SD-WAN and MPLS Layer 3 VPN Architecture Comparison

For supported software information, click here.

This article compares how the Versa SD-WAN solution and MPLS Layer 3 VPNs handle the control plane and the forwarding plane. For these two architectures, the control planes are similar, but the Versa SD-WAN solution provides a very different forwarding paradigm.

Control Plane

Traditional MPLS Layer 3 VPN relies on MP-BGP and an IGP, commonly OSPF or IS-IS. The Versa control plane also uses MP-BGP. Versa SD-WAN CPE devices act as PE devices from an MP-BGP perspective, distributing VRF labels and leveraging the route distinguisher and route target attributes for installing routes in the appropriate LAN VRFs. The Versa Networks SD-WAN solution uses MP-BGP to distribute routing information among branches, leveraging SD-WAN Controller devices, which act as route reflectors. Each SD-WAN CPE (branch) maintains secure control channels with a set of Controllers, for redundancy. MP-BGP sessions are carried within this secure control channel. However, Versa Networks has augmented its MP-BGP implementation with new attributes to allow the distribution of additional information among branches.

MP-BGP is an extensible protocol, and Versa has added a new set of BGP attributes (NLRI) that carry the information necessary additional information to build SD-WAN forwarding tunnels between CPEs, Controllers and gateways. This information includes the transport WAN interfaces, NAT information, and PKI exchanges.

Another notable difference is that the Versa SD-WAN solution does not need an IGP for BGP next-hop resolution. This is because the SD-WAN components (Controllers, CPEs, gateways) are all directly connected using direct overlay tunnels. This means that the BGP next hop is directly connected and does not need to be resolved by an IGP.

A major advantage of the Versa solution is that it leverages existing and proven control plane technology (MP-BGP). This means that all service provider best practice designs and implementations, such as BGP route reflector clustering and BGP architecture scaling, remain the same, and it also means that operational aspects remain the same, thus greatly reducing the learning curve for service provider engineering and operations staff.

Forwarding Plane

Traditional MPLS Layer 3 VPN architecture has the following components: CE router, PE router, and P router.

The CE-to-PE forwarding plane is based on the traditional IP paradigm that uses static or dynamic protocols, while the PE-to-PE forwarding plane is based on MPLS, driven by either LDP or RSVP. Other technologies, such as GRE tunnels, can replace MPLS. As previously explained, the idea behind the Versa SD-WAN solution is to collapse the PE functionality into CE routers and replace the MPLS transport plane with overlay tunnels. The Versa SD-WAN implementation relies solely on its control plane for distributing the necessary information for branches to establish secure overlay forwarding tunnels between themselves without the need to run an IGP along with other MPLS transport layer—related signaling protocols between branches or Controllers and gateways to establish the secure overlay forwarding tunnels.

The forwarding plane is created using the routing information distributed by the MP-BGP-driven control plane. This routing information can then result in any appropriate topology (hub and spoke, full mesh, partial mesh).

The following table compares the forwarding plane for MPLS Layer 3 VPNs and the Versa SD-WAN solution.

Item	**MPLS Layer 3 VPN**	**Versa Networks SD-WAN**
Components	CE routers PE routers P routers + MP-BGP route reflectors	CPEs Controllers
Control Plane	MG-BGP + IGP	MP-BGP within secure control channels, and static routes
	—	Supports dynamic routing protocol for learning the default (OSPF or BGP) if required
Forwarding Plane	Based on LDP and RSVP	Secure overlay tunnels: • IPSec over VXLAN

Another advantage of the Versa SD-WAN solution is that it is agnostic when it comes to the transport layer. The transport layer can be IP or MPLS.

Not only does SD-WAN simplify and reduce the costs, complexity, and time for service delivery and activation, but it also provides additional capabilities over MPLS Layer 3 VPN technology, such as dynamic per-flow or per-application SLA-based end-to-end traffic engineering.

The Versa SD-WAN solution offers zero-touch provisioning (ZTP) that includes a two-factor authentication process. This means that service providers do not need to send on-site technicians to install CPE devices. Instead, they can ship CPE devices to their end customers using any third-party carrier, and they can guarantee that the devices end up at the right place and in the hands of the right person.

After the two-factor authentication process succeeds, Versa Director pushes the appropriate post-staging template, which contains the subscribed services, to the CPE device to finalize the configuration.

This leads to another important aspect of the SD-WAN solution, which is the self-care portal for service subscription/ activation. The Versa Networks SD-WAN solution does not provide a self-care portal for service subscription management and . Instead, Versa Director provides a northbound REST API to leverage the service provider's existing self-care portal.

Let’s discuss two examples that illustrate the ease of the Versa SD-WAN solution and how it can speed up service delivery to the service provider’s end customers:

Example 1:

Customer Acme wants to create a new VPN for its Marketing department to separate it from the Sales department VPN.

- VPN MPLS approach:

  1. Make changes on all required PEs.
  2. Create appropriate VRF.
  3. Modify PE-to-CE configuration (new subinterface, routing).

  Delivery time is generally a couple of weeks away from when the order was placed.

- Versa SD-WAN approach:

  1. Customer logs on to the self-care portal and orders a new VPN.
  2. Self-care portal triggers updates using REST API towards Versa Director, which pushes the appropriate configuration only to the appropriate customer CPEs.
  3. No changes are required at the underlying transport layer.

  Delivery time is a few clicks.

Example 2:

Customer Acme”wants to migrate its existing Engineering VPN from a full-mesh to a hub-and-spoke topology.

- VPN MPLS approach:

  1. Change the configuration on PEs to filter out unwanted BGP announcements (route targets or communities based) to avoid remote PEs to import them in the appropriate VRF.
  2. Configure the default route on the hub and distribute it to spokes.
  3. Modify PE-to-CE configuration (new subinterface, routing).

- Versa SD-WAN approach:

  1. Configure default route on the hub CPE and tag it with the appropriate community.
  2. Configure a filter on spoke devices that is based on the community.
  3. Configure CPEs to accept routes only with the defined community as hub site.

In summary, the fewer devices you touch the less error-prone the process is and the less time it takes to activate and validate the required changes. In these two example cases, to add or change VPN-related parameters-topology when using traditional Layer 3 VPN MPLS, administrators must touch both CPEs and PEs, while with the Versa SD-WAN solution, the changes happen only on CPEs, thus eliminating the risk of jeopardizing other end-customer services. Another important aspect of SD-WAN technology is that it is agnostic regarding the underlying transport layer, thus allowing the service provider to deliver VPN services over the top (OTT), outside of its footprint, without having to deploy and install required MPLS PE routers in locations and countries where it has no presence.

Supported Software Information

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