
Configure EVPN Multihoming for SD-WAN

 For supported software information, click [here](#).

You can configure Ethernet VPN (EVPN) multihoming on Versa Operating System™ (VOS™) devices to connect to a Layer 2 switch at a customer site with a branch device. EVPN multihoming helps improve network performance and increase the reliability of traffic flows among multihomed devices.

EVPN Multihoming Overview

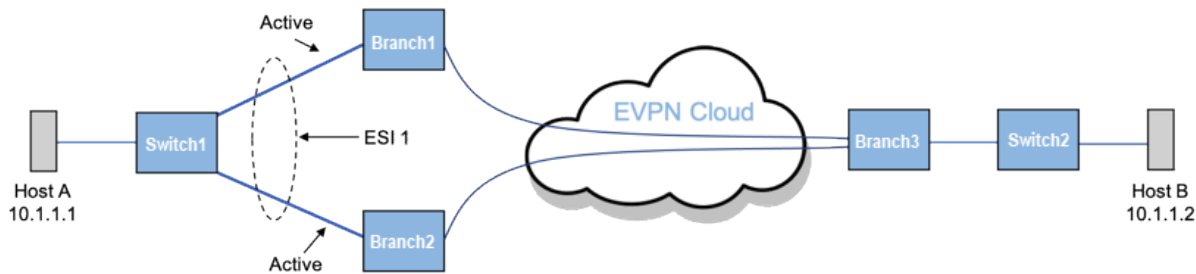
An EVPN carries Layer 2 Ethernet traffic as a virtual private network using wide-area network (WAN) protocols. An EVPN consists of a VOS device which is a Layer 2 switch at a customer site, that connects to a branch device. In EVPN multihoming, a switch connects to two or more branches using a set of Ethernet links. The set of Ethernet links is called an Ethernet segment (ES). Each shared Ethernet segment across the branches is identified by an Ethernet segment identifier (ESI), which is a 10-octet, non-zero value that is unique across the network. You configure the ESI for an interface in much the same way as you configure a native VLAN ID.

EVPN Multihoming Modes

VOS devices support two EVPN multihoming modes: all-active and single-active.

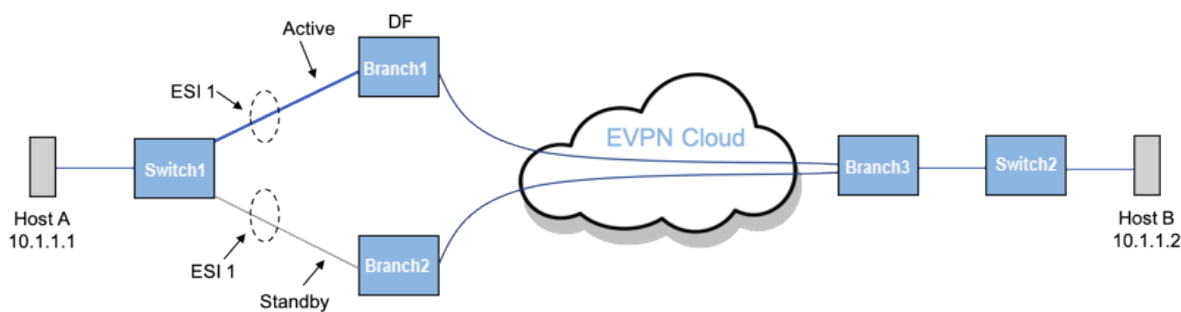
In all-active mode, all the branch devices to which the multihomed switch connects are in active mode, which means that they can all forward traffic. All-active mode provides active-active redundancy among the branch devices and allows load balancing of Layer 2 traffic across all the multihomed links to and from the switch.

The following figure illustrates EVPN all-active multihoming mode. Here, Switch1 is multihomed to Branch1 and Branch2. Both Branch1 and Branch2 have active links to Switch1 using ESI1, and both Branch1 and Branch2 can forward traffic.



In single-active mode, only one of the branch devices to which the multihomed switch connects is in active mode, which means that this is the only branch device that forwards traffic. The remaining branch devices are in standby mode. If a link or branch device on the Ethernet segment fails, the standby link or branch device becomes active and takes over forwarding traffic to and from the multihomed switch.

The following figure illustrates single-active mode. Here, Switch1 is multihomed to Branch1 and Branch2. Branch1 is the designated forwarder device, which is responsible for forwarding broadcast, unknown, and multicast (BUM) traffic to and from a switch, and Branch1 has an active link to Switch1 over ESI 1. Branch2 has a standby link to Switch1 over ESI 1. If the active link between Switch1 and Branch1 fails, the standby link between Switch1 and Branch2 becomes active.



Forwarding Actions

The branch device is responsible for forwarding broadcast, unknown, and multicast (BUM) traffic to and from a switch is called the designated forwarder (DF). A backup designated forwarder (BDF), also called a non-designated forwarder (non-DF) device, is available if the designated forwarder encounters a failure.

In an EVPN multihomed topology, the forwarding action depends on the multihoming mode, as follows:

- All-active mode
 - If the multihomed link on the branch device is in active state and the device is a designated forwarder on the link, the link accepts and forwards BUM traffic arriving from the EVPN core.
 - If the multihomed link on the branch device is in active state and the device is a backup designated forwarder on the link, the link forwards known unicast traffic from the EVPN core and drops BUM traffic from the EVPN core.
- Single-active mode

- If the multihomed link on the branch device is in active state, the link accepts and forwards BUM traffic arriving from the EVPN core.
- If the multihomed link on the branch device is in standby state, the link drops unicast and BUM traffic arriving on the link, and the link does not forward unicast or BUM traffic to that link coming from other links in the bridge domain.

The following table describes how unicast and BUM traffic are forwarded in all-active and single-active EVPN multihoming modes.

Traffic Type	All-Active Mode	Single-Active Mode
Known unicast		
<ul style="list-style-type: none"> Local to EVPN core traffic 	<ul style="list-style-type: none"> Load-balance traffic to all branch devices on the multihomed link. 	<ul style="list-style-type: none"> Only the designated forwarder branch device learns MAC addresses and forwards traffic.
<ul style="list-style-type: none"> EVPN core to local traffic 	<ul style="list-style-type: none"> Load-balance traffic from the EVPN core to all branch devices on the multihomed link. 	<ul style="list-style-type: none"> Remote branch device learns MAC addresses only from the designated forwarder. Remote branch device forwards all known unicast traffic to designated forwarder branch device.
BUM		
<ul style="list-style-type: none"> Local to EVPN core traffic 	<ul style="list-style-type: none"> Branch device forwards received BUM traffic to all remote branch devices over the EVPN core. 	<ul style="list-style-type: none"> Only the branch device that is the designated forwarder learns MAC addresses and forwards BUM traffic.
<ul style="list-style-type: none"> EVPN core to local traffic 	<ul style="list-style-type: none"> Only the branch device that is the designated forwarder forwards BUM traffic received from the EVPN core. 	<ul style="list-style-type: none"> Only the branch device that is the designated forwarder forwards BUM traffic received from EVPN core.

For BUM traffic, a BUM route has both regular and EVPN branch-based bridge domain interfaces. When forwarding traffic to a multihomed branch device, an extra ESI label is added to prevent transient loops in the network. For more information, see [Split-Horizon Filtering](#) section.

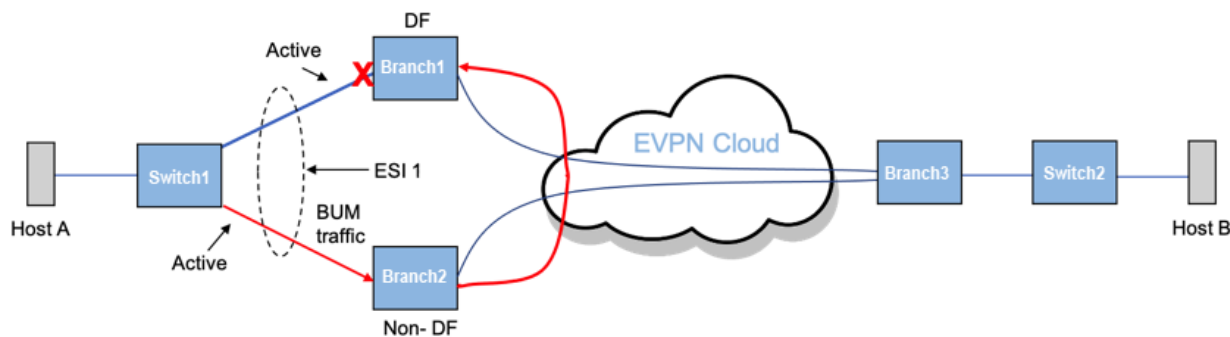
In order for the destination branch device to forward packets, it first performs an EVPN lookup to determine the bridge domain. Then, it performs a MAC lookup and uses the information in the MAC entry to forward packets.

Split-Horizon Filtering

EVPNs implement split-horizon filtering to prevent packets from looping.


In all-active mode, split-horizon filtering works as follows. If the switch sends a BUM packet to a branch device that is a non-designated forwarder, the branch device tags the packet with two labels, a split-horizon label (which is the branch device's ESI) and an EVPN BUM label. The branch device then forwards the BUM packet to the other branch devices in the EVPN instance, including the designated forwarder branch device for the Ethernet segment. Then, the designated forwarder branch device to which the switch is multihomed drops the packet and so does not forward it back to the originating switch.

In the following figure, the non-designated forwarder device, Branch2, receives BUM traffic from Switch1 and forwards it to the other branch device in the Ethernet segment, Branch1. Because Branch1 is the designated forwarder device, it drops the BUM traffic and does not forward it back to Switch1.



In single-active mode, split-horizon filtering prevents transient loops when the Ethernet segment fails or is recovering from a failure.

Configure EVPN Multihoming

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 the organization in the left navigation panel.
 - d. Select a post-staging template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking  > Interfaces in the left menu bar. The Interfaces dashboard displays, and the Ethernet tab is selected by default.
4. Click an interface name in the main pane. The Edit Ethernet Interface screen for the selected interface displays, and the Ethernet tab is selected by default.

You can also configure multihoming from the Aggregate Ethernet tab:

5. In the Multihoming group of fields, enter information for the following fields.

Field	Description
Active Mode	Select the active mode: <ul style="list-style-type: none"> ◦ All Active—Use active-active mode.

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Configure_EVPN...

Updated: Wed, 23 Oct 2024 08:25:02 GMT

Copyright © 2024, Versa Networks, Inc.

Field	Description
	<ul style="list-style-type: none"> Single Active—Use active-standby mode.
ESI	Enter the ESI hexadecimal list value, which is a 10-octet value separated by colons (:), for example, 00:10:00:00:00:00:00:00:01:00.

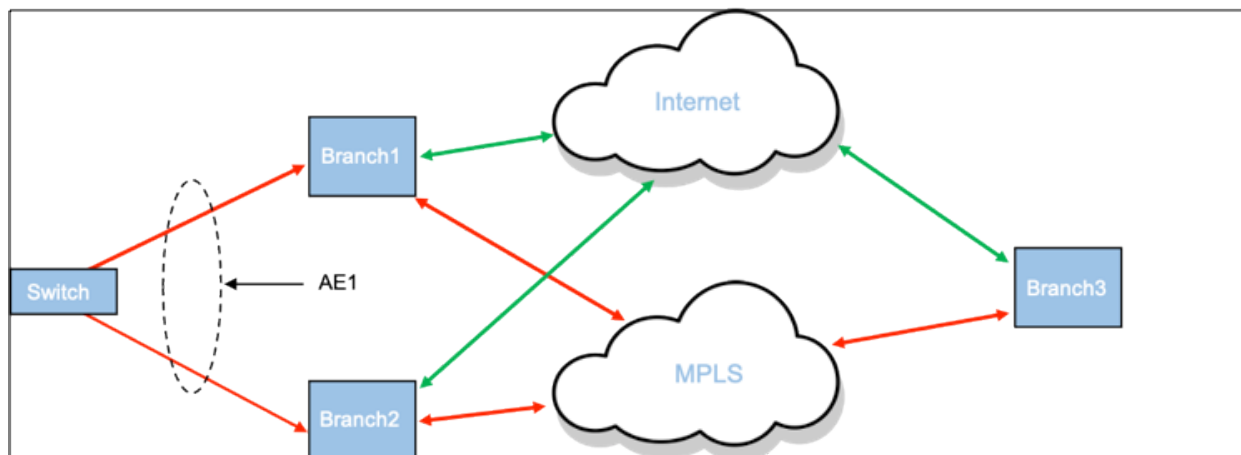
6. Click OK.

Configure Link Aggregation for All-Active Multihoming

In all-active mode, when a multihomed switch is a host, it connects to multihomed branch devices over individual links. However, when it is a switch, it must connect to multihomed branch devices using static link aggregation (LAG) and the Link Aggregation Control Protocol (LACP).

Note that multihomed switches in single-active mode cannot use LAG to connect to multihomed branch devices. However, links connecting to same branch device can use LAG.


The following figure shows a switch that connects to two branch devices, Branch1 and Branch2, using an aggregated Ethernet link, AE1. The two branch devices forward traffic from the switch to Branch3 over the internet and an MPLS network.

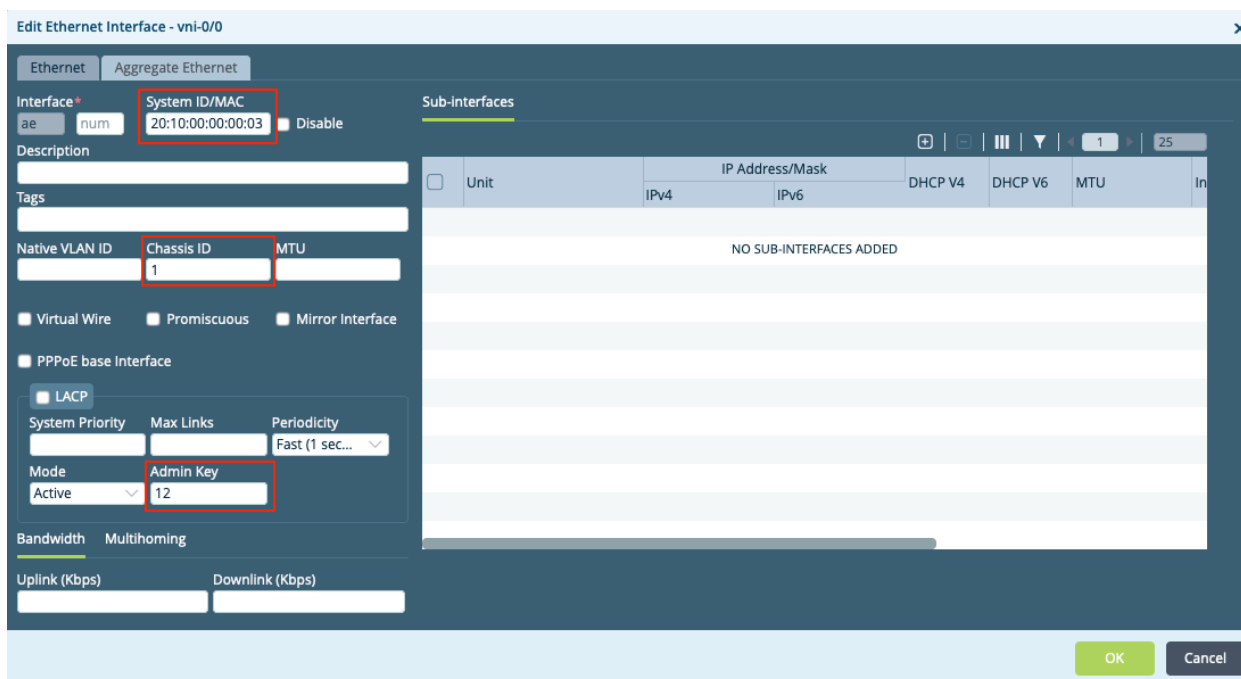


To enable LACP on a switch, you configure the same LACP system identifier and administrative key on all the branch devices that are bundled in the aggregated link. You also configure a unique chassis ID on each branch device.

Note that you cannot configure xSTP on a link that has an ESI ID, or vice versa.

To configure link aggregation for all-active-mode multihoming:

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  > Interfaces in the left menu bar. The Interfaces dashboard displays, and the Ethernet tab selected by default.
4. Click the desired interface in the main pane. The Edit Ethernet Interface screen displays.
5. Select the Aggregate Ethernet tab, and enter information for the following fields.



Field	Description
System ID/MAC	Enter a user-defined system identifier for the device, which must be exactly 6 octets (for example, 20:10:00:00:00:03).
Chassis ID	Enter a chassis ID number. For multichassis LAG, a port from each VOS device should be uniquely identifiable. It is possible for each VOS device to assign the same port ID to its aggregate member interface. To avoid this issue, configure a unique chassis ID on each VOS device. The chassis ID is

Field	Description
	<p>combined with the locally assigned port ID to determine a unique Actor_Port number that is sent in the LACPDU frame.</p> <p><i>Range:</i> 1 through 7</p> <p><i>Default:</i> None</p>
Admin Key	<p>Enter an administrative key number. The administrative key, in conjunction with the system ID, enables ports from two separate VOS devices to behave as if they are part of the same aggregate interface. For multichassis LAG, configure the same administrative key and system ID on the two VOS devices. The administrative key corresponds to the Actor_Key value encoded in the LACPDU frame.</p> <p><i>Range:</i> 1 through 65535</p> <p><i>Default:</i> None</p>

6. Click OK.

Monitor Links in the EVPN Core

In all-active mode and in single-active mode if the branch device is the active device, if the interface on the LAN access side of the branch device is operationally up, the switch sends traffic to the branch device. However, when the transport network at the branch device is down, traffic on the LAN access side of the branch device is blackholed. To avoid the blackholing of traffic, you can configure a monitor group and apply it to the access side of the LAN interface configured for the Ethernet segment. Using monitor groups, if all the uplinks on the branch device are down, the branch device's interface toward the LAN access side is brought down. With this configuration, traffic is not blocked if the EVPN core side of network is down and a switch sends traffic toward other branch devices.



Depending on your scenario, you can configure the monitor group to contain different monitors, as follows:

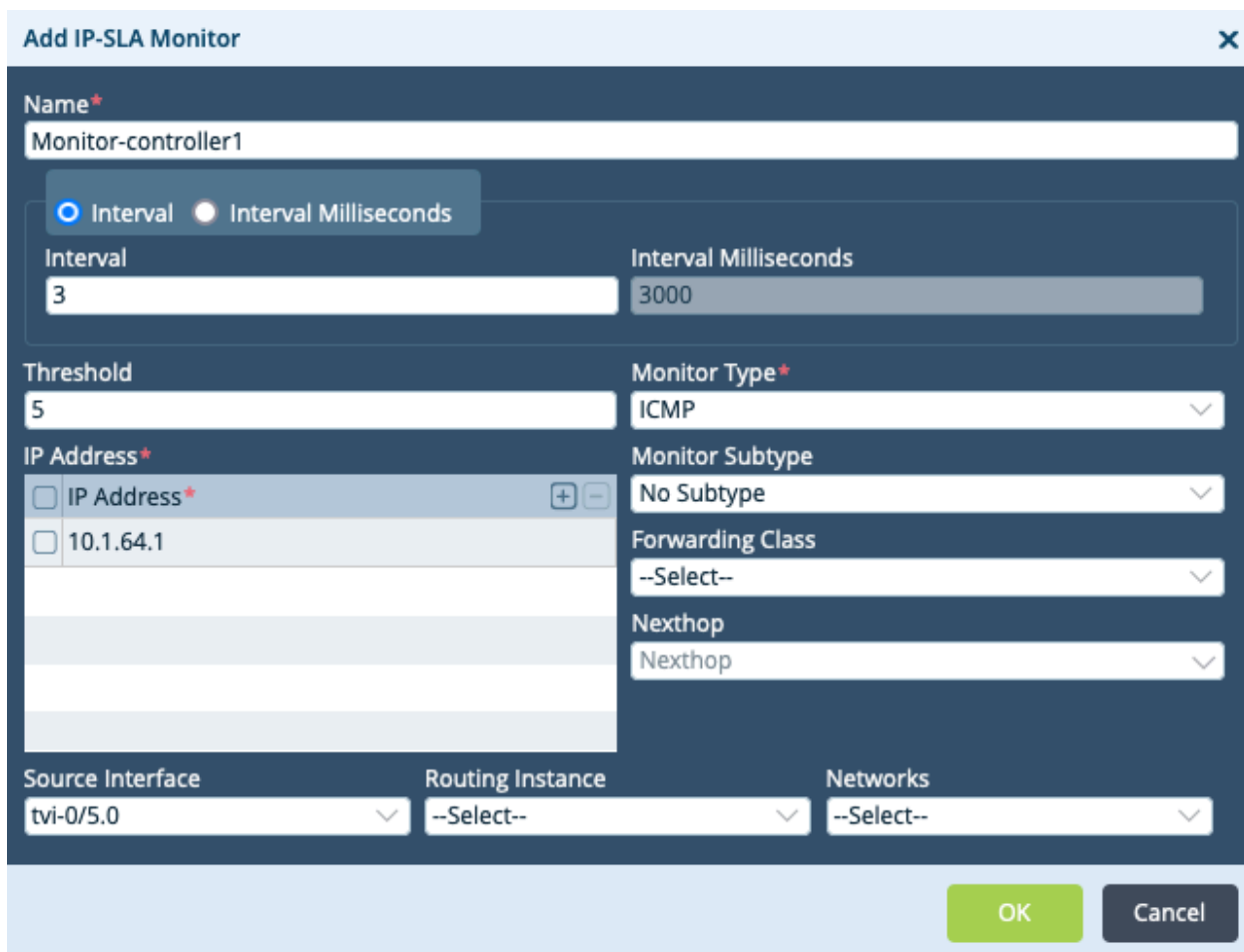
- Monitor group consists of monitors to each Controller node. One issue with monitoring for BGP Controllers is that if the VOS switch loses connectivity to the Controller nodes, the LAN-side interface goes down even though the device is still able to connect to other devices. If only the network towards the Controller node is down, all the multihomed devices could bring down the LAN-side network.
- Monitor group consists of monitors to each Controller node and to all multihomed peers. This option improves the probability of determining the black out. However, if the Controller nodes and all the multihomed peers encounter a

split-brain scenario, the LAN interface goes down.

- Monitor group consists of monitors to each Controller node, to each multihomed peer, and to some of the VOS devices. Of the first three options, this one has the best probability of detecting a transport network failure.
- Monitor group consists of monitors to each Controller node, to each multihomed peer, and to all VOS devices participating in the bridge domain. This option works in all scenarios, but it requires that each VOS device perform a large amount of monitoring.

To configure monitors:

1. In Director view, select the Administration tab in the top menu bar.
2. Select Appliances in the left menu bar.
3. Select a device in the main pane.
4. Select the Configuration tab in the top menu bar.
5. Select Network  > IP SLA > Monitor in the left menu bar.
6. Click the  Add icon to create a monitor for the Controller. The Add IP SLA Monitor popup window displays. Enter information for the following fields.





The image shows a screenshot of the 'Add IP-SLA Monitor' configuration window. The window has a title bar with 'Add IP-SLA Monitor' and a close button. The main area contains several fields and controls:

- Name***: A text field containing 'Monitor-controller1'.
- Interval Selection**: Two radio buttons, 'Interval' (selected) and 'Interval Milliseconds'.
- Interval**: A text field containing '3'.
- Interval Milliseconds**: A text field containing '3000'.
- Threshold**: A text field containing '5'.
- Monitor Type***: A dropdown menu with 'ICMP' selected.
- Monitor Subtype**: A dropdown menu with 'No Subtype' selected.
- Forwarding Class**: A dropdown menu with '--Select--' selected.
- Nexthop**: A dropdown menu with 'Nexthop' selected.
- IP Address***: A list of IP addresses with checkboxes. The first row has 'IP Address*' and a '+' button. The second row has '10.1.64.1'.
- Source Interface**: A dropdown menu with 'tvi-0/5.0' selected.
- Routing Instance**: A dropdown menu with '--Select--' selected.
- Networks**: A dropdown menu with '--Select--' selected.
- Buttons**: 'OK' and 'Cancel' buttons at the bottom right.

Field	Description
Name	Enter a name for the IP SLA monitor object. This example uses the name Monitor-controller1.
Interval	Click, and enter the frequency, in seconds, at which to send ICMP packets to the IP address. <i>Range:</i> 1 through 60 seconds <i>Default:</i> 3 seconds
Threshold	Enter the maximum number of ICMP packets to send to the IP address. If the IP address does not respond after this number of packets, the monitor object, and hence the IP address, is marked as down. <i>Range:</i> 1 through 60 <i>Default:</i> 5
Monitor Type	Select ICMP for the type of packets to send to the IP address.
Monitor Subtype	Select the No subtype option, which is the default setting.
Source Interface	Select the source interface on which to send the probe packets. This interface determines the routing instance through which to send the probe packets. This routing instance is the target routing instance for the probe packets.
IP Address	Enter the IP address of the Controller to monitor.

7. Click OK.

To create a monitor group and add the monitor object:

1. Continuing from the previous procedure, select Network  > IP SLA > Group in the left menu bar.
2. Click the  Add icon to create a monitor group. The Add IP SLA Monitor Group popup window displays. Enter information for the following fields.

Add IP-SLA Monitor Group

Name*

Monitor-Controllers-group

Operation

or

List of Monitors

Available
Add All

Search

Monitor-controller1
>

Monitor-controller2
>

Selected
Remove All

Search


OK

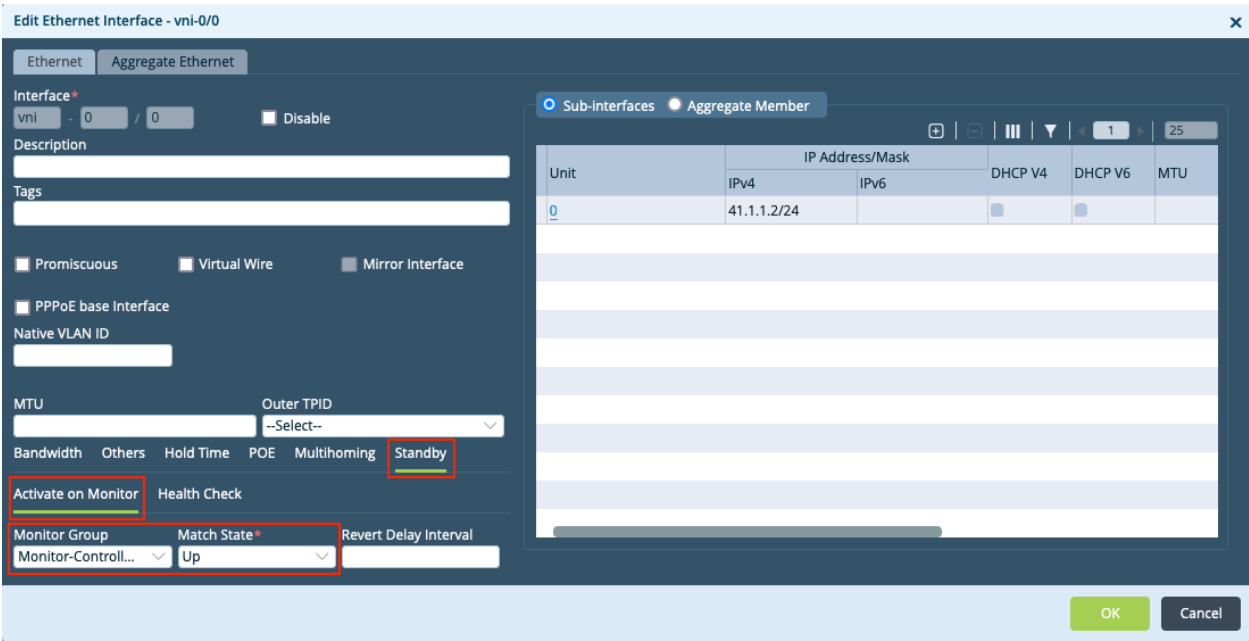
Cancel

Field	Description
Name	Enter a name for the IP SLA monitor group. This example uses the name Monitor-Controllers-group.
Operation	Select the or boolean operation to perform on the monitors
List of Monitors (Table)	
<ul style="list-style-type: none"> Available 	Displays the list of available monitors for this appliance. Select and click on the monitor that you want to add to the group. This example uses the names Monitor-controller1 and Monitor-controller2.
<ul style="list-style-type: none"> Selected 	Displays the monitor that you added to the group.

3. Click OK.

Next, you associate the monitor group with a LAN interface as the standby option, with the match state configured as "Up". To configure this use case scenario:

1. Continuing from the previous procedure, select Network  > Interfaces in the left menu bar.
2. Select the LAN interface (vni-0/0) in the main pane. The Edit Ethernet Interface popup window displays.
3. Select the Standby tab and the Activate on Monitor tab, and enter information for the following fields.



Unit	IP Address/Mask	DHCP V4	DHCP V6	MTU
0	41.1.1.2/24	<input type="checkbox"/>	<input type="checkbox"/>	

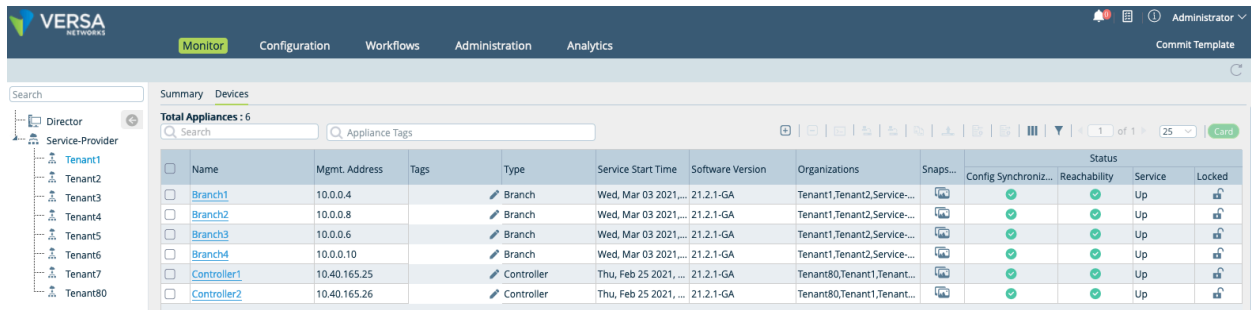
Field	Description
Monitor Group	Select the monitor group, for example, Monitor-Controllers-group.
Match State	Select the Up option.

4. Click OK.

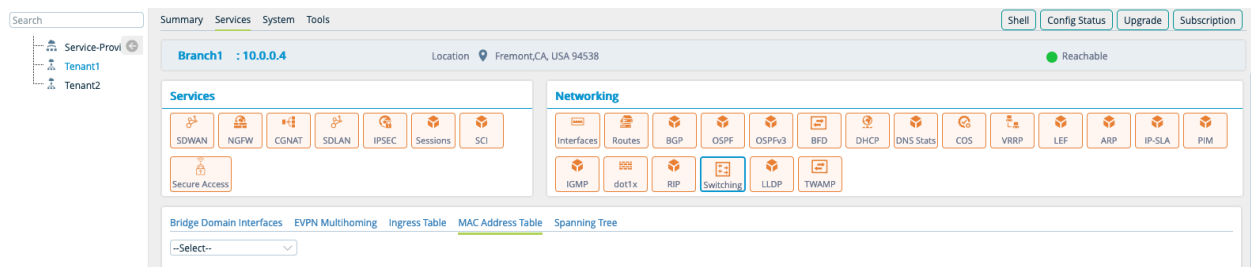
Verify the EVPN Multihoming Configuration

To verify the EVPN multihoming configuration:

1. In Director view, select the Monitor tab in the top menu bar.
2. Select the organization in the left navigation panel.
3. Select the Devices tab.



4. Select a device in the main pane.
5. Select the Services tab.
6. In the Networking pane, select Switching.



7. Select the MAC Address Table in the horizontal menu bar.
8. Select a switch name from the first drop-down list.
9. Select a VLAN from the second drop-down list.
10. Select the type of output to display from the third drop-down list, either Brief (default) or Statistics. The screen displays bridge MAC table information.

Bridge Domain Interfaces

EVPN Multihoming

Ingress Table

MAC Address Table

Spanning Tree

Tenant1-default-switch

vlan-1001

Brief

Search

|||

▼

◀ 1 ▶

25

MAC Type Legend:

C: Control

S: Static

D: Dynamic

R: Router

V: Vrrp

B: Sink

M: Multi-Home

Bridge Domain Interface	MAC Address	Vlan ID	MAC Type	Remote Branch / VTEP
dtvl-0/204	06:28:a5:0c:01:01	1001	SC	Branch2
irb1.1001	00:00:5e:00:01:01	1001	V	N/A
irb1.1001	06:28:a5:0b:01:01	1001	R	N/A
vni-0/6.1	52:0a:28:a5:1f:02	1001	D	N/A

11. Select the EVPN Multihoming tab. The screen displays the EVPN monitoring data for the selected virtual switch and VLAN (Tenant1-default-switch and vlan-1001 in the screen capture below) for active-active mode. Note that EVPN monitoring data is not available for active-standby mode.

Bridge Domain Interfaces EVPN Multihoming Ingress Table MAC Address Table Spanning Tree									
Tenant1-default-switch	vlan-1001								
Bridge Logical Interface	Interface Vlan	Total Neighbors	Ethernet Segment ID	Ethernet Segment Neighbor	Mode	Remote Branch	Label / VNID	Gateway IP	DTVI Index
es-0/0.2	1001	1	00:00:00:00:20:00:00:00:11	1	active	Branch2	26848	10.0.0.8	1218
es-0/0.3	1001	1	00:00:00:00:20:00:00:00:12	1	active	Branch2	26320	10.0.0.8	1218
es-0/0.5	1001	2	00:00:00:00:20:00:00:00:31	2	active	Branch4	26310	10.0.0.10	1220

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Configure_EVPN...

Updated: Wed, 23 Oct 2024 08:25:02 GMT

Copyright © 2024, Versa Networks, Inc.

Supported Software Information

Releases 21.2.1 and later support all content in this article.

Additional Information

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

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

[Configure EVPN VXLAN for ZT-LAN](#)

[Configure Interfaces](#)

[Configure Layer 2 Forwarding](#)