GlobalData.

The Customer Journey to SD-WAN

Functional, Technical, and Economic Considerations

Part 2: SD-WAN: Is It Right for Your Network?

Technology

Joel Stradling, Research Director
joel.stradling@globaldata.com

Sponsored by

TATA COMMUNICATIONS

Published: December 2016

Summary: Software-Defined Wide-Area Networking (SD-WAN) can offer a number of advantages over traditional networking techniques for enterprises moving to virtualized IT environments. This paper reviews the main architectural options open to enterprises considering the adoption of SD-WAN, and their technical, functional, and economic attributes, to help networking teams to decide if SD-WAN is the right choice for them.

SD-WAN: Is It Right for Your Network?

Amid the flurry of SD-WAN product introductions from networking vendors and SD-WAN service launches by WAN service providers, many enterprise networking teams are asking the question: Is SD-WAN the right solution for our network?

GlobalData Technology research has identified some key determinants that early adopters of SD-WANs have used to justify – or not justify – the use of SD-WAN within their network:

1) **Are your IaaS/SaaS/PaaS solutions performing according to spec**? If so, then there's not necessarily a need to deploy new networking technology such as a software-defined WAN. If not, then a new solution might give better cloud app performance and flexibility.
2) **Do considerable changes in the network need to be made on a continuous or ongoing basis?** These changes may include technical changes as well as commercial ones. This point also relates to the overall evolution of IT towards pay-as-you-go. If the pay-as-you-go model is attractive in the organization, then SD-WAN solutions will help to achieve this compared to more static and traditional IP/MPLS VPNs.
3) **Do we have mission-critical applications that are bandwidth-hungry or particularly jitter-sensitive and which need to be secure and free of congestion or quality of service issues?** Organizations that have adopted SD-WAN have reported an enhanced ability to segment off portions of the network to address quality of service issues resulting from congestion on 'peaky' traffic from apps using voice or video.
4) **Do we have a large number of remote sites with multiple WAN links, or are we planning to?** For larger networks with multiple sites and WAN links, SD-WAN functional and economic advantages can be compelling. However, with a smaller number of sites or if a majority of sites are singly connected, the advantages are harder to identify.

Architecture Choices: Three Options

If SD-WAN seems to answer one or more of these key questions, then it's worth taking a closer look at the options to deploy SD-WAN in your network. Three approaches can be considered, making more or less use of existing routing equipment and virtual CPE (vCPE) or universal CPE (uCPE):

- **Deploy an overlay SD-WAN solution leveraging the existing IP router footprint**
    - If the enterprise has a major existing IP router estate then it may wish to preserve the existing equipment and leverage an overlay solution for implementing SD-WAN. The overlay solution offers the ability to failover to the traditional WAN setup in case there are issues with the SD-WAN infrastructure.

- Overlay solutions may lack capabilities in aligning existing OSS/BSS platforms in place with the service provider, meaning a loss of some flexibility for billing and flexible payment for utility SD-WANs.
- This approach will also require efforts for the existing WAN – be that IP VPN or Ethernet VPN, as well as implementing policy routing and on-going service chaining.
- Some routers available in the market today can support per-flow path forwarding based on link performance and application policy, and network and application monitoring.

- **Deploy a mixture of existing IP routers and vCPE/uCPE**
  - The vCPE or 'thin CPE' involves the virtualization of CPE, and this runs in the cloud.
  - uCPE – or 'Universal CPE' is a site-based Intel server module that can support physical networking such as being a branch router for multiple WAN interfaces including 3g/LTE, and be remotely manageable for running for example VNFs and hosted business communications like media gateways for SIP interoperability, etc .
  - Most enterprise customers will want to explore a blend of existing IP VPN architecture with some aspects of the WAN, featuring core SD-WAN based on core SDN/NFV and vCPE/uCPE. Such deployments might begin with the SD-WAN architecture initially focusing on automating IT between HQ sites and the data centres where cloud apps are being served from.
  - Some of the technical issues mentioned in the overlay architecture are likely to apply to this mixed set-up scenario, such as lack of support for fully integrated orchestration of the OSS/BSS functions.

- **Deploy full SD-WAN based entirely on a new appliance, x86 server, or gateway on site, or on vCPE/uCPE**
  - Virtualized software runs on x86 as a VM or containerized solution.
  - The SD-WAN benefits from central orchestration and policy-based routing control.
  - Enterprises adopting the full SD-WAN approach may employ the full range of SD-WAN features, including intelligent path selection, policy management, full automation, integration with OSS/BSS, zero touch deployment and security functions like IPsec VPN and firewalling.

Enterprises also need to consider whether to use a virtual SD-WAN controller in the cloud, or premises-based SD-WAN controller software. This choice tends to be sector-specific. For example, banking and financial firms today tend to prefer premises-based controllers since financial firms more often run private MPLS environments; whereas retail chains, which favor public Internet and broadband links, may opt for cloud-hosted SD-WAN controller solutions.

Key Use Cases for SD-WAN: Technical, Functional, and Economic

Technical

Traditional WANs are not Architected Specifically for Running Cloud Apps – Most SD-WAN solutions in the market focus on solving business connectivity that demands among other things major use of services from within the cloud. Traditional IP/MPLS VPNs have adapted and evolved to feature connectivity to cloud estates, including both private and public clouds but there remain certain limitations on performance (i.e., scaling bandwidth) and app priority parameters over public Internet. Hybrid WAN solutions do offer APM and WAN optimization features, but for more comprehensive applications control, it is important to be able to understand how apps are behaving in the network and to be in a position to tailor or tweak SD-WAN parameters to maintain the apps running in the cloud in an efficient working fashion. Enterprises are right to

expect a self-serve interface within an online portal that allows them to make changes – and behind the self-serve feature lies automation so that changes do not demand intensive manual actions.

Functional

Adding or removing sites – There are too many manual procedures for implementing such changes at the branch. Often a large enterprise will need to scale or shrink operations and this requires new office locations and end-users to be integrated with the existing WAN. The new SD-WAN environment should support the addition of new sites rapidly over multiple access types, such as leased line, Internet access, MPLS, 3G/4G LTE, and broadband. Provisioned circuits and interconnections need to meet the corporate security policy and be documented as per governance rules. SD-WAN services demonstrated that moves, adds, and changes can be performed more conveniently and with fewer complications that might arise from say re-writing CLI scripts from scratch for every site. Policy driven SD-WAN configurations combined with automated policy selection and configuration enable zero-touch provisioning for drop-shipped CPE devices on existing IP routers or via universal CPE (uCPE). SD-WAN techniques such as these reduce human errors that creep into networks configured with manual configuration steps.

Try before you buy and Rapid Provisioning – MPLS does not offer the flexibility or agility for quickly deploying changes and for example trying out features for a short duration before committing to buy. SD-WAN solutions increasingly support more choice of virtual network functions (VNFs) and both solution architecture and VNFs running over the test network design give engineers far greater flexibility for testing the network and the performance of cloud apps on the network before scaling to a full deployment.

Economic

Scaling MPLS Can Take Time and Drive Up Costs – how can a new network solution help bypass the current inflexible nature of MPLS circuits? The central orchestration software for an SD-WAN should provide the systems administrator or network engineer with an interface that supports quick changes to circuit design and performance parameters.

SD-WAN: Differences with Traditional MPLS WANs

Attributes	SD-WAN	Legacy WAN
Provisioning	Zero-touch provisioning	Manual provisioning
On-demand app support	Try before you buy & pay-as-you-go IT	Inflexible platform for trying out new configuration and services for a short period
Configuration changes	Automated features	Manual procedures
Orchestration	Central orchestration	Many disparate parts to the network including hardware CPE, provider edge, core
Support for Cloud application architecture	Cloud ready	Not necessarily architected from the outset for cloud and virtualization
Security capabilities	Security mechanisms can be deployed quickly	MPLS is perceived as highly secure
Scaling properties	Scale solution components horizontally	More static traditional fixed components (for example non-hosted in the cloud)
Change processes	Security and Compliance changes	MPLS is highly secure and compliant, however making policy changes and expanding or shrinking requires more manual processes
Availability and Redundancy	Availability and redundancy for cloud apps, including over public Internet and private clouds	MPLS has good characteristics for availability and redundancy (providing of course back-up circuits are present) for site, edge, and core transport, but may not meet demands for heavy cloud-based traffic routing and app control between clouds and over the Internet
Security features	SD-WAN solutions support security segmentation in cloud and virtualized IT	Security features are static, spin-up of virtual VNFs such as firewall possible but integration is required
Path control and selection	Flexible path control/selection inherent in SD-WAN in most cases	Path control and selection is possible but demands integration and overlays, and more manual processes that are more prone to problems arising from human error
WAN provider choice	WAN provider independent	Tied to specific WAN providers
Policy-based management	Simplified policy based operations for multiple functions like application performance, security, and connectivity	Enterprise has to manage multiple devices and services
Management options	Self-managed or Provider managed	Provider managed