HOW ADVANCED ANALYTICS DIFFERENTIATES CSP SD-WAN SOLUTIONS

Jim Metzler, Vice-President, Ashton-Metzler & Associates

Introduction

Today's most commonly used branch office WAN architecture was initially implemented around the turn of the century. This architecture is based on the use of MPLS for connectivity and the presence of high-priced, hardware-based appliances at each end of a WAN link to provide functionality such as optimization and security. Unfortunately, because of the engineering required to deploy a new circuit, MPLS is not only an expensive service but it also involves long lead times. That may have been tolerable in the pre-iPhone business environment of the early 2000s, but in today's fast-paced, super-connected world it's no longer acceptable.

One of the primary reasons that the turn-of-the-century WAN architecture has lasted so long is that until recently no fundamentally new WAN technologies or architectures had been introduced into the marketplace. That situation began to change a couple of years ago with the introduction of a new class of WAN solutions that is typically referred to as "Software Defined WAN" (SD-WAN). Because they support dynamic load balancing of traffic over multiple WAN links, the primary value proposition associated with SD-WAN solutions is that they enable network organizations to reduce the cost of their WAN by either reducing or capping their use of MPLS and leveraging the low cost and rapid deployment of Internet bandwidth.

The potential reduction in MPLS revenues is just one source of the pressure facing CSPs.

While there is no doubt that the emergence of SD-WANs is a threat to Communications Service Providers (CSPs), it is also an opportunity, and numerous CSPs around the globe have begun to respond accordingly. Some CSPs have embraced SD-WAN concepts as part of offering a Network-as-a-Service (NaaS) solution while others have included SD-WAN functionality acquired from a vendor as part of a managed SD-WAN solution.

As part of their response to the opportunities that SD-WANs present, many CSPs are architecting their SD-WAN solutions based on network function virtualization (NFV) architectures. Many of these solutions include, for example, virtual CPE (vCPE), either on a customer premise, in a central office, or in a datacenter. The vCPE they are deploying consists of commodity hardware, a hypervisor, and a number of virtualized network functions (VNFs), such as firewalls and WAN optimization controllers. Unlike the hardware-based appliances that are part of traditional branch office networks, VNFs can be more easily provisioned and deployed, and they can be more readily priced on a pay-as-you-go, pay-as-you-grow basis. As such, vCPE-based SD-WAN solutions position CSPs to increase revenue by providing a range of networking functionality in addition to transmission services.

The potential reduction in MPLS revenues is just one source of the pressure facing CSPs. They also face a large and growing challenge from Over The Top (OTT) players that leverage the CSPs' own networks to compete against them in offering a wide range of services such as unified communications.

The goal of this white paper is to discuss how advanced analytics capabilities enable CSPs on two crucial fronts: to successfully differentiate their SD-WAN solutions and to compete more effectively with OTT players.

SD-WAN Deployment Offerings

As customers adopt SD-WAN, one of the deployment choices they face is whether to implement an SD-WAN on a Do-it-Yourself (DIY) basis or to adopt a Network-as-a-Service (NaaS) or a managed service option. In a DIY solution, the customer is responsible for the entire lifecycle of their WAN, meaning the planning, designing, implementing, and managing of all components. As discussed below, many customers don't want to take on that responsibility, so they choose either a NaaS or a managed service solution.

With a NaaS solution the customer is freed from the responsibility of planning, designing, and implementing their WAN, but in most cases they can still actively manage it via a portal. Managed Service Providers (MSPs), on the other hand, typically acquire and implement the same SD-WAN functionality as an enterprise network organization, and they leverage that functionality to provide their customers with a turnkey solution that includes active management. In the vast majority of cases, however, the MSP also provides a portal that enables the customer to at least monitor their network and, in many cases, to make changes.

In our analyst ebook The 2017 Guide to WAN Architecture and Design we included the results of a survey question that was designed to determine the interest that enterprise organizations have in each of the SD-WAN implementation options. Participants were asked, "If your organization were to adopt an SD-WAN, which implementation option are you most likely to implement?" Their responses are shown in Figure 1.

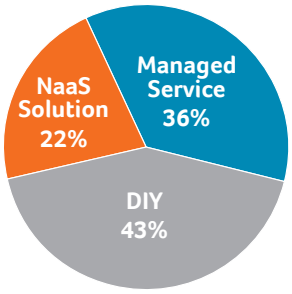

Figure 1: SD-WAN Implementation Options

While there is strong interest in a DIY approach to implementing an SD-WAN, there is a notably stronger interest in involving a 3rd party, whether that is a provider of managed services or of a NaaS solution.

In the traditional branch office WAN architecture, most if not all of the WAN functionality is provided on the customer's premises. When deploying an SD-WAN, however, that functionality can be housed in many more places. In our ebook The 2017 State of the WAN Report we presented the results of a survey in which the respondents were asked to indicate where their organization thinks that WAN functionality should be located. Their responses are shown in Figure 2.

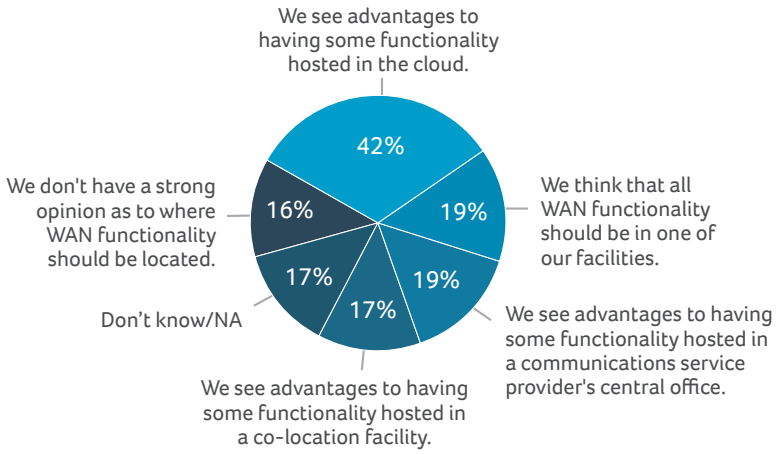

Figure 2: Location of WAN Functionality

One of the interesting observations that can be drawn from these results is that, going forward, relatively few network organizations believe that all WAN functionality should be housed on site. Another such observation is that by a very wide margin, the most popular place that the survey respondents believe that network functionality should be housed is in the cloud.

Using Advanced Analytics to Differentiate SD-WAN Offerings

Enterprise customers are very receptive to managed SD-WAN and NaaS offerings. But unfortunately, that doesn't necessarily favor CSPs. In order to preserve their share of the WAN market, CSPs will need to go beyond me-too offerings and find real points of differentiation.

The 2017 State of the WAN Report contained the results of a survey in which the respondents were given a lengthy set of factors and asked to indicate which three would be the primary factors that would cause their organization to make significant changes to their current WAN architecture over the next twelve months. Given the high monthly cost associated with a WAN, it's not surprising that reducing cost was the most important factor.

Since the primary value proposition associated with SD-WAN solutions is that they enable network organizations to reduce cost, SD-WANs are well positioned to respond to the key issue driving change in the WAN. It is highly unlikely, however, that a given SD-WAN solution will enable notably more transmission savings than other similar solutions. That fact, combined with the reluctance on the part of CSPs to aggressively advocate for solutions that reduce their MPLS revenues, means that few if any CSPs will differentiate their SD-WAN offering based on a race to zero transmission costs.

Insight into how CSPs can differentiate their SD-WAN offerings comes from examining the two factors that were tied for second place in the previously mentioned survey about driving change in the WAN. One of these two factors was supporting real-time applications such as voice and video. The other was increasing security.

Regarding real-time applications, one of the challenges of SD-WAN is its dependence on internet links that may be any number of ISP hops (Autonomous Systems) away from a critical campus, datacenter, or cloud provider. While MPLS and internet links traverse the same underlying fiber

transport connectivity, the variability of traffic and routing behavior on the internet can create more unpredictable impacts on application and service delivery. SD-WAN solutions typically measure the relative performance of multiple internet or MPLS links and can favor higher-performing links for more sensitive applications. However, just knowing that real-time applications are getting the best local option doesn't mean that they are getting acceptable end-to-end performance. A value-added service portal that leverages advanced analytics that help find and solve end-to-end performance issues, including pin-pointing internet root causes, is a differentiating capability that enterprise IT buyers will welcome.

To win the SD-WAN game, service providers need advanced analytics that unify rather than silo data.

As for security, this is an area where most vendor-supplied SD-WAN solutions are relatively weak. While they typically offer encryption and enable customers to make more economical use of firewalls, they don't protect against threats such as DDoS attacks. Real-time traffic analytics can holistically detect DDoS attacks across connections including campuses, datacenters, and branch office/retail locations, and can trigger centralized mitigation measures. CSPs can differentiate their offerings by including DDoS protection for SD-WAN connectivity.

Bundling DDoS protection with SD-WAN services showcases how CSPs can differentiate their SD-WAN solutions by leveraging their broader service portfolios. Another cross-service bundling opportunity is cloud-connect services to help SD-WAN users to gain better performance from critical IaaS, PaaS, and SaaS providers.

Legacy Network Management Approaches Are Insufficient

We've seen how advanced analytics can support differentiation, but unfortunately CSPs will not be able to effectively differentiate their services if they have access only to traditional, siloed management and analytics tools. Without integrating deep, real-time, Internet- and performance-aware analytics into their network operations, CSPs won't have the network traffic intelligence needed to make sound recommendations for cloud-connect services, to offer pervasive DDoS protection, or to provide performance insights to enterprise buyers.

The traditional approach to management and analytics typically involves collecting, storing, accessing, and analyzing management data within individual service, technology, or use case domains. Traditional management tools are deployed on single-server appliances that, even when federated, have severe compute and storage limitations, which means that the high volume of data generated by network elements must be rapidly summarized to keep a useable history.

Because summarization is based on use cases, it is common that several tools are each collecting largely the same network data while retaining completely different summary data snapshots that can't be cross-correlated. Each tool is in a sense, an island. Unfortunately, these islands are at best highly inefficient and in most cases wholly un-useable for revealing deep insights, accurately defending against DDoS attacks, and adding value across service offerings.

To win the SD-WAN game, service providers need advanced analytics that unify rather than silo data. By collecting end-to-end service delivery data — traffic flows, routing, performance, geolocation, and DNS — across a provider's entire range of infrastructure and services, then unifying that data into a complete, correlated whole, advanced analytics provides a platform for valuable real-time decision-making and service creation.

Unifying various types of end-to-end network data requires cloud-scale approaches that can accommodate the huge volumes of information that must be continuously and pervasively gathered and stored. A big data approach is necessary to enable ad-hoc analysis of huge data sets both in real time and historically. An advanced analytics architecture must also support multi-tenancy to ensure that the actions of one customer, or a group of customers, doesn't negatively impact other customers.

Unlike a traditional management solution, an advanced analytics solution for CSPs must also have scalable and open APIs. This will enable a CSP to integrate advanced analytics with other OSS and BSS applications and will foster more productive data sharing across organizations.

Summary

The potential to reduce MPLS revenues makes SD-WANs a threat to CSPs. But by aggressively adopting advanced analytics, CSPs can respond by building differentiated SD-WAN solutions that minimize or eliminate the overall reduction in WAN service revenues. They can also grow revenues by offering SD-WAN functionality bundled with end-to-end performance visibility, DDoS protection, and cloud-connect services.

Beyond preserving critical WAN service revenues, investment in advanced analytics also offers a major strategic benefit: raising the long-term competitiveness of CSPs relative to OTTs. By developing a culture of data mastery, CSPs set the stage for increasing levels of network automation, operational efficiency, and service creation agility. In the long term, the benefits of an analytics-driven transformation may well prove to be existentially important for CSPs.

ABOUT KENTIK

Kentik is the network traffic intelligence company. Kentik turns network traffic – billions of digital footprints – into real-time intelligence for both business and technical operations. Network operators, engineers, and security teams use Kentik to manage and optimize the performance, security, and potential of their networks and their business. To learn more about Kentik and its award-winning solutions, visit www.kentik.com.