NOKIA

Empowering military forces everywhere with ultra-broadband IP and cloud networking

Soldiers can go weeks without food, days without water, but only minutes without data

Strategic White Paper

NOKIA

Contents

Defense market and trends	3
Network-Centric Warfare, a competitive advantage	4
Defense imperatives	4
Cost effectiveness and simplicity	5
Robustness and reliability	5
Flexibility and asset optimization	5
Security and cyber defense	5
Military network solutions for defense	6
IP network for defense	7
Converged IP/MPLS WAN with optical transport network	7
Ensuring integrity of classified communications	9
Protecting network and traffic	10
IP/MPLS backhauling for defense	11
Unified network management for defense	12
Data center interconnect and virtualized network services for defense	13
Ultra-broadband access for defense	14
Why partner with Nokia?	16
Acronyms	18

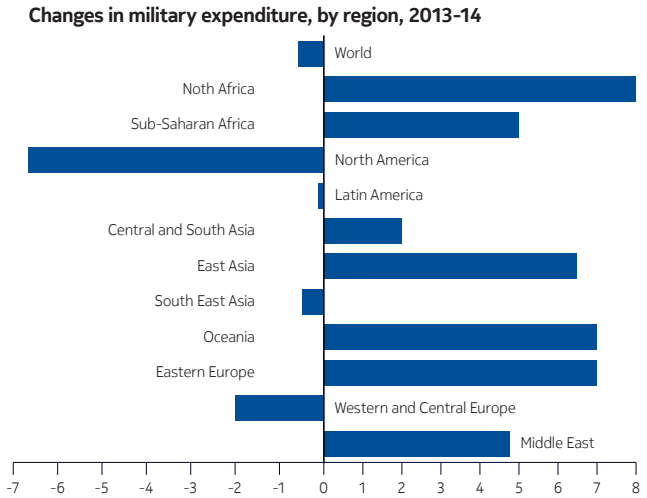
Defense market and trends

For several years after the end of the Cold War, military spending on operations and equipment (OPEX and CAPEX) continued to rise. The much-anticipated 'Peace Dividend' never actually materialized. It was rapidly overtaken by events – regional tensions in the Balkans, military interventions in Afghanistan, Iraq, Libya and Mali, as well as the enduring 'Global War on Terror'. Moreover, instability arising from the 'Arab Spring' has added to this long list of international security priorities.

Against this backdrop of increased insecurity lies the unwelcome impact of the 2008 financial crisis on military budgets in the West. While countries in the Middle East and Asia are experiencing unprecedented military expansion, NATO and its closest allies have had to drastically reduce their spending.

New areas of competitiveness will be about highly interconnected military forces, enhancing situational awareness and shortening the time it takes to make decisions, to take action on a particular event or situation, through distributed electronic Network-Centric Warfare (NCW) capabilities across the air, land and sea domains. Faster access to secure, ubiquitous real-time data/voice/video communications is becoming the key advantage on the battlefield and beyond. In today's operational theaters, soldiers can go weeks without food, days without water, but only minutes without data.

Figure 1. Changes in military expenditure by region in % (Source SIPRI)



NOKIA

Network-Centric Warfare, a competitive advantage

Network-Centric Warfare (NCW) is a combat-proven concept that translates information superiority into a battlefield advantage by shortening the time it takes to distribute data via linked electronic networks embracing aircraft, vehicles, warships and most importantly people. NCW is based on the following core principles:

- A robustly networked force improves information sharing.
- Information sharing enhances shared situational awareness.
- Enhanced, shared situational awareness improves and accelerates decision-making.

These simple functions dramatically increase mission effectiveness and success rates, reducing the requirement for overwhelming force levels. Next-generation IP/ultra-broadband solutions enable the robust interconnection of forces in a seamless way, providing more efficient information sharing, leading to the increased mission effectiveness that many nations now require.

Defense imperatives

"Current organizational structures, modus operandi and Rules of Engagement differ from one operation to another. Moreover, their tendency to change frequently during the same military operation demands ever more agility and versatility. For these reasons, armed forces must be equipped with ever more efficient, interoperable and flexible information and communications systems that can adapt to any kind of situation.

A dynamic cyber-secure network infrastructure provides safe real-time data/information transmission, especially video. This is vital as it offers military Chiefs, Ministers and Heads of Government a clear understanding of any given situation and helps them take the appropriate decisions for adapting to the changes in the battlefield," says Lieutenant-General (Retd) in French Army, Etienne LAFONTAINE.

To address these specific military needs for hyper-connected and empowered forces, a next-generation dynamic telecommunications and IT infrastructure is required enabling the following features.

NOKIA

Cost effectiveness and simplicity

Having to spend defense budgets more cost effectively has resulted in military organizations, especially in western nations, looking to employ advanced civil telecommunications technologies instead of expensive bespoke systems. Consequently, the ability to leverage the advances of commercial off-the-shelf (COTS) technology in military networks is one of the major priorities facing today's defense organizations.

Increasingly, military staff turns toward IP standard systems that are user-friendly and intuitive, as well as easy to implement and manage.

Robustness and reliability

The key, however, is to leverage the technical advances and cost effectiveness achieved by COTS equipment without sacrificing reliability. The defense establishment requires carrier-grade reliable network solutions that are engineered to meet or exceed high availability standards, and provide very fast fault recovery through redundancy measured in milliseconds. Moreover, user-friendly manageability of mission-critical traffic is essential for achieving flawless and effective mission execution.

Flexibility and asset optimization

Electronic intelligence systems, sensors, airborne drones (UAVs), robots (UGVs)... the vast array of platforms and equipment in use by modern militaries are interconnected and generate a lot of data traffic. Then, armed forces should be able to benefit from the proliferation of new types of applications and data traffic, such as advanced unified collaboration, digital imaging and video streaming. Therefore, any new system based on a next-generation IP/Multiprotocol Label Switching (MPLS) WAN combined with data center consolidation, must take this into account in order to realize the benefits of these new applications.

Security and cyber defense

All connected systems must guarantee the highest levels of security and cyber defense across the entire network. It must be possible to segregate and protect networks as well as detect cyber intrusions.

- Network segregation ensures flawless separation of data flows according to the user community's classification levels. Unclassified networks, which are generally used for day-to-day administrative tasks, can be connected to the public Internet, whereas classified networks should be isolated in order to maintain secrecy.

- Network protection is paramount as defense departments are increasingly relying on greater levels of connectivity between command nodes, sensors and weapon systems. These critical data links need to be protected from physical and electronic threats. The resiliency offered by mesh networks greatly enhances service protection. Similarly, “trust of supply” is a significant added protection against malware threats.
- Intrusion detection requires not just impenetrable defenses but also a global security policy framework that includes a monitoring capability to detect unwanted intrusions through the network perimeter.

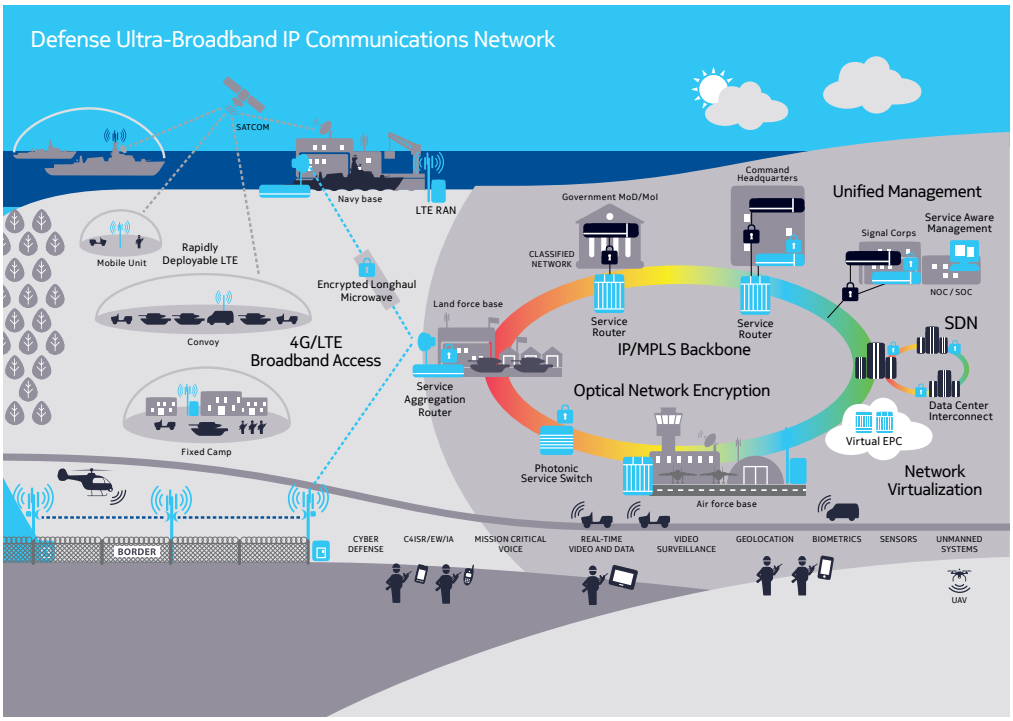
Military network solutions for defense

Network applications for defense – Command and Control (C2) systems, multinational information sharing, situational awareness, collaborative mission planning, split-base operations, virtual intelligence teams and so on - are flourishing and rely on secure and reliable communication networks, which are generally distinguished as follows:

- Strategic networks: consisting of static networks that connect national defense infrastructures for general-purpose and operational services supporting unclassified and classified information. They are usually based on a mission-critical optical and IP/MPLS network for the WAN infrastructure with wireless Long-Term Evolution (LTE) systems for coverage or interconnection of fixed military enclaves at national scale.
- Tactical networks: communications systems addressing field requirements. Generally, tactical networks are made of information and communications technology (ICT) bubbles for:
  - Deployable military camps
  - Warship communications
  - Military convoy communications
  - Battlefield communications

  Outside of radio combat systems, they rely on high-capacity network solutions, predominantly consisting of wireless and 4G/LTE deployable systems for data overlay communications combined with compact IP/MPLS core and backhaul infrastructure.
- Satellite networks: enable long-distance connectivity between national territories, overseas theaters of operation and naval vessels. Satellite communications are also used by deployed forces for communicating with aircraft and when the local terrain, such as mountains or urban areas, prevents direct connection.

Figure 2. Ultra-Broadband IP Communications Network for Defense



IP network for defense

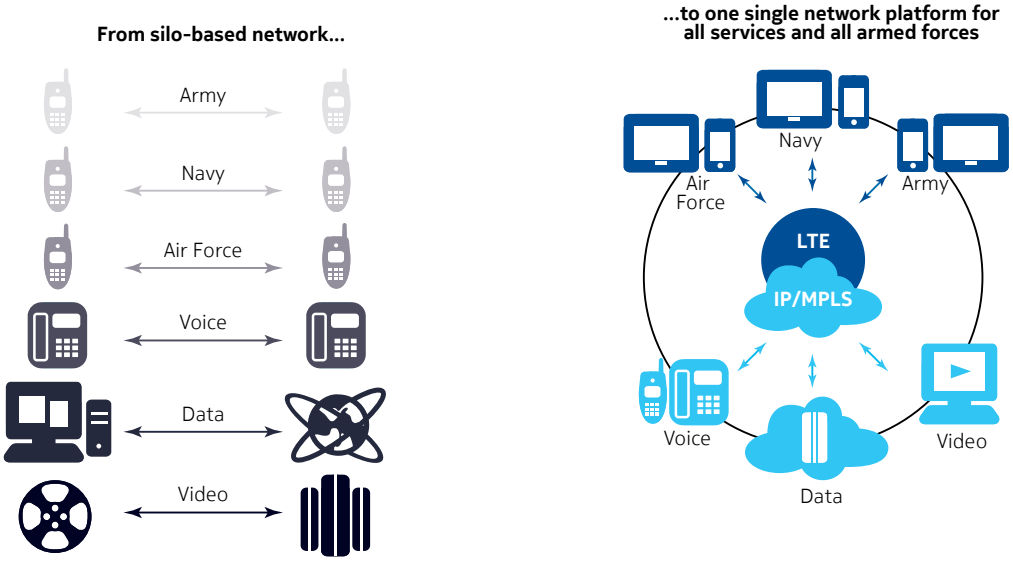
IP/MPLS network transformation will dramatically improve the response capability of defense organizations, allowing broader use of IP-based applications for improved information sharing, situational awareness and faster decision-making.

Converged IP/MPLS WAN with optical transport network

According to Lt Col Giles Ebbutt (Retd), former Royal Marines Communications Officer and Consultant Editor of Jane's C4ISR and Mission Systems, "Everyone is adopting IP systems these days. In a sense, if you are not IP then you are not in the game. It allows the move from siloed stovepipes to a unified network where it is much easier and quicker to move the data around and share it with those who need it. Silos can mean that you are left with an incomplete picture. Put another way, your situational awareness is not as good as it could be because some of the information which has been collected is not available on a particular network. IP/MPLS technology could solve this problem. In fact, it already does."

Indeed, higher capacity, next-generation IP/MPLS networks deliver the required bandwidth to efficiently support IP-based applications' traffic and legacy applications simultaneously. They replace silo-based networks like Synchronous Digital Hierarchy/Synchronous Optical Networking (SDH/SONET) and Time Division Multiplexing (TDM) with a single unified network that implements standard technologies, for easier cooperation between defense organizations.

Figure 3. A typical strategic WAN in a Defense application



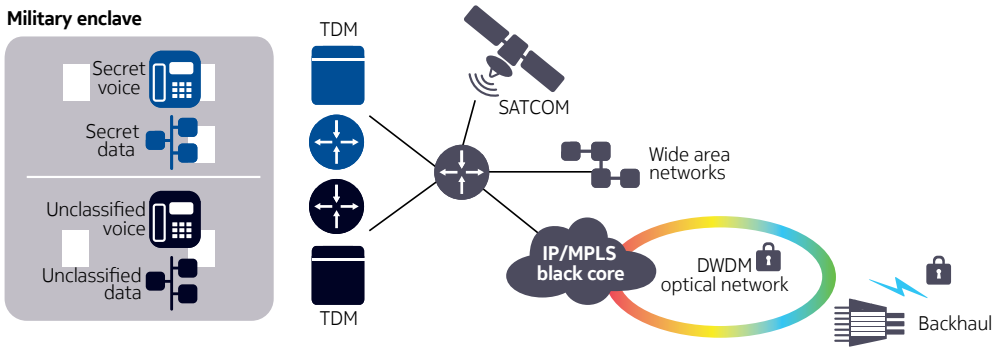
IP/MPLS technology enables the provision of premium service-grade Layer 1 (TDM) as well as Layer 2 and 3 virtual private network (VPN) end-to-end services. The versatility of its 'Tunnel Label' technology enables organizations to adapt to new services and applications with service-level privacy, security and reliability standards, regardless of whether the communication is point-to-point or multipoint - Ethernet, IPv4/v6, IP/MPLS.

The IP/MPLS backbone over an optical Wavelength Division Multiplexing (WDM) multiservice transport solution is therefore a simplified robust architecture that supports a wide range of applications and services. It guarantees high performance and an evolution path from 100G to 400G transport. Furthermore, the integrated packet optical transport cost effectively manages the grooming of IP/Ethernet traffic for better fiber utilization, and generates savings in terms of overlay router ports.

Ensuring integrity of classified communications

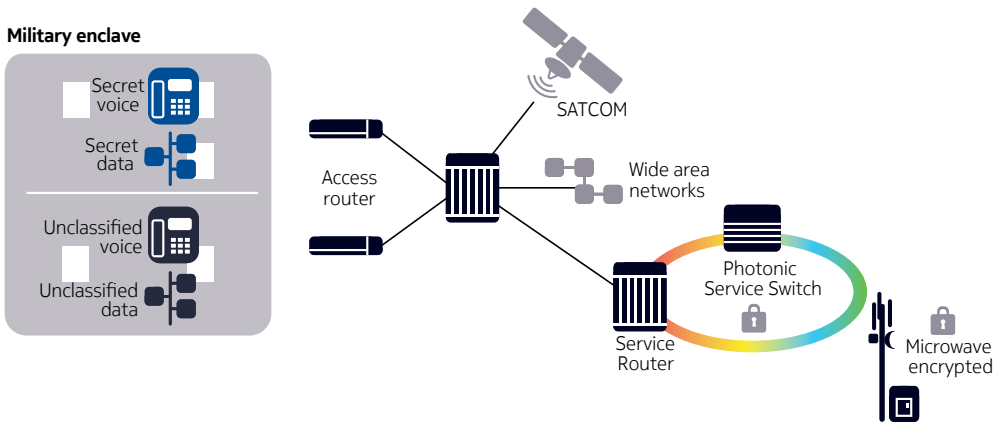
In defense applications, the notion of Red/Black communications, as depicted in Figure 4, refers to the type of information that can be transmitted over a particular media solution. A Red communications system carries fully protected classified plain text data, whereas, a Black system carries unclassified plain text and classified cipher text. Consequently, if classified information is to be transmitted over a Black network, it must first be encrypted or ciphered using an approved Communications Security (COMSEC) system.

Figure 4. Typical Red/Black architecture in a defense WAN



A dynamic network solution would associate products in a Red/Black network as shown in Figure 5. In the inner military enclave, a router like the Nokia 7705 Service Aggregation Router (SAR) allows the smooth migration of legacy services over IP/MPLS architecture while also enabling new Ethernet-based services. When associated with a core router such as the Nokia 7750 Service Router (SR), VPN services are established in the Black core network over a Dense Wavelength Division Multiplexing (DWDM) layer.

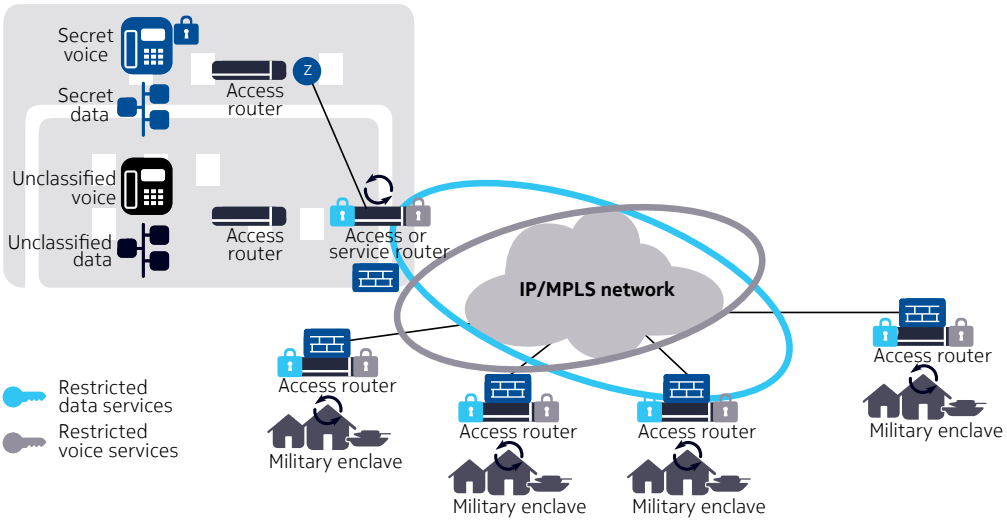
Figure 5. Nokia solution for Red/Black architecture



Protecting network and traffic

In a traditional strategic network, where all military enclaves are able to communicate with each other, IP Security (IPSec) encryption is set according to scale. This can present significant challenges for the provisioning and management of encryption keys. To overcome this complexity, a Network Group Encryption solution provides native MPLS any-to-any encrypted connectivity as shown in Figure 6. As a result, the number of keys to be managed is simply linked to the number of user groups sharing the same encryption domain whatever the complexity and size of the network. In addition, the use of a native MPLS solution protects the migration and transport of critical legacy services, ensuring traffic integrity, confidentiality and authenticity.

Figure 6. Network Group Encryption



On an optical network, Layer 1 encryption is indeed the most appropriate solution for transporting data in the most secure manner without scarifying the latency as it prevents theft or intrusion on the network and any subsequent malicious use of data.

Layer 1 encryption solutions can complement traditional IPSec point-to-point encryption for data center interconnection or optical backbone protection where traditional encryption systems lack sufficient scale, performance and multiprotocol support.

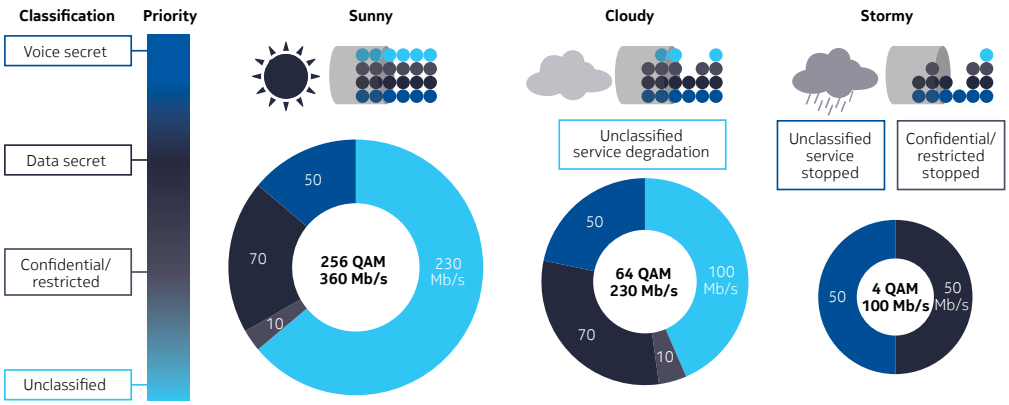
In addition, the Nokia optical solution allows integrated detection intrusion and monitoring of the fiber with a high degree of precision traditionally performed with expensive external Optical Time-Domain Reflectometer (OTDR) systems. The solution is simple to install and manage and enables fiber monitoring with GPS accuracy embedded into the 1830 Photonic Service

Switch. Moreover, it delivers an optical intrusion alarm trigger for proactive and remote monitoring of the fiber infrastructure with very high precision - within a few meters.

IP/MPLS backhauling for defense

For defense applications, microwave capabilities are generally used to interconnect remote military camps where fiber or cable is not available or would be too costly to deploy (over the sea, tropical forests, deserts and mountains). The Microwave Packet Radio (MPR) system is designed to meet military requirements by protecting and guaranteeing the delivery of the most critical information (secret or critical for combat operations) in all conditions. Resilience and high-availability features (cross-polarization, XPIC, 1+1 hot) are complemented by the support of best-in-class hitless adaptive modulation, which tunes the air link according to external conditions.

Figure 7. Adaptive modulation guarantees Voice Secret traffic to pass over the air link



In a traditional architecture, IP/MPLS is laid over microwave transmission, as an additional platform. However, in a dynamic IP/MPLS network solution, the MPR system is fully integrated with the 7705 Service Aggregation Router (SAR), delivering a single, seamless platform that converges the IP and microwave domains. This level of integration provides numerous benefits when microwave media are widely deployed, including:

- Elimination of multiple network managers
- Convergence of multiple indoor units (IDUs) and IP/MPLS router(s) into one platform

- Reduction of space and spare parts requirements, power consumption and cooling needs
- Streamlining of installation and operations management

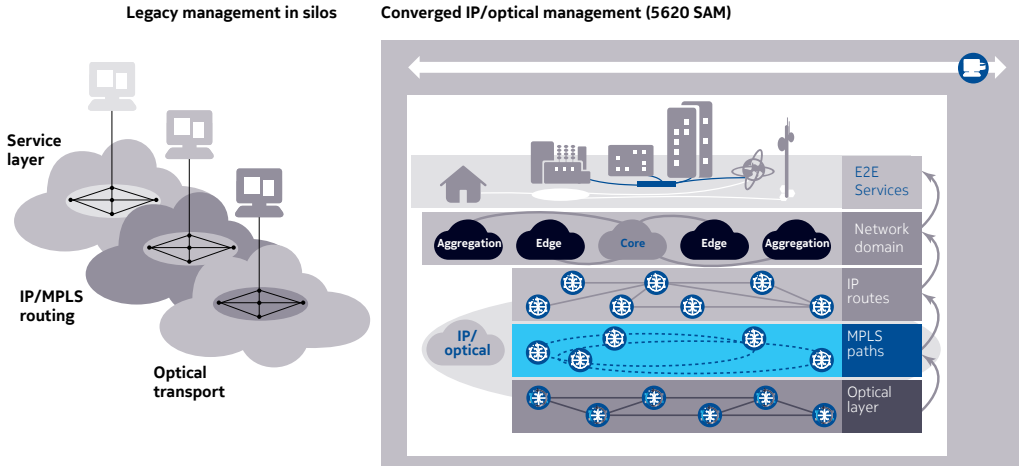
Converged IP/MPLS solutions include:

- End-to-end IP/MPLS solution from core, edge to access: 7705 Service Aggregation Router (SAR) and 7750 Service Router (SR)
- Integrated optical WDM backbone: 1830 Photonic Service Switch (PSS)
- Integrated IP/MPLS backhaul: 9500 MPR with the 7705 SAR
- Single unified service and network management system: 5620 Service Aware Manager (SAM)

Unified network management for defense

Traditional network management systems take a single-domain approach resulting in a fragmented network management perspective. This can make it difficult to isolate faults impacting multiple domains, and introduces error-prone labor-intensive operations across the domains.

Figure 8. Network management simplicity enabled by the unified 5620 SAM



The Nokia 5620 Service Aware Manager (SAM) enables end-to-end and cross-domain management of routing and transport assets to simplify and speed up complex operations. It is quick and easy to configure and allows network elements to be changed, facilitates routing infrastructure and service and resolves problems before they can affect network users. In short, the solution simplifies operations and reduces OPEX.

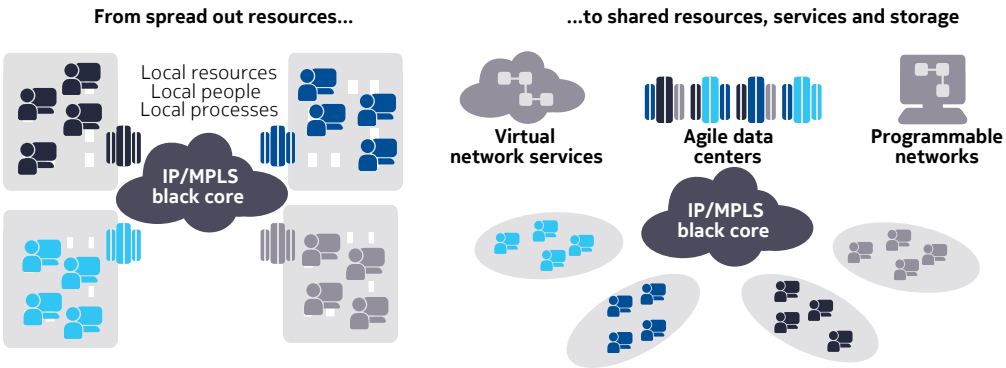
Data center interconnect and virtualized network services for defense

Current defense modernization evolution is fundamentally changing the way services will be delivered in the future. Traditional ICT facilities are spread out over many locations without standardized and optimization resources. The new trend, however, is to centralize management over shared resources based on standardized services. This innovative centralized approach enables the shift from local resources and heterogeneous platforms and processes to centralized, shared-platform and standard processes. This brings significant benefits and cost savings including:

- Reduced manpower required to provide and maintain services
- Reduced life-cycle costs
- Improved availability of ICT services via an enhanced Business Continuity and Disaster Recovery (BCDR) posture
- Better sustainability
- Increased mobility and flexible working

The move towards the centralized private data center, where applications and information are consolidated, involves a drastic transformation of networks. Networks need to be more flexible, while at the same time providing more bandwidth and ensuring full traffic and data security. High-capacity DWDM optical networks with Level 1 encryption and software defined networking (SDN) are enabling the levels of on-demand connectivity for storage, database replication and connectivity for high-volume, low-latency data flows now increasingly demanded.

Figure 9. Private data center consolidation for better efficiency



For the consolidation of data centers, networks and operations, SDN solutions offer considerable value by virtualizing any data center network infrastructure and automatically establishing connectivity between computer resources upon their creation. They simplify operations support systems/network integration with a centralized point of management and control, which accelerates service automation and innovation in multilayer networks, giving greater network visibility so networks can run more efficiently and support new services.

Furthermore, virtualization and automation will benefit defense organizations that are operating under constrained budgets, but also looking to optimize their network assets.

Ultra-broadband access for defense

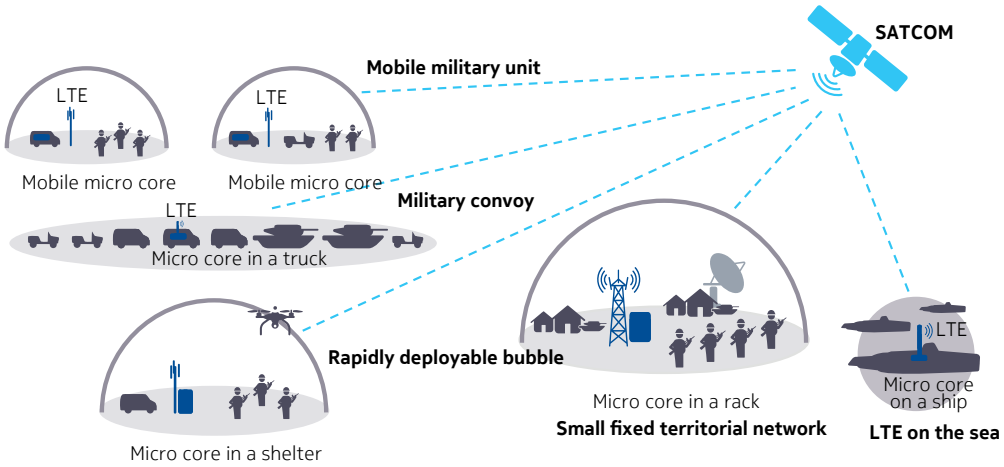
As stated by the Lt Col Giles Ebbutt (Retd), "There has always been a requirement for large amounts of communications bandwidth within military organizations. However, the recent proliferation of intelligence, surveillance and reconnaissance (ISR) systems which capture and distribute vital intelligence about the enemy - full-motion video, imagery, simultaneous voice/data, graphics and so on has led to an explosion in the amounts of information available to commanders and those operating on the front line. But, in order to get the maximum benefit of this intelligence it has to be distributed as far forward as possible, to what is sometimes known as 'the tactical edge', where timely actionable intelligence can mean the difference between success and failure."

Fourth-generation, Long Term Evolution (4G LTE) cellular technology is raising more and more interest as the possible standard for wireless broadband and deployable communications systems at the logistical/semi-tactical edge of the military newtork. Forces will benefit from improved situational awareness and increased mobility with instant access to large amounts of real-time, multimedia information enabled by high-bandwidth IP-based data services, innovative devices and applications. Consequently, many defense organizations are investigating how to extend secure wireless communications with LTE, providing downlink peak rates of 150 Mb/s (with 20 MHz bandwidth), low latency (around 10 ms) and quality of service provisions to ensure guaranteed and prioritized delivery of applications. LTE technologies support failover, automatically switching to a redundant hardware component in the event of the failure of one or more components.In addition, an LTE solution extends anywhere within range of broadband connectivity, allowing the type of remote temporary coverage crucial for faster distribution of data and video - at a speed at which vital information is required to travel.

Indeed, LTE is well adapted to serve the many diversified missions that defense organizations have to deal with: disaster management, humanitarian assistance and peace support to counter-terrorism and high-intensity war fighting.

It can range from rapidly deployable bubbles for mobile military units and camps to communications systems for moving military convoys and naval vessels as shown in Figure 10.

Figure 10. Tactical 4G LTE bubbles enable new multimedia and real-time services



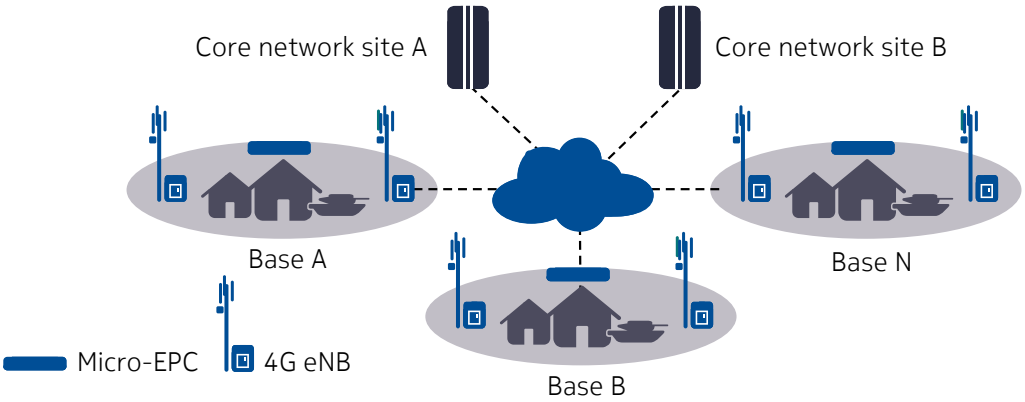
Benefits of LTE for defense:

- Widespread number of frequency bands and systems for all sizes of deployments (LTE radio access network (RAN) with flexible options, Evolved Packet Core (EPC), Mobile Backhaul, Internet Multimedia Subsystem (IMS), 5620 Service Aware Manager
- Reduced total cost of ownership with COTS equipment
- Enhanced data, voice and video services for improved operational efficiencies

In strategic networks as shown in Figure 11, LTE is implemented to cover a large military campus with mobile users: a typical example is where LTE enables seamless intra- and intercommunication between military air force bases. LTE dedicated networks provide highly resilient communications with built-in redundancy available for normal day-to-day operations as well as in crisis situations.

Some nations at the forefront of innovation are already testing and even deploying LTE systems for enhanced operations.

Figure 11. LTE for national and fixed military camp coverage



Why partner with Nokia?

Because every success has its network, Nokia invents and delivers dynamic and resilient networks to support the missions and operations of armed forces around the world. We are a leading IP networking, ultra-broadband access and cloud technology specialist. Our mission is to create networks at scale, and to apply our expertise and passion to the implementation of dynamic and secure networks adapted to the requirements and priorities of the defense sector. We bring the best of civilian technologies to defense organizations.

Nokia has been recognized by Thomson Reuters as a Top 100 Global Innovator, and by the Dow Jones Sustainability Indices review as the Technology Hardware & Equipment industry group leader for 2014. Nokia has built a strong and trusted reputation based on:

- Decades of experience in the network technology and communications sector and long-lasting relationships with world-leading international telecom service providers
- Intensive investment in R&D every year with a participation in 100 standards bodies and 27,900 active patents
- Bell Labs innovative technologies and revolutionary solutions in multiple domains – 400 Gb/s optical transmission technology, WDM, 400 Gb/s FP3 routing silicon for IP service router and so on
- World-leading positions in many domains: #1 in Microwave Long Haul, LTE in 8 of the top 10 mobile service providers in the world

- Bell Labs Consulting practice to help our customers address important strategic and operational issues and unleash the value in the network
- Unique and comprehensive portfolio of IP/MPLS, microwave, optics, IP cloud, fixed and mobile ultra-broadband access and network management communications products

We are committed to earning your trust. We operate according to the highest ethical standards, embedding responsible innovation at the heart of our activities and supply-chain partnerships.

We actively participate in standards development for cost-efficient multivendor interoperability and implement standard carrier-grade technology as well as standard RFCs so that customers are not locked into a vendor-specific feature.

We innovate for you. We conceive and invent the future through open collaboration with customers, stakeholders and our Bell Labs researchers, pushing the limits of communications and shaping the digital world. We combine the world's best network of minds with a 'startup culture' eager to solve today's major challenges and develop breakthrough technologies.

NOKIA

Acronyms

BCDR	Business Continuity and Disaster Recovery
C2	Command and control
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
COMSEC	Communications Security
COTS	Commercial off-the-shelf
DWDM	Dense Wavelength Division Multiplexing
EPC	Evolved Packet Core
ICT	Information and communications technology
IDU	Indoor unit
IMS	Internet Multimedia Subsystem
IPSec	IP Security
LTE	Long Term Evolution
MPLS	Multiprotocol Label Switching
MPR	Microwave Packet Radio
NCW	Network-Centric Warfare
OTDR	Optical Time-Domain Reflectometer
PSS	Photonic Service Switch
RAN	Radio access network
RFC	Request for comments
SAM	Service Aware Manager
SAR	Service Aggregation Router
SDH	Synchronous Digital Hierarchy
SDN	Software Defined Networking
SONET	Synchronous Optical Networking
SR	Service Router
TDM	Time Division Multiplexing
UAV	Unmanned aerial vehicle
UGV	Unmanned ground vehicle
VPN	Virtual private network

WDM	Wavelength Division Multiplexing
XPIC	Cross-Polarization Interference Cancelation

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

Product code: PR1506011781EN

