http:d2cigre.org

CONSEIL INTERNATIONAL DES GRANDS RESEAUX ELECTRIQUES
INTERNATIONAL COUNCIL ON LARGE ELECTRIC SYSTEMS

STUDY COMMITTEE D2
INFORMATION SYSTEMS AND TELECOMMUNICATION

2013 Colloquium
November 13-15, 2013
Mysore – KARNATAKA - INDIA

Paper Number : D2-01_07

Architecting a packet-based wide area network to support current, developing, and future utility use cases and applications.

R. IRONS-MCLEAN*

Cisco Systems

GB

SUMMARY

Electrical power grids continue to evolve to meet the challenges of standardisation and grid modernisation in order to enhance existing use cases [1] and applications, while simultaneously enabling new use cases driven by the concept of the smart grid. The addition of new technologies has the potential to allow a utility to realise a more stable, reliable, efficient and visible power grid capable of handling any type of communication flow.

Grid communications infrastructure often consists of multiple media types, including media such as pilot wire, microwave, radio, serial, and PDH/SDH. Traditional deployments often consist of multiple siloed networks with limited or no capability to exchange data between them. Because of changing system requirements, standardisation, and equipment end of life, these infrastructures no longer adequately support utility long-term needs. Many are built and operated for specific applications or solutions, making it more challenging to integrate new use cases and operational processes.

There is a steady increase in bandwidth consumption and any-to-any communication flows. Wide Area Measurement Protection and Control Systems (WAMPACS), adaptive relaying, situational awareness, video-based physical security, and AMI backhaul over the WAN, amongst other applications mean that TDM-based networks can no longer cost-effectively support these use cases. In addition regulations and standards such as NERC CIP and IEC 62351 compel utilities to enable better communications to support cyber and physical security, auditing and monitoring.

In response to these challenges, packet based systems allow utilities to not only meet operational goals but also enable the enterprise and operations applications to co-exist. The key to modernising and securing grid communications is to provide a common multi-service network which provides a platform for current and future requirements. For utilities replacing their TDM networks, MPLS is viewed as the strategic technology of choice and we shall consider requirements when designing packet networks for utilities using MPLS.

KEYWORDS

WAN, MPLS, IP, Packet, Management, Standards, Architecture, Timing, System Control, Protection.

Cisco Systems, 9-11 New Square, Bedfont Lakes, Feltham, TW14 8HA, UK
rironsmc@cisco.com

Industry challenges

Utilities face large increases in electrical consumption, with demand projected to grow by 70% to 32,000 TWh by 2035 [2]. This means an additional 5,890 GW capacity before 2035 which is more than the global installed capacity in 2011. At the same time we are seeing a shift in energy generation sources. Wind, hydro, bioenergy and solar PV will represent almost half the required capacity additions [2].

Globally there is an increase in distributed generation leading to a lack of visibility and control for power system operators at the distribution level, and leading to imbalance at transmission and generation levels. Coupled with the ageing utility infrastructure this leads to a decrease in reliability and an increase in operational costs. As a result the power industry is investigating new ways to implement, manage and control generation, transmission and distribution infrastructures, as well as rethinking the communications network to cope with these challenges as system control and substation automation use cases change.

Wide area network for system control and substation application use cases

Electric utilities are among the largest users of privately owned and operated wide area network infrastructures. These are built on a hybrid mix of fiber optics, microwave, power line carrier, a variety of licensed and unlicensed wireless, PDH/SDH, plus more recently packet-based technologies. Communication flow models have largely followed a one-way power delivery flow from generation to consumer. As a result most communication networks consist of multiple point-to-point circuits connecting substations to control centers for SCADA and EMS applications, and point-to-point circuits between substations for protection applications.

The introduction of packet has mostly been restricted to IT networks (although there are many implementations of SCADA over MPLS), while OT communications have largely remained on traditional TDM networks [3]. The industry is experiencing a steady uptake in TDM to packet migration due to a number of reasons including end of life of many TDM solutions, emerging standards such as IEC 61850, interoperability and cyber security [4]. Indeed CENELEC (2012) [5] specify the use of IP to future-proof grid communications. In addition utilities are consolidating networks on a common infrastructure as part of refresh cycles, to minimise operational expenditure, and to introduce new use cases.

The future grid wide area network

Electrical flow on the grid is becoming more transactional with multiple generation points. As such it is transforming into a two-way or any-to-any power delivery infrastructure where system balance is maintained by matching controllable resources with variations in load and supply. An efficient network infrastructure that enables, monitors and manages reliable communication among disparate control elements of the power grid is an essential component of this grid transformation.

Industry standards (primarily from the IEC) are driving towards an open standard, packet-based, interoperable communications network with a much greater emphasis on cyber security. The introduction of real-time applications like Remedial Action Schemes (RAS) or System Intergrity Protection Schemes (SIPS), technologies like Phasor Measurement Units (PMUs) and protocols like Sampled Values (SV) are also driving the need for enhanced timing capabilities across the grid. Coupled with GPS vulnerability concerns timing and synchronisation distribution over the WAN is also being introduced. Newer, advanced use cases are also driving the need for more bandwidth, multipoint connectivity, and less centralised architectures. As such we see a move away from the traditional grid architecture in *Figure 1*, towards the future architecture in *Figure 2*.

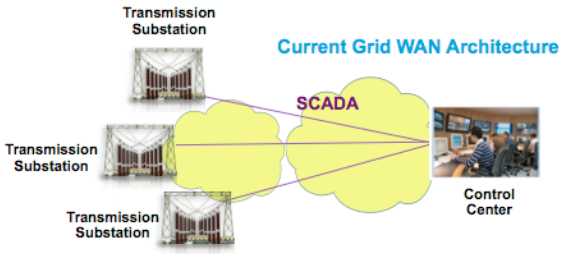


Figure 1 : Traditional Grid WAN Architecture

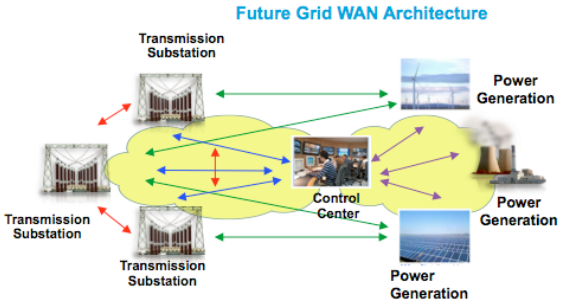


Figure 2 : Future Grid WAN Architecture

An architectural approach, consistent with industry and standards organisations (e.g. NIST, IEC, EPRI, CENELEC), networking companies, and also power vendors [6] is essential to understand the interdependencies and communications between systems that exist, but equally important to provide a seamless platform for future use case integration. An architectural process defines a set of artifacts required to describe a system so that it can be reproduced and maintained over its lifespan. These artifacts provide components, structure, interdependencies, and the guidelines determining the design and evolution over time. This is important as each utility may have subtly or very different requirements and WAN design will only reflect the use cases and services a utility wishes to deploy.

Starting from a reference model such as Cisco GridBlocks [7], determining current and future use cases and applications, architectures can be derived to focus on requirements of a specific utility (*Figure 3)* including the WAN requirements.

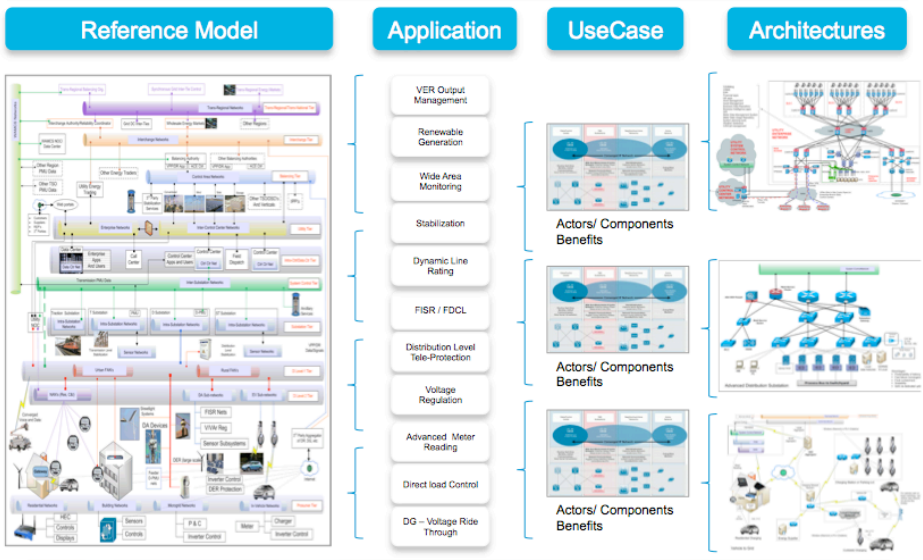


Figure 3 : Reference model to utility-specific architectures

The packet WAN must support multiple use cases. Common ones are identified in *Figure 4*.

Type	Use Case	Data Flow
Monitoring, Control, & Protection	SCADA (DNP3, Modbus, T101) serial tunneling with Raw Sockets	Substation <> Control Center
	SCADA (DNP3-IP, Modbus-TCP & T104) IP transport	Substation <> Control Center
	Wide Area Measurement Systems (WAMS) with C37.118.2 and IEC 61850-90-5	Substation <> Control Center
	Traditional Teleprotection (Current Differential) with legacy interfaces	Inter-substation
	IEC 61850 Teleprotection (Current Differential) with Ethernet interfaces	Inter-substation
	System Integrity Protection Schemes (SIPS)	Substation <> Control Center
Security & Management	Substation physical security	Substation <> Control Center
	Network management and security management	Substation <> Control Center
Workforce Enablement	Substation remote workforce management	Substation <> Control Center
	Remote engineering access to substation devices	Substation <> Control Center
	Wireless Remote Workforce Enablement	Substation <> Control Center
Transport	Field Area Network (FAN) aggregation	FAN <> Substation <> Control Center
IT	Multiple data and voice services	Any to Any

Figure 4 : Common utility WAN use cases

Many of these use cases such as SCADA have been deployed over production packet WANs for some time and communication requirements are proven. Following are developing and future use cases for packet WAN implementation and the design requirements which should be considered when architecting a next generation packet network.

Teleprotection over packet

Teleprotection is often viewed as the most stringent application on the WAN with key considerations:

- Communication network latency typically expected to be 4 - 16ms (but not set in stone, with IEC61850 suggesting 10ms)
- Delay asymmetry and packet delay variation impact differential schemes without GPS assistance. Tolerable jitter depends on the protection relay vendor and is typically in the range of 0.25 – 1.0 milliseconds
- Relay attachment requirements: C37.94, E1/T1, X.21, E&M, RS422, and recently Ethernet
- Transport requirements include circuit emulation (CESoPSN, SATOP) for traditional teleprotection and EoMPLS for IEC61850 based teleprotection, frequency synchronisation (Synch-E, 1588 PTP) of MPLS devices for TDM transport, and traffic engineering to ensure path symmetry for non-GPS assisted differential schemes.

Dependent on the protection relay there are a number of solutions as demonstrated in *Figure 5*. With the addition of traffic replication technologies we can see zero packet loss implementations for protection across the WAN. Teleprotection is successfully deployed across live Cisco MPLS operational networks including BKK (Norwegian Distribution Operator), with full packet network interoperability testing (current differential and distance schemes) without failure in collaborative testing between Cisco and Siemens.

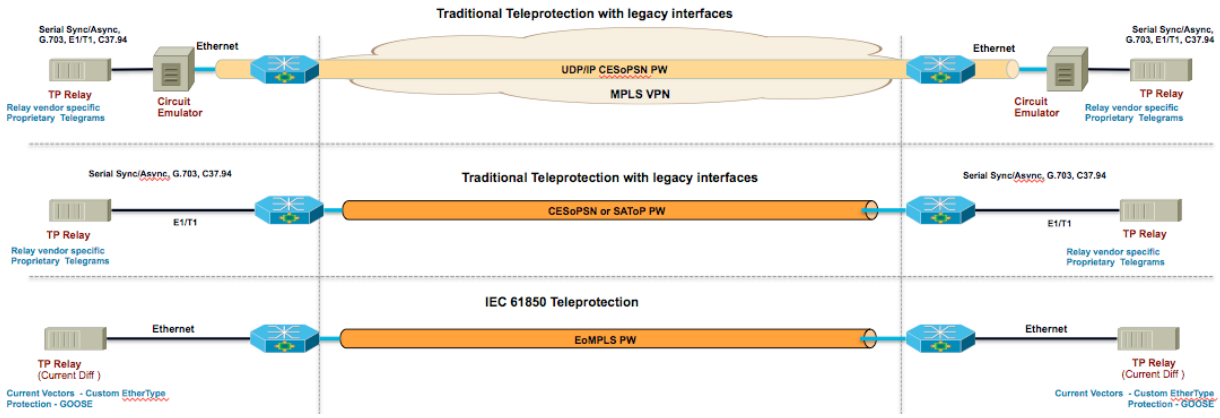


Figure 5 : Teleprotection deployments across a packet WAN

IEC 61850 Edition 2

Part 90-5 defines a way of exchanging synchrophasor data between end-points and control applications which supersedes C37.118.2. For the first time we have recommendations for 61850 traffic leaving the substation with defined routable Layer 3 profiles for IEC 61850-8-1 GOOSE and IEC 61850-9-2 SV packets on top of IP unicast/multicast.

These routable packets can be used to transport general IEC 61850 data and not just synchrophasors. From a WAN perspective this now introduces the need for multicast and multicast security mechanisms to be included in the design. *Figure 6* shows a comparison of traditional and 61850 based synchrophasor requirements.

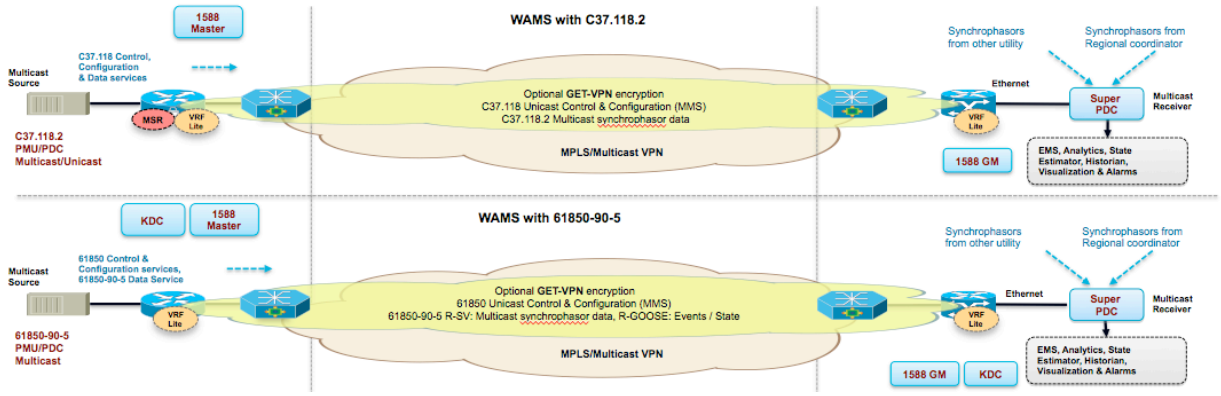


Figure 6 : PMU/Synchrophasor transport across a packet based network

Next generation Energy Management Systems

Power vendors are integrating synchrophasor 'measurement-based' analytics with 'model-based' stability analytics to create the next generation Energy Management System, augmenting SCADA based state estimation with real-time synchrophasor data. PMU measurement-based methods monitor grid stability in real-time with model-based techniques providing the predictive 'what if? analysis' component.

Bandwidth may also increase. The approximate bandwidth for C37.118 synchrophasor data (20 measurements per PMU) at 60 samples per second generated by 10 PMUs is around 440kbps. With standards evolving from C37.118.2 to IEC 61850-90-5 based transport using secure multicast, SV at 80 samples per second traffic can reach 5-6Mb per stream.

Network requirements include unicast and multicast, layer 3 VPN technologies, precise timing distribution (Synch-E and 1588 PTP), multicast and a Group Domain of Interpretation (GDOI) server for key distribution.

PMUs with multicast architectures have been implemented over Cisco MPLS networks with NASPInet and WECC in North America.

Wide area monitoring, control and protection schemes

Utilities are now moving beyond monitoring and are working on projects which tie together monitoring, control and protection functions to provide real-time adaptive control and protection. The use of system-wide information and communication of selected local information to a remote location to counteract the propagation of large disturbances is seen in RAS, C-RAS and SIPS.

Cisco have worked with Southern California Edison on their C-RAS project focused on adaptive generator shedding based on a pre-fault calculation using on-line power system information. This results in closed loop control between PMUs at substations, Control Center and IEDs at the power plants. Results demonstrated design considerations including round trip delay latencies from substations to generator plant is <=38ms including encryption.

These projects mean specific requirements must be designed into the network including L2TPv3, EoMPLS, 61850 90-5 tunneling, multicast, GDOI key server for key distribution, Synch-E and 1588 PTP (*Figure 7)*.

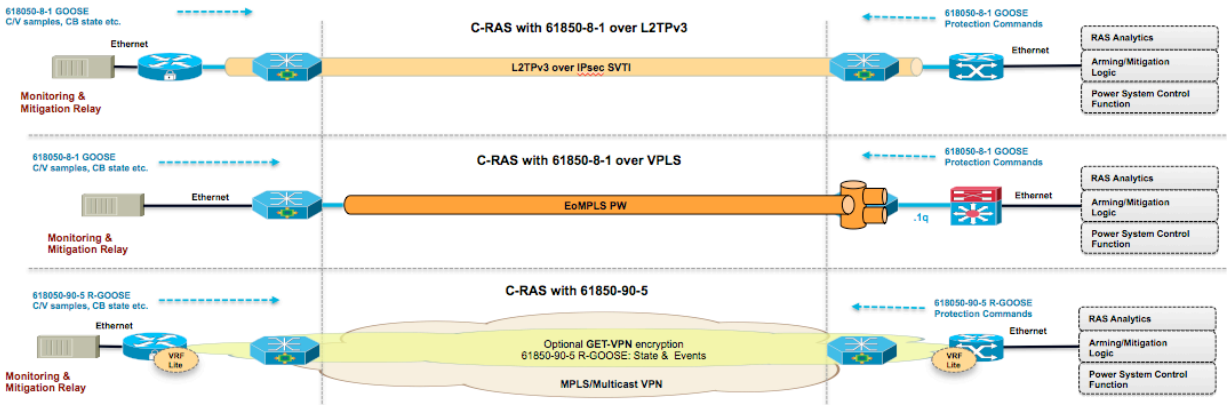


Figure 7 : Centralised Remedial Action Schemes across a packet network

Design principles – key network requirements

Based on the requirements of traditional and emerging utility applications a packet architecture must deliver many of the features of traditional communication mechanisms, while introducing new enhanced features. It should provide a multiservice and multi-vendor environment with the highest levels of quality, reliability, scalability and cost-effectiveness**.** The key is to meet application performance requirements (whether from standards such as IEC 61850, or utility defined) or exceed them with the introduction of new technologies. As a minimum, when architecting a packet WAN the following must be met:

- Determinism – guarantee mission critical traffic meets latency and jitter bounds, particularly when looking at applications such as current differential teleprotection.
- Path selection control – provide symmetrical forward and return paths, pre-determined primary and back up paths, or dynamic path selection dependent on use case.
- Security – traffic isolation via logical service virtualization between Operational and IT traffic, and between different traffic types. Firewalling, encryption, and intrusion prevention/detection.
- Resiliency - high availability at the network, transport, and service layers, as well as at communication device level.
- Traffic engineering - specify paths to avoid congested or bad links. Introduction of traffic replication (single stream duplicated via two network paths to remote destination) to provide zero packet loss on the WAN in the event of network path failure or reconvergence.
- Ease of Operations - OAM tool kit similar to SONET/SDH, plus a comprehensive NMS for network management, provisioning, assurance and security.
- Timing and synchronisation distribution - GPS vulnerability concerns are forcing consideration of IEEE 1588 PTP and Synch-E over the WAN.
- Multiple traffic type support - ability to transport legacy/traditional TDM traffic as well as packet based data.

Selection of packet transport

MPLS is a recommended option for next generation packet WANs for a number of reasons:

- OPEX forcing infrastructure convergence for better utilisation of fiber and microwave assets, driving the need for virtualisation. MPLS enables this virtualisation with advanced L2 and L3 VPN technologies.
- Legacy/traditional TDM, serial interfaces, and industry specific interfaces like C37.94 will exist for many years. MPLS supports the transport of this traffic with pseudowire based circuit emulation
- Packet solutions involving mixed packet transport technologies (like MPLS core with Ethernet or IP edge) are operationally complex due to multiple control planes and OAM translation. End-to-end MPLS across the transport infrastructure reduces the time to

deploy OT and IT services by separating transport from service operations, and simplifying the operational process with single touch point service enablement and contiguous OAM.

- Some industry specific use cases (like current differential teleprotection) require symmetric forward and return paths for time synchronised measurements. MPLS traffic engineering enables explicitly routed paths through an equal-cost multi-path (ECMP) network.
- Security - MPLS provides full address and routing separation as in traditional Layer 2 VPN services. It hides addressing structures of the core and other VPNs, and penetration tests [8] show it is not possible from the outside to intrude into the core or other VPNs abusing the MPLS mechanisms. It is also not possible to intrude into the MPLS core if it is properly secured.
- Longevity/extensibility – MPLS has been extensively deployed across multiple industries including service provider, finance, government and utilities and we see continued investment in the communications industry.
- It can be implemented end to end across a network.

MPLS/IP and/or MPLS TP?

- The MPLS transport profile (TP) is not a standalone technology, rather it is a subset of MPLS/IP.
- MPLS/IP and MPLS-TP each have their technical merits and trade-offs as a transport technology in a utility environment.
- MPLS-TP is more 'SONET/SDH-like' in terms of operational traffic (and OAM capabilities today) and may appeal to a utility comfortable with transport operations and continuing to support existing services.
- MPLS/IP is much more mature and flexible, and is well suited to support both existing and advanced smart grid use cases over a common multiservice network.
- A network platform should support both MPLS/IP and MPLS-TP to allow for a mixed use case environment to meet all utility requirements.

System Overview

High level architectures for an MPLS based communications system are shown in *Figure 8* (substation to control centre) and *Figure 9* (substation to substation).

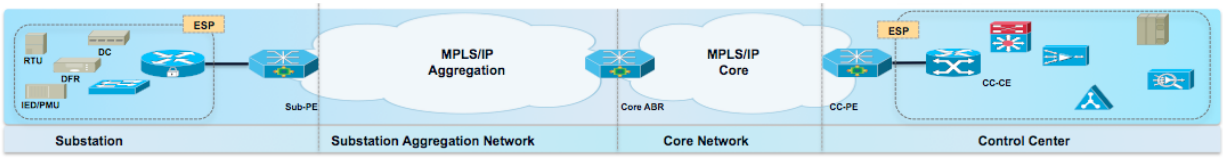


Figure 8 : High level substation to control centre packet architecture

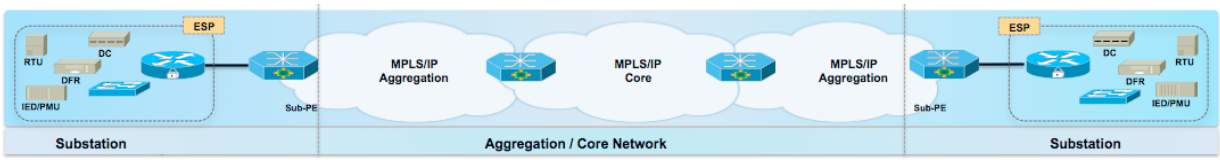


Figure 9 : High level substation to substation packet architecture

The design considerations must also include a number of key elements to ensure application and use case performance.

Quality of Service (QoS)

Traffic marking, classification and prioritisation are essential design elements to ensure application service level requirements are met. The goal of end-to-end QoS is to control and predictably service a variety of network applications and traffic types in an upstream and

downstream direction. Implementing QoS guarantees complete control of resources and allows co-existence of several traffic types (such as network management and security management) with mission-critical traffic (SCADA, PMU, protection). A proper QoS design mitigates any loss of mission-critical traffic and also ensures the efficient utilisation of available resources for various other applications by:

- Supporting dedicated bandwidth
- Reducing loss characteristics
- Avoiding and managing network congestion
- Shaping network traffic
- Setting traffic priorities across the network

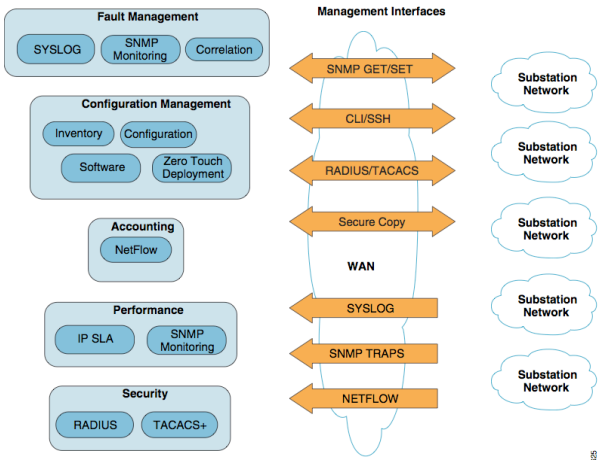
QoS is particularly important for networks that need to transport loss, latency, and jitter-sensitive data, especially in cases where there is a limited amount of bandwidth. A QoS model for the next generation packet WAN is demonstrated in *Figure 10.*

Category	Traffic Class	PHB	Substation Network Tier			Wide Area Network Tier		Control Center Network Tier	
			Process Bus Station Bus	Multiservice Bus	Substation CE	Substation PE Core & Agg. Nodes Control Center PE		Control Center CE	Control Center LAN
			802.1P	802.1P	DSCP	DSCP	MPLS EXP	DSCP	802.1P
Network Infrastructure	Network Management	AF	7	7	56	56	56	56	7
	Network Control Protocols	AF	6	6	48	48	6	48	6
Protection & Control	Protection Intra-Substation	EF	4	NA	NA	NA	NA	NA	NA
	Teleprotection	EF	4	NA	NA	NA	4	NA	NA
	WAMPC – Protection Traffic SIPS / RAS – Protection Traffic	EF	4	NA	32	32	4	32	4
Synchronization Distribution	PTP 1588 Telecom Profile	EF	NA	NA	46	46	5	46	5
	PTP 1588 Power Profile	EF	5	NA	NA	NA	NA	NA	NA
Monitoring	SCADA WAMS WAMPC – Monitoring Traffic SIPS / RAS – Monitoring Traffic Situational awareness State Estimation	AF	3	3	24	24	3	24	3
Physical Security	Surveillance Video / CCTV	AF	NA	2	16	16	2	16	2
	Electronic access control	BE	NA	0	0	0	0	0	0
Workforce Enablement	VoIP / Telephony	EF	NA	5	46	46	5	46	5
	Remote Engineering Access	BE	0	0	0	0	0	0	0
	Remote Workforce Management	BE	0	0	0	0	0	0	0
Transport	FAN Backhaul	AF	NA	NA	8	8	1	8	1

Figure 10 : Recommended utility QoS model for WAN use cases

Operations, Administration and Management/Maintenance

A general view of network management functions for a utility network is shown in *Figure 11* following the Fault, Configuration, Accounting, Performance, Security [FCAPS] model.



Specifically to the WAN an OAM design should include both service and transport elements with protocols serving two distinct functions. The service OAM is a service-oriented mechanism for operating and managing the services transported over the smart grid. It is provisioned at touch points associated with the end-to-end service, is used for monitoring liveliness and performance management of the service, with a primary purpose of understanding what the service is doing. The transport OAM is a network-oriented mechanism for operating and managing the network infrastructure. It is ubiquitous in network elements, is used for monitoring liveliness and performance management of the transport mechanisms that carry

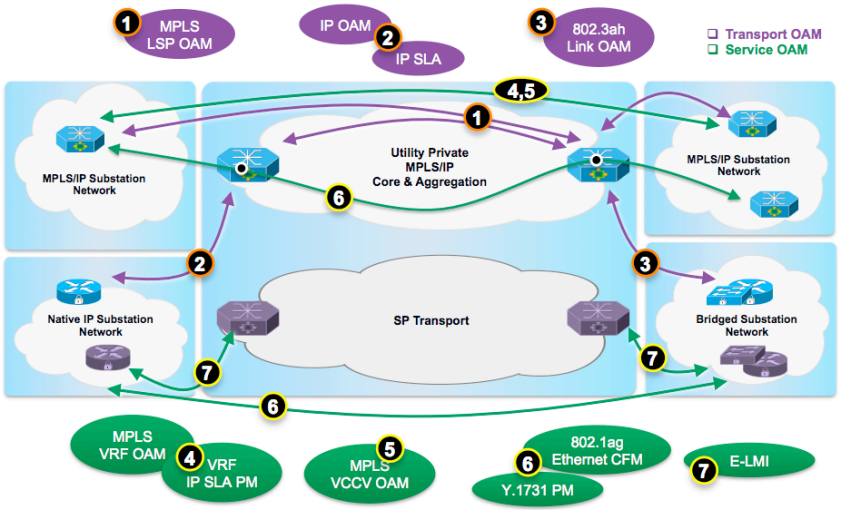


Figure 11 : OAM for packet WAN

services in the smart grid, with a primary purpose to know what the transport entities (MPLS LSP, Ethernet VLAN) are doing. *Figure 12* shows the various design element considerations for OAM on a packet network.

Timing and Synchronisation

Precise timing and synchronisation for time of day and frequency is required to ensure that devices connected to the grid and the communications networks have accurate clocks. Accuracy of the clocks is measured relative to a national standard, and can vary from an order of milliseconds to microseconds, depending on the application. Historically millisecond and tens of microsecond accuracy has been provided by SNTP and IRIG-B amongst other mechanisms for clock redistribution. However, newer applications such as PMUs and protocols such as 61850 SV require microsecond accuracy. Accurate clocks enable sophisticated analysis of real-time and post-disturbance faults and events within a short amount of time. This leads to faster and more reliable fault isolation and resolution, and better planning of transmission resources on the electric grid.

GPS is used to provide an accurate time reference for redistribution, however when GPS is not available the system cannot operate as intended for long, and therefore vulnerabilities of the GPS have become a major concern [9]. Alternative methods for clock redistribution design are being considered. A packet based WAN provides the ability to introduce end-to-end architectures for clock redistribution based on non-GPS time source references, with the ability to use GPS for redundancy. The 1588 PTP precise timing protocol can deliver end-to-end time and frequency across a WAN and into the substation with protocol translation between layer 2 and layer 3 transport and power profiles. Synch-E can be used to mitigate clock drift on the core MPLS WAN devices. A high level architecture is shown in *Figure 12*.

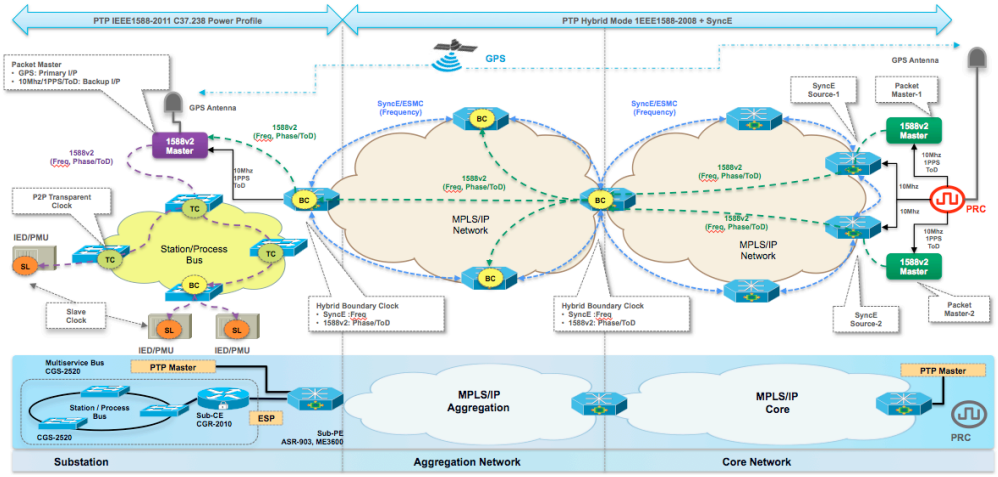


Figure 12 : WAN Architecture for precise timing distribution

Security

A security reference architecture offers guidance on deployment of grid-specific applications, as well as providing a framework for designing and implementing comprehensive management and security solutions across the grid, all of which are essential in a multi-service environment. The security considerations for WAN design should include the following principles:

- Access Control: Authentication and authorization of all personnel and devices
- Data Confidentiality and Privacy: Data privacy and data integrity for all operational and control data must be ensured (SCADA, Automation, Protection, etc.)
- Threat Detection and Mitigation: Protection of all critical assets
- Integrity of Platforms and Devices: Secure devices over the entire life-cycle

Conclusions and summary

The electrical power industry is seeing a shift of WAN design from TDM to packet networks due to a fundamental shift in use cases and applications, in addition to end of life equipment and utility OPEX planning. New industry requirements such as IEC 61850 are defining Layer 3 unicast and multicast encapsulation for advanced applications, GPS vulnerability concerns are driving the need for time synchronisation across the WAN, and the communication flows of applications are moving from a point-to-point to an any-to-any model.

Utilities have been deploying MPLS and other packet based communications networks for some time, but traditionally for IT use cases. More recently the shift has been to deploy OT applications over an MPLS WAN. However just creating an MPLS WAN is not an answer to successfully transporting many use cases such as teleprotection and PMUs. The WAN architecture needs careful design consideration to cope with multiple different application reqirements across the same infrastructure and must have appropriate QoS, multicast, timing and synchronisation, security, OAM, redundancy, reconvergence and resilience mechanisms. A packet MPLS WAN supports the needs of the power grid, maximizing ROI for infrastructure investments by virtualising the transport and capping investment in legacy networks. The technology exists today to transport any power application successfully across an MPLS packet WAN. It is no longer a technology challenge, but an education and testing challenge to ensure the successful migration onto a multiservice packet WAN.

BIBLIOGRAPHY

[1] R. Malan & D. Bredemeyer. Use Case Definition. Functional Requirements and Use Cases, (2001) http://www.bredemeyer.com/pdf_files/functreq.pdf

[2] International Energy Agency (2011) World Energy Outlook Report. http://www.worldenergyoutlook.org

[3] UTC (2012). Managing an IP/MPLS Utility Network–It's Simpler Than You Think! http://www.utc.org/event/webinar-managing-ipmpls-utility-network–it's-simpler-you-think

[4] Cisco (2013). White Paper. Multiprotocol Label Switching for the Utility WAN http://www.cisco.com/web/strategy/docs/energy/mpls_wp.pdf

[5] CENELC (2012). Smart Grid Reference Architecture. http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/xpert_group1_reference_architecture.pdf

[6] M. Braendle & S.A. Kunsman. ABB White Paper. 'Balancing the Demands of Reliability and Security Cyber Security for Substation Automation, Protection and Control Systems

[7] Cisco Gridblocks Reference Model. http://www.cisco.com/web/strategy/docs/energy/gridblocks_ref_model.pdf

[8 & 9] Cisco Systems. White Paper. Security of the MPLS Architecture http://www.cisco.com/en/US/tech/tk436/tk428/technologies_white_paper09186a00800a85c5.shtml#wp31502

[10] Symmetricom (2013) Power Utilities Mitigating GPS Vulnerabilities and Protecting Power Utility Network Timing