Multiprotocol Label Switching for the Utility Wide Area Network

Throughout the world, electric utilities are increasingly planning for a future based on smart grid applications requiring advanced telecommunications systems. Made possible by technologies such as multiprotocol label switching (MPLS), many such applications utilize packet connectivity for communicating information and control signals across the utility's wide area network (WAN), including:

- Grid measurement and control traffic (SCADA, teleprotection, system integrity protection schemes [SIPS], distributed and centralized remedial action solutions)
- Non-control grid data (condition-based monitoring, digital fault recorders, feeder meter data)
- Physical security (access control and video surveillance cameras)
- Remote worker access (voice communications, geographic information mapping systems [GIS], remote configuration, workforce management, safety training)
- Environmental information (temperature, battery status, wind speed, and so on)
- Field area network data backhaul (advanced metering infrastructure [AMI], distribution grid management, distributed generation)
- Enterprise traffic (corporate data, email, collaboration tools, business operations)

WANs support this wide variety of traffic to and from substations, the distribution grid, generators, between control centers, and between work locations and data centers. To maintain this rapidly expanding set of applications, however, many utilities are taking steps to evolve present time-division multiplexing (TDM)–based and frame relay infrastructures to packet systems. Packet-based networks are designed to provide greater functionality and higher levels of service for applications, while continuing to deliver reliability and deterministic (real-time) traffic support.

The Cisco® MPLS solution for electric utilities is designed as a flexible network foundation that supports both TDM-based services and packet-based application requirements. This core network platform provides flexibility that is unmatched in the industry, making it possible for the utility to protect its current investments while planning a communications infrastructure roadmap for years into the future. Cisco's MPLS offering:

- Interoperates with and supports traditional networks and systems, integrating them into a single network infrastructure
- Extends virtualization across the network, allowing utilities to manage and add new services with minimal business disruption
- Allows end-to-end security to be built into the network, providing multiple layers of protection
- Provides utility-grade reliability to support grid operational requirements and minimize outages
- Supports today's smart grid features (such as wide area measurement, remedial action schemes, and video monitoring) and applications that require their operational logic to be distributed and decoupled from communication flows
- Provides highly scalable infrastructure for field area networking (FAN), data center, and control center implementations

- Includes comprehensive operations administration and management to keep systems running at optimum levels
- Is built on powerful, ruggedized Cisco routing and switching technologies designed specifically for the utility industry
- Includes access to a dedicated incident response program 24 hours a day, seven days a week that manages investigation, repair, and reporting of security vulnerability information

Challenges Facing Today's Utilities

As critical infrastructure operators, utilities have the responsibility to maintain electric power delivery and control grid equipment in all circumstances, even when public service provider networks are congested or an extended power outage occurs. To achieve this goal, most utilities have traditionally relied on private TDM-based solutions such as SONET/SDH. These technologies deliver carrier-class performance, support the deterministic traffic critical for grid operations, and are relatively straightforward to deploy initially.

However, because of changing system requirements and equipment end of life, TDM infrastructures no longer adequately support utility long-term needs. Many are built and operated for specific applications or solutions, creating siloed infrastructures that make it more challenging to integrate new systems and operational processes. This inflexibility promotes the deployment of more specialized overlay networks, creating a spiral of ever-greater complexity. Such overbuilt networks are inefficient, require a great deal of manual administration, are more challenging to troubleshoot, and increase maintenance costs. As a result, such environments are also less secure and add operational risk over time.

Within the same systems, we are also seeing a steady increase in bandwidth consumption as communications traffic increases. Wide Area Measurement Systems (WAMS), video-based applications such as networked physical security, and AMI backhaul over the WAN are promoting bandwidth usage to a point that TDM-based networks can no longer cost-effectively support.

These shortcomings are amplified by today's increasingly complex regulatory environment. Evolving regulatory requirements such as U.S. NERC CIP compel utilities to enable better communications to support cyber and physical security, audit and monitoring, and grid interoperability.

In response to all these challenges, packet-based systems allow utilities to take advantage of new technologies that not only meet operations goals but also enable the enterprise and operations applications demanded by the smart grid to coexist. For utilities replacing their TDM networks, MPLS is viewed as the strategic technology of choice.

Why MPLS?

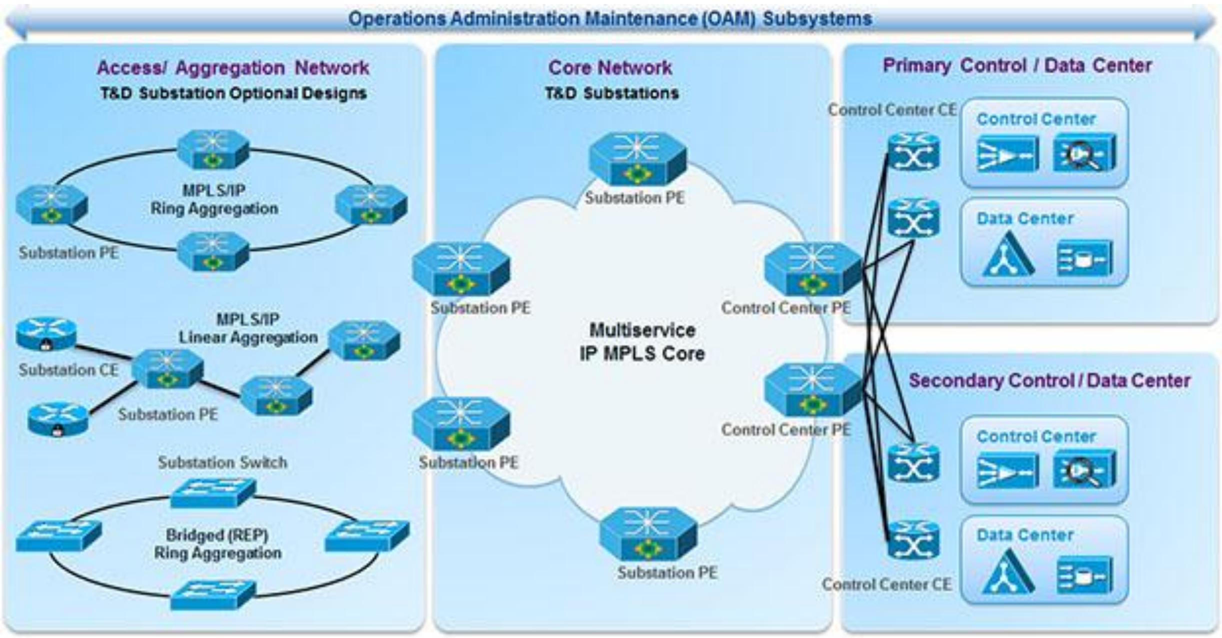
MPLS is a proven WAN technology for network operators who need to support diverse legacy systems as well as modernize for next-generation applications. Enabling transparent integration of traditional and smart grid capabilities, MPLS facilitates transport of most forms of traffic, from traditional serial-based technologies such as SCADA remote terminal units (RTUs) to today's IEC 61850 packet-based intelligent electronic devices (IEDs).

MPLS was first introduced in 1999 by the Internet Engineering Task Force (IETF) and has been rapidly adopted by almost every major service provider as a platform for supporting thousands of customers over a common infrastructure. It is based on a Cisco innovation called tag switching, first announced in 1996; tag switching was then adopted and used as the basis for the vendor-independent MPLS protocol. MPLS is also utilized by private enterprises such as financial institutions and airports to transport time-critical and confidential information. In the utility industry, MPLS is by far the most commonly selected WAN technology for smart grid implementations because of its:

- Maturity and proven capabilities across large-scale industrial and enterprise networks
- Ability to support both traditional applications and next-generation requirements
- Ability to virtualize the WAN into independent sub-networks
- Centralized management of physical infrastructure and virtualized sub-networks
- Ability to enhance and become an integral part of the security framework across the WAN
- Modularity for scalability and flexibility, as well the ability to protect the overall system from domain failures

Cisco implements MPLS based on its modular Cisco GridBlocks™ reference model. By supporting multiple applications on a converged network, our smart grid solutions provide a framework for integrating new technologies and utility-specific applications. The modular approach enables implementation of projects over time, allowing utilities to plan their investments and flexibly adapt to changing business circumstances.

Figure 1. MPLS architectural configuration options



Key Features of MPLS

MPLS offers a number of features that make it especially suitable for multiservice, high-security industrial environments. By protecting existing system investments while enabling the transition to the modernized grid, MPLS provides a secure, flexible, high-performance foundation for utility systems.

Network Virtualization

In high-security, geographically distributed environments, large flat networks are usually neither practical nor reliable. They create a single fault domain and do not permit the kind of modularity needed for dependable, secure system management over large distances. As a result, grid applications suffer due to congestion, poor performance, reliability and security issues, and administrative complexity.

Within an MPLS infrastructure, however, applications can be logically separated and secured to support specific business functions while remaining on a single physical network. These software-defined segments operate securely and independently from each other, minimizing the fault domain. Within each virtual network, MPLS supports deterministic traffic, prioritization of traffic flows, and flexible allocation of bandwidth to enable optimal, consistent performance.

Traffic is secured by policy-based trust boundaries, with each operations system accessible only to an approved group of users. Administrators can also create new secure segments as needed based on scalable Layer 2 and Layer 3 virtual private networking (VPN) domains, including point-to-multipoint capabilities.

Support for Existing Networks

One of the most valued features of MPLS is that it allows utilities to perpetuate the use of existing TDM circuits, ATM, frame relay, and other traditional communication networks on the same WAN backbone with next-generation packet-based systems. This is achieved either by running these legacy systems over an MPLS network using techniques such as circuit emulation with Pseudo Wire Emulation Edge-to-Edge (PWE3) and/or by overlaying MPLS onto an existing TDM-based network infrastructure. Cisco's framework for PWE3 is embodied in its Any Transport over MPLS (AToM) strategy.

Enhanced by MPLS Traffic Engineering (TE), networks can integrate virtually all forms of traffic without having to disruptively replace still-functioning older systems. This helps to unify the network management environment, making it significantly more cost-effective to administer. By running new applications alongside older systems on the same network, utilities can protect their current investment while transitioning the business to the smart grid.

Security in MPLS

MPLS virtualization greatly enhances network security. By creating logical separation of routing and data flows, utilities are able to safeguard specific information for each segmented domain. In doing so, it assures greater security for a variety of applications.

For example, many utilities are considering how they might improve mobile worker connectivity through Wi-Fi, especially in remote areas where public cellular signals are not always reliable. However, a security threat exists in the potential of Wi-Fi traffic mingling with operations traffic. This issue can be resolved by utilizing robust Wi-Fi security mechanisms as well as MPLS to create a totally segregated virtual network for all Wi-Fi traffic. Along the way, MPLS mechanisms such as rate shaping, priority handling, and traffic engineering mechanisms help to guard against denial of service and other malicious attacks.

Cisco MPLS designs are based on standardized implementation guides for both cyber and physical security, creating a consistent, end-to-end security scheme that covers all kinds of network traffic. Capabilities include:

- Risk identification, prioritization, and management during the design process
- Six nines of availability, redundancy, and resiliency enabled with in-service software upgrades, stateful switchover, and nonstop forwarding
- Network reliability through containment and isolation for mission-critical traffic with support for virtual local area networks (VLANs), Virtual Routing and Forwarding (VRF), MPLS-VPN, zone-based firewalls, and intrusion detection/intrusion prevention systems
- Next-generation confidentiality and integrity mechanisms based on the latest protocols to protect critical data

- Remote access for operations staff and vendors through remote workforce management tools, including authentication, authorization, confidentiality, and integrity
- Advanced forms of Quality of Service (QoS) for granular, service-level control

Cisco also offers access 24 hours a day, seven days a week to a dedicated global task force called the Product Security Incident Response Team (PSIRT) that manages the receipt, investigation, repair, and public reporting of security vulnerabilities. This team works closely with users, independent security researchers, consultants, industry organizations, and other vendors to gather information, identify, and quickly patch possible security problems. It further supports the monitoring of internal and external security threats.

Cisco runs a variety of programs to support the development of trustworthy utility systems, including the Product Security Lifecycle, which drives development of products to a security baseline; international certifications compliance; the Cisco Security Intelligence Operation; and participation in public/private standards organizations.

Utility-Grade Performance

Utilities have traditionally accepted SONET/SDH for its ability to deliver high-performance connectivity. By contrast, packet solutions have sometimes been characterized as “best-effort networks,” especially in situations where they are based on T1 or low-bandwidth connectivity. But this not true for well-designed packet networks, especially not for high-speed MPLS networks designed with Quality of Service, traffic engineering, fault detection, and Fast Reroute (FRR) features.

In contrast to other forms of packet solutions, which function on a hop-by-hop basis, MPLS TE steers traffic across predetermined routes in case of a network failure. Features such as bidirectional forwarding detection (BFD) and FRR can detect failures and reroute traffic on a par with SONET, helping to assure reliability and speed of network traffic.

Multicast

Packet-based networking supports functionalities such as multicast, in which traffic is simultaneously sent to a subscribed subset of endpoints. Multicast is critical for industry solutions such as IEC 61850 and is used to transmit messages between devices for applications such as teleprotection. Not only does this decrease the time required for messages to be communicated to multiple endpoints, but it opens up the potential for dynamic new protection schemes. Multicast is therefore an increasingly important feature for both Layer 2 and Layer 3 packet communications.

IP/MPLS and MPLS-TP for the WAN

The flexibility of MPLS allows utilities to transport data using a variety of static and dynamic techniques, including fully switched or circuit-oriented connections, or quite commonly for a hybrid configuration supporting both. The appropriate deployment approach is determined by assessing such issues as the nature of the environment, the coverage area, the level of SONET/SDH functions, dynamic signaling, control plane policing as well as operational business requirements.

Cisco’s Utility-Specific Solutions

The Cisco MPLS offering is based on a portfolio of utility-specific communication infrastructure solutions:

- **The Cisco GridBlocks Architecture** provides a forward-looking framework for integrating the end-to-end electrical grid to deliver a highly secure, reliable communications infrastructure.
- **Transmission and substation solutions** support MPLS-based remote communications with substations using the ruggedized Cisco 2010 Connected Grid Router (CGR), the Cisco 2520 Connected Grid Switch, and the Aggregation Services Router (ASR) Series product family.

- **Grid security solutions** enable critical infrastructure-grade security for the network and for physical facilities to achieve compliance and reduce vulnerability to threats for systems, data, and assets.
- **Workforce enablement solutions and services** to support workforce collaboration for field personnel, integrating disparate communications such as radios, cellphones, and public safety systems.
- **Field area network solutions** integrate FAN data backhaul for AMI and distribution automation, as well as workforce management, based on the multiservice CGR 1000 Series.
- **Connected Grid Network Management Solution** such as Cisco Prime™ for IP Next Generation Networks (NGN) offer communications infrastructure administration of the MPLS network with lifecycle management that simplifies and automates configuration, monitoring, and troubleshooting; as well as service design, fulfillment, and performance analysis.

The Cost Efficiencies of MPLS

A key benefit of the virtualized MPLS infrastructure is that it can help utilities to cut costs in a number of areas. It assists in capital management by eliminating duplicate equipment and minimizing spares and inventory. As well, asset management is improved with a less complex infrastructure and management capabilities. Utilities also avoid early depreciation with planned, timely investments in strategic equipment.

Utilities have seen reduced operations and administrative costs of overlay networks, tools, and management systems by as much as 50 percent, according to industry studies. Based on the single network platform, organizations eliminate duplicate vendor support services and contracts, and optimize service provider contracts (and circuits). They minimize downtime with less maintenance and out of service conditions and reduce the potential for regulatory fines.

Applying MPLS to Real-World Smart Grid Challenges

Cisco Services help utilities to implement MPLS networks by providing CCIE® level architects, who bring experience and ideas from leading utilities around the world. Cisco works closely with utility operations teams to create business-fostered end-to-end architectures and detailed designs that are prerequisites to sound project implementation and integration. Using industry-proven methodologies, Cisco has helped utilities develop a wide variety of strategic solutions. Some recent onsite examples with Cisco customers include:

- **SONET/TDM to MPLS conversions:** Using AToM, the Cisco MPLS solution enabled maintenance of legacy TDM applications and circuits while introducing packet-based sub-networks for growth applications. Aging SONET terminals were decommissioned.
- **Phasor Management Unit (PMU) deployments:** Leveraging network virtualization and multicast, Cisco enabled PMU traffic evolution from postmortem analysis to real-time control, eliminating future network changes. The modularity of the design allowed migration of the utility’s infrastructure to occur over time, deferring capital and expense.
- **System protection:** Cisco MPLS enables Layer 2 traffic to be seamlessly carried across a utility wide area environment reliably and with extremely low latency.
- **Frame relay to MPLS migration:** The Cisco solution acted as a distributed frame relay switch, allowing a utility’s substations (which didn’t need upgrading) to maintain frame connections, while allowing those that needed advanced features to adopt MPLS. Frame relay data link connection identifiers (DLCIs) are mapped across the MPLS core, transparent to frame relay access devices (FRADs).

- **Making Ethernet WANs more reliable:** The Cisco MPLS solution replaced an unreliable, extensive, and hard-to-manage Ethernet network to substations with hierarchical virtual private LAN service (VPLS). Using MPLS, the environment was segmented and virtualized so that business operations could be reliably performed.

Why Cisco?

MPLS is being adopted by many utilities as a strategic WAN solution that provides a flexible, scalable framework to support expansion and change. Cisco is the leader in end-to-end communications solutions and standards development, bringing more than 30 years of industry networking experience to each utility project. It provides the design expertise, industry partnerships, and a portfolio of standards-based products and solutions to optimize MPLS within energy operations. These scalable, secure implementations support applications both today and well into the future, allowing operations managers to confidently plan for tomorrow's capabilities while continuing to maximize existing technologies.

To learn more about Cisco's smart grid solutions, contact your representative or visit our Connected Grid website.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA

MF/LW-18590 01/13