Description:

Type: IBGP

Peer AS: 1 to 4294967295 Or <0.65535>.<0.6553

Local Address: tvi-0/100.0

Disable: --Select--

Hold Time (seconds): Allowed Range is 3 - 65535

TTL: Allowed Range is 1 - 255

Password:

AS Origination Interval: Allowed Range is 1 - 65535

Local Network Name: --Select--

Local AS: 0 to 4294967295 Or <0.65535>.<0.6553

Local AS Mode: --Select--

Weight: Allowed Range is 1 - 2147483647

☐ Suppress Peer AS ☐ Relax First AS Check ☐ Soft Reconfiguration

General **Neighbors** Allow Advanced

	Neighbor IP	Disable	Local AS	Peer AS	Local Address	Import	Export	Local AS Mode
<input type="checkbox"/>	6.6.6.6			64514	tvi-0/100.0			

OK Cancel

10. Select the neighbor, and in the Edit BGP Instance Edit Peer Group popup window, select the Neighbors tab and Edit Neighbor, and enter the following information:

Edit BGP Instance
Edit Peer Group
Edit Neighbor

Neighbor IP \*

6.6.6.6

Peer AS

64514

Local Address

tvi-0/100.0

Hold Time (seconds)

Allowed Range is 3 - 65535

TTL

Allowed Range is 1 - 255

Password

Local Network Name

--Select--

Local AS

0 to 4294967295 Or <0..65535>.

Local AS Mode

--Select--

AS Origination Interval

Allowed Range is 1 - 65535

Weight

Allowed Range is 1 - 2147483647

☐ Suppress Peer AS

Description

Disable ⓘ

--Select--

☐ Relax First AS Check

☐ Soft Reconfiguration

General

Advanced

Family ⌵

Loop Count

Prefix Limit

Restart Interval

Action

Soft Reconfiguration

--Select--

Allowed Range is 1 - 1

Maximum

Threshold

Allowed Range is 1 - 1

Allowed Range is 30 -

--Select--

☐ Soft Reconfigur

L2VPN EVPN

drop

false


OK

Cancel

11. Click OK twice.

## Configure BGP on the Remote Router (VTEP2)

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

- In Director view:
  - Select the Configuration tab in the top menu bar.
  - Select Templates > Device Templates in the horizontal menu bar.
  - Select an organization in left navigation panel.
  - Select a post-staging template in the main pane. The view changes to Appliance view.
- Select the Configuration tab in the top menu bar.
- Select Networking > Virtual Routers in the left menu bar.
- Click the  Add icon. In the Edit WAN3-Transport-VR popup window, select BGP in the left menu bar.



Edit WAN3-Transport-VR

Virtual Router Details Static Routing OSPF RIP **BGP** PIM IGMP Router Advertisement Prefix Lists Redistribution Policies Instance Import Policies

<input type="checkbox"/>	Instance ID	Disable	Local AS	View	Router ID	Peer AS	Local AS Mode
<input type="checkbox"/>	100		64513	👁	6.6.6.6		

OK Cancel

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

Edit BGP Instance

**General** Prefix List SLA Profile Peer/Group Policy Peer Group Route Aggregation Damping Policy Versa Private TLV Advanced

Description: IBGP-To-VTEP1 Instance ID: 100 Disable: --Select--

Router ID: 6.6.6.6 Local AS: 64513 Peer AS: 1 to 4294967295 Or <0.65535>.<0.65535> excl Local Address: tvi-0/100.0

Hold Time (seconds): Allowed Range is 3 - 65535 TTL: Allowed Range is 1 - 255 Password: Local Network Name: --Select--

IBGP Preference: Allowed Range is 1 - 255 EBGP Preference: Allowed Range is 1 - 255 Local AS Mode: --Select-- AS Origination Interval: Allowed Range is 1 - 65535

SLA Community: ☐ Suppress Peer AS ☐ Relax First AS Check ☐ Community 4 byte

☐ Passive ☐ Remove All Private AS# ☐ Route Reflector Client ☐ Enable Alarms

☐ Site Of Origin ☐ Soft Reconfiguration

Prefix Limit Maximum: Allowed Range is 1 - 2147483647 Threshold: Allowed Range is 1 - 100 Restart Interval: Allowed Range is 30 - 86400 Action: --Select--

**Family** Debug

Family	Loop Count	Prefix Limit		Restart Interval	Action	Soft Reconfiguration	
		Maximum	Threshold				
L2VPN EVPN	Allowed Range is 1 - 255	Allowed Range is 1 - 21474	Allowed Range is 1 - 100	Allowed Range is 30 - 8640	Drop	<input type="checkbox"/> Soft Reconfiguration	+

No Records to Display

OK Cancel

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

Edit BGP Instance

General Prefix List SLA Profile Peer/Group Policy **Peer Group** Route Aggregation Damping Policy Versa Private TLV Advanced

<input type="checkbox"/>	Name	Disable	Local AS	Type	Peer AS	Import	Export	Peers		Allow	Local AS Mode	AS Origina
								Neighbor Address	Local Address			
<input type="checkbox"/>	IBGP_To_VTEP1			exte...				5.5.5.5	tvi-0/100.0			

OK Cancel

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

Edit BGP Instance Edit Peer Group

Name \* IBGP\_To\_VTEP1

Description

Type IBGP

Peer AS 1 to 4294967295 Or <0.65535>.<0.6553

Local Address tvi-0/100.0

Disable --Select--

Hold Time (seconds) Allowed Range is 3 - 65535

TTL Allowed Range is 1 - 255

Password

AS Origination Interval Allowed Range is 1 - 65535

Local Network Name --Select--

Local AS 0 to 4294967295 Or <0.65535>.<0.6553

Local AS Mode --Select--

Weight Allowed Range is 1 - 2147483647

☐ Suppress Peer AS ☐ Relax First AS Check ☐ Soft Reconfiguration

General Neighbors Allow Advanced

Family	Loop Count	Prefix Limit		Restart Interval	Action	Soft Reconfiguration	
		Maximum	Threshold				
--Select--	Allowed Range is 1 - 2	Allowed Range is 1 - 2	Allowed Range is 1 - 1	Allowed Range is 30 -	--Select--	<input type="checkbox"/> Soft Reconfigurati	+
L2VPN EVPN					drop	false	

OK Cancel

- Select the Neighbors tab, and configure the following information:

Edit BGP Instance Edit Peer Group

Name \* IBGP\_To\_VTEP1

Description

Type IBGP

Peer AS 1 to 4294967295 Or <0.65535>.<0.6553

Local Address tvi-0/100.0

Disable --Select--

Hold Time (seconds) Allowed Range is 3 - 65535

TTL Allowed Range is 1 - 255

Password

AS Origination Interval Allowed Range is 1 - 65535

Local Network Name --Select--

Local AS 0 to 4294967295 Or <0.65535>.<0.6553

Local AS Mode --Select--

Weight Allowed Range is 1 - 2147483647

☐ Suppress Peer AS ☐ Relax First AS Check ☐ Soft Reconfiguration

General Neighbors Allow Advanced

	Neighbor IP	Disable	Local AS	Peer AS	Local Address	Import	Export	Local AS Mode
<input type="checkbox"/>	5.5.5.5			64514	tvi-0/100.0			

OK Cancel

- Select the neighbor, and in the Edit BGP Instance Edit Peer Group popup window, select the Neighbors tab and Edit Neighbor, and enter the following information.

[https://docs.versa-networks.com/Secure\\_SD-WAN/01\\_Configuration\\_from\\_Director/SD-WAN\\_Configuration/Advanced\\_SD-W...](https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/SD-WAN_Configuration/Advanced_SD-W...)

Updated: Wed, 23 Oct 2024 08:11:12 GMT

Copyright © 2024, Versa Networks, Inc.

Edit BGP Instance Edit Peer Group Edit Neighbor

Neighbor IP \*

5.5.5.5

Peer AS

64514

Local Address

tui-0/100.0

Hold Time (seconds)

Allowed Range is 3 - 65535

TTL

Allowed Range is 1 - 255

Password

Local Network Name

--Select--

Local AS

0 to 4294967295 Or <0..65535>.

Local AS Mode

--Select--

AS Origination Interval

Allowed Range is 1 - 65535

Weight

Allowed Range is 1 - 2147483647

☐ Suppress Peer AS

Description

Disable ⓘ

--Select--

☐ Relax First AS Check

☐ Soft Reconfiguration

General

Advanced

Family

--Select--

Loop Count

Allowed Range is 1 -

Prefix Limit

Maximum

Allowed Range is 1 -

Threshold

Allowed Range is 1 -

Restart Interval

Allowed Range is 30 -

Action

--Select--

Soft Reconfiguration

☐ Soft Reconfigur

L2VPN EVPN

drop

false

OK

Cancel


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:

- In Director view:
  - Select the Configuration tab in the top menu bar.
  - Select Templates > Device Templates in the horizontal menu bar.
  - Select an organization in left navigation panel.
  - Select a post-staging template in the main pane. The view changes to Appliance view.
- Select the Configuration tab in the top menu bar.
- Select Networking > Virtual Switches in the left menu bar.
- Click the  Add icon. In the Edit VS1\_VXLAN popup window, select Virtual Switch Details in the left menu bar.
- Enter the following information.

6. 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 Configuration tab in the top menu bar.
  - b. Select Templates > Device Templates in the horizontal menu bar.
  - c. Select an organization in left navigation panel.
  - d. Select a post-staging template 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:

## Edit Bridge Domains

Bridge Domain Name \*

vlan-2000

VLAN ID \*

2000

## VXLAN VNI

2000

## Routing Interface

--Select--

## L2 Learning

✓ MAC Learning

☒ MAC Move

MAC Limit

16...131072

MAC Table Aging Time(seconds)

300

☐ Suppress Unknown Unicast☐ ARP Suppression

## BD Interfaces For VLAN Translation

Interfaces 

--Select--

No Records to Display

## Logical Interfaces

+    <  > 25 

Logical Interface Name

## MAC Learning

MAC Limit

### No Logical Interfaces Added

OK

Cancel

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

1. In Director view:
  - a. Select the Configuration tab in the top menu bar.
  - b. Select Templates > Device Templates in the horizontal menu bar.
  - c. Select an organization in left navigation panel.
  - d. Select a post-staging template 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.

## 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 Configuration tab in the top menu bar.
  - b. Select Templates > Device Templates in the horizontal menu bar.
  - c. Select an organization in left navigation panel.
  - d. Select a post-staging template 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 Virtual Switch Details in the left menu bar, and enter the following information:

Edit VS1\_VXLAN

×

Virtual Switch Details

Spanning Tree Protocol

EVPN

L2 Learning

Instance Name \*

VS1\_VXLAN

Description

Instance type

Virtual Switch

EVPN Service Type

VLAN Aware Bundle

▼

Route Distinguisher

1L:5

VRF Import Target

VRF Export Target

VRF Both Target

target:3L:3

☐

MPLS Services

☐

Interfaces

+

⌵

☐

vni-0/3.2000

Bridge Domains

+

⌵

⌂

🔍

<

>

25

▼

<input type="checkbox"/>	Bridge Domain Name	VLAN ID
<input type="checkbox"/>	vs1_vxlan	2000

OK

Cancel

6. Click OK.

## Configure the VLAN-to-VXLAN VNI Mapping for VTEP2

- In Director view:
  - Select the Configuration tab in the top menu bar.
  - Select Templates > Device Templates in the horizontal menu bar.
  - Select an organization in left navigation panel.
  - Select a post-staging template in the main pane. The view changes to Appliance view.
- Select the Configuration tab in the top menu bar.
- Select Networking > Virtual Switches in the left menu bar.
- Select a virtual switch, and edit it. In the Edit Bridge Domains popup window, enter the following information:

## Edit Bridge Domains

Bridge Domain Name \*

vlan-2000

VLAN ID \*

2000

VXLAN VNI

2000

## Routing Interface

--Select--

## L2 Learning

✓ MAC Learning

☒ MAC Move

MAC Limit

16...131072

MAC Table Aging Time(seconds)

300

☐ Suppress Unknown Unicast☐ ARP Suppression

## BD Interfaces For VLAN Translation

Interfaces 

--Select--

No Records to Display

## Logical Interfaces



Logical Interface Name

## MAC Learning

MAC Limit

No Logical Interfaces Added

OK

Cancel

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

1. In Director view:
  - a. Select the Configuration tab in the top menu bar.
  - b. Select Templates > Device Templates in the horizontal menu bar.
  - c. Select an organization in left navigation panel.
  - d. Select a post-staging template 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:





6. Select the MAC Address Table in the horizontal menu bar.
7. Select a switch name from the first drop-down list.
8. Select a VLAN from the second drop-down list.
9. Select the type of output to display from 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-0/440 bridge domain interface connected to the remote branch/VTEP at Branch2.

The screenshot shows the Network Configuration page with the 'Switching' tab selected. Under the 'Switching' tab, the 'MAC Address Table' sub-tab is active. The configuration shows 'Tenant1-default-switch' and 'vlan-1'. The output type is set to 'Brief'. The table below displays the MAC Address Table for the selected interface and VLAN.

Bd Interface	MAC Address	VLAN ID	MAC Type	Remote Branch / VTEP
dtvi-0/440	06:30:f8:45:f0:01	1	SC	Branch2
enet-0/6.1	00:11:08:00:00:00	1	D	N/A
enet-0/6.1	00:11:08:00:00:01	1	D	N/A
enet-0/6.1	00:11:08:00:00:02	1	D	N/A
enet-0/6.1	00:11:08:00:00:03	1	D	N/A
enet-0/6.1	00:11:08:00:00:04	1	D	N/A

10. Select the Ingress Table tab to display the remote VXLAN tunnel endpoints. The following screenshot shows the interface VLAN 1.

The screenshot shows the Network Configuration page with the 'Switching' tab selected. Under the 'Switching' tab, the 'Ingress Table' sub-tab is active. The configuration shows 'Tenant1-default-switch' and 'vlan-1'. The table below displays the Ingress Table for the selected interface and VLAN.

Access Circuit	Interface VLAN	Encap Type	BC Label / VNI ID	Remote Branch / Tunnel IP
enet-0/4.2	1	N/A	N/A	N/A
dtvi-0/440	1	SDWAN	24716	Branch2
enet-0/6.1	1	N/A	N/A	N/A

## Supported Software Information

Releases 21.2.1 and later support all content described in this article, except:

- Releases 22.1.1 and later support EVPN type 5 routes.

## Additional Information

[Configure EVPN Multihoming for SD-WAN](#)

[Configure EVPN Multihoming for Hosts Using ZT-LAN](#)

[https://docs.versa-networks.com/Secure\\_SD-WAN/01\\_Configuration\\_from\\_Director/SD-WAN\\_Configuration/Advanced\\_SD-W...](https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/SD-WAN_Configuration/Advanced_SD-W...)

Updated: Wed, 23 Oct 2024 08:11:12 GMT

Copyright © 2024, Versa Networks, Inc.

[Configure EVPN VXLAN for 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)