Centralized Control Policy

Centralized control policy is policy that is configured on a vSmart controller (hence, it is centralized and operates on the control plane traffic in the Viptela overlay network, influencing the determination of routing paths through the overlay network. Centralized control policy affects the route information that is exchanged between vSmart controllers and vEdge routers in the Viptela overlay network.

Centralized Control Policy Overview

In the Viptela network architecture, centralized control policy is handled by the vSmart controller, which effectively is the routing engine of the Viptela network. The vSmart controller is the centralized manager of network-wide routes, maintaining a master route table for these routes. The vSmart controller builds its route table based on the route information advertised by the vEdge routers in its domain, using these routes to discover the network topology and to determine the best paths to network destinations. The vSmart controller distributes route information from its route table to the vEdge routers in its domain, and the vEdge routers use these routes to forward data traffic through the network. The result of this architecture is that networking-wide routing decisions and routing policy are orchestrated by a central authority instead of being implemented hop by hop, by the devices in the network.

Centralized control policy allows you to influence the network routes advertised by the vSmart controllers. This type of policy, which is provisioned centrally on the vSmart controller, affects both the route information that the vSmart controller stores in its master route table and the route information that it distributes to the vEdge routers.

Centralized control policy is provisioned and applied only on the vSmart controller. The control policy configuration itself is never pushed to vEdge routers in the overlay network. What is pushed to the vEdge routers, via the Overlay Management Protocol (OMP), are the results of the control policy, which the vEdge routers then install in their local route tables and use for forwarding data traffic. This design means that the distribution of network-wide routes is always administered centrally, using policies designed by network administrators. These policies are always implemented by centralized vSmart controllers, which are responsible for orchestrating the routing decisions in the Viptela overlay network.

Within a network domain, the network topology map on all vSmart controllers must be synchronized. To support this, you must configure identical policies on all the vSmart controllers in the domain.
All centralized control plane traffic, including route information, is carried by OMP peering sessions that run within the secure, permanent DTLS connections between vEdge routers and the vSmart controllers in their domain. The end points of an OMP peering session are identified by the system IDs of the Viptela devices, and the peering sessions carry the site ID, which identifies the site in which the device is located. A DTLS connection and the OMP session running over it remain active as long as the two peers are operational.

Control policy can be applied both inbound, to the route advertisements that the vSmart controllers receives from vEdge routers, and outbound, to advertisements that it sends to them. Inbound policy controls which routes and route information are installed in the local routing database on the vSmart controller, and whether this information is installed as-is or is modified. Outbound control policy is applied after a route is retrieved from the routing database, but before vSmart controller advertises it, and affects whether the route information is advertised as-is or is modified.

### Route Types

The vSmart controller learns the network topology from OMP routes, which are Viptela-specific routes carried by OMP. There are three types of OMP routes:

- **Viptela OMP routes**—These routes carry prefix information that the vEdge router learns from the routing protocols running on its local network, including routes learned from BGP and OSPF, as well direct, connected, and static routes. OMP advertises OMP routes to the vSmart controller by means of an OMP route SAFI (Subsequent Address Family Identifier). These routes are commonly simply called OMP routes.

- **TLOC routes**—These routes carry properties associated with transport locations, which are the physical points at which the vEdge routers connect to the WAN or the transport network. Properties that identify a TLOC include the IP address of the WAN interface and a color that identifies a particular traffic flow. OMP advertises TLOC routes using a TLOC SAFI.

- **Service routes**—These routes identify network services, such as firewalls and IDPs, that are available on the local-site network to which the vEdge router is connection. OMP advertises these routes using a service SAFI.

A straightforward way to see the difference in these three types of routes is by using the various `show omp` operational commands when you are logged in to the CLI on a vSmart controller or a vEdge router. The `show omp routes` command displays information sorted by prefix, the `show omp services` command display route information sorted by service, and the `show omp tlocs` command sorts route information by TLOC.
Default Behavior without Centralized Control Policy

By default, no centralized control policy is provisioned on the vSmart controller. This results in the following route advertisement and redistribution behavior within a domain:

- All vEdge routers redistribute all the route-related prefixes that they learn from their site-local network to the vSmart controller. This route information is carried by OMP route advertisements that are sent over the DTLS connection between the vEdge router and the vSmart controller. If a domain contains multiple vSmart controllers, the vEdge routers send all OMP route advertisements to all the controllers.

- All vEdge routers send send all TLOC routes to the vSmart controller or controllers in their domain, using OMP.

- All vEdge routers send all service routes to advertise any network services, such as firewalls and IDPs, that are available at the local site where the vEdge router is located. Again, these are carried by OMP.

- The vSmart controller accepts, as is, all the OMP, TLOC, and service routes that it receives from all the vEdge routers in its domain, storing the information in its route table. The vSmart controller tracks which OMP routes, TLOCs, and services belong to which VPNs. The vSmart controller uses all the routes to develop a topology map of the network and to determine routing paths for data traffic through the overlay network.

- The vSmart controller redistributes all information learned from the OMP, TLOC, and service routes in a particular VPN to all vEdge routers in the same VPN.

- The vEdge routers regularly send route updates to the vSmart controller.

- The vSmart controller recalculates routing paths, updates its route table, and advertises new and changed routing information to all the vEdge routers.
Behavior Changes with Centralized Control Policy

When you do not want to redistribute all route information to all vEdgeouters in a domain, or when you want to modify the route information that is stored in the vSmart controller's route table or that is advertised by the vSmart controller, you design and provision centralized control policy. To activate the control policy, you apply it to specific sites in the overlay network in either the inbound or the outbound direction. The direction is with respect to the vSmart controller. All provisioning of centralized control policy is done on the vSmart controller.

Applying a centralized control policy in the inbound direction filters or modifies the routes being advertised by the vEdge router before they are placed in the route table on the vSmart controller. As the first step in the process, routes are either accepted or rejected. Accepted routes are installed in the route table on the vSmart controller either as received or as modified by the control policy. Routes that are rejected by a control policy are silently discarded.

Applying a control policy in outbound direction filters or modifies the routes that the vSmart controller redistributes to the vEdge routers. As the first step of an outbound policy, routes are either accepted or rejected. For accepted routes, centralized control policy can modify the routes before they are distributed by the vSmart controller. Routes that are rejected by an outbound policy are not advertised.

Examples of Modifying Traffic Flow with Centralized Control Policy

This section provides some basic examples of how you can use centralized control policies to modify the flow of data traffic through the overlay network.

Create an Arbitrary Topology

When data traffic is exchanged between two vEdge routers, if you have provisioned no control policy, the two vEdge routers establish an IPsec tunnel between them and the data traffic flows directly from one router to the next. For a network with only two vEdge routers or with just a small number of vEdge routers, establishing connections between each pair of routers is generally not be an issue. However, such a solution does not scale. In a network with hundreds or even thousands of branches, establishing a full mesh of IPsec tunnels would tax the CPU resources of each vEdge router.
One way to minimize this overhead is to create a hub-and-spoke type of topology in which one of the vEdge routers acts as a hub site that receives the data traffic from all the spoke, or branch, routers and then redirects the traffic to the proper destination. This example shows one of the ways to create such a hub-and-spoke topology, which is to create a control policy that changes the address of the TLOC associated with the destination.

The figure here illustrates how such a policy might work. The topology has two branch locations, West and East. When no control policy is provisioned, these two vEdge routers exchange data traffic with each other directly by creating an IPsec tunnel between them (shown by the red line). Here, the route table on the West vEdge router contains a route to vEdge East with a destination TLOC of 2.1.1.1, color gold (which we write as the tuple \{2.1.1.1, gold\}), and vEdge East route table has a route to the West branch with a destination TLOC of \{1.1.1.1, gold\}.

To set up a hub-and-spoke--type topology here, we provision a control policy that causes the West and East vEdge routers to send all data packets destined for the other router to the vEdge hub router. (Remember that because control policy is always centralized, you provision it on the vSmart controller.) On the West vEdge router, the policy simply changes the destination TLOC from \{2.1.1.1, gold\} to \{10.1.1.1, gold\}, which is the TLOC of the vEdge hub router, and on the East router, the policy changes the destination TLOC from \{1.1.1.1, gold\} to the hub’s TLOC, \{10.1.1.1, gold\}. If there were other branch sites on the west and east sides of the network that exchange data traffic, you could apply these same two control policies to have them redirect all their data traffic through the hub vEdge router.

**Set Up Traffic Engineering**

Control policy allows you to design and provision traffic engineering. In a simple case, suppose that you have two vEdge routers acting as hub devices. Here, you might want data traffic destined to a branch vEdge router to always transit through one of the hub vEdge routers. To engineer this traffic flow, you set the TLOC preference value to favor the desired hub vEdge router.
The figure on the left shows that Site ID 100 has two hub vEdge routers, one that serves the West side of the network and a second that serves the East side. We always want data traffic from the West vEdge branch router to be handled by the West vEdge hub, and similarly, we want data traffic from the East vEdge branch router to go through the East vEdge hub.

To engineer this traffic flow, you provision two control policies, one for Site ID 1, where the West vEdge branch router is located, and a second one for Site ID 2. The control policy for Site ID 1 changes the TLOC for traffic destined to the East vEdge router to \{10.1.1.1, gold\}, and the control policy for Site ID 2 changes the TLOC for traffic destined for Site ID 1 to \{20.1.1.1, gold\}. One additional effect of this traffic engineering policy is that it load-balances the traffic traveling through the two vEdge hub routers.

With such a traffic engineering policy, a route from the source router to the destination router is installed in the local route table, and traffic is sent to the destination regardless of whether the path between the source and destination vEdge routers is available. Enabling end-to-end tracking of the path to the ultimate destination allows the vSmart controller to monitor the path from the source to the destination, and to inform the source router when that path is not available. The source router can then modify or remove the path from its route table.
The figure to the right illustrates end-to-end path tracking. It shows that traffic from vEdge-A that is destined for vEdge-D first goes to an intermediate router, vEdge-B, perhaps because this intermediate router provides a service, such as a firewall. (You configure this traffic engineering with a centralized control policy that is applied to vEdge-A, at Site 1.) Then vEdge-B, which has a direct path to the ultimate destination, forwards the traffic to vEdge-D. So, in this example, the end-to-end path between vEdge-A and vEdge-D comprises two tunnels, one between vEdge-A and vEdge-B, and the second between vEdge-B and vEdge-D. The vSmart controller tracks this end-to-end path, and it notifies vEdge-A if the portion of the path between vEdge-B and vEdge-D becomes unavailable.

As part of end-to-end path tracking, you can specify how to forwarded traffic from the source to the ultimate destination via an intermediate router. (You do this by setting the TLOC action in the action portion of the control policy.) The default method is strict forwarding, where traffic is always sent from vEdge-A to vEdge-B, regardless of whether vEdge-B has a direct path to vEdge-D or whether the tunnel between vEdge-B and vEdge-D is up. More flexible methods forward some or all traffic directly from vEdge-A to vEdge-D. You can also set up a second intermediate router to provide a redundant path with the first intermediate router is unreachable and use an ECMP method to forward traffic between the two. The figure below adds vEdge-C as a redundant intermediate router.
Additional Information

Centralized Control Policy Configuration Examples
Configuring Centralized Control Policy
Policy Overview
Service Chaining