

# TECHNICAL REPORT



## Communication networks and systems for power utility automation – Part 90-12: Wide area network engineering guidelines



## THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2015 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

IEC Central Office  
3, rue de Varembé  
CH-1211 Geneva 20  
Switzerland

Tel.: +41 22 919 02 11  
Fax: +41 22 919 03 00  
[info@iec.ch](mailto:info@iec.ch)  
[www.iec.ch](http://www.iec.ch)

### About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

### About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

#### IEC Catalogue - [webstore.iec.ch/catalogue](http://webstore.iec.ch/catalogue)

The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

#### IEC publications search - [www.iec.ch/searchpub](http://www.iec.ch/searchpub)

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,...). It also gives information on projects, replaced and withdrawn publications.

#### IEC Just Published - [webstore.iec.ch/justpublished](http://webstore.iec.ch/justpublished)

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

#### Electropedia - [www.electropedia.org](http://www.electropedia.org)

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

#### IEC Glossary - [std.iec.ch/glossary](http://std.iec.ch/glossary)

More than 60 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

#### IEC Customer Service Centre - [webstore.iec.ch/csc](http://webstore.iec.ch/csc)

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: [csc@iec.ch](mailto:csc@iec.ch).

# TECHNICAL REPORT



---

## Communication networks and systems for power utility automation – Part 90-12: Wide area network engineering guidelines

INTERNATIONAL  
ELECTROTECHNICAL  
COMMISSION

ICS 33.200

ISBN 978-2-8322-2806-7

**Warning! Make sure that you obtained this publication from an authorized distributor.**

## CONTENTS

FOREWORD.....	11
INTRODUCTION.....	13
1 Scope.....	15
2 Normative references .....	15
3 Terms, definitions, abbreviations, acronyms and symbols.....	20
3.1 Terms and definitions.....	20
3.2 Abbreviations and acronyms .....	25
3.3 Network diagram symbols .....	32
4 Wide Area Communication in electrical utilities.....	34
4.1 Executive summary.....	34
4.2 Use Case: ENDESA, Andalusia (Spain) .....	36
4.3 Typical interface between a substation and the WAN .....	38
4.4 WAN characteristics and actors .....	39
4.5 SGAM Mapping.....	40
4.6 Network elements and voltage level .....	42
4.7 WAN interfaces in substation automation (IEC 61850-5) .....	43
4.8 Logical interfaces and protocols in the TC57 Architecture IEC TR 62357 .....	44
4.9 Network traffic and ownership .....	45
5 WAN overall requirements and data transmission metrics.....	45
5.1 Traffic types.....	45
5.2 Quality of Service (QoS) of TDM and PSN .....	46
5.3 Latency calculation .....	46
5.3.1 Latency components.....	46
5.3.2 Propagation delay.....	46
5.3.3 Residence delay .....	47
5.3.4 Latency accumulation .....	47
5.3.5 Example: latency of a microwave system.....	47
5.3.6 Latency and determinism.....	47
5.3.7 Latency classes in IEC 61850-5.....	48
5.4 Jitter .....	50
5.4.1 Jitter definition.....	50
5.4.2 Jitter classes in IEC 61850 .....	51
5.5 Latency symmetry and path congruency .....	51
5.6 Medium asymmetry.....	51
5.7 Communication speed symmetry.....	52
5.8 Recovery delay .....	52
5.9 Time accuracy .....	52
5.9.1 Time accuracy definition .....	52
5.9.2 Time accuracy classes.....	53
5.10 Tolerance against failures.....	54
5.10.1 Failure .....	54
5.10.2 Reliability.....	54
5.10.3 Redundancy principles.....	55
5.10.4 Redundancy and reliability.....	55
5.10.5 Redundancy checking.....	56
5.10.6 Redundant layout: single point of failure .....	57



5.10.7	Redundant layout: cross-redundancy .....	57
5.10.8	Maintainability .....	58
5.10.9	Availability .....	58
5.10.10	Integrity .....	60
5.10.11	Dependability.....	62
5.10.12	Example: Dependability of GOOSE transmission .....	62
6	Applications analysis .....	62
6.1	Application kinds.....	62
6.2	Teleprotection (IF2 & IF11) .....	63
6.2.1	Teleprotection schemes.....	63
6.2.2	Teleprotection data kinds.....	64
6.2.3	Teleprotection requirements for latency .....	64
6.2.4	Teleprotection requirements for latency asymmetry .....	64
6.2.5	Teleprotection requirements for integrity.....	64
6.2.6	Teleprotection summary .....	65
6.3	Telecontrol (IF1, IF6) .....	65
6.4	Substation to control centre (IF10) .....	66
6.5	CMD (IF7).....	67
6.5.1	CMD overview .....	67
6.5.2	CMD communication requirements .....	67
6.6	Control Centre to Control Centre (IF12) .....	67
6.7	Wide Area Monitoring System (IF13).....	68
6.7.1	WAMS overview .....	68
6.7.2	WAMS topology .....	68
6.7.3	WAMS communication requirements.....	70
6.8	Wide area monitoring, protection and control (WAMPAC) IF13.....	71
6.8.1	WAMPAC overview .....	71
6.8.2	WAMPAC communication requirements .....	71
6.8.3	Use case WAMPAC .....	73
6.9	Wind turbines and wind virtual power plants.....	74
6.10	Distributed Energy and Renewables (DER) .....	74
6.11	Summary of communication requirements for WAN .....	74
7	Wide-area and real-time network technologies.....	75
7.1	Introduction.....	75
7.2	Topology.....	75
7.3	Overview.....	76
7.4	Layer 1 (physical) transmission media .....	78
7.4.1	Summary .....	78
7.4.2	Installation guidelines .....	78
7.4.3	Metallic lines .....	79
7.4.4	Power line carrier (PLC) .....	80
7.4.5	Radio transmission .....	84
7.4.6	Fiber optics.....	89
7.4.7	Layer 1 redundancy .....	96
7.4.8	Use case: Diverse redundancy against extreme contingencies (Hydro-Quebec) .....	97
7.4.9	Layer 1 security .....	98
7.5	Layer 1,5 (physical) multiplexing .....	98
7.6	Layer 2 (link) technologies .....	99

7.6.1	Telephony technologies .....	99
7.6.2	SDH/SONET .....	101
7.6.3	Optical Transport Network .....	111
7.6.4	Ethernet .....	112
7.6.5	Ethernet over TDM .....	122
7.6.6	Carrier Ethernet.....	123
7.6.7	Audio-Video Bridging .....	125
7.6.8	Provider Backbone Bridge (PBB) .....	125
7.6.9	Multiprotocol Label Switching (MPLS).....	127
7.7	Layer 3 (network) technologies .....	135
7.7.1	Internet Protocol (IP) .....	135
7.7.2	IP QoS.....	148
7.7.3	IP multicast.....	151
7.7.4	IP redundancy .....	152
7.7.5	IP security .....	152
7.7.6	IP communication for utilities .....	154
7.7.7	IP summary .....	156
7.8	Layer 4 (transport) protocols .....	157
7.8.1	Transport layer encapsulation.....	157
7.8.2	UDP .....	157
7.8.3	TCP .....	158
7.8.4	Layer 4 redundancy .....	159
7.8.5	Layer 4 security .....	159
7.9	Layer 5 (session) and higher.....	159
7.9.1	Session layer.....	159
7.9.2	Routable GOOSE and SMV .....	160
7.9.3	Example: C37.118 transmission.....	160
7.9.4	Session protocol for voice and video transmission .....	161
7.9.5	Application interface redundancy .....	161
7.9.6	Application device redundancy .....	162
7.10	Protocol overlay – tunneling.....	162
7.10.1	Definitions .....	162
7.10.2	Tunneling principle .....	163
7.10.3	Tunneling Layer 2 over Layer 3 .....	163
7.10.4	Use Case: Tunneling GOOSE and SMV in IEC 61850.....	164
7.10.5	Circuit emulation service (CES) .....	165
7.11	Virtual Private Networks (VPNs) .....	169
7.11.1	VPN principles.....	169
7.11.2	L2VPNs .....	169
7.11.3	L2VPN multicast on MPLS.....	171
7.11.4	L3VPN.....	171
7.11.5	VPN mapping to application.....	173
7.12	Cyber Security .....	176
7.12.1	Security circles .....	176
7.12.2	Network security .....	177
7.12.3	Access Control .....	180
7.12.4	Threat detection and mitigation.....	180
7.12.5	Security architecture.....	184
7.12.6	Application (end-to-end) communication security .....	185

7.12.7	Security for synchrophasor (PMU) networks (IEC TR 61850-90-5)	186
7.12.8	Additional recommendations	187
7.13	QoS and application-specific engineering	187
7.13.1	General	187
7.13.2	SDH/SONET QoS and SLA	187
7.13.3	PSN QoS and SLA	187
7.13.4	Application and priority	188
7.13.5	QoS chain between networks	188
7.13.6	QoS mapping between networks	189
7.13.7	QoS engineering	190
7.13.8	Customer restrictions	191
7.13.9	Clock services	191
7.14	Configuration and OAM	191
7.14.1	Network configuration	191
7.14.2	OAM	191
7.15	Time synchronization	193
7.15.1	Oscillator stability	193
7.15.2	Mutual synchronization	193
7.15.3	Direct synchronization	194
7.15.4	Radio synchronization	194
7.15.5	GNSS synchronization	195
7.15.6	Frequency distribution	195
7.15.7	Time distribution	196
7.15.8	PTP telecommunication profiles	203
7.15.9	PTP over MPLS	203
7.15.10	Comparison of time distribution profiles based on IEC 61588	203
7.15.11	Use Case: Synchrophasor time synchronization	205
7.15.12	Use case: Atomic Clock Hierarchy	205
8	Use cases	206
8.1	Use case: Current differential teleprotection system (Japan)	206
8.2	Use case: SDH / MPLS network (Japan)	210
8.3	Use Case: Wide area stabilizing control system (Japan)	211
8.4	Use Case: experimental PMU-based WAMPAC system	213
	Bibliography	216
	Figure 1 – Symbols	33
	Figure 2 – Substation locations in Andalusia	36
	Figure 3 – Topology of the Andalusia network	37
	Figure 4 – Cabinet of the substation edge node	38
	Figure 5 – Communication interfaces in a SEN	39
	Figure 6 – Communicating entities	40
	Figure 7 – SGAM communication model	41
	Figure 8 – Principle of grid voltage level and network technology	42
	Figure 9 – Communication paths and interfaces	43
	Figure 10 – IEC TR 62357 Interfaces, protocols and applications	44
	Figure 11 – Composition of end-to-end latency in a microwave relay	47
	Figure 12 – Example of latency in function of traffic	48

Figure 13 – Jitter for two communication delay types.....	50
Figure 14 – Precision and accuracy definitions .....	52
Figure 15 – Redundancy of redundant systems.....	56
Figure 16 – Redundancy calculation .....	56
Figure 17 – Redundancy layout with single point of failure .....	57
Figure 18 – Redundancy layout with cross-coupling.....	58
Figure 19 – Availability definitions.....	59
Figure 20 – Residual error rate in function of the BER .....	61
Figure 21 – Principle of synchrophasor transmission.....	69
Figure 22 – Target phenomena for WAMPAC.....	71
Figure 23 – Example of main function and general information flow .....	72
Figure 24 – PMUs and data flow between TSO and regional data hubs.....	73
Figure 25 – Network topology (Carrier Ethernet) .....	76
Figure 26 – Phase-to-ground coupling for PLC.....	80
Figure 27 – HV PLC coupling with suspended line traps .....	81
Figure 28 – Phase to phase signal coupling for PLC .....	81
Figure 29 – Phase-to-phase signal coupling.....	82
Figure 30 – Power line carrier, line traps.....	83
Figure 31 – Terrestrial microwave link .....	85
Figure 32 – Layer 2 transport on radio systems .....	88
Figure 33 – Radio network in feeder automation .....	89
Figure 34 – ADSS fiber cable.....	90
Figure 35 – ADSS installation with splicing box.....	91
Figure 36 – OPGW in ground cable.....	91
Figure 37 – OPGW with two “C”-tubes with each 32 fibers .....	92
Figure 38 – OPGW fibers .....	93
Figure 39 – Splicing box .....	94
Figure 40 – WDM over one fiber .....	95
Figure 41 – OCh optical components .....	95
Figure 42 – Optical link with microwave back-up .....	97
Figure 43 – Picture of partially destroyed 735 kV line.....	98
Figure 44 – E1 and E2 channel .....	100
Figure 45 – Digital Transmission Hierarchy (T – Standards).....	100
Figure 46 – Digital Transmission Hierarchy (E-standard) .....	101
Figure 47 – Example of an SDH network for utilities.....	102
Figure 48 – SONET multiplexing hierarchy.....	103
Figure 49 – SDH multiplexing hierarchy .....	103
Figure 50 – SDH/SONET with point-to-point topology .....	105
Figure 51 – SDH/SONET with linear topology .....	105
Figure 52 – BLSR/BSHR topology in normal conditions (from A to D).....	107
Figure 53 – BLSR/BSHR topology in failure conditions.....	107
Figure 54 – UPSR/USHR topology in normal conditions .....	108
Figure 55 – UPSR/USHR topology in failure conditions.....	109

Figure 56 – Example of information flow relationship in OTN .....	112
Figure 57 – IEEE 802.3 (Ethernet) frame format .....	113
Figure 58 – IEEE 802.3 (Ethernet) topology with RSTP switches (IEC TR 61850-90-4) .....	114
Figure 59 – IEEE 802.1Q-tagged Ethernet frame format .....	115
Figure 60 – Direct Ethernet with VLAN in substation-to-substation transmission .....	116
Figure 61 – Substation-to-substation Layer 2 transmission tunneled over IP .....	117
Figure 62 – PRP structure (within and outside a substation) .....	118
Figure 63 – HSR ring connecting substations and control centre .....	118
Figure 64 – MACsec frame format.....	120
Figure 65 – IEEE 802.1X principle .....	121
Figure 66 – Ethernet for substation-to-substation communication.....	122
Figure 67 – Packets over TDM .....	123
Figure 68 – IEEE 802.1Q/ad/ah network configuration .....	126
Figure 69 – Case of IEEE 802.1Q/ad network for utility .....	127
Figure 70 – Basic MPLS architecture .....	128
Figure 71 – Example of MPLS frame format with IPv4 payload.....	129
Figure 72 – MPLS building blocks .....	130
Figure 73 – MPLS network architecture for utilities .....	131
Figure 74 – IP/MPLS and MPLS-TP features .....	132
Figure 75 – MPLS-TP redundant routing .....	134
Figure 76 – Ethernet frame with IP network header .....	136
Figure 77 – Mapping of IPv4 to Ethernet frames .....	137
Figure 78 – Mapping of IPv6 to Ethernet frames .....	140
Figure 79 – IPv6 unicast address structure .....	141
Figure 80 – IPv6 ULA address structure.....	142
Figure 81 – IPv6 link local address structure.....	142
Figure 82 – Mapping of IPv4 to IPv6 addresses .....	145
Figure 83 – IPv6 evolution .....	147
Figure 84 – IEC 61850 stack with IPv4 and IPv6 .....	148
Figure 85 – DiffServ codepoint field .....	150
Figure 86 – Unidirectional protocol independent multicast.....	151
Figure 87 – Bidirectional protocol independent multicast.....	152
Figure 88 – Frame format for IPsec (authenticated) .....	153
Figure 89 – Frame format for IPsec (encrypted) .....	153
Figure 90 – Layer 3 direct connection within same address space .....	154
Figure 91 – Connecting substations to SCADA by a NAT .....	155
Figure 92 – Substation to SCADA connection over ALG.....	156
Figure 93 – Ethernet frame with UDP transport layer .....	157
Figure 94 – UDP header .....	158
Figure 95 – TCP header.....	158
Figure 96 – Session and presentation layers for MMS.....	160
Figure 97 – Session and presentation layers for R-GOOSE .....	160
Figure 98 – IEEE C37.118 frame over UDP.....	161

Figure 99 – Redundant network transmission handled by the application layer .....	161
Figure 100 – Tunneling in IEC TR 61850-90-1 .....	163
Figure 101 – L2TP transporting Layer 2 frames over IP .....	164
Figure 102 – Tunneling GOOSE over IP in IEC TR 61850-90-5 .....	165
Figure 103 – Pseudo-wire principle .....	166
Figure 104 – Non-IP voice communication over PSN .....	167
Figure 105 – Circuit emulation over PSN .....	168
Figure 106 – L2VPNs VPWS and VPLS .....	170
Figure 107 – L3VPN .....	171
Figure 108 – Emulation of L3VPN by L2VPN and global router .....	172
Figure 109 – Tele-protection over VPWS, .....	174
Figure 110 – WAMS over VPLS .....	175
Figure 111 – VPN for IP-based SCADA/EMS traffic .....	176
Figure 112 – VPN deployment options .....	179
Figure 113 – IP network separator .....	181
Figure 114 – Security architecture (using segmentation and perimeter security) .....	185
Figure 115 – QoS chain .....	189
Figure 116 – Timing pulse transmission methods of legacy teleprotection devices .....	194
Figure 117 – SyncE application.....	195
Figure 118 – Synchronous Ethernet Architecture .....	196
Figure 119 – SNTP clock synchronization and network delay measurement.....	197
Figure 120 – Model of GMC, two BCs in series and SC over Layer 3 .....	200
Figure 121 – Timing diagram of PTP (end-to-end, 2-step, BCs) .....	200
Figure 122 – Timing diagram of PTP (peer-to-peer, 2-step TCs) .....	201
Figure 123 – Substations synchronization over WAN .....	205
Figure 124 – Example of synchronization network.....	206
Figure 125 – Current differential 1:1 configuration .....	207
Figure 126 – Network configuration for centralized multi-terminal line protection.....	207
Figure 127 – Network configuration for distributed multi-terminal line protection .....	208
Figure 128 – Current differential teleprotection for HV multi-terminal transmission line using Layer 2 network.....	208
Figure 129 – Configuration of wide area current differential primary and backup teleprotection system employing Carrier Ethernet and IEC 61588 time synchronization .....	210
Figure 130 – Achieving protection for teleprotection services .....	211
Figure 131 – System configuration for wide area stabilizing control system.....	212
Figure 132 – Appearance of typical CCE cabinet .....	213
Figure 133 – Configuration for PMU-based WAMPAC system .....	214
Table 1 – Latency classes in IEC 61850-5 .....	49
Table 2 – Latency classes in IEC TR 61850-90-1 .....	49
Table 3 – Latency classes for WANs.....	50
Table 4 – Jitter classes in IEC TR 61850-90-1 .....	51
Table 5 – Jitter classes for WAN .....	51
Table 6 – Recovery delay classes for WAN.....	52

Table 7 – IEC TR 61850-90-1 time accuracy classes .....	53
Table 8 – IEC 61850-5 time accuracy classes for IED synchronization .....	53
Table 9 – WAN time synchronization classes .....	54
Table 10 – Latency for line protection .....	64
Table 11 – Summary of operational requirements of line protection .....	65
Table 12 – Summary of communication requirements for teleprotection .....	65
Table 13 – Communication requirements for CC to SS/PS .....	66
Table 14 – Latency and timing requirements from IEC TR 61850-90-2 .....	66
Table 15 – Communication requirements for CMD .....	67
Table 16 – Communication requirements for inter-control centre communications .....	68
Table 17 – Summary of synchrophasor requirements .....	70
Table 18 – Summary of communication requirements for wide area monitoring .....	71
Table 19 – Typical communication requirements for WAMPAC .....	73
Table 20 – Classification of communication requirements .....	74
Table 21 – Communication requirements of wide-area applications .....	74
Table 22 – Communication technologies .....	77
Table 23 – Physical communication media .....	78
Table 24 – DSL communication over twisted pairs .....	79
Table 25 – Trade-offs in copper cable communication .....	80
Table 26 – PLC communication technologies .....	83
Table 27 – PLC communication advantages and disadvantages .....	84
Table 28 – Microwave link performance .....	86
Table 29 – Terrestrial microwave advantages and disadvantages .....	86
Table 30 – Public mobile radio technologies .....	87
Table 31 – Terrestrial radio advantages and disadvantages .....	87
Table 32 – Satellite radio advantages and disadvantages .....	87
Table 33 – Optical fibers: advantages and disadvantages .....	96
Table 34 – SONET and SDH hierarchies .....	104
Table 35 – Summary of SDH/SONET .....	111
Table 36 – Ethernet physical layers .....	113
Table 37 – Payload mapping using SDH/SONET and Next Generation SDH/SONET .....	123
Table 38 – Carrier Ethernet summary .....	125
Table 39 – IP/MPLS characteristics .....	133
Table 40 – MPLS-TP characteristics .....	134
Table 41 – MPLS summary .....	135
Table 42 – Differences between IPv4 and IPv6 .....	143
Table 43 – IPv6 versus IPv4 addresses [RFC 4291] .....	144
Table 44 – List of DiffServ codepoint field values .....	150
Table 45 – IP Summary .....	156
Table 46 – Pseudowire protocols .....	169
Table 47 – VPN services .....	174
Table 48 – IEC 62351 series .....	186
Table 49 – Example of simple application priority assignment .....	188

Table 50 – Typical oscillator stability.....	193
Table 51 – IEC 61588 option comparison.....	202
Table 52 – Precision time distribution protocols based on IEC 61588.....	204
Table 53 – Requirements for the YONDEN IP network .....	211
Table 54 – Technologies for the YONDEN IP network .....	211
Table 55 – Main system specifications for wide area stabilizing control system.....	213
Table 56 – Specifications for PMU-based WAMPAC system .....	215



## INTERNATIONAL ELECTROTECHNICAL COMMISSION

## COMMUNICATION NETWORKS AND SYSTEMS FOR POWER UTILITY AUTOMATION –

### Part 90-12: Wide area network engineering guidelines

#### FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC TR 61850-90-12, which is a technical report, has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

The text of this technical report is based on the following documents:

Enquiry draft	Report on voting
57/1536/DTR	57/1576/RVC

Full information on the voting for the approval of this technical report can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts in the IEC 61850 series, published under the general title *Communication networks and systems for power utility automation*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC website under "<http://webstore.ch>" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

**IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.**

## INTRODUCTION

Utilities use data networks to interconnect equipment between their premises, over distances from under a kilometer to thousands of kilometers, called a “Wide Area Network” or WAN.

WANs encompass communication means of different nature (optical, radio, power line carrier, copper, etc.), with a variety of topologies (rings, trees, meshes, etc.), using different protocols (SDH/SONET, Ethernet, IP, MPLS, etc.), medium sharing (packet switching, time division multiplex, etc.) and for different applications (teleprotection, SCADA, voice, video, etc.).

This contrasts with substation automation networks as described in the LAN Engineering Guidelines (IEC TR 61850-90-4), which are based on one technology (switched Ethernet), make extensive use of Layer 2 multicast (GOOSE, SMV, PTP, etc.) and use Layer 3 communication (MMS, FTP, etc.), typically without routers within the substation.

The IEC 61850 suite sets up numerous requirements on the network but does not state how to achieve them:

- IEC 61850-5 specifies the basic requirements for data networks used in Power Utility Automation networks;
- IEC 61850-7 focuses on data modelling, leaving out physical interconnection details;
- IEC 61850-8-1 and IEC 61850-9-2 specify interoperable communication within substations;
- IEC TR 61850-90-1 describes substation-to-substation traffic, specifies the requirements for communication, defines object models for substation-to-substation teleprotection, models the gateway and the tunneler, but leaves the WAN undefined;
- IEC TR 61850-90-2<sup>1</sup> provides substation to control centre network configuration for IEDs, proxies and applications;
- IEC TR 61850-90-5 (synchrophasor transmission) addresses the transport of synchrophasor data between PMUs and control centres and defines a tunneling protocol as well as a data security method;
- IEC TR 61850-90-4 provides guidelines for network engineering focused on Ethernet-based real-time and highly available networks in substations. Some of these guidelines are applicable to networks outside of the substation;
- IEC 60870-6 (TASE2), IEC 61968 and IEC 61970 (CIM) describe the information interchange at the application layer without specifying the network.

Each of these documents deals separately with application, transport or network layer mechanism. There exist no comprehensive engineering guides for wide-area and real-time networks for control and protection. The growing success of IEC 61850 calls for guidelines for engineering the WANs.

Complementing IEC TR 61850-90-4, this Technical Report proposes guidelines for wide-area and real-time networks for various IEC 61850-based applications including teleprotection, wide area measurement, protection and control (WAMPAC), power system monitoring (WASA, WAMS), operation SCADA, and condition monitoring and diagnosis (CMD) and non-operational traffic.

This Technical Report is based on existing standards for semantics, services, protocols, system configuration language and architecture. It is based on work done by various IEC working groups including:

- Power system IED communication and associated data models;

---

<sup>1</sup> To be published.

- Energy management system application program interface;
- Data and communications security;
- Interoperability within TC 57 in the long term;
- Industrial networks;
- Highly Available Automation Networks.

Contributions were included from:

- IEEE 802.1 WG (Higher layer LAN protocols);
- IEEE 1588 WG (Precise Networked Clock Synchronization);
- IEEE Power System Relaying Committee (PSRC);
- UCA International Users Group;
- The North American Synchrophasor Initiative (NASPI);
- CEN/CENELEC/ETSI Smart Grids Coordination Group;
- CIGRE working groups D2.26, D2.28, D2/B5.30, D2.35; and
- Different utilities, providers and research institutes, in particular the Central Research Institute of Electric Power Industry (Japan), Hydro-Quebec [50]<sup>2</sup> (Canada), Swissgrid (Switzerland) and ENEL (Italy).

---

<sup>2</sup> Numbers in square brackets refer to the bibliography.

## COMMUNICATION NETWORKS AND SYSTEMS FOR POWER UTILITY AUTOMATION –

### Part 90-12: Wide area network engineering guidelines

#### 1 Scope

This Technical Report is intended for an audience familiar with electrical power automation based on IEC 61850 and particularly for data network engineers and system integrators. It is intended to help them to understand the technologies, configure a wide area network, define requirements, write specifications, select components and conduct tests.

This Technical Report provides definitions, guidelines, and recommendations for the engineering of WANs, in particular for protection, control and monitoring based on IEC 61850 and related standards.

This Technical Report addresses substation-to-substation communication, substation-to-control centre and control centre-to-control centre communication. In particular, this Technical Report addresses the most critical aspects of IEC 61850 such as protection related data transmission via GOOSE and SMVs, and the multicast transfer of large volumes of synchrophasor data.

The Technical Report addresses issues such as topology, redundancy, traffic latency and quality of service, traffic management, clock synchronization, security and maintenance of the network.

This Technical Report contains use cases that show how utilities tackle their WAN engineering.

#### 2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60050, *International Electrotechnical Vocabulary*

IEC 60834-1, *Teleprotection equipment of power systems – Performance and testing – Part 1: Command systems*

IEC 60834-2, *Performance and testing of teleprotection equipment of power systems – Part 2: Analogue comparison systems*

IEC 60870-5-104, *Telecontrol equipment and systems – Part 5-104: Transmission protocols – Network access for IEC 60870-5-101 using standard transport profiles*

IEC 61400-25 (all parts), *Wind turbines – Communications for monitoring and control of wind power plants*

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 61588:2009, *Precision clock synchronization protocol for networked measurement and control systems*

IEC 61850-5:2013, *Communication networks and systems for power utility automation – Part 5: Communication requirements for functions and device models*

IEC 61850-8-1, *Communication networks and systems for power utility automation – Part 8-1: Specific communication service mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3*

IEC 61850-9-2:2011, *Communication networks and systems for power utility automation – Part 9-2: Specific communication service mapping (SCSM) – Sampled values over ISO/IEC 8802-3*

IEC PAS 61850-9-3:2015, *Communication networks and systems for power utility automation – Part 9-3: Precision time protocol profile for power utility automation*

IEC TR 61850-90-1:2010, *Communication networks and systems for power utility automation – Part 90-1: Use of IEC 61850 for the communication between substations*

IEC TR 61850-90-2:2015, *Communication networks and systems for power utility automation – Part 90-2: Use of IEC 61850 for the communication between substations and control centres<sup>3</sup>*

IEC TR 61850-90-4:2013, *Communication networks and systems for power utility automation – Part 90-4: Network engineering guidelines*

IEC TR 61850-90-5:2012, *Communication networks and systems for power utility automation – Part 90-5: Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118*

IEC 61869-9, *Instrument Transformers – Part 9: Digital interface for instrument transformers<sup>3</sup>*

IEC TS 62351-1, *Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security – Introduction to security issues*

IEC TS 62351-2, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms*

IEC 62351-3, *Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP*

IEC TS 62351-4, *Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS*

IEC TS 62351-5, *Power systems management and associated information exchange – Data and communications security – Part 5: Security for IEC 60870-5 and derivatives*

IEC TS 62351-6, *Power systems management and associated information exchange – Data and communications security – Part 6: Security for IEC 61850*

---

<sup>3</sup> To be published.

IEC TS 62351-7, *Power systems management and associated information exchange – Data and communications security – Part 7: Network and system management (NSM) data object models*

IEC TS 62351-8, *Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control*

IEC TS 62351-9, *Power systems management and associated information exchange – Data and communications security – Part 9: Cyber security key management for power system equipment*<sup>4</sup>

IEC TR 62351-10, *Power systems management and associated information exchange – Data and communications security – Part 10: Security architecture guidelines*

IEC 62351-11, *Power systems management and associated information exchange – Data and communications security – Part 11: Security for XML files*<sup>5</sup>

IEC TR 62357-200, *Power systems management and associated information exchange – Part 200: Guidelines for migration to Internet Protocol version 6 (IPv6)*

IEC 62439-1:2010, *Industrial communication networks – High availability automation networks – Part 1: General concepts and calculation methods*

IEC 62439-3:—, *Industrial communication networks – High availability automation networks – Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR)*<sup>6</sup>

IEC TS 62443-1-1, *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*

IEC 62443-2-1, *Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program*

IEC TR 62443-3 (all parts), *Industrial communication networks – Network and system security*

IEC TR 62443-3-1, *Industrial communication networks – Network and system security – Part 3-1: Security technologies for industrial automation and control systems*

IEC 62488-1, *Power line communication systems for power utility applications – Part 1: Planning of analogue and digital power line carrier systems operating over EHV/HV/MV electricity grids*

ANSI T1.403-1999, *Network and Customer Installation Interfaces – DS1 Electrical Interface*

IEEE 802.1ag, *IEEE standards for local and metropolitan area network; Virtual Bridged Local Area Networks Amendment 5: Connectivity Fault Management*

IEEE 802.1ah, *IEEE standards for local and metropolitan area network; Provider Backbone Bridges*

---

4 To be published.

5 To be published.

6 To be published.

IEEE 802.1Qay, *Provider Backbone Bridge Traffic Engineering*

IEEE 802.1X, *Port-based Network Access Control*

IEEE 802.3, *IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications*

IEEE 487.3, *IEEE Standard for the Electrical Protection of Communication Facilities Serving Electric Supply Locations Through the Use of Hybrid Facilities*

IEEE 802.1Q, *IEEE standards for local and metropolitan area network; Virtual bridged local area networks (VLANs and priorities)*

ITU-T G.703, *Physical/electrical characteristics of hierarchical digital interfaces*

ITU-T G.707/Y.1322, *Network node interface for the synchronous digital hierarchy (SDH)*

ITU-T G.803, *Architecture of Transport Networks Based on Synchronous Digital Hierarchy (SDH)*

ITU-T G.810, *Definitions and terminology for synchronization networks*

ITU-T G.811, *Timing characteristics of primary reference clocks*

ITU-T G.812, *Timing Requirements of SDH Equipment Slave Clocks (SEC)*

ITU-T G.813, *Timing Requirements of Slave Clocks Suitable as Node Clocks in Synchronization Networks (SEC)*

ITU-T G.821, *Error performance of an international digital connection operating at a bit rate below the primary rate and forming part of an Integrated Services Digital Network*

ITU-T G.8260, *Definition and terminology for synchronization in Packet Networks*

ITU-T G.8265, *Architecture and requirements for packet-based frequency delivery*

ITU-T G.8265.1, *Precision Time Protocol telecom profile for frequency synchronization*

ITU-T G.8275.1, *Precision Time Protocol telecom profile for phase/time synchronization*

ITU-T G.7041, *Generic Framing Procedure*

ITU-T G.7042, *Link Capacity Adjustment Scheme*

ITU-T G.8032, *Ethernet ring protection switching*

ITU-T G.8261, *Timing and synchronization aspects in packet networks*

ITU-T G.8262, *Timing characteristics of a synchronous Ethernet equipment slave clock*

ITU-T G.8264, *Distribution of timing information through packet networks*

ITU-T Y.1731, *OAM functions and mechanisms for Ethernet based networks*



RFC 0768, *User Datagram Protocol (UDP)*

RFC 0791, *Internet Protocol (IPv4)*

RFC 0792, *Internet Control Message Protocol (ICMPv4)*

RFC 0793, *Transmission Control Protocol (TCP), Protocol Specification*

RFC 0826, *An Ethernet Address Resolution Protocol (ARP)*

RFC 0894, *A Standard for the Transmission of IP Datagrams over Ethernet Networks*

RFC 1240, *OSI Connectionless Transport Services on top of UDP, Version 1*

RFC 1661, *The Point-to-Point Protocol (PPP)*

RFC 1918, *Address Allocation for Private Internet*

RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*

RFC 2328, *OSPF Version 2*

RFC 2460, *Internet Protocol, Version 6 (IPv6) Specification*

RFC 2464, *Transmission of IPv6 Packets over Ethernet Networks*

RFC 2474, *Definition of Differentiated Services Field (DS Field) in IPv4 and IPv6 Headers*

RFC 2615, *Point-to-Point Protocol over SDH/SONET*

RFC 2663, *IP Network Address Translator (NAT) Terminology and Considerations*

RFC 3022, *Traditional IP Network Address Translator (Traditional NAT)*

RFC 3031, *Multiprotocol Label Switching Architecture*

RFC 3168, *The Addition of Explicit Congestion Notification (ECN) to IP*

RFC 3246, *An Expedited Forwarding PHB (Per-Hop Behavior)*

RFC 3247, *Supplemental Information for the New Definition of the EF PHB (Expedited Forwarding Per-Hop Behavior)*

RFC 3260, *New Terminology and Clarifications for DiffServ*

RFC 3261, *SIP: Session Initiation Protocol*

RFC 3376, *Internet Group Management Protocol, Version 3*

RFC 3410, *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*

RFC 3547, *The Group Domain of Interpretation*

RFC 3985, *Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture*

RFC 4193, *Unique Local IPv6 Unicast Addresses*

RFC 4213, *Basic Transition Mechanisms for IPv6 Hosts and Routers*

RFC 4291, *IP Version 6 Addressing Architecture*

RFC 4301, *Security Architecture for the Internet Protocol (IPsec)*

RFC 4303, *IP Encapsulating Security Payload (ESP)*

RFC 4330, *Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI*

RFC 4459, *MTU and Fragmentation Issues with In-the-Network Tunneling*

RFC 4664, *Framework for Layer 2 Virtual Private Networks (L2VPNs)*

RFC 4861, *Neighbor Discovery for IP version 6 (IPv6)*

RFC 5246, *The Transport Level Security (TLS) Protocol Version 1.2*

RFC 5424, *The Syslog Protocol*

RFC 5641, *Layer 2 Tunneling Protocol Version 3 (L2TPv3) Extended Circuit Status Values*

RFC 5771, *IANA Guidelines for IPv4 Multicast Address Assignments*

RFC 5880, *Bidirectional Forwarding Detection (BFD)*

RFC 5905, *Network Time Protocol version 4*

RFC 6052, *IPv6 Addressing of IPv4/IPv6 Translators*

RFC 6864, *Updated Specification of the IPv4 ID Field*

RFC 7011, *Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information*

### **3 Terms, definitions, abbreviations, acronyms and symbols**

#### **3.1 Terms and definitions**

For the purposes of this document the terms and definitions given in IEC 60050-191 [6], as well as the following, apply.

##### **3.1.1 availability**

###### **3.1.1.1 availability**

<of an item>ability to be in a state to perform as required

Note 1 to entry: Availability depends upon the combined characteristics of the reliability (192-01-24), recoverability (192-01-25), and maintainability (192-01-27) of the item, and the maintenance support performance (192-01-29).

Note 2 to entry: Availability may be quantified using measures defined in Section 192-08, Availability related measures.

[SOURCE: IEC 60050-192:2015 [7] (192-01-23)]

#### **3.1.1.2**

##### **punctual availability**

probability of a system to be operational at a given point in time or over a given interval

#### **3.1.1.3**

##### **asymptotic availability**

ratio of mean up time to the sum of mean up time and mean down time over a given time interval

#### **3.1.1.4**

##### **availability**

<of a data security system> subjective quality of a data security system to maintain its service in the face of malicious attacks

#### **3.1.2**

##### **access network**

A network that connects a substation or power plant LAN to a WAN, at a lower hierarchical level (in contrast to core network)

#### **3.1.3**

##### **add-drop multiplexer**

network node in the SDH/SONET network

#### **3.1.4**

##### **backbone**

synonym for core network

#### **3.1.5**

##### **backhaul**

synonym for access network (middle level with three levels of hierarchy)

#### **3.1.6**

##### **bridge**

network device that connects network segments at the data link layer (Layer 2) of the OSI model

[SOURCE: ISO/IEC 10038 and ANSI/IEEE 802.1D:2004]

#### **3.1.7**

##### **Carrier Ethernet**

extensions to Ethernet that enable use of this technology in a WAN or MAN

#### **3.1.8**

##### **core network**

top-level network in the utility hierarchy

#### **3.1.9**

##### **commercial traffic**

data traffic over excess bandwidth that utilities sell to Internet Service Providers or lease to other companies

### 3.1.10

#### **congruency**

property of a network to allocate the same path for backward and forward traffic between end points, ensuring that the delays are approximatively identical

### 3.1.11

#### **customer edge**

IP router located at the edge of the customer network and administrated by the customer, which connects to the next IP router in the provider network

### 3.1.12

#### **deterministic delay**

characteristic of a communication system that the latency from end-to-end has a maximum bound, independently of traffic, except in case of failure or disturbance

### 3.1.13

#### **dependability**

probability that a system will perform correctly when required to in the presence of faults

Note 1 to entry: This definition is aligned with IEC 60834-1 and is different from IEC 60050-192:2015 [7].

### 3.1.14

#### **encapsulation**

transport from end to end of protocol data over another protocol

### 3.1.15

#### **enterprise traffic**

data traffic supporting the enterprise, such as email, data servers, accounting, software updates, etc.

### 3.1.16

#### **fault**

abnormal electricity flow requiring reaction of a protection device

### 3.1.17

#### **Frame Relay**

1990 telephony technology providing permanent virtual circuits

### 3.1.18

#### **grid**

electrical interconnection

### 3.1.19

#### **integrity**

#### **3.1.19.1**

##### **integrity**

<of a data stream> probability of undetected errors in a data stream subject to a certain bit error ratio

#### **3.1.19.2**

##### **integrity**

<of a system> quality of a system not to produce undetected erroneous data

#### **3.1.19.3**

##### **integrity**

<of a data security system> subjected quality of a data security system to resist malicious forging of information

Note 1 to entry: This document uses the term “authenticity” instead.

### **3.1.20**

#### **jitter**

variation of the latency, expressed in relative time (e.g.  $\pm 10$  ms) or in percentage of the latency (e.g.  $\pm 0,1$  %)

### **3.1.21**

#### **latency**

one-way time delay between two end-to-end network interfaces, excluding the delay that the end devices take to process the signal

Note 1 to entry: In this document, “latency” is synonymous to “communication delay” or “network delay”, but not to “transfer delay” (IEC 61850-5), which is the application to application delay.

### **3.1.22**

#### **network**

data transmission system

Note 1 to entry: The term “network” is reserved for data networks, for electrical interconnection “grid” is used instead.

### **3.1.23**

#### **operational traffic**

data traffic needed to protect, operate and supervise the electrical elements of the grid

Note 1 to entry: This includes traffic critical for the maintenance of the grid, e.g. emergency phones, staff organization, messaging or access to documentation.

### **3.1.24**

#### **overlay network**

data network build using the services of an underlying network

EXAMPLE IP on top of SDH.

### **3.1.25**

#### **persistency**

ability of a system to continue producing correct data in the presence of faults

### **3.1.26**

#### **pseudowire**

emulation of a direct, not shared wire with constrained latency using a PSN

### **3.1.27**

#### **protection**

##### **3.1.27.1**

#### **protection**

<of a power grid> measures to avoid damages by acting on circuit breakers or other power control devices

Note 1 to entry: This document uses “protection” and “teleprotection” exclusively for this meaning.

##### **3.1.27.2**

#### **protection**

<in relation to a data path> measures taken to ensure availability in the case of failure of the active data path

Note 1 to entry: This document uses the terms “redundancy” and “fault-tolerance” instead. However, “protection” in this sense still appears in abbreviations and referenced documents.

### 3.1.27.3

#### **protection**

<in relation to a cyber-security> measures taken to prevent or fend off cyber-attacks

Note 1 to entry: This document uses the term “defense” instead. However, “protection” still appears in abbreviations and referenced documents.

### 3.1.28

#### **private address**

address belonging to an address range administrated by the network operator, reusable in another network

### 3.1.29

#### **provider edge**

node located at the edge of the provider network and administrated by the provider, which connects to the customer network’s customer edge node

### 3.1.30

#### **public address**

address belonging to an address range allocated by IANA or IEEE, which is unique in the context of the network

### 3.1.31

#### **public internet**

worldwide network using public addresses

### 3.1.32

#### **quality of service**

#### **QoS**

set of metrics for the performance offered by a communication system, among them: latency (delay), jitter (delay variation), delay asymmetry, throughput (bit rate), packet loss rate, bit error ratio (BER), flow sequence preservation, but excluding security aspects

### 3.1.33

#### **router**

network node able to route traffic, either through dynamic paths (IP) or through pre-established paths (MPLS) at Layer 3

### 3.1.34

#### **traffic engineering**

allocation of network resources (prioritized queues, bandwidth, time slots, etc.) to achieve a certain QoS

### 3.1.35

#### **triple play**

transmission of voice, video and internet

### 3.1.36

#### **unavailability**

expression of availability as the time during which a system is not available over a time interval (e.g. 2 min/year)

### 3.1.37

#### **virtual leased line**

#### **VLL**

point-to-point connection overlaid on top of another network, also called VPC or VPWS

**3.1.38****virtual private circuit****VPC**

point-to-point connection overlaid on top of another network, also called VLL or VPWS

**3.1.39****virtual private LAN service****VPLS**

point-to-multipoint connection overlaid on top of another network

**3.1.40****virtual private wire service****VPWS**

point-to-point connection overlaid on top of another network, which it possibly shares with other VPCs, also called VPC or VLL

**3.1.41****virtual private network****VPN**

network overlaid on top of another network, which it possibly shares with other VPNs

**3.2 Abbreviations and acronyms**

6LoWPAN	IPv6 over Low power Wireless Personal Area Network [RFC 4919], [RFC 6775]
AAA	Authentication, Authorization and Accounting (security)
AAAA-record	128-bit IPv6 address record from DNS [IPv6]
ACL	Access Control Lists [IP]
ADM	Add Drop Multiplexer [SDH]
ADSS	All Dielectric Self-Supporting (optical fiber)
AF	Assured Forwarding [RFC 3260]
AH	Authentication Header [RFC 4302]
ALG	Application Layer Gateway
APLC	Analog Power Line Carrier
AR	Access Router (node)
A-record	32-bit IPv4 address record from DNS
ARP	Address Resolution Protocol [RFC 0826]
ATM	Asynchronous Transfer Mode [ITU-T]
BC	Boundary Clock [IEC 61588]
BER	Bit Error Ratio
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol (successor of EGP in Internet)
BIDIR-PIM	Bi-Directional-Protocol Independent Multicast
BITS	Building Integrated Timing Supply
BLSR	Bidirectional Line Switch Ring
Capex	Capital expenditures
CBS	Committed Burst Size [MEF]
CC	Control Centre
CCTV	Closed Circuit TeleVision
CDM	Code Division Multiplex
CDMA	Code Division Multiple Access

CE	Customer Edge (node)
CEM	Circuit EMulation
CES	Circuit Emulation Services
CESoPSN	Circuit Emulation Services over Public Switched Network [ITU-T Y.1413, Y.1453]
CFM	Connectivity Fault Management
CIA	Confidentiality, Integrity, Availability (against malicious attacks)
CIDR	Classless InterDomain Routing [RFC 4632]
CIGRE	Conseil International des Grands Réseaux Electriques
CIR	Committed Information Rate
CMD	Condition Monitoring and Diagnosis
CoS	Class of Service [IEEE 802.1Q]
COTS	Common, off-the-shelf software
CPE	Central Processing Equipment (WAMPAC)
CWDM	Coarse Wavelength Division Multiplexing (ITU-T G.671, see WDM, DWDM)
DAC	Doubly Attached Clock
DACS	Digital Access Carrier System (UK)
DACS	Digital Access Cross-connect System (US)
DANH	Doubly Attached Node with HSR [IEC 62439-3]
DCC	Data Communications Channel (SDH/SONET)
DCN	Data Communications Network (SDH/SONET)
DF	Don't Fragment [IPv4]
DHCP	Dynamic Host Configuration Protocol [RFC 2131]
DiffServ	Differentiated Services [RFC 2474]
DMZ	DeMilitarized Zone
DNP3	Distributed Network Protocol [IEEE 1815]
DNS	Domain Name Server
DoS	Denial of Service (security)
DPLC	Digital Power Line Carrier
DS	Digital Signal (SDH channel)
DSCP	Differentiated Services CodePoint [RFC 4594]
DSO	Distribution System Operator
DTLS	Datagram Transport Layer Security [RFC 6347]
DWDM	Dense Wavelength Division Multiplexer [ITU-T G.694.1]
EAP	Extensible Authentication Protocol [RFC 3748]
EAPoL	Extensible Authentication Protocol over LAN
EBS	Excess Burst Size [MEF]
ECMP	Equal Cost MultiPath Routing
ECN	Explicit Congestion Notification
EEC	Ethernet Equipment Clock [G.8261]
EF	Expedited Forwarding [RFC 3246/RFC 3247]
EGP	Exterior Gateway Protocol [RFC 904]
EHV	Extra High Voltage



EIR	Excess Information rate [MEF]
E-LAN	Ethernet LAN service [MEF]
E-line	Ethernet wire service [MEF]
E-LMI	Ethernet Local Management interface
EMS	Energy Management System
EoATM	Ethernet over ATM
EoS	Ethernet over SDH/SONET
EoSDH	Ethernet over SDH
EoSONET	Ethernet over SONET
EoTDM	Ethernet over TDM
ERPS	Ethernet Ring Protection Switching [G.8032]
ESMC	Ethernet Synchronization Messaging Channel [G.8264]
ESP	Electronic Security Perimeter
ESP	Encapsulating Security Payload
E-tree	Routed-Multipoint EVC Ethernet (point-to-multipoint service) [MEF]
EVPL	Ethernet Virtual Private Line [MEF]
EXP	EXPerimental [MPLS]
FCAPS	Fault Configuration Accounting Performance Security
FDB	Filtering DataBase [IEEE 802.3]
FDM	Frequency Division Multiplexing
FDV	Frame Delay Variation [MEF]
FRR	Fast Re Route [MPLS]
FTP	File Transfer Protocol [RFC 959]
GDOI	Group Domain of Interpretation [RFC 6407]
GFP	Generic Framing Procedure [G.7041]
GMC	GrandMaster Clock [IEC 61588]
GMPLS	Generalized MPLS
GNSS	Global Navigation Satellite System
GOOSE	Generic Object-Oriented Substation Event [IEC 61850-7-2, IEC 61850-8-1]
GPRS	General Packet Radio Service (2 <sup>nd</sup> generation cell phone)
GPS	Global Positioning System
GSM	Global System for Mobile communications (1st generation cell phone)
HAN	Home Area Network
HMAC	Hash-based Message Authentication Code
HMI	Human-Machine Interface
HSPA	High-Speed Packet Access (3 <sup>rd</sup> generation cell phone)
HSR	High-availability Seamless Redundancy [IEC 62439-3]
HTTP	Hypertext Transfer Protocol [RFC 7230-7237]
HV	High Voltage
IAM	Identity and Access Management
IANA	Internet Assigned Numbers Authority
ICCP	Inter-Control Centre Protocol [IEC 61870-6]
ICMP	Internet Control Message Protocol [RFC 792]

ID	IDentity
IDS	Intrusion Detection System
IED	Intelligent Electronic Device [IEC 61850]
IGMP	Internet Group Management Protocol [RFC 3376]
IGP	Internal Gateway Protocol
IntServ	Integrated Services [RFC 2210]
IP	Internet Protocol [RFC 791]
IP/MPLS	MPLS with IP routing
IPS	Intrusion Protection System
IRIG	Inter-Range Instrumentation Group
ISDN	Integrated Services Digital Network [ITU-T]
IS-IS	Intermediate System to Intermediate System [ISO/IEC 10589]
KDC	Key Distribution Centre
L2TP	Layer 2 Tunneling Protocol [RFC 5641]
L2VPN	Layer 2 VPN [RFC 7152]
L3VPN	Layer 3 VPN
LAN	Local Area Network
LCAS	Line Capacity Adjustment Scheme (SDH/SONET NG) [G.7042]
LDP	Label Distribution Protocol [RFC 5036]
LER	Label Edge Router [MPLS]
LKR	Lock Report [MPLS]
LLDP	Link Layer Discovery Protocol [IEEE 802.1AB]
LSP	Label Switching Path (MPLS)
LSR	Label Switching Router (MPLS)
LTE	Long-Term Evolution (4 <sup>th</sup> generation cell phone)
LV	Low Voltage
MAC	Medium Access Control [IEEE 802.1]
MAC	Message Authentication Code (security)
MACsec	MAC security [IEEE 802.1AE]
MAN	Metropolitan Area Network
MC	Master Clock [IEC 61588]
MEF	Metro Ethernet Forum
MF	More Fragment [IPv4]
MFA	MPLS Forum Association (now IPMPLS)
MIB	Management Information Base (SNMP)
MMS	Manufacturing Messaging Specification (ISO 9506)
MP2MP	Multipeers-to-multipeers
MPLS	Multi-Protocol Label Switching [RFC 3031]
MPLS-TP	MPLS with Traffic Profiling
MTBR	Mean Time Between Repairs
MTTF	Mean Time To Failure
MTU	Maximum Transmission Unit
MV	Medium Voltage

NAC	Network Access Control
NASPI	North American SynchroPhasor Initiative
NAT	Network Address Translation [RFC 2663/RFC 3022]
NCD	Network Configuration Description [IEC 61850-6]
NDP	Neighbor Discovery Protocol [RFC 4861]
NERC	North-american Electricity Reliability Corporation
NMS	Network Management Services
NPCC	Northeast Power Coordinating Council
NPDU	Network Protocol Data Unit [ISO/IEC 7498]
NTP	Network Time Protocol [RFC 5905]
OAM	Operation, Administration and Maintenance
OC	Optical Carrier (SONET channel)
Opex	Operation expenditures
OPGW	Optical Ground Wire (high voltage transmission cable)
OS	Operating System
OSI	Open System Interconnection [ISO/IEC 7498]
OSPF	Open Shortest Path First [RFC 5340]
OSSP	Organization Specific Slow Protocol [IEEE 802.3]
OTN	Optical Transport Network (ITU-T G.709)
P2MP	Point To Multipoint (Peer to Multipeers)
P2P	Point-to-Point (Peer-to-Peer)
PABX	Private Automatic Branch eXchange (telephony)
PBB	Provider Backbone Bridging ("Mac-in-Mac", IEEE 802.1ah-2008)
PBB-TE	Provider Backbone Bridge Traffic Engineering (IEEE 802.1Qay-2009)
PCM	Pulse Code Modulation
PDC	Phasor Data Concentrator [IEC TR 61850-90-5]
PDH	Plesiochronous Digital Hierarchy (ITU-T)
PDU	Protocol Data Unit [ISO/IEC 7498]
PDV	Packet Delay Variation [RFC 3393, ITU-T G.8260 (PSN), ITU-T Y.1541 (IP), ITU-T Y.1563 (Ethernet)]
PE	Provider Edge (node)
PFD	Probability to Fail (dangerously) on Demand [IEC 61508]
PHB	Per Hop Behavior [MPLS]
PIM-SM	Protocol Independent Multicast – Sparse Mode [RFC 4601]
PM	Performance Monitoring
PMU	Phasor Measurement Unit
PMU	Phasor Measurement Unit [IEC TR 61850-90-5]
PON	Passive Optical Network
POS	Packet over SDH/SONET
POTS	Plain Old Telephone System
ppm	part per million (replaced by $\mu\text{Hz}/\text{Hz}$ or $\mu\text{s}/\text{s}$ )
PPP	Point-to-Point Protocol [RFC 1661]
PPS	Pulse Per Second

PRC	Primary Reference Clock
PRP	Parallel Redundancy Protocol [IEC 62439-3]
PRTC	Primary Reference Time Clock
PS	Power Station
PSN	Packet Switched Network
PTP	Precision Time Protocol [IEC 61588]
PW	Pseudo-Wire (pseudo wire)
PWE3	Pseudo-Wire Edge-to-Edge [RFC 3985]
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RAN	Regional Area Network
RAS	Remedial Action Schemes (referred to as WAMPAC in this document)
RBAC	Role Based Access Control
RF	Radio Frequency
RIR	Regional Internet Registry
RP	Rendezvous Point
RPL	Routing Protocol for Low power and lossy networks [RFC 6550]
RSPEC	Reservation Characteristics in IntServ [RFC 2210]
RSTP	Rapid Spanning Tree Protocol [IEEE 802.1D]
RSVP	Resource ReSerVation Protocol [RFC 2205]
RSVP-TE	RSVP-Traffic Engineering
RTU	Remote Terminal Unit (decentralized measurement and control device)
SAToP	Structure-Agnostic TDM over Packet [RFC 4553], [ITU-T Y.1413], [Y.1453]
SCADA	Supervisory Control And Data Acquisition (control centre)
SCL	System Configuration Language [IEC 61850-6]
SCP	Secure Copy (UNIX service)
SDH	Synchronous Digital Hierarchy [ITU-T]
SEM	Security Event Management
SEN	Substation Edge Node
SFP	Small Form-factor Pluggable (Ethernet)
SGAM	Smart Grid Architecture Model [CEN-CENELEC-ETSI Smart Grid Coordination Group]
SHDSL	Single pair Highspeed Digital Line Subscriber
SIM	Security Information Management
SIP	Session Initiation Protocol [RFC 3261]
SIPS	System Integrity Protection Schemes (referred to as WAMPAC in this document)
SLA	Service Level Agreement
SLAAC	StateLess Address Auto Configuration [RFC 4862]
SMV	Sampled Measurement Values [IEC 61850-7-2, IEC 61850-9-2]
SNMP	Simple Network Management Protocol [RFC 3410]
SNTP	Simple Network Time Protocol [RFC 4330]
SONET	Synchronous Optical NETwork
SPDU	Session Protocol Data Unit

SPE	SONET Payload Envelope
SPS	Special Protection System (WAMPAC, called SIPS in this document)
SS	SubStation
SSH	Secure Shell (UNIX service)
SSL	Secure Socket Layer
ssPDC	substation Phasor Data Concentrator
STM	Synchronous Transport Module (SDH/SONET)
STS	Synchronous Transport Signal (SDH/SONET)
SV	Sampled Values (of current and voltage) [IEC 61850-9-2]
SyncE	Synchronous Ethernet [ITU-T G.8010]
TAI	Temps Atomique International
TC	Transparent Clock [IEC 61588]
TCP	Transmission Control Protocol [RFC 0793]
TDM	Time Division Multiplexing
TDMoIP	Time Division Multiplexing over Internet Protocol [ITU-T Y.1413, Y.1453]
TE	Traffic Engineering
TLS	Transport Layer Security
TLV	Time-Length-Value [ISO/IEC 8825 and IEC 61588]
TM	Terminal Multiplexer (SDH/SONET)
ToS	Type of Service
TPDU	Transport Protocol Data Unit [ISO/IEC 7498]
TSAP	Transport Service Access Point
TSPEC	Traffic description in IntServ
TTL	Time To Live (IP, MPLS)
UDP	User Datagram Protocol [RFC 0768]
ULA	Unique Local unicast Address [RFC 4193]
UMTS	Universal Mobile Telecommunications System (3 <sup>rd</sup> generation cell phone)
UNI	User Network Interface [MEF]
UPSR	Unidirectional Path Switch Ring
URL	Unique Resource Locator
UTC	Universal Time Coordinated
VC	Virtual Circuit
VCAT	Virtual Concatenation (SDH/SONET NG) [G.7043]
VCCV	Virtual Circuit Connectivity Verification [RFC 5085]
VDSL	Very high speed Digital Subscriber Line (ITU-T last mile)
VID	VLAN identifier [IEEE 802.1Q]
VLAN	Virtual Local Area Network [IEEE 802.1Q]
VLL	Virtual Leased Line (also called VPWS)
VoIP	Voice over IP
VPLS	Virtual Private LAN Service [RFC 4761 and RFC 4762]
VPMS	Virtual Private Multicast Services [IETF work in progress]
VPN	Virtual Private Network
VPRN	Virtual Routed Private Network (L3VPN for MPLS)

VPWS	Virtual Private Wire Service (pseudo-wire)
VRF	Virtual Routing and Forwarding
VRRP	Virtual Router Redundancy Protocol [RFC 5798]
VT	Virtual Tributary (SDH/SONET)
WAMPAC	Wide Area Monitoring, Protection and Control
WAMS	Wide Area Monitoring System
WAN	Wide Area Network
WASA	Wide Area Situational Awareness
WDM	Wavelength Division Multiplexing
XML	Extended Markup Language
ZBFW	Zone-Based FireWall

### **3.3 Network diagram symbols**

This document uses the symbols shown in Figure 1.

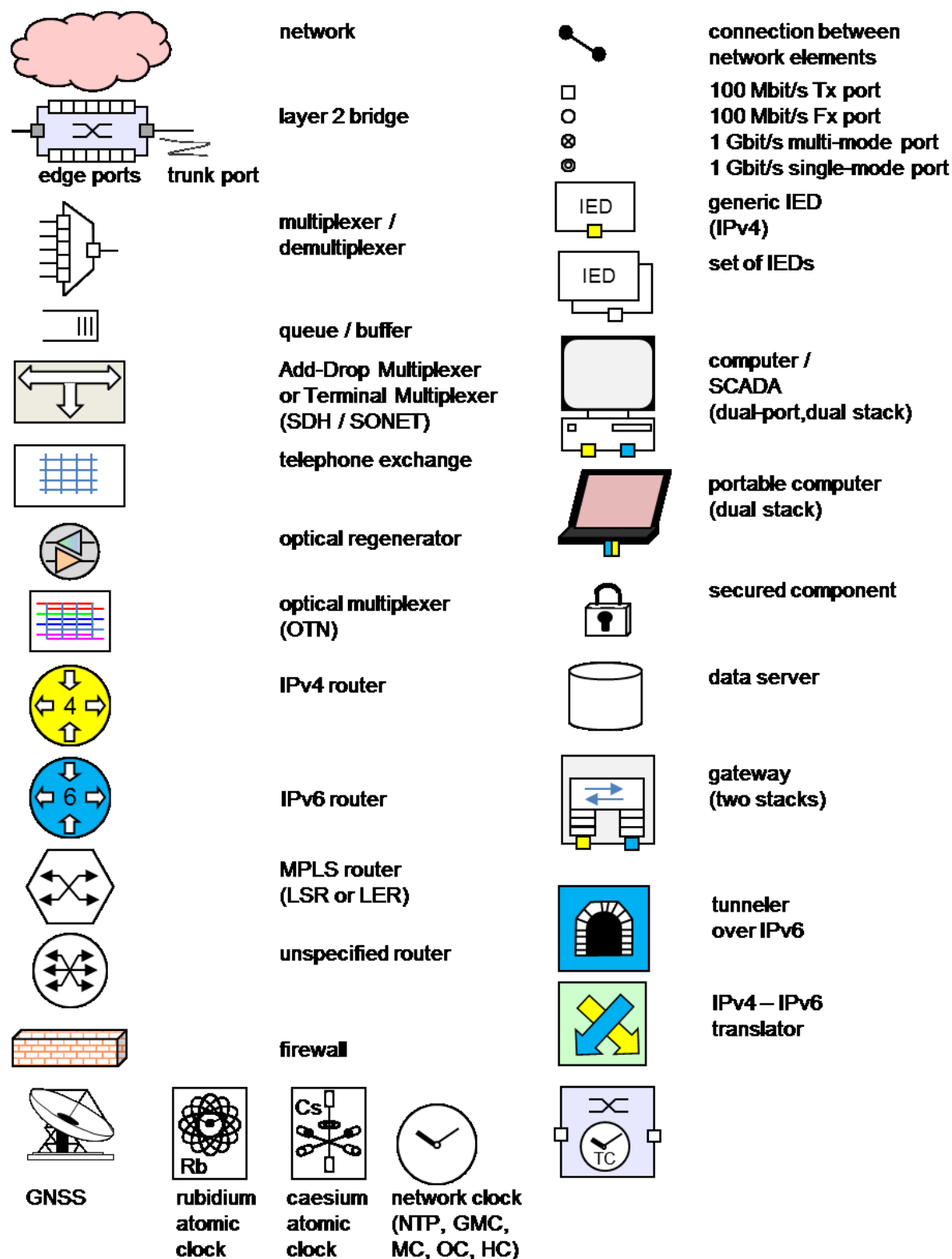


Figure 1 – Symbols

## 4 Wide Area Communication in electrical utilities

### 4.1 Executive summary

The electrical grid is part of the critical infrastructure of a country. The communication network on which the grid relies must have an even higher availability than the grid itself, and has to survive contingencies and blackouts in order to keep the grid stable and restore the grid as quickly as possible, even from a complete black start.

In the past, operational communication (teleprotection, telecontrol, operational voice, etc.) was separate from enterprise communication (energy management, mail, internet, company telephone, etc.). In particular, telephones in substations and control centres were independent from the public telephone system and used dedicated powerline, microwave or radio links. The public telephone system was untrusted since it would break down in case of wide-area emergency, due to the number of simultaneous calls; it would run on batteries for only a few hours after losing the grid, which is insufficient to recover from a land-wide blackout.

The operational network used robust technologies from the established telephony technology (e.g. ATM, SDH/SONET) that guaranteed bandwidth, deterministic latency, predictable jitter and high reliability through redundant paths. The operational network changes little over the years, configuration changes are seldom. The personnel in charge of the legacy network are proficient in this technology, which is however becoming obsolete.

With the deployment of protocols using packet switching such as IEC 61850, the operational telephony network had to transport variable size, sporadic packet traffic in addition to its fixed-size cyclic traffic, a task that it was not designed for and that it did not perform efficiently.

New generation SDH/SONET NG allows more efficient packet transport. Deployment of this technology will continue for some years, especially to support operational traffic, but its further development (e.g. OTN) is uncertain.

New actors appeared as Smart Grids developed (e.g. distributed generation, demand side management, etc.), letting the operational packet-switched traffic grow.

On the other hand, the enterprise network based on internet technologies (email, business servers, internet access, etc.) grew exponentially, requiring bandwidth well in excess of what the operational network needs.

The personnel in charge of the enterprise network have a background oriented towards informatics. They are more experienced in managing large amounts of users and data but less acquainted with the requirements – especially temporal and dependability aspects – of operational networks.

Therefore, a divergence can exist between the philosophy of the department managing traditional operational networks and the department managing the enterprise network. Merging the departments could be as difficult as merging the infrastructures.

Technology advances and technical necessity are not the only motors for change. The lifespan of office equipment (5 to 10 years) is significantly shorter than the lifespan of teleprotection equipment (10 to 25 years). Early obsolescence will cause additional costs during the life cycle, with little benefit for the basic teleprotection function. Total cost of ownership is what counts.

The continuous technological evolution leads to heterogeneous networks, even in the rare cases that started on the green field. Networks consist of clusters of hardware from the same manufacturer, interfacing over a reduced number of specially engineered devices with other clusters from other manufacturers, technologies and vintage. While in networks within substations interoperability of equipment is a major incentive, interoperability within WAN



clusters is not a primary goal, and interchangeability of equipment between manufacturers is not a requirement – as long as spares are available.

Utilities see savings and earnings by merging the operational network with the enterprise network. With the installation of optical fibers with excess bandwidth, they can also offer commercial services to Telecom companies and Internet Service Providers (ISPs).

Merging the networks makes sense as long as the non-operational services do not compromise operation. Indeed, enterprise and commercial communications should not be able to influence the operational communication, either through incorrect messages or through exhaustion of shared resources. In particular, the dynamic services of enterprise networks require frequent human intervention for fixes and updates. This presents a major risk for the grid when sharing the network, a risk the utilities must weigh against the economics of using public networks.

The traditional physical separation between operational, enterprise and commercial data can partially be enforced by virtual private networks (VPNs) and by priority management. However, since the same physical medium carries all traffic, the operational network will dictate the dependability requirements of the enterprise and commercial networks, possibly affecting their economics.

This not only applies to bandwidth and processing power allocation, but also to all resources such as battery backup, maintenance team deployment and spares disposition.

Therefore, a utility has to balance the benefits of merging the infrastructures against the disadvantages of imposing the strict requirements of operational networks onto the whole infrastructure, and may choose to keep the networks separated.

Cost savings also lead utility companies, especially small ones, to outsource communication entirely to a Telecom company or Internet Service Provider under a Service Level Agreement (SLA). Even if the service provider is a trusted entity, its business goals are different from that of the utilities and its operation is not transparent to the electrical utility. Since its teams are not familiar with grid contingencies, they are less aware of the importance of operational data, which they often do not identify as such.

Here again, a utility has to choose between keeping the infrastructure in the ownership of the utility and outsourcing the network.

The network becomes vulnerable to cyber-attacks when it spans over public ground, belongs to third-party providers and connects in some places directly or indirectly to the public internet. The protection of the infrastructure goes beyond what traditional communication needs. A virtual separation may be insufficient, so cyber-security protocols become important, possibly at several levels, depending on the trusted entities. In both owned and outsourced networks, utilities must ensure cybersecurity policies and architectures sometimes exceeding the regulatory requirements (NERC for example).

Only continuous monitoring and sporadic exercising of contingencies with the network team can guarantee grid availability. Cost pressure cannot be an excuse for fair-weather solutions, which later on need costly extensions. Therefore, the evaluation of network solutions must consider comprehensive Operation And Maintenance (OAM) and simulation tools.

These guidelines are intended to give advice on the potential conflict points:

- Traditional telephony versus packet switching networks
- Operation versus enterprise and commercial network
- Utility-owned versus outsourced network
- Defense-in-depth security versus simple application data authentication

Clauses 4, 5 and 6 deal with the network requirements of operational protocols, most of them are covered by IEC standards. These are not the only critical services, as voice transmission for operation and maintenance is indispensable for operation.

Clause 7 describes the technologies from the restricted viewpoint of electrical utilities. It mostly lists what is important to know for procurement and gives appreciation of their usefulness.

Clause 8 consists of use cases. Some use cases are scattered through the document. The first use case in 4.2 is an example that shows the network aspects of a small grid.

## 4.2 Use Case: ENDESA, Andalusia (Spain)

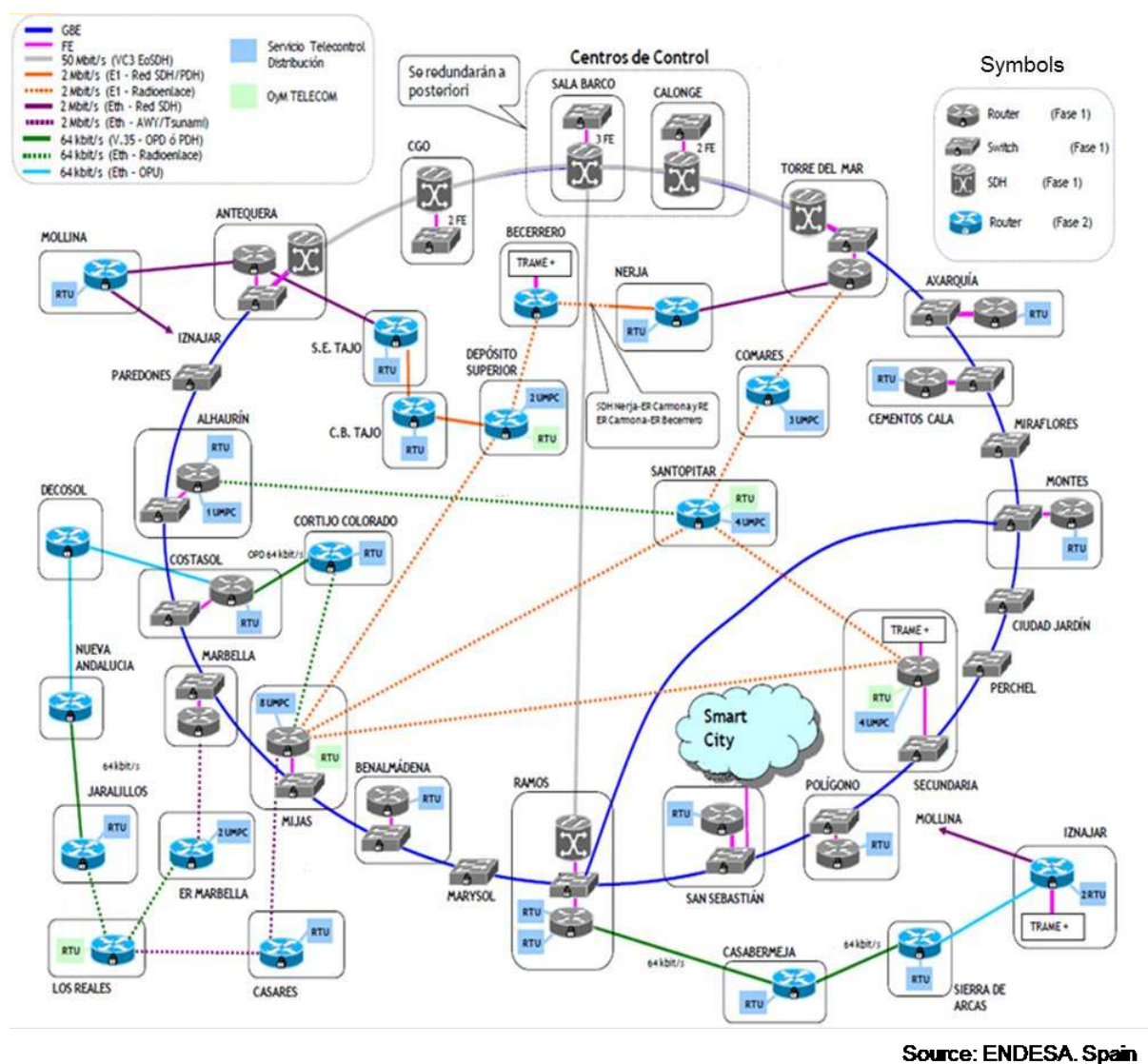
A typical Distribution System Operator (DSO) grid, the Andalusia (southern Spain) grid spans about a 100 km diameter and some 30 substations (Figure 2).



IEC

**Figure 2 – Substation locations in Andalusia**

The network topology is that of a partially meshed ring with spokes and subrings (Figure 3).



IEC

Figure 3 – Topology of the Andalusia network

The northern half of the main ring is a traditional SDH network over VC3; the southern part of the ring uses Gbit/s Metro Ethernet with bridges. Spokes and subrings interconnection use a variety of media: radio links, E1, 100 Mbit/s Ethernet, etc. Routers ensure IP connectivity. The diversity of media, protocols and manufacturers characterizes networks that evolved over time. A special case is the city of San Sebastian with its Smart Grid infrastructure.

The basic services that the Andalusia network provides are:

- Teleprotection
- Telecontrol: generation, substations, regulation, measurements, batteries
- Voice
- Video surveillance
- SCADA
- OAM
- Metering
- Distribution automation

- Synchronization

The guidelines for development were:

- Keep a very high availability
- Reduce costs by sharing links and minimizing their number without losing redundancy
- Allow future evolution and scalability
- Allow integration of public operator and private network where convenient
- Define the SLAs

Evaluation of the technologies considered:

- Investments plan for the next 5 years
- Life cycle for investments (around 10 years)
- Priority to choices with minor operational costs
- Quality of the recommended solutions should be similar in terms of the provided service

#### 4.3 Typical interface between a substation and the WAN

Substations connect to a WAN through a Substation Edge Node (SEN), which aggregates a number of different traffic streams between the substation and the WAN. It can serve as a protocol converter, multiplexer and as a network element, switch or router. The SEN is however not application-aware.

Figure 4 shows a typical SEN in the equipment cabinet of a substation.

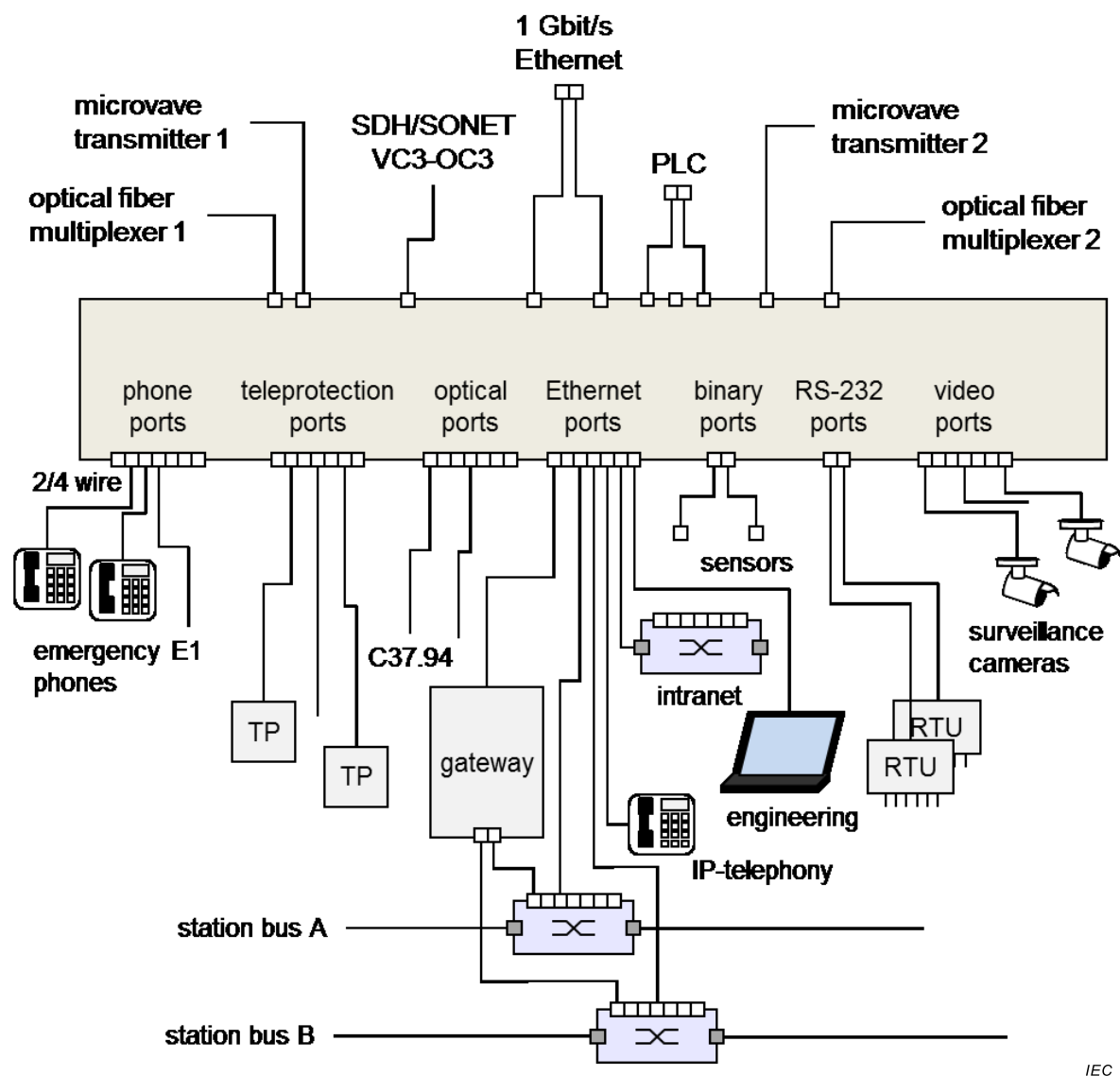


IEC

**Figure 4 – Cabinet of the substation edge node**



Figure 5 shows the typical interfaces of a full-fledged SEN: the lower part goes to the substation equipment and the upper part to the transmission equipment. The actual interfaces installed depend on each substation. Redundancy is an option, depending on the importance; the communication equipment can be duplicated or only parts thereof. IEC 61850 is only a fraction of all communications.



IEC

Figure 5 – Communication interfaces in a SEN

#### 4.4 WAN characteristics and actors

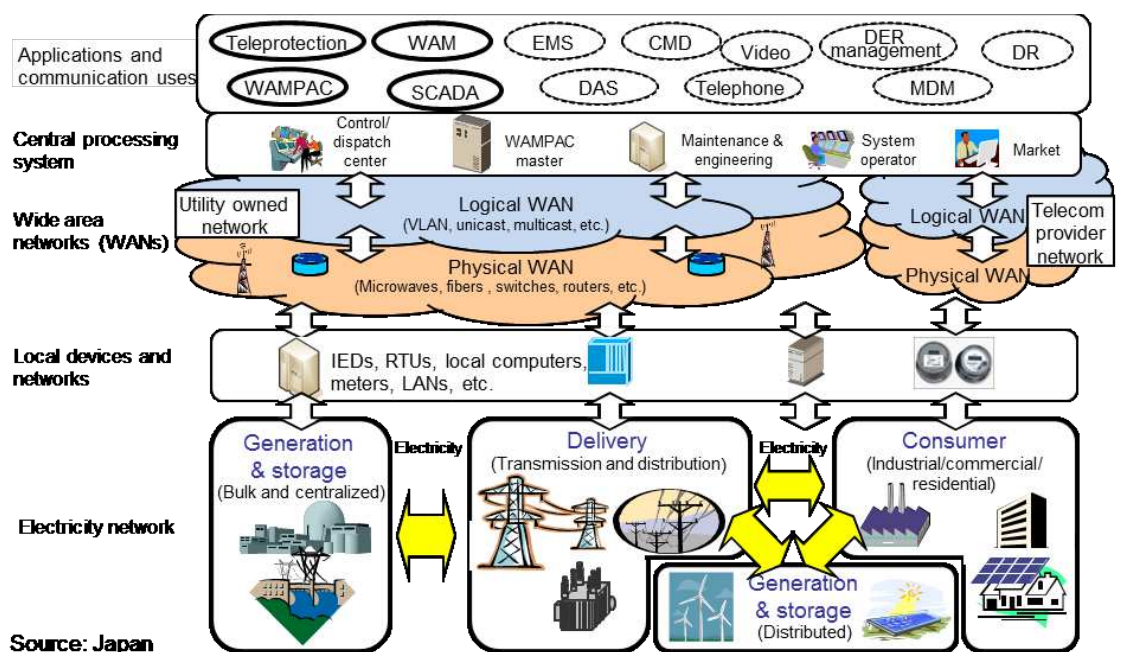
WANs are categorized by:

- Ownership:
  - Private network of a utility
  - Shared network operated by independent utilities or by a national grid, or
  - Public network of telecom service providers
- Hierarchy
  - Core (backbone)
  - Access (backhaul), or

- Local area (regional)
- Networks
  - Physical communication media equipment, or
  - Logical networks providing connectivity over unspecified physical networks.

Figure 6 shows the actors and the WANs.

- On top are the applications using communication, detailed with their requirements in Clause 6.
- The level below shows the processing entities.
- The next level WAN connects the processing entities among themselves and with the remote devices, considering two owners of WANs: utility and telecom provider (leased).
- The bottom level includes the remote devices, representing producers, consumers and substations. The remote devices can also communicate directly over WANs.

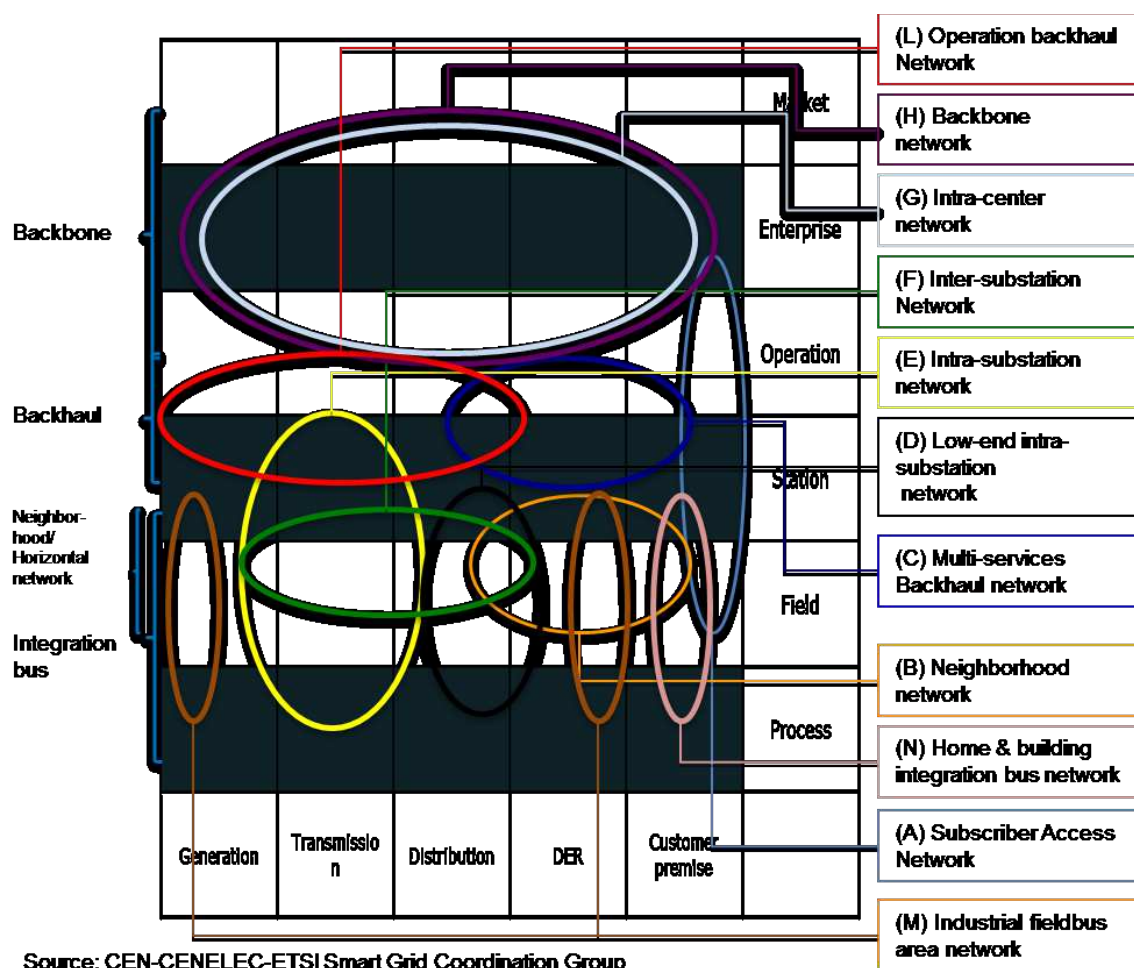


IEC

Figure 6 – Communicating entities

#### 4.5 SGAM Mapping

The SGAM Communication Model [1] details the view of the networks (Figure 7).



IEC

Figure 7 – SGAM communication model

SGAM [1] defines a number of network types, in particular:

- Subscriber access network
- Neighborhood network
- Multi-services backhaul network
- Low-end inter-substation network
- Intra-substation network
- Inter-substation network
- Intra control centre network
- Backbone network
- Operation backhaul network
- Home and building integration network
- Industrial fieldbus area network.

This document only assumes two levels of hierarchy in the wide area network:

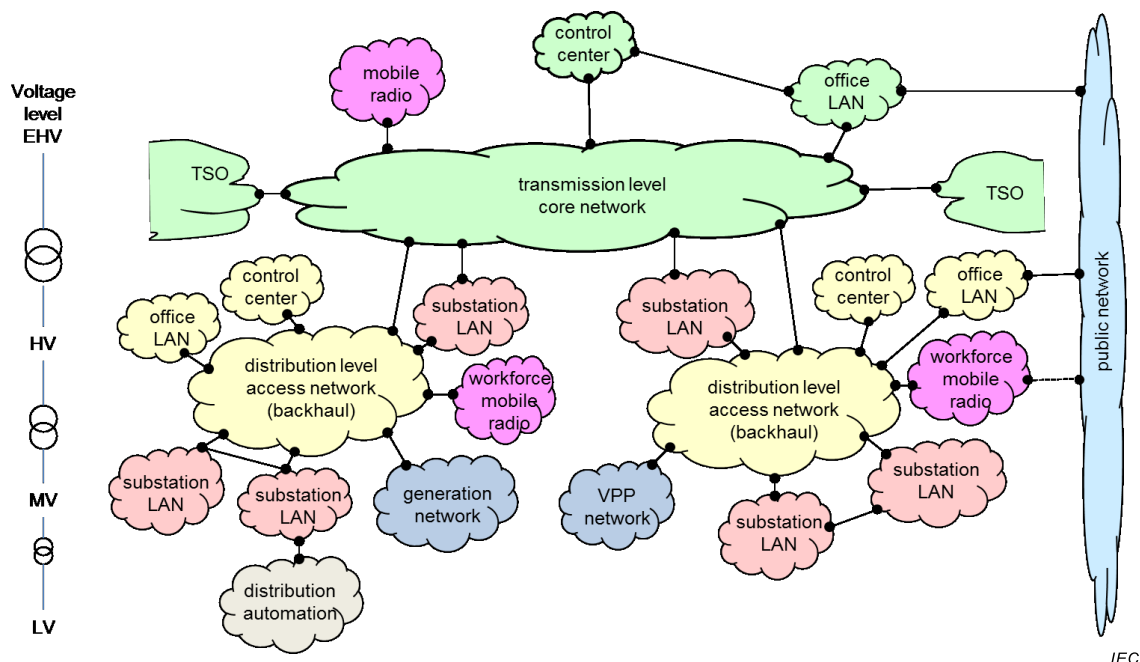
- a) core network, which roughly corresponds to the SGAM backbone network
- b) access or backhaul network, which roughly corresponds to the SGAM inter-substation network and operation backhaul network.

This does not preclude networks with more than two levels of hierarchy.

These concepts are shared with NIST [34].

#### 4.6 Network elements and voltage level

The relationship between voltage levels and network elements appears in Figure 8.



**Figure 8 – Principle of grid voltage level and network technology**

The communication architecture mirrors the grid voltage hierarchy:

- The core network ensures the operation of the Extra High Voltage transmission grid, under responsibility of the TSO. It interfaces to other TSOs and to the DSOs.
- The access networks ensure the operation of the High Voltage and Medium Voltage distribution grid for a reduced number of substations, under the responsibility of the DSOs. They interface to the core network and to the substations.
- The substation LAN ensures the operation of the substation. Substations are normally identical with the connection points between the networks, except at the office and workshop buildings.
- The generation has its own network, e.g. for a wind farm.
- The distribution automation network extends down to the households.
- The networks have interfaces to the public internet (e.g. to access meteorological data and trading information) and to mobile radio networks, either public or operating over disaster-proof radio links.

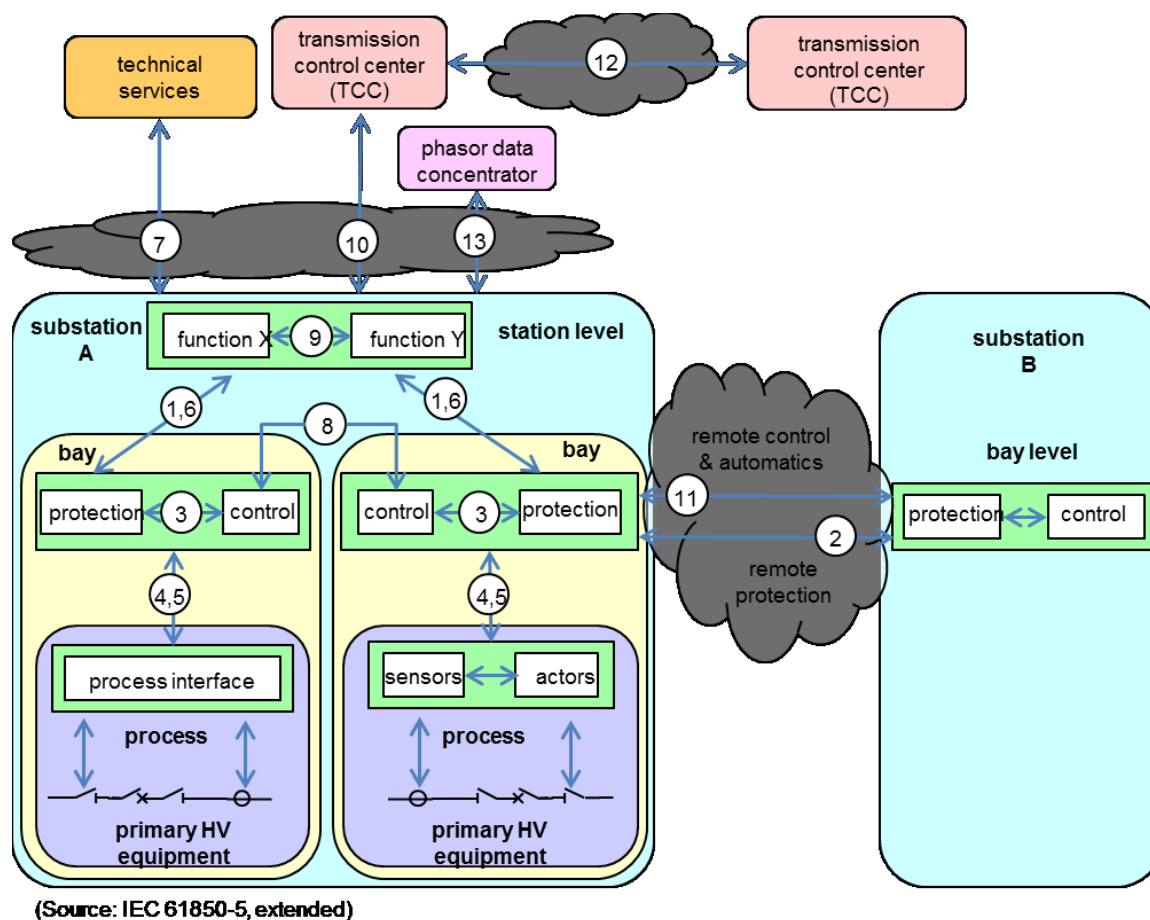
The networks are not homogeneous in technology, vintage and protocols, and require routers or gateways at the network connection points, symbolized by the connected circles in Figure 8.

The communication equipment is located in the substations, with some exceptions such as SCADA, dispatching centres or trading offices.



#### 4.7 WAN interfaces in substation automation (IEC 61850-5)

The model follows the interfaces as defined in IEC 61850-5, extended by WAN elements, as shown in Figure 9.



IEC

**Figure 9 – Communication paths and interfaces**

Meaning of the interfaces in Figure 9:

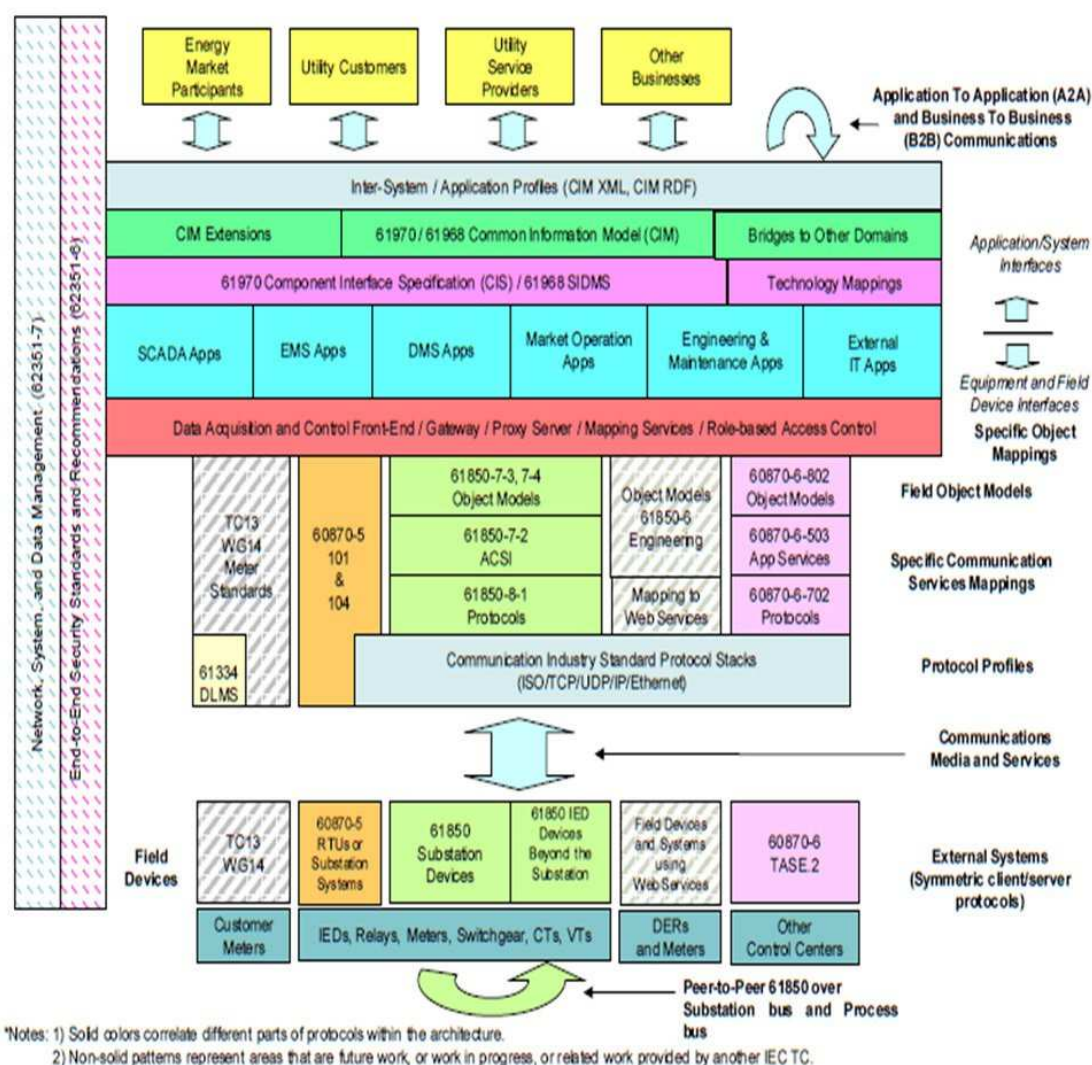
- IF1: protection-data exchange between bay and station level
- IF2: protection-data exchange between bay level and remote protection horizontal time-constrained exchange involving high traffic analog data (e.g. line differential protection) and low traffic binary data (e.g. protection blocking), see IF 11.
- IF3: data exchange within bay level
- IF4: analogue data exchange between process and bay level (samples from current transformer and voltage transformer)
- IF5: control data exchange between process and bay level
- IF6: control data exchange between bay and station level
- IF7: data exchange between substation (level) and a remote engineer's workplace
- IF8: direct data exchange between the bays especially for fast functions like interlocking
- IF9: data exchange within station level
- IF10: vertical data exchange between the substation and remote control centre(s) includes remote monitoring and telecontrol

- IF11: control data exchange between substations  
horizontal exchange involving mainly low-traffic binary data (e.g. for interlocking functions or other inter-substation automatics), see IF2.
- IF12: transmission control centre to transmission control centre (added here)
- IF13: synchrophasors to PDC and control centre (added here)

Figure 9 symbolizes the WAN by the clouds with interfaces IF2, IF7, IF10, IF11, IF12 and IF13. The WAN connects primary substations and Transmission Control Centres.

#### 4.8 Logical interfaces and protocols in the TC57 Architecture IEC TR 62357

IEC 62357 describes the logical interfaces for standardized applications (Figure 10). The boundary between what is in the substation and what is outside can vary.



Source: IEC TR 62357

IEC

Figure 10 – IEC TR 62357 Interfaces, protocols and applications

Applications use utility protocols to exchange data, especially considering the protocols defined in IEC 61850-8-1 and IEC 61850-9-2, IEC TR 61850-90-1, IEC TR 61850-90-2 and IEC TR 61850-90-5.

Several application-layer protocols coexist with IEC 61850, with similar technologies, such as:

- IEC 60870-5-104 (telecontrol)
- IEC 60870-6 (ICCP, TASE-2)
- IEEE 1815 (formerly DNP-3)
- IEC 61400-25 (wind turbines)
- IEEE C37.118 (formerly IEEE 1344) (synchrophasors)

While in substation automation the utility protocols represent the bulk of traffic, outside of the substation, WANs carry a number of other protocols related to operation, such as voice and video surveillance (CCTV).

The actual protocols used are not important for network engineering, only their addressing capability and their timely behavior matter.

In all cases, engineering the different substations or terminals requires tools that generate the SCD files of all participants and in addition the network information. These tools must be able to import the SCD files of each substation and modify them to generate a NCD (network configuration description).

#### **4.9 Network traffic and ownership**

A utility company will strive to reduce the network Capex and Opex by using the same infrastructure for all three major functions:

- 1) Operational services;
- 2) Enterprise services;
- 3) Commercial services.

There are strong reasons to keep the operational network separated from the other traffic:

- Company philosophy of keeping the infrastructure for disaster recovery completely independent of other entities. This especially includes black start ability after a long blackout;
- Easier migration from the traditional telephony services, risk mitigation;
- QoS requirements for the critical operational service that burden the enterprise and commercial services too much.

Utility Companies answer this issue differently. The commercial traffic increases drastically since the operational traffic requires only a low bandwidth and the utilities draw a large number of fibers that they themselves do not need.

Due to the nature of the applications (discussed in Clause 6) and their requirements, utilities use dedicated private communication network, and more seldom Service Provider Networks.

### **5 WAN overall requirements and data transmission metrics**

#### **5.1 Traffic types**

Independently from the application, two major traffic kinds are distinguished:

- 1) periodical or sporadic traffic with strict time constraints, requiring an upper bound to the latency, and consisting of small data items (100 to 200 octets); for instance, process data exchange for protection and commands (GOOSE and SMV), but also voice messages of high quality;  
Networks optimized for that traffic are characterized as Time Division Multiplexing networks (TDM):

- 2) sporadic traffic of messages with relaxed time constraints, satisfied with an average latency, and consisting of large pieces of data, often distributed into separate packets; for instance: MMS data object exchange, events, file transfer, condition monitoring, but also video, management, mail and document transfer;  
Networks optimized for that traffic are characterized as Packet Switching Networks (PSN).

## 5.2 Quality of Service (QoS) of TDM and PSN

QoS expresses how well a network complies with the time and dependability constraints for a given traffic, e.g. throughput, packet losses, errors, latency, jitter, out-of-order, etc. The network provider guarantees a certain QoS in a SLA.

A basic difference exists between TDM and PSN:

- TDM networks such as SDH/SONET transmit data periodically in fixed time slots. Once a circuit is established, the latency from end to end is constant and depends only on the propagation delay of the signal over the medium and on the residence time in the multiplexers, which is nearly constant. When TDM networks are cascaded, depending on the coincidence of the cycles, the latency varies, but will never exceed the sum of the latencies in the individual subnets. This ensures a deterministic latency and jitter (see 5.3.6).  
In TDM, QoS consists only in allocating sufficient bandwidth to time-critical data, since in contrast to industrial networks; the period is fixed (64 kbit/s).
- PSNs such as Ethernet use statistical multiplexing and cannot offer the deterministic latency of a TDM network. While the propagation delay remains constant, the residence delay in the nodes depends on the traffic. Indeed, PSN nodes buffer the traffic in queues and delay incoming messages until their turn in the queue comes. In the worst case, the queue overflows and incoming messages are dropped (overbooking). Therefore, PSNs have a variable average latency depending on the traffic load.  
To ensure that time-critical data are forwarded, PSN use priorities to give the highest priority packets the minimum latency. Even the highest priority class packets may have to wait in output queues behind other packets of the same class or because transmission of lower priority packets already started.  
PSN could guarantee latency if all resources on the path are properly reserved, but this goes at the expenses of efficiency.

QoS is a fundamental difference to consider in the migration from TDM to PSN.

QoS for WANs depends on the underlying network architecture and technology. QoS requires managing traffic based on pre-defined traffic classes, especially to achieve low-latency for critical applications. Typical traffic classes are derived from applications: teleprotection, SCADA, WAMPAC and network management, time synchronization/distribution, video surveillance, etc.

## 5.3 Latency calculation

### 5.3.1 Latency components

The (one-way, end-to-end transfer delay) latency may be broken down into propagation delay (5.3.2) and residence delay (5.3.3), while the recovery delay (5.7) is a particular case.

### 5.3.2 Propagation delay

Propagation delay related to the medium is in the range of 5  $\mu$ s/km for copper cables or optical fibers, and 3  $\mu$ s/km for radio links (Table 23). The propagation delay is not negligible in WANs; in substation LANs, the propagation delay only matters for the precise time synchronization.

### 5.3.3 Residence delay

The residence delay stems from the network elements (bridges, routers, gateways) and their interconnection (cable, patch panel, etc.) as well as on the traffic.

In TDM, the residence delay is constant since the operation is cyclic. There is only a small buffering to account for synchronization of the cycles.

In PSN, the residence delay varies with traffic and consists of:

- 1) processing delay (waiting to parse and check the message, including integrity and security);
- 2) queuing delay (waiting in the queue with other messages to be sent);
- 3) packetisation delay (waiting to aggregate received flows before sending);
- 4) jitter buffering (waiting for the compensation of jitter introduced by a PSN);
- 5) transmission delay (waiting for the transmission of the message trailer).

### 5.3.4 Latency accumulation

The latency of the different network elements in series cumulate.

Therefore, the number of elements in series should be limited, so as not to exceed the maximum delay specified in Table 2.

Careful network engineering assisted by simulation tools allows controlling the latency, provided a good model of each component exists.

### 5.3.5 Example: latency of a microwave system

The end-to-end latency is composed of the end-to-end accumulation of node (packet communication equipment such as switch and radio equipment), processing, propagation, transmission and queuing delays as shown in Figure 11.

Processing delays include error correction, which used to take hundreds of microseconds. Improved error correction mechanisms reduce processing delay to less than 100  $\mu\text{s}$ .

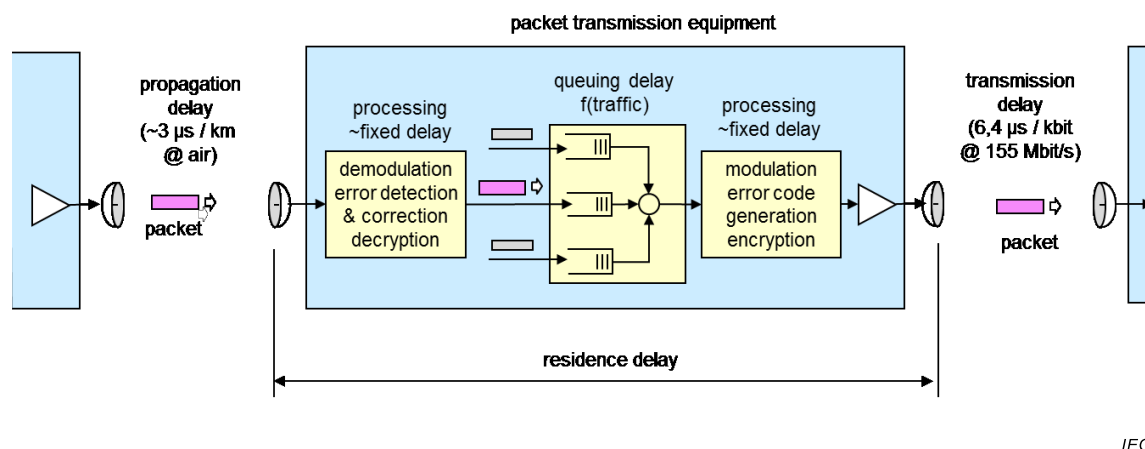
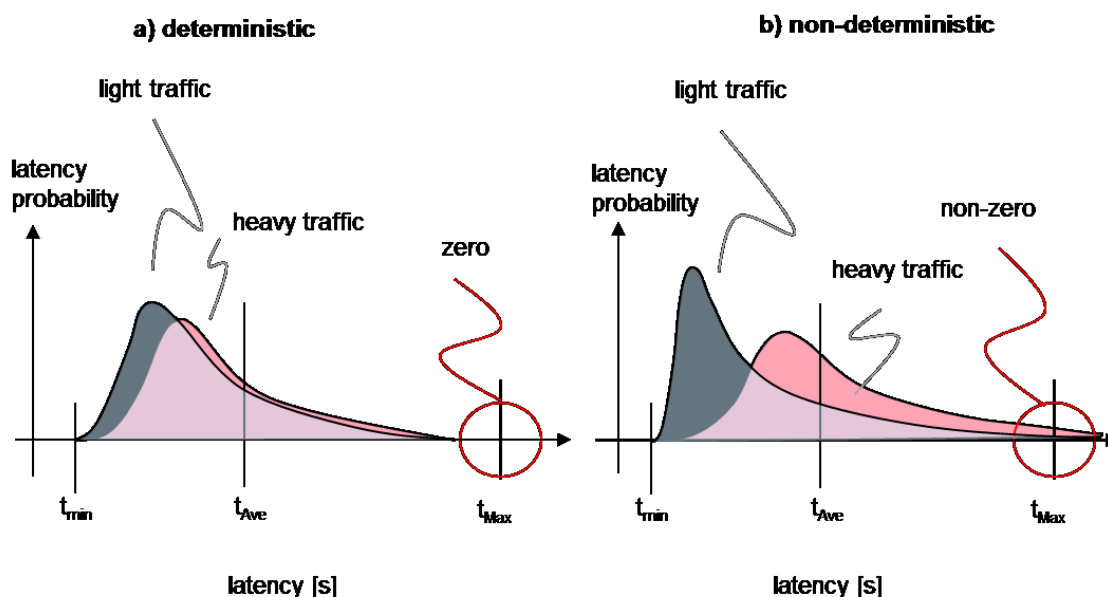


Figure 11 – Composition of end-to-end latency in a microwave relay

### 5.3.6 Latency and determinism

Latency is a statistical value, depending on the generation rate of the nodes sharing the network, on the topology, on the policy within the nodes and on the link capacities.

- In a deterministic transmission (Figure 12 a), the probability that the delay exceeds the deadline  $t_{Max}$  is zero, disregarding failures. When the medium sharing is strictly periodic, there is no difference between the light traffic and the heavy traffic plots in Figure 12 a.
- In a non-deterministic transmission (Figure 12 b), the average delay may be shorter than the average delay of the deterministic transmission (which is why it is used), but the probability that the delay exceeds a deadline  $t_{Max}$  is non-zero.



IEC

**Figure 12 – Example of latency in function of traffic**

The worst-case end-to-end latency is the sum of the latencies introduced by each element in series. The average delay is however smaller than the worst-case delay, it rises approximately with the square root of the number of elements in series, assuming that each element exhibits a latency with a Gaussian distribution.

End to end transmission can only be deterministic if all elements in the chain are deterministic. To this effect, all network elements reserve all resources beforehand: processing time, buffers, etc. For instance, SDH achieves determinism intrinsically by assigning each permanent circuit a time slot (hence, TDM) for transmission and processing.

A strict periodic operation is not required for latency determinism if all resources can be reserved when establishing a connection, e.g. through the Resource Reservation Protocol (RSVP), and if all sources limit their production rate, so the highest priority traffic cannot exceed a certain value. In this case, the probability distribution depends on the traffic, but still has an upper bound. This requires conservative network engineering and discipline on all devices.

The latency is rarely a nice mathematical function since it depends on traffic patterns, traversed networks and routers or bridges buffer size.

### 5.3.7 Latency classes in IEC 61850-5

IEC 61850-5 specifies latency classes (Table 1).

**Table 1 – Latency classes in IEC 61850-5**

Latency class	Latency	Application example
TT0	> 1000 ms	File, events, log contents
TT1	≤ 1000 ms	Alarms and Events
TT2	≤ 500 ms	Operator commands
TT3	≤ 50 ms	Slow automatic interaction
TT4	≤ 20 ms	Fast automatic interaction
TT5	≤ 10 ms	Releases, status changes
TT6	≤ 3 ms	Trip, blockings
SOURCE: IEC 61850-5:2013, Table 1.		

IEC TR 61850-90-1 defines the latencies for the substation-to-substation traffic using the numbering of IEC 60834-1, slightly different from IEC 61850-5; the differences appear in the second column of Table 2.

**Table 2 – Latency classes in IEC TR 61850-90-1**

IEC TR 61850-90-1 latency class	IEC 61850-5 latency class	Latency	Application example
TT1	TT1	≤ 1000 ms	Operator, file transfer
TT2	TT2	≤ 500 ms	Type 3 low speed messages
TR5	(TT3)	≤ 100 ms	Type 1B “automation” normal
TR4	TT4	≤ 20 ms	Type 1B “automation”, fast
TR3	(TT5)	≤ 15 ms	Type 1A “Trips” to neighboring substation (analog)
TR2	TT5	≤ 10 ms	Type 1A “Trip” within one substation raw message data between substations
TR1	TT6	≤ 3 ms	Type 1A “Trip” within one bay
SOURCE: IEC TR 61850-90-1:2010, 6.4			

NOTE IEC TR 61850-90-1 does not prescribe a deterministic value for the latency, but rather specifies that the probability that a GOOSE message takes more than 10 ms (TR2) should be  $< 10^{-4}$ .

The above latencies are given for end-to-end applications, but do not detail which part is allocated to the WAN (called  $t_{b0}$  in IEC 61850-5:2013, Figure 16). Since WANs serve different applications with different requirements for network latency, a new classification is introduced to WAN performance classes in Table 3.

**Table 3 – Latency classes for WANs**

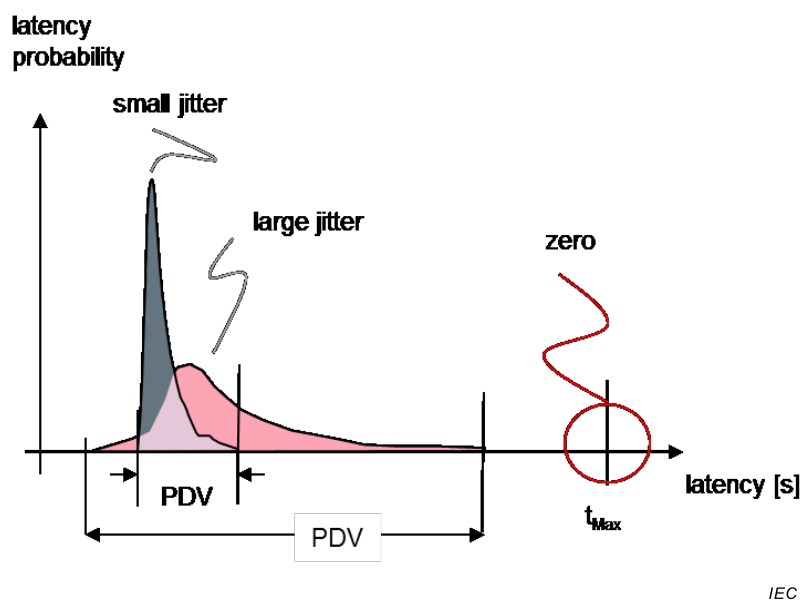
WAN latency class	IEC 61850-5 latency class	Latency	Use
TL1000	TT1	$\leq 1000$ ms	All other messages
TL300	(TT2)	$\leq 300$ ms	Operator commands
TL100	TT3	$\leq 100$ ms	Slow automatic interactions
TL30	(TT4)	$\leq 30$ ms	Fast automatic interactions
TL10	TT5	$\leq 10$ ms	Teleprotection
TL3	TT6	$\leq 3$ ms	Differential protection

NOTE The measurement method is indicated in IEC 61850-5:2013, Figure 16. The abbreviation has been changed from IEC 61850-5 TT to TL in order to prevent confusion.

## 5.4 Jitter

### 5.4.1 Jitter definition

The average value of the latency is not a sufficient criterion. One-way delay variation, called jitter or Packet Delay Variation (PDV) [RFC 3393] or Frame Delay Variation (FDV) expresses by how much the delay can vary (Figure 13).

**Figure 13 – Jitter for two communication delay types.**

Jitter produces unpredictable errors in differential (analog) protection analog comparison schemes when transmission relies on mutual synchronization, i.e. the end devices assume a constant delay in the communication line, and especially a symmetric delay (same back and forth).

This was the case with legacy relays interconnected by direct wiring with practically no jitter.

To support these relays, the network should mimic the “wire” behavior (pseudo wire).

NOTE Jitter is not relevant if measurement sampling is synchronized by global, synchronized clocks.



For engineering, a deterministic jitter (with a guaranteed upper bound) is desirable. Indeed, a deterministic latency (as in Figure 13) is not sufficient, since pseudo-wire behavior requests that the upper bound on the jitter is much smaller than the upper bound on latency. A method to reduce jitter is the use of de-jitter buffers as described in 7.10.5.1.

#### 5.4.2 Jitter classes in IEC 61850

IEC TR 61850-90-1 defines jitter classes as in Table 4, which may be sufficient to support legacy protection devices.

**Table 4 – Jitter classes in IEC TR 61850-90-1**

Class	Jitter ( $\Delta TA$ ) [ms]	Application
TT3	20 ms	External signal synchronization
TT2	10 ms	External signal synchronization
TT1	0,2 ms	External signal synchronization or mutual synchronization
SOURCE: IEC TR 61850-90-1:2010, Table 4		

Table 5 lists the quality classes for jitter that a WAN should deliver.

**Table 5 – Jitter classes for WAN**

Class	Jitter [ms]	Application
TJ00	unspecified	All other
TJ10	10 ms	External signal synchronization
TJ0,3	0,3 ms	External signal synchronization or mutual synchronization
NOTE The abbreviation has been changed to TJ to distinguish jitter from latency.		

### 5.5 Latency symmetry and path congruency

In a meshed network, messages between two partners can take different paths in each direction. Path congruency is a property of a network that routes messages between two partners over the same path back and forth. In circuit-switched networks, congruency ensures symmetry of latency, which allows measuring the delay. In packet-switched networks, congruency does not guarantee that the latency is the same in both directions, since latency depends on the other traffic.

### 5.6 Medium asymmetry

Precise clock synchronization protocols, such as IEC 61588, require measurement of link delays. Clocks measure the link delay with a request/response exchange, but this method only measures the sum of the back and forth delays; medium propagation asymmetry therefore introduces an error. While negligible in substation Ethernet, this medium asymmetry can be considerable in WANs, for instance, ISO 11801 allows 30 ns of asymmetry over 100 m in optical fibers.

IEC 61850-5 does not specify a medium asymmetry. To support a PTP clock that fulfils the requirements of IEC 61850-9-2 (process bus) and IEC 61869-9 (instrument transformers), a medium link or medium converter should present an asymmetry of less than 25 ns, as specified in IEC 62439-3 and IEC 61850-9-3. This is however more an internal property of a network than a general WAN QoS, so asymmetry is only relevant when end devices synchronize each other directly.

## 5.7 Communication speed symmetry

Some communication links are asymmetrical, with the data throughput in one direction different from the data throughput in the other direction, for instance ADSL. This applies only to the last mile and it is not a relevant parameter for backbone or backhaul WANs.

## 5.8 Recovery delay

The recovery delay stems from recovery from network breakdown. Depending on the technology, the recovery delay may vary from zero to several seconds or even minutes. When non-zero, this delay depends strongly on the protocols and on the topology. The recovery delay is sometimes called “convergence time”.

The recovery delay classes for WAN appear in Table 6 and Table 21.

**Table 6 – Recovery delay classes for WAN**

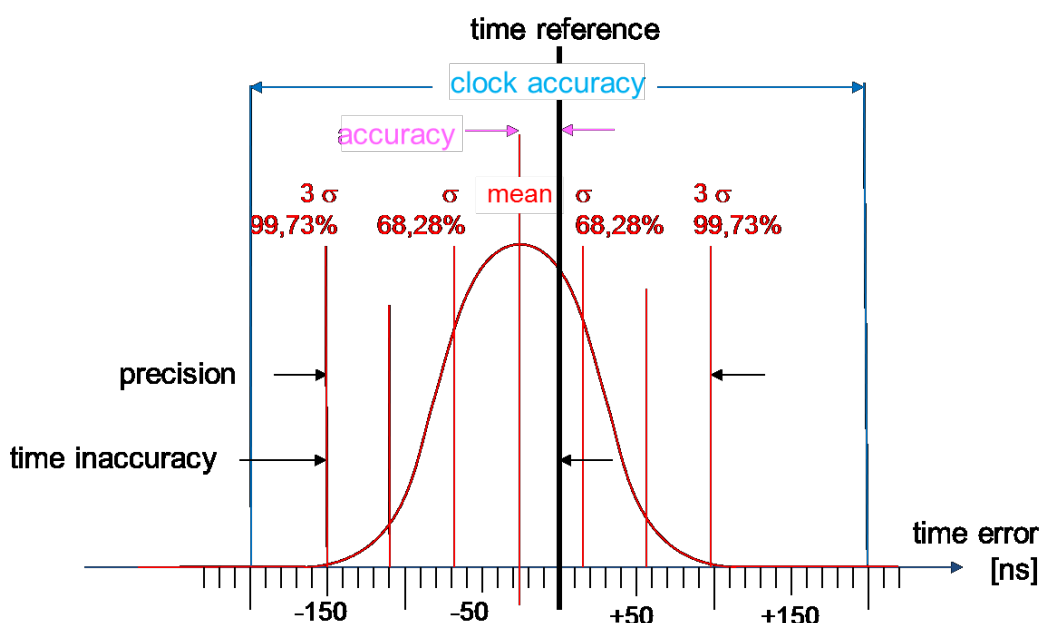
Class	Recovery delay [ms]	Application
TR500	500 ms	IP traffic
TR50	50 ms	Telecontrol
TR0	0 ms	Differential protection

## 5.9 Time accuracy

### 5.9.1 Time accuracy definition

The network provides distribution of absolute time, relative time or frequency as a service (details in 7.15 and IEC 62439-3:—, Annex D).

Time accuracy is the deviation of a clock from the reference time, with a certain confidence, e.g.  $3\sigma$ , as shown in Figure 14.



Source: IEC62439-3

IEC

**Figure 14 – Precision and accuracy definitions**

### 5.9.2 Time accuracy classes

IEC TR 61850-90-1 specifies the accuracy classes for distribution of relative time as shown in Table 7.

**Table 7 – IEC TR 61850-90-1 time accuracy classes**

IEC TR 61850-90-1 Time Accuracy Class	Time Accuracy [μs]	Purpose
T1	± 1 000	Time tagging of events
T2	± 100	Time tagging of zero crossings and of data for the distributed synchrocheck, support for point-on-wave switching
T3	± 25	Instrument transformer synchronization
T4	± 4	Instrument transformer synchronization
T5	± 1	Instrument transformer synchronization
SOURCE: IEC TR 61850-90-1:2010, Tables 5 and 6		

IEC 61850-5 defines the accuracy classes for distribution of absolute time, e.g. for the precise sampling of analog values (Table 8) for the purpose of synchrophasor transmission.

**Table 8 – IEC 61850-5 time accuracy classes for IED synchronization**

IEC 61850-5 Time synchronization class	Time Accuracy [μs]	Phase angle accuracy for 50 Hz [°]	Phase angle accuracy for 60 Hz [°]	Fault location accuracy [%]
TL	> 10 000	> 180	> 216	Not applicable.
T0	10 000	180	216	Not applicable.
T1	1 000	18	21,6	7,909
T2	100	1,8	2,2	0,780
T3	25	0,5	0,5	0,195
T4	4	0,1	0,1	0,031
T5	1	0,02	0,02	0,008
SOURCE: IEC 61850-5:2013, Table 2.				

Regardless of the clock synchronization protocol, asymmetric delays affect time accuracy (see 5.5). Asymmetry cannot be measured, but a known asymmetry can be compensated for.

NOTE It is hardly possible to fulfil the T5 requirement with a 200 μs network asymmetry in the clock distribution.

Table 9 lists the time accuracy classes that the WAN has to provide for different applications.

**Table 9 – WAN time synchronization classes**

WAN Accuracy class	IEC TR 61850-90-5 Accuracy class	Time Accuracy classes [μs]	Application
TX00	TL	unspecified	All other
TX10000	T0	10 000	Event stamping This class can be achieved with SNTP over a WAN
TX1000	T1	1 000	Zero-crossing and synchrocheck This class can be achieved with SNTP within a LAN only
TX30	T3	30	Synchrophasors this class requires PTP
TX1	T5	1	SMVs this class requires PTP

## 5.10 Tolerance against failures

### 5.10.1 Failure

The grid may suffer from two types of unwanted behavior of the automation equipment (for the definitions, see [8]):

- overfunction (unwanted trip), and
- underfunction (missing trip when required).

The communication network can cause such failures, because of:

- integrity breach (wrong data not recognized as such can cause an overfunction),
- persistency breach (no data or data too late can cause an underfunction).

For communication equipment, a failure occurs when the equipment is incapable to operate at all (no partial failures or degraded modes are considered).

For communication links, failures are volatile, assuming that the network recovers by itself. Volatile failures are expressed as Bit Error Ratio (BER), or number of wrong bits per sent bits. ITU-T G.821 gives guidelines to measure the error performance. Permanent failures belong to the same category as device failures.

A failure can also be the late delivery of information due to congestion or recovery.

For instance, IEC 60834-1 considers that a command has failed if not received within 10 ms, indicating a certain probability for this ( $10^{-4}$ ). In other words, it considers the transmission as “failed” only if more than one message in 10 000 is delayed more than 10 ms. If transmission is not deterministic, such a latency can occur statistically without any deficiency in the hardware.

### 5.10.2 Reliability

Reliability is the probability that a component or system fails after having worked correctly until its failure (reaching a terminal state). Reliability is therefore a function of time,  $R(t)$ . A simple expression of reliability is the Mean Time To Failure (MTTF) for an element or a system, defined as:

$$MTTF = \int_0^{\infty} R(t) dt \quad [1]$$

When a system such as a power utility grid includes redundancies, a component failure does not necessarily cause a function failure. Indeed, a substation or distribution grid should never fail completely because of a single component failure.

IEC TR 61850-90-1, IEC 60834-1 and CIGRE [4] define a protection system failure as the probability of an unwanted, permanent trip, but do not specify the interval between two such events.

### 5.10.3 Redundancy principles

Regardless of the actual dependability requirements, many utilities request that the network fulfils the N-1 criteria, i.e. no single component failure can stop operation.

Redundancy applies two principles:

- Workby or massive redundancy, in which redundant components are continuously active and immediately inserted (for instance several energized power supplies, sharing the load and tolerating the failure of one). Workby applies to the network, components or any resource.

For instance, IEC 62439-3 networks carry the same information simultaneously and their recovery is immediate (zero recovery delay).

The “workby” method is called:

“1+1 redundancy” with two simultaneously active resources;

- Standby or spare redundancy, in which the redundant component is normally inactive and it will take a recovery delay to become active in case of fault detection. The recovery delay can be so long as to render redundancy useless. This is typically the case in IP communication networks, where re-routing can take from seconds (with traffic engineering) to minutes (with best effort).

For instance, in RSTP [IEEE 802.1Q] (7.6.4.8.2), redundant links only carry administrative traffic to check that there are still up, they need seconds to resume carrying operational traffic after a severe failure.

The standby methods is called “m:n”, with the special cases:

“1:1 redundancy” one redundant element backs up one single working elements,

“n:1 redundancy” when n redundant elements back up one working element and

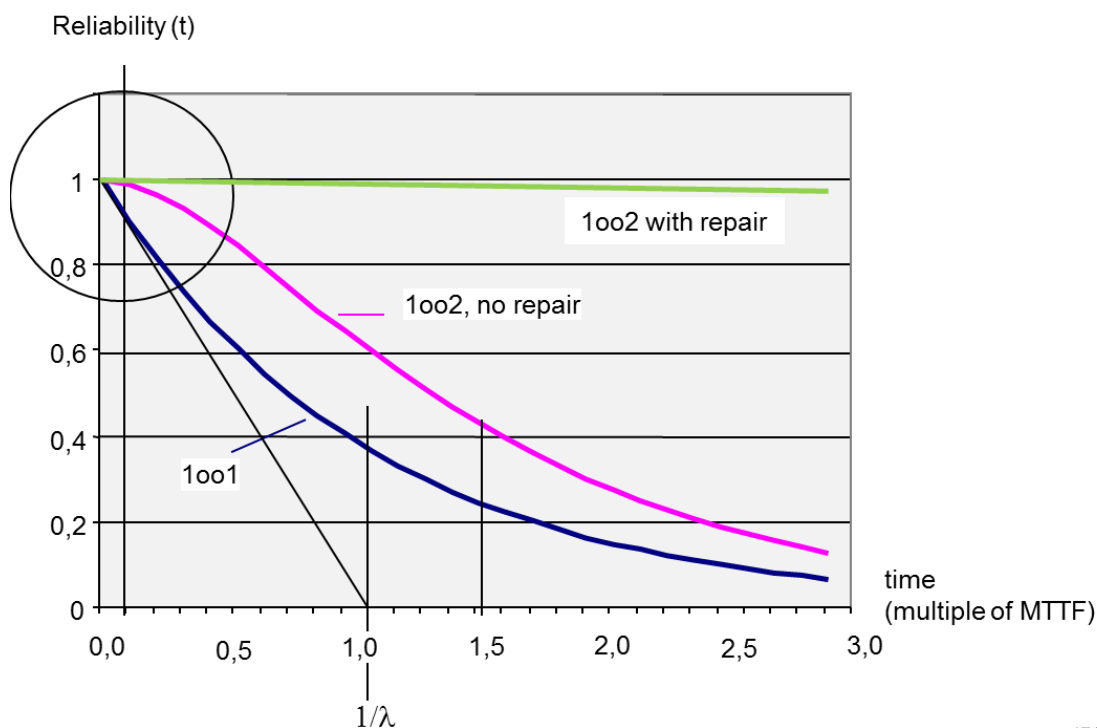
“1:n redundancy” when one redundant element backs up n working elements.

Main and backup protection typically operate normally in workby, and additionally in diverse workby, in the sense that the protections are simultaneously active and not of the same kind (e.g. different manufacturers) to fend off design or installation errors.

Figure 43 shows a case where diverse redundancy ensured the survival of the communication network, since the redundant microwave towers were separate from the high-voltage towers.

### 5.10.4 Redundancy and reliability

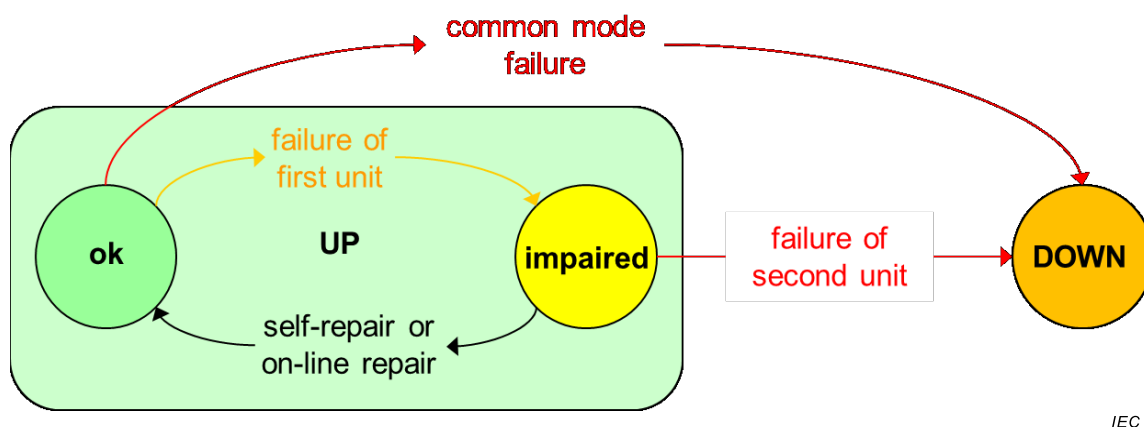
Figure 15 shows the reliability of a doubly redundant, one-out-of-two (1oo2) system. The MTTF of the one-out-of-two (1oo2) system without repair is only one-and-a-half that of a non-redundant, one-out-of-one (1oo1) system. Only repair increases significantly reliability. A doubly redundant system without repair is of little help in a grid automation system that operates for years: indeed, it provides only an improvement for the initial phase.



IEC

Figure 15 – Redundancy of redundant systems

Figure 16 shows the calculation base for the 1oo2 system with repair. The probability that the system fails completely is equal to the probability that both redundant components fail before repair of a failed component. Of course, a common mode failure can bring the system down, regardless of redundancy.



IEC

Figure 16 – Redundancy calculation

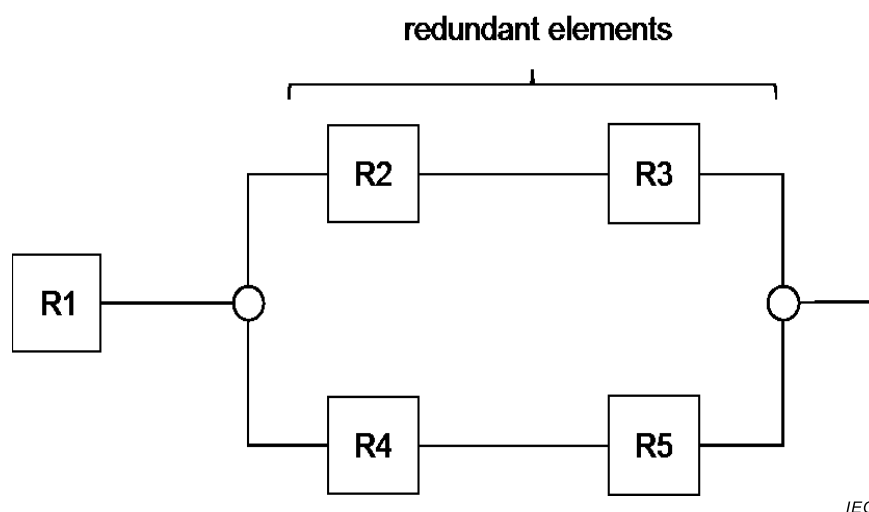
### 5.10.5 Redundancy checking

Redundancy is useless if not constantly supervised. The above calculation mode assumes that the back-up unit fails with about the same failure rate as the on-line unit fails. Since calculations include the time to detect a failure in the mean time to repair, the failure of the back-up unit should be detected as fast as the failure of the on-line unit. However, the time to detect a failure affecting non-operative components can be long, while failures are usually visible immediately if the component is operating. Therefore, background checking of non-operative components is necessary.

### 5.10.6 Redundant layout: single point of failure

Redundancy is only useful if the redundant elements fail independently. Any common mode of failure would affect the overall reliability.

For instance, in Figure 17 assuming all elements have approximately the same reliability, the reliability of the redundant elements R2, R3, R3 and R5 influences little. The reliability of the whole chain is dominated by element R1, which represents the common modes of failure, e.g. common power supply, mounting on the same frame, and software errors if the two redundant elements are from the same design.



**Figure 17 – Redundancy layout with single point of failure**

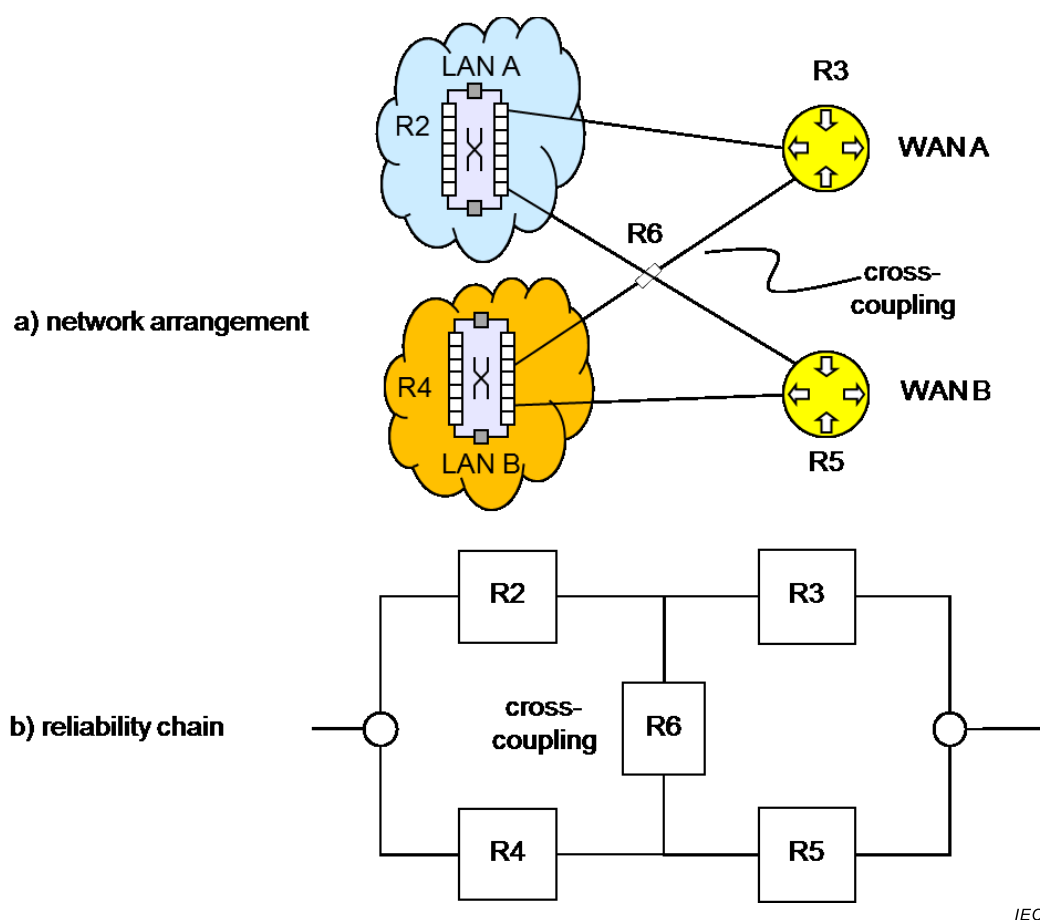
For the network design, it means that making all elements redundant and ensuring that two paths always exist between two end points is not sufficient: the design must be free of common modes of failure.

Therefore, keeping the redundant elements completely separated and free from common mode of failure is a priority. A complete freedom of single point of failure is however sometimes not economical. Authorities can issue recommendations, for instance regarding separation of redundant elements, see 7.4.8.

For instance, the North American Power Coordination Council (NPCC) accepts that a microwave tower is not a single point of failure because of its very high reliability.

### 5.10.7 Redundant layout: cross-redundancy

In Figure 18, cross-coupling (R6) allows to continue operation in case two elements on opposite rungs fail, e.g. R2 and R5. Such an arrangement is often seen in connecting networks. However, cross-redundancy only brings an advantage if the reliability of the coupling element (R6) is an order of magnitude better than the reliability of the elements that can fail. This is often not the case, and in fact, such cross-redundancy can lower the overall reliability.



**Figure 18 – Redundancy layout with cross-coupling**

For instance, protection engineers keep Main1 and Main2 protection completely separated and do not try to exploit fringe benefits from sharing elements.

### 5.10.8 Maintainability

Practically, reliability's most important expression for utilities is the Mean Time Between Repairs (MTBR), i.e. how often the repair team intervenes in the field, assuming that the repair takes place after redundancy is lost, but with no failure of the protection and control function. As 5.10.4 shows, this is crucial for reliability.

The strategy for maintenance depends on the probability of occurrence of a second failure before repair of a first failure.

Failure of the communication system affects the MTBR.

Introducing more redundancy decreases the MTBR, since the reserve components can also fail.

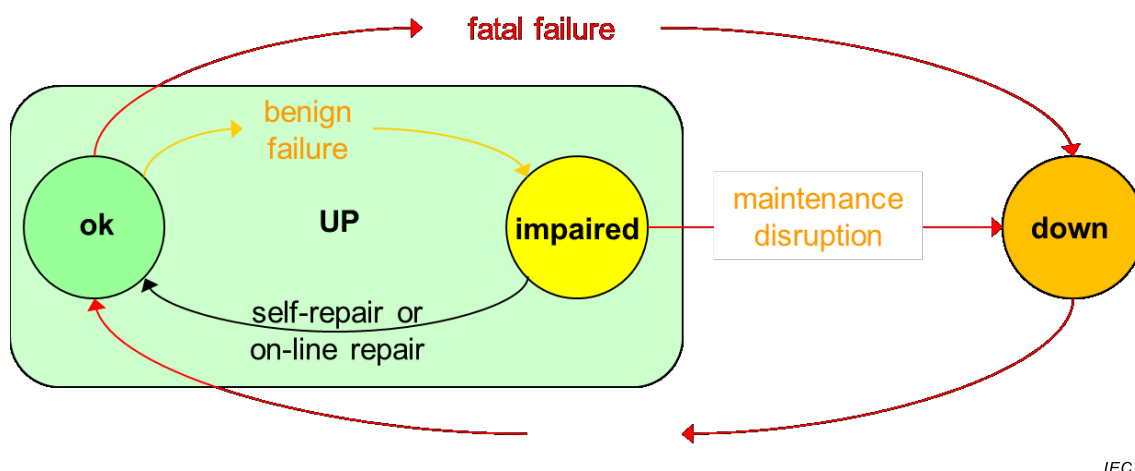
Policies for network components maintenance, spare distribution over the network, availability of field crews are other factors influencing the MTBR.

### 5.10.9 Availability

Availability applies only to repairable systems, when a total failure is not fatal. The utilities require availability expressed as "unavailability hours per year".



Availability applies to a repairable system that oscillates between up-time and down-time (Figure 19). The up-time includes the time during which the network is still operating, but impaired (due to redundancy loss). Also, maintenance itself can cause downtimes.



**Figure 19 – Availability definitions**

(Asymptotical) availability is the ratio of up-time to the lifetime of the system:

$$A = \frac{MUT}{MUT + MDT} = \frac{MUT}{MTBR} \quad [2]$$

*MUT* = Mean Up Time

*MDT* = Mean Down Time

*MTBR* = Mean Time Between Repairs

*MTTR* = Mean Time To Repair

Availability can be expressed as a percentage, e.g. 99,99 % or preferably as Unavailability, e.g. 1 hour per year corresponds to 99,99 % availability.

However, the meaning of availability varies, depending if the purpose of the equipment is monitoring, control or protection.

Requirements such as “availability > 99,9 %” are not defined, unless the conditions for being in the “Up Time” are stated.

In substations, few functions would cause immediate loss of power when the network fails. The worst situation is an integrity failure, in which a communication failure causes an unwanted trip (overfunction) or causes the loss of a trip command or of a blocking signal (underfunction).

In monitoring applications, it becomes unsafe to operate the network when the outage of the network lasts too long.

In control applications, the network must be available when the operator needs it.

In protection applications, a loss of power happens if the protection algorithm becomes unable to calculate correctly the fault due to a loss of communication. In this case, an unwanted trip could happen.

Telecontrol being the most demanding application, its dependability dictates the network dependability.

Methods to calculate network availability appear in IEC 62439-1 and IEC TR 61850-90-4.

Unavailability includes also the probability that the operation does not complete within useful time. The probability of a protection trip that takes place simultaneously with a reconfiguration of the network is not negligible, since they could have the same root cause (e.g. lightning stroke).

Preventive and proactive maintenance influence the availability calculation, they should be considered in the contracts since they depend on a policy of the utilities and of the suppliers.

Network specifications must include the conditions for terming the network “available”. Since calculating availability is a difficult endeavor, and difficult to verify, many utilities that lack the expertise and simulation tools specify instead that redundancy must be available for all functions.

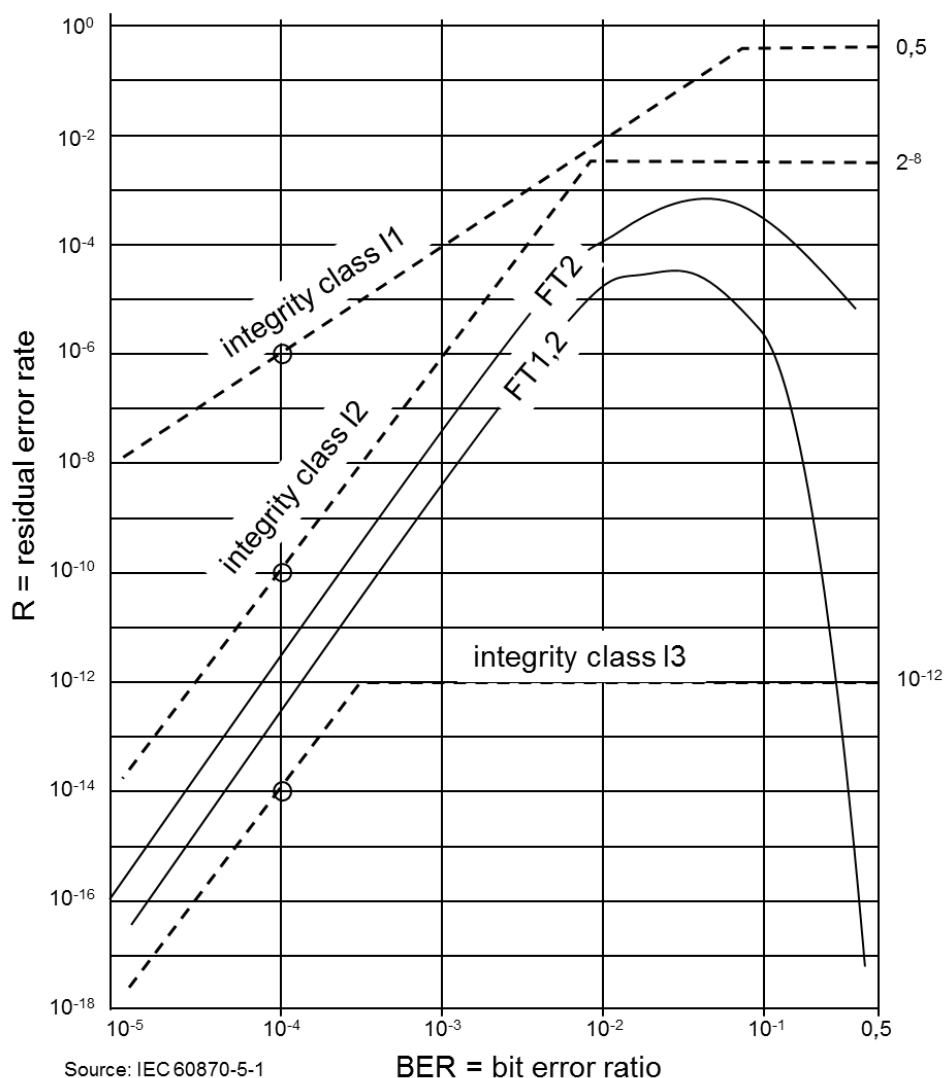
In that case, the recovery delay of non-redundant elements must be significantly shorter than the permitted communication downtime. This also applies to “self-repair” when elements recover from transient failures, without a hardware failure.

#### **5.10.10 Integrity**

Integrity is the probability to recognize data falsified by errors as incorrect. Integrity relies on an error detection code, whose efficiency depends on the BER of the medium. At the application layer, plausibility checks can help.

NOTE IEC 60834-1 uses instead of “integrity” the term “security” as “the ability of the receiver to reject false teleprotection information that has been simulated by the channel degradations”. Since this term can be confused with cyber-security, it is not used in this document.

More precisely, IEC 60870-4 considers the residual error rate as a function of the BER, as shown in Figure 20.



IEC

**Figure 20 – Residual error rate in function of the BER**

One metric for integrity is the Hamming Distance, e.g. the number of independent errors that would cause an erroneous message to appear as good.

The asymptote to the curve in Figure 20 is the Hamming Distance. When the BER approaches 0,5 (every second bit is in error), the residual error loses its meaning.

The checksum or Cyclic Redundancy Check (CRC) algorithm that checks the data and ensures integrity assumes certain error patterns: the BER is not a sufficient indication, since random errors do not corrupt data the same way as a burst error would.

The residual error rate serves to select a suitable error detection checksum, several of which are standardized. For instance, Ethernet uses a CRC-32 for this purpose.

Truncation errors can reduce the Hamming Distance down to one if the frame has no size supervision. In this case, the application has to apply its own checksums or plausibility checks.

Error correcting schemes degrade integrity since they may correct wrongly a damaged piece of information. They are used when the disturbances are large such as in radio or in optical fibers with marginal transmission.

Integrity prevents wrong commands from being issued. A device that receives a corrupt message ignores it. Thus, integrity does not help in maintaining persistency, on the contrary.

### 5.10.11 Dependability

Dependability in a protection system is the probability that the protection will operate as required in the presence of faults.

NOTE IEC 60834-1 defines “dependability” as “the ability to deliver a teleprotection information at the receive end in spite of the presence of channel degradations”, a definition that contradicts IEC 60050-192 [7], but which is nevertheless used in this document.

IEC 61508 defines the PFD, or Probability of dangerous Failure on Demand, expressed as the probability that the teleprotection will not operate when required. It is the 1's complement of the availability of the protection function:

$$(PFD = 1 - A)$$

IEC 60834-1 specifies that the probability of a “command” not being received within 10 ms should be  $< 10^{-4}$  for a single system (HV) and  $< 10^{-7}$  for a double redundant system (EHV). This is not properly an expression for the availability, but a criteria to declare that a communication error took place.

Assuming that IEC 60834-1 applies to a time interval of one year and not to the number of commands issued,  $R = 10^{-4}$  corresponds to an unavailability of about 50 min, respectively  $R = 10^{-7}$  to 3 s of downtime per year.

A part of the PFD budget is allocated to the end-to-end communication unavailability. Achieving this value requires a high reliability of the elements, redundancy in the devices and in the network and a suitable maintenance strategy (maintainability schedule, spare parts availability and spreading over their territory, planned cuts, etc.).

### 5.10.12 Example: Dependability of GOOSE transmission

To increase persistency, a GOOSE message is repeated typically three times in a row with a small interval, i.e. 1 ms. A receiver rejects a corrupted GOOSE message.

However, if the network fails while a GOOSE message triplet is sent, all three messages could get lost and neither the publisher nor the subscribers will know it – until the background GOOSE message is transmitted, e.g. every second, which may be too late.

Within a substation LAN, seamless redundancy (7.6.4.8.4, 7.6.4.8.5) copes with this situation, but in a WAN with a typical recovery delay of 50 ms, all GOOSE messages could get lost. Increasing the interval between duplicates does not help since trip signals should be received within 5 ms.

The calculation of dependability in 5.10.11 basically asks how likely is it that a network reconfiguration takes place while a GOOSE message is transmitted, and how likely long-lasting bursts are.

## 6 Applications analysis

### 6.1 Application kinds

Engineering of a network bases on an estimate of the data flow in terms of throughput, latency, jitter and quality of service, as required by different classes of applications.

Utility companies use WANs for various applications that may or may not share the same network, classified in:

- 1) Operational traffic immediately needed for grid operation and covered by IEC, CIGRE and IEEE standards and recommendations and
- 2) Enterprise traffic used for the utilities themselves.
- 3) Commercial traffic, as a service provider.

The distinction is however blurred. For instance, voice is an essential operational communication while IEC standards do not cover it.

The following application kinds are considered:

- Teleprotection (horizontal between SS); [IEC TR 61850-90-1]
- Telecontrol (SCADA to SS); [IEC TR 61850-90-2]
- Wide Area monitoring (WAMS); [IEC TR 61850-90-5]
- Wide Area monitoring, protection and control (WAMPAC); [IEC TR 61850-90-5]
- Dispatching (EMS, DMS), communication between CC
- Condition monitoring and diagnosis (CMD) and Asset Management
- Voice for operation (fixed)
- Remote access to substation equipment, log retrieval
- Maintenance and workforce support (scheduling, documentation)
- Mobile voice and data
- Network management
- Cyber-security management
- Physical security and video surveillance
- Enterprise communications
- Access to internet (documentation, weather, email).

Subclauses 6.2 to 6.8.3 detail the requirements of these applications, with reference to the interfaces listed in Figure 9. The actual values are taken from existing IEC and CIGRE documents.

## **6.2 Teleprotection (IF2 & IF11)**

### **6.2.1 Teleprotection schemes**

Teleprotection senses abnormal voltage, current or frequency conditions in the grid and opens a circuit breaker within the fault clearing time (80 ms to 120 ms), striving to reduce impact on non-affected parts of the grid.

Teleprotection relies on communication to detect fault conditions (differential comparison) and to send commands (direct transfer trip, permitting trip and blocking commands).

IEC TR 61850-90-1 (substation to substation communication), CIGRE Report 461 [2] and CIGRE Report 521 [3] describe the different protection schemes.

From a communication point of view, two main categories appear:

- 1) analog protection, comprising:
  - Phase comparison protection
  - Differential protection

2) binary protection, comprising:

- Distance line protection with permissive overreach
- Distance line protection with blocking
- Directional comparison protection
- Transfer/direct tripping
- Interlocking
- Multiphase auto-reclosing for parallel line systems

### 6.2.2 Teleprotection data kinds

IEC TR 61850-90-1 considers three main kinds of transmission (see Table 2):

- 1) analog values, e.g. for line differential protection, consisting of current values sampled at a precise time, called Sampled Values (SV), which represent a high throughput or of synchronized phasor values (Synchrophasors) at a somewhat lower rate;
- 2) binary values, e.g. binary protection status and control, consisting in a few bits that must be transmitted with a short and deterministic latency;
- 3) others, such as time distribution, network and asset management, low speed communication to the operator, and file transfer.

### 6.2.3 Teleprotection requirements for latency

Table 10 lists the latency requirements for the protection schemes. For WANs, it makes little sense to differentiate the latencies since the same WAN must carry all traffic. Therefore, when a WAN transports teleprotection data, the requirements of differential protection apply to the other traffics also.

**Table 10 – Latency for line protection**

Teleprotection	Max. Latency	Latency class
Differential protection	2,5 ms to 10 ms	TL3
Blocking	10 ms	TL3
Permissive tripping	20 ms	TL3
Transfer tripping	40 ms	TL3

### 6.2.4 Teleprotection requirements for latency asymmetry

Legacy relays communicate with each other by direct wiring (“pilot wire”). This method causes practically no jitter, which allows mutual synchronization (see 7.15.2).

Mutual synchronization requires a small two-way differential delay (Packet Delay Asymmetry). A two-way differential delay of  $2 \times \Delta\tau$  causes a sampling synchronization error of  $\Delta\tau$ .

Allowable two-way differential delay is around 200  $\mu\text{s}$  for a differential current error of 4 % with respect to sampling timing synchronization error.

To interconnect this class of relays, the network should mimic the pilot wire behavior (pseudo wire).

### 6.2.5 Teleprotection requirements for integrity

For generic telecontrol protocols, IEC 60870-5-1 defines the residual error rate for different integrity classes in function of the BER (see Figure 20).

To this effect, IEC 60834 requires that the BER of the medium does not exceed  $10^{-6}$ .

Table 11 summarizes the dependability requirements for line protection operation.

**Table 11 – Summary of operational requirements of line protection**

Dependability	Analog comparison (Current differential)	Command	Transfer tripping
PFD	$> 1-10^{-5}$	$> 1-(10^{-2} \text{ to } 10^{-3})$	$> 1-10^{-4}$
Integrity	$> 1-10^{-6}$	$> 1-(10^{-4} \text{ to } 10^{-7})$	$> 1-10^{-8}$
Operation delay (excluding CB operation)	< 33 ms to 40 ms (< two cycles)	< 40 ms to 50 ms (< two cycles + 10 ms)	0,1 s to 1,0 s
SOURCE: IEC 60834-1, IEC 60834-2, CIGRE 521 D2			

### 6.2.6 Teleprotection summary

Table 12 lists the communication requirements. Other factors such as network operability, serviceability, maintainability, and cost (installation and operation) are out of scope.

**Table 12 – Summary of communication requirements for teleprotection**

	Analog comparison (Current differential)	Command	Transfer tripping
Direction	Bidirectional	Bidirectional	Unidirectional
Message (useful) size	50 bits to 100 bits <sup>1)</sup>	Few bits (On/off)	Few bits (On/off)
Message (frame) periodicity	3 to 12 times per cycle	Sporadic	Sporadic
Bit rate (Bandwidth) <sup>2)</sup>	9,6 to 64 kbit/s	< 10 kbit/s	< 10 kbit/s
Latency	< 3 ms to 10 ms (TL6 or TL5)	< 10 ms (TL5)	< 10 ms (TL5)
Jitter <sup>3)</sup>	< 100 $\mu$ s	Not required	Not required
Latency asymmetry	< 200 $\mu$ s <sup>4)</sup>	Not critical	Not critical
Time accuracy (relative)	< 100 $\mu$ s	Not critical	Not critical
Error rate (BER)	< $10^{-6}$ to $10^{-8}$	< $10^{-6}$	< $10^{-6}$
Recovery delay	< 50 ms	< 50 ms	< 50 ms
Unavailability	< $10^{-4}$ for single system (HV) < $10^{-7}$ for double redundant system (EHV)	< $10^{-2}$ to $10^{-3}$ (order of 1-dependability)	< $10^{-4}$ (order of 1-dependability)

NOTE 1 One phase or segregated (three-phase) current differential protection.

NOTE 2 Throughput is generally not an issue for teleprotection with high-speed networks, since the message size is small. It could only become an issue for differential protection with a high sampling frequency.

NOTE 3 0,25 to  $0,05 \times$  Unit Interval (ITU-T G.823).

NOTE 4 Some legacy standards required only an asymmetry of 750  $\mu$ s for teleprotection equipment; this value sometimes still appears, depending on the voltage level.

### 6.3 Telecontrol (IF1, IF6)

This interface is substation-internal.

#### 6.4 Substation to control centre (IF10)

IEC TR 61850-90-2 specifies the communication between control centres and substations/power stations. These applications include telemetry, supervision and telecontrol used to report state information of primary and secondary grid equipment to control centres and control them from the control centres.

Table 13 lists typical communication requirements.

**Table 13 – Communication requirements for CC to SS/PS**

	Telemetry	Supervision	Telecontrol (Automatic/manual)	Load dispatch/ Load frequency control
Direction	Unidirectional (SS/PS to CC)	Unidirectional (SS/PS to CC)	Unidirectional and/or bidirectional (e.g. SBO) (CC to SS/PS)	Bidirectional (CC to PS)
Message size [octets]	160	160	160	160
Message rate [Hz]	0,3 to 1	0,3 to 1	Event-driven	0,03 to 0,5 (LFC) 0,001 to 0,017 (LDC)
Bit rate [kbit/s]	1 to 10	1 to 10	1 to 10	10 to 100
Latency	< 300 ms (TL300) < 2 s to 4 s <sup>1</sup>	< 300 ms (TL300) < 2 s to 4 s <sup>1</sup>	< 300 ms (TL300) < 0,5 s <sup>1</sup>	< 2 s to 5 s
Latency asymmetry	N/A	N/A	N/A	N/A
Jitter	N/A	N/A	N/A	N/A
Time accuracy	N/A	N/A	N/A	N/A
Error rate	< 10 <sup>-6</sup>	< 10 <sup>-6</sup>	< 10 <sup>-6</sup>	< 10 <sup>-6</sup>
Recovery delay [s]	20	20	2	2
Unavailability	< 7 × 10 <sup>-5</sup>	< 7 × 10 <sup>-5</sup>	< 7 × 10 <sup>-5</sup>	< 2 × 10 <sup>-5</sup>
SOURCE: Japanese utilities				
<sup>1</sup> MV and LV applications				

IEC TR 61850-90-2 specifies the latency and time classes for CC to SS /PS (Table 14).

**Table 14 – Latency and timing requirements from IEC TR 61850-90-2**

WAN latency class	IEC 61850-5 class	Typical latency [ms]	Time resolution [ms]	Application examples Transfer of:
TL10000	TT0	10 000	1	Files, events, log contents
TL1000	TT1	1 000	1	Events, alarms, status changes,
TL300	TT2	300	1	Operator commands
TL100	TT3	100	1	Automatic interactions
SOURCE: IEC TR 61850-90-2, Table 5, modified to the nearest latency class.				



## 6.5 CMD (IF7)

### 6.5.1 CMD overview

Condition monitoring and diagnosis system includes video surveillance, transmission line fault location, on-line condition monitoring and field workforce voice communication. The fault location on a transmission line with a surge reception scheme requires a precise time synchronization to reduce fault location errors. On-line CMD requires almost the same as telemetry.

### 6.5.2 CMD communication requirements

Table 15 lists the communication requirements for condition monitoring of primary equipment.

**Table 15 – Communication requirements for CMD**

	Video surveillance	Fault location	On-line condition monitoring
Direction	Bidirectional	Unidirectional (SS/PS to CC)	Unidirectional (SS/PS to CC)
Message (frame) size [octets]	1000	160	160
Message (frame) rate [Hz]	1	event-driven	0,3 to 1
Bit rate [kbit/s]	100 to 2 000	1 to 10	1 to 10
Latency [ms]	< 1 000 (TL1000)	30 (TL30)	< 1 000 (TL1000)
Transfer delay asymmetry	–	–	–
Time accuracy [μs]	–	< 3 (TX3)	–
Jitter	–	–	–
Error rate	–	< 10 <sup>-6</sup>	< 10 <sup>-6</sup>
Recovery delay [s]	–	20	20
Unavailability	< 10 <sup>-4</sup>	< 10 <sup>-4</sup>	< 7 × 10 <sup>-5</sup>
NOTE A recovery delay of 18 s is compatible with a TCP recovery delay.			

## 6.6 Control Centre to Control Centre (IF12)

Inter-control centre communications include the message exchange of SCADA information in each control area and operational file or historian data exchanges between control centres. Other communications include load dispatch voice and meteorological information collections.

The ICCP / TASE-2 standard IEC 60870-6 makes recommendation on communication that are obsoleted by technology progress. The CIM standard IEC 61970 makes no recommendation on the network topology or performance.

The required performance is summarized in Table 16.

**Table 16 – Communication requirements  
for inter-control centre communications**

	SCADA	File transfer	Telephony
Direction	Bidirectional	Bidirectional	Bidirectional
Message (frame) rate [Hz]	0,2 to 1	–	–
Bit rate (Bandwidth) [bit/s]	10 to 100	1 000 to 10 000	64
Latency [s]	< 3	<10	< 0,1
Transfer delay asymmetry	–	–	–
Time accuracy	–	–	–
Jitter	–	–	–
Bit error ratio	< $10^{-6}$	–	< $10^{-6}$
Recovery delay [s]	20	–	–
Unavailability	< $7 \times 10^{-5}$	–	< $7 \times 10^{-5}$
SOURCE: Japanese utilities			

## 6.7 Wide Area Monitoring System (IF13)

### 6.7.1 WAMS overview

Wide Area Monitoring Systems (WAMS) gather the values of current and voltage over a large area (a region or a country, sometime several countries) for monitoring, i.e. there is no direct action on the electrical conducting equipment.

IEC TR 61850-90-5 describes the WAMS applications as part of synchrophasor distribution.

WAMS include the visualization and situational awareness (e.g. for generating stations, regional transmission interfaces and separation islands), and the monitoring and alarming (e.g. state estimation, small-signal stability monitoring, voltage stability monitoring, thermal monitoring and congestion monitoring).

Wide-area situational awareness (WASA) monitors and displays grid components and performance across interconnections and over large geographic areas in near real time. The goals of situational awareness are to understand and ultimately optimize the management of grid components, behavior, and performance, as well as to anticipate, prevent, or respond to problems before disruptions arise [41].

### 6.7.2 WAMS topology

The WAMS application uses the current and voltage phasors information to detect abnormal grid situations.

The WAMS consists of Phasor Measurement Units (PMUs), Phasor Data Concentrators (PDCs), and Central Processing Equipment (CPE) such as data processing and storage (historian) and display as well as WANs.

NOTE IEC TR 61850-90-5 calls the Central Processing Equipment “Central Equipment”, this term is not used here because of abbreviation clash.

The PMUs measure the phasors in the substation, synchronized to a common reference clock with a precision of some 4  $\mu$ s with respect to absolute time. This precision requires a precise time source such as a GSSN receiver. However, due to the lack of trust in GNSS (7.15.4), the network is required to serve as time reference (7.15.7).

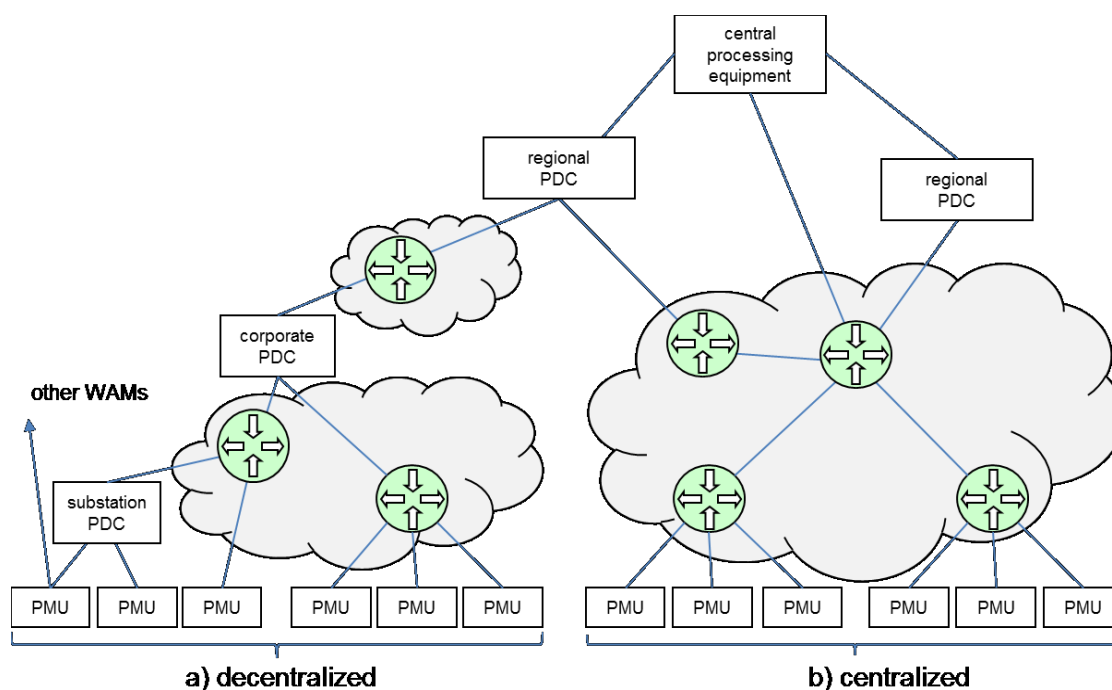
The phasors values transits over the WAN to the PDCs, either at the substation level (ssPDC) or at the regional control centre level:

- Decentralized PDCs (Figure 21 a) bring the advantage that they can resample data coming at different rates, make better use of the bandwidth through aggregation and can keep a record in case of network breakdown. They play the role of an Application-Layer Gateway (ALG), segmenting the WAN.
- Centralized PDC at the CPE (Figure 21 b) is also feasible when the network provides sufficient bandwidth and supports multicast. This lowers costs by avoiding intermediate, utility-specific units in the network and improves scalability.

IEEE C37.118-2 defines the communication between PMUs and PDCs.

IEEE C37.244 defines the PDCs.

IEC TR 61850-90-5 specifies the transmission of the synchrophasors to a hierarchy of PDCs over a WAN. The same PMU can broadcast the data to several PDCs, which is the reason why IEC TR 61850-90-5 specifies UDP multicast rather than TCP as transport protocol.



IEC

**Figure 21 – Principle of synchrophasor transmission**

The latency is not critical, since WAMS does not react automatically.

Table 17 summarizes the communication requirements of IEC TR 61850-90-5.

**Table 17 – Summary of synchrophasor requirements**

Function	Reporting rate [Hz]	End-to-end latency [ms]	Measurement timing error [μs]	Sensitivity to transmission jitter	Sensitivity to lost packets	Currently covered in IEC 61850
Synchrocheck	≥ 4	100	25	Medium	High	SMV service
Predictive dynamic stability control	25 to 100 at 50 Hz 30 to 120 at 60 Hz	30	25	Medium	Medium	SMV service
Undervoltage load shedding	25 at 50 Hz 30 at 60 Hz	100	25	Medium	Medium	SMV service
Adaptive relaying	≥ 4 (10)	300	25	Low	Medium	SMV service
Out-of-step protection	≥ 10	300	25	Medium	Medium	SMV service
Situational awareness inter-area oscillation	10	3 000	25	Low to medium	Low to medium	Periodic reporting, SMV-service
Situational awareness local oscillation	50	3 000	25	Low to medium	Low to medium	Periodic reporting, SMV-service
Situational awareness series resonance	3 × f	3 000	25	Low to medium	Low to medium	Periodic reporting, SMV-service
Situational awareness phase angle, power flow	1	3 000	25	Low to medium	Low to medium	Periodic reporting, SMV-service
Situational awareness voltage profile	1	3 000	25	Low to medium	Low to medium	Periodic reporting
Situational awareness power flow	1	3 000	25	Low to medium	Low to medium	Periodic reporting, SMV-service
State-estimation & security assessment	1/300 to 10	3 000	25	Low	Medium	Periodic reporting, SMV-service
Event data	–	–	25	Low	Medium	All as needed
Data archiving	–	–	25	Low	Medium	All as needed
SOURCE: IEC TR 61850-90-5:2012, 7.4						

### 6.7.3 WAMS communication requirements

NASPI document [37] gives guidelines where to place the PMUs.

The communication requirements for WAMS are summarized in Table 18.

**Table 18 – Summary of communication requirements for wide area monitoring**

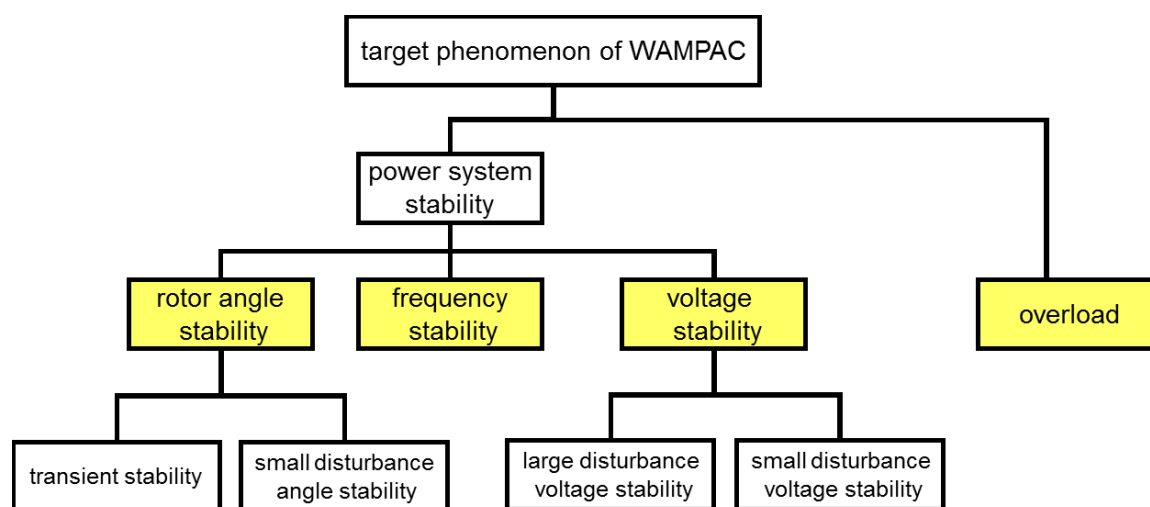
	<b>Class B</b> (State estimation)	<b>Class C</b> (Visualization and monitoring)	<b>Class D</b> (Disturbance analysis, off-line)
Direction	Bidirectional between PMU, PDC and CPE		
Message size	Tens of octets or more for data, configuration, header, and command messages		
Message rate (30 to 120 samples per second)	Somewhat critical	Somewhat critical	Critical
Bit rate	Several tens of kbit/s to several Mbit/s		
Latency	Fairly critical	Somewhat critical 3 s to 10	Not critical 3 s to 10
Time accuracy	Critical 1)	Somewhat critical	Not critical
Data accuracy (Error rate)	Somewhat critical	Not critical	Critical
Reliability/availability	Somewhat critical, redundancy needed	Not critical	Fairly critical
NOTE 1 The 50 $\mu$ s accuracy required by IEC TR 61850-90-5 is too relaxed for this application. The requirements for the clock is an absolute time accuracy of 5 $\mu$ s, see in particular 7.15.11.			

## 6.8 Wide area monitoring, protection and control (WAMPAC) IF13

### 6.8.1 WAMPAC overview

WAMPAC systems are also referred to as System Integrity Protection Scheme (SIPS), Remedial Action Scheme (RAS) and grid stabilizing control.

Figure 22 categorizes the target phenomena for WAMPAC, each imposing its own communication requirements.



IEC

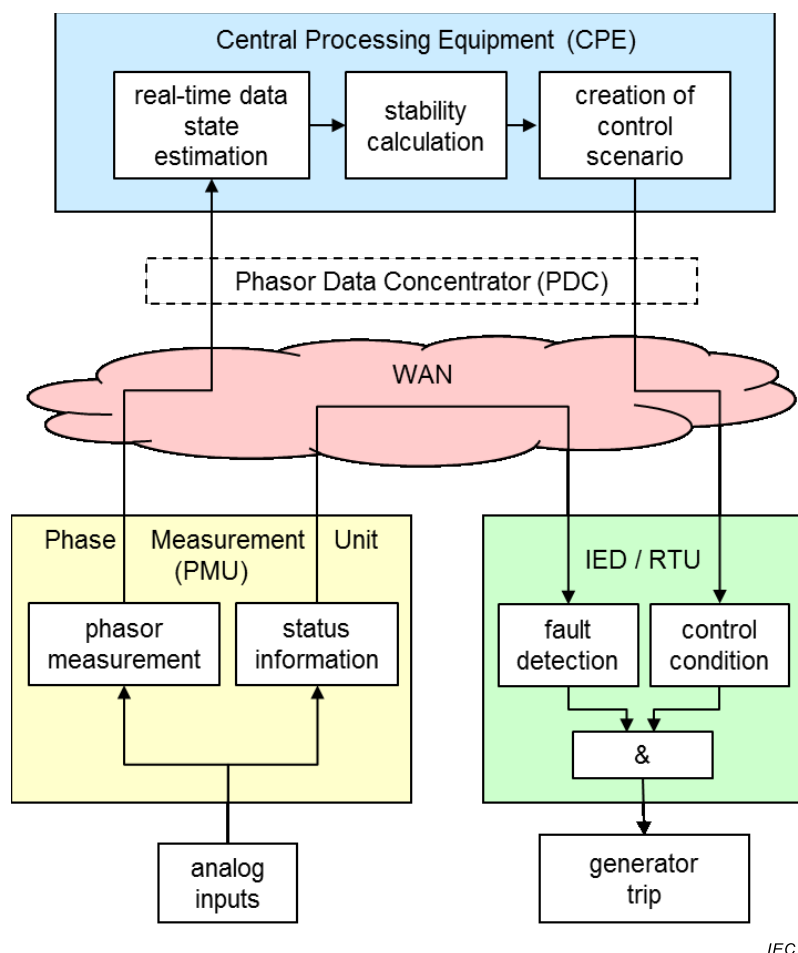
**Figure 22 – Target phenomena for WAMPAC**

NOTE More detailed typical use cases for WAMPAC are described in IEC TR 61850-90-1 and IEC TR 61850-90-5.

### 6.8.2 WAMPAC communication requirements

WAMPAC systems receive information over the WAN from across a large area of the grid and perform control actions to maintain grid stability.

Figure 23 shows an example of general architecture, functions and information flow.



IEC

**Figure 23 – Example of main function and general information flow**

The PMUs are installed at each of the measurement points in the grid. They send the measurement data and switchgear status information to the CPE via a WAN (and PDCs if necessary). They send the same information to an IED that also participate in the stability.

The CPE estimates the grid state using the data received from the PMUs. If it detects an instability phenomenon, it creates as a countermeasure a control scenario and sends it to the IED. The IED sends the tripping signal(s) to the generator(s) determined from the status of the grid, relevant switchgear status and other information received from the PMU in accordance with the respective control scenario for each type of fault sent from the CPE.

In addition to the WAMS functionality, a WAMPAC system is able to act on the electrical grid, e.g. for load shedding or adjustment of FACTS devices. This requests not only an upward communication from the PMUs to the control centre, but also a downward communication to the substations to operate the switching equipment. This up-to-down control path with strict timing requirements is what distinguishes WAMPACS from WAMS.

Table 19 summarizes the typical communication requirements of WAMPAC. Precise time synchronization is required to synchronize the phasor data measurement in the PMUs. The required latency, time synchronization, etc. depend upon each phenomenon of grid instability.

Table 19 also indicates the quantity of PMUs, the data size and the transmission distance because these items are needed for engineering of the practical WANs.

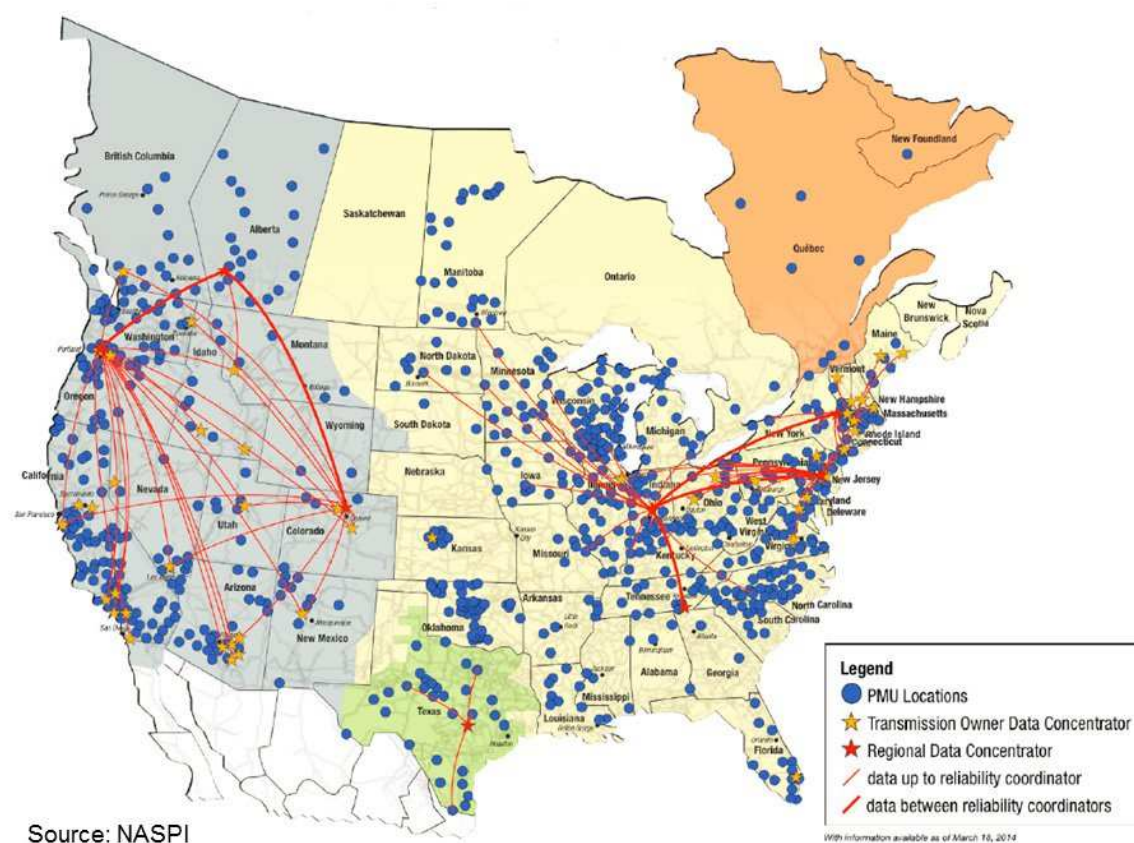
**Table 19 – Typical communication requirements for WAMPAC**

Phenomena	Operating delay [ms]	Route	Data	Time accuracy	Latency [ms]	Interval	PMUs Qty.	Data [octets]	Range [km]
Rotor angle stability (Transient Stability)	150 to 250	PMU to PDC or CPE PMU to IED	Phasor	50 $\mu$ s	5 000 20	100 ms to 1 s 20 ms	500	100	500
Rotor angle stability (small disturbance angular stability)	1 000 to 5 000	PMU to IED	Phasor	50 $\mu$ s	20	1 / cycle	10	100	500
Frequency stability	200	PMU to IED	Phasor	50 $\mu$ s	20	20 ms	50	100	250
Voltage stability	100 to 10 000	PMU to IED	Phasor	100 ms	20	1 / cycle	10	100	250
Overload	3 000 to 100 000	PMU to IED	Phasor	1 s	1000	2 s	10	100	500

SOURCE: [40]

### 6.8.3 Use case WAMPAC

NASPI [37] documented the synchrophasor distribution for North America, shown in Figure 24. Some 1000 PMUs were installed until 2014, March 19.

**Figure 24 – PMUs and data flow between TSO and regional data hubs**

## 6.9 Wind turbines and wind virtual power plants

IEC 61400-25, *Communications for monitoring and control of wind power plants* and IEC 61400-25-4, *Mapping to communication profile* make no recommendation on network topology or performance.

## 6.10 Distributed Energy and Renewables (DER)

IEC 61968 and IEC TR 61850-90-7 make no recommendation on network topology or performance.

## 6.11 Summary of communication requirements for WAN

Table 20 reduces the communication requirements to four distinct classes to which all requirements are mapped, with about one order of magnitude in between.

**Table 20 – Classification of communication requirements**

	Class WA	Class WB	Class WC	Class WD
Application field	EHV	HV	MV	General purpose
Latency	3 ms	10 ms	100 ms	1000 ms
Jitter	10 µs	100 µs	1 ms	10 ms
Latency asymmetry <sup>1)</sup>	100 µs	1 ms	10 ms	100 ms
Time accuracy <sup>2)</sup>	1 µs	10 µs	100 µs	10 to 100 ms
Bit error ratio	10 <sup>-7</sup> to 10 <sup>-6</sup>	10 <sup>-5</sup> to 10 <sup>-4</sup>	10 <sup>-3</sup>	
Unavailability	10 <sup>-7</sup> to 10 <sup>-6</sup>	10 <sup>-5</sup> to 10 <sup>-4</sup>	10 <sup>-3</sup>	
Recovery delay)	zero	50 ms <sup>3)</sup>	5 s <sup>4)</sup>	50 s <sup>5)</sup>
NOTE 1 The jitter requirement can be relaxed if common clock synchronization exists.				
NOTE 2 Applies to time distribution only.				
NOTE 3 Compatible with SDH/SONET, MPLS and IP (FRR).				
NOTE 4 Compatible with RSTP/MSTP.				
NOTE 5 Compatible with IP recovery.				

Since the requirements vary with power system configurations, operations and regulations, the requirements are classified by the order of magnitude as shown in Table 21, but actual numbers may differ.

**Table 21 – Communication requirements of wide-area applications**

Application (Function)	Link	Bandwidth [kbit/s]	Latency [ms]	Jitter [ms]	Asymmetry [ms]	Time accuracy [µs]	Error rate	Unavailability	Recovery delay [ms]
Analog comparison line protection	SS-SS	9,6 to 64	3	0,01		1	10 <sup>-6</sup>	10 <sup>-6</sup>	0
State comparison line protection	SS-SS	< 10	10	0,1	–	1	10 <sup>-6</sup>	10 <sup>-6</sup>	0
Transfer tripping	SS-SS	< 10	3	0,3	–	1	10 <sup>-6</sup>	10 <sup>-6</sup>	25
WAMS	SS-CC	10 to 100	100	1	–	1	10 <sup>-6</sup>	10 <sup>-6</sup>	50



Application (Function)	Link	Bandwidth [kbit/s]	Latency [ms]	Jitter [ms]	Asymmetry [ms]	Time accuracy [ $\mu$ s]	Error rate	Unavailability	Recovery delay [ms]
WAMPAC for transient stability	SS/PS-CC	10 to 100	10	0,1	A	1	$10^{-6}$	$10^{-6}$	50
WAMPAC for dynamic stability	SS/PS-CC	10 to 100	10	0,1	–	1	$10^{-6}$	$10^{-6}$	50
WAMPAC for frequency stability	SS/PS-CC	10 to 100	10	0,1	–	1	$10^{-6}$	$10^{-6}$	50
WAMPAC for voltage stability	SS-CC	10 to 100	10	0,1	–	1	$10^{-6}$	$10^{-6}$	50
WAMPAC against overload	SS-CC	10	10	0,1	–	1	$10^{-6}$	$10^{-6}$	50
SCADA (Supervision, telemetry, telecontrol)	SS/PS-CC	1 to 10	100	1	–	1	$10^{-6}$	$10^{-6}$	50
Load dispatch, AFC	PS-CC	10 to 100	100	1	–	1	$10^{-6}$	$10^{-6}$	50
Inter-control centre SCADA data exchange	CC-CC	10 to 100	100	1	–	–	$10^{-6}$	$10^{-6}$	50
Inter-control centre file transfer	CC-CC	~1 000	100	1	–	–	$10^{-6}$	$10^{-6}$	500
Dispatch command voice	PS-CC	< 64	100	1	–	–	$10^{-6}$	$10^{-6}$	50
Workforce voice	SS-CC	< 64	100	1	–	–	$10^{-6}$	$10^{-6}$	50
Video surveillance	SS-CC	100 to 1 000	1000	10	–	–	$10^{-6}$	$10^{-6}$	500
Fault location	SS-CC	< 10	10	0,01	0,01	1	$10^{-6}$	$10^{-6}$	25

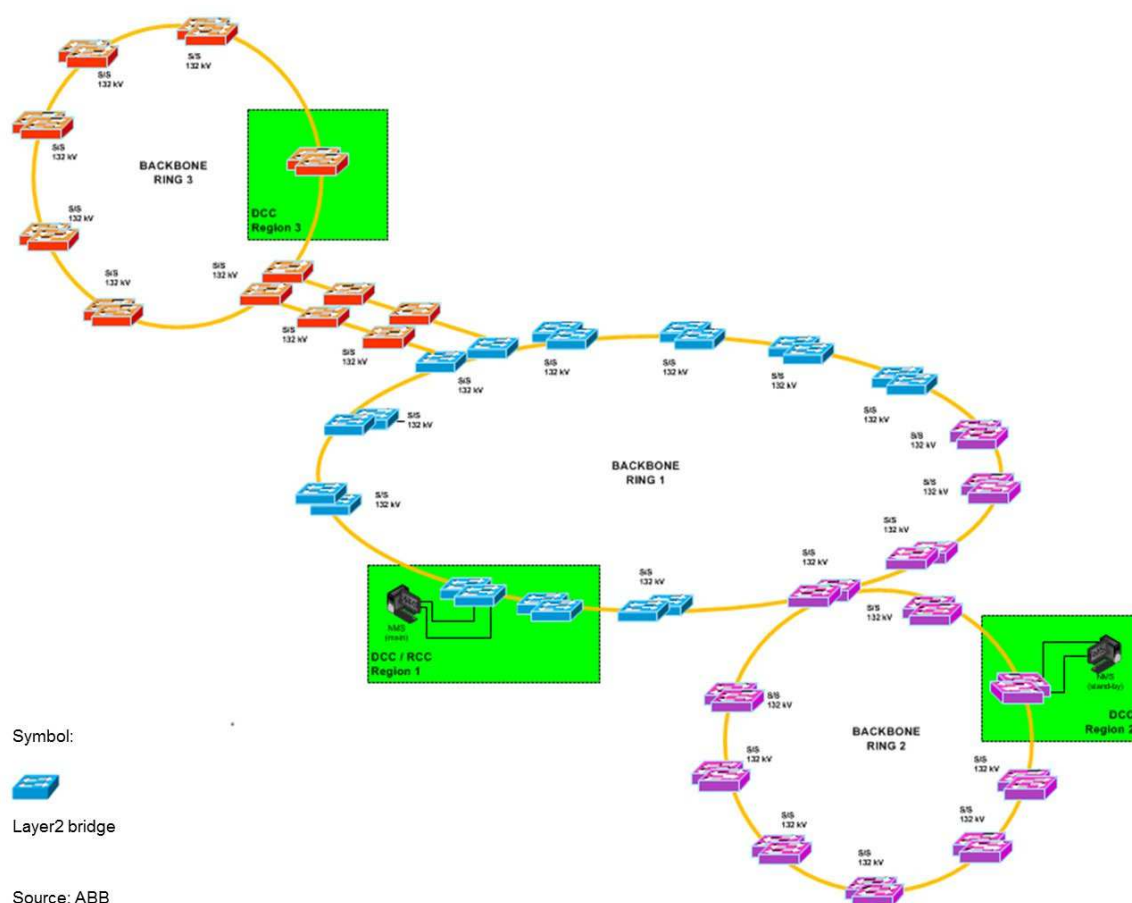
## 7 Wide-area and real-time network technologies

### 7.1 Introduction

Clause 7 describes the technologies available for WAN in utility networks. The description of the technologies is kept general (with a few exceptions), with emphasis on the power utility application.

### 7.2 Topology

The topology of the WANs varies widely. Popular topologies are rings and meshed rings since they provide inherently link redundancy. Since the topology follows that of the high voltage lines, limitations exist. For instance, the network for power plants located at the end of a long valley do not fit easily into a ring. Figure 25 shows an example in which the rings are explicit.



IEC

**Figure 25 – Network topology (Carrier Ethernet)**

### 7.3 Overview

Any network has:

- a data plane that switches the circuits or packets (corresponding to the old relays in analog telephony);
- a control plane that determine how data are routed from network element to network element (corresponding to the dialing pulses processing in analog telephony); the control plane can be either “in-band”, using the same channels as the data or “out-band”, using another channel.
- a management plane for installing, configuring and supervising the network elements.

Table 22 summarizes the technologies for building the WANs while providing the performance required.

**Table 22 – Communication technologies**

Technology	ATM	SDH/ SONET	Carrier Ethernet	IP	IP/MPLS	MPLS-TP
Layer	2	1 & 2	2	3	2,5	2,5
Medium	ATM	OCxx, STMxx	IEEE 802.3	Any	Based on IEEE 802.3	Based on IEEE 802.3
Topology	Mesh	Mesh, ring linear, P2P	Mesh, ring (Logical tree)	Mesh	Mesh, rings	Mesh, rings
Bandwidth	Depends on Layer 1	Up to 40 Gbit/s	Ethernet speed	Depends on Layer 2	Depends on Layer 2	Depends on Layer 2
Medium access	TDM	TDM	Prioritized random access, no pre-emption	Prioritized random access, no pre-emption	Prioritized random access, no pre-emption	Prioritized random access, no pre-emption
Recovery delay	50 ms	50 ms	RSTP: 50 ms typical  ITU-T G.8032: < 50 ms  PRP & HSR: zero.	50 ms achievable with FRR, otherwise no upper bound (some seconds)	50 ms (ring redundancy)	50 ms (ring redundancy)
Path congruency	Same circuit back and forth	Same circuit back and forth	yes (broadcast domain)	Path in both directions can vary	Can be enforced by engineering	Can be enforced by engineering
Synchronization	Native	Native	1588, SyncE	NTP, SNTP	SyncE, PTP Telecom profile Layer 3, PTP Time and Phase	SyncE, PTP
Routing	Circuit- switched	Circuit- switched	Broadcast with MAC address filtering and VLANs	Automatic: OSPF, IS-IS	Automatic, LSP or static by TE: 802.1ag, ITU-T Y.1731	Static
Configuration	Control plane or management plane	Control plane	Automatic (RSTP, IEEE 802.1D )	Automatic (OSPF, IS- IS, SNMP)	Automatic (LDP)	Management plane
Quality of service	ATM	TDM	802.1Q	DiffServ, IntServ	MPLS	MPLS
Virtual network	Virtual paths, virtual circuits	None	VLAN	VRF	VPWS, VPLS, L3VPN	VPWS, VPLS
Suitability for differential protection	Yes	Yes	Only with precise time distribution	Only with precise time distribution	Only with precise time distribution	Only with precise time distribution
Suitability for binary teleprotection	Yes	Yes	Yes	With careful engineering	Yes	Yes
Packet transport	EoATM	EoSDH EoSONET EoTDM	Native	Native	Native	Native
Pseudowire (VPWS)	native	native	yes	yes	yes	yes
Suitable for	Large networks	Large networks	Small networks	Very large networks	Large networks	Medium networks

Technology	ATM	SDH/ SONET	Carrier Ethernet	IP	IP/MPLS	MPLS-TP
Observations	Obsolete	Widely used in utility networks	Widely used in Metropolitan and access networks	Widely used in WANs	Widely used in carrier networks, increasing use in utilities	Possible migration path from SDH/SONET to PSN

Subclauses 7.4 to 7.11 describe the layers of communication in the order of the OSI model.

## 7.4 Layer 1 (physical) transmission media

### 7.4.1 Summary

Table 23 lists the media detailed in Clauses 7.4.3 to 7.4.6.

**Table 23 – Physical communication media**

Name	Type	Bit rate	Propagation delay	Distance without repeaters	Standard
Metallic wire					
	Twisted Wire Pair	1 kbit/s to 10 Gbit/s	5 µs / km	500 m	RS 485
	Coaxial	1 kbit/s to 10 Gbit/s	5 µs / km	1 km	Various, e.g. ITU-T G.623
	CAT5-CAT6	100 Mbit/s to 10 Gbit/s	5 µs / km	100 m	ANSI/TIA-568
Optical fiber					
	Multimode (led transmitter)	100 Mbit/s to 10 Gbit/s	5 µs / km	2 km	ITU-T G.957
	Single mode (laser)	1 Tbit/s	5 µs / km	>100 km	ITU-T G.652 ITU-T G.653
	Single mode (WDM)	> 1 Tbit/s	5 µs / km	>100 km	ITU-T G.671 ITU-T G.694.1 ITU-T G.694.2
Radio					
	Omnidirectional	1 Gbit/s	3,3 µs / km	10 km	-
	Microwave	10 Gbit/s	3,3 µs / km	up to 150 km (200 km at reduced bit rate)	-
Power line carrier					
	HV (point to point)	few kbit/s to 300 kbit/s	13 µs to 4,2 µs per km	1000 km	IEC 60495 IEEE P1901 (TDM)
	MV, LV meshed	10 kbit/s to 100 kbit/s, up to 30 Mbit/s	5 µs / km	Up to 2 km depending on power cable	IEEE 1901

### 7.4.2 Installation guidelines

IEEE 487.3 provides guidelines for installation of communication facilities for power utilities.

### 7.4.3 Metallic lines

While metallic lines are not properly a WAN technology, they are mentioned here since it is generally the “last mile” access to the WAN and the interface to the SEN.

WAN router ports are normally metallic lines and therefore these standards are relevant for the understanding of WAN vocabulary.

There exist a number of standards for attaching RTUs such as RS-232 and RS-485, which offer speed of up to 256 kbit/s over short distances. Such standards make no assumption on the transported signals. RS-485 requires the use of twisted pair cables with an impedance of 120  $\Omega$ .

Ethernet cables are shielded, twisted pair cables with several twisted pairs in the same shield. The category of the Ethernet cable expresses over which distance the cable can transmit the Ethernet frames at a given bit rate. The recommended technology is Cat6, which is suitable for all Ethernet speeds up to 1 Gbit/s over a distance of 100 m and it is therefore future-proof. However, in substation environment, it is not recommended to span copper cables over such distances, fibers are recommended instead.

Twisted pair cables are used not only for analog telephone links (POTS) but also for digital data communications based on so-called digital subscriber lines (DSLs).

DSLs include Asymmetric DSL (ADSL) and Very high-bit-rate DSL (VDSL) whose data rates on downstream and upstream are not the same (asymmetric) as well as High-bit-rate DSL (HDSL), Symmetric DSL (SDSL) and Single line High speed DSL (SHDSL) whose data rates are symmetric.

ADSL over analog telephone lines utilizes a band from 26,075 kHz to 137,825 kHz for upstream communication and one from 138 kHz to 1104 kHz for downstream communication.

VDSL utilizes a band from 25 kHz to 12 MHz.

Twisted pair cable communications suffer from signal attenuation and noise caused internally (e.g. crosstalk, reflections and echo) and caused externally (e.g. disturbances from power supply and radio emissions). These effects limit the data rates and transmission distances.

Table 24 compares the different DSL technologies.

**Table 24 – DSL communication over twisted pairs**

Name	Downstream rate	Upstream rate	Maximum range	Standard and note
ADSL over POTS	12,0 Mbit/s	1,3 Mbit/s	8 km	ITU-T G.992.1 Annex A
VDSL	55,0 Mbit/s	3,0 Mbit/s	300 m	ITU-T G.993.1
HDSL	2,048 Mbit/s	2,048 Mbit/s	4 km	ITU-T G.991.1 One to three pairs
SDSL	2,048 Mbit/s	2,048 Mbit/s	3 km	ITU-T G.991.2 One pair
SHDSL	4,608 Mbit/s	4,608 Mbit/s	6 km	ITU-T G.991.2 Two pairs

Table 25 details the trade-offs of copper cable communication.

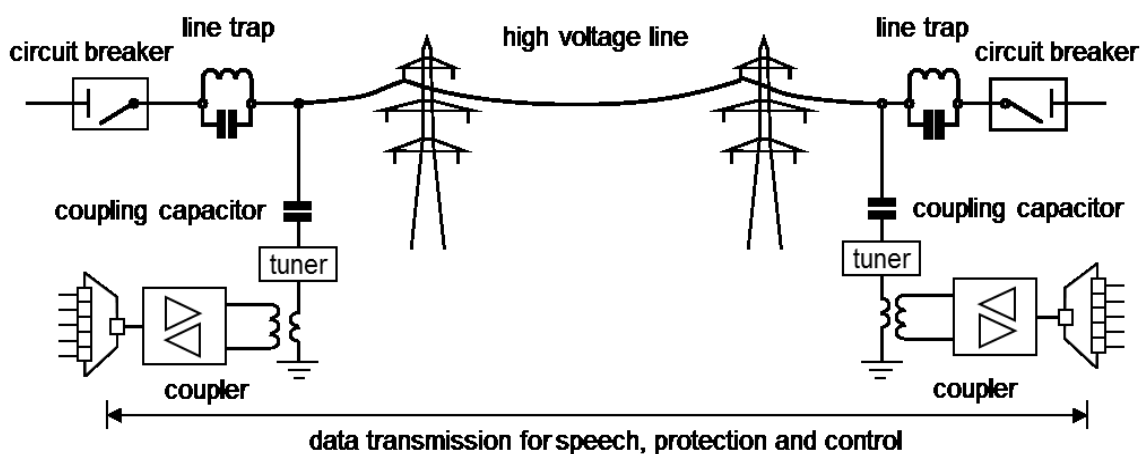
**Table 25 – Trade-offs in copper cable communication**

Advantages	Disadvantages
Cost-effective	Disaster susceptible (overhead cable)
Medium transmission rate (a few Mbit/s)	Short transmission range

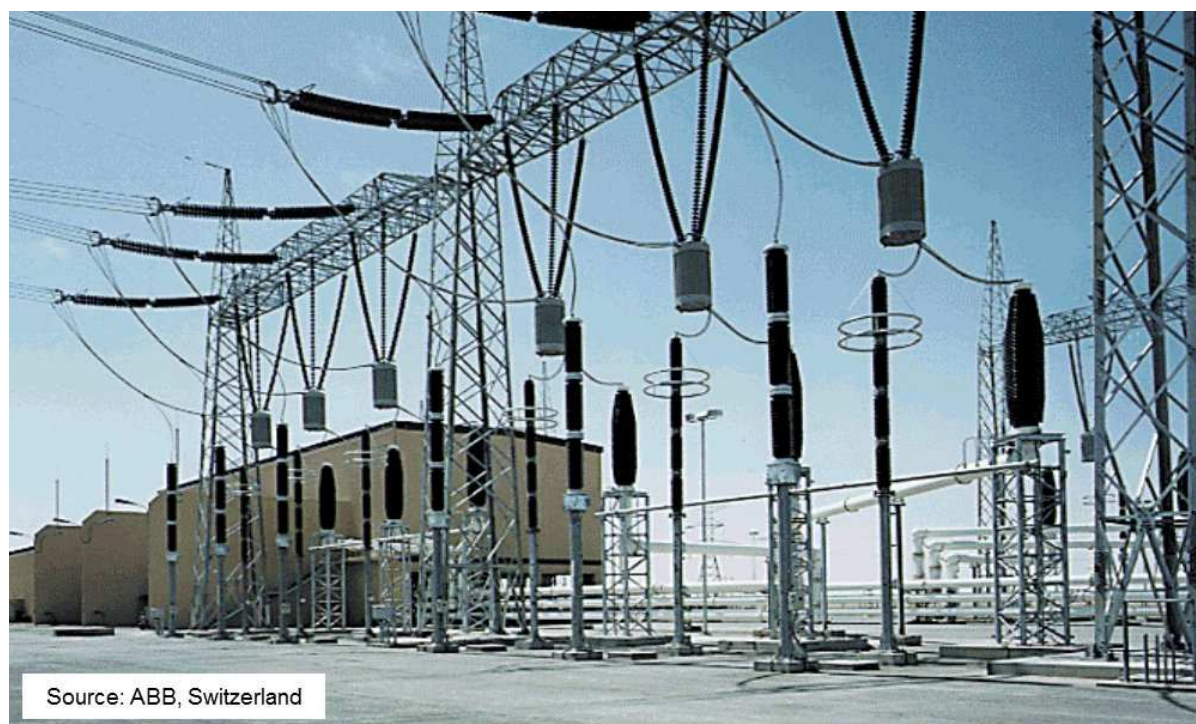
#### 7.4.4 Power line carrier (PLC)

PLC is one of the oldest data transmission schemes in power transmission. It uses the high-voltage lines as a waveguide. The HF signal is coupled and decoupled by means of coupler, coupling capacitors and line traps. Phase to ground and phase-to-phase coupling/ differential coupling may be used.

Figure 26 and Figure 27 show the phase-to-ground coupling, which is seldom used in HV.



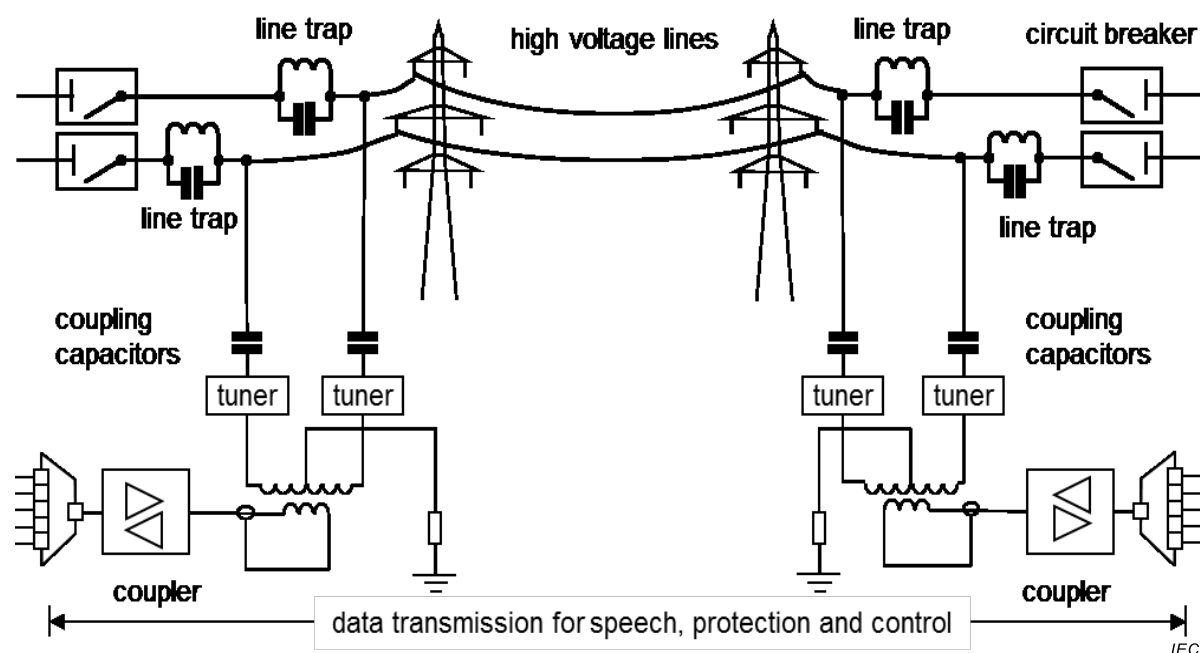
**Figure 26 – Phase-to-ground coupling for PLC**



IEC

**Figure 27 – HV PLC coupling with suspended line traps**

Signal coupling phase to phase is recommended because of the lower attenuation and the possibility to maintain data transmission even with a phase down. Figure 28 and Figure 29 show the phase-to-phase coupling.



**Figure 28 – Phase to phase signal coupling for PLC**





IEC

**Figure 29 – Phase-to-phase signal coupling**

Figure 30 shows the installation of the traps.





**Figure 30 – Power line carrier, line traps**

The transmission speed of PLC has increased due to progress in the encoding scheme, which started as simple Analogue Power Line Carrier (APLC) with one voice channel. The Digital Power Line Carrier (DPLC) equipment allows transmission at 128 kbit/s and 256 kbit/s. The DPLC equipment uses the same coupling system (coupler, coupling capacitors, line traps) to the HV Line as the APLC.

The PLC technology is also used in distribution networks without line traps, with reduced distance, but increased data rate, as shown in Table 26.

**Table 26 – PLC communication technologies**

Voltage level	Technology	Narrowband	Broadband
		9 kHz to 95 kHz, 10 kHz to 490 kHz	1,8 MHz to 30 MHz
		Low/medium data rate	High data rate
		4,8 kbit/s to > 128 kbit/s	> 100 Mbit/s
High voltage 380 kV (WAN)			
	Range	> 1 000 km	
	Application	Teleprotection, utility communication, SCADA	
	Standards	IEC 60495, IEC 62488-1	
Medium voltage 30 kV (RAN)			
	Range	0,5 km to 10 km	0,5 to 1,5 km
	Application	Distribution automation Ripple Control	Smart Grid backbone

Voltage level	Technology	Narrowband	Broadband
		9 kHz to 95 kHz, 10 kHz to 490 kHz Low/medium data rate 4,8 kbit/s to > 128 kbit/s	1,8 MHz to 30 MHz High data rate > 100 Mbit/s
	Standards	IEC 62488-1, IEC 61334-5-4, PRIME, PLC G3, IEEE 1902.2	IEEE 1901
Low voltage 230/380V (NAN)			
	Range	50 m to 1 000 m	50 m to 1 000 m (3 km)
	Application	AMR, Demand Response	Last mile Internet access
	Standards	IEC 61334-5-x, IEEE 1901.2, ITU G.hnmem	IEEE 1901, ITU-T G.hn
Low voltage 230/380V (HAN, LAN)			
	Range	50 m	50 m
	Application	Building automation	In-house data network
	Standards	X-10, LON PLC, KNX-PLC IEEE 1901.2 ITU G.hnem	HomePlug IEEE 1901, ITU-T G-hn

The propagation delay of PLC varies depending on the line characteristics (F/m, H/m); it typically lies between 4  $\mu$ s/km and 13  $\mu$ s/km.

Table 27 shows the advantages and disadvantages of PLC communication.

**Table 27 – PLC communication advantages and disadvantages**

Advantages	Disadvantages
Communication independent of external provider	Disaster susceptible (if high-voltage lines are damaged)
Uses existing power lines	Needs access to the high-voltage line
Cost-effective	Low bandwidth (< 1 Mbit/s) with narrowband technology
Robust, long-distance communication	Correlation between line fault and communication channel: not suited for analog comparison schemes

## 7.4.5 Radio transmission

### 7.4.5.1 General

Radio links are part of the WAN transmission, especially when used for substation to substation communication and for distribution grids.

Radio transmission features can be divided into:

- omnidirectional versus directional depending on the type of antenna;
- licensed bands (costly, difficult to obtain, but in principle interference-free) versus unlicensed bands (free, but shared with an unpredictable traffic);
- fixed versus mobile – the latter being interesting for workforce communication;
- indoor units versus outdoor units depending on the suitability for shelter or field mounting.

The covered range depends on:

- frequency band;
- topography (the higher the frequency, the more the antennas must be in line-of-sight);

- data transmission bandwidth (the data rate is reduced when the signal quality deteriorates);
- radio propagation conditions (reflection, refraction, diffraction, multipath, rain/snow attenuation) and interference from other radio systems;
- transmitting power, this may be regulated in some countries.

Moiré effects due to multiple paths or several senders can create dark spots even when nodes located further away still operate correctly.

The range impacts the distance between relays and the battery lifetime.

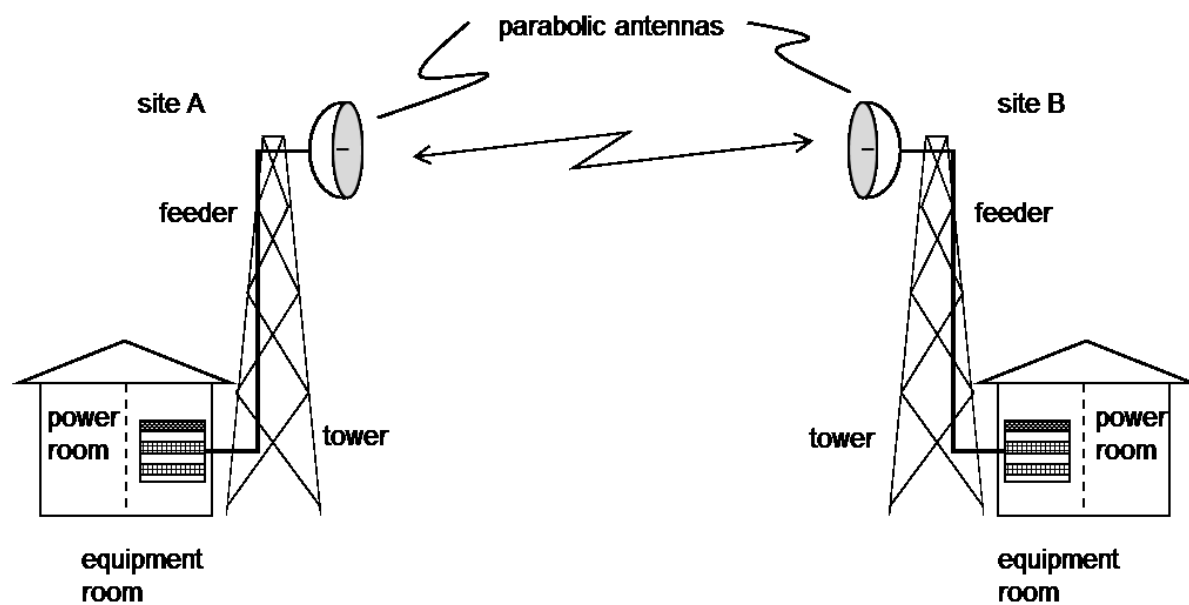
Space and frequency diversity can be used (separately or not) to increase the reliability.

Although the range of one radio link is limited, terrestrial radio networks can be built by using each node as a relay (as in distribution grids) or base station (as in public mobile radio).

#### 7.4.5.2 Terrestrial fixed microwave radio

Terrestrial fixed microwave radio has long been in use for critical applications such as power system monitoring, protection and control.

Microwave technologies are deployed in clear line-of-sight conditions and offer point-to-point connectivity, as shown in Figure 31.



IEC

**Figure 31 – Terrestrial microwave link**

Table 28 shows typical microwave link performances.

**Table 28 – Microwave link performance**

Link type	Carrier	Range	Bandwidth	Configuration
long-haul	4 GHz to 11 GHz	100 km to 150 km	10 Gbit/s	Multichannel 10+0
short-haul	13 GHz to 42 GHz	few tens of km	2 Gbit/s to 2,5 Gbit/s	Multichannel 4+0.
very short link	60 GHz to 80 GHz	few km	1 Gbit/s to 2 Gbit/s	Single channel at 500 MHz
NOTE The covered distance depends on regulations (permitted transmission power)				

Table 29 shows the advantages and disadvantages of terrestrial microwave.

**Table 29 – Terrestrial microwave advantages and disadvantages**

Advantages	Disadvantages
Relatively cost-effective installation, no digging required.	Bandwidth depends on link design and local conditions
long haul communication capability;	Short period of outages during fading and/or attenuation in certain terrains and frequency bands, depending also on the weather and other meteorological phenomena.
little interference from the power system asset failures (unlike optical fibers using the power masts)	Disaster-sensitive if antenna located on power masts. (isolated microwave towers are preferred)

#### 7.4.5.3 Terrestrial omnidirectional radio

VHF and UHF radio connections serve as a backup, especially for disaster recovery, although their data rate is limited (some 10 kbit/s), since their main use is voice.

Popular bands are:

- 135 MHz to 180 MHz (VHF)
- 290 MHz to 350 MHz (VHF/UHF)
- 380 MHz to 470 MHz (UHF)

For instance, the TETRA UHF technology is in wide use for Digital Mobile Radio (DMR) connection to mobile workforce and supports group calls, which is not the case for public mobile radio.

#### 7.4.5.4 Terrestrial mobile radio (licensed/unlicensed) and wireless LAN/MAN

Table 30 lists the major terrestrial mobile radio technologies.

**Table 30 – Public mobile radio technologies**

Technology	Bands country dependent	Range	Data rate	Status
GSM	850 MHz to 1 900 MHz	26 km	9,6 kbit/s	1 <sup>st</sup> generation
GPRS	850 MHz to 1 900 MHz	26 km	80 kbit/s (downlink) 40 kbit/s (uplink)	2 <sup>nd</sup> generation
UMTS	850 MHz to 2 100 MHz	29 km	384 kbit/s to 2 Mbit/s	3 <sup>rd</sup> generation
UMTS WCDMA	850 MHz to 2 500 MHz	200 km	7,2 Mbit/s	3 <sup>th</sup> generation
UMTS – HSPA+	850 MHz to 2 500 MHz	29 km	28 Mbit/s to 42 Mbit/s 168 Mbit/s downlink)	3 <sup>th</sup> generation enhanced for IP data traffic
WiMAX (IEEE 802.16-2004)	2 GHz to 66 GHz	100 m	30 Mbit/s to 40 Mbit/s (1 Gbit/s)	Obsoleted by LTE
LTE	700 MHz to 2 600 MHz	14 km to 103 km	150 Mbit/s (300 Mbit/s (4G+))	4 <sup>th</sup> generation
Wi-Fi/WLANs (IEEE 802.11)	2,4 GHz, 5 GHz	100 m	11 Mbit/s to 54 Mbit/s to 600 Mbit/s	hotspots

A multi-hop WLAN can offer longer-range transmission links. Although they have drawbacks regarding availability and latency for protection application, terrestrial radio serves as backup for short-range telecontrol links in face of natural disasters (see Table 31).

**Table 31 – Terrestrial radio advantages and disadvantages**

Advantages	Disadvantages
Cost-effective and easy to install	Short transmission range (< 10 km)
Disaster tolerant	Performance degradation due to radio interference and screening, radio jamming attack susceptible
Transmission rate of tens of Mbit/s depending on radio environment	Dozens of milliseconds up to seconds (depending on technology, topology etc.) of residence delay per hop

#### 7.4.5.5 Satellite radio

Satellite radios use microwave bands to communicate via geostationary or low-orbit satellites, see Table 32.

**Table 32 – Satellite radio advantages and disadvantages**

Advantages	Disadvantages
Ubiquitous	Limited bandwidth, very long latency
Can be used for back-up and disaster-recovery	Frequent outages during fading and/or attenuation in certain terrains and frequency bands (depending also on the weather and other meteorological phenomena).
Little interference from the power system asset failures (unlike optical fibers in earthing cables)	Costly, precious bandwidth
	Subject to jamming, DoS attacks, spoofing and interception

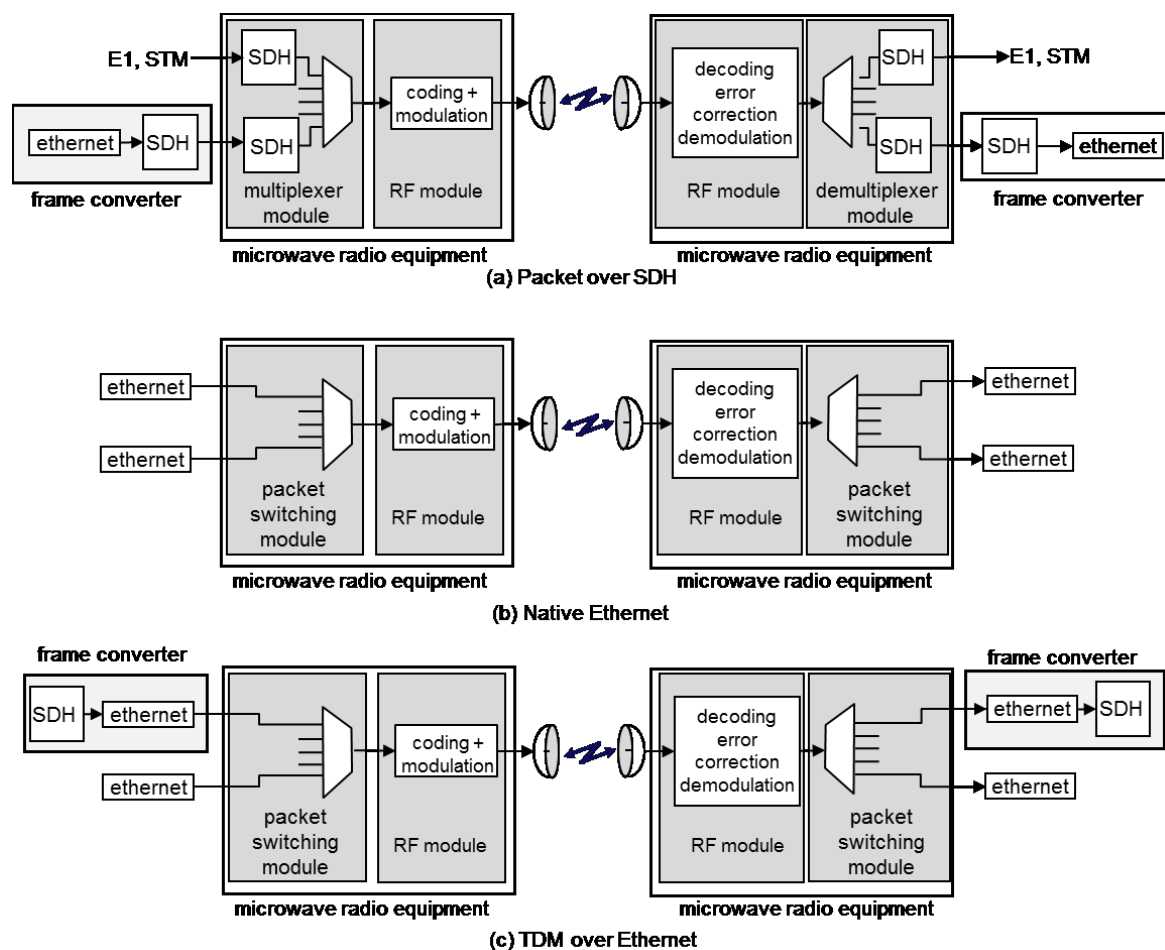
#### 7.4.5.6 Microwave radio links

Digital radio links transport Layer 2 as:

- a) PDH/SDH/SONET interfaces T1 or E1 interfaces (see 7.6.1.2), (Figure 32 a);

b) native Ethernet interfaces (Figure 32 b);

c) TDM traffic converted to packet stream and all traffic handled as packets (Figure 32 c).

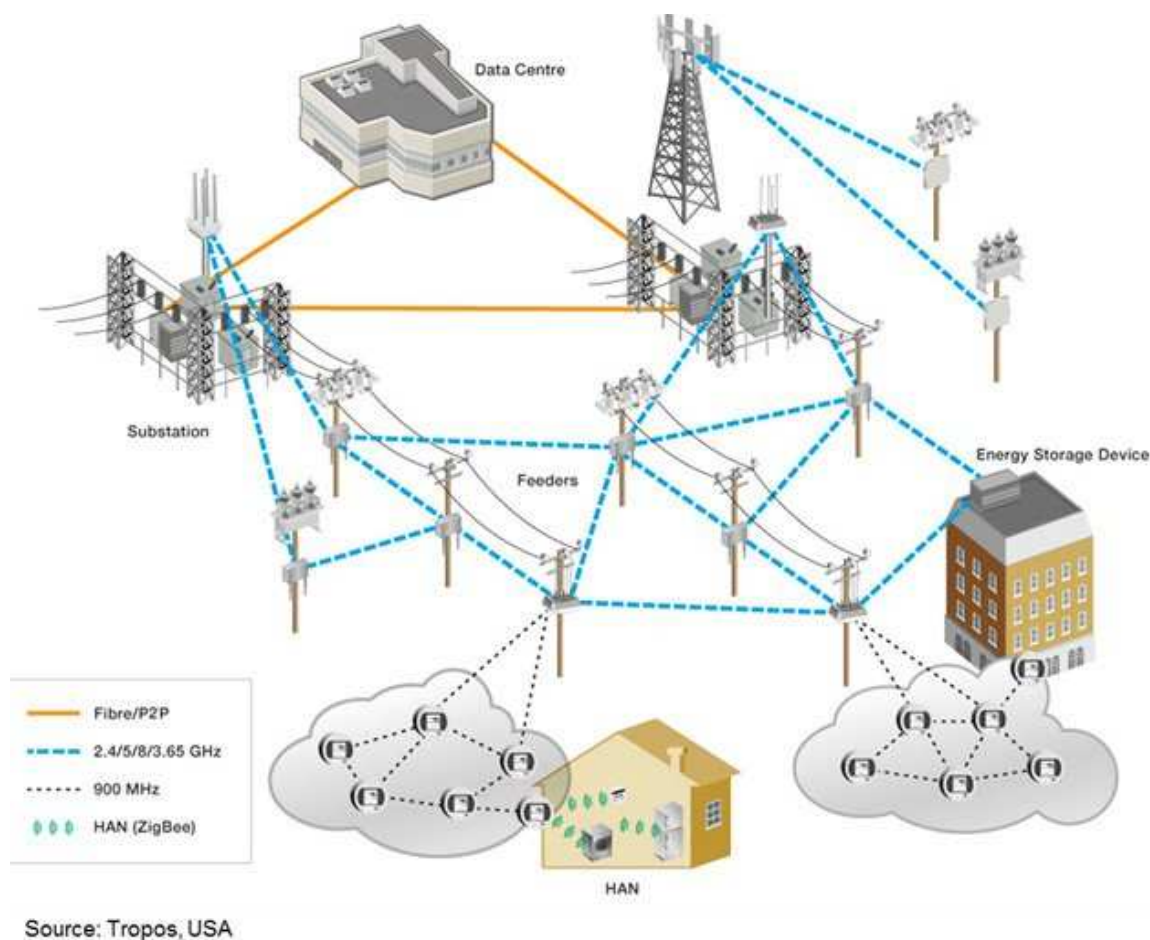


IEC

Figure 32 – Layer 2 transport on radio systems

#### 7.4.5.7 Application of radio in distribution networks

In spite of its high BER, radio communication is well suited for distribution and feeder automation. Each radio node acts as a relay and some nodes connect to a trunk network in a substation, as shown in Figure 33.



IEC

**Figure 33 – Radio network in feeder automation**

NOTE The Home Area Network (HAN) is not addressed in this Technical Report.

## 7.4.6 Fiber optics

### 7.4.6.1 General

Optical fibers are the medium of choice for all utility communications, within and outside substations. The available bandwidth is well in excess of what is needed for the operation communication. Since optical fibers are laid on the electrical high voltage towers, the topography of the network closely follows that of the electrical grid, with each substation becoming a network node. ITU publication [10] gives a comprehensive overview.

### 7.4.6.2 Fiber types

Fibers used within substations are usually multi-mode fibers (50/125  $\mu\text{m}$ ) operated at 1 300 nm wavelength (near infrared) and limited to distances of a few kilometers without repeaters.

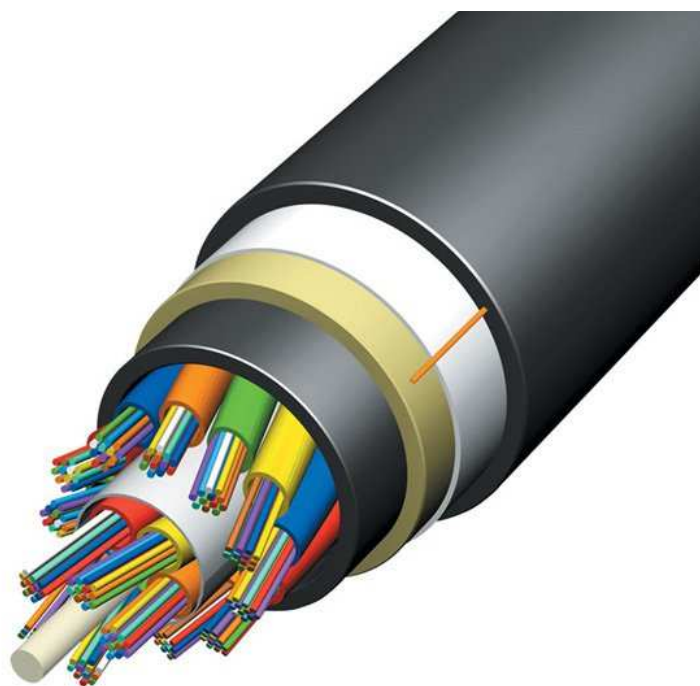
Fibers used in WAN are usually single mode fibers (9/125  $\mu\text{m}$ ) operated at 1 310 nm or 1 550 nm which present an attenuation of 0,3 dB/km plus 0,1 dB per splice and some 0,75 dB per connector. Single-mode fibers allow spanning more than 100 km without repeaters.

Fibers offer a strict separation since crosstalk is not a factor. Therefore, this allows separating the critical traffic from the non-critical by giving each of them dedicated fibers.

NOTE IEEE C37.94 standardizes a fiber optical interface between teleprotection and multiplexer equipment for 50  $\mu\text{m}$  and 62,5  $\mu\text{m}$  multi-mode optical fibers operating at 830 nm with BFOC/2.5 connectors. In addition, it also defines an application layer frame structure that will not be considered here since it is a pure point-to-point, not a WAN technology. WANs transport C37.94 messages as a service.

#### 7.4.6.3 Fiber in separate cable

All Dielectric Self-Supporting (ADSS) optical cables are attached to high-voltage towers or poles (Figure 34). They are used for retrofit, lashed to a conductor (when the line has no ground cable) or to a ground wire (to avoid laying out a new ground cable). These fibers are therefore not shielded from the magnetic field of the line and this affects the optical characteristics and the dielectric of the fiber when the voltage exceeds 150 kV. ADSS cables are often used in 132 kV lines.



Source: AFL, USA

IEC

**Figure 34 – ADSS fiber cable**

Figure 35 shows a HV line with the retrofitted ADSS fiber cable and splicing box.

The ADSS may also be buried underground in a trench, which makes its failure independent from possible breakdown of high-voltage towers.





Source: Transener/Transba, Argentina

IEC

**Figure 35 – ADSS installation with splicing box**

#### 7.4.6.4 Fiber in ground cable

Fibers are often and preferably embedded in the earthing cable of high-voltage power lines, called Overhead Power Ground Wire (OPGW), see Figure 36. As a result, the network topology closely follows the high voltage lines topology, with the data communication equipment located in the substations.



Source: Kabelwerke Brugg, Switzerland

IEC

**Figure 36 – OPGW in ground cable**

The earthing cable contains one or more “C” tubes that each holds a bundle of fibers (Figure 37).



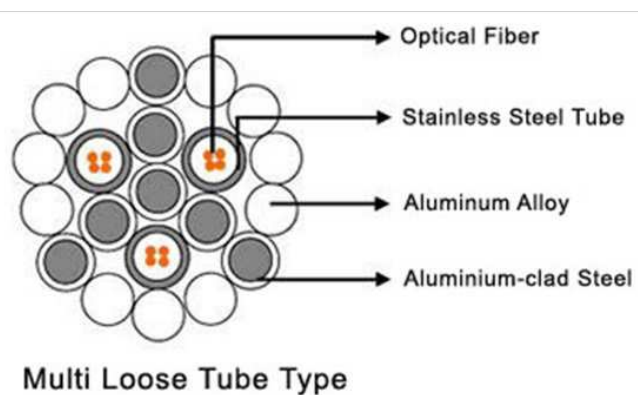
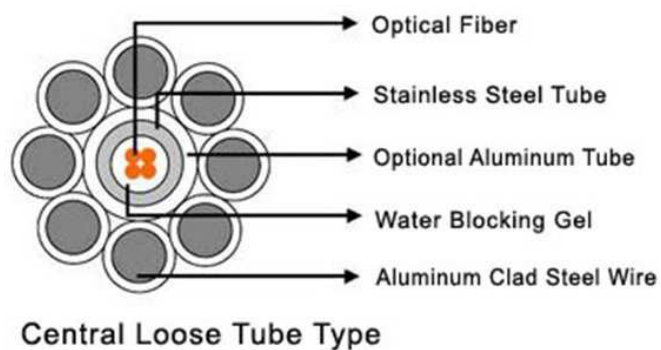
**Source: Kabelwerke Brugg, Switzerland**

*IEC*

**Figure 37 – OPGW with two “C”-tubes with each 32 fibers**

NOTE Figure 37 only illustrates a cross-section; a cable end for splicing would separate the “C” tubes from the cable down to the splicing box while the earthing cable would be fastened and stretched.

While a single tube can accommodate some 48 fibers, a multitube can accommodate over 200 fibers (Figure 38).



Source: Caledonian Ltd.

IEC

**Figure 38 – OPGW fibers**

IEC 60794-4-10 and IEC 60794-1-2 standardize OPGW.

#### **7.4.6.5 Fiber splicing**

The fibers are spliced about every 4 km in a box located on a high voltage mast. Some utilities install the boxes at ground level for easier access (Figure 39), other install it at 3 m to 5 m above ground. Figure 39 shows the splicing cassette box at the right.



Source: LightCom, Switzerland

IEC

**Figure 39 – Splicing box**

The same kind of box shelters repeaters or communication equipment.

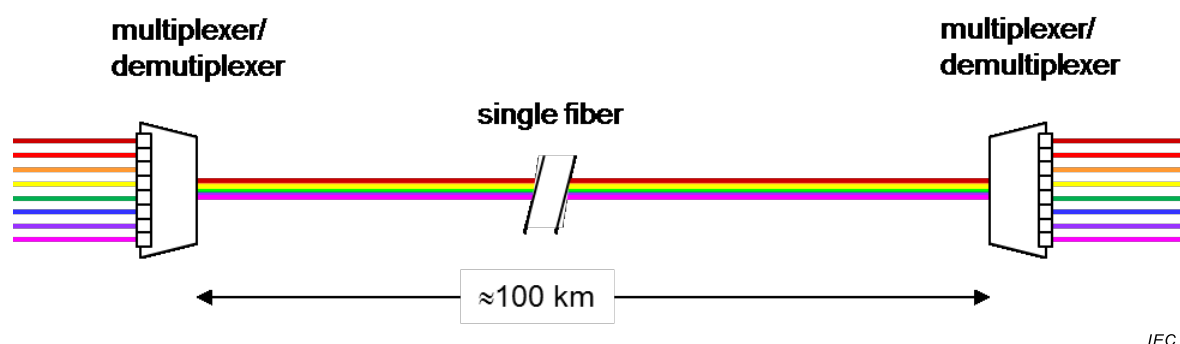
Fibers do not provide a better security than copper cables, splicing boxes outside of the premises are exposed and therefore intrusion control and data security apply to all communications over public ground.

#### **7.4.6.6 Wavelength Division Multiplexing (WDM)**

Each fiber can carry multiple optical channels when multiplexed by WDM.

While multimode optical fibers (such as used within a substation) are restricted to one wavelength only, single mode fibers allow sending simultaneously several optical beams with different wavelength, or “color”, as shown in Figure 40.

NOTE Colors in Figure 40 are for understanding only since present standards operate in the infrared wavelength region (1 600 nm to 1 200 nm – “red” would be 750 nm).



**Figure 40 – WDM over one fiber**

The complexity of WDM is hidden in the multiplexers; the user considers that corresponding ports are directly connected by individual fibers.

ITU-T standardized two multiplexing methods:

- Coarse Wavelength Multiplexing (CWDM) [ITU-T G.694.2] that operates with 16 channels from 1 270 nm to 1 610 nm separated by 20 nm;
- Dense Wavelength Multiplexing (DWDM) [ITU-T G.694.1] that operates with a small channel separation of 0,4 nm to 1,6 nm, requiring expensive and temperature-controlled equipment.

The weak point of WDM is the reliability of the transmitters, especially of laser diodes, which is in the range of 100 years to 200 years and decreases at higher bit rates due to warming.

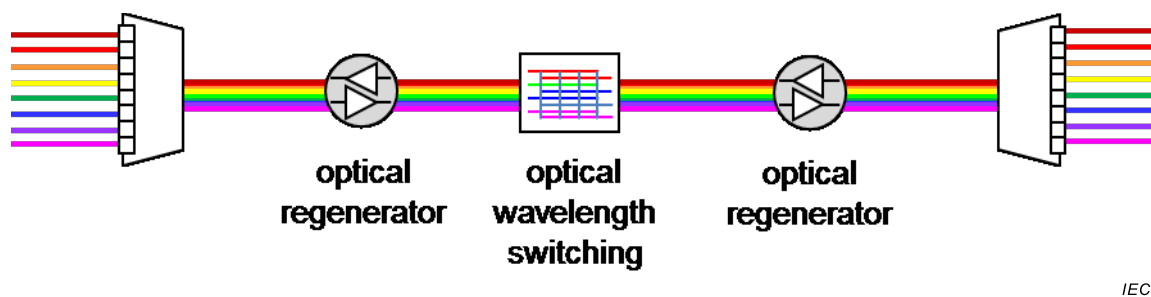
WDM multiplexing allows using the same fiber in both directions for full-duplex operation. This minimizes the medium asymmetry for very high accuracy clock synchronization.

When longer distances are needed, optical regenerators are used, which are based on erbium-doped fiber amplifiers.

#### 7.4.6.7 Optical Transport Network (OTN) OCh

OTN (ITU-T G.709) (7.6.2.10) specifies as a physical layer an optical channel OCh that uses optical switching.

ITU-T G.872 defines a Layer 1 data encoding that uses Forward Error Correction to reduce the level of signals in WDM fibers. It foresees optical regenerators and optical wavelength switching (Figure 41).



**Figure 41 – OCh optical components**

There exist a number of purely optical switching devices, the most promising ones being based on the MEMS technology.

#### 7.4.6.8 Passive Optical networks (PON, EPON)

Passive optical networks allow splitting of one fiber signal into different fibers with a passive splitter. Dividing the signal into a number of channels reduces in consequence the signal strength and the covered distance. To compensate this, EPON (IEEE 802.3av) uses Forward Error Correction. It is therefore interesting for asymmetrical communication, e.g. for distributing video signals.

This technology developed for the last mile and residential area has little importance in WANs.

#### 7.4.6.9 Fiber reliability and supervision

Fibers present the highest reliability of all communication media.

The weak points are the transmitters.

Example: Hydro-Québec specifies for the OPGW a failure rate of 0,36 interruptions per year over 2 500 km.

Nevertheless, constant supervision of the fibers is necessary and tools exist for it. A general rule is to try to cut the communication in the opposite direction if an optical channel ceases to operate, to attract the attention of the sender.

#### 7.4.6.10 Fiber advantages and disadvantages

Table 33 summarizes the optical fiber characteristics.

**Table 33 – Optical fibers: advantages and disadvantages**

Advantages	Disadvantages
Excellent BER / km	Disaster susceptible if carried on HV towers
Very high bandwidth	Reliability of transmitters, especially laser diodes
Physical separation of traffic in different fibers and within a fiber	Difficult to repair (e.g. OPGW), risk of long outage time
Electrical isolation between terminals, wide immunity against EMI	Splicing boxes are exposed
Earthing cable contains numerous fibers	

Therefore, the data transmission capacity of a high voltage line is very high, much in excess of the needs of a Utility Company, which often just keep one or two fibers from the bundle and leases the rest. In some cases, utilities outsource the whole fiber communication to a telecom company with a SLA concerning the fibers indispensable for operation.

#### 7.4.7 Layer 1 redundancy

To keep availability high upon failure or disaster, medium redundancy is applied, e.g. parallel fibers in optical networks.

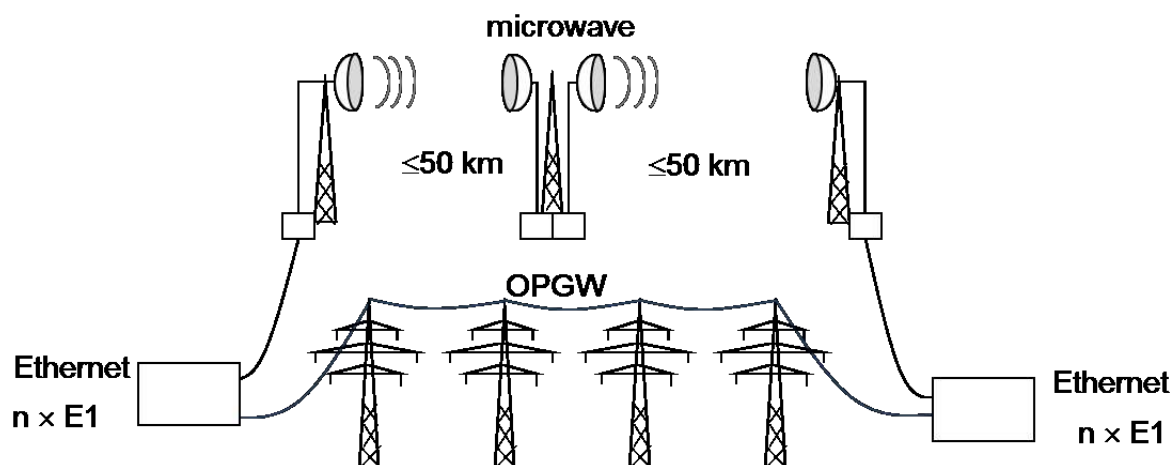
Redundancy itself is not sufficient – engineering and deployment must ensure the independence of the failure modes, for instance:

- independent power supplies;
- media with different principles (PLC – satellite);
- independent physical layout (route diversity, different ducts, different transmission tower, different routers);
- radio frequency separation and/or polarizations in microwave radio links;
- means to avoid simultaneous exposure to threat (unpowered backup, attacks).

Example: Radio communication on neighbor bands can be jammed by a wideband perturbation, but using frequency bands far apart (e.g. 2,4 GHz and 5,4 GHz) has been reported as being largely fail-independent against natural or industrial disturbances, but not against intentional jamming.

Without supervision, redundancy is useless. Therefore, non-active links need to be energized and exercised regularly. Better than occasional checking of redundancy is a parallel operation of redundant medium, where energy consumption and service restriction allow it.

The selection of the redundant medium is usually done by the Layer 2 or the Layer 3. Figure 42 shows an example of diverse redundancy through microwave towers separated from the OPGW transmission.



IEC

**Figure 42 – Optical link with microwave back-up**

#### **7.4.8 Use case: Diverse redundancy against extreme contingencies (Hydro-Quebec)**

The following example shows the benefits of redundancy in the communication system of a high-voltage grid. The telecommunications network, essential to maintain the appropriated grid operations, provides one of the two circuits composing the teleprotection and SPS (SIPS) systems.

Figure 43 shows one of two high voltage transmission lines collapsed under an ice storm. Power could be maintained thanks to fail-independence of the redundancy.

Communication path diversity was not deployed over the same corridor because the utility specified the minimum distance separating the two paths. Indeed, each utility defines its required diameter to sufficiently clear each path from each other and preserve the redundancy, for example, 50 km.

Nevertheless, medium diversity should be applied when feasible (OPGW and buried, OPGW and microwave, etc.).





Source: Hydro-Québec, Canada

IEC

**Figure 43 – Picture of partially destroyed 735 kV line**

#### **7.4.9 Layer 1 security**

Layer 1 security mostly relates to physical security attacks such as physical cut-off of communication cables including optical fibers or jamming.

Although power transmission lines are in general inaccessible, communication systems installed along power transmission lines such as OPGW or microwave are not well defended from physical attacks.

Tapping into an optical fiber at a splicing box is possible with sophisticated equipment and disrupting the communication quite easy. Radio communications can be easily jammed. Communication can be spied upon, e.g. by receivers in the line-of-sight of microwave towers or spoofed by stronger transmitters. For instance, GPS signals can easily be jammed or spoofed.

Encryption or authentication at the encoding level can defend Layer 1 communications against spoofing or eavesdropping, but not against denial of service.

Where Layer 1 security attacks are expected, medium redundancy (7.4.7) may be a practical solution.

#### **7.5 Layer 1,5 (physical) multiplexing**

The same physical medium can be subdivided into virtual circuits by several techniques:



- Time division multiplexing (TDM), in which each channel receives a fixed time slot in the same channel (Synchronous time division) or a variable time slot (asynchronous time division) transmission). The fixed time slot TDM is the usual multiplexing method for telephony and LANs (7.6.1.2).
- Frequency division multiplexing (FDM), in which each channel is modulated over a different frequency, with sufficient separation to avoid overlaps. FDM is what is taking place in the radio broadcast, but it is also used to subdivide microwave links. FDM over coaxial cables or microwave links was the technique of choice for the telephony network for decades, before the more efficient TDM replaced it. Radio and microwave transmission technique still use it (7.4.5).
- Wavelength division multiplexing (WDM), in which different light wavelengths are used to send signals in parallel over the same optical fiber. For instance, using CWDW, up to 16 channels can share the same fiber (see 7.4.6.6).

As long as each channel is firmly allocated, one can consider a multiplexed physical medium as a set of dedicated channels, keeping in mind that the medium is a common failure cause.

## **7.6 Layer 2 (link) technologies**

### **7.6.1 Telephony technologies**

#### **7.6.1.1 Analog telephony and DSL**

Legacy teleprotection systems operate over dedicated analog telephone lines that provide excellent real-time properties, but a limited bandwidth. They are still in use today and the challenge of digital communications is to mimic the real-time and confidentiality of a telephone wire while providing the bandwidth of digital transmissions, thus achieving a “pseudo wire” behavior.

The old modem communication over analog lines disappeared, except in the form of ADSL or VDSL as a point-to-point connection for the last mile. However, a number of legacy protection devices and RTUs still use it.

#### **7.6.1.2 Digital telephony**

The PCM, ATM and Frame Relay technologies are obsolete and this document does not cover them.

Digital telephony came with the PCM system, which samples the voice at 8 kHz with an 8-bit analog-to-digital converter after proper shaping. The voice channel DS0 of  $8 \times 8 = 64$  kbit/s is the base of all telephony-based communication, the transmission frequency of a given channel is always 8 kHz, regardless of the bit rate.

A hierarchy of aggregations allows integrating a large number of voice channels [ITU-T G.703].

A T1 channel agglomerates 24 time slots for voice channels, thus offering  $24 \times 64 + 8 = 1\,544$  kbit/s = 1,544 Mbit/s of raw bandwidth. The payload of  $24 \times$  DS0 is called DS1 (ANSI T1.403-1999).

The E1 frame (see Figure 44) carries 32 DS0 channels, each with 64 kbit/s, at 2,048 Mbit/s [ITU-T G.703].

The E2 frame carries 132 channels, each having 64 kbit/s, at 8,448 Mbit/s.

The repetition rate of the frames is always 8 kHz. Some of the frames serve for synchronization, error detection, signaling and management.

The E3 channel (ITU-T G.751] used in Europe and Japan agglomerates 192 channels (plus overhead), operating at a raw data rate of 34,368 Mbit/s.

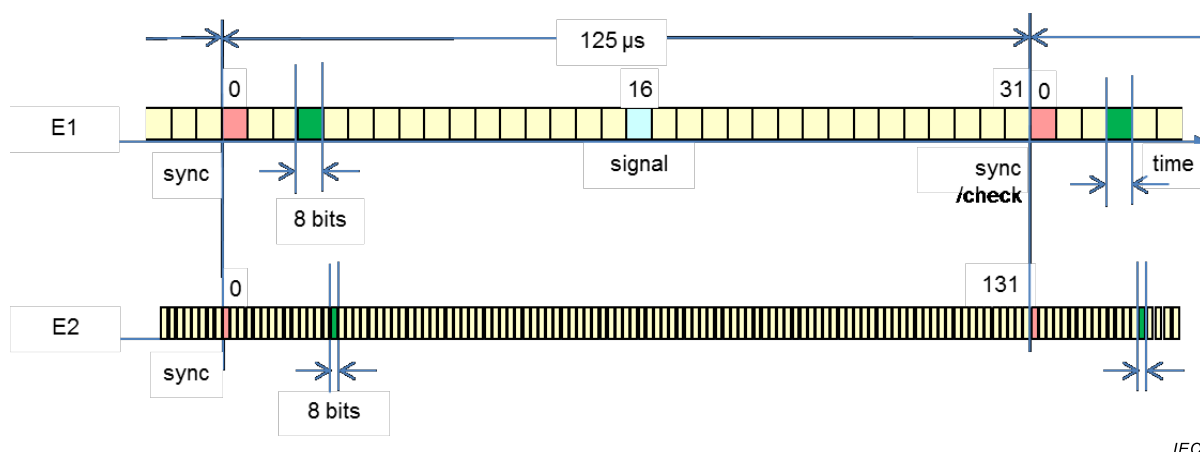


Figure 44 – E1 and E2 channel

### 7.6.1.3 PDH

The plesiochronous digital hierarchy (ITU-T G.702] is an obsolete telephony technology, but a large number of legacy devices still use it and its interfaces subsist for backward compatibility. PDH provides real-time behavior through TDM based on basic DS0 circuits that offer each 8 bits at 8 kHz (64 kbit/s), originally intended for voice.

Figure 45 and Figure 46 illustrate the basic multiplexing structure of PDH.

ITU-T G.703 specifies the physical characteristics of the copper connections from 64 kbit/s to 155,520 Mbit/s used to connect the end devices to the network.

Since its principles are identical to SDH/SONET (except for its synchronization), PDH will not be further explained.

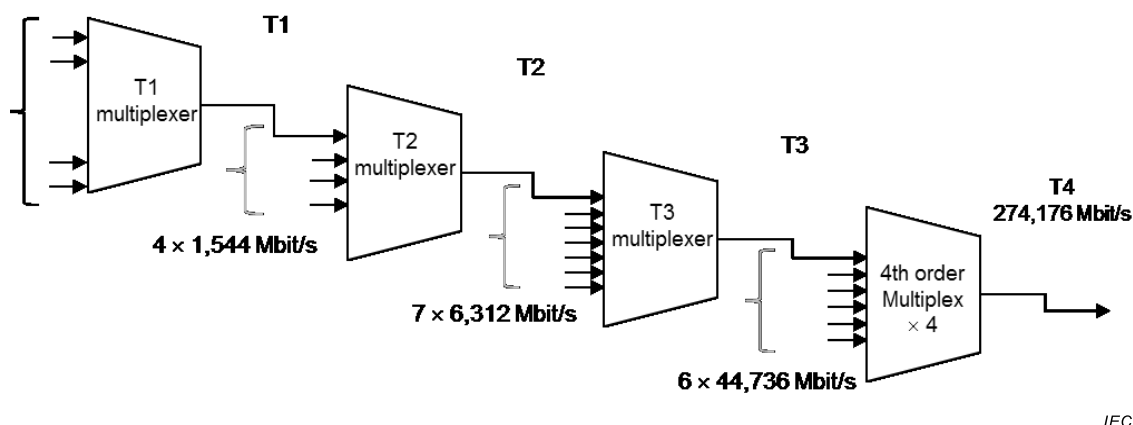
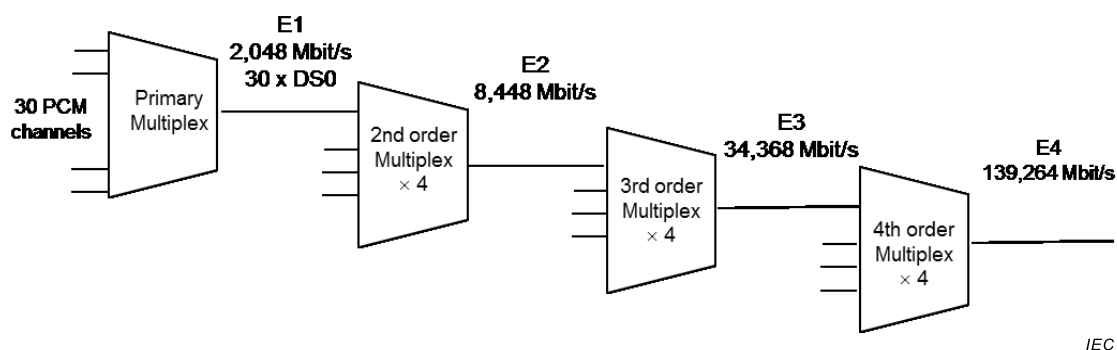


Figure 45 – Digital Transmission Hierarchy (T – Standards)



**Figure 46 – Digital Transmission Hierarchy (E-standard)**

#### 7.6.1.4 Quality of service

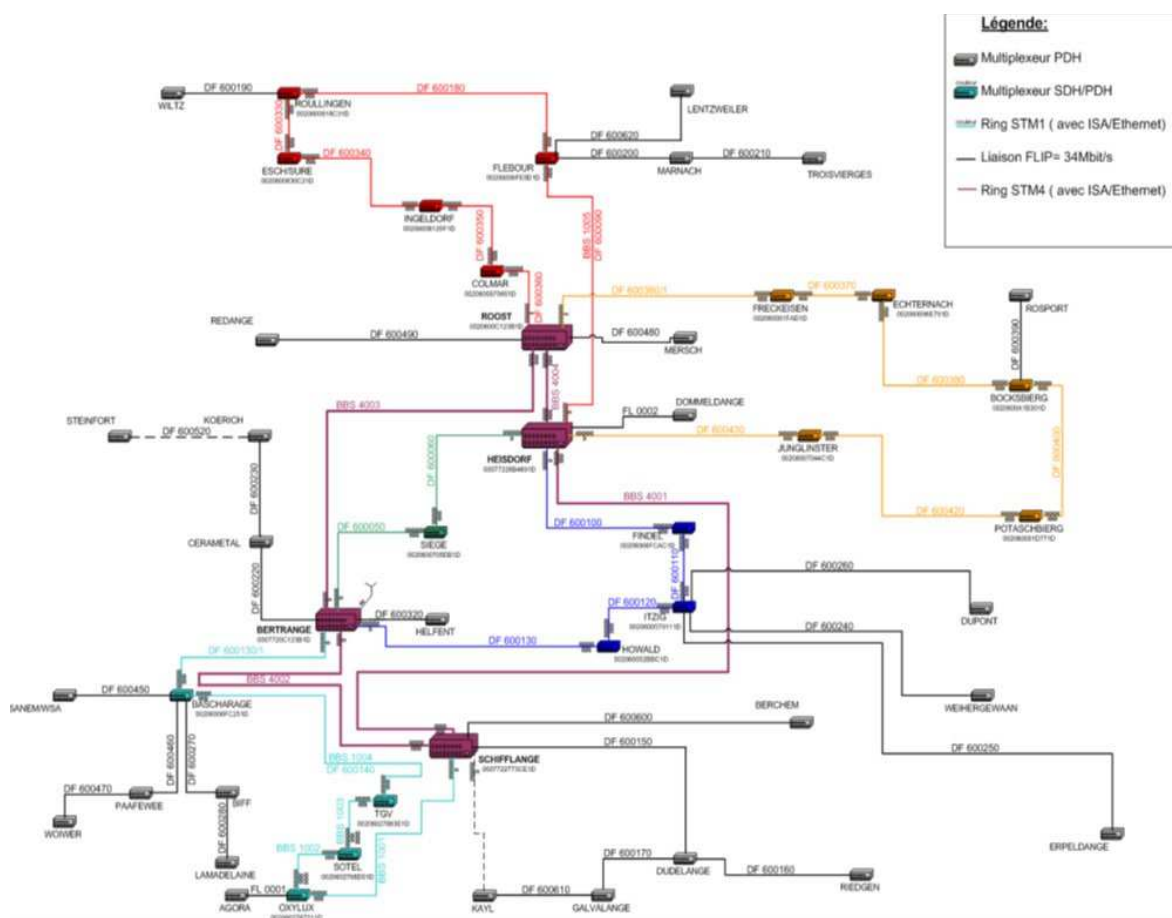
PDH uses TDM for medium access, which guarantees that once a virtual circuit has been allocated, it will remain in place with a deterministic maximum latency.

For a DS0 64 kbit/s communication channel, ITU-T G.823 provides limits of jitter at the transmission output and the receiver input of PDH networks based on the 2,048 Mbit/s hierarchy.

### 7.6.2 SDH/SONET

#### 7.6.2.1 Use Case for an SDH network

Figure 47 shows an SDH network, consisting of several interconnected sub-networks.



Source: CREOS, Belgium

IEC

Figure 47 – Example of an SDH network for utilities

### 7.6.2.2 SDH/SONET overview

SONET (North America) and SDH (rest of the world) are standardized (transport) protocols that transfer multiple digital streams over electrical connections (short links), optical fiber (very long distances at high data rates possible) or microwave radio (for difficult topological environment, low to medium bandwidth).

SDH and SONET are essentially the same; they were originally designed to transport circuit switched communications (telephony), supporting real-time, uncompressed, circuit-switched voice encoded in PCM. SDH/SONET provides deterministic channels for different types of services. Today these protocols transport the various utility specific legacy and TDM signals, as well as Ethernet with Next-Generation SDH/SONET equipment (see ITU-T G.707).

Figure 48 shows the SONET digital transmission hierarchy (ITU-T G.803). Figure 49 shows the SDH hierarchy. Synchronous and non-synchronous line rates and the relationships between each appear in Table 34.

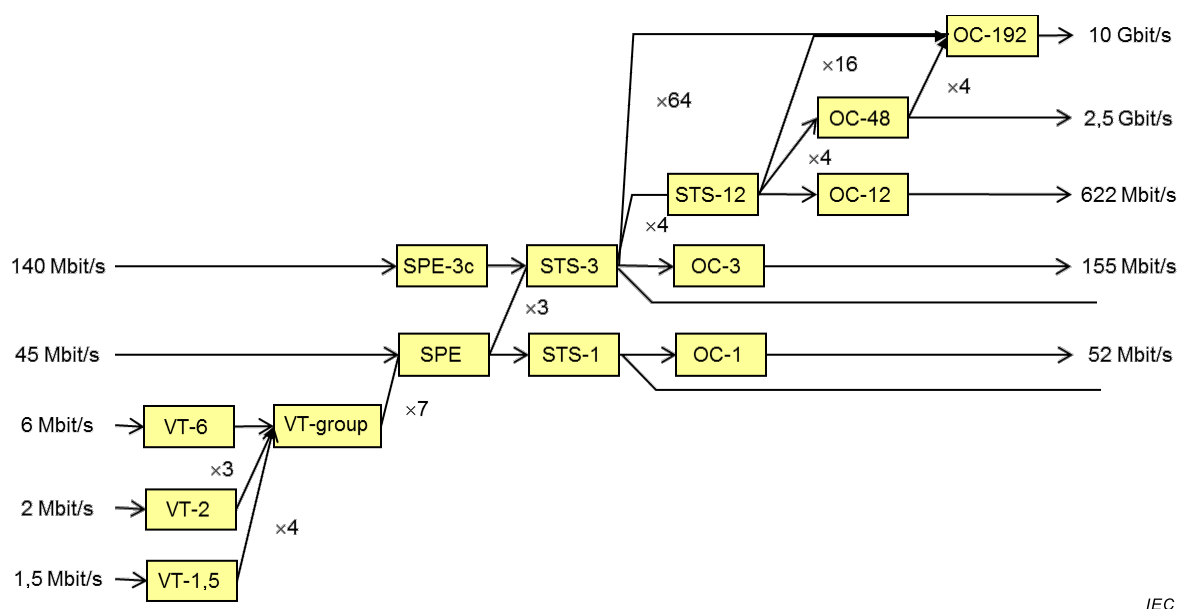


Figure 48 – SONET multiplexing hierarchy

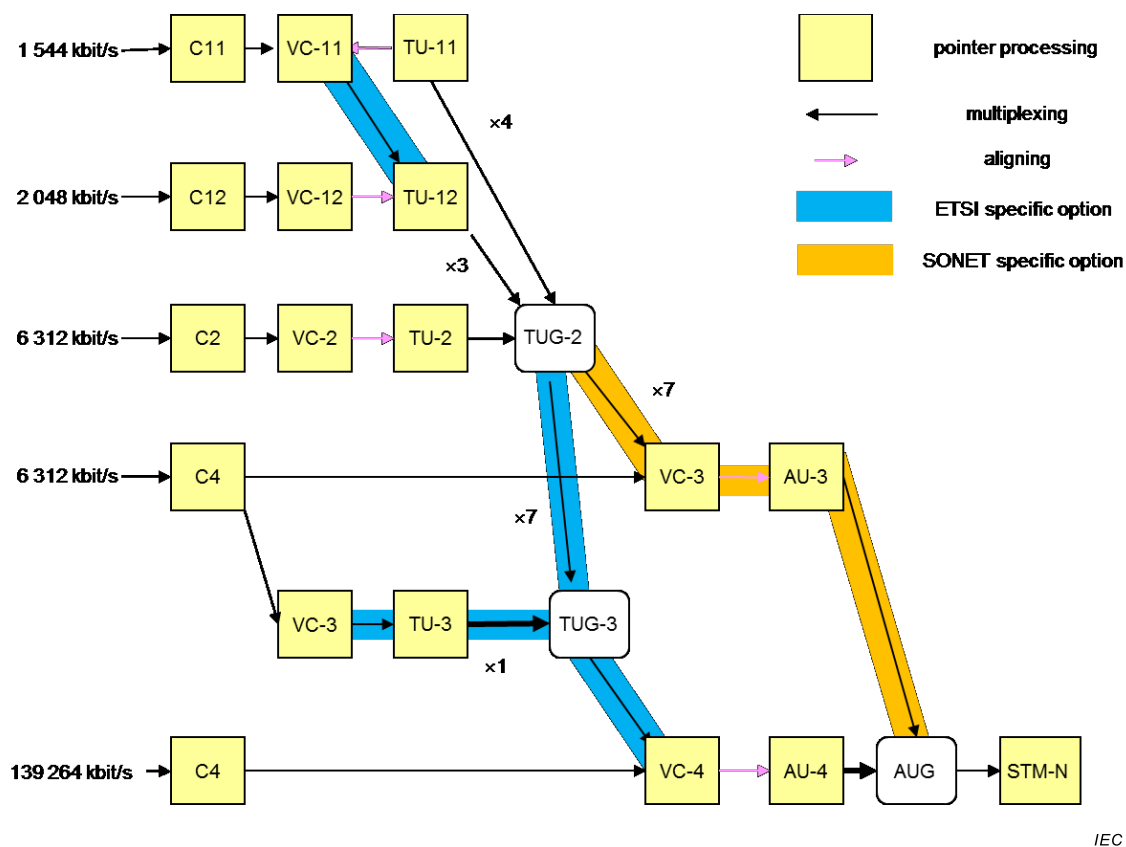


Figure 49 – SDH multiplexing hierarchy

**Table 34 – SONET and SDH hierarchies**

Optical medium	Electrical medium	SDH Signal	Bit rate Mbit/s	Payload rate (Mbit/s)	Overhead (Mbit/s)	Aggregation capacity	SDH capacity
	T-1		1,544			24 × DS0 at 64 kbit/s	
	E-1		2,048			32 × DS0 at 64 kbit/s	
	E-3		34,368			–	16 × E1
	T-3		43,368			28 × T-1	16 × E1
OC-1	STS-1	STM-0	51,840	50,112	1,728	28 DS1 = 1 DS3	21 E1s
OC-3	STS-3	STM-1	155,520	150,336	5,184	84 DS1 = 1 DS3 100 × T-1 63 × T-1	63 E1s or 1 E4
OC-12	STS-12	STM-4	622,080	601,344	20,736	336 DS1 = 1 DS3 4 × OC-3 4 × STM-1	252 E1s or 4 E4s
OC-48	STS-48	STM-16	2 488,320	2 405,376	82,944	1344 DS1 = 1 DS3 4 × OC-12 4 × STM-4	1 008 E1 or 16 E4s
OC-192	STS-192	STM-64	9 953,280	9 621,504	331,776	5376 DS1 = 1 DS3 4 × OC-48 4 × STM-16	4 032 E1s or 64 E4s
OC-768	STS-768	STM-256	39 813,12	38 486,016	1 327,104	28 DS1 = 1 DS3 4 × OC-192 4 × STM-64	16 128 E1s or 256 E4

### 7.6.2.3 SDH/SONET synchronization

SONET and SDH differ from PDH by the use of global synchronization (atomic clocks) across the entire network. ITU-T G.810 contains the corresponding definitions. This synchronization allows the networks to operate synchronously (ITU-T G.811), reducing greatly the amount of buffering required between elements in the network.

It also allows to directly access individual containers (e.g. VC-12 / VT3) inside a higher layer payload (e.g. STM-16 / OC-48), as opposed to PDH where complete demultiplexing had to be performed.

The average frequency of all clocks in the system will be (nearly) the same. Every clock traces back to a highly stable and accurate primary reference clock (ITU-T G.811) (7.15.6). The synchronization network relies on a master-slave relationship with clocks of the higher-level nodes feeding timing signals to clocks of the lower-level nodes (ITU-T G.812, ITU-T G.813). The sources available to a network element are:

- Local external timing (atomic clock or satellite-derived clock).
- Line-derived timing (S1 sync-status).
- Messaging.
- Holdover (own internal oscillator).

#### 7.6.2.4 SDH/SONET Quality of service

Like PDH, SDH/SONET uses TDM for medium access, which guarantees that once allocated, a virtual circuit will offer a deterministic maximum latency, symmetrical in both directions.

For a 64 kbit/s DS0 communication channel, ITU-T G.823 provides limits of jitter at the transmission output and the receiver input based on the 2,048 Mbit/s E1.

#### 7.6.2.5 SDH/SONET network topologies

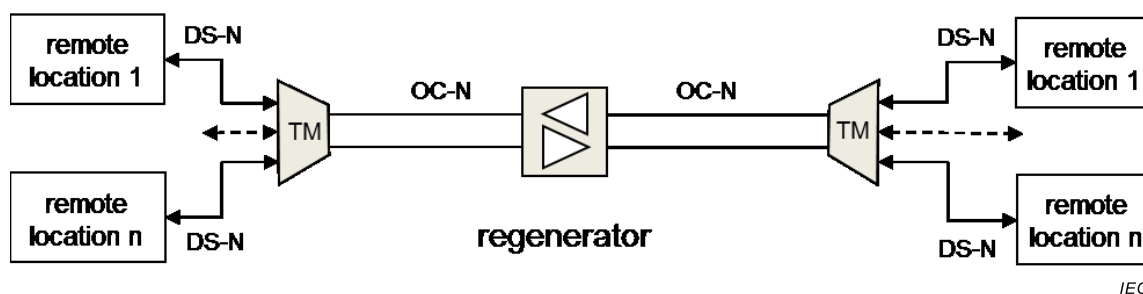
##### 7.6.2.5.1 Point-to-point topology

The main SDH/SONET network elements include:

- Terminal Multiplexer (TM), which multiplexes several low-speed channels on a high-speed path;
- Add-Drop-Multiplexer (ADM), which adds and drops tributaries at intermediate points along a path;
- Digital Cross Connect (DXC), which interconnects several directions.

Typical SDH/SONET equipment can cover all of these types and offers flexibility in topology.

Point-to-point topologies consist of connecting two ADMs or TMs back to back (Figure 50).

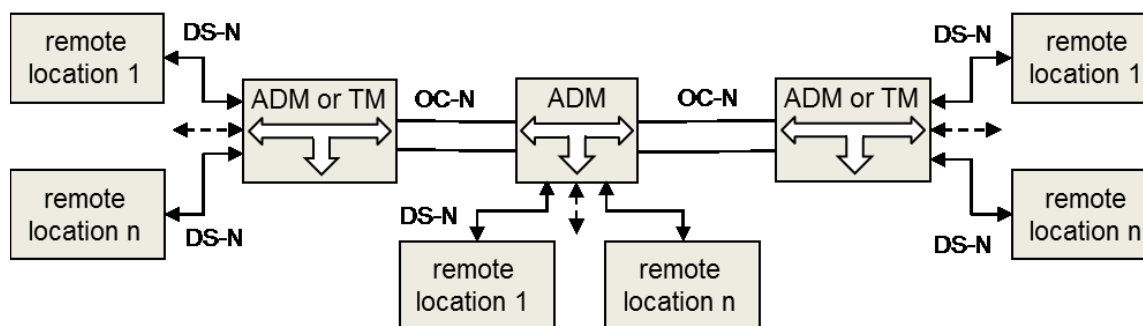


IEC

Figure 50 – SDH/SONET with point-to-point topology

##### 7.6.2.5.2 Linear topology

A linear topology (Figure 51) uses ADMs and TMs placed along a SDH/SONET path. Service providers use this topology for medium and long haul linear SDH/SONET architectures.



IEC

Figure 51 – SDH/SONET with linear topology

#### **7.6.2.5.3 Ring topology**

By far the most popular topology for SDH/SONET is the ring. SDH/SONET rings provide 50 ms and lower recovery time as well as robust recovery mechanisms. The main advantage of the ring topology is its survivability and fast restoration or healing time of specific ring redundancy schemes.

#### **7.6.2.5.4 Meshed topology**

Given that the fiber or microwave layout dictate the topology in utility networks, the creation of single ring networks is not always possible. SDH/SONET technologies offer the flexibility in the circuit configuration (cross-connections) to build networks in a meshed topology. Meshed topologies typically offer the possibility to reach a station through several paths thus providing redundancy.

#### **7.6.2.6 SDH/SONET redundancy**

##### **7.6.2.6.1 Redundancy mechanisms**

SDH/SONET can provide in case of failure switchover times below 50 ms. Depending on the used mechanism, the switching affects the complete payload of a section or only individual channels. Unidirectional and bidirectional mechanisms are available.

NOTE ITU calls redundancy “protection”. This document reserves the word “protection” for a protecting mechanism, while it calls a functional redundancy mechanism “redundancy”, or where appropriate, “backup”.

##### **7.6.2.6.2 Point-to-Point redundancy**

Multiplex Section Protection (MSP 1+1) applies to a point-to-point link. Two fiber pairs are used, one providing the working link, the other one providing the backup link. In case of a link or equipment failure, the whole payload (e.g. VC-4) is switched, not individual channels.

MSP 1+1 can provide symmetric switchover of RX and TX path within 50 ms.

##### **7.6.2.6.3 Ring Redundancy**

Line switched rings use the SDH / SONET line level indications to supervise the health state. The transmission is said bidirectional because both directions of transmission use the same set of nodes.

Redundancy against cuts and node failures is provided by reserving redundant bandwidth on the ring. In case of link failure, the complete payload on the affected section is rerouted over “the long way” around the ring. Switchover times of 50 ms are achievable.

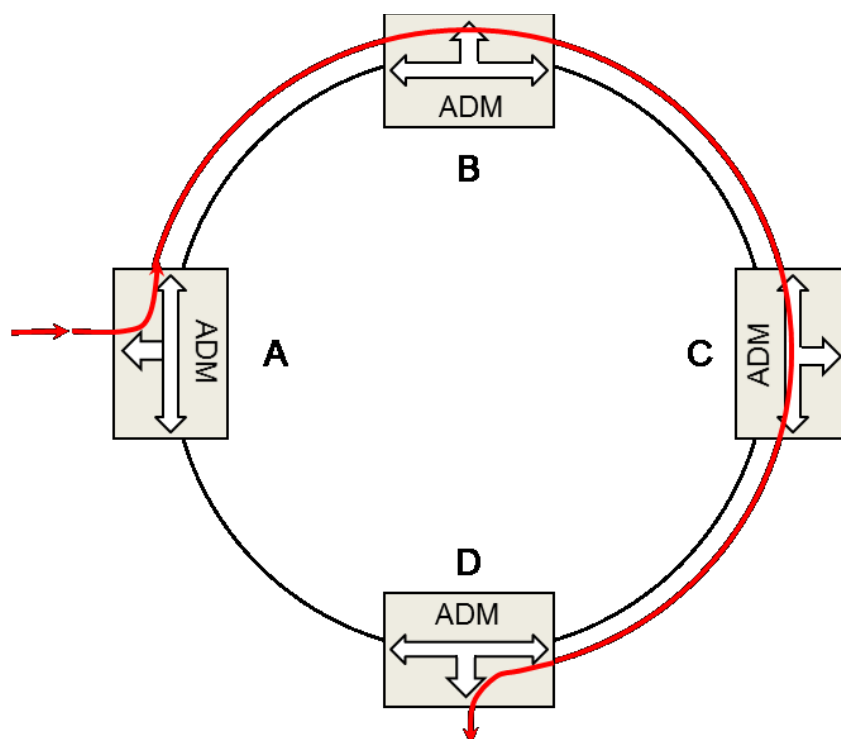
Multiplex Section Shared Protection Ring (MS-SPRing) in SDH, respectively Bidirectional Line Switched Ring (BLSR) in SONET, provide two redundancy mechanisms:

- 2-fiber: half of the capacity in the ring (e.g.  $2 \times \text{VC-4}$  on STM-4 /  $2 \times \text{STS-3}$  on OC-12) are used for working traffic, the other half is reserved for redundant traffic
- 4-fiber: 2 fibers are used for working traffic, another 2 fibers are reserved for redundant traffic (each fiber pair providing full capacity e.g.  $4 \times \text{VC-4}$  /  $4 \times \text{STS-3}$ )

During the ring switching time, tests verify the presence of any noise or signal. All the network elements present in the ring must be aware of the incoming switching before initiating recovery.

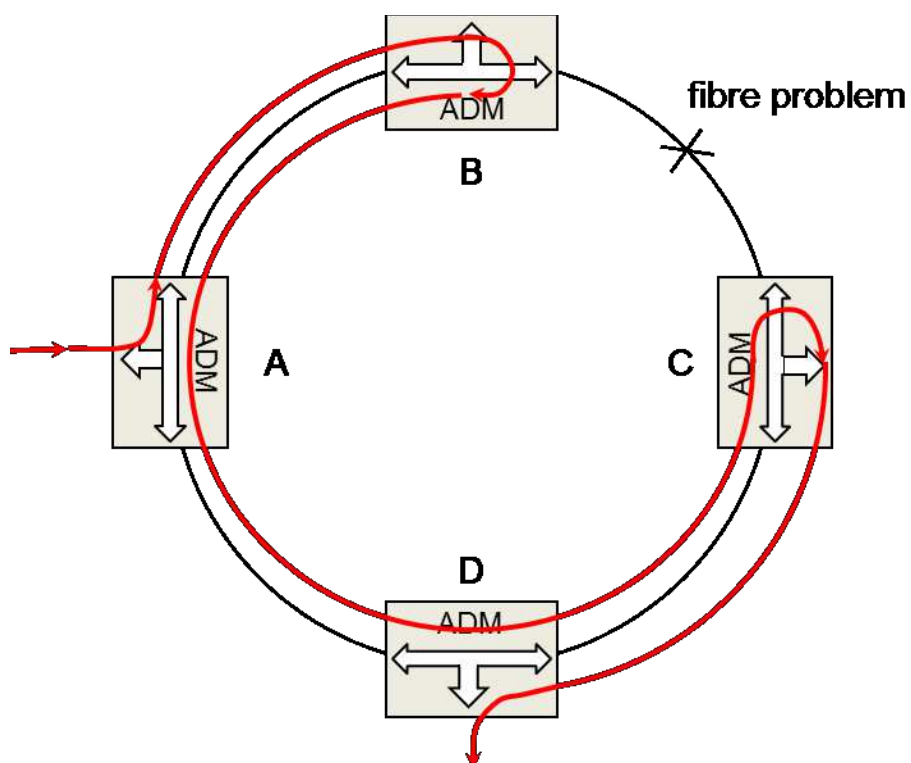
Because BLSR/BSHR does not send redundant copies of the traffic on both sides, the total bandwidth can be reused and be much more than the traffic between two nodes. Figure 52 show how BLSR/BSHR works under normal conditions and Figure 53 shows the same under failure conditions.





IEC

Figure 52 – BLSR/BSHR topology in normal conditions (from A to D)



IEC

Figure 53 – BLSR/BSHR topology in failure conditions

#### 7.6.2.6.4 End-to-end redundancy

SubNetwork Connection Protection (SNCP) in SDH, respectively Unidirectional Path Switched Ring (UPSR) in SONET provides end-to-end redundancy.

In SNCP/UPSR topology, the traffic between two nodes is provisioned to travel either clockwise or counter clockwise around a ring under normal conditions.

Two redundant (path-level) copies of traffic circulate in both directions around the ring. A selector at the receiving node determines which copy has the highest quality and uses it. Each node makes the decision to switch independently, without communicating with any of the other nodes. All the bandwidth is available on the entire ring.

Figure 54 shows how UPSR /USHR work in normal condition and Figure 55 shows the failure condition.

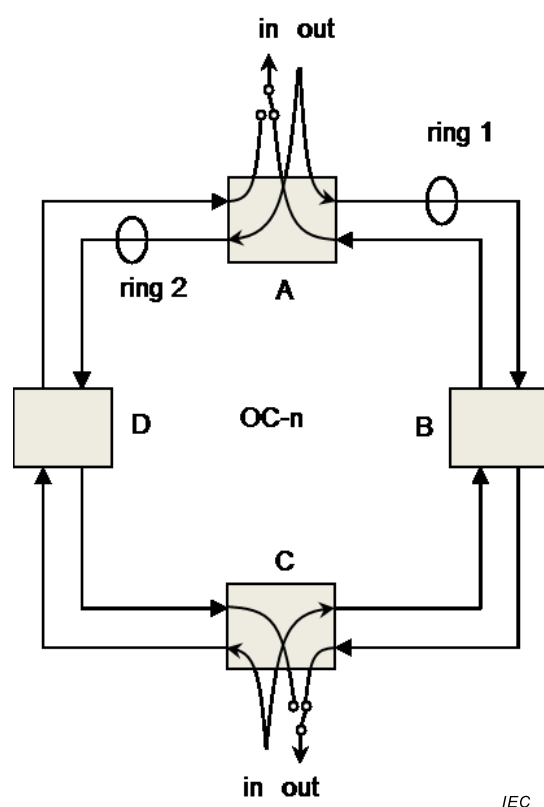
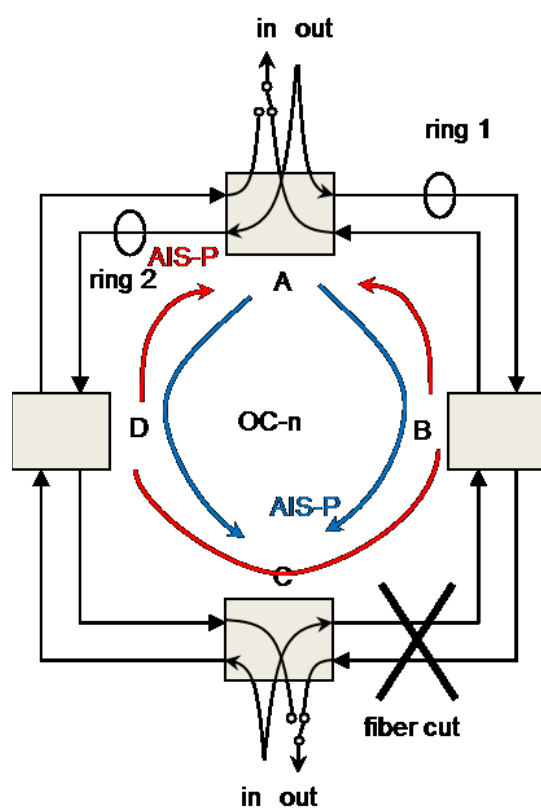


Figure 54 – UPSR/USHR topology in normal conditions



IEC

**Figure 55 – UPSR/USHR topology in failure conditions**

SNCP/UPSR is implemented for individual channels e.g. VC-12/VT2. Redundancy switching can be unidirectional or bidirectional and provides switch over times of 50 ms.

Path Protection / Trail Protection (SDH) implements the same mechanism as SNCP and provides the same performance. Compared to SNCP based on ring topology, path fault tolerance can also be implemented for end-to-end channels in meshed networks providing 50 ms switchover.

#### 7.6.2.6.5 SDH/SONET hardware redundancy

To increase reliability of network element, the APS 1+1 (workby) and 1:N (standby) are used on different cards, based on their strategic roles, typically: CPU modules, switching modules, power supplies.

Specifically for power supply units, the remaining units must be sufficient to distribute the total load of the network element, to maintain the services unaffected and the network element alive when a unit fails and until repair.

Some SDH/SONET multiplexers implement the concept of distributed power supply, which does not use dedicated power supply modules, but distributes the low voltage power supply to the different interface cards.

Since the power supply is a major source of unreliability, distributed power supplies avoid a single point of failure.

### **7.6.2.7 Next Generation SDH/SONET**

Next Generation SDH / SONET is a standardization effort to solve the earlier deficiencies of SDH/SONET payload mapping, in particular to raise the efficiency of packet transport and improve flexibility.

Next Generation SDH / SONET adds new features that allow to group channels for better efficiency (see 7.6.5).

### **7.6.2.8 SDH/SONET conformity with utility requirements**

#### **7.6.2.8.1 Latency**

The residence delay of an ADM or network element amounts to tens of microseconds per network element. The entry port to exit port latency is deterministic.

However, there is no guarantee for latency when opening a new connection.

The number of elements in series must be limited to meet the delays expressed in 5.3.

#### **7.6.2.8.2 Reliability**

The reliability depends on the underlying network and components, not on the protocols.

#### **7.6.2.8.3 BER**

SDH/SONET network element and network fulfil the criteria of 6.2.5.

#### **7.6.2.8.4 Asymmetrical delay for legacy differential teleprotection**

The requirement of 5.5 for a maximum asymmetry limits the topology.

The RX and TX circuits transporting differential teleprotection data must be co-routed and no unidirectional switching is allowed in case of failure.

The point-to-point and linear topologies can be used. SNCP/UPSR operates in unidirectional mode (as per standard) and the constant differential delay required for differential protection cannot be guaranteed during switchover. Some SDH multiplexers allow bidirectional switching for SNCP/path protected channels. In this case, the differential delay does not change much when switchover takes place.

Since MS-SPRing/BLSR switch all the VCs/VTs in the line, it is impossible to lock the switching of specific VTs like UPSR does.

### **7.6.2.9 SDH/SONET OAM**

All SDH/SONET network elements, in different topologies, should be managed from a centralized centre or from decentralized centres, based on the utility policies. Often these functionalities are offered on user-friendly graphical network management tools that simplify the operation and maintenance of SDH/SONET systems.

Network management traffic may in “in-band” or “out-of-band”:

- In-band: Octets D1-D3 or D4-D12 inside the SDH/SONET overhead carry the management information over the Data Communication Channel (DCC), without using any SDH/SONET payload.
- Out-of-band: A dedicated Data Communication Network (DCN) in parallel transports the SDH/SONET management information.

### 7.6.2.10 SDH Security

Due to its non-routable nature and clear traffic segregation in Virtual Containers, (also for Ethernet over SDH traffic), SDH/SONET is less susceptible to security attacks than other technologies. Protocols like LCAS (for EoSDH) provide security as well since one data stream can be split to 2 diverse paths through the network which makes it difficult to interfere.

### 7.6.2.11 SDH/SONET summary

Table 35 summarizes SDH/SONET.

**Table 35 – Summary of SDH/SONET**

Feature	Comment
Acceptance	Well known and understood in the utility world
Bandwidth efficiency	TDM has low overhead in raw packets TDM inefficient for packet switching due to resources reservation since TDM cannot be overbooked. NG SDH/SONET improves efficiency.
Routing	Circuit switching
Traffic engineering	Circuit switching
Configuration	Connection-oriented
Recovery	50 ms recovery delay
Determinism	TDM cannot be overbooked. Latency is deterministic once route is established
VPN	Various L2VPN
Application	Telecom in general, all applications

### 7.6.3 Optical Transport Network

OTN is an extension of SDH/SONET based on optical multiplexing (xDWDM). ITU-T G.878 and ITU-T G.709 describe the frame format and payload. OTN is intended for the high-end links up to 100 Gbit/s. Figure 56 shows the structure of an OTN interface.

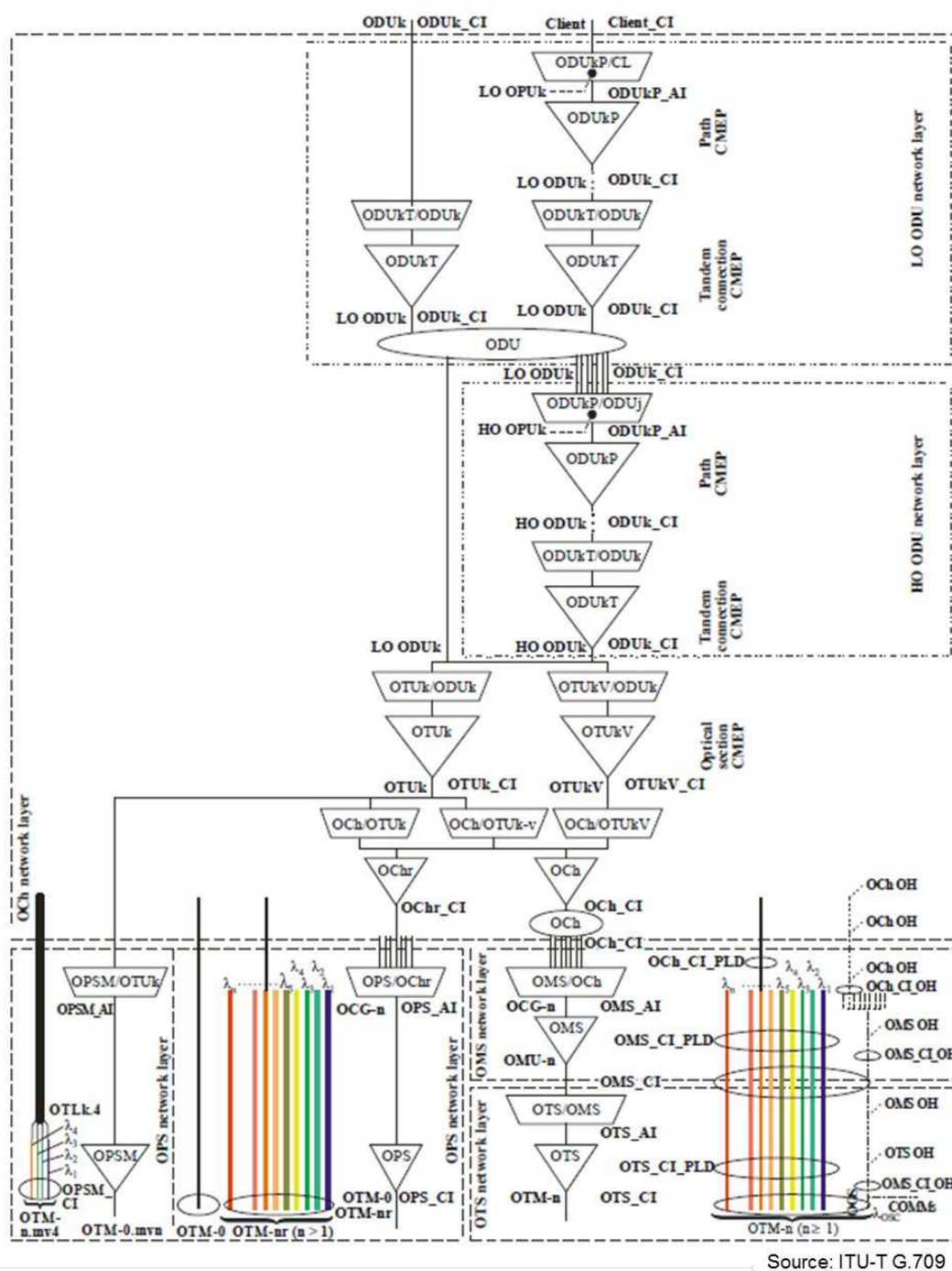


Figure 56 – Example of information flow relationship in OTN

OTN is becoming increasingly interesting although no deployment in utilities is known of.

## 7.6.4 Ethernet

### 7.6.4.1 Ethernet technology

Ethernet is originally a Local Area Network technology standardized as IEEE 802.3, which started on coaxial cables of 10 Mbit/s over distances of 500 m, with a diameter limited to 1 500 m and poor bandwidth efficiency due to the CSMA/CD medium access and half-duplex operation.

Ethernet evolved into “switched Ethernet”, using bi-directional, full-duplex switched links over optical fibers that overcame the former limitations. Optical fibers cover distances of several kilometers without repeaters, and hundreds of kilometers with repeaters. The total available bandwidth of an Ethernet network exceeds the bandwidth of a single link.

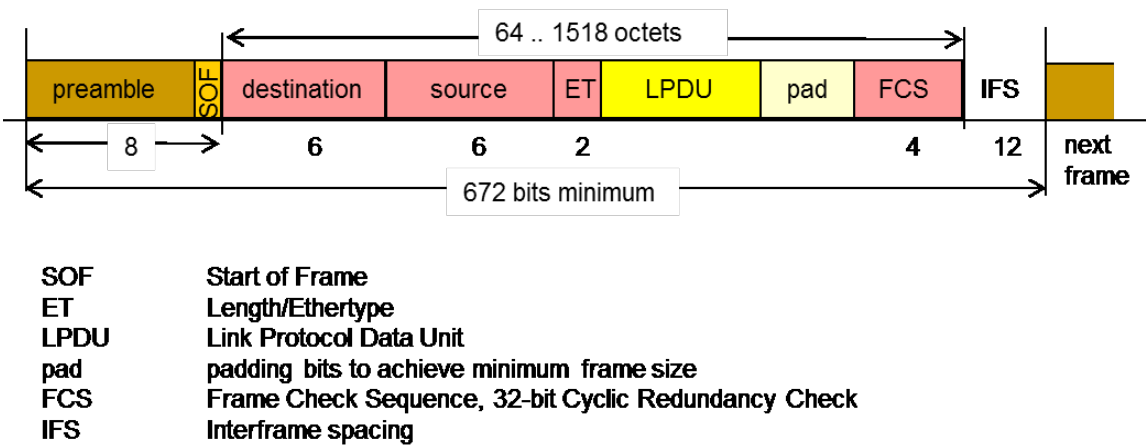
IEEE 802.3 specifies many physical layers; Table 36 shows the most important.

Table 36 – Ethernet physical layers

Standard	Rate (Mbit/s)	Medium	Properties
100Fx	100 Mbit/s	Multimode fiber single mode fiber	Most widely used in substations single mode little used
1000Fx	1 Gbit/s	Multimode fiber single mode fiber	Most widely used in wans
LX-4	10 Gbit/s	CDWM 4 × 3,125 Gbit/s	WAN technology
SyncE	diverse	Optical fibers	Offers frequency distribution, see 7.15.6

In many bridges, the medium can be simply changed by plugging-in another SFP-module.

All speeds share the same data frame format (see Figure 57), which is really what makes “Ethernet”. This frame format has become the common reference of WANs.



IEC

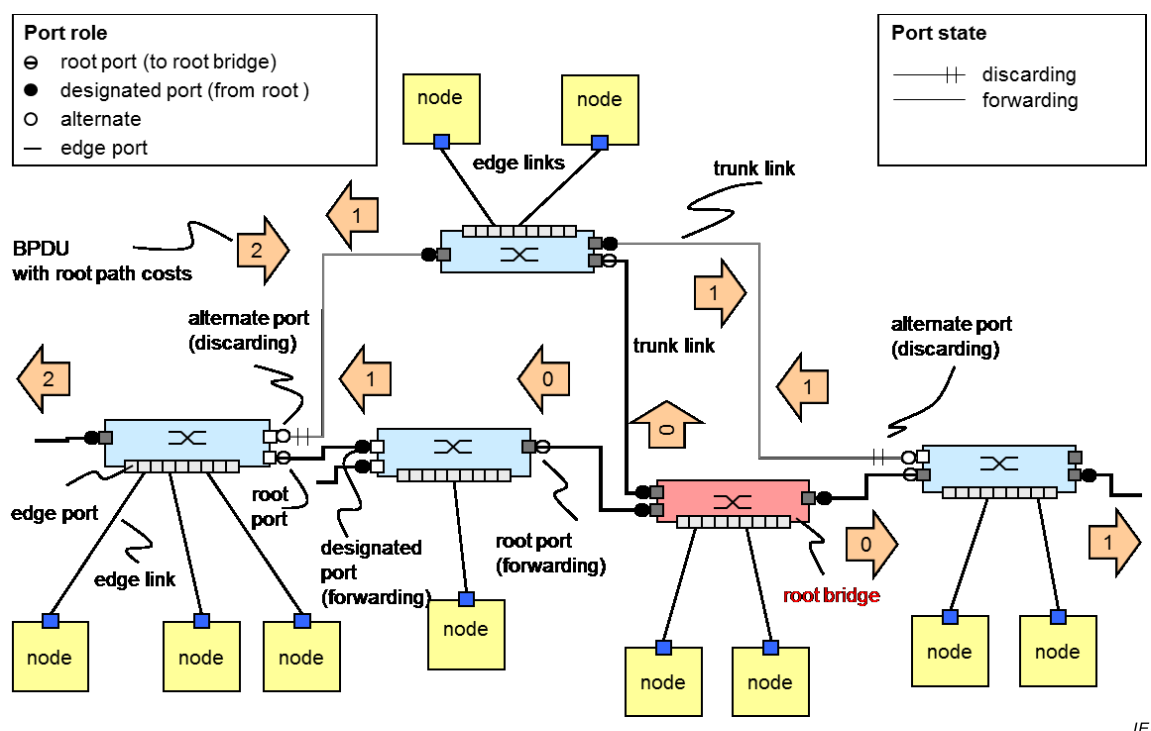
Figure 57 – IEEE 802.3 (Ethernet) frame format

Ethernet uses 48-bit MAC addresses for the source and the destination. The physical MAC address of an Ethernet controller is unique worldwide. The logical address used for communication may be the physical or a logical address.

NOTE IEEE decided that in the future, devices will be identified by a 64 bit world-wide address EUI-64, consisting of the 3 first octets of the physical address (Organization Unique Identifier) separated by the two octets “FFFE” for the least significant three octets (serial number).

7.6.4.2 Ethernet configuration

An Ethernet LAN consists of a number of nodes interconnected by bridges (though IEEE calls it “switched Ethernet”). To prevent loops when the network is meshed, the bridges execute the Rapid Spanning Tree Protocol (RSTP) [IEEE 802.1Q] to impose a logical tree structure (Figure 58).



**Figure 58 – IEEE 802.3 (Ethernet) topology with RSTP switches (IEC TR 61850-90-4)**

Other technologies such as HSR [IEC 62439-3] and ERPS [G.8032] also prevent loops in meshed Ethernet networks, especially in rings (Figure 63).

#### 7.6.4.3 Ethernet routing and control plane

Ethernet has no dedicated control plane. All traffic is by nature broadcast, the destination recognizes its traffic by the destination address.

Bridges can limit the traffic by sending the frames selectively to the ports where they discovered a specific destination, updating this information in their Filtering Database (FDB) by listening.

While this learning mechanism saves bandwidth and reduces latency, it is not effective during recovery since reconfiguration after failure of a switch requires falling back into broadcast mode again and flooding the network with traffic until the learning reduces the traffic.

#### 7.6.4.4 Ethernet path symmetry

Ethernet is a broadcast medium, constrained to a logical tree topology by RSTP. Once the tree is established, a call message takes the same path as the reply. The latency will however depend on the traffic and the queues in the bridges. During recovery, a path asymmetry may exist.

In the case of HSR (7.6.4.8.5), the path may become asymmetric, since a Doubly Attached Node with HSR (DANH) takes the first frame that comes. This is especially the case when the communicating entities are on opposite sides of the ring and the latency is about the same in both directions.



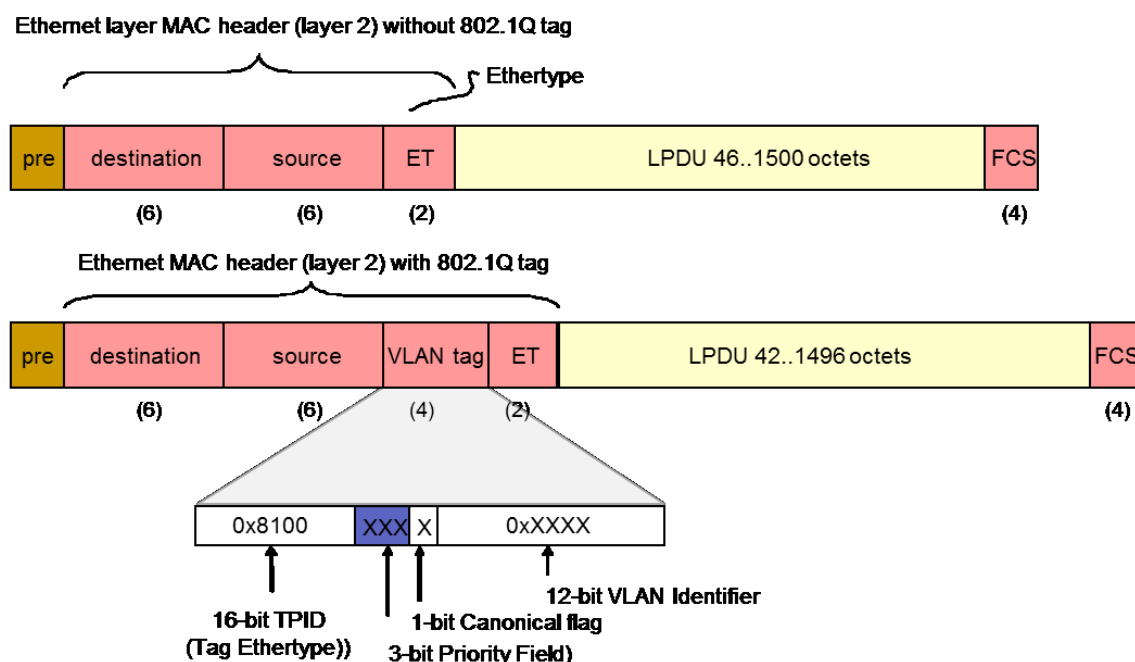
### 7.6.4.5 Ethernet multicast settings

Layer 2 networks provide broadcast as a basic functionality: a Layer 2 network is a broadcast domain. Multicast filtering in the bridges reduces the traffic by building multicast zones; see IEC TR 61850-90-4.

NOTE This is in contrast to Layer 3 networks where multicast requires subscription e.g. by IGMP.

### 7.6.4.6 Ethernet Virtual Local Area Network (VLAN)

IEEE 802.1Q specifies the concept of VLAN that allows multiplexing several distinct Ethernet streams over the same physical media. To this effect, an Ethernet frame receives an 802.1Q tag (Figure 59). Figure 59 shows only one 802.1Q tag, but several such tags may be stacked.



**Figure 59 – IEEE 802.1Q-tagged Ethernet frame format**

VLAN allows segregating address spaces and assigning each address space a priority. This allows the bridges to limit the broadcast domains. The configurator of the bridge ports is responsible for the separation of the address spaces. VLANs do not increase the available bandwidth over trunks.

A device with a given VLAN is only able to communicate with other devices of the same VLAN and cannot interfere with other VLANs. However, some LANs allow end devices to participate in several VLANs and therefore cannot ensure full separation of the address spaces, especially if the assignment of VLANs is automatic. SCADA nodes, for instance, need access to all VLANs.

### 7.6.4.7 Use of VLANs for remote addressing over the LAN

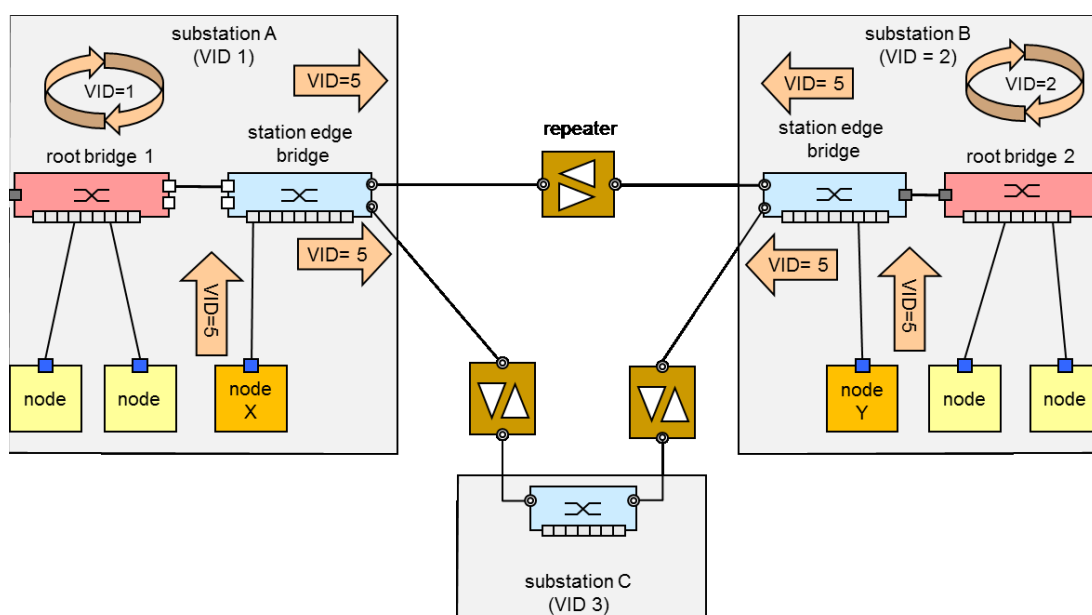
Substations can communicate directly over Layer 2, either using single mode fiber or using a WDM channel. The arrangement of Figure 60 is well suited when optical fibers connect directly the substations (e.g. OPGW). The latency depends on the traffic in the station edge bridges, while the link delay is well controlled with 5 µs/km plus repeater delay (if repeaters are present). GOOSE messages can be exchanged directly.

In this case, VLANs allow separating the traffic coming from one substation from the locally generated VLAN traffic (Figure 60).

Such a direct connection implies that the engineering on all sides (there can be more than two substations, e.g. for teleprotection in HV branches) agree on the VLANs.

In Figure 60, the traffic between substations and the traffic within a substation have different VLAN tags. Node X sends data to substation B and C (tagged with VID=5), its frames are distributed in substation B and C to all devices that need them. By contrast, the traffic tagged with VID=1 remains within substation A. This avoids flooding a substation with the traffic of other substations. Multiple separate VLANs can be used between substations for different applications, traffic priorities or scopes.

The connection between substations can present loops as shown in Figure 60. RSTP should execute per substation, since it would be awkward to have the root bridge of one substation located in another substation. It is therefore necessary to apply another loop removal protocol such as the Multiple Rapid Spanning Tree Protocol (MSTP) [IEEE 802.1Q-2005]. MSTP is however not a frequently used protocol. HSR can be used instead. This shows a limitation of Ethernet when applied to WAN technology.



IEC

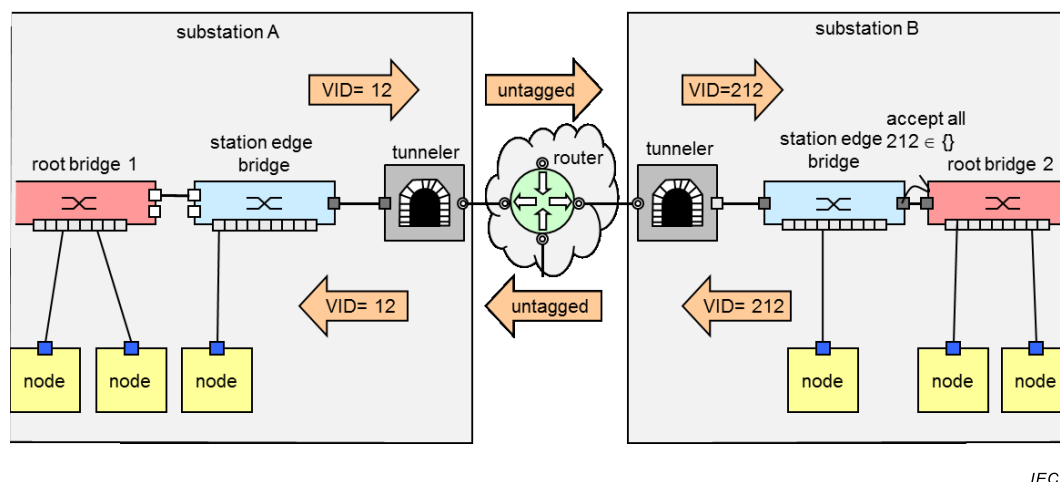
**Figure 60 – Direct Ethernet with VLAN in substation-to-substation transmission**

Another solution is to carry Ethernet traffic as an overlay (tunnel) over another network (IP, SDH/SONET, MPLS, PBB, etc.). This is what IEC TR 61850-90-1 recommends for tunneling GOOSE and SMV and IEC TR 61850-90-5 recommends for tunneling synchrophasor values over IP.

If the tunnel type does not preserve the Layer 2 header, the corresponding VLAN identifiers may differ in both substations, giving the network engineer more freedom (Figure 61). The situation is similar when the Layer 2 packets are tunneled over a link that does not preserve the VLAN tags.

In the example of Figure 61, substation A sends the GOOSE messages intended for substation B with VID=12; the tunneler removes the tag; the link between the substations forwards the untagged frames; the tunneler at substation B retags the frames with VID=212.

Conversely, substation B sends the GOOSE messages for substation A tagged as 212, the tunneler of substation A retags them to VID 12.



**Figure 61 – Substation-to-substation Layer 2 transmission tunneled over IP**

The traffic to be carried over the tunnel (in either direction) should have its own identifier. The tags can be mapped into MPLS labels (7.6.9) or IP addresses (7.7.1.2.4), effectively forming a tunnel for GOOSE transmission (see 7.11.2).

#### **7.6.4.8 Ethernet redundancy**

##### **7.6.4.8.1 Redundancy methods**

Link-layer redundancy applies exclusively within a Layer 2 multicast domain. IEC 61850-8-1 and IEC 61850-9-2 specify as redundancy methods:

##### **7.6.4.8.2 RSTP redundancy**

RSTP (7.6.4.2) is primarily a LAN auto-configuration protocol (removal of loops) and secondarily a redundancy protocol. IEC 62439-1:2010, Clause 8 provides methods to calculate the recovery delay depending on the topology. RSTP recovery delays are in the order of 5 ms per hop, but in case of failure of the root node, recovery can take up to 20 seconds.

##### **7.6.4.8.3 ERPS redundancy**

Ethernet Ring Protection Switching (ERPS) is a configuration and recovery protocol specified in ITU-T G.8032. It allows to couple rings and offers a recovery delay of less than 50 ms. ERPS is used in Carrier Ethernet applications. The recovery scheme is similar to 7.6.2.6.3, with data circulating in one ring direction and control frames in the opposite direction.

##### **7.6.4.8.4 PRP**

PRP (IEC 62439-3:—, Clause 4) allows operating two LANs in parallel with zero switchover delay, but requires a full duplication of the LAN. This technique is applicable within substations and outside substations (Figure 62).

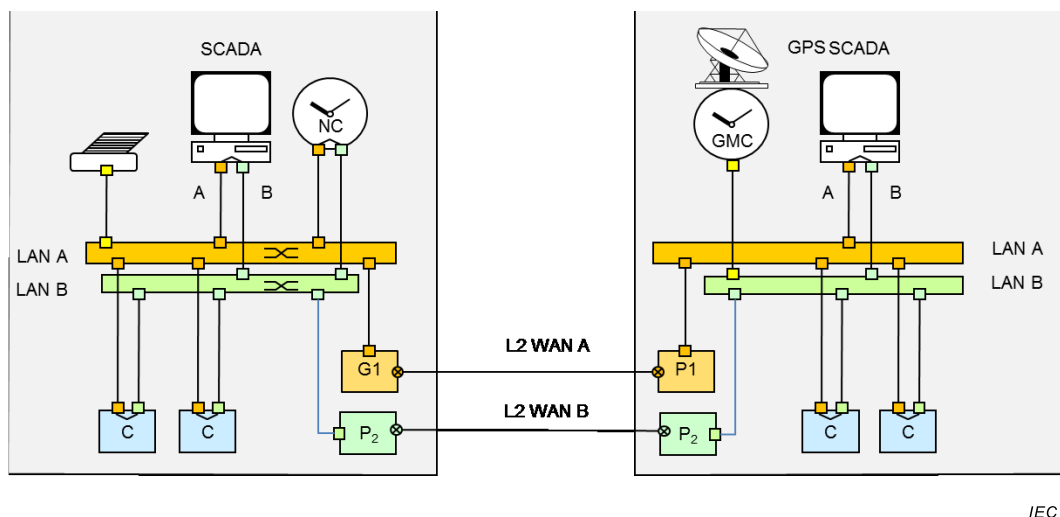


Figure 62 – PRP structure (within and outside a substation)

#### 7.6.4.8.5 HSR

HSR (IEC 62439-3:—, Clause 5) uses the same principle as PRP to offer zero recovery delay in a ring or in a ring of rings network. At the same time, it prevents loop building. This technique is applicable in the Layer 2 of WANs (Figure 63).

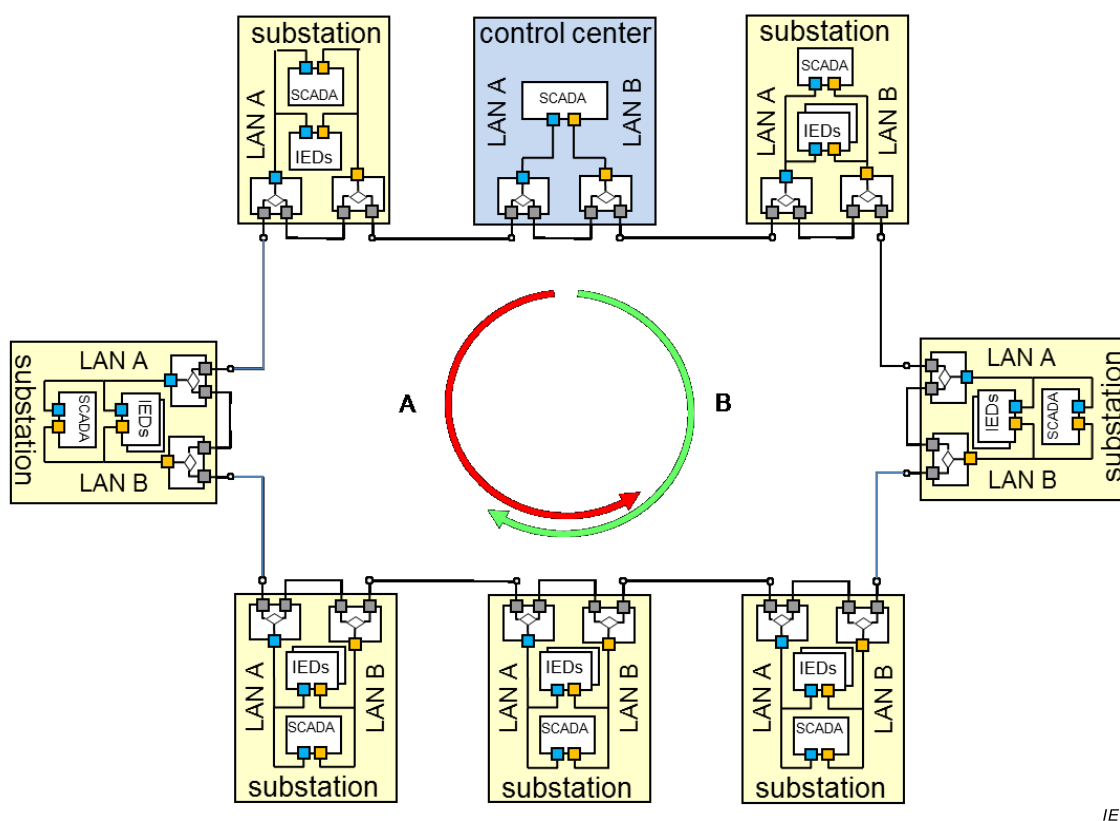


Figure 63 – HSR ring connecting substations and control centre

In HSR, the duplicate discard algorithm considers propagation delays, which amount to  $5 \mu\text{s}/\text{km}$  (without repeaters), processing delays (some  $5 \mu\text{s}/\text{node}$ ) and transmission delays (at  $100 \text{ Mbit/s}$ , the minimum frame takes  $6 \mu\text{s}$  to transmit, which corresponds to a propagation

distance of 1,2 km). IEC 62439-3 gives a guideline to dimension the duplicate discard algorithm.

**EXAMPLE** In a ring of 16 nodes spaced by 36 km, the maximum number of frames in transit at the same time will be 480 in a 100 Mbit/s network, or 4 800 in a 1 Gbit/s network, although such a traffic is not typical. With a residence delay of 5 µs per node in the absence of other traffic, the delay between A and B frames at the node next to the sender is  $16 \times (36 \times 5 + 5) = 3$  ms.

#### **7.6.4.9 Ethernet Classes of Service (CoS)**

Ethernet is a PSN subject to unpredictable delays in the bridges as stated in 5.2 and therefore quality of service (called CoS) is improved by introducing priorities together with the VLAN mechanism.

**NOTE** The non-determinism due to the CSMA/CD does not exist anymore with switched Ethernet, but the non-determinism due to packet queuing persists.

IEEE 802.1Q tags provide CoS by giving each of the 4 094 possible VLANs a priority from 0 to 7. However, CoS does not provide bandwidth reservation, although some implementations may provide it. Therefore, Ethernet does not provide a deterministic behavior since the queue size in the bridges and the generation rate is not throttled.

However, when a TDM (e.g. E3) link carries Ethernet frames (see 7.6.4.12) it provides a deterministic latency, since the underlying channel is deterministic. At the end of that channel, within the Ethernet subnet, this property gets lost.

Bridges usually allow traffic limitation on a per-port basis to prevent monopolization of the bridge by a device with a high generation rate.

Ethernet does not have a resource reservation protocol. Further developments provide resource reservation through OAM (see 7.6.6).

#### **7.6.4.10 Ethernet security**

##### **7.6.4.10.1 MACsec**

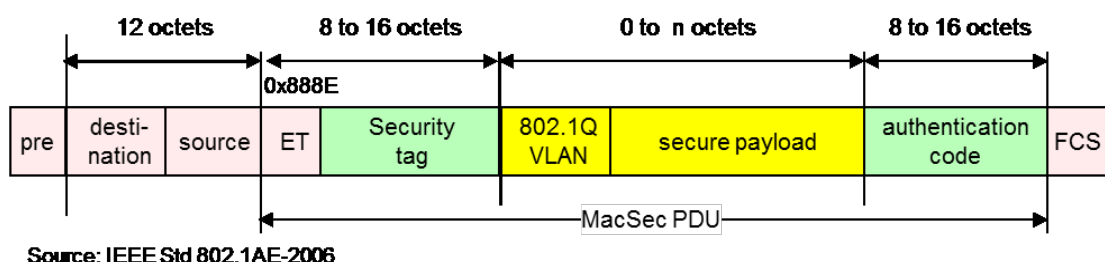
Layer 2 confidentiality and authentication can be assured by IEEE 802.1AE (MACsec). MACsec provides security on the LAN between endpoints and the bridge as well as between the bridges themselves.

MACsec could be used to protect Layer 2 protocols such as GOOSE (IEC 61850-8-1], SMV (IEC 61850-9-2] and IEC 61588, but this has not been standardized.

**NOTE** Frames corrupted by transmission errors will be rejected by the FCS checker and will not be evaluated for MACsec.

The MACsec frame extends the Ethernet frame by two fields (Figure 64):

- Security Tag, which is an extension of the EtherType
- Authentication Code



IEC

**Figure 64 – MACsec frame format**

MACsec does not provide key management and does not establish secure associations; this is delegated to IEEE 802.1X. Latest MACsec based implementations overcome the former deficits (e.g. the restriction to point-to-point applications) and allow service-aware encryption schemes across non-MACsec aware networks. Combining Layer 2 encryption with PTP / IEEE 1588v2 is demanding and only possible with optimized hardware implementations.

#### 7.6.4.10.2 IEEE 802.1X

To support user authentication, substation bridges may provide port based network control using IEEE 802.1X.

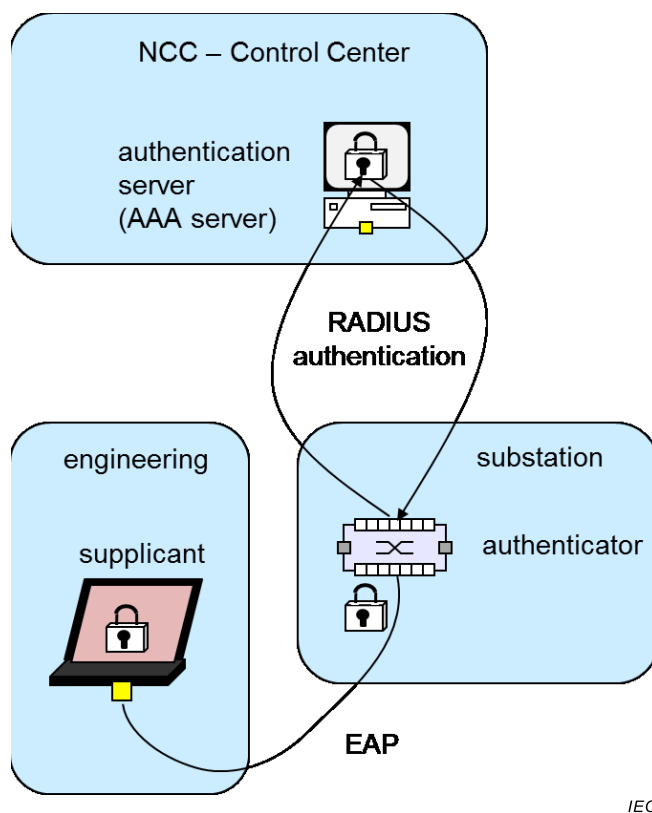
IEEE 802.1X allows authenticating user access within a substation on designated user access port(s) by username/password.

The security level of IEEE 802.1X-based access control depends on its Extended Authentication Protocol (EAP) used. Typical authentication mechanisms used in the context of this protocol are EAP-TLS, EAP-MD5 or EAP-IKEv2.

To this effect, IEEE 802.1X specifies encapsulation mechanisms for the transport of:

- EAP [RFC 3748],
- EAP over LAN (EAPoL) and
- EAP over PPP.

Figure 65 shows the IEEE 802.1X mechanism in a scenario in which an engineering station connects to a substation-internal bridge using an authentication server in the network control centre.



**Figure 65 – IEEE 802.1X principle**

IEEE 802.1X consist of three actors (Figure 65):

- Supplicant:** software component on the device or client machine used to request network access
- Authenticator:** the network node, typically a switch (e.g. in the substation automation network) which is placed between the supplicant and the authentication server
- Authentication server:** a server which receives an authentication request and validates it against an authentication system. Typically an authentication server based on Remote Authentication Dial In User Service (RADIUS), a protocol that provides centralized “Authentication, Authorization, and Accounting” (AAA) management for users and devices that connect and use a network resource.

#### **7.6.4.11 Ethernet OAM**

Ethernet OAM is described in IEEE 802.1ag and ITU-T Y.1731, allowing checking the connectivity of the network. Ethernet OAM has been extended in Metro Ethernet (see 7.13).

Ethernet uses services of the network layer to transport OAM objects.

For simple configuration of the bridges, SNMP can be used with dedicated MIBs, often depending on the manufacturer.

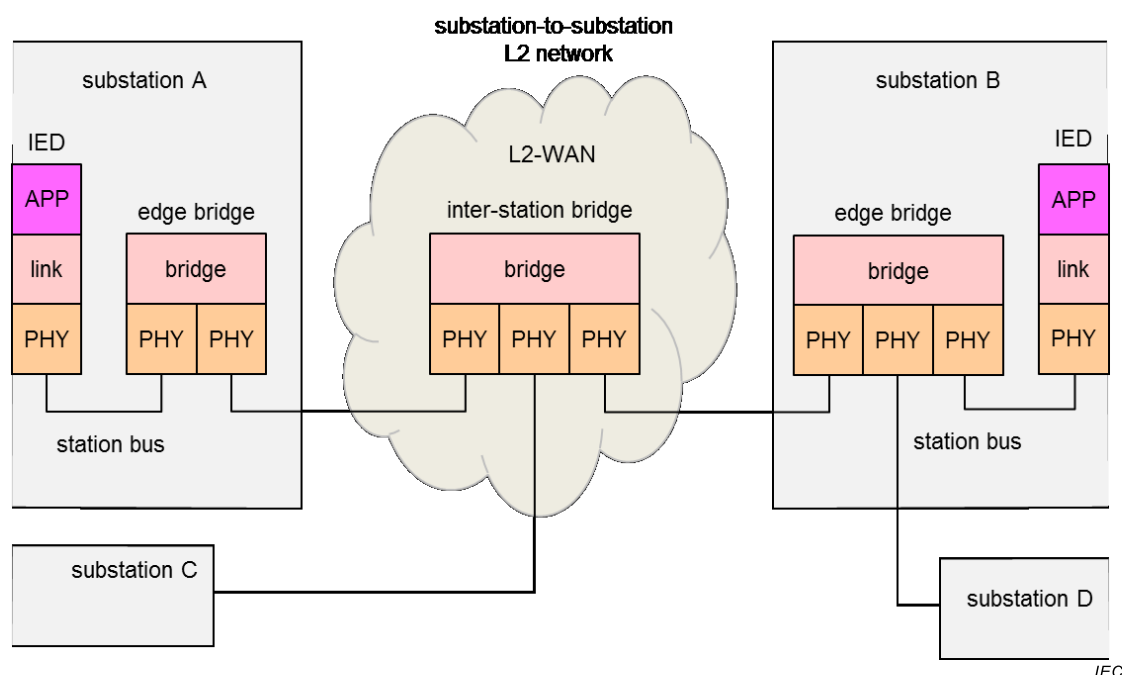
IEC TR 61850-90-4 allows to configure bridges and supervise the basic function of the network through IEC 61850 objects.

**NOTE** The objects of IEC TR 61850-90-4 will be moved to IEC 61850-7-4.

#### 7.6.4.12 Ethernet for substation to substation communication

Ethernet is the backbone of communication within the substation (especially GOOSE, SMV and IEC 61588); it can also carry the traffic outside of the substation, using the same type of bridges as within the substation. The bridges are located within the substation. Repeaters or bridges may also be located at intermediate premises. Ethernet is a convenient link for limited substation-to-substation communication according to IEC TR 61850-90-1, also when more than two substations are connected, e.g. for a high-voltage fork (Figure 66).

To add redundancy to this topology, methods such as in 7.6.4.8 apply. Multicast filtering or VLANs limit the traffic to where it is needed. Broadcast is possible, e.g. for time synchronization



**Figure 66 – Ethernet for substation-to-substation communication**

This solution is suitable for local communication, but not for a WAN that has to carry diverse traffic. To this purpose, Carrier Ethernet (7.6.6), PBB (7.6.8) and MPLS (7.6.9) are natural developments.

#### 7.6.5 Ethernet over TDM

Overlaid Ethernet emulates an Ethernet channel over a TDM transport. Older system sent Ethernet frames over a single voice channel, for instance over ISDN or another 64 kbit/s connection with the Point-to-Point Protocol (PPP) [RFC 1661].

Fitting a 100 Mbit/s Fast Ethernet connection inside a 155 Mbit/s STS-3c / STM-1 wastes bandwidth. For higher speed and better bandwidth efficiency of TDM, New Generation SDH/SONET (see 7.6.2.7) offers services by grouping several voice channels using:

- Generic Framing Procedure (GFP) [G.7041];
- Link Capacity Adjustment Scheme (LCAS) [G.7042] and
- Virtual Concatenation (VCAT) [G.7043].

The assignment of a number of VC-x to an Ethernet link guarantees full bandwidth for this service, with no Ethernet queueing delays. Other Ethernet or SDH/SONET channels do not



have an impact on already provisioned services, as they will use another set of VC-x containers.

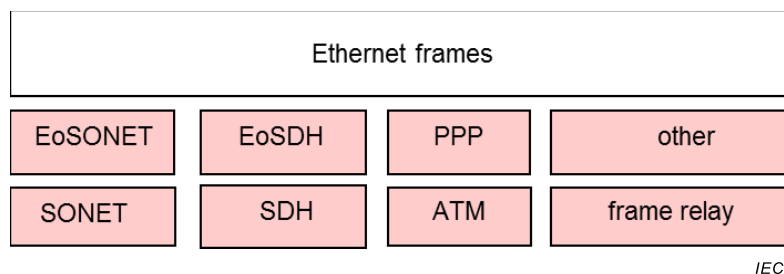
The protocols VCAT and LCAS allow to change/adapt the assigned bandwidth to the Ethernet service ‘on the fly’ without interruption of the traffic.

Table 37 shows the differences in mapping Ethernet based payloads in SDH/SONET and the efficiency increase using Next Generation SDH / SONET with VCAT.

**Table 37 – Payload mapping using SDH/SONET and Next Generation SDH/SONET**

Service	SDH / SONET Payload	Bandwidth efficiency	SDH / SONET Payload using VCAT	Bandwidth efficiency using VCAT
Ethernet 10 Mbit/s	STS-1 / STM-1	20 %	VT2-5v VC12-5v	98 %
Fast Ethernet 100 Mbit/s	STS-1 / STM-1	67 %	STS-1-2v VC3-2v	100 %
Gigabit Ethernet, Fiber Channel, FICON	STS-48 / STM-64	42 %	STS-3c-7v VC4-7v	95 %
FICON Express	STM-64	84 %	STS-3c-13v VC4-13v	99 %

Ethernet over SDH (EoSDH) and Ethernet over SONET (EoSONET) traffic can make use of the different fast SDH redundancy switching mechanisms (see 7.6.2.6), but can also use the LCAS protocol to sustain the Ethernet traffic (Figure 67).



IEC

**Figure 67 – Packets over TDM**

They offer as a basic rate that of STS-3c/STM-1 at 155 520 Mbit/s (useful bandwidth 149 760 Mbit/s) when removing section, line and path overhead. EoSDH offers nxVC12 (nx2Mbit/s) granularity, but also nxVC3 or nxVC4.

Modern SDH/SONET multiplexers include EoSDH/EoSONET modules with integrated switching functionality, thus offering Layer 2 services directly on the multiplexer.

IP traffic may be forwarded over SDH/SONET (Layer 3 over Layer 2), called “Packet over SDH” (POS) [RFC 2615].

## 7.6.6 Carrier Ethernet

### 7.6.6.1 Carrier Ethernet principle

Carrier Ethernet is the extension of Ethernet to Metropolitan Area Networks (MAN) and WANs. It evolved from Ethernet and particularly from the 802.1Q VLAN concept. The intention was to use the Ethernet physical layer and frame format as a base and to use VLAN tags as labels to

traverse a metropolitan network. It has been promoted by the Metro Ethernet Forum (MEF) [11].

MEF, IETF and ITU-T developed the specifications ([11] to [34]). New features depart from the classical “switched Ethernet”, in particular the concept of Quality of Service and features that allow a better scalability. Carrier Ethernet uses OAM services of Layer 3 and Layer 4.

#### **7.6.6.2 Carrier Ethernet QoS**

The MEF developed guidelines to deploy Ethernet as a WAN (Metro-Ethernet). MEF calls the interface to Carrier Ethernet “User Network Interface” (UNI).

The MEF defines classes of traffic that can serve to define a SLA [32]:

- Committed Information Rate (CIR): average rate up to which “green” frames are delivered.
- Committed Burst Size (CBS): maximum number of octets that comply with CIR
- Excess Information rate (EIR): average rate at which frames exceeding CIR (“yellow” frames) are admitted
- Excess Burst Size (EBS): maximum number of octets that comply with EIR.

To reserve bandwidth, a token bucket algorithm keeps track of the traffic. Its implementation is specific of the bridge manufacturer and requires configuration tools to reserve bandwidth statically, in contrast to RSVP (see 7.7.2.3).

This only works if all sources limit their production rate. To enforce this, ports may be equipped with rate limitation.

#### **7.6.6.3 Carrier Ethernet services**

MEF defines three services over Carrier Ethernet as:

- E-line emulates a point-to-point line, cf. VPWS in 0.
- E-tree emulates a point to multipoint communication.
- E-LAN emulates a multipoint to multipoint communication (see VPLS in 0)

#### **7.6.6.4 Carrier Ethernet summary**

Table 38 summarizes the Carrier Ethernet characteristics.

**Table 38 – Carrier Ethernet summary**

Feature	Comment
Acceptance	Well known and understood, widespread use in LANs
Bandwidth efficiency	Packet-switching makes efficient use of bandwidth on the active links. To resolve loops in meshed networks, Ethernet uses RSTP (7.6.4.2), which blocks the unused links. These links cannot be used to share load.
Forwarding	Layer 2 forwarding is simple. Ethernet forwards traffic on the base of the 48-bit MAC addresses. Layer 2 forwarding is not explicit since Ethernet floods the network, leaving it to the bridges to filter out the packets after a learning phase (7.6.4.3).
Traffic engineering	MAC addresses cannot serve to bundle traffic and limit traffic regions. VLAN tags in conjunction with VLAN bridge configuration and Multiple Spanning Tree Protocol (MSTP) allows segmenting the network.
Configuration	RSTP and HSR can be used to remove loop automatically QoS is engineered in the bridges (VLANs, 802.1Q tags).
Recovery	Zero-recovery time with PRP and HSR at the cost of additional hardware. Ethernet Ring Protection Switching (ERPS, G.8032] provides only a 50 ms switchover latency. 5 ms / hop recovery delay with RSTP (7.6.4.2), but up to 20 s in case of root bridge failure
Latency and jitter	Statistical value, depends on traffic, technology and priorities, packet path vary
VPN	L2VPN Q-in-Q
Application	Small to medium-sized networks

### 7.6.7 Audio-Video Bridging

Ethernet is still an evolving technology. IEEE is working on Time Sensitive Networks for transmission of time-critical data. This work was formerly called Audio/Video Bridging and encompasses several IEEE standards such as IEEE 802.1AS (Timing and Synchronization), IEEE 802.1Qat (Stream Reservation Protocol) and IEEE 802.1BA Audio Video Bridging. This work could influence Carrier Ethernet.

### 7.6.8 Provider Backbone Bridge (PBB)

#### 7.6.8.1 General

PBB is a Carrier Ethernet technology with improved scalability and redundancy, which allows coupling several LANs, each with its VLAN tagging, while preserving the VLAN tags from end to end.

A PBB network may be engineered with PBB-TE (IEEE 802.1Qay-2009) to allocate fixed paths and ensure a predictable route.

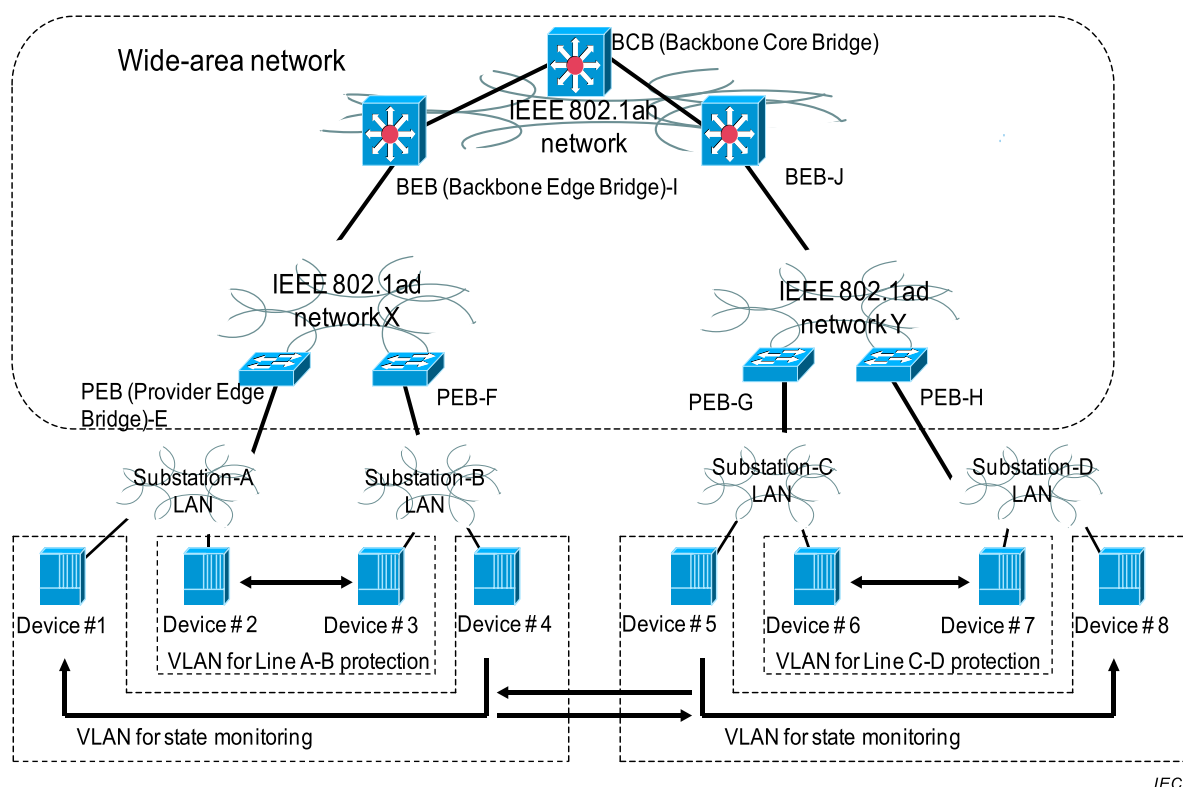
While PBB had a promising start, it lacks support and could not impose itself. It is therefore not recommended for future developments. It is displaced in favor of MPLS (7.6.9). Since a number of utilities still use PBB, especially in Japan, a brief description follows in

#### 7.6.8.2 PBB principle

The PBB concept evolved from the introduction of Ethernet for metro networks. Nortel created PBB to overcome the scalability limitations that hinders the use of LANs as WANs: limited number of VLANs (4 094), resolution of the 48-bit MAC addresses and handling of broadcast packets storms that affect throughput. The basic idea is to use IEEE 802.1Q VLAN tags to route packets rather than rely on IP addresses or MAC filtering.

PBB (IEEE 802.1ah-2008) also known as MAC-in-MAC, is an extension of Ethernet that allows Ethernet LANs to be coupled hierarchically into a WAN, by taking advantage of the IEEE 802.1ad (Q-in-Q) technique.

Figure 68 shows a LAN hierarchy in which several IEEE 802.1Q-based substation LANs are aggregated by IEEE 802.1ad (Q-in-Q) LANs, themselves interconnected by an IEEE 802.1ah- (PBB) wide-area network. IEEE 802.1ah-capable networks carry communications between IEEE 802.1ad networks.



**Figure 68 – IEEE 802.1Q/ad/ah network configuration**

The advantages are:

- More than 4 094 VLANs available network-wide;
- Arbitrary VLAN identifiers assigned in any IEEE 802.1ad network;
- Communications between VLANs belonging to each IEEE 802.1ad network with different VLAN identifiers available through an IEEE 802.1ah network.

#### 7.6.8.3 Use case: PBB application to power utility (EPDC)

For power system applications, PBB seems attractive since it can easily interconnect several substation LANs, each of which has its own VLAN tagging, while preserving the VLAN tags from end to end.

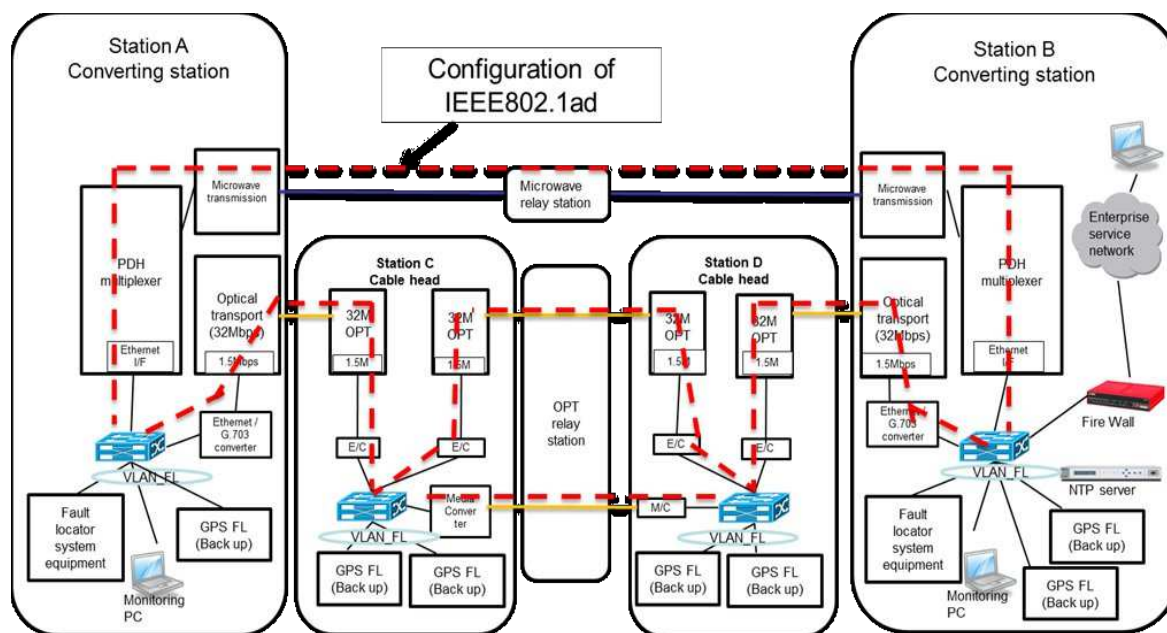
Figure 69 shows a use case of a PBB network for a fault locator (FL) system for HVDC submarine cables and overhead lines in EPDC, Japan.

The FL system needs single segment Layer 2 network at four sites. The PBB network can provide the VLAN for FL at several stations. Since the PBB is based on Layer 2 network technology, it is easier to configure and operate the network than Layer 3 or MPLS network.

The PBB equipment has advantages of higher availability and lower cost than Layer 3 equipment. In the future, other VLANs will be added to this network sharing the Layer 1.

Since the bandwidth of Layer 1, especially microwave path, is limited, it is necessary to control QoS in this network.

In addition, PB networks will be installed in other areas of EPDC, and they will be interconnected by IEEE 802.1ah network in the future. Other advantages of PBB include enough scalability for a large number of VLANs and fast path switching by using RSTP.



Source: EPDC, Japan

IEC

Figure 69 – Case of IEEE 802.1Q/ad network for utility

## 7.6.9 Multiprotocol Label Switching (MPLS)

### 7.6.9.1 MPLS principles

MPLS merges the dynamic, connectionless routing of packets of Ethernet with the connection-oriented, time division multiplex routing of the classical circuit-switched telephone networks PDH/SDH/SONET.

MPLS was in 2015 the emerging technology for new deployments in WAN utility communication.

MPLS allows multi-service transport over a wide variety of Layer 1 and Layer 2 technologies (fiber, copper, wireless, power line carrier, etc.), and supports the consolidation of networks onto a common infrastructure.

MPLS inherits from SDH/SONET in that it is a connection-oriented protocol.

MPLS inherits from Carrier Ethernet in that it uses the Ethernet physical layer and frame format as a base. The routing itself bases on labels inserted between the Layer 2 – and the Layer 3 headers hence the name “Layer 2,5” (see Figure 71 for an example).

MPLS inherits from IP in that it is a packet transport networking. In an MPLS network, packets are tagged with labels (similar to VLAN tags). IP addresses are only used during connection establishment for setting up the path.

The routers in the MPLS network decide how to forward packets solely on the content of these labels, not on the base IP network addresses or any other packet data.

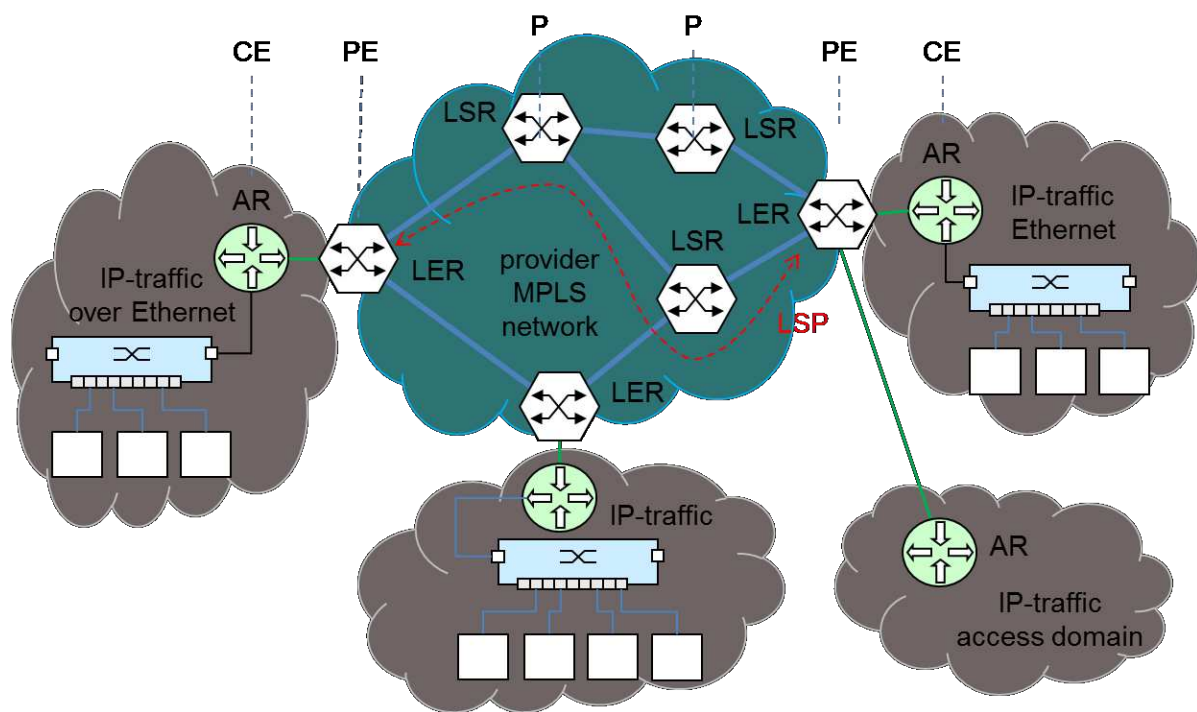
### 7.6.9.2 MPLS architecture

The typical components of a MPLS network comprise (Figure 70):

- Access Router (AR) at the Customer Edge (CE): a classical IP router where the customer networks connect to the MPLS network over a link with IP frames.
- Label Edge Router (LER) at the Provider Edge (PE): the router that inserts and removes MPLS labels and sets up the route. Several streams can enter the LER, not only IP.
- Label Switching Router (LSR) within the provider domain (P): routers within the MPLS core network that forward MPLS-labelled packets.

NOTE In a utility WAN, with no clear demarcation line between provider and customer, PE and CE functionality are often aggregated in the same SEN. The same device can implement all three functions: CE, LER and LSR.

A Label-Switched Path (LSP) is a path through an MPLS network, from LER to LER. The path starts and ends at the LER. Alternatively, redundant paths can be set up as back up.



IEC

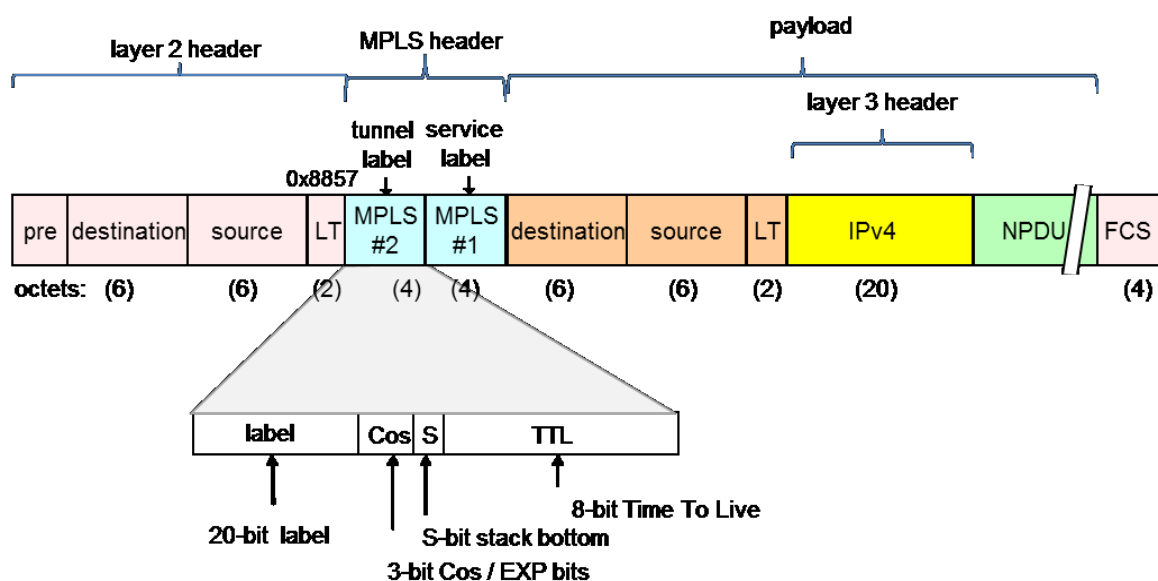
**Figure 70 – Basic MPLS architecture**

To achieve this, MPLS opens a connection from end-to-end (virtual circuits or LSP).

### 7.6.9.3 MPLS transport over Ethernet

MPLS frame format as shown in Figure 71 bases on Ethernet frames in which label field replace the VLAN tags between the Layer 2 header (MAC) and the Layer 3 (IP) header. As for

VLANs in Q-in-Q, there can be several stacked labels, normally two, one for packet forwarding and one for the service; management traffic in IP/MPLS has no label.



IEC

Figure 71 – Example of MPLS frame format with IPv4 payload

#### 7.6.9.4 MPLS Services

MPLS networks MPLS supports the following connectivity:

- Point to Point (P2P) – exactly two end points are connected
- Point to Multipoint (P2MP) – multicast from one source (root node) to multiple destinations (leaf nodes)
- Multipoint to Multipoint (MP2MP): multicast from several sources over the same LSP.

MPLS offers services based on this connectivity:

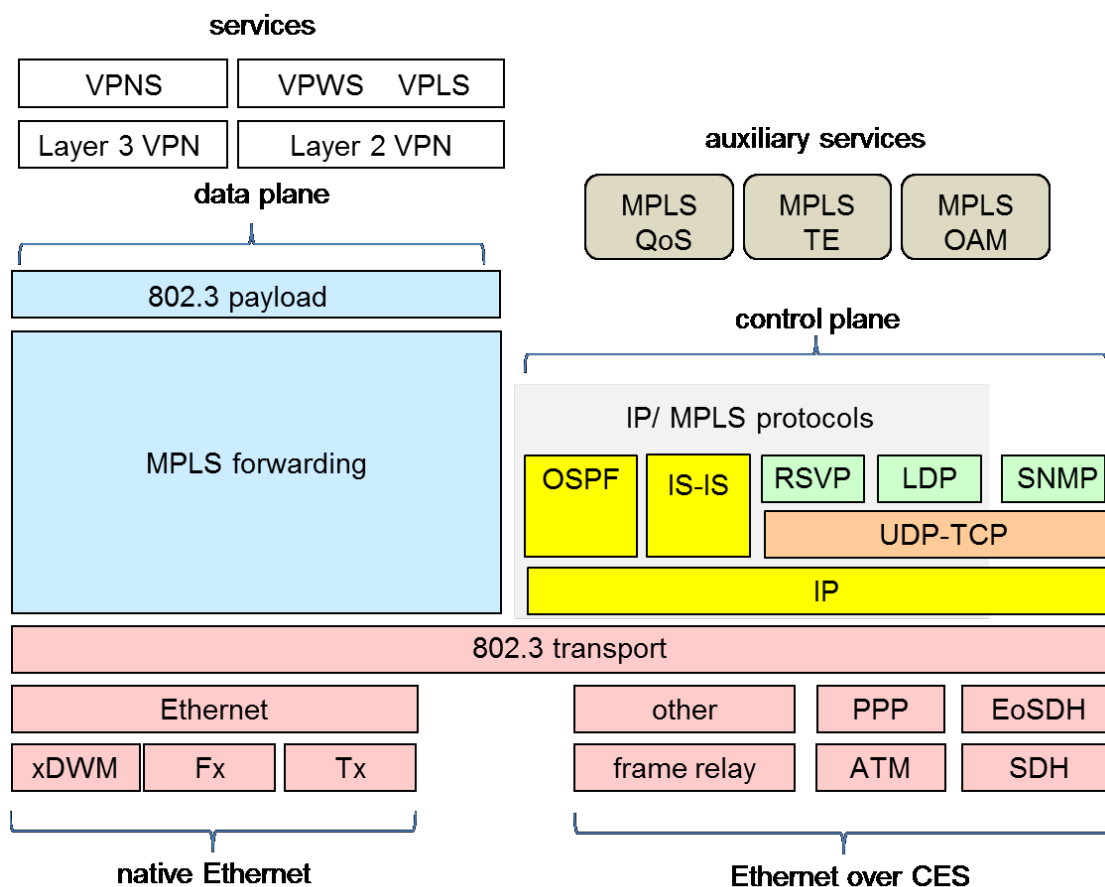
- Virtual Private Wire Service (VPWS): Layer 2 P2P service
- Virtual Private LAN Service (VPLS): Layer 2 P2MP service
- Virtual Private Network Layer 3 (L3VPN): Layer 3 service.

These services will be described in more detail in 7.11.

#### 7.6.9.5 MPLS building blocks

Figure 72 depicts the main building blocks of MPLS. MPLS relies on auxiliary services (in particular QoS, OAM and TE).

NOTE The Ethernet frames appear at two layers: once as a transport for MPLS, once as a transported service.



IEC

Figure 72 – MPLS building blocks

#### 7.6.9.6 MPLS QoS

MPLS is a PSN and therefore presents a non-deterministic latency as explained in 5.2. Therefore, it needs QoS to give time-critical data a higher priority.

MPLS QoS enables differentiated types of service across an MPLS network based on network administration. Differentiated services meet a wide range of requirements by supplying for each transmitted packet the service specified for that packet by its QoS, using the same methods as DiffServ in IP (7.7.2.4).

In a MPLS network, classification and marking bases on the EXP field [RFC 5642], which stands for “experimental” bits in the MPLS label used to indicate QoS. Routers use the EXP field within the MPLS label to apply QoS to the traffic.

NOTE In a MPLS network, the LSRs do not use the IP header in the forwarding process.

#### 7.6.9.7 MPLS OAM

MPLS OAM provides remote monitoring, detection, and resolution of path errors on a MPLS based network. MPLS OAM provides capabilities to LSPs and isolates MPLS forwarding problems to assist with fault detection and troubleshooting in an MPLS network.





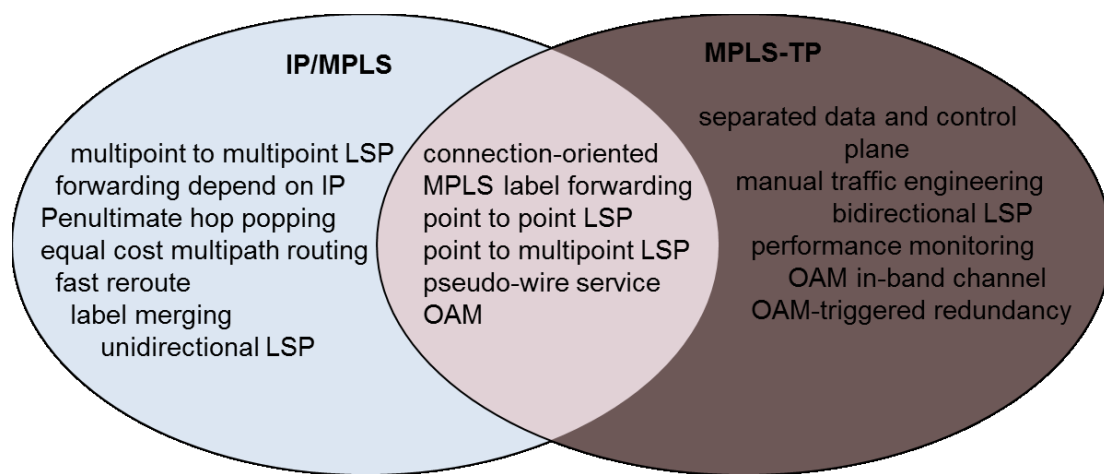
### 7.6.9.10 MPLS variants

#### 7.6.9.10.1 General

There exist two variants of MPLS, IP/MPLS and MPLS-TP, which differ in the method used to establish LSPs and which are compatible to a certain extent:

- IP/MPLS uses routing and label distribution protocols to set the labels in different routers:
  - Label Distribution Protocol (LDP);
  - Resource Reservation Protocol – Traffic Engineering (RSVP-TE);
  - Border Gateway Protocol (BGP); or
  - Constraint-based Routing Label Distribution Protocol, which has been displaced by RSVP-TE.
- MPLS-TP uses static LSPs, which are setup by the operator through network management, similarly to what is done in SDH/SONET virtual circuits.

Figure 74 shows the differences and the overlapping features.



IEC

**Figure 74 – IP/MPLS and MPLS-TP features**

#### 7.6.9.10.2 IP/MPLS

The original MPLS is termed IP/MPLS. A comprehensive protocol suite allows automatic configuration of the network through IP routing protocols and label distribution protocols. The LSRs establish the routes based on the IP addresses and routing protocols such as BGP and distribute this information to the LSR using the LDP.

MPLS-TE (for Traffic Engineering) allows controlling where and how traffic is routed on the network. TE allows managing capacity, prioritizing different services, and preventing congestion in the network.

IP/MPLS allows multipoint-to-multipoint communication.

The main specifics and capabilities of MPLS are summarized in Table 39.

**Table 39 – IP/MPLS characteristics**

<b>Data plane</b>	P2P, P2MP / MP2MP LSP forwarding ECMP (Equal-cost multi-path routing)
<b>Control plane</b>	Dynamic, by BGP and LDP
<b>OAM (Operations, Administration, and Maintenance)</b>	Based on LSP Ping, Trace Route, Trace Tree
<b>Resiliency</b>	50 ms switchover (recovery) Link/Node and path redundancy with Traffic Engineering (TE)—Fast Reroute (FRR) Link and Node redundancy Link/Node redundancy with Free Alternate Fast Reroute "1:1 protection" provides active / standby redundancy by two different paths to overcome link or router failure. In contrast to restoration, the recovery path is pre-computed.
<b>Traffic engineering</b>	Bandwidth reservation with RSVP-TE, advertised by the IGP and maintained in the TE database stored on each node
<b>Services</b>	VPWS (point-to-point), VPLS (multicast) and VPMS (Virtual Private Multicast Service)

**7.6.9.10.3 MPLS-TP**

MPLS-TP is a subset of the IP/MPLS protocol, with a focus on providing typical transport-type functions, developed jointly by IETF and ITU-T, and standardized as RFC 5921.

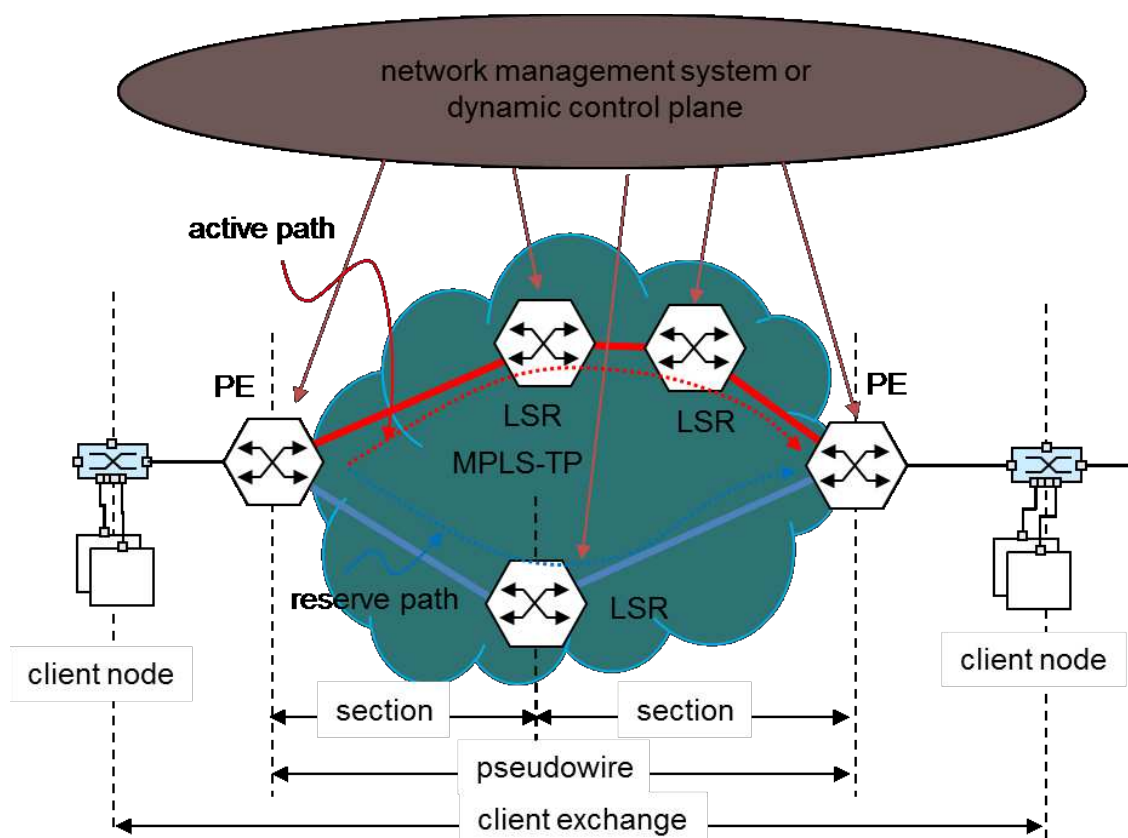
MPLS-TP uses static provisioning under control of the operator through network management to establish connections and reserve bandwidth at each hop.

MPLS-TP offers predictable path redundancy for normal operation and recovery.

Table 40 contains the basic characteristics of MPLS-TP; Figure 75 shows the basic architecture.

**Table 40 – MPLS-TP characteristics**

<b>Data plane</b>	<p>P2P, P2MP (no MP2MP)</p> <p>Bidirectional P2P and unidirectional P2MP LSP (no LSP merging)</p> <p>In-band associated channel (G-Ach / GAL)</p> <p>Co-routed (same forward and reverse paths following exactly the same nodes)</p> <p>LSP contained within a tunnel acting as a container for LSP</p>
<b>Control plane</b>	<p>Static; does not need MPLS control plane capabilities</p> <p>Enables the management plane to set up LSPs manually</p> <p>Dynamic (in GMPLS)</p>
<b>OAM</b>	<p>Dedicated, In-band OAM channel (Generic Associated Channel (G-ACh)) which enables a rich set of OAM features</p> <p>Guaranteed resources for management</p> <p>Continuity check, remote defect indication</p> <p>Connectivity verification and route tracing</p> <p>Fault OAM (e.g. MPLS Lock Report)</p> <p>Performance management</p> <p>OAM does not need any IP layer functionalities</p>
<b>Resiliency/Fault tolerance</b>	<p>50 ms switchover (recovery)</p> <p>Path (Linear) fault tolerance – 1:1, 1+1, 1:N</p> <p>Ring fault tolerance</p>
<b>Services</b>	<p>VPWS (point-to-point) and VPLS (multicast).</p>



IEC

**Figure 75 – MPLS-TP redundant routing**

#### 7.6.9.10.4 MPLS summary

Table 41 summarizes MPLS.

**Table 41 – MPLS summary**

Feature	Comments
Acceptance	Increasing use in carrier and telecom networks
Bandwidth efficiency	Packet-switching, efficient label switching
Routing	Routing uses the IP protocols (IP/MPLS) or traffic engineering (MPLS-TE, MPLS-TP) When routing is done by traffic engineering, scalability suffers
Traffic engineering	Required for predictable routing
Configuration	Via routing protocols or via management
Recovery	50 ms recovery time (1+1 mode in MPLS/TP, FRR in IP/MPLS)
Latency and jitter	Statistical value which depends on traffic, technology and priorities. Route can be deterministic and congruent
VPN	L2VPN or L3VPN necessary for operation. Configuring VPWS and VPLS is a manual operation
Application	Medium (MPLS-TP) to large networks (IP/MPLS) – transport of any service (TDM, voice, etc.)

### 7.7 Layer 3 (network) technologies

#### 7.7.1 Internet Protocol (IP)

##### 7.7.1.1 General

Layer 3 communications such as IP involve packet switching and routing. They rely on Layer 2 communication.

NOTE OSI Layer 3 protocols such as ISO 8208 / ISO 8473, or ITU protocols such as X25 only have historical status; they are out-of-scope.

Within a substation, many protocols rely on IP, the origin and final nodes being identified by their IP address.

However, there is normally no Layer 3 router within a substation; forwarding is left to the Ethernet bridges. Outside of the substation, Layer 3 routers are the rule.

NOTE Clauses 7.7.1.2 and 7.7.1.3 have been inherited from IEC TR 62357-200 and will be maintained in this TR only, so this document will be the future reference.

##### 7.7.1.2 IP version 4 (IPv4)

###### 7.7.1.2.1 IPv4 Origin

IP version 4 (IPv4) [RFC 0791] has been the base for the Internet since 1980 and it is still the most widely used network protocol in 2015. Its main characteristics are:

- IPv4 is connectionless, i.e. routers retain no knowledge of previous messages;
- IPv4 operates with 32-bit network source and destination address.
- IPv4 is supported by a suite of routing protocols.

### 7.7.1.2.2 IPv4 mapping to Ethernet

RFC 0894 defines the mapping of IPv4 to Ethernet frames. The Layer 3 header comes just after the Layer 2 header in an Ethernet frame (see Figure 76).

NOTE GOOSE and SMV frames do not carry a network header within a substation, but often an IEEE 802.1 Q tag.

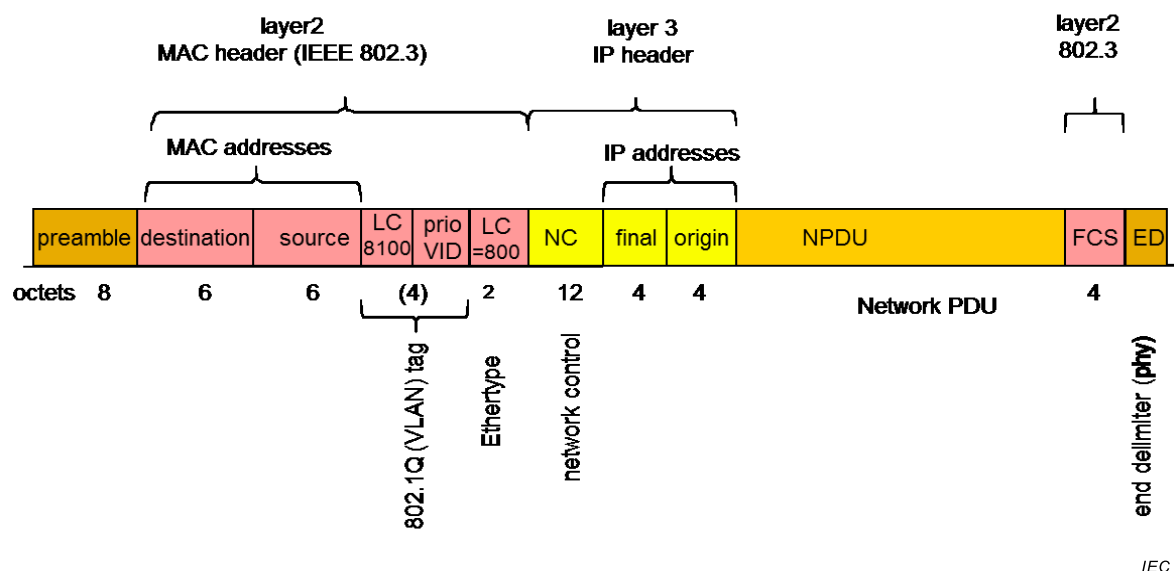


Figure 76 – Ethernet frame with IP network header

### 7.7.1.2.3 IPv4 network header

The IPv4 network header carries the two 32-bit IP addresses and a protocol type indicating which kind of payload – called Network Protocol Data Unit (NPDU) – follows (see Figure 77).

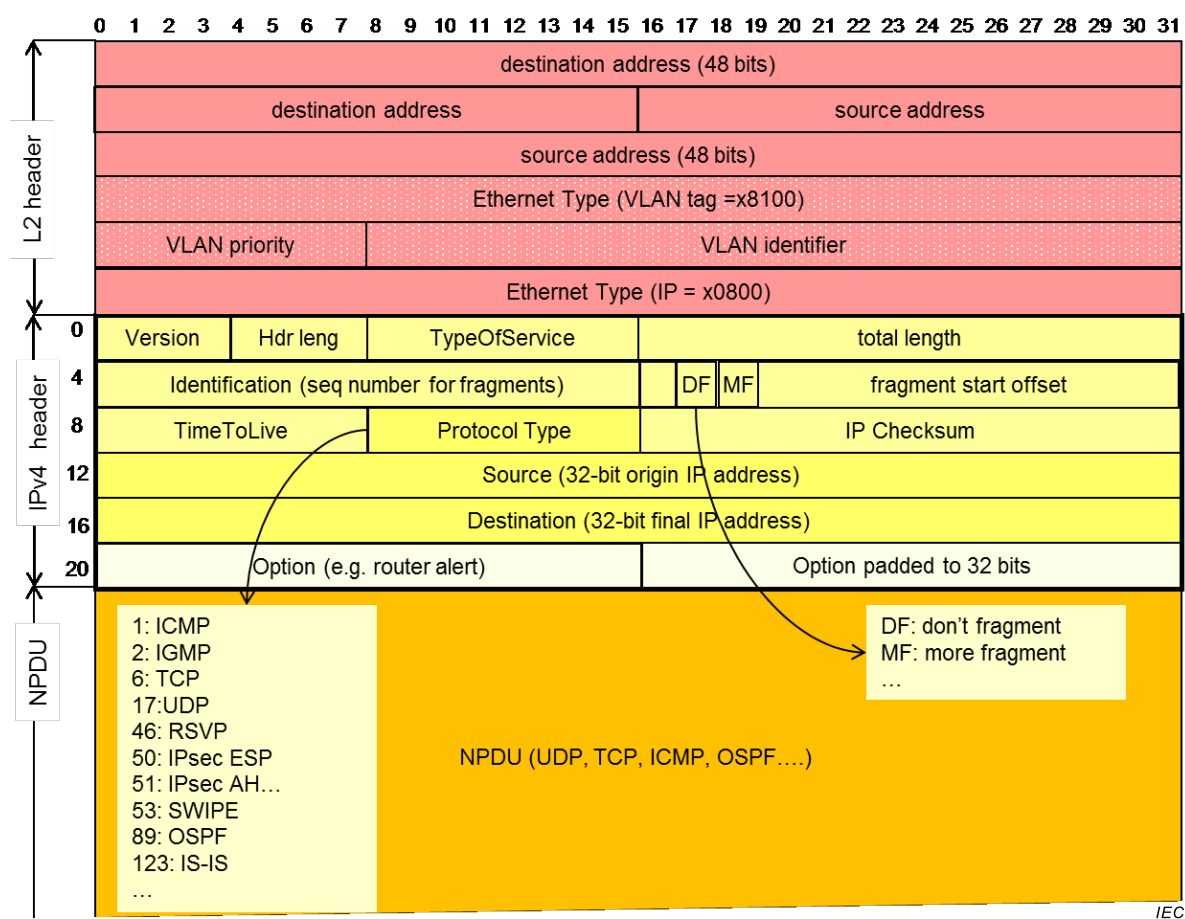


Figure 77 – Mapping of IPv4 to Ethernet frames

#### 7.7.1.2.4 IPv4 addresses

The IPv4 addresses have a size of 32 bits. Their human-readable representation is a sequence of four decimal digits separated by dots, each digit representing one octet.

Example: "10.12.127.4" translates as "00001010'00001100'01111111'00001000"b.

The IP addresses are divided into a public address space (unique worldwide and administrated by the Internet Assigned Numbers Authority (IANA) through Regional Internet Registry (RIR) and a private address space (which can be reused, for instance be the same in different companies, industrial plants or internet service provider domains). RFC 1918 gives guidelines on the allocation of IPv4 addresses.

The public IPv4 addresses are exhausted (see 7.7.1.3.1), but this does not concern networks that operate with private addresses or that are separated from the public internet.

The router at the boundary of a private address subnet may translate from an internal to an external address or vice-versa as standardized in the Network Address Translation (NAT) [RFC 2663/RFC 3022]. NAT allows at the same time to multiplex the IP addresses by the port identifiers in UDP and TCP traffic. NATs helped stretching the life of IPv4 since they allowed reusing addresses in private networks and translating them to public addresses.

The IPv4 addresses are structured into subnets, which are of varying size, as the Classless Inter-domain Routing (CIDR) [RFC 4632] defines.

**Example** The notation 10.12.127.0/24 means that all nodes that share the same 24 most significant bits belong to the same subnet.

Subnetting allows structuring the network and improves efficiency of the routing since addresses can be bundled.

The assignment of IPv4 multicast addresses is specified in RFC 5771.

#### **7.7.1.2.5 IPv4 fragmentation and packet size**

The Maximum Transmission Unit (MTU) is the maximum size of an IP packet that a node or router transmits without fragmentation.

If an IPv4 node cannot forward a message because the next link has too small an MTU size, it may fragment the message into several IP packets with smaller NPDU's, while another node will reconstitute the message at the other end.

To this effect, the IP header has a 16-bit sequence number, called "Identification" and a "fragment start offset", which indicates the position in the original messages where the fragment begins. It also holds a "More Fragment" bit (MF) that indicates that this NPDU is not the last fragment. The "Don't Fragment" bit (DF) is an indication to the next router(s) not to fragment this NPDU.

In the path between the end nodes, any IPv4 node may fragment if DF is not set, and if it cannot forward a received NPDU without fragmenting, it returns an error through ICMP. The sending node must then reduce its MTU size until the other node accepts it. IPv4 nodes cannot agree on an MTU that is smaller than 68 octets.

The minimum datagram size that all hosts must be capable of accepting has a value of 576 octets for IPv4.

Nearly all IP over Ethernet use an MTU value of 1 500 octets.

More details are available in RFC 6864 and RFC 4459.

#### **7.7.1.2.6 IPv4 auxiliary protocols**

Auxiliary protocols allow managing the IP network. For end devices, the relevant auxiliary protocols are:

- Address Resolution Protocol (ARP) [RFC 0826] allows a device to obtain the Layer 2 MAC addresses knowing the IPv4 address of the partner. To this effect, a node broadcasts a Layer 2 message "who has IP address X", to which the owner of that IP address responds with its MAC address. If the caller receives no response, it assumes that the owner of the IP address is not within the LAN and it directs the messages to the MAC address of the router for further forwarding. ARP operates on Layer 2.
- Internet Control Message Protocol (ICMP) [RFC 0792] allows asking a remote node about its presence and checking how long it takes to respond. One often-used service of ICMP is the "Echo", better known as "Ping". Additional services allow error reporting and statistics. ICMP operates on Layer 3.
- Dynamic Host Configuration Protocol (DHCP) assigns dynamically an IP address to connected devices. To this effect, a host asks the DHCP server for an IP address and receives an IP address for a certain lease time. This is useful for client devices and allows reusing private addresses. Servers receive a fixed IP address by configuration and benefit little from DHCP. DHCP version 4 (DHCPv4) [RFC 2131] operates on Layer 4 with UDP over ports 67 and 68.
- Domain Name Service (DNS) provides the IP address given the Uniform Resource Locator (URL) of a remote node. To this effect, a host asks the DNS for the IP address



corresponding to a given URL, to which the DNS responds with an “A-record” containing the IPv4 address. This avoids using hard-coded IP addresses in the applications and gives room for some redundancy. DNS becomes important when translating protocols. DNS operates on Layer 4 over TCP or UDP port 53.

#### **7.7.1.2.7 IPv4 routing**

The routers execute the most complex part of the IP protocol. To determine the path that messages take, the routers exchange control messages to actualize their routing tables in order to establish over which path to forward an incoming packet.

IETF standardized numerous routing algorithms. The Interior Gateway Protocol (IGP) manages the routing within an Autonomous System (AS) (e.g. within a company), for instance using the Open Shortest Path First (OSPF) [RFC 2328] or the Intermediate System to Intermediate System (IS-IS) [RFC 1142] protocols.

The Internet routers connect the different AS and exchange their routing information using the Exterior Gateway Protocol, called today Border Gateway Protocol (BGP) [RFC 4271].

IP makes no effort to ensure that the forward and backward path between two partners is the same (path coherence).

The routing protocol is determinant for the recovery time of the network. Indeed, the loss of a link causes lengthy reconfiguration with a recovery time in the order of seconds or even minutes. IP fast reroute and Bidirectional Forwarding Detection (BFD) can speed up recovery.

#### **7.7.1.3 IP Version 6**

##### **7.7.1.3.1 IPv6 motivation**

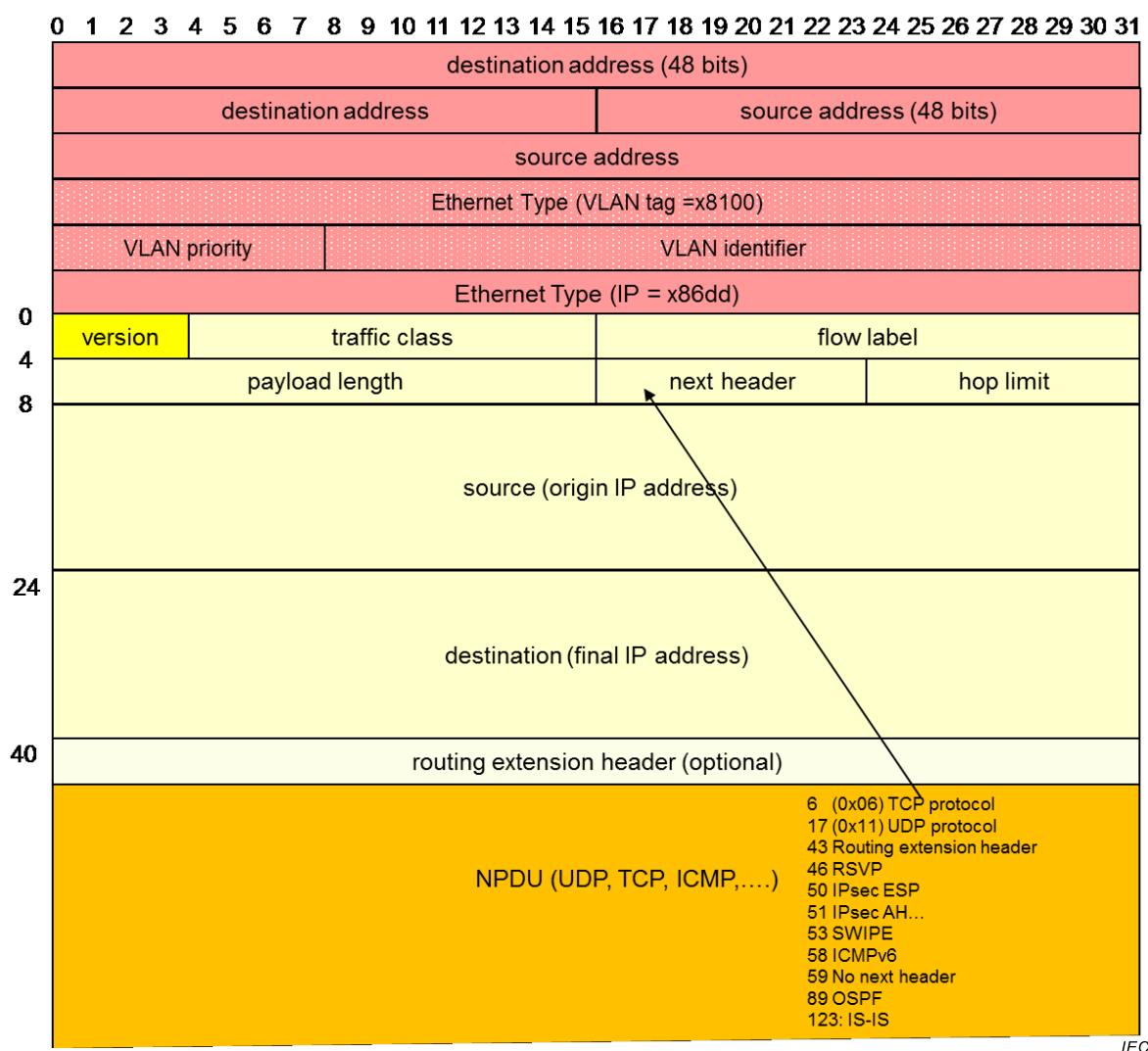
In view of the shortage of public addresses in IPv4 (the pool became exhausted in 2011), IETF standardized IP Version 6 (IPv6) [RFC 2460] that has 128-bit addresses. At the same opportunity, IPv6 introduced a number of improvements over IPv4, such as better security and routing, some of which were ported back to IPv4.

This does not immediately affect utility networks, since they have sufficient private addresses with IPv4 and tools and hardware should support IPv4 for a long time.

However, IETF will not support IPv4 anymore and network providers could stop support. It is therefore advisable to start now the migration process, as 7.7.1.5 recommends.

##### **7.7.1.3.2 IPv6 header**

RFC 2464 defines the mapping of IPv6 to Ethernet frames as shown in Figure 78.



**Figure 78 – Mapping of IPv6 to Ethernet frames**

The Ethertype “0x86dd” identifies the IPv6 packets.

The IPv6 header has a fixed size of 40 octets. The only field retained from the previous IPv4 header is the Version Number. Extension headers allow appending parameters for routing, security, tunneling, etc.

This means that IPv4 and IPv6 are not compatible, but distinguishable through the Ethertype at Layer 2 and the Version Number at Layer 3.

### 7.7.1.3.3 IPv6 addresses

#### 7.7.1.3.3.1 IPv6 address representation

[RFC 4291] structures the human readable representation of IPv6 addresses in a different way from IPv4. Rather than using dotted decimal, it expresses the 128-bit addresses as eight groups of four hexadecimal (lowercase) digits, separated by colons.

Example: The notation 2001:0db8:85a3:0000:0000:8a2e:0370:7334 maps to:

```
0010 0000 0000 0001 0000 1101 1011 0100 1000 0101 1010 0011 0000 0000 0000 0000
0000 0000 0000 0000 1000 1010 0010 1110 0000 0011 0111 0000 0111 0011 0011 0100
```

In addition, a double colon represents one contiguous string of “0”, irrespective of the length of the string, but at only one place in the address.

Example: the previous address becomes 2001:0db8:85a3::8a2e:0370:7334.

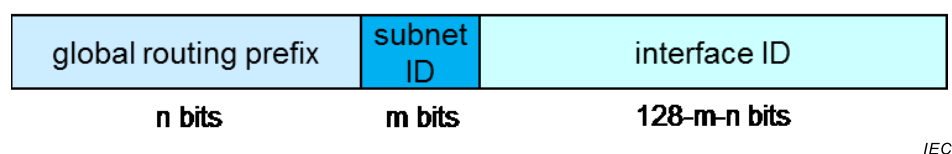
To facilitate IPv4 integration, IPv4 addresses can appear (once) in an IPv6 address as “dotted decimals” separated by “.”.

Example: 192.0.2.1 -> 64:ff9b::192.0.2.1.

NOTE [RFC 5952] could present problems to the parsers since it mandates lowercase hexadecimal characters in the IPv6 addresses, contradicting [RFC 4291].

### 7.7.1.3.3.2 IPv6 global unicast address format

[RFC 4291] specifies the format of the unicast addresses. The unicast and anycast IPv6 addresses consists of three fields, an n-bit routing, an m-bit subnet ID field and a 64-bit interface identity field (Figure 79).



**Figure 79 – IPv6 unicast address structure**

The 64-bit interface ID is either:

- derived from the interface's IEEE 802.3 MAC address using the EUI-64 format;
- obtained from a DHCPv6 server (using prefix delegation or not);
- auto configured randomly; or
- assigned manually.

NOTE Regarding the usage of EUI-64, see the EUI-64 guidelines of IEEE RA (<http://standards.ieee.org/develop/regauth/tut/eui64.pdf>).

The global unicast addresses are administrated by IANA through RIRs.

### 7.7.1.3.3.3 IPv6 subnets

There are no subnet masks in IPv6. IPv6 replaces subnet masks by the root address and the number of most significant identical bits. [RFC 5942] explains the differences between the IPv4 subnet mask and the IPv6 prefix.

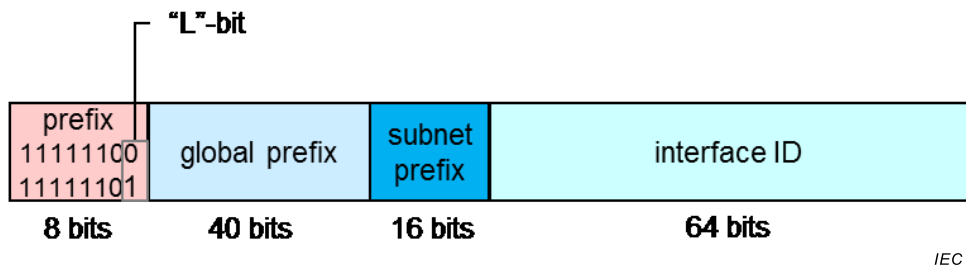
Example: fc00::/7 represents all addresses whose first 7 bits are “1111 110”.

### 7.7.1.3.3.4 IPv6 unique local unicast (ULA) addresses

[RFC 4193] defines two address blocks, taken from the fc00::/7 block, distinguished by the “L-flag” bit (Figure 80):

fc00::/8 (“L-flag” bit set to ‘0’); or

fd00::/8, (“L flag” bit is set to ‘1’).



**Figure 80 – IPv6 ULA address structure**

The “L flag” is set to one if the prefix is locally assigned (this corresponds to the most common rule)

ULA addresses are routable within a private network.

#### 7.7.1.3.3.5 IPv6 local addresses

The link-local IPv6 address (Figure 81) has a prefix of fe80::/10 according to RFC 4291.



**Figure 81 – IPv6 link local address structure**

Link-local addresses are for use on a single link, they are not routable.

#### 7.7.1.3.4 IPv6 fragmentation and packet size

IPv6 allows MTUs well in excess of the Ethernet frame size (jumbo frames) on a hop-to-hop basis, but IEC TR 61850-90-5 rules them out.

The minimum datagram that all IPv6 hosts must be capable to accept has a size of 1 280 octets.

IPv6 allows fragmentation only at hosts (including tunnelers), not at the intermediate routers as IPv4 does [RFC 4944].

IPv6 requests that a node is capable of MTU path discovery [RFC 1191], i.e. to detect which is the MTU size of all entities in the end-to-end path.

IPv6 end points will not agree on an MTU that is smaller than 1 280 octets.

#### 7.7.1.3.5 IPv6 auxiliary protocols

IPv6 comes with a suite of auxiliary protocols, in particular:

- Internet Control Message Protocol version 6 (ICMPv6) [RFC 4443] replaces ICMPv4, is it a mandatory component without which IPv6 does not work; It is a transport layer protocol on the same layer as TCP or UDP.

- Neighbor Discovery Protocol for IPv6 (NDPv6) [RFC 4861] provides Stateless Address AutoConfiguration (SLAAC). NDP replaces IPv4's ARP and ICMP, it is part of ICMPv6.
- DHCPv6 [RFC 3315] and DHCPv6lite [RFC 3736] extend DHCP.
- Internet Protocol Security (IPsec) [RFC 4301] makes use of the security headers Authentication Header (AH) [RFC 4302] and Encapsulating Security Payload (ESP) [RFC 4303]. This protocol suite partially applies to IPv4 also. IPsec support is mandatory in IPv6, but its use is not.
- A number of routing protocols have been adapted for IPv6, with no technological change (only the format of the exchanged information changes). In addition to OSPF routing, the IS-IS routing is gaining popularity.
- 6LoWPAN provides IPv6 support over low power and lossy networks.
  - [RFC 4944] specifies fragmentation;
  - [RFC 6282] obsoletes the header compression mechanism specified in [RFC 4944];
  - [RFC 6775] provides an adaptation of NDP for 6LoWPAN networks.

#### 7.7.1.3.6 IPv6 routing

IPv6 uses the same protocols as IPv4 for routing, for example OSPF or IS-IS.

#### 7.7.1.4 Comparison IPv4 and IPv6

##### 7.7.1.4.1 Main differences

Table 42 summarizes the main differences between IPv4 and IPv6:

**Table 42 – Differences between IPv4 and IPv6**

Property	IPv4	IPv6
Address size	32 bits	128 bits
Address resolution	ARP	NDP
Header length	variable, containing transport protocol indication	fixed size
Optional headers	none	optional extension headers to indicate transport protocol
Header compression	none	allowed
IP header checksum	yes	none
Fragmentation	by intermediate routers	only by hosts or network nodes in host mode
Security support (IPsec)	IPsec optional	IPsec support mandatory, use optional
Routing protocols	unspecified: OSPF, IS-IS, etc., but not RPL	OSPFv3, RPL and other protocols adapted to IPv6
ICMP	ICMPv4	ICMPv6 (mandatory)

##### 7.7.1.4.2 IPv4 to IPv6 address mapping

##### 7.7.1.4.3 IPv4 and IPv6 address classes

Both IPv4 and IPv6 operate with a fixed address size. This makes the handling of the different address sizes the most difficult issue in the migration from IPv4 to IPv6.

NOTE IPv4 addresses can be extended by including the port addresses, but this works only for TCP and UDP (nevertheless more than 99,9 % of Internet traffic).

Table 43 compares the addresses in IPv4 and IPv6.

**Table 43 – IPv6 versus IPv4 addresses [RFC 4291]**

Address scope	IPv4	IPv6 [RFC 4291]
Unspecified	0.0.0.0	::
Loopback	127.0.0.0/8	0::1
Multicast	224.0.0.0/4	ff00::/8
Link Local –only valid on a link –never routed, –traffic local to the link	169.254.0.0/16	fe80::/10 (auto-configured)
Private address space –never routed outside a private domain	10.0.0.0 /8, (24-bit block) 172.16.0.0 /12 (20-bit block) 192.168.0.0 /16 (16-bit block)	fc00::/7 fd00::/8 pseudorandom fc00::/8 user specific (ULA) [RFC 4193]
Global Address –public and routable registered to a RIR	all other	2000/3
Broadcast	255.255.255.255	ff02::1 (not recommended)

#### 7.7.1.4.4 Address representation in IEC 61850

The Substation Configuration Language (SCL) [IEC 61850-6] represents IPv6 addresses as the following XML code example shows:

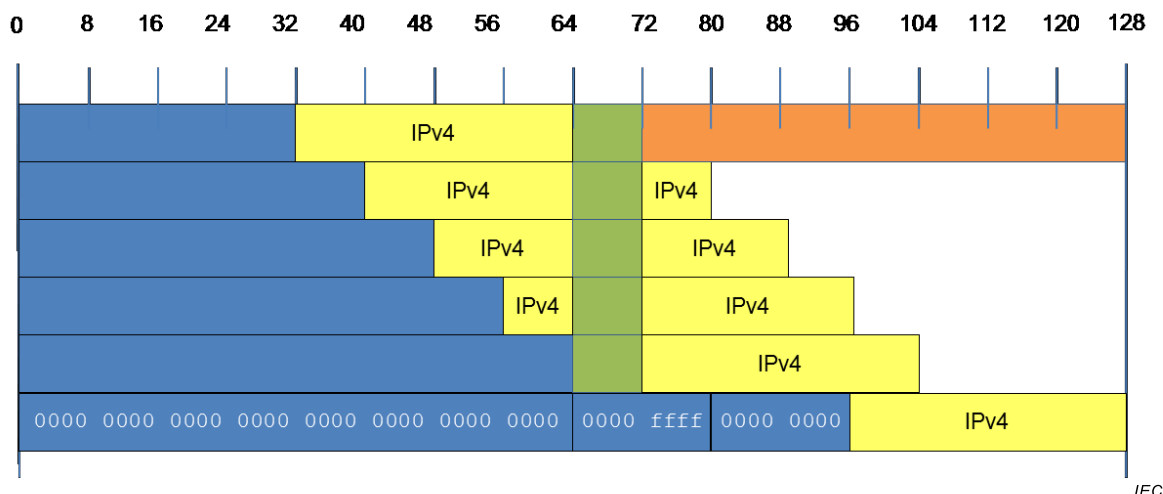
```
<Address>
<P type="IP">2001:0db8:85a3:0000:0000:8a2e:0370:7334</P>
<P type="IP-SUBNET">/56</P>
<P type="IP-GATEWAY">2001:0db8:85a3:0000:0000:8a2e:0370:0001</P>
<P type="OSI-AP-Title">1,1,999,1,1</P>
<P type="OSI-AE-Qualifier">12</P>
<P type="OSI-PSEL">00000001</P>
<P type="OSI-SSEL">0001</P>
<P type="OSI-TSEL">0001</P>
</Address>
```

A device may have both an IPv4 and an IPv6 address (and may have several addresses):

```
<Address>
<P type="IP" xsi:type="tP_IP">2001:0db8:85a3:0000:0000:8a2e:0370:7334</P>
<P type="IP-SUBNET" xsi:type="tP_IP-SUBNET">/56</P>
<P type="IP-GATEWAY" xsi:type="tP_IP-GATEWAY">2001:0db8:85a3:0000:0000:8a2e:0370:0001</P>
<P type="IP" xsi:type="tP_IP">10.0.0.11</P>
<P type="IP-SUBNET" xsi:type="tP_IP-SUBNET">255.255.255.0</P>
<P type="IP-GATEWAY" xsi:type="tP_IP-GATEWAY">10.0.0.101</P>
<P type="OSI-AP-Title" xsi:type="tP_OSI-AP-Title">1,1,999,1,1</P>
<P type="OSI-AE-Qualifier" xsi:type="tP_OSI-AE-Qualifier">12</P>
<P type="OSI-PSEL" xsi:type="tP_OSI-PSEL">00000001</P>
<P type="OSI-SSEL" xsi:type="tP_OSI-SSEL">0001</P>
<P type="OSI-TSEL" xsi:type="tP_OSI-TSEL">0001</P>
</Address>
```

#### 7.7.1.4.5 IPv4 to IPv6 recommended address mapping in IEC 61850

[RFC 6052] defines several mappings from IPv4 to IPv6, but recommends not to use “::ffff:0:0/96” (the bottom one in Figure 82) that RFC 2765 recommends.



**Figure 82 – Mapping of IPv4 to IPv6 addresses**

IPv4 – IPv6 protocol translation faces the problem that protocols such as UDP and TCP embed the IP addresses in their checksums. Therefore, the UDP and TCP checksums would need adjustment if the address changes. To ease migration from IPv4 to IPv6, RFC 6052 proposes a “checksum neutral” translation, in the form of the construct “64:ff9b::” closed by the IPv4 address.

Example:

```
64:ff9b::/96 | 172.16.2.33 |
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
0000'0000'0110'0100'1111'1111'1001'1101'0000'0000'0000'0000'0000'0000'0000'0000
0000'0000'0000'0000'0000'0000'0000'0000'1010'1100'0001'0000'0000'0010'0010'0001
```

There is no way to assign automatically IPv6 addresses to IPv4, except by restricting the address space of IPv6 to a subnet with a 32-bit address, which defeats IPv6's purpose.

Statically configured address translation may be used.

Every translation beyond this requires identification of the partners by a universal name (e.g. URL) resolved by a DNS (or statically configured out of a database). A DNS in IPv6 responds to a request with an AAAA record, that contains the 128-bit IPv6 address.

#### 7.7.1.4.6 IPv6 address plan

The IPv6 address plan is related to the network part of the addresses (64 most significant bits). The host part is always 64 bit long. There is no address plan defined for the host part.

All current substations use IPv4 private addresses belonging to the groups:

```
10.xx.xx.xx /8,
172.32.xx.xx /11,
192.168.xx.xx /16
```

To remain non-routable over a public IPv6 network, these addresses should be mapped to IPv6 ULA addresses “fd00::/8” or “fc00/8” (conserving the checksum over the TCP/UDP pseudo-header).

The IPv6 address space affects engineering of a network. The network partition becomes flexible, i.e., there are no subnet masks any more. The selection of prefixes replaces subnetting.

NOTE In substation automation, the established static assignment of IPv4 addresses based on the physical topography relative to a plant, as defined in IEC TR 61850-90-4 can be kept with IPv6, provided a suitable prefix is used before the topography suffix.

When the devices are IPv6-enabled, they no longer need NATs (7.7.6.2).

A utility can segment its private address space (ULAs) geographically for the operational network, for instance as:

<operational><region><substation><voltage level><bay><IED>

The IPv6 address plan is related to the network part of the addresses (64 most significant bits). The host part is always 64 bit long. There is no address plan defined for the host part.

The amount of bits for the least significant part of the network part can be identical to that of IPv4 in IEC TR 61850-90-4, while the most significant bits can be allocated flexibly, the number of substations per region and the number of regions varies from utility to utility.

The same schema can be used:

- for Virtual Power Plants: <operational><region><wind park><turbine><IED> or
- for Smart Grids: <operational><region><sector><block><house><IED>

The enterprise network can be segmented differently from the operational network.

### **7.7.1.5 From IPv4 to IPv6**

#### **7.7.1.5.1 IPv4 to IPv6 evolution**

Due to the exhaustion of the 32-bit IPv4 addresses, the public Internet is moving towards IPv6, which offers a practically unlimited address space of 128 bits.

IPv6 is growing rapidly and many new devices support it. A large number of servers still operate with IPv4.

Figure 83 shows the probable evolution of the IPv6 traffic in the public internet. Around the year 2030, there should be only a few IPv4-only nodes around, many of them in private networks.



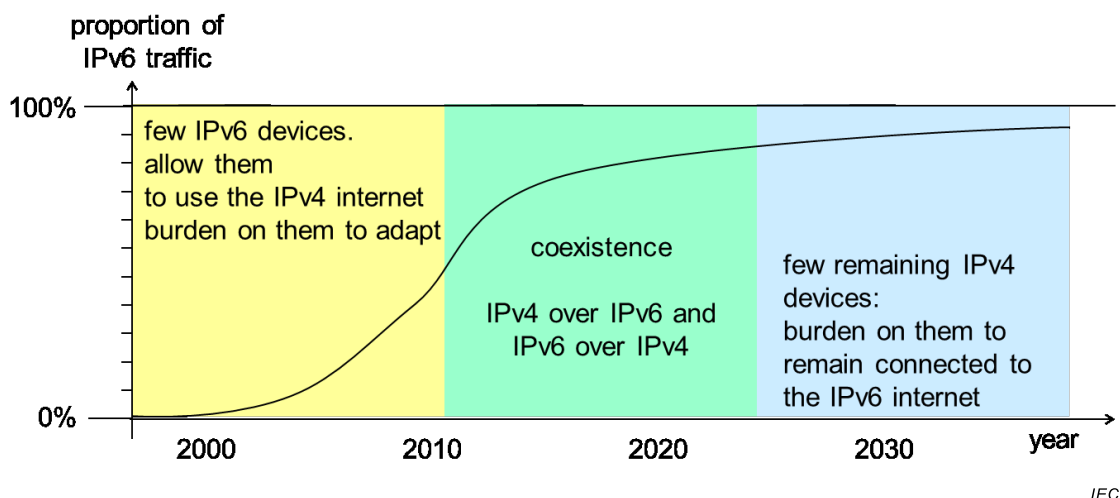


Figure 83 – IPv6 evolution

#### 7.7.1.5.2 IPv4 to IPv6 migration

IPv6 is growing rapidly and most new devices support it, but a large number of servers still operate with IPv4 only. IETF devised migrations strategies [RFC 4213].

Two different migrations are considered:

a) application migration:

applications currently written for IPv4 are migrated to IPv6, while possibly preserving compatibility with IPv4 devices. Examples are engineering tools, debug and traffic monitoring tools, protection applications. This involves reprogramming and re-engineering of devices while preserving the application code.

b) device and system migration:

- new IPv6 devices must be able to operate over the IPv4 infrastructure;
- installed IPv4 devices, including routers, must be able to interoperate with IPv6 devices;
- installed IPv6 must not disturb the operation of already installed IPv4 devices;
- new devices should access IPv4 and IPv6 devices (dual-stack);
- IPv4-only devices must be accessible over an IPv6-only network (tunnel or translator).

IEC TR 62357-200 defines guidelines for migration.

#### 7.7.1.5.3 IEC 61850 stack with IPv4 and IPv6

Figure 84 shows the location of IPv4 and IPv6 in the IEC 61850 stack. In principle, the protocols on top of IPv4 | IPv6 should not be aware of the communication stack used and the layers below IP (link layer, PRP, HSR) and in particular all hard protocols of the hard real-time stack are not affected.

However, over a WAN, it is not possible to route directly Layer 2 traffic. This traffic can be tunneled over IP as described in IEC TR 61850-90-1 and IEC TR 61850-90-5.

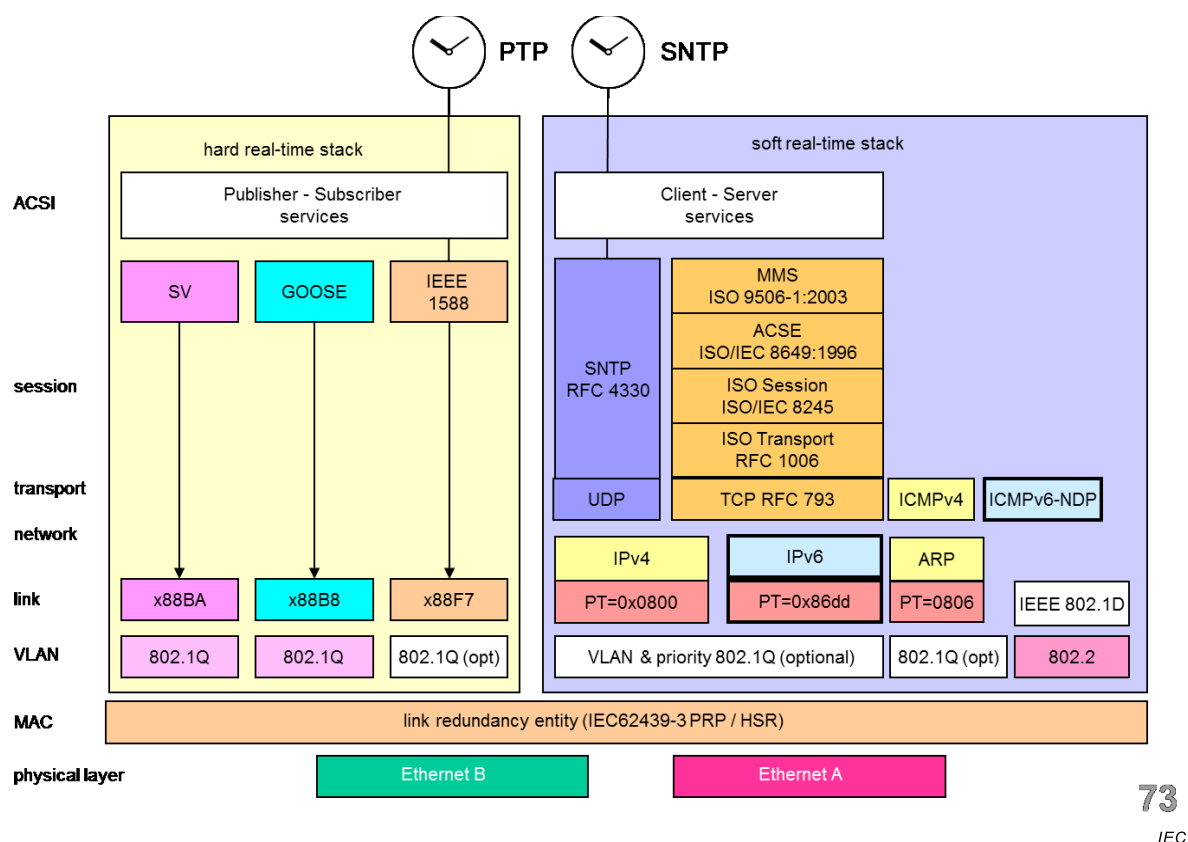


Figure 84 – IEC 61850 stack with IPv4 and IPv6

## 7.7.2 IP QoS

### 7.7.2.1 IP-Intrinsic QoS

IP is a PSN and relies on QoS to ensure that time-critical data are transmitted timely, see 5.2.

IP networks rely on priorities. While protocols exist to reserve resources, their implementation remains proprietary.

### 7.7.2.2 IP QoS methods

QoS in an IP based network consists in managing and classifying network traffic. Access Routers (Client Edge) implement this service based on requests of the end devices.

Routers can give a higher priority to some kind of traffic, see 5.3 and reserve resources.

IP considers two basic QoS methods, which both use the Type of Service (ToS) bits in the IP header (same for IPv4 and IPv6), but in a different way:

- Integrated Services (IntServ) [RFC 2210], [RFC 2211] and [RFC 2212] and
- Differentiated Services (DiffServ) [RFC 2474]

### 7.7.2.3 IntServ

IntServ is a QoS method that prioritizes IP packets through a network scheduler in each node.

The resources in the routers (bandwidth, processing, queues, etc.) are allocated per connection or “flow” and not per packet class.

IntServ uses RSVP, in which a node asks all routers in the path to reserve resources (processing time, buffers) for its traffic. If all respond positively, a QoS agreement is valid for the duration of the connection.

IntServ uses the ToS field in the IP packets to specify the Traffic Descriptor (TSPEC) and the Reservation Characteristics (RSPEC).

Although IntServ permits control of QoS, it is today obsolete. In fact, IntServ breaches the connectionless nature of IP routers in that it imposes them a knowledge of the flow to which a packet belongs, leading to stateful routers, and poorly scalable.

#### **7.7.2.4 DiffServ**

##### **7.7.2.4.1 DiffServ principles**

DiffServ allows the end application to mark and assign packets to a specific priority class. Each router handles and manages network traffic according to this classification, with no memory of the flow to which it pertains (stateless router).

Within utility automation architecture, DiffServ is used on the substation access routers (Client Edge) as well as on the Control Centre access router (Customer Edge). DiffServ is seldom used within substations (see IEC TR 61850-90-4:2013, Annex D, for such a case).

As an example, an access router will assign pre-allocated bandwidth accordingly. With DiffServ, policy definition and classification are enforced at the DiffServ domain boundaries, typically on the access router.

##### **7.7.2.4.2 DiffServ packet classification**

Packets entering a DiffServ domain or region (collection of DiffServ routers) can be classified in a variety of ways – including Layer 4 protocol and port numbers, IP precedence, and Layer 2 information (such as Ethernet 802.1Q VID and priority). Once these packets are classified, they can be processed, conditioned and marked.

##### **7.7.2.4.3 DiffServ packet marking**

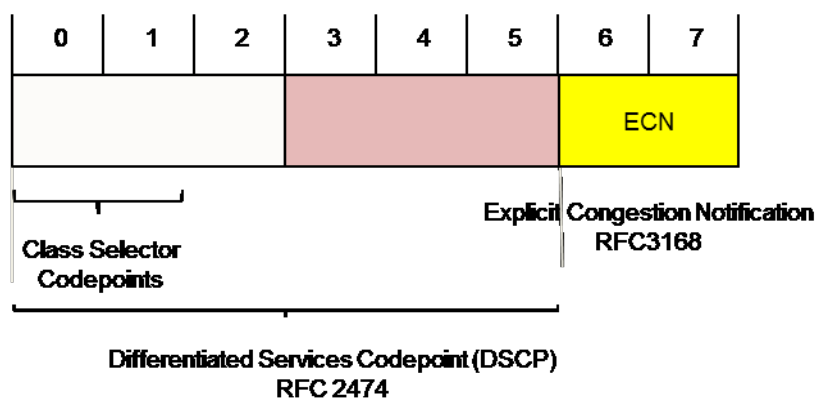
DiffServ redefined the IPv4 ToS octet in the IP header (Figure 77) from the 3-bit IP-precedence to a 6-bit DSCP field (see Figure 85), allowing to distinguish 64 classes of traffic.

The packet classification determines the router's treatment of the packet as Per-Hop Behavior (PHB) including:

- Assured Forwarding (AF) [RFC 3260], which allows carving out the bandwidth between multiple classes in a network according to the desired policies.
- Expedited Forwarding (EF) [RFC 3246/RFC 3247] characterizes traffic with the lowest latency, jitter and assured bandwidth services which are suitable for applications such as voice transmission.

Packets can be marked with an arbitrary or predefined standard DSCP value, corresponding to the appropriate AF, EF or user defined class (see Table 44).

For example, the codepoint "101110" designates EF. The codepoint "000000" designates "best-effort traffic".



IEC

Figure 85 – DiffServ codepoint field

Table 44 – List of DiffServ codepoint field values

Name	Dec	ToS	Binary
AF11	10	40	001010
AF12	12	48	001100
AF13	14	56	001110
AF21	18	72	010010
AF22	20	80	010100
AF23	22	88	010110
AF31	26	104	011010
AF32	28	112	011100
AF33	30	120	011110
AF41	34	136	100010
AF42	36	144	100100
AF43	38	152	100110
CS1	8	32	001000
CS2	16	64	010000
CS3	24	96	011000
CS4	32	128	100000
CS5	40	160	101000
CS6	48	192	110000
CS7	56	224	111000
EF	46	184	101110
default	0	0	000000
AF = Assured forwarding			
EF = Expedited forwarding			
CS = Class Selector			

#### 7.7.2.4.4 DiffServ congestion control

The two least significant bits of the ToS field are used for congestion control [RFC 3168].

### 7.7.3 IP multicast

While multicast is the rule in substation local area networks, and represent the bulk of the traffic (GOOSE and SMV), it is much more difficult to use multicast in WANs due to the large number of devices involved, and broadcast would flood the network.

However, applications in power systems use the same process data (e.g. circuit breaker status, voltage and current values) and IP multicast allows the transmission of IP packets from a single sender to multiple receivers.

IEC TR 61850-90-5 also provides a use case of IP multicast from the PMUs. Except in special cases (redundancy), multicast applies only to UDP traffic (see 7.7.6.2) since acknowledged multicast costs a large overhead.

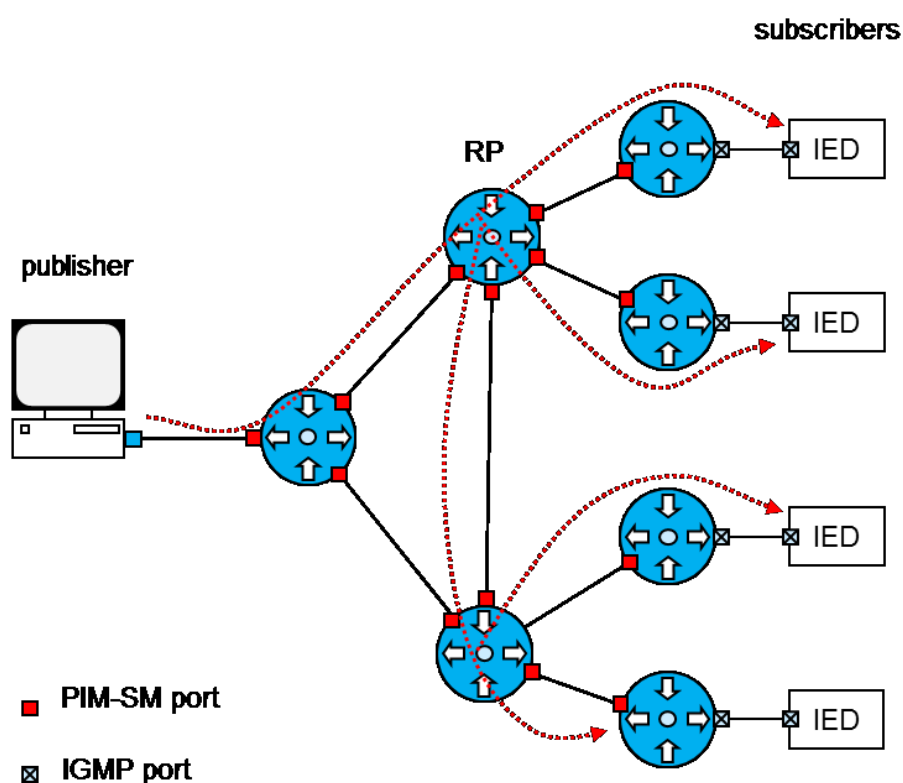
The Protocol Independent Multicast protocol – Sparse Mode (PIM-SM) [RFC 4601] is one of the IP multicast protocols. It is used where hosts are scattered over a wide area.

The functional elements of PIM-SM are the publisher, the subscribers and RP (Rendezvous Point).

A subscriber transmits a request message to a publisher to join a multicast group through the Internet Group Management Protocol (IGMP) [RFC 3376]

IGMP is executed by publishers, subscribers and Layer 3 routers in the network. IGMP allow joining the multicast group, leaving the multicast group and managing the multicast group members.

The RP receives data transmitted from the publisher and distributes it to many subscribers (1:N) (Figure 86).

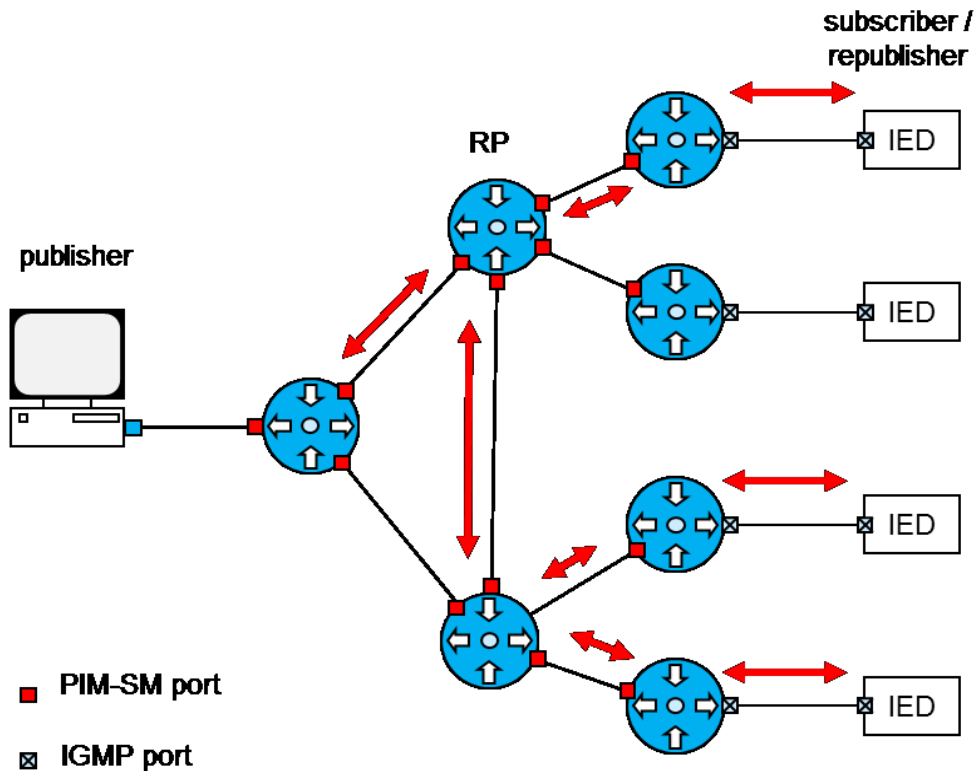


IEC

Figure 86 – Unidirectional protocol independent multicast

Bi-directional PIM (BIDIR-PIM) is available for many-to-many (N:N) connections [RFC 5015]. This protocol is capable of transmitting from many publishers to many subscribers.

The bidirectional IP Multicast scheme is useful for a decentralized computing application where each IED sends its data to other IEDs, all the IEDs process the data, and then each IED sends back the processed result to others (Figure 87).



**Figure 87 – Bidirectional protocol independent multicast**

#### 7.7.4 IP redundancy

IP provides redundancy against router failures or link failures by rerouting the packets.

If IP bases on robust Layer 2 technology providing redundant paths, Layer 2 can hide communication failures.

In case of router failure, IP provides redundancy through the Virtual Router Redundancy Protocol (VRRP) [RFC 5798].

IP fast reroute (FRR) [RFC 5286] provides redundancy against link and router failures, attempting to achieve 50 ms depending on topology (preferably rings).

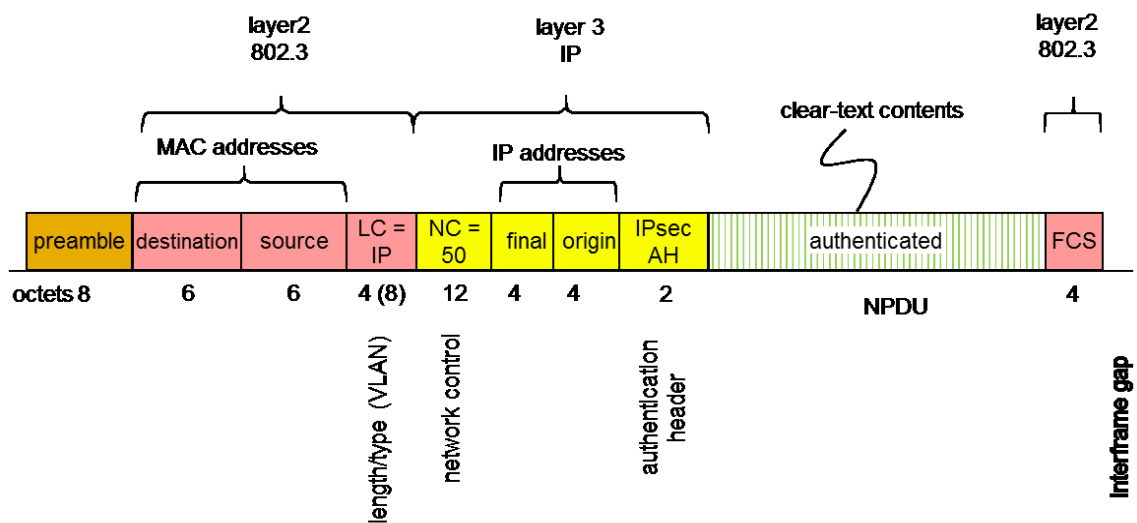
#### 7.7.5 IP security

IPsec is a security protocol for Layer 3 that defends the NPDU. It carries a security checksum between the network and the transport header; the information that comes after it is either authenticated (AH) or encrypted (ESP).

In IPv4, IPsec lies somehow between Layer 3 and Layer 4, while in IPv6 it is part of the network header. IPsec carries the transport protocol identifier that IP would carry in its absence.

IPsec supports two modes: transport and tunnel:

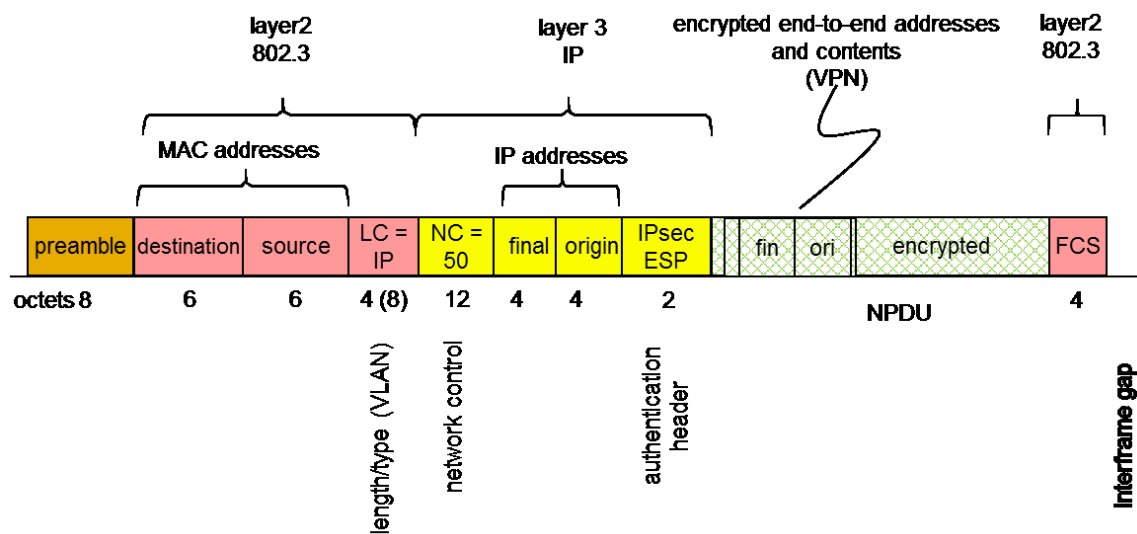
- IPsec transport encrypts the messages except headers, addresses and routing information. This is acceptable for a peer-to-peer scenario, for instance, between a client and a server. Figure 88 shows the frame format for authentication.



IEC

Figure 88 – Frame format for IPsec (authenticated)

- IPsec tunnel mode encrypts the whole IP packet and inserts its own header. This mode allows to tunnel packets securely from one domain (e.g. substation) to the other (e.g. SCADA). In this case, the NPDUs contains a whole IP packet with origin and final IP addresses which are distinct from the IP addresses uses for the transport over the IPsec-defended segment (Figure 89). This way, the IP addresses of the end user remain hidden. IPsec in tunnel mode implements a VPN, see 7.11.



IEC

Figure 89 – Frame format for IPsec (encrypted)

The exchange of cryptographic keys for IPsec is detailed in 7.12.2.2.

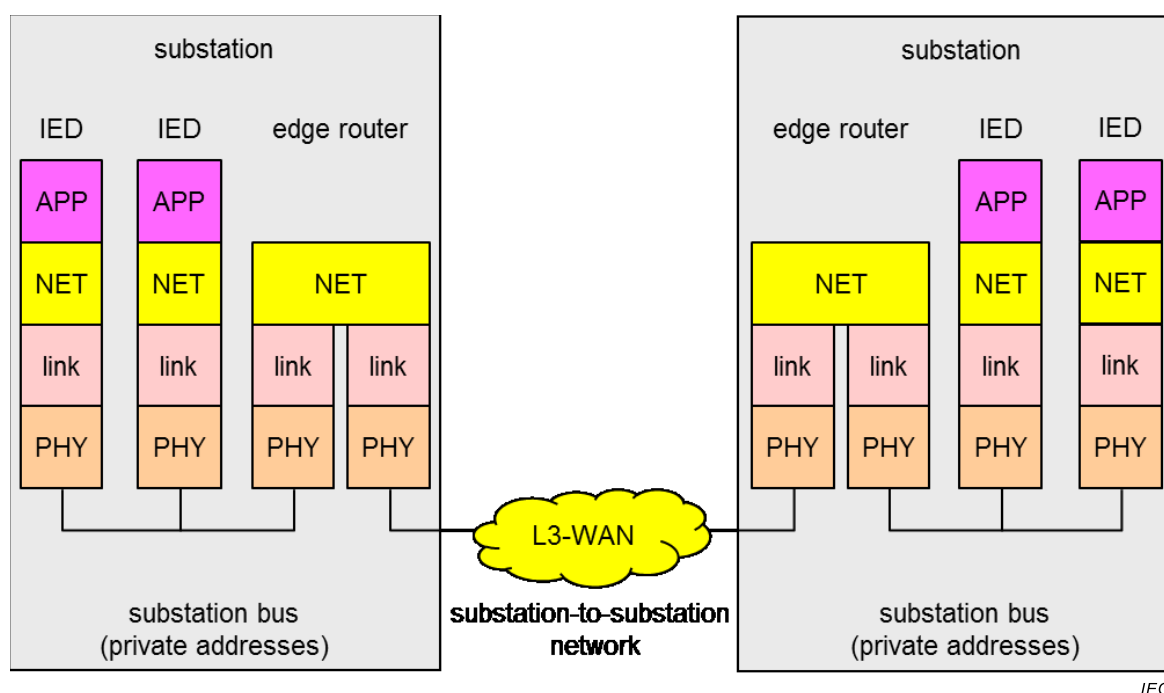
## 7.7.6 IP communication for utilities

### 7.7.6.1 IP direct communication

Within a substation, IEC 61850-8-1 specifies Layer 3 communication for the substation objects (MMS) and time distribution (SNTP). Other protocols using Layer 3 communication that IEC 61850 does not explicitly mention are file transfer (FTP), network management (SNMP), web interface (HTTP) and the Layer 3 support protocols (e.g. ICMP).

Outside of the substation, connection to RTUs base on DNP3 or IEC 60870-5-104, which also use TCP/IP. However, this traffic does not necessary share the Station Bus.

The use of Layer 3 allows in principle direct access from the network external to the substation to all substation devices, when both share the same address space (Figure 90).



**Figure 90 – Layer 3 direct connection within same address space**

### 7.7.6.2 IP remote access by NAT

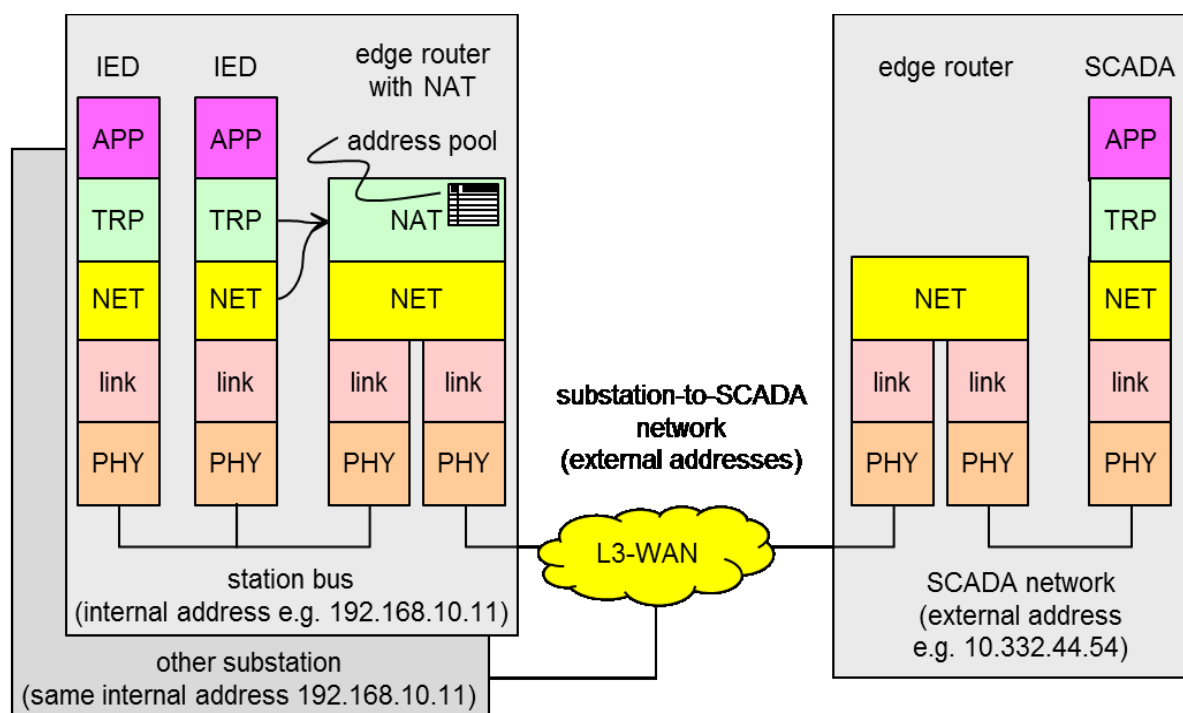
Within a substation, devices use IPv4 with a private address space as proposed in IEC TR 61850-90-4, which is not routable outside of a private domain.

The IEC TR 61850-90-4 address scheme allows assigning an IP address to the different IEDs according to their geographical position in the substation. The same IP address could appear in different substations, so these addresses are unsuited for substation-to-substation communication.

To allow network access from outside the substation, the edge router has a NAT that owns a pool of global addresses. These addresses are not necessarily public internet addresses, in most cases, there will be enterprise addresses taken from the company's address space (e.g. 10.x.x.x). Only a few communications go the public internet. There will be another NAT in the network connected to the public internet, probably with stricter security policies.



Figure 91 shows the protocol stacks involved in the translation of substation-internal addresses to external IP addresses for access to a SCADA network using external addresses.



IEC

**Figure 91 – Connecting substations to SCADA by a NAT**

For access outside of the substation, a NAT maps the internal addresses to external addresses.

To this purpose, the edge router includes a NAT with a pool of external IP addresses that it will map to internal, private addresses.

The network engineer can allocate global addresses to the internal addresses. This involves more than just address translation.

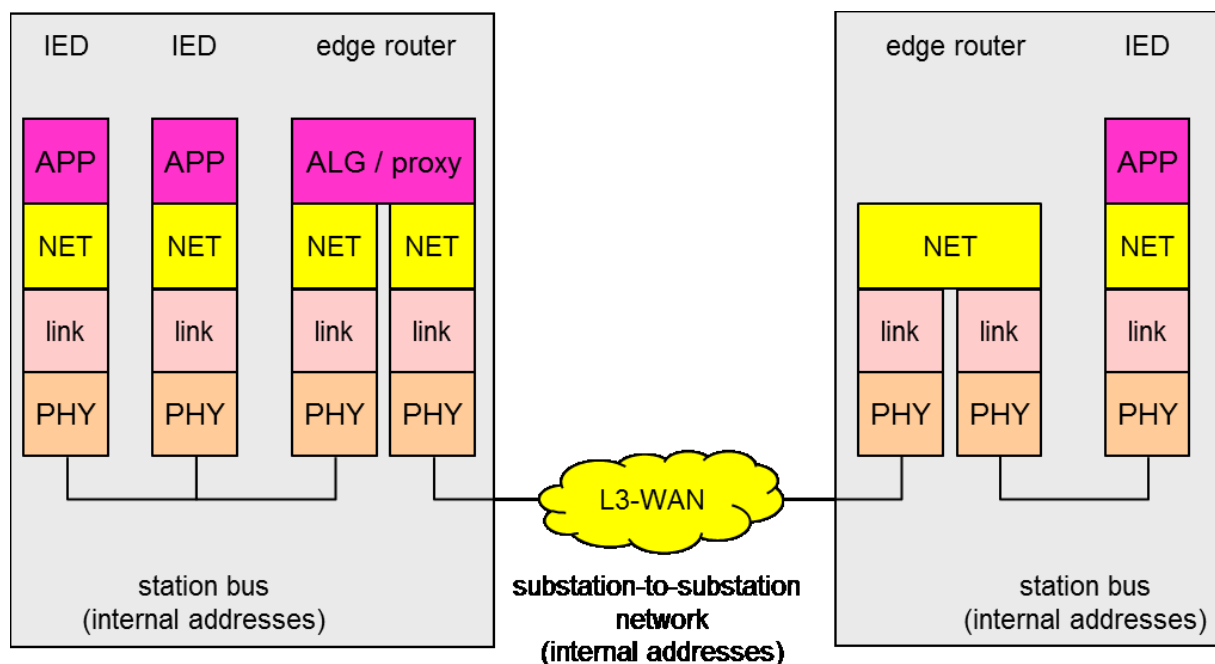
If an independent operator operates the external network, it may require using IPv6 for communication. In this case, the edge router must in addition convert the IPv6 into IPv4 addresses and vice-versa. This translation is detailed in 7.7.1.5.3.

A dynamic allocation of addresses (e.g. by DHCP) is not advisable since the IEDs are by definition servers that need a fixed address assigned by the SCD. Tying the IP address to the MAC address as IPv6 foresees for auto configuration would cause problems when exchanging the device hardware.

Translating private addresses into network addresses is not always advisable. Network engineers should consider that remote direct access to all devices within a substation presents a security issue, even if no evil action was intended.

Therefore, it is advisable to use proxies for network access that only allow a controlled access to the substation and only makes those objects visible that require it, according to the “need-to-know” principle. This leads to the structure of Figure 92, which shows the connection of a remote SCADA or engineering station to a substation.

The substation is visible only through the ALG, which manages a pool of public IP addresses. The ALG mimics an individual access to the IEDs, but the structure of the substation can be different and the ALG can block information that should not be known outside. The SCADA side (or maintenance side) does not need an ALG.



IEC

**Figure 92 – Substation to SCADA connection over ALG**

Although the network communication controller or SEN is a logical host for the ALG, the ALG functionality could be located at any appropriate device in the substation, for instance the substation controller.

If the ALG is dual stack IPv4/IPv6, it can translate between IPv4 and IPv6, but only for objects managed by the ALG.

### 7.7.7 IP summary

Table 45 summarizes the IP technology.

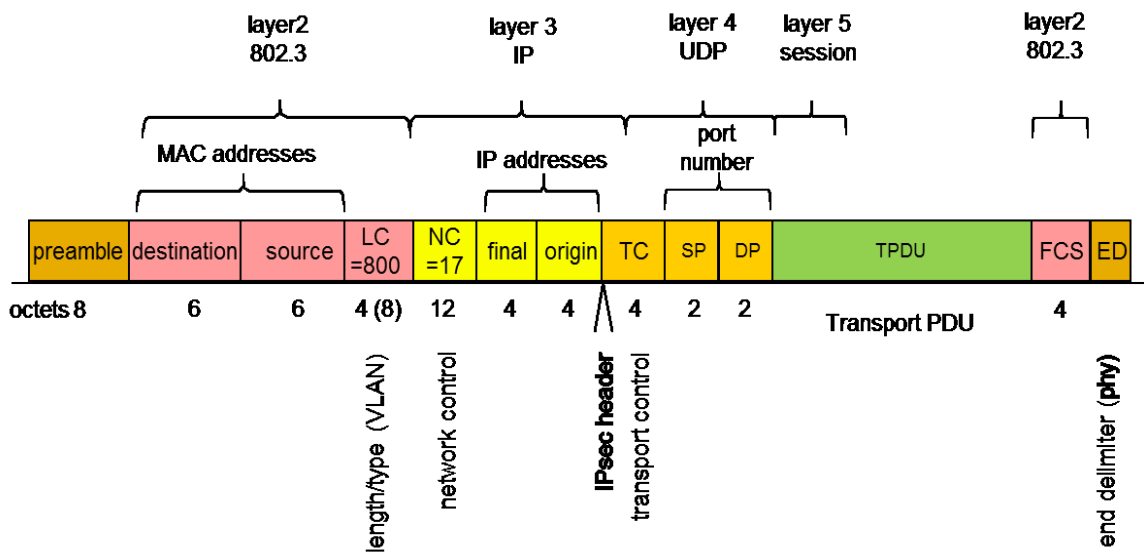
**Table 45 – IP Summary**

Feature	Comments
Acceptance	Well known and understood, used since 40 years
Bandwidth Efficiency	High – bandwidth can be shared over different paths
Routing	Unpredictable without traffic engineering
Traffic engineering	QoS mechanisms IntServ and DiffServ, resource reservation allow to prioritize traffic
Configuration	Automatic (OSPF, BGP...)
Recovery	Disaster-tolerant, redundant paths 50 ms recovery delay in special topologies (FRR) Without special measures, several seconds of recovery delay.
Latency and jitter	No upper bound
VPN	Numerous techniques available
Application	Non time-critical, wide area networks

7.8 Layer 4 (transport) protocols

7.8.1 Transport layer encapsulation

The transport layer cares for end-to-end flow control and error recovery. The transport header follows the network header and precedes the transport payload (TPDU) (Figure 93).



IEC

Figure 93 – Ethernet frame with UDP transport layer

The two main transport protocols in use are:

- User Datagram Protocol or Unacknowledged Datagram Protocol (UDP) [RFC 0768] and
- Transport Control Protocol (TCP) [RFC 0793]

The user will see only TCP and UDP as services. Auxiliary protocols have their own transport (e.g. ICMP, IS-IS).

7.8.2 UDP

UDP provides best-effort-to-deliver but no flow control and error recovery. It is stateless and therefore offers the same service as a Layer 2 transmission. Delivery time is subject to the delay variations due to the routing. Applications sensitive to latency such as voice over IP (VoIP) use the Real Time Protocol (RTP) on top of UDP in combination with de-jittering and packet re-ordering.

UDP is typically used to achieve short response time (Figure 94),

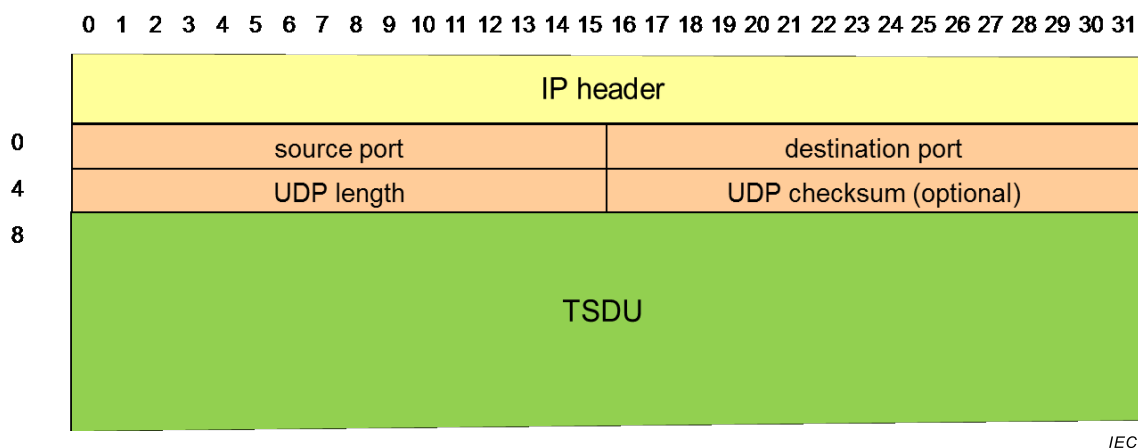


Figure 94 – UDP header

### 7.8.3 TCP

TCP offers end-to-end flow control and error recovery through retransmission. The time constants of recovery are in the range of seconds, making it unsuitable for real-time transmission (Figure 95).

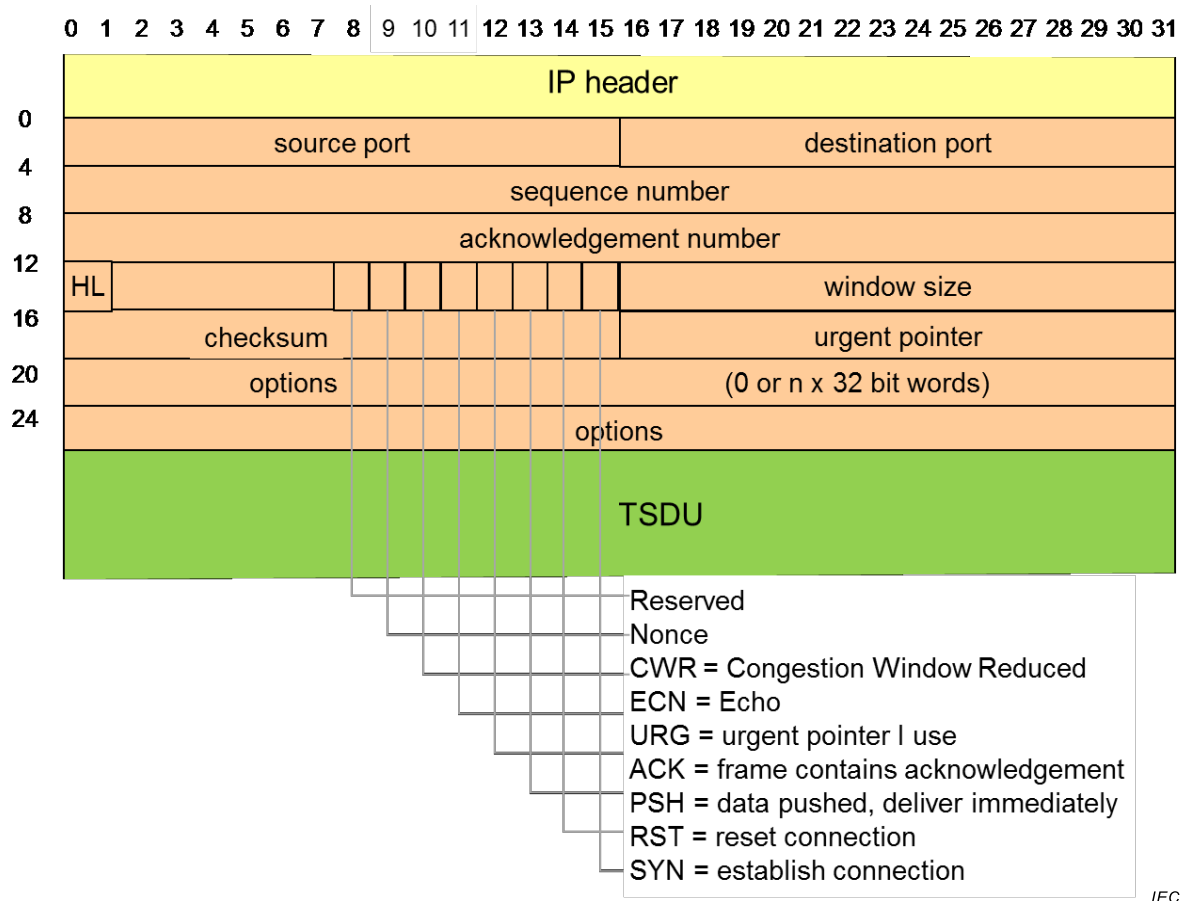


Figure 95 – TCP header

NOTE In IEC 61850-8, the Client/Server MMS protocol bases on TCP, while the routable protocols for GOOSE and SMV in IEC TR 61850-90-1 use UDP.

#### 7.8.4 Layer 4 redundancy

There exists no proper Layer 4 redundancy, but Layer 4 protocols such as TCP support redundancy of the network layer through packet numbering, which discards duplicates in the TCP engine.

NOTE Multipath TCP [RFC 6824], an ongoing IETF standardization, provides path redundancy (among other features).

UDP has no such sequence number and therefore the application layer has to care of possible duplicates.

NOTE IP provides a 16-bit packet numbering to support fragmentation, which is unique per {source address, destination address protocol} [RFC 6864]. This identification could be used for redundancy, provided the end nodes implement it even if they do not support fragmentation.

#### 7.8.5 Layer 4 security

Layer 4 security applies from port to port in the UDP and TCP protocols.

The Transport Layer Security (TLS) [RFC 5246] is a widely used method of securing network traffic in order to prevent eavesdropping and tampering. TLS is a cryptographic protocol which runs on top of the Transport Layer, i.e. on top of TCP. It supersedes the SSL protocol, as RFC 6176 states.

NOTE Nevertheless, the term SSL/TLS often appears.

TLS uses X509 certificates and asymmetric cryptography to enable authentication and to exchange a symmetric key used for encrypting data during transmission.

TLS is not an appropriate protocol to defend UDP/IP traffic. In this case, Datagram Transport Layer Security (DTLS) [RFC 6347] is applied.

Several use cases based on TLS are relevant for TC57 WAN communication (7.12.2.3). TLS is widely used to secure remote engineering and configuration access to IEDs and other system and devices that employ web based applications.

NOTE Sometimes, TLS is considered as a session protocol, the distinction is however academic.

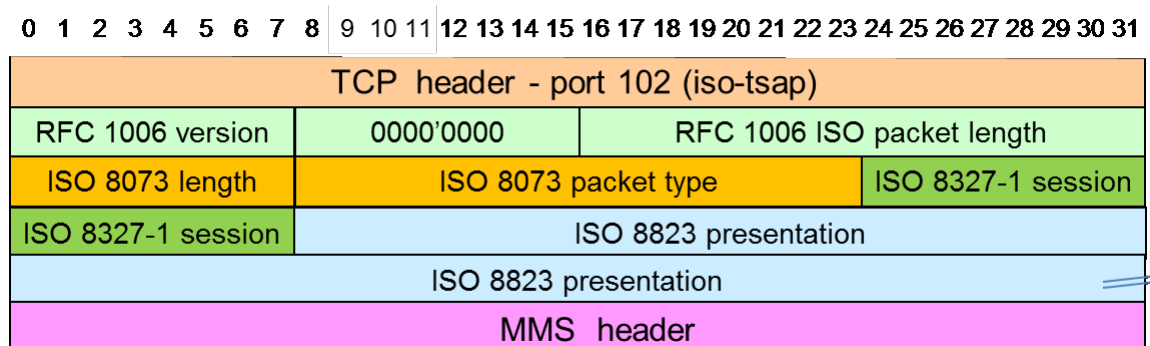
The exchange of cryptographic keys for TLS is detailed in 7.12.2.2.

### 7.9 Layer 5 (session) and higher

#### 7.9.1 Session layer

The session layer (defining the beginning and end of a stream of transport packets) defined in ISO/OSI as Layer 5 is seldom used in the Internet protocols, delegating this function to the application.

As an exception, the MMS protocol uses a session layer because it originally bases on ISO/OSI and ITU-X protocols. To keep compatibility, IEC 61850 introduced a shim layer between OSI/ISO protocols on TCP over port 102 [RFC 1006]. This interface is stateless and costs only a few octets of overhead (Figure 96).

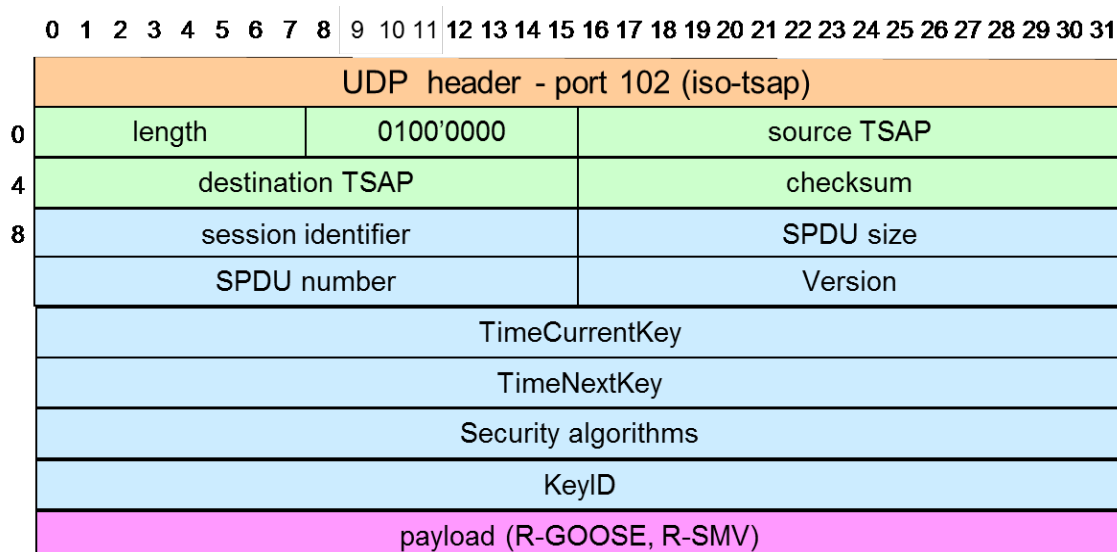


IEC

**Figure 96 – Session and presentation layers for MMS**

### 7.9.2 Routable GOOSE and SMV

IEC TR 61850-90-5 uses the same stack as MMS for transmitting synchrophasors, but over UDP port 102 so it can use the multicast RFC 1240 shim layer to carry the ISO traffic (Figure 97).



IEC

**Figure 97 – Session and presentation layers for R-GOOSE**

Both RFC 1006 and RFC 1240 are protocol overlay as will be further developed in 7.10.

IEC TR 61850-90-5 supports both a direct and a tunnel mode (see Figure 102).

### 7.9.3 Example: C37.118 transmission

Legacy protocols such as IEEE C37.118 can be directly transmitted from port to port; this is a raw socket application.

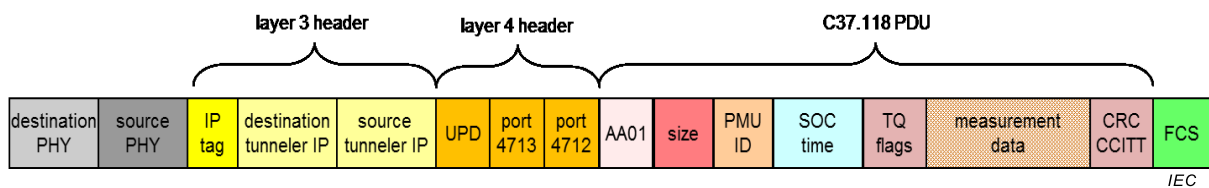


Figure 98 – IEEE C37.118 frame over UDP

7.9.4 Session protocol for voice and video transmission

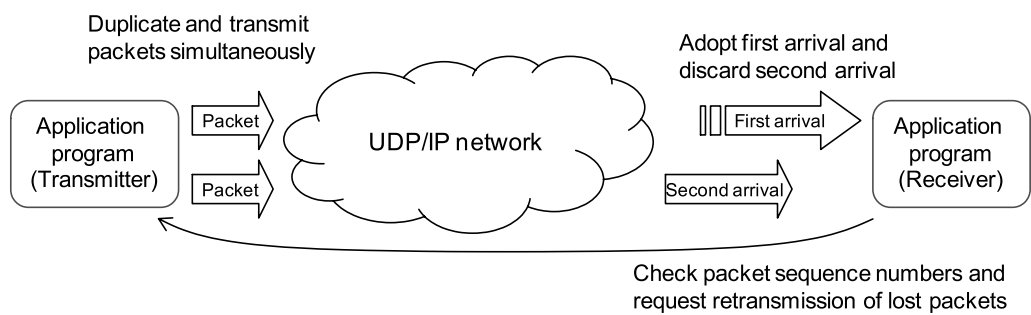
Although not an IEC 61850 protocol, voice and video are important operational data streams. Telephony over the IP protocol is widely in use, since it allows building cost-effective PABX with off-the-shelf computers. The Session Initiation Protocol (SIP), specified in RFC 3261, allows opening streaming sessions for voice, video and instant messaging, in unicast and in multicast. It can run on TCP, UDP and on the Stream Control Transmission Protocol.

NOTE Voice and video are more tolerant to a poor QoS than teleprotection applications.

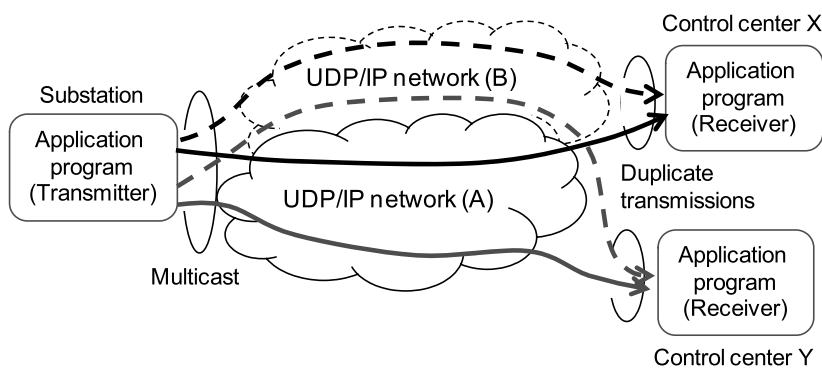
7.9.5 Application interface redundancy

IEC TR 61850-90-2 shows examples of application interface redundancy, in which the application choses explicitly between different communication paths available to it.

Figure 99 [7] shows an example of redundancy in the end-to-end application layer using multicast duplicate transmission and retransmission mechanisms.



(a) Duplicate transmission and retransmission



(b) Multicast and duplicate transmission for multiple locations

Figure 99 – Redundant network transmission handled by the application layer

Application layer redundancy is problematic since it requires the application to be aware that it is redundant and that its partner is possibly also redundant. Handling of IP addresses pairs is clumsy. When several applications share the same hardware, it makes little sense to let every application with different criteria for switchover. In addition, switchover time is dictated by time-outs and unspecified criteria.

Therefore, the application should not address network reliability problems, but only application redundancy, see 7.9.6.

### **7.9.6 Application device redundancy**

Application interface redundancy does not help against failure of the device that executes the application, or against faults in the application itself (such as programming errors). To address this, device redundancy is necessary.

Although device redundancy is not properly a network redundancy issue, the network has to support the application device redundancy, especially by providing the same information to all redundant units and by allowing cross-synchronization and actualization of the redundant units and teaching of the newly inserted spares.

A particular problem is that the sender of the messages must be aware that its destination has changed and that the replacement partner has another IP address.

To avoid this, the stand-by unit could, upon detection of the failure of the on-line unit, take over its IP address and request a reassignment of the IP address to the MAC address (e.g. with an unsolicited ARP in IPv4). The recovery delay can be larger than what most applications expect.

Examples of this appear in IEC TR 61850-90-2.

## **7.10 Protocol overlay – tunneling**

### **7.10.1 Definitions**

Protocol overlay is the transport of one protocol over another, also called tunneling.

The transported protocol can be of a higher, same, or lower layer protocol.

The transport of higher layer protocols over a lower layer is not generally regarded as tunneling.

Layer 3 protocols may also be transported over another Layer 3 protocol, e.g. IPv4 over IPv6.

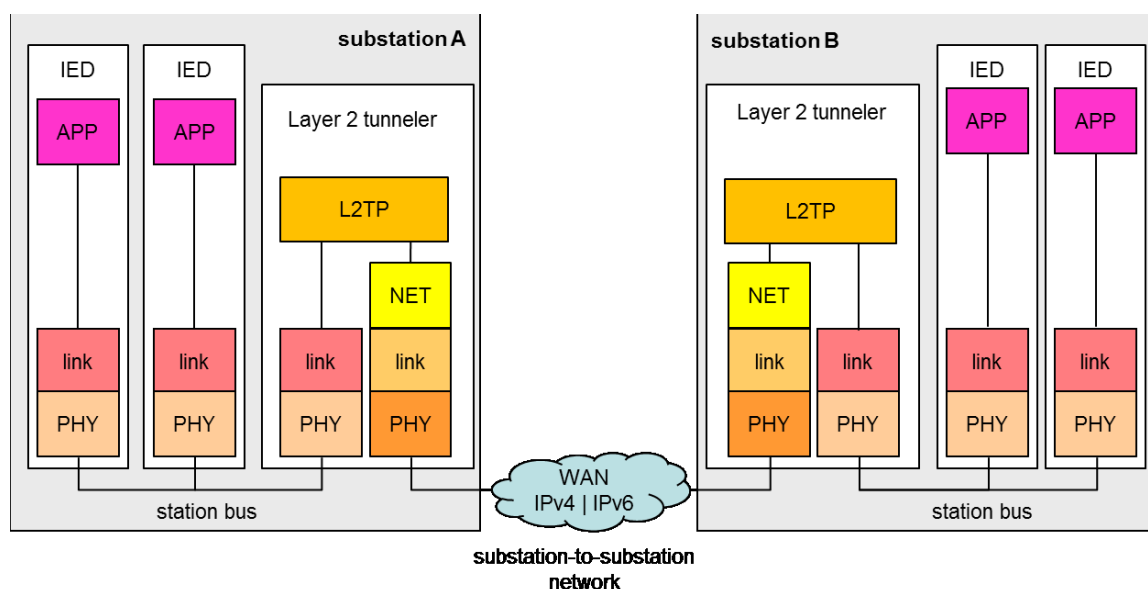
Different types of Ethernet services can be offered over a Layer 2.5 or Layer 3 transport, for instance using SDH/SONET, IP/MPLS or Carrier Ethernet Transport (PBB).

The MEF defined names:

- Ethernet Private Line (EPL): connecting two specific Ethernet ports
- Ethernet Virtual Private Line (EVPL): like the EPL but capable of transporting multiple individual EPL services
- Ethernet Private LAN (EVP-LAN): connecting a set of Ethernet ports creating the appearance of all ports being connected to a single LAN
- Ethernet Private Tree (EVPT): point to multipoint connection using VLAN configuration for multicast services







IEC

**Figure 101 – L2TP transporting Layer 2 frames over IP**

#### 7.10.4 Use Case: Tunneling GOOSE and SMV in IEC 61850

IEC 61850-8-1 and IEC 61850-9-2 specify Layer 2 communication for GOOSE and SMV messages. Other protocols that rely directly on Layer 2 services are IEC 61588 and LLDP.

These Layer 2 protocols operate with MAC addresses, they may include a VLAN tag as address extension, but they ignore network addresses.

In addition, message payloads may carry additional addressing information that will be considered, especially when crossing the substation boundaries.

When going out of the substation to a WAN, the options are:

- a) Forward directly the Layer 2 messages from one terminal to the others over a Layer 2 link (Figure 60), with a Layer 2 being:
  - a Layer 2 direct link (e.g. a dark fiber in an earthing cable), or
  - a switched Ethernet network or
  - a Layer 2 emulation over another network.
- b) Encapsulate Layer 2 information at one terminal into Layer 3 packets in a Layer 2 tunneler and deliver them as Layer 2 information at the other end, emulating a Layer 2 connection. The network addresses used are known only to the tunneler and invisible on the station bus.

Since the Layer 2 frames are in principle delivered identically to the other terminal in both cases, the engineer has to ensure either that the address space is common or that the address spaces are properly separated (see 7.6.4.12).

IEC TR 61850-90-1 does not specify the tunnel, but only models the tunneler.

IEC TR 61850-90-5 (see 7.9.2) specifies a tunnel protocol for synchrophasors, GOOSE and SMV based on the ISO/OSI Connectionless Transport Layer (not widely used outside of Utility Automation), which is a tunnel protocol including security (Figure 102). The tunneler is particular to the IEC 61850 protocols.

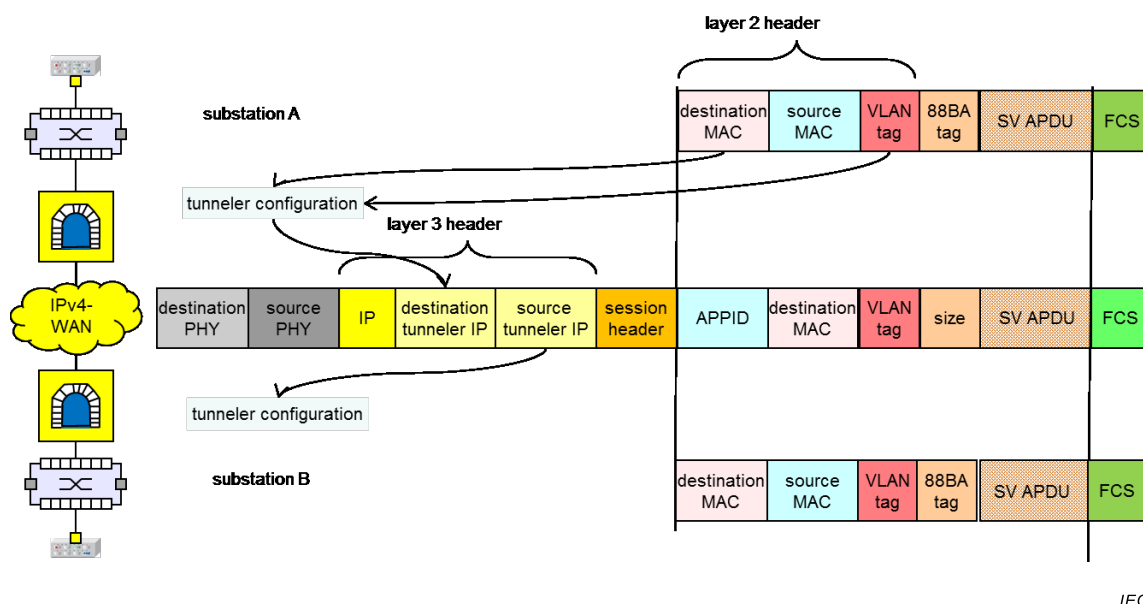


Figure 102 – Tunneling GOOSE over IP in IEC TR 61850-90-5

### 7.10.5 Circuit emulation service (CES)

#### 7.10.5.1 CES definition and pseudo-wire emulation

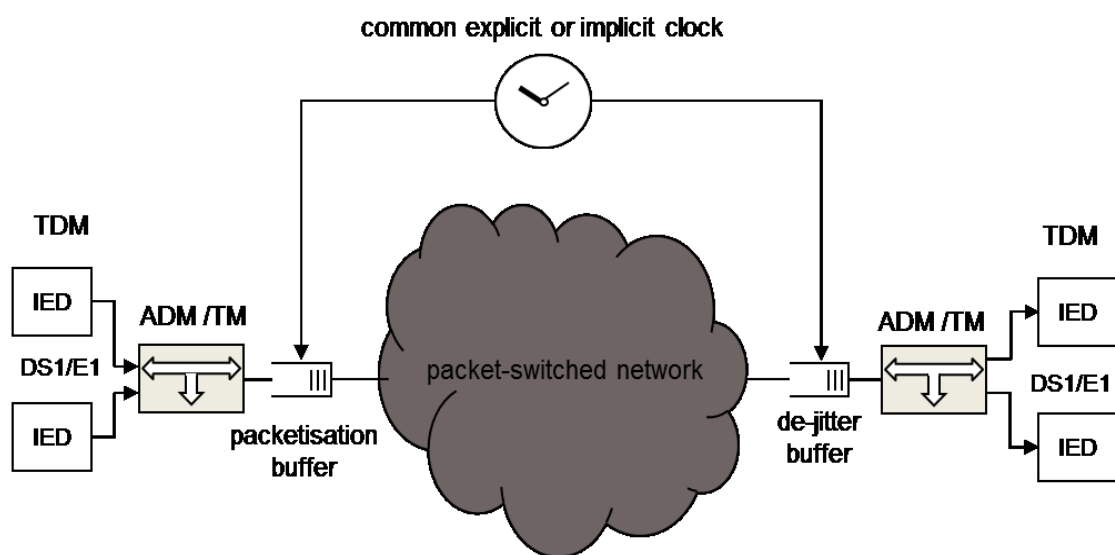
At the beginning of packet traffic, protocol overlay was about transporting packets on top of TDM services (EoSDH, POS, etc.). After the breakthrough of PSN, the game reverses: to support legacy SDH/SONET devices and provide telephone services, packet networks have to support virtual circuit with strict timing requirements, so-called pseudo-wires.

SDH/SONET traffic may be transmitted over a packet-switched network such as IP using a variety of protocols, in particular SAToP, CESoPSN and TDMoIP.

The transport of telephony channels over a packet switched network aims at providing the same QoS as a TDM system would. While CES easily emulates the logical behavior, it can only imperfectly emulate the timing behavior of the statistical nature of PSN. Achieving this behavior is called a “pseudo-wire” or “C-pipe”. Implicit clocks (using clock recovery) or explicit clocks (e.g. GPS clocks at the termination points or clock distribution based e.g. on IEC 61588) allow to reach the same level of timing behavior as in end-to-end TDM networks.

This behavior is what one would expect from VoIP.

Figure 103 shows the principle of pseudo-wire. The TDM traffic from one access TDM network arrives in the packetization buffer, waiting for the packets to be enough filled for transmission. The PSN forwards these packets with a variable (but bound) latency to the de-jitter buffer at the other access network side. The packets are not immediately unpacked and transmitted, but stored in the de-jitter buffer. The de-jitter buffer reconstructs a TDM behavior based on the worst expected latency on the PSN. To this effect, it might use an implicit clock, derived from the traffic it receives, or an explicit clock if global clock exists or if the PSN provides a precision clock. For the TDM equipment on the destination side, the latency is always constant and equal to the worst expected latency of the PSN.



IEC

Figure 103 – Pseudo-wire principle

#### 7.10.5.2 PWE3

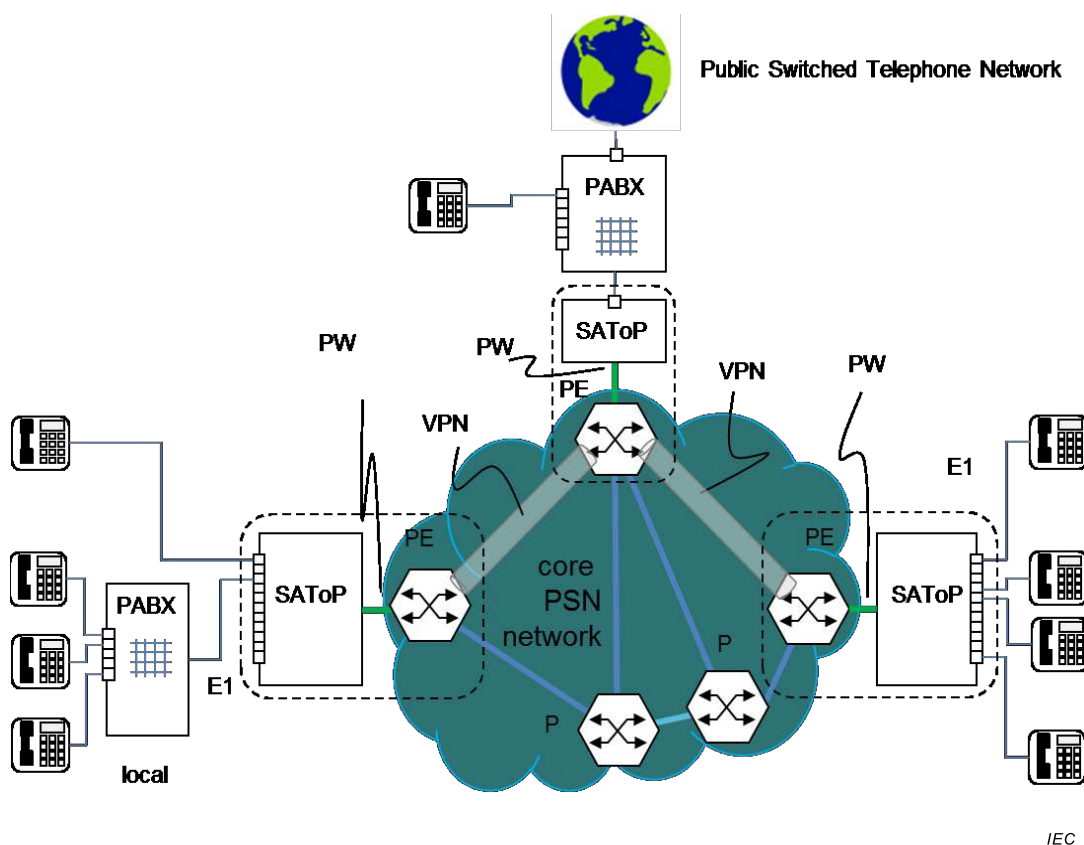
IETF standardized pseudo-wires under the title “Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture” [RFC 3985], which specifies the emulation of services such as Frame Relay, ATM, Ethernet, TDM, and SDH/SONET over PSNs using IP or MPLS.

- IETF RFC 3985 (PWE3)
- IETF RFC 4197 (Edge-to-edge emulation of TDM circuits over PSN)

A typical “pseudo-wire” system for non-IP telephony is shown in Figure 104.

The known solutions are:

- PE routers with integrated SAToP (and/or CESoPSN) functionality
- TDM-to-IP/Ethernet gateways with Circuit Emulation based on SAToP (and/or CESoPSN)



**Figure 104 – Non-IP voice communication over PSN**

#### 7.10.5.3 SAToP

Structure-Agnostic TDM over Packet (SAToP) [RFC 4553] carries unframed E1/T1 or E3/T3 flows over IP, MPLS or Ethernet with no regard to the TDM slot structure. This simple method suits applications where the provider edges do not interpret TDM data or do not participate in the TDM signaling. SAToP requires that the PSN have almost no packet loss and very low jitter.

The SAToP standards are:

- IETF RFC 4553 (SAToP)
- ITU-T Y.1413 (TDM-MPLS network interworking)
- ITU-T Y.1453 (TDM – IP interworking)
- MEF 8 (Emulation of PDH Circuits over Metro Ethernet Networks)
- MFA 8.0.0 (Emulation of TDM circuits over MPLS using raw encapsulation)

#### 7.10.5.4 CESoPSN

CES over Packet network (CESoPSN) [RFC 5096] transports structured E1/T1 or E3/T3 data flows on IP, MPLS or Ethernet packets with static assignment of timeslots inside a bundle according to the following standards:

- IETF RFC 5086 (CESoPSN).
- ITU-T Y.1413 (TDM-MPLS network interworking)
- ITU-T Y.1453 (TDM – IP interworking)
- MEF 8 (Emulation of PDH Circuits over Metro Ethernet Networks)
- MFA 8.0.0 (Emulation of TDM circuits over MPLS using raw encapsulation)

The TDM structure must be chosen for proper payload conversion such as the framing type (i.e. frame or multiframe). This method is less sensitive to PSN impairments but lost packets could still cause service interruption.

#### 7.10.5.5 TDMoIP

TDM over IP is the transport of E1/T1, E3/T3, STS-1 and other serial flows over IP, MPLS or Ethernet.

It supports E1/T1 structured or unstructured mode according to the following standards:

- IETF RFC 5087 (TDMoIP)
- ITU-T Y.1413 (TDM-MPLS network interworking)
- ITU-T Y.1453 (TDM – IP interworking)
- MEF 8 (Emulation of PDH Circuits over Metro Ethernet Networks)
- MFA 4.1 (TDM Transport over MPLS Using ATM Adaptation Layer 1)

Some consider TDMoIP as the preferred choice over CESoPSN in terms of bandwidth efficiency, packet loss, signaling and congestion avoidance. However, TDMoIP pays it with a higher computational complexity.

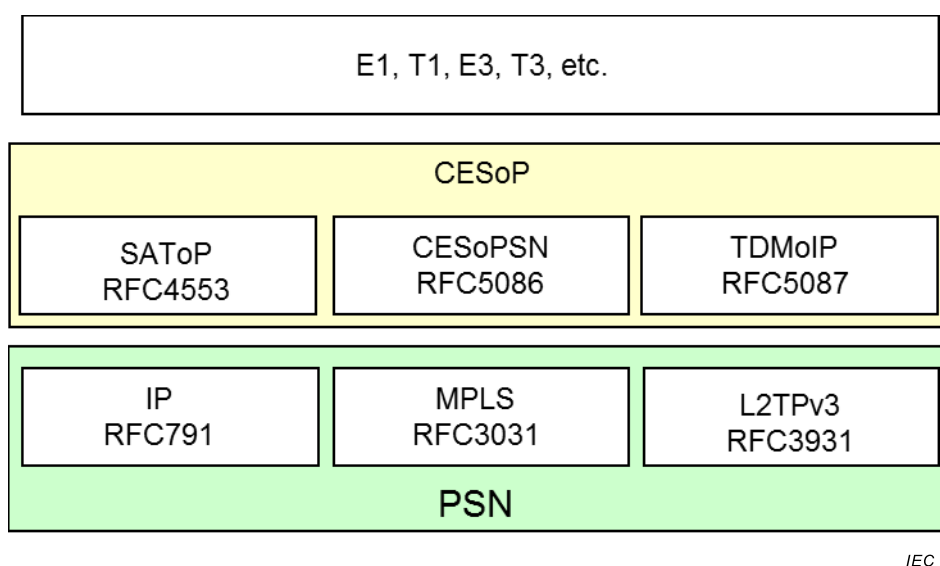
#### 7.10.5.6 Clock recovery

A particular problem of CES is the recovery of the clock according to which the original data were sampled.

Although several schemes exist that recover the clock from the packet stream, it is preferable to synchronize the pseudo-wire endpoints from a common clock source in the WAN.

#### 7.10.5.7 Comparison of PW over PSN

Figure 105 shows the protocol layering of the three CES over PSN.



IEC

**Figure 105 – Circuit emulation over PSN**

Table 46 compares the pseudowire protocols.

**Table 46 – Pseudowire protocols**

Technology	TDM service supported	Advantages	Disadvantages	Standards
SAToP	Unframed	Low overhead lowest end-to-end delay	TDM service is susceptible to frame loss and out-of-sequence  No DS0 grooming available	RFC 4553  ITU-T Y.1413, ITU-T Y.1453
TDMoIP	Unframed; Framed, channelized	Complete support of TDM services in one protocol	Higher delay when transporting several time slots due to $n \times 48$ octet frames	RFC 5087
CESoPSN	Framed, channelized	Lower packetization delay when transporting several time slots (DS)	No support for unframing, use SAToP instead	RFC 5086

## 7.11 Virtual Private Networks (VPNs)

### 7.11.1 VPN principles

Virtual Private Networks span several completely disjoint logical networks over a shared physical network, e.g. over SDH/SONET, Layer 2 Ethernet, IP/MPLS or MPLS-TP.

VPNs allow separating classes of traffic, each with its own QoS.

Disjoint means that the address space of the VPNs are separate: one VPN cannot address objects from another VPN and the same address may appear in different VPNs, but with another owner.

Private means complete separation of the VPNs, e.g. by interface separation at access side, addressing (e.g. VLAN tags, MPLS labels) and encapsulation.

NOTE “Private” comes from the transport of private (e.g. enterprise) communication over public networks.

Within a VPN, routing takes place independently from the shared physical network, i.e. the logical topology may be different.

Tunneling is one of the methods to build VPNs.

VLANs allow implementing VPNs by properly configuring the bridges. This is used in Q-in-Q and PBB (see 7.6.8).

VPNs are categorized in Layer 2 VPNs (L2VPN) and Layer 3 VPN (L3VPN).

VPNs can run with or without encryption, encryption is not necessary for separation.

### 7.11.2 L2VPNs

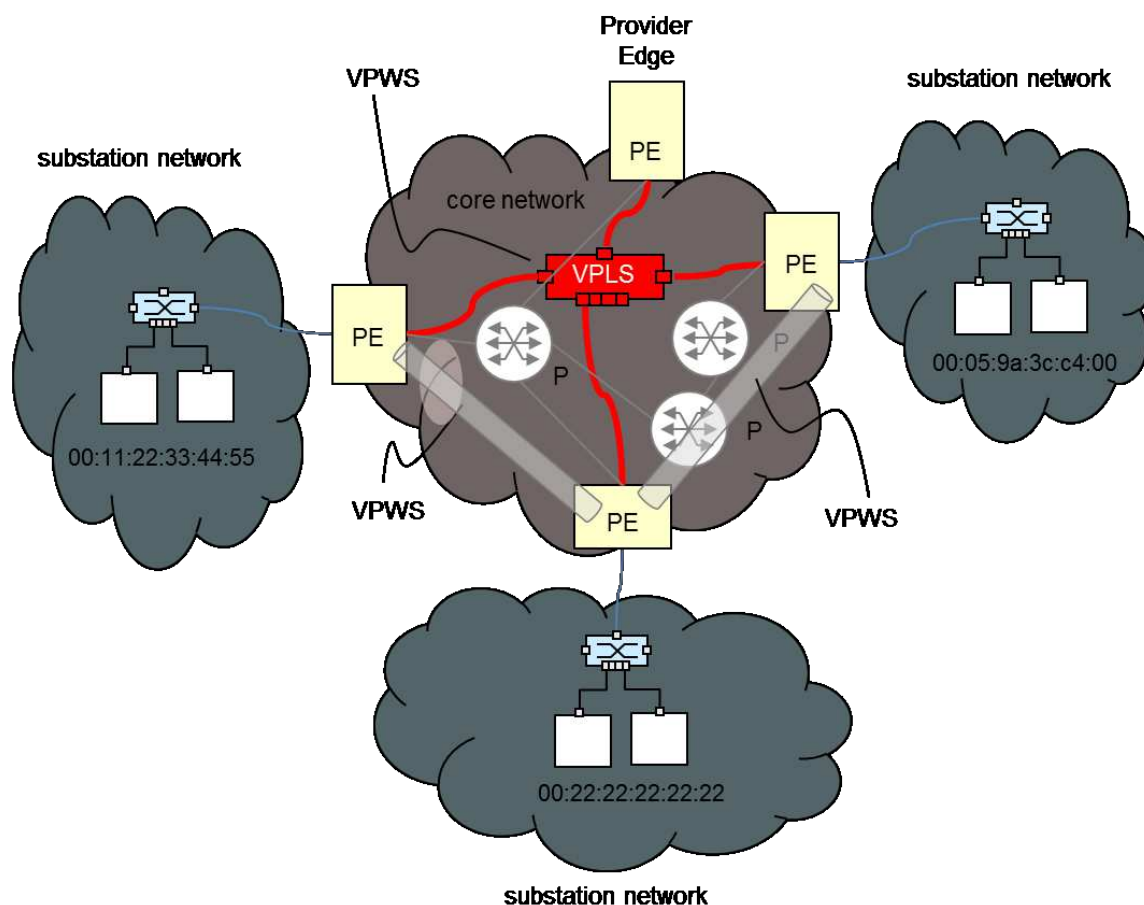
A L2VPN extends the Layer 2 address space over another network.

A core network may offer three L2VPN services [RFC 4664]:

- Virtual Private Wire Service (VPWS) emulates an Ethernet point-to-point Layer 2 link over a shared network; on top of this, services that require only point-to-point communication may be emulated.

- Virtual Private LAN Service (VPLS) emulates an Ethernet multipoint Layer 2 connection over a shared network. VPLS provide Ethernet multipoint connectivity to sites, as if they were connected using a LAN with broadcast or multicast messages. This means that intermediate nodes can prevent loops and optimize traffic
- IP-only LAN-like Service (IPLS) emulates an IP service including routing on top of a shared network (IPLS is ignored here since it is seldom used)

Figure 106 shows a conceptual view of VPWS and VPLS. The VPLS “bridge” is a virtual device and the VPWS “pipe” is a virtual link; they symbolize a function carried out by the PE nodes and the intermediate P-nodes.



IEC

**Figure 106 – L2VPNs VPWS and VPLS**

L2VPNs make it possible to operate private, multipoint, and point-to-point LANs through wide area networks. L2VPNs provide usually Ethernet-like LAN services.

NOTE TDM protocols are carried usually over pseudowire emulation services (PWE3) based e.g. on SAToP or CESoPSN. This service is different from L2VPN but can run in parallel on the same underlying physical network (e.g. MPLS-based).

L2VPNs also overcomes the limit in network segmentation explained in 7.6.6.4.

The provider network is involved in the customer routing. The protocol used is for instance RFC 2547bis (Layer 2 MPLS-VPN).

When the underlying network is MPLS, an additional label in the label stack identifies each VPN, the outer label is used for label forwarding in the network; the inner label is not used in the core but addresses the VPN services at the PE.



### 7.11.3 L2VPN multicast on MPLS

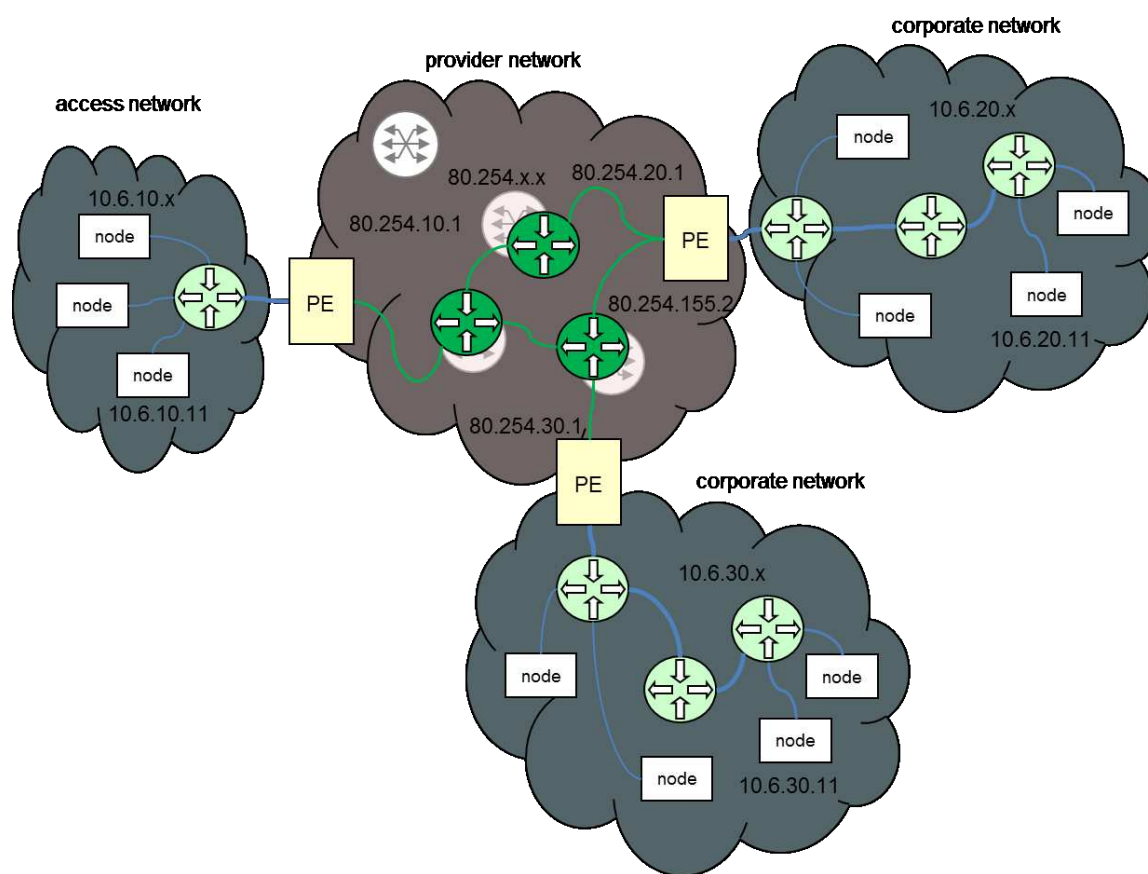
MPLS implements VPWS and VPLS in an efficient way using label stacking.

### 7.11.4 L3VPN

#### 7.11.4.1 L3VPN General

A L3VPN connects multiple IP address domains over an underlying network. Like any Layer 3 protocol, it provides routing on the base of IP addresses and does not forward the MAC addresses. Figure 107 shows a VPN established between three domains that share the IP group 10.6.x.x, connected by VPN over a provider that operates with public addresses of the 80.254.x.x. group.

L3VPNs provide unicast as well as multicast services, using the capabilities of the underlying IP networks or MPLS networks.



IEC

**Figure 107 – L3VPN**

The routers within the provider network and/or in the customer edge operate both with the provider network IP addresses and with the carried IP addresses.

Each L3VPN has its own routing. This means that the routers in the network implement several virtual routers, one for each L3VPN, each having its own forwarding information base.

#### 7.11.4.2 L3VPN on MPLS

L3VPNs on MPLS are also known as Virtual Private Routed Network (VPRN) [RFC 4364].

VPN uses Virtual Routing and Forwarding (VRF) to provide multiple routing instances. Customer specific routing tables are created on the PE when a VRF instance is configured. A separate IP routing and forwarding table is assigned to each VPN. A VRF forwarding table stores VPN routes with associated labels.

The Control Plane for MPLS VPN is based on Multi-Protocol BGP.

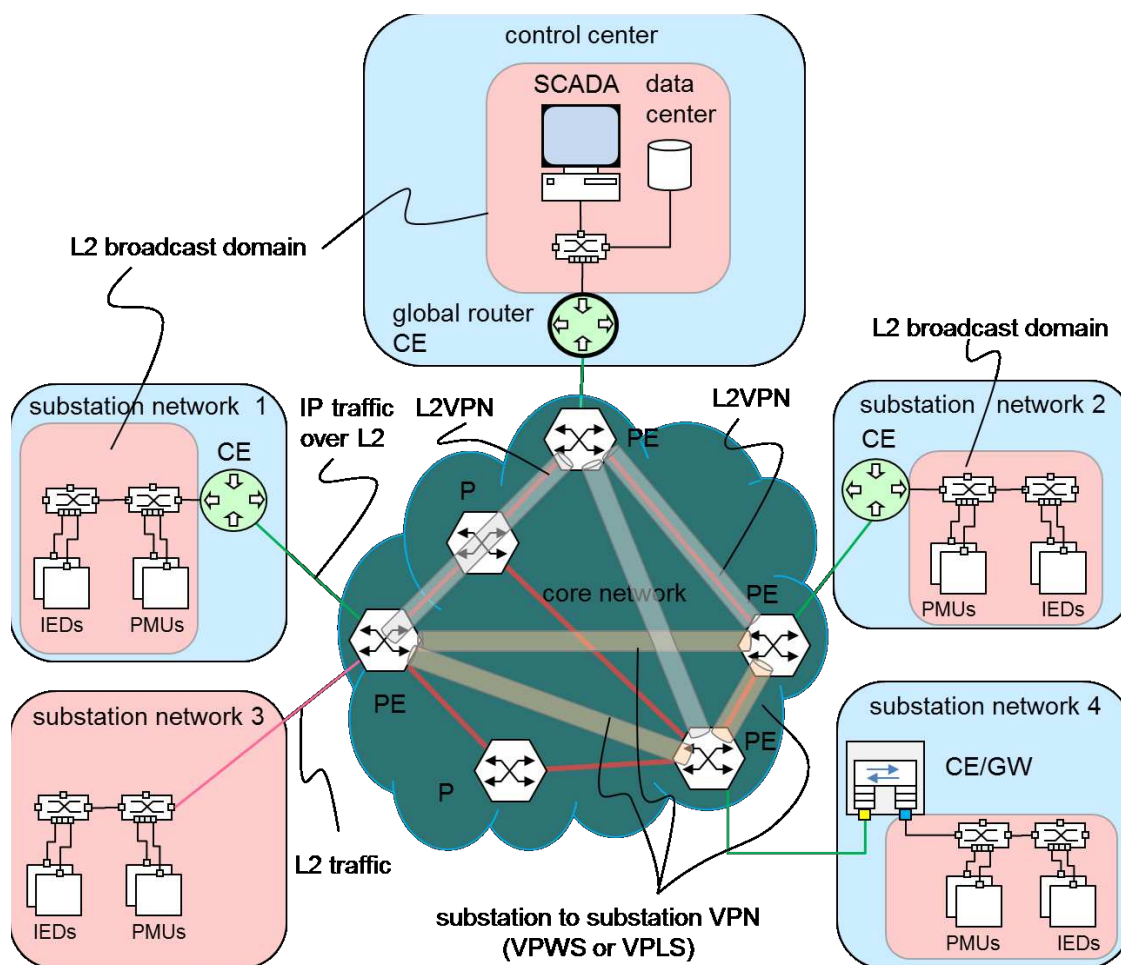
PIM, IGMP, MSDP and other multicast protocols operate in the context of the VRF.

The Multicast VPN—IP Multicast Support for MPLS allows to configure and support multicast traffic. This feature supports routing and forwarding of multicast packets for each individual VRF instance, and it also provides a mechanism to transport VPN multicast packets across the service provider backbone.

#### 7.11.4.3 L3VPN emulation by a L2VPN

An L3VPN requires that the PEs be able to execute a routing protocol such as OSPF or BGP and support VRFs for the individual L3VPNs. This behavior can be emulated by using an external router accessed through L2VPNs. The efficiency depends on the implementation and on the L2VPN topology (star, meshed, etc.).

Figure 108 shows an example combining L2VPN and Layer 3 communication. All Layer 3 communication passes through the router in the control centre. Layer 2 traffic uses the L2VPNs, some substations such as substation 3 are attached by Layer 2 only.



IEC

Figure 108 – Emulation of L3VPN by L2VPN and global router

#### **7.11.4.4 VPN security**

VPNs do not inherently imply the use of security. VPN security can be provided by additional functions, see 7.12.2. Security measures for VPNs are covered in 7.12.5.

#### **7.11.5 VPN mapping to application**

##### **7.11.5.1 VPN summary**

VPN in the context of these use cases are not used for security purposes, but to separate traffic from different applications.

VPNs are built on top of IP, IP/MPLS, MPLS-TP or other transport protocols to emulate a Layer 2 or Layer 3 network.

VPNs are superfluous if the core network offers only IP transport and is fully owned and administrated by the utility. But even in this case, VPNs are convenient to marshal application traffic into traffic classes with different administration and QoS. QoS and VPN are independent concepts, but a VPN is generally associated with a QoS.

VPNs are unavoidable when the core network is operated by an independent network operator (service provider).

L2VPNs are indispensable when MPLS is the core network technology. All core networks support L2VPNs, which allows tunneling Layer 2 traffic such as GOOSE. L2VPNs are divided into VPWS (single Ethernet link emulation, pseudo-wire) and VPLS (Ethernet bridge emulation)

L3VPNs should be used for IP traffic. L3VPNs provide a virtual routing on top of the core network routing. If the core network does not support natively L3VPNs (VPRN), they can be emulated by L2VPNs connected to a CE that performs as a router,

L3VPNs are divided into unicast VPNs (unicast IP emulation) and MC-VPRN (multicast IP emulation).

Table 47 shows the application cases with the recommended VPNs and QoS.

**Table 47 – VPN services**

Application	Partner	Partner	Type of VPN	QoS	Example
Network Management	Engineering	Network Elements	L2VPN L3VPN	7	SNMP
Teleprotection	SS	SS	VPWS (VPLS)	6	GOOSE, SV (for more than 2 substations)
Telecontrol	SCADA	IEDs	L2VPN	6	GOOSE
WAMPACS, SIPS (down link)	CPE	IEDs	L2VPN L3VPN	6	GOOSE R-GOOSE, R-SV
Operational voice (non-IP)	CC, SS	SS	CES	5	SAToP, TDM over MPLS
Operational voice (IP)	CC, SS	SS,CC	L3VPN	5	SIP
WAMS, WAMPACS (up link)	PMUs / PDC	PDC / CPE	VPLS MC-L3VPN M-VPN	4	GOOSE, SV, raw C37.118 R-SV, IEC TR 61850-90-5
SCADA non-IP legacy	RTUs	SCADA EMS	CES	4	IEC 60870-5-101, DNP3, Modbus
SCADA IP	IED/GW	SCADA EMS	L3VPN	3	IEC 61850-MMS, IEC 60870-5- 104
Supporting services	SS or CC	SS or CC	L3VPN	2	- Incident response systems - SS physical security (video surveillance, access control, alarms) - Remote workforce management
Company internal informatics	Office	Office	L3VPN	1	Email, servers, directories
Internet	Office	Office	L3VPN	0	Documentation, Weather

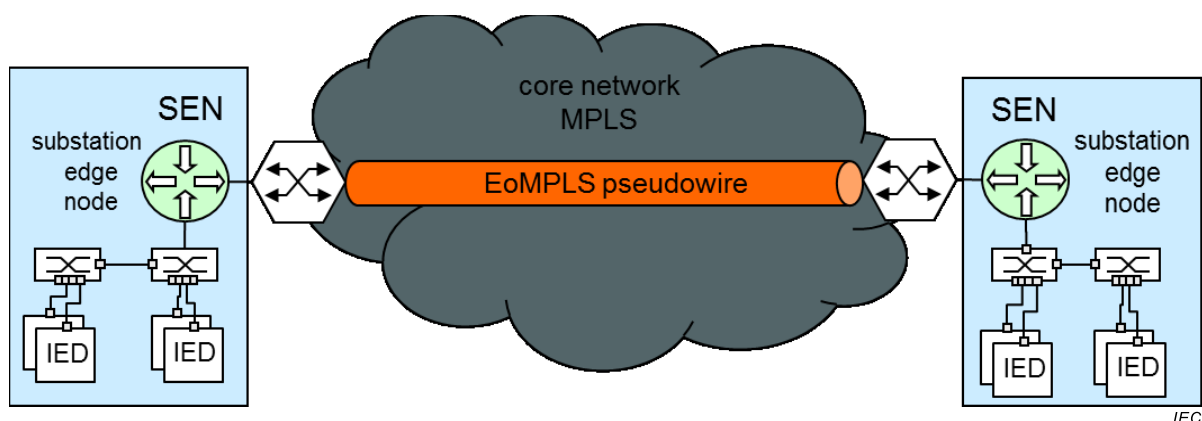
NOTE 1 As explained in 7.11.4.3, a L3VPN can also be emulated by a L2VPN with external routers

NOTE 2 Depending on detailed requirements (e.g. number of nodes, quantity or type of applications, network size, etc.), Layer 2 networks with VLANs offer an alternative to VPNs.

### 7.11.5.2 Utility applications over MPLS VPNs

#### 7.11.5.2.1 VPN for teleprotection (IEC 61850-8-1/GOOSE)

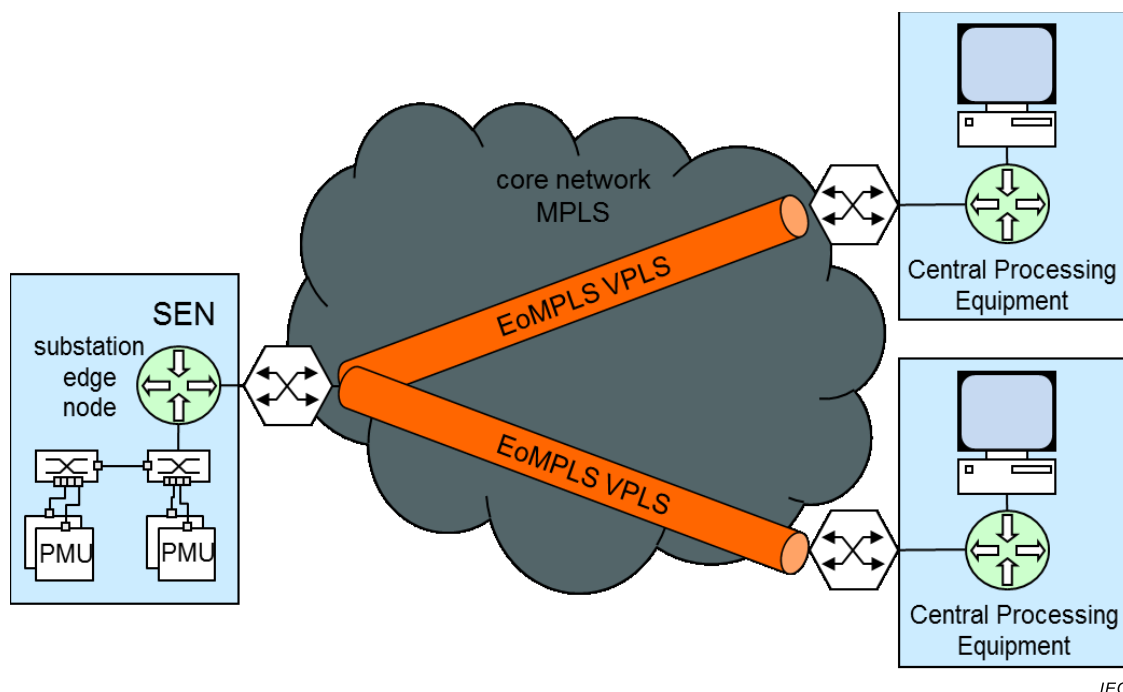
IEC 61850-8-1 (GOOSE) and IEC 61850-9-2 (SMV) messages can be carried over MPLS networks over pseudo-wires (Figure 109).



**Figure 109 – Tele-protection over VPWS,**

### 7.11.5.2.2 L2VPN for WAMS

IEC 61850-9-2 SMV messages can be transported point-to-multipoint (P2MP) through a VPLS (Figure 110) to the Central Processing Equipment that computes the grid stability conditions.



IEC

Figure 110 – WAMS over VPLS

### 7.11.5.3 VPNs for legacy RTU-SCADA traffic

#### 7.11.5.3.1 Categories of legacy protocols

Legacy protocols were originally transported over telephone lines, preferably as asynchronous character-oriented streams such as Modbus, DNP3 or IEC 60870-5-101.

These protocols were later transported over IP, such as Modbus-IP, DNP-IP or IEC 60870-5-104.

These two modes are treated differently for transmission over WANs

#### 7.11.5.3.2 Asynchronous legacy protocols

The asynchronous legacy protocols can be tunneled between the endpoints using a circuit emulation using TDM pseudowires over MPLS.

Depending on the relay or channel-bank requirement, the TDM pseudowire can be configured to perform raw channel circuit emulation with SAToP or structured circuit emulation using CESoPSN.

Traffic-engineered of forward and return paths between substations allows path congruency. Paths can be traffic-engineered using statically provisioned MPLS-TP tunnels or dynamic RSVP-TE tunnels.

### 7.11.5.3.3 IP-based legacy protocols

Serial SCADA protocols can be threaded using TCP Raw Socket, which is a method for transporting serial data over a PSN or can be translated into an IP flow using protocol translation mechanisms.

SCADA protocols based on TCP/IP such as Modbus-TCP, DNP3-IP, IEC 60870-5-104 etc. can be transported as IP over a Layer 3 MPLS VPN (Figure 111).

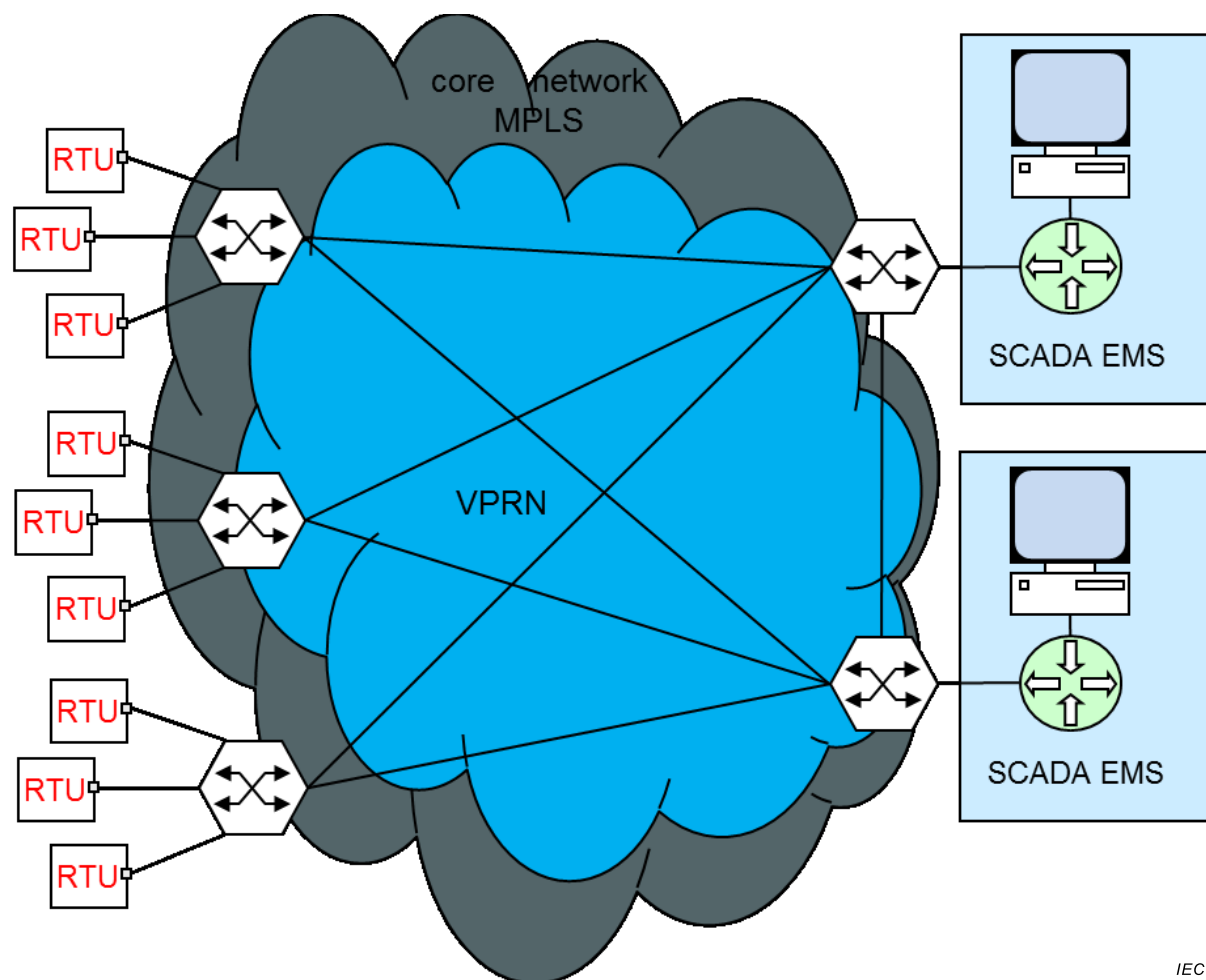


Figure 111 – VPN for IP-based SCADA/EMS traffic

By comparison, 7.9.3 details the case of C37.118 synchrophasor transmission without a VPN.

## 7.12 Cyber Security

### 7.12.1 Security circles

Power automation installations belong to the critical infrastructure and cyber-attacks could cause blackouts or grid disruption. Strong cyber security concepts are needed; weak cyber security implementations might lull into a false sense of security.

PSNs are much more vulnerable for cyber-attacks than the traditional legacy infrastructure of power utilities and measures to secure such networks have to be taken. Cyber Security needs to be adapted to the special conditions existing in operational networks such as specific protocols, real time communication with strict latency and jitter/ wander requirements. It has also to be considered that security related activities (e.g. updating security patches) must not interfere with the utility operation or even interrupt the operational traffic.

The IEC 62443 suite specifies a defense for industrial communication networks which applies to mixed installations, such as power plants with a substation. It defines the security assessment, such as:

- What has to be protected, e.g. applications, end-to-end communication, WAN communication etc.?
- What level, e.g. traffic separation, authentication, encryption etc.?
- How exposed is the infrastructure to attacks? What kind of different network areas/zones are included?

Depending on such an assessment, some of the methods described in the following paragraphs may be applied or not.

The IEC 62351 series specifies how to defend power utility communications, with emphasis on the end-to-end (application layer) security.

IEC TR 62351-10 describes “defense in depth” as “the application of security controls in barriers and at different layers. “Barriers” imply multiple security barriers between the attacker and the target, while “layers” relate to the different communication layers in the infrastructure underlying any cyber system (transport, application, etc.). This concept ensures that if one security barrier is broken (for instance the lock on a door), the next barrier may prevent the attack (the attacker does not have the correct password) or it may just differ the attack until it is detected (such as video surveillance or an alarm notifying that an excess of passwords have been attempted).

Security involves three circles:

- Host-based security implemented in the processes, systems and devices, which prevent access of unauthorized persons to the network. This includes proper virus scan, role-based access, etc. which is outside of the scope of the document.
- Application layer security using application-specific security, but which can use generic network security mechanisms such as TLS or HTTPS; implemented in the upper layers of the protocol stack
- Network security comprises all measurements to defend the communication network. It comprises inherent communication mechanism as well as dedicated security measurements and devices. The main technical security controls to defend a power systems based on network security can be implemented using the security services detailed in the sequel.

Three threats are particularly important for network communication:

- denial of service – countered by filtering in the network elements;
- eavesdropping sensitive information – countered by encryption (confidentiality);
- forging of messages – countered by source and message authentication.

NOTE Source and message authentication are part of “integrity”, which as a general term encompasses transmission errors.

## **7.12.2 Network security**

### **7.12.2.1 Network security layers**

Network security applies to all communication layers (network security) and to the application information (application-layer security).

- Physical assets security (access control, IR cameras, video surveillance, etc.) is not in the scope of this Technical Report. Many physical security devices need connection to the network. Especially, video surveillance can generate a considerable traffic;

- Layer 1 security (7.4.9) prevents unauthorized eavesdropping or traffic injection. It is requested when the media run over public ground;
- Layer 2 security defends messages sent across Ethernet networks (7.6.4.10.1) or SDH networks (7.6.2.10) and prevents unauthorized access to bridge ports (7.6.4.10.2).
- Layer 3 security (7.7.5) defends messages sent over several LAN segments.
- Layer 4 security (7.8.5) defends messages sent across several networks.
- Application-layer security (IEC TR 61850-90-5 and IEC 62351) defends the data on the whole path from end user to end user.

Application-layer security does not dispense from implementing security on lower communication layers. For instance, the traffic patterns can reveal much information.

According to the defense-in-depth security principle, a combination of network security and end-to-end security is needed.

The goal is to secure data authenticity and confidentiality for operational and control data used in the power system. This typically applies to all data sent between substations (IEC TR 61850-90-1), between substation and control centres (IEC TR 61850-90-2) and for synchrophasor networks (IEC TR 61850-90-5).

#### **7.12.2.2 Key distribution**

Cybersecurity protocols such as TLS or IPsec rely on secret keys that are known to the producer and the consumers of the information. These keys must be made available to the concerned devices, either by configuration or through a secure protocol from a Key Distribution Centre (KDC). Most communication depends on symmetrical keys, i.e. the producer and the consumer of the data use the same key, once for encrypting the data, once for decrypting the data.

In multicast communication, a group of devices may share the keys, so that each one can communicate with each other.

To this effect, a key distribution is needed. The Group Domain of Interpretation (GDOI) standard [RFC 3547] defines how keys are to be distributed and periodically refreshed for a group of devices.

GDOI is specified for IPsec and for the IEC TS 62351-6 protocols.

#### **7.12.2.3 Layer 3 security in utility communications**

A network security concept may consider security implementations at the different network layers as described in 7.12.2.1. Exemplary only Layer 3 security is discussed in 7.12.2.3.

IPsec can be used to defend data traversing networks between substations and control centre or between substations.

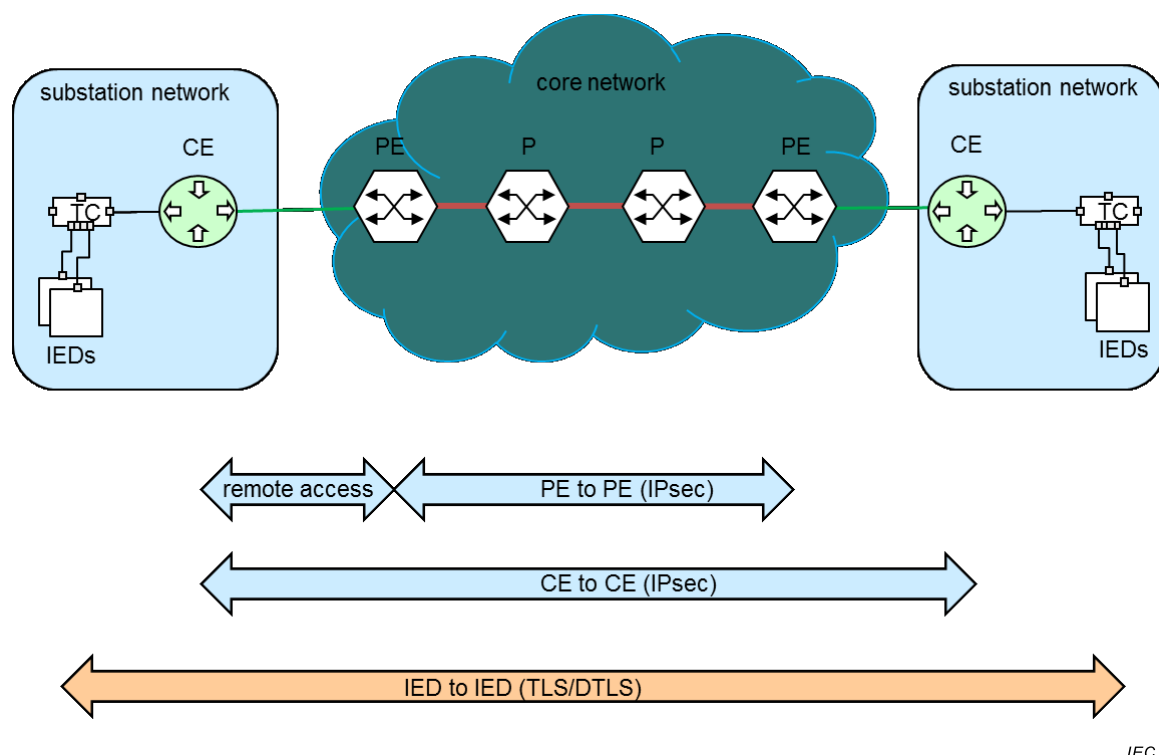
The location of IPsec termination points is a critical design decision. A termination endpoint must be operated by a trusted party and within a trusted zone of the network. The following options exist:

- 1) Within the installations (VPN sites) – this is an end-to-end use case and is not in the scope of this TR.
- 2) Between the Access Routers of the VPN – the trust is managed and under the responsibility of the Access Router owner (e.g.: substation owner); the WAN core is not involved in the security services.



- 3) Between the PE routers within the MPLS VPN core network – the security services are under the responsibility of the core network (WAN) owner; for instance a service provider manages the IPsec services.
- 4) Between a point in the VPN and the PE – this applies to remote access use cases (e.g.: remote engineering).

Figure 112 shows options 2 to 4. The direct IED to IED security is not required when the IEDs are within the same substation.



**Figure 112 – VPN deployment options**

Termination point location decisions are just one perspective. The subsequent bullets list technologies and deployment scenarios for IPsec:

- **Static IPsec:** IPsec nodes are configured statically with their peers (in terms of authentication information and security policy).
- **Dynamic IPsec:** Typically used in a hub-and-spoke topology where only the spokes know how to connect to the hub and must authenticate themselves in order to establish an IPsec tunnel.
- **GDOI-based VPNs** use only a single security association for the whole domain of IPsec nodes within the VPN (see 7.12.2.2).  
GDOI-based VPNs provide appropriate defense for telecontrol and SCADA traffic, IP-based or serial (tunneled). Furthermore, the security architecture for PMU networks in IEC TR 61850-90-5 considers GDOI-based VPNs as optional security function. It is based on a defense-in-depth approach and utilizes the security model of IEC TR 61850-90-5 that also uses a GDOI approach to ensure security.
- In parallel to sound technical definitions, VPN security operation needs to be based on a VPN security policy.
- Optional application or transport layer encryption (as defined in IEC 62351 for the IEC 61850 protocol suite depends on the capability of the end devices).

### 7.12.3 Access Control

Access control ensures that only authorized personnel are accessing the network and that only valid devices and systems are part of the grid automation and control network. Access control is used to prevent intruders from gaining access to networks and devices.

Network Access Control (NAC) can be based on IEEE 802.1X (see 7.6.4.10).

The subsequent bullets list more network-based security technologies to assure strict access control:

Role-Based Access Control (with username and passwords and/or X.509 certificate based identities) is a mechanism to restrict access based on roles and should be used to control device access within the substation.

RADIUS, LDAP and other protocols for Authentication, Authorization and Accounting (AAA) of users and devices. An AAA service is used to authenticate and authorize user access.

- ACL on VLAN ports (especially for teleprotection and other inter-substation use cases); Unused ports must be shut down
- Authenticating and authorizing of field technicians or operations centre staff before they can view or configure devices, track changes made (RBAC)
- Authenticating of every device and application connected to the substation and control centre networks: routers, switches, servers, workstations, IEDs, RTU's, etc.
- Mutually authenticating user and supported devices by relying on strong certificate based identities
- Remote Access using Telnet must be secured by SSH to prevent man-in-the middle attacks. In order to comply with policies and regulations, banner might be requested.
- End point posture assessment for devices as laptops, workstations, servers connecting to Substation and Control Centre LAN segments to detect any viruses before allowing access to the network, forcing remediation such as installing software patches or updating anti-virus database

### 7.12.4 Threat detection and mitigation

#### 7.12.4.1 General

Threat detection and mitigation defend critical assets against cyber-attacks and insider threats throughout the power system.

#### 7.12.4.2 Traffic separation

A first measure is traffic separation, in the sense that data should not travel farther than necessary. Islands can be built for bay traffic, for substation traffic or for regional traffic. Only a small part of the traffic should be allowed to leave the area.

For instance, the use of private addresses ensures that all traffic has to go through controlled routers.

Logically segmentation allows the separation of traffic based on application classes (e.g. SCADA, engineering, phasor data, video, physical security). Segregation of network traffic is a strong defense since it prevents one category of traffic to access the resources allocated to another class of traffic (except non-reserved bandwidth).

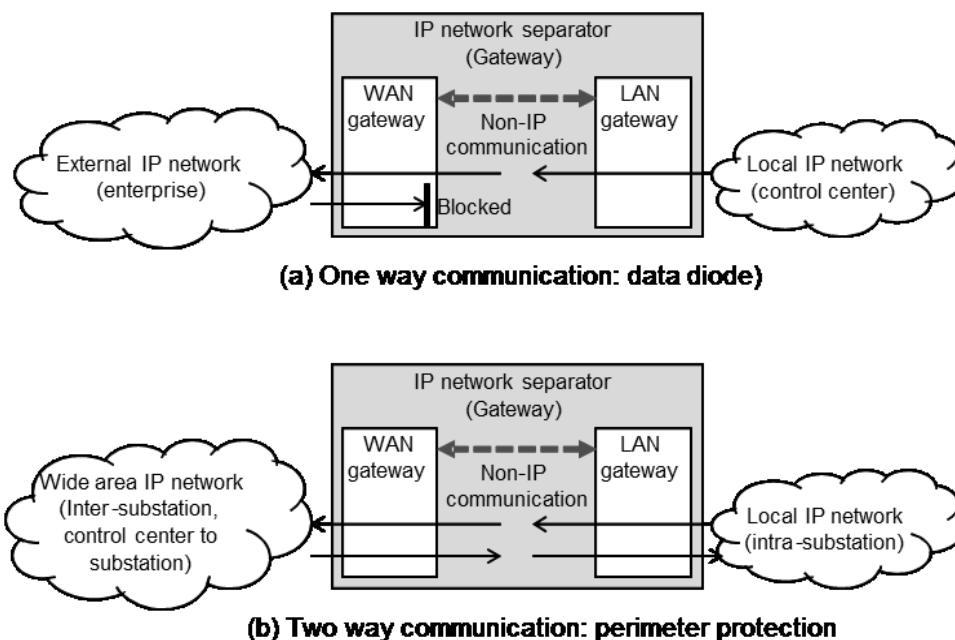
Traffic segregation must be enforced at WAN networking devices as well as on the connected LAN segments (e.g. Substation LAN). From the system perspective, all inter-connected segments needs to be defended and addressed in the security architecture.

Within the substation network, VLANs allow to segregate the traffic (e.g. SCADA LAN, Network management VLAN, PMU VLAN).

Outside the substation network, VPNs, VLANs or dedicated SDH channels (or a hybrid approach using different technologies) allow to segregate the traffic. Assignment of traffic to dedicated channels is based on traffic identification (e.g. VLAN ID) or on port identification.

For interconnected systems (e.g. in a substation-to-control centre use case), mapping with corresponding traffic segregation within the peers (Substations, Control Centre) is recommended.

IP-network separation using a security gateway as Figure 113 shows is another measure.



IEC

**Figure 113 – IP network separator**

Access control lists should be applied to filter, log and authorize traffic between segments and zones within the network.

#### 7.12.4.3 Security zones

Security zones, called Electronic Security Perimeter (ESP) in NERC-CIP, are critical parts of a security architecture to divide the network into a series of virtual sections, so that various levels of trust and security policies can be established. Network traffic between zones is implicitly denied, unless a zone pair is configured to permit the traversal.

In a substation-control centre scenario, a Zone-Based FireWall (ZBFW) enables the creation of different substation security zones. Typically integrated in a substation automation router, the ZBFW is responsible for perimeter security and the enforcement of the security zone concept. Zone pairs could be: SCADA-WAN (control centre-facing zone), SCADA (substation-facing zone) or NMS-WAN (control centre-facing zone), NMS (substation-facing zone).

By definition, a firewall examines the traffic and applies rules to it. It permits or denies the traffic based on these rules that can apply to inbound and outbound traffic. A firewall utilizes access control lists (ACL) to filter and restrict traffic based utility-specific policies. Typical deployment scenarios for firewalls within the TC57 architecture are also described in IEC TR 62351-10.

#### **7.12.4.4 DeMilitarized Zone (DMZ)**

Beside the zones for designated functions, a DMZ is an appropriate tool to deploy and host services that are directly connected to inbound traffic such as terminal server. A DMZ enables inbound access only to systems isolated in the DMZ and not directly into a critical network segment. A DMZ is a firewall functionality that provides physical isolation between two networks enforced by connectivity rules within the firewall implementation.

#### **7.12.4.5 Intrusion Detection Systems (IDS)**

An IDS monitors the network for abnormal activities or policies violations. An example of an IDS is the open source Snort tool [48].

#### **7.12.4.6 Intrusion Prevention Systems (IPS)**

IPSs are integrated on network nodes or as stand-alone appliances to detect network intrusions through use of IPS/IDS at critical points in the network. Customization with SCADA IPS signatures addresses domain-specific threats.

#### **7.12.4.7 Anti-Malware software**

Anti-Malware software safeguards against viruses, trojans, etc. It is needed where standard software (COTS) is used; typically in the control centre applied to operating systems, databases and applications based on standard components.

#### **7.12.4.8 Software update management**

Software update management (or patches) for COTS systems – typically in the control centre and in the substation- is needed for operating systems, databases, middle-ware, web server, etc.

It has to be ensured that installing updates does not affect the network availability as well as the performance of communication channels.

#### **7.12.4.9 Access control**

Enhanced access control mechanisms is based on port security (IEEE 802.1X) and endpoint posture assessments to support detective and preventive security controls (see 7.12.3).

#### **7.12.4.10 White-listing**

White listing registers all applications allowed execute on critical system within control centre and substations.

#### **7.12.4.11 Network security and event management**

Network security and event management is typically hosted in the network control centre (Figure 114) and comprises the following security functions:

- Collection and aggregation of trace data from network devices in order to analyze network events, potential attacks. Syslog [RFC 5424] is a format to export collected event notification messages from within a computer, but which is not secure by itself. IPFIX [RFC 7011] is a standardized data exchange format for collected network traces.
- Security event management (SEM): real-time processing of security event data for incident response and threat management. Event data sources comprise IDS/IPS, firewalls, networking equipment, security software and appliances, system malware reports, and host activity logs. Correlation with IDS/IPS events supports the identification of security incidents. Notification of cyber security depends on severity, rules as well as underlying policies.

- Security information management (SIM): analysis of log data for compliance reporting and privileged user and resource access. Log data sources encompass host system and security logs, database activity and audit logs, directories, identity and access management (IAM) systems, application logs, and transaction logs. Archiving of security events for forensic analysis and regulation reporting.

#### **7.12.4.12 Device and platform defense**

All devices connected to the power system need to be defended in order to withstand physical and cyber-attacks. This may include strong physical security defenses, depending on the installation, as well as internal defenses that prevent tampering.

As a part of normal network operations, each node should receive remote software updates from the control centre. These upgrades should happen only after authentication of the source and validation of the software's data. Other measures to defend devices and platforms comprise:

- Secure Device Identity
- Use of X.509 Certificates
- Hardening of network devices
  - Disabling unnecessary network services
  - Control Plane Policy
- Hardening of all secondary equipment attached to the network
  - Shut down unnecessary ports
  - Within the substation, used ports must be explicitly enabled; the maximum number of secure MAC addresses for a port should be 1 (one)
  - Disabling of services that are not needed for operation

#### **7.12.4.13 Other security measures**

In order to achieve security in depth, more security measures beyond the technical security controls need to be established. The subsequent bullets list the most important:

- Integration of physical security
- Secure remote access – In the substation/control centre, field technicians or operations centre staff must be authenticated and authorized through strong certificate-based identities and role-based access before they can view or engineer devices.
- Security Policies
- Training and education
- Honeypots (i.e. Victim Hosts) are active security tools that appear to an attacker as being the system or service he is looking for. Honeypots distract attackers from more valuable assets on the network. Typically, honeypots can be deployed in large control centre installations.

#### **7.12.4.14 Network configuration and management**

Network configuration and management is an important tool to support network security inherently.

- A Network Management System (NMS) supports network security as a part of Fault, Configuration, Accounting, Performance and Security (FCAPS). A NMS typically supports the process of controlling access to networks and devices. An operator uses a NMS to configure and monitor the performance of the network deployment. A NMS is typically hosted by the Network Operating Centre.
- Network traffic analysis is an important tool to monitor, analyze and measure traffic in the network, see 7.12.4.11. Furthermore, slow network performance, and bandwidth

consumption can be identified and diagnosed. Such information supports detection and diagnosis of anomalies and security incidents such as Denial-of-Service (DoS) attacks.

- Network security monitoring system: typically encapsulates critical security services; e.g.: management of user access logs, management of security events, detection of network attacks (see Threat Detection and Mitigation).
- QoS policies: QoS needs to be assured for critical data flows; DoS prevention by QoS policy:
  - Control Plane defense
  - Denial-of-Service defense
  - Control Plane Authentication and Policies

#### **7.12.5 Security architecture**

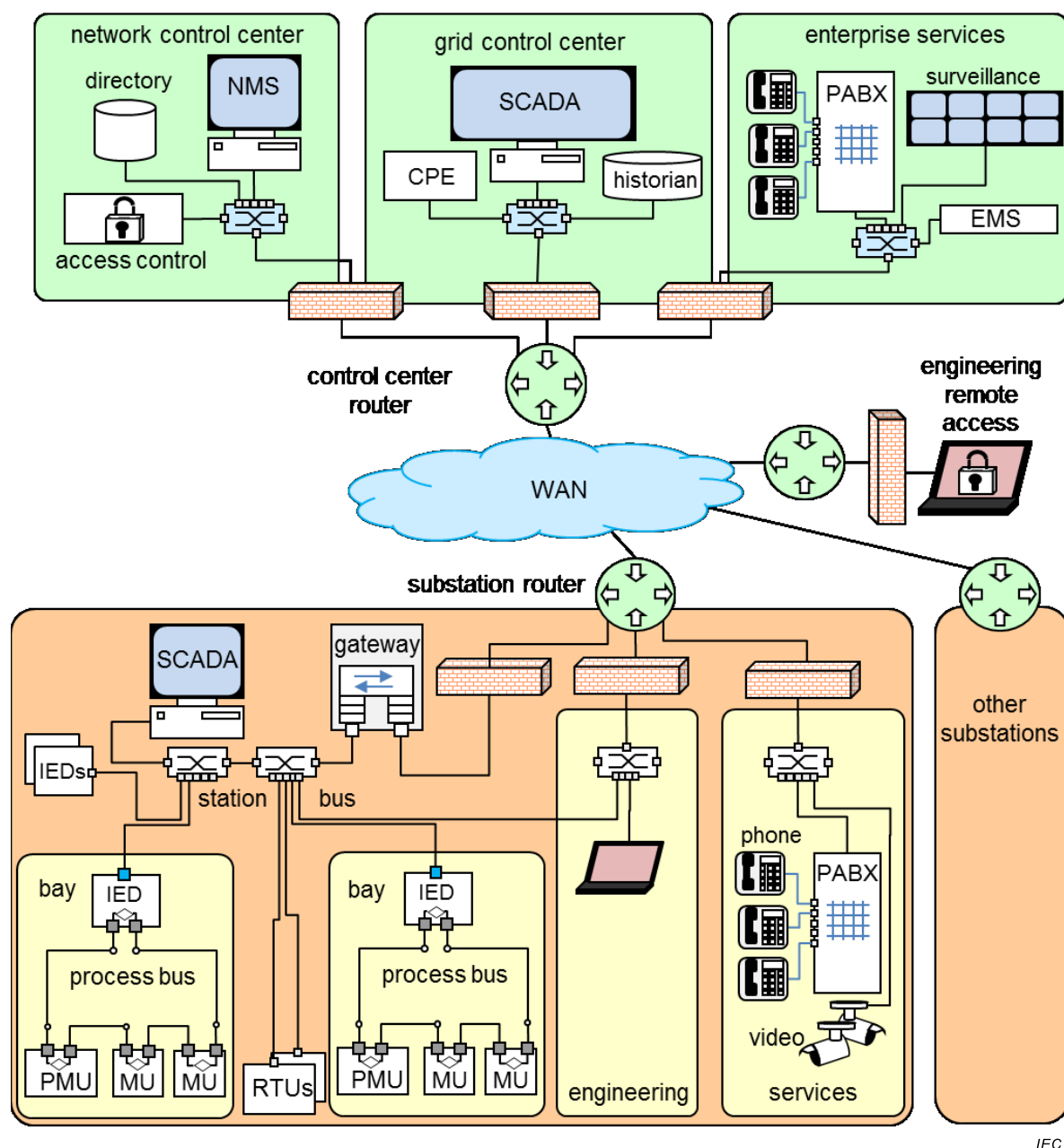
The security architecture is the foundation to implement and introduce the appropriate security measures to the overall power system in an end-to-end manner. A security architecture addresses the most important security principles in terms of defense-in-depth as well as general architectural quality attributes such as extensibility and scalability. A selection of security services as described in the Clauses 7.12.1 to 7.12.4 need to be combined, depending on the individual utilities situation and requirements.

Figure 114 depicts the typical components and peers within the scope of a power automation network with the focus on substation automation, substation-to-substation and substation to control-centre communication.

Depending on the utility security requirements, WAN links may be separated and encrypted. A zone-based firewall enables the security zones for perimeter security.

Within the Substation Automation Network, traffic is segregated into the following zones:

- Protection and control: IEDs, PMUs and RTUs
- Engineering: Hosting HMI and network engineering capabilities
- Service: IP telephones, IP cameras as well as other IP-based service equipment
- Network control: access server, key server, possibly redundant



IEC

**Figure 114 – Security architecture (using segmentation and perimeter security)**

### 7.12.6 Application (end-to-end) communication security

Authentication is more important than encryption for SCADA and protection security.

End-to-end security can be provided in several ways:

- the end device is providing the security function directly (e.g. an RTU having IPsec functionality integrated);
- application based security mechanisms provided by the communication equipment for devices installed in the field but not having encryption capabilities.

The IEC 62351 standard series addresses security for the utility protocols. Table 48 lists the parts of IEC 62351 with a brief overview of the content.

IPsec and TLS/DTLS provide the foundation for many secure tunneling solutions to support use cases such as remote access or mobile workforce support.

For any other communication which needs to be defended, network security based functions should be used. This applies as well for any data exchange where IEC 62351 implementations are not available. IEC TR 62351-10 contains corresponding recommendations.

**Table 48 – IEC 62351 series**

Part	Content
IEC TS 62351-1	Introduction and overview – contains general aspects like security threats, vulnerabilities, requirements, attacks, and countermeasures typically for a substation environment as well as basic concepts
IEC TS 62351-2	Glossary – contains key terms and definitions used in the scope of IEC 62351
IEC 62351-3	Profiles including TCP/IP – applies to: [IEC 60870-6 TASE.2, IEC 61850 over MMS, IEC 60870-5-104 and DNP3]  Specifies use of TLS for SCADA and tele-control protocols based on TCP/IP (IEC 61850 MMS, ICCP (TASE2)).  defines cipher suite requirements, session and X509 certificate handling
IEC TS 62351-4	Profiles including MMS – applies to: [IEC 60870-6 TASE.2, IEC 61850 over MMS]
IEC TS 62351-5	IEC 60870-5 and Derivatives – applies to: [IEC 60870-5-104 & DNP3, IEC 60870-5-101,102,103 and Serial DNP]
IEC TS 62351-6	Security for IEC 61850 – applies to: [IEC 61850 over MMS, IEC 61850 GOOSE, SMV]
IEC TS 62351-7	Network and system management (NSM) data object models – defines NSM data objects specific for power system operations; uses naming conventions of IEC 61850
IEC TS 62351-8	Roles Based Access Control (RBAC) for power system management – specifies mandatory roles for TC 57 domains like substation automation based on IEC 61850; covers a PUSH and PULL model; defines credential (security token) and transport profiles
IEC TS 62351-9	Cyber security key management for power system equipment (not released yet)
IEC TR 62351-10	Security architecture guidelines – describes guidelines for the security power systems based on essential security controls
IEC TR 62351-11	Security for XML files (not released yet)

### 7.12.7 Security for synchrophasor (PMU) networks (IEC TR 61850-90-5)

IEC TR 61850-90-5 contains a particular security model for synchrophasor networks that specifies cryptographic functions and key management as a special form of application layer security.

IEC TR 61850-90-5 defines information authentication as mandatory and confidentiality as optional. It specifies the use of a secure Hash-based Message Authentication Code (HMAC) [RFC 2104] over the entire content of a Session Protocol Data Unit (SPDU) through symmetric keys.

Furthermore, the IEC TR 61850-90-5 session protocol supports the option to encrypt the content of the SPDU payload. In addition, the security model of IEC TR 61850-90-5 includes the security definitions as specified in IEC TS 62351-6 to address end-to-end security.

Based on the defined security perimeter, the security model of IEC TR 61850-90-5 supports a variety of combinations based on the defined endpoint.

IEC TR 61850-90-5 specifies group-key management based on GDOI [RFC 3547). The concept of “perfect-forward” security uses key rotation and specifies usage and integration of one or more Key Distribution Centre (KDC), in a centralized or decentralized manner.



The security definitions in IEC TR 61850-90-5 amend GDOI in order to address use cases where more than one subscribing entity may reside on a single IP-address in order to enable Dataset specific keys.

The security standard IEC TS 62351-6 (Security for IEC 61850) defines the security for IEC 61850 GOOSE and SMV messages.

### 7.12.8 Additional recommendations

- Time synchronization security (NTPv3 and IEC 61588) – work in progress;
- SNMP: SNMPv3 security options;
- Secure web server and HTTPS: HTTPS must be used for all web applications. Web-based remote engineering applications based on HTML/HTMLS must use HTTPS to defend data in transit.

## 7.13 QoS and application-specific engineering

### 7.13.1 General

WAN utility communication transit over a core network that is under the responsibility of the network provider. The network provider may be a third-party provider or a department of the same utility company. Regardless of the ownership, a QoS is contractually agreed between the client (utility) and the (core network) provider in the form of an SLA.

The SLA is independent from the used network technology; it indicates the agreed values for the performance parameters (latency, bandwidth, etc.) and for the dependability (availability, disruption duration and frequency, etc...).

### 7.13.2 SDH/SONET QoS and SLA

Traditional SDH/SONET networks provide a hard QoS: once a virtual circuit is established, the latency is deterministic, jitter is limited and the bandwidth is guaranteed. All traffic types/applications in an SDH/SONET network are always handled at the highest priority, comparable to priority class 7 in Table 49. The SLA is expressed in terms of absolute performance and availability.

**NOTE** QoS is provided once the virtual circuit or path is established and persists until a disconnection occurs, e.g. because of a time-out. The delay to re-establish a lost connection can be orders of magnitude larger than the packet latency, as one can experience with the telephone service. The task of the network is to provide sufficient QoS so that a disconnection occurs with a very small probability.

### 7.13.3 PSN QoS and SLA

With PSNs, the deterministic qualities of TDM are approximated by a set of priorities and resource reservation protocols. PSN need additional QoS engineering work. For PSN, the SLA expresses performance as statistical values.

PSN protocols allow expressing the priority in the packet, in particular:

- At Layer 2, the 802.1p-field in the VLAN tag expresses 8 levels of priority (see 7.6.4.6);
- At Layer 3, the ToS field in IPv4 and IPv6 packets expresses 64 levels of priority (see 7.7.2.2);
- At Layer 2.5, the EXP field in MPLS expresses 8 levels of priority (see 7.6.9.6).

Simple priority can be extended by more sophisticated schemes, for instance traffic policies, strategies for discarding packets, congestion notification, etc. Discarding packets should be avoided if possible by buffering the less delay sensitive traffic. Some transports (e.g. TCP) would rather experience more delay through buffering than experience loss.

In addition to the priority information, the IP addresses or labels are sometimes used in the context of resource reservation, based on a previous configuration.

QoS is engineered and implemented network-wide including access, aggregation and core parts in a consistent way. Traffic flows of the different applications need to be identified, prioritized and classified into similar QoS classes. These QoS classes need to be handled equally in all sections of the network: a teleprotection service should be treated with the highest priority in the access, aggregation and core sections of the network (would the service cross the complete network). Tuning of the QoS policies in the CE/PE/P routers is essential for an optimal application flow in a utility network.

#### 7.13.4 Application and priority

Only simple priority is considered here.

Table 49 shows an example of assignment of different utility applications to 8 priority levels. This yields a simple mapping to 802.1Q, DSCP and EXP fields.

**Table 49 – Example of simple application priority assignment**

Traffic Class	Application	802.1Q, EXP	DSCP
Network Control	Network Management, IS/IS, LDS, RSVP-TE, BGP	7	NC, CS7
Expedited	Teleprotection, IEC TR 61850-90-1 (SS-SS) operational voice	6	EF, CS6
Real-Time	Telecontrol, WAMPACs IEC TR 61850-90-5 (SS-CC)	5	EF, CS5
Streaming	IP telephony, Video surveillance	4	AF41, AF42, AF43, CS4
Operation	SCADA, DNP-3, IEC TR 61850-90-2 IEC 61850-8-1	3	AF31, AF32, AF33, CS3
Support	EMS (CC-CC), CIM, OAM	2	AF21, AF22, AF23, CS2
Business	Mail, File Exchange	1	AF11, AF12, AF13, CS1
Internet	browsing, downloads, videos, webinars, web learning	0	Best Effort

#### 7.13.5 QoS chain between networks

A PSN is not application-aware and categorizes packets based on the priority and addresses or labels of the transported packets. An application-aware instance (e.g. Proxy-Gateway or CE) therefore maps the application messages to these network categories.

Figure 115 shows a conceptual network chain between two access networks communicating over a core network, e.g. between a substation network and a SCADA network over a service provider or company-owned core network.

The substation LAN is connected to the access network through a proxy-gateway that is application-aware. The proxy-gateway generates IP traffic, including IEC 61850, legacy and other traffic. The proxy-gateway sends the IP packets to the CE router on the access network. The CE performs routing for the substation network. The CE may be implemented in the same device as the proxy-gateway, the distinction is conceptual.

The interface between the access network and the core network consists of the CE-router on the customer site and of the PE at the provider side. Both devices can be aggregated into one device, the distinction is conceptual.

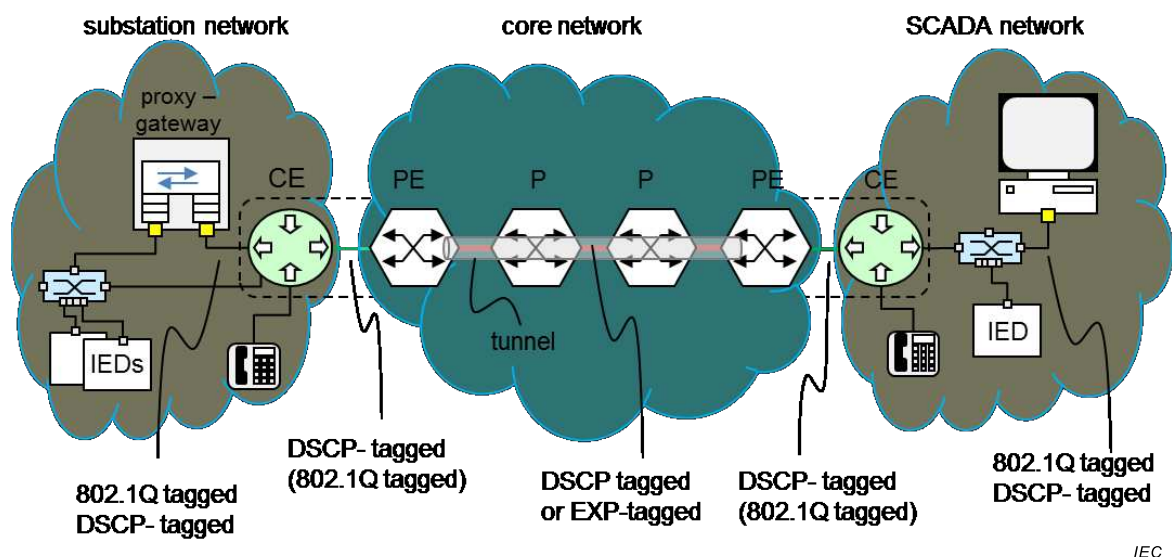
The CE router sends the IP traffic it receives from the proxy-gateway to the PE. It also encapsulates other traffic such as TDM or video surveillance streams into IP-packets (if not already packetized), while considering the timing constraints.

The PE receives the packets from the CE and categorizes them according to its configuration. It can send the packets in raw form if the core network is not shared, or encapsulate them in tunnels or VPNs.

The core network is not application-aware; the P-routers consider the priorities in the packets they receive, i.e. the DSCP (IP) or EXP (MPLS) priority field in the outer header or the 802.1p priority (Ethernet). If the P-routers are engineered, they can assign resources based on IP addresses or label. However, they cannot read the tunneled traffic.

The packets arrive at the PE at the SCADA end. This PE reconstitutes the original packets and forwards them to the CE, which sends them to the SCADA LAN.

The same applies in the opposite direction.



IEC

Figure 115 – QoS chain

#### 7.13.6 QoS mapping between networks

The configuration of priorities becomes complex when networks are cascaded.

The priority in a LAN is mapped to the priority of the IP traffic on the access network, which is then mapped to the trunk network priority (e.g. MPLS). Depending on the core network, not all mappings are applicable.

At each interface between connected networks, the priorities are assigned to the traffic. This requires QoS engineering, an integral part of the network design. Indeed, there is no automatic translation of the priority of one network to the next. Direct mapping can be used in first approximation, but is often insufficient since the priorities have a scope only within their network.

For instance, GOOSE and SV traffic may have a VLAN tag with a high priority, but since this traffic does not leave the substation, this 802.1Q value will not be reflected in a DSCP value.

Strict priority is not sufficient; fairness is needed to avoid starving low-priority services. Therefore, applying QoS to a port or sub port that is carrying traffic with different 802.1p or

DSCP settings may require not only a policy to be applied for each QoS level, but also to the group. A hierarchical QoS policy will ensure not only that service priority is maintained but also the interaction of one service against another has no detrimental effect. Applying the QoS policy at the service ingress ensures that priority and fairness is set and maintained.

### **7.13.7 QoS engineering**

#### **7.13.7.1 Proxy-gateway engineering**

The proxy-gateway is application-aware: it can assign the IEC TR 61850-90-1 and IEC TR 61850-90-5 (R-GOOSE and R-SV) a higher priority, give MMS packets a lower priority, etc. e.g. according to Table 49.

#### **7.13.7.2 CE-router engineering**

The CE is responsible to communicate the priority information to the PE. A CE itself is not necessarily application-aware, except that it can have multiple ports, which may have pre-assigned priorities, such as LAN ports. A CE may support multiple QoS per port. A CE can also adapt legacy traffic to packets.

The CE is expected to prioritize all traffic, for instance according to Table 49.

#### **7.13.7.3 PE-router engineering**

At the entry of the core network, the PE-router in Figure 115 assigns priorities to the traffic flowing on the CE-PE link, according to its previous configuration.

This configuration lets the ingress PE identify traffic based on several criteria and lets it assign a priority in the core network (e.g. expressed in the EXP in MPLS) or assign a VPN with a given priority. The ingress PE can inherit the priority from the incoming traffic or assign its own.

Such criteria in the incoming packets are:

- VID in the Ethernet frames (Layer 2 traffic)
- 802.1p field in the VLAN header of the Ethernet frames (Layer 2 traffic)
- MAC source and destination address (for Layer 2 traffic)
- DSCP priority in IP headers (Layer 3 traffic)
- IP source and destination addresses (Layer 3 traffic)
- TCP/UDP port number in the IP messages (L4 traffic)

Conversely, the egress PE at the SCADA side generates the priorities for the SCADA network. These priorities are mapped from the packet priority (possibly after extraction from the tunnel). The CE then generates the priorities for the SCADA LAN or access network. These priorities are not necessary identical to the core network priorities or to the original values on the substation LAN.

Therefore, here again, the (egress) PE is configured to generate the correct priorities for the (egress) CE.

#### **7.13.7.4 P-router engineering**

The P-router operates with the markings in the incoming packets and allocates priority and – if reserved – bandwidth.

### 7.13.8 Customer restrictions

The client application, especially the proxy-gateway but also the IEDs respect rules to allow the network provider to fulfil the SLA. The configuration is an important part of the SLA of the client with the core network provider and should remain manageable and measurable.

A first rule is to use a simple priority assignment to traffic classes to simplify the configuration both of the CE, the PE and the P routers.

A second rule is to limit the generation rate: if the application generates packets at too high a frequency (even of the highest priority), the PE will start dropping packets, since it is bound to a CIR. The dropping policy is part of the PE/P configuration.

A third rule is to submit packets that are small enough to be correctly encapsulated on all network segments, since fragmenting could double the transmission rate as long packets are split. Not all networks allow negotiating the MTU size.

### 7.13.9 Clock services

The clock synchronization service can also be part of an SLA. In this case, time or frequency synchronization, clock accuracy and redundancy are specified.

## 7.14 Configuration and OAM

### 7.14.1 Network configuration

Network configuration management and fulfilment are core functions of a Network Management System (NMS). In order to support the work of a network operator efficiently, a NMS should contain the following functional blocks:

- Service configuration and provisioning process support including VPN configuration and management
- Resource management, provisioning, and diagnostics tools for service validation and troubleshooting
- Virtual connectivity discovery, root-cause identification, troubleshooting,
- Performance monitoring and statistics for network devices with actionable information
- Inventory and event/alarm management

### 7.14.2 OAM

#### 7.14.2.1 Classification

The seven main families of management are (the first five known as “FCAPS”):

- 1) Fault
- 2) Configuration
- 3) Accounting
- 4) Performance
- 5) Security
- 6) Provisioning
- 7) Monitoring

An OAM subsystem falls into two categories: Service OAM and Transport OAM. Service OAM and Transport OAM rely on the same set of protocols to provide end-to-end OAM capabilities, including fault and performance management, but focus on different functional areas.

#### 7.14.2.2 Service OAM

Service OAM is a service-oriented mechanism that operates and manages the end-to-end services carried across the network. It is provisioned only at the touch points associated with the end-to-end service, and is primarily used for monitoring the health and performance of the service. Service OAM ensures services are up and functional, and that the SLA is being met.

When services are affected due to network events, it provides the mechanisms to detect, verify, and isolate the network faults. The following protocols provide the core services of OAM including performance monitoring (PM) for the different segments, traffic types and technologies:

- 1) Ethernet service OAM and PM:
  - IEEE 802.1ag Connectivity Fault Management (CFM)
  - MEF Ethernet Local Management interface (e-LMI)
  - ITU-T Y.1731: OAM for Ethernet-based networks
- 2) MPLS VPWS service OAM and PM:
  - Virtual Circuit Connectivity Verification (VCCV) [RFC 5085]
  - Pseudo-Wire OAM: Pseudo-Wire Ping,
  - Bidirectional Forwarding Detection (BFD) [RFC 5880]
  - IP SLA PM based on CFM.
- 3) MPLS VPLS service OAM and PM:
  - VCCV
  - Pseudo-Wire OAM: Pseudo-Wire Ping,
  - BFD
  - IP SLA PM based on CFM
- 4) IP/MPLS VPRN services OAM and PM:
  - IP and VRF ping and trace route
  - BFD single and multi-hop failure detection
  - IP SLA PM based on CFM

#### 7.14.2.3 Transport OAM

Transport OAM is a set of network-oriented mechanisms that operate and manage the network infrastructure. It is ubiquitous in the network elements that make up the network infrastructure, and it is primarily used for monitoring health and performance of the underlying transport mechanism on which the services are operated and carried.

The primary purpose of Transport OAM is to keep track of the state of the transport entities (MPLS LSP, Ethernet VLAN, etc.). It monitors the transport entities to ensure that they are up and functional and performing as expected, and provides the mechanisms to detect, verify, and isolate the faults during negative network events. The following protocols are the building blocks of Transport OAM:

- 1) Ethernet Transport OAM and PM:
  - IEEE 802.3ah: Ethernet Link OAM
  - IEEE 802.1ag Connectivity Fault Management (CFM)
  - ITU-T Y.1731: OAM for Ethernet-based networks
  - IP SLA PM based on CFM
- 2) IP/MPLS Transport OAM and PM:
  - BFD single and multi-hop failure detection

- IP and MPLS LSP “ping” and “traceroute”
- IP SLA PM
- G-ACh-based OAM and PM for MPLS-TP LSPs

## 7.15 Time synchronization

### 7.15.1 Oscillator stability

The achievable frequency stability of clocks depends on the technology and particularly on the temperature range as shown in Table 50.

**Table 50 – Typical oscillator stability**

Type	Abbreviation	Suited for stratum [ANSI T1.101] <sup>1)</sup>	Drift (free-running) <sup>2)</sup>	Conditions
Hydrogen maser	–	1 Time and frequency definition	-	laboratory
Cesium atomic clocks (distributed over GPS or radio)	CeO	1 Primary Reference Clock (PRC)	-	constant temperature
Rubidium atomic clock (synchronized sporadically e.g. by GNSS)	RbO	1	±0,01 ns / s ±2 µs / day ±8 ms / year	–25 °C to 70 °C
Oven-controlled crystal oscillator	OCXO	2	±10 ns / s ±1 ms / day ±0,4 s / year	constant temperature
Temperature compensated crystal oscillator	TXCO	3	±50 ns / s ±5 ms / day ±16 s / year	0 °C to 60 °C
Controlled cell phone crystal oscillator	CXO	4	±2,5 µs / s (GSM) ±1,5 µs / s (UMTS)	commercial range
Wristwatch crystal	XO	4	±6 µs / s ±0,5 s / day	at constant (body) temperature (31 °C)
NOTE 1 This definition of stratum differs from the NTC stratum definition.				
NOTE 2 The ambiguous term “ppm” for frequency stability has been replaced by IEC.				

The Primary Reference Clock (PRC) is the clock that supplies the frequency reference.

The Primary Time Reference Clock (PTRC) is the clock that supplies the time reference

A clock is “traceable” when it receives its reference from a better clock that is itself hierarchically connected up to a stratum 1 clock. This does not mean that the connection is continuous, as the signal is intermittent, but sufficiently frequently resynchronized to guard its accuracy. Traceability includes the ability to adjust leap seconds.

Typically, a clock is traceable while it receives the GPS signal. When a clock that was previously traceable loses the connection during a certain time, it enters “holdover”. In reality, the clock enters holdover time immediately after reception of a synchronization signal and remains in “holdover” as long as it can maintain its accuracy class.

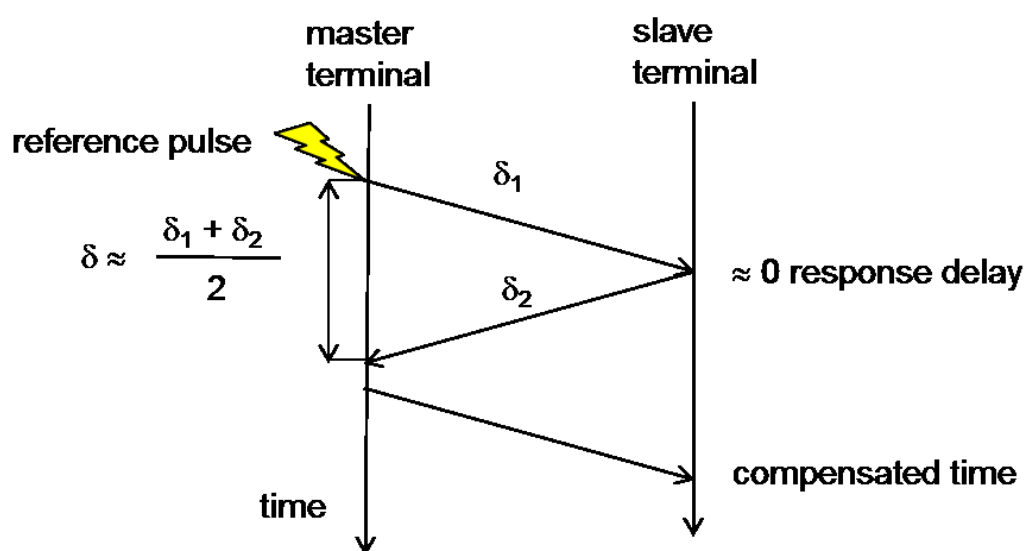
### 7.15.2 Mutual synchronization

In many applications, the absolute time is not important, but the relative time between two events is. If a direct physical link with a known propagation delay exists between the communicating partners, the parties can synchronize mutually their clocks and time-stamp

their samples. Calculating and compensating the asymmetry (if it is predictable) increases precision. This is the solution teleprotection has been using for years for differential protection, which leads to the requirement in 6.2.4.

Figure 116 shows a time synchronization scheme for conventional numerical current differential protection relays. A slave node can adjust its own timing to the master reference timing by measuring the time difference of pulse transmission and reception. This assumes that the latency is symmetrical on both ways, which is the case for direct lines, but also for PDH, SDH/SONET and other TDM networks. The end-to-end timing synchronization error remains below a few microseconds in legacy PDH networks.

Packet switching networks that allocate paths dynamically do not guarantee symmetry. Especially in IP networks, packets of the same session can take different paths, and the path is not necessarily the same on the forward and backward paths. MPLS can provide path coherency with proper engineering, but even so, residence delays in routers will be different in the forth- and back paths and mutual synchronization cannot be used on PSN unless an additional synchronization exists (see 7.10.5.1)



IEC

**Figure 116 – Timing pulse transmission methods of legacy teleprotection devices**

### 7.15.3 Direct synchronization

In substations, synchronizing the devices by dedicated wires (star, tree or daisy-chain-like) is frequent.

- The 1 PPS method sends just a precise pulse, which allows synchronizing on the second.
- The IRIG-B transmission allows distributing also time-of-day, also using a dedicated fiber. Such methods do not scale up to WANs and they are no further considered.

The source of 1 PPS or IRIG-B is generally a GNSS radio signal often with a high-stability oscillator for back-up.

### 7.15.4 Radio synchronization

Direct synchronization by radio is sometimes used (e.g. WWV Boulder, DCF-77 Frankfurt), but conditions within the substation may prevent reception and external antennas are not popular.



### 7.15.5 GNSS synchronization

GPS or in general GNSS allow a sub-microsecond synchronization in fixed locations. Given the low cost of GPS receivers, it would be tempting to give each IED or PMU its own satellite receiver.

However, the GPS signal can be easily jammed (intentionally or by solar storms) or spoofed.

The signal may also be intermittent, for instance if the substation is located in a deep valley. In case of war, the GPS signals could just cease.

For that reason, many utilities are concerned about relying on GNSS synchronization for critical operation functions such as differential protection.

Utilities turn to high-precision clocks (Rubidium, Cesium) tuned by multiple GNSS receivers, and use the network itself to distribute frequency and time to the end devices.

### 7.15.6 Frequency distribution

#### 7.15.6.1 Frequency distribution by SyncE

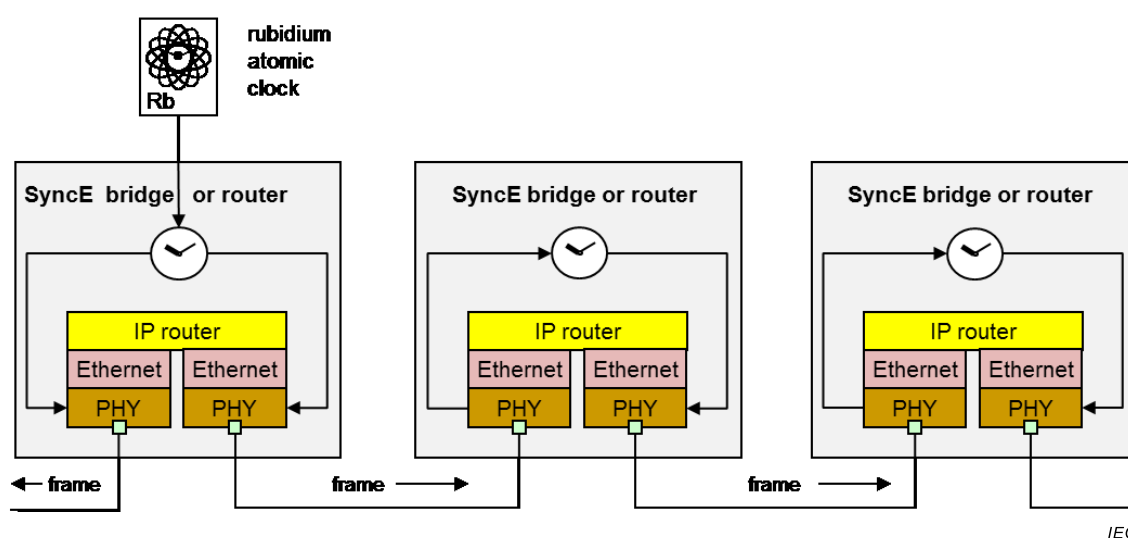
##### 7.15.6.1.1 SyncE principle

ITU-T G.8261 (Architecture), ITU-T G.8262 (clocks) and ITU-T G.8264 (synchronization message channel) describe SyncE, which uses Ethernet frames to the transport of precise frequency, with the same precision as SDH/SONET. However, SyncE only distributes frequency, not phase or absolute time.

The original frequency comes from a high-precision atomic clock. SyncE introduces at the physical layer a frequency clock signal between communication equipment, so all equipment operate exactly at the same frequency. The receiving device uses the bit rate of the sent Ethernet frames to synchronize its clock over a phased-locked loop.

To ensure proper transfer of the timing signals, all equipment in the entire network must support SyncE.

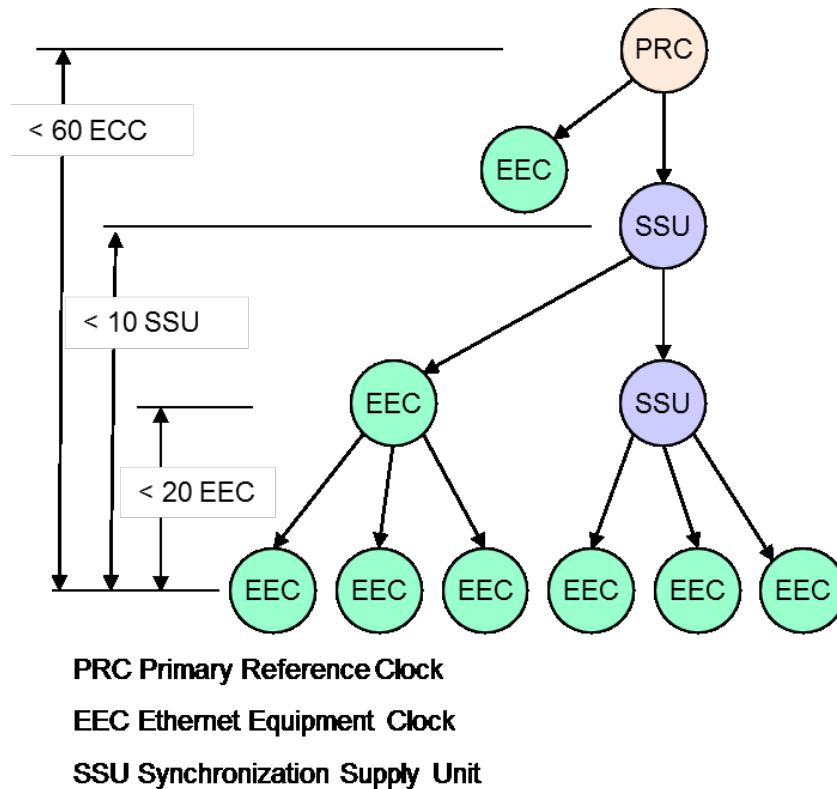
This technology allows connecting two or more SDH/SONET networks via Ethernet. It is gaining acceptance for connecting mobile telephony base stations and improving the time synchronization by providing a stable frequency reference (Figure 117).



IEC

Figure 117 – SyncE application

Similar as for SDH/SONET networks, synchronization signals are distributed in a hierarchical manner, hop-by-hop (Figure 118). Each SyncE equipment has an internal clock feeding the physical layer. Consequently, the entire network is acting as a synchronous network. Synchronization for SDH can be transported via SyncE networks and vice versa.



IEC

Figure 118 – Synchronous Ethernet Architecture

#### 7.15.6.1.2 SyncE Clocks (G.8262]

Ethernet Equipment Clocks (EEC) are defined in accordance with SDH / SONET networks with dedicated criteria regarding accuracy, noise transfer, noise tolerance, noise generation as well as holdover performance. EECs must comply with a minimum accuracy of  $\pm 4,6 \mu\text{Hz/Hz}$ , which is about 20 times more stable than the standard Ethernet clocks ( $\pm 100 \mu\text{Hz/Hz}$ ), to account for signal losses and drift between frames.

#### 7.15.6.1.3 SyncE Messaging Channel (G.8264)

In SyncE, the Ethernet Synchronous Messaging Channel (ESMC) signals the quality of the source of the synchronization signal to the receiving equipment. These heart beat messages use the Organization Specific Slow Protocol (OSSP) protocol defined in IEEE 802.3.

#### 7.15.6.2 Frequency distribution by IEC 61588 (G.8264)

ITU-T G.8265 specifies the “Telecom Profile”, a frequency distribution that uses IEC 61588 at Layer 3 with end-to-end path delay measurement.

### 7.15.7 Time distribution

#### 7.15.7.1 Time distribution by NTP/SNTP

The most widespread time distribution protocols in WANs operate over Layer 3:

- Network Time Protocol (NTP) [RFC 5905]
- Simple Network Time Protocol (SNTP) [RFC 4330], which is specified in IEC 61850-8-1 for the traffic within substations.

NOTE The definition of “stratum” differs in NTP and NIST.

Most personal computers implement SNTP as part of their operating system communication stack. Usual implementations provide accuracy of about 1 ms within a substation LAN and of 10 ms across a WAN.

NTP/SNTP operates over UDP/IP using port 123, and therefore crosses routers.

NTP/SNTP defines a clock hierarchy of several levels, called stratum.

The SNTP clock synchronization is initiated by the client (slave clock), who sends a time request to the server (master clock, higher stratum), which responds with the current time, as shown in Figure 119 a (upper exchange).

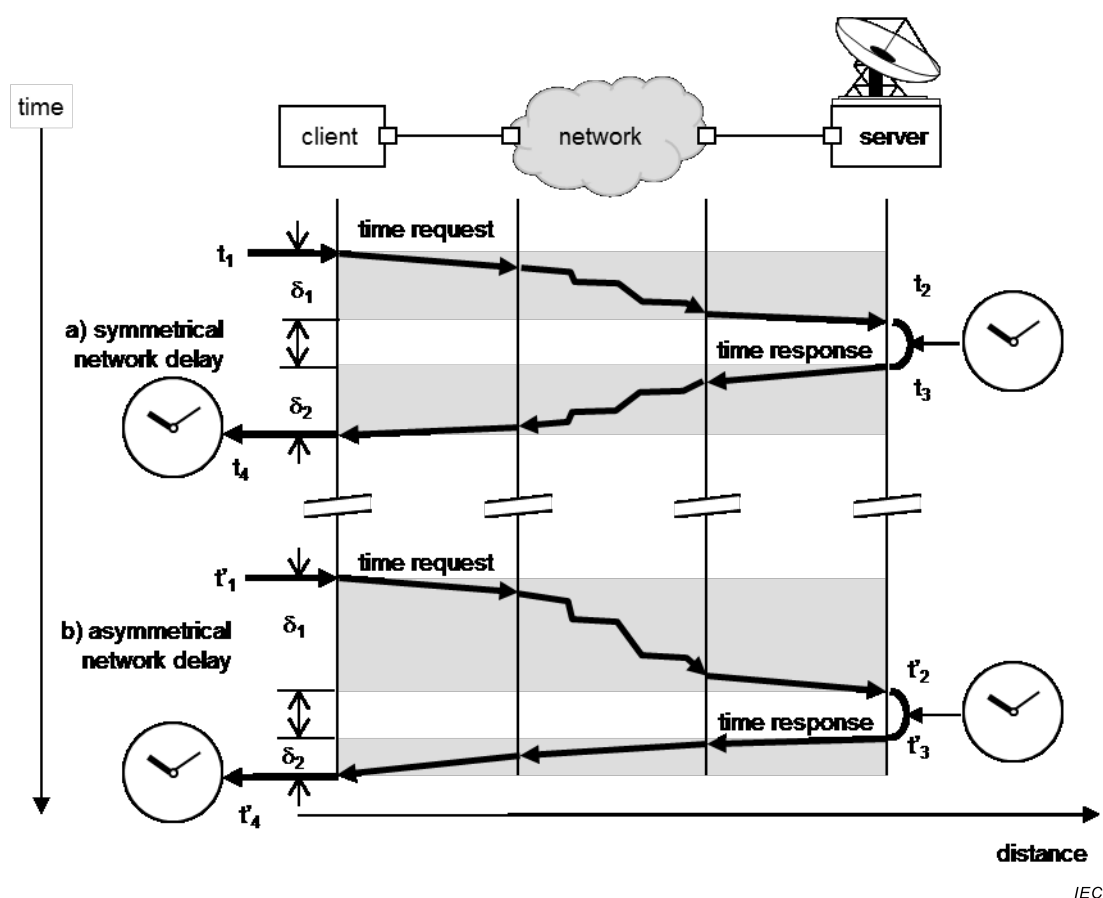


Figure 119 – SNTP clock synchronization and network delay measurement

The client needs to compensate for the delays in the network by calculating the round-trip delay between the clock server and itself. To this effect, the client registers its local time when sending the request (transmit timestamp) and registers its local time when receiving the response (receive timestamp). The server also registers its local time when it received the request and includes this time in the response, together with the time at which it sent the response. The client adds to the clock time the network delay  $\delta$ , which it estimates as:

$$\hat{d} = \frac{(t_4 - t_1) - (t_3 - t_2)}{2}$$

Where

- $t_1$  is the time the client sent the request,
- $t_2$  is the time the server received the request,
- $t_3$  is the time the server sent the response,
- $t_4$  is the time at which the client received the response.

This calculation assumes that the delays in the network are symmetrical, i.e. the request and the response take the same path and that each router takes the same amount of time to treat each message, which is not the case in a PSN.

For instance, the lower Figure 119b shows an asymmetrical round trip delay which then leads to an incorrect estimation of the network delay. Algorithms consider the average over several measurements and known asymmetries.

This method is limited by uncertainty due to asymmetrical latency and varying residence delays in the routers and bridges, possibly due to overload and route changes. This uncertainty cumulates with the number of hops.

The time-stamping in NTP is imprecise, since NTP clocks usually handle the protocol in software over Layer 3 and time-stamp with no hardware support.

Routers do not correct their residence delay, and therefore the PDV affects time accuracy.

NTP allows clients to request time from multiple servers. This can improve client synchronization by evaluating different sources, identifying degraded sources and penalizing noisy network paths.

For precise synchronization using SNTP, network engineers should care that the network presents a symmetrical behavior regarding the path that a time request and time response take. Routers can enforce it by using pre-established routes rather than routes chosen depending on the network load.

This requirement makes it difficult to achieve a high accuracy in a NTP in a WAN, since many routing protocols (in particular IP) cannot ensure that the reply takes the same path as the request.

SNTP carries UTC, although some interpret it as TAI. The 64-bit timestamps used by NTP consist of a 32-bit seconds counter and a 32-bit fractional second part, giving NTP a time scale that rolls over every  $2^{32}$  seconds (136 years) and a theoretical resolution of  $2^{-32}$  seconds (233 ps). SNTP has an epoch of first of January 1900. The first rollover will occur in the year 2036, prior to the UNIX year 2038 problem (see IETF RFC 4330), introducing a 200 ps interval in which time is invalid (all zero).

This rollover will occur within the lifespan of presently delivered devices. To mitigate this, IETF issued the concept of Era. Therefore, unless a future time format of 128 bit is used, testing is recommended.

NOTE As there exist probably no archived NTP timestamps before bit 0 was set in 1968, a convenient way to extend the useful life of NTP timestamps is the following convention: If bit 0 (MSB) is set, the UTC time is in the range [1968..2036], and UTC time is reckoned from 0 h 0 m 0 s UTC on 1 January 1900. If bit 0 is not set, the time is in the range [2036 to 2104] and UTC time is reckoned from 6 h 28 min 16 s UTC on 7 February 2036.

For more details, see IEC TR 61850-90-4.

### 7.15.7.2 Time distribution by IEC 61588 (PTP)

#### 7.15.7.2.1 IEC 61588 (PTP) principle

IEC 61588 specifies a precision time protocol with microsecond precision. To this effect, all network elements, bridges and routers, compensate for the path delay and for their residence delay. This requires that all devices support this protocol, any non-conformant network element ruins precision. For details, see IEC TR 61850-90-4 and the tutorial in IEC 62439-3: —, Annex D.

IEC 61588 is a master-slave protocol, in which one of the master-capable clocks takes initiative as master to send the time to all slave clocks.

The highest-ranking clock in an IEC 61588 time domain takes the role of GrandMaster Clock (GMC); it is generally a Primary Reference Time Clock (PRTC).

If the GMC receives its signal from a clock hierarchy connected up to the worldwide network of atomic clocks, the GMC is said to be “traceable”. Traceability includes for instance the ability to receive leap second announcements. The term “locked” indicates that the GMC receives the synchronization signals regularly.

The network elements act as:

- Ordinary Clock (OC), that can become slave or master over one port, unless it is slave-only;
- Transparent Clock (TC), a multi-port device that forwards the PTP messages and compensates for their residence delay;
- Boundary Clocks (BC), a multi-port device in which one port is slave to another BC or to a GMC and at least one other port acts as a master clock (MC) for the lower-ranking BCs or OCs. In the absence of a GMC, a BC can become GMC even if its precision is regular if it turns out to be the best remaining clock.

OCs and BCs execute the Best Master Clock Algorithm (BMCA) to ensure that only the clock with the best quality synchronizes the network and to create the distribution topology from that source clock through the BCs to each OC at the edge of the network. There exist variants of the BMCA (e.g. static provisioning, multiple active grandmasters or letting the slave clocks select their source).

IEC 61588 has three major options:

- a) Layer [L3 versus L2]: operate over Layer 3 using unicast or multicast or over Layer 2 (raw Ethernet) using multicast;
- b) Path delay measurement [E2E versus P2P]: operate with end-to-end delay measurement (IEC 61588:2009, J.3) or peer-to-peer measurement (IEC 61588:2009, J.4);
- c) Correction transport [1-step versus 2-step]: operate with 1-step correction or with 2-step correction.

For Layer 3 PTP, IEC 61588:2009, Annex D (IPv4) and IEC 61588:2009, Annex E (IPv6) apply. Although the protocol runs over Layer 4 (UDP), the hardware time-stamps the messages, which is not the case with SNTP. IEC 61588 foresees two options for Layer 3: unicast or multicast communication. Multicast communication requires that the network engineers define multicast domains at the IP layer for the clock. Unicast leads to an increase in the communication volume, it must be negotiated.

For Layer 2 PTP, IEC 61588:2009, Annex F, defines the multicast addresses to use.

Figure 120 shows a chain of TCs and BCs between a GMC and a slave clock to show the difference between transparent and boundary clocks. The boundary clock maintains absolute

time while the transparent clocks only need to calculate the residence and link delays based on the local clock. The local clock of the TCs nevertheless benefits from frequency synchronization from the boundary clock or grandmaster clock.

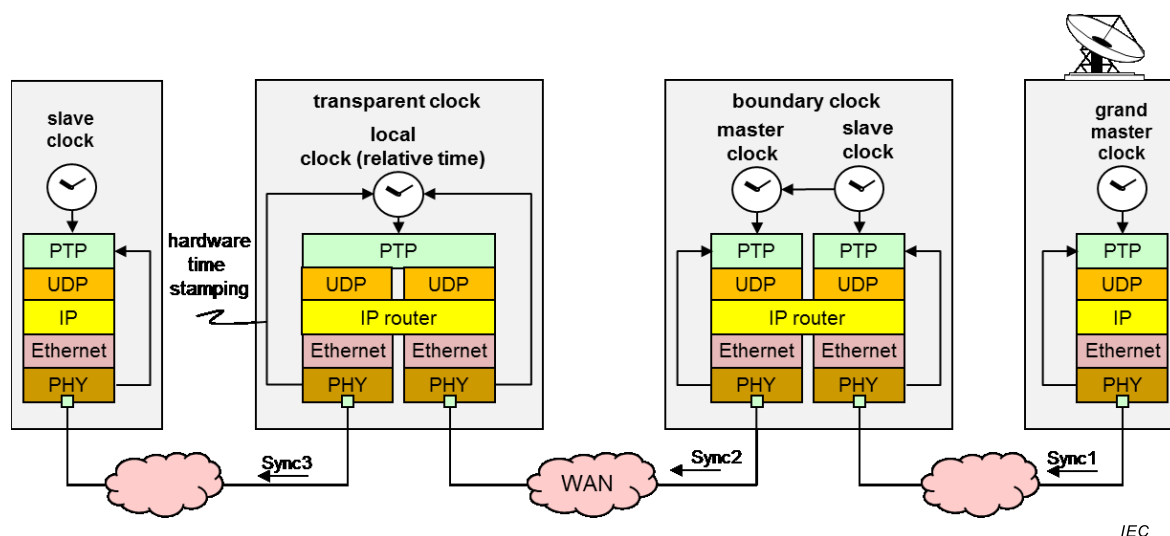


Figure 120 – Model of GMC, two BCs in series and SC over Layer 3

Figure 121 shows the timing diagram, with the BC using a different Sync period as the GMC. Of course, all periods could be the same, e.g. one second; this is simply to demonstrate that the BCs are independent.

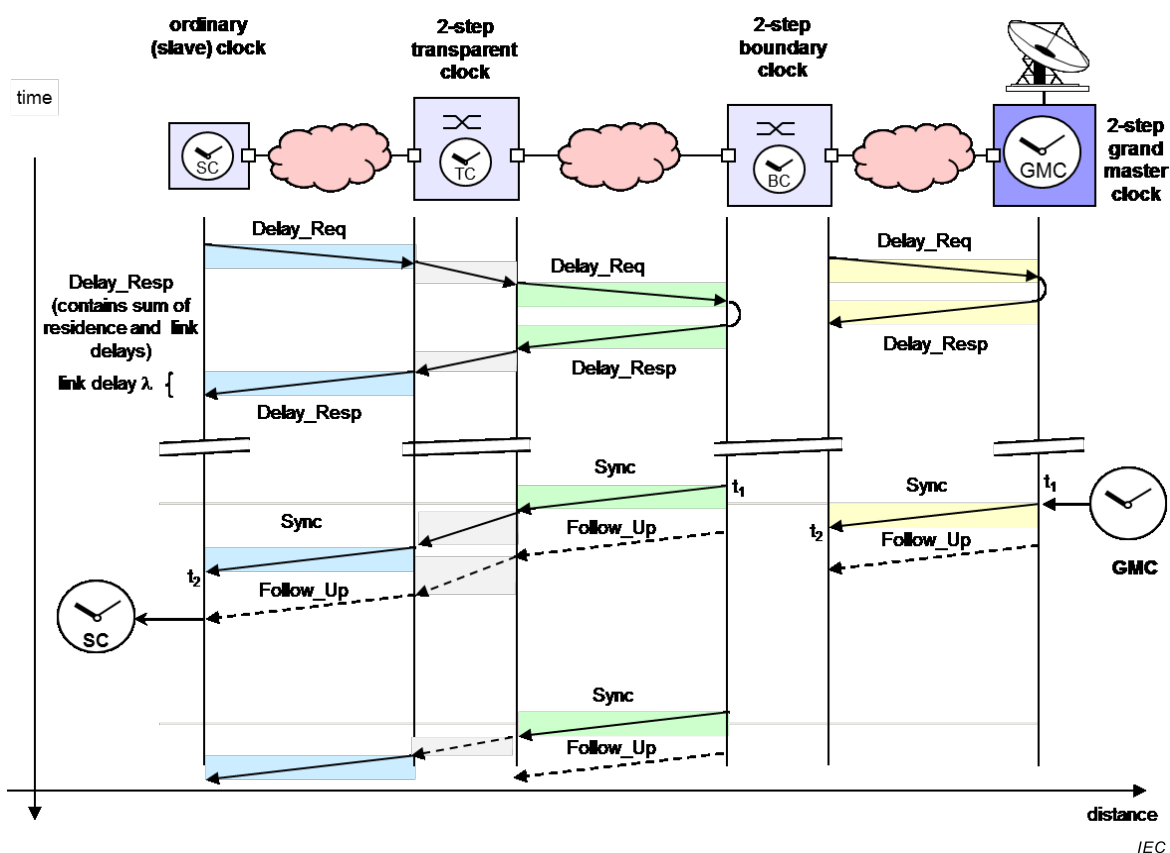


Figure 121 – Timing diagram of PTP (end-to-end, 2-step, BCs)

Figure 122 shows the synchronization messages in a network with 2-step TCs and peer-to-peer path delay measurement.

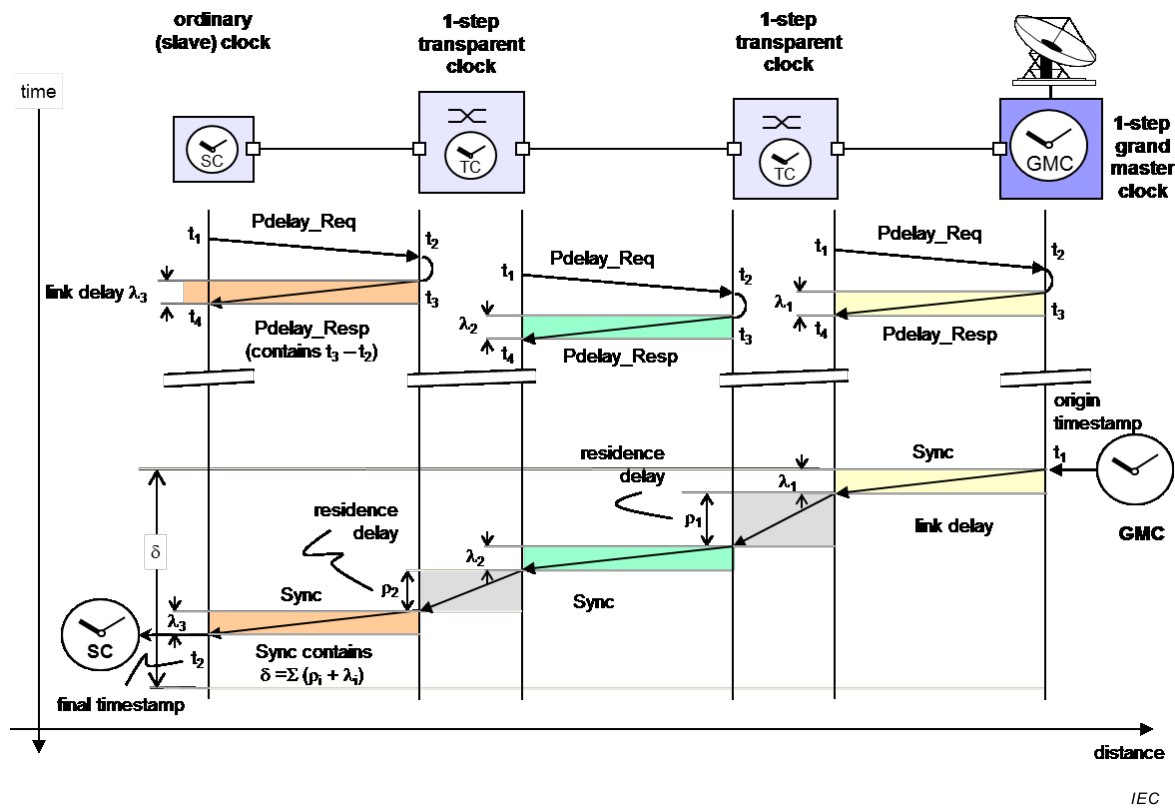


Figure 122 – Timing diagram of PTP (peer-to-peer, 2-step TCs)

Table 51 compares different options available with IEC 61588.

**Table 51 – IEC 61588 option comparison**

Type	Advantages	Drawbacks
End-to-End link delay measurement	Can work when non-PTP network elements exist (with substantially degraded performance)  Established method in WANs, Telecom Profile	Non-PTP elements severely degrade performance.  Transparent clocks are stateful in two-step correction and therefore complex.  Boundary clocks are more complex than transparent clocks  Long recovery time in case of reconfiguration  High computational load on the master, which receives all Delay_Req.
Peer-to-Peer link delay measurement	Simple method  Fast recovery since also inactive paths are checked  Master has a small computational load	Introduced only since IEC 61588:2009  Do not operate when non-PTP elements are inserted (but this is rather an advantage since it detects misconfiguration)
1-step correction	Simple method  Reduced traffic	Require on-the-fly correction of the time stamp in hardware,  Could exclude some security methods
2-step correction	Can be executed in software with hardware support only for time-stamping	Needs that Sync and Follow_Up take the same path.  Doubles the synchronization traffic
Layer 2 transmission	Simple, can be executed in hardware directly	Limited to a broadcast domain in Carrier Ethernet or MPLS
Layer 3 transmission	Can be used over routers	Use of unicast or multicast depending on the application or profile.

#### 7.15.7.2.2 PTP profiles for high-availability automation networks (IEC 62439-3)

IEC 62439-3:, Annex A, defines how a clock can be attached by two ports to two separate networks (PRP) or to two separate ring directions (HSR). A Doubly Attached Clock (DAC) operates as a normal IEC 61588 clock when only one port is operational.

IEC 62439-3 specifies additions to IEC 61588:2009:

- OCs and BCs with two ports for redundancy (two MC in different LANs);
- Handling of DACs with an extended BMCA that is identical to IEC 61588 for singly attached clocks (IEC 62439-3:—, Annex A);
- Supervision of configuration and redundancy;
- a MIB that serves several profiles, consistent with IEC TR 61850-90-4 and including the ALTERNATE\_TIME\_OFFSET\_INDICATOR TLV (IEC 62439-3:—, Annex E).

IEC 62439-3 defines two profiles of IEC 61588:2009, both of which can be used in WANs, inclusive MPLS:

- L3E2E (Layer 3, end-to-end), using IP transport as defined in IEC 61588:2009 Annex D (IPv4), respectively IEC 61588:2009 Annex E (IPv6) and the default profile with end-to-end delay measurement as defined in IEC 61588:2009 Annex J.3, but with fixed message intervals (IEC 62439-3:—, Annex C.5);
- L2P2P (Layer 2, peer-to-peer), using Ethernet transport as defined in IEC 61588:2009 Annex F and the default profile with peer-to-peer delay calculation as defined in IEC 61588:2009 Annex J.4, but with fixed message intervals of 1 s (IEC 62439-3:—, C.6). The L2P2P profile has been explicitly developed for substation-internal LANs and for WANs with Carrier Ethernet or HSR rings.



### 7.15.7.2.3 PTP power utility profile

IEC 61850-9-3 is identical to IEC 62439-3:—, C.6, but leaves double attachment of clocks as an option and differs in the profile identifier.

NOTE 1 Therefore, when IEC 61850-9-3 is mentioned, doubly attached clocks are optional, while when IEC 62439-3:—, C.6, is mentioned, doubly attached clocks are mandatory.

NOTE 2 The profile identifier of IEC 62439-3:—, C.6 and IEC 61850-9-3, differ, since they belong to different working groups of the IEC. Future developments are not necessarily coordinated.

### 7.15.8 PTP telecommunication profiles

ITU-T defined “Telecom Profiles” of IEC 61588, originally for distribution of frequency to mobile radio stations (e.g. GSM, UMTS, LTE, etc.), and later focused on time distribution, in several specifications:

- ITU-T G.8265.1 –Frequency Profile (only frequency distribution);
- ITU-T G.8275.1 – Time and Phase Profile in a network comprising BCs;
- ITU-T G.8275.2 –Time and Phase Profile in a network with non-PTP switches and routers.

These telecom profiles operate over packet-switching WANs, while remaining interoperable with SDH/SONET and SyncE.

Table 52 lists the technical details.

Since ITU-T G.8265 transmits only frequency, delay calculation is not necessary.

### 7.15.9 PTP over MPLS

IETF produced a draft [35] for time distribution over MPLS, intended to harmonize the NTP and PTP time distribution, and specifying:

- Time-stamping at the physical layer both in the LER and LSR;
- Layer 2 support in MPLS using special LSPs (Timing LSPs) using pseudowires to avoid deep packet inspection;
- Support for BCs (TCs are under consideration);
- Operation with 1-step and 2-step;
- BMCA and spanning tree for time distribution adapted to MPLS and MPLS-TP.

NOTE This draft has been returned to experimental status. In fact, IEC 61588 can be used instead when Ethernet is used as Layer 2.

### 7.15.10 Comparison of time distribution profiles based on IEC 61588

Table 52 lists the technical characteristics of the precision time protocols used over WANs (NTP and SNTP belong to a lower accuracy class and are not listed here).

**Table 52 – Precision time distribution protocols based on IEC 61588**

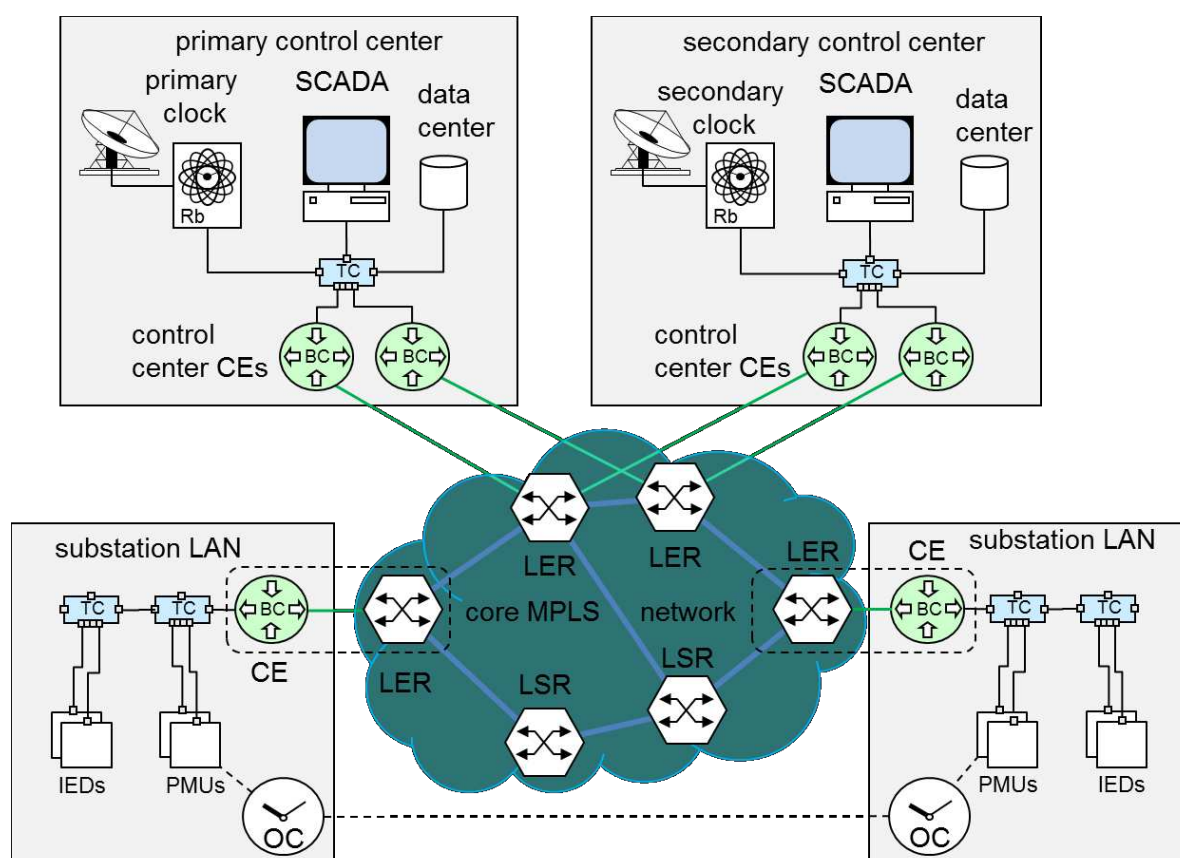
–	ITU-T G.8265.1	IEC 62439-3 L2PTP IEC 61850-9-3	ITU-T G.8275.1
Service	Frequency	Time	Time
Media	IPv4 (IEC 61588:2009, Annex D) IPv6 (IEC 61588:2009, Annex E)	Ethernet (Annex F)	Ethernet (Annex F with addresses, see below)
MAC addresses		01-90-C2-00-00-0E (Pdelay_Req / Pdelay_Resp) 01-1B-19-00-00-00 (all other messages)	for all messages 01-90-C2-00-00-0E or 01-1B-19-00-00-00 by configuration
Topology	Full- and Half-duplex	Full-duplex links	Full-duplex links
Cast	Unicast-only with negotiation	Layer 2 Multicast	Layer 2 Multicast
Clocks	OCs only	GM/OC, slave-only OC, TCs, BCs	T-GM (GM-only) T-TSC (OC slave-only) T-BC (GM-and OC able)
Path delay measurement	end-to-end	peer-to-peer	end-to-end
Steps	1-step and 2-step	1-step and 2-step	1-step and 2-step
Layer	Layer 3, IPv4 and IPv6	Layer 2	Layer 2
Redundant attachment	none	Doubly attached clocks (mandatory in IEC 62439-3)	none
Clock domains	multiple	one	multiple {24..43}
VLAN	N.A.	not specified, supported by the MIB	prohibited
Ethertype	N.A.	0x88F7	0x88F7
Subtype	–	default 0	0
Announce period [s]	Default 2 s, ≤ 16 s	1 s	1/8 s
Sync period [s]	1/128 s to 16 s	1 s	1/16 s
Delay period [s]	1/128 s to 16 s for Delay_Req	Pdelay_Req 1 s	1/16 s (± 30 %) for Delay_Req
Supervision	Announce time-out	Timeouts on all messages	Announce time-out
Precision	Not specified	1 µs after 15 TCs	1,1 µs after 10 BCs
Local clock precision	–	50 ppm needed	–
Transmission of clock accuracy / precision	Clock Class set based on frequency source QL (SSM or ESMC).	uses ClockQuality in Announce messages	ClockQuality values based on GNSS lock or not
Syntonzation	–	necessary	–
Time base	PTP (TAI)	PTP (TAI)	PTP (TAI)
Leap seconds	N.A.	handled	N.A.
Holdover time	–	5 s	–
BMCA	Fixed masters and slaves, alternate BMCA,	BMCA extended for doubly attached clocks (PRP/HSR) only	alternate BMCA, includes portDS.notSlave state several grandmasters active
Backup master	alternate master	default BMCA	alternate master
Signaling	used for negotiation	unused	unused
Management	for further study	unused	for further study
MIB	not specified	MIB in IEC 62439-3 and IEC TR 61850-90-4	not specified
Profile TLV	none	none	none
Security	recommendations	not specified	not specified

### 7.15.11 Use Case: Synchrophasor time synchronization

IEEE C37.118 does not indicate how to obtain the primary clock that gives the common time reference to several substations and PMUs. For instance, every substation could have a GNSS receiver. Many utilities however consider GNSS to be unreliable, especially in regions where sun storms can disturb the ionosphere, where substations are located below ground or just because of fear of jamming or spoofing.

The alternative is synchronization through the WAN, with atomic clocks located at strategic places, as shown in Figure 123 (see also Figure 124). The GNSS connection is used for periodic alignment in time, a continuous signal is not needed.

For redundancy, connection to the WAN takes place over several routers (CEs or LERs). The BMCA cares for failover. If the whole network supports PTP, all clocks know the identity of their grandmaster and this allows checking if all synchrophasor sensors are synchronized to the same time source.



IEC

**Figure 123 – Substations synchronization over WAN**

WANs of different technology (TDM, MPLS) and profile (Layer 2, Layer 3) that need a single time synchronization can be connected by a BC. A BC can have different time protocols on different ports.

### 7.15.12 Use case: Atomic Clock Hierarchy

Figure 124 shows an example of deployed hierarchical atomic clocks. The time distribution relies on 18 rubidium clocks and of 4 cesium clocks. Each island is independent, within each island there are several redundant clocks, one Ce and 3 to 5 Rb clocks.

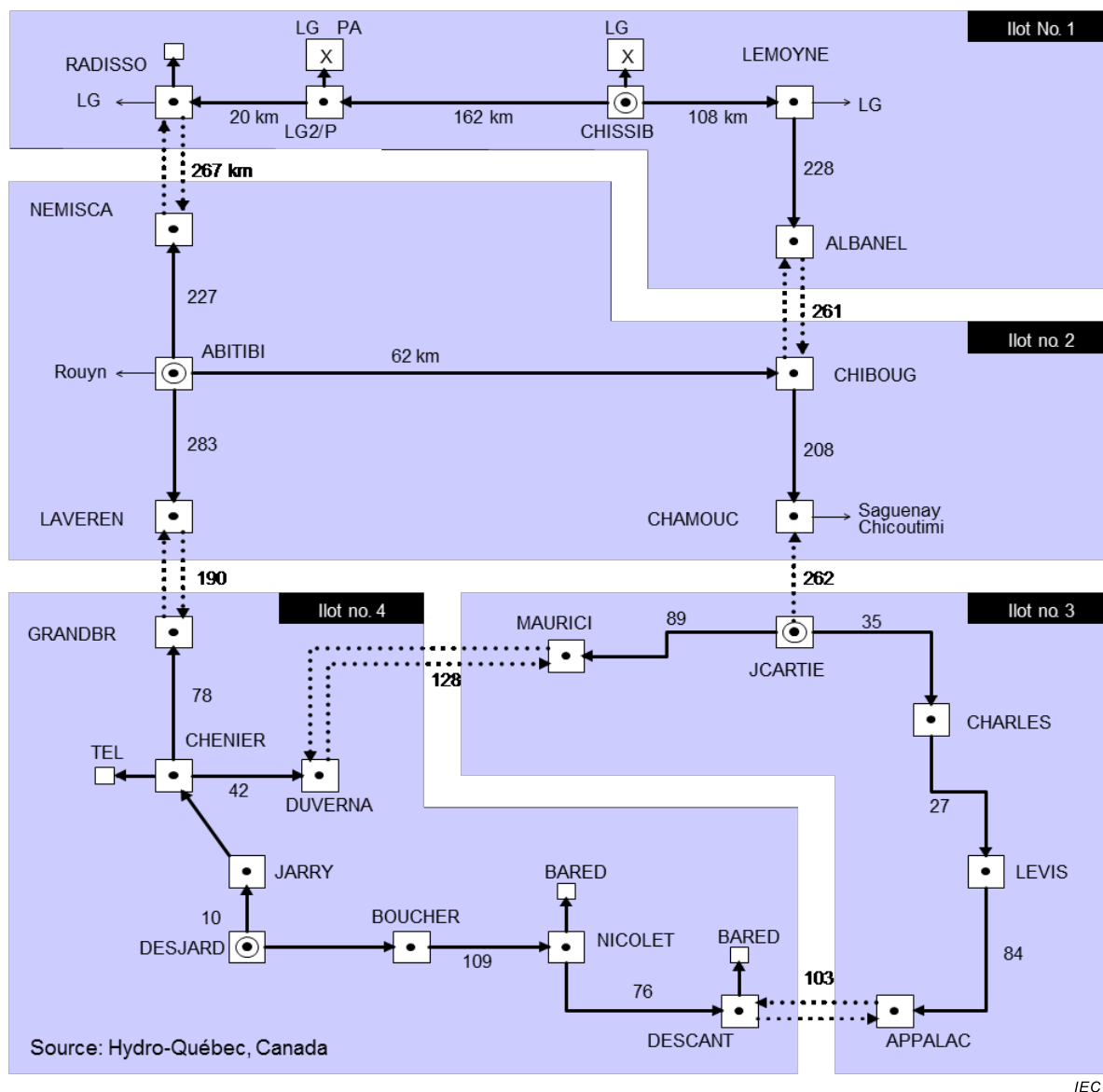


Figure 124 – Example of synchronization network

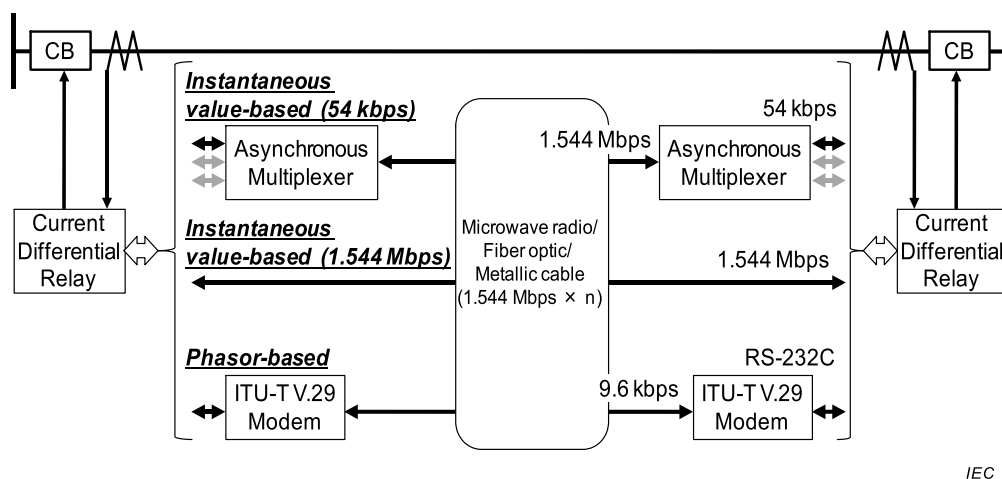
## 8 Use cases

### 8.1 Use case: Current differential teleprotection system (Japan)

This system has been in operation by TEPCO since January 2013 [47], [51]

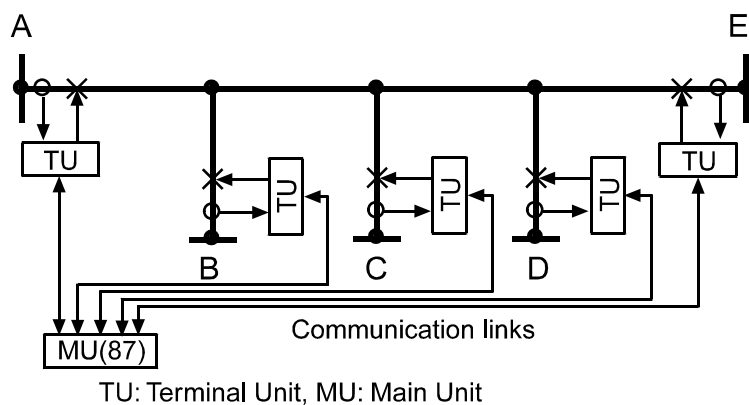
System configurations include 1:1, centralized multi-terminal protection configuration, and distributed multi-terminal protection configuration.

Figure 125 shows the 1:1 configuration where various communication channels can be selected.



**Figure 125 – Current differential 1:1 configuration**

Figure 126 shows an example of line protection for a five-terminal EHV line. Each terminal has a terminal unit that detects the current and transmits the data to the main unit terminal via a communication channel. This configuration simplifies the terminal units and communication channels. Since the main unit has current data of all terminals, the fault locator function can be easily implemented by using these data.

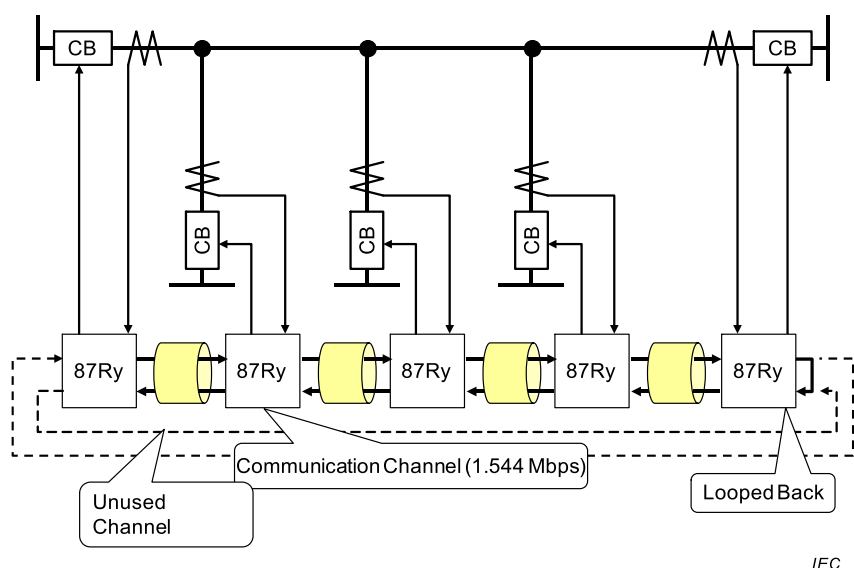


**Figure 126 – Network configuration for centralized multi-terminal line protection**

Figure 127 shows a distributed configuration of five-terminal current differential line protection system. Each terminal has the current differential protection function as well as the signal transmitting function that multiplexes current data at each terminal into one communication signal.

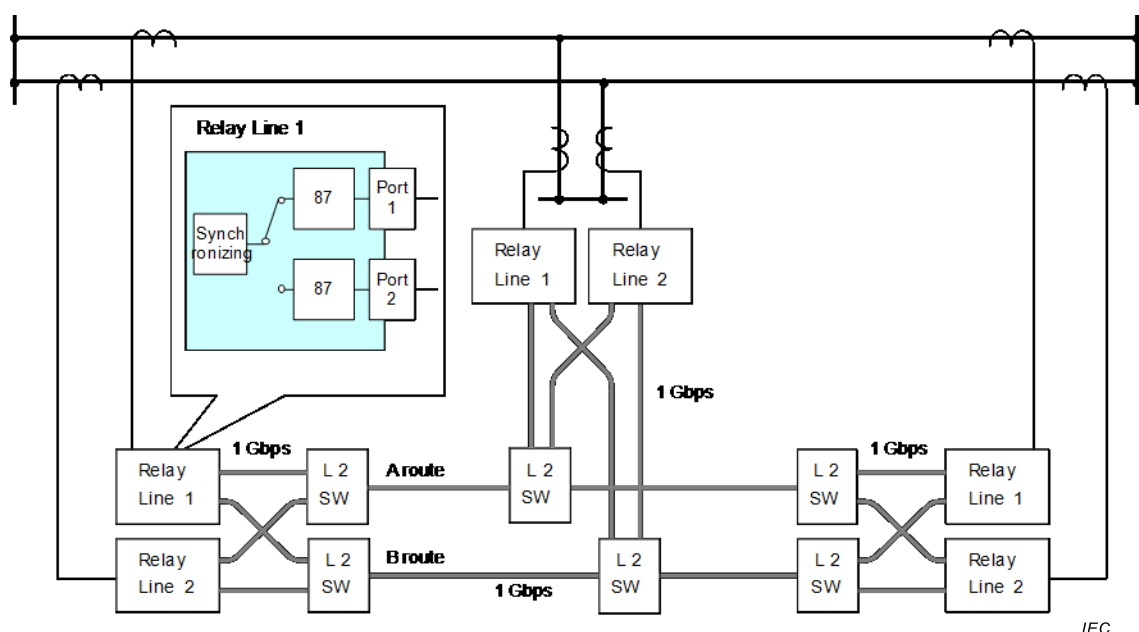
Master station A sends its own current data to slave station B. Slave stations B, C, D and E multiplex their current data over communication signal. Slave station E turns back this signal toward slave station D. Now current data of all terminals are on communication line and available for protection.

In addition, this system contains sampling synchronization function that enables the simultaneous sampling of current data at each terminal with high accuracy. Many installations were conducted using a 1,544 Mbit/s fiber-optic communications channel for HV double-circuit multi-terminal (up to ten terminals) or tapped lines. In this network configuration where current differential calculation is usually carried out at each terminal, a centralized scheme where only master station conducts the calculation and sends the transfer trip signal to all slave stations is also available.



**Figure 127 – Network configuration for distributed multi-terminal line protection**

Delay performance analysis of Layer 2 and/or Layer 3-based networks for current differential teleprotection indicates that a Layer 2-based network is easily applicable to the wide-area application. A current differential teleprotection system for HV transmission line using Layer 2 network dedicated to protection systems was developed as shown in Figure 128.



**Figure 128 – Current differential teleprotection for HV multi-terminal transmission line using Layer 2 network**

Conventional current differential relays use a dedicated hardware to measure the timing of sending and receiving in order to perform sampling synchronization.

However, a general purpose Network Interface Controller (NIC) cannot measure this timing. As a solution, a timing measurement circuit was added inside the relay to measure the timing of sending and receiving. In addition, Ethernet frame with VLAN tag based on IEEE802.1Q is

applied. However, the collision of data frame used for calculation of current differential relays and synchronizing frame affects the precision of sampling synchronization.

This issue is solved by prioritizing the synchronizing frame. Verification tests have shown a sampling synchronization performance comparable to the conventional current differential relay systems. In addition, during switching of transmission routes, the conventional system loses its protection functions whereas this system eliminates such issue by redundant transmission routes and relay functions. This also solves the IP network's low reliability.

The above mentioned Ethernet-based line teleprotection (primary protection) can be extended to wide area (covering tens of substations and hundreds of kilometers of transmission lines) current differential backup teleprotection utilizing Carrier Ethernet and time synchronization such as IEC 61588 as shown in Figure 129 where operation sequences are illustrated with the numbers in parentheses.

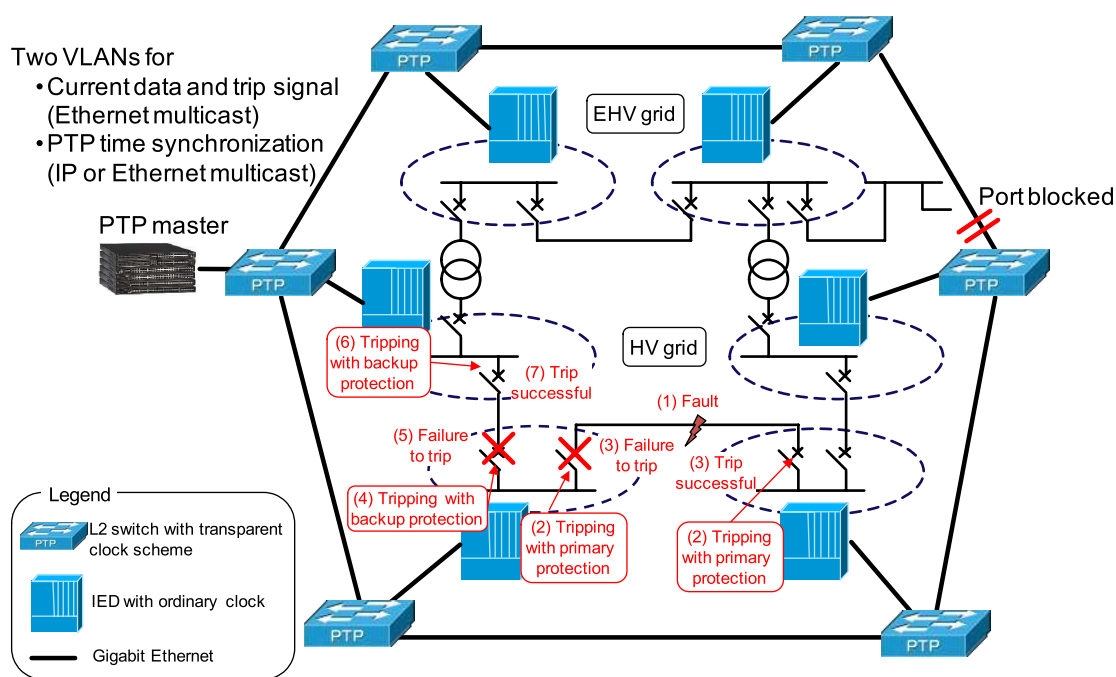
While conventional distance relay-based backup protection needs zone and operation time coordination among distance relays that leads to slower operation for some faults, the current differential backup protection does not need such coordination, and can operate faster than existing distance relay-based backup protection, which helps improve stability against transmission line and busbar faults.

The system can extend its operation zones with successive failures to trip, calculating the current differential algorithm using the data sampled simultaneously at each terminal and multicast to all relevant terminals thanks to the wide area time synchronization and VLANs.

The system has two VLANs; one for sampled current data and trip signals transmitted 12 times per cycle and the other for IEC 61588 TCs with Delay\_Req or Pdelay\_Req messages transmitted every 6 s to 10 s and Sync messages every 1 s.

While there are some IEC 61588 options to be chosen such as a clock scheme, E2E or P2P transparent clock, and Layer 2- or Layer 3-based operation, the implementation depend on its network availability and operational requirements, as IEC 61850-9-3 recommends P2P over Layer 2.

For the clock redundancy, the best master clock algorithm is applied. The time synchronization accuracy is better than 1  $\mu$ s, which is fully satisfactory for the wide area current differential processing.



IEC

**Figure 129 – Configuration of wide area current differential primary and backup teleprotection system employing Carrier Ethernet and IEC 61588 time synchronization**

## 8.2 Use case: SDH / MPLS network (Japan)

The following describes a deployment of a mixed SDH/MPLS network serving the purpose of power system telemetry and telecontrol (SCADA) and facility maintenance for the Shikoku Electric Power Company (YONDEN) in Japan [42], [54].

Figure 130 shows the network configuration. To meet the requirements (Table 53), technologies such as MPLS-VPN, VRRP, MPLS-TE and path protection were employed as shown in Table 54.

This is a mix of IP/MPLS for the backbone network and Ethernet over SDH rings for the regional network, all of which are owned by the utility company. The IP messages from the LAN over SDH are tunneled into the backbone router network comprising L3VPNs where the routers perform BGP to route the messages by distributing and advertising routes, but do not perform NAT. Those VPNs are configured by using VRF in accordance with each application system need. The commissioning and testing were conducted by the communication department and a network integrator for half a year. The communication department also plans and manages IP addresses.



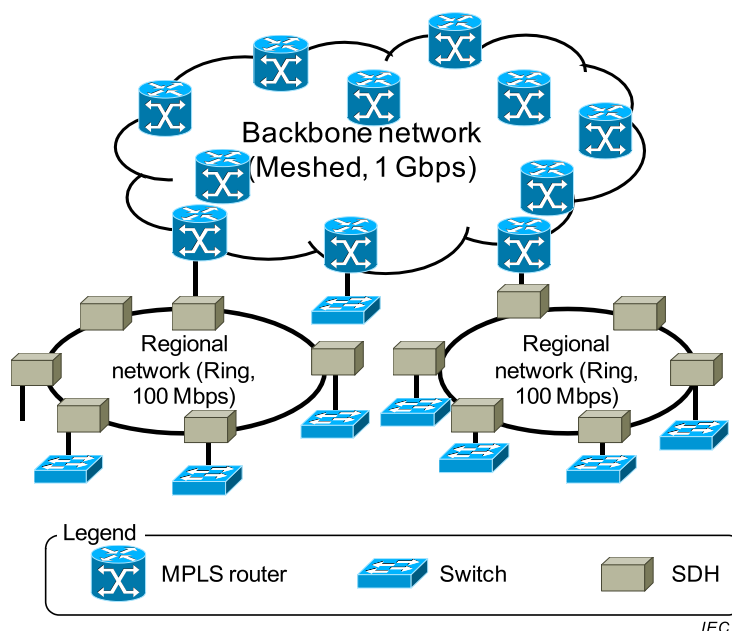


Figure 130 – Achieving protection for teleprotection services

Table 53 – Requirements for the YONDEN IP network

Item	Specification
Reliability	Logical separation of application communication
Unavailability (Down time ratio)	$7 \times 10^{-5}$
End-to-end latency	150 ms
Redundancy	Two separate redundant routes between ends
Recovery Delay	Less than 4 s

Table 54 – Technologies for the YONDEN IP network

Item	Description	Applied technologies			
		VPN (BGP, MPLS-VPN)	Router redundancy (VRRP)	Route management (MPLS-TE)	Rapid rerouting (Path protection)
Reliability	Logical separation	✓			
Redundancy	Separate route Recovery delay		✓	✓	✓
Functionality	Layer 2 and Layer 3 function	✓			
Scalability	Simple & scalable setting	✓			
OAM	Route and network management			✓	
Economy	Accommodation of various applications	✓			

### 8.3 Use Case: Wide area stabilizing control system (Japan)

A WAMPAC for transient stability phenomenon is in service in Japan since 2005.

Figure 131 shows a WAMPAC system for transient stability phenomenon and Figure 132 shows the appearance of typical equipment cabinet.

When a severe fault such as a complete loss of an important power flow route occurs, generators may lose synchronism with the grid. In this situation, this system trips generators in order to maintain synchronism between the remaining generators and the main grid.

The Central Processing Equipment (CPE), installed at a central load dispatching centre, calculates the pre-fault grid stability for the assumed severe fault case using the power system status (e.g. P, Q, V, circuit breaker status) provided by the triggering terminal equipment (RTU-S) installed in the substations. In addition, it considers the load dispatching information received over the network.

The CPE then creates a power system stability control scenario based on this pre-fault calculation and sends the control scenario table to the Central Control Equipment (CCE) installed at a control centre.

When the CCE assumes a severe fault, it sends generator tripping commands to the controlling terminal equipment (RTU-T) installed at the power stations.

The communication among equipment is carried out via a network owned by the utility and dedicated to protection. This network uses PDH-based microwave radio links. The main specifications including communication requirements are shown in Table 55.

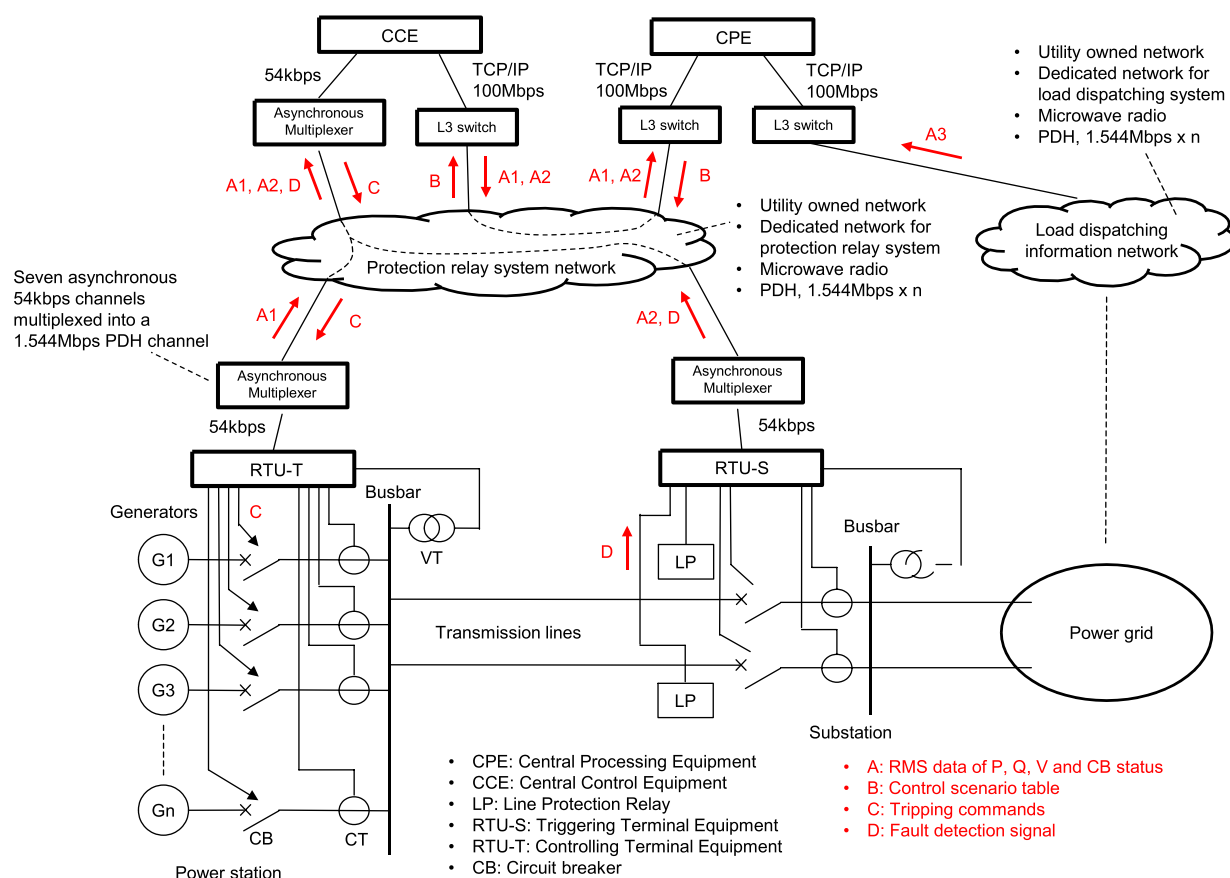


Figure 131 – System configuration for wide area stabilizing control system



**Figure 132 – Appearance of typical CCE cabinet**

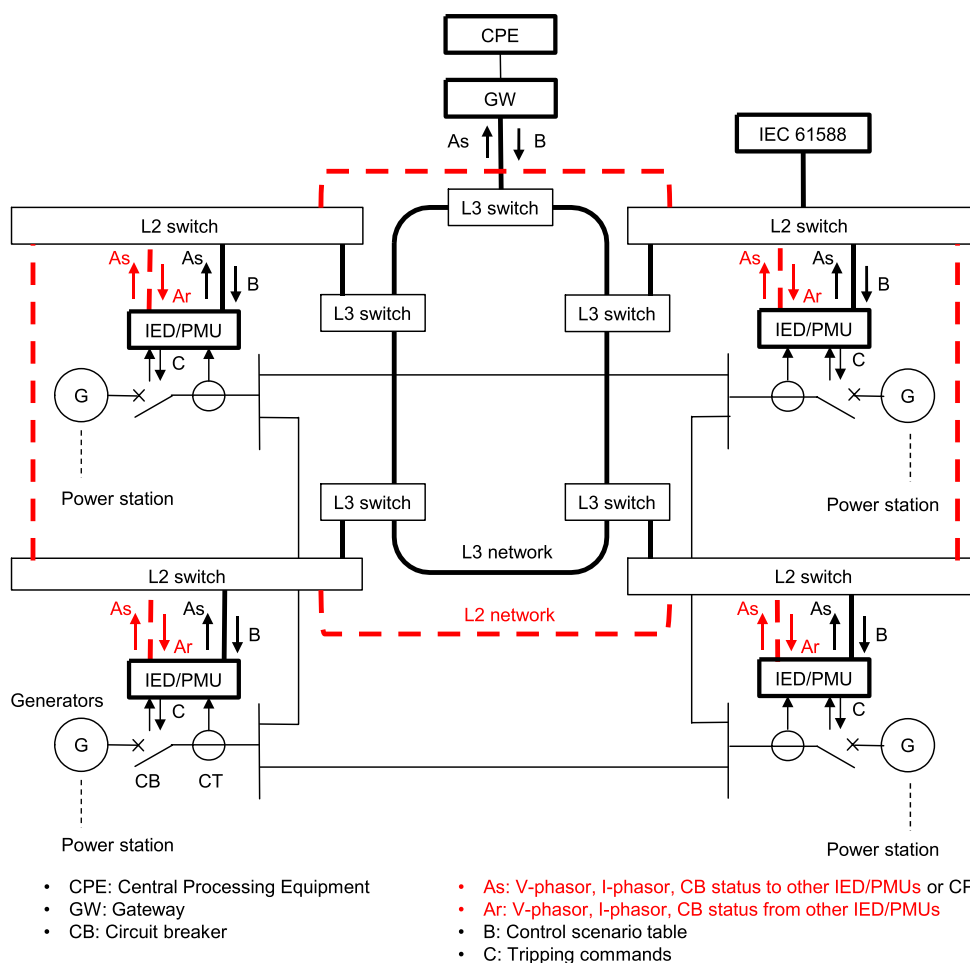
**Table 55 – Main system specifications for wide area stabilizing control system**

Item	Specification
Equipment	CPE: redundant configuration, installed at a central load dispatching centre CCE: redundant configuration, installed at a control centre RTU-S: redundant configuration, approx. 5 sets installed at substations RTU-T: redundant configuration, approx. 10 sets installed at power stations CPE – CCE: approx. 20 km CCE – RTU-S/T: approx. 400 km
Operating delay	Less than 150 ms from fault occurrence to generator tripping
Latency	CCE – RTU-S/T: less than 10ms
Network	Utility owned network Dedicated network for protection relay system Microwave radio PDH, 1,544 Mbit/s × n
Protocol	CPE – CCE: Ethernet, TCP/IP, 100 Mbit/s, approx. 25 kbytes data CCE – RTU-S/T: Cyclic, 54 kbit/s, approx. 100 bytes data

#### 8.4 Use Case: experimental PMU-based WAMPAC system

Synchrophasor is one of the appropriate measuring quantity which can be covered almost all applications for WAMPAC system. Furthermore, international communication standards related to WAMPAC system have been recently developed. The establishment of WAMPAC system based upon PMU and international standards such as IEC 61850 series is expected from this situation and development and evaluation of this kind of WAMPAC system have been ongoing, [52], [53]. A preliminary WAMPAC system based upon PMU and international standards was constructed.

Figure 133 shows the grid and network topology.



IEC

**Figure 133 – Configuration for PMU-based WAMPAC system**

This system is composed of Central Processing Equipment (CPE), gateway equipment (GW), four IEDs as power system stability control devices with PMU function (IED/PMU). In this example, IED/PMU means one integrated device with controlling and measuring functions, however IED and PMU can also be independent devices for controlling and measuring. Power system stabilizing control functions for transient stability phenomenon were implemented and evaluated.

It is supposed that each IED/PMU is installed at each power station and IED/PMU sends synchrophasor data (e.g. I, V) and circuit breaker status information to CPE via a Layer 3 network and GW. The same information is sent simultaneously to other IED/PMUs via a Layer 2 network to decrease latency in the IED/PMU for the power system stability control function.

The CPE creates a grid stability control scenario for an assumed severe fault based upon pre-fault power system stability calculation and send the control scenario table to the IED/PMUs.

GW is communication equipment which has Phasor Data Concentrator (PDC) function and communication function to send the control scenario table from CPE to IED/PMUs. When the assumed severe fault is detected in IED/PMU, IED/PMU sends generator tripping commands based upon the control scenario table to maintain synchronization in a power system.

In this system, it is supposed that the communication among IED/PMUs is carried out via utility owned Layer 2 network and the communication between IED/PMU and GW is carried

out via utility owned Layer 3 network. The main specifications including communication requirements are summarized in Table 56.

**Table 56 – Specifications for PMU-based WAMPAC system**

Item	Specification
Equipment	CPE: installed at a central load dispatching centre GW: installed at a central load dispatching centre IED/PMU: four units, installed at a power station, integrated device with controlling and measuring functions (possibly as independent devices as IED and PMU)
Operating delay	Less than 150 ms from fault occurrence to generator tripping
Latency	IED/PMU – IED/PMU: less than 5 ms IED/PMU – CPE: less than 5 s
Network	IED/PMU – IED/PMU Utility owned network (assumption) Layer 2 network (Gigabit Ethernet) IED/PMU – CPE Utility owned network (assumption) Layer 3 network (Gigabit TCP/IP, UDP/IP)
Protocol	IED/PMU – IED/PMU: IEC 61850 / SV / GOOSE, IEEE 802.Q (VLAN) IED/PMU – CPE: IEC TR 61850-90-5 / R-SV / R-GOOSE
Time synchronization	IEC 61588 Time accuracy: better than 50µs

## Bibliography

- [1] CEN-CENELEC-ETSI Smart Grid Coordination Group, *Smart Grid Architecture Model*, November 2012
- [2] CIGRE Report 461 D2.26, Telecommunication Service Provisioning and Delivery in the Electrical Power Utility, April 2011
- [3] CIGRE Report 521 D2/B5.30 Line and System Protection using Digital Circuit and Packet Communications, December 2012
- [4] CIGRE Technical Brochure No. 192, *Protection Using Telecommunications*
- [5] EPRI Report, *System and Network Management of Utility Automation Systems*, Joseph Hughes
- [6] IEC 60050-191, *International Electrotechnical Vocabulary – Chapter 191: Dependability and quality of service*
- [7] IEC 60050-192, *International Electrotechnical Vocabulary – Chapter 192: Dependability*
- [8] IEC 60050-371, *International Electrotechnical Vocabulary – Chapter 371: Telecontrol*
- [9] IEEE PSRC H12 Report R10, Report on Configuration of Ethernet Networking Devices Used for P&CI in Electrical Substations, 2001 December 11
- [10] ITU Manual 2009 – Optical fibers, cables and systems
- [11] MEF 2, Requirements and Framework for Ethernet Service Protection
- [12] MEF 3, Circuit Emulation Service Definitions, Framework and Requirements in Metro Ethernet Networks
- [13] MEF 4, Metro Ethernet Network Architecture Framework – Part 1: Generic Framework
- [14] MEF 6.1, Metro Ethernet Services Definitions – Phase 2
- [15] MEF 7, EMS-NMS Information Model
- [16] MEF 8, Implementation Agreement for the Emulation of PDH Circuits over Metro Ethernet Networks
- [17] MEF 9, Abstract Test Suite for Ethernet Services at the UNI
- [18] MEF 10.1, Ethernet Services Attributes Phase 2\*
- [19] MEF 11, User Network Interface (UNI) Requirements and Framework
- [20] MEF 12, Metro Ethernet Network Architecture Framework – Part 2: Ethernet Services Layer
- [21] MEF 13, User Network Interface (UNI) Type 1 Implementation Agreement
- [22] MEF 14, Abstract Test Suite for Traffic Management Phase 1

- [23] MEF 15, Requirements for Management of Metro Ethernet Phase 1 Network Elements
- [24] MEF 16, Ethernet Local Management Interface
- [25] MEF 17, Service OAM Framework and Requirements
- [26] MEF 18, Abstract Test Suite for Circuit Emulation Services
- [27] MEF 19, Abstract Test Suite for UNI Type 1
- [28] MEF 20, User Network Interface (UNI) Type 2 Implementation Agreement
- [29] MEF 21, Abstract Test Suite for UNI Type 2 Part 1: Link OAM
- [30] MEF 22, Mobile Backhaul Implementation Agreement Phase 1
- [31] MEF 23, Class of Service Implementation Agreement Part 1
- [32] MEF 23.1, Carrier Ethernet Class of Service – Phase 2, January 2012
- [33] MEF 24, Abstract Test Suite for UNI Type 2 Part 2: E-LMI
- [34] MEF 5, Traffic Management Specifications
- [35] IETF *Transporting Timing messages over MPLS Networks* draft-ietf-tictoc-1588overmpls-06
- [36] NIST Special Publication 1108R3, NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0
- [37] NASPI, Guidelines for Siting Phasor Measurement Units
- [38] UCA, Security Profile for Wide Area Monitoring, Protection and Control, 2011
- [39] Y. Ohsako, et al., *New Distributed SCADA Systems on Wide-Area IP Network*, Toshiba Review, Vol. 63, No. 4, 2008
- [40] A. Ishibashi, T. Tanaka, K. Hamamatsu, Y. Ishihara, T. Kase, Y. Sumida, *A Proposal for the Standardization of WASA which Complies with International Standards*, Transmission and Distribution Conference and Exposition (T&D), 2012 IEEE PES, 7-10 May 2012.
- [41] S. Matsumoto, Y. Serizawa, F. Fujikawa, T. Shioyama, Y. Ishihara, S. Katayama, T. Kase, A. Ishibashi, *Wide-Area Situational Awareness (WASA) System based upon International Standards*, 11th International Conference on Developments in Power Systems Protection 2012 (DPSP 2012), 23-26 April 2012.
- [42] The current status of YONDEN IP network deployment for electric power system, IEEJ technical report, 2010]
- [43] Y. Serizawa et al., *Prototype and Evaluation of Communication Network Prototype and Evaluation of Communication Network*, CIGRE SC D2 Colloquium 2013, No. D2-01\_24, Mysore, Karnataka – India, November 2013

- [44] IEEE *Transaction on Power Systems*, Vol. 19, No.2, May 2004, IEEE/CIGRE Joint Task Force on Stability Terms and Definition
  - [45] R. Bobba, E. Heine, H. Khurana and T. Yardley, *Exploring a Tiered Architecture for NASPInet*, IEEE PES Innovative Smart Grid Technology Conference (ISGT), Washington DC, January 2010.
  - [46] ITelcordia GR-253-CORE, *Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria* (October 2009), issue 5.
  - [47] K. Kuroi et al., *Practical Use Challenge of WDM & IP Communication Technologies for Protection Systems*, No. B5\_113\_2014, CIGRE Session 2014, Paris, France, August 2014
  - [48] Snort home page, <https://snort.org/>
  - [49] Abdul Kasim et al., *Delivering carrier Ethernet*, McGRAW-HILL ISBN 978-0-07-148747-4
  - [50] Raymond Jean (Hydro-Québec) and Maghsoodlou, Faramarz (Cisco), Use cases proposal for IEC TR 61850-90-12, available on-line at "[http://www.hydroquebec.com/pdf/en/proposal-IEC .pdf](http://www.hydroquebec.com/pdf/en/proposal-IEC.pdf)"
  - [51] P. Beaumont et al., "Commercial Line Current Differential Relay Operating over native Ethernet with Tokyo Electric Power Company", CIGRE Belgium Conference, Brussels, Belgium, March 2014.
-





INTERNATIONAL  
ELECTROTECHNICAL  
COMMISSION

3, rue de Varembe  
PO Box 131  
CH-1211 Geneva 20  
Switzerland

Tel: + 41 22 919 02 11  
Fax: + 41 22 919 03 00  
[info@iec.ch](mailto:info@iec.ch)  
[www.iec.ch](http://www.iec.ch)