# Operationalizing carrier-managed SD-WAN deployments

app note

ADVA™ Optical Networking | EXFO

# Operationalizing carrier-managed SD-WAN deployments

app note

Authors:

Ken Gold
Solution marketing leader
EXFO

Prayson Pate
ADVA Optical Networking - Chief Technology Officer
ADVA

## How we got here

Software-defined WAN (SD-WAN) started out as a way for enterprises to gain control of their access costs and has since blossomed into today's killer app for communications service providers (CSPs) looking to transform their network from physical to virtual and to drive new revenue. SD-WAN starts with the benefits that software-defined networking (SDN) brought to core networks – an open, scalable, software-based solution. It then builds on those benefits adding simplified networking, security and policy models that provide overlay VPNs built using low-cost broadband access. The problem for enterprises is that today's SD-WAN puts them in the role of managing their own networks – and that's a job many CIOs do not want.

CSPs are responding to enterprise-managed SD-WANs with their service offerings. The problem is that doing so means using low-cost access – which, in most cases, means low quality. The challenge for CSPs is to maintain or improve service quality in this highly dynamic and quickly evolving environment. Now, more than ever, network and service visibility is critical to delivering a high quality of experience (QoE) to all customers, not just the big ones.

## SD-WAN under the hood

Today, CSPs deliver carrier-managed enterprise WAN or VPN services on MPLS networks, often using expensive, dedicated access facilities. Enterprises see SD-WAN as a way to drive down the cost of their VPNs and get better control of their data.

For the enterprise, some of the key features of SD-WAN include tunneling, "hybrid WAN," and policy control. Tunneling abstracts the VPN topology from the access infrastructure, while hybrid WAN enables enterprises to leverage multiple access methods, such as dedicated T1, FTTx or public internet. Hybrid WAN directs traffic according to policies based on the traffic characteristics and the cost and quality of the links. The policies also dictate access to sites for different users and applications.

SD-WAN is great for the enterprise in terms of cost, bandwidth, and control. But, it also means the enterprise is responsible for maintaining their own WAN infrastructure, including troubleshooting issues across their access provider's network.

Additionally, most SD-WAN implementations are provided by a single supplier, and they use hardware appliances at the customer site. Having a hardware appliance means the enterprise is locked into a single vendor and is at the mercy of that vendor's roadmap. Upgrades are a major logistical headache because they involve scheduling outages after business hours, at multiple sites.

How can enterprises get the benefits of SD-WAN without the headaches?

## The return to carrier-managed WAN

Enter the CSP and managed SD-WAN services. The enterprise can enjoy the benefits of lower cost and application control while offloading the burden of managing the SD-WAN. However, most CSPs are rolling out managed SD-WAN with vendor-specific appliances, and this means there are still the issues of vendor lock-in, upgrade scheduling and lack of flexibility to select best-in-breed applications or new services.

Fortunately, advances in 'white box' hardware appliances have allowed carriers to replace vendor-specific hardware with commercial off-the-shelf (COTS) hardware hosting network functions virtualization (NFV) software. CSPs combine NFV and COTS to build replacements for standard networking appliances, such as a firewall or router. When used at the edge of the network this model is referred to as universal customer premises equipment (uCPE). uCPE replaces traditional customer premises equipment with a single platform and personalizes functionality using software virtual network functions (VNFs). With uCPE, enterprises once again offload the management of the WAN to the carrier, but without the drawbacks of a closed hardware platform. Enhancing or upgrading the WAN service is now as simple as a software upgrade.

Additionally, by using a CSP-managed SD-WAN service, the enterprise gets access to the global reach of the carrier, an evergreen technology solution, and carrier grade robustness.

## Managing the service

There are, however, challenges to realizing the benefits of a managed SD-WAN service offering. SD-WAN leverages NFV and uCPE to remove vendor lock-in, provide an open platform for best-in-breed applications and deliver the ability to evolve services and bandwidth without truck-rolls. At the same time, breaking up appliances means it's more challenging to guarantee the performance of the service. Previously, the operator (CSP or enterprise) built a service using a well-architected, monolithic implementation, with thousands of hours of QA testing. Now, new services are based on a collection of disaggregated functions that interact through a set of published application programming interfaces (APIs) and are often made using a DevOps approach. Consequently, basic tools like end-to-end service visibility and network quality monitoring need to become part of the NFV toolset and designed into the service, rather than integrated into the appliance. The dynamic nature of SD-WAN demands an orchestrated service assurance solution built into the service chain and constantly monitoring service integrity, even as the service changes due to customer-initiated enhancements, network or service optimization, or fault recovery.

## Orchestrated service assurance

As with any managed service, the CSP needs to follow well-accepted operations processes, both when turning up the SD-WAN service and after handing it over to the customer. The difference with software-defined services, however, is that a service orchestrator, rather than a human, automatically turns up and hands over the service.

In SD-WAN, services are built by connecting, or chaining, specific VNFs together to form a service chain. It is the service chain that defines the specific features of a service, such as traffic classification or policing, and the order in which these features are arranged. When a new managed service is established, the CSP will validate it using a service activation test (SAT) such as Y.1564. Doing so will ensure the service was properly built (service chain integrity) and that the network can deliver the service as defined. Once verified, the service can be turned over to the customer.

The service may then be monitored to ensure it continues to operate as defined. For this, various tests are available. For example, operators track basic Layer 2 or 3 functionality, such as end-to-end connectivity, latency or jitter, using protocols like RFC 5357 Two-Way Active Measurement Protocol (TWAMP) or Y.1731. Additionally, higher-level application performance monitoring functionality, such as VoLTE call quality or video delivery quality, may require other test capabilities.

As part of the service orchestration function, specific test or monitoring VNFs can be installed in the service chain and activated to perform the required tests. In the case of SAT, the VNF could be installed during service instantiation and then removed prior to turning the service over to the customer. For ongoing service monitoring, the VNFs can be added during service instantiation or at any time after turning over to the customer. For services that have a service level agreement (SLA), monitoring would be there all the time. Additionally, monitoring VNFs could be added during trouble-shooting to provide the network or service operations teams with specific diagnostic information.

As a matter of best practice, the CSP may choose to monitor all services all the time. Because SDN and SD-WAN abstract the service topology away from the physical topology, the only way to truly know if a service is working properly is to monitor it continuously. This breaking of the 1:1 relationship between service and network topology means you can no longer infer the quality of a service from the quality of the network. Additionally, by generating key performance indicators (KPIs) on all services all the time, and by leveraging big data analytics, the CSP will be able to proactively detect subtle changes in network and service performance and address them, possibly before the customer notices.

Automating SAT and service assurance through the service orchestrator has the additional benefit of guaranteeing consistency in coverage and results, and is required to support the massive scaling anticipated in next-generation, 5G and IoT networks.

## ADVA + EXFO: a partnership for orchestrated service assurance

As industry leaders in the fields of SD-WAN service orchestration and service assurance, ADVA and EXFO are in a unique position to offer a combined solution that allows CSPs to deliver a best-in-class SD-WAN managed service offering.

**ADVA** provides a comprehensive set of hardware and software products to simplify network virtualization.

Within ADVA, Ensemble is a full network functions virtualization (NFV) software architecture. It includes the following components that can work together or separately as needed.

- **Ensemble Connector**: High-performance network operating systems and virtual network function (VNF) hosting platform with device management and CE 2.0 features
- **Ensemble Orchestrator**: ETSI MANO NFV orchestrator and VNF manager
- **Ensemble Controller**: SDN controller based on Open DayLight
- **Ensemble Director**: FCAPS system

The key benefits of the Ensemble suite include:

### Networking

- Fast and light forwarding engine with high performance on low-end servers
- L2 or L3 VPN over anything
- Encryption in software

### Operations

- Zero touch provisioning
- All cloud deployment models
- Upgraded management for CPE

### Choice

- Largest ecosystem of VNFs
- Largest set of supported compute platforms / BYOH
- Neutrality

ADVA also provides NFV hardware in the form of its FSP 150 series. These include the ProVMe and XG304u hybrid NIDs and the ProVMi hardened server.

**EXFO**, a leading supplier of network testing, monitoring and analytics solutions, provides a complete line of products for assuring applications and services in virtual, hybrid or traditional networks.

EXFO service assurance solutions for SD-WAN are designed to be easily integrated into service orchestration platforms, such as the ADVA Ensemble solution. The EXFO solution consists of the following software products:

- **EXFO Virtual Agent**: Service assurance application for mobile devices
- **vVerifiers**: Virtual probes (VNFs) that provide service assurance functionality for Layers 2-7
- **Physical verifiers**: Physical probes that can be installed at fixed endpoints (hybrid network)
- **EXFO Worx**: Test controller for setup and management of service activation and service assurance tests, with APIs for interaction with end-to-end service orchestrators
- **EXFO Xtract**: Analytics platform for fault detection and correlation
- **EXFO Ontology**: Automated service topology mapping and active inventory management to maintain an accurate view of the SD-WAN and provide automated common cause analysis for assisting in root cause determination involving multiple faults

The key benefits of EXFO's service assurance solution include:

### Operations

- Zero touch provisioning support
- End-to-end service and application visibility
- In-service upgradable test functionality

### Choice

- Over 50 monitoring and testing solutions spanning Layers 2-7
- Standards-based testing for interoperability with third-party probes
- Vendor-agnostic, end-to-end service and application monitoring

EXFO service assurance solutions are available as software applications and VNFs, for entirely virtual implementation, or as platform based for hybrid and traditional networks.

## Conclusion

Managed SD-WANs provide significant benefits to both the CSP and their enterprise customers. These customers get an open, secure, scalable, future-proof platform that leverages lower-cost access facilities without burdening their IT departments with the management of the WAN network. The CSPs get an attractive, managed service offering that allows them to compete against emerging providers and retain their enterprise customer base.

Maintaining or enhancing service quality will be critical to a successful transition to SD-WAN. The nature of an open, VNF-based solution requires a different approach to network and service assurance since service quality can no longer be inferred from network and equipment quality metrics. By including service assurance VNFs in the service chain, the service orchestrator can automatically test and verify a service before turning it over to the customer and can implement end-to-end service monitoring, based on policy or operations' needs. Automating these functions is the only way to address the anticipated scaling of new 5G and IoT services.

By combining their industry-leading solutions, SD-WAN orchestration and orchestrated service assurance, ADVA and EXFO enable CSPs to deliver on the promise of SD-WAN – a fully managed, lower-cost, open enterprise WAN solution that delivers a better quality of experience than appliance-based solutions.