MISSION-CRITICAL COMMUNICATIONS NETWORKS FOR POWER UTILITIES

ENABLING RELIABLE TRANSPORT FOR TELEPROTECTION

APPLICATION NOTE

Alcatel·Lucent

ABSTRACT

As power utilities worldwide embark on smart grid projects such as grid modernization, substation automation, distribution automation and advanced metering infrastructure, they face the challenge of migrating legacy mission-critical traffic from TDM-based transport networks to new IP/MPLS-based communications networks. Legacy mission-critical applications, particularly teleprotection applications, demand stringent and deterministic transport. This application note explains how an Alcatel-Lucent IP/MPLS network can help network operators to meet this challenge and engineer the network to meet their requirements.

TABLE OF CONTENTS

INTRODUCTION

Power utilities worldwide are at different stages of considering, planning and deploying new communications networks in preparation for smart grid deployment. These efforts are driven by various needs: from simply making the power grid more reliable (avoiding blackouts), to coping better with the challenges of renewable energy and electric vehicles, to improving the quality of power (eliminating voltage surges and brownouts).

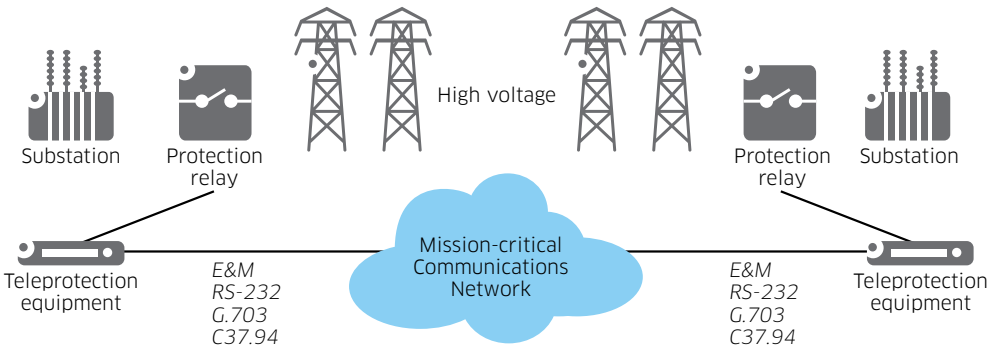
The smart grid applications include new supervisory control and data acquisition (SCADA) applications based on **IEC 60870-5-104** [6], Distributed Network Protocol, **Version 3 (DNP 3)** [4] or **Modbus**; synchrophasor systems for wide-area monitoring, and video surveillance to strengthen physical security. However, the grid still depends on already-deployed mission-critical applications for its daily operation. The most prominent of these is teleprotection[1].

Because electricity is the bedrock of modern society, it is vital to employ all possible means to avoid major outages. Teleprotection systems, typically installed in high-voltage transmission grids where distances are usually greater than in distribution grids, play a critical role in preventing instability in the grid and damage to expensive substation equipment. Teleprotection systems monitor conditions on transmission lines and coordinate tripping of the transmission lines to quickly isolate faults.

A teleprotection system usually has two components: a protection relay, which executes the actual switching; and teleprotection equipment, which is the interface to the mission-critical communications network (see Figure 1).

Teleprotection systems rely on the communications network for real-time exchange of status information and commands between teleprotection equipment. To ensure the power systems are properly protected, the teleprotection messages must be reliably transferred with tightly-controlled latency.

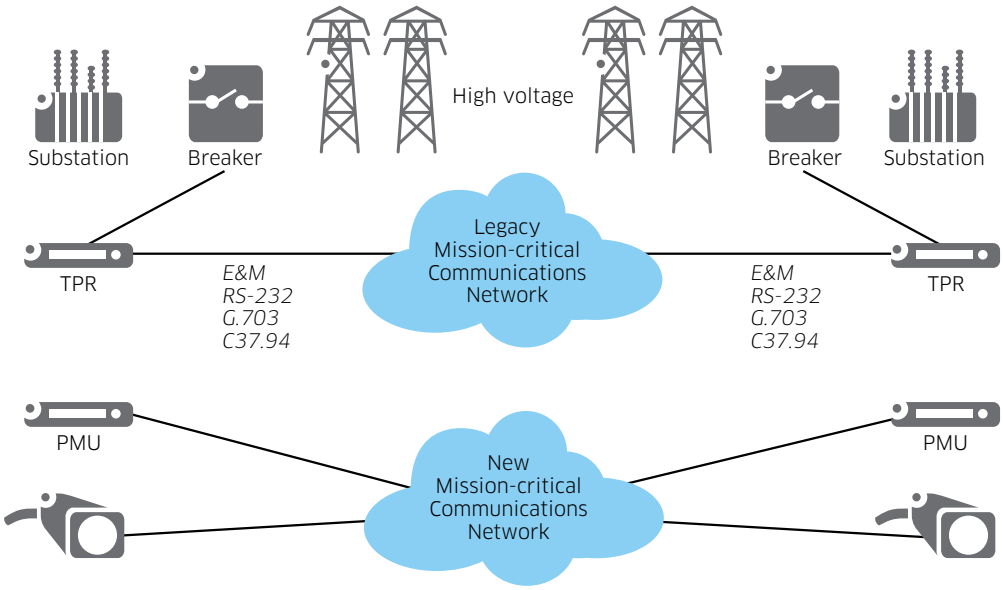
Figure 1. A typical teleprotection system in a mission-critical communications network



1 For more information on teleprotection, please see Dominique Verhulst, **Teleprotection Over Packet Networks** [14].

A traditional approach to modernize power utilities' telecommunications infrastructure is to deploy two networks. In this architecture, new IP/Ethernet-centric traffic is carried over the new mission-critical communications network. Legacy mission-critical applications remain on the already-deployed network, which typically uses older TDM multiplexor and optical SONET/SDH equipment (see Figure 2).

Figure 2. A network architecture with two parallel mission-critical communications networks



In this two-network architecture, there are multiple communications network elements deployed in the substation. In the legacy network, TDM and optical SONET/SDH equipment continue to transport legacy mission-critical traffic. In the new network, a new substation router is required.

In this situation, network operators require a large variety of network equipment and associated network managers plus multiple sets of hardware spares. This architecture incurs significant OPEX. Moreover, TDM and SONET/SDH equipment is generally at end-of-life or only a few years from it, further complicating the task of maintaining the older network.

To optimize operational efficiency and minimize costs as well as be ready for the future, many power utilities plan to deploy a new network to carry both new and legacy mission-critical traffic. This converged communications network can carry a combination of application traffic — old and new, mission-critical and best-effort — over the same network infrastructure without compromising performance.

ALCATEL-LUCENT IP/MPLS PORTFOLIO FOR A CONVERGED MISSION-CRITICAL NETWORK

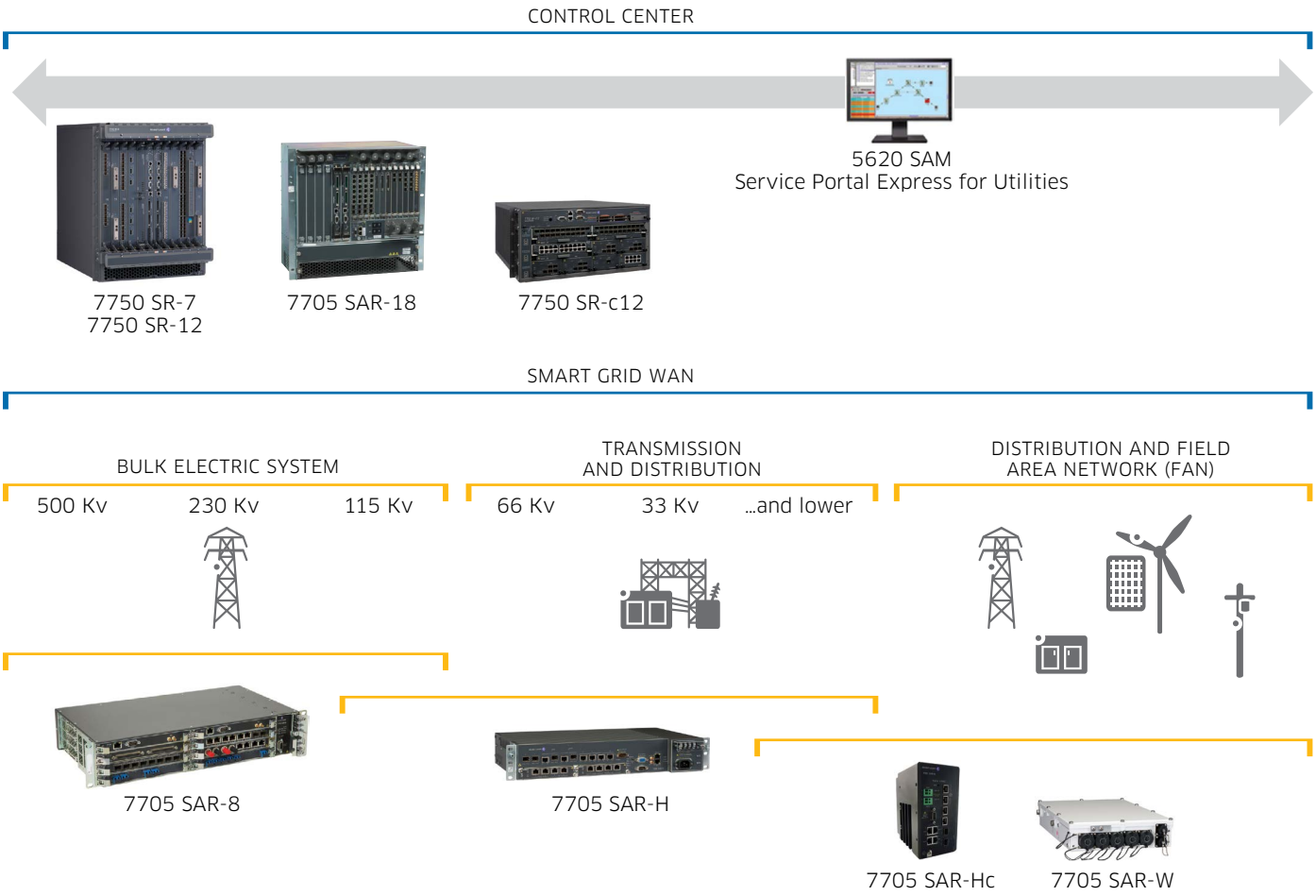
The most promising network technology for a converged network is IP/MPLS. An IP/MPLS network fulfills all convergence requirements, including network resiliency, quality of service (QoS), security and manageability[2]. For these reasons, it has become the technology of choice for new mission-critical converged networks.

2 For a detailed discussion of this subject, please see Alcatel-Lucent, **Deploying IP/MPLS Communications Networks for Smart Grids [1] and Alcatel-Lucent, MPLS for Mission-Critical Networks** [2].

The Alcatel-Lucent IP/MPLS product portfolio for a converged mission-critical network is very extensive with different capacities and form factors to fit various parts in the grid. All the products share the same Service Router Operating System (SR OS) heritage, which optimizes network design, configuration, maintenance and training.

Figure 3 shows an overview of the **Alcatel-Lucent IP/MPLS portfolio** for a mission-critical power utilities network.

Figure 3. Alcatel-Lucent mission-critical IP/MPLS solution for power utilities



To smoothly migrate legacy applications to a converged network, the IP/MPLS router must support a wide range of legacy interfaces. The **Alcatel Lucent 7705 Service Aggregation Router** (7705 SAR) can be equipped to natively support commonly deployed legacy interfaces, including E&M, FXS/FXO, RS-232, X.21, ITU-T G.703 and IEEE C37.94 [7]. This capability allows operators to seamlessly migrate TDM traffic to IP/MPLS without disrupting daily operations.

TELEPROTECTION OVER AN IP/MPLS NETWORK

Considerations and misconceptions

Migration of legacy mission-critical applications such as teleprotection, SCADA and Land Mobile Radio (LMR) requires an understanding of how TDM circuits are transported over IP/MPLS in order to render the same level of performance as in the legacy network. This is particularly important for teleprotection because it requires the most stringent QoS of all legacy mission-critical applications.

IP/MPLS is often incorrectly perceived as connection-less IP-technology that can provide data transport but only with best-effort QoS. While this is true for an IP-only network, an IP/MPLS network provides traffic engineering that renders the network connection-oriented, predictable and deterministic.

Another concern about using IP/MPLS networks for teleprotection is the notion that the statistical nature of packet networks will adversely impact the performance of teleprotection systems. Because the IP/MPLS network uses a label switched path (LSP) to transport other applications, including video surveillance and best-effort LAN, advanced and flexible traffic management capability is crucial to guarantee deterministic end-to-end QoS, including tightly-controlled jitter.

A major concern is how an IP/MPLS network can meet the strict latency requirements for teleprotection commands to be exchanged between TPRs at two transmission substations. It is imperative to guarantee the delay, called transmission time in **IEC Recommendation 60834-1** [5], the industry standard for performance and testing of teleprotection equipment.

The doubts about IP/MPLS usually concern the ability to guarantee low-latency service. The following section explains how TDM traffic is transported over an IP/MPLS network using Circuit Emulation Service over Packet Switched Network (CESoPSN) TDM pseudowire[3], and how delay is incurred and can be optimized.

Circuit Emulation Service

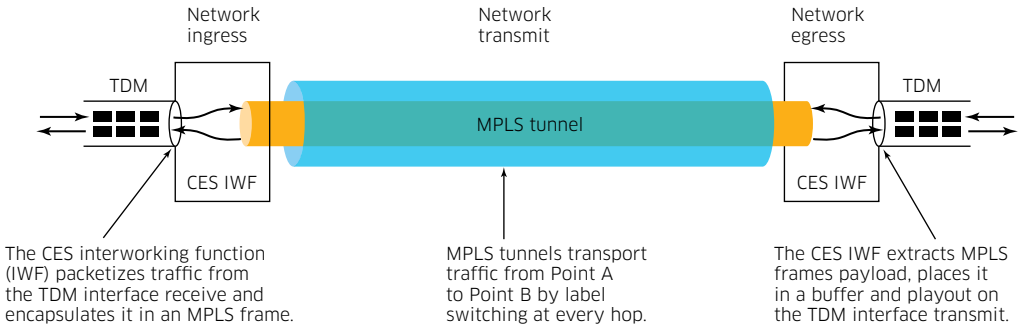
An IP/MPLS network uses a Circuit Emulation Service (CES) to migrate traditional teleprotection applications. The key design consideration for supporting teleprotection is how to minimize latency.

The latency for TDM traffic consists of packetization delay at network ingress, network transit delay, and jitter buffer/playout delay at network egress. To address these issues effectively and provide the most optimized delivery performance, IP/MPLS routers need to allow network operators to fine-tune packetization delay and jitter buffer/playout delay based on their network topology.

Operating with legacy TDM networks and services is straightforward when using MPLS CES functionality. CES delivers the same quality of experience as the existing TDM network infrastructure with the same level of predictability. The MPLS network has a CES interworking function that ensures all information required by a TDM circuit is maintained across the packet network (see Figure 4). This functionality provides a full transition to the packet network while providing TDM service continuity.

3 IETF. RFC 5086. **Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN)** [9], December 2007.

Figure 4. Circuit Emulation Service



The major delay contributors for TDM CES are:

- TDM packetization at network ingress
- MPLS label switching during network transit (at every hop)
- TDM playout delay at network egress

TDM packetization

The packetization process is shown in Figure 5. The ingress MPLS router receives parcels of digital information at a fixed interval (e.g., 1 byte every 125 microseconds for a DS0 circuit). The router encapsulates the digital information in an MPLS frame that has two labels: a tunnel label that specifies an LSP and a service label that specifies a pseudowire circuit associated with the particular CES service. It is also important that the EXP field, a 3-bit field, is marked appropriately, reflecting an expedited class of QoS. The actual EXP value depends on the network QoS policy set by the network operator.

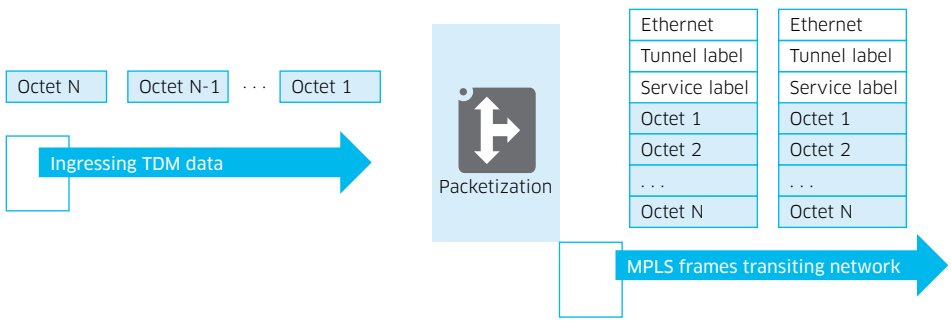
The operator has two choices: to package this byte in an MPLS frame and transmit it across the network immediately with practically no packetization delay (other than that incurred by hardware processing); or to wait until a pre-configured number of bytes arrive before transmitting them all together in one MPLS frame, thereby incurring more packetization delay.

Smaller payload sizes lead to a higher number of MPLS frames per second, resulting in higher bandwidth but lower packetization delay and, ultimately, lower end-to-end delay. Larger payload sizes with a lower number of packets per second result in lower bandwidth but higher packetization delay and higher end-to-end delay.

The packet payload size is configurable.

It is important to note that the more delay that is incurred, the lower the transport overhead.

Figure 5. Packetization process at ingress



In the case of an analog interface such as E&M, the router needs to digitize the analog signal with pulse code modulation (PCM) before packetization. The PCM algorithms commonly used are μ-law in North America and A-law outside North America.

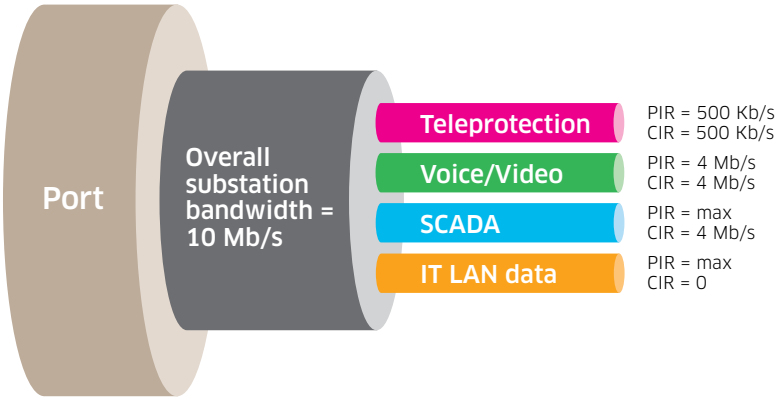
MPLS Label switching during network transit

Transit delay, incurred when a packet traverses the network hop by hop, is usually familiar to operators. The delay at every hop is negligible, usually in the range of tens of microseconds.

After the TDM traffic is packetized, the transit MPLS router switches the MPLS frame along a pre-established LSP based on the tunnel label. Traffic in the tunnel and in other tunnels is aggregated towards a router's network port, competing to be scheduled and transmitted.

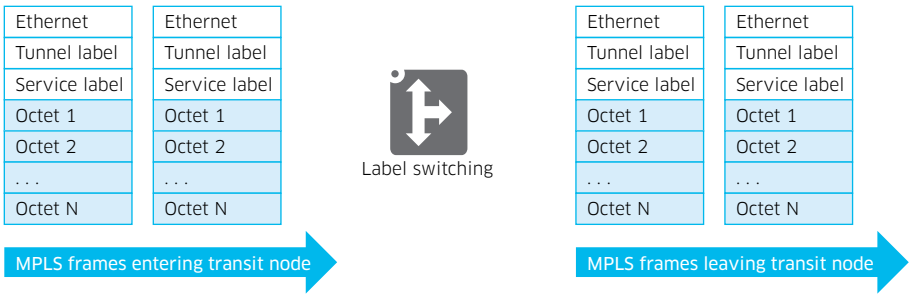
Because TDM-based applications are extremely sensitive to delay and jitter, their traffic needs to be treated with higher priority than other applications. When traffic arrives at a router, it needs to be classified based on header marking (EXP field for MPLS frames) and be placed in different queues. TDM traffic such as teleprotection must be placed in the high-priority queue and be exhaustively serviced continuously in order to achieve minimal delay and jitter (see Figure 6).

Figure 6. Priority-based scheduling



During the label switching (see Figure 7), the priority of the MPLS frames carrying TDM traffic is denoted by the EXP field. With proper marking and network engineering, the frames are placed in the top-priority queue and are serviced without incurring unnecessary queuing delay. As a result, the delay incurred at each label switching hop is negligible[4]. Also, because frames are switched immediately with no queuing delay, minimal jitter is incurred.

Figure 7. Multi-protocol Label Switching



4 The actual delay is hardware dependent. It is typically in the order of tens of microseconds.

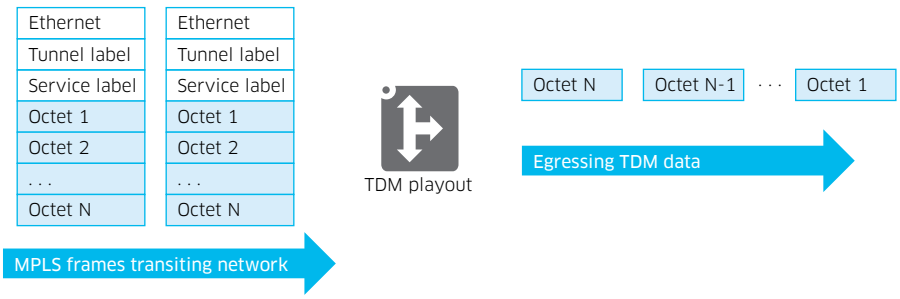
TDM playout delay at network egress

The playout process is shown in Figure 8.

When MPLS frames carrying TDM payload are received, the payload is extracted and placed in the playout buffer. To accommodate jitter incurred on the MPLS frames during transit, the payload gathered in the buffer is not immediately played out, or transmitted, on the TDM transmit circuit. Instead, it waits until half of the configured buffer is full before playing out.

The buffer size can be configured based on the number of transit hops and other network engineering factors.

Figure 8. Playout process



Summary of CES

Smaller payload size leads to a higher number of MPLS frames per second, resulting in lower packetization and playout buffer delay, and ultimately lower end-to-end delay. But this comes at the cost of higher bandwidth that is required to transport the TDM data stream. By contrast, a larger payload size results in a lower number of packets per second, incurring a higher packetization and playout delay, and eventually higher end-to-end delay. The benefit is lower bandwidth. Depending on the network design and delay budget of the teleprotection equipment, network operators can optimize the setting to achieve engineered targets.

End-to-end delay considerations

With proper engineering design, a service as stringent as teleprotection can reliably meet the strict latency requirement.

At ingress, CES starts with packetization whose delay is fixed and depends on the packetization delay. On egress playout, CES uses a jitter buffer to ensure that received packets are tolerant to jitter incurred in the transit network. This ensures the successful de-packetization of the payload back into the TDM interface needed for communication with the teleprotection equipment. This playout delay is also fixed.

The smaller the jitter buffer, the less delay. However, the jitter buffer needs to be set at a large enough value to ensure that jitter cannot cause a communications failure on the teleprotection equipment.

The selection of jitter buffer size must take into account the size of the TDM encapsulated packets. Larger payloads will require larger jitter buffer sizes.

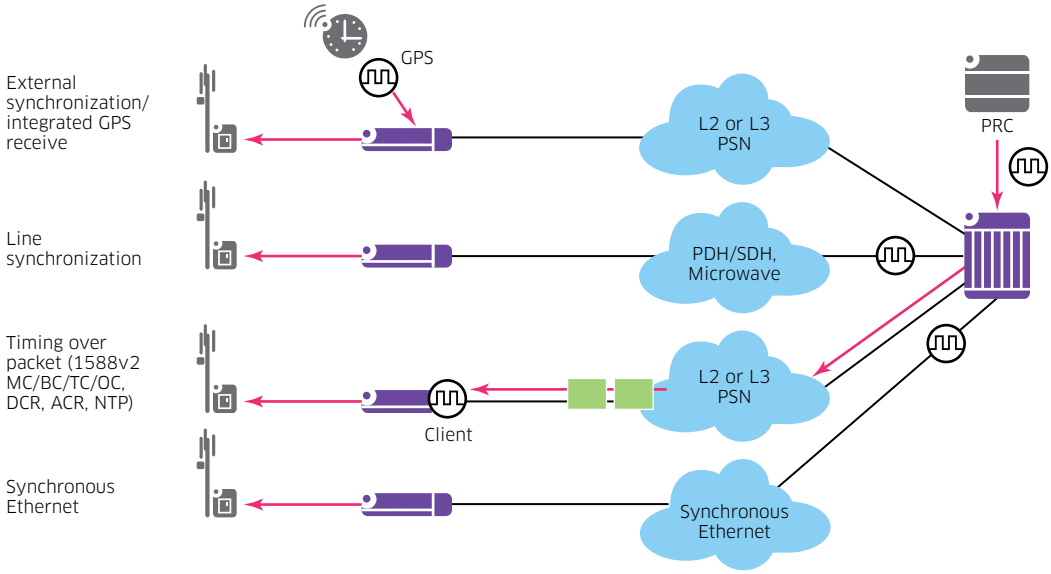
A properly configured jitter buffer provides continuous playout, thereby avoiding discards due to overruns and underruns.

Network operators can customize configurations to control these two delay parameters as well as the network transit delay to fall within the network delay budget for the teleprotection applications. Because the delay parameters are fixed, the end-to-end delay in the network is very deterministic to the stringent delay requirement for teleprotection application.

Alcatel-Lucent synchronization technologies

Synchronization of the TDM circuit end to end is also a prime consideration for CES. As shown in Figure 9, the Alcatel-Lucent 7705 SAR can support a full range of synchronization technologies to adapt to a network operator's synchronization infrastructure.

Figure 9. Synchronization technologies supported by Alcatel-Lucent 7705 SAR



IP/MPLS teleprotection features

Traditional SONET/SDH networks can be provisioned to provide alternate routes for mission-critical traffic such as the routes between teleprotection equipment. When operating correctly, the network provides less than 50 ms switchover time. This recovery speed has become a yardstick for any new network technologies.

In a similar manner, IP/MPLS networks support alternate paths and fast route with less than 50 ms switchover time. It is also important to note that with proper engineering design, IP/MPLS will guarantee that the end-to-end latency for the alternate path is at the same levels as the primary path.

An IP/MPLS network also supports teleprotection applications through the following features:

- IP/MPLS networks use LSPs to ensure that all packets associated with a particular service, such as teleprotection, follow the same path. This ensures that the predetermined latency target is always met.
- The packets associated with teleprotection communication can be assigned a high priority to guarantee that teleprotection requirements are met and reduced packet delay variation through the network is assured.
- The IP/MPLS network supports many synchronization options to ensure that the network is properly synchronized. Because the IP/MPLS routers are synchronized, they can provide a good reference clock to the connected teleprotection equipment Next-generation teleprotection equipment that is connected using Ethernet can also be synchronized because the Alcatel-Lucent IP/MPLS routers support Synchronous Ethernet (ITU-T recommendations **G.8262** [12] and **G.8264** [13]) and **IEEE 1588v2 Precision Time Protocol (PTP)** [8].

IP/MPLS TELEPROTECTION IN LAB AND PRODUCTION NETWORK

The misconception that teleprotection traffic cannot be reliably transported over an IP/MPLS network as in a traditional PDH/SONET/SDH network has been disproved through extensive testing and implementation in production networks.

Internal laboratory testing

As shown in Figure 10, teleprotection was tested under three setup scenarios in the Alcatel-Lucent Interoperability Laboratory:

- Test setup 1: Back-to-back with two 7705 SARs to simulate teleprotection equipment between two substations directly connected with optical fiber
- Test setup 2 The edge 7705 SARs connected via a two-node core network
- Test setup 3: The edge 7705 SARs connected via a two-node congested core network

Figure 10. Three internal laboratory test setups

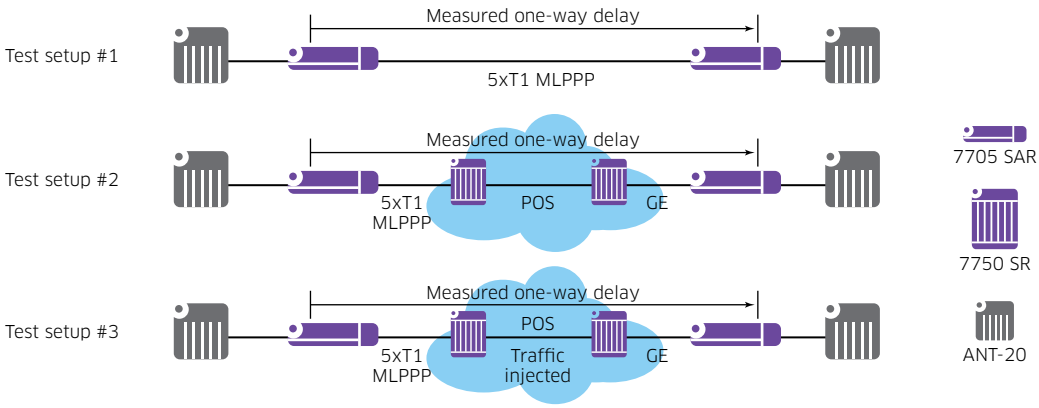


Table 1 shows delay test results.

Table 1. Delay test results

CONFIGURATION			CALCULATED			RESULTS: ANT-20 MEASURED ONE WAY DELAY (MS)		
Number of time slots	Jitter buffer (ms)	Payload size (Octets)	Packetization delay (ms)	Frames per packet	Packets per second	Test setup # 1	Test setup # 2	Test setup # 3
1	2	2	.25	2	4000	1.9	2.0	2.2
1	4	8	1	8	1000	3.6	3.8	3.8
1	8	16	2	16	500	6.7	6.8	6.8
12	2	24	0.25	2	4000	2.0	2.1	2.1
12	4	96	1	8	1000	4.1	4.2	4.2
12	10	192	4	16	500	7.1	7.2	7.3
24	2	48	0.25	2	4000	2.0	2.0	2.1
24	5	192	1	8	1000	4.1	4.3	4.4
24	5	384	2	16	500	5.1	5.3	5.4
24	10	384	2	16	500	7.1	7.3	7.3
3	2	6	.25	2	4000	2.0	2.1	2.2
3	4	24	1	8	1000	3.7	3.9	3.9
3	8	48	2	16	500	6.7	7.0	7.0

Some conclusions can be drawn from the laboratory results:

- The delay is well within the typical delay budget-to-teleprotection command transmission time.[5]
- The use of an MPLS core between two substations, as in Test setup 2, causes negligible additional delay because the switching delay of a label-switched router is in the order of tens of microseconds.
- The delay performance of teleprotection traffic is deterministic. The core link congestion in Test setup 3 causes only negligible delay, thanks to proper EXP field marking and advanced traffic management.

External independent laboratory validation

Alcatel-Lucent engaged both **Iometrix™**, the networking industry's preeminent testing and certification authority, and Strathclyde University in the United Kingdom to test and validate the ability of the IP/MPLS-based Alcatel-Lucent 7705 SAR and **Alcatel-Lucent 7750 Service Router** (7750 SR) to implement an IP/MPLS network to support teleprotection[6].

Based on a comprehensive set of tests, it was concluded that a network composed of Alcatel-Lucent IP/MPLS routers complies with all the requirements of teleprotection with a substantial margin. The IP/MPLS network performed well within the requirements of the teleprotection application that has, to this point, been supported by only TDM-based networks.

5 Typically, power systems are designed and engineered to withstand disruption by a fault for a brief duration in the 100 ms range. This means that, to protect the grid, teleprotection system needs to perform line tripping within 100 ms from when the fault occurs. Three factors contribute to the delay between fault occurrence and line tripping: TPR fault detection time; teleprotection command transmission time over the network (typical budget is between 10 to 20 ms); and protection relay switching time.

6 The Iometrix report [10] can be downloaded at **http://www.utilinet-europe.com/Iometrix_-_Teleprotection_Test_Report.pdf** The University of Strathclyde technical paper [3], co-authored with Alcatel-Lucent, can be downloaded at **http://strathprints.strath.ac.uk/48971/1/B5_111_2014.pdf**

Production deployment

Teleprotection over IP/MPLS has also been proven in actual deployments. Some power utilities in Europe and North America have already been relying on IP/MPLS to carry teleprotection in the last few years with various teleprotection equipment vendors. Various legacy interface types, including ITU-T. G.703 [11], E&M and IEEE C37.94, are used. The utilities have been reaping the benefits of a converged mission-critical communications network, optimizing operations in preparation for the future.

CONCLUSION

Power utilities rely on reliable, fast and secure transport of mission-critical traffic to monitor, analyze, control and maintain the grid. The Alcatel-Lucent IP/MPLS communications network can play a seminal role in assisting power utilities to consolidate all their operational applications over a converged network without performance degradation. This new network will enable utilities to maximize their grid flexibility and reliability in the face of energy demand surge without jeopardizing safety, security or reliability. This new network also paves the way for the introduction of future smart grid applications that can further improve operational effectiveness and achieve higher grid efficiencies. Alcatel-Lucent leverages cutting-edge technologies, along with the company's broad and deep experience in the energy segment, to help utilities build better, new generation IP/MPLS networks.

For more information about Alcatel-Lucent's solution for power utilities, go to **http://www2.alcatel-lucent.com/power-utilities/**

REFERENCES

1. Alcatel-Lucent. *Deploying IP/MPLS Communications for Smart Grids*, application note. November 2012. **http://resources.alcatel-lucent.com/asset/162351**
2. Alcatel-Lucent. *MPLS for Mission-Critical Networks*, technology white paper. December 2013. **http://resources.alcatel-lucent.com/asset/172097**
3. Blair, Coffele, Booth, de Valck and Verhulst. *Demonstration and analysis of IP/MPLS communications for delivery power system protection using IEEE 37.94, IEC 61850 Sampled Values, and IEC 61850 GOOSE protocols*.
4. DNP3 Users Group. *Overview of the DNP3 Protocol.* **http://www.dnp.org/pages/aboutdefault.aspx**
5. IEC. 60834-1 ed2.0. *Teleprotection equipment of power systems – Performance and testing – Part 1: Command systems*. Oct. 8, 1999. **http://webstore.iec.ch/webstore/webstore.nsf/artnum/025391!opendocument**
6. IEC. 60870-5-104. *International Standard – Telecontrol Equipment and Systems, Part 5-104, Transmission Protocols: Network Access for IEC 60870-5-101 Using Standard Transport Protocols*, Second Edition. June 2006. **http://webstore.iec.ch/preview/info_iec60870-5-104%7Bed2.0%7Den_d.pdf**
7. IEEE. C37.94-2002. *IEEE Standard for N Times 64 Kilobit Per Second Optical Fiber Interfaces Between Teleprotection and Multiplexer Equipment*. **http://standards.ieee.org/findstds/standard/C37.94-2002.html**
8. IEEE. 1588-2008. *IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems.* September 24, 2008. **http://www.ieee802.org/1/files/public/docs2008/as-garner-1588v2-summary-0908.pdf**

9. IETF. RFC 5086. *Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN).* December 2007. **http://www.ietf.org/rfc/rfc5086.txt**

10. iometrix. *Teleprotection Test Report.* 2013. **http://www.utilinet-europe.com/Iometrix_-_Teleprotection_Test_Report.pdf**

11. ITU-T. G.703, *Physical/Electrical Characteristics of Hierarchical Digital Interfaces,* November 2001 plus Erratum 1, July 2205, *Corrigendum 1*, March 2008 and *Amendment 1*, August 2013. **https://www.itu.int/rec/T-REC-G.703/en**

12. ITU-T. G.8262, *Timing Characteristics of a Synchronous Ethernet Equipment Slave Clock,* July 2010 and amendments February 2012 and October 2012. **http://www.itu.int/rec/T-REC-G.8262**

13. ITU-T. G.8264, *Distribution of Timing Information Through Packet Networks.* May 2014. **https://www.itu.int/rec/T-REC-G.8264/en**

14. Verhulst. *Teleprotection Over Packet Networks*. **https://itunes.apple.com/us/book/teleprotection-over-packet/id566617641?mt = 11**

ACRONYMS

7705 SAR	Alcatel-Lucent 7705 Service Aggregation Router
7750 SR	Alcatel-Lucent 7750 Service Router
ACR	Adaptive Clock Recovery
BC	Boundary Clock
CAPEX	capital expenditures
CES	Circuit Emulation Service
CESoPSN	Circuit Emulation Service over Packet Switched Network
CIR	Committed Information Rate
DCR	Differentiated Clock Recovery
DNP	Distributed Network Protocol
E&M	Earth & mouth
GE	Gigabit Ethernet
EXP	Experimental Bits
FAN	Field Area Network
FXO	Foreign eXchange Office
FXS	Foreign eXchange Subscriber
GPS	Global Positioning System
H-QoS	Hierarchical quality of service
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineer
IETF	Internet Engineering Task Force
IP	Internet Protocol
ITU-T	International Telecommunication Union – Telecommunications section
LAN	Local Area Network
LSP	label-switched path
MC	Master Clock
MLPPP	Multi-link Point-to-Point Protocol
MPLS	Multi-protocol Label Switching
NTP	Network Timing Protocol
OPEX	operating expenditures
PCM	pulse code modulation
PDH	Plesiochronous Digital Hierarchy
PIR	Peak Information Rate
PMU	phasor measurement unit
POS	Packet over SONETPTP Precision Timing Protocol
PRC	Primary Reference Clock
PSN	Packet-switched Network
QoS	Quality of Service
SCADA	supervisory control and data acquisition
SDH	Synchronous Digital Hierarchy
SONET	Synchronous Optical Network
TDM	Time Division Multiplexing
TC	Transparent Clock
WAM	Wide-Area Monitoring

Alcatel·Lucent