WHITE PAPER

How SD-WANs are Revolutionizing Satellite Connectivity

By Gerardo Melesio, Jeff Schoch, and Julio Carranza

April 2024

Table of Contents

Introduction

Satellite networks offer their customers several advantages over other types of connectivity. They are easily deployed, reliable, and allow a wide degree of mobility, making them a perfect fit for Disaster Recovery Plans (DRP). Satellite communications are essential in places where other connectivity methods are not available, such as oil rigs, sea vessels, and airplanes. However, they have several characteristics that make them harder to manage when compared to other kinds of networks. This document will discuss those challenges and explore how the a secure SD-WAN solution can help you extract better performance from your satellite links.

Some characteristics that make satellite links unique and challenging are higher latency and limited bandwidth. The available bandwidth is also expensive and is often not allocated symmetrically for upload and download or even along the same path, and the available space and power for networking equipment can be inadequate, especially in remote locations. When deploying satellite networks, a customer must consider all these factors and deploy innovative networking solutions to help overcome them.

The ideal SD-WAN solution provides intelligent link bonding between potentially diverse transport systems, integrating them into a seamless network for the end customer. The network operator can match applications to the path that most closely matches the needs of the traffic patterns as well as provide resilience options. The SD-WAN should also integrate advanced networking functions like TCP optimization and hierarchical class of service (HCoS). Using these services, customers can prioritize the most important applications for their business while optimizing the performance of their connections to their critical services. Finally, by integrating advanced security features into the same operating system, you can consolidate your network and reduce your appliance sprawl.

Satellite use cases and verticals

From cargo and cruise ships to remote terrestrial locations, a secure SD-WAN is ideal for any scenario in various verticals that requires network intelligence and security, including the below.

Maritime and aviation

Long-range and mobile deployments, such as maritime and aviation applications, require satellite links because ships and planes that can travel well beyond the range of cellular and other terrestrial-based radio technologies. These vehicles often have several communication methods and networks that would benefit from a standard management method. Large ships may need to segregate networks into different VPNs, to serve other purposes—for example, crew traffic, internet for passengers, or corporate services. Ideally, the onboard system should detect the best available network path depending on the ship’s location and make the necessary changes automatically.

Remote sites

Although the internet sometimes appears almost ubiquitous, there are still vast areas with no access to fiber, cable, or even cellular networks, due to low population density or the high cost or impossibility of providing such services. Many islands, oil rigs, or remote research facilities are obviously by nature going to depend on satellite communications, but many developing nations also need to use satellite networks while they develop their wired networking infrastructure. Some of these deployments may need multiple private networks that share the same transport links and could benefit from optimization features such as intelligent traffic steering, TCP optimization, and intelligent class-of-service.

Cellular backhaul

Mobile networks are almost omnipresent these days. To work, operators must install cells close to the users so that the wireless signal gets to users adequately. The operators then get the traffic back to their core network, where it can be processed and forwarded accordingly. However, there are remote places where conventional connectivity methods like fiber or microwave links are unavailable. Mobile operators usually depend on satellite links to connect their cell sites in those scenarios.

For the cellular backhaul use case, multitenancy is undoubtedly one of the critical features needed. Operators must isolate traffic from different mobile providers or MVNOs in different VRFs. The ideal solution should enable operators to create both L2VPNs and L3VPNs in a fast, reliable, and automatic way.

Critical SD-WAN features to look for

Route performance monitoring

A performance monitoring system measures many aspects of the paths used for the SD-WAN traffic. The system can enact policies based on jitter, latency, packet loss, or several other measurements to help decide the “best” path for any particular traffic. For example, if a specific application is susceptible to packet loss or jitter, a policy can be put in place to send it over path 1 by default. If rain fade causes packet loss or jitter on path 1 above a certain threshold, then that application will automatically move to path 2.

Route monitoring capabilities can also be very helpful in hybrid environments. For example, in some countries where fiber is in its early days, optical networks have to coexist with satellite networks. Although fiber usually offers higher throughput rates and lower delay, it may be unreliable in new deployment areas. An SD-WAN can automatically switch from one transport network to another, ensuring the connectivity is always working.

Link bonding in hybrid satellite environments

A good SD-WAN solution can be used to bond different satellite links. For example, a customer may have a MEO (Medium Earth Orbit) connection for most of their low latency requirements and a GEO (Geosynchronous Earth Orbit) connection for redundancy. Because GEO satellites orbit much higher than MEO satellites, they naturally incur much higher latencies than the MEO paths. However, the electromagnetic spectrum that the MEO satellites use is more affected by weather conditions.

The SD-WAN can be configured so that, by default, traffic less sensitive to latency will flow over the GEO connection so that the latency-sensitive traffic has more bandwidth available on the MEO connection. For example, data transfer traffic for update services such as Windows Update or storage sites like Dropbox can be forwarded over the GEO connection. In contrast, conferencing traffic services such as Skype or Zoom are forwarded over the MEO path. Policies can also be set up so that in the event of an outage on one of the paths, the less important traffic is blocked to allow more critical traffic to flow.

There may be some situations where a path between two sites cannot use the same satellite connections. Perhaps all the uplink bandwidth for link one is provisioned for other products, but it has downlink bandwidth available. The customer can get their uplink service via link 2. Link 1 will need to have enough bidirectional bandwidth available for control and OAM functions of the SD-WAN path. The ideal solution can tie links 1 and 2 together as two unidirectional traffic paths combined for bidirectional service. The platform should have intelligent tools to apply these bidirectional routing techniques only to specific applications or perform them solely under congestion conditions.

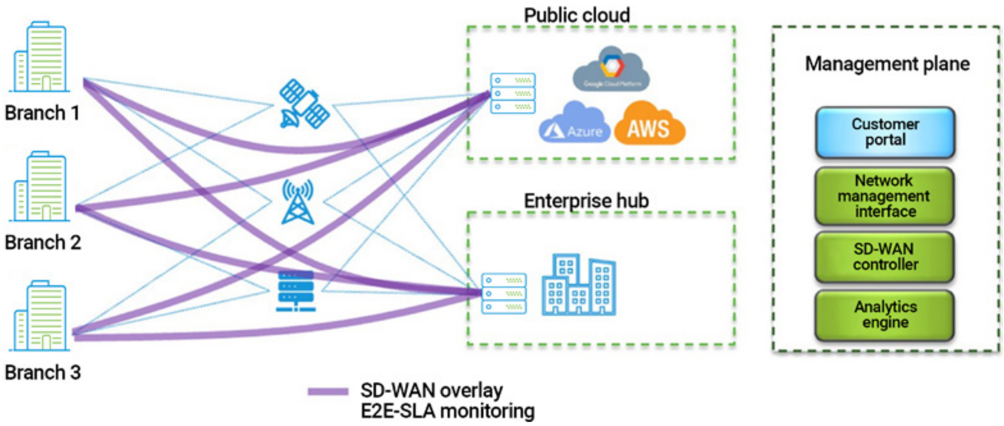

Figure 1 – A secure SD-WAN supports policies based on jitter, latency, packet loss, and several other measurements to determine the best path for any given traffic.

Sometimes, the customer will want to simply use all the available WAN links to utilize their bandwidth fully. A secure SD-WAN can also implement path-weighted round robin to load balance sessions across satellite links with different bandwidths. In a hub and spoke scenario, the hub distributes the sessions considering the download speed of the spoke. The download and upload bandwidths should be configured in the physical or sub-interface in the spoke.

Best path and gateway selection

Although most use cases above assume a fixed data topology, satellite networks also benefit mobile applications such as maritime or aviation. In some mobile applications, combining satellite communications with LTE, WiFi, or other kinds of wireless connectivity may make sense to take advantage of different billing or bandwidth properties when LTE or WiFi networks are in the range.

For example, the SD-WAN can be set up to prefer the shorter range transport when a plane is on the ground and then switch over automatically to the satellite service when it is in flight without needing to change any of the local network settings. The transition from one transport to another is seamless to the end user as the system's abstraction of data plane tunnels, performance monitoring, and a failover mechanism ensures a smooth transition. The same idea applies to ships, which might prefer using an LTE connection when they are close to the port, and then fall back to satellite links once they are in the open sea.

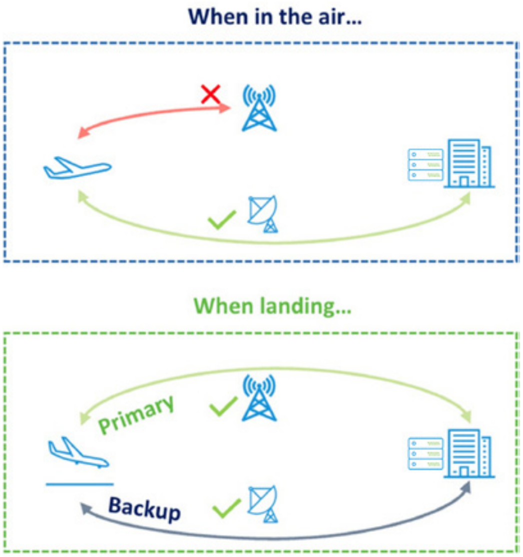

Figure 2 – Seamless, automated switching between connection options based on path performance and location.

Several types of branch SD-WAN applicances have LTE and WiFi modems built directly into the device to simplify the deployment and maintenance of the solution. Also, the user can leverage the available Ethernet ports to connect to an external device.

SaaS application monitoring can be added to enhance the path selection process between multiple local break-out (LBO) paths where the SD-WAN system monitoring is unavailable between branches. Administrators can set up ICMP, TCP, or HTTP monitoring for a specified host and set thresholds for latency or loss on the monitoring profile. These monitoring profiles are then used to determine the best choice between the two internet connections.

For maritime and aviation businesses, and any others with users continuously on the move, SaaS monitors also allow you to choose the best gateway for every application.

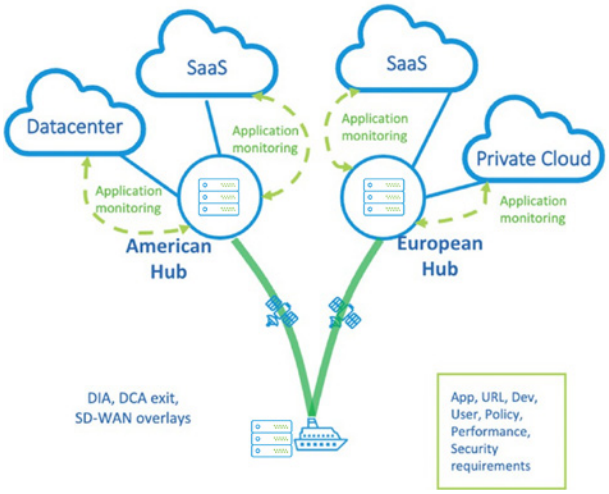

Figure 3 – Application monitoring enhances the path selection process.

Automation

Satellite operators can leverage an SD-WAN offering's REST API infrastructure to develop REST API automation to update the satellite bandwidth using their telemetry. The latter task is essential as satellite bandwidth changes with the location of the mobile deployment on a ship or with the weather.

Another task that satellite operators can automate is to use the GPS to update the location of the SD-WAN device. The latter enables the operators to modify the priority of hubs or links based on the ship location.

TCP optimization

The long latencies introduced with satellite links are a good case for TCP optimization. TCP optimization splits the high-latency TCP session into multiple TCP segments. By enabling the TCP optimization service at one or more points between the client and server, both slow-start convergence and loss recovery times are dramatically improved since the end-to-end latency is split into smaller, independent segments.

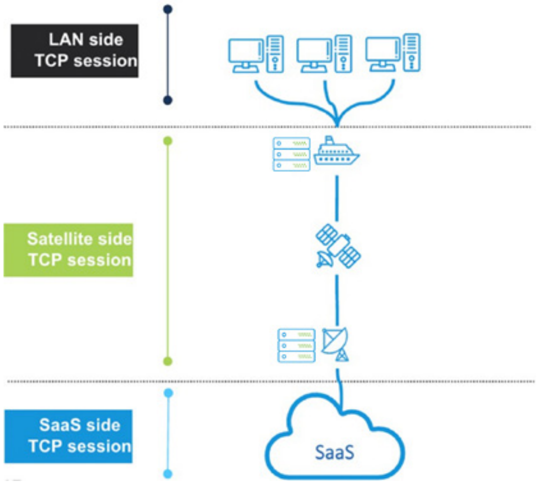

Figure 4 – TCP optimization significantly reduces loss recovery times caused by high latency.

State-of-the-art congestion control protocols can also be implemented to improve the performance of TCP connections, especially when they are subject to high latency or packet loss in the link. There are many congestion control protocols in the industry. Some of them are engineered to achieve high throughput transactions in low-latency environments. Others are designed to get the best output from a link under hardship conditions, such as a satellite link in the middle of the sea. By letting you implement different congestion protocols on different segments of the connection, you can choose the appropriate protocol according to the conditions of the link. Furthermore, you could overcome any client or server limitation, especially in hand-held devices that might have smaller TCP buffers. Typical TCP congestion avoidance protocols include: Cubic, BBR, New Reno, and Hybla.

Quality-of-service and traffic shaping

The limited bandwidth available with satellite transport means that network operators will want to classify their traffic and prioritize the more critical sessions in times of congestion. The ability to match application signatures in the SD-WAN system allows classification and prioritization beyond the traditional patterns of interfaces or IP prefixes. For example, some mobile customers may use a particular conferencing application such as Skype, WhatsApp, or Zoom for meetings or maintenance windows, which requires these applications to be prioritized over other traffic. Class-of-service markings can be updated in the 801.2 P-bit or DSCP bit fields of the outer encapsulation so that the transport network honors the prioritization set by the customer in case of congestion in the underlay.

In addition to shaping local traffic at the physical interface, logical interface, or forwarding-class level, the SD-WAN system should allow a device to signal its configured receive rate to remote devices.

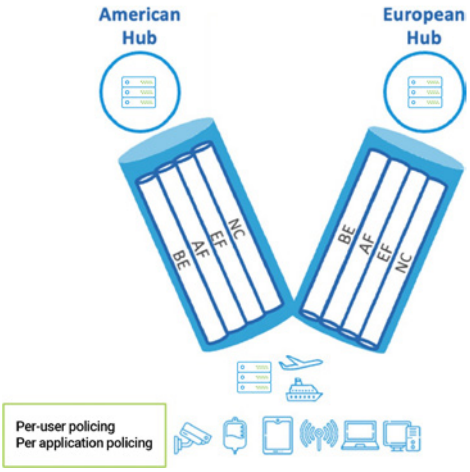

Figure 5 – Hubs can dynamically shape and prioritize traffic from sea vessels and planes to avoid congestion.

In an SD-WAN deployment, adaptive shaping allows a branch or hub device to enforce a dynamic egress shaping rate on any device sending its traffic to force the sending device to limit the amount of traffic it sends. The adaptive-shaping feature tells the remote device to shape traffic to the advertised rate, and then apply a scheduler map so that the quality-of-service policy can be preserved and prevent traffic from using underlay resources dropped at a congested satellite modem. This feature can also be used so that a device can signal to multiple devices to lower their transmit rates when the receiver is being oversubscribed. Using adaptive shaping allows a hub to send traffic to numerous spoke devices without having to manually configure a transmit rate to each spoke, and reduces the number of logical interfaces that would otherwise be needed to control traffic flow to the spokes.

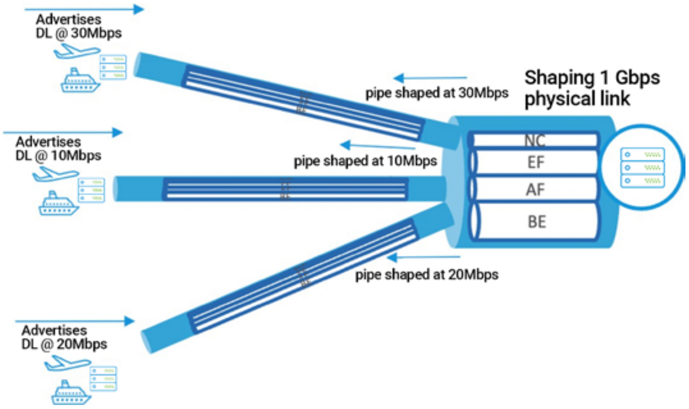

Figure 6 – Adaptive shaping allows hubs to send traffic to spoke devices without having to manually configure a transmit rate to each spoke.

Security features

The SD-WAN should include the ability to integrate security features such as next generation firewall, intrusion prevention, and anti-malware capabilities into the same device. This allows the power and space footprint to be reduced compared to using separate network and security devices, and also allows simpler logistics for a total network solution. Hardware can be added into a greenfield package to bundle SD-WAN and security functions as a single device. The functionality can be added to replace existing security devices in brownfield SD-WAN implementations.

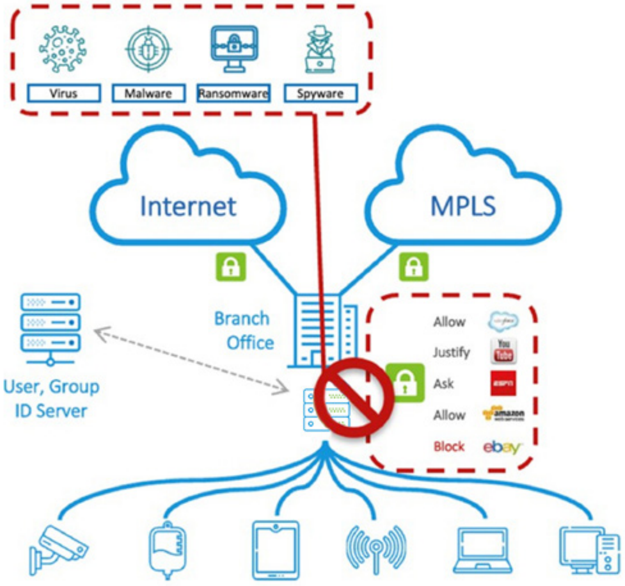

Figure 7 – Comprehensive security features can be added for a total network solution.

uCPE to optimize space and power consumption

Satellite sites are usually located in remote places where operators must optimize the use of power and space. Specific types of uCPE allow the customer to implement different network functions (firewalls, WAN optimization, authentication, etc.) in a single box, leveraging VNFs of other vendors. Usual options for deployment include white boxes, hypervisors, cloud environments, or solution provider-branded boxes that adapt to each customer's needs and requirements.

uCPE
FORTINET
ribbon
JUNIPER NETWORKS
VERSA NETWORKS

Figure 8 – Different network functions (firewalls, WAN optimization, authentication, et al.) can be implemented in uCPE, leveraging the VNFs of other vendors and minimizing equipment power and space utilization.

Analytics

The analytics cluster is the central resource for SD-WAN network reporting. It provides status and statistics for data aggregation, per-port and per-application, to monitor trends over time and report outages on the network. Satellite customers find it helpful to know the latency for tenant endpoints measured per path and value the ability to measure which applications are flowing over particular links so they can fine-tune steering policies. The operators can use APM output information to confirm how applications perform for particular transport paths and to see how much bandwidth any specific application uses.

When security features are enabled on the SD-WAN, the analytics dashboard will also present audit trails for security events related to the security policies enabled in the network. If required, the analytics dashboard can be presented to end customers using role-based access controls for on-demand information specific to that customer. Periodic reports can also be implemented to email a daily health report to end customers automatically.

Conclusion

Satellite networks provide ideal use cases for secure SD-WAN deployments. The strengths of the route performance monitoring combined with the traffic steering policies allow users to always take advantage of the best available paths for their traffic types. The power of bundling security features with SD-WAN devices and uCPE enables a reduction in the overall hardware footprint in deployments where space and power may be at a premium. Intelligent class-of-service features allow fine granularity with classification and scheduling, along with the ability to signal the link shaping configurations via the SD-WAN network, while analytics' tools provide visibility into network operations.

About Versa Networks

Versa Networks, the leader in single-vendor Unified SASE platforms, delivers AI/ML-powered SSE and SD-WAN solutions.The platform provides networking and security with true multitenancy, and sophisticated analytics via the cloud, on-premises, or as a blended combination of both to meet SASE requirements for small to extremely large enterprises and service providers.

Thousands of customers globally with hundreds of thousands of sites and millions of users trust Versa with their mission critical networks and security. Versa Networks is privately held and funded by Sequoia Capital, Mayfield, Artis Ventures, Verizon Ventures, Comcast Ventures, BlackRock Inc., Liberty Global Ventures, Princeville Capital, RPS Ventures and Triangle Peak Partners.For more information, visit https://www.versa-networks.com or follow Versa Networks on X (Twitter) @versanetworks.

Versa Networks, Inc, 2550 Great America Way, Suite 350, Santa Clara, CA 95054
+1 408.385.7660 | info@versa-networks.com | www.versa-networks.com

© 2024 Versa Networks, Inc. All rights reserved. Portions of Versa products are protected under Versa patents, as well as patents pending. Versa Networks and FlexVNF are trademarks or registered trademarks of Versa Networks, Inc. All other trademarks used or mentioned herein belong to their respective owners. Part# WPSDWANSATISPUC-01.1