Part 3 of 3

How Nokia Enables MSOs to Realize The Full Potential of SD-WAN Services

With a Foundation Built on Nuage Networks from Nokia's Virtualized Network Services, Operators Can Leverage Advanced VPN Connectivity in Multiple Revenue-Generating Scenarios

TABLE OF CONTENTS

Introduction
A Fully Featured Cost-Effective Approach to SD-WAN based Connectivity
A Comprehensive Approach to SD-VPN Service Assurance
Leveraging Nokia Solutions to Support Value-Added Services
- The OSS Role in Enabling VAS
- Integrating Legacy VPN and SD-VPN Infrastructures
- Enabling Enhanced Security
- Bundling Third-Party SaaS Solutions with the SD-VPN Service
- Enabling Extension of SD-VPNs into the Cable Wireless Domain

Conclusion

Introduction

The scope of cable MSOs' opportunities and the technological requirements tied to VPN connectivity delivered via software defined techniques for the SMB market were spelled out in the first two parts of this three-part series, leaving to be answered the question of whether there’s a readily available practical way forward.

As outlined in Part 2, the simplest and most cost-effective solution is one that supports SD-VPNs offering business customers dedicated and secure connectivity as an IP application that can be made ubiquitously available over any type of broadband access network. The widely deployed Nuage Networks Virtualized Network Services (VNS) platform, architected on the basis of these principles, demonstrates their benefits when it comes to delivering SD-VPNs over MSOs’ broadband networks.

The approach opens an immediate path for delivering a new kind of VPN service that supports much greater provisioning and operational flexibility at lower costs. Critically, operators can implement this new highly competitive means of retaining customers and adding new ones using virtualized cloud technology without having to convert facilities to support full network function virtualization (NFV).

Nokia, as a leading force behind network service providers’ migrations to NFV worldwide, can supply MSOs with any and all the elements they need to support a highly scalable, distributed NFV architecture without having to convert facilities to support full network function virtualization (NFV).

Nokia, as a leading force behind network service providers’ migrations to NFV worldwide, can supply MSOs with any and all the elements they need to support a highly scalable, distributed NFV architecture. But while NFV is widely seen as an inevitable progression over time, it’s vital that operators be able to move immediately into providing SD-VPN connectivity as a highly appealing alternative to the more costly types of VPN service traditionally supplied by incumbent carriers.

As discussed previously, the opportunity for SD-VPN service starts with the benefits of giving customers console-provisioned connectivity with control over usage policies, applications and much else, including a smooth transition to SD-VPN for MSOs already providing a traditional VPN service. At the same time, the potential benefits of SD-VPN connectivity extend much farther by opening a path to providing value-added services (VAS) in a market hungry for low-cost access to essential cloud-based applications.

Nuage Networks VNS positions operators who have deployed SD-VPN connectivity to expand the range of VAS they can support by utilizing other components of the Nokia product portfolio. These include the far-reaching back-office enhancement capabilities that can be enabled without disrupting existing BSS/OSS through use of components in the Nokia Customer & Network Operations (OSS) solution set.

The following discussion focuses first on how operators build SD-VPN services using the Nuage Networks VNS platform and the range of capabilities available to operators and end users once the platform is operating. We then look at how operators can move up the value chain in the SMB market and expand their appeal to larger enterprises with VAS strategies built on the Nokia framework.

A Fully Featured Cost-Effective Approach to SD-VPN Connectivity

The emergence of VPN services based on the software defined networking framework by MSOs into the SMB market has been driven by the growth in large enterprises building their NOKIA

Note to readers: With Alcatel-Lucent’s recent combination with Nokia, the solutions and services developed by Alcatel-Lucent through its long-standing role as a leading supplier to the cable industry are now fully supported with sales, integration and ongoing development activities under Nokia.
own WAN services as an alternative to IP-VPN service. This approach, commonly referred to as SD-WAN, is fueling the desire for a new breed of connectivity services across the whole enterprise market. Innovative MSOs can leverage the increased market awareness to bring the capabilities to even the smallest businesses by implementing Nokia-enabled SD-VPN connectivity as a software-based overlay to business-class broadband services offered over DOCSIS-enabled HFC, EPON and IP MPLS facilities.

Nuage VNS not only enables an affordable VPN service for businesses that have never used VPNs; it makes it possible for companies currently using traditional VPNs to take advantage of SD-VPN connectivity to connect new office and datacenter locations in a way that integrates seamlessly with the existing VPN infrastructure. In all cases, the benefits include support for virtualized CPE that MSOs’ customers can use to activate the VPN service without requiring a visit from installers.

Whereas traditional VPN services are based on set functionalities, leaving little room for per-enterprise customization and forcing complex custom-branch networking, the Nuage VNS overlay model allows MSOs to use any IP network to provide connectivity between sites and eliminate the network complexity. As a result, cable operators can provide all commercial customers an affordable mode of secure dedicated connectivity across office locations and among employees wherever they are.

In so doing, this new approach to VPN connectivity allows companies of all sizes to seamlessly link work processes across all locations, from simple printing jobs to IT tools and systems of every description. Moreover, any company can utilize SD-VPN connectivity to take advantage of a rapidly growing cloud-based ecosystem of advanced IT applications that in the past only big enterprises could afford.

The Nuage Networks VNS components that make this possible can all be implemented as software modules running on COTS (commodity off-the-shelf) servers. They include: 

**Virtualized Services Directory (VSD)**

The VNS centralized policy engine defines, deploys and enforces the platform’s many functions in support of SD-VPN with IPSec security mechanisms applied on all links. This programmable policy and analytics engine provides a flexible network policy framework that enables a business customer’s administrators, including non-technical personnel, to define and enforce the business policies being applied across the SD-VPN service connections in a user-friendly manner.

With VNS those rules are translated to access control lists and routing entries, enabling a virtual fabric that automatically programs all SD-VPN service end points. Administrators, utilizing the platform’s key provisioning process, can easily associate rules of access and usage on a per-person basis at all locations.

The VSD network service directory supports role-based administration of network resources through an intuitive graphical user interface where personnel can quickly implement new and change existing points of connectivity and set and change policies on a site-specific or network-wide basis. Users can also access site and service-wide trending reports generated by the VSD through its traffic data collection and analytics processes for both service assurance and business planning purposes.

The VNS platform also provides support for common network functions such as firewalling, load balancing, IP address management, including DHCP/NAT execution, and domain name services. MSOs can empower customers to select such functions as tiered service options from the VSD Network Functions Store for insertion directly into their SD-VPN service, greatly reducing customers’ need to obtain this type of support from dedicated network elements, including third-party appliances.

**Virtualized Services Controller (VSC)**

VSC is the network control plane used to program the core MSO SD-VPN platform and each customer’s CPE with the network overlay paths that comprise the topology for the SD-VPN service. Using the OpenFlow protocol, the VSC establishes the virtual routing and switching constructs in a highly scalable approach to programming multiple instances of connectivity. In support of connectivity beyond the MSO’s network footprint, VSC leverages the Multi-Protocol Border Gateway Protocol (MP-BGP) to federate encrypted SD-VPN connectivity across broadband access facilities of other providers serving remote locations of the MSO’s customers.

**Network Services Gateway (NSG)**

NSGs are positioned at the MSO’s operations datacenter and in each customer location to terminate the SD-VPN overlay tunnels. At the customer end the gateway provides service demarcation and network functionality utilizing x86 COTS hardware wherever available. In instances where such facilities are not available the operator can box and ship the virtualized CPE appliance along with the enabling software to the designated location.

Either way the NSG includes the form factors essential to meeting diverse throughput, network interface and network functionality parameters across all locations. With the auto-configuration processes built into the VSC, the NSG approach to remote connectivity greatly speeds SD-VPN deployment velocity while affording plug-and-play customer implementation that avoids the need for operator-provided technical support at the premises.

**A Comprehensive Approach to SD-VPN Service Assurance**

Executing all the mechanisms essential to comprehensive SD-VPN service assurance starts with the overlay service assurance capabilities embodied in the Nuage VNS platform. These mechanisms are implemented under the direction of the VSD policy engine.

In order to facilitate comprehensive service assurance that scales consistently as complexities mount with the addition of ever more end points, the policy engine allows administrators to set sophisticated rules for things such as data collection frequencies, rolling averages and samples and the generation of Threshold Crossing Alerts (TCAs) to identify current and historic performance lapses. Data is also compiled for auditing and ensuring compliance in conjunction with industry regulations such as the Sarbanes-Oxley Act.

All data from network-wide surveillance, CPE and other sources pertinent to service assurance at the overlay layer is fed into the VNS analytics engine, which supports automated proactive fault-management measures and generates actionable information for CSRs and technicians to use in trouble shooting and remedying problems. Managers can set the aggregation of each category of statistics to occur over hourly, daily or much longer timeframes. All collected data is stored in a Hadoop analytics cluster to facilitate data mining and reporting.

In addition, the VNS platform makes it possible to leverage data generated by quality control systems monitoring the underlay facilities networks to instantly flag root network causes of any SD-VPN service issues. This includes letting operations personnel know how any changes in edge routers or router architecture may be impacting the SD-VPN service.

Of course, the ability to incorporate the full scope of network monitoring and analytics processes across the core and multiple access networks into execution of service assurance requirements by VNS requires a means of bridging the gap between the overlay and underlay domains. This is one of the major benefits opera-
tors can draw from implementation of the Nokia Motive Dynamic Operations (MDO) platform.

The integration of underlay and overlay service assurance processes is facilitated by pre-built workflows implemented on the Nokia OSS platform. The workflow construction component of Nokia OSS provides an out-of-the-box palette of workflow templates, control, display and device/service operation objects that workflow designers can use to engage operations in a wide range of applications, in particular including service assurance.

With this integration framework in place, Nokia OSS makes it easier to define, publish and execute advanced troubleshooting and proactive or reactive repair logic relative to performance at the physical network level as part of the service assurance processes executed on the Nuage VNS platform. CSRs and technicians addressing customer care requirements of the SD-VPN service can key all the information and management capabilities they need to diagnose and resolve service issues.

In addition, operators who lack state-of-the-art solutions for monitoring and addressing network-layer issues can leverage the advanced analytics capabilities of the Nokia OSS solutions. Drawing data from virtually any common network interface technology, Nokia OSS provides a sophisticated analytics and event correlation engine to support proactive, real-time network-wide surveillance and fault management, dynamically adaptable alarm models and Web interface configurations generating customizable views with fast drill down to subsystems and network elements.

**Leveraging Nokia Solutions to Support Value-Added Services**

Implementation of the Nuage Networks VNS platform to deliver SD-VPN services creates a foundation MSOs can build on to support a wide range of value-added services (VAS), enabling new sources of revenue and increasing customer incentives to engage with cable operators as their core broadband service providers. MSOs can tap an array of other Nokia solutions to complement VNS in pursuit of these goals, including the Nokia OSS platform to bring functionalities of existing OSS/BSS systems into play.

**The Nokia OSS Role in Enabling VAS**

MSOs’ ability to cost effectively automate provisioning, life-cycle management, billing and settlements, customer care and other essential functions essential to delivering new IP-based services and applications requires implementation of a trans-silo back-office integration solution that can bring all existing functions into play without requiring a complete OSS/BSS overhaul. With Nokia’s OSS solutions in place, MSOs are able to meet these requirements, thereby addressing immediate needs and opportunities associated with SD-VPN services while creating a back-office foundation for ongoing service evolution wherever it may lead.

Beyond helping operators fulfill the service assurance requirements of an SD-VPN service as described above, an NFV platform such as Nokia CloudBand provides support essential to seamless integration of VAS components into the Nuage VNS solution. With a view of the entire MSO service topology, Nokia OSS solutions utilize any VNF and Network Service catalogs and tie-ins to existing OSS platforms to automate the deployment processes of VAS. This makes it possible for VAS options to be automatically provisioned onto any SD-VPN connection in response to commands from CSRs and self-help portals.

Using the open, extensible Nokia API architecture, MSOs can benefit from pre-integrations of Nokia NFV & OSS solutions and from professional services to handle existing OSS/BSS systems as well as facilitate new integrations to enable end-to-end service management in the overlay IP domain. By providing a unified, accurate view of all network and IT resources, Nokia OSS makes it possible to identify and abstract those resources as well as virtualized network resources as they are implemented over time and deliver real end-to-end service assurance capabilities.

**Integrating Legacy VPN and SD-VPN Infrastructures**

One important advantage to be derived from combining VNS and Nokia OSS capabilities is support for integration between customers’ legacy VPN infrastructures and the VNS delivered SD-VPN service. This enhances the MSO’s service value in instances where the operator has been supplying traditional VPNs to existing customers and positions the MSO as an alternative supplier to larger enterprises who want to exploit the benefits of SD-VPN connectivity. In both cases the SD-VPN service provides businesses a faster, more flexible way to extend VPN services to new locations while allowing them to retain existing VPN service or phase it out gradually as they see fit.

The multi-OSS integration framework supported by the Nokia OSS platform makes it possible to encapsulate the Nuage VNS SD-VPNs within the legacy VPN operations to create seamless flows between the two operations environments. VNS tunnels are terminated on deployed routers and mapped to those points of connection into the existing VPN infrastructure, which is accomplished by Nokia OSS integration with existing functions interfacing with the operator’s router infrastructure.

**Enabling Enhanced Security**

Enhanced security, too, is a benefit that can be provided via SD-VPN services utilizing another component of the Nokia solutions portfolio. As noted earlier, support for firewall security options as well as IPSec-based protection for the SD-VPN tunnels is intrinsic to Nuage VNS. But there is also widespread demand among businesses for advanced security protection, described as Unified Threat Management in Part 1, which MSOs can provide as a VAS with the SD-VPN connectivity service through utilization of additional Nokia security solutions.

For example, Nokia provides MSOs security solutions for the underlay network, which are also essential to protecting the integrity of the overlay connections. The solution set enables centralized security administration, support for rapid response to threats and intrusions, identification of points of vulnerability and network-wide policy management with regard to limiting access to just the points in the network any given party is authorized for.

This network security includes protection against unauthorized entry at the network level by employees, third-party providers or other authorized users of SD-VPN connectivity based on single sign-in policies that confine each party’s access to specifically assigned network elements. Any time an employee leaves the company or an authorized supplier is no longer under contract, the system automatically de-authorizes network access without the need for manual intervention.

As SD-VPNs are used to deliver secure VPN connectivity to employees’ personal devices there’s also a need to ensure devices connecting to the VPN network are free from malware. MSOs utilizing Nokia security solutions in conjunction with network-based probes can enable their SD-VPN customers to screen employee devices before they are authorized for connectivity and on an ongoing basis thereafter.

Beyond these safeguards, Nokia provides MSOs additional options for intrusion detection support. Mechanisms in the security portfolio can be employed by business customers to add extra protection to any point of interface between

---

**Market Intelligence >> MSO BUSINESS SERVICES**

---

**Nokia OSS Role in Enabling VAS**

Leveraging Nokia Solutions to systems and network elements. customizable views with fast drill down to sub- and Web interface configurations generating management, dynamically adaptable alarm models common network interface technology, Nokia OSS solutions. Drawing data from virtually any advanced analytics capabilities of the Nokia ing network-layer issues can leverage the management capabilities they need to diag- nose and resolve service issues.

In addition, operators who lack state-of-the-art solutions for monitoring and addressing network-layer issues can leverage the advanced analytics capabilities of the Nokia OSS solutions. Drawing data from virtually any common network interface technology, Nokia OSS applies a sophisticated analytics and event correlation engine to support proactive, real-time network-wide surveillance and fault management, dynamically adaptable alarm models and Web interface configurations generating customizable views with fast drill down to subsystems and network elements.

**Leveraging Nokia Solutions to Support Value-Added Services**

Implementation of the Nuage Networks VNS platform to deliver SD-VPN services creates a foundation MSOs can build on to support a wide range of value-added services (VAS), enabling new sources of revenue and increasing customer incentives to engage with cable operators as their core broadband service providers. MSOs can tap an array of other Nokia solutions to complement VNS in pursuit of these goals, including the Nokia OSS platform to bring functionalities of existing OSS/BSS systems into play.

**The Nokia OSS Role in Enabling VAS**

MSOs’ ability to cost effectively automate provisioning, life-cycle management, billing and settlements, customer care and other essential functions essential to delivering new IP-based services and applications requires implementation of a trans-silo back-office integration solution that can bring all existing functions into play without requiring a complete OSS/BSS overhaul. With Nokia’s OSS solutions in place, MSOs are able to meet these requirements, thereby addressing immediate needs and opportunities associated with SD-VPN services while creating a back-office foundation for ongoing service evolution wherever it may lead.

Beyond helping operators fulfill the service assurance requirements of an SD-VPN service as described above, an NFV platform such as Nokia CloudBand provides support essential to seamless integration of VAS components into the Nuage VNS solution. With a view of the entire MSO service topology, Nokia OSS solutions utilize any VNF and Network Service catalogs and tie-ins to existing OSS platforms to automate the deployment processes of VAS. This makes it possible for VAS options to be automatically provisioned onto any SD-VPN connection in response to commands from CSRs and self-help portals.

Utilizing the open, extensible Nokia API architecture, MSOs can benefit from pre-integrations of Nokia NFV & OSS solutions and from professional services to handle existing OSS/BSS systems as well as facilitate new integrations to enable end-to-end service management in the overlay IP domain. By providing a unified, accurate view of all network and IT resources, Nokia OSS makes it possible to identify and abstract those resources as well as virtualized network resources as they are implemented over time and deliver real end-to-end service assurance capabilities.

**Integrating Legacy VPN and SD-VPN Infrastructures**

One important advantage to be derived from combining VNS and Nokia OSS capabilities is support for integration between customers’ legacy VPN infrastructures and the VNS delivered SD-VPN service. This enhances the MSO’s service value in instances where the operator has been supplying traditional VPNs to existing customers and positions the MSO as an alternative supplier to larger enterprises who want to exploit the benefits of SD-VPN connectivity. In both cases the SD-VPN service provides businesses a faster, more flexible way to extend VPN services to new locations while allowing them to retain existing VPN service or phase it out gradually as they see fit.

The multi-OSS integration framework supported by the Nokia OSS platform makes it possible to encapsulate the Nuage VNS SD-VPNs within the legacy VPN operations to create seamless flows between the two operations environments. VNS tunnels are terminated on deployed routers and mapped to those points of connection into the existing VPN infrastructure, which is accomplished by Nokia OSS integration with existing functions interfacing with the operator’s router infrastructure.

**Enabling Enhanced Security**

Enhanced security, too, is a benefit that can be provided via SD-VPN services utilizing another component of the Nokia solutions portfolio. As noted earlier, support for firewall security options as well as IPSec-based protection for the SD-VPN tunnels is intrinsic to Nuage VNS. But there is also widespread demand among businesses for advanced security protection, described as Unified Threat Management in Part 1, which MSOs can provide as a VAS with the SD-VPN connectivity service through utilization of additional Nokia security solutions.

For example, Nokia provides MSOs security solutions for the underlay network, which are also essential to protecting the integrity of the overlay connections. The solution set enables centralized security administration, support for rapid response to threats and intrusions, identification of points of vulnerability and network-wide policy management with regard to limiting access to just the points in the network any given party is authorized for.

This network security includes protection against unauthorized entry at the network level by employees, third-party providers or other authorized users of SD-VPN connectivity based on single sign-in policies that confine each party’s access to specifically assigned network elements. Any time an employee leaves the company or an authorized supplier is no longer under contract, the system automatically de-authorizes network access without the need for manual intervention.

As SD-VPNs are used to deliver secure VPN connectivity to employees’ personal devices there’s also a need to ensure devices connecting to the VPN network are free from malware. MSOs utilizing Nokia security solutions in conjunction with network-based probes can enable their SD-VPN customers to screen employee devices before they are authorized for connectivity and on an ongoing basis thereafter.

Beyond these safeguards, Nokia provides MSOs additional options for intrusion detection support. Mechanisms in the security portfolio can be employed by business customers to add extra protection to any point of interface between...
the MSO network and the larger e-commerce environment to ensure that the connectivity with outside suppliers, partners and customers isn’t compromised by malware infections.

Bundling Third-Party SaaS Solutions with the SD-VPN Service

Another important revenue-generating VAS strategy that can contribute to enhancing the appeal of MSOs’ SD-VPN services entails support for bundling of third-party SaaS (Software-as-a-Service) products based on partnership arrangements with SaaS providers. As noted in Part 1, research has shown SMBs prefer bundled SaaS offerings over having to pull together the services they need on an a la carte basis.

MSOs can support such offerings through two approaches. One involves “service-chaining” whereby MSO customers can choose a particular SaaS provider through their SD-VPN service portals. In this instance, operators can leverage a component of the previously described MDO platform, tying their back-office systems into the Nuage VNS and extending that tie-in via hybrid virtual networking mechanisms that make it possible to connect the SD-VPN service with whatever public cloud service is hosting the SaaS. In this scenario it’s left to the partner SaaS provider to take the orders and provision the service through the tie-in with the SD-VPN service.

Operators can add value to bundled SaaS offerings by hosting value-added services to create a more instantaneous and higher quality experience for their customers with the same automated provisioning support in response to commands from CSRs and self-help portals that VNS provides for the basic SD-VPN connectivity service. By hosting these SaaS options in their SDN-enabled clouds operators can also apply the full range of the previously described VNS- and Nokia OSS-enabled overlay/underlay service assurance mechanisms to those services.

Nokia facilitates MSOs’ ability to host such services through direct integration of the VNS platform with Nokia’s CloudBand virtualization platform. CloudBand makes it possible for MSOs to build a carrier-grade cloud infrastructure that can orchestrate, automate and optimize services hosted in operators’ datacenters while providing lifecycle and datacenter appliance capacity management for all the virtual network functions intrinsic to those services.

All networking functions, voice and security applications, routing and firewalls tied to these hosted services are managed through CloudBand in a multi-tenant hosting environment that can be scaled over time with strict adherence to latency performance, raw throughput and other parameters intrinsic to each application. Through ongoing dashboard control over those apps, customer administrators can manage usage and other policies on a per-employee basis and set up access for outside collaborators as they’re brought in to work on specific projects.

It’s also important to note that as an industry-leading standards-based platform supporting service providers’ migration to NFV infrastructures worldwide, CloudBand not only provides MSOs a means of putting NFV capabilities to immediate use in conjunction with the VAS options offered over SD-VPN connectivity. It also positions them for ongoing NFV expansion in the future with support for automated, highly programmable set-up and orchestration of NFV components and the services and applications that run on them across all cable datacenter locations.

Enabling Extension of SD-VPNs into the Cable Wireless Domain

Rounding out the capabilities that can be accommodated by Nuage Networks VNS in combination with other Nokia solutions is the extension of access to SD-VPN services to customer employees on the go via MSOs’ Wi-Fi infrastructures. As noted in Part 2, MSOs have an opportunity to greatly expand their profiles in wireless business services through use of technologies like HotSpot 2.0 with automated certification and 802.11ac to expand their reach and build commercial-grade connectivity, including Wi-Fi First capabilities that ensure users’ devices always choose the operator’s Wi-Fi connection over mobile service connectivity wherever possible.

Bringing SD-VPN connectivity into this environment can significantly enhance the appeal of MSOs’ commercial services within and beyond the SMB sector. The back-office integration enabled by Nokia OSS makes this possible by providing the means by which the VNS-based SD-VPN service can be stitched into the MSO’s Wi-Fi operations infrastructure to provide employees secure, policy-authorized access to company resources whenever they’re in reach of the operator’s Wi-Fi access points.

Through Nokia OSS-enabled back-office workflows operators are able to set up SSIDs (Service Set Identifiers) focused on enabling user access to business-class services and to provision routing equipment and gateways to support the VPN overlay. In addition, one of the important aspects to making such extensions possible are the previously described enhanced security mechanisms Nokia provides to prevent breaches in the BYOD environment.

The Nokia OSS solution set also has a big role to play in adding voice capabilities to Wi-Fi and therefore to creating an extended unified communications environment for SD-VPN users. Nokia OSS solutions can provide the back-office support required to enable an IMS-based VoIP experience over Wi-Fi connections. It authenticates the device, mediates with the MNO/MVNO BSS/OSS environment and pushes the necessary service settings to iOS and Android phones.

Conclusion

SD-WAN technology has greatly expanded MSOs’ opportunities in the fast-growing commercial services arena. By taking advantage of the SD-VPN capabilities enabled by the Nuage Networks VNS platform, cable operators can provide secure VPN connectivity and all the benefits that come with that to customers of all sizes in the SMB market while positioning themselves to provide compelling service alternatives in the larger enterprise market.

Adding to the benefits, Nokia provides the full range of solutions through its OSS-enhanced security and CloudBand platforms that make it possible for MSOs to move aggressively into the VAS domain without having to invest heavily in new IT staffing, replace existing OSS/BSS platforms or build new infrastructure. Integrating SD-VPN connectivity with Nokia’s cable Wi-Fi platforms, operators can also create enhanced value-added connectivity service bundles for their SMB and enterprise customers. Moreover, by embracing the power of Nokia-enabled virtualization technology on an incremental basis that leads directly to new revenue, MSOs can implement ROI-based migration paths to NFV at whatever pace suits their needs.

Along with the basic technology platforms, well-honed integration skills and support services supplied by Nokia, MSOs can also benefit from the expert strategic development services provided by Nokia Bell Labs. Through access to a practice that leverages the expertise Bell Labs has long employed to drive telecommunications advancement, MSOs can create go-to-market frameworks that greatly enhance their ability to identify opportunities and model at a highly granular level the costs, pricing and staffing requirements that go into enabling SD-WAN services and any types of VAS they may wish to pursue.