SD-WAN Gateway Use Cases

For supported software information, click here.

There are three main use cases for VOS edge devices that act as SD-WAN gateways:

- Connect to sites on an MPS Layer 2 VPN network
- Connect to sites over disjointed underlay networks
- Act as a gateway for internet-bound traffic

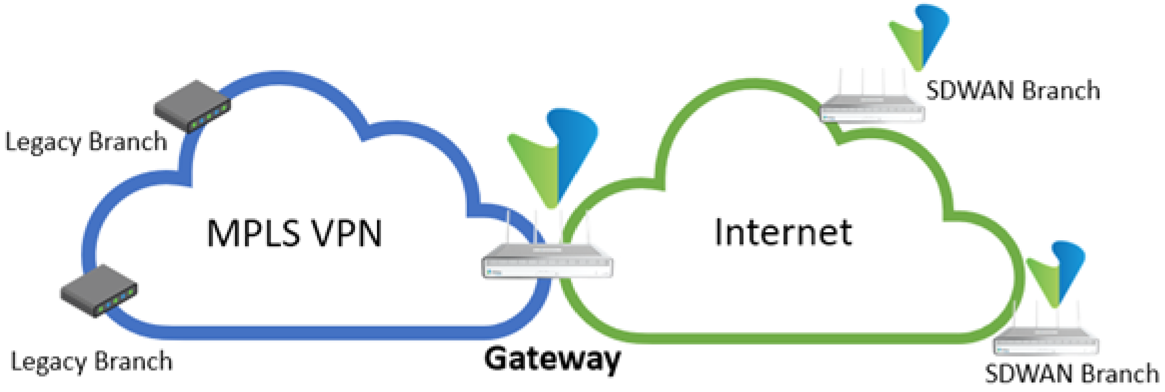
This chapter discusses each of these use cases.

Connect to Sites on an MPLS Layer 3 VPN Network

An SD-WAN gateway allows sites connected to the SD-WAN VPN network to communicate with sites that are connected to a legacy MPLS VPN network. To enable this communication, you configure a VOS edge device as a gateway. This gateway facilitates the routing of information between the MPLS underlay network and the SD-WAN VPN network. The exchange of routes is typically done using a dynamic routing protocol such as BGP.

When you are migrating to SD-WAN, you can set up a gateway temporarily so that sites in the MPLS Layer 3 VPN network can continue to connect to sites that have already migrated to SD-WAN. After you have migrated all the sites to they SD-WAN-based VPN, the gateway is no longer required. You can also use a permanent gateway when the MPLS network has sites or services that must be accessed by SD-WAN–enabled sites, for example, if the SD-WAN–enabled sites need to access Azure Express Route connection in the MPLS network.

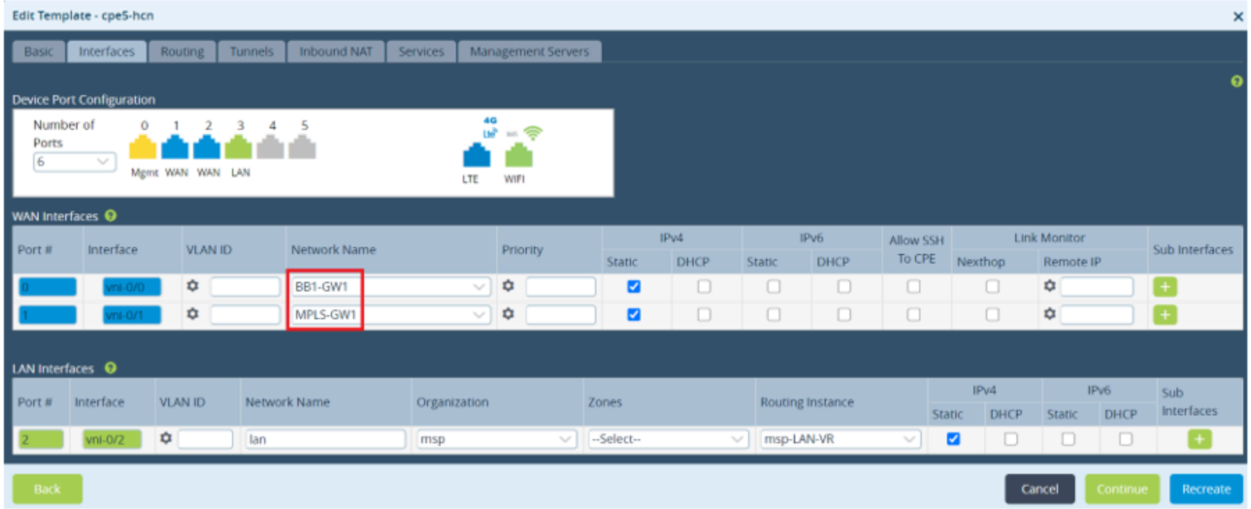
The following figure illustrates an SD-WAN gateway.



The SD-WAN gateway uses the same VOS edge device software that is used in a regular SD-WAN branch, which means that a regular branch can also serve as a gateway. SD-WAN gateways can be multitenant, and in a service provider environment, it is common to find such multitenant gateways that serve multiple customer networks. An SD-WAN gateway can also be used for non-SD-WAN interconnects, in which you can replace the MPLS Layer 3 VPN with any IP network.

The following are best practices for SD-WAN gateways:

- For device-level redundancy, use HA-enabled sites as gateway.
- For redundancy, use multiple gateways across different availability zones or geographic regions.
- Keep traffic symmetric. For routes that the gateway exchanges with the provider, modify the BGP path attributes to ensure that bidirectional traffic uses the same gateway device. Asymmetric routing may cause issues in the SD-WAN when you use SD-WAN traffic-steering policies.
- If you have multiple gateway sites that establish peering to the same MPLS provider, use the same BGP AS number for the SD-WAN and the provider side of the BGP session. (Note that the default SD-WAN IBGP AS number is 64512.) The BGP AS path check ensures that routing loops are not formed when a route learned from one gateway is inadvertently advertised back to another gateway. The BGP AS path check also takes care of routing loops if the same route learned from an MPLS provider is advertised back to any gateway site. Similarly, an SD-WAN route advertised from one gateway to the provider must not be advertised back by the provider at another gateway site.
- It is recommended that you use BGP communities to color the routes when they are advertised and received at each BGP gateway. An example is to color routes based on region. For example, you can use different communities to identify routes from EMEA and North America. You can configure BGP filters in the EBGP peering session with the MPLS provider to accept or advertise only routes that are required. You can craft these filtering policies based on BGP community values.
- An existing branch, data center, or hub site can also double as the gateway. Make sure that you dimension the system to handle the expected amount of traffic.
- On gateways and hubs, it is recommended that you always use unique network names for the WAN links, as illustrated in the following screenshot. Also, the WAN link names must be unique across the entire SD-WAN network as shown in Figure 2 in the Add/Edit Template > Interfaces tab. For more information, see Create Device Templates.



Device Port Configuration

Number of Ports: 6

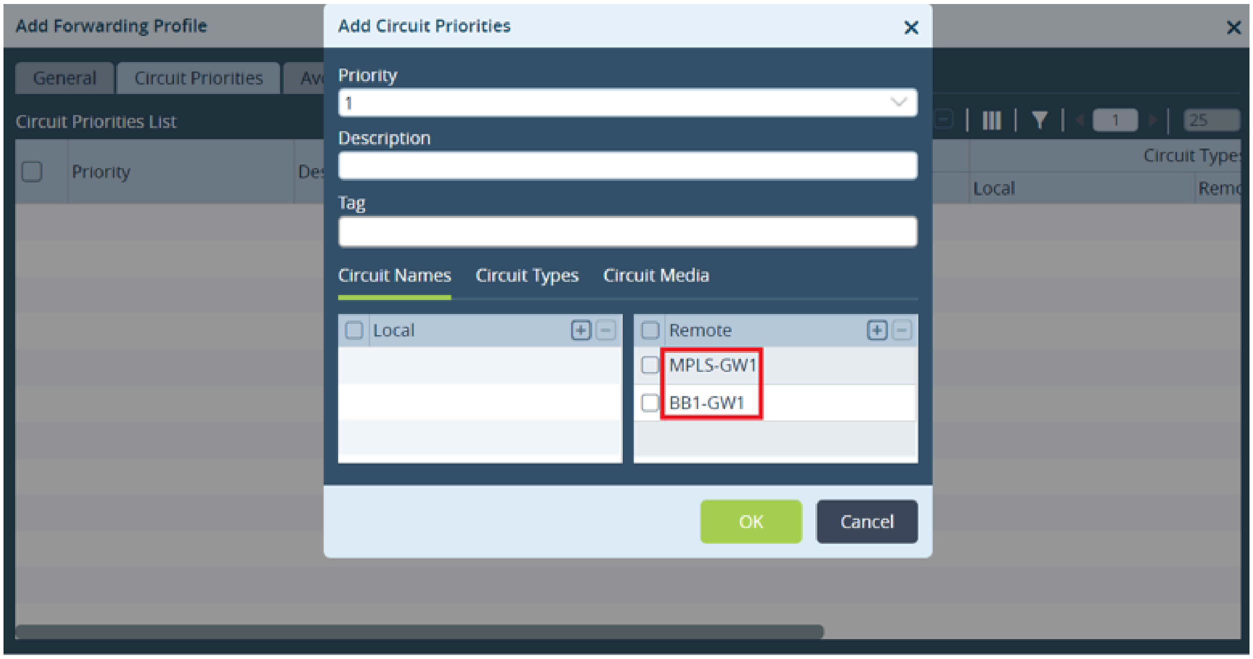
WAN Interfaces

Port #	Interface	VLAN ID	Network Name	Priority	IPv4		IPv6		Allow SSH To CPE	Link Monitor		Sub Interfaces
					Static	DHCP	Static	DHCP		Nexthop	Remote IP	
0	vni-0/0		BB1-GW1		☑	☐	☐	☐	☐	☐		+
1	vni-0/1		MPLS-GW1		☑	☐	☐	☐	☐	☐		+

LAN Interfaces

Port #	Interface	VLAN ID	Network Name	Organization	Zones	Routing Instance	IPv4		IPv6		Sub Interfaces
							Static	DHCP	Static	DHCP	
2	vni-0/2		lan	msp	--Select--	msp-LAN-VR	☑	☐	☐	☐	+

This naming strategy allows remote branches to use the remote circuit option to influence the traffic path in the SD-WAN policy. This behavior is not specific to disjoined underlay networks, but rather it is a general recommendation for gateways and hubs. You can make this selection in the SD-WAN forwarding profile on the remote branch. For more information, see Configure SD-WAN Traffic-Steering Forwarding Profiles.



Priority: 1

Description:

Tag:

☐ Local	☐ Remote
	☐ MPLS-GW1
	☐ BB1-GW1

Interconnect Legacy Networks with SD-WAN Gateways

This sections describes two methods for interconnecting legacy networks with SD-WAN gateways. They differ in how the routes are exchanged with the MPLS provider. The two methods are:

- Use BGP to exchange routes with the MPLS provider on the MPLS WAN interface.

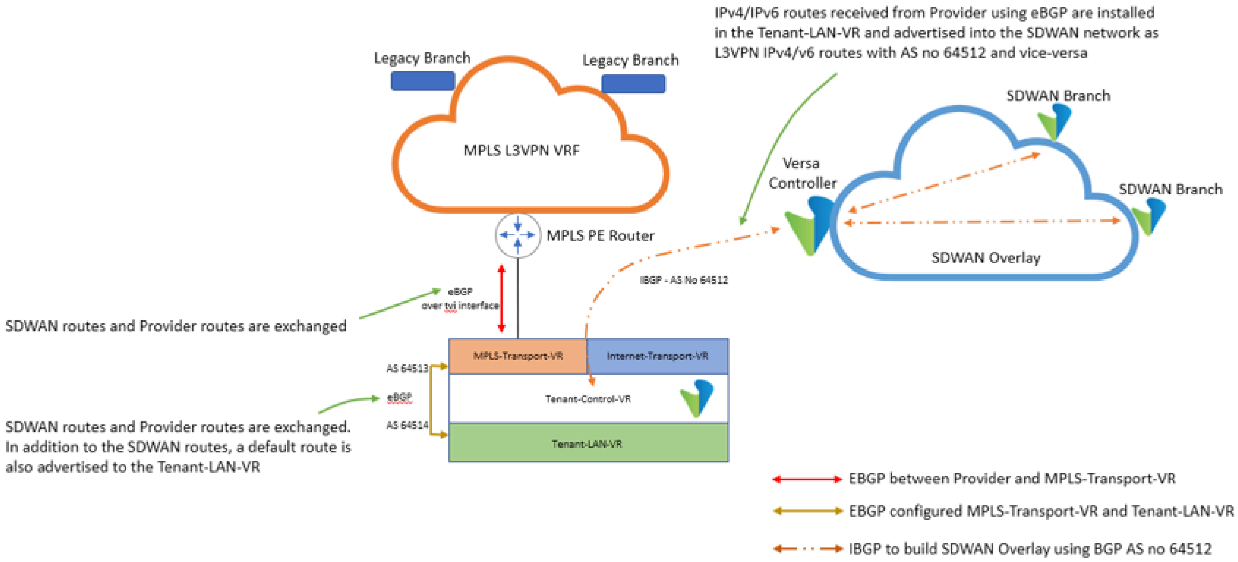
- Establish a BGP session with the MPLS provider on a LAN interface.

Use BGP to Exchange Routes with the MPLS Provider on the MPLS WAN Interface

Using BGP to exchange routes with the MPLS provider on the MPLS WAN interface is the most common method for DIY enterprise SD-WAN deployments. For this method, you configure a BGP peering session on the MPLS-Transport-VR on the gateway to exchange routes from the MPLS Provider to the SD-WAN network. You can use Director Workflows to automate this configuration.

The advantage of this approach is that you need only a single IP interface to connect to the MPLS provider, and this is the interface over which you establish the BGP peering session. Having a singe IP interface is commonly seen in enterprise network designs in which a single MPLS provider offers MPLS VPN underlay services. This MPLS VPN network has connections to the legacy branches and provides MPLS underlay connectivity to SD-WAN branches. Whether an SD-WAN branch has an MPLS or internet underlay, the SD-WAN VPN network uses only the WAN IP addresses to establish connectivity with other SD-WAN branches and the gateway. The SD-WAN branch routes are exchanged over an encrypted overlay.

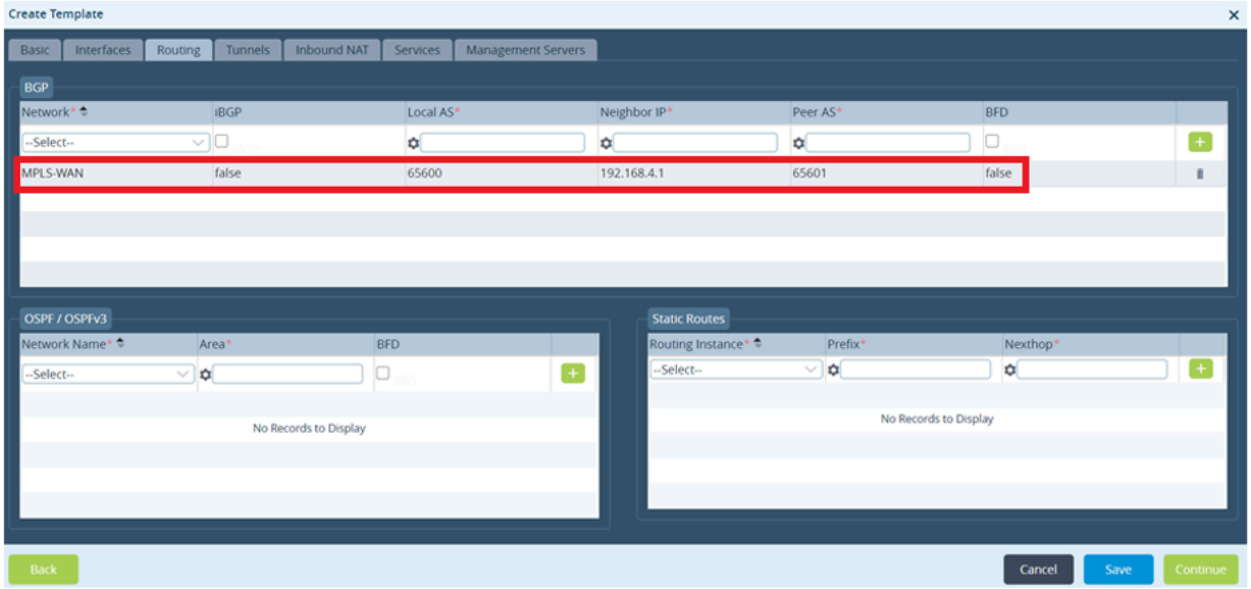
The following figure shows how the gateway is configured internally. A virtual TVI interface pair is created (using a Director Workflow) in the MPLS-Transport-VR and Tenant-LAN-VR. Over this virtual interface, an EBGP neighbor session is established with AS numbers 64513 and 64514. When the route is advertised to the SD-WAN network, the default BGP AS number of the SD-WAN overlay, 64512, is appended to the BGP AS path list. If the SD-WAN route advertised by one gateway is inadvertently learned by another gateway through the MPLS underlay provider, the route is automatically blocked as a result of the AS path check.


IPv4/IPv6 routes received from Provider using eBGP are installed in the Tenant-LAN-VR and advertised into the SDWAN network as L3VPN IPv4/v6 routes with AS no 64512 and vice-versa
Legacy Branch
Legacy Branch
MPLS L3VPN VRF
MPLS PE Router
Versa Controller
SDWAN Branch
SDWAN Branch
SDWAN Overlay
IBGP - AS No 64512
eBGP over tvi interface
SDWAN routes and Provider routes are exchanged
MPLS-Transport-VR
Internet-Transport-VR
AS 64513
eBGP
AS 64514
Tenant-Control-VR
Tenant-LAN-VR
SDWAN routes and Provider routes are exchanged. In addition to the SDWAN routes, a default route is also advertised to the Tenant-LAN-VR
EBGP between Provider and MPLS-Transport-VR
EBGP configured MPLS-Transport-VR and Tenant-LAN-VR
IBGP to build SDWAN Overlay using BGP AS no 64512

To configure an EBGP session on the MPLS WAN link to the MPLS PE router:

1. In Director view, select the Workflows tab in the top menu bar.
2. Select Template > Templates in the left menu bar.

3. Click the ⊞ Add icon, or select an existing template. The Create/Edit Template window displays. For more information, see Create Device Templates.



BGP

Network*	iBGP	Local AS*	Neighbor IP*	Peer AS*	BFD
--Select--	□				□
MPLS-WAN	false	65600	192.168.4.1	65601	false

OSPF / OSPFv3

Network Name*	Area*	BFD
--Select--		□

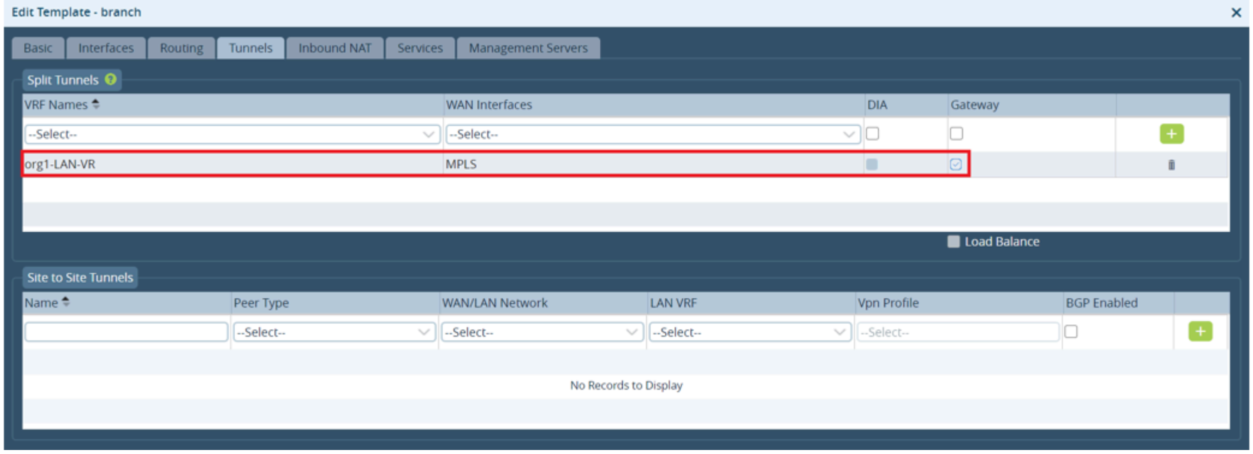
No Records to Display

Static Routes

Routing Instance*	Prefix*	Nexthop*
--Select--		

No Records to Display

4. Select the Routing tab, and configure the MPLS WAN link.
5. Select the Tunnels tab, and create the BGP session between the MPLS-Transport-VRE and Tenant-LAN-VR over a virtual interface pair (TVI interface) as shown below.



Split Tunnels

VRF Names	WAN Interfaces	DIA	Gateway
--Select--	--Select--	□	□
org1-LAN-VR	MPLS	□	☑

□ Load Balance

Site to Site Tunnels

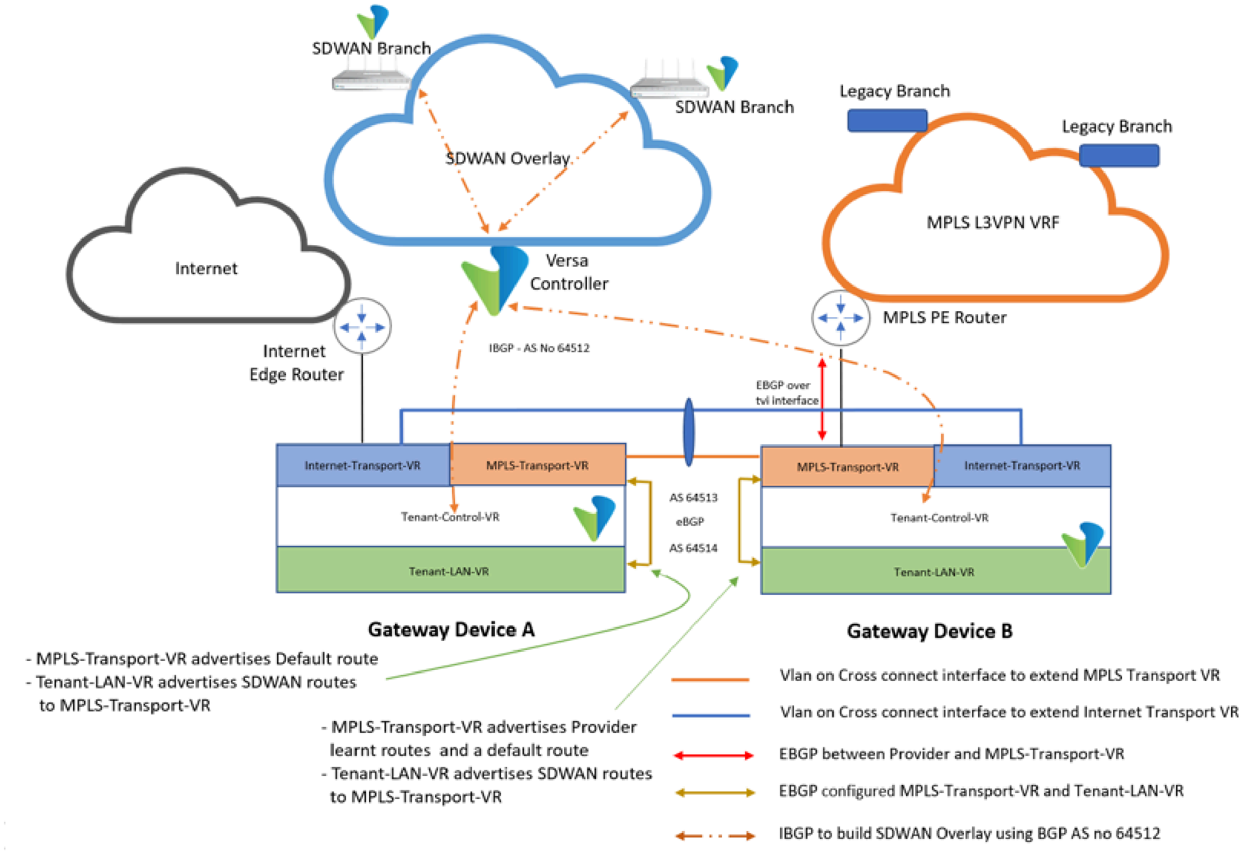
Name	Peer Type	WAN/LAN Network	LAN VRF	Vpn Profile	BGP Enabled
	--Select--	--Select--	--Select--	--Select--	□

No Records to Display

6. Click OK.

High Availability

The following figure illustrates how to achieve high availability (HA) when you use BGP to exchange routes with the MPLS provider on the MPLS WAN interface.


SDWAN Branch
SDWAN Branch
SDWAN Overlay
Legacy Branch
Legacy Branch
MPLS L3VPN VRF
Internet
Versa
Controller
MPLS PE Router
Internet
Edge Router
IBGP - AS No 64512
EBGP over
tvi interface
Internet-Transport-VR
MPLS-Transport-VR
Tenant-Control-VR
Tenant-LAN-VR
MPLS-Transport-VR
Internet-Transport-VR
Tenant-Control-VR
Tenant-LAN-VR
AS 64513
eBGP
AS 64514
Gateway Device A
Gateway Device B
- MPLS-Transport-VR advertises Default route
- Tenant-LAN-VR advertises SDWAN routes
to MPLS-Transport-VR
- MPLS-Transport-VR advertises Provider
learnt routes and a default route
- Tenant-LAN-VR advertises SDWAN routes
to MPLS-Transport-VR
Vlan on Cross connect interface to extend MPLS Transport VR
Vlan on Cross connect interface to extend Internet Transport VR
EBGP between Provider and MPLS-Transport-VR
EBGP configured MPLS-Transport-VR and Tenant-LAN-VR
IBGP to build SDWAN Overlay using BGP AS no 64512

When you configure the branch with active-active (HA) and with the gateway option selected, a TVI interface is created between the MPLS-Transport-VR and the Tenant-LAN-VR on both devices. Over this TVI interface, an EBGP peering session is established between the ASs 65413 and 65414. A cross-connect cable between the two devices extends the MPLS-Transport-VR to Device A and extends the Internet-Transport-VR to Device B.

For Device B, the figure shows that where the MPLS link terminates, there is an EBGP session with the MPLS provider over the MPLS WAN link. Over this EBGP session, routes are exchanged between the SD-WAN network and the legacy MPLS Layer 3 VPN VRF network. In addition, the MPLS-Transport-VR advertises a default route to the Tenant-LAN-VR. When routes from the MPLS provider are installed in the Tenant-LAN-VR, they are advertised to the SD-WAN network.

Based on the figure above, the following are HA design recommendations:

- On Device A, the EBGP session between the MPLS-Transport-VR and the Tenant-LAN-VR advertises only a default route to the Tenant-LAN-VR. The SD-WAN routes from the Tenant-LAN-VR are advertised into the MPLS-Transport-VR. The MPLS-Transport-VR has a static default route pointing to the MPLS-Transport-VR on Device B using the cross-connect interface. Device A learns the routes received from the MPLS provider on Device B using the SD-WAN multiprotocol IBGP session, specifically through the Tenant-Control-VR using a route reflector through the Controller node. The Tenant-LAN-VR on Device A does not receive the MPLS provider routes over the EBGP session from the MPLS-Transport-VR. As a result, Device B is always the primary path for all traffic to and from the MPLS provider. On both Devices A and B, the EBGP session between the MPLS-Transport-VR and the Tenant-LAN-VR advertises the SD-WAN routes to the MPLS-Transport-VR, and it advertises a default route to the Tenant-LAN-VR. If you do not need or want to advertise the default route, you can configure the redistribution policy for the MPLS-Transport-VR on both devices not to advertise the default route. In the example in the Best Practices policy, you configure this in the redistribution policy named ST-Policy.

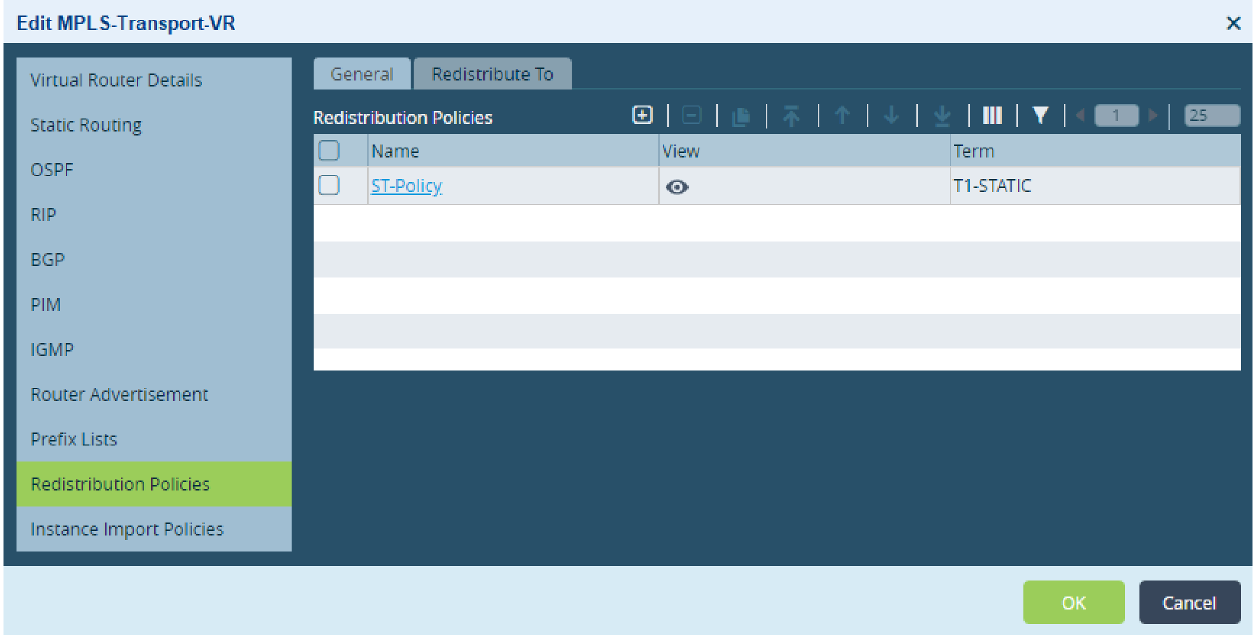
- It is recommended that you run a routing protocol, such as BGP or OSPF, on the LAN to avoid any issues with asymmetric routing. However, if the LAN router connected to Device B fails, the LAN network is left relying only on the default route. In addition to configuring a default route, you can configure Device A to advertise the specific routes learned from the MPLS provider. To do this, you configure IBGP can be configured between Device A and Device B over the MPLS cross-connect link. For more information see the configuration example in the section Establish a BGP Session with the MPLS Provider on a LAN Interface, below.
- If you use VRRP on the LAN for redundancy, the active device in HA must terminate the MPLS transport link to maintain symmetric traffic.
- If the device is a dedicated gateway with only one internet and MPLS link, configuring the device as HA in Director Workflows is not useful, because if one of the WAN links or devices fail, the gateway becomes non-functional. However, if the device is not a dedicated gateway, that is, if it also functions as a regular site, hub, or data center branch, it makes sense to configure HA using Director Workflows, because the device is usable even if one of the WAN link or devices fails. If the device is a dedicated gateway and if you can replicate the WAN links, it is recommended that, for redundancy, you have twice the number of single gateway devices.
- Because Device A in the figure above does not receive routes from the MPLS provider, it relies on a default route that is advertised into the SD-WAN and LAN networks. In some scenarios, it may be helpful for Device A to also have a copy of the MPLS provider routes so that it does not have to rely on the default route. To do this, you can configure iBGP peering between the MPLS-Transport-VR on both devices over the MPLS cross-connect interface.

Best Practices

When you use BGP to exchange routes with the MPLS provider on the MPLS WAN interface, a default route is created in the MPLS-Transport-VR that points to the Provider MPLS PE router as the next hop. This default route is advertised to the SD-WAN network over the EBGP session between the MPLS-Transport-VR and Tenant-LAN-VR. If you do not want this default route to be advertised to the SD-WAN network, use a redistribution policy to delete it. For example, to delete the term T1-STATIC from the Redistribution Policy ST-Policy in the MPLS-Transport-VR:

1. In the Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Devices > Devices in the horizontal menu bar.
   c. Select an organization in the left menu bar.
   d. Select a branch or controller in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.

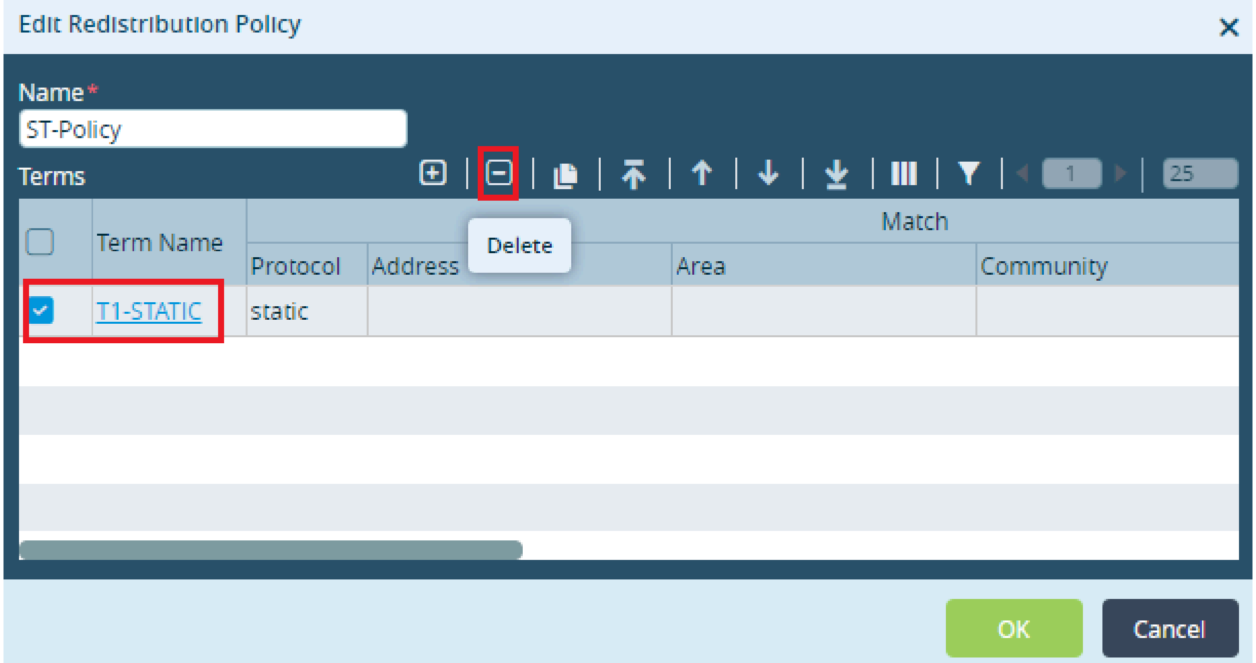
3. Select Networking > Virtual Routers in the left menu bar
4. Select a virtual router instance, here, MPLS-Transport-VR.
5. In the Edit VR popup window, select the Redistribution Policies tab.



Redistribution Policies

□	Name	View	Term
□	ST-Policy	👁	T1-STATIC

6. Click a term name, here, ST-Policy. The Edit Redistribution Policy window displays.



Name*
ST-Policy

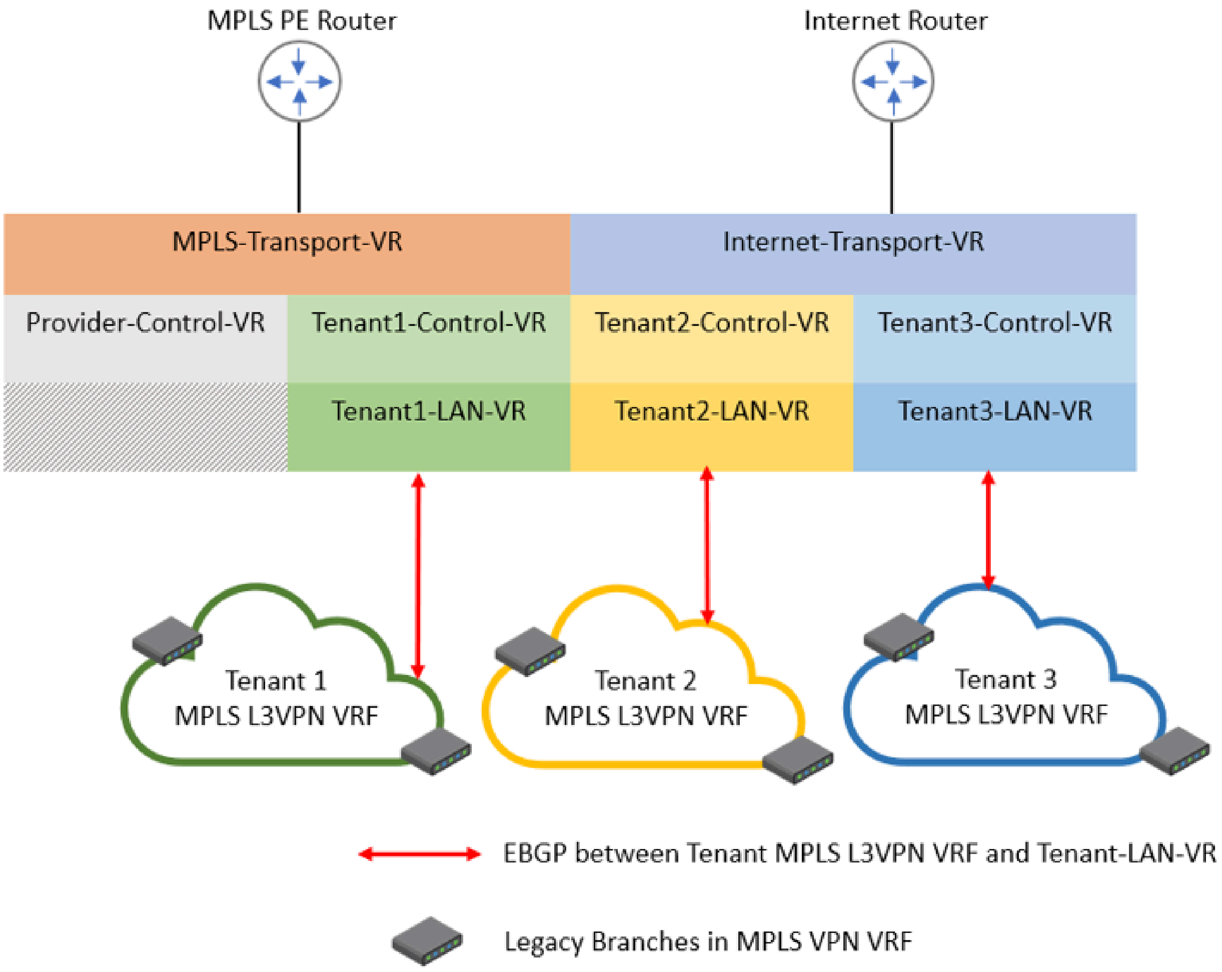
Terms

		Match			
□	Term Name	Protocol	Address	Area	Community
☑	T1-STATIC	static			

7. Select the term to delete, here, T1-STATIC, and click the ⊟ Delete icon.
8. Click OK.

Establish a BGP Session with the MPLS Provider on a LAN Interface

In a scenario in which you establish a BGP session with the MPLS provider on a LAN interface, you use Director Workflows to configure a BGP peering session to exchange routes with the MPLS provider through an IP interface in the Tenant-LAN-VR, as illustrated below.

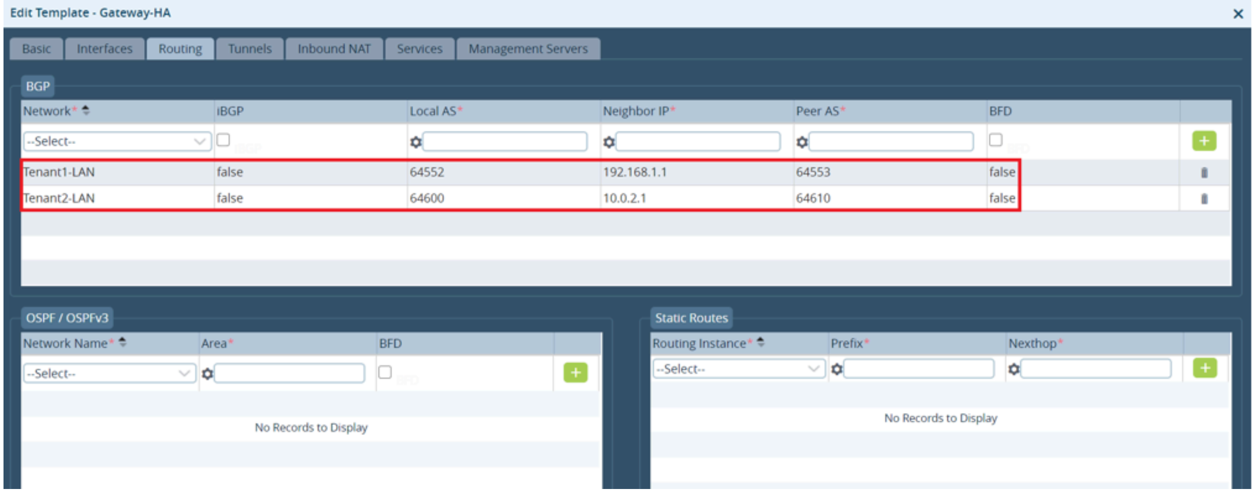


Enterprises hosting their own gateways need two interfaces or logical subinterfaces from the MPLS provider, one that terminates on the MPLS-Transport-VR and that is the underlay to connect to other SD-WAN-enabled sites on MPLS, and a second that terminates in the Tenant-LAN-VR and that is used to connect to non-SD-WAN sites on the MPLS network.

This configuration is commonly seen when a service provider offers a dedicated gateway service their customers and is also the MPLS service provider for their customers. In this scenario, the MPLS provider has one interface or subinterface in the customer VRF that terminates in the customer's Tenant-LAN-VR. The interface that connects to the WAN-Transport-VR is used only to connect to SD-WAN–enabled sites. For any two sites to connect over SD-WAN, only the branch WAN IP connectivity is required. Hence, the peering with the provider on the MPLS-Transport-VR can be a common VRF into which the branch WAN IP addresses of customer VRFs are placed, but the individual customer VRFs have only the WAN IP address of the gateway branch. The EBGP peering session in the Tenant-LAN-VR is with an interface on the provider's MPLS PE router that is part of the customer's VRF in which the legacy branch routes are placed. This design allows each site in the customers SD-WAN network to set up an SLA to the gateway using its underlay IP address, but sites in two different customer networks cannot establish an SLA or any communication path between them. To achieve this, the customer SD-WAN branch MPLS interface WAN IP addresses must be unique or source-NATed.

To configure this type of gateway:

1. In Director view, select the Workflows tab in the top menu bar.
2. Select Template > Templates in the left menu bar.
3. Click the ⊞ Add icon to create a new template, or select an existing template, as shown here. For more information, see [Create Device Templates](#).
4. Select the Routing tab, and configure the tenant LANs, as shown below:



Network*	iBGP	Local AS*	Neighbor IP*	Peer AS*	BFD
--Select--	□				□
Tenant1-LAN	false	64552	192.168.1.1	64553	false
Tenant2-LAN	false	64600	10.0.2.1	64610	false

Network Name*	Area*	BFD
--Select--		□
No Records to Display		

Routing Instance*	Prefix*	Nexthop*
--Select--		
No Records to Display		

5. Click OK.

You can modify the routing policy to filter sent and received routes in the device template or directly for the VOS device. In the configuration, in the Appliance view, select Networking in the left menu bar, select the MPLS-Transport-VR, and select BGP. Then select the BGP instance ID and select Peer/Group Policy. For more information, see [Configure Peer and Peer Group Policy](#).

High Availability

You can use Director Workflows to configure gateways with or without HA. You can use BGP path attributes, such as AS-path prepend, local preference, or MED, to select the gateway device that you want to serve as the primary gateway.

Best Practices

- When you modify the route preference, ensure that you avoid asymmetric routing.
- If you chose a gateway device as the primary, this device must be the primary device for traffic flow in both

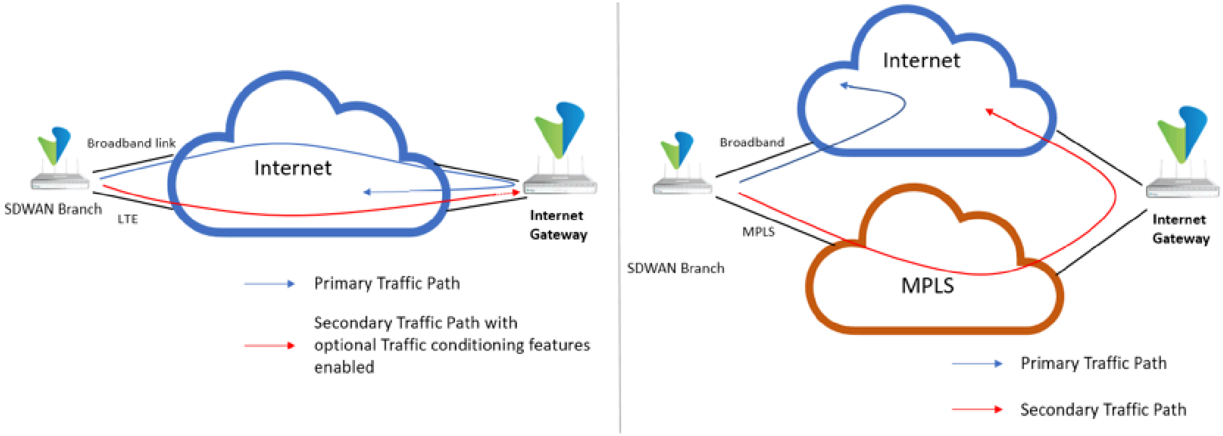
directions.

- If the device is a dedicated gateway, configuring the device as HA in Director Workflows is not useful, because if one of the WAN links or devices fail, the gateway becomes non-functional. However, if the device is not a dedicated gateway, that is, if it also functions as a regular site, hub, or data center branch, it makes sense to configure HA using Director Workflows, because the device is usable even if one of the WAN link or devices fails. If the device is a dedicated gateway and if you can replicate the WAN links, it is recommended that, for redundancy, you have twice the number of single gateway devices.

Gateway for Internet-Bound Traffic

You can configure a VOS branch device as a gateway in the following scenarios:

- To apply SD-WAN path selection policies on internet-bound traffic with optional traffic conditioning features such as forward error correction (FEC) or packet replication. This configuration can mitigate last-mile WAN link degradation.
- To use an MPLS circuit as secondary path to break out from a gateway if the local internet circuit is unavailable, as shown in the following figure.



Supported Software Information

Releases 20.2 and later support all content described in this article.

Additional Information

[Configure Basic Features](#)
[Configure Virtual Routers](#)