NOKIA

MPLS for mission-critical networks

Converging robust, reliable services for critical applications

Technology white paper

Mission-critical industries and agencies—from power utilities to oil and gas drilling to public transport and public safety to defense—are increasingly relying on resilient, secure, service-aware networks to provide the essential communications for their daily operations. New mission-critical applications, developed on powerful computing platforms, are becoming IP/Ethernet-based and are more bandwidth-intensive so that they can supply the richer information required. Network operators are considering cost-effective technologies that fulfill legacy and new application requirements without degrading performance or reliability.

Multiprotocol Label Switching (MPLS)-based technology, with its service-oriented virtual private network (VPN) capabilities, easily fulfills these requirements by controlling application traffic and 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 center 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

NOKIA

Evolving role of MPLS in communications networks

Today's network operators face a range of challenges.

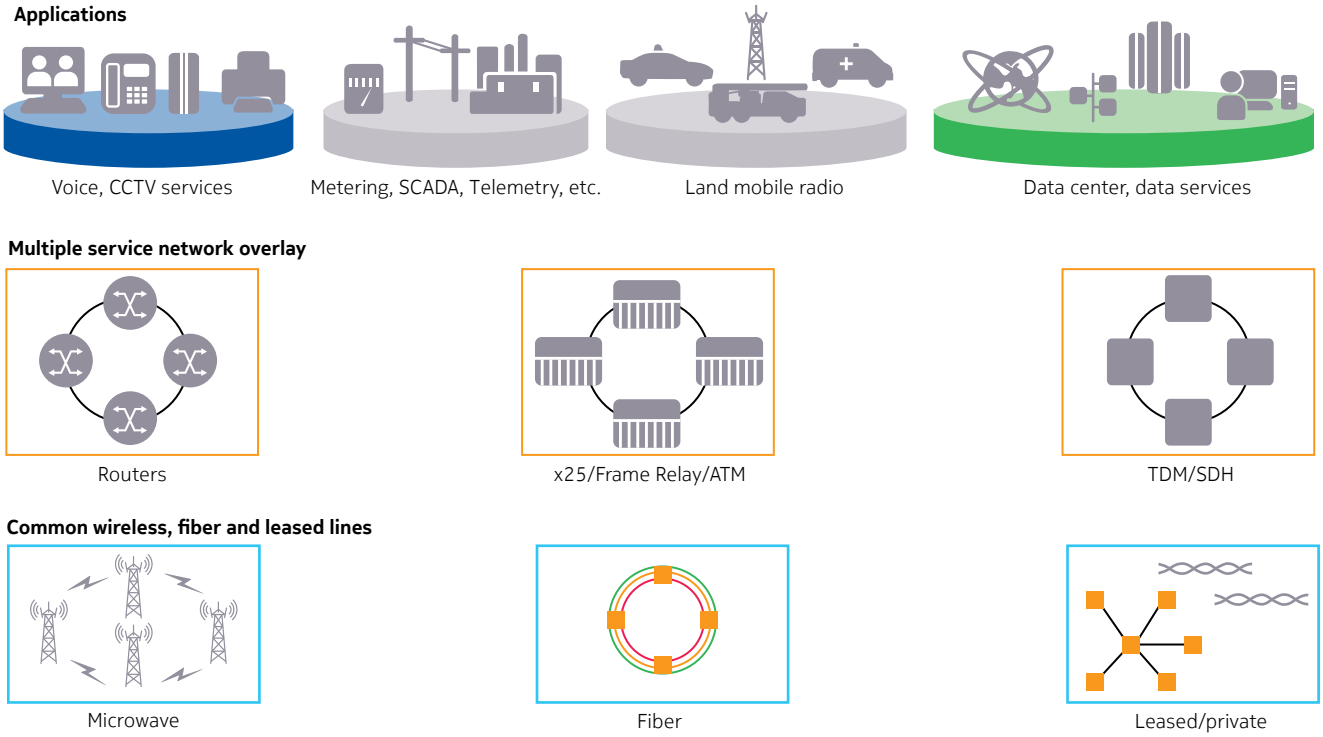
1. With the wide adoption of inexpensive processors, remote equipment is becoming increasingly intelligent, gathering more information for the associated applications; for example, high-definition video surveillance and supervisory control and data acquisition (SCADA).
2. Bandwidth usage for communications is rapidly increasing, and IP/Ethernet connectivity is required.
3. Legacy end equipment is expected to remain in operation for another five to ten years, running over legacy proprietary protocols.
4. Communications network reliability and performance requirements remain stringent.
5. Cost control is essential.

Many operators of mission-critical networks have already made a strategic decision to adopt IP/MPLS to meet their requirements.

Today's operations networks

Figure 1 shows a current operations network. Different applications utilize different protocol-based communications, such as proprietary Time Division Multiplexing (TDM), Point-to-Point Protocol (PPP), Ethernet and IP, and each application has unique bandwidth and quality of service (QoS) requirements for latency and jitter. Operators must often resort to building different service network overlays while sharing the underlying physical transmission medium assets.

Figure 1. Multiple service network overlay with shared physical assets



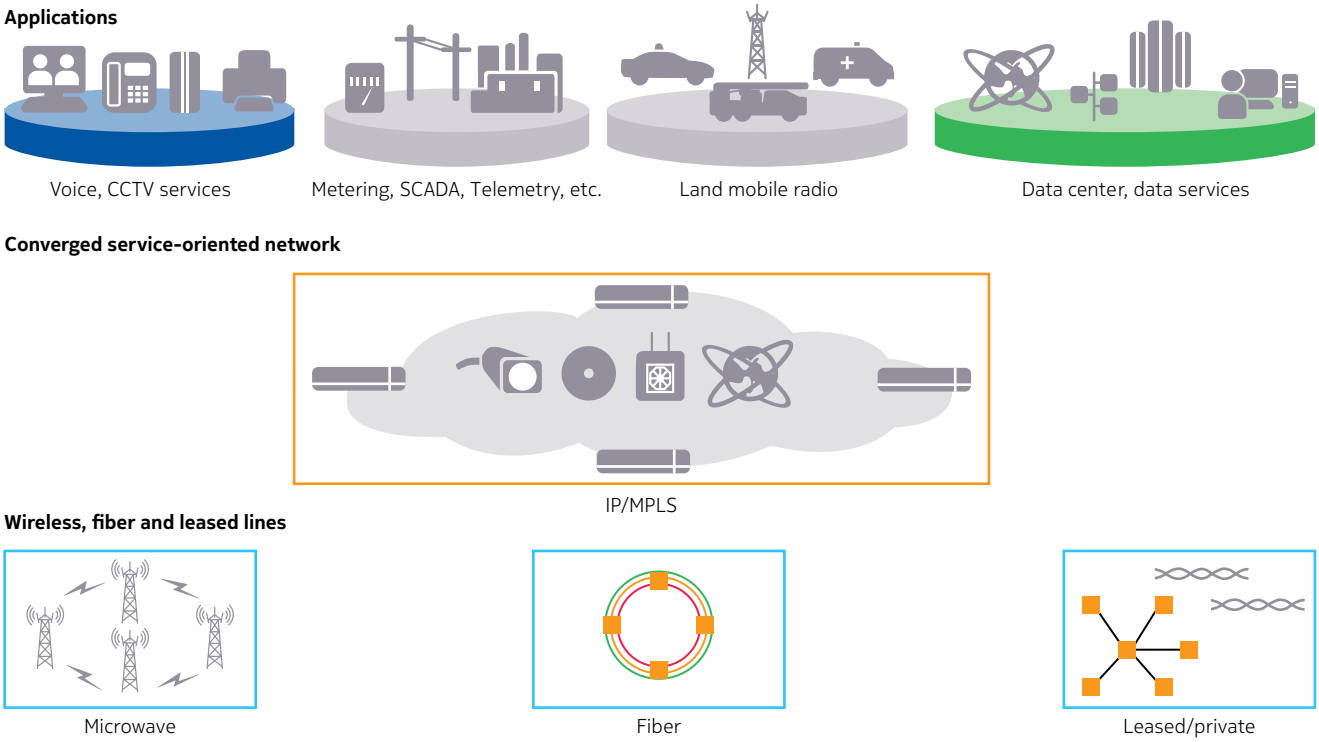
The current model is expensive because it involves multiple network technologies, equipment and management systems. Moreover, much network equipment has reached or is approaching end-of-life, while new applications are being developed and deployed. Finding a cost-effective solution to build networks 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 virtual private network (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 immensely versatile, adapting to new services and applications with service-level privacy, security and reliability. For critical operations networks in industry markets, traffic from key applications such as SCADA, land mobile radio (LMR) and teleprotection is increasingly carried over IP/MPLS networks.

Leveraging the uniquely rich capabilities of IP/MPLS, network operators have found they can consolidate all their services into one IP/MPLS network without compromising QoS. Operators are effectively adopting a converged network architecture, as shown in Figure 2.

Figure 2. 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 its daily successful and safe operation. With a range of powerful capabilities, MPLS is a key enabling technology for implementing mission-critical networks.

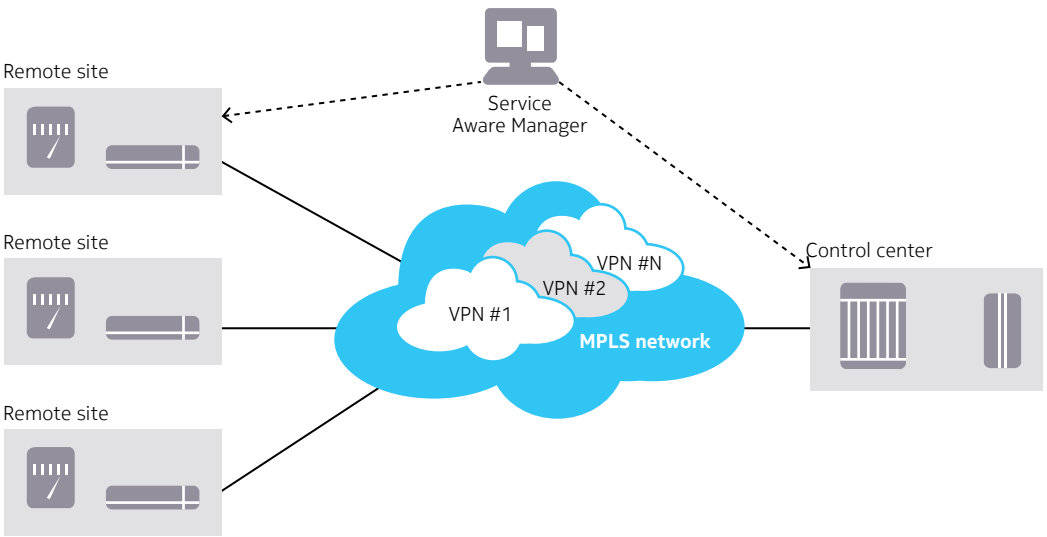
Support for Layer 1, 2 and 3 VPNs

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 for each application.

With full service awareness, each VPN has its own service and QoS policy, just as in physically separate networks. Each VPN is fully segregated, preventing application traffic from one application interfering with another because of congestion, for example. Instead of requiring multiple network overlays in a traditional model, multiple distinct 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 services and be ready to easily scale up the network and services when application requirements grow. Figure 3 shows an MPLS network provisioned with multiple VPNs. Each VPN can be Layer 1, 2 or 3. The remote sites can be LMR locations for public safety applications, substations for power utilities, terminals for transportation authorities, field offices for military applications, and so on. The control center could be a head office, main data center or command center.

Figure 3. MPLS network with multiple managed L1, L2 and L3 VPNs



Traffic engineering

In an IP-only, non-MPLS-based network, packets from source nodes to destination nodes travel along a path that is determined by routing information computed by the 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, where an MPLS tunnel (logical circuit) can be defined to follow explicit paths for quality assurance rather than uncontrolled paths based only on least cost. 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, secure network utilization.

Deterministic network recovery behavior

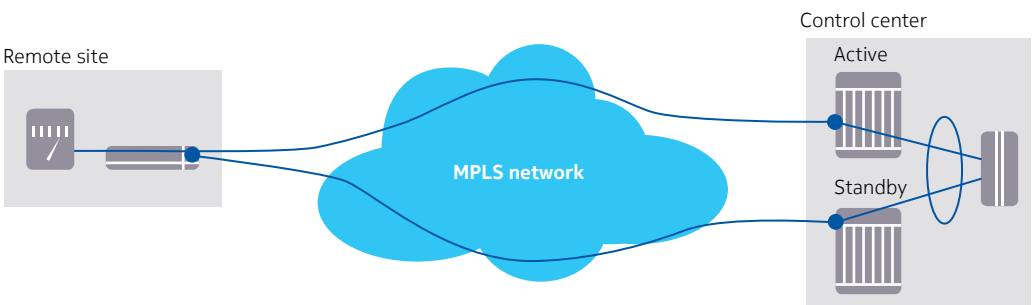
In a typical Ethernet network running Spanning Tree Protocol (STP), it is difficult to predict recovery times when links or switches fail, and so these are referred to as best-case recovery. Best-case recovery times are in the order of seconds, and while new Ethernet ring technologies such as G.8032 have improved recovery times somewhat, these are mostly confined to simple ring topologies because of complications when 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 or less—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”), MPLS offers central router and interface equipment protection, as shown in the control center in Figure 4.

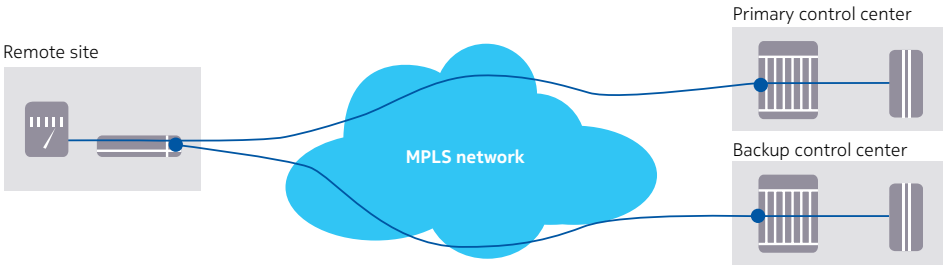
Figure 4. Central router and interface equipment protection



Central site protection

It is imperative that a mission-critical network develop a recovery plan 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 4 can be extended to cover such a scenario, as shown in Figure 5.

Figure 5. Central site protection

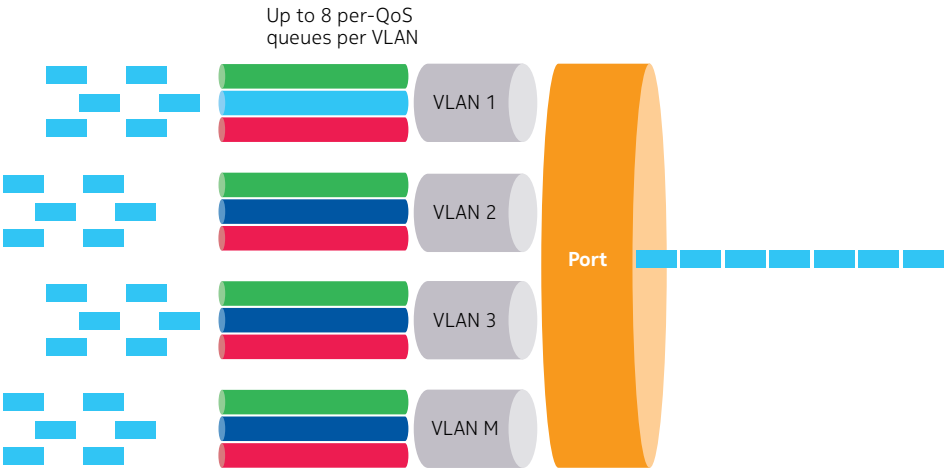


Hierarchical QoS

While Ethernet switches typically support port-based queuing, an 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. Such highly flexible QoS engineering enables numerous different services for each of the 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. This capability ensures the more critical traffic gets though regardless of other traffic, while the less critical traffic will use any available bandwidth left over.

Figure 6 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. The blue boxes and colored tubes represent application traffic, each with their own QoS levels for each VLAN; each VLAN has its own QoS levels within the port, giving ultimate control of traffic flow.

Figure 6. Hierarchical QoS for multiple queues and VLAN interfaces

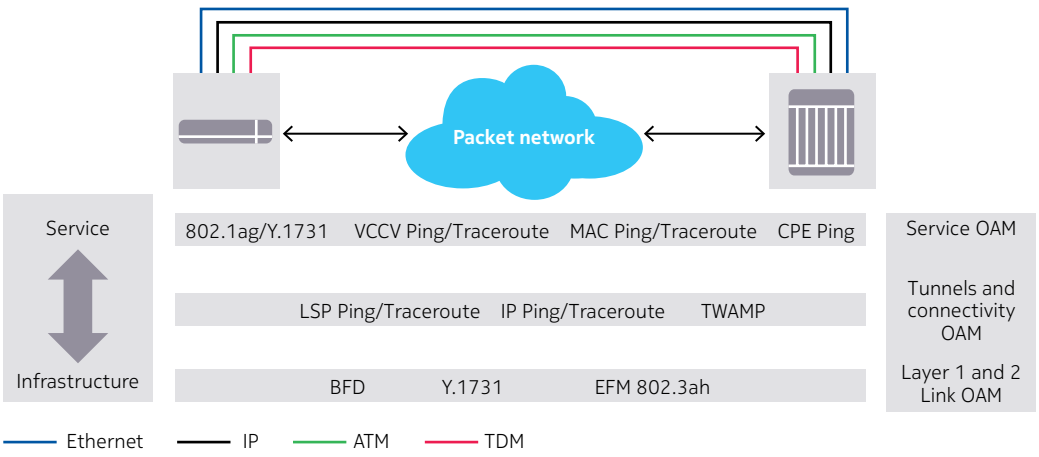


Comprehensive OAM capabilities

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

As shown in Figure 7, MPLS networks can expand beyond the Ethernet OAM tools to provide comprehensive OAM tools across multiple layers, such as Label Switched Path (LSP) ping and traceroute, 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 7. 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.

Inherent security protection

An MPLS network provides inherent security protection, with application traffic carried inside an LSP tunnel. This means if a hacker tries to inject illegitimate traffic from an end device attached to an MPLS edge router, that traffic would be discarded.

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, they can be mixed to form an end-to-end network with MPLS running seamlessly. This flexibility enables optimal use of all transmission assets. Network management and operation are also more efficient because microwave radio, Coarse Wavelength Division Multiplexing (CWDM) add/drop multiplexer and copper DSL modems are integrated in some MPLS platforms, simplifying network design and integration.

Compact, ruggedized outdoor platform

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

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 supports Layers 1, 2 and 3 VPNs, with all the previously described benefits of MPLS.

MPLS Layer 1 VPN (TDM pseudowire)

However, the support of Layer 1 VPNs for TDM traffic, with the same stringent delay, strict QoS and rapid switching protection performance, is essential because many legacy mission-critical applications still need to be supported. MPLS, with its range of capabilities, is in a unique position to address this challenge.

Some critical applications, such as SCADA, are point-to-multipoint, with the central master application 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 for 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.

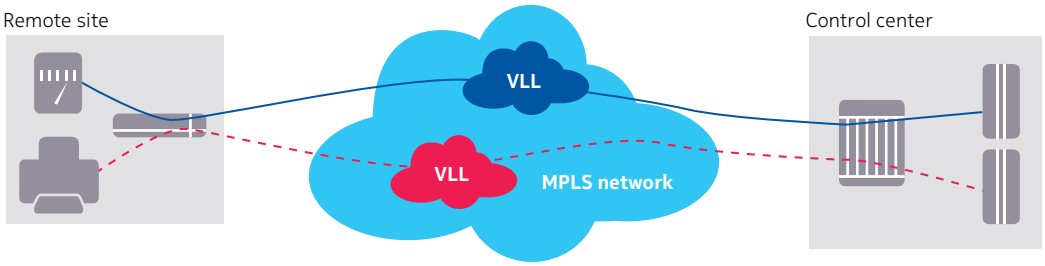
Layer 2 VPN - VLL

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 in the realm of 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 requirements. 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 8 shows two end-to-end VLLs that separately connect two end devices to a central site.

Figure 8. Layer 2 VPN – VLL

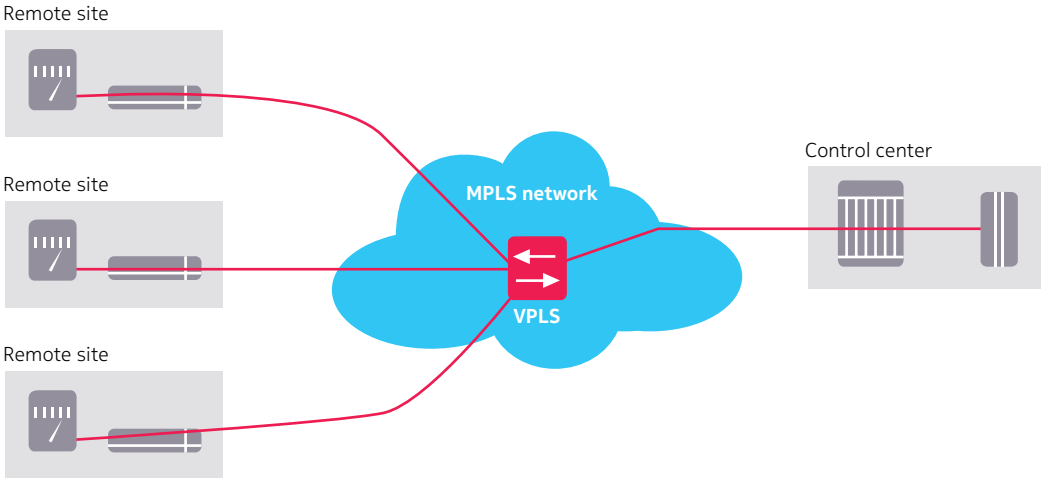


Layer 2 VPN - VPLS

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 9 shows a VPLS instance in a MPLS network, connecting four devices (three from remote sites and one from the control center) 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



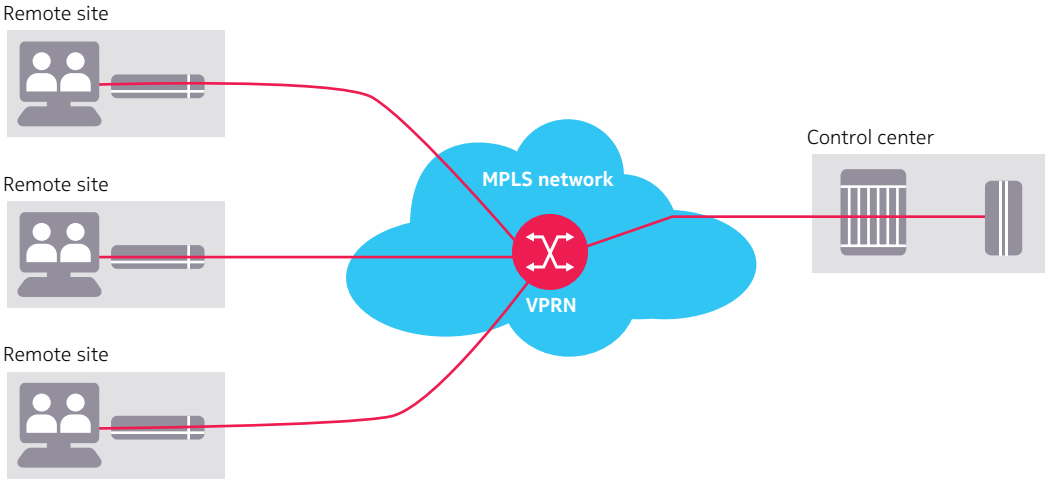
In a Layer 2 VPN - VPLS, forwarding decisions are based on the Ethernet MAC address. Each application or department can be assigned a dedicated VPLS or Layer 2 broadcast domain. MAC address duplications are therefore supported across domains because all VPLS instances are segregated.

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 transparent 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, for example.

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 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)

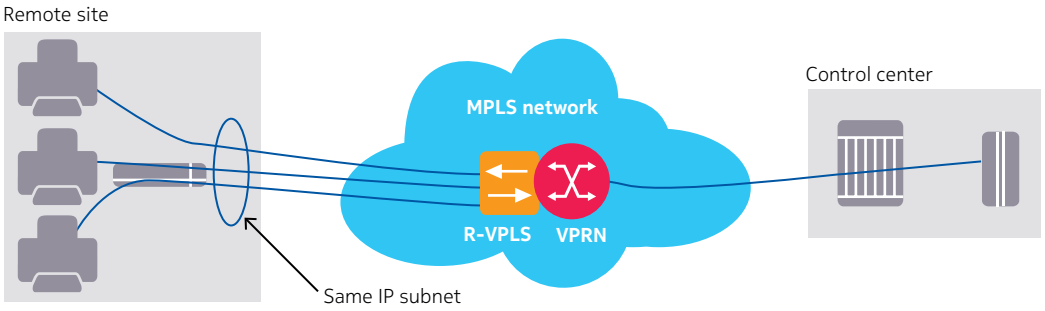


A Layer 3 VPN is implemented only for IP traffic and provides multipoint-to-multipoint IP connectivity with forwarding decisions based on the IP address. IP packet forwarding decisions can optionally be policy-based for greater flexibility. Overlapping IP address schemes are supported because each Layer 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 11. This integration of a Layer 2 VPN into a Layer 3 VPN is also known as 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.

NOKIA

Service-aware management

An effective, powerful management platform is a key element of reliable, flexible, secure and scalable IP/MPLS-based networks. A service-aware management platform provides easy network configuration and inventory control; fast, effective fault isolation and resolution; traffic analysis and monitoring, and support for new applications.

Conclusion

Operators of mission-critical networks face immense daily challenges. They must keep current network applications running smoothly to support their organization's operations and applications while planning telecommunications and applications technology transformations to reap the full benefits of an IP/Ethernet-based world. Operators must determine how to use their resources to extend their networks to the edge, where fiber is not always available, and how to manage networks that comprise nodes with different capacities.

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

The Nokia MPLS product portfolio ranges from terabit core systems to outdoor compact access form factors that share the same operating system base, 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 world-class MPLS platforms and comprehensive end-to-end MPLS managed solutions. Nokia IP/MPLS-based service routing and switching products offer operators of mission-critical networks the flexibility, scalability, security, 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
CPE	customer premises equipment
CWDM	Coarse Wavelength Division Multiplexing
DSL	Digital Subscriber Line
E-LAN	Ethernet LAN
E-Line	Ethernet Line
EFM	Ethernet in the First Mile
FRR	Fast Reroute
GOOSE	Generic Object Oriented Substation Event
HDLC	High-Level Data Link Control
IP-VPN	IP Virtual Private Network
LMR	land mobile radio
LSP	Label Switched Path
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: PR1605020294EN (July)