NOKIA

A blueprint for modernizing defense IT

How agile cloud networks can drive the digital transformation of defense

White paper

Defense organizations must prioritize the digitalization of their operations to maintain an edge in a highly interconnected, competitive global landscape and safeguard against a range of threats, including emerging ones such as hybrid warfare, cyberattacks and climate security. The essential enabler for this digital transformation is a modernized IT infrastructure that offers four key attributes: cloud agility and extensibility, strong survivability, high adaptability and robust cybersecurity. This calls for a novel cloud networking approach that extends connections beyond data centers into the strategic core network, linking user locations to cloud resources.

This white paper presents an end-to-end cloud networking blueprint that provides these four attributes to empower defense organizations and users with the digital capabilities they need to succeed in their missions.

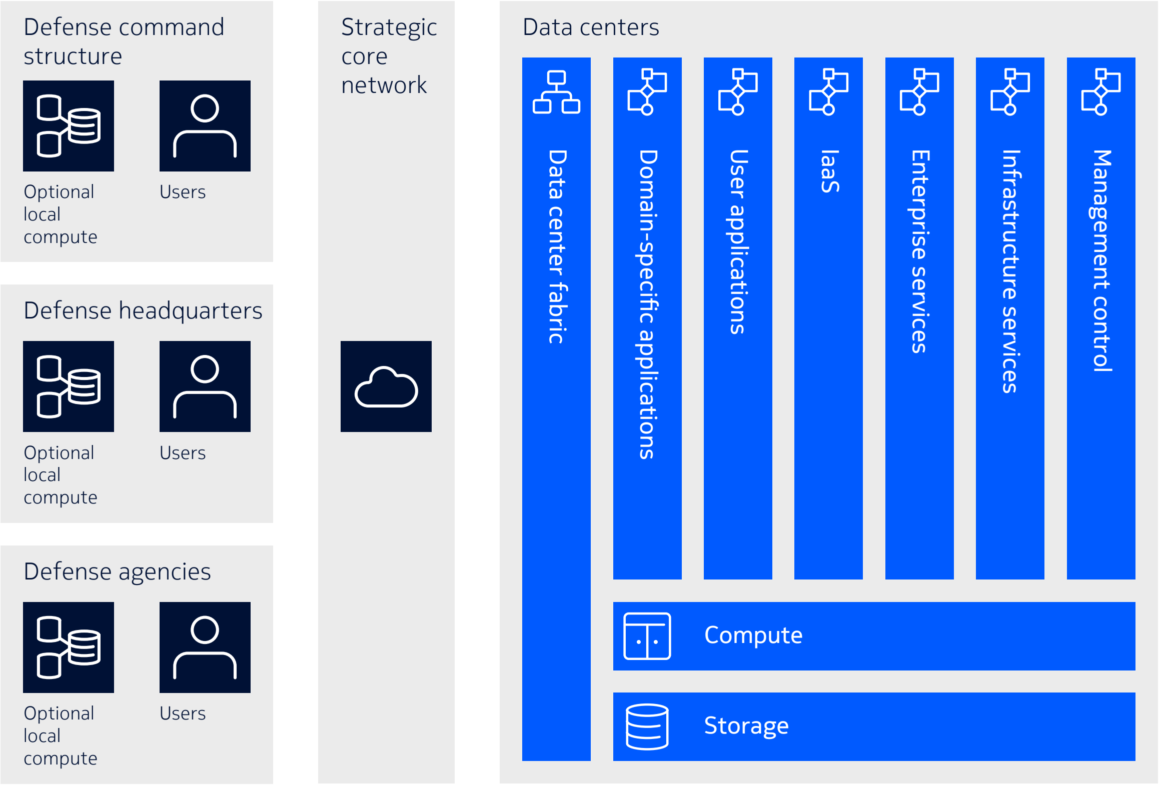
Contents

Introduction

Defense organizations are working to digitalize their command, control and communication (C3) systems because they recognize that superior military hardware alone no longer assures a competitive edge. Faced with a constantly evolving threat landscape, these organizations need uninterrupted access to innovative applications and data to address persistent challenges and stay on top.

The core of this digital transformation is a modernized IT infrastructure (Figure 1) that encompasses compute, storage and networking across the whole defense organization. Compute and storage are housed across centralized data center facilities and strategically distributed at user sites to improve responsiveness. Networking links compute and storage resources with users across the organization through the strategic core network and the data center network, also known as the data center fabric.

Figure 1: Defense IT infrastructure



This modernized IT infrastructure serves as a central component within a data-centric digital defense environment. It requires four essential attributes to meet the demands of defense organizations and users:

1. Cloud agility and extensibility: Application development teams are charged with swiftly delivering new and enhanced digital capabilities that will help defense organizations respond to emerging threats and maintain a strategic edge. These demands are driving them to adopt the DevOps paradigm and Continuous Integration/Continuous Development (CI/CD) concepts in cloud computing environments. Many development teams are also evaluating artificial intelligence (AI) as defense organizations embrace Artificial Intelligence for IT Operations (AIOps). To support these efforts, the IT infrastructure

needs agility to promptly satisfy user demands for infrastructure as a service (IaaS) and platform as a service (PaaS) compute services. It also needs to be extensible to incorporate AI and other emerging frontier technologies.

2. Robust survivability: The IT infrastructure needs to provide the utmost resiliency and rapid recovery capabilities in the face of challenges such as disasters, adversarial actions and equipment failures. These capabilities will ensure that users have uninterrupted access to critical applications and data so they can continue to execute their missions without delay or compromise.
3. High adaptability: Maintaining consistently high IT performance is essential for mission success. To attain this goal, an IT infrastructure needs to be highly adaptable so that it can gracefully navigate adverse conditions and effectively mitigate impacts. It must dynamically reallocate its resources to maintain high performance for critical applications while allowing controlled performance degradation for other services in accordance with contingency plans.
4. Strong cybersecurity: The attack surface expands significantly for modernized IT infrastructure, with threats ranging from cyberattacks seeking to eavesdrop, disrupt and infiltrate to physical attacks on IT facilities. Attackers use diverse methods, including social engineering, phishing and vishing techniques, and exploit emerging technologies to launch quantum computing or brute-force attacks. This multifaceted threat landscape underscores the need for a multilayered defense-in-depth cybersecurity framework.

Existing defense network infrastructure cannot readily support these four attributes, so it must evolve along with compute and storage. The evolved network infrastructure needs to embody the agility and extensibility of a cloud environment, continuously ensuring secure and timely data delivery for critical applications, even during challenging circumstances. The remainder of this paper will describe an agile cloud networking blueprint aimed at achieving this goal.

An agile cloud networking blueprint for defense IT

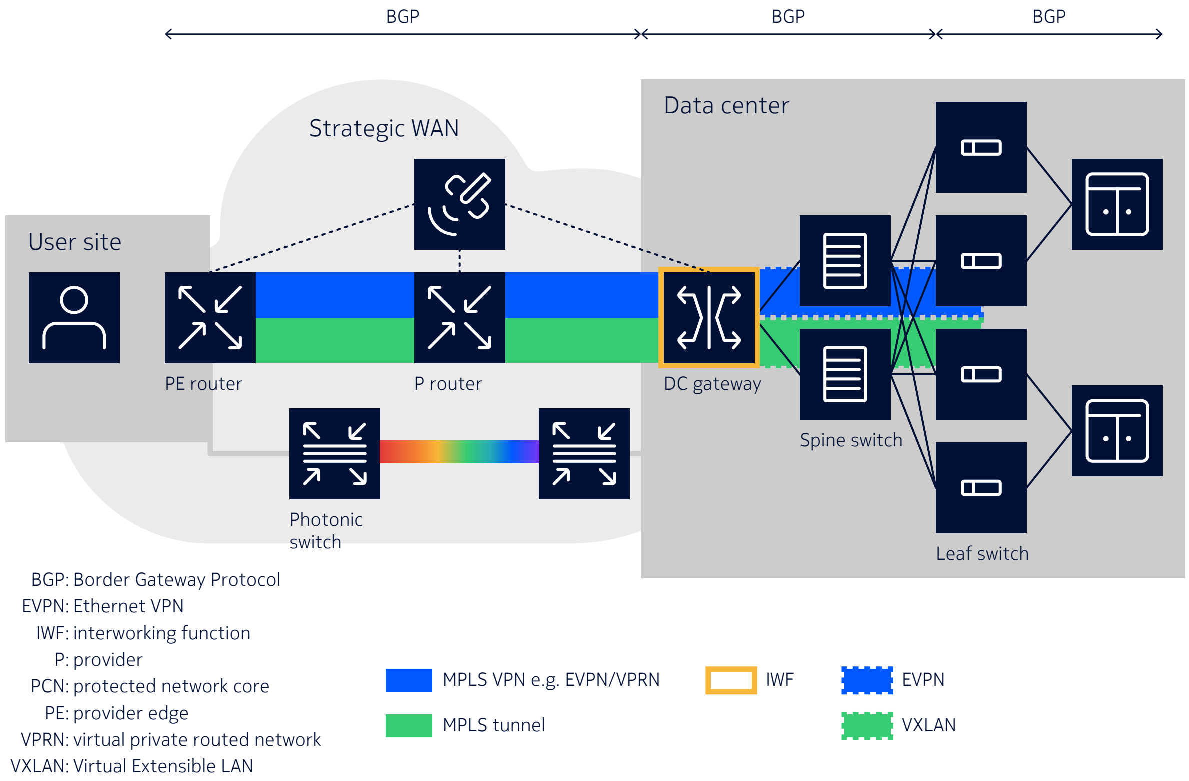
This blueprint supports network extensibility for user-built capability, utilizes Border Gateway Protocol Version 4 (BGP4) for dynamic user-to-cloud survivability, employs traffic engineering with real-time telemetry to adapt to network impairments, and fortifies the network with quantum-safe encryption.

As shown in Figure 2, the blueprint combines two network realms:

- A multilayer core network for connecting user sites and data centers
- A data center network for connecting compute and storage resources.

Together, these network realms provide seamless end-to-end connectivity that enables users across numerous locations to access applications, data and cloud resources within data centers.

Figure 2: An agile cloud networking blueprint



BGP: Border Gateway Protocol
EVPN: Ethernet VPN
IWF: interworking function
P: provider
PCN: protected network core
PE: provider edge
VPRN: virtual private routed network
VXLAN: Virtual Extensible LAN

Multilayer IP/MPLS core network

The strategic core network is a multiplayer IP/MPLS core network. It comprises provider edge (PE) routers, Provider (P) routers at the IP layer and photonic switches at the optical layer. At the IP layer, the blueprint adopts a service-centric paradigm where MPLS virtual private networks (VPNs) ride over MPLS tunnels in the data plane to meet the diverse connectivity needs of numerous entities within the organization and associated application domains. In the control plane, the BGP4 protocol distributes VPN-specific routes and establishes VPN services across all PE routers. The PE routers enforce network segmentation between entities and application domains with virtual routing and forwarding (VRF) instances. The P routers are core routers that connect PE routers. In real-life deployments, the P routers are often PE routers in larger user sites. BGP4 can be used between user gateway routers and PE routers to support dynamic customer route distribution. To address escalating bandwidth demand, the blueprint scales effectively with the use of ultra high-speed router links such as 100GE/400GE and 800GE.

The blueprint also includes an optical layer with photonic switches that provide flexible, efficient transport of traffic within the protected core network (PCN). Fiber capacity is optimally utilized through multiplexing techniques such as dense wavelength-division multiplexing (DWDM), optical transport networks (OTNs) and reconfigurable optical add-drop multiplexers (ROADMs) as determined by the bandwidth and application needs of various network users. Transport speed scales easily to more than 1.2 Tb/s per wavelength using modern coherent optical detection and processing.

Data center network

The data center network consists of a data center fabric (hereafter referred to as “the fabric”) and a data center gateway (hereafter referred to as “DC gateway”). The fabric connects racks of servers and storage that house applications and data. In a DevOps environment that leverages virtual compute technology such as containers and microservices, a leaf-and-spine architecture optimizes connectivity between microservices for the so-called “east–west” traffic within the data centers. When additional racks are deployed, new compute-connected switches (called leaf switches) can be seamlessly added to connect to existing core switches (called spine switches) without disrupting existing connections.

Like the core network, the data center network adopts a service-centric paradigm, with Ethernet VPN (EVPN) over Virtual Extensible LAN (VXLAN) tunnels with BGP4 distributing EVPN-specific routes and establishing EVPN services in the leaf switch. BGP4 is used between leaf switches and application endpoints on servers to enable dynamic end-to-end routing.

The DC gateway, straddling the core network and data center network realms, performs the pivotal task of internetworking in this blueprint. Harnessing its internetworking function at the service and network layers, it joins the VPN services in the PCN realm and the EVPN services in the data center network realm to enable end-to-end cloud networking connectivity. It also performs the important task of extending BGP4 from the PCN realm to the data center network realm, elegantly unifying service provisioning in both realms. Additionally, the DC gateway serves as a a crucial quality of service (QoS) enforcer that prevents traffic overload in the core network. It acts as the first line of defense for data center security, implementing comprehensive security policy through access control list (ACL) without compromising performance.

Essential network blueprint attributes

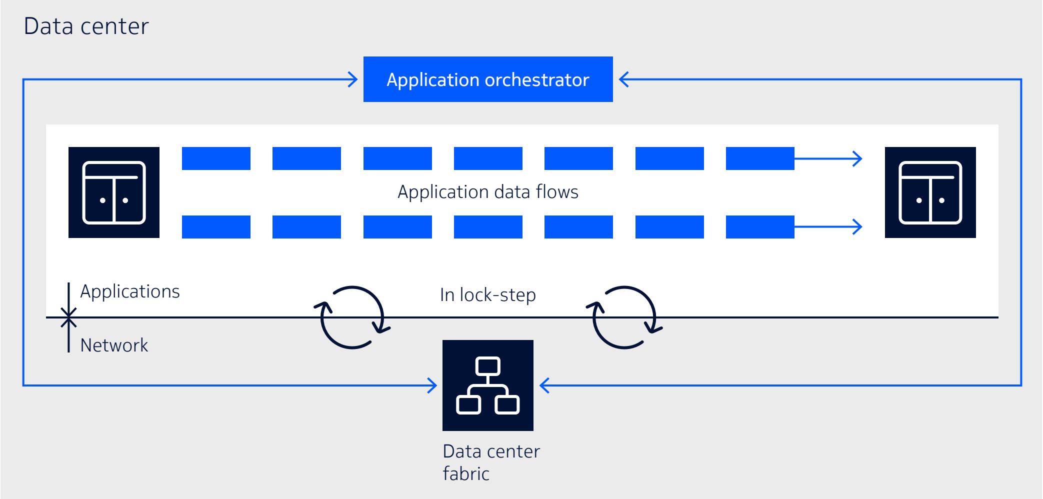
This section explores how the essential attributes of the network blueprint satisfy the requirements of the modernized IT infrastructure outlined earlier in the paper.

High network agility and extensibility

IT network operations are used to operate as isolated silos with minimal automation and limited interactions with applications. With DevOps and CI/CD, the fabric must adapt to new challenges created by rapid changes in application development. These include quickly provisioning new network services, continuously optimizing fabric configurations and expanding capacity to synchronize with the heartbeat of the application layer (Figure 3).

The NetOps paradigm harnesses the power of automation to effectively address these challenges. NetOps applies DevOps principles to the network layer, making network resources agile and responsive to on-demand consumption of compute resources by different applications. It empowers IT teams with the capabilities they need to start new projects, enhance existing applications and rapidly deliver software fixes.

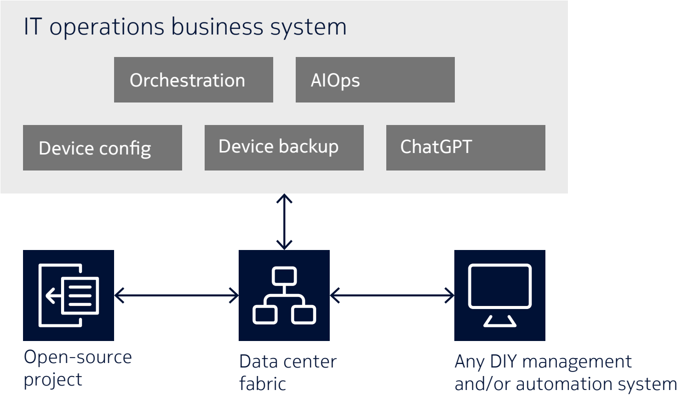
Figure 3: Fabric synchronizes with the application layer



At the core of NetOps is a NetOps development kit (NDK). The NDK is a programmable toolkit for the network operating system (NOS) of fabric switches. It enables the development and execution of custom applications in the switch, running alongside native NOS modules. Using language-agnostic, open protocols such as the gRPC network management interface (gNMI), the NDK brings agility to the fabric and ensures that it seamlessly integrates with IT ecosystems, including cloud management systems (CMSs), to provide on-demand connectivity.

The NDK also brings extensibility to the network by enabling the integration of custom applications with external systems and services. For example, an application could use the NDK to connect with the International Space Station (ISS) tracking system by making an HTTP request to https://api.wheretheiss.at/v1/satellites/25544.[1] It could then add the obtained ISS coordinates to the NOS's state data store, which is accessible through interfaces such as command-line interfaces (CLIs), gNMI and JavaScript Object Notation Remote Procedure Call (JSON-RPC). Similar approaches could be utilized to develop applications that trigger network actions, such as modifying QoS policy. The NDK can also support the development of applications that integrate with AIOps services such as the OpenAI API and ChatGPT to harness the power of AI to assist in fabric operations.[2]

Figure 4: Seamless integration into IT ecosystems and other external services



[1] Visit https://github.com/KTodts/srl-satellite-tracker for more details.
[2] Visit https://learn.srlinux.dev/ndk/apps/srl-gpt/ for more details.

Robust network survivability

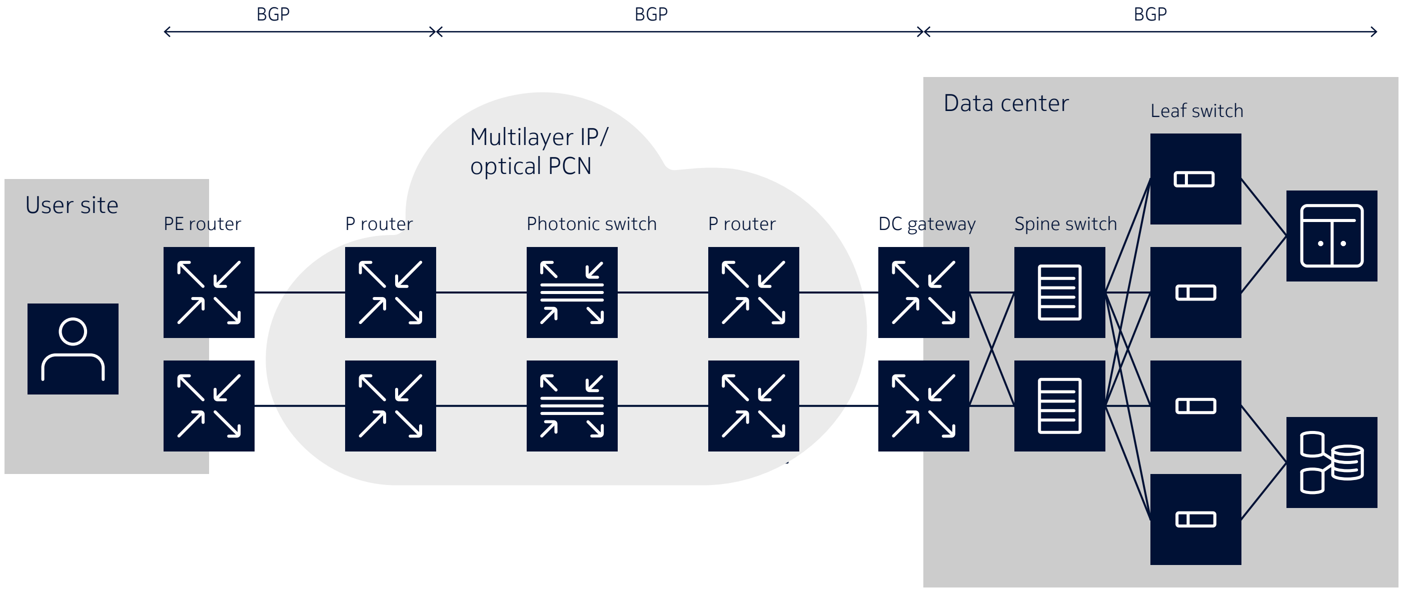
It is imperative for the cloud networking blueprint to incorporate the highest level of resiliency from data centers to user sites. The blueprint addresses this need by extending a multilayer, end-to-end network protection framework across the PCN and data center network realms. Harnessing various resiliency capabilities at different layers, the protection spans from application endpoints connected to leaf switches to gateway routers at user sites (Figure 5).

Figure 5: A cross-domain multilayer resiliency framework

Protocol layer	Protection scheme
Service	EVPN/BGP4/PW routing
IP	VRRP/ECMP/BGP4/FRR/NSF/graceful restart
Ethernet	LAG/MC-LAG
Nodal	1+1 hardware redundancy/dual gateway
Topology	Dual-homing

Protocol layer	Protection scheme
Service	Not applicable
IP	ECMP/BGP4/FRR/NSF/graceful restart/TI-LFA
Ethernet	LAG/MC-LAG
Nodal	1+1 hardware redundancy
Topology	Ring/mesh diverse path redundancy

Protocol layer	Protection scheme
Service	EVPN/BGP4/PW redundancy
IP	ECMP/NSF/graceful restart
Ethernet	LAG/MC-LAG
Nodal	1+1 hardware protection
Topology	Leaf/spine path redundancy/dual DC gateway

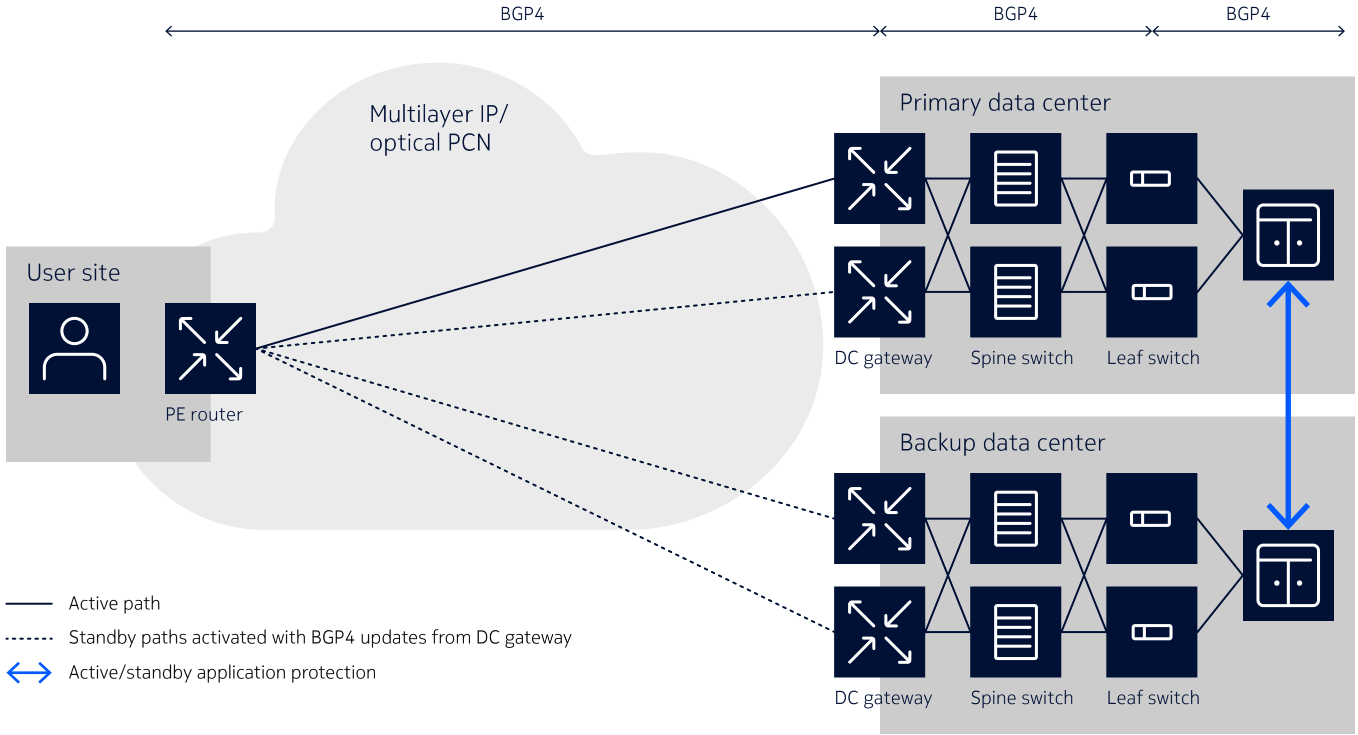


When implementing the protection framework, the IT team must analyze and understand the protection requirements at each protocol layer:

- Topology layer: Path diversity is a key consideration for high connectivity availability. It starts at the edge, where dual PE routers at user sites are connected to the P routers and servers in data centers are dual-homed to leaf switches. In the core network, a ring complemented by mesh links over diverse optical paths wherever possible can provide excellent path redundancy. In the data centers, a leaf-spine topology offers full path redundancy towards the data center gateway.

- Nodal layer: Deploying dual gateways in data centers and priority user sites can significantly boost network resiliency. IT teams can also capitalize on 1+1 hardware redundancy protection in gateways to support high nodal availability. The deployment of new routing technology breakthroughs such as warm restart and warm reboot in a non-redundant router platform can further boost network resiliency. Warm restart allows hitless upgrades of specific protocol stacks without affecting data forwarding. Warm reboot enables software upgrades without a service impact.
- IP and Ethernet layer: IETF an IEEE have defined a rich set of standard-based protection tools (see the IP and Ethernet rows in the Figure 5 tables).
- Service layer: Service layer resiliency plays a vital role in maintaining high application availability. In the data center, active/active dual-homing to leaf switches with EVPN using BGP4 offers strong survivability. Moreover, dynamic BGP4 routing in the strategic core network and data center network realms enables geo-redundancy protection for applications. In Figure 6, an application has its active and standby instances in two different data centers. If the active instance fails, BGP4 routing can propagate route withdrawal all the way to the PE router, activating the standby path. This triggers the redirection of data to the standby application instance in the secondary data center, restoring access to the application.

Figure 6: Geo-redundancy with BGP4



High network adaptability

Consistently high network performance is essential for maintaining high application performance at all times. However, network congestion and impairments occur from time to time. When they happen, the network needs to adapt intelligently to ensure that critical application performance is not impacted while allowing the performance of non-critical applications to degrade in a graceful manner.

When a new network service is initially provisioned, it is allocated the necessary network resources to meet the defined service intent, including aspects such as bandwidth and delay. As more services are integrated into the network, network resource contention inevitably arises, creating the potential for deviations from the original service intent. In addition, unforeseen disruptions such as major fiber cuts could cause affected traffic to re-route to other network paths, leading to congestion that results in packet loss. All these factors have the potential to impair application performance and keep users from completing their missions or performing their daily tasks.

Real-time network observability and resource control are essential for tackling these challenges. These capabilities can be enabled with network nodes that support real-time network telemetry using the open protocol gNMI. Supplied with the telemetry information, the network operations support system (OSS) can detect and adapt to network issues in near-real time. For example, if real-time telemetry reveals that network congestion is causing packet drop (Figure 7a), the OSS could use traffic engineering capabilities offered by Resource Reservation Protocol - Traffic Engineering (RSVP-TE) in IP/MPLS and Segment Routing Traffic Engineering (SR-TE) to re-route the non-critical traffic to an alternate path and resolve the congestion issue. The critical traffic would stay on course to ensure that delay and path policies such as hop count are not violated (Figure 7b).

Figure 7a: Congestion detected by real-time telemetry

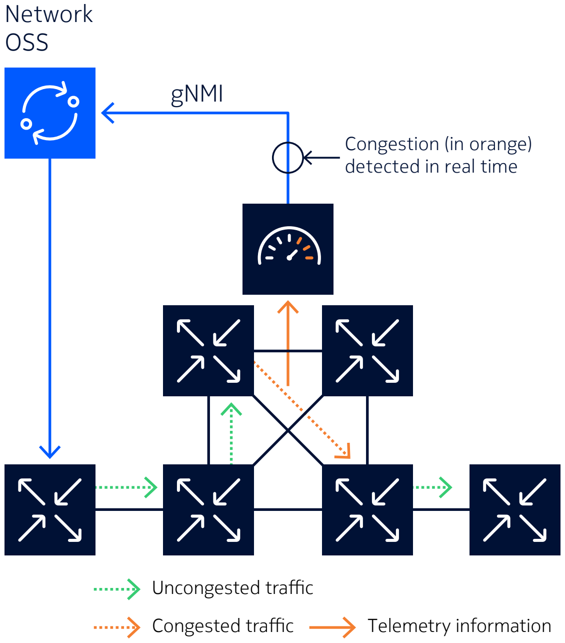
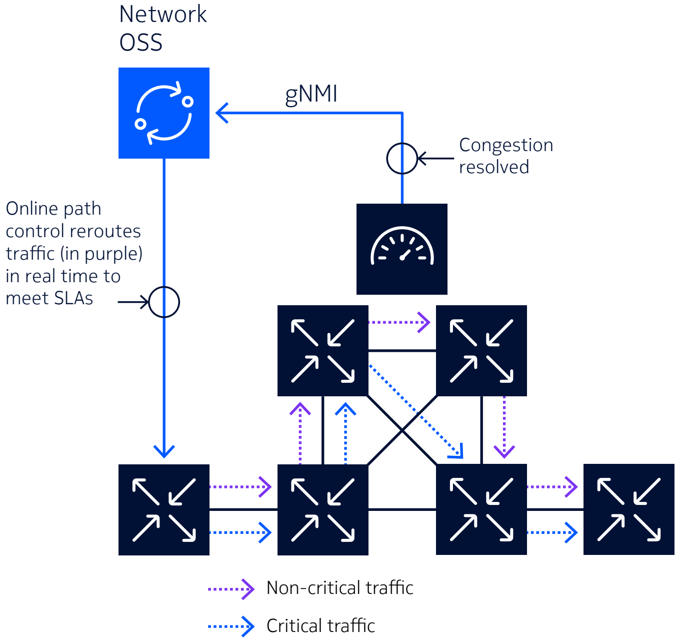


Figure 7b: Network OSS re-routes non-critical traffic to alternate path to resolve congestion


Network OSS
gNMI
Congestion resolved
Online path control reroutes traffic (in purple) in real time to meet SLAs
Non-critical traffic
Critical traffic

Strong network security

The network is the first line of defense in a defense-in-depth framework. Network security tools that can be used to protect a modernized defense IT infrastructure include:

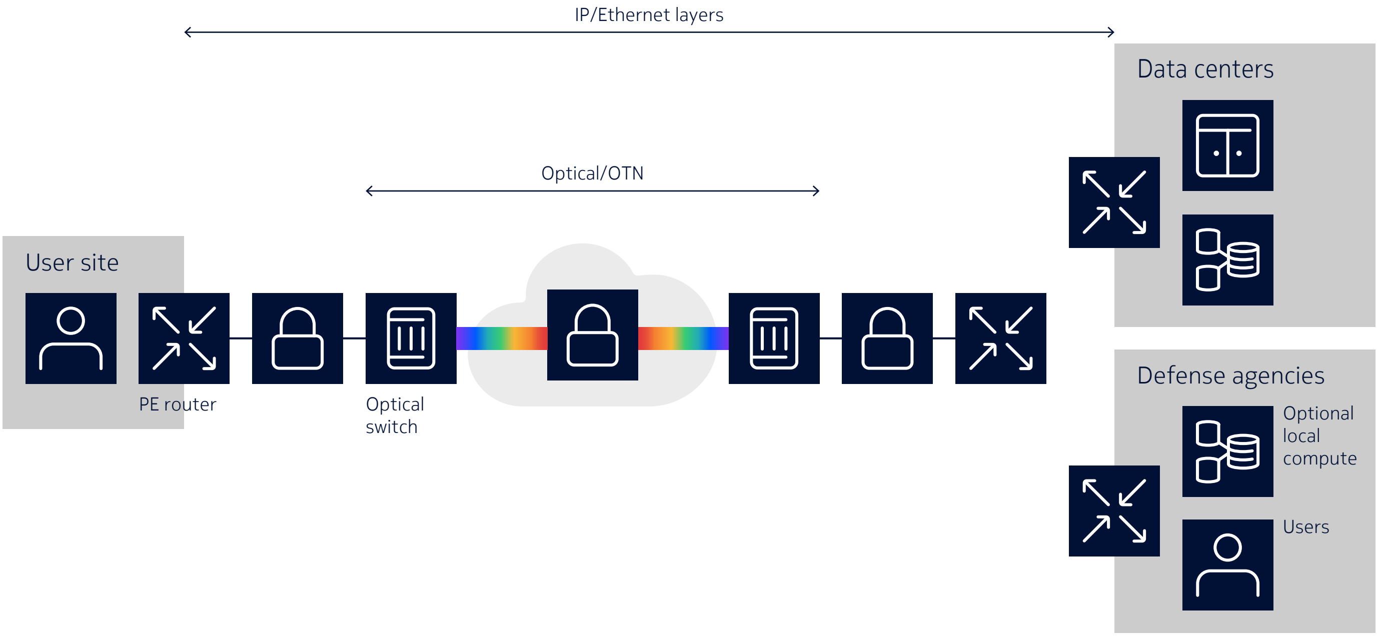
- Network segmentation: VPN services such as EVPN can be used to virtually split the network into different segments dedicated to specific user or application domains. This protects the users or applications from illicit traffic coming from compromised domains. Network segmentation effectively limits the lateral movement of bad actors.

- IP filtering: IP filtering with ACLs can stop illicit traffic sent by attackers or compromised servers or user devices. Cutting-edge router hardware can now filter traffic beyond the typical 5-tuples (source/destination IP addresses, source and destination port numbers and protocol numbers) into the IP payload. Orchestrated with distributed denial-of-service (DDoS) mitigation applications, IP networks can play an integral role in DDoS mitigation, filtering out attack traffic before it enters the network.
- Quantum-safe encryption: Traffic transported across the network is vulnerable to eavesdropping. It may include highly sensitive intelligence information or command and control traffic for physical defense infrastructure. This data has significant value to potential adversaries who may seek to access sensitive information or disrupt system operations. Encryption has been an effective way to safeguard the confidentiality, integrity and authenticity of traffic.

There are now deep concerns about the advent of cryptographically relevant quantum computers (CRQCs) that could crack today's widely used asymmetric cryptography.[3] With CRQCs, bad actors can "harvest" data now and decrypt it later (HNDL). While quantum key distribution (QKD) and post-quantum cryptography (PQC) are promising future security solutions, it is important for defense organizations to deploy quantum-safe protection now.

Symmetric cryptography such as Advanced Encryption Standard (AES) with a key size of 256 is recognized as an effective protection against quantum threats. This blueprint adopts AES256 encryption with a multilayered approach. It offers full flexibility to apply Layer 1 encryption to secure wavelengths in the optical core[4] and extend the quantum-safe protection to the IP edge at the user site with MACsec or ANYsec[5] (Figure 8).

Figure 8: A multilayered quantum-safe encryption framework



[3] Read the paper entitled "A quantum cybersecurity agenda for Europe" and the report entitled "Quantum-Readiness: Migration to Post Quantum Cryptography" for more details.

[4] Please visit https://www.nokia.com/networks/optical-networks/secure-optical-transport/ for more details.

[5] Please visit https://www.nokia.com/networks/security/ip-network-security/ for more details.

Conclusion

This paper presents a novel blueprint for agile cloud networking that joins the data networking and core network realms. The blueprint provides the four attributes that modernized defense IT infrastructures need to support the digital transformation of C3 systems: high agility and extensibility, robust survivability, high adaptability and strong security. These attributes are instrumental in ensuring that users have continuous, secure access to digital applications and data as they carry out their missions in securing and safeguarding critical strategic interests.

Learn more

Visit our website to learn more about Nokia solutions for defense:

- Defense technology and communications
- Data center solutions
- IP networks
- Network Services Platform

Abbreviations

ACL	access control list
AES	Advanced Encryption Standard
AI	artificial intelligence
AIOps	Artificial Intelligence for IT Operations
C3	command, control and communication
CE	customer edge
CLI	command-line interface
CMS	cloud management system
CRQC	cryptographically relevant quantum computers
BGP4	Border Gateway Protocol version 4
DDoS	distributed denial of service
DWDM	dense wavelength-division multiplexing
ECMP	Equal Cost Multipath
EVPN	Ethernet virtual private network
FRR	Fast Re-Route
gNMI	gRPC network management interface
gRPC	remote procedure call
IaaS	infrastructure as a service
IP	Internet Protocol

ISS	International Space Station
IT	information technology
IWF	internetworking function
JSON	JavaScript Object Notation
LAG	link aggregation group
MC-LAG	multi-chassis link aggregation group
MPLS	Multi-protocol Label Switching
NDK	network development kit
NSF	non-stop forwarding
NOS	network operating system
OTN	optical transport network
OSS	operations support system
PaaS	platform as a service
PCN	protected core network
PE	provider edge
PQC	post-quantum cryptography
P router	Provider router
PW	pseudowire
QKD	quantum key distribution
QoS	quality of service
RPC	remote procedure call
RSVP-TE	Resource Reservation Protocol - Traffic Engineering
SR-TE	Segment Routing Traffic Engineering
TI-LFA	topology-independent loop free alternate
VPN	virtual private network
VPRN	virtual private routed network
VRF	virtual routing and forwarding
VRRP	Virtual Router Redundancy Protocol
VXLAN	Virtual Extensible LAN

About Nokia

At Nokia, we create technology that helps the world act together.

As a B2B technology innovation leader, we are pioneering networks that sense, think and act by leveraging our work across mobile, fixed and cloud networks. In addition, we create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs.

Service providers, enterprises and partners worldwide trust Nokia to deliver secure, reliable and sustainable networks today – and work with us to create the digital services and applications of the future.

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: 789903 (December) CID213822