Independent market research and competitive analysis of next-generation business and technology solutions for service providers and vendors

HEAVY READING WHITE PAPER

SD-WAN Implementation & Differentiation Layer Strategies

A Heavy Reading white paper produced for Juniper Networks Inc.

AUTHOR: JIM HODGES, PRINCIPAL ANALYST, HEAVY READING

INTRODUCTION

One of the clear outcomes associated with the commercialization of network functions virtualization (NFV) is that the adoption of advanced virtualized software techniques will usher in a new age of programmable service innovation. Since NFV and the cloud address all layers of the network, the impact will be profound, as illustrated by the many relevant use cases that have emerged over the past few years.

One such leading use case is software-defined wide-area network (SD-WAN). There are several reasons for SD-WAN's market momentum, but the key considerations are that SD-WAN provides enterprise customers with a programmable, evolvable and lower-cost alternative to Multiprotocol Label Switching (MPLS); while for communications service providers (CSPs), SD-WAN enables new revenue streams and empowers service differentiation in a mature enterprise marketplace. SD-WAN also allows CSPs to target new market segments, including on-net and off-net customers in new geographic markets where traditional cost structures have thwarted network deployments.

However, SD-WAN is still very much an emerging technology, which means that multiple implementation and monetization questions remain outstanding. Accordingly, the purpose of this white paper is to detail the technical factors that must be addressed to achieve a successful SD-WAN implementation. Areas relevant to the discussion include security, orchestration, integration, network management and their linkage to customer requirements.

To fully capture the impact of these factors, this white paper presents key findings from a major survey created by Heavy Reading in collaboration with Juniper Networks. The survey, which contained 30 questions, was promoted in the second quarter of 2016 and received input from a global mix of 93 qualified high-value CSP respondents.

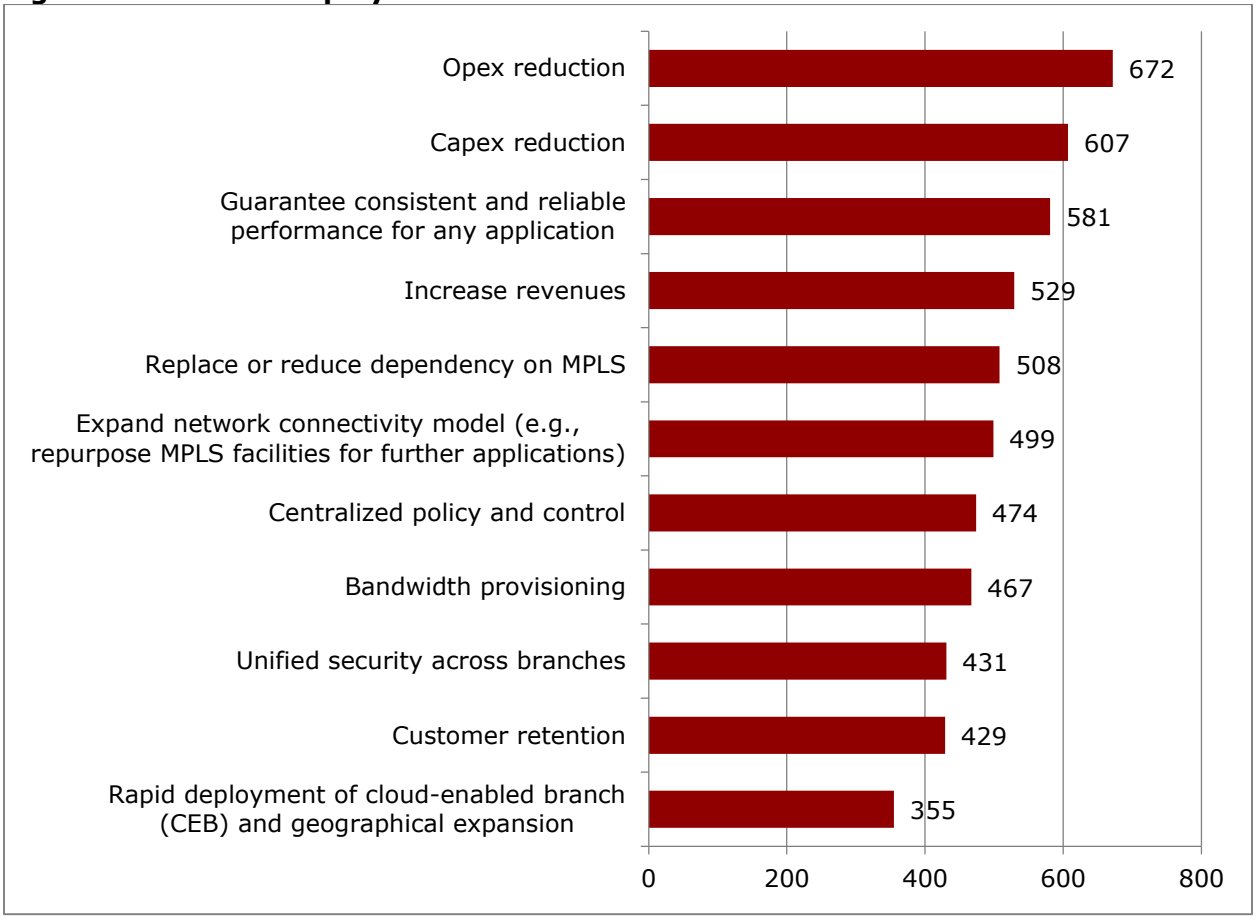
SD-WAN BUSINESS & TECHNICAL DRIVERS

As noted, SD-WAN's flexible, programmable design methodology represents a strong value proposition, enabling a cogent mix of technical and business drivers. These drivers in many respects generically embody the criteria that CSPs have defined for assessing successful cloud deployments. They are multi-layer, address security requirements of cloud connections, rapid deployment requirements, application enablement, as well as supporting the introduction of lower-cost self-care operational models.

Consequently, as shown in **Figure 1**, CSP input confirms that SD-WAN is strongly aligned with the criteria for cloud success on many levels. The top two drivers – opex and capex reduction – are not surprising, as they pragmatically reflect an industry-wide consensus that bandwidth growth will demand new business and technical models to most effectively monetize the cloud.

Since SD-WAN supports the ability to offload traffic to the Internet, the cycle of capex-heavy core capacity upgrades is reduced or eliminated. Similarly, SD-WAN can significantly reduce opex by leveraging programmability traits to enable zero-touch provisioning, which eliminates truck rolls by using customer self-care portals, centralized policy management and real-time analytics.

Figure 1: SD-WAN Deployment Drivers



Question: Please rank the following SD-WAN deployment drivers in order of importance.
Source: Heavy Reading, Juniper vCPE and SD-WAN Custom Survey, 2Q16 (N=92)

In addition to these two drivers, CSPs also rank other factors highly. For example, the third-place ranking of "guarantee consistent and reliable performance for any application" is a strong endorsement that, with SD-WAN, enterprises can still achieve the benefit of MPLS for those applications requiring it, but also leverage Dedicated Internet Access (DIA) or standard broadband for Internet traffic and cloud applications.

One such use case is virtual customer premises equipment (vCPE), which is also driven by the need to achieve service innovation at lower price points, without sacrificing business continuity and carrier-grade reliability. Thus, in many cases, vCPE and SD-WAN initiatives are happening simultaneously, to enable CSPs to leverage the power of the distributed model and maximize investment return.

However, the scoring of other features highlighted in the figure shows that other strategic and adjacent key attributes are also driving SD-WAN deployment. These include:

- Replace or reduce dependency on MPLS
- Centralized policy and control
- Unified security across branches

Since SD-WAN is often characterized as a disruptive, lower-cost approach for re-architecting the WAN at the expense of MPLS, it's not surprising that CSPs are focusing on SD-WAN to reduce dependency on their MPLS business.

Still, given that the deployment of SD-WAN will be gradual, SD-WAN must also be designed with the mandate of supporting an intelligent hybrid model that integrates MPLS and SD-WAN to maintain support of traditional service-level agreements (SLAs). Another, related benefit is that the continuous monitoring of applications for SLA enforcement will also allow CSPs to differentiate on a service and customer experience level.

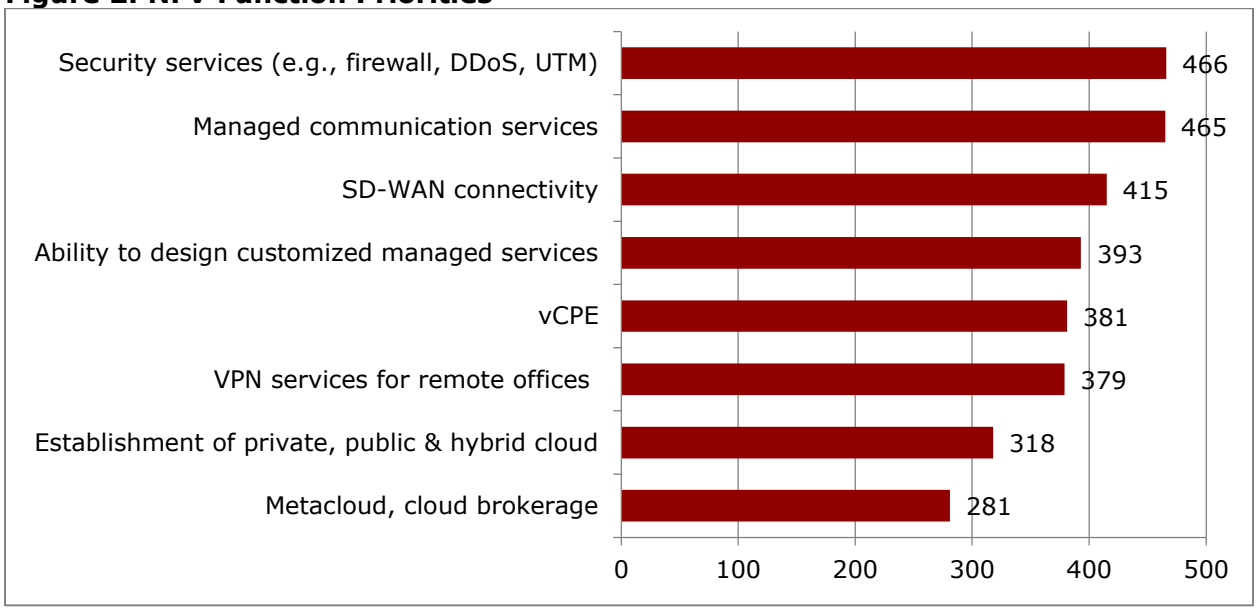
Another attribute that must be addressed is centralized policy and control. There are several factors in play here, but the key consideration is that policy control provides the functionality that unleashes the power of cloud programmability. This includes not only defining policies to empower application enablement via orchestration, but also the creation of security policies to ensure that an SD-WAN implementation supports dynamic provisioning and enforcement of unified security policies across *all* enterprise branches.

SECURITY & THE SD-WAN

In order to shed additional light on the relationship between SD-WAN and security, this section of the white paper considers SD-WAN security requirements on a more granular level, as well as the opportunities for CSPs to leverage security to achieve market differentiation.

As a starting point, it's important to clarify that security is not simply an SD-WAN issue, but rather a crucial topic that must be addressed for any NFV-based cloud implementation. For example, as shown in **Figure 2**, in the context of the importance of various virtualized network functions (VNFs), CSPs identify security services as their top priority.

Figure 2: NFV Function Priorities



Question: Please rank the following VNFs in order of importance to your company.
Source: Heavy Reading, Juniper vCPE and SD-WAN Custom Survey, 2Q16 (N=90)

The top four inputs reinforce the strong level of interplay between virtualization and security services from the perspective of both service differentiation and network requirements. Stated another way, the responses show that SD-WAN is redefining both network design and the managed services delivery model.

There are several factors to consider here. First, while security is a well-documented factor for all VNFs, SD-WAN introduces new security demands. One of the leading factors is that MPLS security is very different from securing the SD-WAN. For example, MPLS networks do not typically support encryption, since the network is provisioned to emulate a private network connection, and is therefore assumed to be secure.

In contrast, as a purely software-based implementation, SD-WAN requires encryption to ensure secure access. Thus, several new technical requirements are introduced, since SD-WAN connects some branch offices directly to the Internet. This includes integrating security policies into software while simultaneously maintaining the programmability and automation that SD-WAN delivers.

Furthermore, the execution of this strategy must also address hybrid network requirements associated with running both MPLS and SD-WAN networks. The challenge in this scenario is not to compromise the performance of existing security infrastructure, such as security gateways that must be enhanced to support encrypted traffic.

It is also important to note that by moving from MPLS to SD-WAN, many enterprises are also moving from a centralized security model to a distributed model supporting connected branch endpoints that have direct Internet access. The challenge in dealing with these endpoints is meeting the requirements of deploying an end-to-end solution that is fully integrated and automated, as opposed to simply adding an additional security gateway to manage IPsec connections, which increase cost and diminish programmability.

To meet these demands, analytics is now also a key component, since it provides the real-time insight to identify potential threats to provide a window to execute threat-mitigation policies. However, successful analytics deployments must also consider the enterprise architecture and be able to support both private WAN connections and Internet-based connections.

In response to these requirements, some enterprises are now reconsidering security strategies, including the adoption of a managed security model when they implement SD-WAN. In general, since some security features can be supported via a virtualized software approach rather than an appliance, SD-WAN is complementary to vCPE, which supports the on-premises deployment of virtual firewall software.

On the CSP side of the equation, there is also a much broader managed security-as-a-service (SECaaS) business opportunity to upsell high-value hosted managed security services that run on their cloud, or even a third-party hosted cloud. SECaaS represents a superior value proposition because the startup delivery model is much simpler. In addition, it incorporates the most up-to-date security measures, allows for growth as needs evolve, and the software design is extensible and customizable to meet specific customer requirements, which is reflected in the fourth-ranked input.

Software extensibility is also a crucial tool for meeting future security services requirements. These include managing lifecycle orchestration, multi-tenancy services and distributed mobile-edge compute network access requirements. Software extensibility is also a valuable tool

that allows CSPs to create and introduce additional integrated managed service offerings to address these demands.

Given the impact of these factors, SD-WAN is redefining the services and technical landscape, while empowering service differentiation on *every* layer of the network. As a result, a new landscape is emerging in which SD-WAN will be deployed in close collaboration with complementary capabilities, such as security, policy and analytics, to support high-value use cases, such as vCPE.

OSS ORCHESTRATION & INTEGRATION

Protecting SD-WAN and achieving the true measure of services monetization will also require SD-WAN deployments to be fully "orchestratable" and integrated into existing operations support systems (OSSs). This section addresses SD-WAN OSS and orchestration integration impacts, as well as the opportunities to differentiate on these functional layers.

OSS & the Orchestrated Edge

SD-WAN drives adoption of new service and charging models. However, since OSSs have developed over many years, they are in many respects not "cloud-enabled." More specifically, SD-WAN and virtualization mandate that new OSS capabilities be designed to facilitate the transition from a dedicated hardware "silo" platform model to a shared common NFV infrastructure (NFVI) model.

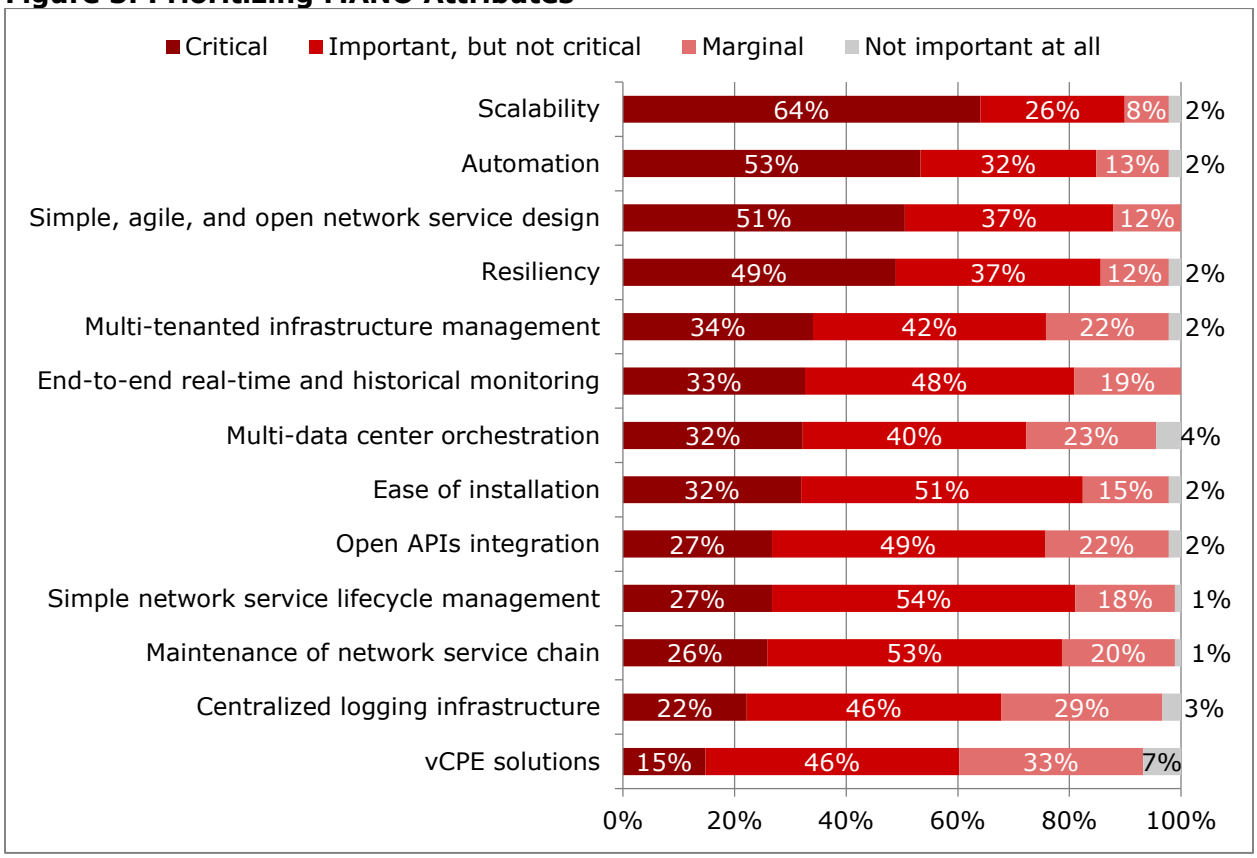
However, since the scope of NFVI is broad, several configurations must be supported. This includes support for a "white box" distributed model, on or near the customer premises. Of course, SD-WAN must also support this model, given its relationship to enterprise services such as vCPE. This means that SD-WAN and service VNFs must be orchestrated not only in the centralized cloud, but also at the enterprise network edge.

Therefore, SD-WAN injects additional complexity into OSS, given the shift away from a dedicated appliance model and the requirement to support the software invocation and orchestration at the edge. Essentially, what is required in an OSS context is the ability to support a single management approach for both MPLS and SD-WAN networks, because the operation of hybrid networks will mandate that an OSS have end-to-end visibility to support security features and policy enforcement.

As a result, integration is even more complex, since SD-WAN separates the data plane from the control plane, which introduces a requirement to manage not only data flows via policy-based analytics, but also control-plane sessions. This separation is a critical step, since by splitting these two functions it is possible to enhance software-driven automation into the data and control planes, thereby achieving a much better scalability and end-to-end integration model.

Perhaps another way to articulate the synergies of this model is that integration of SD-WAN and security in a fully automated and orchestrated environment results in a much richer, scalable managed service offering and better business outcomes for enterprise users. Consistent with this view, as shown in **Figure 3,** carriers rank scalability (64%) and automation (53%) as the top attributes to optimize management and orchestration (MANO).

Figure 3: Prioritizing MANO Attributes



Question: Please rate the importance of the following attributes to NFV MANO.
Source: Heavy Reading, Juniper vCPE and SD-WAN Custom Survey, 2Q16 (N=90-92)

The high ranking of scalability of MANO solutions also reinforces the view that MPLS and SD-WAN paths will require elastic scale to enable their coexistence and migrate subscribers over the hybrid period. Similarly, the prioritization of automation shows that it is a key construct for enabling SD-WAN and zero-touch provisioning, as well as for executing complex "service chains" that will ultimately result in an improved lifecycle for enterprise customer services.

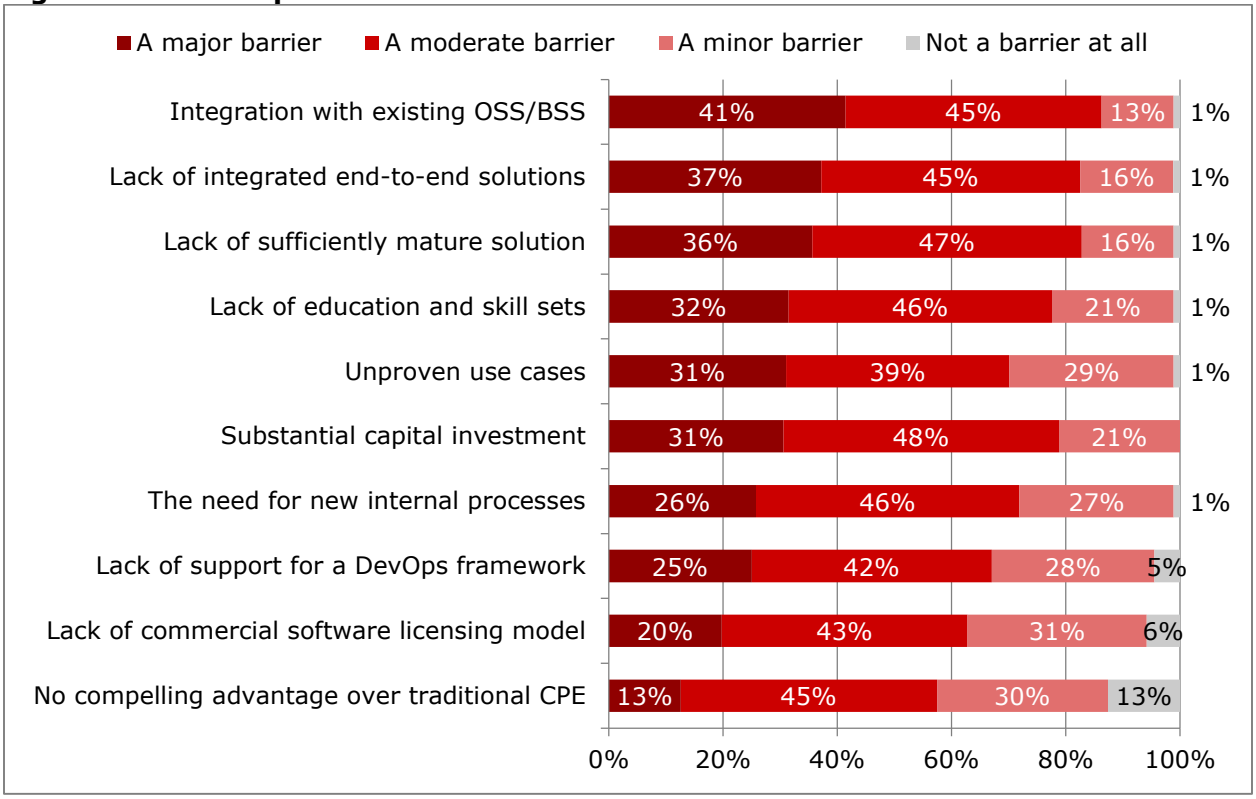
Still, achieving MANO-based scale and automation will require careful execution and will impact several network layers. For example, to enable service chaining and achieve scale, SD-WAN and complementary use cases, such as vCPE, must all work within a standards-based MANO architecture.

Therefore, common application programming interfaces (APIs) will be mandatory to ensure that service chaining can be supported in a managed services agreement if SD-WAN is deployed as part of an overall program that includes vCPE and SECaaS.

Another way to look at this is that SD-WAN is one link in a chain – a service chain that, in order to be agile, automated and scalable, must be open and interoperable with the other edge VNF use cases. The definitive measure for validating this openness will be assessing interworking potential between an SD-WAN edge node and the SD-WAN controller. If there is to be full, open interworking, open APIs will be mandatory to ensure integration into OSS/BSS, as well as MANO lifecycle service orchestration (LSO).

Consistent with this view, as shown in **Figure 4**, when asked about the greatest barrier to implementing vCPE, the survey respondents selected integration with existing OSS/BSS as the most significant challenge (41%).

Figure 4: vCPE Implementation Barriers



Question: Please rate the following potential barriers to vCPE deployment.
Source: Heavy Reading, Juniper vCPE and SD-WAN Custom Survey, 2Q16 (N=85-88)

Yet it's important to note that two other factors also scored highly: the lack of integrated end-to-end solutions (37%) and lack of sufficiently mature solutions (36%). While these barriers remain an area of concern, there are several industry-driven initiatives that are addressing the challenge.

One example is the New IP Agency (NIA), an independent non-profit agency that, in conjunction with the European Advanced European Networking Test Center (EANTC), has conducted several testing cycles to assess and benchmark NFVI performance, VNF interworking and OSS/BSS integration.

This program has been a success because it has allowed a vendor such as Juniper Networks to independently validate solution interoperability and OSS/BSS integration of its Contrail Cloud Platform (CCP) with a diverse set of OSS vendors, including Amdocs, NEC and IBM, as well as security, control plane, orchestration and vCPE vendors, such as Adtran, Ciena, NetNumber and Fortinet.

Looking ahead, the NIA plans to shift focus to more complex use cases that address NFV orchestration, VNF manager and VIM interoperability, followed by multi-vendor SDN and NFV integration testing.

SD-WAN FUTURE REQUIREMENTS

SD-WAN has gained strong market momentum due to its ability to elegantly extend the software-defined model to many network layers – thus enabling CSPs to achieve service differentiation on multiple layers, as well. This is unlikely to change as SD-WAN matures and the issues previously noted, such as interoperability, OSS integration and orchestration, diminish in impact. Still, given that the software world is by nature extremely fluid, SD-WAN requirements will continue to evolve in response to service requirements.

Accordingly, this section considers the factors that will have a major impact on shaping future SD-WAN deployments. These include:

- Resiliency & Performance
- NFVI & Hybrid Network Requirements
- Extending Policy Control & Analytics

Resiliency & Performance

One way to achieve service differentiation using SD-WAN is to leverage its programmable nature to ensure that latency-sensitive services are matched with the lowest-latency media path. However, to truly achieve this goal requires that the SD-WAN have well-defined and mature resiliency capabilities.

Without these, services will be negatively impacted by VNF failure or WAN failure scenarios. Therefore, what is required is an advanced suite of resiliency tools that support the ability to detect failure states and seamlessly divert services. This can be a complex undertaking if the network is orchestrating a complex service chain, encrypting traffic and also monitoring VNF failure state. Factoring in the fact that resiliency applies to failures not only on the data plane but also on the control plane provides additional perspective of the scope of the challenges that await.

Thus, it's not surprising that resiliency was the fourth-ranked MANO implementation barrier (49%) cited in **Figure 3**. Looking ahead, managing resiliency requirements will become even more difficult as more features are deployed at the network edge, and the concept of a network edge is extended to support 5G and fog computing. The adoption of this network edge model will also make it important to consider resiliency and performance in a platform design context to ensure that a VNF is optimized and supported on dual interfaces and hardened operating systems.

NFVI & Hybrid Network Requirements

This paper has touched upon the impact and additional complexity associated with managing NFVI in a hybrid network environment. However, as SD-WAN rollouts continue to gain critical mass, additional challenges must be addressed. For example, SD-WAN's flexibility enables diverse technology deployment models, including the deployment of SD-WAN as an overlay in some branches of the network, while maintaining MPLS in others for the same customer.

As traffic scales, this introduces a suite of security and interoperability issues, particularly if multiple vendor products are deployed. Similarly, OSS/BSS and MANO requirements will

become more complex as the network shifts to an NFVI-based SD-WAN model, with the expectation that SD-WAN, MPLS services, security and any other managed service will be consolidated under a common, open and standards-based MANO.

A third consideration that has the potential to inject additional complexity is the integration of open source, third-party software model into existing vendor SD-WAN software deployments. While the move to open source has been somewhat slow, support continues to build, and it's now evident that on some level, open source software will find its way into future commercial SD-WAN deployments. But this also has security implications, since botnet threats, such as Mirai, are adopting this same open source publishing model to facilitate the mass distribution of malware.

Extending Policy Control & Analytics

In the emergent programmable world that awaits, policy control and analytics will continue to expand in relative importance to manage more complex service outcomes. Here again, a few new challenges and open questions must be addressed. For example:

- What are the OSS/BSS, MANO, security and integration implications of moving to a dynamic, end-to-end, layer-driven policy model for the SD-WAN?
- What additional requirements must an end-to-end policy model support to integrate SDN controller policies with policies for the upper layers of the network (e.g., PCRF-driven), in order to thoroughly manage security threats?
- What are the implications of utilizing real-time analytics to enable dynamic policy enforcement and customer care for complex service-chaining-based features?
- What additional policy control and analytics capabilities will be required to create a service layer that supports stateless, decomposed microservices?
- Finally, what are the implications for an SD-WAN to support predictive policy and analytics capabilities for emerging, advanced services that embed artificial intelligence capabilities?

CONCLUSION

The rise to prominence of SD-WAN can be attributed to several factors. First and foremost, as documented, SD-WAN empowers CSPs to achieve service differentiation on all network layers: the service layer, the orchestration layer, the policy control and analytics layer, the OSS layer and even the NFVI layer. In addition, SD-WAN's ability to deliver a programmable template that is capable of meeting future service requirements is a chief consideration.

Given these traits, SD-WAN will continue to represent a strong value proposition, ensuring that future waves of service innovation and differentiation can be achieved holistically, on all network layers, irrespective of how these layers are redefined in the future.