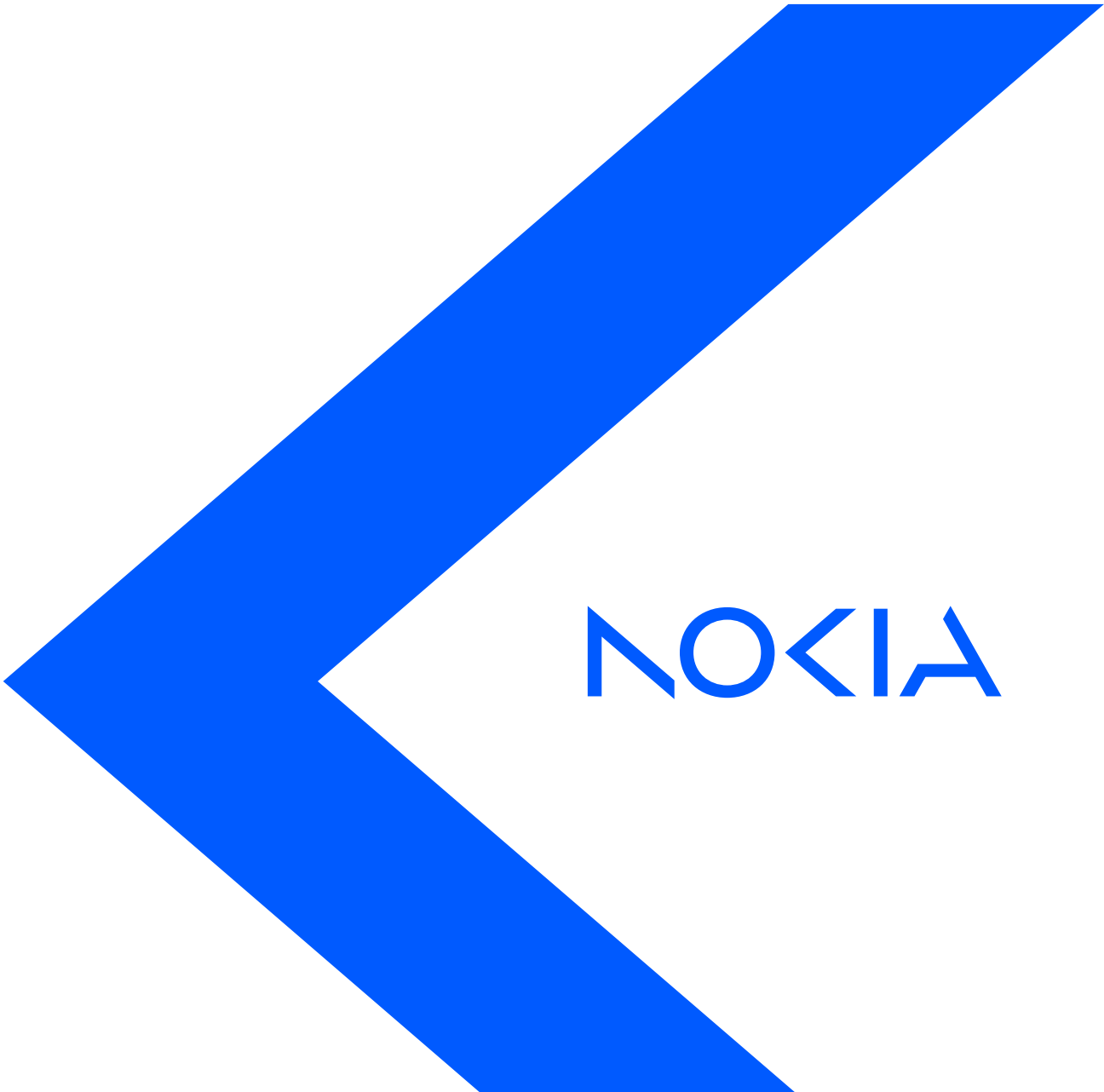
Optical networks for defense

Network modernization with the Nokia 1830 Photonic Service Switch (PSS)

Application note



Abstract

Governments need to protect their citizens from an increasing variety of threats while supporting connected forces. Often the need for increased connectivity among defense forces is at odds with threats posed by cyber enemies. The need for better connectivity can not compromise force security or sensitive information.

Optical transport provides the foundation for a powerful network that securely connects elements of the modern warfighter, support systems, command centers and data centers. It provides the backbone for all defense networks, supporting a net-centric data strategy.

This application note outlines requirements, technology options and Nokia solutions needed to construct a modern packet-optical defense network.

Contents

Supporting cyber defense forces

Defending a nation's resources is a constantly fluid task as new threats emerge and the methods through which they are addressed change. What was once accomplished through boots on the ground now depends on managing advanced technologies based in chemistry, physics, meteorology, aeronautics, robotics and computing. Modern defense is a complex mixture of coordinating intelligence with advanced sensors and weapons that can neutralize threats with lethal accuracy while minimizing risk to friendly personnel.

Commanding a modern defense force requires an ability to coordinate resources among a range of assets through secure networks. These networks must deliver information to ground, air and maritime forces with speed and high integrity.

At the same time, the network must have the ability to rapidly adapt to changing mission requirements and evolving command, control, communications and intelligence (C3I) systems. Meeting the defense mission increasingly requires a flexible, agile, scalable and secure network infrastructure: a mission-ready, quantum-secure network.

Construction of the mission-ready network requires a means to reliably connect multiple applications, including the tactical Internet of Things (IoT), related operational units, multimedia, video and data centers through a flexible, highly scalable and secure networking foundation: a fiber optic backbone. The network should be highly scalable, allowing for current and future capacity needs. It also should be capable of providing connectivity for embedded, legacy systems that may continue in operation for years. At the same time, the network must be capable of connecting future applications and systems.

Lastly, the network must be highly secure. In a dangerous world, defense networks must protect sensitive data, be safe from interruption and able to recover quickly from any unforeseen disaster. The expected emergence of cryptographically relevant quantum computers (CRQC) requires defense networks that utilize multiple layers of cryptography in a defense-in-depth architecture.

Requirements: Moving toward a packet optical network

Building mission-ready infrastructure requires a modernized, scalable, agile network that supports existing communications and control systems. Modernization cannot occur in a single step; older systems are replaced over time, with gradual upgrades. Throughout the modernization process, the network must be highly reliable and secure to ensure force integrity and mission readiness. The defense communications network must consider the following requirements.

Flexibility and scalability: Application-specific networks are no longer viable in an environment where needs change rapidly and resources are limited. For example, in a net-centric battlefield environment, the communications networks must be able to provide dynamic connectivity to a variety of weapons platforms, sensor systems and command centers. These networks need to scale in capacity while being flexible enough to support any type of data protocol, including Ethernet, IP, TDM, video, Fibre Channel and others.

Reliability: Force safety demands network resiliency and reliability. Networks must be built using equipment designed for high availability, utilizing redundant systems and automatic protection mechanisms. The network also should utilize diverse connectivity paths and a rich set of diagnostics to predict and prevent outages before they occur.

Security: Networks are the essential link among personnel, tactical platforms and command, making security vital. Communications networks must be protected from intrusion and data theft that could lead to loss of life and defeat of force objectives. Networks must be safe against attack by a CRQC, now and into the future.

Network traffic segregation and multitenancy: Using a shared physical network for multiple applications requires measures to segregate different network traffic streams. The defense network backbone may be shared among several user classes and armed forces agencies. This implies a need for logical network segregation.

Deterministic performance: The network should assign priority to critical applications, ensuring availability during peak traffic periods. For example, tactical force communications should be assigned a higher priority than routine data backup, such that if total demand exceeds available bandwidth, only the lower priority traffic is temporarily impacted.

Ease of use: The network must be easy to provision, operate and maintain. Software control should extend across network elements, reducing the need for physical hardware changes and allowing remote provisioning.

Long asset life: Like all government budgeting decisions, defense systems face sensible demands for long operational lifespan. A modern network must support technologies from at least fifteen years ago and for decades into the future. This implies use of a modular and extensible architecture, allowing older technologies to be easily maintained or phased out while new technologies are gradually introduced.

Economically attractive: All of the previous requirements must be met with defensible economy, balancing initial capital expense with ongoing operational expense. Use of common platforms for multiple applications and a high degree of software control are desirable, as are modular equipment architectures and common software control.

Optical transport in the defense communications network

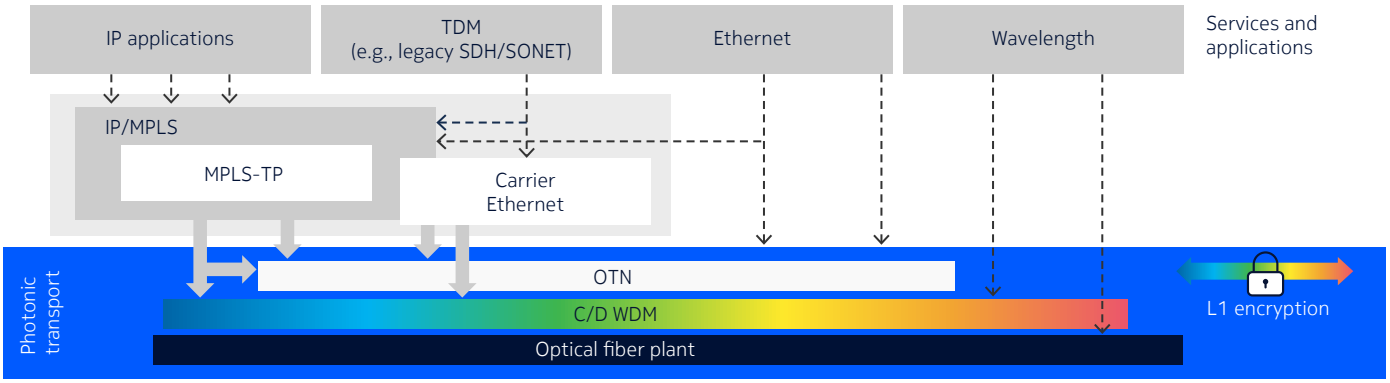
Meeting the requirements outlined in the previous chapter demands a network that makes use of modern technologies. Packet optical transport (P-OT) combines the efficiency and flexibility of packet services with the scalability, reliability and determinism of optical transport. P-OT usually includes technologies such as:

- Wavelength division multiplexing (WDM)
- Synchronous Digital Hierarchy/Synchronous Optical Network (SDH/SONET)
- ITU-T G.709 optical transport network (OTN)
- MEF 2.0 Carrier Ethernet
- Multiprotocol Label Switching – Transport Profile (MPLS-TP).
- Quantum-Safe Networks (QSN)

Each technology offers different benefits to the defense network; the exact architectural choice depends on specific applications and objectives. Optical transport technologies are discussed in this application note.

Together, optical layer transport, switching and routing technologies provide connectivity for applications and services that accomplish a given task. Figure 1 shows these technologies positioned roughly within the Open Systems Interconnection (OSI) reference model and shows their chief interdependencies.

Figure 1. Optical transport ecosystem



Optical (Physical) layer

At the physical layer, fiber is used to build the physical connectivity among offices, data centers, weapons platforms, sensors, tactical units and command/control centers. This may be accomplished through a combination of privately owned outside fiber plant complemented with leased dark fiber. Fiber is terminated by agency-owned or leased equipment. Capacity can be scaled easily using coarse or dense wavelength division multiplexing (CWDM/DWDM) systems.

In optical line systems utilizing C+L band channels, each fiber offers 9600GHz of WDM spectrum, each delivering traffic at speeds of1.2Tbps or more. Individual wavelengths can be dropped or added around the network and reconfigured as needed. In some applications, individual wavelengths provide logical separation between user groups carried along the same fiber.

In addition to pure capacity, optical WDM can transport data over a wide range of distances, from very short spans within a data center to undersea cables connecting continents.

SDH/SONET and OTN

Optical wavelength capacity is usually shared among applications and users through various multiplexing and switching technologies. SDH/SONET is a TDM method that was widely used to share capacity, deliver circuit-based services and ensure high reliability. As networks are upgraded, they must efficiently carry both circuit-based TDM services and packet-based services.

Interestingly, technologies have emerged to emulate circuit services over packet networks, essentially reversing roles. Standards for this emulation include Circuit Emulation Service over Ethernet (CESoE) and Transparent SONET over Packet (TSoP).

SDH/SONET was developed in the 1980s to transport increasing volumes of voice traffic over fiber. Data rates were set based on fixed increments of voice channels plus signaling overhead. Exponential increases in demand for packet data were not part of the design.

In 2001, the ITU-T offered standards that define an OTN in G.872, later refined in G.709 and G.798.

OTN evolves optical networks beyond TDM transport and reduces the complexity associated with scaling capacity and service diversity. OTN is often called a digital wrapper technique because any client protocol, including packet or TDM, is placed into a flexible container as a payload for transmission over an optical channel. Because the entire client signal is carried as payload, OTN is transparent to the end application.

OTN also provides a much stronger forward error correction (FEC) mechanism through use of a Reed-Solomon 16-byte scheme, resulting in significant improvements in optical link signal-to-noise ratio. This improvement is very valuable as data rates or span lengths increase.

OTN places no restrictions on switching line rates; as the industry advances, higher bit rates (i.e., higher capacity optical transmissions units/optical data units [OTUs/ODUs]) can be added to the standards, providing broad scalability.

OTN also offers comprehensive operations, administration and maintenance (OAM) capability.

Table 1 shows a comparison of SDH/SONET and OTN. As legacy TDM technologies reach end of life, OTN is likely to remain as a core network transport mechanism.

Table 1. SONET/SDH and OTN comparison

	SONET/SDH	OTN
Timing distribution	Tight timing distribution required to recover data at terminals	Not required
Protocol transparency	Not transparent: Designed for TDM voice transport. Synchronous payload mapping, fixed frame size per line rate require external framing hardware for transport of some protocols.	Transparent: Asynchronous mapping of client signals and matching frame and client rates allow transport of any protocol.
OAM&P capabilities	Strong	Strong
Forward error correction (FEC)	Limited: In-band frame checks at certain rates	Strong: HD or SD-FEC through out-of-band 16-byte interleaved scheme
Line rate limit	Standards ceased at OC-768 (40 Gb/s)	Essentially unlimited: Standardized above 112 Gb/s (OTU4) through OTUCn (n x 100) structure
Sub-wavelength grooming	Not capable	Designed to map various clients into optical data units (ODUs), maximizing wavelength utilization

Migration from an SDH/SONET network toward OTN is not done solely to increase capacity. OTN offers scalability plus the ability to transport any protocol, including packet-based traffic such as IP/MPLS or Ethernet. Virtually any application can be encapsulated into an OTN payload container for transport.

To ensure data integrity, client traffic from different end applications or user sets can be segregated from other traffic through provisioning onto separate optical payload units. Aggregated traffic can then be encrypted for further security. For a defense network, the decision to upgrade from an SDH/SONET network should be driven by overall capabilities and expected future services.

Security and encryption

Ensuring data integrity is essential to communications; networks must be safe from data theft and intrusion. Data must be protected while at rest in a data center, contained with storage media or in-flight across a network. Governments should consider adopting Quantum-Safe Network approaches- protection against the increasing threat posed by CRQC. Protecting data in-flight requires layers of protection working together in a “defense in depth” approach.

Quantum-Safe Networks include security measures at the optical layer, protecting higher layer applications within a wavelength, multiple wavelengths or an entire fiber cable. This includes:

- **Optical encryption**: application of AES-256 bit cipher to each optical link
- **Centralized key management**: a symmetric key management system that removes the key material from the data plane, while controlling key rotation, expiration and destruction
- **Optical path monitoring**: methods to monitor minute changes in received optical power levels, which could indicate tampering along a fiber span
- **User authentication and network element control**: multiple levels of user classes with robust password protection
- **Independent certification**: solutions should be certified by independent entities for compliance with relevant standards including FIPS and common criteria (CC).

Nokia modernized optical transport solution

A modernized photonic network provides a foundation for any application or service needed for defense infrastructure. It includes a scalable P-OT network that can support any traffic type, including IP/MPLS, Ethernet or legacy TDM. This foundation utilizes OTN encapsulation and switching and has native support of packet transport methods such as Ethernet provider bridging, MPLS-TP or Carrier Ethernet as well as TDM transport capabilities. The network should also be safe from theft or intrusion through certified Layer 1 encryption with centralized, symmetric key management.

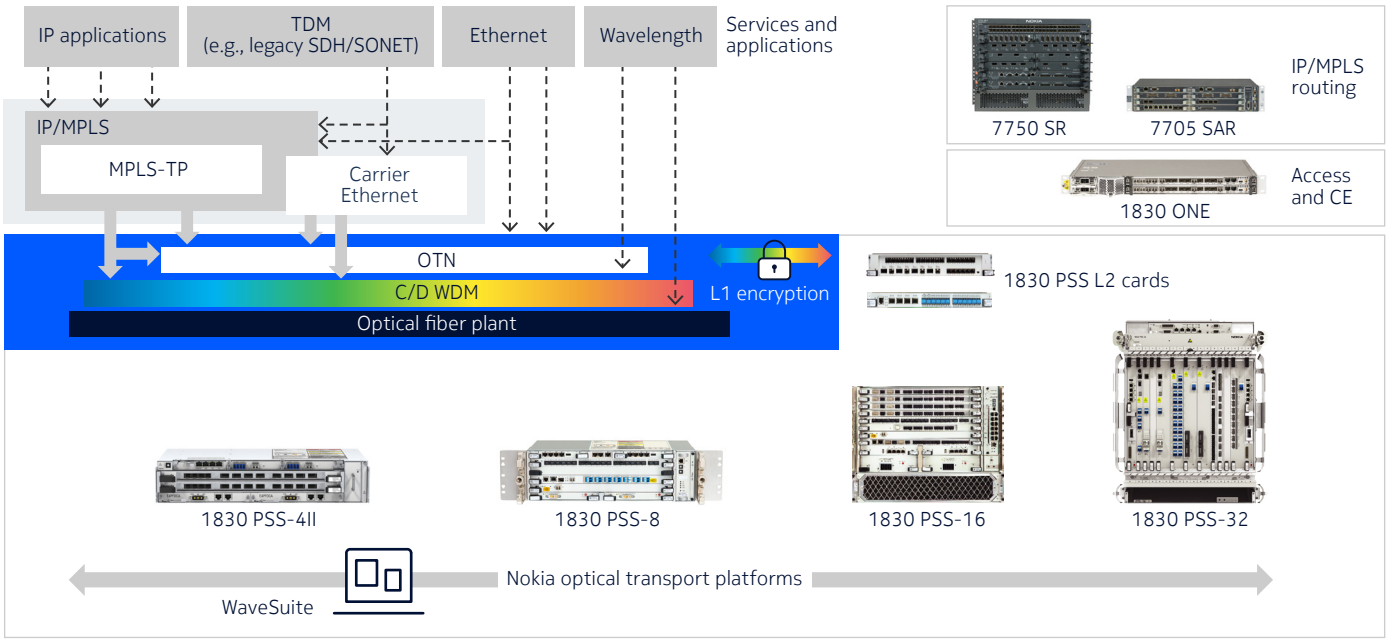
The Nokia 1830 Photonic Service Switch (PSS) offers capabilities exceeding the requirements of a modern photonic network. This includes a chassis sized to match network capacity needs, flexible modules for optical transponder, amplification and add-drop functions, packet switching and transport, blade or centralized OTN switching, and Layer 1 encryption. The 1830 PSS supports Layer 2 packet switching through integrated switching cards that support provider bridging, MPLS-TP and Carrier Ethernet service or through other Nokia products.

Legacy TDM services are supported by 1830 PSS interfaces. Additionally, these services are complemented by the IP/MPLS routing of the Nokia 7750 Service Router (SR) and Nokia 7705 Service Aggregation Router (SAR) product families.

Meeting the requirements for an agile and scalable defense communications network requires a range of technologies spanning optical transmission, Carrier Ethernet, IP/MPLS and network automation. Nokia offers solutions based on decades of experience delivering advanced communications networks to government agencies, enterprises and service providers. Leveraging Nokia Bell Labs as the innovation engine, Nokia solutions build dependable, scalable, yet flexible network infrastructure that bring together IP routing, optical transport and software.

Figure 2 shows the relevant products from the Nokia optical and IP portfolios that can be used to modernize defense networks. Products can be selected to match needs based on service type, density, form factor and technology functionality.

Figure 2. Nokia portfolio in the transport ecosystem



Nokia 1830 PSS product family highlights

The Nokia 1830 PSS forms a flexible transport layer through its agile photonics, multi-layer switching capabilities and network intelligence. Using the Nokia Photonics Service Engine (PSE), the 1830 PSS is built on the first commercially available 100G coherent DWDM solution. It enables high scalability, easier operations, accelerated provisioning and reduced cost. The 1830 PSS employs distributed OTN switching and a range of interface cards that can be used across the different chassis types with few limitations.

Highlights of the 1830 PSS platform include:

- Ethernet and SONET/ SDH interfaces
- Industry leading coherent DWDM line-side interfaces
- 10/100/400GE LAN/WAN interfaces
- High-availability optical protection switching

- Chassis sized to match application needs, including data center interconnect (DCI), optical access/ aggregation and an optical WAN backbone with capacities ranging from 240 Gb/s to beyond 8 Tb/s
- PSE super-coherent silicon technology provides the basis for software-controlled interface cards capable of optimizing span reach and data rate. The PSE supports adaptive modulation, variable baud rates, advanced soft decision FEC and optical super channels.
- Advanced P-OT interfaces, providing MEF 2.0 Carrier Ethernet and MPLS-TP capabilities, seamlessly operating with Nokia IP routing platforms through the Service Router Operating System (SR OS)
- TDM migration options through Layer 2 packet interfaces, providing a flexible means to evolve toward packet services
- Quantum-Safe Network security capabilities, including AES-256 encryption per wavelength and centralized, symmetric key management exceeding NIST and NSA recommendations, certified to FIPS, CC and ANSSI standards.

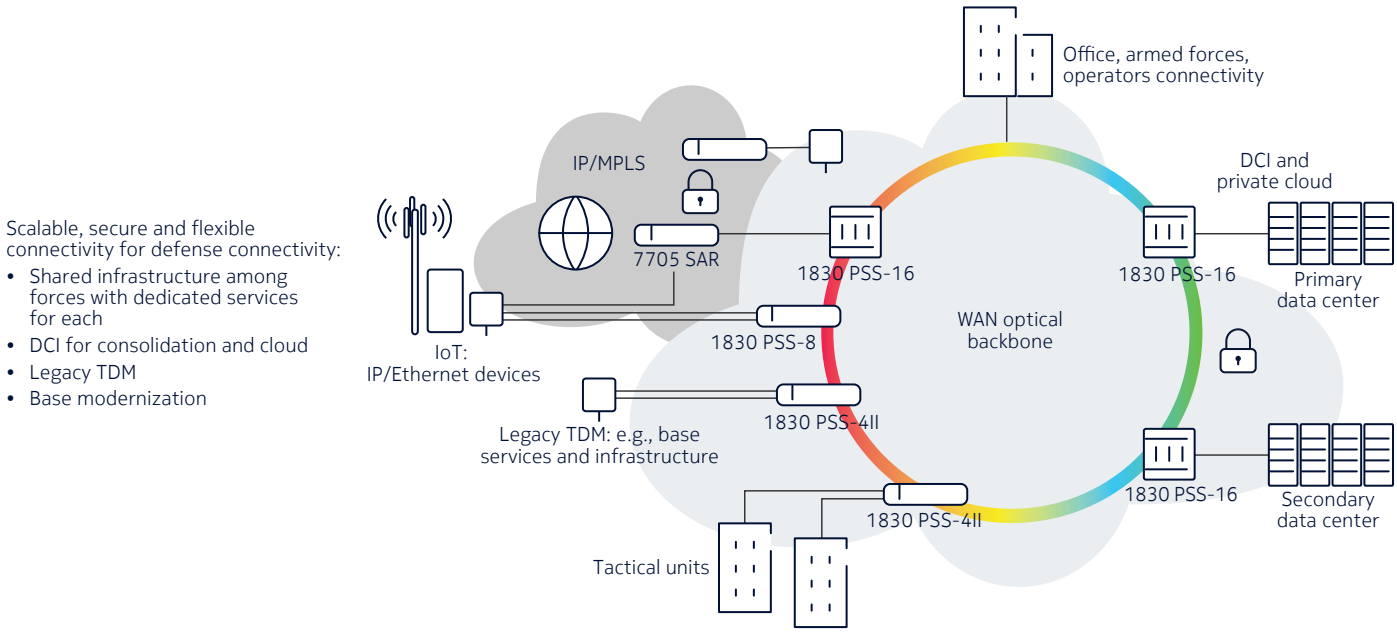
The Nokia 1830 PSS offers defense agencies the scalability, agility and efficiency to maximize value through an integrated optical backbone. With a feature set supporting SDH/SONET, Carrier Ethernet, storage area networks and other interfaces, plus OTN and packet switching capabilities, and Quantum-Safe Networking, the Nokia 1830 PSS is the premier optical backbone solution.

Conclusion

Defense forces can enhance mission readiness, force safety and net-centric capabilities through construction of a high-capacity, agile photonic backbone network. Meeting the defense mission increasingly requires the ability to support multiple applications and users coordinating air, ground and maritime forces spread over vast geographies. Accomplishing this requires communications networks that are agile to meet constantly changing service requirements, scalable to carry increasing capacity demand, and highly secure to protect vital information and infrastructure.

Figure 3 shows how this network could be built as a defense forces mission-critical WAN, with the Nokia 1830 PSS forming an optical backbone that transports traffic from various applications.

Figure 3. Defense mission-critical WAN with 1830 PSS



This paper has provided context for several of these choices and the Nokia solutions that support them, specifically:

- Capacity scaling and continued capabilities for embedded traffic such as TDM services
- Migration toward a packet-optical transport core supporting Ethernet and IP traffic
- Protocol-agnostic photonic transport utilizing OTN
- Flexible Layer 2 architecture, capable of supporting multiple packet technologies
- Quantum-safe transport through Layer 1 Quantum-Safe Networking as part of a defense-in-depth strategy.

The Nokia product portfolio offers the industry's most complete set of options to meet modern defense forces' communications requirements. In addition, Nokia has the experience and pedigree from hundreds of successful mobile access and fixed backhaul projects supporting government, enterprises and service providers over the past 30 years. The Nokia 1830 PSS offers the most powerful photonic transport solution to meet these needs. To learn more, visit our optical networking web site on nokia.com.

Abbreviations

AES	Advanced Encryption Standard
CC	common criteria (security standards)
CC EAL	common criteria evaluation assurance level
CE	customer equipment
CRQC	cryptographically relevant quantum computer
CWDM	coarse wavelength division multiplexing
DCI	data center interconnect
DWDM	dense wavelength division multiplexing
FEC	forward error correction
FIPS	Federal Information Processing Standard
IPSec	IP security
ITU-T	International Telecommunication Union – Standardization Sector
L1	Layer 1
L2	Layer 2
MACsec	media access control security
MEF	Metro Ethernet Forum
MPLS	Multiprotocol Label Switching
MPLS-TP	MPLS - Transport Profile
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OAM&P	operations, administration, maintenance and provisioning
ODU	optical data unit
OTN	optical transport network/networking
OTU	optical transmission unit
PON	passive optical network
P-OT	packet-optical transport
PSE	Photonic Service Engine

PSS	Nokia 1830 Photonic Service Switch
QSN	Quantum-Safe Networks
SAR	Nokia 7705 Service Aggregation Router
SCADA	supervisory control and data acquisition
SDH	Synchronous Digital Hierarchy
SONET	Synchronous Optical Network
SR	Nokia 7750 Service Router
TDM	time division multiplexing
WAN	wide area network
WDM	wavelength division multiplexing

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: (July) CID200993