
System and Interfaces Overview

Setting up the basic system-wide functionality of Viptela network devices is a simple and straightforward process. These basic parameters include defining host properties, such as name and IP address; setting time properties, including NTP; setting up user access to the devices; defining system log (syslog) parameters; and creating network interfaces. In addition, the Viptela software provides a number of management interfaces for accessing the Viptela devices in the overlay network.

Host Properties

All Viptela devices have basic system-wide properties that specify information that the Viptela software uses to construct a view of the network topology. Each device has a system IP address, which provides a fixed location of the device in the overlay network. This address, whose function is similar to that of a router ID on a router, is independent of any of the interfaces and interface addresses on the device. The system IP address is a component of each device's TLOC address.

A second host property that must be set on all Viptela devices is the IP address of the vBond orchestrator for the network domain, or a DNS name that resolves to one or more IP addresses for vBond orchestrators. As discussed in [Components of the Viptela Solution](#), the vBond orchestrator automatically orchestrates the bringup of the overlay network, providing the introductions that allow vEdge routers and vSmart controllers to locate each other.

Two other system-wide host properties are required on all devices, except for the vBond orchestrators, to allow the Viptela software to construct a view of the topology: the domain identifier and the site identifier.

To configure the host properties, see [Viptela Overlay Network Bringup](#).

Time and NTP

The Viptela software implements the Network Time Protocol (NTP) to synchronize and coordinate time distribution across the Viptela overlay network. NTP uses a returnable-time design in which a distributed subnet of time servers operating in a self-organizing, hierarchical master-slave configuration synchronizes local clocks within the subnet to national time standards by means of wire or radio. The servers also can redistribute reference time using local routing algorithms and time daemons. NTP is defined in RFC 5905, [Network Time Protocol Version 4: Protocol and Algorithms Specification](#).

User Authentication and Access with AAA, RADIUS, and TACACS+

The Viptela software uses Authentication, Authorization, and Accounting (AAA) to provide security for Viptela devices on the network. AAA, in combination with RADIUS and TACACS+ user authentication, controls which users are allowed access to Viptela devices and what operations they are authorized to perform once they are logged in or connected to the devices.

Authentication refers to the process by which the user trying to access the device is authenticated. To access Viptela devices, users log in with either a standard or a custom username and a password. The local device can authenticate

users, or authentication can be performed by a remote device, either by a Remote Authentication Dial-In User Service (RADIUS) server or by a Terminal Access Controller Access-Control System (TACACS+) system, or by both in sequence.

Authorization determines whether the user is authorized to perform a given activity on the Viptela device. In the Viptela software, authorization is implemented using role-based access. Access is based on groups that are configured on the Viptela devices. A user can be a member of one or more groups. External groups are also considered when performing authorization; that is, the Viptela software retrieves group names from RADIUS or TACACS+ servers. Each group is assigned privileges that authorize the group members to perform specific functions on the Viptela device. These privileges correspond to specific hierarchies of the configuration commands and the corresponding hierarchies of operational commands that members of the group are allowed to view or modify.

The Viptela software does not implement AAA accounting.

For more information, see [Role-Based Access with AAA](#).

Authentication for WANs and WLANs

For wired networks (WANs), vEdge routers can run IEEE 802.1x software to prevent unauthorized network devices from gaining access to the WAN. IEEE 802.1x is a port-based network access control (PNAC) protocol that uses a client-server mechanism to provide authentication for devices wishing to connect to the network. You enable 802.1x on vEdge router interfaces to have the router act as an 802.1x authenticator, responsible for authorizing or denying access to network devices.

IEEE 802.1x authentication requires three components:

- **Supplicant**—Client device, such as a laptop, that requests access to the WAN. In the Viptela overlay network, a supplicant is any service-side device that is running 802.1x-compliant software. These devices send network access requests to the vEdge router.
- **Authenticator**—Network device, here a vEdge router, that provides a barrier to the WAN. In the overlay network, you can configure an interface vEdge router to act as an 802.1x authenticator. The vEdge router supports both controlled and uncontrolled ports. For controlled ports, the router acts as an 802.1x port access entity (PAE), allowing authorized network traffic and preventing unauthorized network traffic ingressing to and egressing from the controlled port. For uncontrolled ports, the router, acting as an 802.1x PAE, transmits and receives Extensible Authentication Protocol over IEEE 802 (EAP over LAN, or EAPOL) frames.
- **Authentication server**—Host running authentication software that validates and authenticates supplicants that want to connect to the WAN. In the overlay network, this host is an external RADIUS server. This RADIUS server authenticates each client connected to the vEdge router's 802.1x port interface and assigns the interface to a VLAN before the client is allowed to access any of the services offered by the router or by the LAN.

For wireless LANs (WLANs), vEdge routers can run IEEE 802.11i prevents unauthorized network devices from gaining access to the WLANs. IEEE 802.11i implements Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) to provide authentication and encryption for devices that want to connect to a WLAN. WPA authenticates individual users on the WLAN using a username and password. WPA uses the Temporal Key Integrity Protocol (TKIP), which is based on the RC4 cipher. WPA2 implements the NIST FIPS 140-2-compliant AES encryption algorithm along with

IEEE 802.1x-based authentication, to enhance user access security over WPA. WPA2 uses the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP), which is based on the AES cipher. Authentication is done either using preshared keys or through RADIUS authentication.

Network Interfaces

In the Viptela overlay network design, interfaces are associated with VPNs. The interfaces that participate in a VPN are configured and enabled in that VPN. Each interface can be present only in a single VPN.

The overlay network has three broad types of VPNs:

- **Transport VPN**—This is VPN 0. All interfaces activated in this VPN connect to a transport network of some type, such as the Internet, metro Ethernet, or an MPLS cloud, and these interfaces carry overlay network control traffic. The interfaces in VPN 0 are referred to as transport-side interfaces. You can configure transport VPNs on all Viptela devices.
- **Service VPNs**—These are all VPNs up through VPN 65535 except for VPN 0 and VPN 512. You can configure service-side VPNs only on vEdge routers. All service-side interfaces activated in these VPNs connect to a local or branch network that is generally located at the same site as the vEdge router. These interfaces carry data traffic throughout the overlay network.
- **Management VPN**—VPN 512 handles out-of-band management traffic. You can configure the management VPN on all Viptela devices.

For all Viptela devices, you can configure transport interfaces to run either IPv4 or IPv6, or you can configure them to run both, for a dual-stack implementation.

For each network interface, you can configure a number of interface-specific properties, such as DHCP clients and servers, VRRP, interface MTU and speed, and PPPoE. At a high level, for an interface to be operational, you must configure an IP address for the interface and mark it as operational (no shutdown). In practice, you always configure additional parameters for each interface.

Management Interfaces

Management interfaces provide access to devices in Viptela overlay network, allowing you to collect information from the devices in an out-of-band fashion and to perform operations on the devices, such as configuring and rebooting them.

The following management interfaces are available:

- Command-line interface (CLI)
 - IP Flow Information Export (IPFIX)
 - RESTful API
 - SNMP
-

- System logging (syslog) messages
- vManage web server

CLI

You can access a command-line interface (CLI) on each Viptela device, and from the CLI you configure overlay network features on the local device and gather operational status and information regarding that device. While a CLI is available, it is strongly recommended that you configure and monitor all Viptela network devices from a vManage web server, which provides visual views of network-wide operations and device status, including drill-downs that display details operation and status data. In addition, the vManage web server provides straightforward tools for bringing up and configuring overlay network devices, including bulk operations for setting up multiple devices simultaneously.

You access the CLI either by establishing an SSH session to a Viptela device. For a hardware vEdge router, you can also connect to the device's console port.

For a Viptela device that is being managed by a vManage NMS, if you create or modify the configuration from the CLI, those changes are overwritten by the configuration that is stored in the vManage configuration database.

From a device's CLI, you can log in to the underlying shell running on the device, referred to as the vshell. The vshell filesystem stores system logging (syslog) and other files that contain status information about the device. The vManage NMS periodically retrieves the information in these files and makes the information available to be displayed on a vManage web server.

It is recommended that you log in to a device's shell only when you are working to debug an issue with the device or with the network.

IPFIX

the IP Flow Information Export (IPFIX) protocol, also called cflowd, is a tool for monitoring the traffic flowing through vEdge routers in the overlay network and exporting information about the traffic to a flow collector. The exported information is sent in template reports, which contain both information about the flow and data extracted from the IP headers of the packets in the flow.

The Viptela cflowd performs 1:1 traffic sampling. Information about all flows is aggregated in the cflowd records; flows are not sampled. vEdge routers do not cache any of the records that are exported to a collector.

The Viptela cflowd software implements cflowd version 10, as specified in [RFC 7011](#) and [RFC 7012](#).

For a list of elements exported by IPFIX, see [Traffic Flow Monitoring with Cflowd](#).

To enable the collection of traffic flow information, you create data policies that identify the traffic of interest and then direct that traffic to a cflowd collector. For more information, see [Traffic Flow Monitoring with Cflowd](#).

You can also enable cflowd visibility directly on vEdge routers without configuring data policy so that you can perform traffic flow monitoring on traffic coming to the router from all VPNs in the LAN. You then monitor the traffic from the vManage GUI or from the router's CLI.

RESTful API

The Viptela software provides a RESTful API, which is a programmatic interface for controlling, configuring, and monitoring the Viptela devices in an overlay network. You access the RESTful API through the vManage web server.

The Viptela RESTful API calls expose the functionality of Viptela software and hardware features and of the normal operations you perform to maintain Viptela devices and the overlay network itself.

For more information, see [Viptela REST APIs](#).

SNMP

The Simple Network Management Protocol (SNMP) allows you to manage all Viptela devices in the overlay network. The Viptela software supports SNMP Version 1, Version 2 (also known as Version 2c, or v2c), and SNMPv3. All three versions of SNMP are supported simultaneously. For SNMPv1 and SNMPv2, the Viptela software does not include any of the security features that were originally included in the IETF SNMP drafts, but were later dropped because of the inability to standardize on a particular method. In SNMP v1, SNMP v2 user access is controlled by communities, so AAA rules for users and user groups are not enforced in this case.

You can configure basic SNMP properties—device name, location, contact, and community—that allow the device to be monitored by an SNMP NMS.

You can configure trap groups and SNMP servers to receive traps.

The object identifier (OID) for the Internet port of the SNMP MIB is 1.3.6.1. The OID for the private portion of the Viptela MIB is 1.3.6.1.4.1.41916.

For a list of supported MIBs, see [Supported SNMP MIBs](#).

SNMP traps are asynchronous notifications that a Viptela device sends to an SNMP management server. Traps notify the management server of events, whether normal or significant, that occur on the Viptela device. By default, SNMP traps are not sent to an SNMP server. Note that for SNMPv3, the PDU type for notifications is either SNMPv2c inform (InformRequest-PDU) or trap (Trapv2-PDU). For a list of supported trap types, see [Configuring SNMP](#).

Syslog Messages

System logging operations use a mechanism similar to the UNIX syslog command to record system-wide, high-level operations that occur on the Viptela devices in the overlay network. The log levels (priorities) of the messages are the same as those in standard UNIX commands, and you can configure which priority of syslog messages are logged. Messages can be logged to a file on the Viptela device or to a remote host.

vManage NMS

The vManage NMS is a centralized network management system that allows configuration and management of all Viptela devices in the overlay network and provides a dashboard into the operations of the entire network and of individual devices in the network. Each vManage NMS runs on a web server in the network. Three or more vManage web servers are consolidated into a vManage cluster to provide scalability and management support for up to 6,000 vEdge routers, to distribute vManage functions across multiple devices, and to provide redundancy of network management operations.

Additional Information

[Configuring SNMP](#)

[Configuring Time and Location](#)

[Configuring User Access and Authentication](#)