# Configure Layer 2 Forwarding

*For supported software information, click here.*

Layer 2 forwarding allows a switching device to transmit traffic on a LAN based on the destination Media Access Control (MAC) addresses of the devices connected to the LAN. You can configure a Versa Operating System$^{TM}$ (VOS$^{TM}$) device as a virtual switch, which is a software object that functions like a hardware-based Layer 2 switch. A VOS device acting as a virtual switch can perform the functions of a standard switch. Just as with a physical switch, on a virtual switch you configure the Spanning-Tree Protocol (STP), EVPN, and Layer 2 learning.

This article describes how to configure Layer 2 forwarding on a VOS device.

## Layer 2 Forwarding Overview

VOS devices support the following Layer 2 forwarding features:

- Virtual switches, bridge domains, and interfaces—You enable VOS Layer 2 forwarding by defining a virtual switch instance (VSI). For a single VOS instance, you can configure multiple VSIs, and within each VSI, you can configure multiple bridge domains. Each bridge domain has its own MAC forwarding table and forms a distinct learning and forwarding domain. You add interfaces of type *bridge* to a virtual switch.
- IRB interfaces—Integrated routing and bridging (IRB) associates a Layer 3 interface with a Layer 2 bridge domain so that packets can be routed to and from the bridge domain. On IRB interfaces, you can configure all standard Layer 3 interface settings, such as DHCP and VRRP.
- Trunk Layer 2 ports—Trunk Layer 2 ports allow you to configure multiple VLANs on an interface. These trunk ports are also known as *enterprise-style* trunk ports.
- Native VLAN IDs—Native VLAN IDs are used in conjunction with trunk Layer 2 ports to allow an untagged packet to be treated as a tagged packet.
- Access interfaces—An access interface is an interface with an explicit VLAN ID. Any untagged packet that arrives on an access interface is associated with that interface and is treated as a tagged packet with the VLAN ID of the access interface.
- MAC features—VOS devices support the following MAC features:
  - MAC learning—Dynamically builds and maintains Layer 2 forwarding tables.
  - MAC aging—Allows you to specify how long an inactive MAC address remains in a Layer 2 forwarding table.
  - MAC limit—Controls the maximum number of MAC addresses that can be dynamically learned.
  - MAC move—Allows a switch to update its Layer 2 forwarding table if the switch receives a packet whose MAC address matches an existing entry but that arrives on a different port than is stored in the existing forwarding table entry.

    - Static MAC addresses—Allows you to configure MAC addresses that remain in the forwarding table after the device is rebooted.
- RSTP—Rapid Spanning-Tree Protocol, which is defined in IEEE 802.1w, enables fast spanning-tree reconvergence by simplifying the port states and changing the way ports transition between states.
- EVPN (type 2 and type 3) over SD-WAN—(For Releases 21.1.1 and later.) VOS devices support the following EVPN features:
    - One route target (RT) and route distinguisher (RD) per virtual switch.
    - Selective signaling of certain bridge domains.
    - Broadcast and multicast labels per bridge domain VLAN.
    - Distribution of local IRB and VRRP MAC addresses through BGP.
    - Centralized IRB, in which an IRB is configured in one of the provider edge (PE) devices and all traffic that needs to be routed is carried to that PE and is routed on that node.
- MSTP—(For Releases 21.1.1 and later.) Multiple Spanning-Tree Protocol is an extension of the STP and RSTP protocols that enables the use of alternate spanning trees for different VLANs or groups of VLANs. Using alternate spanning trees can allows alternate paths being to be used more effectively.
- VLAN translation—(For Releases 21.1.1 and later.) A VLAN identifier in a packet acts like a circuit identifier and is normalized to the bridge domain VLAN for learning and forwarding purposes. When the packet egresses the logical interface, it is translated to a VLAN logical interface.

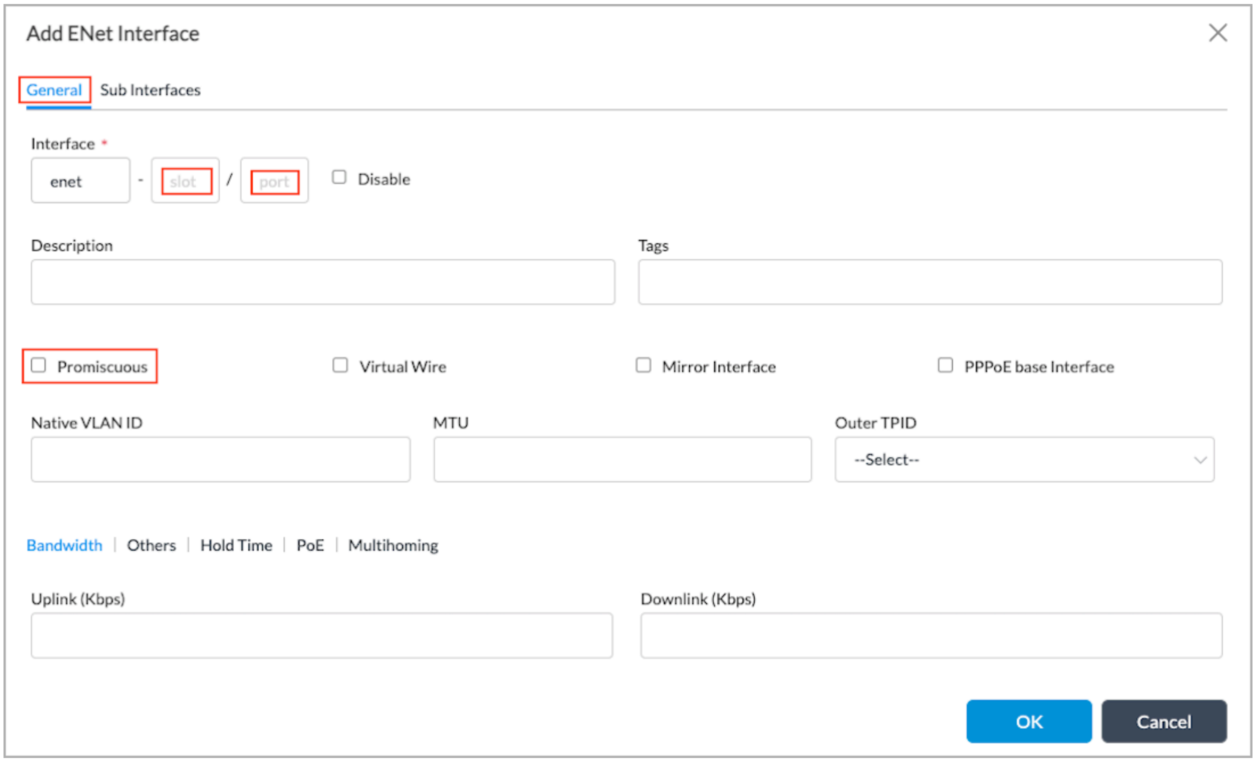
# Configure Bridge Interfaces

To create a virtual switch, you must configure an interface whose type is *bridge*. In additional, at the organization level, you must identify the Layer 2 interfaces to use to forward Layer 2 traffic. If you do not identify the interfaces, all Layer 2 traffic for that organization is dropped. Also, you can configure paired tunnel virtual interfaces (TVIs) as family bridge interfaces

## Configure a Bridge Interface

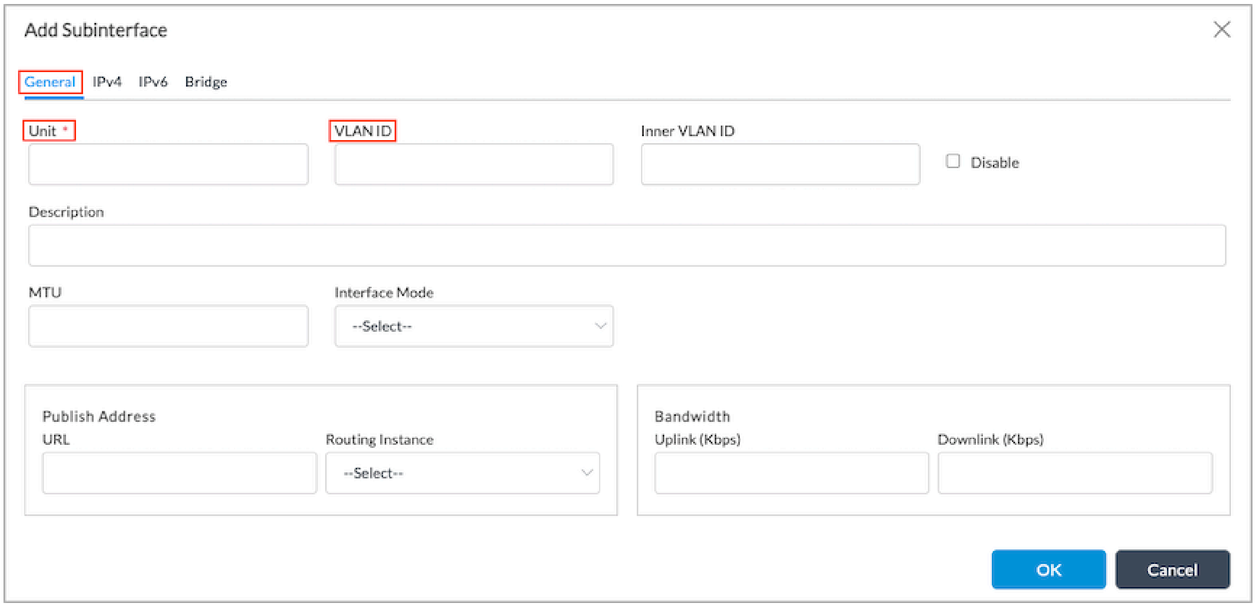
To configure a bridge interface:

1. In Director view:
    a. Select the Administration tab in the top menu bar.
    b. Select Appliances in the left menu bar.
    c. Select an appliance in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > Interfaces in the left navigation bar. The main pane displays the Interfaces table.
4. Select the Ethernet tab
5. Click the + Add icon. The Add ENet Interface popup window displays.



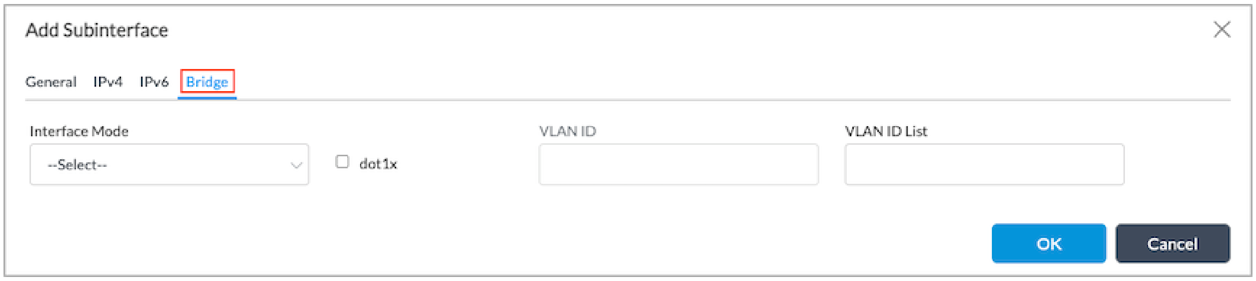
6. In the Interface field, enter the slot and port numbers.
7. Click Promiscuous. Note that you must enable promiscuous mode on a bridge interface.

8. Select the Subinterfaces tab, and then click the + Add icon.
9. Select the General tab, and then enter information for the following fields.



| Field | Description |
|---|---|
| Unit (Required) | Enter the unit number of the subinterface. Note that the family type bridge is not supported on unit 0. |
| VLAN ID | Enter the VLAN ID of the subinterface. |

10. Select the Bridge tab, and then enter information for the following fields.



| Field | Description |
|---|---|
| Interface Mode | Select the interface mode:<br>◦ Access<br>◦ Trunk |
| ◦ dot1x | If you select the Access interface mode, click to enable 802.1x on the subinterface. |
| VLAN ID | If you select the Access interface mode but do not enable 802.1x, enter a single VLAN identifier for the subinterface. To associate the subinterface with a bridge domain, the VLAN ID of the subinterface must be the same as the VLAN ID of the bridge domain.<br>If you select the Access interface mode and enable 802.1x, the value "dot1x" is automatically entered in the VLAN ID field.<br>*Range:* 1 through 4094 |
| VLAN ID List | If you select the Trunk interface mode, enter a list of VLAN identifiers. You can enter a range of VLANs (for example, 10-20), a list of VLAN IDs separated by |

| Field | Description |
|---|---|
| | spaces (for example, 1 25 27), or as a combination of the two (for example, 1 15-20 25 27). |

11. Click OK in the Add Subinterface popup window.
12. Click OK in the Add Ethernet Interfaces popup window.

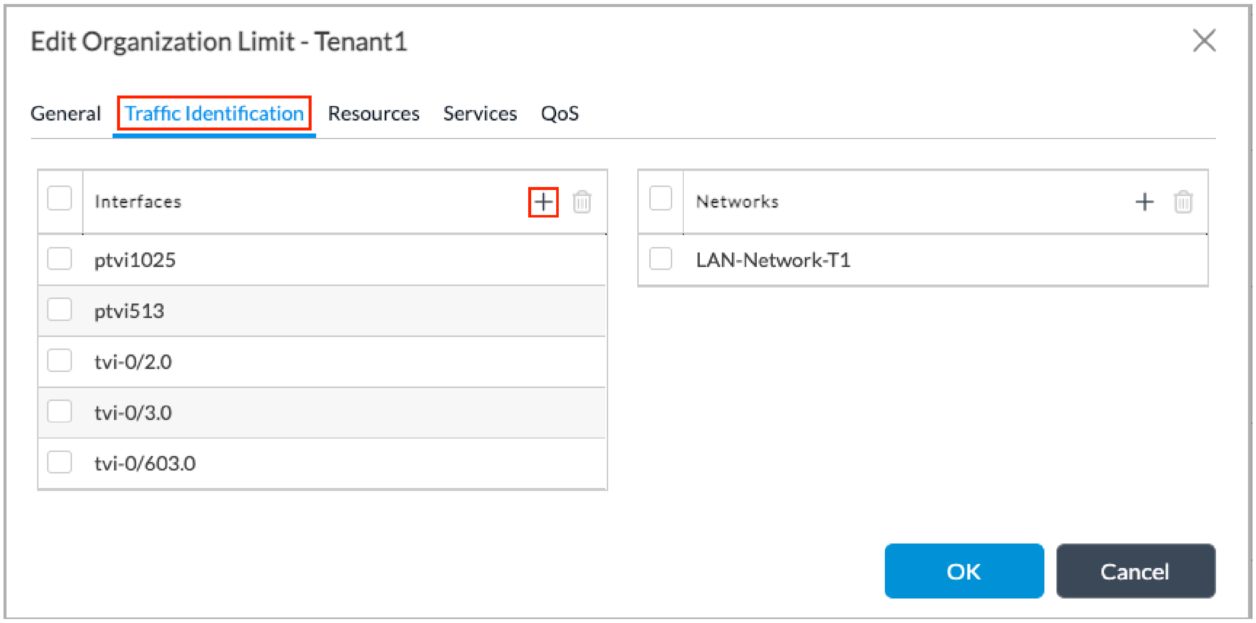
## Configure Layer 2 Traffic Identification

*For Releases 21.1.1 and later.*

At the organization level, you must identify the Layer 2 interfaces to use to forward Layer 2 traffic. If you do not identify the interfaces, all Layer 2 traffic for that organization is dropped.

To configure Layer 2 traffic identification for an 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 an appliance in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Others > Organizations > Limits in the left menu bar.
4. Select an organization in the main pane. The Edit Organization Limit popup window displays.
5. Select the Traffic Identification tab, click the Add icon in the Interfaces table, and select an interface.



Edit Organization Limit - Tenant1

| □ Interfaces |
|---|
| □ ptvi1025 |
| □ ptvi513 |
| □ tvi-0/2.0 |
| □ tvi-0/3.0 |
| □ tvi-0/603.0 |

| □ Networks |
|---|
| □ LAN-Network-T1 |

6. Repeat Step 5 to add additional interfaces.
7. Click OK.

## Configure Paired TVI Interfaces as Family Bridge Interfaces

*For Releases 21.1.1 and later.*

You can configure paired TVI interfaces as family bridge interfaces, and they can be either trunk or access interfaces. You can use bridge paired TVI interfaces to connect Layer 2 domains in hub nodes that use either the same or different Layer 2 technologies within a branch. For example, with bridge paired TVI interfaces, you can:

- Interconnect a VXLAN domain with an SD-WAN domain.
- Interconnect two SD-WAN domains.
- Interconnect two VXLAN domains.

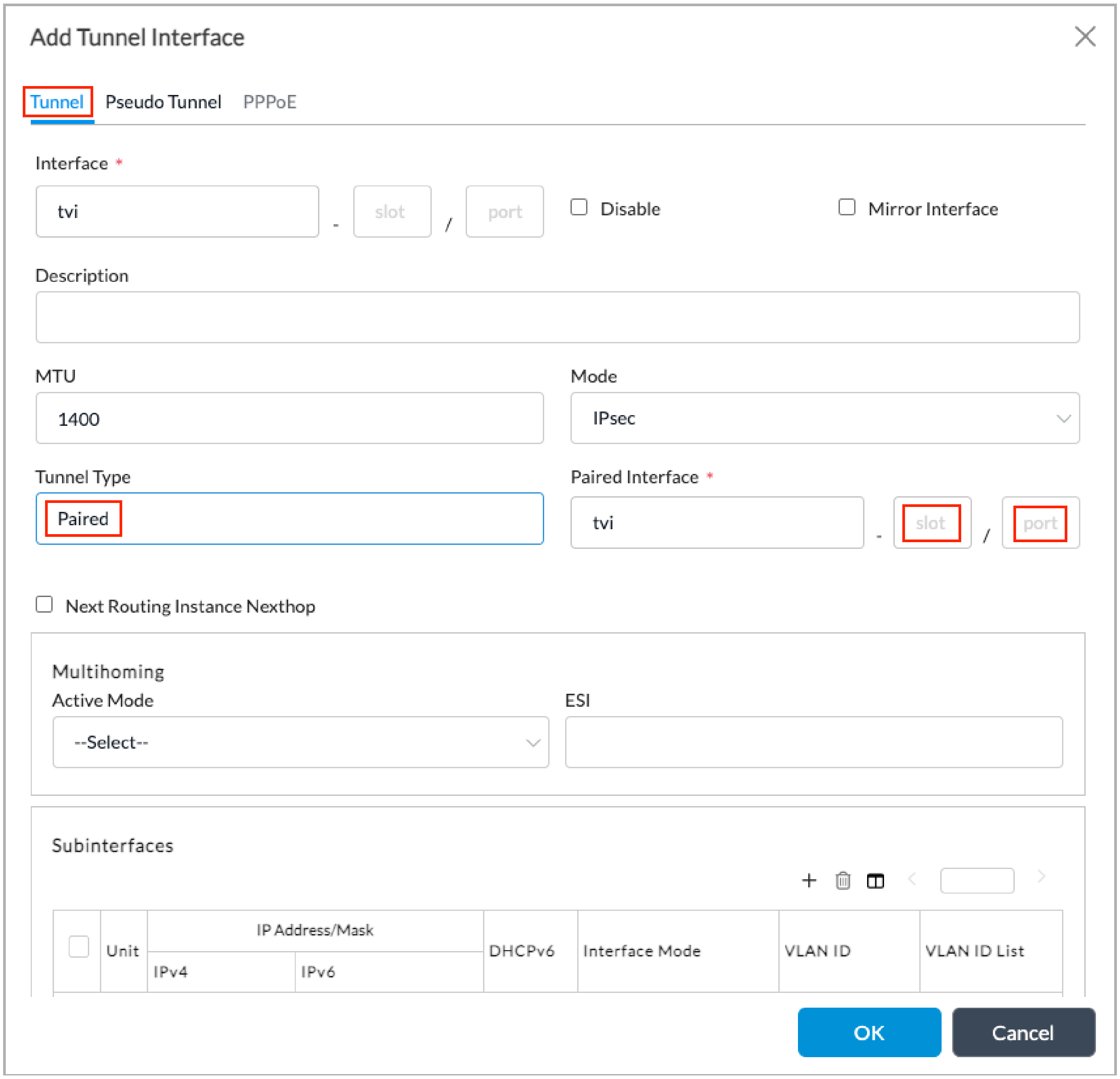
Bridge paired TVI interfaces support all spanning-tree protocols (STP, RSTP, and MSTP) to prevent accidental loops.

You configure family bridge paired TVI interfaces the same way that you configure all other Layer 2 logical interfaces, except for the following:

- Only one unit is supported for trunk and access interface modes, whereas more than one unit is supported in a service provider–type configuration.
- The unit number of a bridge paired TVI interface cannot be 0.
- Paired TVI interfaces do not support VLAN translation.

To configure a family bridge paired TVI interface:

1. In the Director view:
    a. Select the Administration tab in the top menu bar.
    b. Select Appliances in the left menu bar.
    c. Select an appliance in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select the Networking tab > Interfaces > Tunnel tab in the left menu bar.
4. Click the + Add icon. In the Add Tunnel Interface popup window, select the Tunnel tab and then enter information for the following fields.



Add Tunnel Interface

Interface *: tvi - slot / port

□ Disable □ Mirror Interface

Description:

MTU: 1400

Mode: IPsec

Tunnel Type: Paired

Paired Interface *: tvi - slot / port

□ Next Routing Instance Nexthop

Multihoming

Active Mode: --Select--

ESI:

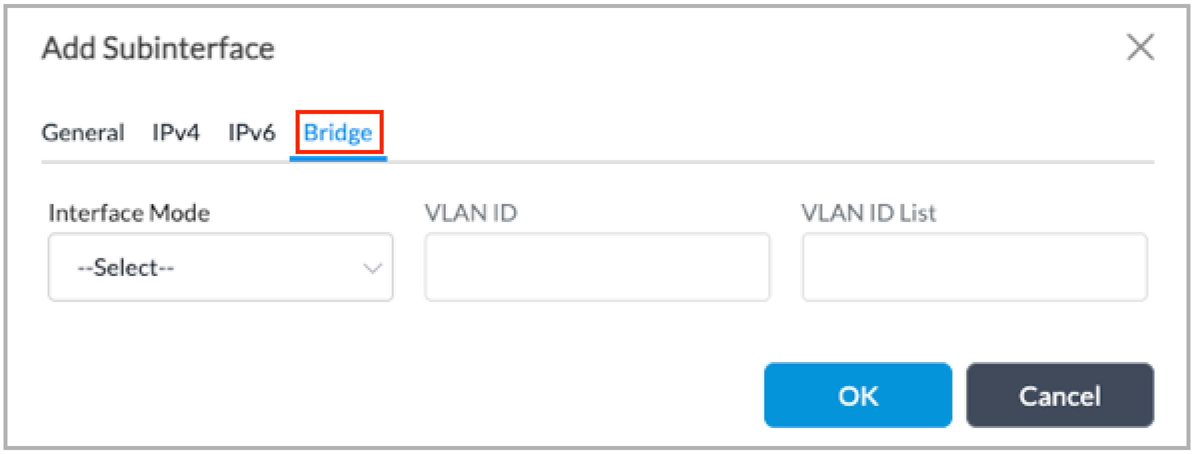
Subinterfaces

| □ | Unit | IP Address/Mask | | DHCPv6 | Interface Mode | VLAN ID | VLAN ID List |
|---|---|---|---|---|---|---|---|
| | | IPv4 | IPv6 | | | | |

| Field | Description |
|---|---|
| Interface Slot/Port (Required) | Enter the unit number and port number of the interface. For family bridge interfaces, the unit number cannot be 0. |
| Tunnel Type | Select Paired. |
| Paired Interface (Required) | Enter the slot number and the port number of the paired interface. |

5. In the Subinterfaces table, click the + Add icon. In the Add Subinterfaces popup window, select the Bridge tab,

and then enter information for the following fields.



| Field | Description |
|---|---|
| Interface Mode | Select the interface mode:<br>◦ Access<br>◦ Trunk |
| VLAN ID | For access interfaces, enter a single VLAN identifier for the subinterface. To associate the subinterface with a bridge domain, the VLAN ID of the subinterface must be the same as the VLAN ID of the bridge domain.<br>*Range:* 1 through 4094 |
| VLAN ID List | Enter a list of VLAN identifiers. You can enter a range of VLANs (for example, 10-20), a list of VLAN IDs separated by spaces (for example, 1 25 27), or a combination of the two (for example, 1 15-20 25 27). |

6. Click OK.

## Configure IRB Interfaces

You create an IRB interface to associate a Layer 3 interface with a bridge domain so that packets can be routed to and from a Layer 2 bridge domain. You can configure all standard Layer 3 interface settings, such as DHCP and VRRP, on an IRB interface.

To decide whether to route or bridge an incoming packet, a virtual switch uses information in the Layer 2 frame's MAC address. If the destination MAC address in the ingress frame matches the MAC address of one of the IRB interfaces, the packet is routed using that IRB as the ingress interface, and the packet is treated as Layer 3 packet. If the destination MAC address of the ingress frame does not match the MAC address of one of the IRB interfaces, the packet is bridged based on the destination MAC address. Other switches obtain the MAC address of an IRB interface by issuing an Address Resolution Protocol (ARP) request for the associated IP address.

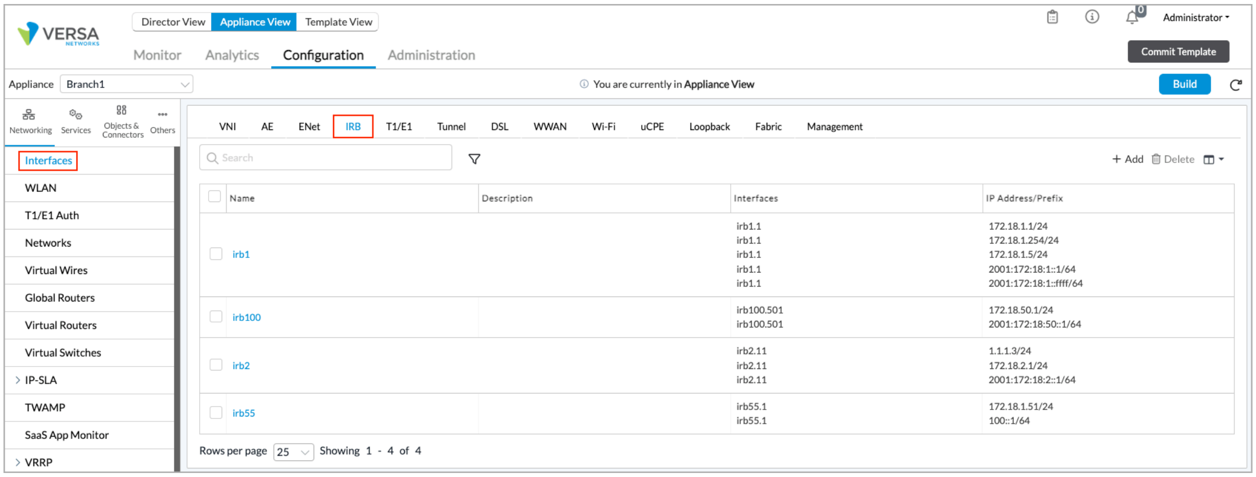
An IRB interface is operationally up when any one of the Layer 2 interfaces associated with the corresponding bridge domain is up. When all associated Layer 2 interfaces of a bridge domain are down, the IRB interface is considered to be operationally down.

For Releases 21.1.1 and later, the state of an IRB interface depends on the following:

- State of all underlying Layer 2 logical interfaces. For EVPN, this includes the state of remote TVIs that belong to that bridge domain.
- State of all underlying Layer 2 *x*STP interfaces.
- Administrative state of the IRB.

To configure an IRB interface:

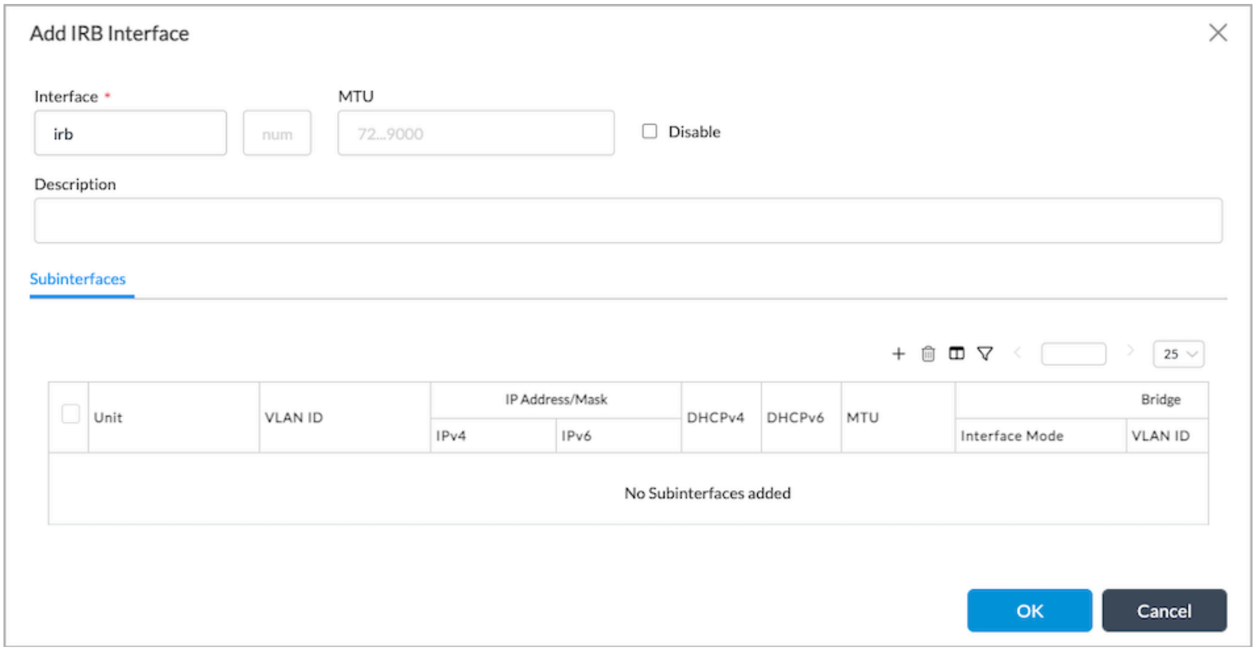
1. In Director view.
    a. Select the Administration tab in the top menu bar.
    b. Select Appliances in the left menu bar.
    c. Select an appliance in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Configuration > Networking > Interfaces in the left menu bar. The main pane displays the Interfaces table.
4. Select the IRB tab.



| Name | Description | Interfaces | IP Address/Prefix |
|---|---|---|---|
| irb1 | | irb1.1<br>irb1.1<br>irb1.1<br>irb1.1<br>irb1.1 | 172.18.1.1/24<br>172.18.1.254/24<br>172.18.1.5/24<br>2001:172:18:1::1/64<br>2001:172:18:1::ffff/64 |
| irb100 | | irb100.501<br>irb100.501 | 172.18.50.1/24<br>2001:172:18:50::1/64 |
| irb2 | | irb2.11<br>irb2.11<br>irb2.11 | 1.1.1.3/24<br>172.18.2.1/24<br>2001:172:18:2::1/64 |
| irb55 | | irb55.1<br>irb55.1 | 172.18.1.51/24<br>100::1/64 |

Rows per page 25 Showing 1 - 4 of 4

5. Click the + Add icon. In the Add IRB Interface popup window, enter information for the following fields.



Interface: irb | num

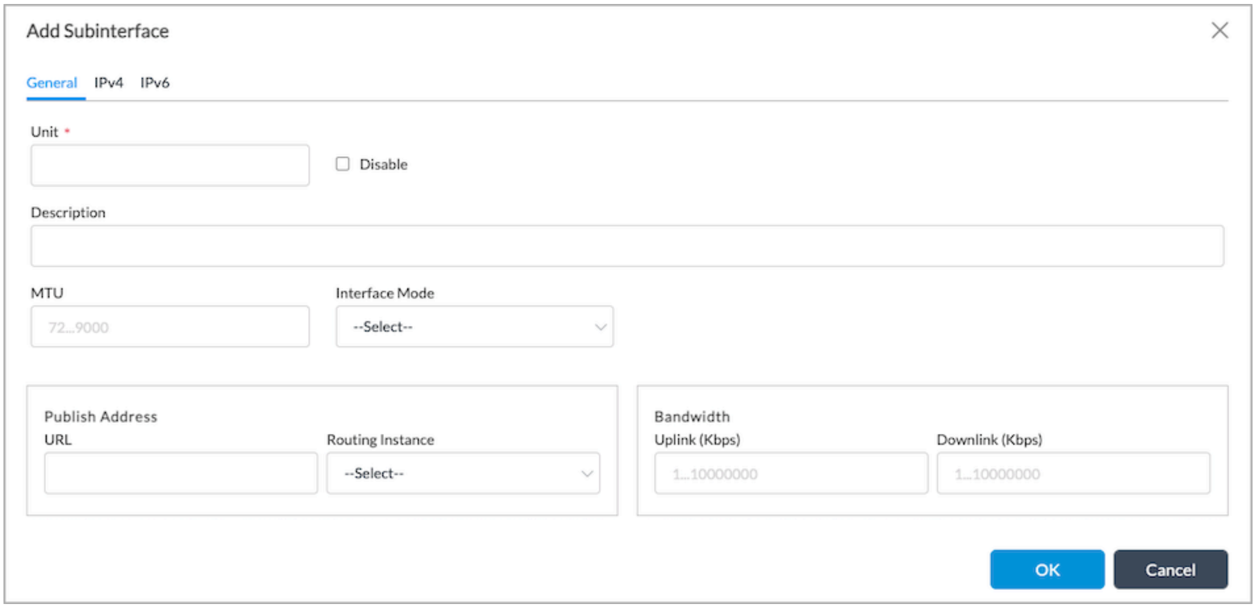
MTU: 72...9000

☐ Disable

| | Unit | VLAN ID | IP Address/Mask | | DHCPv4 | DHCPv6 | MTU | Bridge | |
|---|---|---|---|---|---|---|---|---|---|
| | | | IPv4 | IPv6 | | | | Interface Mode | VLAN ID |
| ☐ | No Subinterfaces added | | | | | | | | |

| Field | Description |
|---|---|
| Interface (Required) | Enter the IRB interface number.<br>*Range:* 1 through 128. |
| Disable | Click to not activate the IRB interface after you configure it. |
| Description | Enter a text description for the IRB interface. |
| Subinterfaces (Table) | Lists the subinterfaces that are already configured. |

6. Click the + Add icon. In the Add Subinterface popup window, configure the IRB subinterface. You configure an IRB subinterface the same way as you configure an Ethernet subinterface. For more information, see [Configure WAN Ethernet Interfaces](). Note, however, that each IRB interface can support only one unit, and the unit number range is 1 through 4094. However, unlike Ethernet interfaces, you cannot configure the following on IRB interfaces: VLAN ID, inner VLAN ID, bridge mode, and standby.



7. Click OK.

## Configure a Virtual Switch with Bridge Domains and Bridge Interfaces

To enable Layer 2 forwarding, you must define a VSI. You can configure multiple VSIs within a single VOS instance.

Within a VSI, you can configure multiple bridge domains. A bridge domain is a set of logical interfaces in a virtual switch that are part of the same broadcast domain. Each bridge domain is associated with a unique VLAN ID, and each bridge domain has its own MAC forwarding table and forms a distinct learning and forwarding domain. You add the interfaces of family bridge to a virtual switch.

To associate an interface with a specific bridge domain, you configure the VLAN ID of the interface to be the same as the VLAN ID of the bridge domain in the virtual switch.

To illustrate how virtual switches and VSI interfaces work, let's look at an example. Suppose you configure a virtual switch (vs1) as follows:

- Configure two bridge domains, bd1, and bd2.
- Assign VLAN ID 10 to bd1, and VLAN ID 20 to bd2.
- Add interfaces. In this discussion, we add WAN interfaces vni-0/0.1, vni-0/0.2, vni-0/1.1, and vni-0/1.2. For LAN interfaces, you can add enet interfaces.

To have the vni-0/0.1 and vni-0/1.1 interfaces be part of bridge domain bd1, you assign them VLAN ID 10. To have the vni-0/0.2 and vni-0/1.2 interfaces be part of bridge domain bd2, you assign them VLAN ID 20.

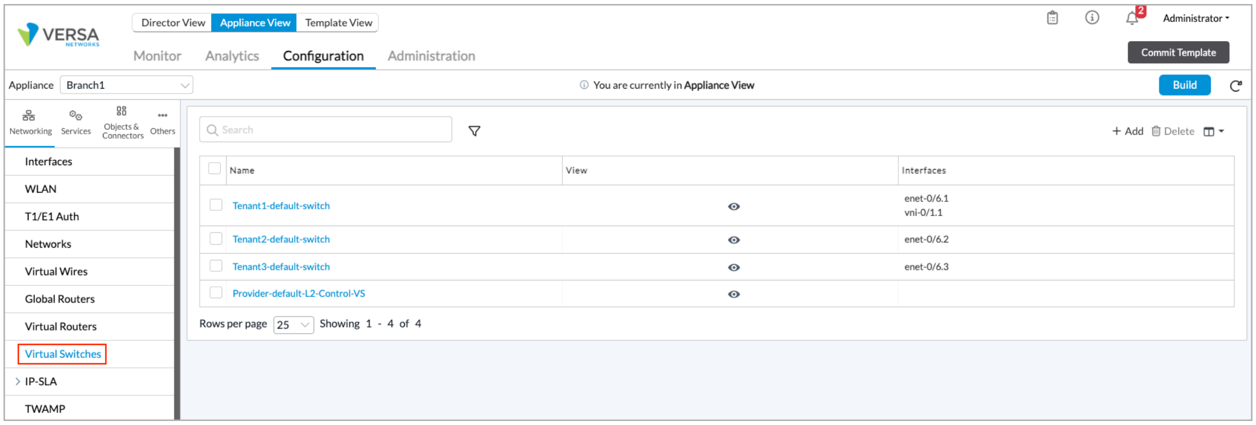
When traffic enters a virtual switch, the interface in the bridge domain learns the source MAC addresses from the VNI interfaces in its domain. In our example of the vs1 virtual switch, the MAC addresses that the vni-0/0.1 and vni-0/1.1

interfaces learn belong to bridge domain bd1, and the MAC addresses that the vni-0/0.2 and vni-0/1.2 interfaces learn belong to bridge domain bd2

When traffic enters virtual switch vs1, the source MAC addresses are learned by the interface in the bridge domain to which the ingress interface belongs. In this example, the MAC addresses learned by vni-0/0.1 and vni-0/1.1 belong to bridge domain bd1, and the MAC addresses learned by vni-0/0.2 and vni-0/1.2 belong to bridge domain bd2. All traffic, that is, all unicast traffic and all broadcast, unknown, and multicast (BUM) traffic, is forwarded only within the bridge domain to which the ingress interface belongs. For example, BUM traffic that originates from vni-0/0.1 is flooded only to the other interfaces in bridge domain bd1 (in this case, vni-0/1.1). Similarly, unicast traffic is forwarded to one of the interfaces in the bridge domain. For example, a packet entering vs1 through vni-0/0.1 that has a destination MAC address that matches interface vni-0/1.1 is forwarded only to vni-0/1.1.

To create a virtual switch with bridge domains:

1. In Director view:
    a. Select the Administration tab in the top menu bar.
    b. Select Appliances in the left menu bar.
    c. Select an appliance in the main pane. The view changes to Appliance view.
2. Select Configuration in the top menu bar.
3. Select Networking > Virtual Switches in the left menu bar. The main pane displays a list of the already configured virtual switches.



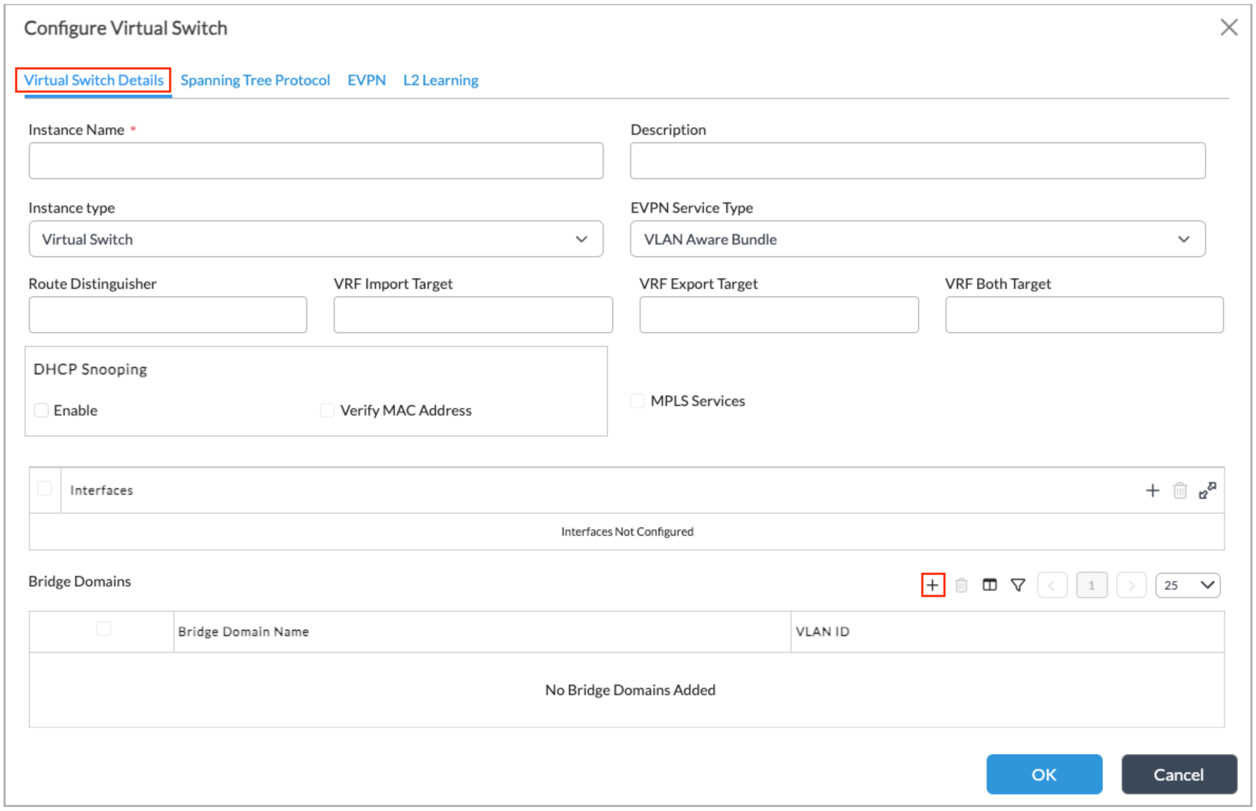
Appliance Branch1

You are currently in Appliance View

| Name | View | Interfaces |
|---|---|---|
| Tenant1-default-switch | 👁 | enet-0/6.1<br>vni-0/1.1 |
| Tenant2-default-switch | 👁 | enet-0/6.2 |
| Tenant3-default-switch | 👁 | enet-0/6.3 |
| Provider-default-L2-Control-VS | 👁 | |

Rows per page 25 Showing 1 - 4 of 4

4. Click the + Add icon. In the Configure Virtual Switch popup window, select the Virtual Switch Details tab, and then enter the information for the following fields.



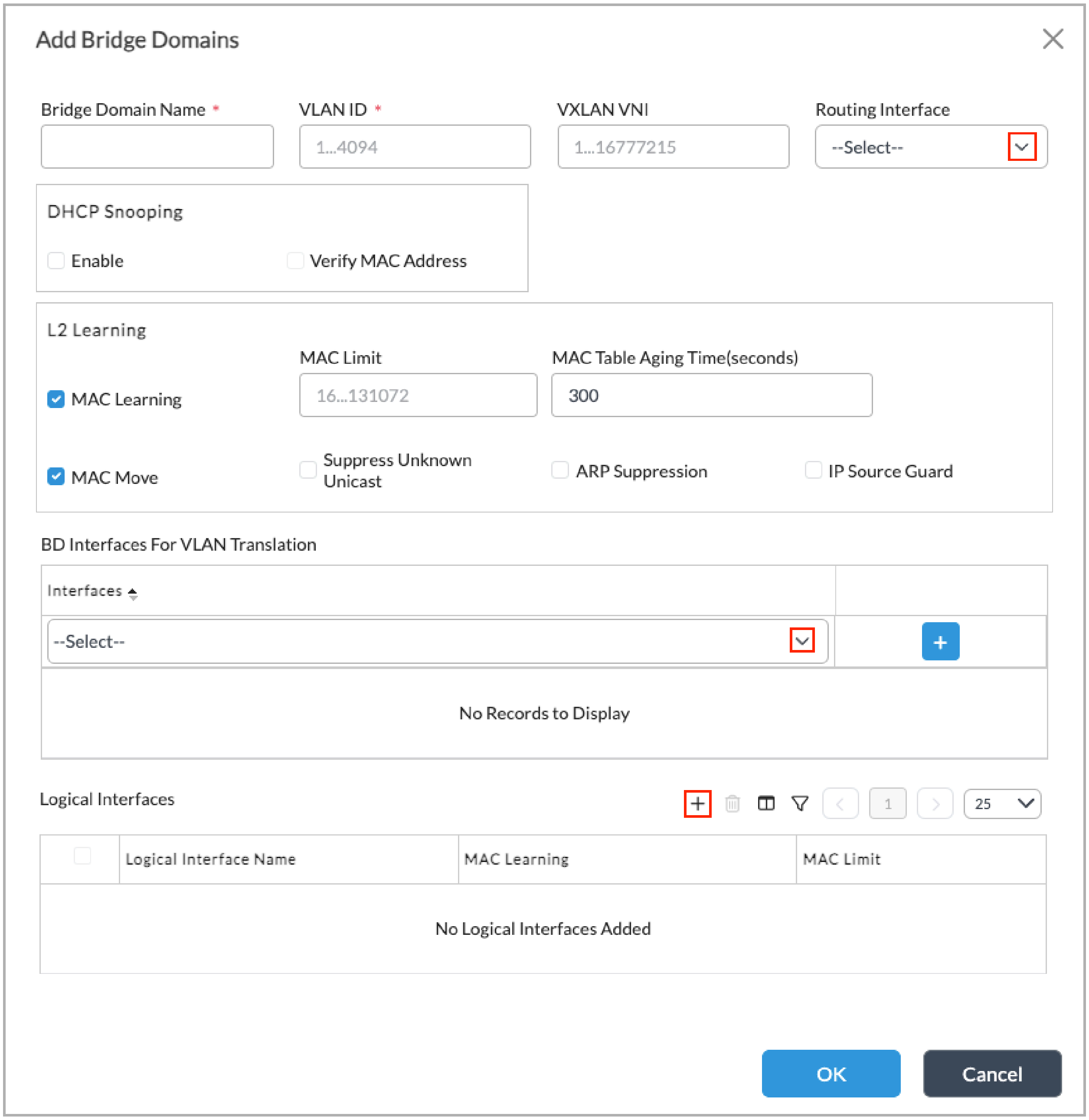
Instance type: Virtual Switch

EVPN Service Type: VLAN Aware Bundle

| Field | Description |
|---|---|
| Instance Name (Required) | Enter a name for the virtual switch. |
| Description | Enter a text description for the virtual switch. It can be a text string up to 255 characters. |
| Instance Type | Select Virtual Switch. |
| EVPN Service Type | (For Releases 22.1.1 and later.) Select the EVPN service type:<br>◦ VLAN-Aware Bundle—Map multiple VLANs to an EVPN instance (EVI).<br>◦ VLAN—Map a single VLAN to an EVI. |
| Route Distinguisher | Enter the route distinguisher for the instance. |
| VRF Import Target | Enter the target community to use when filtering imported EVPN routes. |
| VRF Export Target | Enter the target community to use when exporting EVPN routes. |

| Field | Description |
|---|---|
| VRF Both Target | Enter the target community to use when exporting EVPN routes and when filtering them when they are imported. |
| DHCP Snooping (Group of Fields) | (For Releases 22.1.4 and later.) Configure DHCP snooping. For more information, see Configure DHCP Snooping. |
| MPLS Services | (For Releases 22.1.1 and later.) Click to enable services for Layer 2 MPLS traffic. If you enable MPLS services, you must also enable Layer 2 services for the organization that owns the virtual switch. For more information, see Configure Layer 2 Services. |
| Interfaces | Click the + Add icon, and then select one or more interfaces to add to the virtual switch. |
| Bridge Domains (Table) | Displays the bridge domains that are already configured. Continue with Step 6 to add bridge domains. |

6. Click the + Add icon in the Bridge Domains table. In the Add Bridge Domains popup window, enter information for the following fields.



Add Bridge Domains

Bridge Domain Name *

VLAN ID * 1...4094

VXLAN VNI 1...16777215

Routing Interface --Select--

DHCP Snooping

□ Enable □ Verify MAC Address

L2 Learning

☑ MAC Learning

MAC Limit 16...131072

MAC Table Aging Time(seconds) 300

☑ MAC Move □ Suppress Unknown Unicast □ ARP Suppression □ IP Source Guard

BD Interfaces For VLAN Translation

| Interfaces | |
|---|---|
| --Select-- | + |

No Records to Display

Logical Interfaces

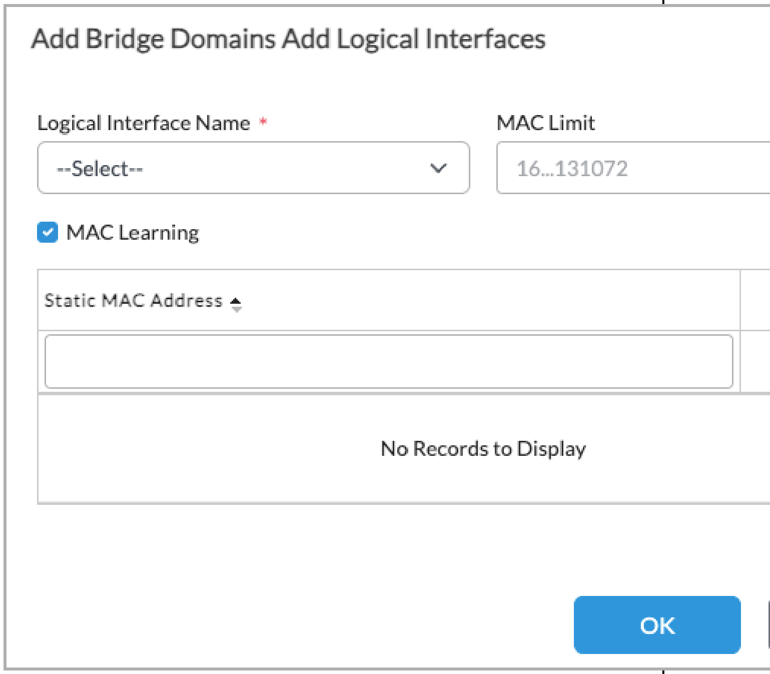
| □ | Logical Interface Name | MAC Learning | MAC Limit |
|---|---|---|---|

No Logical Interfaces Added

| Field | Description |
|---|---|
| Bridge Domain Name (Required) | Enter a name for the bridge domain. |
| VLAN ID (Required) | Enter the VLAN ID of the bridge domain. Each bridge domain must have a unique VLAN ID.<br>*Range:* 1 through 4094 |

| Field | Description |
|---|---|
| VXLAN VNI | Enter a VXLAN VNI number.<br>*Range*: 1 through 16777215<br>*Default*: 1 |
| Routing Interface | Select the IRB interface for the bridge domain. |
| DHCP Snooping (Group of Fields) | (For Releases 22.1.4 and later.) Enable DHCP snooping. For information, see Configure DHCP Snooping. |
| Layer 2 Learning (Group of Fields) | |
| ◦ MAC Learning | Click to enable or disable MAC learning. By default, MAC learning is enabled. |
| ◦ MAC Limit | Enter the maximum number of MAC addresses that can be dynamically learned by the virtual switch.<br>*Range:* 16 through 131072<br>*Default:* None |
| ◦ MAC Table Aging Time | Enter how long an inactive MAC address remains in a Layer 2 forwarding table, in seconds.<br>*Range:* 10 through 3600 seconds<br>*Default:* 300 seconds |
| ◦ MAC Move | Click to enable or disable MAC loop detection and prevention at the bridge-domain level. For more information, see Configure MAC Move, below. |
| ◦ Suppress Unknown Unicast | Click to suppress the broadcast of unknown unicast traffic in the EVPN core.<br>*Default:* Suppression is disabled. |
| ◦ ARP Suppression | (For Releases 22.1.1 and later.) Click to prevent the flooding of ARP requests across an EVPN network. ARP suppression prevents the flooding of ARP |

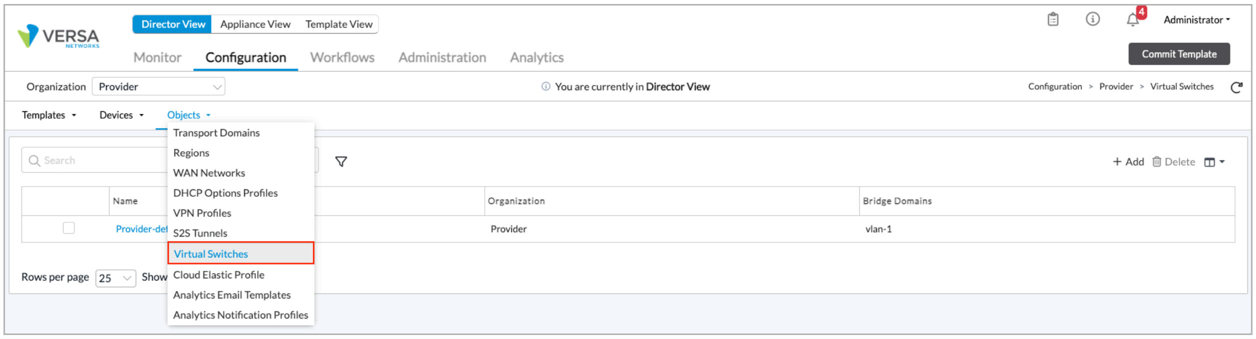
| Field | Description |
|---|---|
| | requests across an EVPN network. When enabled, ARP suppression sends the IP addresses from the locally learned ARP entries and the MAC addresses across the EVPN network to all peers. The EVPN peers perform the proxy ARP functionality when they receive an ARP request for a remotely learned ARP entry. You can enable ARP suppression at either the bridge-domain level or at the protocol level.<br>For Releases 22.1.4 and later, note that for Versa Networks appliances that have network processing (NPU) switching hardware, if you enable ARP suppression on a specific bridge domain, it is enabled for all bridge domains. |
| BD Interfaces for VLAN Translation | Configure VLAN translation for the bridge domain. For more information, see Configure VLAN Translation, below. |
| Logical Interfaces | To add a logical interface, click the + Add icon and enter information for the following fields. |

| Field | Description |
|---|---|
|  | <br>Add Bridge Domains Add Logical Interfaces<br>Logical Interface Name * --Select--<br>MAC Limit 16...131072<br>☑ MAC Learning<br>Static MAC Address<br>No Records to Display<br>OK<br>◦ Logical Interface Name—Select a logical interface.<br>◦ MAC Limit—Enter a MAC limit value, in the range 16 through 131072.<br>◦ MAC Learning—Click to enable or disable MAC learning at the logical-interface level.<br>◦ Static MAC Address—Enter a static MAC address for the logical interface, and then click the + Add icon to add the static MAC address.<br>◦ Click OK. |

7. Click OK.

You can also configure a virtual switch from the Objects menu:

1. In Director view, select the Configuration tab in the top menu bar.
2. Select Objects > Virtual Switches in the horizontal menu bar.

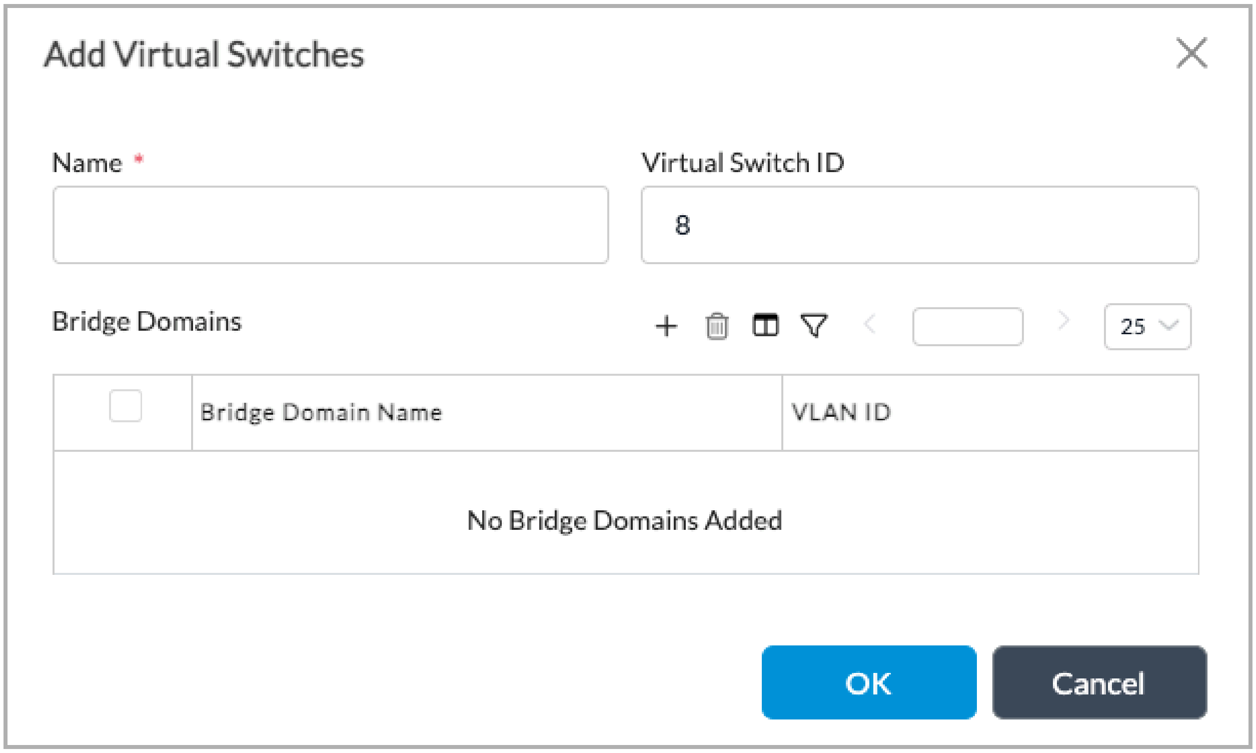


Organization: Provider

| Name | Organization | Bridge Domains |
|---|---|---|
| Provider-det | Provider | vlan-1 |

Rows per page: 25

3. Click the + Add icon. In the Add Virtual Switches popup window, enter information for the fields, as described above.



Name *:

Virtual Switch ID: 8

| □ | Bridge Domain Name | VLAN ID |
|---|---|---|

No Bridge Domains Added

25

4. Click OK.

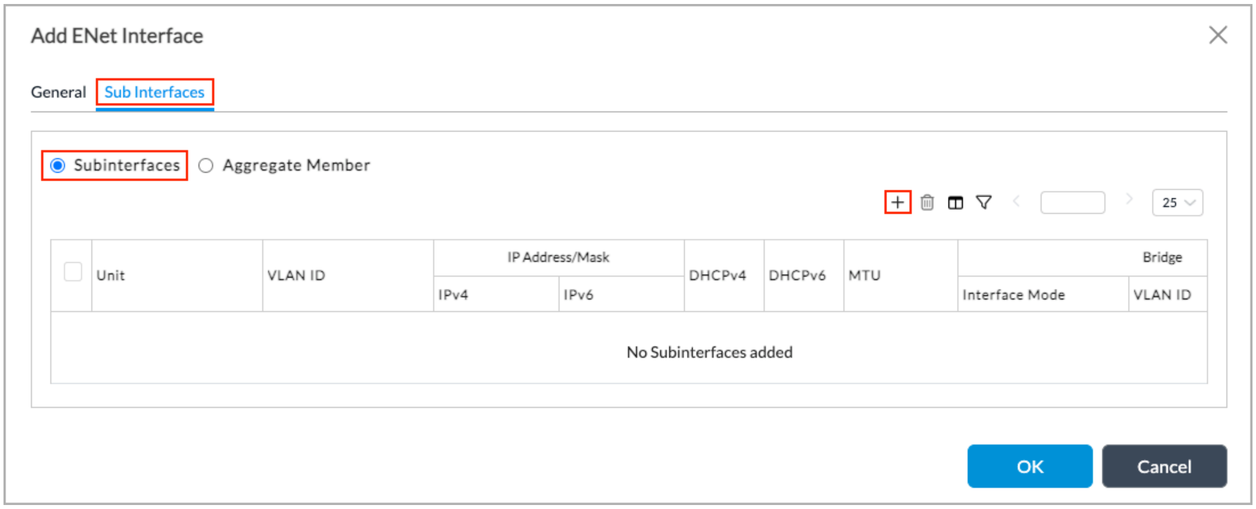
## Configure Trunk Interfaces

To configure multiple VLANs on a single interface, you configure a trunk interface. (These trunk interfaces are also known as enterprise-style trunk interfaces.) You configure a trunk interface under a interface, assign it to the family bridge, configure the interface mode as "trunk", and then assign the VLAN IDs of all applicable bridge domains to it. The trunk interface in a bridge domain learns MAC addresses based on the VLAN ID in the ingress packet.

To configure a trunk interface:

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select an appliance in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > Interfaces in the left menu bar. The main pane displays a list of configured interfaces. You can configure trunk interfaces using VNI, aggregated Ethernet, or Ethernet interfaces. This example uses an Ethernet interface.

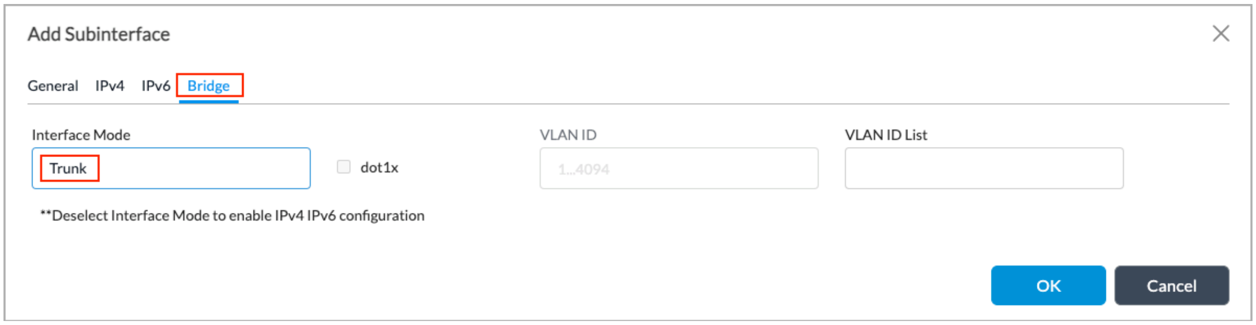
4. Select the ENet tab,and then click the + Add icon. The Add ENet Interface popup window displays.



● Subinterfaces ○ Aggregate Member

| | Unit | VLAN ID | IP Address/Mask | | DHCPv4 | DHCPv6 | MTU | Bridge | |
|---|---|---|---|---|---|---|---|---|---|
| | | | IPv4 | IPv6 | | | | Interface Mode | VLAN ID |
| No Subinterfaces added | | | | | | | | | |

5. Select the Subinterfaces tab, click Subinterfaces, and then click the + Add icon. The Add Subinterface popup window displays.
6. Select the Bridge tab, and then enter information for the following fields.



Interface Mode: Trunk

□ dot1x

VLAN ID: 1..4094

VLAN ID List:

**Deselect Interface Mode to enable IPv4 IPv6 configuration

| Field | Description |
|---|---|
| ◦ Interface Mode | Select Trunk. |
| ◦ VLAN ID List | Enter a list of VLAN identifiers. You can enter a range of VLANs (for example, 10-20), a list of VLAN IDs separated by spaces (for example, 1 25 27), or as a combination of the two (for example, 1 15-20 25 27). |

7. Click OK.

## Configure a Native VLAN ID

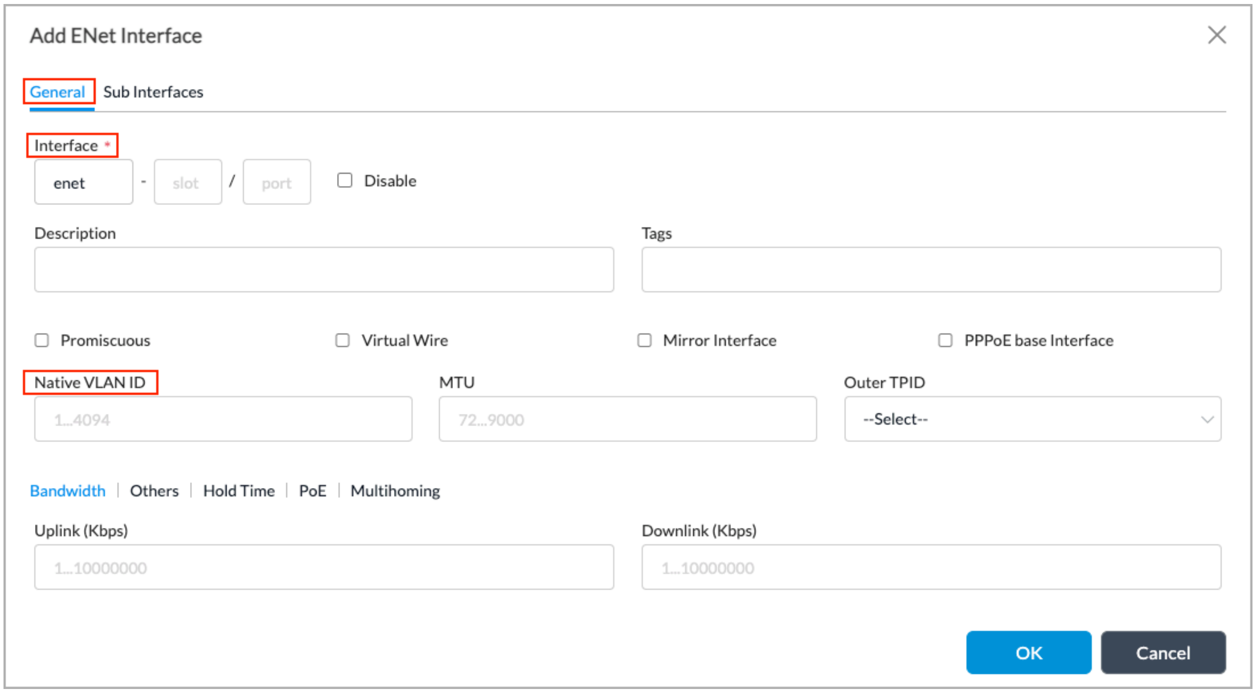
You configure a native VLAN ID on a trunk Layer 2 port to allow an untagged packet to be treated as a tagged packet. The native VLAN ID must be the same as the VLAN ID of the trunk Layer 2 port. For example, if you configure interface vni-0/1 with a VLAN ID of 10, you configure the native VLAN ID as 10. In this case, if an untagged packet arrives on vni-0/1, it is treated as a VLAN-tagged packet with a VLAN ID of 10 and is associated with trunk Layer 2 port vni-0/1.1.

Note: Native VLAN ID and access interfaces are mutually exclusive. You can configure only one of them on a Layer 2 interface (also called a port). An example of an interface is vni-0/1.

Note: If you do not define a native VLAN ID or an access interface for a Layer 2 port, untagged Layer 2 packets are dropped.

To configure a native VLAN ID:

1. In Director view:
    a. Select the Administration tab in the top menu bar.
    b. Select Appliances in the left menu bar.
    c. Select an appliance in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > Interfaces in the left menu bar. The main pane displays the list of configured interfaces. You can configure the native VLAN ID using VNI, aggregated Ethernet, or Ethernet interfaces. This example uses an ENet interface.
4. Select the ENet tab.
5. Click the + Add icon. In the Add ENet Interface popup window, select the General tab, and then enter information for the following fields.

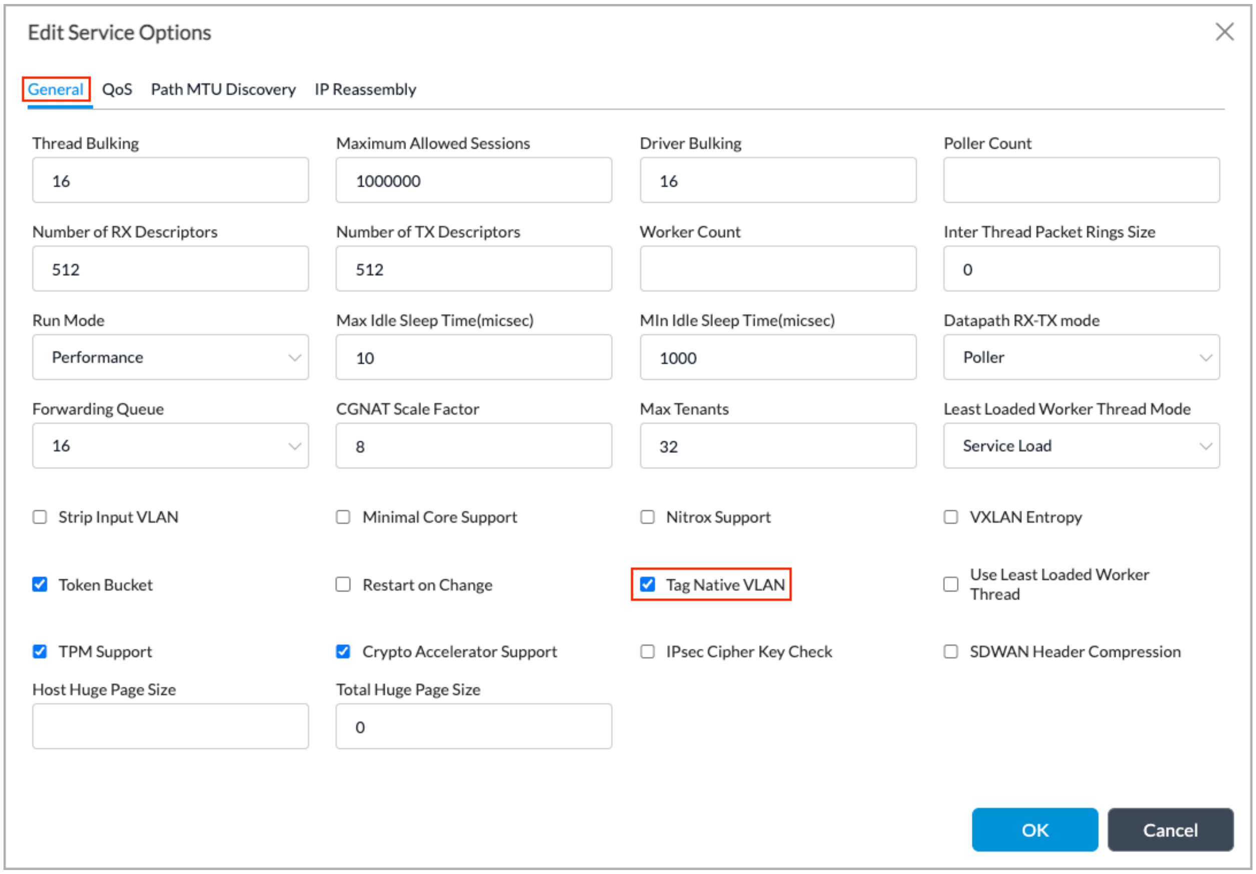


| Field | Description |
|---|---|
| Slot /Port (Required) | Enter the slot number and the port number of the interface. |
| Native VLAN ID | Enter the native VLAN ID for the interface. |

6. Click OK.

To tag traffic received on the native VLAN so that only tagged frames are admitted:

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select an appliance in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Others > System > Configuration > Configuration in the left menu bar.
4. In the Service Options pane, click the ✎ Edit icon. The Edit Service Options popup window displays.



| | | | |
|---|---|---|---|
| Thread Bulking<br>16 | Maximum Allowed Sessions<br>1000000 | Driver Bulking<br>16 | Poller Count<br> |
| Number of RX Descriptors<br>512 | Number of TX Descriptors<br>512 | Worker Count<br> | Inter Thread Packet Rings Size<br>0 |
| Run Mode<br>Performance | Max Idle Sleep Time(micsec)<br>10 | MIn Idle Sleep Time(micsec)<br>1000 | Datapath RX-TX mode<br>Poller |
| Forwarding Queue<br>16 | CGNAT Scale Factor<br>8 | Max Tenants<br>32 | Least Loaded Worker Thread Mode<br>Service Load |
| ☐ Strip Input VLAN | ☐ Minimal Core Support | ☐ Nitrox Support | ☐ VXLAN Entropy |
| ☑ Token Bucket | ☐ Restart on Change | ☑ Tag Native VLAN | ☐ Use Least Loaded Worker Thread |
| ☑ TPM Support | ☑ Crypto Accelerator Support | ☐ IPsec Cipher Key Check | ☐ SDWAN Header Compression |
| Host Huge Page Size<br> | Total Huge Page Size<br>0 | | |

5. Click Tag Native VLAN.
6. Click OK.

## Configure Access Interfaces

You can handle untagged packets by creating an access interface with an explicit VLAN ID. Any untagged packet arriving on the interface is associated with the access interface and is considered to be a tagged packet with the VLAN ID of the access interface.

Note: Native VLAN ID and access interface are mutually exclusive. You can configure only one of them on a Layer 2 interface (also called a port). An example of an interface is vni-0/1.

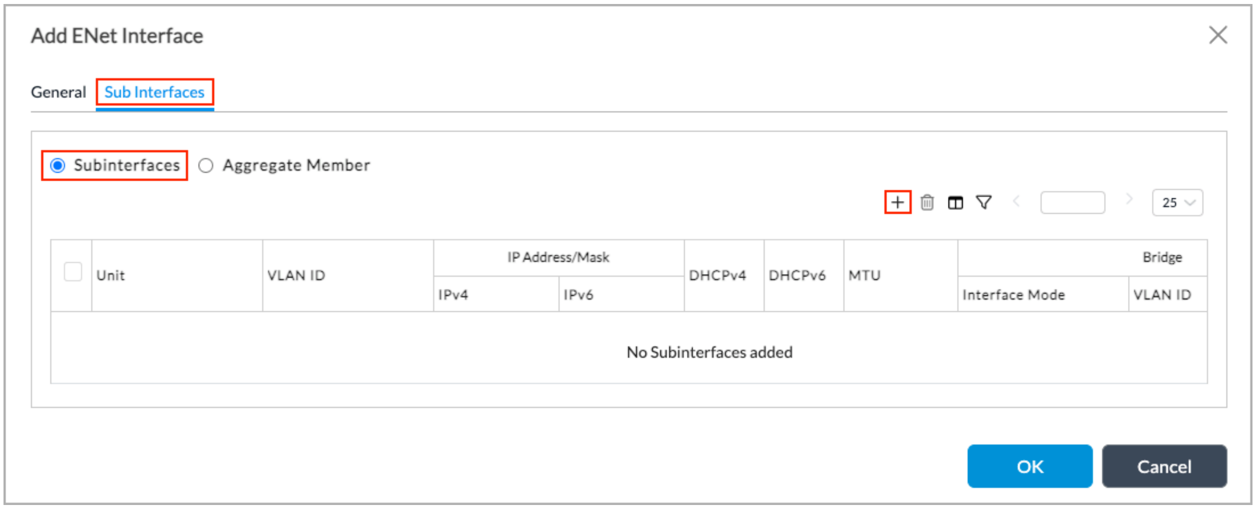
Note: If you do not define a native VLAN ID or an access interface for a Layer 2 port, untagged Layer 2 packets are dropped.

To configure an access interface:

1. In Director view:
    a. Select the Administration tab in the top menu bar.
    b. Select Appliances in the left menu bar.

   c. Select an appliance in the main pane. The view changes to Appliance view.

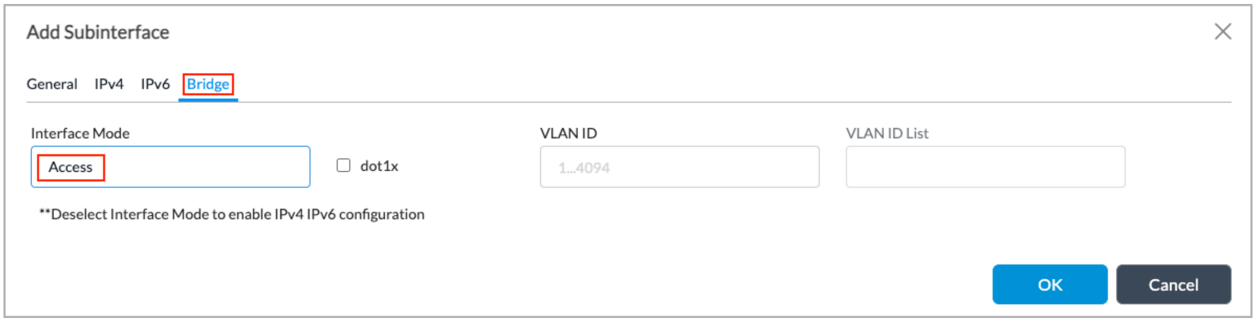
2. Select the Configuration tab in the top menu bar.
3. Select Networking > Interfaces in the left menu bar. The main pane displays a list of configured interfaces. You can configure trunk interfaces using VNI, aggregated Ethernet, or Ethernet interfaces. This example uses an Ethernet interface.
4. Select the ENet tab, and then click the + Add icon. The Add ENet Interface popup window displays.



| □ | Unit | VLAN ID | IP Address/Mask | | DHCPv4 | DHCPv6 | MTU | Bridge | |
|---|---|---|---|---|---|---|---|---|---|
| | | | IPv4 | IPv6 | | | | Interface Mode | VLAN ID |

No Subinterfaces added

5. Select the Subinterfaces tab.
6. Click Subinterfaces, and then click the + Add icon. The Add Subinterface screen displays.
7. Select the Bridge tab, and then enter information for the following fields.



Interface Mode: Access

□ dot1x

VLAN ID: 1...4094

VLAN ID List:

**Deselect Interface Mode to enable IPv4 IPv6 configuration

| Field | Description |
|---|---|
| Interface Mode | Select Access. |
| VLAN ID | Enter an explicit VLAN ID for the subinterface. Do not |

| Field | Description |
|---|---|
|  | enter a range of VLAN IDs. For the subinterface to be associated with a bridge domain, the VLAN ID of the subinterface must be the same as the VLAN ID of the bridge domain.<br>*Range:* 1 through 4094 |

8. Click OK.

## Configure MAC Parameters

You can configure the following MAC-related parameters on VOS devices:

- MAC learning—Dynamically builds and maintains Layer 2 forwarding tables.
- MAC aging—Specifies how long an inactive MAC address remains in a Layer 2 forwarding table.
- MAC limit—Controls the maximum number of MAC addresses that can be dynamically learned.
- MAC move—Allows a switch to update its Layer 2 forwarding table if the switch receives a packet whose MAC address matches an existing entry but that arrives on a different port than is stored in the existing forwarding table entry.
- Static MAC addresses—Allows you to configure MAC addresses that remain in the forwarding table after the device is rebooted.

For Release 21.1.1 and later, VOS devices apply MAC parameters hierarchically. The hierarchy, from highest to lowest, is:

- Virtual switch
- Bridge domain
- Bridge-domain interface

For configuration options that enable or disable certain features, such as MAC learning and suppress unknown unicast, the lower-level configurations take precedence.

If you do not configure a MAC parameter at a lower hierarchy level, the configuration information is inherited from the next higher level, as follows:

- If you do not configure a parameter for an interface in a bridge domain (the lowest level in the hierarchy), the VOS software uses the configuration information from the bridge domain.
- If you do not configure that MAC parameter for the bridge domain, the VOS software uses the configuration information from the virtual switch.
- If you do not configure a MAC parameter at the virtual switch level, the VOS software uses the default value for that parameter.

## Configure MAC Learning, MAC Aging, and MAC Limit

Each switch dynamically builds and maintains a Layer 2 forwarding table. As traffic enters the switch, the switch adds to the forwarding table the source device's MAC address and the port on which the frame was received. This process is called *MAC learning*.

By default, MAC learning is enabled.

You can enable and disable MAC learning at the following configuration hierarchy levels. If you configure MAC learning at multiple levels, the value at the lowest hierarchy level (that is, the most granular level) is honored.

- Bridge domain—Configuration > Networking > Virtual Switches > L2 Learning
- Bridge interface—Configuration > Networking > Virtual Switches > Virtual Switch Details > Add Bridge Domains > Add Bridge Domains Add Logical Interfaces

MAC aging specifies how long an inactive MAC address remains in a Layer 2 forwarding table. When the aging timer for a MAC address expires, the address is removed from the forwarding table. In this way, the forwarding table is continuously updated to ensure that it stays current as network topologies change.

The MAC aging check is done every 5 minutes, so it can take anywhere from 5 minutes to 5 minutes plus the configured aging time for addresses to be removed from the forwarding table. Stated another way, in the worst case, expired MAC addresses are removed in 5 minutes plus the configured aging time. For example, if you configure the MAC aging value to be 200 seconds, expired MAC addresses are removed any time between 300 seconds (5 minutes) and 500 seconds (300 + 200 seconds, or 8.33 minutes) from when the addresses were added to the forwarding table. The default MAC aging value is 300 seconds

Note: The MAC aging process does not remove static MAC addresses or EVPN MAC addresses from the forwarding table.

You can configure MAC aging at the following configuration hierarchy levels. If you configure MAC aging at multiple levels, the value at the lowest hierarchy level (that is, the most granular level) is honored.

- Virtual switch level—Configuration > Networking > Virtual Switches > L2 Learning
- Bridge domain level—Configuration > Networking > Virtual Switches > Virtual Switch Details > Add Bridge Domains > Add Bridge Options

The MAC limit controls the maximum number of MAC addresses that can be dynamically learned. When this limit is reached, no more MAC addresses are learned. When the number of MAC addresses drops below 90 percent of the limit value, MAC learning is reenabled.

Note: Static, VRRP, and IRB MAC addresses are not considered when calculating the MAC limit.

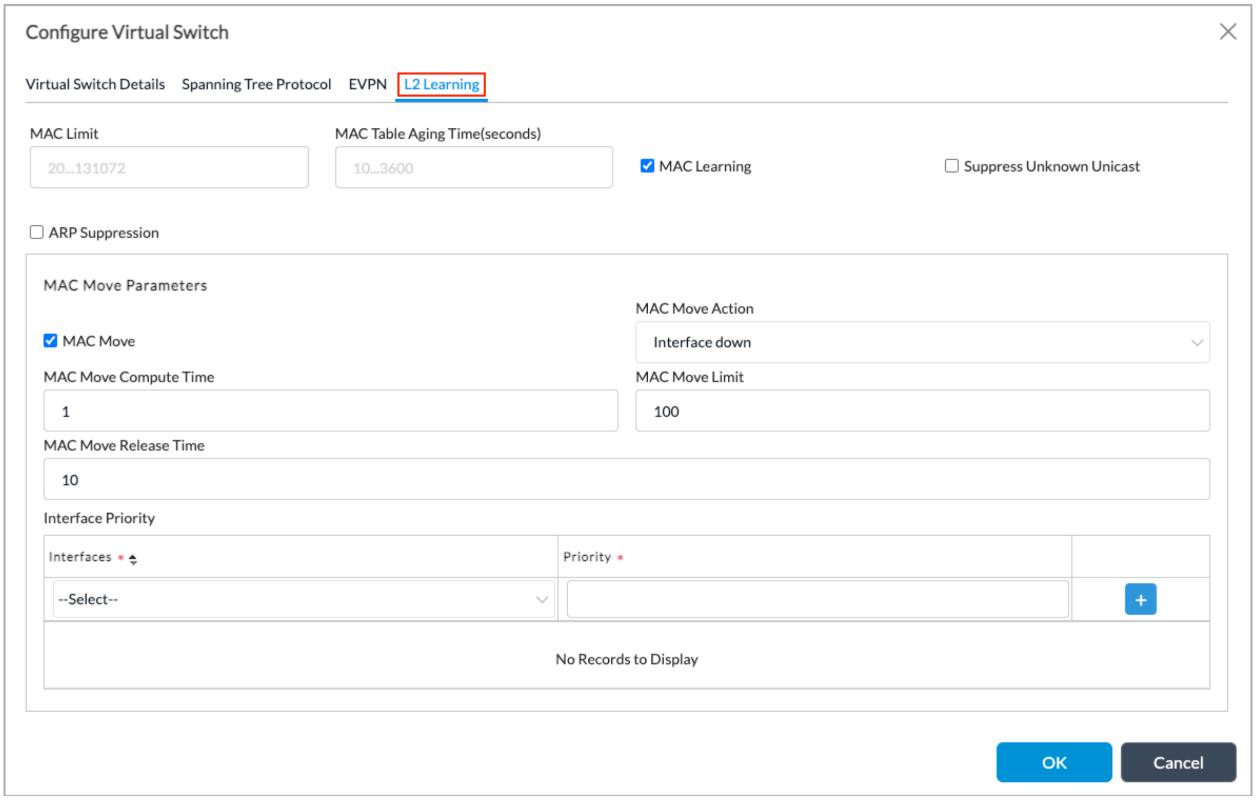
You can configure MAC limit at the following configuration hierarchy levels. If you configure MAC limit at multiple levels, the value at the lowest hierarchy level (that is, the most granular level) is honored.

- Virtual switch level—Configuration > Networking > Virtual Switches > L2 Learning

- Bridge domain level—Configuration > Networking > Virtual Switches > Virtual Switch Details > Add Bridge Domains
- Bridge domain level—Configuration > Networking > Virtual Switches > Virtual Switch Details > Add Bridge Domains > Add Bridge Domains Add Logical Interfaces

To enable or disable MAC learning, MAC limit, and MAC aging for a virtual switch:

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select an appliance 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. The Configure Virtual Switch popup window displays.
5. Select the Virtual Switch Details tab, and in the Instance Name field, enter a name for the virtual switch instance.
6. Select the L2 Learning tab, and then enter information for the following fields.



Configure Virtual Switch

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

MAC Limit: 20...131072

MAC Table Aging Time(seconds): 10...3600

☑ MAC Learning

□ Suppress Unknown Unicast

□ ARP Suppression

MAC Move Parameters

☑ MAC Move

MAC Move Action: Interface down

MAC Move Compute Time: 1

MAC Move Limit: 100

MAC Move Release Time: 10

Interface Priority

| Interfaces * | Priority * | |
|---|---|---|
| --Select-- | | + |
| No Records to Display | | |

| Field | Description |
|---|---|
| MAC Limit | Enter the maximum number of MAC addresses that the virtual switch can dynamicall |

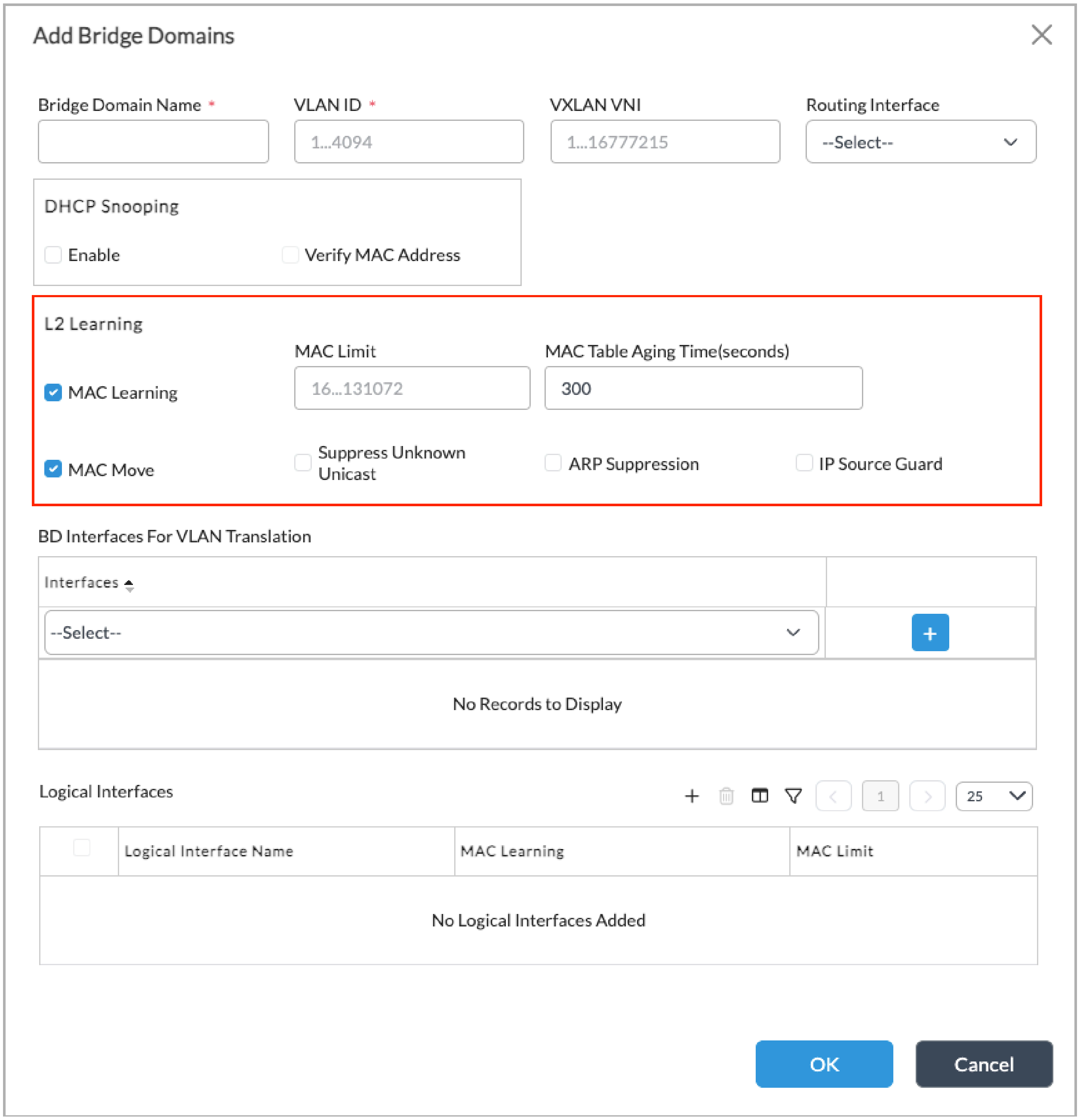
| Field | Description |
|---|---|
| | *Range:* 16 through 131072<br>*Default:* None |
| MAC Table Aging | Enter how long an inactive MAC address remains in a Layer 2 forwarding table, in se<br>*Range:* 10 through 3600 seconds<br>*Default:* 300 seconds |
| MAC Learning | Click to enable or disable MAC learning.<br>*Default:* MAC learning is enabled. |
| Suppress Unknown Unicast | Click to suppress the broadcast of unknown unicast traffic in the EVPN core.<br>*Default:* Suppression is disabled. |
| ARP Suppression | Click to prevent the flooding of ARP requests across a EVPN network. |
| MAC Move Parameters (Group of Fields) | |
| ◦ MAC Move | Click to enable or disable MAC loop detection and prevention for the virtual switch. |
| ◦ MAC Move Action | Select the action to take when a MAC move is identified:<br>◦ Bring down the VLAN interface—This is the default.<br>◦ Drop the traffic containing the looping MAC |
| ◦ MAC Move Compute Time | Enter the time interval during which MAC moves are evaluated, in seconds.<br>*Default*: 1 second<br>*Range*: 1 through 65535 seconds |
| ◦ MAC Move Limit | Enter the maximum number of MAC moves allowed before the MAC move action is i<br>*Default*: 100 |

| Field | Description |
|---|---|
| | *Range:* 1 through 65535 |
| ◦ MAC Move Release Time | Enter the amount of time during which the MAC move action is enforced, in seconds<br>interval elapses, the MAC move action is discontinued (released).<br>*Default*: 10 seconds<br>*Range*: 2 through 300 seconds |
| Interface Priority (Group of Fields) | Assign priorities to interfaces for invoking MAC move actions. An interface with a hig MAC move action. If the priorities are the same, the interface with the higher interfac MAC move action. |
| ◦ Interface | Select the interface. |
| ◦ Priority | Enter a number for the priority. |
| ◦ + Add | Click the + Add icon. |

7. Click OK.

To enable or disable MAC learning, MAC limit, and MAC aging for a bridge domain:

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select an appliance 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 configured virtual switches.
4. Click the + Add icon. The Configure Virtual Switch popup window displays with the Virtual Switch Details tab selected by default.
5. Select the Virtual Switch Details tab, and in the Instance Name field, enter a name for the virtual switch instance.
6. Click the + Add icon in the Bridge Domains table. 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

VLAN ID: 1...4094

VXLAN VNI: 1...16777215

Routing Interface: --Select--

DHCP Snooping

□ Enable □ Verify MAC Address

L2 Learning

☑ MAC Learning

MAC Limit: 16...131072

MAC Table Aging Time(seconds): 300

☑ MAC Move □ Suppress Unknown Unicast □ ARP Suppression □ IP Source Guard

BD Interfaces For VLAN Translation

| Interfaces | |
|---|---|
| --Select-- | + |
| No Records to Display | |

Logical Interfaces

| □ | Logical Interface Name | MAC Learning | MAC Limit |
|---|---|---|---|
| No Logical Interfaces Added | | | |

| Field | Description |
|---|---|
| Layer 2 Learning (Group of Fields) | |
| ◦ MAC Learning | Click to enable or disable MAC learning.<br>*Default:* MAC learning is enabled. |
| ◦ MAC Limit | Enter the maximum number of MAC addresses that can be dynamically learn |

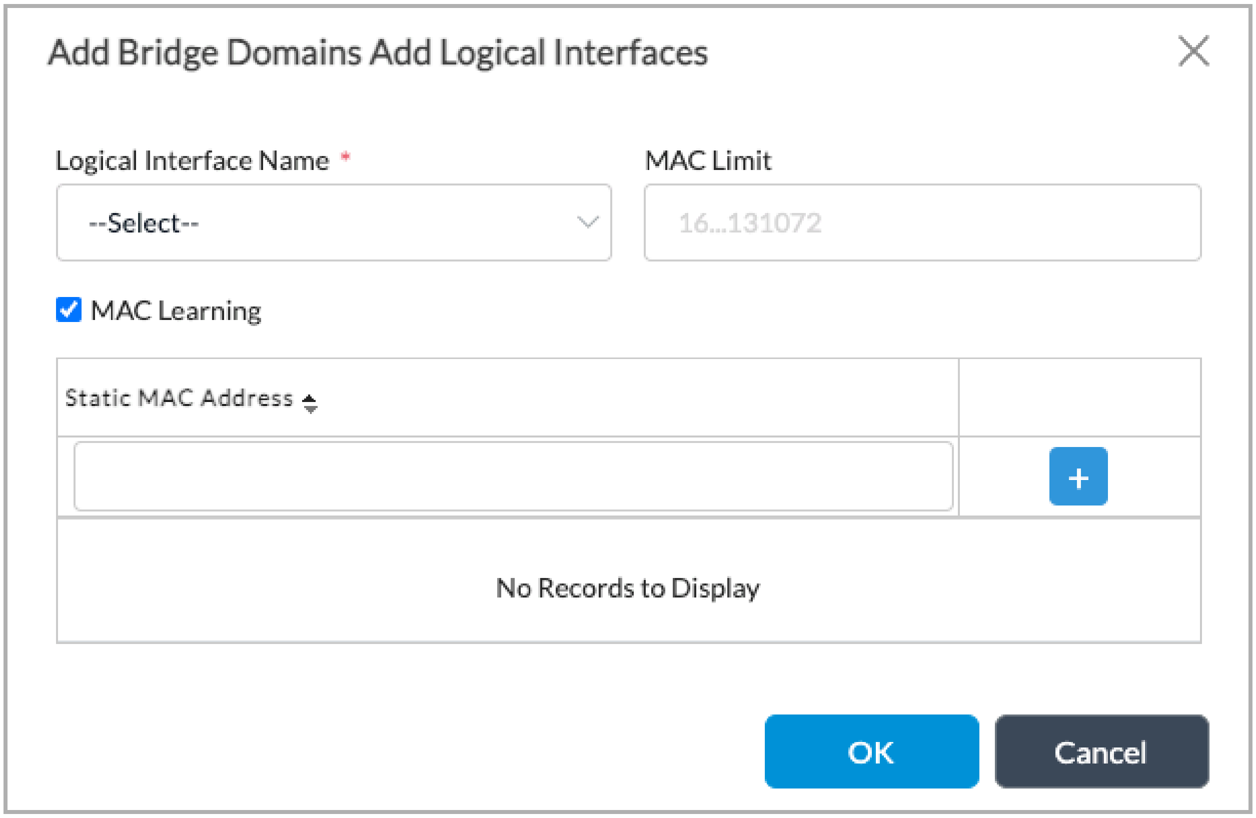
| Field | Description |
|---|---|
| | *Range:* 16 through 131072<br>*Default:* None |
| ◦ MAC Table Aging | Enter how long an inactive MAC address remains in a Layer 2 forwarding tab<br>*Default:* 300 seconds<br>*Range:* 10 through 3600 seconds |
| ◦ MAC Move | Click to enable or disable MAC loop detection and prevention at the bridge-d |
| ◦ Suppress Unknown Unicast | Click to suppress the broadcast of unknown unicast traffic in the EVPN core.<br>*Default:* Suppression is disabled. |
| ◦ ARP Suppression | Click to prevent the flooding of ARP requests across a EVPN network. |

7. Click OK.

To enable MAC learning and MAC limit for a bridge-domain interface:

Note: You cannot configure MAC aging for a bridge-domain interface.

1. In Director view:
    a. Select the Administration tab in the top menu bar.
    b. Select Appliances in the left menu bar.
    c. Select an appliance 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. The main pane displays a list of configured virtual switches.
4. Click the + Add icon. The Configure Virtual Switch popup window displays.
5. Click the + Add icon in the Bridge Domains table. In the Add Bridge Domains popup window, enter the required information.
6. Click the + Add icon in the Logical Interfaces table. In the Add Bridge Domains Add Logical Interfaces popup window, enter information for the following fields.



Add Bridge Domains Add Logical Interfaces

Logical Interface Name *

--Select--

MAC Limit

16...131072

☑ MAC Learning

Static MAC Address

No Records to Display

| Field | Description |
|---|---|
| Logical Interface Name | Select a logical interface. |
| MAC Limit | Enter the maximum number of MAC addresses that can be dynamically learne<br>*Range*: 16 through 131072<br>*Default*: None |
| MAC Learning | Click to disable or enable MAC learning.<br>*Default:* MAC learning is enabled. |

7. Click OK.

## Configure MAC Move

To clear a port from the MAC move blocked state, issue the **request clear mac move-action** CLI command.

For Releases 21.1.1 and later, the following changes have been made to the MAC move behavior:

- If you select vlan-interface down as the MAC move action, only the local VLAN interface is brought down. If both VLAN interfaces are local, the interface priority setting is used to determine which VLAN interface to bring down. If the MAC moves between a local VLAN interface and a remote provider edge (PE) device, the vlan-interface down action occurs on the local VLAN interface. The vlan-interface down action does not apply to TVIs.
- If a MAC address moves between remote PE devices, the MAC address is dropped (this is the default action) and the route is blackholed.
- If you set a drop action for a MAC address (for example, if you internally configure a blackhole route for a MAC address), all data traffic with that MAC address as a source or destination is dropped until the drop action is removed.
- EVPN does not advertise a MAC address that is marked for drop, but it learns the new route if it is received from a Layer 2 EVPN advertisement for that MAC address.
- If a new route is received from a Layer 2 EVPN advertisement for a MAC address that is marked as drop, the new route is learned but the data traffic continues to be dropped until the drop condition is removed.
- The MAC move logic has been changed to 100 MAC moves per second. That is, the threshold limit is 100 and the compute time is 1 second.
- By default, the MAC move logic continues to be enabled by default, as follows:
    - The default MAC move action (vlan-interface down) is invoked automatically if the system detects a MAC move. You can enable or disable the MAC move configuration for a virtual switch or a bridge domain.
    - MAC move is enabled by default at the virtual switch and bridge domain levels. If you manually configure a MAC move action at the bridge domain level, the bridge domain MAC move configuration is honored. Otherwise, the virtual switch MAC move configuration is honored. For example, if you do not configure MAC move enable or disable for the virtual switch but you disable MAC move in a particular bridge domain, MAC move is disabled in that bridge domain.

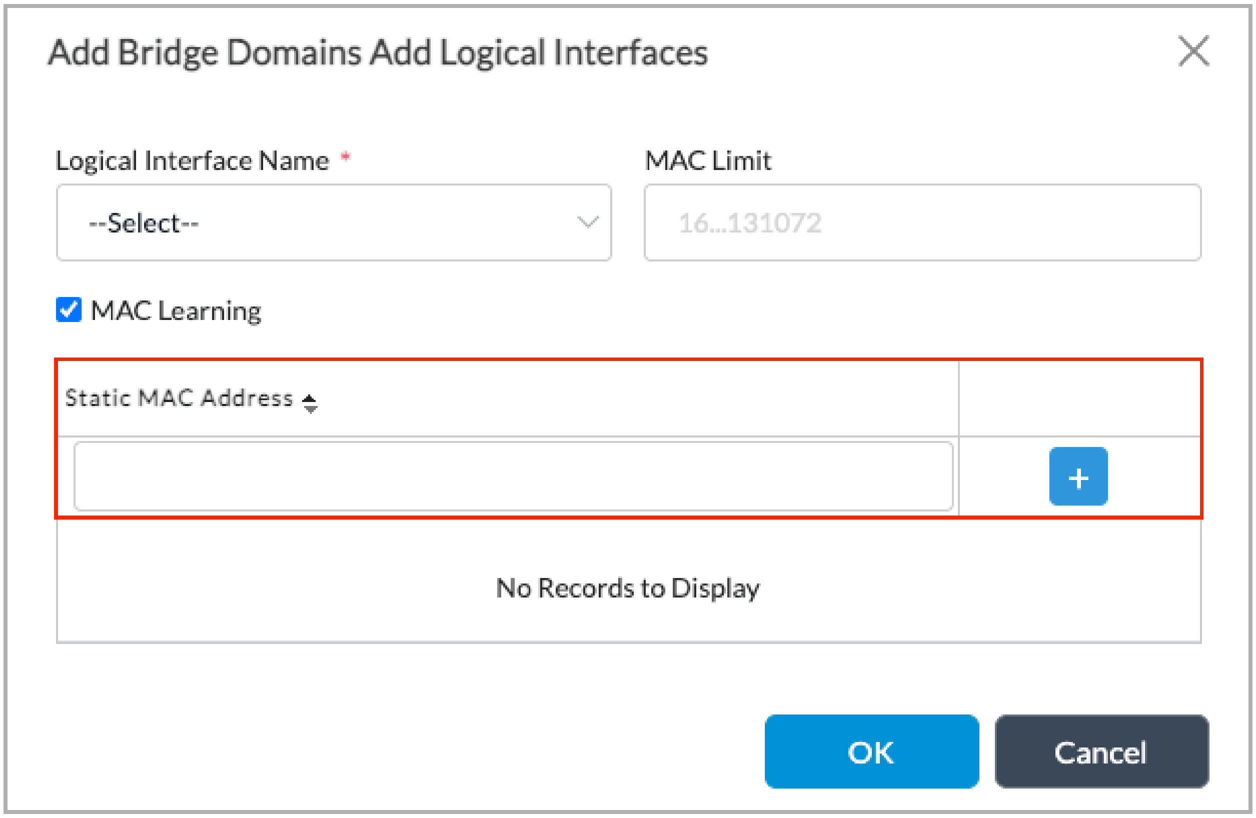
## Configure Static MAC Addresses

You can configure static MAC addresses, which are MAC addresses that remain in the forwarding table after the device is rebooted.

To configure a static MAC address:

1. In Director view:
    a. Select the Administration tab in the top menu bar.
    b. Select Appliances in the left menu bar.
    c. Select an appliance 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. The main pane displays a list of the virtual switches that are already configured.
4. Click the + Add icon.The Configure Virtual Switch popup window displays.
5. Click the + Add icon in the Bridge Domains table. In the Add Bridge Domains popup window, enter the required information.
6. Click the + Add icon in the Logical Interfaces table. In the Add Bridge Domains Add Logical Interfaces popup

window, enter information for the following fields.



Add Bridge Domains Add Logical Interfaces

Logical Interface Name * --Select--

MAC Limit 16...131072

☑ MAC Learning

Static MAC Address

No Records to Display

| Field | Description |
|---|---|
| Logical Interface Name | Select a logical interface. |
| Static MAC Address | Enter a MAC address, and then click the + Add icon to add a static MAC addr associate multiple static MAC addresses with a logical interface. |

7. Click OK.

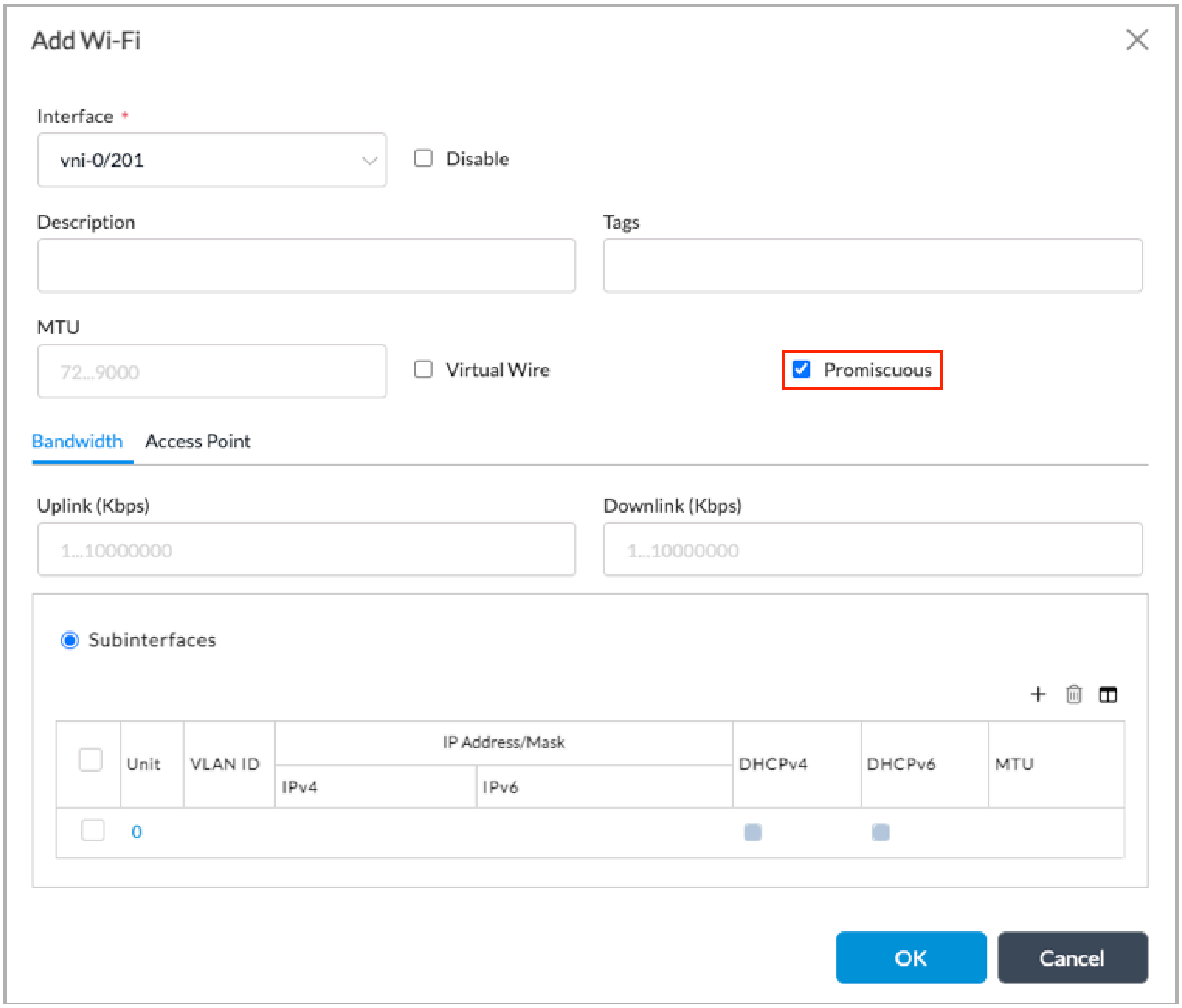
## Configure Layer 2 WiFi Interfaces

You can configure a WiFi interface to be a Layer 2 interface; that is, you can configure a WiFi interface to be a bridge interface. If you configure an Ethernet VNI and a WiFi interface to be bridge interfaces and assign them to the same bridge domain, they can then communicate with each other.

To configure a Layer 2 WiFi interface:

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

   b. Select Appliances in the left menu bar.
   c. Select an appliance in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > Interfaces in the left menu bar. The main pane displays a list of the interfaces that are already configured.
4. Select the WiFi tab, and then click the + Add icon. In the Add WiFi popup window, enter information for the following fields.



Add Wi-Fi

Interface * vni-0/201 □ Disable

Description

Tags

MTU 72...9000 □ Virtual Wire ☑ Promiscuous

Bandwidth Access Point

Uplink (Kbps) 1...10000000

Downlink (Kbps) 1...10000000

● Subinterfaces

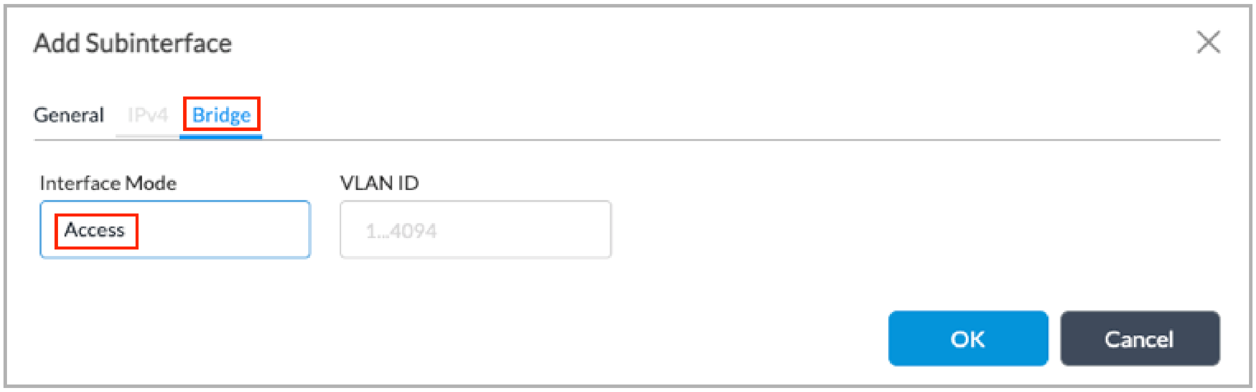
| □ | Unit | VLAN ID | IP Address/Mask |  | DHCPv4 | DHCPv6 | MTU |
|---|---|---|---|---|---|---|---|
|  |  |  | IPv4 | IPv6 |  |  |  |
| □ | 0 |  |  |  | □ | □ |  |

OK Cancel

| Field | Description |
|---|---|
| Interface (Required) | Select an interface. |
| Promiscuous | Click if the interface is a bridge interface. |
| Subinterfaces | By default, the Subinterfaces field is selected, and the |

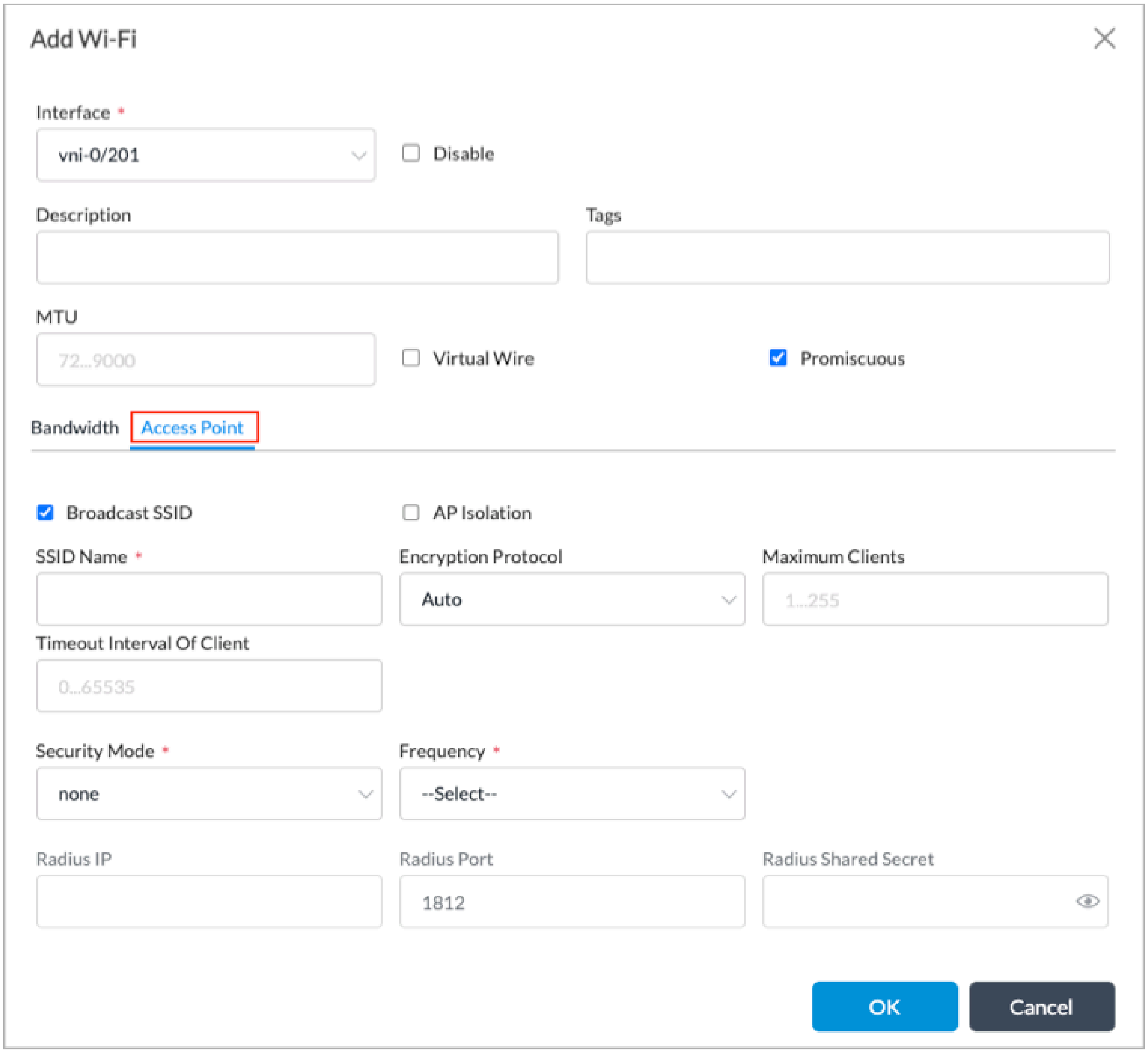
| Field | Description |
|---|---|
| | table displays the subinterfaces that are already configured. To add a subinterface, continue with Step 5. |

5. Click the + Add icon in the Subinterfaces table. In the Add Subinterface popup window, select the Bridge tab and then enter information for the following fields.



| Field | Description |
|---|---|
| Unit (Required) | Enter the unit number of the subinterface. The subinterface unit number cannot be 0. |
| Bridge (Tab) | |
| ◦ Interface Mode | Select Access. You must configure WiFi subinterfaces as access mode interfaces. |
| ◦ VLAN ID | Enter the VLAN ID of the subinterface. |

6. Click OK.
7. Select the Access Point tab in the Add WiFi popup window, and then enter information for the following fields.



Add Wi-Fi

Interface * vni-0/201

□ Disable

Description

Tags

MTU 72...9000

□ Virtual Wire

☑ Promiscuous

Bandwidth | Access Point

☑ Broadcast SSID

□ AP Isolation

SSID Name *

Encryption Protocol: Auto

Maximum Clients: 1...255

Timeout Interval Of Client: 0...65535

Security Mode *: none

Frequency *: --Select--

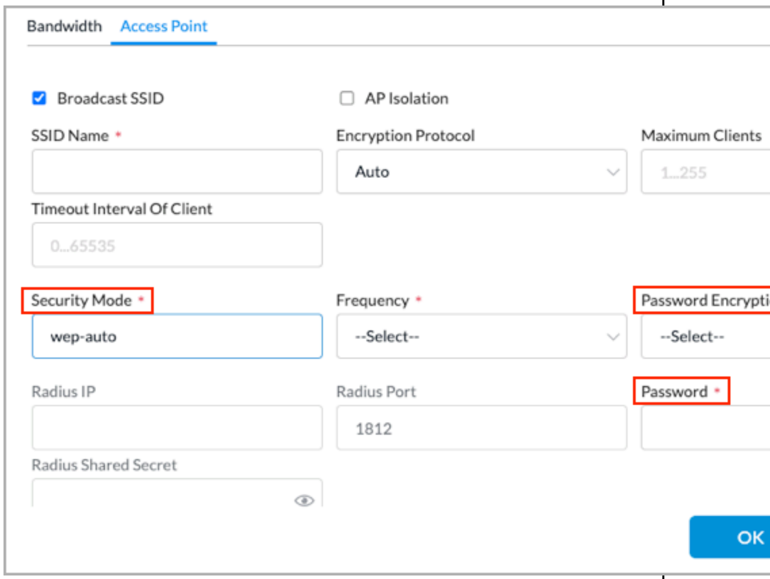
Radius IP

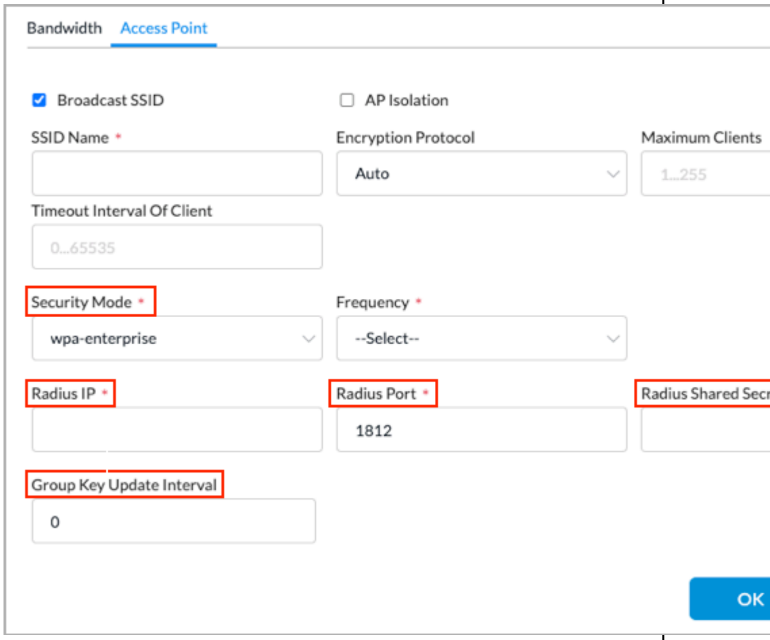
Radius Port: 1812

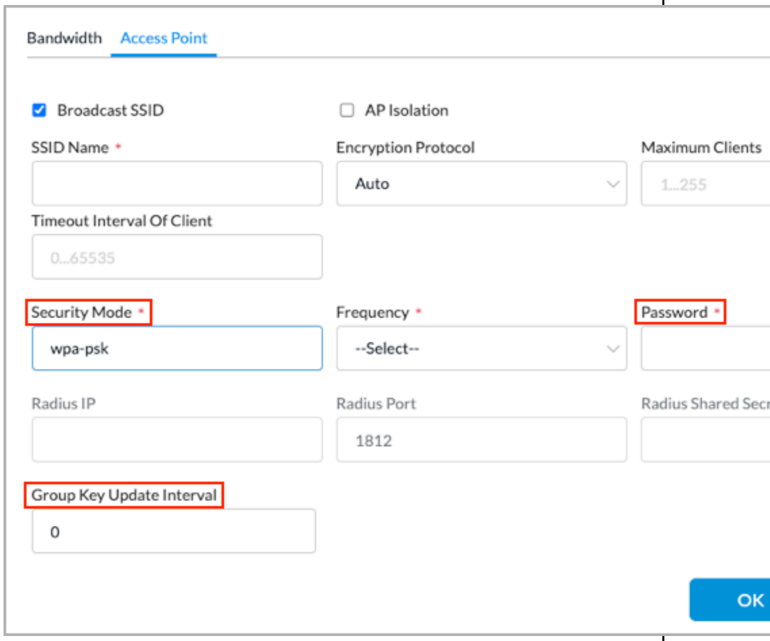
Radius Shared Secret

| Field | Description |
|---|---|
| Broadcast SSID | Click to enable broadcasting the service set identifier (SSID) of the access point. |
| AP Isolation | Click to prevent clients connected to the WiFi network from connecting to other non-WiFi networks. |
| SSID Name (Required) | Enter an SSID name for the WiFi network. |
| Encryption Protocol | Select the encryption protocol:<br>◦ CCMP |

| Field | Description |
|---|---|
| | ◦ TKIP |
| Maximum Clients | Enter the maximum number of WiFi clients that can connect to the access point.<br>*Range*: 1 through 255 |
| Timeout Interval of Client | Enter how long a WiFi client can be idle before timing out.<br>*Range*: 0 through 65535 |
| Security Mode (Required) | Select a security mode:<br>◦ wep-auto<br>◦ wep-open<br>◦ wep-share-key<br>◦ wpa-enterprise<br>◦ wpa/wpa2-auto-enterprise<br>◦ wpa1-enterprise<br>◦ wpa-psk<br>◦ wpa/wpa2-auto-pak<br>◦ wpa2-psk |
| ◦ WEP Security Modes | For WEP security modes, enter information for the following fields: |

| Field | Description |
|---|---|
| | <br> <br>☑ Broadcast SSID<br>□ AP Isolation<br>SSID Name *<br>Encryption Protocol: Auto<br>Maximum Clients: 1...255<br>Timeout Interval Of Client: 0...65535<br>Security Mode *: wep-auto<br>Frequency *: --Select--<br>Password Encrypti: --Select--<br>Radius IP<br>Radius Port: 1812<br>Password *<br>Radius Shared Secret<br>◦ Password Encryption—Select a password-encryption option.<br>◦ Password—Enter a password for selected security mode. |
| ◦ WEP with PSK Security Modes | For WEP security modes with PSK, enter information for the following fields: |

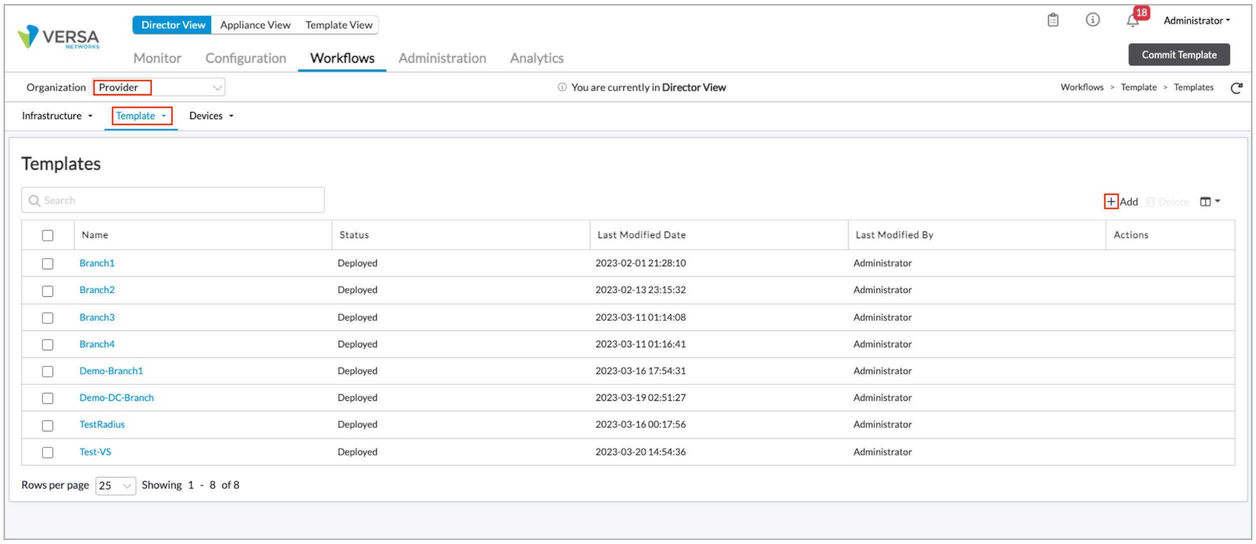
| Field | Description |
|---|---|
|  | <br>Bandwidth Access Point<br>☑ Broadcast SSID<br>□ AP Isolation<br>SSID Name *<br>Encryption Protocol: Auto<br>Maximum Clients: 1...255<br>Timeout Interval Of Client: 0...65535<br>Security Mode *: wpa-enterprise<br>Frequency *: --Select--<br>Radius IP *<br>Radius Port *: 1812<br>Radius Shared Secr<br>Group Key Update Interval: 0<br>OK<br>◦ RADIUS Port—Enter the port number to use on the RADIUS server.<br>*Range*: 0 through 65535<br>◦ RADIUS Shared Secret—Enter the shared secret password for the RADIUS server.<br>◦ Group Key Update Interval—Enter the amount of time in between automatic updates of the group key. Enter a value of 0 to disable updates.<br>*Range*: 0 through 65535 |
| ◦ WPA with PSK Security Modes | For WPA PSK security modes, enter information for the following fields: |

| Field | Description |
|---|---|
|  | <br> Bandwidth<br>Access Point<br>SSID Name *<br>Maximum Clients<br>1...255<br>Timeout Interval Of Client<br>0...65535<br>Password *<br>Radius IP<br>Radius Shared Secr<br>OK<br>☑ Broadcast SSID<br>☐ AP Isolation<br>Encryption Protocol: Auto<br>Security Mode *: wpa-psk<br>Frequency *: --Select--<br>Radius Port: 1812<br>Group Key Update Interval: 0<br>◦ Password—Enter the WPA password for the WiFi network.<br>◦ Group Key Update Interval—Enter the amount of time in between automatic updates of the WPA group key. Enter a value of 0 to disable updates. *Range*: 0 through 65535 |
| Frequency (Required) | Select the frequency band for the access point. |

8. Click OK.

## Configure Layer 2 WiFi Interfaces Using Workflows Templates

1. In Director view, select the Workflows tab in the top menu bar.
2. Select an organization in the Organization field.
3. Select Template > Templates in the horiztonal menu bar. The Templates page displays.



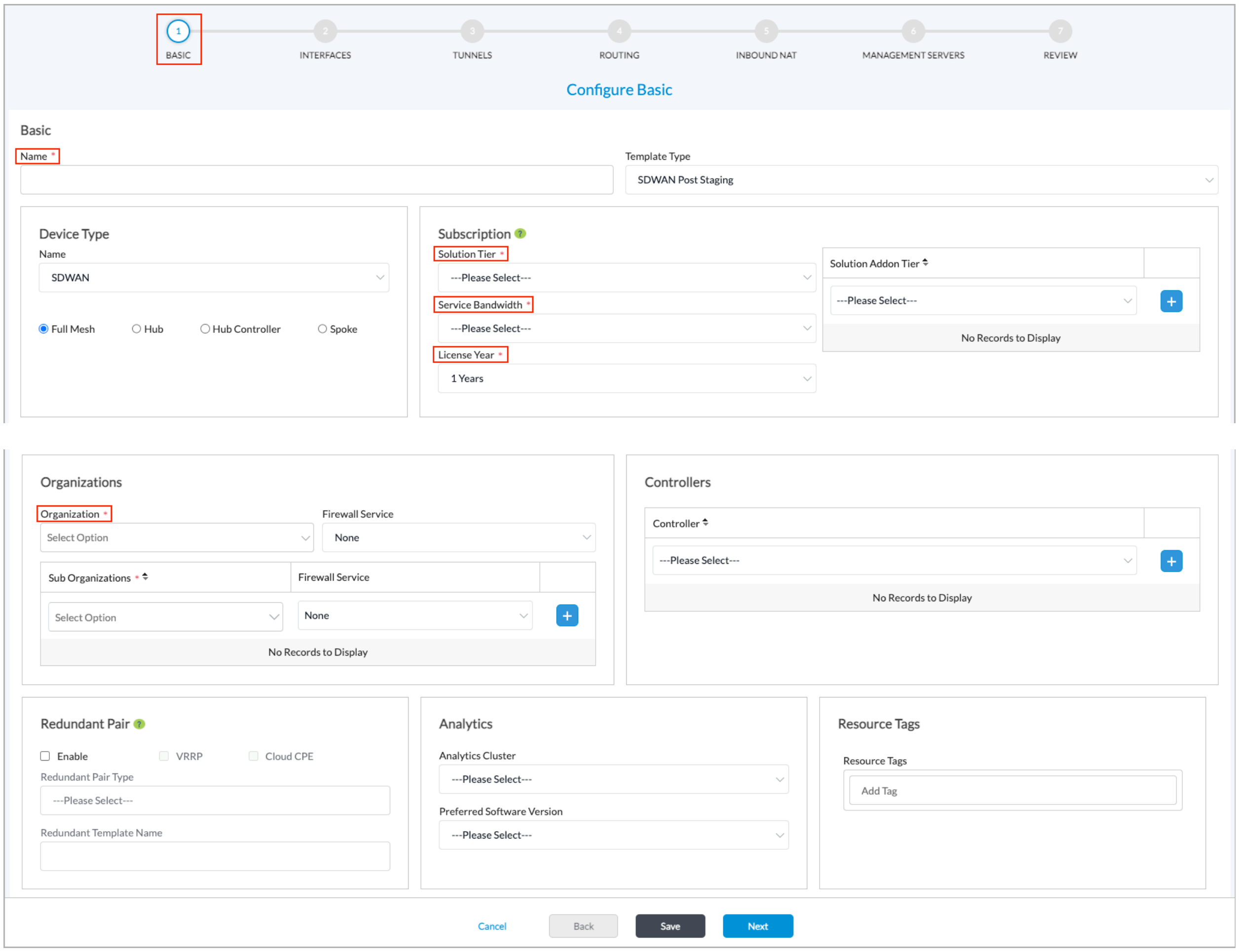
Organization: Provider

## Templates

| Name | Status | Last Modified Date | Last Modified By | Actions |
|---|---|---|---|---|
| Branch1 | Deployed | 2023-02-01 21:28:10 | Administrator | |
| Branch2 | Deployed | 2023-02-13 23:15:32 | Administrator | |
| Branch3 | Deployed | 2023-03-11 01:14:08 | Administrator | |
| Branch4 | Deployed | 2023-03-11 01:16:41 | Administrator | |
| Demo-Branch1 | Deployed | 2023-03-16 17:54:31 | Administrator | |
| Demo-DC-Branch | Deployed | 2023-03-19 02:51:27 | Administrator | |
| TestRadius | Deployed | 2023-03-16 00:17:56 | Administrator | |
| Test-VS | Deployed | 2023-03-20 14:54:36 | Administrator | |

Rows per page 25 Showing 1 - 8 of 8

4. Click the + Add icon. In the Configure Basic screen, enter the required information.



Configure Basic

Basic

Name *

Template Type: SDWAN Post Staging

Device Type

Name: SDWAN

● Full Mesh ○ Hub ○ Hub Controller ○ Spoke

Subscription

Solution Tier *: ---Please Select---

Service Bandwidth *: ---Please Select---

License Year *: 1 Years

Solution Addon Tier: ---Please Select---

No Records to Display

Organizations

Organization *: Select Option

Firewall Service: None

| Sub Organizations * | Firewall Service |
|---|---|
| Select Option | None |

No Records to Display

Controllers

| Controller |
|---|
| ---Please Select--- |

No Records to Display

Redundant Pair

□ Enable □ VRRP □ Cloud CPE

Redundant Pair Type: ---Please Select---

Redundant Template Name

Analytics

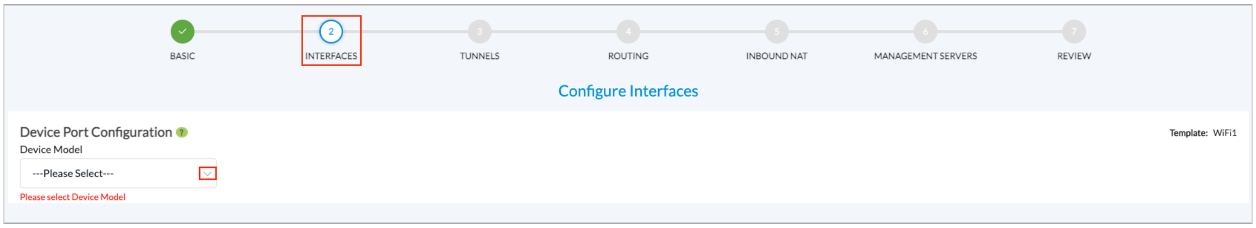
Analytics Cluster: ---Please Select---

Preferred Software Version: ---Please Select---

Resource Tags

Resource Tags: Add Tag

5. Click Next. In the Configure Interfaces screen, select a model in the Device Model field. This example uses a CSG350 device.



Configure Interfaces

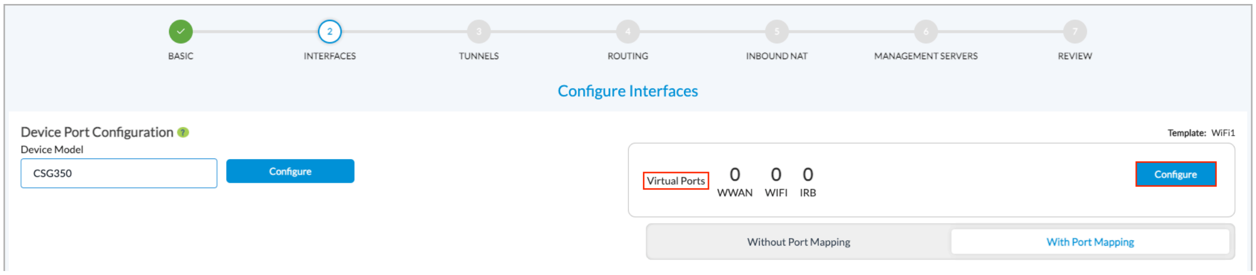
Device Port Configuration

Template: WiFi1

Device Model: ---Please Select---

Please select Device Model

6. In the Virtual Ports box, click Configure.



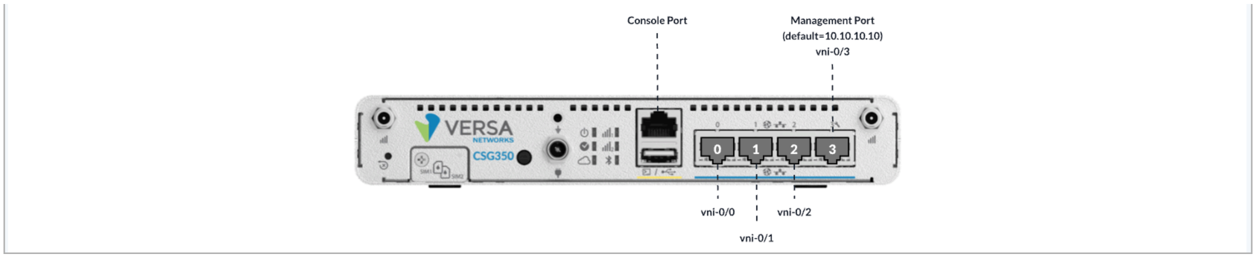
Configure Interfaces

Device Port Configuration

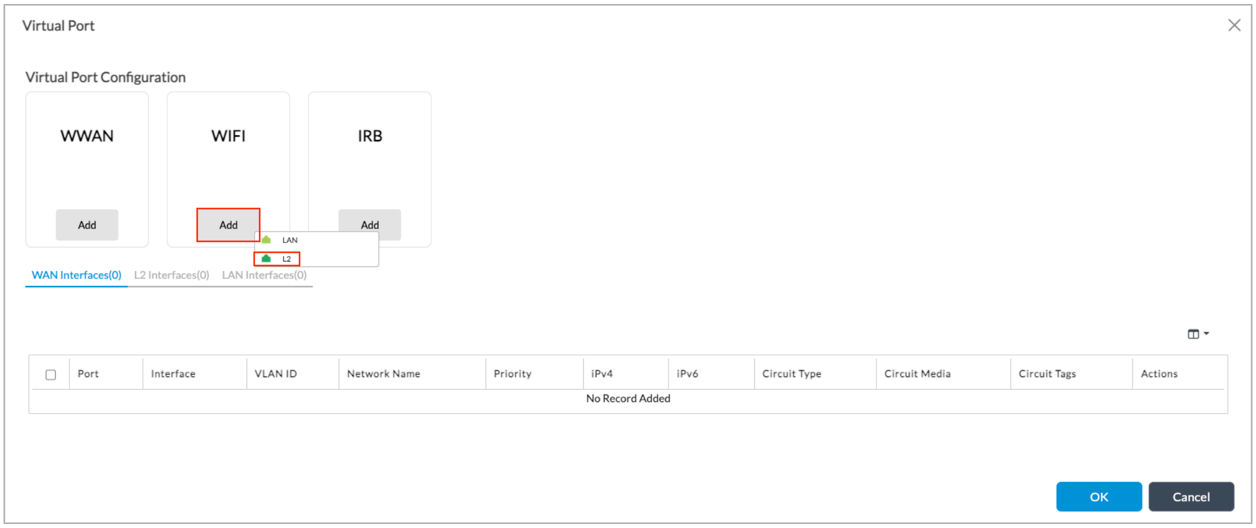
Template: WiFi1

Device Model: CSG350

| Virtual Ports | 0 WWAN | 0 WIFI | 0 IRB |
|---|---|---|---|



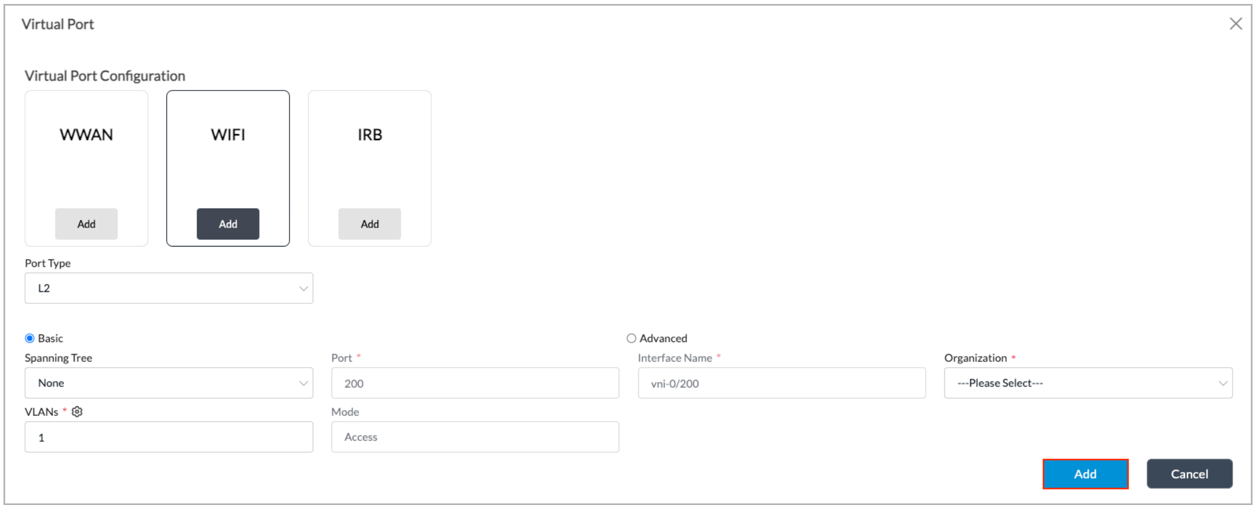
7. In the Virtual Port screen, click Add in the WiFi box, and then select L2 in the popup window.



Virtual Port Configuration

| □ | Port | Interface | VLAN ID | Network Name | Priority | iPv4 | iPv6 | Circuit Type | Circuit Media | Circuit Tags | Actions |
|---|---|---|---|---|---|---|---|---|---|---|---|
| No Record Added | | | | | | | | | | | |

8. Click the blue Add button to add the WiFi interface.


Virtual Port

Virtual Port Configuration

Port Type: L2

● Basic ○ Advanced

Spanning Tree: None

Port *: 200

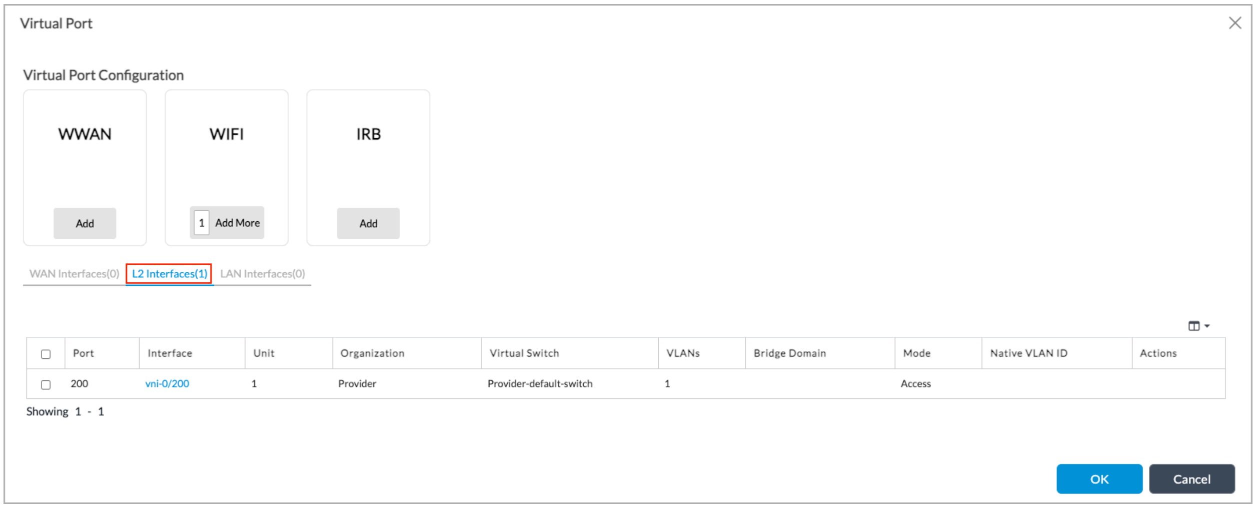
Interface Name *: vni-0/200

Organization *: ---Please Select---

VLANs *: 1

Mode: Access

9. Click the Layer 2 Interfaces tab to display information about the new Layer 2 interface. By default, the WiFi interface has a VLAN ID of 1, and the VLAN ID belongs to an IRB interface. You can change the VLAN ID.

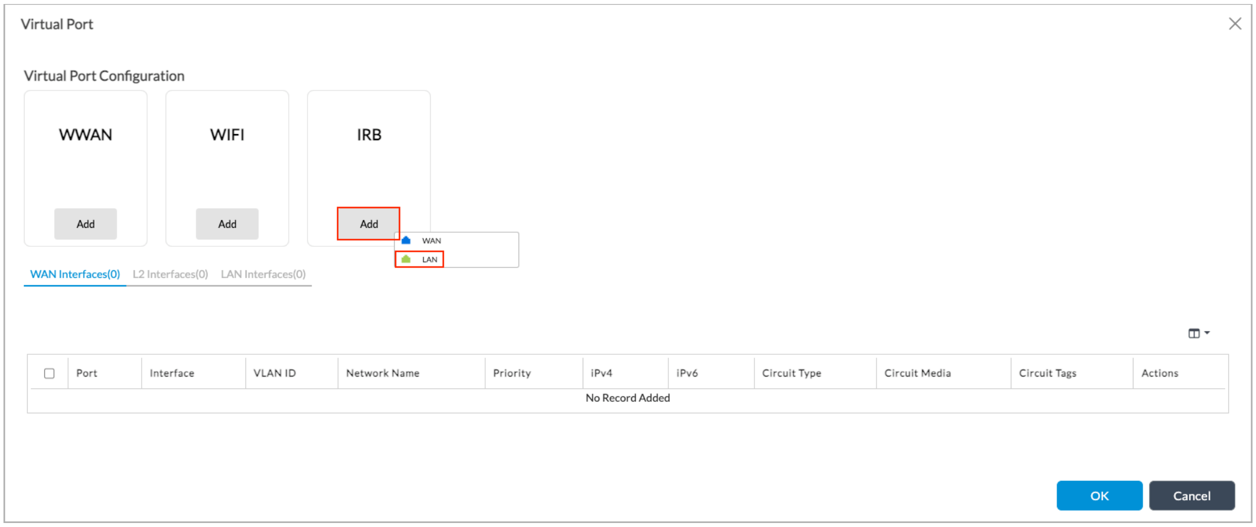

Virtual Port

Virtual Port Configuration

| □ | Port | Interface | Unit | Organization | Virtual Switch | VLANs | Bridge Domain | Mode | Native VLAN ID | Actions |
|---|---|---|---|---|---|---|---|---|---|---|
| □ | 200 | vni-0/200 | 1 | Provider | Provider-default-switch | 1 |  | Access |  |  |

Showing 1 - 1

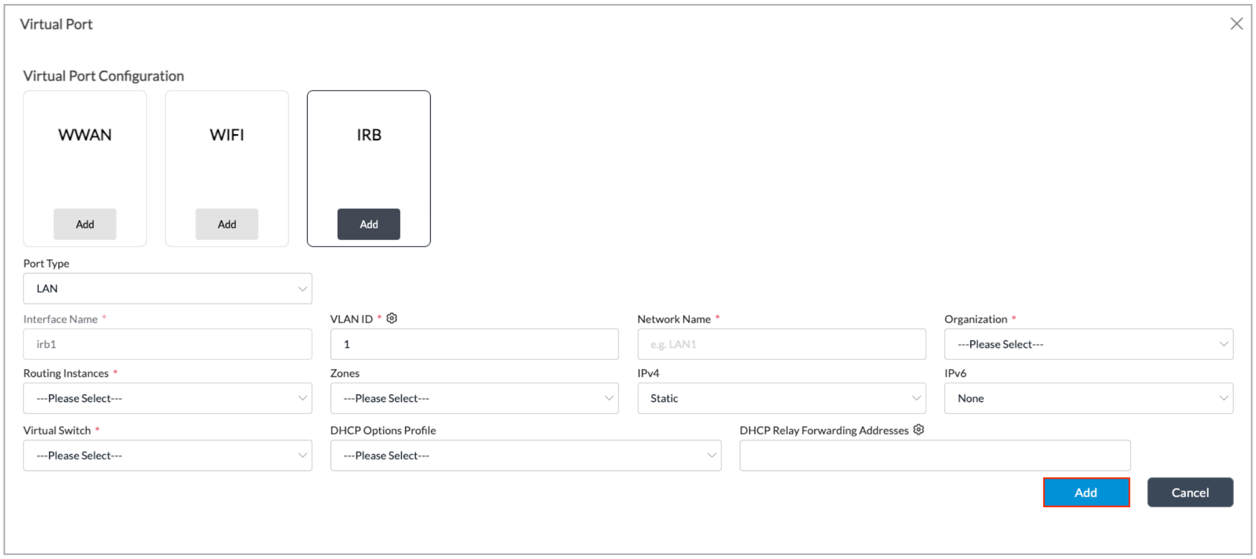
10. To create a LAN IRB interface, click Add in the IRB box on the Virtual Port screen, and then click LAN in the popup window.



| □ | Port | Interface | VLAN ID | Network Name | Priority | iPv4 | iPv6 | Circuit Type | Circuit Media | Circuit Tags | Actions |
|---|---|---|---|---|---|---|---|---|---|---|---|

No Record Added

11. Enter the required information, and then click the blue Add button. Make sure that you use the same VLAN ID that you configured for the WiFi L2 interface.



Port Type: LAN

Interface Name *: irb1

VLAN ID *: 1

Network Name *: e.g. LAN1

Organization *: ---Please Select---

Routing Instances *: ---Please Select---

Zones: ---Please Select---

IPv4: Static

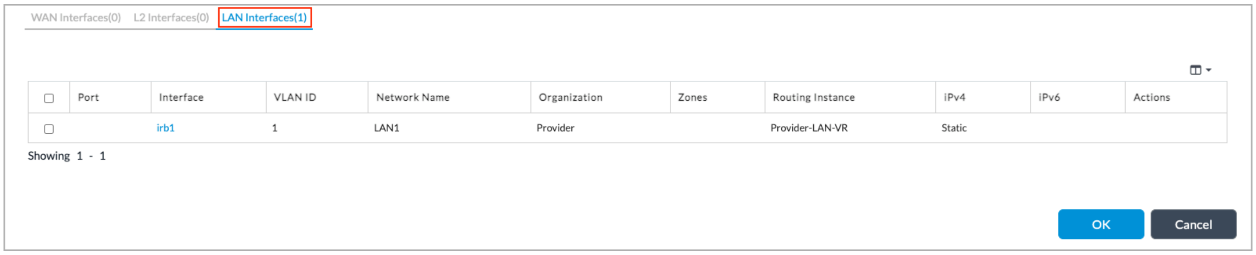
IPv6: None

Virtual Switch *: ---Please Select---

DHCP Options Profile: ---Please Select---

DHCP Relay Forwarding Addresses:

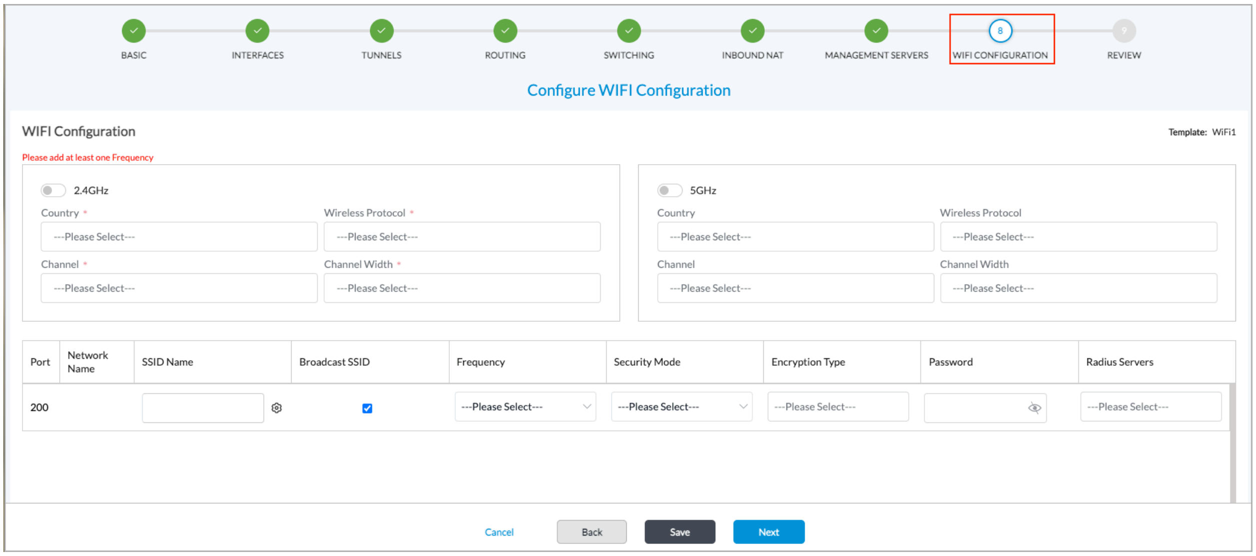
12. Click the LAN Interfaces tab display information about the new IRB interface.



| □ | Port | Interface | VLAN ID | Network Name | Organization | Zones | Routing Instance | iPv4 | iPv6 | Actions |
|---|---|---|---|---|---|---|---|---|---|---|
| □ | | irb1 | 1 | LAN1 | Provider | | Provider-LAN-VR | Static | | |

Showing 1 - 1

13. To configure the WiFi interface, select the WiFi Configuration tab, and then enter information for the following fields.



Configure WIFI Configuration

WIFI Configuration

Template: WiFi1

Please add at least one Frequency

2.4GHz

Country * ---Please Select---

Wireless Protocol * ---Please Select---

Channel * ---Please Select---

Channel Width * ---Please Select---

5GHz

Country ---Please Select---

Wireless Protocol ---Please Select---

Channel ---Please Select---

Channel Width ---Please Select---

| Port | Network Name | SSID Name | Broadcast SSID | Frequency | Security Mode | Encryption Type | Password | Radius Servers |
|---|---|---|---|---|---|---|---|---|
| 200 | | | ☑ | ---Please Select--- | ---Please Select--- | ---Please Select--- | | ---Please Select--- |

| Field | Description |
|---|---|
| Frequency (Required) | Select a frequency:<br>◦ 2.4 GHz<br>◦ 5 GHz |
| Country | Select a country. |
| Wireless Protocol | Select a wireless protocol:<br>◦ b—2.4 GHz<br>◦ g—2.4 GHz<br>◦ n—2.4 GHz |
| Channel | Select a channel:<br>◦ Auto<br>◦ 1 through 11 |
| Channel Width | Select a channel width:<br>◦ 20 MHz<br>◦ 40 MHz<br>◦ 20/40MHz |

| Field | Description |
|---|---|
| SSID Name | Enter a service set identifier name for the WiFi network. |
| Broadcast SSID | Click to enable broadcasting the SSID of the access point. |
| Frequency | Select the frequency at which the WiFi interface operates:<br>◦ 2.4 GHz<br>◦ 5 GHz<br>◦ Dual Band |
| Security Mode | Select a security mode, or select None. |
| Encryption Type | Select an encryption type. For a WEP security mode, the encryption type can be:<br>◦ ascii-64-bit-key<br>◦ ascii-128-bit-key<br>◦ hex-64-bit-key<br>◦ hex-128-bit-key<br>For a WPA security mode, the encryption type can be:<br>◦ auto<br>◦ ccmp (CCM-Mode Protocol)<br>◦ tkip (Temporal Key Integrity Protocol) |
| Password | Enter the password associated with the security mode. |
| RADIUS Servers | Select the RADIUS servers. |

14. Click Create Template.

## Configure RSTP

You can configure the Rapid Spanning Tree Protocol (RSTP), which is defined in IEEE 802.1w. RSTP enables fast spanning-tree reconvergence by simplifying the port states and changing the way ports transition from one state to another. RSTP is backwards compatable with the standard STP. You can enforce regular STP mode.

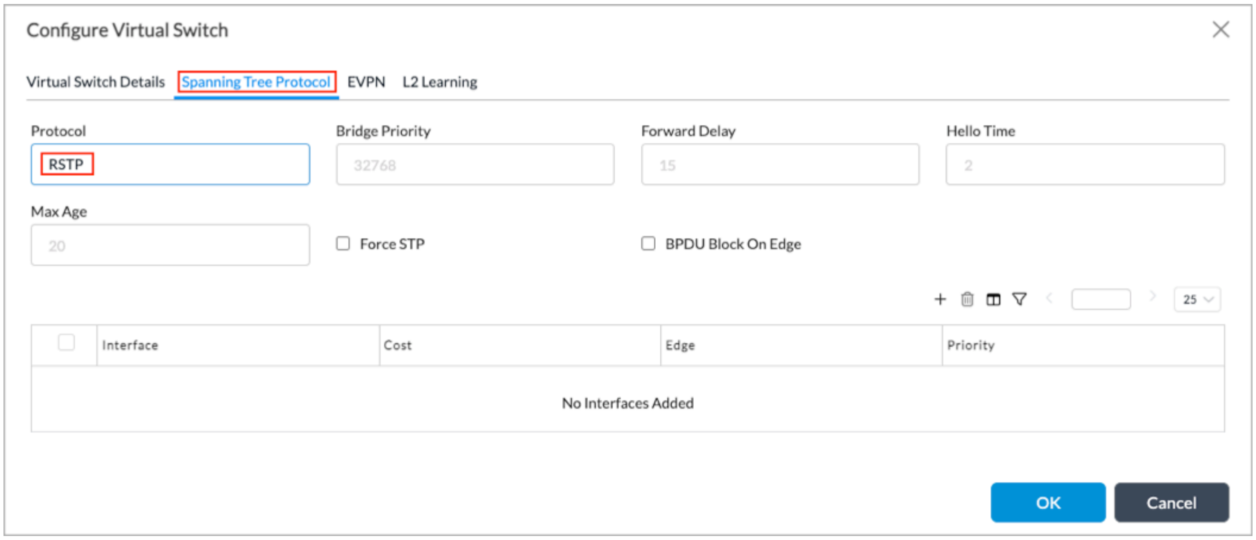
To prevent loops in the Layer 2 network, you should configure RSTP before transmitting Layer 2 traffic through your network.

You configure RSTP in a routing instance, either in a Layer 2 control routing instance or a virtual switch routing instance. When you configure RSTP in a Layer 2 control routing instance, the interface state of a port as determined by the RSTP protocol is associated with all the bridge domain interfaces on the port across all the routing instances. When you configure RSTP in a virtual switch routing instance, all bridge domain interfaces corresponding to that port should be present on the virtual switch only.

Note: You must configure paired TVI interfaces in a virtual-switch control routing instance. If you place both RSTP-enabled paired TVI interfaces in a Layer 2 control routing instance, one of the ports is a blocked port.

To configure RSTP:

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select an appliance 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. The Configure Virtual Switch popup window displays.
5. Select the Virtual Switch Details tab, and then enter a name for the virtual switch instance.
6. Select the Spanning Tree Protocol tab, and then enter information for the following fields.



Protocol: RSTP

Bridge Priority: 32768

Forward Delay: 15

Hello Time: 2

Max Age: 20

□ Force STP

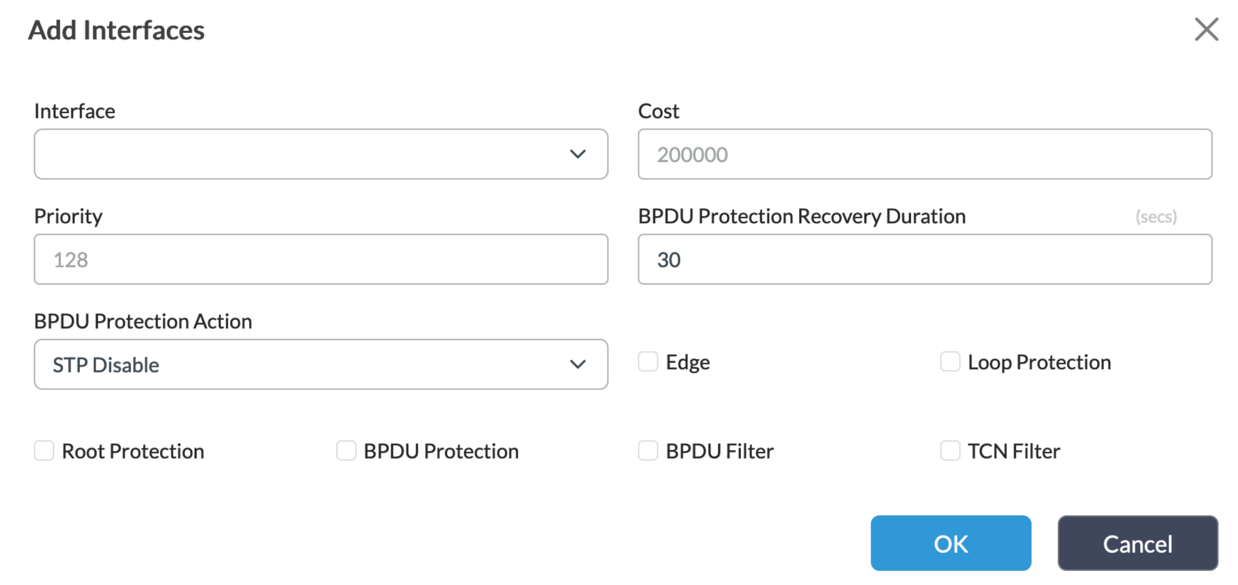
□ BPDU Block On Edge

| □ | Interface | Cost | Edge | Priority |
|---|---|---|---|---|
| | No Interfaces Added | | | |

| **Field** | **Description** |
|---|---|
| Protocol | Select RSTP. |
| Bridge Priority | Enter the priority value to use to determine which device in the spanning tree is the root bridge. A lower priority value configures a higher priority.<br>*Range:* 0 through 61440 (must be a multiple of 4096)<br>*Default:* 32768 |
| Forward Delay | Enter how long an interface remains in the listening and learning states, in seconds.<br>*Range:* 4 through 30 seconds<br>*Default:* 15 seconds |
| Hello Time | Enter the time interval for sending hello BPDUs, in seconds.<br>*Range:* 2 through 10 seconds<br>*Default:* 2 seconds |
| Maximum Age | Enter the aging time for received BPDUs. If another BPDU is not received from the remote bridge before the aging timer expires, the received BPDUs expire and the spanning state machine recomputes a new spanning-tree topology.<br>*Range:* 6 through 20 seconds<br>*Default*: 20 seconds |
| Force STP | Click to use STP to avoid loops for the switching instance. This option forces the switch to communicate on all ports using operations that are compatible with STP, as defined in IEEE 802.1D. |
| BPDU Block on Edge | Click to configure BPDU block on all edge ports of a switch. |

| Field | Description |
|---|---|
| Interface table | Displays the configured interfaces. To add interfaces, continue with Step 7. |

7. Click the + Add icon to add interfaces. In the Add Interfaces popup window, enter information for the following fields.



Add Interfaces

Interface:

Cost: 200000

Priority: 128

BPDU Protection Recovery Duration (secs): 30

BPDU Protection Action: STP Disable

□ Edge □ Loop Protection

□ Root Protection □ BPDU Protection □ BPDU Filter □ TCN Filter

| Field | Description |
|---|---|
| Interface | Select an interface. |
| Cost | Enter a value for the link cost associated with the interface.<br>*Range:* 1 through 200,000,000<br>*Default:* 20000 |
| Priority | Enter the port priority value. A lower priority value configures a higher priority. If there is a loop in the network, the port priority value is used to decide which ports to place in blocking state.<br>*Range*: 0 through 240 (must be a multiple of 16)<br>*Default*: 128 |

| Field | Description |
|---|---|
| BPDU Protection Recovery Duration | (For Releases 22.1.4 and later.) Enter the BPDU protection recovery time for the interface. This time is how long an interface remains blocked as a result of a BPDU protection action.<br>*Default*: 30 seconds |
| BPDU Protection Action | (For Releases 22.1.4 and later.) Select the action to to take when an interface receives a BPDU:<br>◦ Port down—Shut down the port.<br>◦ STP disable—Disable STP on the interface. This is the default.<br>*Default*: STP disable |
| Edge | Click to configure ports that are connected to end nodes to be edge ports. Ports configured as spanning-tree edge ports directly transition to the forwarding state. Edge ports do not generate topology changes when the link state changes. |
| Loop Protection | (For Releases 22.1.4 and later.) Click to enable loop protection on the interface. Loop prevention blocks the interface when it does not receive BPDUs, to prevent the interface from transitioning to the forwarding state. |
| Root Protection | (For Releases 22.1.4 and later.) Click to enable root protection on the interface. This protection prevents the interface from becoming a root port and forwarding traffic. |
| BPDU Protection | (For Releases 22.1.4 and later.) Click to enable BPDU protection on the interface. This protection prevents the interface from forwarding BPDUs. |
| BPDU Filter | (For Releases 22.1.4 and later.) Click to enable BPDU filtering on the interface. This filtering prevents the interface from sending or receiving BPDUs. |
| TCN Filter | (For Releases 22.1.4 and later.) Click to enable enable topology change notification filtering on the interface. This filtering prevents the interface from propagating received topology change notifications to other interfaces. |

8. Click OK.

To verify the RSTP configuration, issue the following CLI commands:

```
admin@VOS-cli> show spanning-tree bridge

switch-instance: vs1
Configured protocol : RSTP
Spanning tree Bridge parameters for instance : 0
Root Bridge Id : 200.0a:56:b2:b3:09:00
Hello time : 4 seconds
Maximum age : 20 seconds
Forward delay : 15 seconds
Number of topology changes : 10
Time since last topology change : 42949668 seconds
Local parameters
    Bridge Id : 200.0a:56:b2:b3:09:00*
```

```
admin@VOS-cli> show spanning-tree interface

switch-instance: vs1
Spanning tree interface parameters for instance : 0

Interface Port Designated            Port       State  Role
Name      Id   Bridge Id             Cost
--------- ---- ---------------------- ---------- ------ ------
vni-0/1    1  200.0a:56:b2:b3:09:00*  200000     FWD   DESG
vni-0/0    2  200.0a:56:b2:b3:09:00*  20         BLK   BKUP
```

## Configure MSTP

*For Releases 21.1.1 and later.*

You can configure the Multiple Spanning Tree Protocol (MSTP), which is defined in the 802.1s IEEE standard. The VOS implementation of MSTP supports one Common Internal Spanning Tree (CIST) and 64 multiple spanning-tree instances (MSTIs).

MSTP uses the following terminology:

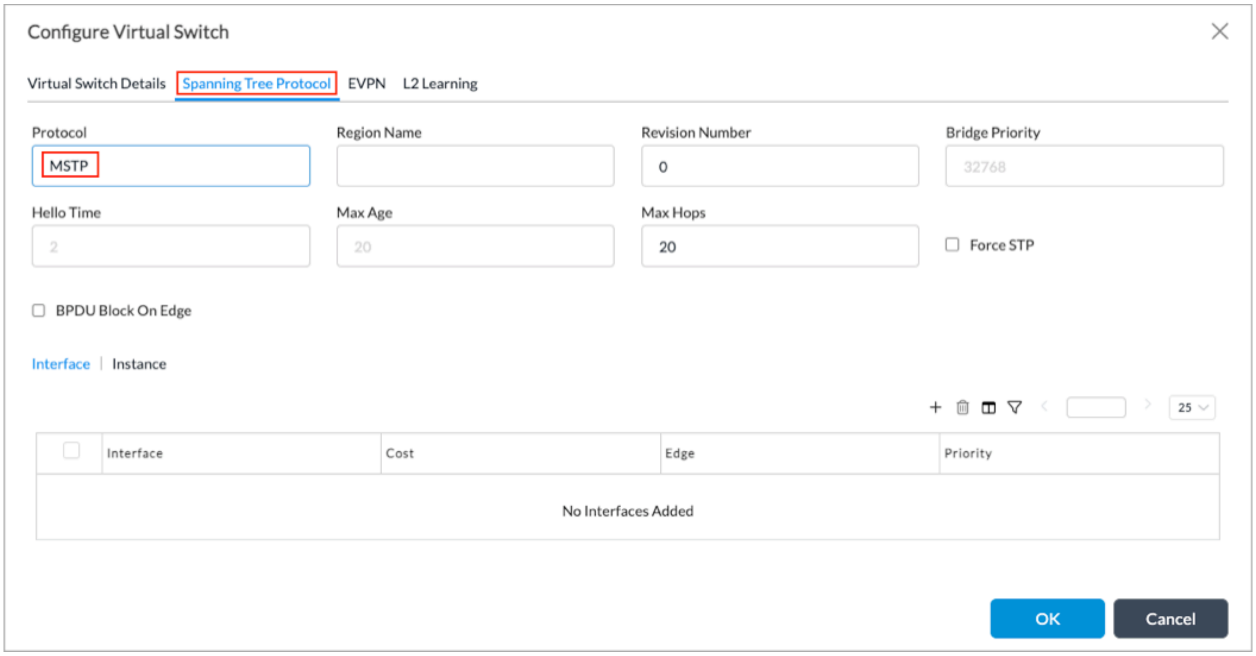
- Common Internal Spanning Tree (CIST)—CIST is same as an Internal Spanning Tree (IST) that is instance 0 inside a region.
- Common Spanning Tree (CST)—Provides connectivity between different MSTP regions and legacy STP and RSTP switches.
- Internal Spanning Tree Instance (IST)—A spanning-tree instance inside an MST region. By default, all VLANs are mapped to an IST with instance 0. All protocol packets (BPDUs) are exchanged in IST0.
- MSTP region—A set of interconnected switches that are configured with the same VLANs and MSTIs, that have the same region name and revision level, and that have the same VLANs mapped to same MSTIs.
- Multiple Spanning-Tree Instance (MSTI)—All static VLANs specifically assigned to an instance. An MSTI must include at least one VLAN.

You can group VLANs into a single MSTI. If a VLAN is not part of any MSTI, it belongs to a CIST. Layer 2 packets follow the MSTI and CIST topology corresponding to that VLAN.

You configure MSTP in a routing instance, either in a Layer 2 control routing instance or a virtual switch routing instance. When you configure MSTP in a Layer 2 control routing instance, the protocol state determined by MSTP is associated with all bridge domain interfaces on a port across all routing instances. When you configure MSTP in a virtual switch routing instance, all bridge domain interfaces corresponding to a port must be present on the virtual switch only.

To configure MSTP:

1. In Director view:
    a. Select the Administration tab in the top menu bar.
    b. Select Appliances in the left menu bar.
    c. Select an appliance 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 configured virtual switches.
4. Click the + Add icon. The Configure Virtual Switch popup window displays.
5. Select the Virtual Switch Details tab, and then enter an instance name for the virtual switch.
6. Select the Spanning-Tree Protocol tab, and enter information for the following fields.



Protocol: MSTP
Region Name:
Revision Number: 0
Bridge Priority: 32768
Hello Time: 2
Max Age: 20
Max Hops: 20
□ Force STP
□ BPDU Block On Edge

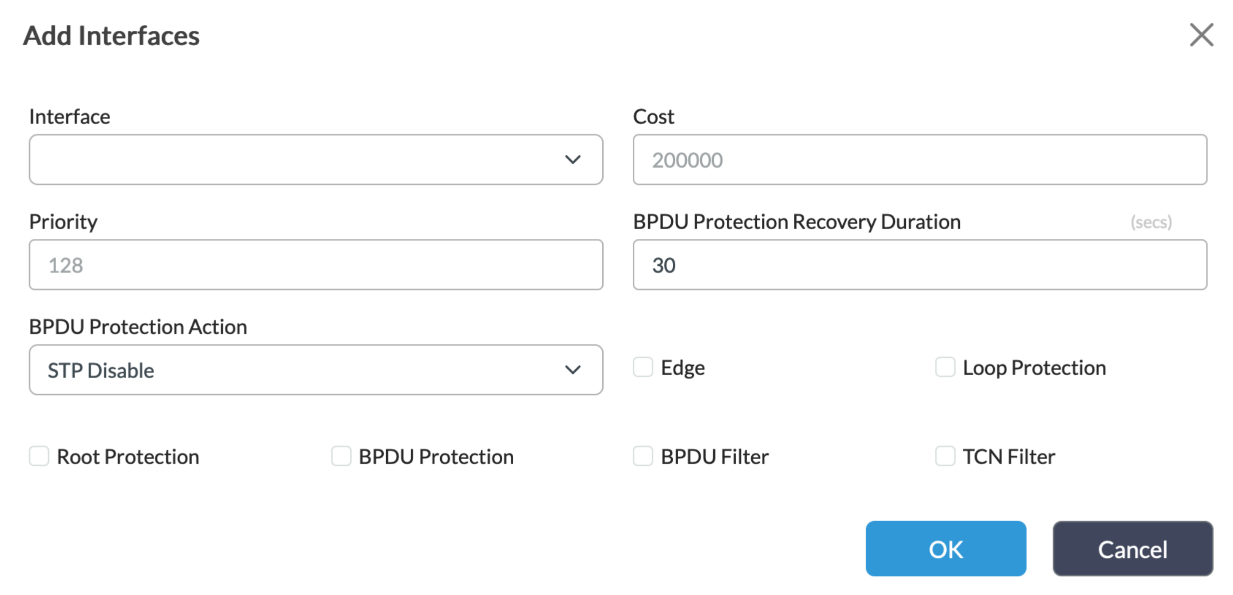
| □ | Interface | Cost | Edge | Priority |
|---|---|---|---|---|
| No Interfaces Added | | | | |

| Field | Description |
|---|---|
| Protocol | Select MSTP. |

| Field | Description |
|---|---|
| Region Name | Enter a name for the MSTP region. |
| Revision Number | Enter the MSTP revision number, which is a 16-bit number that identifies the current MSTP configuration. |
| Bridge Priority | Enter the bridge priority of MSTP. This value is used to determine which device in the spanning tree is the root bridge. A lower priority value configures a higher priority.<br>*Range:* 0 through 61440 (must be a multiple of 4096)<br>*Default:* 32768 |
| Hello Time | Enter the time interval for sending hello BPDUs, in seconds.<br>*Range:* 2 through 10 seconds<br>*Default:* 2 seconds |
| Maximum Age | Enter the aging time for the received BPDUs. If another BPDU is not received from the remote bridge before the maximum age timer expires, the received BPDUs expire and the spanning state machine recomputes a new spanning-tree topology.<br>*Range:* 6 through 20 seconds<br>*Default*: 20 seconds |
| Maximum Hops | Enter the maximum number of hops that a BPDU can be forwarded in an MSTP region.<br>*Range:* 1 through 40<br>*Default*: 20 |
| Force STP | Click to use STP to avoid loops for this switching instance. This option forces the switch to communicate on all ports using operations that are compatible with STP, as defined in IEEE 802.1D. |
| BPDU Block on Edge | Click to configure BPDU block on all edge ports of a |

| Field | Description |
|---|---|
| | switch. |

7. Select the Interface tab, and then click the  Add icon to configure MSTP on an interface. In the Add Interfaces popup window, enter information for the following fields.



Add Interfaces

Interface:

Cost: 200000

Priority: 128

BPDU Protection Recovery Duration (secs): 30

BPDU Protection Action: STP Disable

□ Edge

□ Loop Protection

□ Root Protection

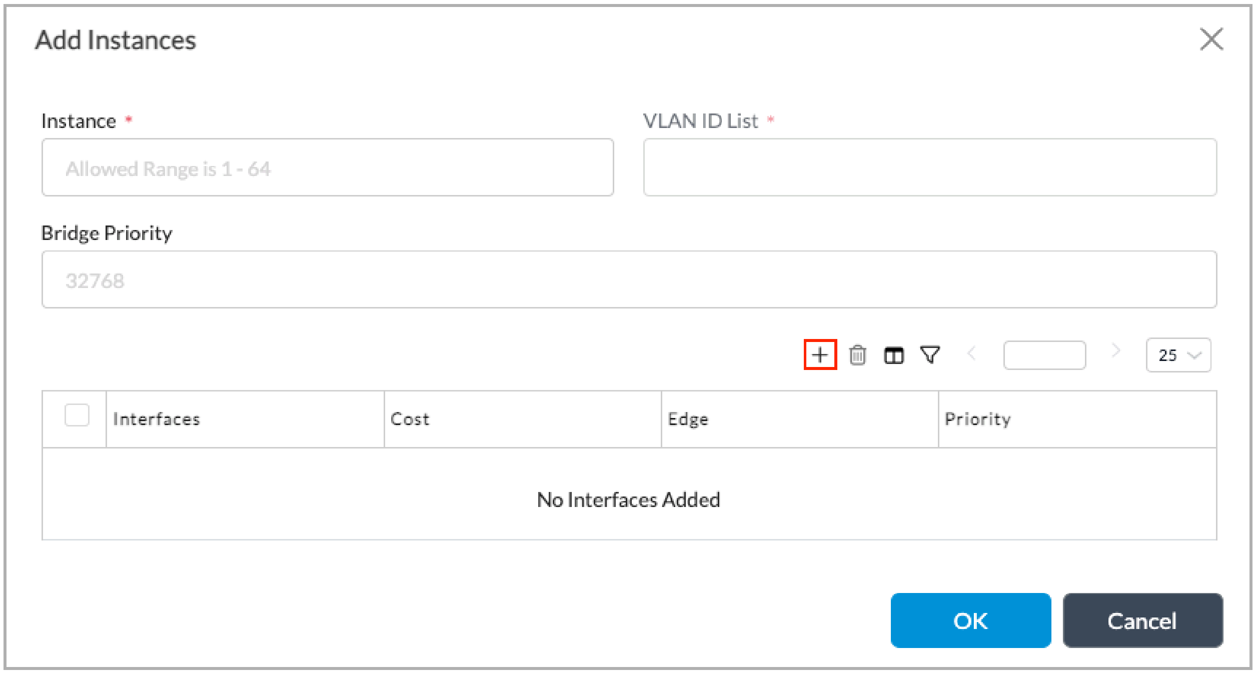
□ BPDU Protection

□ BPDU Filter

□ TCN Filter

| Field | Description |
|---|---|
| Interface | Select an interface on which to enable MSTP. |
| Cost | Enter a value for the link cost associated with the interface. The virtu<br>*Range:* 1 through 200000000<br>*Default:* 20000 |
| Priority | Enter the port priority value. A lower the priority value configures a h decide which ports to place in blocking state.<br>*Range*: 0 through 240, in increments of 16<br>*Default*: 128 |
| BPDU Protection Recovery Duration | (For Releases 22.1.4 and later.) Enter the BPDU protection recovery result of a BPDU protection action.<br>*Default*: 30 seconds |
| BPDU Protection Action | (For Releases 22.1.4 nd later.) Select the action to take when an inte<br>◦ Port down—Shut down the port.<br>◦ STP disable—Disable STP on the interface. This is the default<br>*Default*: STP disable |
| Edge | Click to configure ports that are connected to end nodes to be spanr When the link state changes, edge ports do not generate topology c |
| Loop Protection | (For Releases 22.1.4 and later.) Click to enable loop protection on th BPDUs, to prevent the interface from transitioning to the forwarding |
| Root Protection | (For Releases 22.1.4 and later.) Click to enable root protection on th forwarding traffic. |
| BPDU Protection | (For Releases 22.1.4 and later.) Click to enable BPDU protection on |
| BPDU Filter | (For Releases 22.1.4 and later.) Click to enable BPDU filtering on th BPDUs. |
| TCN Filter | (For Releases 22.1.4 and later.) Click to enable enable topology cha from propagating received topology change notifications to other inte |

8. Select the Instances tab, and then click the  Add icon to add interfaces to the MSTI instance. In the Add Instances popup window, enter information for the following fields. Note that if you configure interfaces at the MSTP > MSTI > Interfaces hierarchy level, the MSTI interfaces values override the values configured at the MSTP > Interfaces hierarchy level.



Add Instances

Instance *: Allowed Range is 1 - 64

VLAN ID List *:

Bridge Priority: 32768

| □ | Interfaces | Cost | Edge | Priority |
|---|---|---|---|---|
| No Interfaces Added | | | | |

| Field | Description |
|---|---|
| Instance (Required) | Enter the instance number.<br>*Range*: 1 to 64<br>*Default*: None |
| VLAN ID List | Enter a list of VLAN identifiers. You can enter a range of VLANs (for 27), or a combination of the two formats (for example, 1 15-20 25 27 |
| Bridge Priority | Enter the MSTP bridge priority. This value is used to determine whic a higher priority.<br>*Range:* 0 through 61440 (must be a multiple of 4096)<br>*Default:* 32768 |
| Interface table | Click the  Add icon to add interfaces to the instance. Enter informatic<br>◦ Interface—Select an interface.<br>◦ Cost—Enter a value for the link cost associated with the interfac<br>*Range:* 1 through 200000000<br>*Default:* 20000<br>◦ Priority—Enter the bridge priority of the instance interface.<br>*Range:* 0 through 61440 (must be a multiple of 4096)<br>*Default:* 32768<br>◦ Edge—Click to configure ports that are connected to end nodes transition to the forwarding state. Edge ports do not generate to<br>Then, click OK. |

9. Click OK.

   To verify the MSTP configuration, issue the following CLI command:

```
admin@br102-cli> show spanning-tree

Routing-instance    : Tenant1_L2
Configured protocol : MSTP
    Region                      : region2
    Revision                     : 3
    Digest                        : 0xbf94d89eaf6de4e7cc93d5709ba43873
    Hello time                    : 2 seconds
    Maximum age                   : 20 seconds
    Forward delay                 : 15 seconds

  Spanning tree Bridge parameters for instance : 0
    CIST regional root bridge Id    : 4096.0a:30:00:1c:69:01
    CIST internal root cost         : 199999
    Root port                     : ae0
    Member Vlans                  : 1-999 1081-4094
    Number of topology changes      : 10
    Time since last topology change : 29 seconds
    Local parameters
      Bridge Id                   : 32768.0a:30:00:1b:8b:01

  Spanning tree Bridge parameters for instance : 1
    MSTI regional root bridge Id    : 32768.0a:30:00:1b:8b:01
    Member Vlans                  : 1000-1080
    Number of topology changes      : 1
    Time since last topology change : 29 seconds
    Local parameters
      Bridge Id                   : 32768.0a:30:00:1b:8b:01*

Routing-instance: Tenant1_L2

Spanning tree interface parameters for instance : 0

Interface    Port Id  Designated Bridge         Port Cost   State   Role
-----------  -------  -----------------------  ---------   -----   ----
ae0          1        4096.0a:30:00:1c:69:01    199999      FWD     ROOT
vni-0/8      2        4096.0a:30:00:1c:69:01    200000      BLK     ALT
vni-0/9      3        32768.0a:30:00:1b:8b:01*  200000      FWD     DESG

Spanning tree interface parameters for instance : 1

Interface    Port Id  Designated Bridge         Port Cost   State   Role
-----------  -------  -----------------------  ---------   -----   ----
ae0          1        32768.0a:30:00:1b:8b:01*  199999      FWD     DESG
vni-0/8      2        32768.0a:30:00:1b:8b:01*  200000      FWD     DESG
vni-0/9      3        32768.0a:30:00:1b:8b:01*  200000      FWD     DESG

Routing-instance: Tenant1_L2

Spanning tree statistics for instance : 0

Interface   BPDUs      BPDUs       Tcn         Proposal    Agreement    Rx
Name        Sent       Received    Tx/Rx       Tx/Rx       Tx/Rx        Errors
---------   ---------  ----------- ----------  --------    -----------  ----------
ae0            48       198053     10/28       13/21      34/198047       0
vni-0/8        59       198066      8/29       20/23      39/198063       0
vni-0/9     197871         159     10/25        18/7      197851/157      0

Spanning tree statistics for instance : 1
```

```
Interface   BPDUs     BPDUs        Tcn         Proposal    Agreement     Rx
Name        Sent      Received     Tx/Rx       Tx/Rx       Tx/Rx         Errors
---------   ---------  -----------  ----------  --------    -----------  ----------
ae0          26            27      2/0          5/0        24/51          0
vni-0/8       26            24      2/2          5/0        25/46          0
vni-0/9       25             0      2/1          4/0        24/2           0
```

The **show spanning-tree** command output displays the following fields:

| **Command** | **Description** |
|---|---|
| Routing Instance | Name of the routing instance in which the bridge is configured. |
| Configured Protocol | Type of spanning-tree protocol that is enabled. |
| Root Bridge ID | Bridge identifier of the elected spanning-tree root bridge. The bridge ID consists of a configurable bridge priority and the MAC address of the bridge. |
| Hello Time | Configured number of seconds between transmissions of configuration BPDUs. |
| Maximum Age | Aging time for the received BPDUs. |
| Forward Delay | How long an STP bridge port remains in the listening and learning states before transitioning to the forwarding state. |
| Number of Topology Changes | Total number of STP topology changes detected since the routing device last booted. |
| Time Since Last Topology Change | Number of seconds that have elapsed since the most recent topology change. |
| Local Bridge ID | Locally configured bridge identifier. The bridge ID consists of a configurable bridge priority and the MAC address of the bridge. |

| Command | Description |
|---|---|
| Region | Collection of switches with the same MSTP configuration. |
| Revision | 16-bit number that identifies the current MSTP configuration. |
| Digest | MD5 digest calculated using VLAN-to-MTSI mapping. |

## Configure EVPN over SD-WAN

*For Releases 21.1.1 and later.*

You can configure EVPN Type 2 and Type 3 control plane–based MAC learning and distribution using BGP, as described in RFC 7432. VOS devices support the following EVPN features:

- Route target (RT) and route distinguisher (RD) per virtual switch
- Selective signaling of certain bridge domains
- BUM label per bridge domain VLAN
- Distribution of local IRB and VRRP MAC addresses using BGP
- Centralized IRB

On edge devices, MAC addresses that are learned through the data plane are propagated through BGP to other edge devices in the EVPN network.

In the forwarding plane, Layer 2 packets from a LAN that are destined for a device that is behind another SD-WAN branch are encapsulated in the VXLAN/IPsec (SD-WAN encapsulation) header and sent over the SD-WAN overlay. When these Layer 2 packets are received by the remote branch device, the SD-WAN header is removed, and the traffic is forwarded by performing a MAC address lookup, as would be the case with regular Layer 2 traffic. For packets from a LAN that are destined to a device in the same LAN, the MAC address lookup returns a local Layer 2 logical interface, and the traffic is forwarded locally, in the same way as regular Layer 2 packets. For packets from a LAN that are destined to a router MAC address, the packet is routed as a Layer 3 packet.

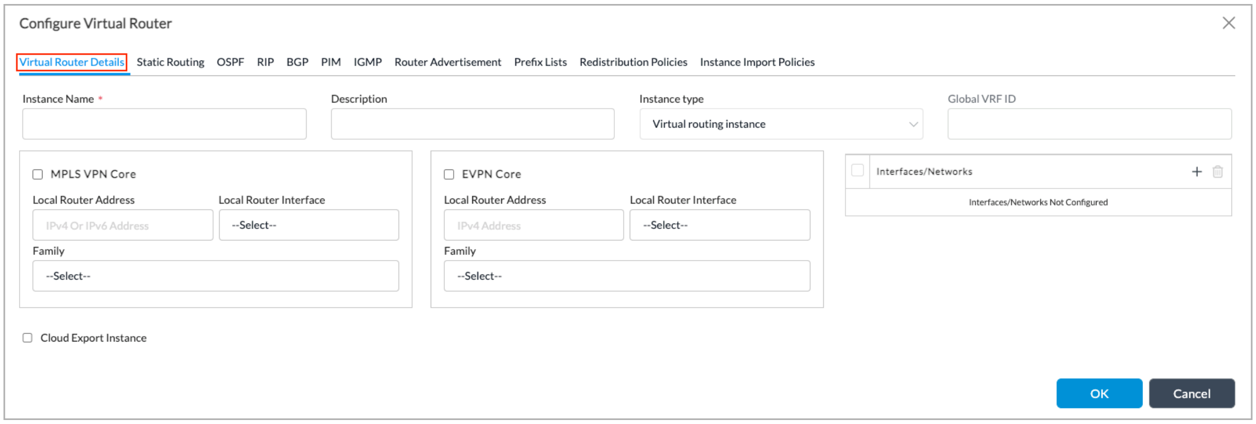
Note that when handling BUM traffic, an ingress replication list supports a maximum of 64 EVPN neighbors.

## Configure a Core EVPN Routing Instance

Before you configure EVPN over SD-WAN, you must create a core EVPN routing instance.

To configure a core EVPN routing instance:

1. In Director view:
    a. Select the Administration tab in the top menu bar.
    b. Select Appliances in the left menu bar.
    c. Select an appliance 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. The screen displays all configured virtual routers.
4. Click the + Add icon. In the Configure Virtual Router popup window, select the Virtual Router Details tab, and then enter the information for the following fields.



Configure Virtual Router

Instance Name *

Description

Instance type: Virtual routing instance

Global VRF ID

□ MPLS VPN Core

Local Router Address: IPv4 Or IPv6 Address

Local Router Interface: --Select--

Family: --Select--

□ EVPN Core

Local Router Address: IPv4 Address

Local Router Interface: --Select--

Family: --Select--

□ Interfaces/Networks +

Interfaces/Networks Not Configured

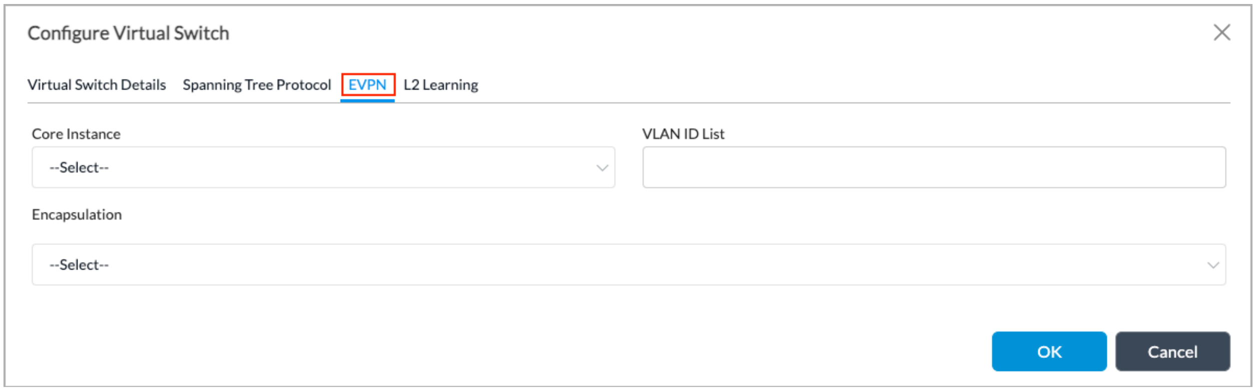
□ Cloud Export Instance

| **Field** | **Description** |
|---|---|
| Instance Name (Required) | Enter a name for the core EVPN routing instance. |
| Instance Type | Select Virtual Routing Instance. |
| Global VRF ID | Enter the global VRF ID number. |
| Interfaces/Networks (Table) | Click the + Add icon, and select one or more interfaces to assign to the routing instance. |
| EVPN Core | Click to enable EVPN core. |
| EVPN Local Router Address | Enter the IP address of the local EVPN router. |
| EVPN Local Router Interface | Select a local router interface for the EVPN core. |
| Family | Select inet. |
| Create Dynamic GRE Tunnels | Click to create GRE tunnels dynamically. |

5. Click OK.

## Configure EVPN over SD-WAN

1. In Director view:
    1. Select the Administration tab in the top menu bar.
    2. Select Appliances in the left menu bar.
    3. Select an appliance in the main pane. The view changes to Appliance view.
2. Select Configuration in the top menu bar.
3. Select Networking in the left menu bar.
4. Select Virtual Switches. The main pane displays a list of the configured virtual switches.
5. Click the + Add icon. The Configure Virtual Switch screen displays.
6. Select the EVPN tab, and then enter the information for the following fields.



| Field | Description |
|---|---|
| Core Instance | Select a core EVPN routing instance. |
| VLAN ID List | Enter a list of VLAN identifiers. You can enter a range of VLANs (for example, 10-20), a list of VLAN IDs separated by spaces (for example, 1 25 27), or a combination of a range and a list (for example, 1 15-20 25 27). |
| Encapsulation | Select MPLS or EVPN encapsulation from the drop-down list. |

7. Click OK.

## Configure VLAN Translation

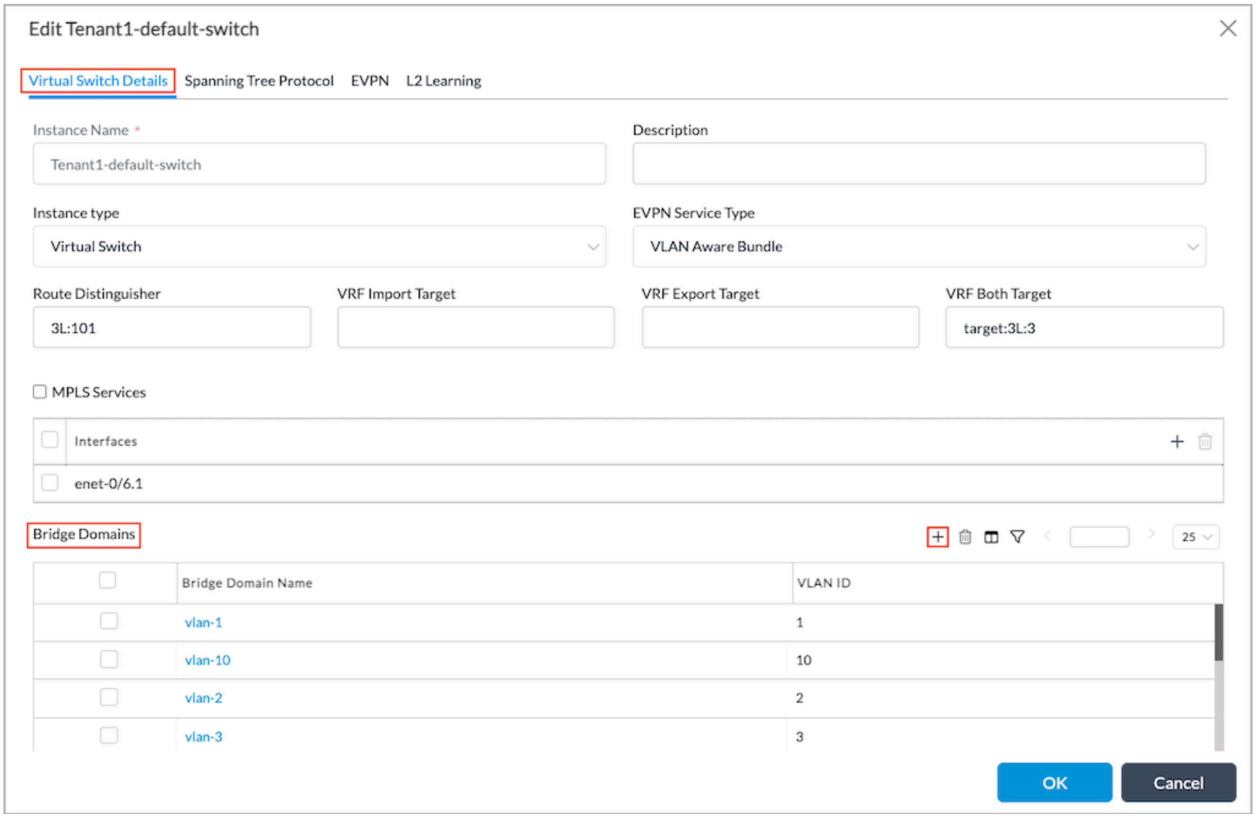
*For Releases 21.1.1 and later.*

VLAN translation maps ingress traffic on one VLAN to a different VLAN on the egress interface. Layer 2 logical interfaces that belong to a bridge domain can have different VLAN IDs from those of the bridge domain to which they belong. As a result, a VLAN identifier in a packet acts like a circuit identifier and, for the purposes of learning and forwarding, it is normalized to the bridge domain VLAN. The VLAN identifier is then translated to the identifier of the VLAN that is configured on the egress VLAN logical interface.

Note: VLAN translation is not supported on trunk or paired TVI interfaces.

To configure VLAN translation:

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 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 a virtual switch in the main pane. The Edit screen displays.
5. Select the Virtual Switch Details tab, and then click the + Add icon in the Bridge Domains table.



Instance Name *: Tenant1-default-switch

Description:

Instance type: Virtual Switch

EVPN Service Type: VLAN Aware Bundle

Route Distinguisher: 3L:101

VRF Import Target:

VRF Export Target:

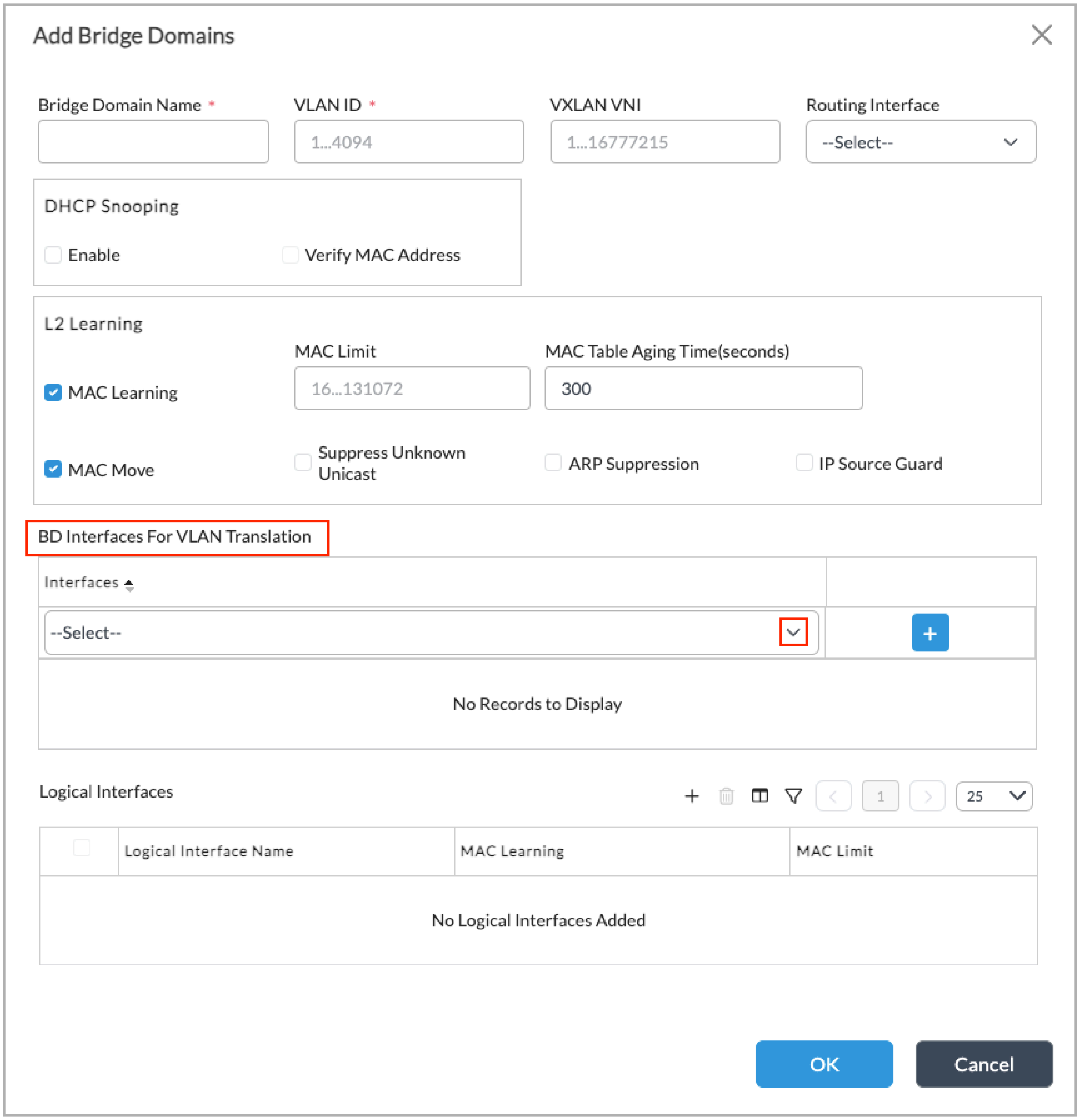
VRF Both Target: target:3L:3

□ MPLS Services

| □ | Interfaces |
|---|---|
| □ | enet-0/6.1 |

| □ | Bridge Domain Name | VLAN ID |
|---|---|---|
| □ | vlan-1 | 1 |
| □ | vlan-10 | 10 |
| □ | vlan-2 | 2 |
| □ | vlan-3 | 3 |

6. Click the + Add icon in the Bridge Domains table. In the Add Bridge Domains popup window, enter information for the fields, as described in Configure a Virtual Switch with Bridge Domains and Bridge Interfaces, above.



Add Bridge Domains

| | | | |
|---|---|---|---|
| Bridge Domain Name * | VLAN ID * | VXLAN VNI | Routing Interface |
| | 1...4094 | 1...16777215 | --Select-- |

DHCP Snooping

□ Enable □ Verify MAC Address

L2 Learning

| | | |
|---|---|---|
| | MAC Limit | MAC Table Aging Time(seconds) |
| ☑ MAC Learning | 16...131072 | 300 |

☑ MAC Move □ Suppress Unknown Unicast □ ARP Suppression □ IP Source Guard

BD Interfaces For VLAN Translation

| Interfaces | |
|---|---|
| --Select-- | + |
| No Records to Display | |

Logical Interfaces

| □ | Logical Interface Name | MAC Learning | MAC Limit |
|---|---|---|---|
| No Logical Interfaces Added | | | |

7. In the BD Interfaces for VLAN Translation table, select a Layer 2 interface. In the ingress direction, the VLAN ID of the interface that you select is translated to the bridge domain VLAN ID, and in the egress direction, the VLAN ID is translated from the bridge domain VLAN ID to the interface VLAN ID. MAC addresses learned on this interface are based on the bridge domain VLAN ID.

8. Click the + Add icon to add the interface.

9. Click OK.

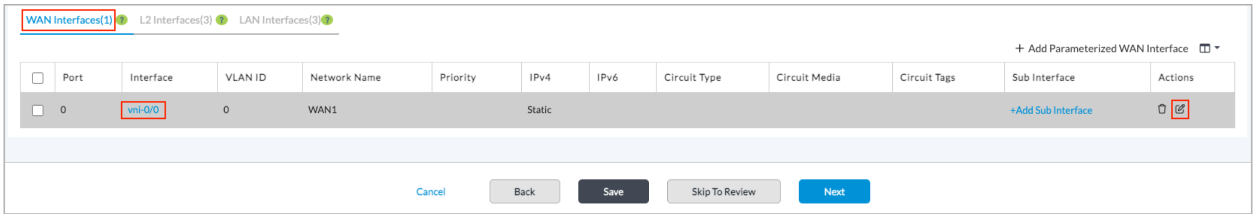
## Configure Layer 2 Forwarding Using Workflow Templates

*For Releases 21.1.1 and later.*

You can configure the Layer 2 forwarding using Workflow templates. For complete information about creating or editing Workflow templates, see Create Device Templates.

To configure Layer 2 forwarding using Workflow templates:

1. In Director view, select the Workflows tab in the top menu bar.
2. Select Template > Templates in the horizontal menu bar.
3. Select an organization from the Organization drop-down list.
4. To edit an existing template, click the template name in the main pane. To add a new template, click the + Add icon. The Create Template or Edit Template screen displays.
5. Select the Basic tab and enter the required information.
6. Select the Interfaces tab.
7. Select the WAN Interfaces tab, and enter the required information to configure WAN interfaces.

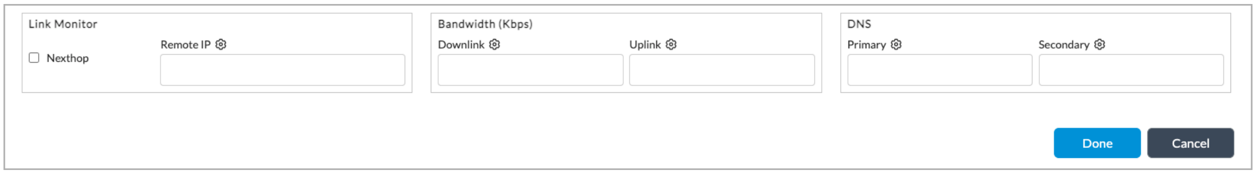


WAN Interfaces(1) L2 Interfaces(3) LAN Interfaces(3)

+ Add Parameterized WAN Interface

| □ | Port | Interface | VLAN ID | Network Name | Priority | IPv4 | IPv6 | Circuit Type | Circuit Media | Circuit Tags | Sub Interface | Actions |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | 0 | vni-0/0 | 0 | WAN1 |  | Static |  |  |  |  | +Add Sub Interface |  |

8. Click the interface name or the Edit icon under the Actions heading to configure additional parameters. Note that you must hover over the row for the interface to see the icons under the Action heading.

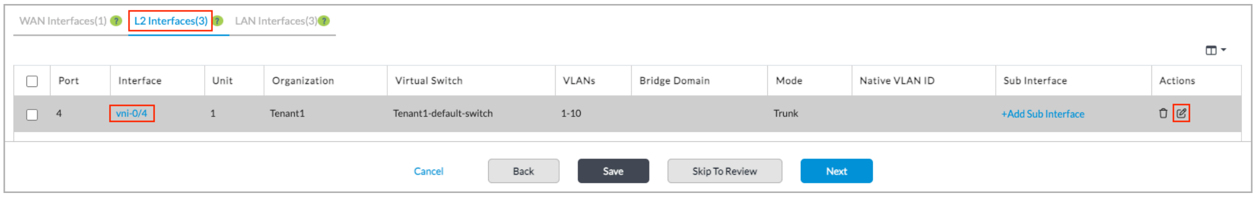


Link Monitor
□ Nexthop
Remote IP

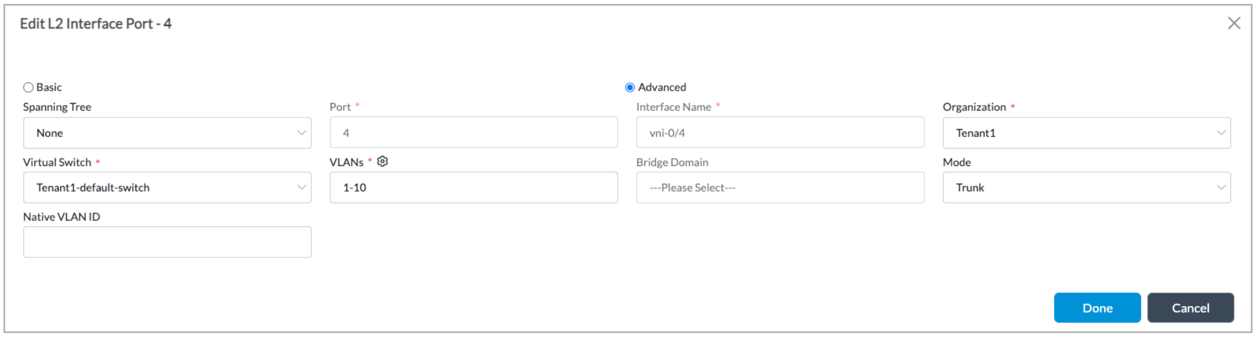
Bandwidth (Kbps)
Downlink
Uplink

DNS
Primary
Secondary

9. Click Done to return to the Interfaces screen.
10. Select the L2 Interfaces tab, and enter the required information to configure L2 interfaces.



| □ | Port | Interface | Unit | Organization | Virtual Switch | VLANs | Bridge Domain | Mode | Native VLAN ID | Sub Interface | Actions |
|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | 4 | vni-0/4 | 1 | Tenant1 | Tenant1-default-switch | 1-10 | | Trunk | | +Add Sub Interface | |



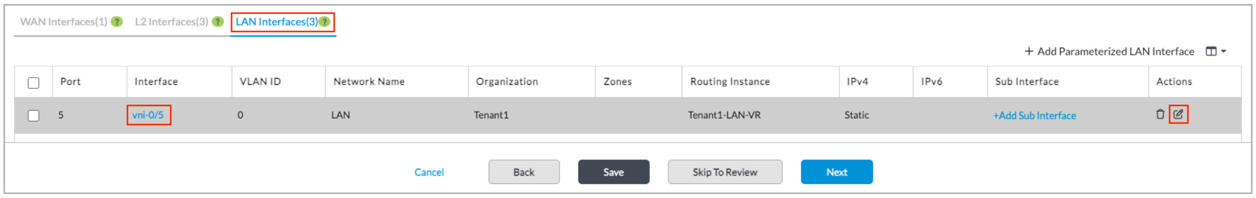
Edit L2 Interface Port - 4

○ Basic

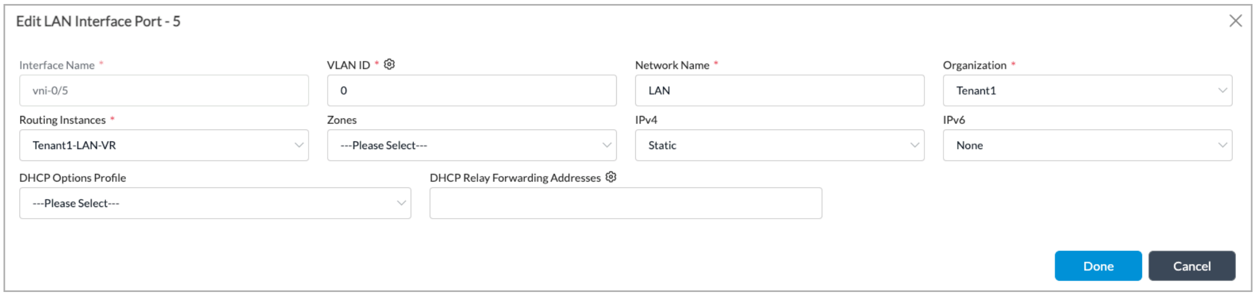
● Advanced

| | | | |
|---|---|---|---|
| Spanning Tree: None | Port *: 4 | Interface Name *: vni-0/4 | Organization *: Tenant1 |
| Virtual Switch *: Tenant1-default-switch | VLANs *: 1-10 | Bridge Domain: ---Please Select--- | Mode: Trunk |
| Native VLAN ID: | | | |

11. Select the LAN Interfaces tab, and enter the required information to configure LAN interfaces.



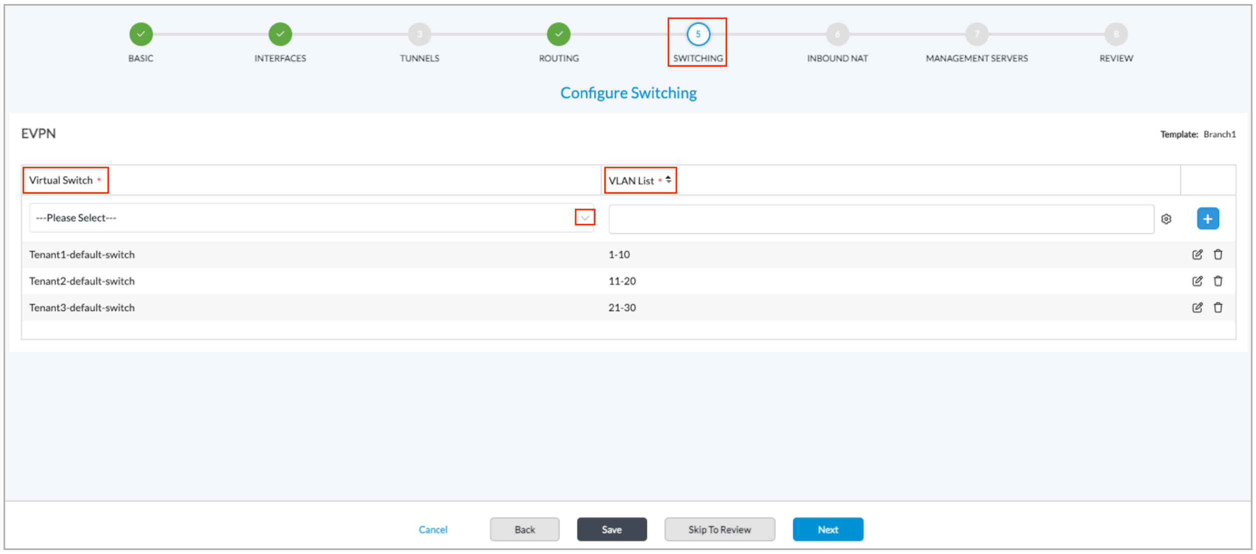
| □ | Port | Interface | VLAN ID | Network Name | Organization | Zones | Routing Instance | IPv4 | IPv6 | Sub Interface | Actions |
|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | 5 | vni-0/5 | 0 | LAN | Tenant1 | | Tenant1-LAN-VR | Static | | +Add Sub Interface | |



Edit LAN Interface Port - 5

| | | | |
|---|---|---|---|
| Interface Name *: vni-0/5 | VLAN ID *: 0 | Network Name *: LAN | Organization *: Tenant1 |
| Routing Instances *: Tenant1-LAN-VR | Zones: ---Please Select--- | IPv4: Static | IPv6: None |
| DHCP Options Profile: ---Please Select--- | DHCP Relay Forwarding Addresses: | | |

12. Select Switching tab, and enter the following information to configure EVPN over SD-WAN.



Configure Switching

EVPN

Template: Branch1

| Virtual Switch * | VLAN List * |
|---|---|
| ---Please Select--- | |
| Tenant1-default-switch | 1-10 |
| Tenant2-default-switch | 11-20 |
| Tenant3-default-switch | 21-30 |

| Field | Description |
|---|---|
| Virtual Switch | Select a virtual switch from the drop-down list. |
| VLAN List | Enter a list of VLAN IDs for the virtual switch. Click the + Add icon to add the VLAN list. |

13. Click Next to advance to the next screen, or click Save or Skip to Review.

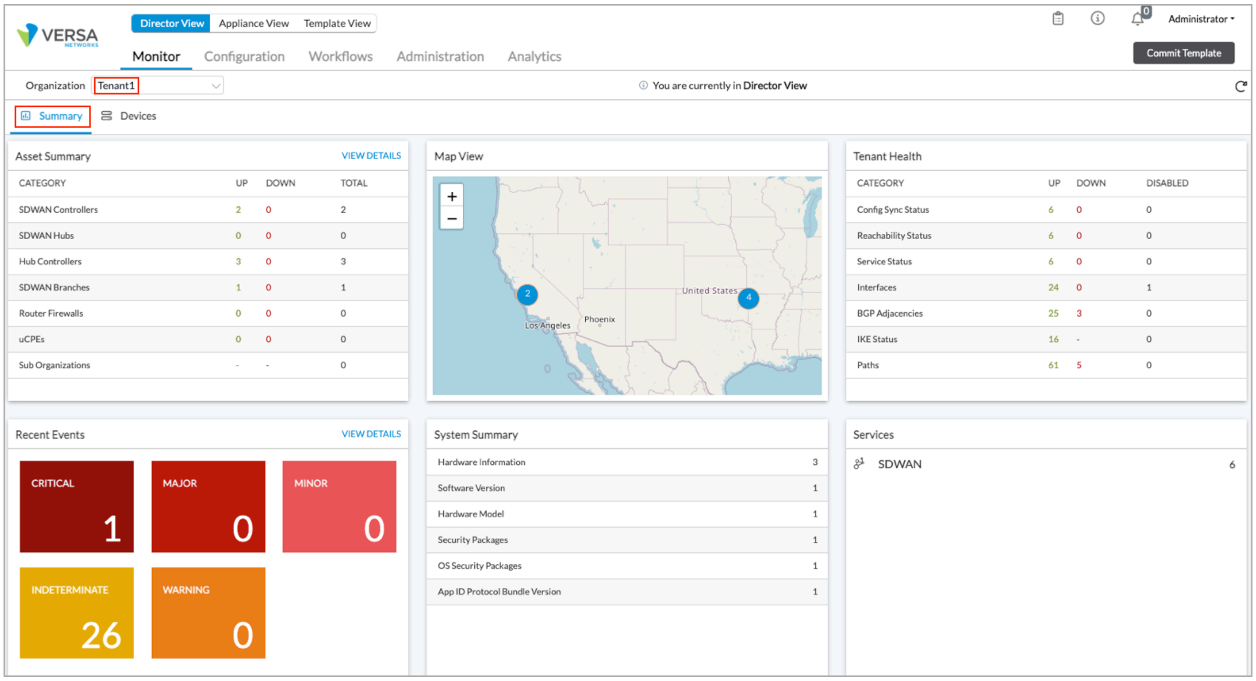
## Monitor Layer 2 Forwarding

You can monitor the following Layer 2 forwarding features:

- ARP suppression
- Bridge domain interfaces
- MAC address table
- Spanning tree

To monitor Layer 2 forwarding:

1. In Director view, select the Monitor tab in the top menu bar.
2. Select an organization in the Organization field.
3. Select the Summary tab in the horizontal menu bar to display status information about that organization.



Asset Summary

| CATEGORY | UP | DOWN | TOTAL |
|---|---|---|---|
| SDWAN Controllers | 2 | 0 | 2 |
| SDWAN Hubs | 0 | 0 | 0 |
| Hub Controllers | 3 | 0 | 3 |
| SDWAN Branches | 1 | 0 | 1 |
| Router Firewalls | 0 | 0 | 0 |
| uCPEs | 0 | 0 | 0 |
| Sub Organizations | - | - | 0 |

Tenant Health

| CATEGORY | UP | DOWN | DISABLED |
|---|---|---|---|
| Config Sync Status | 6 | 0 | 0 |
| Reachability Status | 6 | 0 | 0 |
| Service Status | 6 | 0 | 0 |
| Interfaces | 24 | 0 | 1 |
| BGP Adjacencies | 25 | 3 | 0 |
| IKE Status | 16 | - | 0 |
| Paths | 61 | 5 | 0 |

Recent Events

| | |
|---|---|
| CRITICAL | 1 |
| MAJOR | 0 |
| MINOR | 0 |
| INDETERMINATE | 26 |
| WARNING | 0 |

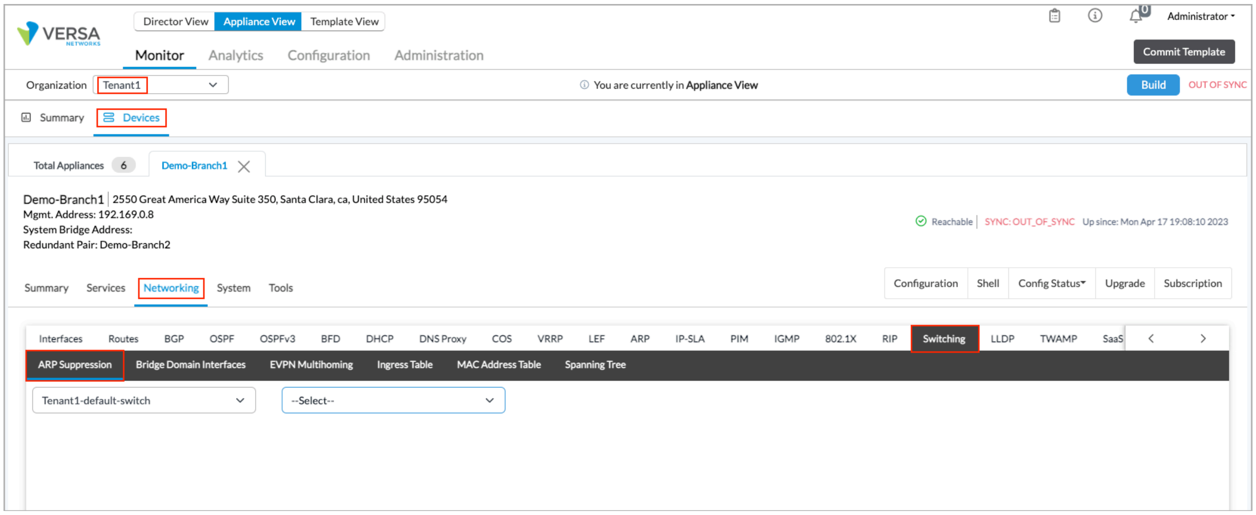
System Summary

| | |
|---|---|
| Hardware Information | 3 |
| Software Version | 1 |
| Hardware Model | 1 |
| Security Packages | 1 |
| OS Security Packages | 1 |
| App ID Protocol Bundle Version | 1 |

Services

| | |
|---|---|
| SDWAN | 6 |

4. Select the Devices tab in the horizontal menu bar.
5. Select a device in the main pane.
6. Select the Networking tab in the horizontal menu bar, and then select Switching.



Demo-Branch1 | 2550 Great America Way Suite 350, Santa Clara, ca, United States 95054
Mgmt. Address: 192.169.0.8
System Bridge Address:
Redundant Pair: Demo-Branch2

Reachable | SYNC: OUT_OF_SYNC Up since: Mon Apr 17 19:08:10 2023

Tenant1-default-switch
--Select--

7. Select ARP Suppression in the horizontal menu bar.
8. Select a routing instance in the first drop-down list.
9. Select an VLAN ID in the second drop-down list. The ARP suppression data displays.

   You can also use the **show bridge arp-suppression-table** CLI command to display the ARP suppression table. The flags indicate whether the ARP entry is locally or remotely learned.

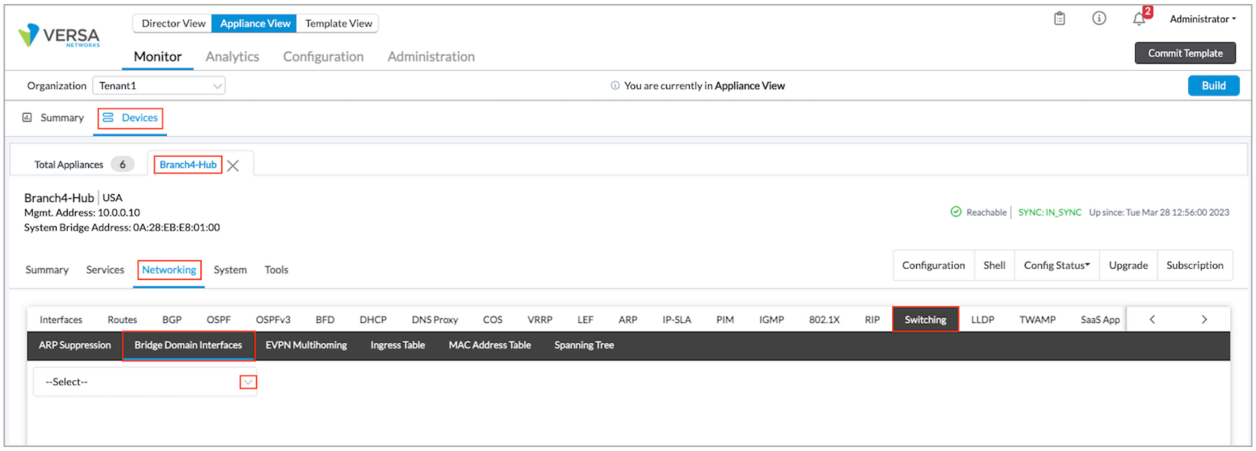
If you issue the **show bridge arp-suppression-table** command on the local branch, the output is similar to the following:

```
> show bridge arp-suppression-table

MAC TYPE Legend
C:Control S:Static D:Dynamic R:Router V:VRRP B:Sink M:Multi-Home A:ARP
                                                REMOTE
                                                BRANCH
ROUTING      BRIDGE     LOGICAL                        OR TUNNEL   IP
INSTANCE     NAME       INTERFACE   MAC-ADDRESS          MAC    VLANID  TYPE      ENDPOINT
ADDRESS
------------------------------------------------------------------------------------------------
l2-vrf       bd-11      vni-0/4.11   00:00:01:00:00:00   DA     11      N/A       192.168.60.20
l2-vrf       bd-11      vni-0/4.11   00:00:01:00:00:01   DA     11      N/A       192.168.60.21
```

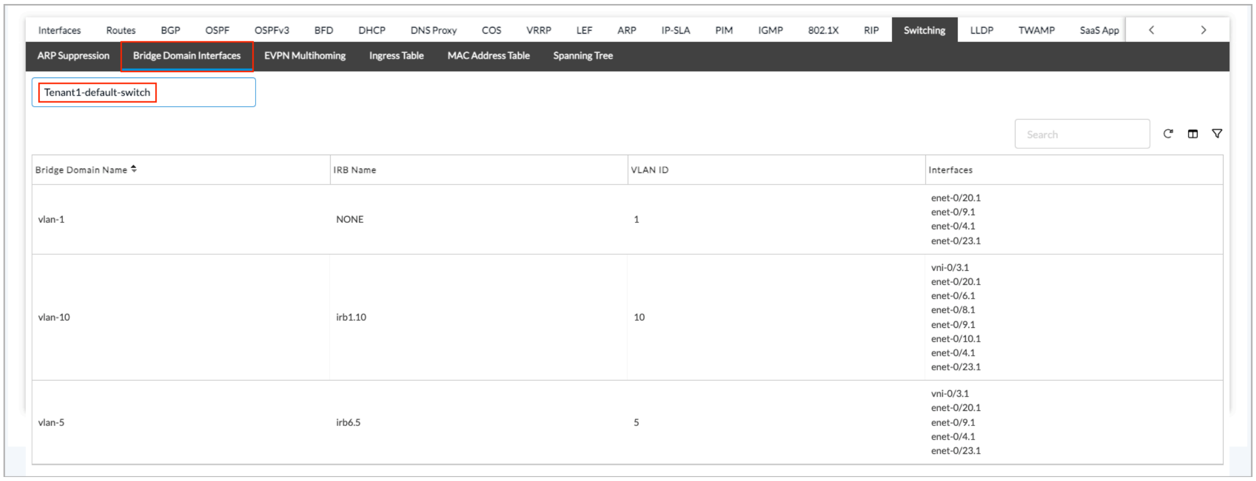
If you issue the **show bridge arp-suppression-table** command on the remote branch, the output is similar to the following:

```
> show bridge arp-suppression-table

MAC TYPE Legend
C:Control S:Static D:Dynamic R:Router V:VRRP B:Sink M:Multi-Home A:ARP
                                                REMOTE
                                                BRANCH
ROUTING      BRIDGE     LOGICAL                        OR TUNNEL   IP
INSTANCE     NAME       INTERFACE   MAC-ADDRESS          MAC    VLANID  TYPE      ENDPOINT
ADDRESS
------------------------------------------------------------------------------------------------
l2-vrf       bd-11      dtvi-0/42   00:00:01:00:00:00   CA     11      Branch1    192.168.60.20
l2-vrf       bd-11      dtvi-0/42   00:00:01:00:00:01   CA     11      Branch1    192.168.60.21
```

10. Select the Bridge Domain Interfaces tab.



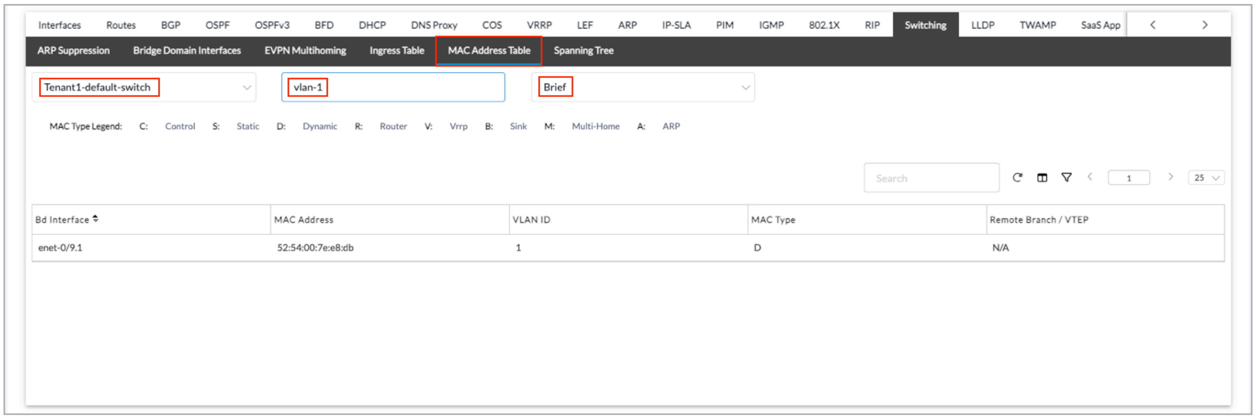
11. Select a switch name from the drop-down list to display information about bridge domain interfaces.



Tenant1-default-switch

| Bridge Domain Name | IRB Name | VLAN ID | Interfaces |
|---|---|---|---|
| vlan-1 | NONE | 1 | enet-0/20.1<br>enet-0/9.1<br>enet-0/4.1<br>enet-0/23.1 |
| vlan-10 | irb1.10 | 10 | vni-0/3.1<br>enet-0/20.1<br>enet-0/6.1<br>enet-0/8.1<br>enet-0/9.1<br>enet-0/10.1<br>enet-0/4.1<br>enet-0/23.1 |
| vlan-5 | irb6.5 | 5 | vni-0/3.1<br>enet-0/20.1<br>enet-0/9.1<br>enet-0/4.1<br>enet-0/23.1 |

12. Select the MAC Address Table tab, select a switch name, and then select a VLAN to display information from the MAC address table.

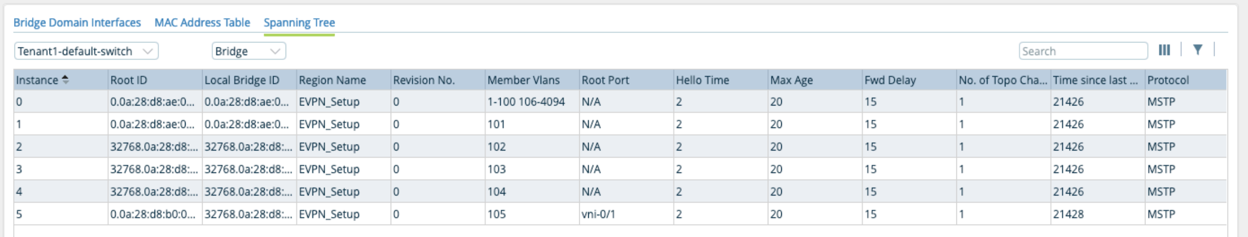


Tenant1-default-switch | vlan-1 | Brief

MAC Type Legend: C: Control S: Static D: Dynamic R: Router V: Vrrp B: Sink M: Multi-Home A: ARP

| Bd Interface | MAC Address | VLAN ID | MAC Type | Remote Branch / VTEP |
|---|---|---|---|---|
| enet-0/9.1 | 52:54:00:7e:e8:db | 1 | D | N/A |

13. Select the Spanning Tree tab, select a switch name, and then select Bridge, Interface, or Statistics to display spanning-tree information.



Tenant1-default-switch | Bridge

| Instance | Root ID | Local Bridge ID | Region Name | Revision No. | Member Vlans | Root Port | Hello Time | Max Age | Fwd Delay | No. of Topo Cha... | Time since last ... | Protocol |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0.0a:28:d8:ae:0... | 0.0a:28:d8:ae:0... | EVPN_Setup | 0 | 1-100 106-4094 | N/A | 2 | 20 | 15 | 1 | 21426 | MSTP |
| 1 | 0.0a:28:d8:ae:0... | 0.0a:28:d8:ae:0... | EVPN_Setup | 0 | 101 | N/A | 2 | 20 | 15 | 1 | 21426 | MSTP |
| 2 | 32768.0a:28:d8:... | 32768.0a:28:d8:... | EVPN_Setup | 0 | 102 | N/A | 2 | 20 | 15 | 1 | 21426 | MSTP |
| 3 | 32768.0a:28:d8:... | 32768.0a:28:d8:... | EVPN_Setup | 0 | 103 | N/A | 2 | 20 | 15 | 1 | 21426 | MSTP |
| 4 | 32768.0a:28:d8:... | 32768.0a:28:d8:... | EVPN_Setup | 0 | 104 | N/A | 2 | 20 | 15 | 1 | 21426 | MSTP |
| 5 | 0.0a:28:d8:b0:0... | 32768.0a:28:d8:... | EVPN_Setup | 0 | 105 | vni-0/1 | 2 | 20 | 15 | 1 | 21428 | MSTP |

## Supported Software Information

Releases 21.1 and later support all content described in this article, except:

- Release 21.1.1 supports EVPN over SD-WAN, MAC aging, MAC learning, MAC move, MAC limit, MSTP, paired TVI interfaces, and VLAN translation, and introduces different ways of determining the IRB state.
- Release 22.1.1 supports enet interfaces; MPLS services; ARP suppression; and, VLAN and VLAN-aware EVPN service types.
- Release 22.1.4 supports configuring DHCP snooping for virtual switches and bridge domains.

## Additional Information

Configure DHCP Snooping
Configure EVPN Multihoming for SD-WAN
Configure EVPN Multihoming for Hosts Using ZT-LAN
Configure EVPN VXLAN for SD-WAN
Configure EVPN VXLAN for ZT-LAN
Configure Layer 2 Services
Configure MOS Score Monitoring
Configure SD-WAN Policy
Configure SD-WAN Traffic Steering
Configure SLA Profiles for SD-WAN Traffic Steering