# Network modernization for power utilities

## Navigating the MPLS landscape

White paper

Power utilities are transforming their grid infrastructures to keep pace with escalating energy demands from new artificial intelligence data centers and the growing electrification movement. To succeed with this transformation, they need to modernize their mission-critical grid communications networks by replacing TDM technologies with packet-based networking. For most utilities, this means choosing between two converged technologies: MPLS-TP and IP/MPLS. But which one is the right choice for grids in transition?

This white paper aims to help power utilities understand and navigate the differences between MPLS-TP and IP/MPLS technologies. It explores the history, evolution and capabilities of each technology and compares their ability to address the demands of modern grids, support digitalization and automation, and provide lasting benefits to utilities and their customers. With the insights in this paper, utilities will have the information they need to choose choose the network technology that will best meet their evolving their evolving grid communications needs for the coming decades.

# Contents

1 Introduction 3

2 Understanding the technologies 4

2.1 IP/MPLS 4

2.2 MPLS-TP 5

3 Beyond perceived MPLS-TP advantages with IP/MPLS 7

3.1 Comparison between MPLS-TP and IP/MPLS technology values 7

3.2 IP/MPLS facilitates IP-based grid communications 12

3.3 Nokia elevates IP/MPLS performance and operations 14

4 MPLS technology convergence and divergence 16

5 Conclusion 18

Abbreviations 18

# 1 Introduction

Driven by gigawatts of new energy demand from artificial intelligence (AI) data centers and the widespread electrification of everything movement, power utilities are working to transform their grid infrastructure. At the heart of this effort is the fundamental need to modernize their mission-critical communications networks with packet networking technology. This paper is intended to help utilities understand the differences between IP/MPLS and MPLS-TP technologies so they can choose the best technology for addressing their evolving grid communications needs.

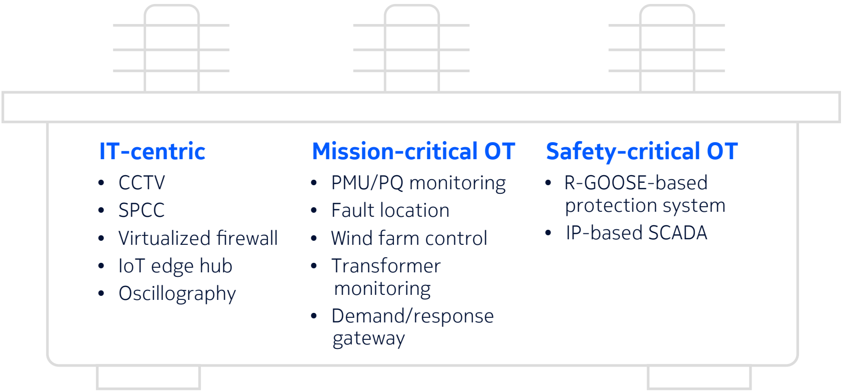
The telecommunications industry began to embrace Internet Protocol/Multiprotocol Label Switching (IP/MPLS) technology in the early 2000s as the demand for reliable, flexible and scalable network services intensified. IP/MPLS quickly became the standard communications technology for telecom service providers worldwide for layer 3 IP, layer 2 Ethernet and legacy layer 1 time-division multiplexing (TDM) transport solutions. It was subsequently deployed with great success in mission-critical networks for industrial organizations such as power utilities, railways, air traffic controllers, defense forces and public safety agencies.

As legacy Synchronous Digital Hierarchy/Synchronous Optical Network (SDH/SONET) and TDM equipment began to reach end-of-life in the late 2000s, the Internet Engineering Task Force (IETF) and the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) collaborated to distill the rich IP/MPLS technology to a transport-centric subset. This effort, in which experts from Alcatel-Lucent (now part of Nokia) played a foundational role as co-authors of the MPLS-TP framework,[1] focused on predictable network performance, traditional operations, administration and maintenance (OAM), and robust redundancy switching for point-to-point transport. This subset of capabilities is called Multiprotocol Label Switching – Transport Profile (MPLS-TP).

Utilities planning to modernize their SDH/SONET networks face a critical choice about which MPLS variant to adopt: IP/MPLS or MPLS-TP. Given that the new network will be deployed for a lifespan of a decade or longer, it is essential for utilities to have the technical information they need to evaluate the two variants and make the best decision.

Beyond assessing both MPLS variants on their protocol capabilities in the context of near-term goals, utilities must also thoroughly consider the ultimate goal of modernization: transitioning from TDM to full packet domains. This complete packetization, as outlined in IEC 61850-90-12:2020, is crucial for future fully digitalized and automated grid operations, where all substation operational technology (OT) and associated IT applications are IP-based (Figure 1) and legacy OT systems are eventually retired.

Figure 1. Digital substations with a plethora of IP-based applications



[1] Experts from the former Alcatel-Lucent (now part of Nokia) were instrumental in the IETF standardization work of MPLS-TP. For example, they co-authored foundational RFCs such as RFC 5921 (A Framework for MPLS in Transport Networks) and RFC 5860 (Requirements for OAM in MPLS-TP Networks).

Making the choice between IP/MPLS and MPLS-TP, therefore, is not merely about addressing current operational needs. It's also about building the foundational network for this entirely IP-based, automated future. Drawing upon the extensive experience of Alcatel-Lucent (now Nokia), which actively contributed to the standardization and development of both MPLS variants, the following sections offer a detailed examination of each technology to inform that strategic choice.

# 2 Understanding the technologies

## 2.1 IP/MPLS

IP/MPLS networks were originally intended to provide generic line-rate IP forwarding for high application performance. Because of its protocol design, IP/MPLS was quickly expanded with new capabilities, including multiservice network segmentation (supporting circuit emulation, LAN and IP services), deterministic quality of service (QoS), strong redundancy protection and robust traffic engineering. It was also enhanced with many restoration schemes designed to provide rapid switchover to pre-established or pre-engineered backup paths. IP/MPLS can also scale effectively, which allows it to accommodate deployments ranging from vast networks of tens of thousands of nodes to localized networks of just tens of nodes.

Equipped with these comprehensive and flexible capabilities, IP/MPLS quickly became the technology of choice for multiservice, or converged, networks. These capabilities make it ideally suited to provide IP, Ethernet, legacy TDM transport and multicast connectivity. With its full service awareness, IP/MPLS supports a diverse mix of applications with diverse QoS requirements, ranging from hitless packet loss to best-effort transport. Furthermore, its protocol versatility allows it to operate seamlessly over a wide range of transport technologies, including LTE, 5G, satellite, dense wavelength-division multiplexing (DWDM) photonic and microwave links.

MPLS leverages routing protocols such as Intermediate System to Intermediate System (IS–IS) and Open Shortest Path First (OSFP) to dynamically discover network topology and link state information. Once it discovers this information, the signaling protocol establishes end-to-end communication paths called label-switched paths (LSPs). These LSPs enable high-performance forwarding by directing traffic based on labels rather than IP addresses. There are three standardized signaling protocols for setting up these LSPs:

1. **Label Distribution Protocol (LDP)** establishes LSPs dynamically based on the underlying IP routing. It provides a straightforward way to forward traffic along the shortest paths derived from the routing protocol.
2. **Resource Reservation Protocol – Traffic Engineering (RSVP-TE)** offers precise control over the route taken by the traffic independent of the IP routing path, as with LDP. This capability, known as traffic engineering, allows LSPs to be established using explicit paths calculated based on constraints either automatically by routers or a centralized path computation element (PCE), or manually specified offline. The constraints range from bandwidth to link attributes and path diversity. This allows IP/MPLS to offer transport capabilities equivalent to those of SDH/SONET. RSVP-TE capabilities support a primary path with Fast Reroute (FRR) backup, and one or more secondary paths. A secondary path can be configured as a standby. Multiple computation methods are available for the LSPs.
3. **Segment Routing** represents a recent evolution of the IP/MPLS control plane. SR-MPLS establishes LSPs in a way similar to RSVP-TE but streamlines the control plane by embedding a label distribution function within the routing protocol (e.g., IS–IS). Like RSVP-TE, SR-MPLS with SR-TE policies streamlines traffic engineering by eliminating the RSVP signaling mechanism, ensuring that network paths are predictable, symmetrical and easy to manage.

Table 1. Comparing LDP, RSVP-TE and SR-TE

| Protocol/characteristic | LDP | RSVP-TE | SR-TE |
|---|---|---|---|
| Operation | Shortest-path forwarding. | Explicit or constraint-based LSPs with traffic engineering. | Explicit or constraint-based paths with traffic engineering. |
| Control plane protocol | A separate protocol (LDP) runs alongside the Interior Gateway Protocol (IGP). | A separate signaling protocol (RSVP-TE) runs alongside the IGP (with TE extensions). | Integrated into existing IGPs (OSPF, IS–IS) and Border Gateway Protocol (BGP). No separate signaling protocol needed. |
| Traffic engineering capabilities | Limited to IGP's shortest path. No explicit path control or resource reservation. | Strong traffic engineering capabilities, including bandwidth reservation, explicit path routing (strict/loose) and administrative group constraints. | Excellent traffic engineering capabilities, allowing for highly flexible and programmable paths, including latency, bandwidth and path avoidance constraints. |
| FRR | Basic FRR mechanisms (e.g., LDP PIC) for limited link/node protection. | Comprehensive FRR support (e.g., facility backup, one-to-one backup) for protecting LSPs within 50 ms. | Robust FRR mechanisms (e.g., Topology-independent Loop-free Alternates (TI-LFA)) for rapid protection within 50 ms. |
| Multicast | mLDP | P2MP RSVP | BIER, SR P2MP |

The evolution of segment routing into Segment Routing IPv6 (SRv6) is attracting attention from large-scale telecommunication service providers. SRv6 significantly reduces control plane protocol overhead and inherently supports static traffic engineering. It is well-suited for ultra-large-scale networks that require advanced capabilities such as service chaining and autonomous operations.

Despite these significant advantages, SRv6 has some limitations for grid communications. Notably, it currently lacks native support for TDM circuit emulation services and provides only limited multicast support—both of which are essential for grid applications. Furthermore, transporting IPv4 traffic over IPv6 encapsulation adds burdens because of the need for an IPv6 address plan and new network operations paradigm. It would take more standard development and IPv6 readiness from utilities before SRv6 could be seriously considered as a viable option for grid communications.

It is worth noting that evolution to SRv6 is not mandatory. Utilities are already deploying Segment Routing to support applications such as current differential protection.

## 2.2 MPLS-TP

Based on IP/MPLS, IETF and ITU-T collaborated to standardize a new transport profile (TP) for the MPLS technology. This joint effort aimed to form the foundation for a next-generation packet transport network. The fundamental idea of this activity was to bring OAM tools commonly used in existing SONET/SDH networks to MPLS. The network would also operate with dynamic signaling and IP routing planes.

As defined in RFC5921, which was co-authored by Alcatel-Lucent (now Nokia) and a few other organizations, MPLS-TP allows the use of MPLS in a transport network, much like traditional transport technologies. This enables MPLS to deliver packet transport services with comparable predictability, reliability and OAM capabilities based on ITU-T Y.1731 or Bidirectional Fault Detection (BFD). Specifically, MPLS-TP defines a subset of MPLS protocols for layer 1 and layer 2 services only. It is important to note that when layer 3 IP services are needed, a separate standalone router is required. Moreover, MPLS-TP provides the option to use a dynamic control plane to make the deployment of MPLS-TP more operationally efficient.

The development of MPLS-TP was driven by several factors. There was a growing demand for legacy transport networks to accommodate packet-based services, which triggered an evolution of SDH/SONET towards MPLS-like behavior. This evolution was accelerated as SDH/SONET equipment increasingly reached end-of-life, which created a pressing need for a modern, packet-centric replacement. Some within the SDH/SONET community perceived IP-based networks as overly complex, leading to a preference for maintaining a distinct IP network domain.

Proponents of MPLS-TP often highlight several key advantages to position it as a suitable technology for grid communications:

- Familiar operational paradigm: MPLS-TP leverages a paradigm akin to traditional SDH/SONET networks, emphasizing a static, manually provisioned connectivity model, without the use of the signaling plane. This approach appeals to organizations accustomed to the deterministic nature and established procedures of TDM-based connections, which leads to a perception that MPLS-TP networks are simple to operate. It is also believed that only static paths can achieve ultra-fast (<50 ms) recovery.
- Robust OAM and strong redundancy: MPLS-TP offers high-performance OAM and protection mechanisms for rapid fault detection and restoration. These capabilities aim to achieve stringent sub-50 ms protection switching times comparable to those provided by SDH/SONET networks—crucial for grid communications.
- Graceful legacy traffic migration: MPLS-TP is considered ideal for migrating traffic from legacy TDM-based systems such as protection relays and SCADA remote terminal units (RTUs).
- Bidirectional paths: LSPs reduce the risk of path mismatch between the forward and return paths. This simplifies fault localization and ensures consistent performance, including delay symmetry.
- Enhanced network security: It is often argued that MPLS-TP has a stronger security posture since it reduces the attack surface associated with control plane protocols.
- Lower total cost of ownership (TCO): There is a market perception that MPLS-TP offers a lower TCO. This is primarily attributed to simplified operations in environments familiar with static provisioning, as well as lower hardware costs compared to feature-rich IP/MPLS routers.
- Network evolution support: MPLS-TP aims to facilitate network modernization by simultaneously offering layer 2 packet networking for new grid applications while maintaining support for existing TDM circuits through TDM pseudowires.

It is crucial to assess these perceived advantages in perspective, especially when comparing MPLS-TP to IP/MPLS and evaluating its applicability for grid applications that require connectivity beyond simple point-to-point circuits. The following section provides this comparative analysis.

# 3 Beyond perceived MPLS-TP advantages with IP/MPLS

This section explores the perceived MPLS-TP advantages outlined previously and compares them with those offered by IP/MPLS. It describes how IP/MPLS approaches these areas and where it might offer enhanced benefits in the context of legacy TDM circuit communications and IEC 61850 packet-based communications.

## 3.1 Comparison between MPLS-TP and IP/MPLS technology values

### 3.1.1 Familiar operational paradigm

Highly reliant on manual provisioning, MPLS-TP is often presented as adopting a familiar operational paradigm for those accustomed to SDH/SONET networks. For safety-critical applications such as current differential protection, utilities have highly stringent communication requirements, including deterministic control over the communication paths that connect protective relays. In this context, MPLS-TP's reliance on manually calculated, static, explicit paths is a natural and suitable fit. This approach aligns with the traditional operational paradigm of transport networks, where direct, granular control over every connection is paramount.

Conversely, IP/MPLS can provide identical, if not superior, control over communication paths by utilizing RSVP-TE or SR-TE. TE policies allow utilities to define paths with extreme precision, either as an explicit strict route (specifying every hop) or an explicit loose route (specifying only a subset of intermediate nodes). With static or manual LSP provisioning, dynamic routing protocols are not utilized, and network failures do not rely on the convergence time required to propagate information across the network. As soon as a failure is detected, traffic is switched to a pre-engineered path. This minimizes packet loss if such protection is required (e.g., for SCADA traffic). LSP switchover capabilities can be disabled for differential protection traffic to avoid delay asymmetry. (Redundancy protection can still be provided at the pseudowire layer, as discussed in section 3.1.4.) Hence, IP/MPLS can fully meet the deterministic path requirements of critical applications.

### 3.1.2 Bidirectional transport of data in LSP

In MPLS-TP networks, a bidirectional LSP comprises a pair of route-symmetric (or co-routed in IETF terminology) unidirectional LSPs, one in the forward direction and one in the reverse direction. While route symmetry is not a strict requirement for most grid applications (e.g., SCADA, synchrophasor and other IEC 61850 applications), it remains a key requirement for legacy line differential protection systems. These older systems often rely on a ping-pong mechanism to precisely establish network delay, a key parameter in the relay protection logic that requires path symmetry, which is crucial for accurate operation.

In IP/MPLS networks, the two unidirectional LSPs can follow either symmetrical or asymmetrical routes in the forward and reverse directions, leveraging the flexibility of dynamic routing. This behavior is intentional by design because not all applications generate equal traffic in both directions—CCTV surveillance backup systems being a prime example. As a result, some links may be heavily utilized while others remain underused. Unidirectional LSP paths offer a solution by distributing traffic across the less-utilized links, thereby ensuring more effective traffic balancing. This approach helps extend the need for capacity upgrades by optimizing existing link utilization. IP/MPLS can also guarantee the LSP path symmetry required for legacy line differential protection systems. Routing policy will enforce this requirement and make sure the symmetry is there in the primary path and the redundant paths.

To meet these needs, IP/MPLS leverages advanced traffic engineering capabilities that provide precise control over LSP routes. With RSVP-TE and SR-TE, utilities can define and enforce the paths to ensure path symmetry.

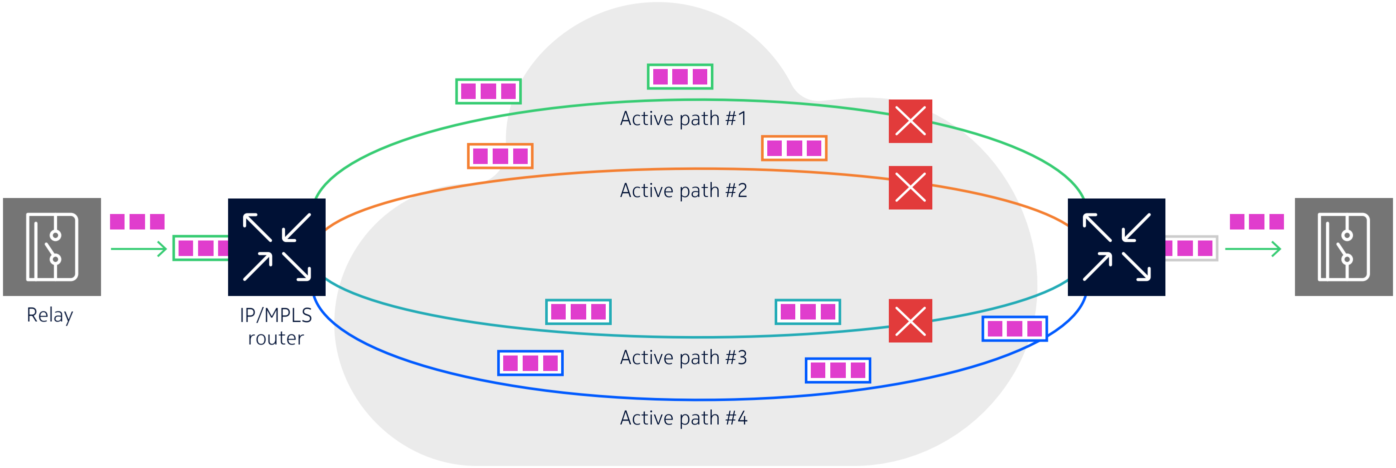
### 3.1.3 Strong redundancy

Grid communications networks need resiliency to withstand network failures. MPLS-TP protection schemes are directly modeled on SDH/SONET and support linear protection (1+1/1:1) and shared protection (1:N). These mechanisms are designed to achieve rapid switching times, typically within 50 ms, and ensure quick recovery from single-point failures in a highly deterministic manner. IP/MPLS, through FRR and primary/secondary LSPs, can also provide this stringent 50 ms level of redundancy.

Beyond traditional single-fault protection, IP/MPLS offers enhanced multi-fault resiliency, a capability that is becoming increasingly important as power grids experience more frequent and severe weather events. Faults can occur at the electrical layer and in the underlying communication network. IP/MPLS's ability to provide multi-fault resiliency stems from the inherent power of its dynamic IP routing.

When multiple network faults occur, IP/MPLS routers can use real-time IP routing information regarding the status of the link to find a path that can reach the destination, provided there is sufficient path diversity within the topology. In the case of differential protection traffic where a deterministic static route is mandatory, an active multipath pseudowire (AMP) mechanism together with RSVP-TE or SR-TE can offer up to four active, diverse paths to protect differential relay communications without any data loss when multiple network faults occur. For example, if faults affect three of the four paths, as shown in Figure 2, the surviving one continues to transport the data to the destination relay with zero recovery time.

Figure 2. AMP uses diverse active paths to ensure zero-time recovery for differential protection

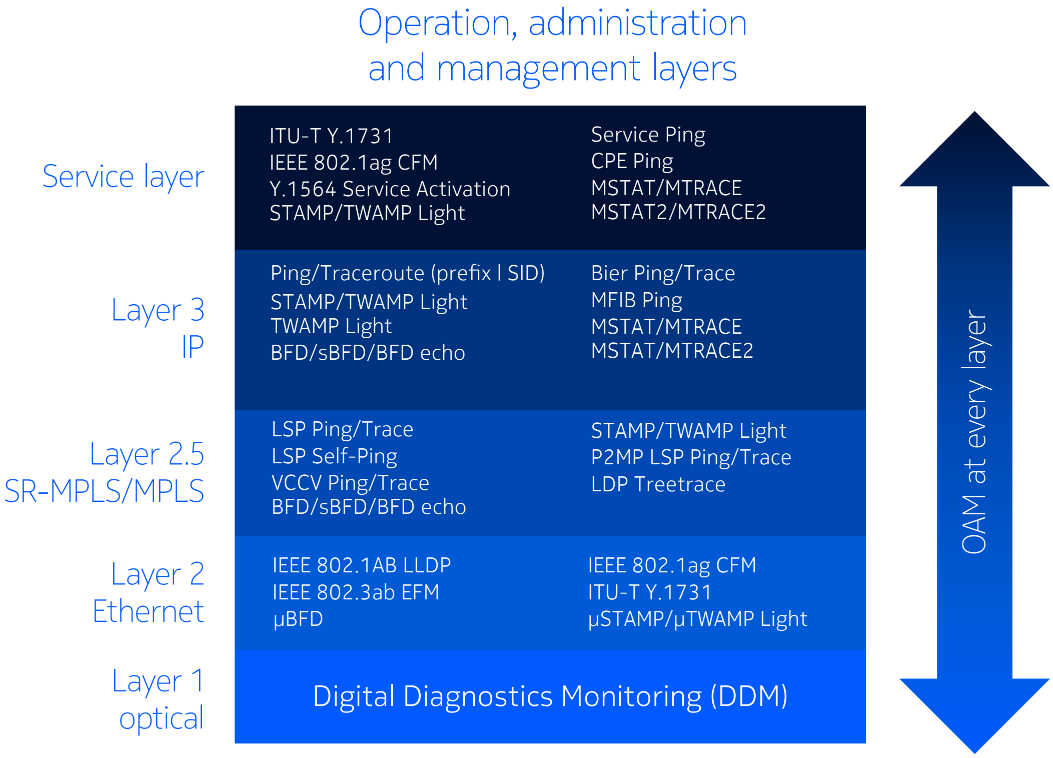


### 3.1.4 Robust OAM

OAM is foundational to ensuring high network reliability and intrinsically linked to achieving strong redundancy. Both MPLS-TP and IP/MPLS provide a suite of robust OAM tools for monitoring LSPs and pseudowires. These include essential functions such as echo request/echo reply (LSP ping) for connectivity verification, connectivity checks and fault detection. To attain recovery speed comparable to SDH/SONET, both technologies can harness a highly efficient fault detection mechanism called BFD. BFD can be configured to transmit messages at intervals as low as 10 ms with a multiplier of 3, resulting in 30 ms detection time.

Because of its service-oriented nature, IP/MPLS can additionally provide a rich set of OAM tools for multipoint virtual private line service (VPLS), unicast and multicast virtual private network (VPN) services to support emerging grid applications (Figure 3). These tools are tailored for multipoint environments and are invaluable for troubleshooting and performance assurance in meshed or multipoint networking environments for many emerging grid applications.

Figure 3. IP/MPLS OAM stack



Operation, administration and management layers

| Service layer | ITU-T Y.1731<br>IEEE 802.1ag CFM<br>Y.1564 Service Activation<br>STAMP/TWAMP Light | Service Ping<br>CPE Ping<br>MSTAT/MTRACE<br>MSTAT2/MTRACE2 |
|---|---|---|
| Layer 3<br>IP | Ping/Traceroute (prefix I SID)<br>STAMP/TWAMP Light<br>TWAMP Light<br>BFD/sBFD/BFD echo | Bier Ping/Trace<br>MFIB Ping<br>MSTAT/MTRACE<br>MSTAT/MTRACE2 |
| Layer 2.5<br>SR-MPLS/MPLS | LSP Ping/Trace<br>LSP Self-Ping<br>VCCV Ping/Trace<br>BFD/sBFD/BFD echo | STAMP/TWAMP Light<br>P2MP LSP Ping/Trace<br>LDP Treetrace |
| Layer 2<br>Ethernet | IEEE 802.1AB LLDP<br>IEEE 802.3ab EFM<br>µBFD | IEEE 802.1ag CFM<br>ITU-T Y.1731<br>µSTAMP/µTWAMP Light |
| Layer 1<br>optical | Digital Diagnostics Monitoring (DDM) | |

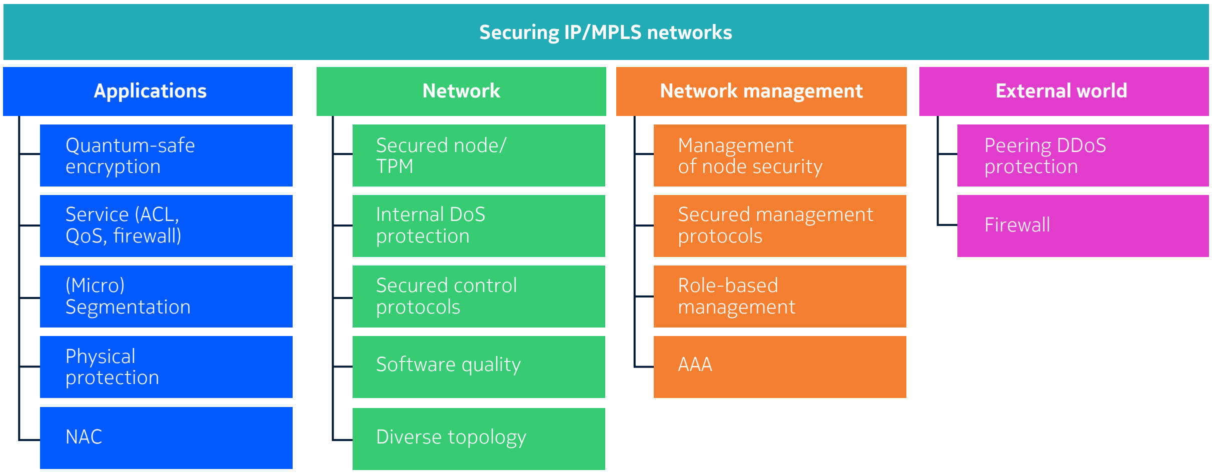
Furthermore, IP/MPLS leverages advanced streaming telemetry provided by the hardware and software components working together. This represents a more modern approach to network monitoring and management compared to traditional SNMP. It offers capabilities for all counters to provide real-time visibility into network performance and enable proactive monitoring and troubleshooting. This comprehensive scalability, combined with the router's ability to stream flow-level data and insights in near-real time, allows network operators to efficiently manage network growth, optimize performance, and respond quickly to changing traffic patterns and demands.

### 3.1.5 High level of security

A popular perception is that MPLS-TP offers superior security because it avoids IP routing. While it is true that the MPLS-TP data plane does not rely on dynamic IP routing as IP/MPLS does, it is crucial to recognize that the MPLS-TP management plane absolutely requires an IP-based data communications network (DCN). This DCN enables the central management system to connect all MPLS-TP nodes in the network to carry out critical management tasks, including configuration, monitoring and troubleshooting. Moreover, IP-based protocols such as Dynamic Host Configuration Protocol (DHCP) are commonly utilized for scenarios such as zero-touch auto-configuration during provisioning. This reliance on an IP-based DCN for management is not unique to MPLS-TP. It is, in fact, a long established best practice also employed in traditional SDH/SONET and TDM networks. Furthermore, modern applications—from SCADA communications using DNP3 and IEC 60870-4-104 to synchrophasor to Routable Generic Object-Oriented Substation Event (R-GOOSE)-based relays and Centralized Remedial Action Scheme (CRAS)—all employ IP-based communications.

Therefore, a realistic approach is not to avoid IP routing, but rather to focus on how to robustly protect it from cyber threats. Fortunately, the IP/MPLS ecosystem can benefit from a rich set of IP security tools and best practices developed over the past few decades to safeguard all IP-based grid communications (Figure 4). DNP3 and IEC-104, widely used for SCADA, are also native IP applications that can benefit from the increased level of security at L3. Examples include strong authentication and authorization in the management plane, encryption, network segmentation, access control lists (ACLs) and firewalls in the data plane and control plane. Utilities can leverage these tools to defend their networks, which serve as the first line of defense for the grid infrastructure.

Figure 4. Security tools and practices for IP/MPLS networks



What is often overlooked is that physical threats such as cable cutting and facility sabotage also represent significant risks to network availability. IP/MPLS networks use dynamic IP routing protocols to continuously maintain the latest link state and reachability information. This real-time awareness allows IP/MPLS to rapidly adapt and reroute traffic around affected areas, maintaining service continuity even in the face of widespread physical damage.

Beyond protocol-level defenses, the underlying software of network nodes forms the backbone of network security. Leading IP/MPLS vendors adhere to rigorous security standards for in-house development, including the foundation of network operating systems and the use of a Trusted Platform Module (TPM). They also strive to obtain stringent third-party certifications (e.g., EAL-3 Common Criteria and FIPS 140-2).

Nokia also understands the evolving cybersecurity landscape and is committed to using innovation to proactively to secure the network. This is exemplified by its implementation of quantum-safe encryption capabilities with MACsec, ANYsec and IPsec, anticipating and mitigating future threats from quantum computing.

### 3.1.6 Support for IP-based applications

For unicast traffic, MPLS-TP supports various applications, including Ethernet and IP-based services, via E-LINE and E-LAN offerings over a layer 2 transport network. E-LINE enables point-to-point connectivity, while E-LAN provides multipoint-to-multipoint functionality.

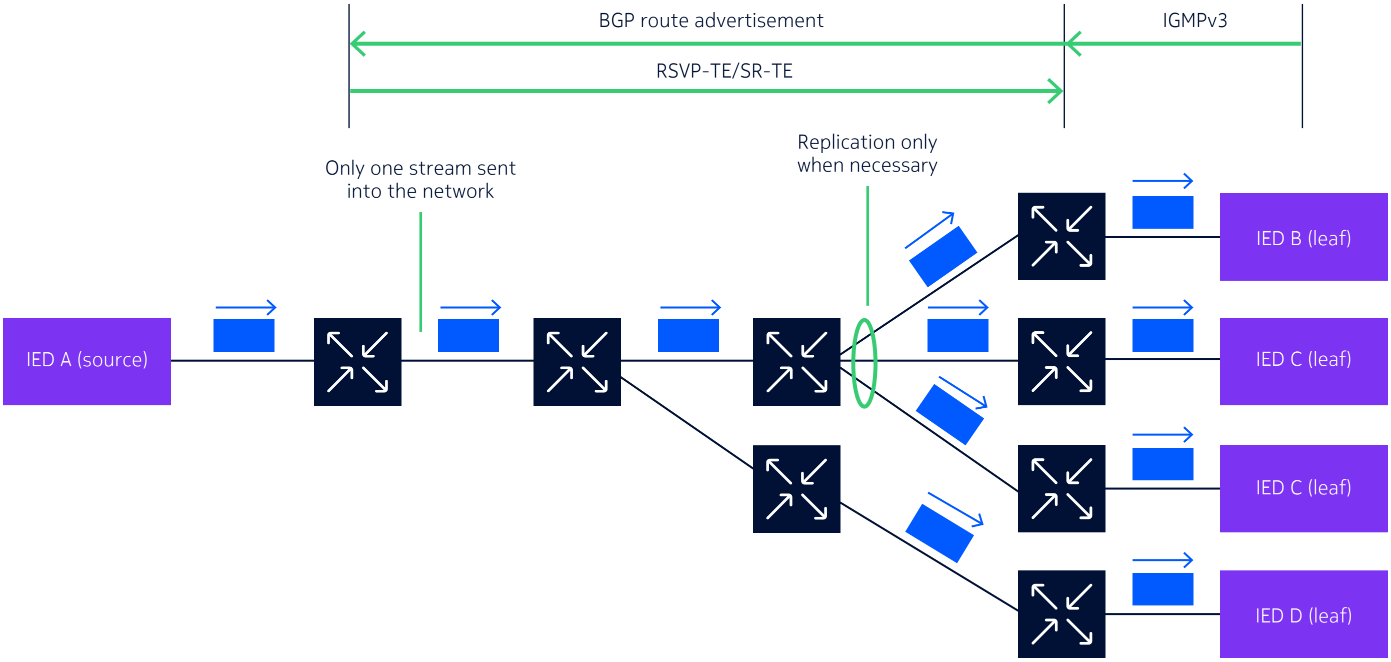
When application requirements extend beyond point-to-point connectivity, additional measures must be taken to maintain network stability. For example, Broadcast, Unknown Unicast and Multicast (BUM) traffic is flooded within an E-LAN service domain, making this solution suitable only for small-scale networks. As the industry transitions to IP-based IEC 61850 intelligent electronic devices (IEDs) and utility networks grow, the E-LAN model within MPLS-TP presents significant stability risks. A fault within the E-LAN domain can trigger cascading failures across all connected nodes within that domain. Additionally, provisioning becomes increasingly complex and demands segmentation for scalability, leading to substantial operational challenges. One notable example is to mitigate the risks of layer 2 loops.

IP/MPLS supports IP-based applications through layer 3 VPN (L3VPN) and Ethernet VPN and enables various types of connectivity, including point-to-point, point-to-multipoint and any-to-any. The IP-centric nature of L3VPN prevents BUM traffic from crossing the WAN, thereby reducing bandwidth usage and improving resource efficiency. With L3VPN and EVPN, there are no more concerns about scalability and reliability. These technologies also enable advanced features such as policy-based routing, QoS and traffic engineering at a much higher level compared to E-LAN.

For multicast traffic such as R-GOOSE, Routable Sampled Values (R-SV) and substation video surveillance applications, MPLS-TP supports IP multicast with a full mesh of LSPs. The edge MPLS-TP node replicates and floods the multicast stream to all LSPs. With Internet Group Management Protocol (IGMP) snooping, the flooding is reduced to all LSPs that have a remote MPLS-TP node with a multicast receiver (or "leaf" in multicast terminology).

With IP/MPLS, multicast streams are delivered over topology-optimized multicast trees, typically established as RSVP-TE point-to-multipoint (P2MP) LSPs, ensuring that traffic is replicated only where network topology absolutely requires it. Figure 5 shows a high-level sketch of this data delivery using IP multicast in an IP VPN. For a receiver IED (or leaf) to join a specific multicast stream from a particular IED source, it sends an IGMPv3 Join message for the known multicast IED source, prompting its connected IP/MPLS router to signal its interest and establish the necessary P2MP connectivity via the BGP and RSVP-TE protocols.

Figure 5. IP/MPLS multicast VPN establishes optimum P2MP multicast tree



As discussed in section 3.2.2, multicast VPN is particularly vital for power utilities that are increasing integration of renewables and complex multi-ended circuits because it provides the ideal P2MP IP connectivity for advanced grid applications.

### 3.1.7 Cost of ownership

The process of evaluating the cost of ownership for a technology encompasses the initial platform expenditure and the long-term total cost. Market adoption of MPLS-TP is steadily declining, with only a few small vendors continuing to implement the technology. Industry focus has shifted entirely toward newer solutions that match and surpass the capabilities of MPLS-TP. This shift explains why major telecom vendors are redirecting their investments away from MPLS-TP, and why chipset manufacturers are concentrating on technologies geared toward IPv4/IPv6 and advanced routing functionalities.

Vendors using merchant silicon for MPLS-TP implementations must often choose between two scenarios: Utilize a legacy chipset or pay a premium for high-end silicon with extensive features that largely go unused.

For utilities, IP/MPLS platforms offer the flexibility to support existing legacy interfaces while providing a clear migration path to scalable, reliable and feature-rich native IP solutions. The adoption of newer-generation merchant silicon is accelerating, delivering enhanced capabilities that are now handled directly in hardware. These advancements enable comprehensive intra-substation and inter-substation connectivity and form a truly converged IP/MPLS network. This unified network extends from field operations through distribution and transmission domains. It significantly reduces the need to rely on multiple technologies and specialized expertise across various operational areas.

## 3.2 IP/MPLS facilitates IP-based grid communications

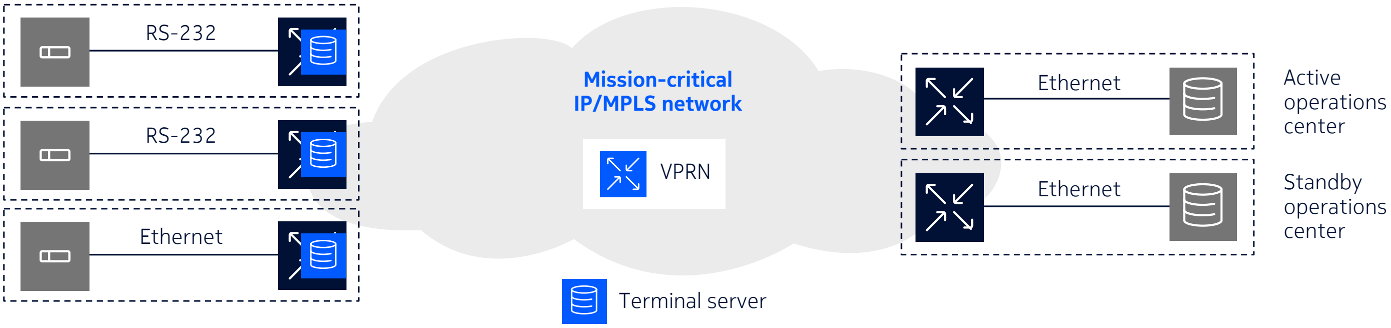
This section discusses how IP/MPLS can offer unique capabilities to support the communications requirements of new and emerging IP-based substation applications.

### 3.2.1 VPRN and raw socket facilitate interoperability of IP-based SCADA with legacy RTUs

Many utilities are refreshing their SCADA applications. They typically deploy new SCADA servers and RTUs with IP/Ethernet interfaces while retaining the use of legacy RTUs with serial interfaces. Therefore, the use of TDM pseudowire for circuit emulation would not suffice because the SCADA server no longer supports serial interfaces.

To tackle this challenge, IP/MPLS routers can incorporate a terminal server to perform raw socket mechanisms that convert legacy serial SCADA data to IP. Figure 6 shows a SCADA server with an IP/Ethernet interface and three RTUs. Two of these are legacy RTUs with serial interfaces and one has an IP/Ethernet interface. The built-in terminal server converts raw socket serial traffic from the two legacy RTUs into TCP/UDP sessions over IP packets and sends them to the server using a VPRN service provided by the IP/MPLS network. At the same time, the SCADA VPRN can also connect new RTUs with the server. This means the IP/MPLS VPRN can allow graceful migration of SCADA systems while retaining the use of legacy RTUs.

Figure 6. IP/MPLS supporting seamless communications for new and legacy RTUs



### 3.2.2 Multicast VPN optimizes R-GOOSE-based applications with P2MP LSPs

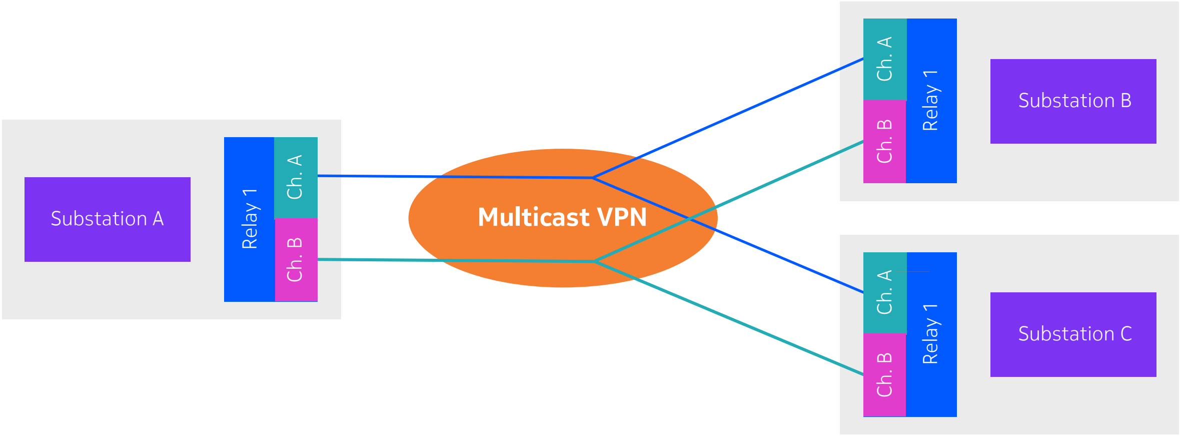
R-GOOSE, defined in IEC 61850-8-1:2011/A1:2020, is an extension of the Generic Object-Oriented Substation Event (GOOSE) protocol designed specifically for wide-area communication. Encapsulated in UDP/IP packets, R-GOOSE operates on a publish–subscribe model over multicast to establish efficient, P2MP IED communications.

In this scheme, there are redundant relays with redundant communication interfaces (A and B channels). Each channel in each relay would send R-GOOSE and R-SV traffic toward the corresponding channel in the other two relays over a topology-optimal P2MP LSP.

#### Multi-terminal line differential protection for multi-ended circuits

Driven by economics, efficiency and renewable integration, multi-terminal transmission lines are becoming increasingly prevalent. This, in turn, is driving the adoption of multi-terminal line differential protection systems that can detect and isolate faults in these complex topologies. Figure 7 shows a multicast VPN connecting relays in a three-terminal line differential scheme with redundant line protection systems.

Figure 7. Multicast VPN provides optimum P2MP connectivity to deliver data to multiple recipients



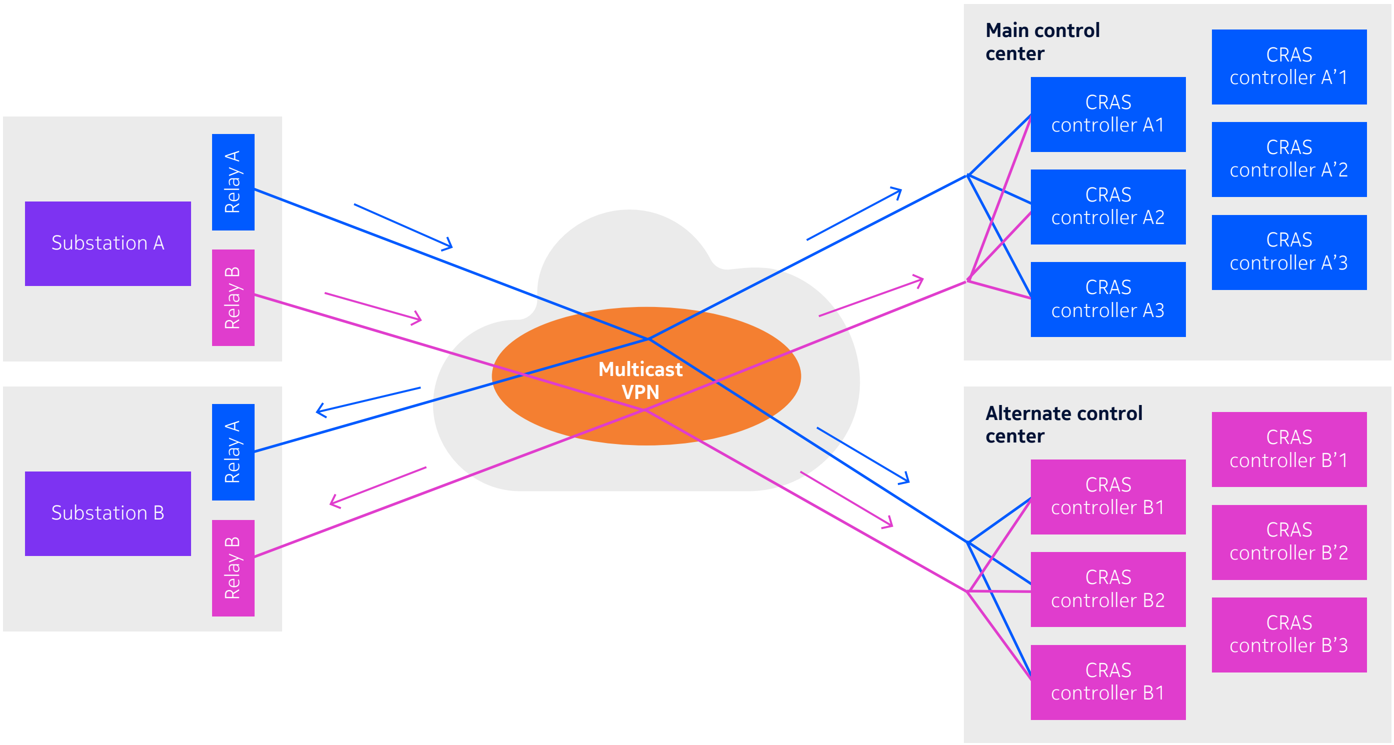
#### Centralized Remedial Action Scheme (CRAS)

CRAS is a wide-area protection and control system that proactively responds to severe grid disturbances. It aggregates real-time data to centrally determine and issue coordinated control actions (e.g., load shedding, generation tripping) to maintain grid stability. Given its highly critical nature, CRAS features the utmost redundancy through parallel A and B subsystems in geographically diverse control centers, with each subsystem having its own set of triple-redundant CRAS servers.

At the substation level, there are two sets of relays for each subsystem. Relays at the substations are either monitoring relays that report line data (e.g., line loading or trip status) to the RAS controllers of their corresponding subsystem as well as the other parallel subsystems, or other relays that subscribe to the information from the monitoring relays. When they detect anomalies, CRAS controllers command mitigating relays to perform remedial actions such as opening circuit breakers at substations or generating locations.

Multicast VPNs provision a dedicated P2MP LSP for each multicast source. In Figure 8, the blue and pink LSPs provide optimum multicast connectivity for Relay A and Relay B in Substation A, respectively. These relays publish real-time information to CRAS controllers in the main and alternative control centers, as well as other subscribing relays in Substation B.

Figure 8. Multicast VPN provides bandwidth-optimum P2MP connectivity for monitoring relay communications for the CRAS system



As the physical safety of substations has also become a top concern, utilities are deploying video surveillance systems in which tens of CCTV cameras multicast high-quality video streams to multiple headend systems to support real-time analytics, monitoring, storage and backup. Multicast VPN can also be used to provide scalable P2MP connectivity for all cameras across the grid.

## 3.3 Nokia elevates IP/MPLS performance and operations

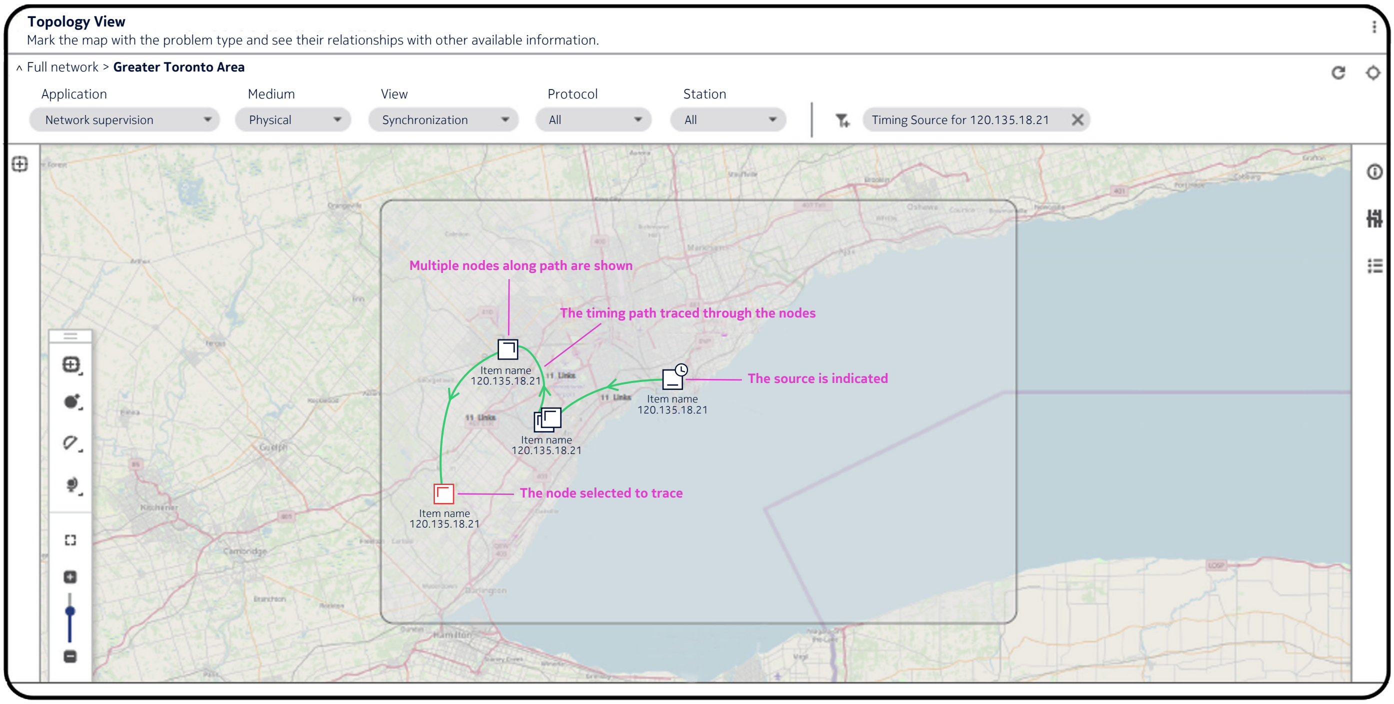
To ensure a comprehensive and fair comparison between MPLS-TP and IP/MPLS, utilities should extend their evaluation beyond basic standards. It's crucial to consider the significant enhancements and specific design implementations that leading vendors such as Nokia have brought to IP/MPLS. A prime example is the use of Nokia Network Services Platform Utilities (NSP Utilities), which enables utilities to extend operational and management capabilities beyond traditional boundaries. These advancements are a clear demonstration of a more mature technology ecosystem specifically tailored to meet the stringent demands of mission-critical power utility networks. Evaluating these real-world, vendor-specific refinements offers a more complete picture of IP/MPLS's capabilities and its suitability for evolving OT communication needs in the grid.

### 3.3.1 Synchronization management

With the growing adoption of IEC 61850 technologies such as GOOSE, synchrophasor and digital fault recording (DFR), accurate time synchronization has become critical. In addition to GNSS/GPS, utilities increasingly rely on IEEE 1588v2 to deliver timing through the WAN and substation buses to assets across the grid. In these implementations, communication nodes in the WAN and substation buses act as boundary clocks (BCs) in the overall synchronization network topology. With BCs in the path between the grandmaster clock and the slave clock, a long route spanning many hops is divided into multiple shorter segments. This segmentation enables better Packet Delay Variation (PDV) control and enhances TimeReceiver (TR) clock performance in IEDs compared to networks comprising of transparent clocks (TCs). BCs also offer more resilient synchronization distribution because each BC can peer with multiple upstream BCs. Additionally, BCs can perform interworking between a telecom profile domain and a power profile domain so that substations can receive timing from existing telecom core networks.

The complexity involved in managing this type of synchronization network presents a significant challenge. The traditional way to approach synchronization management is on a nodal basis. As the number of IEEE 1588 clocks grows, this approach cannot scale. NSP Utilities offers a novel network-based approach for managing synchronization and monitoring the peering relationships. Figure 9 illustrates the use case of tracing  synchronization distribution from a selected node to the source. It also plays an integral role in planning, what-if analysis and troubleshooting, significantly improving synchronization reliability.

Figure 9. NSP Synchronization Manager traces the synchronization distribution to a selected node



**Topology View**

Mark the map with the problem type and see their relationships with other available information.

^ Full network > **Greater Toronto Area**

Application: Network supervision

Medium: Physical

View: Synchronization

Protocol: All

Station: All

Timing Source for 120.135.18.21

Multiple nodes along path are shown

The timing path traced through the nodes

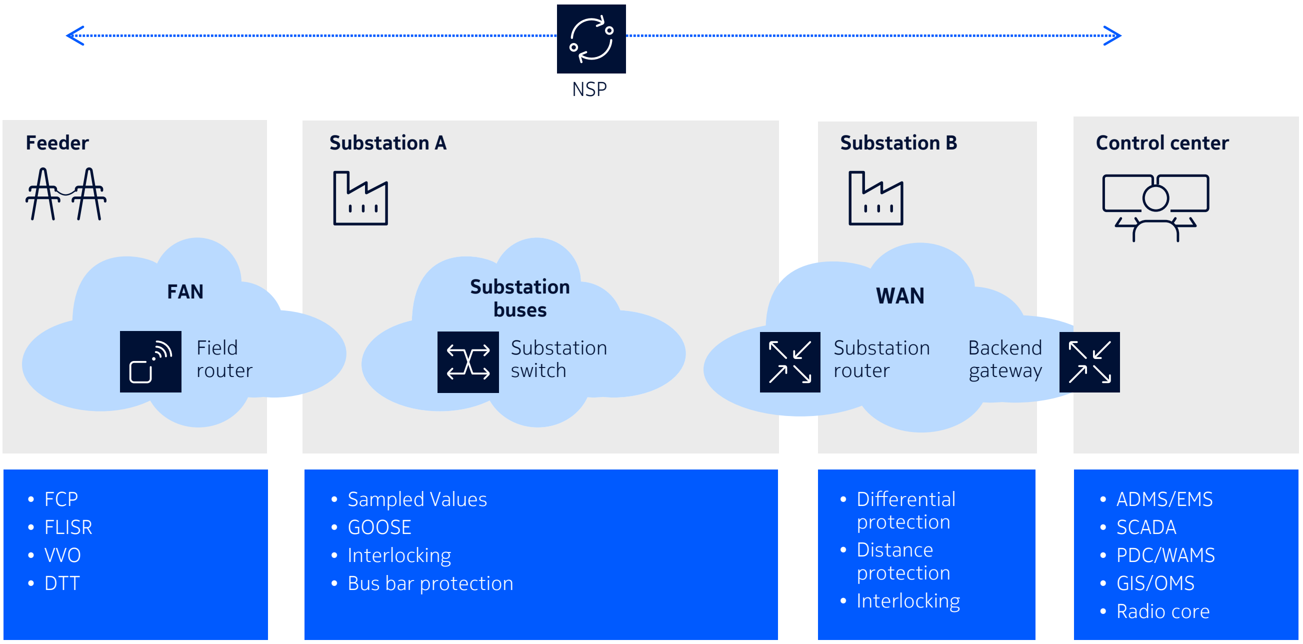
The source is indicated

The node selected to trace

## 3.3.2 Unified WAN/LAN/FAN networking

Substation LANs (or buses in IEC 61850 terminology) and field area networks (FANs) are critical enablers for grid automation aimed at improving the reliability, sustainability and quality of electricity. With a diverse suite of applications ranging from GOOSE and SV to fault location, isolation and recovery (FLISR) and falling conductor protection (FCP), a service-centric paradigm for LAN and FAN is necessary. Nokia NSP Utilities extends network service management from WAN to LAN to FAN as one unified manager. This approach significantly increases operational efficiency and elegance (Figure 10).

Figure 10. Nokia NSP is a unified manager for FAN, LAN and WAN



### 3.3.3 Cross-layer network management

Utility communications infrastructure is commonly built with microwave transmission and an optical DWDM core. Nokia NSP Utilities can significantly boost network management efficiency through cross-layer management, seamlessly integrating IP/MPLS with essential cross-layer coordination for the microwave link and optical DWDM layers.

# 4 MPLS technology convergence and divergence

Building on the preceding section, this section summarizes the key points of convergence and divergence between MPLS-TP and IP/MPLS technologies.

| Feature | IP/MPLS | MPLS-TP |
|---|---|---|
| Predictable, deterministic behavior | Yes | Yes |
| Unidirectional LSPs | Yes | Yes |
| Bidirectional connectivity | Yes by with two unidirectional LSPs | Yes with bidirectional LSPs comprising two unidirectional LSPs |
| Sub-50 ms failover | Yes | Yes |
| OAM | Yes | Yes |
| Simplified static management | No | Yes |
| Manual traffic engineering | Yes | Yes |
| Dynamic traffic engineering | Yes | Basic capabilities only |
| Comprehensive cybersecurity features—encryption, platform trust and zero-trust architecture | Yes | Yes |

| Feature | IP/MPLS | MPLS-TP |
|---|---|---|
| Advanced time and synchronization support—SyncE, PTP profile interworking | Vendor dependent | Vendor dependent |
| Comprehensive OAM capabilities at different OSI layers | Yes | Layer 2 only |
| Support for diverse application slicing technologies across multiple transport tunnels (LDP, RSVP, SR-MPLS, etc.) | Yes (circuit emulation, LAN and IP services) | Yes but without native IP services support |
| Native support for layer 3 multicast in R-GOOSE and R-SV protocols | Yes | Limited flexibility using point-to-point connections and packet broadcase and flooding techniques |
| Support for dual-stack (IPv4 and IPv6) applications and seamless service provisioning across FAN, LAN and WAN | Yes | No |
| Evolution path to Segment Routing and SDN | Yes | No |

While MPLS-TP supports IP-based communication through encapsulation over its layer 2 transport network, it is not IP aware. This fundamental limitation constrains its suitability for scenarios where the packet domain's scale and scope remain small. As new grid automation capabilities inexorably drive a significant expansion of the packet domain, MPLS-TP's layer 2-only networking capabilities will prove increasingly inadequate. It will struggle to scale efficiently and to natively provide essential advanced features such as IP multicast (Figure 11a).

In stark contrast, IP/MPLS, with its inherent and comprehensive IP routing capabilities, is not merely ideally positioned but represents the definitive architectural choice to facilitate the evolution to the the complete, future-ready packet domain envisioned in edition 2 of IEC 61850-90-12 (Figure 11b). This fundamental difference underscores why utilities must prioritize a long-term vision and select a network foundation that can truly meet the demands of tomorrow's fully digitalized grid.

Figure 11a. MPLS-TP evolution halts as packet domain growth exceeds layer 2 capabilities

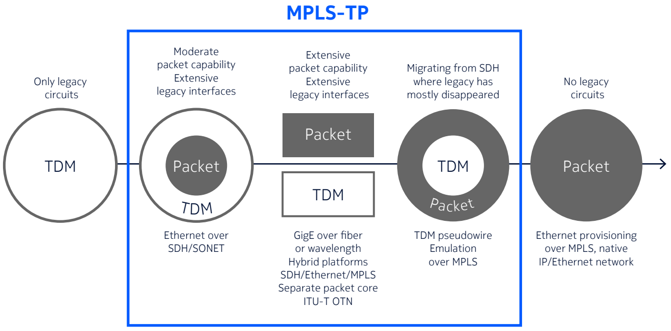
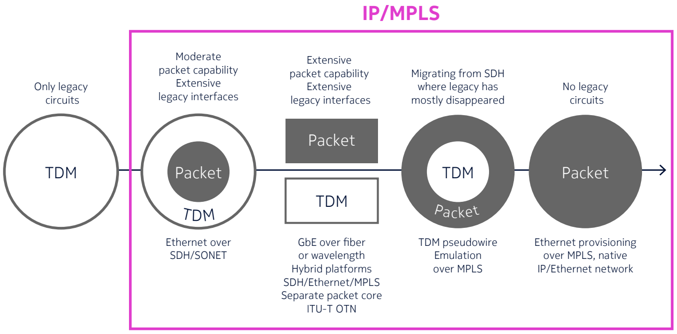

MPLS-TP
Only legacy circuits
TDM
Moderate packet capability Extensive legacy interfaces
Packet
TDM
Ethernet over SDH/SONET
Extensive packet capability Extensive legacy interfaces
Packet
TDM
GigE over fiber or wavelength Hybrid platforms SDH/Ethernet/MPLS Separate packet core ITU-T OTN
Migrating from SDH where legacy has mostly disappeared
TDM
Packet
TDM pseudowire Emulation over MPLS
No legacy circuits
Packet
Ethernet provisioning over MPLS, native IP/Ethernet network

Figure 11b. IP/MPLS enables seamless progression to the final, full-packet domain


IP/MPLS
Only legacy circuits
TDM
Moderate packet capability Extensive legacy interfaces
Packet
TDM
Ethernet over SDH/SONET
Extensive packet capability Extensive legacy interfaces
Packet
TDM
GbE over fiber or wavelength Hybrid platforms SDH/Ethernet/MPLS Separate packet core ITU-T OTN
Migrating from SDH where legacy has mostly disappeared
TDM
Packet
TDM pseudowire Emulation over MPLS
No legacy circuits
Packet
Ethernet provisioning over MPLS, native IP/Ethernet network

# 5 Conclusion

Choosing a next-generation packet technology for a utility network is a generational investment, not just a technical decision. Driven by growing energy demand from sources like AI data centers and electrification, utilities must carefully evaluate all factors, including current and future needs for grid automation, renewable energy integration and high-bandwidth communication. Selecting the right communication foundation today is paramount to ensuring the long-term efficiency, reliability and adaptability of the power grid.

This paper has provided a comprehensive assessment of MPLS-TP and IP/MPLS technologies, examining their respective capabilities in the context of supporting grid modernization. While MPLS-TP was initially designed to bring SONET/SDH-like reliability to packet networks to support IP communications, its static architecture, manual provisioning and non-native IP design ultimately limit its scalability and appeal for evolving grid applications that require future-proof communications networks. Consequently, it can serve only as an intermediate step in the TDM-to-packet transition, and will fall short of fully enabling future-proof networks for grid communications.

In contrast, IP/MPLS, with a full control plane encompassing IP routing and MPLS signaling, exceeds MPLS-TP in aspects such as reliability, OAM capabilities and traffic engineering. Furthermore, its robust support for advanced functionalities, including native IP multicast for critical applications such as multi-terminal line differential protection and CRAS, positions IP/MPLS as a more future-proof foundation. IP/MPLS also continues to evolve with ongoing efforts in segment routing which further enhances its strength. This IP-native, dynamic design makes IP/MPLS the strategically superior and more appealing technology for evolving grid infrastructure and embracing IEC 61850 grid automation.

Nokia, with its comprehensive network portfolio and rich experience in assisting over 300 utilities globally since the 1990s, definitively showcases the viability and benefits of leveraging IP/MPLS for these critical networks. To learn more about how Nokia can help you achieve your grid modernization goals, visit the Nokia Mission-critical WAN for Power Utilities web page.

# Abbreviations

| | |
|---|---|
| AAA | authentication, authorization and accounting |
| ACL | access control list |
| ADMS | Advanced Distribution Management System |
| AMP | active multipath pseudowire |
| BC | boundary clock |
| BFD | Bidirectional Fault Detection |
| BGP | Border Gateway Protocol |
| BIER | Bit Indexed Explicit Replication |
| BUM | Broadcast, Unknown Unicast and Multicast |
| CCTV | closed-circuit television |
| CRAS | Centralized Remedial Action Scheme |
| DCN | data communications network |
| DDoS | distributed denial of service |

| | |
|---|---|
| DFR | digital fault recording |
| DHCP | Dynamic Host Configuration Protocol |
| DNP3 | Distributed Network Protocol version 3 |
| DTT | Direct Transfer Trip |
| DWDM | dense wavelength-division multiplexing |
| EMS | energy management system |
| E-LAN | Ethernet LAN |
| E-LINE | Ethernet Line |
| EAL-3 | Evaluation Assurance Level 3 |
| FAN | field area network |
| FCP | falling conductor protection |
| FIPS | Federal Information Processing Standard |
| FLISR | fault location, isolation and restoration |
| FRR | Fast Reroute |
| GigE | Gigabit Ethernet |
| GIS | geographic information system |
| GNSS | Global Navigation Satellite System |
| GOOSE | Generic Object-Oriented Substation Event |
| GPS | Global Positioning System |
| IEC | International Electrotechnical Commission |
| IED | intelligent electronic device |
| IETF | Internet Engineering Task Force |
| IGMP | Internet Group Management Protocol |
| IGP | Interior Gateway Protocol |
| IP/MPLS | Internet Protocol/Multiprotocol Label Switching |
| IPv4 | Internet Protocol version 4 |
| IPv6 | Internet Protocol version 6 |
| IS-IS | Intermediate System to Intermediate System |
| IT | iinformation technology |
| ITU-T | International Telecommunication International Telecommunication Union Telecommunication Standardization Sector |
| L3VPN | layer 3 virtual private network |
| LAN | local area network |
| LDP | Label Distribution Protocol |
| LSP | label-switched path |

| | |
|---|---|
| LTE | Long Term Evolution |
| mLDP | multicast Label Distribution Protocol |
| MPLS-TP | Multiprotocol Label Switching - Transport Protocol |
| NAC | network access control |
| NMS | network management system |
| NSP | Network Services Platform |
| OAM | operations, administration and maintenance |
| OMS | outage management system |
| OSPF | Open Shortest Path First |
| OT | operational technology |
| P2MP | point to multipoint |
| P2MP RSVP | point to multipoint Resource Reservation Protocol |
| PCE | path computation element |
| PDC | phasor data concentrator |
| PDU | protocol data unit |
| PDV | Packet Delay Variation |
| PIC | Prefix-Independent Convergence |
| PQ | power quality |
| QoS | quality of service |
| R-GOOSE | Routable Generic Object-Oriented Substation Event |
| R-SV | Routable Sampled Values |
| RAS | Remedial Action Scheme |
| RSVP-TE | Resource Reservation Protocol - Traffic Engineering |
| RTU | remote terminal unit |
| SCADA | Supervisory Control and Data Acquisition |
| SDH | Synchronous Digital Hierarchy |
| SONET | Synchronous Optical Network |
| SPCC | spill prevention, control and countermeasure |
| SR P2MP | Service Routing point to multipoint |
| SR-MPLS | Service Routing - Multiprotocol Label Switching |
| SR-TE | Service Routing - Traffic Engineering |
| SRv6 | Segment Routing IPv6 |
| TC | transparent clock |
| TCO | total cost of ownership |

| | |
|---|---|
| TDM | time-division multiplexing |
| TE | traffic engineering |
| TI-LFA | Topology-independent Loop-free Alternate |
| TP | transport profile |
| TPM | Trusted Platform Module |
| TR | TimeReceiver |
| UDP | User Datagram Protocol |
| VPLS | virtual private line system |
| VPN | virtual private network |
| VPRN | virtual private routed network |
| VVO | voltage/VAR optimization |
| WAMS | Wide Area Monitoring System |
| WAN | wide area network |

**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: 1557554 (August) CID215017