Segmentation (VPN) Overview

This article illustrates the segmentation and VPN capabilities of the Viptela overlay network solution.

Network segmentation has existed for over a decade and has been implemented in multiple forms and shapes. At its most rudimentary level, segmentation provides traffic isolation. The most common forms of network segmentation are virtual LANs, or VLANs, for Layer 2 solutions, and virtual routing and forwarding, or VRF, for Layer 3 solutions.

There are many use cases for segmentation:

- An enterprise wants to keep different lines of business separate (for example, for security or audit reasons).
- The IT department wants to keep authenticated users separate from guest users.
- A retail store wants to separate video surveillance traffic from transactional traffic.
- An enterprise wants to give business partners selective access only to some portions of the network.
- A service or business needs to enforce regulatory compliance, such as compliance with HIPAA, the U.S. Health Insurance Portability and Accountability Act, or with the Payment Card Industry (PCI) security standards.
- A service provider wants to provide VPN services to its medium-sized enterprises.
- An enterprise wants to set up a trial run of new service and wants to use a cloud service for development and system test.

One inherent limitation of segmentation is its scope. Segmentation solutions either are complex or are limited to a single device or pair of devices connected via an interface. As an example, Layer 3 segmentation provides the following:

1. Ability to group prefixes into a unique route table (RIB or FIB).
2. Ability to associate an interface with a route table so that traffic traversing the interface is routed based on prefixes in that route table.

This is useful functionality, but the scope is limited to a single device. To extend the functionality throughout the network, the segmentation information needs to be carried to the relevant points in the network. There are two approaches to providing this network-wide segmentation:

- Define the grouping policy at every device and on every link in the network (basically, you perform Steps 1 and 2 above on every device).
- Define the grouping policy at the edges of the segment, and then carry the segmentation information in the packets for intermediate nodes to handle.

The first approach is useful if every device is an entry or exit point for the segment, which is generally not the case in medium and large networks. The second approach is much more scalable and keeps the transport network free of segments and complexity. MPLS-based Layer 3 VPNs are a popular example of segmentation at the edge.
Segmentation using the Viptela Technology

Viptela employs the more prevalent and scalable model of creating segments. Essentially, segmentation is done at the edges, on a vEdge router, and the segmentation information is carried in the packets in the form of an identifier.

The figure below shows the propagation of routing information inside a VPN.

In this figure:

- vEdge-1 subscribes to two VPNs, red and blue.
  - The red VPN caters to the prefix 10.1.1.0/24 (either directly through a connected interface or learned via the IGP or BGP).
  - The blue VPN caters to the prefix 10.2.2.0/24 (either directly through a connected interface or learned via the IGP or BGP).

- vEdge-2 subscribes to the red VPN.
  - This VPN caters to the prefix 192.168.1.0/24 (either directly through a connected interface or learned via the IGP or BGP).

- vEdge-3 subscribes to the blue VPN.
  - This VPN caters to the prefix 192.168.2.0/24 (either directly through a connected interface or learned via the IGP or BGP).
Because each vEdge router has an OMP connection over a TLS tunnel to a vSmart controller, it propagates its routing information to the vSmart controller. On the vSmart controller, the network administrator can enforce policies to drop routes, to change TLOCs (which are overlay next hops) for traffic engineering or service chaining, or to change the VPN ID (see Policy Overview for more details). The network administrator can apply these policies as inbound and outbound policies on the vSmart controller.

All prefixes belonging to a single VPN are kept in a separate route table. This provides the Layer 3 isolation required for the various segments in the network. So, vEdge-1 has two VPN route tables, and vEdge-2 and vEdge-3 each have one route table. In addition, the vSmart controller maintains the VPN context of each prefix.

Separate route tables provide isolation on a single node. So now the question is how to propagate the routing information across the network. In the Viptela solution, this is done using VPN identifiers, as shown in the figure below. A VPN ID carried in the packet identifies each VPN on a link. When you configure a VPN on a vEdge router, the VPN has a label associated with it. The vEdge router sends the label, along with the VPN ID, to the vSmart controller. The vSmart controller propagates this vEdge-to-VPN-ID mapping information to the other vEdge routers in the domain. The remote vEdge routers then use this label to send traffic to the appropriate VPN. The local vEdge routers, on receiving the data with the VPN ID label, use the label to demultiplex the data traffic. This is similar to how MPLS labels are used. This design is based on standard RFCs and is compliant with regulatory procedures (such as PCI and HIPAA).

![VPN Diagram](https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_17.2/04Segmentation/01Segmentation_VPNS.png)

It is important to point out that the transport network that connects the vEdge routers is completely unaware of the VPNs. Only the vEdge routers know about VPNs; the rest of the network follows standard IP routing.

**Default VPNs**

The Viptela solution provides two default VPNs to separate traffic.

To enforce the inherent separation between services (such as prefixes that belong to the enterprise) and transport (the network that connects the vEdges), all the transport interfaces (that is, all the TLOCs) are kept in the transport VPN, which is internally maintained as VPN 0. This ensures that the transport network cannot reach the service network.
by default. Multiple transport interfaces can belong to the same transport VPN, and packets can be forwarded to and from transport interfaces.

Management ports are kept separate as well and maintain a separate VPN, which is internally maintained as VPN 512.

---

**Dual Stack**

In the transport VPN (VPN 0), vEdge routers and vSmart controllers support dual stack. To enable dual stack, configure an IPv4 address and an IPv6 address on the tunnel interface. The vEdge router learns from the vSmart controller whether a destination supports IPv4 or IPv6 addresses. When forwarding traffic, the router chooses either the IPv4 or the IPv6 TLOC based on the destination address.

---

**Additional Information**

Configuring Segmentation (VPNs)
Segmentation (VPN) Configuration Examples