NOKIA

IP transformation of defense communications networks

Enabling flexibility, agility and speed with MPLS

As defense forces globally are fully embracing the network-centric warfare doctrine, network modernization has become a key focus of defense transformation. Operators of mission-critical communications networks in defense must modernize their networks to ready for the implementation of the doctrine. An IP/MPLS network will play a pivotal role in providing the defense communications required by the doctrine. This paper discusses the benefits of MPLS-enabled IP networks for mission-critical defense networks.

NOKIA

Contents

NOKIA

Contents

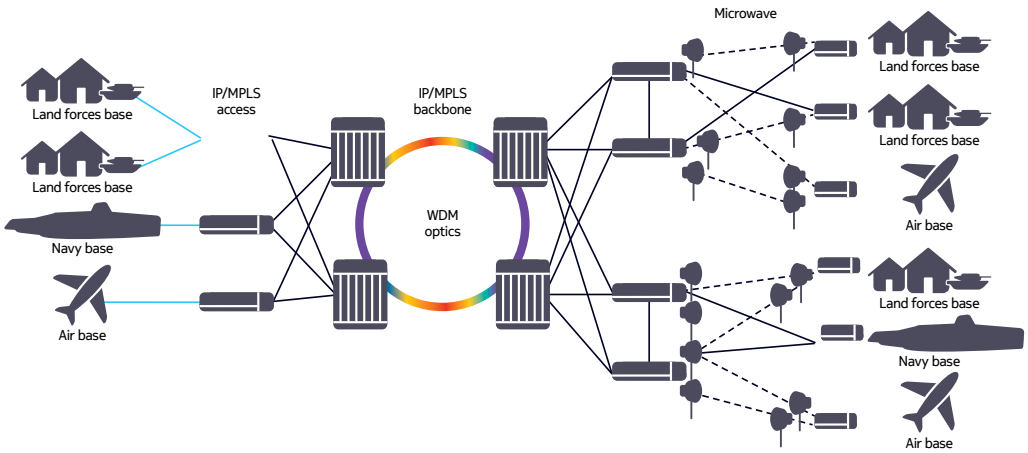
Mission-critical communications in the era of network-centric defense operations

The critical role of national defense encompasses protecting the interests of the state and its citizens, defending the state's sovereignty, safeguarding national borders and strategic locations overseas, and providing necessary civilian rescue assistance during natural catastrophes. To improve defense agility to carry out missions quickly with minimal casualties, it is imperative that the latest information can be shared among military, intelligence and even business operations. This doctrine is called network-centric warfare doctrine and has four tenets:

- A robust networked force improves information sharing.
- Information and intelligence sharing broadens situational awareness.
- Broadened situational awareness enables a sharper and faster response.
- These, in turn, dramatically increase mission effectiveness of the forces.

The bedrock of network-centric warfare doctrine is a mission-critical-grade defense communications network that transports vital voice, video, operational weaponry data and IT traffic during military missions as well as for daily operations. A reference network model is shown in Figure 1.

Figure 1. Defense network reference blueprint



The main requirements for defense communications networks are:

- Strong survivability
- High flexibility
- Deterministic network performance
- Secure communications
- Simplified network management

Each of these requirements is briefly outlined in the following sections and discussed in more detail in the rest of this document.

Strong network survivability

Network outages cause communications disruptions that can have grave consequences, including failed military missions or even casualties. The consequences for natural disaster recovery can be equally dire.

Network operators need to fully leverage redundancy mechanisms offered by different network technologies at different protocol layers to survive network faults, including multi-fault scenarios caused by either deliberate attack or natural catastrophe. If faults occur, the networks must self-heal and also support a rich set of Operations, Administration and Maintenance (OAM) tools to allow rapid troubleshooting.

High network flexibility

Network deployment flexibility over a variety of transmission media, such as microwave, fiber or even a service provider's virtual private network (VPN) service, is crucial for robust and resilient networks. New applications, from drones to body-worn cameras to virtual training systems, are IP-based while some legacy applications are still TDM-based. Networks need the service flexibility to carry both and also to seamlessly migrate legacy applications onto a converged network.

Deterministic network performance

With a large number of applications contending for bandwidth, mission-critical communications networks need to deliver traffic in a deterministic manner and still meet the stringent quality of service (QoS) level required by each application.

NOKIA

Secure communications

Security is a top priority, even for unclassified information such as general business information. Network operators need to evaluate security risks and use network security features effectively to shield the network from intrusive network activities ranging from cyber warfare by a hostile country to pranks by a teenage hacker.

Simplified network management

Because the communications network is an integral part of the defense establishment, it is vital that the network manager perform beyond the traditional boundaries of element, network and end-to-end service management. Operators require unified, end-to-end management that can help them to provision services, monitor performance and troubleshooting proactively. A network manager that extends IP network management to the underlying transport technology, such as optics or microwave, can further streamline network operations.

Evolving role of IP/MPLS in defense communications networks

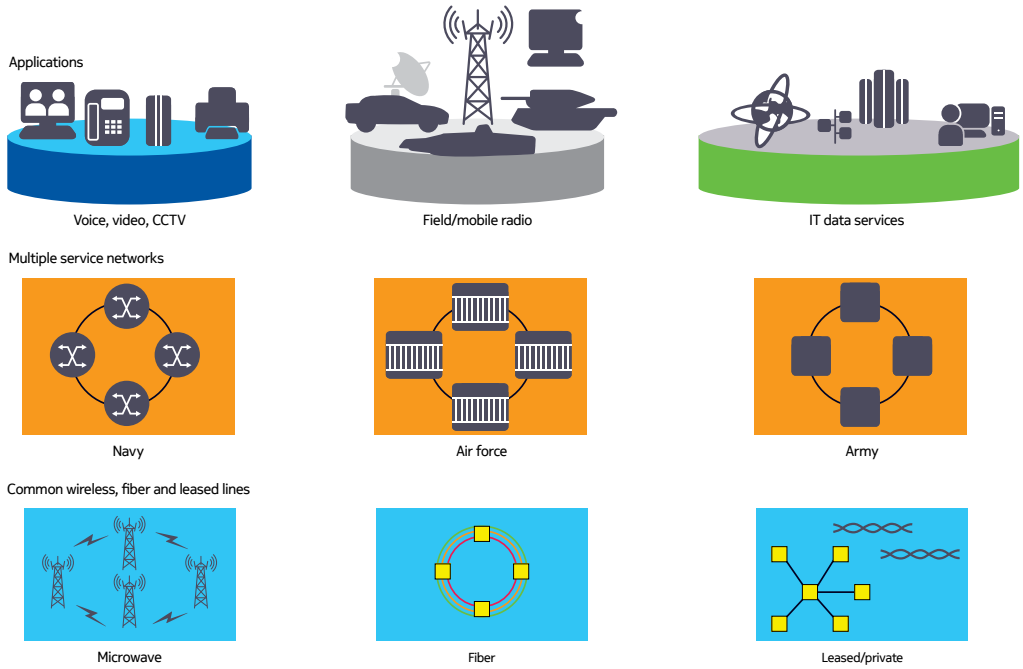
Defense forces need to modernize and transform their communications networks based on proven and extensible network technology that can bridge the past to the present and future, accommodating next-generation and legacy communications and applications while converging to a single network. Many operators of defense networks have already made a strategic decision to adopt IP/MPLS to meet their requirements.

Today's defense networks

Figure 2 shows a common defense network model. Different applications utilize different protocol-based communications, such as TDM with proprietary data, Point-to-Point Protocol (PPP), Ethernet and IP. Each application also has unique bandwidth and QoS requirements for latency and jitter.

In the past, operators often resorted to building and growing different service network overlays using a variety of network technologies such as TDM, ATM, Ethernet and IP. The network service overlays also use a variety of transmission media, including fiber, microwave and even leased lines from service providers.

Figure 2. Multiple service network overlays with shared physical assets



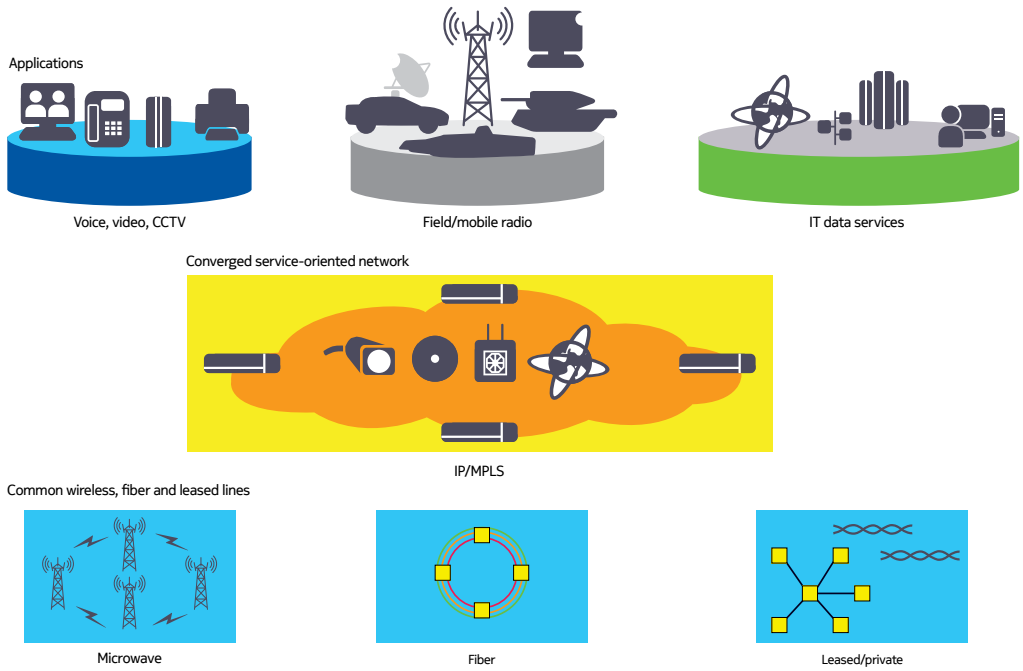
The current model is inefficient and costly because it involves multiple siloed networks built with different network technologies, equipment and management systems. Moreover, much of the deployed network equipment has reached or is approaching end-of-life while new IP/Ethernet-based and bandwidth-intensive applications are being developed and deployed. Even legacy applications such as radar systems are also evolving to IP-based. Finding a cost-effective solution to build networks for next-generation communications and applications has become critical.

Converging to a service-oriented IP/MPLS network

The role of IP/MPLS has evolved from traffic engineering in the internet core to providing premium service-grade Layer 1 (TDM), Layer 2 and Layer 3 VPN services end to end. Whether the communication is point-to-point or multipoint, Ethernet, IPv4 or IPv6, IP/MPLS and its use of label tunnel has proven to be very versatile, adapting to new services and applications with service-level privacy, security and reliability. At the same time, IP/MPLS can transport legacy TDM-based applications as reliably as SDH/SONET networks.

Leveraging IP/MPLS capabilities, network operators can consolidate all their services in one IP/MPLS network without compromising QoS. Operators are effectively adopting converged network architecture, as shown in Figure 3.

Figure 3. Converged service-oriented network



With a range of powerful capabilities, MPLS is a key enabling technology for implementing mission-critical defense networks.

Strong network survivability

Soldiers can go weeks without food, days without water, but only minutes with data. Network outages cause communications disruptions that can have grave consequences.

Operators of mission-critical communications networks need to ensure that their networks have strong survivability, including:

- SDH/SONET-like network restoration
- Multi-fault tolerance
- Command center protection

SDH/SONET-Like network restoration

In an Ethernet network using Spanning Tree Protocol (STP), it is difficult to predict recovery times when links or switches fail. Best-case recovery times are in the order of seconds. Although new Ethernet ring technologies such as ITU-T Recommendation G.8032[1] have improved recovery times, these are mostly confined to simple ring topologies because of complications when applied to multi-ring or mesh topologies.

1 http://www.itu.int/rec/T-REC-G.8032/en

With the Fast Reroute (FRR) mechanism[2], MPLS provides deterministic reroute times that match SDH/SONET transport network recovery times. Fast Reroute can deliver switching performance in the order of 50 ms — equivalent to what SDH/SONET provides. In addition, FRR can be seamlessly deployed in all topologies: single ring, multi-ring/ladder, mesh, daisy-chain with parallel links, or any combination of these.

Multi-fault tolerance

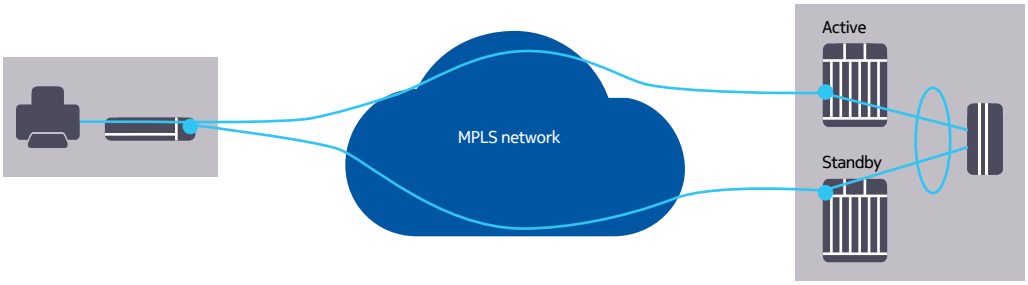
A mission-critical network must be able to withstand not just a single fault but a multi-fault failure scenario. To increase network resilience, operators usually build a multi-ring architecture to provide rich physical path diversity. An IP/MPLS router, being equipped with the complete network topology information, can re-route labeled traffic around multiple faults and maintain connectivity as long as path reachability is provided[3].

Command center protection

The command center is the brain of defense operations, particularly in the middle of a mission. It is crucial that adequate redundancy protection is deployed. Pseudowire[4], an MPLS technology that adapts Layer 1, Layer 2 and Layer 3 traffic for the MPSL network, enables core router and connecting interface protection in the command center (see Figure 4) through the use of a pseudowire redundancy mechanism[5].

Figure 4. Central router and interface equipment protection

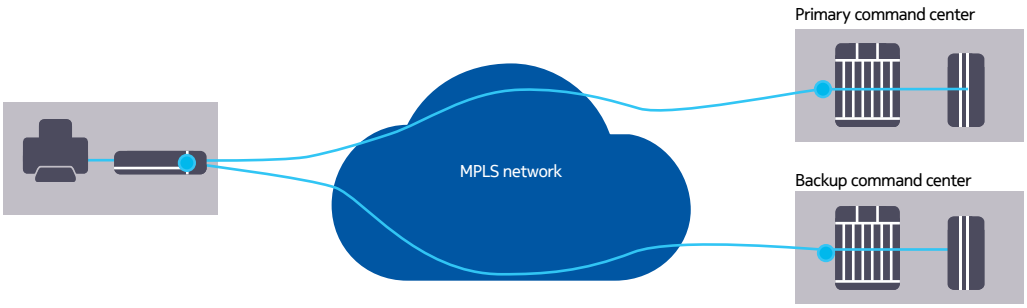
It is also imperative that a mission-critical network develop a recovery plan in case a natural disaster or hostile attack damages, or even destroys, the command center. Typically, a backup control center duplicates the primary



communications and head-end application servers and is located a great distance from the primary control center. The equipment protection scheme shown in Figure 4 can be extended to cover such a scenario, as shown in Figure 5.

2 https://tools.ietf.org/html/rfc4090 and https://tools.ietf.org/html/rfc5286
3 Not every packet technology can recover heal from a multi-fault failure scenario. For a detailed discussion, please read Building a multi-fault tolerant microwave backhaul network. http://resources.alcatel-lucent.com/asset/175593
4 https://www.ietf.org/rfc/rfc3985.txt
5 https://tools.ietf.org/html/rfc6718

Figure 5. Central site protection



High network flexibility

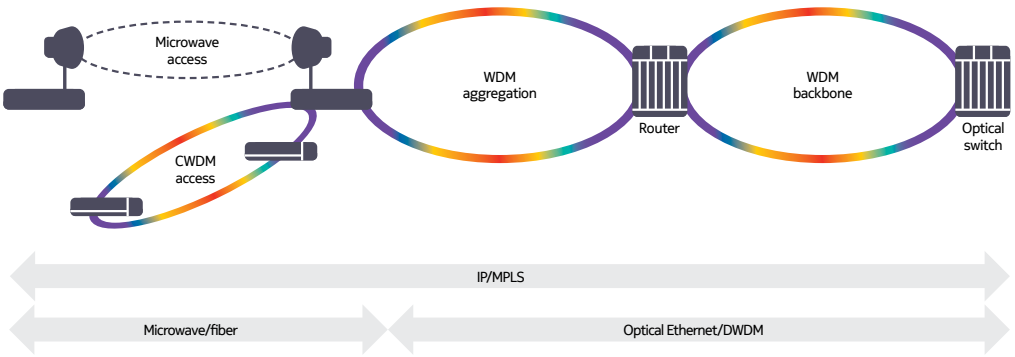
High network flexibility consists of transmission medium flexibility and integration, and service flexibility with MPLS-based VPNs.

Transmission medium flexibility and integration

As shown in Figure 6, MPLS runs effectively over a full range of Layer 1 transmission media (microwave, fiber and even copper) and transmission types (SDH/SONET, PDH and T1/E1). Moreover, the transmission media and transmission types can be mixed and matched to form an end-to-end network with MPLS running seamlessly. This flexibility enables all transmission assets to be used optimally in a resourceful way while maintaining common network operating procedures.

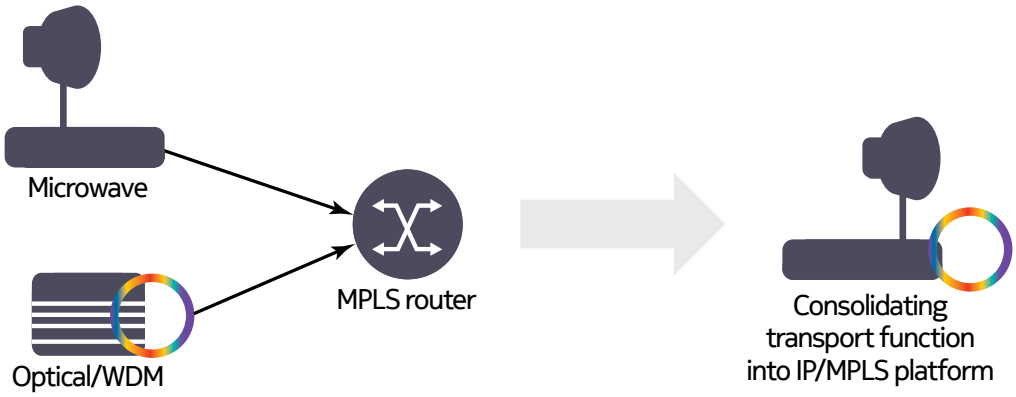
Network management and operation are also more efficient because microwave radio, Coarse Wavelength Division Multiplexing (CWDM) add/drop multiplexors and copper Digital Subscriber Line (DSL) modems are now integrated in MPLS platforms, simplifying network design and integration.

Figure 6. End-to-end MPLS deployment over heterogeneous transport domains



In traditional network equipment, deploying IP/MPLS on top of microwave and Wavelength Division Multiplexing (WDM) optics requires separate nodes managed by disparate management systems. By contrast, a next-generation IP/MPLS router can include integrated microwave radio and WDM capability, consolidating transport layer functions (see Figure 7).

Figure 7. IP/MPLS and transport functions consolidation

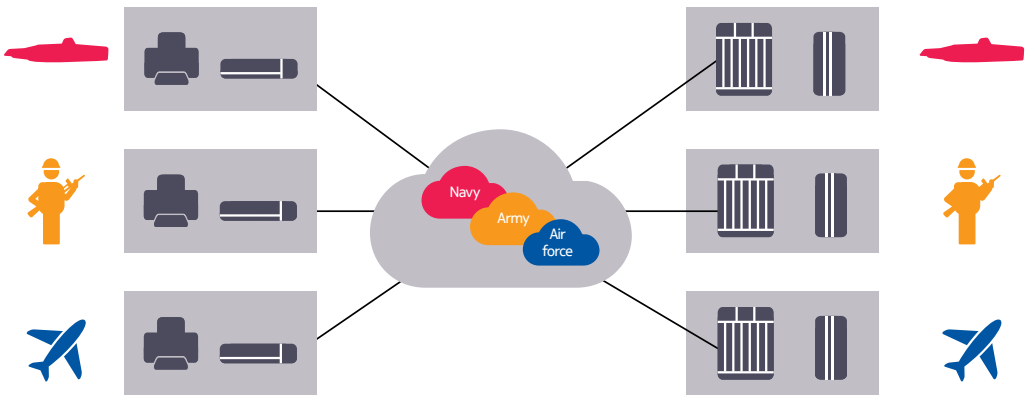


Through this consolidation, instead of a traditional network deployment using disparate network equipment, only one converged IP/MPLS platform is required. The consolidation enables IP/MPLS to work seamlessly with transport layer recovery mechanisms to make the network even more robust. For example, integrating microwave into an MPLS router can allow IP/MPLS be aware of microwave link condition in advance as well as support a 1+1 protection scheme natively.

Service flexibility with MPLS-based VPNs

MPLS-based VPNs enable an MPLS network to be shared by different branches of the armed forces (see Figure 8), with each VPN functioning as its own private or virtually separate network.

Figure 8. Multiple armed forces branches sharing a common IP/MPLS network



Depending on the connectivity and service required, the MPLS-based VPN can be a Layer 1, Layer 2 or Layer 3 VPN with all the benefits of MPLS.

MPLS Layer 1 VPN (TDM pseudowire)

To support future applications and traffic growth, network operators need to adopt new network technologies and architectures. However, support of Layer 1 VPNs for TDM traffic, with the same stringent delay, strict QoS and quick switching protection, is essential because many legacy critical applications still need to be supported. MPLS, with its range of benefits including service-aware QoS and synchronization, is in a unique position to address this challenge.

MPLS Layer 2 and Layer 3 VPNs

A range of Layer 2 and Layer 3 VPNs meet the different communication needs of network applications. A Layer 2 VPN includes virtual leased lines (VLLs), also called pseudowires, and Virtual Private LAN Service (VPLS), which is a virtual Ethernet bridging service. A Layer 3 VPN is called an IP-VPN. An integrated Layer 2 and Layer 3 approach is called Routed VPLS (R-VPLS).

The following sections describe the various types of Layer 2 and Layer 3 VPNs.

Layer 2 VPN - VLL

A VLL (pseudowire or Virtual Private Wire Service [VPWS]) is a point-to-point Layer 2 VPN that connects two endpoints or devices over an MPLS network. The traffic type can be TDM (Layer 1 VPN), Ethernet, ATM, Frame Relay, PPP, or High-Level Data Link Control (HDLC). A VLL is equivalent to a virtual circuit in the realm of older packet technologies such as X.25, Frame Relay and ATM.

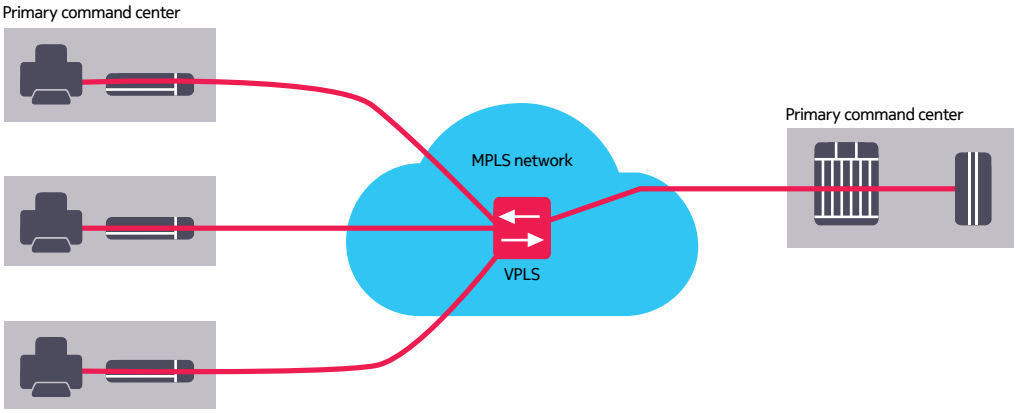
A Virtual Leased Line (VLL) is the simplest type of VPN to deploy and is a preferred solution for new point- to-point connectivity. The VLL is completely transparent to the end-user payload data and application protocol. The VLL endpoints can be configured with the desired traffic parameters, such as required bandwidth and priority of traffic relative to other traffic in the network.

Layer 2 VPN - VPLS

An MPLS-based VPLS is a bridged Ethernet multipoint-to-multipoint Ethernet VPN, also called an Ethernet-LAN (E-LAN). Each VPLS instance is a virtual bridging domain with its own Media Access Control (MAC) forwarding table.

Figure 9 shows a VPLS instance in an MPLS network connecting four devices in a single VPLS. All devices are logically connected to the same broadcast domain, virtualized over the MPLS network as a VPLS.

Figure 9. Layer 2 VPN - VPLS



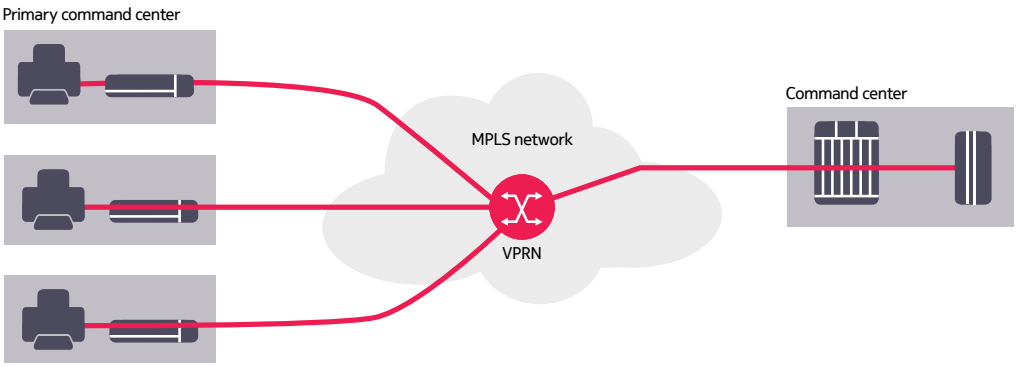
In a VPLS VPN, forwarding decisions are based on the Ethernet MAC address. Each application or department can be assigned a dedicated VPLS or Layer 2 broadcast domain. MAC address duplications are therefore supported across domains because all VPLS instances are segregated.

Because the underlying VPLS mechanism is an IEEE 802.3™[6] MAC learning bridge, minimal configuration is required and adding new sites is simple.

Layer 3 VPN

A Layer 3 VPN, or IP-VPN, is sometimes called a Virtual Private Routed Network (VPRN). Figure 10 shows a VPRN instance in an MPLS network. All customer devices are logically connected to the routing domain, virtualized over the MPLS network as a VPRN service. In a Layer 3 VPN, each MPLS node supports a Virtual Routing and Forwarding (VRF) instance for each VPRN instance and is segregated from all other VRF instances.

Figure 10. Layer 3 VPN (IP-VPN)



6 IEEE. 802® Standards. 802.3: Ethernet. https://standards.ieee.org/about/get/802/802.3.html

A Layer 3 VPN is implemented only for IP traffic and provides multipoint-to-multipoint IP connectivity with forwarding decisions based on the IP address. IP packet forwarding decisions can optionally be policy-based for greater flexibility. Overlapping IP address schemes are supported because each Layer 3 VPN has its own VRF instance.

There is certainly a need for inter-force communications. To allow such communications, specific IP subnets can be advertised among different Layer 3 VPNs. Integrated stateful firewalls can be deployed to further ensure that only authorized IP flows are allowed.

Layer 2 VPN integrated into a Layer 3 VPN

Multiple end devices are often in the same remote location and belong to the same IP subnet. In this situation, a Layer 2 VPN such as VPLS can be tied in virtually to the private routing domain, as shown in Figure 11. This integration of a Layer 2 VPN into a Layer 3 VPN is called Routed VPLS (R-VPLS).

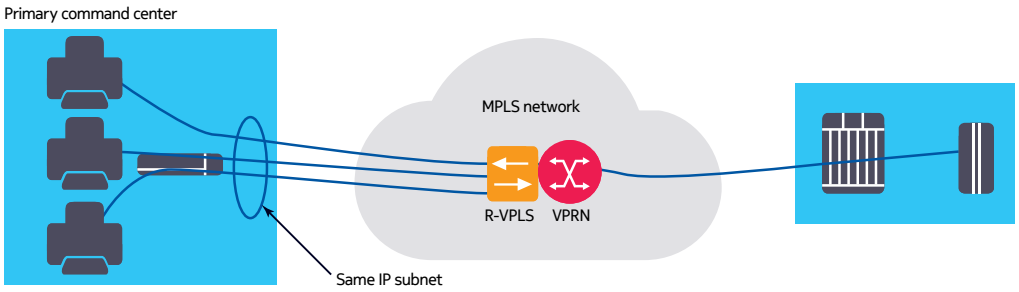


Figure 11. Integrated Layer 2 and Layer 3 VPN (Routed-VPLS)

Such an integrated VPN is essentially a VPRN (IP-VPN) with an Ethernet bridge as its front end grouping all devices under one IP subnet for optimized address planning and administration.

Deterministic network performance

Deterministic network performance is provided by:

- Hierarchical QoS
- Traffic engineering
- Comprehensive OAM capabilities

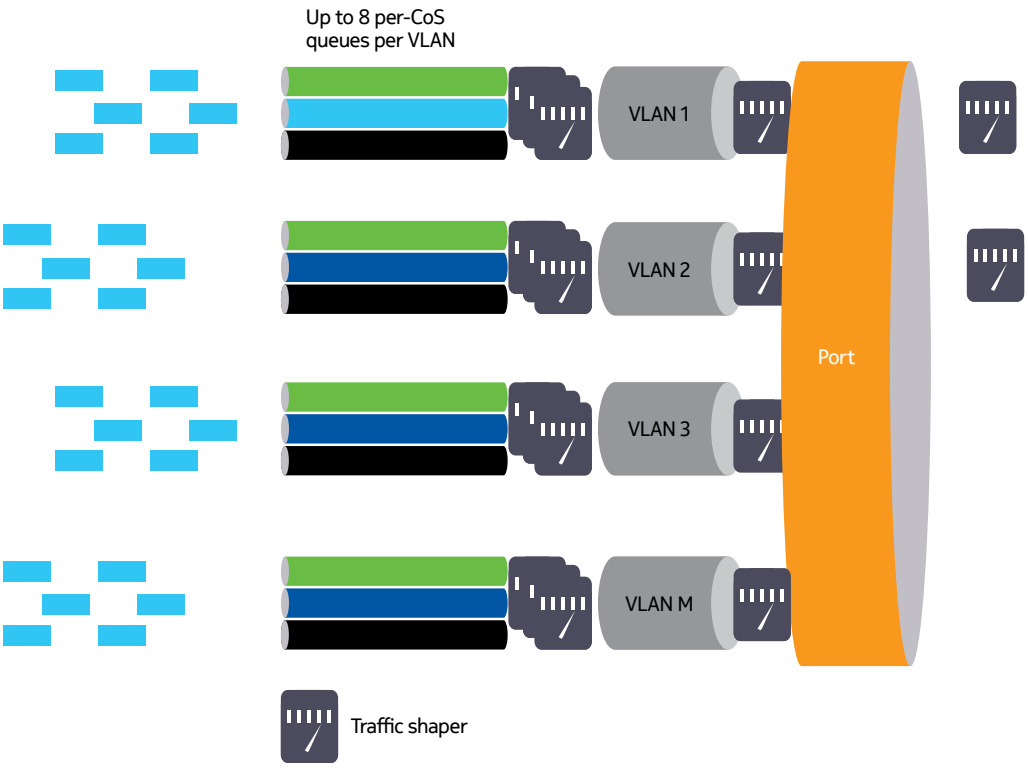
Hierarchical QoS

Ethernet switches typically support port-based queuing, which cannot provide QoS on a per-service basis. By contrast, an IP/MPLS service-oriented network can classify and treat traffic with a fine granularity on a per-service, per-class basis, with extensive hierarchical queuing and shaping versatility. This highly flexible QoS capability enables numerous different services for many applications simultaneously.

Each service can have its own traffic management parameters — committed rate, peak rate, burst size and class of service — sharing the same port in the same network without compromising application performance.

Figure 12 shows an example of how hierarchical QoS can be applied on multiple queues for multiple VLAN interfaces, each for a different application, inside one physical port. Each queue can have its own parameters, including traffic rate and forwarding class priority. This traffic management capability provides great flexibility in controlling packet delivery priority among all applications according to their specific QoS requirements.

Figure12. Hierarchical QoS for multiple queues and VLAN interfaces



Traffic engineering

In an IP-only network, packets from source nodes to destination nodes travel along a path that is determined by routing information computed by IP routers. This method offers little flexibility for operators to provide alternate paths and to control traffic flow.

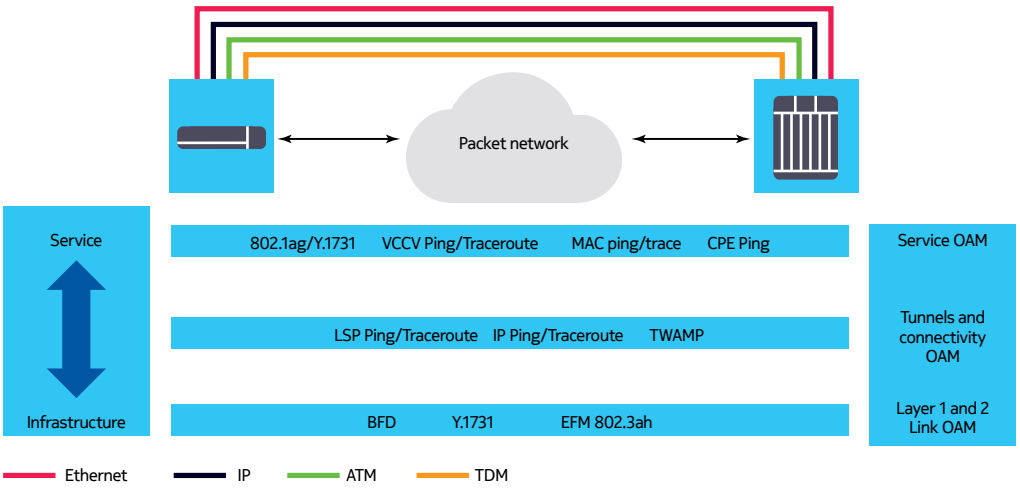
By contrast, an IP/MPLS network supports traffic engineering, with which an MPLS tunnel (logical circuit) can be defined to follow explicit paths that are different from the least-cost IP path. Moreover, in situations where there are multiple tunnels or destinations, forwarding decisions can be made based on the service or packet classification policy. This capability allows operators to achieve more efficient network utilization.

Comprehensive OAM capabilities

An Ethernet bridging-based network supports limited tools to help install and debug the network, based on IEEE 802.3ah EFM (Ethernet in the First Mile) OAM and IEEE 802.1ag CFM (Connectivity Fault Management).

As shown in Figure 13, MPLS networks can expand beyond the Ethernet OAM tools to provide comprehensive OAM tools across layers, such as Label Switched Path (LSP) ping and trace route, Bidirectional Forwarding Detection (BFD) and Virtual Circuit Connectivity Verification (VCCV). In addition, VPLS-based OAM tools such as MAC ping, MAC trace, MAC purge, and customer premises equipment (CPE) ping help simplify the installation and day-to-day operations of an MPLS network.

Figure 13. Comprehensive OAM capabilities

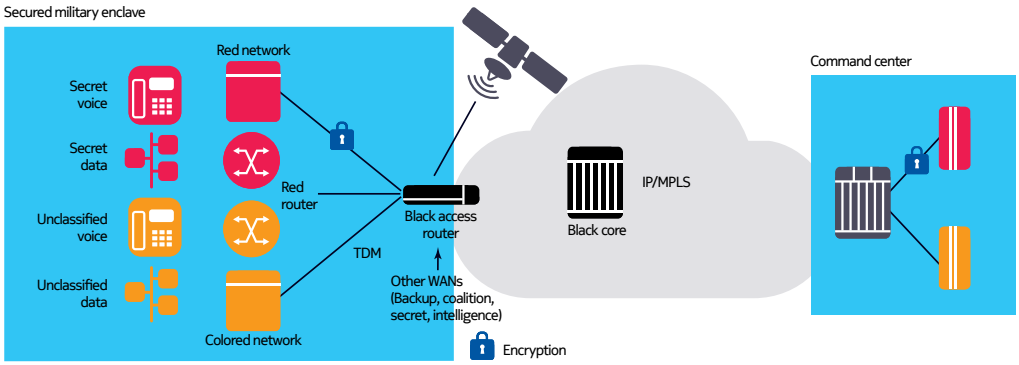


Moreover, with a central service-aware management system, network operators can periodically run OAM tools to verify connectivity, delay and jitter performance for every service; this ensures deterministic network delivery all the time.

Secure communications

Defense network operators often use the term “red/black communications” (see Figure 14) to denote the level of confidentiality of information that can be transmitted over a particular network. A red communications network can transport classified but unencrypted data. A black communications network can transport unclassified unencrypted data and classified encrypted information. When classified information is to be transmitted over a black network, it must first be encrypted.

Figure 14. A red/black defense network blueprint

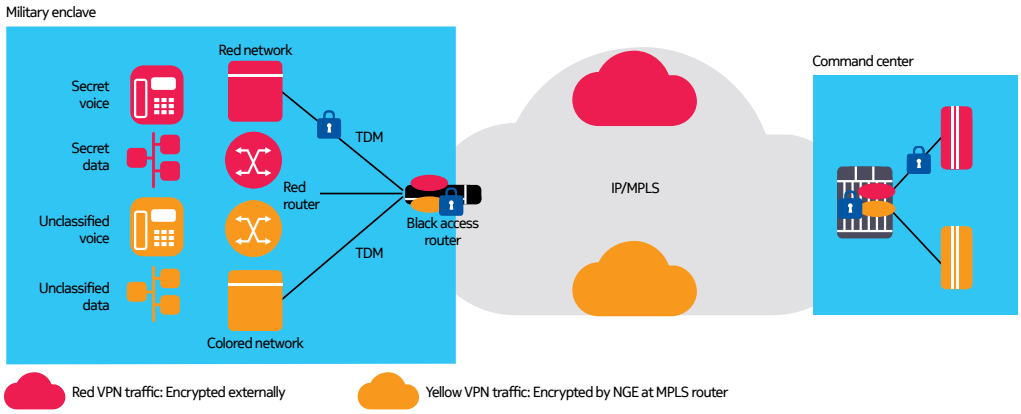


Even though unclassified information is unrestricted, when transporting over a black network the use of network-wide encryption can prevent an unauthorized general information leak or a breach of employee information privacy. Complementing IPsec encryption of classified data before entering a black network, network group encryption (NGE)[7] can provide a full-mesh of secure tunnel to transport unclassified data. Network group encryption provides versatile encryption for not just IP but also general Layer 1 and Layer 2 services. In addition, NGE rides seamlessly over an MPLS network with any-to-any secure tunnel connectivity and full service awareness.

Because NGE is service-aware, it can selectively encrypt only the service that carries unrestricted data but not the confidential data that is already encrypted by the military security gateway (see Figure 15).

7 For a detailed description of NGE and other applicable network security measure, please read Securing Mission-Critical Networks with 7705 SAR. http://resources.alcatel-lucent.com/asset/174129

Figure 15. Service-aware NGE encrypting only unencrypted unrestricted information



Other advanced security techniques such as stateful firewall can also be deployed in parallel to prevent unauthorized IP flows. This stops illicit attempts to contact user equipment attached to the VPN and user equipment trying to reach out to other hosts in the network.

Simplified network management

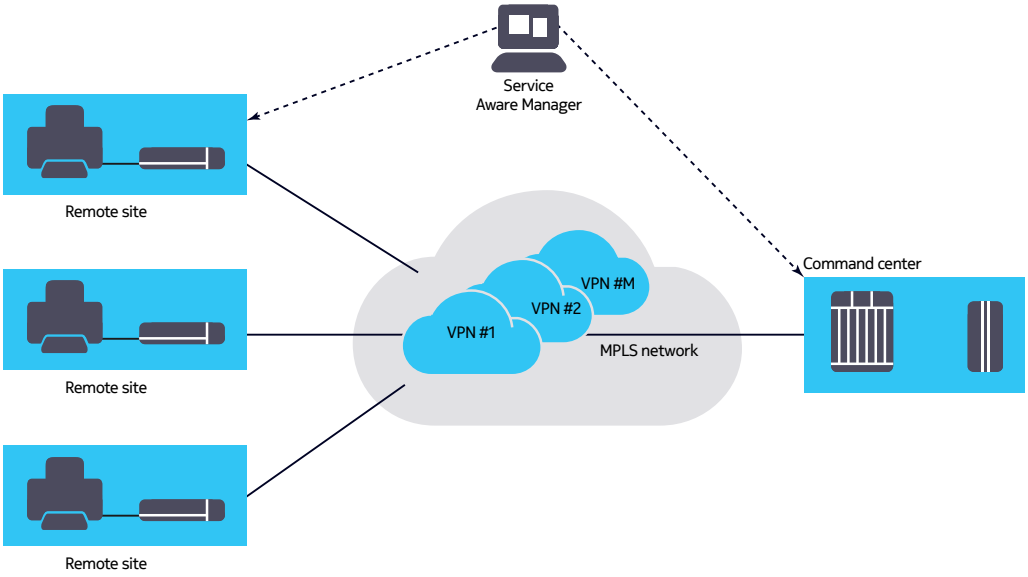
Managing a converged defense network can be an overwhelming and complex task. Operators need to be able to deploy new VPNs quickly, driven by new communications needs as missions are launched. Operators also need to monitor network performance constantly to ensure connectivity for mission-critical communications.

Service-aware management

With a world-class, service-aware management system, operators can quickly provision and efficiently manage end-to-end service and be ready to scale up the number of VPN services when application requirements grow. The management system can also deliver service assurance and network performance monitoring by executing OAM tests continually across the network. If connectivity or performance degrades, the management system notifies operators automatically.

Figure 16 shows an MPLS network provisioned with multiple VPNs. With a pre-defined configuration template and network policies, operators can quickly configure new services or re-configure the network as required.

Figure16. MPLS network with multiple managed Layer 1, Layer 2 and Layer 3 VPNs

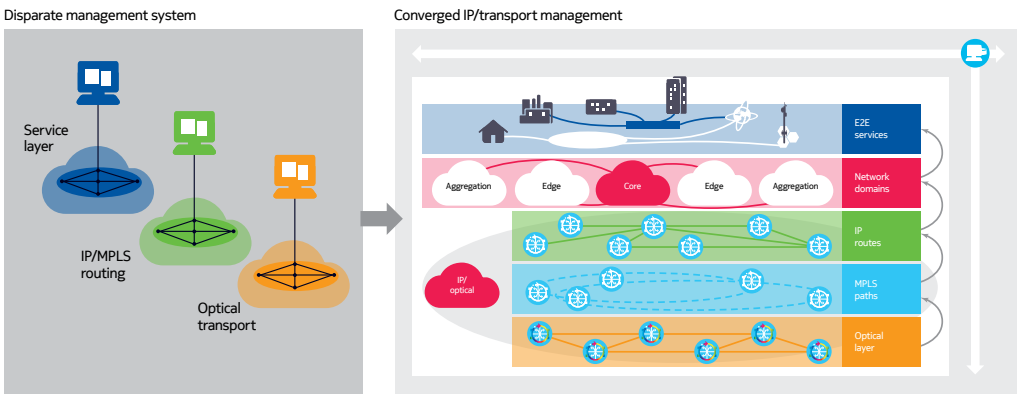


Cross-layer service-aware network management

An IP/MPLS network rides over a transport layer using optics or microwave technology. The traditional way of managing a multi-layer, multi-technology network is to deploy disparate management systems (see Figure 17), one for each layer (IP/MPLS and transport) and each technology (optics and microwave). This approach complicates the task of provisioning, monitoring and troubleshooting. It is also costly and inefficient.

A cross-layer, service-aware network manager integrates transport layer management with the IP/MPLS services layer. Operators can now gain unprecedented visibility of the condition of the network and services, correlate network events and alarms of different layers and technology domains, as well as optimize operation and cost efficiency.

Figure 17. A Converged IP/transport network manager



NOKIA

Conclusion

As defense forces globally are fully embracing the network-centric warfare doctrine, network modernization has become a key focus of defense transformation. Operators of mission-critical communications networks in defense must modernize their networks to ready for the implementation of the doctrine. An IP/MPLS network will play a pivotal role in providing the defense communications required by the doctrine.

A successful execution of network transformation rests not only on technology. Network design expertise and professional services are equally crucial. Complemented by a comprehensive and innovative product portfolio that spans microwave transport, optics transport and IP/MPLS, Nokia can help governments to build a network that serves and protects their citizens better, faster and more efficiently.

Click here to find out more about Nokia solutions for defense.

Acronyms

ATM	Asynchronous Transfer Mode
BFD	Bidirectional Forwarding Detection
CCTV	closed-circuit television
CFM	Connectivity Fault Management
CoS	Class of Service
CPE	customer premises equipment
CWDM	Coarse Wavelength Division Multiplexing
DSL	digital subscriber line
EFM	Ethernet in the First Mile
FRR	Fast Reroute
HDLC	High-Level Data Link Control
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IP-VPN	IP Virtual Private Network
IPv4	IP version 4
IPv6	IP version 6
LAN	local area network

LSP	Label Switched Path
MAC	Media Access Control
MPLS	Multiprotocol Label Switching
NGE	network group encryption
OAM	operations, administration and maintenance
PPP	Point-to-Point Protocol
QoS	Quality of Service
R-VPLS	Routed VPLS
SDH	Synchronous Digital Hierarchy
SONET	Synchronous Optical Network
STP	Spanning Tree Protocol
TDM	Time Division Multiplexing
TWAMP	Two-Way Active Measurement Protocol
VCCV	Virtual Circuit Connectivity Verification
VLAN	Virtual LAN
VLL	Virtual Leased Line
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network
VPRN	Virtual Private Routed Network
VPWS	Virtual Private Wire Service
VRF	Virtual Routing and Forwarding
WDM	Wavelength Division Multiplexing

NOKIA

References

1. Nokia. Building a multi-fault tolerant microwave backhaul network, technical white paper. March 2015.
2. Nokia 7705 Service Aggregation Router: Security overview for mission-critical networks, application note. March 2015.
3. IEEE. 802.1ag-2007 - IEEE Standard for Local and Metropolitan Area Networks Virtual Bridged Local Area Networks Amendment 5: Connectivity Fault Management.
4. IEEE. 802.3-2002 - IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications.
5. IEEE. 802.3ah-2004 - IEEE Standard for Information technology-- Local and metropolitan area networks-- Part 3: CSMA/CD Access Method and Physical Layer Specifications Amendment: Media Access Control Parameters, Physical Layers, and Management Parameters for Subscriber Access Network.
6. IETF. RFC 3985: Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture. March 2005.
7. IETF. RFC 4090: Fast Reroute Extensions to RSVP-TE for LSP Tunnels. May 2005.
8. IETF. RFC 5286: Basic Specification for IP Fast-Reroute: Loop-free Alternatives. September 2008.
9. IETF. RFC 6718: Pseudowire Redundancy. August 2012.
10. ITU-T. Recommendation G.8032: Ethernet ring protection switching.

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

Product code: PR1504010591EN