APPLICATION NOTE

Mission-critical communications networks for power utilities

Enabling reliable transport for teleprotection

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, such as teleprotection applications, demand stringent and deterministic transport. Of the various protection schemes, differential protection further requires symmetric delay.

This application note explains how an Alcatel-Lucent IP/MPLS network can help network operators to meet the challenge of migrating legacy mission-critical traffic and also engineer the network to meet their general requirements. This application note also explains how the innovative capability and asymmetric delay control (ADC) of an Alcatel-Lucent IP/MPLS network can counter the random jitter nature of packet network traffic and attain delay symmetry.

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
- Video surveillance to strengthen physical security

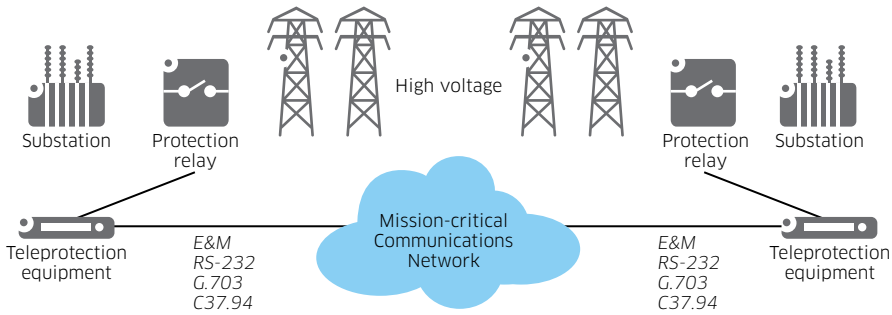
However, the grid still depends on already-deployed mission-critical applications for its daily operation. The most prominent of these is teleprotection[1].

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 that the power systems are properly protected, the teleprotection messages must be reliably transferred with tightly-controlled latency.

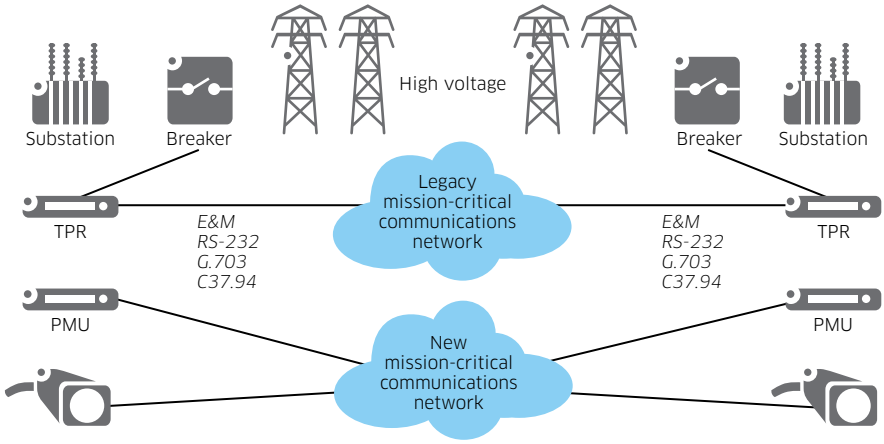
Figure 1. A typical teleprotection system in a mission-critical communications network



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

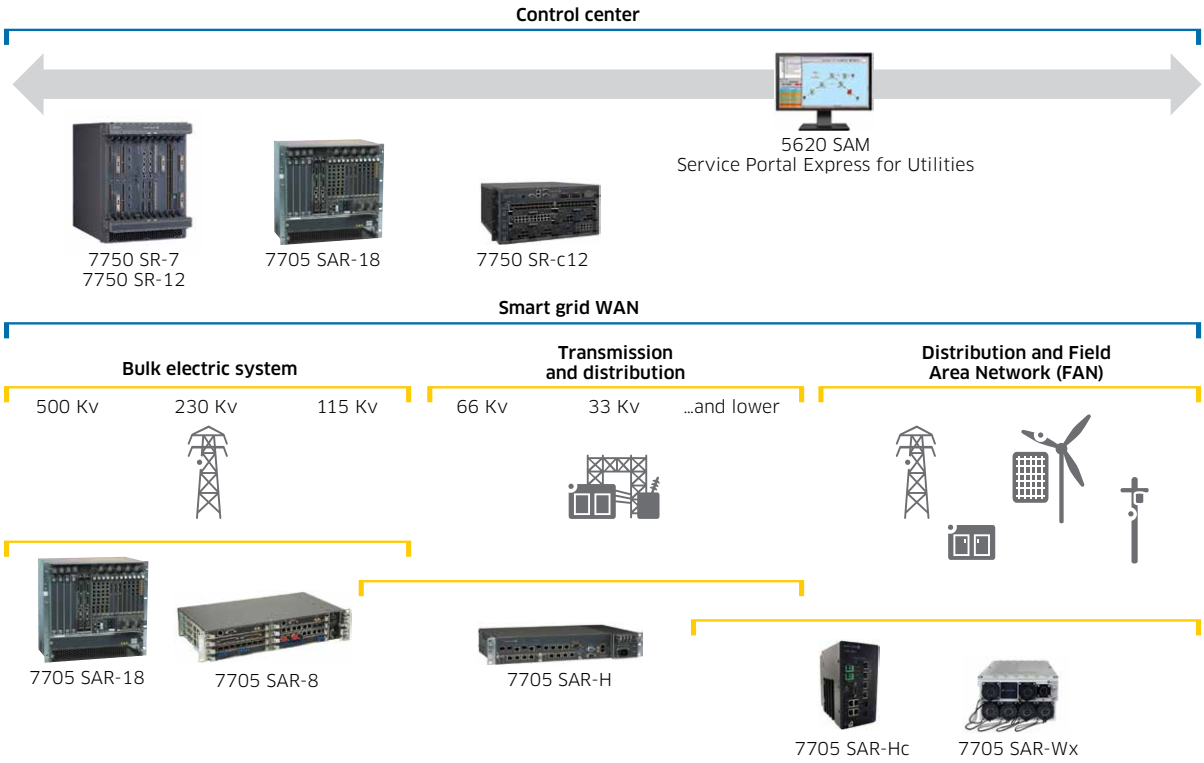
The most promising network technology for a converged network is IP/MPLS. An IP/MPLS network fulfills all convergence requirements, including network resiliency, quality of service (QoS), security and manageability[2]. For these reasons, it has become the technology of choice for new mission-critical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

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.

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].

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 teleprotection relays at two transmission substations. It is imperative to guarantee the delay, called transmission time in IEC Recommendation 60834-1 [6], 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.

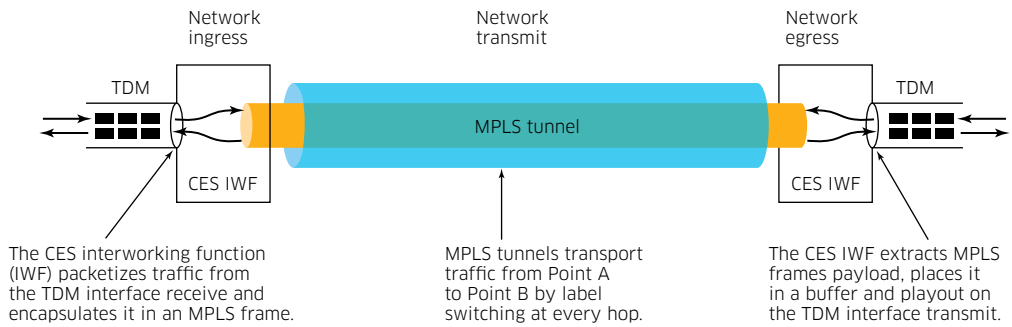
Circuit Emulation Service

An IP/MPLS network uses a Circuit Emulation Service (CES) to migrate traditional teleprotection applications. The key design considerations for supporting teleprotection are how to minimize latency and tackle network jitter.

The latency for TDM traffic consists of packetization delay at network ingress, network transit delay, and playout buffer delay at network egress. The playout buffer's function is to absorb jitter incurred by the network. 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 playout buffer size based on their TDM application requirements and network topology.

Operating with legacy TDM networks and services is straightforward when using MPLS CES functionality. With proper network engineering, 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.

Figure 4. Circuit Emulation Service



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

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 (for example, 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.

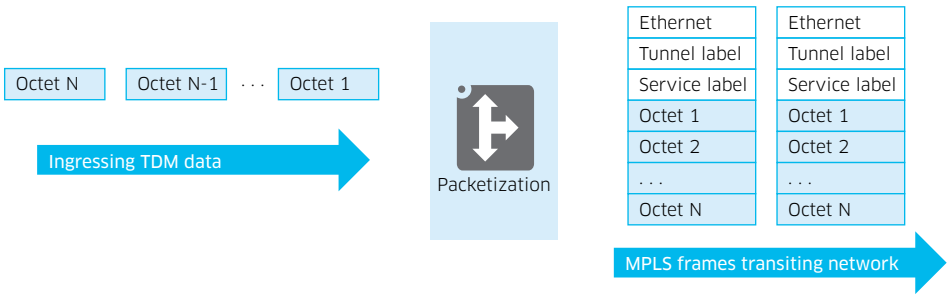
The operator has two choices: to package this byte in an MPLS frame and transmit it across the network immediately with practically no packetization delay (other than that incurred by hardware processing); or to wait until a pre-configured number of bytes arrive before transmitting them all together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

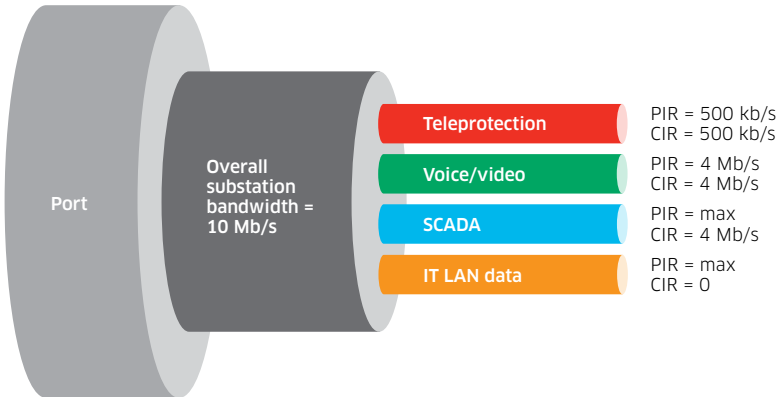
MPLS label switching during network transit

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.

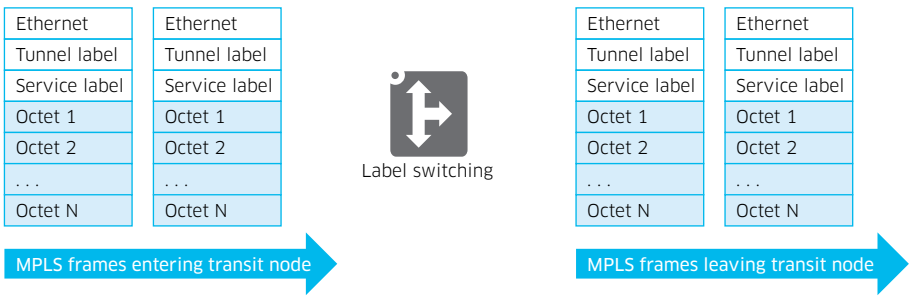
Because TDM-based applications are extremely sensitive to delay and jitter, their traffic needs to be treated with higher priority than other applications. When traffic arrives at a router, it needs to be classified based on header marking (EXP field for MPLS frames) and be placed in different queues. 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. However, even with the proper QoS policy, if a lower priority packet has started transmitting, teleprotection traffic still needs to wait until the low-priority packet transmission is completed. This phenomenon is known as head-of-line (HOL) blocking. The wait duration varies and depends on how many more bytes of the low-priority packet remain to be transmitted and also on the link speed[4], entailing network jitter.

Figure 7. Multi-protocol Label Switching



TDM playout delay at network egress

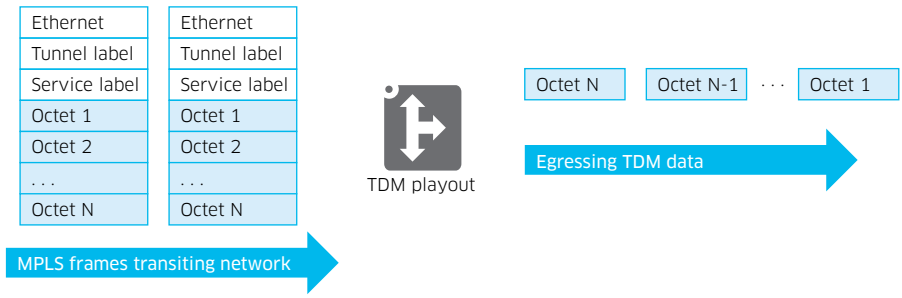
The playout process is shown in Figure 8.

4 The lower the port speed, the higher the jitter caused by HOL blocking. For example, a 10-Mb/s Ethernet link entails ten times the jitter of that incurred in a 100-Mb/s Fast Ethernet link when HOL blocking occurs.

When MPLS frames carrying TDM payload are received, the payload is extracted and placed in the playout buffer. To accommodate network 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 the playout threshold is crossed, when half of the configured buffer is filled, before playing out during the CES service startup phase.

The buffer size can be configured based on the network's jitter characteristics; these depend on various factors, including number of transit hops and their link speed. The smaller the jitter buffer, the less delay incurred. However, the jitter buffer needs to be set at a large enough value to ensure that it can always absorb the network jitter. If the jitter buffer is too small and fails to absorb the jitter, in a worst-case scenario it will experience buffer underrun (depletion of TDM bytes in the buffer) or buffer overrun (overflow of TDM bytes in buffer), causing a service failure that affects the teleprotection equipment. If the jitter buffer is too large, it will introduce extra playout buffer delay, which might exceed the teleprotection application's delay budget. Therefore, the network operator needs to understand the characteristics of the network and applications to determine an optimal buffer size.

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 CES service setting to achieve engineered targets consistently.

Attaining symmetric delay

Among the various types of teleprotection, differential protection imposes an extra network requirement: symmetric delay. Differential teleprotection equipment, while operating in asynchronous sampling mode, measures the one-way end-to-end network delay at both ends of the transmission line and compares these to detect faults.[5] To ensure an accurate comparison is performed, delay symmetry in the order of low or sub-milliseconds is required between the forward and reverse direction communication paths[6]. When the asymmetric delay tolerance is exceeded, relay could trip erroneously even under normal conditions.

5 For a detailed discussion of asymmetric delay in teleprotection, please see Jesus, Diago, Lobo et. al., MPLS networks for inter-substation communication for current differential protection applications in digital substation [16].
6 Actual tolerance depends on the electrical system vendor.

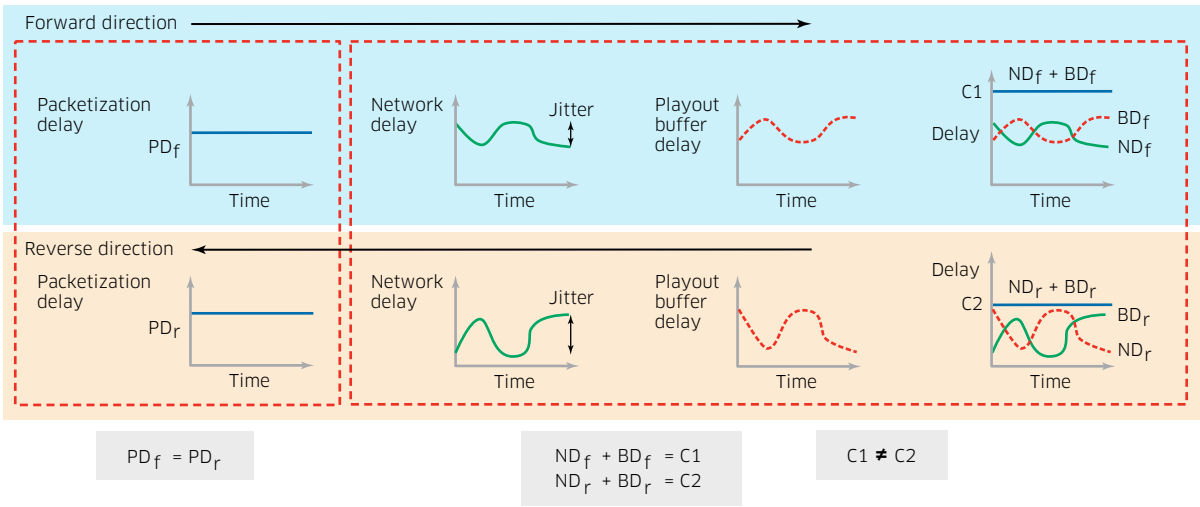
To attain symmetric delay in the network, it is important to first understand the source of asymmetric delay in order to remedy the effect. In a network with symmetric delay, the end-to-end delay experienced by packets sent and received by a pair of endpoints is equal; that is, the end-to-end delay is equal in both forward and reverse directions.

As already explained, CES has three delay contributors: packetization delay at network ingress, transit delay in the network core and playout buffer delay at network egress. Packetization delay and "engineered" playout buffer delay (the time to play out half of full buffer payload in both forward and reverse directions) are enforced to be the same during CES configuration. The nominal transit delay in both directions is also the same because the forward and reverse paths are typically placed on the same physical route, traversing the same set of label switched routers (LSRs) over the same set of network links. However, the actual transit delay each packet experiences varies due to network jitter, which is absorbed by the playout buffer as long as the buffer size can accommodate the network jitter range.

If a packet experiences a larger network delay due to successive HOL blocking at every hop in the network, its buffer playout delay will be smaller. In contrast, a smaller network delay entails a larger buffer delay because even if a packet arrives earlier, it still has to wait for its turn to be transmitted out of the buffer. Therefore, the sum of network delay and buffer delay are always constant (see Figure 9).

Although the sum of network delay and buffer delay for every packet is constant in the forward direction (C1) and reverse direction (C2), these do not equal each other; this is because the network delays in both directions are not the same during CES startup due to the random nature of network jitter. This network jitter during CES startup, in turn, causes asymmetric delay.

Figure 9. A close look at delay in forward and reverse directions

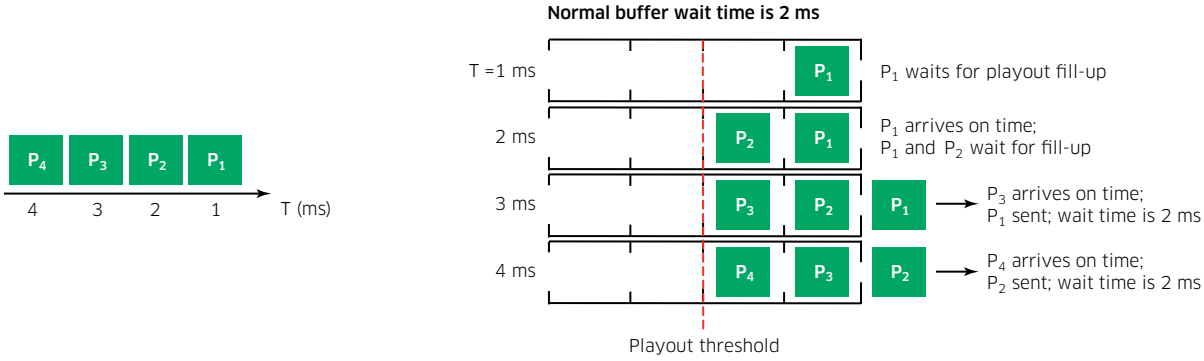


To show how network jitter during CES startup brings about delay asymmetry, we will first examine the playout buffer in action during CES startup without jitter and then compare this to a scenario with jitter.

Scenario of no jitter during startup

As shown in Figure 10, for a jitter buffer with the playout threshold set to 2 buffer units (equivalent to 2 ms wait when using a packet rate of 1000 packets/s), if there is no network jitter, every arriving packet will wait in the buffer for 2 ms.

Figure 10. Buffer delay during CES startup with no jitter

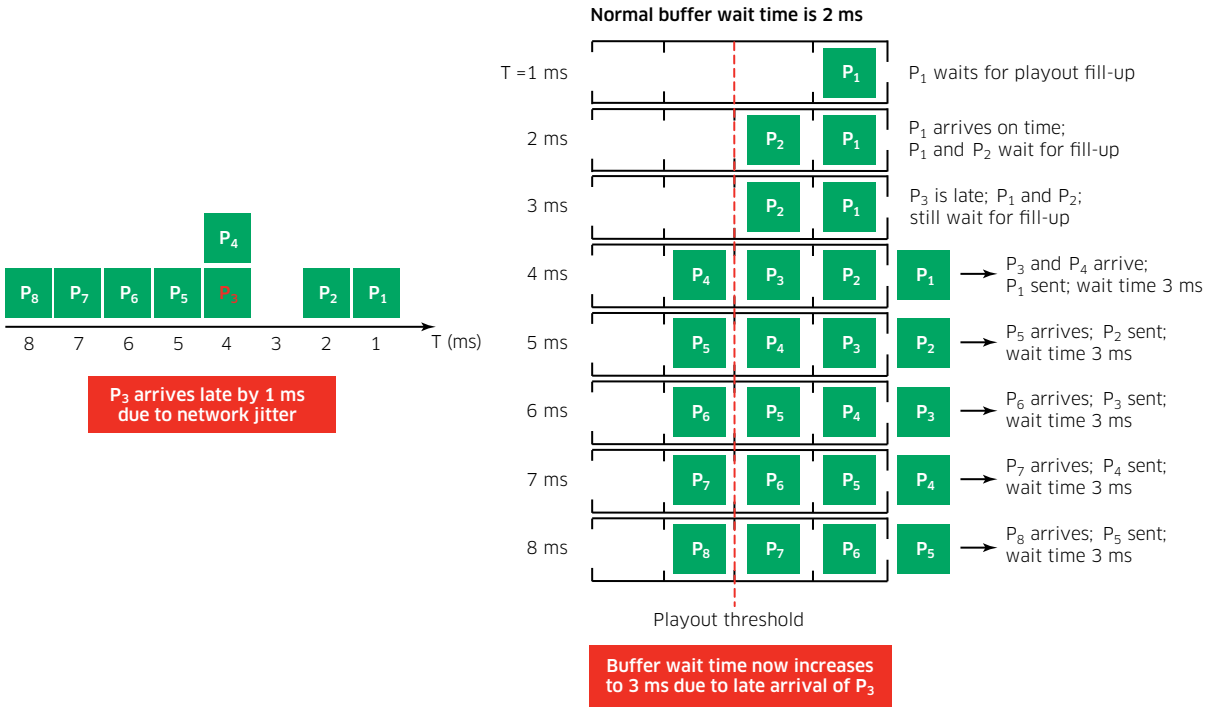


If there is jitter after startup, the playout buffer will compensate for any change in network delay experienced by a packet so the total delay remains constant for every packet.

Scenario of jitter during startup

If network jitter causes a 1-ms delay in the arrival of packet P_3 during startup, this delays the buffer playout startup by 1 ms. As shown in Figure 11, this delay results in a buffer wait time of 3 ms for the initial packets P_1 and P_2 and also all subsequent packets even though they do not experience any network jitter. Therefore, jitter experienced by P_3 causes "permanent[7]" buffer delay of 3 ms instead of the engineered value of 2 ms.

Figure 11. Buffer delay during CES startup with jitter



7 The buffer delay is permanent until the CES service is reset.

Because network jitter is random, the actual playout buffer delay cannot be controlled precisely. Therefore, buffer delays in both directions of the CES carrying teleprotection are very likely to be different, which results in asymmetric delay.

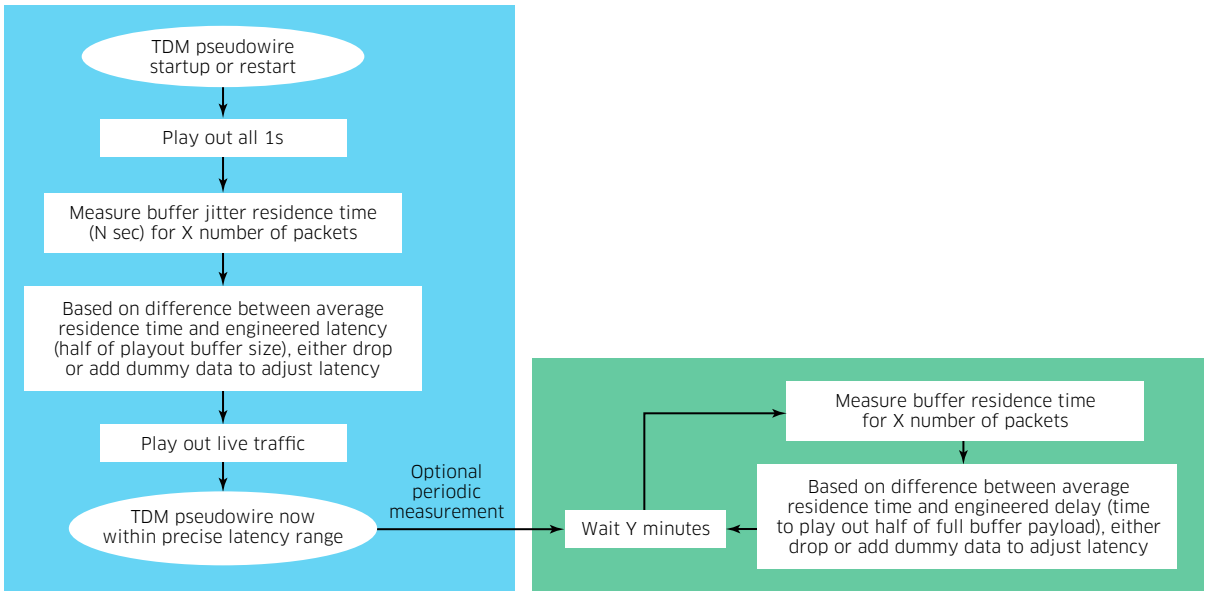
Attaining symmetric delay with ADC

Asymmetric delay control (ADC) is an innovative mechanism to remedy the asymmetric delay in the playout buffer caused by jitter experienced by the triggering packet (P_3) in the Figure 11 example. The ADC is carried out by real-time microcode running in the network processor as packets arrive.

The incremental steps to achieve symmetric delay as part of the CES startup process (see Figure 12) is as follows.

1. Instead of depending on the arrival time of one packet (P_3 in the Figure 11 example), the arrival time of a large number of packets (configurable from thousands to tens of thousands) is measured during startup. Each packet is time-stamped upon arrival and playout at the buffer to determine its buffer residence time.
2. At the end of the measuring period, an average residence time is calculated to adjust the actual playout buffer delay to match the "engineered" delay.
3. A comparison of the measured average residence time and engineered residence time (time to play out half of the buffer content) is made. To compensate for a difference:
   - ¬ If the measured time is higher than the engineered time, an appropriate number of bytes will be discarded.
   - ¬ If the measure time is less than the engineered time, an appropriate number of bytes of padding are added.
4. The CES is now in operation.
   The preceding steps are performed concurrently on the forward and reverse direction paths so that the playout buffer delay in both directions is now aligned to attain a symmetric delay. These steps can be optionally repeated periodically if the playout buffer playout rate on both sides is not the same due to imprecise network synchronization or clock failure.

Figure 12. ADC mechanism flowchart



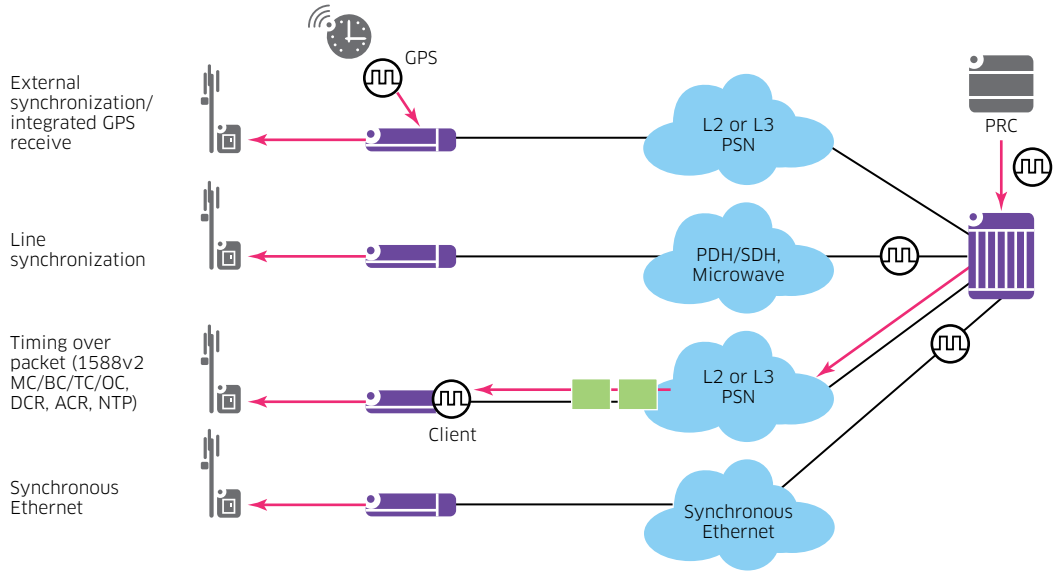
It is expected that ADC will play a seminal role to attain delay symmetry, which is pivotal for deploying current differential teleprotection over an IP/MPLS network.

End-to-end synchronization

Synchronization of the TDM circuit end to end is also a prime consideration for CES. Imprecise network synchronization would cause playout buffer overrun (if the receiving node clock is slower than the transmitting node clock) or buffer underrun (if the receiving node clock is faster than the transmitting node clock).

As shown in Figure 13, the Alcatel-Lucent 7705 SAR can support a full range of synchronization technologies to adapt to a network operator's synchronization infrastructure.

Figure 13. 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 delay for the alternate path is at the same levels as the delay for 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 delay 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 laboratory 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 14, 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 by a two-node core network
- Test setup 3: The edge 7705 SARs connected by a two-node congested core network

Figure 14. Three internal laboratory test setups

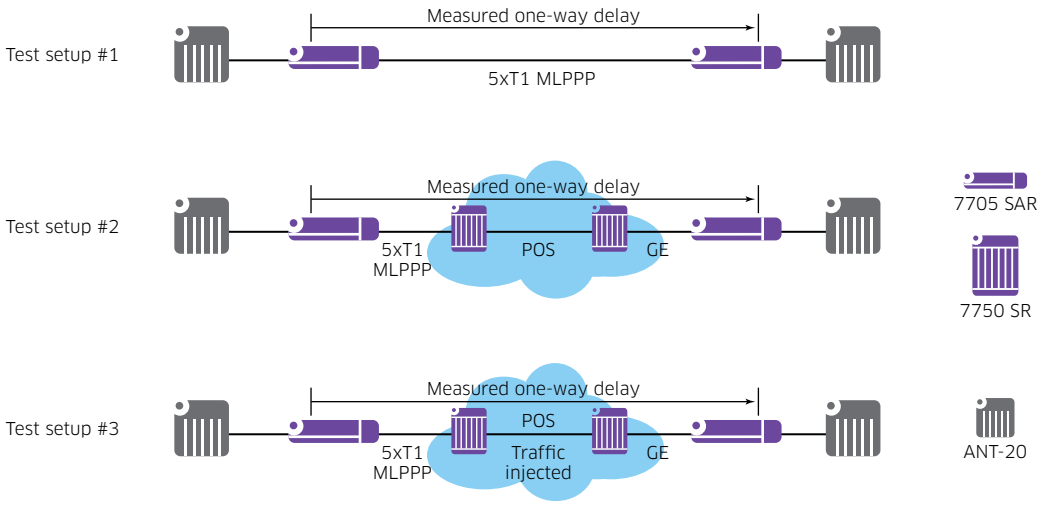


Table 1 shows the delay test results.

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	0.25	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	0.25	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.[8]
- The use of an MPLS core between two substations, as in Test setup 2, causes negligible additional delay because the switching delay of an LSR 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[9].

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.

8 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, the 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: teleprotection relay fault detection time; teleprotection command transmission time over the network (typical budget is between 10 and 20 ms); and protection relay switching time.

9 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 co-directional interface [11], E&M, RS-232, ITU-T X.21 [16] 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. Verhulst. Teleprotection Over Packet Networks. https://itunes.apple.com/us/book/teleprotection-over-packet/id566617641?mt=11
2. Alcatel-Lucent. Deploying IP/MPLS Communications for Smart Grids, application note. November 2012. http://resources.alcatel-lucent.com/asset/162351
3. Alcatel-Lucent. MPLS for Mission-Critical Networks, technology white paper. December 2013. http://resources.alcatel-lucent.com/asset/172097
4. 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.
5. DNP3 Users Group. Overview of the DNP3 Protocol. http://www.dnp.org/pages/aboutdefault.aspx
6. 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
7. 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
8. 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
9. 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

10. 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
11. iometrix. Teleprotection Test Report. 2013. http://www.utilinet-europe.com/Iometrix_-_Teleprotection_Test_Report.pdf
12. 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
13. 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
14. ITU-T. G.8264, Distribution of Timing Information Through Packet Networks. May 2014. https://www.itu.int/rec/T-REC-G.8264/en
15. ITU-T. X.21, Interface between Data Terminal Equipment and Data Circuit-terminating Equipment for synchronous operation on public data networks. https://www.itu.int/rec/T-REC-X.21/en
16. Jesus, Diego, Lobo, Blair and De Valck. MPLS networks for inter-substation communication for current differential protection applications in digital substation. 2014. http://strathprints.strath.ac.uk/48807/

Acronyms

7705 SAR	Alcatel-Lucent 7705 Service Aggregation Router
7750 SR	Alcatel-Lucent 7750 Service Router
ACR	Adaptive Clock Recovery
ADC	asymmetric delay control
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
HOL	head-of-line
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
LSR	label-switched router
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 SONET
PTP	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