Bringing agility and programability to Defense networks

With adaptable and secure SDN

White paper

Defense operations and missions are becoming network-centric today. SDN benefits Defense networks by providing capabilities such as programmable services, automation, network and data center consolidation and sharing, security and cyber-agility, and reduced network operations costs - and for the tactical echelons, rapid incorporation of military-specific nodes and improved C2. This paper describes a variety of use cases and outlines the capabilities of Nuage Networks solutions from Nokia, the Nokia Network Services Platform, Nokia CloudBand, Nokia Virtual Networks Orchestration and Nokia FlowOne.
Contents

SDN gaining wide acceptance 3
Defense SDN use cases 4
Empowering the infrastructure network with SD-WAN and hybrid SD-WAN 5
Extend SDN advantages to the traditional IP network 6
Cross-domain orchestrated hybrid SD-WAN from a single service manager 7
Nokia dynamic network components 8
Nuage Networks solutions 8
Nokia Network Services Platform 9
Nokia CloudBand 10
Nokia Virtual Networks Orchestration 11
About Nokia and SD-WAN 13
Nuage Networks SD-WAN 13
Nokia Carrier SDN 14
Conclusion 14
Abbreviations 14
SDN gaining wide acceptance

Software-defined networking (SDN) and its complementary companion, network function virtualization (NFV), are technologies that have started to gain wide acceptance in the networking industry.

The major features of SDN are:

- **Programmability**: Network behavior is programmed in advance, enabling the network to adapt to ever-changing NFV configurations.
- **Dynamicity**: Network services, including security policies, are added, removed or updated according to instantaneous requirements; this feature is essential to seamless NFV deployment and operation.
- **Adaptability with self-learning**: The deployment of network and network security services can be automated based on network analytics insight.
- **Flexibility with fine-grained control**: SDN allows per-flow and per-subnet address-based resource and security control, as well as bandwidth sharing among and within network services by different applications. These capabilities are also referred to as micro-segmentation.
- **Multi-tenancy**: Network slicing allows the management of the network resources using a multi-tenant paradigm, where tenants are the administrators of their own slice and have total control of their allocated resources without interfering with other tenants, while the traffic separation is strictly preserved.

These powerful features bring significant benefits to networks owners and administrators:

- **Automation and services on-demand**: By programming in advance, SDN enables network automation that can make changes without manual intervention, such as instantiation and (re-)configuration of network services and resources. This improves network operation speed, flexibility and agility. Furthermore, SDN allows the dynamic and automated deployment, maintenance and traffic optimization of a mission-classified network within network constraints, and at the operative and tactical echelons the rapid reconfiguration of forces communication capabilities as missions evolve.

- **Network and data center consolidation and sharing**: SDN provides a good framework for network infrastructure and resource sharing simplifies the consolidation of the various networks and data centers (for armies, national security agencies, governmental agencies, etc.) into a federated global infrastructure with central points of management. This capability is fundamental to temporary or long-term international networks for allies and coalitions, such as NATO’s Federated Mission Networking (FMN).

- **Security and cyber-agility**: SDN leverages real-time network data feeds and can, in turn, automatically trigger security policy updates, swiftly stifling emerging threats. Furthermore, with the information ecosystems evolving to cloud and applications adopting the micro-services paradigm, software-defined security programmed on a per-application basis with the use of micro-segmentation techniques can isolate applications within their own secure logical domain inside the defense network, thwarting intrusion attempts.

- **Reduced operations costs**: SDN automation frees up network administrators’ time to focus on other mission-critical tasks and reduces the number of specialized personnel required at various network locations. Furthermore, acting as service policy interpreter, an SDN controller increases ease of network configurability and reusability and decreases the level of human operator intervention required, thereby reducing the risk of configuration error.
While some Defense networks’ specific issues remain to be resolved when a deployment covers the entire network down to the operative and tactical echelons, today SDN can bring the following promises:

- **Dynamic network and prolongation**: At the tactical echelon, together with software-defined radio (SDR) and NFV, SDN allows the rapid incorporation of military-specific elements such as unmanned aerial vehicles (UAVs) and long-distance links such as satellites into the network, and the ad hoc deployment of coalition mobile ad hoc networks (MANETs).

- **Improved C2**: SDN allows more real-time control and management data collection from the infrastructure and improves visibility on network situational awareness, which in Defense networks translates into shortened operations time.

This paper introduces how SDN’s advanced features can benefit Defense network administrators, and then concludes with a brief survey of Nokia SDN solutions.

**Defense SDN use cases**

Figure 1 provides an illustration of the traditional dichotomy of Defense networks: in the homeland or extended homeland (i.e., oversees territories and allied countries with high-bandwidth, long-distance network reach). The infrastructure networks interconnect the “fixed” Defense and related governmental agencies’ premises, while theater networks are deployed temporarily for specific operations and move inside the theater during operations.

While the adoption of SDN in theater networks faces specific challenges (e.g. SDN controller cascading to support “ivory tower” resiliency, military-grade security of the control plane, or optimization of control traffic across low-bandwidth or degraded network links) that are still under study in Defense organizations, the infrastructure networks can reap immediate benefits from today’s commercial SDN solutions. The remainder of this section will explore a few major use cases for infrastructure networks.
Empowering the infrastructure network with SD-WAN and hybrid SD-WAN

The rise of the Internet of Things (IoT), rich multimedia communications, high-bandwidth-consuming applications such as big data and analytics, cloud-based services, and the diversification of broadband access techniques have affected Defense organizations as much as they have civilian industries. Therefore, new dynamic connectivity bandwidth is increasing at a rate faster than the speed at which network access links and transport trunks can be re-configured/re-dimensioned with traditional techniques. Consequently, many Defense and governmental agency branch offices are looking for new connectivity since their traditional networks are struggling to handle the evolution of network requirements.

The software-defined wide area network (SD-WAN) is a WAN extension of the SDN technology that overcame the challenges described above, and offers these additional advantages:

- Cloud readiness
- Flexible network connection provisioning and re-configuration
- Higher network and cloud application availability

Furthermore, by using SD-WAN solutions, Defense organizations can distribute a site’s data traffic among different network uplinks while increasing the overall network availability and resiliency.

On the other hand, the replacement of IP/MPLS core routers by virtual network functions (VNFs) remains in the distant future since the evolution path analysis, testing and planning of Defense networks are by nature subject to the same meticulous process standards as most Defense-related topics. Consequently, a migration path that replaces traditional Defense IP/MPLS networks by a pure SDN/NFV infrastructure is not a feasible option: the IP/MPLS-based core and distribution networks serving Defense organizations will remain in service and even continue to be upgraded for a long period of time. Therefore, SD-WAN as an overlay to the existing traditional IP/MPLS networks is an attractive option, and such a coexistence can be expected to last for some time. This strategy also preserves past IP/MPLS network investments.

In light of these developments, hybrid SD-WAN has emerged to be a good solution. The hybrid network paradigm flexibly connects geographically dispersed sites via different types of access technology depending on availability and economics. Typically, the traditional IP/MPLS WAN that connects the sites is “augmented” by other paths realized through a broadband connection to another network, e.g., the internet. Normal business traffic that requires a solid service level agreement (SLA) and a high level of security (e.g. a connection to a critical data center) is routed through the IP/MPLS network. Additional traffic that only requires best-effort delivery can be offloaded (while encrypted by IPsec) using SD-WAN over the internet at competitive cost. Note that such internet offloading can also link all sites in a meshed manner as backup to the IP/MPLS connectivity.
Figure 2. Dispatching Defense traffic with hybrid Nuage Networks SD-WAN

In addition to meeting the rapid increase of traffic, such a solution also allows an easy and rapid interconnection of small governmental sites with traffic QoS characteristics that can use the internet, while providing a fair level of security via IPsec. This approach is well suited to provide connectivity work for military attachés stationed in diplomatic missions around the world. The SD-WAN overlays can quickly connect to each other and to the homeland infrastructure network.

**Extend SDN advantages to the traditional IP network**

While transitioning traditional IP/MPLS networks to the VNF paradigm is still distant, Nokia has developed capabilities on IP/MPLS nodes including NETCONF/YANG and PCE to introduce SDN capabilities. With the Nokia Network Services Platform (NSP), SDN capabilities such as network automation and optimization can boost network agility and efficiency. This SDN paradigm is commonly called Carrier SDN.

Figure 3. Dispatching Defense traffic with hybrid Nokia Carrier SDN
Cross-domain orchestrated hybrid SD-WAN from a single service manager

One prominent promise of SDN and its WAN overlay form of SD-WAN, is greater flexibility and ease of service and network management by harnessing the power of the centralized SDN controller, rather than through individual management of each network node.

However, as discussed above the IP/MPLS networks of private or trusted providers will continue to provide mission-critical network services to Defense infrastructure networks. Under such circumstances, how are the SD-WAN benefits to be realized if the overlay SD-WAN and the underlay private IP/MPLS networks remain as two separate domains with no management and control orchestration?

A single point of cross-domain network services orchestrator with an automated mapping between the overlay and underlay network domain is key to unleashing the full potential of SD-WAN. When a new site or extended traffic profile with specific routing rules is added to the global network, the required configuration and provisioning steps are automatically configured at each relevant network domain in order to implement coherent, end-to-end network services management and deployment.

The Nokia Virtual Network Orchestration (VNO) solution, a global orchestrator, plays such a role. It reduces the complexity of the network and network services management compared with a “siloed” situation, and thereby allows the full benefits of SD-WAN. Furthermore, VNO can be complemented by Nokia FlowOne, which provides orchestration at a higher business layer by mapping business service orders into network service ones.

Figure 4. Global hybrid SD-WAN orchestration with Nokia VNO and FlowOne

The Nokia VNO and FlowOne components are highlighted later in this paper.
Nokia dynamic network components

Nuage Networks solutions

At the core of the Nuage Networks SDN and SD-WAN solution from Nokia is the Virtualized Services Platform (VSP). The VSP architecture comprises three major components that play an active role in the management, control and data planes.

Cloud service management plane – Virtualized Services Directory

The Virtualized Services Directory (VSD) is a policy and business logic engine that simplifies the definition of network services in an application-friendly context.

It provides administrators the freedom to specify the networking requirements of cloud applications in familiar IT constructs and automatically translates these requirements into policies that implement the proper scope, security and integrity of consumption of network resources conforming to the enterprise guidelines.

Data center/WAN control plane – Virtualized Services Controller

The Virtualized Services Controller (VSC) maintains the full view of per-tenant network and service topologies and instantiates network service templates defined through the VSD. Through the VSC, virtual routing and switching functionality can be instantiated in virtual machines (VMs) across the virtualized infrastructure relying upon hypervisors as direct extensions.

Leveraging Nokia’s Service Router Operating System (SR OS), which has proven its resiliency, scaling and performance over a decade of operations in many large IP/MPLS and metro Ethernet networks, the VSC has unprecedented capabilities to drive L2–L4 network virtualization across thousands of tenant slices in a heterogeneous environment.

The VSC uses standard BGP-4 routing protocols to peer with existing networks, allowing it to discover full network topology and reachability. Through OpenFlow, it distributes relevant switching and routing information to hypervisors within the virtualized data center network.

To facilitate hybrid cloud deployments, the VSC ensures seamless interconnection with business VPN services (L2 or L3), extending the virtualized data center environment to securely include enterprise locations.

Through federation of controllers, the VSC scales elegantly and seamlessly to meet the expectations of the largest and most demanding data centers’ cloud services.
Data center/WAN data plane – Virtualized Routing and Switching

The Virtualized Routing and Switching (VRS) module serves as a virtual endpoint for network services. It detects changes in the compute environment as they occur and instantaneously triggers policy-based responses to ensure that the network connectivity needs of applications are met. VRS extensions provide control of network interfaces across leading hypervisor platforms including VMware, KVM, and Xen.

With the Nuage Networks solution, the network can react instantaneously and consistently with policies as VMs are turned up or removed.

Integration with virtualized routing and switching gateways

Nuage Networks gateways allow the integration with “bare metal” objects such as non-virtualized servers and appliances.

For low volume deployments, the software-based VRS Gateway (VRS-G) module incorporates bare metal as virtualized extensions to the data center.

For large-scale and high-traffic volume environments, the Nuage Networks 7850 Virtualized Service Gateway (VSG) provides the gateway functionality with native support for 1GE, 10GE and 40GE connections.

Figure 6. Nuage Networks VSP architecture

Nokia Network Services Platform

The Nokia Network Services Platform (NSP) provides automation to deliver network transport services at faster speed, to optimize network utilization and traffic engineering, and to provide dynamic service assurance with maximum performance and reliability.
It operates across multivendor IP/MPLS, Ethernet, optical and microwave networks. It also spans network layers of both physical and virtual network infrastructures to provide automated provisioning and network services assurance.

**Figure 7. Dynamic management with Nokia NSP**

Its powerful network analytics engine, powered by machine-learning algorithms, performs real-time network path computation and optimization driven by KPIs and metrics and assists network administrators in network maintenance. These powerful innovations enable a rapid dynamic adaptation to changing network conditions and improve network reliability.

Furthermore, capitalizing on the NSP’s open application programming interface (API), the NSP brings to network administrators a DevOps platform that unifies service automation, network optimization and dynamic assurance to deliver network services with agility, efficiency and scalability.

**Nokia CloudBand**

The Nokia CloudBand software suite is an ETSI NFV MANO system that can be deployed for any combination of NFV Infrastructure/Virtualized Infrastructure Manager (NFVI/VIM), Generic VNF Manager (G-VNFM), and NFV Orchestrator. Nokia’s CloudBand supports hybrid infrastructures and is open for multivendor VNFs deployment.
The Nokia CloudBand software suite comprises three key components:

- **CloudBand Network Director**: An orchestrator of virtual network resources (NFV) and network services; built for OpenStack and VMware, it manages virtual resources across geo-distributed NFV infrastructure nodes and automates the life cycle of network services such as virtual CPEs, including their forwarding graphs and service chains.

- **CloudBand Application Manager**: A G-VNFM acting upon both Nokia’s and other suppliers’ VNFs; built for OpenStack and VMware, it automates the life-cycle management of VNF resources and associated workflows.

- **CloudBand Infrastructure Software**: A multi-purpose NFV infrastructure (NFVI) and virtualized infrastructure manager (VIM); built for OpenStack, it virtualizes and manages compute, storage, and network resources.

### Nokia Virtual Networks Orchestration

The Nokia VNO solution allows Nokia SD-WAN services to be overlaid on existing WAN services with new and faster hybrid access to branches, and to automate connectivity for rapid delivery of virtualized services to branch sites.

Moreover, Nokia VNO can further automate service chaining - the chaining of a broad range of virtualized security and other value-added service and applications, e.g. firewall, IDS and WAN optimization, in the data center and SDN-enabled sites. This is realized by a customized service portal, enabling a quick user-friendly command of services, which is automatically translated into the right set of instructions across the WAN, the SD-WAN and the data center.
Figure 9. Nokia Virtual Networks Orchestration (VNO)

![Diagram of Nokia Virtual Networks Orchestration (VNO)]

Nokia VNO further boosts network operations agility, and network services administrators gain end-to-end network orchestration and the automation needed for the rapid deployment of dynamic value-added services.

Figure 10. Seamless sites interconnection and network services deployment with Nokia VNO

![Diagram showing seamless sites interconnection and network services deployment with Nokia VNO]

**Nokia FlowOne**

FlowOne is the Service Orchestrator, which may complement the VNO solution. The Service Orchestrator acts at the business service level, i.e., allows definition of business services that can be ordered by customers. It translates business orders into the deployment of one or multiple underlying network services, the configuration of virtual and physical network functions and provisioning data needed to deliver the required service. It potentially covers multiple network domains such as optical, radio, mobile and/or fixed access network segments.
About Nokia and SD-WAN

Nokia is a recognized leader in IP networking, ultrabroadband access and transmission, and cloud-based networking technology. Nokia pioneers dynamic and resilient networking technology to support mission-critical network operations around the world. Nokia’s mission in the Defense sector is to adapt its expertise in the implementation of dynamic and secure networks to the unique requirements and priorities of armed forces and bring the best of civilian technologies to Defense organizations.

Nuage Networks SD-WAN

As more enterprises migrate their business applications to the cloud, they must provide seamless WAN connectivity not only between branch and regional sites, but also to their private data centers, software-as-a-service (SaaS) providers and public clouds — all within a unified security and governance model. Moreover, there is demand from enterprises to dynamically deploy and manage networks services companion features such as new generation software firewalls and value-added services client-side applications such as VoIP or IoT.

Nuage Networks VNS is the industry’s first and only SD-WAN 2.0 offering, providing a services architecture that overcomes these challenges, and allowing the dynamic deployment and orchestration of enterprise ICT services across data centers, public cloud services, SaaS provider clouds and enterprises’ branch sites.

“Along with end-to-end governance and security for our customers, we welcome the versatility of this SD-WAN 2.0 platform which allows us to not only support a hybrid environment in our datacenters, but also extends to our nationwide branch network. This provides us with crucial end-to-end policy-based network automation and security, giving us full visibility on the connectivity conditions of our branches in order to procure an outstanding customer service.”

— Michel Bouffier, CIO at Banco Multiva
Nokia Carrier SDN

In the recent past, the telecom industry has experienced a surge in creative efforts and developments, producing the components needed for networks to become as agile and efficient as the cloud applications they support. These have been occurring under the umbrellas of SDN, NFV, and service orchestration, and focus has been on abstracting and simplifying the development and delivery of multiple types of network services spanning multiple layers of technology and a wide range of deployment domains.

Nokia, who has been a leader in this SDN/NFV evolution, has also taken a position at the leading edge of the networks transformation process toward becoming more agile engines of innovation.

Nokia’s NSP delivers a unique blend of capabilities to service providers and large enterprises to help them realize their agility and innovation goals in their WANs. Embedding a logic honed over the course of 1000s of network deployments in each key layer of the WAN, it realized a rapid penetration of the carrier SDN segment with many major network operators in all continents, and benefits from the ongoing research at Nokia Bell Labs on WAN operations improvement.

“In order for SDN to mean we can really improve our customer experience and impact our network economics, we need approaches that consider the real-time state of the network and relate it to the requirements of the service we provide. Doing so allows us to assure performance and optimize resource usage across all our network layers. Tightly coupling service requirements and performance with network control, as in NSP, promises to deliver real-world benefits of centralized optimization whilst exploiting the strength of existing distributed network.”

— Rob Shakir, BT End-to-End Network Architect

Conclusion

As networking is now pivotal to Defense operations and missions, network modernization has become a key focus of defense transformation. Nokia can help Defense forces to build a network that serves and protects their citizens better, faster and more efficiently.

To learn more about Nokia solutions for Defense, visit our Defense web page.

Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP</td>
<td>Border Gateway Protocol</td>
</tr>
<tr>
<td>C2</td>
<td>Command and Control</td>
</tr>
<tr>
<td>CPE</td>
<td>customer premises equipment</td>
</tr>
<tr>
<td>FMN</td>
<td>Federated Mission Networking</td>
</tr>
<tr>
<td>G-VNFM</td>
<td>Generic VNF Manager</td>
</tr>
<tr>
<td>ICT</td>
<td>information and communications technologies</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>IPsec</td>
<td>IP Security</td>
</tr>
</tbody>
</table>
About Nokia
We create the technology to connect the world. Powered by the research and innovation of Nokia Bell Labs, we serve communications service providers, governments,
large enterprises and consumers, with the industry’s most complete, end-to-end portfolio of products, services and licensing.

From the enabling infrastructure for 5G and the Internet of Things, to emerging applications in digital health, we are shaping the future of technology to transform
the human experience. networks.nokia.com

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

© 2019 Nokia
Nokia Oyj
Karaportti 3
FI-02610 Espoo, Finland
Tel. +358 (0) 10 44 88 000

Document code: SR1907036922EN (September) CID206616