NOKIA

Deploying IP/MPLS Communications Networks for Smart Grids

Network transformation to reliable, secure end-to-end packet-based infrastructures

Application Note

Abstract

Power utilities worldwide are embarking on Smart Grid projects such as Grid Modernization, Substation Automation, Distribution Automation, and Advanced Metering Infrastructure. Communications network transformation to a highly available IP/MPLS network for mission-critical communications is a foundation to the Smart Grid architecture. Nokia delivers a proven converged IP/MPLS communications network for power utilities using new generation products and management tools. Nokia IP/MPLS products support network resiliency, quality of service, virtualization, security, and convergence as well as a management platform that integrates with utility operations to automate and simplify operations management. Reliable communications and end-to-end service consistency from the core network to the field area network is essential to meeting the key Smart Grid application requirements of utilizing information management technologies and two-way communications.

NOKIA

Contents

Introduction

The implementation of a Smart Grid means different things to each system provider or customer. However, at any level of the grid system a smarter communications network is part of the new energy delivery strategy of many power utilities around the world. New Smart Grid applications provide utilities with better visibility to operate the bulk electric systems more efficiently. The increased movement of data with analysis provides the benefits of reduced operating costs, increased power quality, and improved outage response. Governments consider Smart Grid technologies as a means to better power quality, reduced need for additional generation capacity, and reduced carbon emissions. Business and residential customers can take advantage of new features such as time-of-day charging and the increased participation from independent power producers. Finally, regulators even view smarter communications networks as a means to more efficient energy markets and continued safe and reliable energy delivery.

The Smart Grid architecture includes many applications such as transmission substation automation, distribution automation, demand response, distributed generation, and advanced metering infrastructure. These applications require incorporating information management technologies and extending control and monitoring throughout the wider transmission and distribution networks as well as new renewable power generation sources.

A key enabler for the safe and efficient transformation of a power utility network is a modern, reliable, and flexible communications infrastructure that can route increasing amounts of monitoring, control and status information effectively, efficiently and on time. To effectively support Smart Grid applications, it is acknowledged that Internet Protocol (IP)-based networks will serve as a key element for the Smart Grid information networks. For transmission operators who have been maintaining communications infrastructures, this requires them to consider an evolution of their communications infrastructures that would be very different from their traditional time division multiplexing (TDM) over Synchronous Digital Hierarchy (SDH) or Synchronous Optical Network (SONET)-centric networks. Distribution operators, who in the past have only needed minimal communications coverage in most of their medium and low voltage service territories, now face the challenge of extending and deploying new communications infrastructures for distribution automation plus supporting non-traditional micro-generation elements that could unbalance the electrical load.

A flexible transformation is required to preserve existing investments and to minimize risks. The Nokia IP/Multi-protocol Label Switching (MPLS) communications network incorporates state-of the-art technologies to enable a power utility to deploy a future-proof, highly available IP network to continue supporting existing TDM and legacy applications while providing a smooth migration path to IP, Ethernet and IP/MPLS services. This new IP/MPLS network will allow the utility to maximize the cost effectiveness and efficiency of its network without jeopardizing reliability, as well as enabling the deployment of new devices and applications that can improve operational and workflow efficiency. A highly available IP/MPLS network is ideally suited to support both mission-critical operations and all other corporate communications requirements.

In addition, the Nokia network and service management platform allows power utilities to improve their efficiency by integrating their utility operations to automate and simplify operations management for communications services, thus reducing the barrier of introducing IP/MPLS technologies and services.

This application note illustrates the advantage of using IP/MPLS from the core to the field area network (FAN) while leveraging various technologies where appropriate such as microwave transport, wavelength division multiplexing (WDM) transport, and high-speed Ethernet transport from 1 Gigabit (Gb) to 10 Gb and 100 Gb, all within an integrated end-to-end communications infrastructure.

The traditional utility communications network

Utility communications networks are traditionally built to carry information between the utility control center and all remote sites — information that is used to manage capacity, to monitor and control the system, to bill customers and to provide staff communications. Traffic is typically carried over TDM circuits like T1/E1, RS-232, X.21, and E&M.

Bandwidth and quality of service

Transmission operators typically have deployed SDH or SONET networks. These TDM networks support high reliability using mechanisms such as unidirectional path-switched ring (UPSR), which allows a utility communications network to switch over from a failure in less than 50 milliseconds.

With SDH/SONET, the circuits are established in a static configuration. This approach is deployed in many utility communications networks today, but it means that the bandwidth is reserved for a particular circuit, whether it is used or not. Consequently, one application may have insufficient bandwidth while bandwidth that is reserved for an inactive application sits idle. As such, this approach is not optimized to support IP and Ethernet-centric communications required for new Smart Grid applications.

Because each circuit in a traditional TDM implementation is set with predefined bandwidth, quality of service (QoS) is inherent in the system; after the circuit is established, an application can only utilize the bandwidth assigned to it. When new packet-based services are being integrated over a common SDH/SONET infrastructure, the network is not able to effectively discriminate between high-priority mission-critical traffic and lower priority traffic, or enforce upper bounds on delay and jitter across the network.

CAPEX/OPEX and scalability

In a SDH/SONET setting, the granularity of the bandwidth tends to be in the order of 1.5 Mb/s or 2 Mb/s increment, respectively. As IP applications converge over SDH/SONET networks, bandwidth can quickly be exhausted. Operational complexity also grows when running IP applications on top of a TDM infrastructure.

Power utilities must consider cost effectiveness when evaluating any new network or service. The utility must avoid deploying separate application-specific networks to minimize capital expenditures (CAPEX) and be able to add applications and services to a converged network without negatively impacting operating expenditures (OPEX) associated with equipment, maintenance, and network administration.

Smart grid communications network requirements

Today, power utilities are aggressively pursuing communications options that will prepare them for Smart Grid deployment and result in improved operational efficiency and increased productivity as well. This means that many parameters must be kept in balance. First, the solution must be highly reliable: In a mission-critical environment, no compromise is acceptable. Second, CAPEX and OPEX must be minimized. Finally, the network should offer the opportunity to implement new services in a rapid and cost-effective manner. The ideal solution is one that offers at least the same level of reliability, QoS and security as that of traditional utility communications networks while supporting the full array of both TDM and new IP/Ethernet services that are needed for core utility operations and smart grid deployments.

IP and Ethernet will be the key communications protocols for the Smart Grid infrastructure. IP technologies serve as a bridge between applications and the underlying communication medium. This provides utilities with the opportunity to migrate traditional applications to more efficient IP and Ethernet-based implementations and to deploy new IP-centric Smart Grid applications, such as:

- IP-based supervisory control and data acquisition (SCADA) using protocols such as International Electrotechnical Commission (IEC) 104 or Distributed Network Protocol (DNP3), and Modbus over IP that allow for a simplified network architecture, efficient bandwidth utilization, and faster commissioning and deployment.

- IEC 61850-based substation systems that take advantage of the increase in bandwidth that modern networking technologies offer. IEC 61850 intelligent electronic devices (IEDs) that use Ethernet and TCP/IP for efficient communications are easier to scale and implement than legacy approaches. Also there are open initiatives to migrate IEC 101, IEC 104 plus DNP and Modbus toward an international usage of IEC 61850 in the future. This will be complex and challenging but exciting to watch as it develops.

- Synchrophasor systems, for grid stability monitoring and disturbance recording, require IP multicast for effective phasor measurement unit (PMU) communications.

- Video surveillance systems are now required as a key element to ensure the physical security of critical assets. Modern video surveillance systems are IP-based, operate with higher bandwidth, and integrated with the information technology infrastructure of the utilities.

- Distribution automation requires communications to many smaller substations as well as connectivity to a very large number of device endpoints in the field area network to enable distributed control and situation awareness.

- Advanced metering infrastructure requires a capable backhaul communications network to not only aggregate the meter data back to the head end but to perform direct meter reads and outage management.

- Other applications that include voice over IP (VoIP), IP mobile radio, Wi-Fi® mobility, physical substation security, corporate local area network (LAN) access, and more.

- However, in parallel with deploying these forward looking applications and services, there are questions that every utility should consider. Will the network meet my needs now and also in the future? Is it secure? Will it be reliable? Can I manage it? These are all compulsory inquiries that should be considered before building their smart network.

Bandwidth

The growth in IP applications drives the need for bandwidth and, more importantly, the need for bandwidth flexibility and efficiency. The new IP applications tend to exhibit "bursty" traffic behavior. The application grabs a high level of bandwidth to send a large amount of traffic, then, when the transmission ends, releases the bandwidth for other applications. With a traditional TDM implementation, running multiple services of this type becomes a challenge. The utility operator needs a service-aware network that can support legacy, IP and Ethernet applications without jeopardizing system availability.

Security

Existing and new applications require a communications network to support a large variety of traffic profiles and interconnection topologies. The network needs to securely transport this broad range of applications while keeping them virtually separated over a single physical infrastructure. Therefore, the network needs to support and maintain traffic separation and bandwidth traffic engineering, and to restrict access to the authorized traffic on configured ports. As with an optical SDH/SONET-based network, the network needs to be reliable and resistant to security attacks.

Reliability

The network must offer the necessary level of reliability to maintain uninterrupted operations. A single failure in the network should not be service-affecting. Service interruptions in utility environments can include consumers losing power, overload conditions, loss of communications, or the development of other potentially unsafe conditions. TDM systems traditionally support high levels of reliability such as UPSR when using SDH/SONET, allowing for switch-over time in less than 50 milliseconds. That level of service must be matched in a new smart network.

Manageability

The management of a utility communications network has a direct impact on the operational cost of maintaining and scaling the network. OPEX should not escalate exponentially as new services are added. A service-aware management platform, with utility operations awareness, can simplify network operations while streamlining operational processes such as maintenance, troubleshooting, and commissioning.

The Nokia new generation IP/MPLS utility communications network

The Nokia new generation utility communications equipment:

- Supports existing mission-critical TDM services
- Supports new IP and Ethernet applications and Smart Grid services
- Minimizes costs without compromising features, functionality and reliability

- Scales, allowing the utility to increase services and grow the number of users, devices, applications and capacity

- Ensures network and operational system security

- Is highly available and resilient

- Enables advanced QoS to prioritize mission-critical applications over other traffic

- Provides reliable transmission over different transport technologies including wireless microwave and WDM systems

These features support the clear movement toward implementing an IP or packet-based network for a power utility for all of its communications needs. Not all IP-based solutions are appropriate for power utilities. To support the converged mission-critical traffic of power utilities on a single physical network, an IP/MPLS-based communications infrastructure is key. An IP/MPLS network can support all traffic types, increase operational efficiency, and support existing mission-critical applications while providing the benefits of new Smart Grid applications.

IP/MPLS is available from carriers and communications service providers (CSPs) today. However, an increasing number of power utilities have deployed their own private IP/MPLS networks. With either type of deployment, IP/MPLS brings the advantages that utilities trust from a circuit-based network to an IP network, and enables network convergence, virtualization and resiliency.
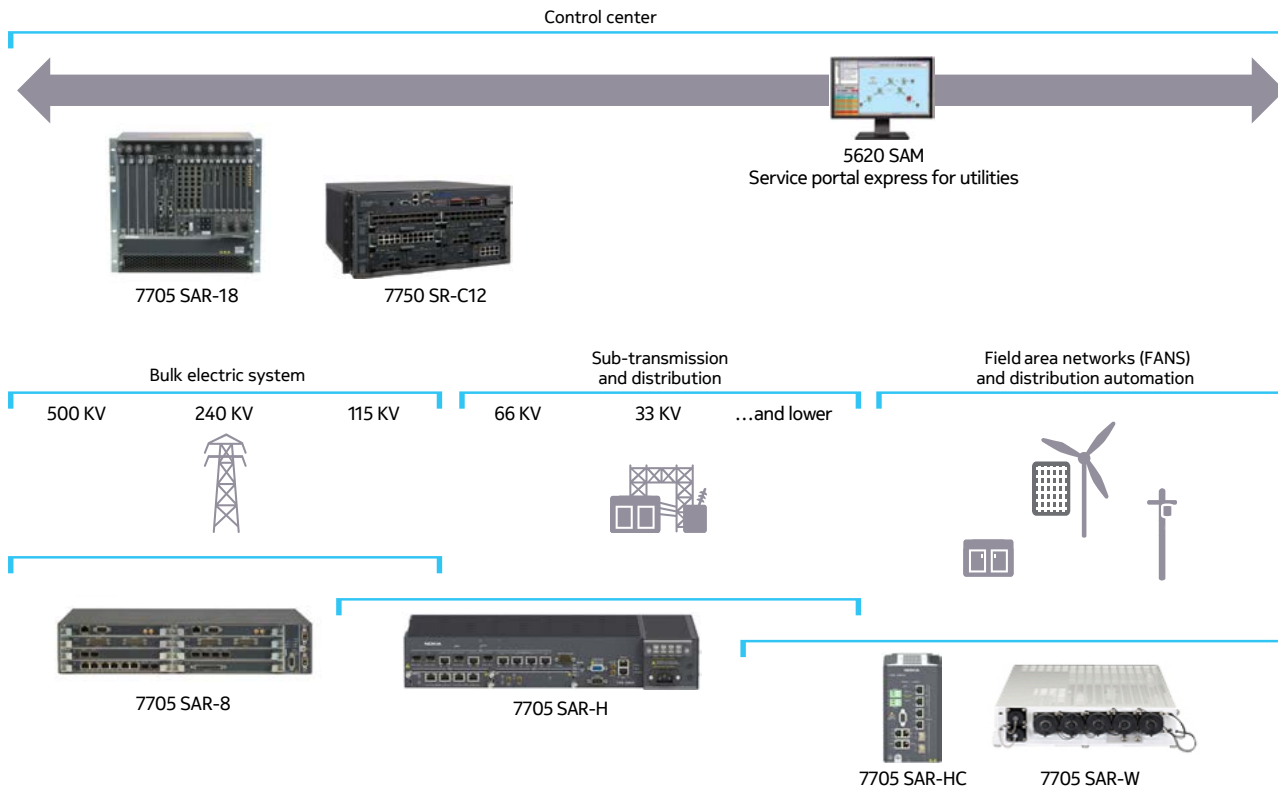
Nokia IP/MPLS network building blocks

The Nokia IP/MPLS communications network leverages multiple state-of-the-art technologies to enable a utility network to continue supporting existing TDM-based applications while providing a smooth migration path to IP and Ethernet services. It can also support a smooth integration of the operational and corporate traffic. The service-aware infrastructure efficiently supports the full range of IP and legacy applications, ensuring that each application can be allocated the resources that it needs in terms of bandwidth, QoS level, security, availability, and so on. The Nokia IP/MPLS implementation provides a service-oriented approach that focuses on service scalability and quality, as well as per-service operations, administration and maintenance (OAM).

The components of the Nokia IP/MPLS infrastructure, which extends IP/MPLS capabilities from the core to access, are based on and can include:

- Nokia 7750 Service Router (SR)

- Nokia 7705 Service Aggregation Router (SAR)

- Nokia 7210 Service Access Switch (SAS)

- Nokia 5620 Service Aware Manager (SAM) Portfolio

- Nokia Service Portal Express for Utilities

- Nokia 9500 Microwave Packet Radio (MPR)

- Nokia 1830 Photonic Service Switch (PSS)

Figure 1 shows the positioning of the key products of the Nokia utility IP/MPLS communications network.

Control center

5620 SAM
Service portal express for utilities

7705 SAR-18   7750 SR-C12

| Bulk electric system | | | Sub-transmission and distribution | | | Field area networks (FANS) and distribution automation |

500 KV   240 KV   115 KV   66 KV   33 KV   …and lower

7705 SAR-8   7705 SAR-H

7705 SAR-HC   7705 SAR-W

The Nokia IP/MPLS products provide routing, switching and multiservice capabilities, enabling the power utilities to support real-time applications across the full extent of the network. The Nokia IP/MPLS implementation includes non-stop routing and non-stop service capabilities that provide unparalleled reliability.

The network and service administration of the Nokia IP/MPLS communications network is handled by the industry-leading Nokia 5620 SAM portfolio, an integrated application that covers all aspects of element, network and service management on one platform. Together with the Nokia Service Portal Express for Utilities, it simplifies the workflow, management, and maintenance of the network. These include automating routine tasks, correlating alarms to problems, real-time IP control plane visualization, managing end-to-end connections, and creating performance reports - all through a user-friendly point-and-click interface. For effective end-to-end network management, the 5620 SAM can manage multi-domain products mentioned above, as well as third-party elements within the network that support standards-based Simple Network Management Protocol (SNMP).

Figure 2 shows an overview of the Nokia utility IP/MPLS communications network and the various services that can be supported.
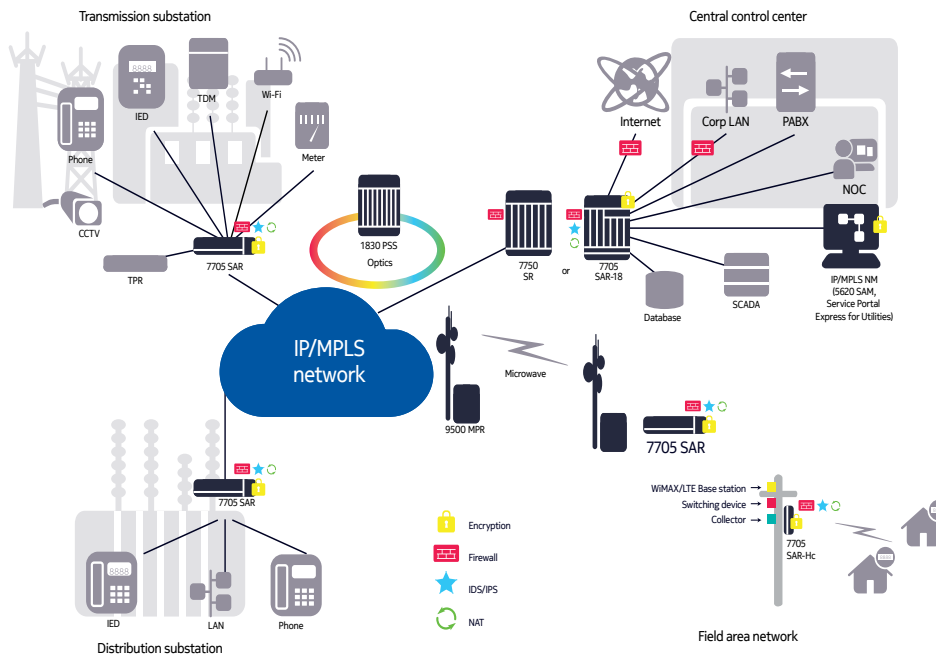
The Nokia IP/MPLS network connects the control center (and backup center) with remote sites and substations with SDH/SONET-like reliability. At each substation, an IP/MPLS switch/router aggregates traffic from energy applications or services. These could include:

- IED/remote terminal unit (RTU) for SCADA

- Protection relays for grid control

- PMU for phasor measurements

- Wi-Fi access point

- VoIP

- Corporate network access

- Physical access control

- Video surveillance

The traffic on the network can be for intra-substation, inter-substation, or control center communications. The IP/MPLS network can also maintain application or service separation and security by carrying traffic within OSI Layer 2 or Layer 3 virtual private networks (VPNs). This allows support of traffic that is inside or outside of established electronic security perimeters (ESPs). For a substation with TDM connectivity requirements, the Nokia 7705 SAR, while handling IP and Ethernet traffic, can also natively support RTU serial interfaces for SCADA, analog voice interfaces for operations voice, and teleprotection interfaces for protection relays. With this IP/MPLS network, traffic is now packet-based, and bandwidth in the network is shared while QoS for mission-critical traffic is strictly maintained. Both packet and TDM services are

concurrently supported by the same IP/MPLS switch/router, even for the substation LAN, reducing the overall number and costs of telecom equipment required.

Underlying transport options for increasing backbone network capacity include point-to-point RF microwave such as the 9500 MPR that can be used to provide connectivity coverage to one or several sections of the network and optical product such as the Nokia 1830 PSS using technologies like Coarse Wavelength Division Multiplexing (CWDM) and Dense Wavelength Division Multiplexing (DWDM).

For distribution automation, the Nokia 7705 SAR-Hc and 7705 SAR-W are used in the field area network to provide connectivity to sensors and field devices such as reclosers, voltage controllers, and capacitors for remote control and monitoring, as well as aggregation for advance metering infrastructure. The communications network can incorporate wireless technologies such as WiMAX and Long Term Evolution (LTE), or wireline technologies like XDSL, Gigabit-capable Passive Optical Network (GPON) and Power Line Carrier (PLC) for extended coverage.

Figure 3 shows how the 7705 SAR-Hc and 7705 SAR-W can be deployed in a field area network.
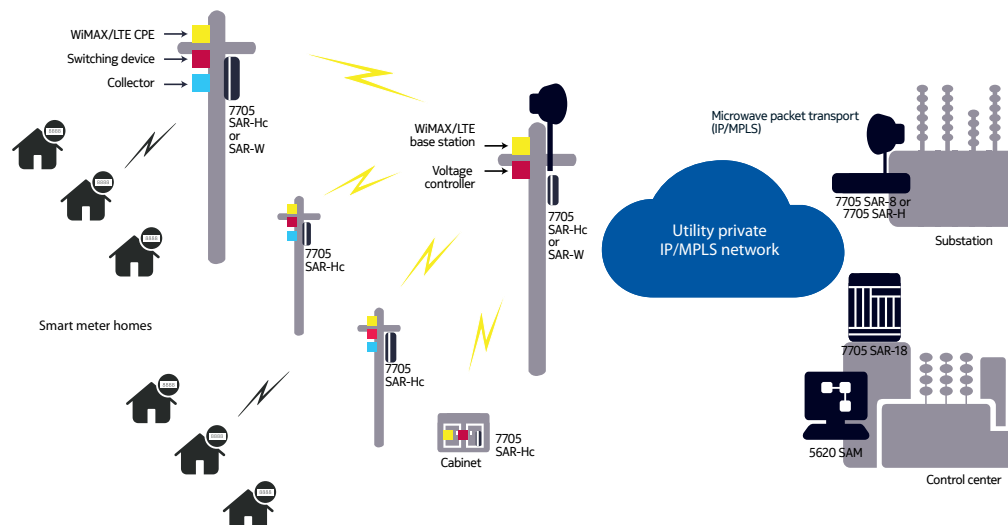
The network topology

A network topology is determined by the graphical mapping of the physical and logical interconnections. The IP/MPLS network can be deployed on a combination of ring-based, partially-meshed, hub and spoke, and linear architectures.

A ring architecture provides an efficient, reliable environment - as traffic can be rerouted in the opposite direction of the ring should a failure occur. In a SDH/SONET application, every node is typically transmitting in both directions to provide end-to-end protection, effectively duplicating all traffic on the ring. In the Nokia IP/MPLS infrastructure typically on high-speed Ethernet, the network relies on the IP/MPLS fast reroute (FRR) feature for resiliency, which eliminates the requirement to duplicate the traffic on the ring. All the bandwidth can then be fully utilized and FRR ensures traffic is rerouted in sub-50 milliseconds in the event of a node or link failure in the ring, preserving all traffic on the ring. This topology is often used in the aggregation part of the network and offers a very efficient way to aggregate and backhaul traffic over a relatively low number of links.

A partially-meshed architecture uses more links and therefore provides more rerouting alternatives. Partially-meshed networks are able to recover from double faults and are often deployed in the core of the network. Traffic engineering is used to efficiently carry the traffic over the different meshed links across the network.

For the field area network, hub and spoke and linear architecture can efficiently aggregate traffic from a large number of distributed devices.

CAPEX/OPEX and scalability

To meet utility's growing requirements in terms of service deployment and bandwidth, the Nokia IP/MPLS network is extremely scalable, according to changing requirements. The IP/MPLS network can accommodate a growing number of applications and services. Minimal CAPEX requirements to deploy and scale this infrastructure are the result of the granularity in bandwidth, scaling options, and statistical multiplexing. The converged architecture and the ease of network management allow for optimized OPEX. A converged network also reduces the number of network elements required, thus also reducing costs.

High availability through IP/MPLS

With the Nokia IP/MPLS network, utilities have the necessary reliability level to maintain uninterrupted operations. The MPLS FRR feature enables the network to reroute connections around a failure in less than 50 milliseconds. Because the network is service aware, FRR can distinguish and prioritize traffic redirection according to priority. To protect the network against node or interconnection failures, end-to-end standby MPLS paths can also be provisioned.

The Nokia IP/MPLS implementation includes the unique additional High Availability features of non-stop routing and non-stop services. The benefits are unparalleled availability and reliability:

- Non-stop routing – ensures that a control card failure has no service impact. Label Distribution Protocol (LDP) adjacencies, sessions and the database remain intact if there is a switchover.

- Non-stop service – ensures that VPN services are not affected when there is a Control Fabric Module switchover.

Quality of service and traffic management

In a utility environment where multiple services converge over a common infrastructure, QoS is essential. The Nokia IP/MPLS network can discriminate among various types of traffic, based on a rich set of classification attributes at Layer 1, Layer 2, Layer 2.5, or Layer 3 and prioritize transmission of higher priority traffic over lower priority. It utilizes extensive traffic management using an advanced scheduling mechanism to implement service hierarchies. These hierarchies provide maximum isolation and fairness across different traffic while optimizing uplink utilization. With multiple levels and instances of shaping, queuing and priority scheduling, the Nokia IP/MPLS network can manage traffic flows to ensure that performance parameters (such as bandwidth, delay and jitter) for each application are met.

Multiservice support

The Nokia IP/MPLS network offers a flexible network and service environment that enables the continuing support of existing services while incorporating new IP and Ethernet applications. These packet applications

are typically more efficient in terms of bandwidth usage when deployed over an IP/MPLS network. All services converge at the access of the network, where the required packet handling, such as encapsulation and QoS capabilities, is executed. Different applications are transported through dedicated VPNs in a point-to-point, point-to-multipoint or multipoint-to-multipoint manner. The network also supports the migration of TDM services on to the IP/MPLS network.

Virtualization

The Nokia IP/MPLS network provides for the virtual isolation of various traffic types on a single infrastructure. This allows the full separation of traffic from different applications or operations within the utility, allowing for a secure environment and effective bandwidth allocation. Advanced MPLS VPNs-such as circuit emulation service (CES), virtual private LAN service (VPLS) and IP VPNs-are supported which can be used to provide different applications or user groups with an environment that is private and unaffected by other traffic. One service is carried across one VPN while the traffic of different services is securely separated in their own VPN, effectively providing separate private networks. With advanced MPLS VPNs, a utility can also leverage the same IP/MPLS network to offer business communications services.
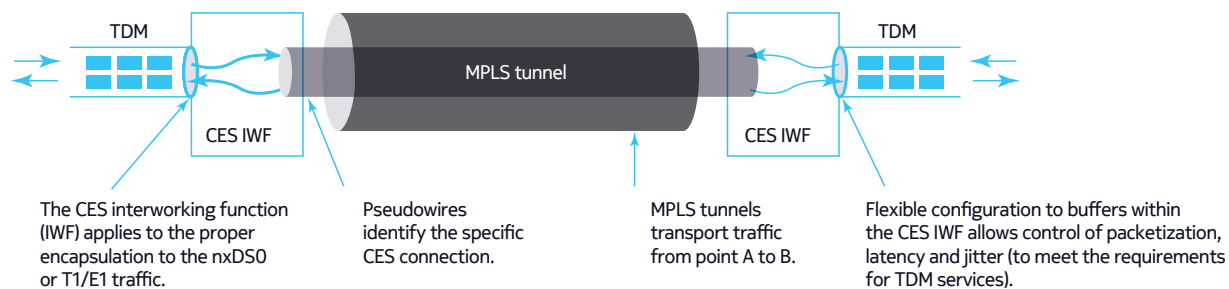
Circuit Emulation Service

Utilities need to consider how to leverage new IP/MPLS network technologies when migrating legacy TDM systems and services. Utilities can take advantage of the IP/MPLS CES functionality and transition their legacy applications gradually. CES delivers the same quality of service as the existing TDM network infrastructure, with the same level of predictability. The Nokia IP/MPLS network has a circuit emulation interworking function that ensures all information required by a TDM circuit is maintained across the packet network. This provides a full transition to a packet network over time while providing TDM service continuity. Example TDM services that can be supported include teleprotection, analog voice or modem connections, and SCADA over serial links .

Two principal types of circuit emulation can be used: Circuit Emulation Service over Packet (CESoPSN) and Structured Agnostic TDM over Packet (SAToP). CESoPSN allows NxDS0 service, including full T1/E1 capability. SAToP provides the ability to carry unstructured T1/E1 circuits across the IP/MPLS network.

In an IP/MPLS network, the MPLS tunnel is used as the transport layer (Figure 4). A pseudowire (PWE3) is created to identify the specific TDM circuit within the MPLS tunnel. The circuit emulation interworking function ensures that all information required by the TDM circuit is maintained across the packet network. This provides a transparent service to the end devices.

Figure 4. Circuit Emulation Service functionality overview

The CES interworking function (IWF) applies to the proper encapsulation to the nxDS0 or T1/E1 traffic.

Pseudowires identify the specific CES connection.

MPLS tunnels transport traffic from point A to B.

Flexible configuration to buffers within the CES IWF allows control of packetization, latency and jitter (to meet the requirements for TDM services).

A pseudowire encapsulates traffic over label switched paths (LSPs) to create a point-to-point service. An MPLS pseudowire is analogous to a private line within the MPLS network. It offers a point-to-point connection between any two end devices. Figure 5.1. depicts three different types of pseudowires — TDM, FR, and Ethernet. The pseudowire can be used for applications that require dedicated point-to-point connectivity.

Figure 5. IP/MPLS-based VPN services
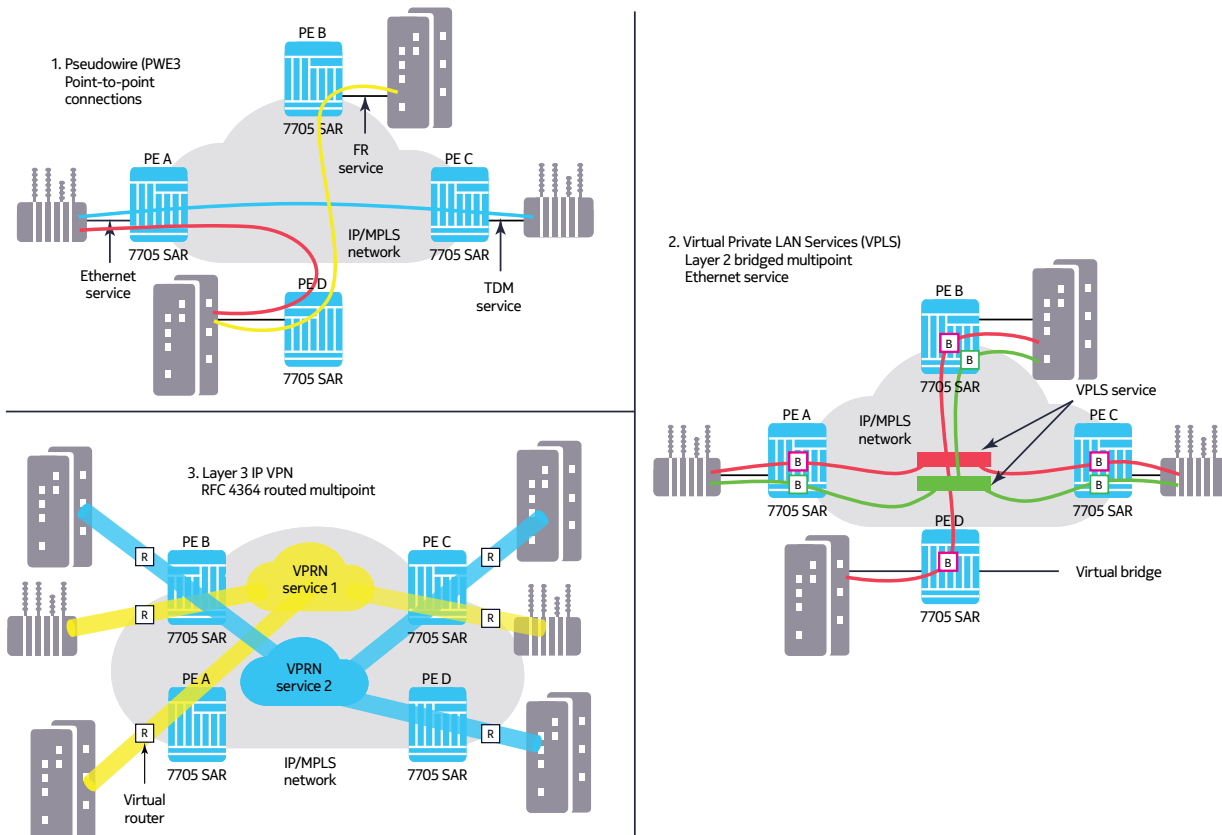
VPLS

VPLS is a bridged multipoint service that forwards traffic based on the media access control (MAC) address. A VPLS service is protocol-independent and enables multipoint connectivity at Layer 2 within the IP/MPLS network. Figure 5.2. depicts two VPLS instances within a network. VPLS is composed of virtual bridges at each node. Each virtual bridge performs MAC learning and constructs a table that maps MAC addresses and corresponding MPLS paths. The VPLS concept is similar to a logical LAN connection where all end devices connected to the VPLS appear as if they are within the same LAN segment. For utilities, a VPLS service can be used to support Ethernet-based SCADA systems and IEC 61850 Generic Object Oriented Substation Events (GOOSE) messaging over multipoint Ethernet connections, for example.

IP VPN

An IP VPN is a Layer 3 VPN and is implemented specifically for IP traffic only. An IP VPN is a routed service that forwards traffic based on the IP address. An IP VPN enables multipoint connectivity at Layer 3 within the IP/MPLS infrastructure (Figure 5.3.). With IP VPNs, each IP/MPLS node supports virtual routing and forwarding (VRF) instances. For example, an IP VPN can be used to support multiple independent departmental networks with no routing table interactions among the different VRF instances. IP VPN is also suitable for application separation to support corporate access, SCADA over IP, IP video surveillance, or voice over IP.

Teleprotection over IP/MPLS

Teleprotection systems monitor and compare conditions on transmission lines for coordinated tripping of transmission lines to quickly isolate faults in order to prevent damages to expensive substation equipment and instability in the power system. These systems rely on the communications network for real-time status exchange between teleprotection relays (TPRs). To ensure the power system is protected, relay signals must be transferred with minimal latency.

The Nokia IP/MPLS network can support the stringent latency requirement for teleprotection. Setting up the right quality of service in an IP/MPLS network will enable the network to discriminate among various types of traffic and forward higher priority protective relay traffic over lower priority traffic. A Nokia IP/MPLS network can manage protective relay traffic flows to ensure performance parameters like bandwidth, delay, and jitter will be met. This minimizes the need to maintain a parallel TDM network for teleprotection.

Figure 6 shows how teleprotection can be supported by the Nokia IP/MPLS network. The interface from the teleprotection relay can be IEEE c37.94, G.703, E&M, or RS-232. For traditional TDM-based implementation, these relay interfaces are connected to a multiplexer for TPR signal transport using a T1/E1 and over SDH/SONET or microwave links to the next substation. With the migration to an IP/MPLS network, a Nokia 7705 SAR can be used to support teleprotection as all these relay interfaces are natively supported and can be connected directly to the 7705 SAR for pseudowire connection to the far end 7705 SAR. Alternatively, in cases where a multiplexer continues to be used, a T1/E1 from the multiplexer can be terminated onto the 7705 SAR

Figure 6. Using an IP/MPLS network for teleprotection
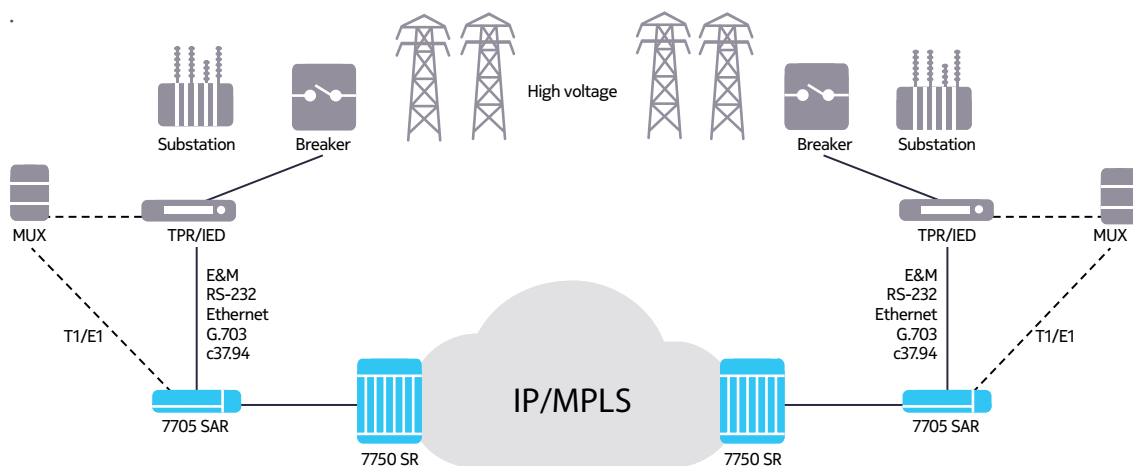
IEC 61850 GOOSE messaging over Ethernet was originally intended for intra-substation communications but has now been expanded to include inter-substation communications. For this and other Ethernet-based implementation, the 7705 SAR can concurrently support protective relay traffic over Ethernet with VPLS service, allowing for easy migration to newer protection systems.

Network synchronization and timing

Accurate synchronization and microsecond timing is critical in communications networks to maintain network operational integrity. In most TDM networks, synchronization is distributed within the network using the SDH/SONET mechanisms built into the physical layer definition or by distributed GPS clocks. To deliver the TDM service through a packet network, the same synchronization accuracy or better must be achieved. In the packet world, high quality stratum-based master clocks distribute timing using Synchronous Ethernet or IEEE 1588v2 Precision Timing Protocol (PTP). Packet-based microsecond timing allows generation and transmission equipment to operate closer to operational limits. This promotes efficiency and allows more power to be delivered over the existing grid. The greater precision will support newer and more stringent timing requirements of applications like syncrophasor measurement which has a much higher frequency of sensor readings for greater accuracy, and real-time sampled values which can be acted upon to align and rebalance the current and voltage loads in much faster cycles. These important applications allow for future grid improvements.

To enable rapid and smooth migration of these networks, the Nokia IP/MPLS products support a wide range of synchronization and timing options to ensure that the network is properly synchronized and to allow for deployment of new timing technologies such as IEEE 1588v2 PTP. The following features are supported:

- External reference timing
- Line timing
- Adaptive clock recovery (ACR) timing
- Synchronous Ethernet
- IEEE 1588v2 PTP

Cybersecurity

Cybersecurity is paramount for utilities to safeguard critical infrastructures as they could be targeted by cyber attacks and other security threats. There have been increased efforts from governments worldwide to further the cause. For example, the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) regulations are aimed at protecting the reliability of the bulk power system of North America. The Nokia IP/MPLS network has extensive integrated security features that help utilities to defend against cybersecurity threats, ensure data privacy, and meet regulatory compliance such as NERC CIP.

The Nokia IP/MPLS network provides mechanisms to protect the management, control and data planes through access control lists, filters and authentication of signaling messages, assisting in the prevention of session hijacking, spoofing, denial of service attacks and other such malicious network behavior. Strong password security is provided by SNMPv3 confidentiality and integrity features and Secure Shell (SSH) encryption. Integrated stateful firewall helps stop unexpected and unwanted traffic from entering the network. Network address translation (NAT) protects and hides private addressing space from external

entities. Group encryption protects sensitive data during transit and ensures data integrity and privacy. Intrusion detection system (IDS) and intrusion protection system (IPS) detect and protect against network and traffic anomalies.

Integrated multi-drop data bridge

Utilities have extensive SCADA system investments and many of these systems will continue to operate with serial or modem interface connections. To minimize the need to deploy a large number of serial interfaces and to provide efficient network architecture, the Nokia IP/MPLS network supports integrated multi-drop data bridge (MDDB) function to allow utilities to continue operations with existing SCADA RTU infrastructures.

Effective management for easy day-to-day operations

A key element of reliable and flexible IP/MPLS communications infrastructure is a set of effective, simplified management tools that provide easy configuration and control of the network, effective problem isolation and resolution, and support of new management applications. The Nokia IP/MPLS network supports OAM tools that simplify the deployment and day-to-day operation of a utility communications network. For example, service tests, interface tests and tunnel tests allow for rapid troubleshooting and enable proactive awareness of the state of traffic flows to help minimize service downtime.

The Nokia IP/MPLS network is fully managed by the industry-leading Nokia 5620 Service Aware Manager portfolio, which automates and simplifies operations management of a converged IP/MPLS network, driving network operations to a new level of efficiency. It also provides simplified diagnosis and intuitive visualization of the relationship between services, the MPLS infrastructure and the routing plane.

The Nokia Service Portal Express for Utilities is tightly coupled with the Nokia 5620 SAM to simplify network operations and management by maximizing the efficiency of day-to-day tasks, such as provisioning circuits for SCADA or protection, monitoring real-time status, troubleshooting problems, reporting on NERC CIP asset inventory, and validating service performance.

The Service Portal Express for Utilities enables staff from various operational teams to perform routine network management tasks without needing specialist network knowledge. Its interface includes a predefined set of profiles, such as SCADA, protection and video surveillance, with pull-down menus that simplify use and greatly reduce the possibility of user error. In addition, workflows may also be routed to proper authorizations for review and approval. For added security, access to its functionality are controlled and only through users who are assigned a set of roles, each of which grant access to various functions of the portal. Users are authenticated and then associated with their authorized roles. All user activities are logged for security and NERC CIP access control management.

Network metrics can be easily retrieved in reports designed specifically for utilities on network applications, status, performance and NERC CIP asset inventory.

Figure 7 shows the key modules and features of the Service Portal Express for Utilities.

Figure 7. Service Portal Express for Utilities
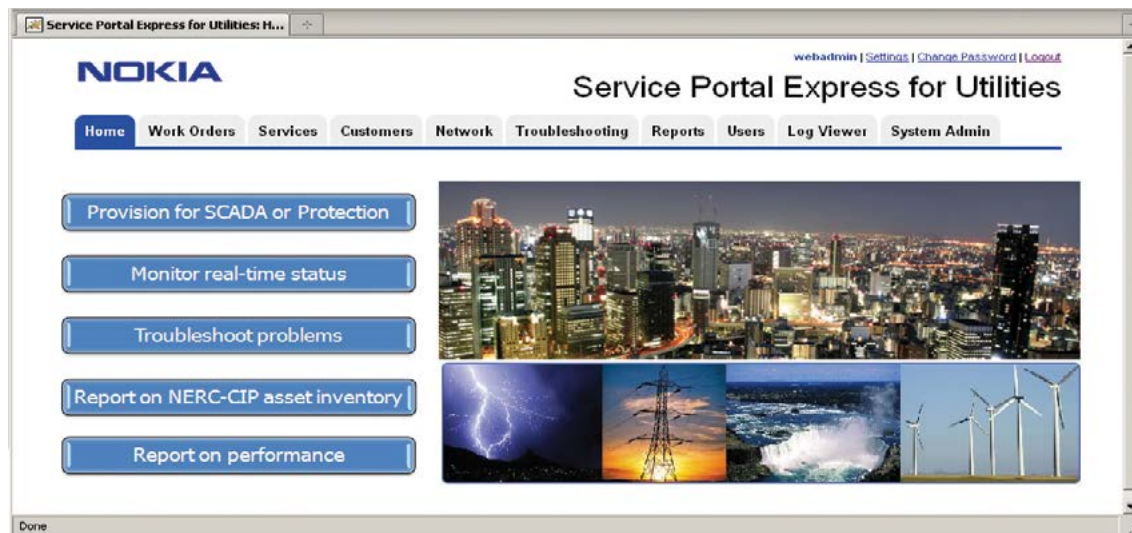
Conclusion

Utilities are experienced at building and operating reliable and effective electricity grids and the communications networks to ensure the delivery of essential information to monitor, analyze, control and maintain flawless service delivery. The Nokia IP/MPLS communications infrastructure can help a utility extend and enhance its network with new technologies like IP, MPLS, and Ethernet. These new technologies will enable the utility to optimize its network flexibility and management in order to reduce both CAPEX and OPEX without jeopardizing safety, security or reliability. Advanced technologies also allow the introduction of new Smart Grid applications that can improve operational effectiveness and workflow efficiency within the utility. Nokia leverages cutting-edge technologies, along with the company's broad and deep experience in the utility industry, to help utilities build better, new generation networks with IP/MPLS.

Acronyms

ACR	adaptive clock recovery
CAPEX	capital expenditures
CCTV	closed-circuit television
CES	Circuit Emulation Service
CESoPSN	Circuit Emulation Service over Packet
CPAM	Control Plane Assurance Manager
CSP	communication service provider
CWDM	Coarse Wavelength Division Multiplexing
DNP	Distributed Network Protocol

DWDM	Dense Wavelength Division Multiplexing
ESP	electronic security perimeter
ESS	Ethernet Service Switch
FAN	field area network
FRR	Fast Reroute
GOOSE	Generic Object Oriented Substation Events
GPON	Gigabit-capable Passive Optical Network
H-QoS	Hierarchical quality of service
IDS	intrusion detection system
IEC	International Electrotechnical Commission
IED	intelligent electronics devices
IP	Internet Protocol
IPS	intrusion protection system
IP VPN	IP virtual private network
LAN	local area network
LDP	Label Distribution Protocol
LSP	label switched path
LTE	Long Term Evolution
MAC	media access control
MDDB	multi-drop data bridge
MPLS	Multi-protocol Label Switching
MPR	Microwave Packet Radio
NAT	network address translation
NERC CIP	North American Electric Reliability Corporation Critical Infrastructure Protection
OAM	operations, administration and maintenance
OPEX	operating expenditures
PMU	phasor measurement unit
PSS	Photonic Service Switch
PTP	Precision Timing Protocol
QoS	quality of service
RTU	remote terminal unit
SAM	Service Aware Manager

SAR	Service Aggregation Router
SAS	Service Access Switch
SAToP	Structured Agnostic TDM over Packet
SCADA	supervisory control and data acquisition
SDH	Synchronous Digital Hierarchy
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SR	Service Router
SSH	secure shell
TDM	time division multiplexing
TPR	teleprotection relay
UPSR	unidirectional path-switched ring
WDM	wavelength division multiplexing
VoIP	voice over IP
VRF	virtual routing and forwarding
VPLS	virtual private LAN service
VPN	virtual private network

NOKIA

nokia.com