

SMART GRID NETWORK: MPLS DESIGN APPROACH

By Tom Hulsebosch, Dan Belmont, and Mike Manske

CREATING A NERC CIP COMPLIANT SMART GRID IP COMMUNICATION NETWORK

Energy and utility companies across North America are investigating, preparing, or deploying a variety of Smart Grid solutions. These substantial initiatives—Advanced Metering Infrastructure (AMI), distribution automation, substation automation, demand side management programs, and the like—are designed to improve the efficiency, capacity, and reliability of the electric grid and equip it for the 21st Century challenges of plug-in hybrid electric vehicles (PHEVs) and the growth of interruptible renewable energy such as wind and solar.

At the same time, utilities also must comply with tough security regulations related to protecting the Bulk Electric System. The North American Electric Reliability Corporation (NERC) has outlined cyber security requirements in the Critical Infrastructure Protection (CIP) standards. Eight CIP standards (CIP-002 to CIP-009) contain a number of activities and polices related to securing the Bulk Electric System.

THE NERC CIP STANDARDS REQUIRE UTILITIES TO IMPLEMENT COMPLEX NETWORKS IN ORDER TO PROTECT CRITICAL CYBER ASSETS AND THE RELIABILITY OF THE BULK ELECTRIC SYSTEMS IN NORTH AMERICA.

The NERC CIP standards require utilities to implement complex networks in order to protect Critical Cyber Assets and the reliability of the Bulk Electric Systems in North America. These standards include a very specific list of regulations and best practices for physical security, change management processes, logging practices, etc. Failure to comply could lead to profound penalties—potentially millions of dollars per violation per day. Utilities must comply with NERC CIP standards by the middle of 2009. Full compliance audits begin in 2010.

CRITICAL ASSETS AND CRITICAL CYBER ASSETS

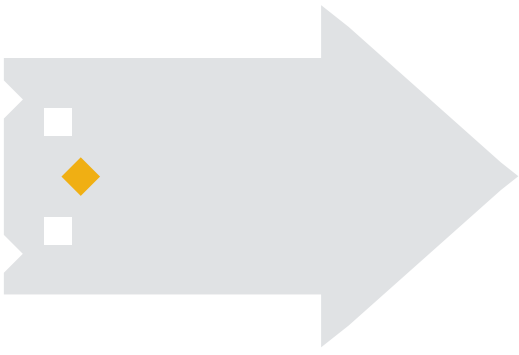
The NERC CIP standards define Critical Assets (CAs) as control centers, transmission substations, generation resources, or systems that integrate with the overall operation of the Bulk Electric System. In short, any asset that supports or could affect the overall reliability of the Bulk Electric System of North America is considered a CA.

If an asset is defined as a CA and the communication to this asset is either routable or accessible by dial-up, then the device is considered a Critical Cyber Asset (CCA) and is governed by the NERC CIP standards. While the NERC CIP standards outline best practices for securing CCAs, utility companies want to limit their exposure and liability from having CCAs. Defining substations as CCAs most likely will add additional costs and administrative overhead.

NON-ROUTABLE COMMUNICATIONS: WHAT IS THE ISSUE?

The NERC CIP standard (CIP-002) creates some gray areas around classifying substations as CCAs because of the interpretation around non-routable protocols. Within CIP-002, routable protocols are defined by protocols providing switching and routing as described by the Open System Interconnection (OSI) model Layer 3 (e.g., IP is a layer 3 protocol) or higher. This means that if a substation is considered a CA, any communication to the substation would need to be sent over Layer 2; otherwise, the substation would need to meet the NERC CIP standards (CIP-002 to CIP-009). But, implementing analog Layer 2 circuits to every substation is not a scalable solution. Compared to digital communication network alternatives, analog communication circuits have limited bandwidth and high error rates, and they are more expensive.

Utilities, then, face a dilemma: How do we build a flexible IP communication network for our Smart Grid solutions without creating a NERC CIP compliance problem that erodes the Smart Grid solution's potential savings and benefits?



WHAT ARE UTILITIES DOING?

When communication is required at a substation considered to be a CA, utilities typically take one of three approaches:

1. Removing all communication to the substation (no remote communication).
2. Reverting back to serial communication over frame-relay circuits or narrow band point-to-multipoint SCADA radios (Layer 2 only).
3. Enabling IP communications (Layer 3) and becoming compliant with the NERC CIP standards.

None of these approaches is perfect. Avoiding routable communications is not a practical, long-term solution to cyber security since IP routed networks are considered a best practice for designing networks. Many utilities, therefore, are implementing a combination of Layer 2 and Layer 3 communications circuits to ensure their Smart Grid solutions are compliant with the NERC CIP standards for CCAs. The problem is, even though frame-relay circuits are considered Layer 2, back-end administration at the Internet Service Providers (ISPs) network is Layer 3. The CIP standards, however, do not address telecommunications or ISP networks, so this is considered out-of-scope and, therefore, compliant within the NERC CIP standards for non-routable communications. Future versions of NERC CIP standards may eliminate the non-routable exception and extend into the telecommunications area. But, until these changes are made to the NERC CIP standards, utilities still must comply with the current standards in 2009, as audits will begin in 2010.

A DESIGN APPROACH: MULTIPROTOCOL LABEL SWITCHING

When CA communication is required, one network design approach is to implement a backbone using Multiprotocol Label Switching (MPLS) technology. This technology provides the layers of security and flexibility to meet regulatory security requirements. Its biggest benefit, though, is traffic segmentation with the use of VPNs. MPLS can provide point-to-point Layer 2 service to meet NERC CIP non-routable standards of today while providing full Layer 3 routing as the standards evolve.

MPLS OVERVIEW

Multiprotocol Label Switching systems provide many benefits over similar transport technologies, including traffic segmentation with VPNs, traffic engineering (TE), and end-to-end quality of service. There are three types of MPLS VPNs deployed in networks today: Point-to-point, Layer 2 (VPLS), and Layer 3 (VPRN). MPLS VPNs give network engineers the flexibility to transport and route several types of network traffic using the technologies of a MPLS backbone.

Point-to-point (Pseudowire)

Point-to-point MPLS VPNs employ VLLs (Virtual Leased Lines) for providing Layer2 point-to-point connectivity between two sites. Ethernet, TDM, and ATM frames can be encapsulated within these VLLs. Some examples of how point-to-point VPNs might be used by utilities include encapsulating TDM T1 circuits attached to RTUs or forwarding non-routed DNP3 traffic across the backbone network to the SCADA master controller.

Layer 2 VPN (VPLS)

Layer 2 (L2), or VPLS (Virtual Private LAN Service), offers a “switch in the cloud” style VPLS service. VPLS provides the ability to span VLANs between sites. L2 VPNs are typically used to route voice, video, and AMI traffic between substation and datacenter locations.

Layer 3 VPN (VPRN)

Layer 3 (L3), or VPRN (Virtual Private Routed Network), utilizes layer 3 VRF (VPN/Virtual Routing and Forwarding) to segment routing tables for each “customer” utilizing the service. The customer peers with the service provider router and the two exchange routes, which are placed into a routing table specific to the customer. Multiprotocol-BGP (MP-BGP) is required in the cloud to utilize the service, which increases complexity of design and implementation. L3 VPNs are typically not deployed on utility networks due to their complexity; however, a L3 VPN could be used to route traffic between corporate or datacenter locations.



TRAFFIC SEPARATION AND NETWORK SECURITY

One of the greatest benefits of MPLS is the ability to create virtual circuits to encapsulate Layer 2 traffic. One of the common protocols used today within the utility industry is DNP3, which is a Layer 2 non-routable protocol. While DNP3 traffic will pass through devices that have IP addresses assigned to them, it will be in a separate network segment with no IP connectivity; a Layer 2 connection from a substation directly to the SCADA Master Control System. Since the MPLS virtual circuit is provided by a telecommunications provider, according to the NERC CIP standards, it is out-of-scope and compliant with the standards.

With MPLS, utilities can create multiple virtual circuits at each substation to provide for IP services such as cameras, technicians' PCs, Voice over IP, and future DNP3 over IP traffic. The flexibility of MPLS VPNs provides utility companies the ability to utilize routable IP communication, along with being compliant with the NERC CIP standards for non-routable traffic. For IP traffic,

each substation can be provisioned on its own VPN to ensure that all communication between substations is separated and secure. With different MPLS VPNs at substations, the idea of trust zones for each substation is easily implemented with centralized firewalls, reducing overall implementation costs.

BENEFITS OF MPLS

The three major benefits of MPLS are consolidation, security/control, and resiliency.

Consolidation

Within utilities there are several types of networks deployed: AMI, SCADA, corporate, voice, etc. Each one of these networks is maintained and supported independently. Figure 1 illustrates the consolidation of several networks into a single MPLS network. MPLS enables consolidation of these disparate networks, which in turn lowers capital and operating costs while ensuring security among networks.

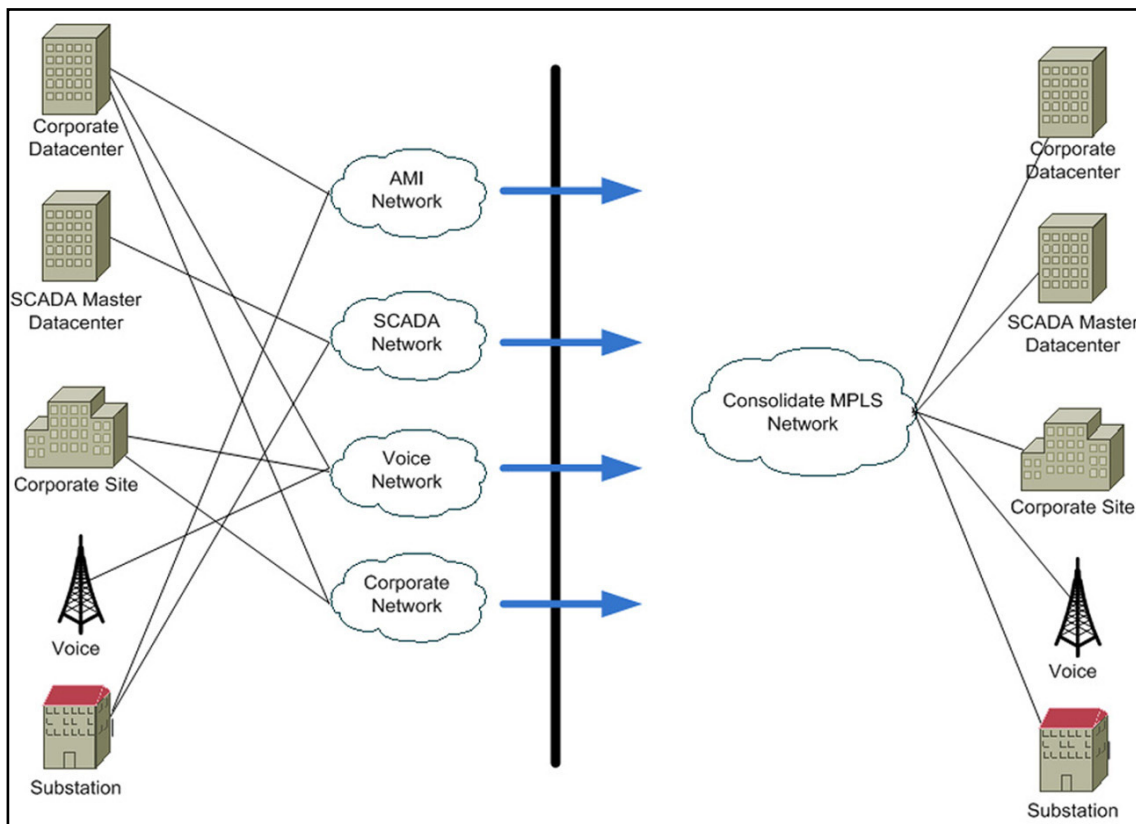
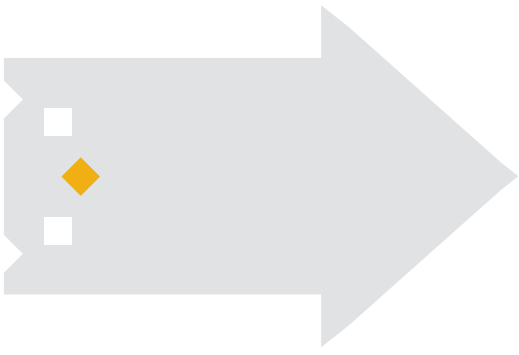


FIGURE 1 - MPLS CONSOLIDATION



Security/Control

With the strict NERC CIP standards that utilities must follow, security and control is extremely important and is required by industry regulations. MPLS delivers security and control through traffic segmentation. Traffic segmentation is possible by implementing multiple MPLS-based VPNs. AMI, SCADA, and substation traffic is segmented before traveling over the consolidated MPLS backbone. Segmentation of substation traffic protects and ensures security at other substations in the event one substation is compromised. Figure 2 illustrates the segmentation of AMI and SCADA traffic. In addition to security and control, moving to an MPLS network provides business benefits such as improved network availability, performance, and policy enforcements.

Resiliency

With SCADA and voice traffic running over a consolidated MPLS network, network availability becomes critical. MPLS provides network resiliency with fast reroute and traffic engineering. MPLS-based traffic engineering enables a fine-tuning of the network to deliver appropriate levels of services to prioritize SCADA traffic and guarantee its delivery to the SCADA master controller. Finally, in the event of a network node or link failure, MPLS provides sub-50 millisecond reroute and failover times.

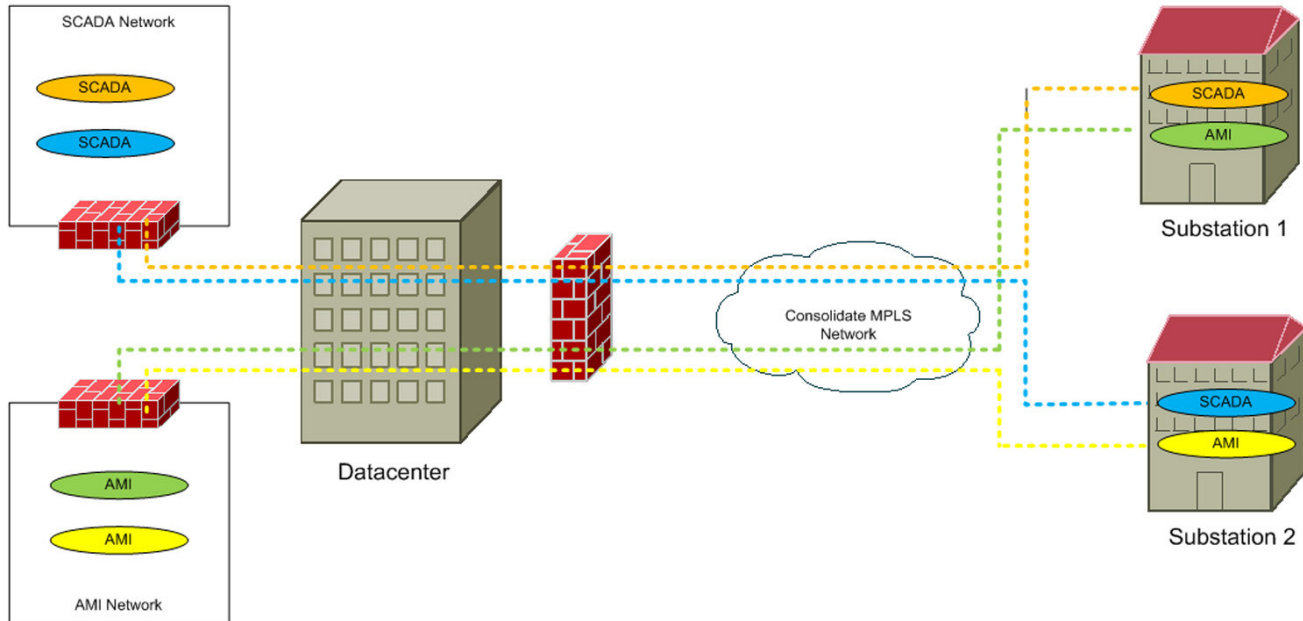
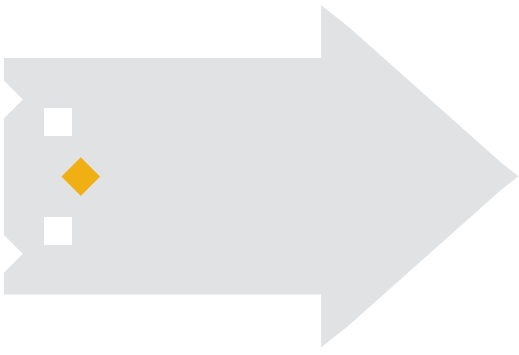


FIGURE 2 - NETWORK SEGMENTATION



POINT OF VIEW

PREPARING TODAY FOR EVOLVING REGULATION

Utilities have a number of options for complying with NERC CIP standards. Some are doing so at the cost of communication flexibility and efficiency, while others are looking into the future and designing their communication networks to address both today's security requirements and tomorrow's Smart Grid solutions. But, the NERC CIP standards will continue to evolve as new vulnerabilities and threats emerge, and just because a utility is complainant today doesn't mean it will be tomorrow.

It is important to remember that the NERC CIP regulations only apply to utilities' CAs; however, these regulations are best practices for protecting all network assets. While all substations will not be classified as CCAs initially, utilities with a conservative mindset will use many of the NERC CIP guidelines as best practices to guide physical security, change management processes, logging practices, and other activities across all substations and distribution automation devices. With regulatory bodies discussing the possibility of extending NERC CIP into distribution substations in the future, utilities that take this approach today will be in a strong initial position for bringing the rest of their substations into compliance, should that change in regulation occur.

West Monroe Partners helps energy and utility companies establish themselves at the forefront of building smarter, greener power grids. For more information, please contact Mike Manske at mmanske@westmonroepartners.com or Dan Belmont at dbelmont@westmonroepartners.com.

- West Monroe Partners is an international, full-service business and technology consulting firm focused on guiding organizations through projects that fundamentally transform their business. With the experience to create the most ambitious visions as well as the skills to implement the smallest details
- of our clients' most critical projects, West Monroe Partners is a proven provider of growth and efficiency to large enterprises, as well as more nimble middle-market organizations. Our more than 300 consulting professionals drive better business results by harnessing our collective experience across a range of industries, serving clients out of offices across the United States and Canada.