NOKIA

Mission-critical communications for the oil and gas industry

Converging robust, reliable services for critical applications

Technology White Paper

The oil and gas industry relies on resilient, secure, service-aware networks to provide essential communications for their daily operations. New mission-critical applications, developed on powerful computing platforms, are starting to become IP/Ethernet-based. They are also more bandwidth intensive, providing richer information to the control center. Network operators are considering cost-effective technologies that can fulfill both legacy and new application requirements without degrading performance or reliability.

Multiprotocol Label Switching (MPLS)-based technology, with its service-oriented virtual private network (VPN) capability, can fulfill these requirements by converging applications in a single network. With new generations of silicon technology, MPLS and VPNs can be deployed end-to-end, from terabit core systems in a climate-controlled operations centers, to hardened and ruggedized gigabit edge platforms in environmentally challenging locations. This paper discusses the benefits of MPLS-enabled networks for mission-critical operations networks.

NOKIA

Contents

Mission-critical communications in the era of digital oil and gas operations	3
The evolving role of MPLS in communications networks	5
Today's operations networks	5
Converging to a service-oriented MPLS network	6
The value of MPLS for mission-critical networks	7
Support for Layer 1, 2 and 3 VPNs	7
Traffic engineering	8
Deterministic network recovery behavior	8
Redundant control center equipment protection	9
Central site protection	9
Hierarchical QoS	10
Comprehensive OAM capabilities	11
Security protection	11
Physical medium flexibility and integration	12
Compact, ruggedized outdoor platform	12
MPLS-based VPNs	13
MPLS Layer 1 VPN (TDM pseudowire)	13
MPLS Layer 2 and Layer 3 VPNs	13
Service-aware management	16
Conclusion	17
Acronyms	18

Mission-critical communications in the era of digital oil and gas operations

To feed the world's insatiable appetite for energy, oil and gas companies are undergoing momentous changes. They are extracting fuel at a faster rate, from more distant fields, and under more perilous operating conditions. They are adopting new and innovative digital technologies to maximize production efficiency and workforce productivity, while minimizing impacts on the environment and workforce health and safety. At the same time, they must also extend the life of deployed operational assets to avoid unnecessary disruptions.

A mission-critical communications network is indispensable during this transformation to digital oil and gas operations. Whether it is offshore explorations (Figure 1a), pipeline operations (Figure 1b), or other scenarios, the network plays a seminal role in ensuring oil and gas operations run optimally.

Figure 1a. Offshore Operation Communications Network

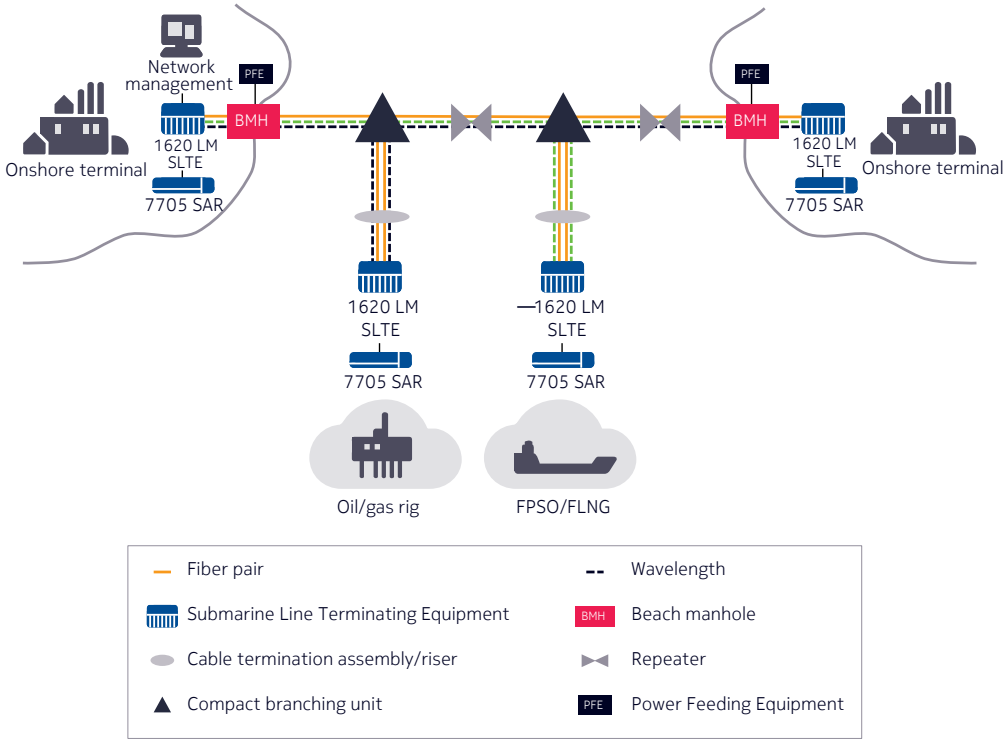
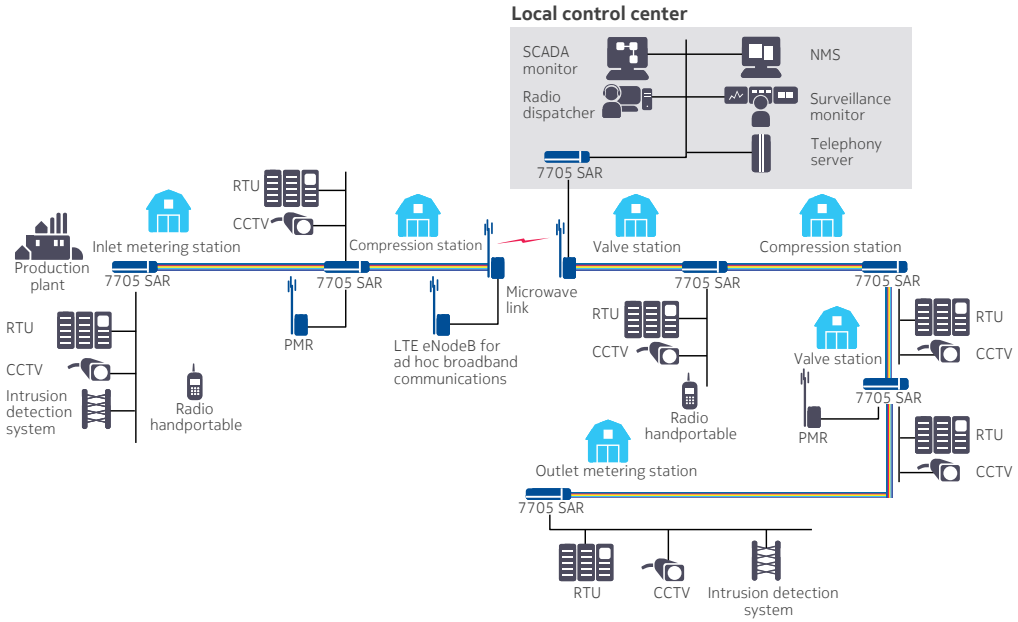


Figure 1b. Offshore Operation Communications Network



The major challenges posed to mission-critical communications network operators are:

Flexibility - While new operational applications are based on Ethernet and IP, legacy applications based on time-division-multiplex (TDM) technology still play a critical role. Operators need network flexibility to adapt to new applications while migrating legacy applications seamlessly onto a converged network.

Scalability - New applications are also becoming more intelligent and bandwidth intensive. Systems such as surveillance and supervisory control and data acquisition (SCADA) and IP video surveillance cameras have been extensively deployed to increase efficiency. Remote collaboration applications are more prevalent. Operators need scalability to accommodate future bandwidth growth and the deployment of more devices and applications.

Predictability - With a large number of applications contending for bandwidth, operators need to deliver traffic in a deterministic manner and still meet the stringent quality of service (QoS) levels required by the applications.

Resiliency - Network outages disrupt applications, which could lead to operation and production stoppages, potentially incurring huge economic losses. Operators need to leverage redundant mechanisms at multiple layers to protect against network faults. They also need Operation, Administration and Maintenance (OAM) tools to rapidly identify and fix any problems that do produce outages.

Security – Cyber attacks are on the rise. With the adoption of IP-based technology and networking, mission-critical IP networks are vulnerable. Operators need to evaluate their security risks and effectively use network security features to shield the network from malicious activities.

Simplicity – As the communications network becomes integral to oil and gas operations, it is crucial that the network manager goes beyond traditional boundaries of element, network and end-to-end service management. Operators require unified, end-to-end network management that can help them to provision services, monitor performance and troubleshoot problems proactively.

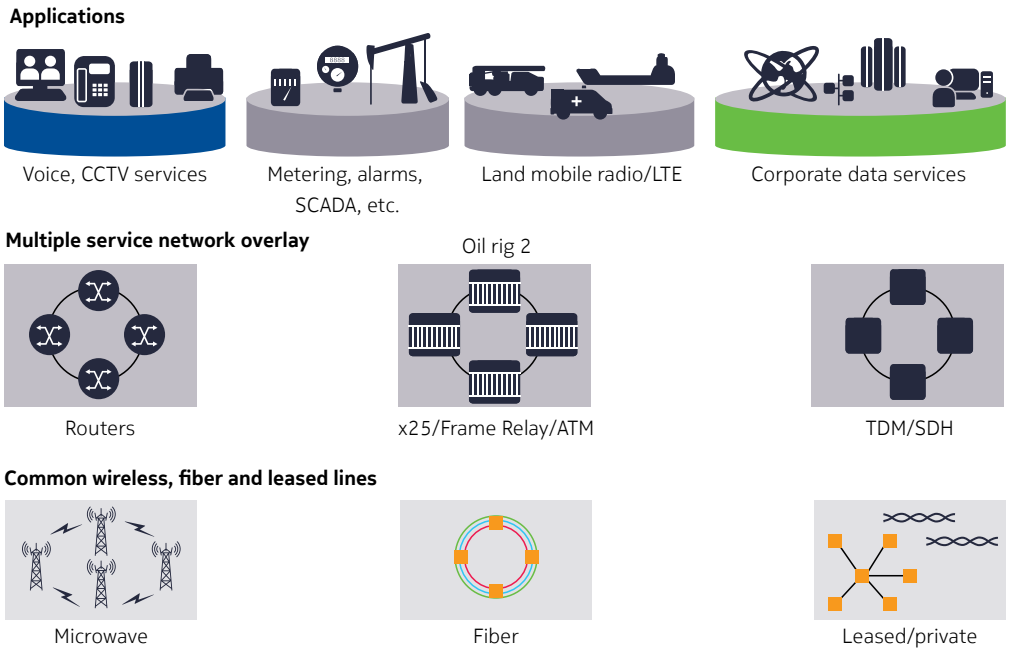
The evolving role of MPLS in communications networks

To address these challenges, operators need to build networks 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 mission-critical network operators have already made a strategic decision to adopt IP/MPLS to meet their requirements.

Today's operations networks

Figure 2 shows a current operations network. Different applications use different protocol-based communications, such as proprietary TDM, PPP, Ethernet and IP, and each application has unique bandwidth and QoS requirements for latency and jitter. Operators often must resort to building different service network overlays while sharing the underlying physical assets of the transmission medium.

Figure 2. Multiple service network overlay with shared physical assets



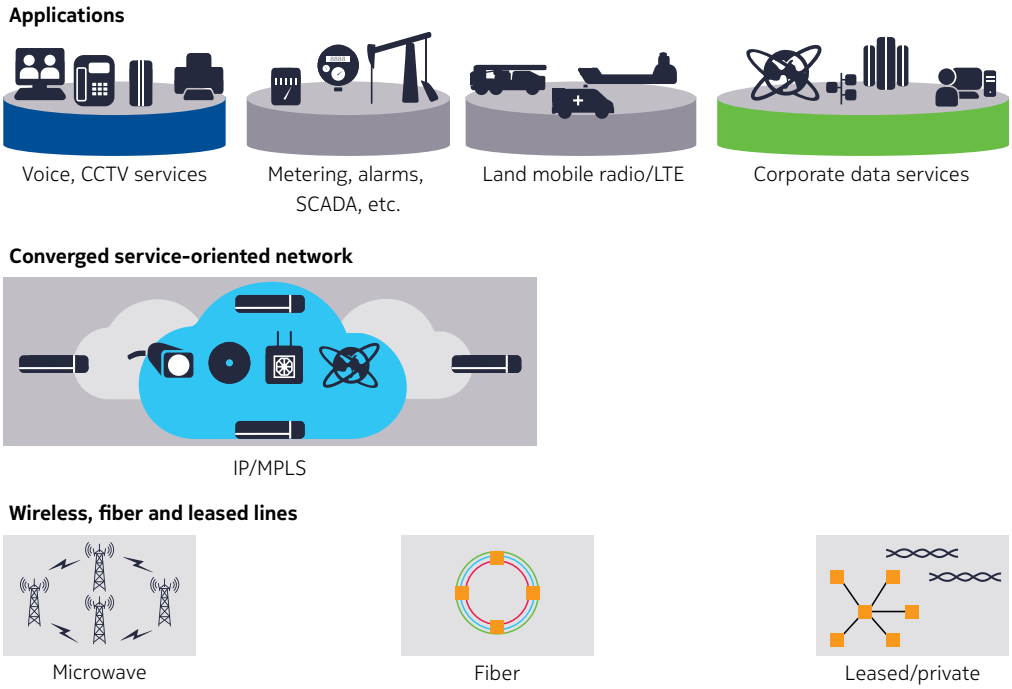
The current model is expensive, because it involves multiple network technologies, equipment and management systems. Moreover, much of the networking equipment has reached - or is approaching - end-of-life, while new applications are being developed and deployed. Finding a cost-effective solution to build networks for next-generation communications and applications has become critical.

Converging to a service-oriented MPLS network

The role of 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 tunnel label has proven to be immensely versatile, adapting to new services and applications with service-level privacy, security and reliability. For mission-critical networks in the oil and gas segment, traffic from key applications, such as SCADA, land-mobile radio and teleprotection is increasingly carried over IP/MPLS networks.

Network operators have found they can use the unique capabilities of IP/MPLS to consolidate all their services into one network without compromising QoS. Operators are effectively adopting a converged network architecture, as shown in Figure 3.

Figure 3. Converged service-oriented network



The value of MPLS for mission-critical networks

A mission-critical network is a private network that provides its organization with a range of services that are essential to the success of its daily operations. MPLS's range of powerful capabilities makes it a key enabling technology for implementing mission-critical networks.

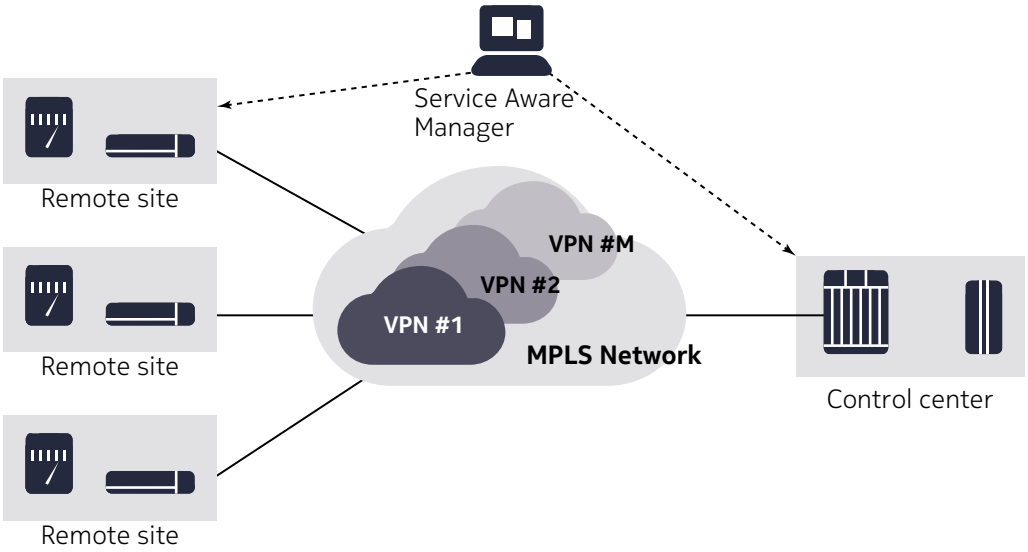
Support for Layer 1, 2 and 3 VPNs

Depending on an application's communication technology, operators can choose to deploy a Layer 1, 2 or 3 VPN over a common network, with each VPN appearing as a dedicated private network to each application.

With full service awareness, each VPN has its own service and QoS policy, just like in an actual physical network. Each VPN is fully segregated, preventing application traffic interference due to congestion. Instead of multiple network overlays in a traditional model, many applications can share a common MPLS infrastructure over a single converged network.

Paired with a world-class, service-aware management system, operators can rapidly provision and efficiently manage end-to-end service and be ready to scale the network and service when application requirements grow. Figure 4 shows an MPLS network provisioned with multiple VPNs. Each VPN can be Layer 1, 2 or 3.

Figure 4. MPLS network with multiple managed L1, L2 and L3 VPNs



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 control traffic flow.

In 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.

Deterministic network recovery behavior

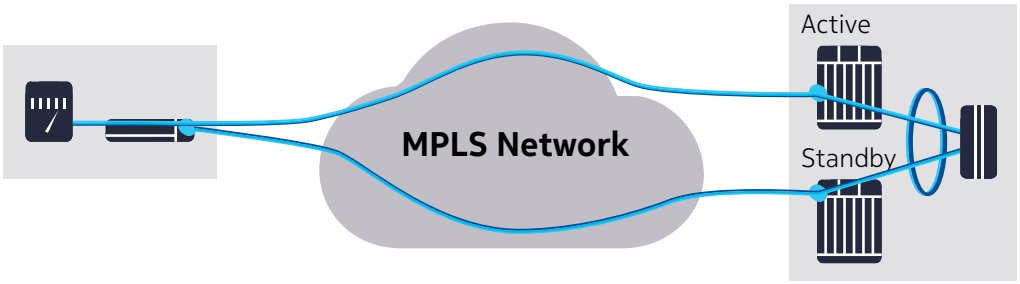
In an Ethernet network running Spanning Tree Protocol (STP), it is difficult to predict recovery times when links or switches fail. Best-case recovery times are in the order of seconds, and while new Ethernet ring technologies such as G.8032 have improved recovery times, these are mostly confined to simple ring topologies due to complications that arise when they are applied to multi-ring/meshed topologies.

With the Fast Reroute (FRR) mechanism, MPLS provides deterministic reroute times that match SDH/SONET transport network recovery times. FRR can deliver switching performance in the order of 50 ms - equivalent to what SDH/SONET provides. FRR is network-topology agnostic and seamless, whether the topology is a single ring, multi-ring, meshed, chain with parallel links, or any combination.

Redundant control center equipment protection

In addition to SDH/SONET-like network protection and pseudowire technology that enables VPN services (see "MPLS-based VPNs" section below), MPLS offers central router and interface equipment protection, as shown in the control center in Figure 5.

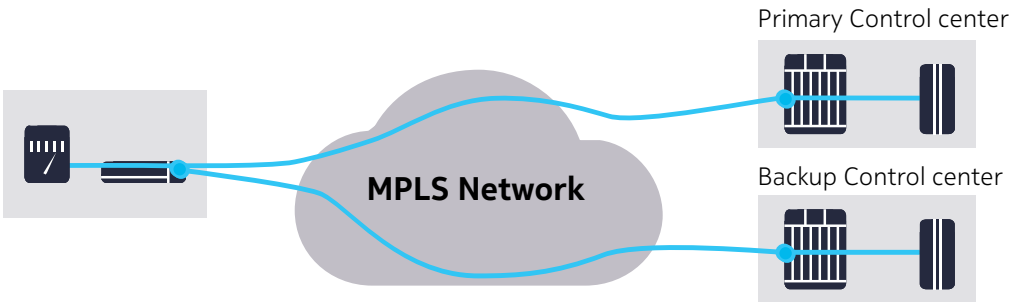
Figure 5. Central router and interface equipment protection



Central site protection

It is imperative that mission-critical networks develop recovery plans in case a natural disaster or other serious accident damages the control 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 5 can be extended to cover such a scenario, as shown in Figure 6.

Figure 6. Central site protection

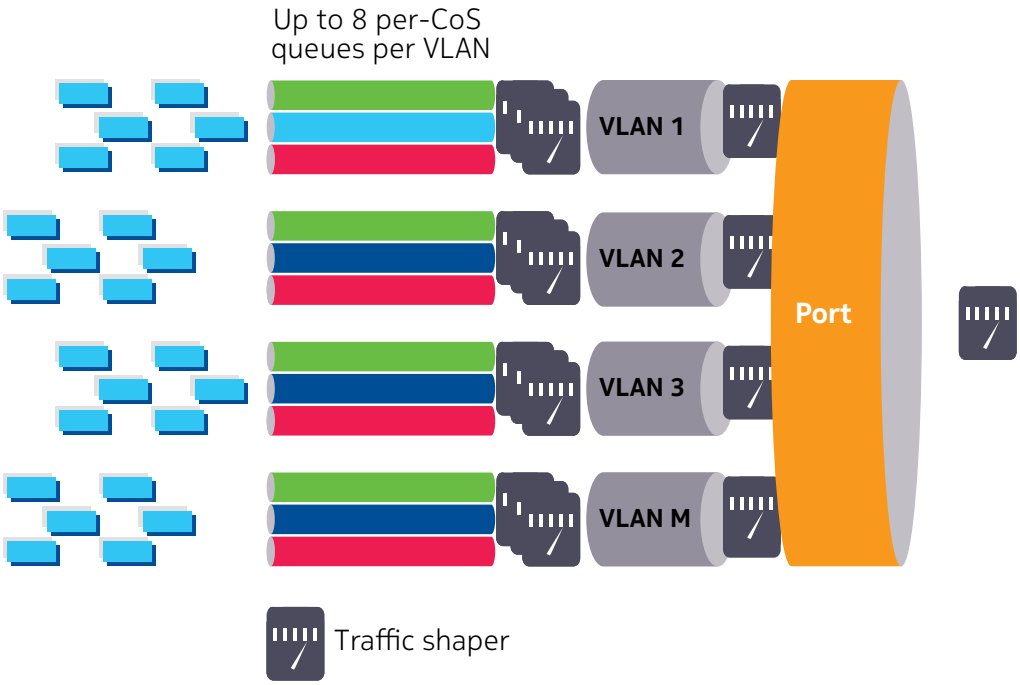


Hierarchical QoS

While Ethernet switches typically support port-based queuing, an MPLS service-oriented network can classify and treat traffic with fine granularity on a per-service, per-class basis, with extensive hierarchical queuing and shaping versatility. Such highly flexible QoS engineering enables numerous different services for many applications. Each service can have its own traffic management parameters - committed rate, peak rate, burst size and class of service - in the same network, without compromising application performance.

Figure 7 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 gives great flexibility in controlling packet delivery priority among all applications according to their specific QoS requirements.

Figure 7. Hierarchical QoS for multiple queues and VLAN interfaces

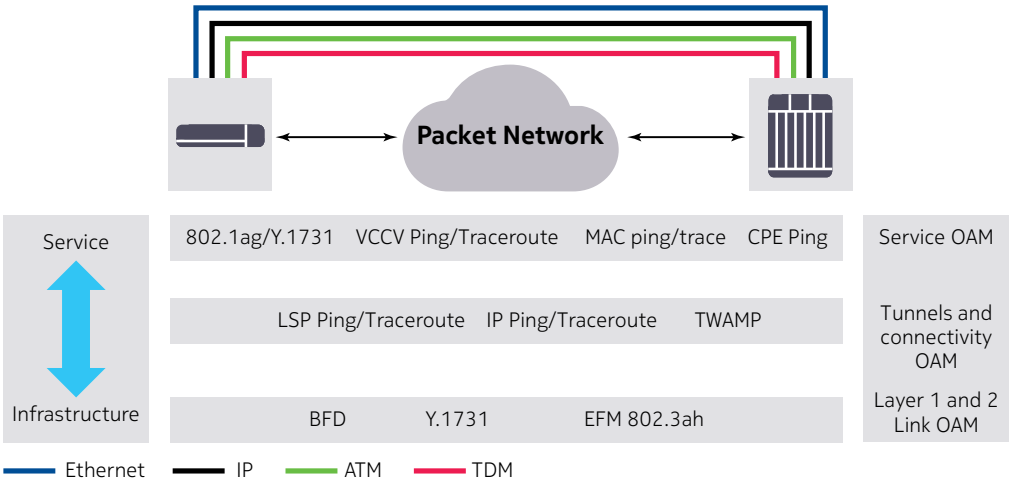


Comprehensive OAM capabilities

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 8, 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, Virtual Private LAN Service (VPLS)-based OAM tools, such as Media Access Control (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 8. 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.

Security protection

MPLS traffic is inherently secure due to its use of LSPs. Since an LSP is a tunnel switched by a network-assigned label, it is immune to malicious traffic. All such traffic sent by attackers will be dropped by the MPLS platform. Even if the attacker can masquerade attack traffic - for example, in the form of labeled packets - those packets would be dropped because they come from an outside, non-MPLS domain. This is why unauthorized packets can never penetrate the MPLS network.

The use of VPN in an MPLS-based network provides further protection. For each MPLS-based VPN, there is a dedicated and isolated routing and forwarding instance or cross-connect table, depending on the VPN type. It is not possible to interfere with VPN service.

Moreover, advanced techniques such as stateful firewall and MPLS traffic encryption are available to stop compromised hosts inside a VPN from sending illicit traffic and to ensure data confidentiality and integrity, respectively.

Physical medium flexibility and integration

MPLS runs effectively over a full range of Layer 1 transmission technology (microwave, fiber and copper DSL) and physical links (SDH/SONET, PDH and T1/E1). Moreover, these technologies can be mixed 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.

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

Compact, ruggedized outdoor platform

With a new generation of powerful, energy-efficient silicon, MPLS is available in com- pact, ruggedized and outdoor form factors without sacrificing the richness of network features. Coupled with passive cooling, this new type of MPLS platform allows MPLS deployment to extend to the edge of the network, even in uninhabitable terrain.

NOKIA

MPLS-based VPNs

MPLS-based VPNs enable an MPLS network to be shared by each application, functioning as its own private or separate network. Depending on connectivity, the network can be a Layer 1, 2 or 3 VPN, with all the previously described 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 for Layer 1 VPNs for TDM traffic - with the same stringent delay, strict QoS and rapid switching protection performance - is essential because many legacy critical applications still need to be supported. MPLS, with its range of benefits, is in a unique position to address this challenge.

Some critical applications such as SCADA are point-to-multipoint, with the central master sequentially polling individual slaves for data and status information over serial interfaces. As a result, TDM bridging is required to support such applications - a frequent barrier to the adoption of new network technologies. Fortunately, some advanced MPLS platforms support this type of Layer 1 (TDM) VPN with Multi-Drop Data Bridge (MDDB) capability.

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 approach, commonly referred to as a Layer 2 VPN, includes virtual leased lines (VLLs), also known as pseudowires, and VPLS, which is a virtual Ethernet bridging service. A Layer 3 approach is referred to as a Layer 3 VPN or IP-VPN. An integrated Layer 2 and Layer 3 approach is known as Routed VPLS (R-VPLS). The following sections describe the various types of Layer 2 and Layer 3 VPNs.

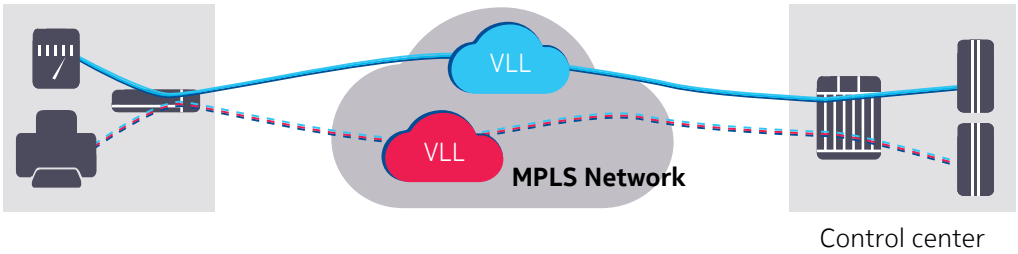
Layer 2 VPN - VLL

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 as previously described), Ethernet, frame relay, PPP, High-Level Data Link Control (HDLC) or ATM. Other than TDM, the most popular traffic type is Ethernet (pseudowire or E-Line). A VLL is like a virtual circuit, similar to older packet technologies such as X.25, frame relay and ATM.

A 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.

Figure 9 shows two end-to-end VLLs that separately connect two end devices to a central site.

Figure 9. Layer 2 VPN – VLL

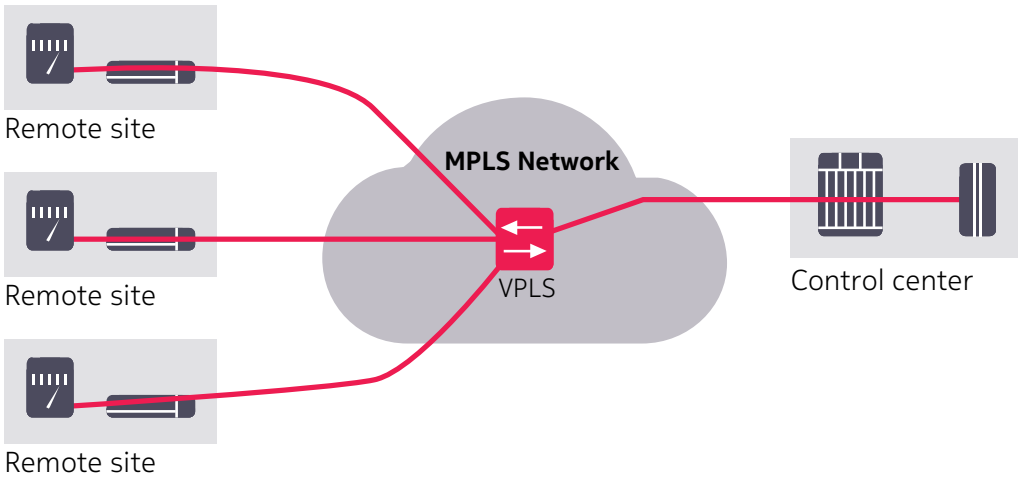


Layer 2 VPN - VPLS

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

Figure 10 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 10. Layer 2 VPN – VPLS



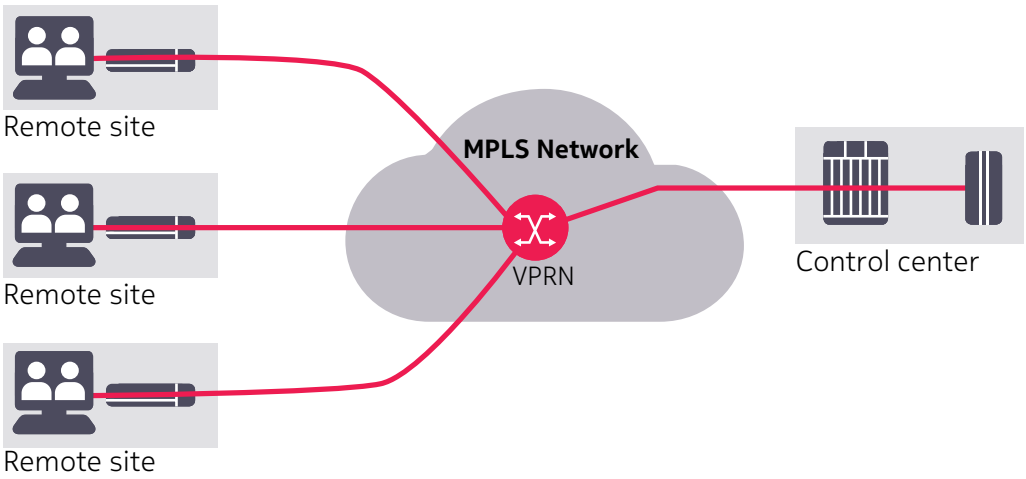
In a Layer 2 VPN - VPLS, forwarding decisions are based on the Ethernet MAC address. Each application or department can be assigned a dedicated VPLS or Layer 2 broadcast domain. MAC address duplications are, therefore, supported across domains because all VPLS instances are segregated.

The underlying VPLS mechanism is an IEEE 802.3 MAC learning bridge, so minimal configuration is required and adding new sites is simple. A Layer 2 VPN - VPLS is trans- parent to Layer 3 routing protocols and is an ideal solution for non-IP communications such as Generic Object Oriented Substation Events (GOOSE) messaging, used in power utilities teleprotection applications.

Layer 3 VPN

A Layer 3 VPN, or IP-VPN, is sometimes called a Virtual Private Routed Network (VPRN). Figure 11 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 11. Layer 3 VPN (IP-VPN)

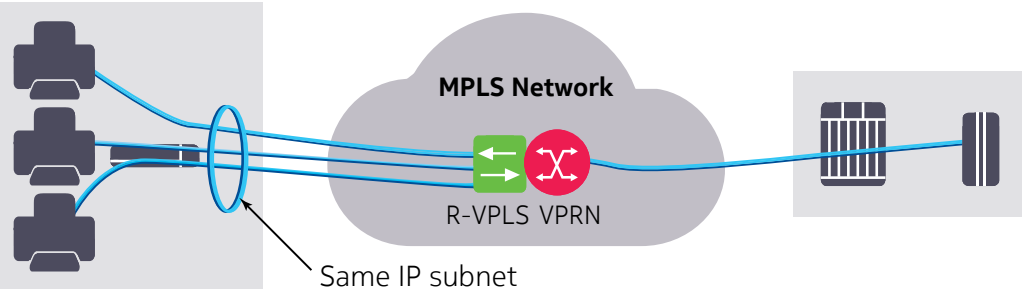


A Layer 3 VPN is implemented only for IP traffic and provides multipoint-to-multipoint IP connectivity, with forwarding decisions based on the IP address. IP packet forwarding decisions can, optionally, be policy-based for greater flexibility. Overlapping IP address schemes are supported because each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

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 12. This integration of a Layer 2 VPN into a Layer 3 VPN is also known as Routed VPLS (R-VPLS).

Figure 12. 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.

Service-aware management

An effective, powerful management platform is a key element of reliable, flexible and scalable IP/MPLS-based infrastructures. A service-aware management platform provides easy network configuration and inventory control; fast, effective fault isolation and resolution; and support for new applications. It can also enable operators to perform proactive network performance monitoring and alarms correlation to help resolve problems before they affect operations.

The cost to provision, operate and maintain an IP/MPLS-based network is optimized when service-aware management is combined with other management applications, such as a web-based portal and IP control plane assurance manager.

NOKIA

Conclusion

Oil and gas operators face immense daily challenges. They must keep their deployed operational applications running smoothly to support current operations and production. At the same time they must plan to transform their strategic telecommunications and applications technology to reap the full benefits of an IP/Ethernet-based world. Operators must be resourceful when expanding their network to newly discovered fields, and, at the same time, keep cyberattackers at bay.

With MPLS, network operators can support legacy applications while fully emulating TDM and SONET/SDH-based network stability, security and reliability. MPLS provides a full suite of VPN service capabilities to provision connectivity for next-generation applications. It is also transmission media- and physical layer-agnostic, for optimum network architectural flexibility. Finally, MPLS can run seamlessly over various transmission mediums, such as fiber, microwave, satellite and copper, rendering a unified end-to-end, service-oriented view to operators. MPLS has, therefore, become the networking technology of choice when building converged, mission-critical networks.

The Nokia MPLS product portfolio ranges from terabit systems to outdoor compact form factors that share the same operating system, command-line interface (CLI), routing and service capability and service-aware management.

Nokia is a market leader and technology innovator, with years of experience developing and helping operators deploy world-class MPLS platforms and comprehensive end-to-end MPLS managed solutions. Nokia IP/MPLS-based service routing and switching products offer mission-critical network operators the flexibility, scalability and feature sets required by next-generation applications.

NOKIA

Acronyms

ATM	Asynchronous Transfer Mode
BFD	Bidirectional Forwarding Detection
CCTV	Closed-circuit television
CFM	Connectivity Fault Management
CLI	Command-line interface
CoS	Class of Service
CPE	Customer premises equipment
CWDM	Coarse Wavelength Division Multiplexing
DSL	Digital subscriber line
E-LAN	Ethernet LAN
E-Line	E-Line
EFM	Ethernet in the First Mile
FRR	Fast Reroute
GOOSE	Generic Object-Oriented Substation Event
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, IPv6	IP version 4, IP version 6
LAN	Local area network
LMR	Land Mobile Radio
LSP	Label Switched Path
LTE	Long Term Evolution
MAC	Media Access Control
MDDB	Multi-Drop Data Bridge
MPLS	Multiprotocol Label Switching
OAM	Operations, administration and maintenance
PPP	Point-to-Point Protocol
QoS	Quality of Service

R-VPLS	Routed VPLS
SCADA	Supervisory control and data acquisition
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

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

Product code: MKT2014118774EN