Features and Capabilities

The Versa Networks solution includes a rich set of networking, security, and other features and functionality. This article describes some of the major features:

Network Software Features

Versa Operating System™ (VOS™) devices provide carrier-grade network routing protocols that allow you to use a VOS device as a standalone virtual router or as part of an end-to-end SD-WAN solution.

The following routing protocols are supported:

- Bidirectional Forwarding (BFD)—Detects the aliveness of BGP peers, OSPF neighbors, and static route next hops
- Border Gateway Protocol (BGP) and Multiprotocol BGP (MP-BGP)—BGP and MP-BGP are standardized exterior gateway protocols (EGPs) that allow the exchange of routing information between devices in different autonomous systems (ASs). These protocols define network reachability based on IP prefixes that are part of an AS.
- Equal-cost multipath routing (ECMP)—VOS devices support up to 16 ECMP paths to any destination.
- Open Shortest Path First (OSPF)—Uses dynamic methods to determine routes to network destinations. OSPF uses link-state advertisements (LSAs) to share route information with other routers. By using this route information and assigning a cost to each router interface, OSPF makes routing decisions. OSPF processes a large amount of route information dynamically, so it requires a faster processor and more memory than other protocols.
- Route redistribution—Policy rules redistribute routes from a source routing protocol (BGP, OSPF, and static) to a destination protocol (BGP and OSPF).
- Static routing—You configure static routes to forward traffic on the network.
- Virtual routing and forwarding (VRF) and multi-VRF—Allow multiple instances of a routing table to exist simultaneously in a single router so that identical or overlapping IP addresses can be used without causing conflicts.
- Virtual Router Redundancy Protocol (VRRP)—Enables hosts on a LAN to use redundant routing platforms on the LAN simply by configuring a single default route on the hosts.

The following Layer 2 forwarding features are supported:

- Bridge domain—A set of logical interfaces in a virtual switch that are part of the same broadcast domain.
- Virtual switch—A software object that functions like a hardware-based Layer 2 switch. A virtual switch allows a VOS device to perform the functions of a standard switch.
- VXLAN—A data-plane encapsulation protocol that allows you to run Layer 2 Ethernet VPN (EVPN) over a Layer 3 IP network using standard VXLAN encapsulation over UDP
- VLAN, QinQ—A VLAN is a logical grouping of devices in the same broadcast domain. Q-in-Q (802.1Q encapsulation) is a method that adds a VLAN tag to VLAN Ethernet frames so that switches know to which VLAN

the traffic belongs.

- MSTP—Multiple Spanning Tree Protocol (MSTP) is a protocol that creates multiple spanning trees for each VLAN on a single physical network, which allows each VLAN to have a configured root bridge and forwarding topology.
- RSTP—Rapid Spanning Tree Protocol (RSTP) enables fast spanning-tree reconvergence by simplifying the port states and changing the way ports transition from one state to another. RSTP is backward-compatible with the Spanning Tree Protocol (STP)
- ZTP—Zero touch provisioning (ZTP) is a way to automatically configure and provision network devices, eliminating the need for administrators to handle tese tasks manually.

Security Software Features

The Versa security features fall into three broad categories:

- Layer 4 security
- Layer 7 security
- Unified threat management (UTM)

Layer 4 security features include:

- Carrier-grade NAT (CG-NAT)—NAT employed on a large scale translates multiple private IPv4 addresses to a limited number of public IPv4 addresses using Network Address and Port Translation (NAPT) methods. You can define private IPv4 addresses in your network and use CG-NAT to manage the translation of addresses to the public IPv4 addresses.
- Denial-of-service (DoS) prevention—Protects against DoS attacks, providing both zone and end protection. DoS prevention capabilities can recognize and provide protection against Layer 3 and Layer 4 flooding, spoofing techniques, scans, and packet anomalies.
- IPsec support—IPsec is a set of protocols that uses encryption services to secure communications over IP networks. IPsec provides integrity, replay protection, confidentiality, access control, and authenticity.
- Stateful firewall services—Enable the configuration and deployment of Layer 4-based stateful firewall services. These services include configurable objects, such as addresses, zones, and schedules; and access policies, such as matching and actions.

Layer 7 security features include:

- Application identification—Automatically identifies the application that network traffic is using when Layer 7 network functions, such as next-generation firewall (NGFW), are enabled. VOS devices currently recognize 3881 applications and protocols and provide built-in application groups for easy and consistent application traffic management. (Note that this number could change as Versa adds more applications to the list.)
- DNS proxy and load balancing—Support for split proxy mode and transparent proxy mode. In split proxy mode, a proxy server splits DNS queries based on the interface and the domain names. In transparent proxy mode, a transparent DNS proxy server, which redirects requests and responses without modifying them, sits between a host and the internet. (A nontransparent proxy server is one that modifies requests and responses.) You can use transparent proxy mode to forward a client's DNS queries to designated or well-known DNS servers.
- Next-generation firewall (NGFW)—Identifies applications and manages and secures application traffic flows using policies. NGFW policy actions include allow, deny, restrict access, redirect, captive portal-based application access management and logging, and advanced actions, such as scripting.

- URL reputation and filtering—Screens web traffic to determine whether it poses a security risk, is out of compliance with company policies, needs to be filtered for parental control, or needs to be authenticated or authorized further for access or other purposes. You can use predefined URL categories and define custom classes.
- User-level and group-level control—Built-in user-based and group-based control capabilities that integrate with Microsoft Active Directory (AD) through LDAP and Kerberos mechanisms. You can create and execute user- and group-specific services, such as parental guidance, enforcement of company compliance, access and authorization policies, and policies tailored for specialized users.

Unified threat management (UTM) security features include:

- Antivirus—Provides multilayered virus detection using heuristics, signature matching, and emulation. The Versa antivirus signatures on Versa Director are updated regularly from the Versa cloud. Versa Director then updates the VOS instances.
- File filtering—Protects against viruses and vulnerabilities that are associated with various file types and file attributes. File filtering can block potentially risky file transfers based on file attributes such as file application, file size, transfer protocol, and traffic path. File filtering supports FTP, HTTP, IMAP, MAPI, and SMTP.
- HTTP and SSL proxy—Provides end-to-end SSL security by transparently decrypting outbound and inbound SSL traffic, inspecting decrypted traffic for threats, and re-encrypting traffic to clients and servers. SSL decryption allows you to apply consistent policies for applications, security, content, and compliance. HTTP and SSL proxy includes optimized capabilities for HTTPS, SMTP, SSH, and other flows, and it allows you to manage public and private keys with role-based access control (RBAC).
- Lateral movement detection and prevention—The VOS IPS and antivirus engines protect against lateral movement threats. The antivirus engine detects malware binaries that use lateral movement techniques. The intrusion prevention system (IPS) engine inspects network traffic to identify the ransomware and malware activities, as well as activities typically seen with tools such as Responder.
- Next-generation IPS—Provides a robust set of detection, prevention, logging, and reporting capabilities, and serves as a tool to detect out-of-compliance users and applications. Versa IPS software includes attack profiles tailored for various operating systems, servers, and clients. These attack profiles use pattern-matching algorithms to detect and prevent attacks.

High Availability

The Versa SD-WAN solution provides network resilience and high availability both at the data center and in the branch, ensuring continuous access to applications, data, and content.

To achieve the greatest level of high availability, it is recommended that redundant components be deployed in geographically separated locations.

The following components can be deployed in redundant fashion:

- Versa Director—Active-standby mode only
- Versa Controller
- Versa Analytics cluster nodes—Active-active mode, and in Releases 21.2.1 and later, active-backup mode
- Branch node—Active-active or active-standby mode

Versa Director Redundancy

You can deploy Versa Directors for system-level high availability in active-standby mode, as shown in Figure 1. The standby Versa Director is in read-only mode.

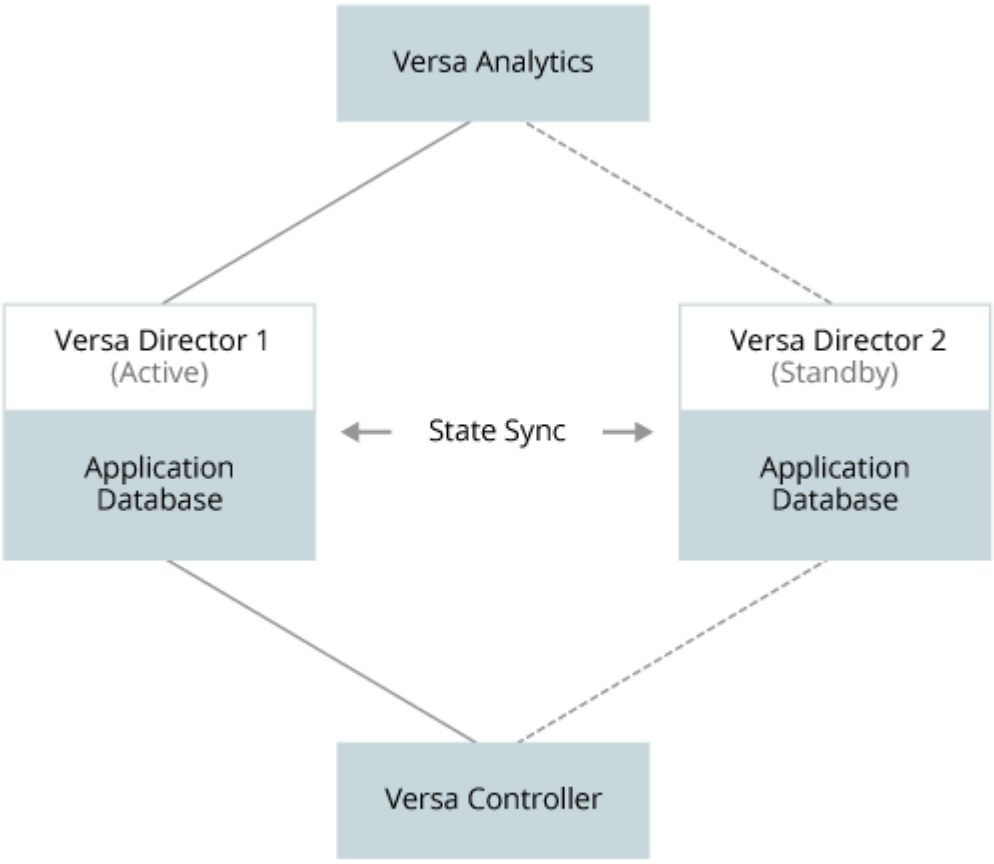

Figure 1. Redundant Versa Directors

The active and standby Versa Director instances can be located in the same data center or in different data centers. The state of the active Versa Director data base is periodically synchronized with the standby Versa Director database. By default, synchronization occurs every 300 seconds (5 minutes), with a maximum of three timeouts before a failover is initiated (these values are configurable).

If the active Versa Director fails or a communications disruption occurs between the active and standby instances, automatic failover is initiated and the standby instance becomes the active instance. When the original active instance recovers, the standby instance can remain in the active state or can yield the active state to the original active Versa Director instance, depending on the configuration. You can also initiate a manual switchover.

Versa SD-WAN Controller Redundancy

You can deploy SD-WAN Controllers in a cluster for redundancy and scalability. The pair of redundant Controllers use MP-BGP to communicate with each other.

Each branch device connects to each SD-WAN Controller. The ZTP process is managed by one primary controller only. If the first controller is not responsive, ZTP contacts the next configured controller. A primary controller is designated for each branch and it manages overlay tunnels between branches and the probes sent between branches.

Figure 2 shows redundant SD-WAN Controllers in active-active mode.

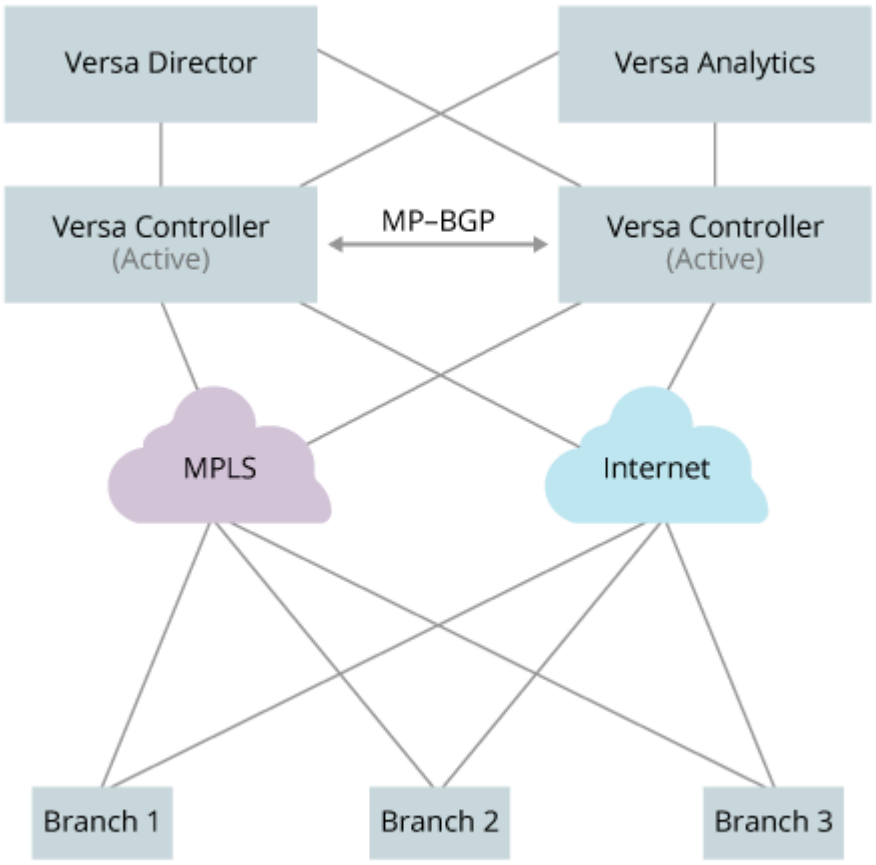

Figure 2. Redundant Versa Controllers

Versa Analytics Redundancy

The nodes in a Versa Analytics cluster run in active-active mode and achieve redundancy by replicating the data

between the pair of nodes in the cluster. Figure 14 shows an example in which the local Versa Analytics cluster has two analytics nodes (Analytics1 and Analytics2) to replicate analytics data and two search nodes (Search1 and Search2) to replicate search data.

To provide live backup, you can deploy another Versa Analytics cluster with two or more nodes in a remote data center, as shown in Figure 3. If the local data center fails, Versa Director can then connect to the Versa Analytics cluster in the remote data center. You can configure VOS devices to send logs to the Versa Analytics cluster in the remote data center.

Note: To ensure that the remote cluster can handle the same amount of data as the local cluster, deploy the same number of nodes in the remote cluster as are deployed in the local cluster.

You can also configure the Versa Controller to act as a load balancer between the Versa Analytics clusters in the local and remote data centers.

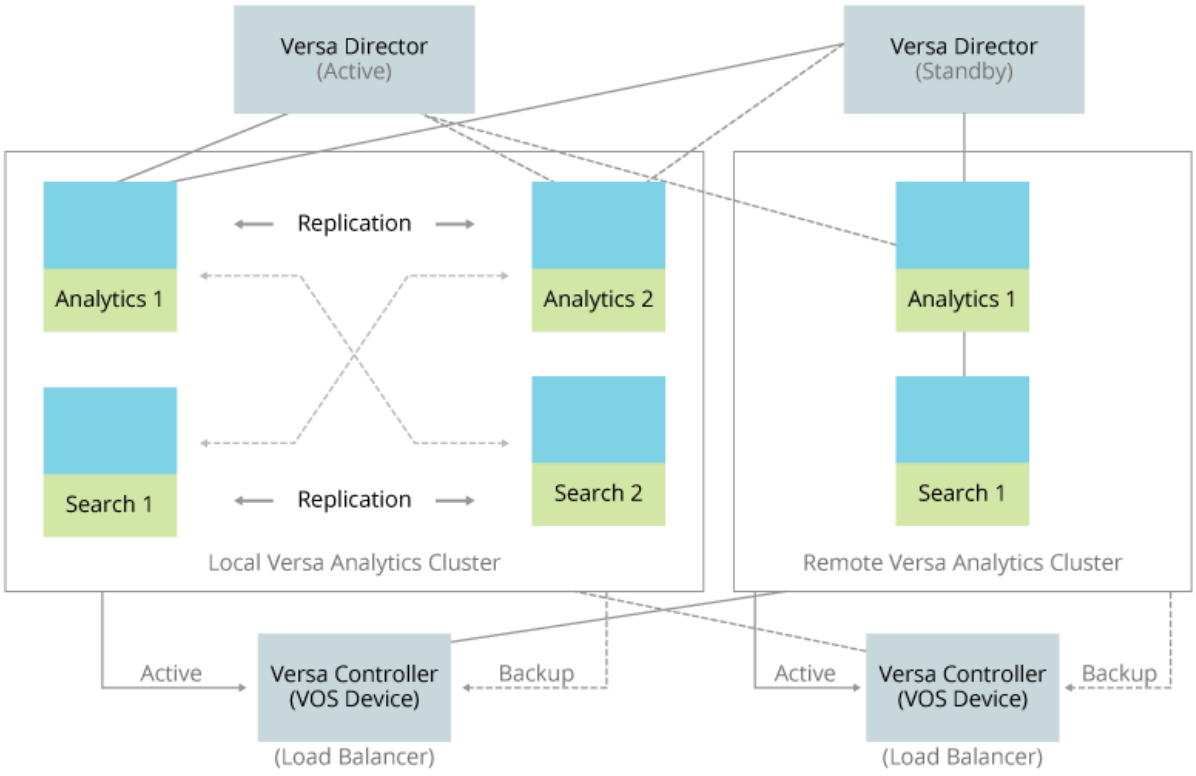

Figure 3. Versa Analytics Clusters in Local and Remote Data Centers

Versa Branch Redundancy

You can deploy branch nodes redundantly in either active-standby or active-active mode. Figure 4 shows a branch node with two CPEs, one in active mode and one in standby mode, connected to a client, with VRRP running to ensure high availability between the redundant CPEs.

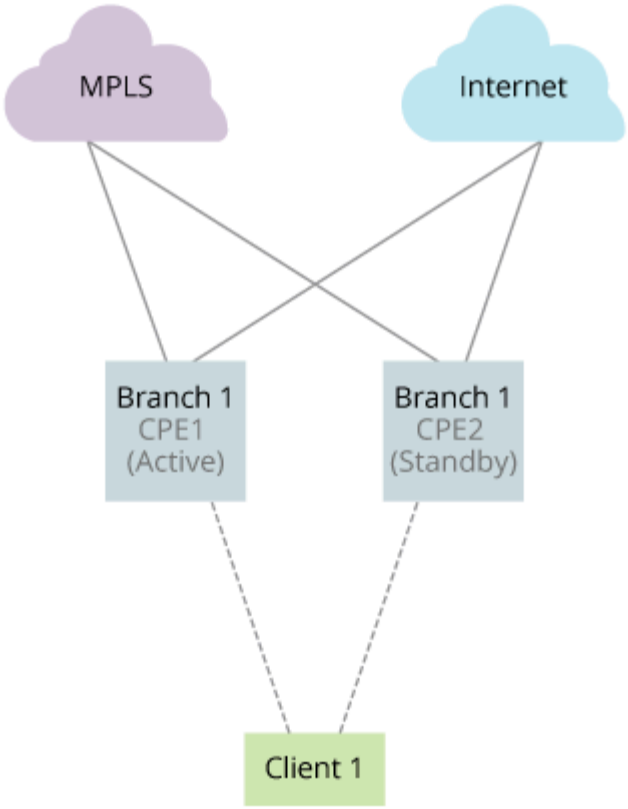

Figure 4. Redundant Branch Nodes (Active-Standby)

Figure 5 shows a branch node with two CPEs, both of which are in active mode, with VRRP running to ensure high availability between the redundant CPEs.

Updated: Wed, 23 Oct 2024 07:32:47 GMT

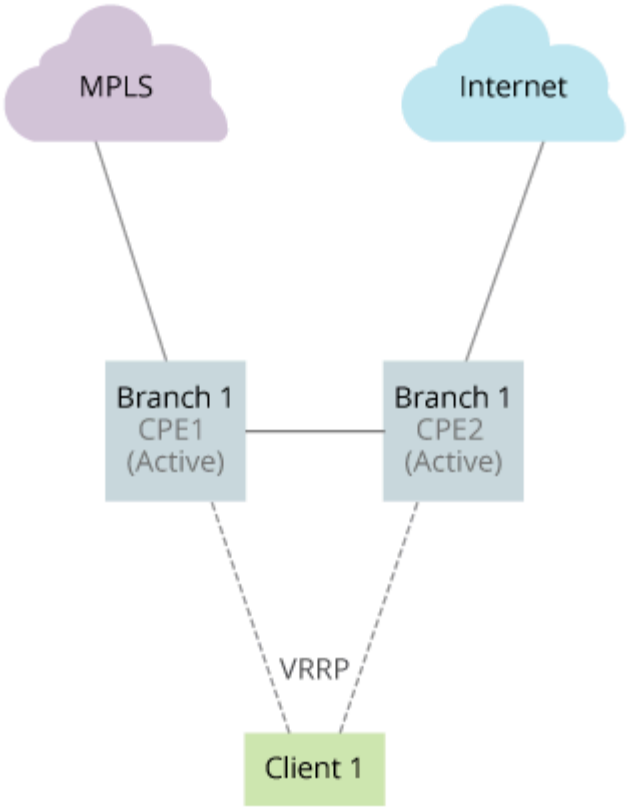

Figure 5. Redundant Branch Nodes (Active-Active)

Multitenancy

All Versa Networks solutions and components support multitenancy, using per-tenant secure overlay networks in the control and data planes to provide traffic isolation and privacy. A single VOS instance, whether deployed as an SD-WAN branch or an SD-WAN Controller, can support up to 256 tenants.

Each tenant in a VOS instance is fully isolated from other tenants that are hosted in the same VOS instance. To effect this isolation, each tenant has its own routing instances (virtual routers and VRFs), its own secure control and forwarding overlay tunnels, and its own service chains, role-based access control (RBAC), traffic steering policies, networking and security policies, and visibility.

RBAC provides access to a tenant's own appliances and services regardless of the access mode, whether that access is done directly using SSH, through a web UI using Versa Director, or through dashboards and reports using Versa Analytics. For branch node deployments, multitenancy securely segments traffic as required by business needs. Both

Versa Director and Versa Analytics leverage RBAC to limit a user's access to the tenant resources that they are authorized to use.

SLA Monitoring and Traffic Steering

The Versa Networks SD-WAN solution helps service providers fulfill their service-level agreements (SLAs) with their customers by continually monitoring and measuring WAN network performance and by making intelligent routing decisions based on this performance data.

For enterprise deployments, SLA monitoring and SD-WAN help ensure resilient business continuity by delivering services reliably and with quality, creating an automated infrastructure that dynamically adjusts itself as needed.

You can measure and act on the following SLA criteria:

- Jitter
- Latency
- Packet loss
- Mean opinion scores (MOS)
- Link utilization percentage

To enable SLA monitoring, you define SLA profiles, forwarding profiles, and application-based forwarding policies. SLA profiles define the network criteria to monitor and the threshold values for each.

Forwarding profiles define what should happen when SLA violations occur, including:

- Whether traffic should be forwarded, dropped, or throttled.
- Which circuits have priority when there is no SLA violation on the circuit. Traffic flows over the higher-priority circuit until an SLA violation occurs, at which point it switches to a lower-priority circuit that is not in violation of an SLA.
- When normal traffic flow can return after an SLA violation is resolved.

You use SLA policies to match types of application traffic to the forwarding table that should be used for that type of application traffic. In policies, you can also configure IP addresses to be monitored and an action to take if the IP addresses are unreachable.

Versa uses IP-encapsulated ITU Y.1731_CFM probes to monitor connectivity between sites and to measure performance metrics, such as delay, delay variation, loss, and availability, for each forwarding class.

For example, you can create an SLA for a business-critical application that specifies the following:

- Maximum link latency of 250 ms
- Maximum jitter of 30 ms
- Primary interface
- Secondary interface

Here, if the link-latency metric or the maximum jitter metric violates the SLA by exceeding the configured limits, traffic for

the application is switched from the primary interface to the secondary interface. When the SLA violation is resolved, the application traffic is switched back to the primary interface.

NAT Traversal

In SD-WAN deployments, branches typically establish tunnels to other branches, often over multiple networks, and each branch can have a network address translation (NAT) device that sits between the branch and the network. To ensure that the NAT devices do not disrupt communication between SD-WAN branches, the Versa SD-WAN solution implements NAT traversal, as defined in RFC 3947 and RFC 3948. NAT traversal includes the STUN relay protocol, to allow traffic to traverse NAT end point independent mapping (EIM) along the traffic path, and the TURN relay protocol, to allow traffic to traverse NAT end point dependent (ED) devices along the traffic path.

Quality of Service

The VOS QoS feature allows you to define and control the quality of service for real-time and high-bandwidth traffic that is prone to jitter and latency, such as VoIP, video on demand, and voice conferencing. QoS provides application-aware queuing, scheduling, and routing based on time of day, link type (MPLS, internet, and LTE), application requirements (bandwidth, delay, jitter, and error rate), and link performance.

The Versa QoS framework allows you to:

- Prioritize network and application traffic.
- Provide the appropriate amount of bandwidth required by different subnets, users, or classes in a network.
- Allocate bandwidth to internal and external traffic.
- Apply QoS for upload traffic and download traffic, or both.
- Ensure low latency for revenue-generating network traffic.
- Implement application traffic profiling for ensuring bandwidth usage.
- Associate SLA requirements with certain classes of traffic and then choose the paths that meet the SLA requirements.

You configure QoS by assigning QoS profiles and policies to network interfaces, to optimize and prioritize network traffic flow on the interfaces, to configure interface bandwidth usage, and to rewrite fields in the packets. With QoS configuration you can control the traffic flow at different points along the traffic path.

The Versa Networks solution applies QoS processing in five stages, as shown in Figure 6:

- Classification—Identify and separate incoming data traffic. There are two types of classifications: Layer 3/Layer 4 rule-based and Layer 7 rule-based. Layer 7 classification takes precedence over Layer 3/Layer 4 classification.
- Policing—Prevent incoming traffic from overloading a node or an outgoing link.
- Remarking—Alter the class of service (CoS) value in the packet header as the packet exits the node.
- Queuing—Define traffic priority, define the weights of queues used during periods of network congestion, and define the RED and WRED mechanisms for dropping traffic.
- Scheduling—Control the order of packets sent out of the node based on packet priority.

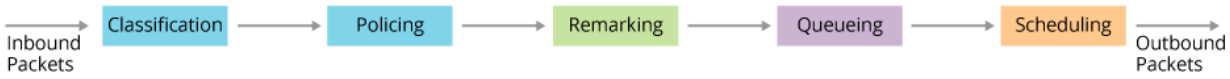

Figure 6. QoS Stages

Versa QoS supports 16 forwarding classes and 16 queues. In the classification and policing stages, data traffic is mapped into 16 forwarding classes. From theses 16 forwarding classes, four traffic classes are created, each containing four forwarding classes.

The traffic classes and their associated forwarding classes are:

- Traffic class 0, network control—Includes forwarding classes 0 through 3
- Traffic class 1, expedited forwarding (EF)—Includes forwarding classes 4 through 7
- Traffic class 2, assured forwarding (AF)—Includes forwarding classes 8 through 11
- Traffic class 3, best effort (BE)—Includes forwarding classes 12 through 15

Figure 7 shows how QoS processes data traffic, placing incoming traffic into forwarding classes and queues and scheduling outgoing traffic for transmission.

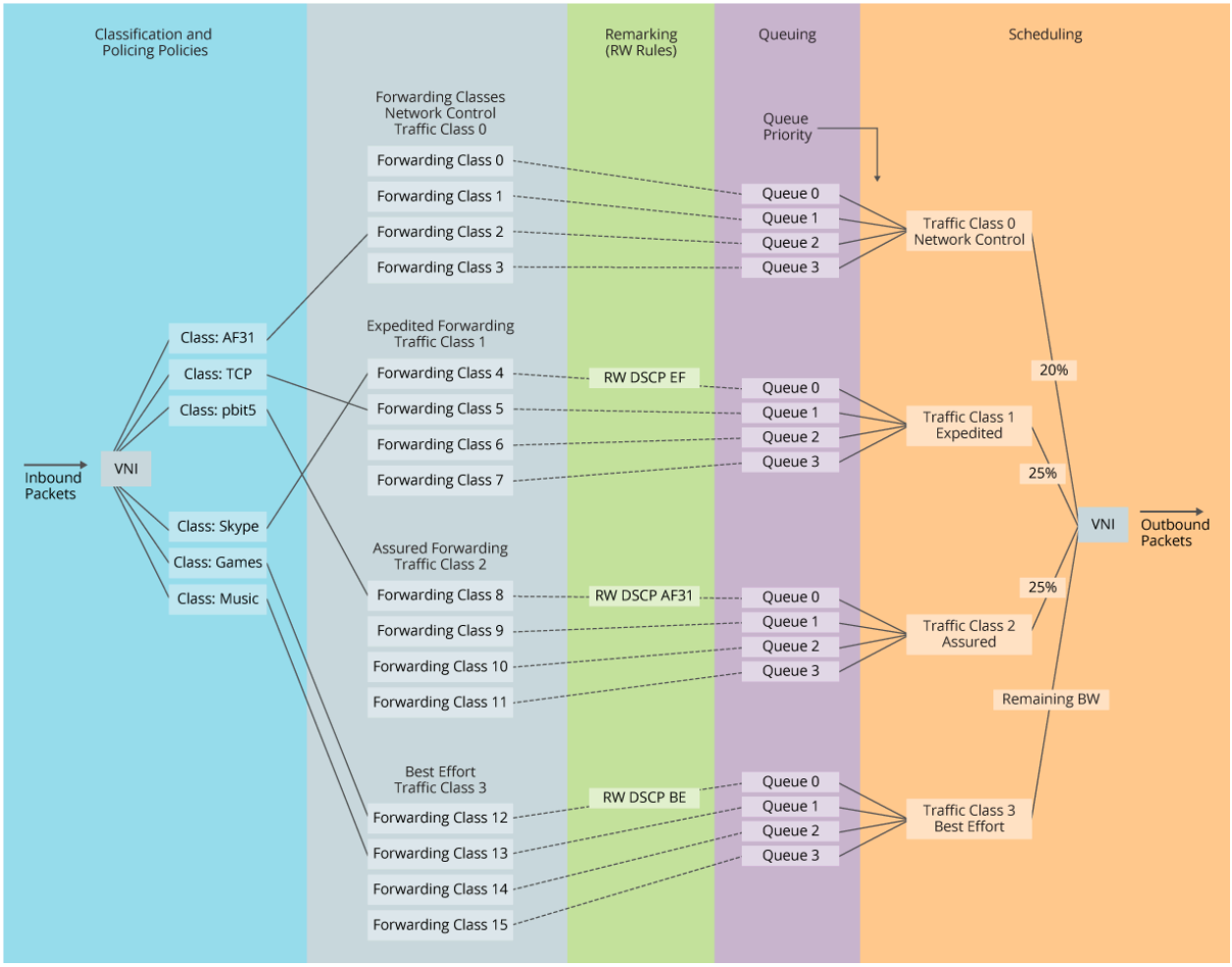

Figure 7. End-to-End QoS

Fabric Flow Control and Adaptive Shaping

Versa fabric flow-control and adaptive shaping monitors sources of traffic across SD-WAN sites and, in the event of sustained traffic congestion, implements flow-control mechanisms using the MP-BGP control plane. Flow control allows sources to throttle their traffic and provides a controlled traffic-distribution mechanism that is directed at the sources of the traffic. This mechanism also provides better traffic management and ensures the enforcement of traffic policies across sites within the SD-WAN fabric.

Service Chaining

Service chaining is a method for connecting virtualized network services in a logical way so that, as traffic flows along the chain, each service is applied in the order specified in the configuration. When different applications require different services, you can create multiple service chains, with each chain providing a certain set of services, to form a service node group (SNG). With SNGs, application traffic can be sent through any or all the configured service chains, as

needed. Because service functions are virtualized, you can create and remove them as required by the application traffic flows in your network.

VOS devices include built-in services that you can use in service chains, including routing, NGFW, DPI, DoS protection, IDS, carrier-grade NAT, Layer 4 to Layer 7 application-delivery controller (ADC), and SD-WAN VPN services. VOS devices provide built-in service-chaining capabilities for third-party VNFs and physical network functions (PNFs). When application traffic enters a VOS device, it passes through a classifier that determines the type of application that generated the flow and then applies any service chains that have been configured for that type of application traffic. You can connect internal and external services in the same service chain.

Figure 8 shows application traffic flowing through two SNGs, with each SNG consisting of a different set of service functions, in a VOS native service chain.

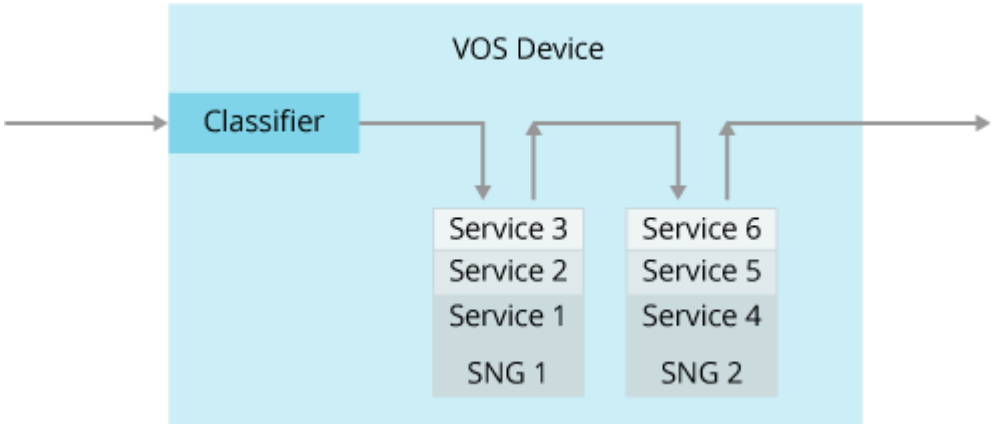

Figure 8. VOS *Service Chain*

Figure 9 shows two traffic flows, red and black, and three SNGs, two of which are native to VOS devices (SNG1 and SNG3) and one that is a third-party SNG (SNG2).

Updated: Wed, 23 Oct 2024 07:32:47 GMT

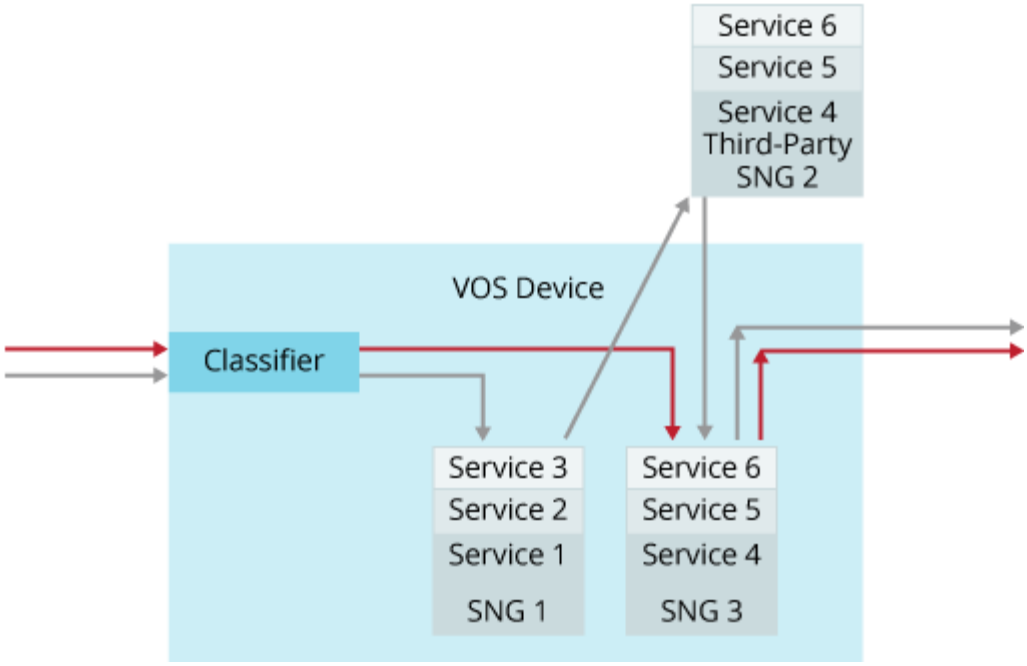

Figure 9. Service Chains with Native VOS *and Third-Party SNGs*

In this illustration, the black traffic flow passes first through SNG1, then through the third-party SNG2, and finally through SNG3. The red traffic flow goes directly to SNG3, bypassing the other SNGs. VOS devices use standard headers, including GRE, MPLS, NSH, and VLAN, to steer traffic to and from third-party network functions.

For virtualized data-center deployments, VOS devices leverage the service-chaining and traffic-steering functions that SDN controllers provide. While you can deploy the native service-chaining and traffic-steering functions of VOS devices in these environments, it is more likely that a data center operator would leverage an already installed SDN solution for this purpose. In these cases, VOS devices leverage the functions of the underlying SDN environment.

Zero-Touch Provisioning

The Versa Networks SD-WAN solution provides zero-touch provisioning (ZTP) functionality to automatically provision and configure new VOS devices.

Versa provides the following methods to provision and configure new VOS devices:

- Global ZTP—Global ZTP uses the call-home feature to connect to a cloud-based Versa Staging server that validates the device owner and then redirects the device to the enterprise's or service provider's staging controller to complete the provisioning process. For authentication with the Versa Staging server, VOS devices use a Versa signed certificate that is stored within a Trusted Platform Module. During the ZTP process, you can replace this Versa signed certificate with a certificate that is signed by your certificate of authority (CA).
- URL-based ZTP—In this approach, the URL of a VOS activation website is emailed to the installer at the customer site. The installer connects a laptop to the WiFi or LAN port of the Versa branch device, clicks on the URL, and then completes the provisioning process.

- Mobile application—You can perform out-of-band provisioning of a VOS device using an iOS- or Android-based application. The handheld device communicates with VOS device over Bluetooth.
- CLI or script—Versa provides a CLI or script-based approach in which you log in to the VOS device and configure the controller address and security credentials. You can use this option before the device is sent to the site location, and an on-site technician can also use it.

Supported Software Information

Releases 20.2 and later support all content described in this article, except:

- Release 21.2.1 supports active–backup mode for Versa Analytics cluster node redundancy.

Additional Information

Solution Architecture
Solution Components
Solution Overview
Solution Use Cases