IEC TR 61850-90-12

Edition 2.0 2020-07

TECHNICAL REPORT

colour inside

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

IEC TR 61850-90-12:2020-07 (en)

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

Tel.: +41 22 919 02 11
info@iec.ch
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 corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
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 It also gives information on projects, replaced and withdrawn publications.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
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - 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: sales@iec.ch.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
67 000 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 TR 61850-90-12

Edition 2.0 2020-07

TECHNICAL REPORT

colour inside

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 33.200

ISBN 978-2-8322-8657-9

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

CONTENTS

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.

This second edition cancels and replaces the first edition published in 2015. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) extension of use case with respect to distribution and customer-side applications;
b) extensions of wireless access technologies as well as power line communication ones applicable to the above-mentioned use case;

c) revisions regarding radio communication technology performance;

d) extension of network migration with respect to packet switched network;

e) a new mapping of multiprotocol label switching technology to teleprotection.

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

Enquiry draft	Report on voting
57/2136/DTR	57/2203/RVDTR

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 "https://www.webstore.iec.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.

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 kilometre to thousands of kilometres, called a "Wide Area Network" or WAN.

WANs encompass communication means of different natures (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 series 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 tunneller, but leaves the WAN undefined;
- IEC TR 61850-90-2[1] 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 tunnelling 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 61870-6 (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.

IEC TR 61850-90-4 provides guidelines for engineering of IEC 61850-based, local-area substation networks. In contrast, 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 document 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;

[1] In preparation. Stage at the time of publication: IEC TR/PWI 61850-90-2:2019.

- 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] [2] (Canada), Swissgrid (Switzerland) and ENEL (Italy).

[2] 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 part of IEC 61850, which is a Technical Report, is intended for an audience familiar with electrical power automation based on IEC 61850 and related power system management, 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 document 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 document addresses substation-to-substation communication, substation-to-control centre, and control centre-to-control centre communication. In particular, this document 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 document addresses issues such as topology, redundancy, traffic latency and quality of service, traffic management, clock synchronization, security, and maintenance of the network.

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

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60834-1, *Teleprotection equipment of power systems – Performance and testing – Part 1: Command 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 energy generation systems – 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 61850-8-1, *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 61850-5:2013, *Communication networks and systems for power utility automation – Part 5: Communication requirements for functions and device models*

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

IEC/IEEE 61850-9-3, *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[3], *Communication networks and systems for power utility automation – Part 90-2: Using IEC 61850 for the communication between substations and control centres*

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*

IEC TS 62351-1:2011, *Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security – Introduction to security issues*

IEC TS 62351-2:2008, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms*

IEC 62351-3:2014, *Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP*
IEC62351-3:2014/AMD1:2018

IEC TS 62351-4:2007, *Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS and derivatives*

IEC TS 62351-5:2013, *Power systems management and associated information exchange – Data and communications security – Part 5: Security for IEC 60870-5 and derivatives*

IEC TS 62351-6:2007, *Power systems management and associated information exchange – Data and communications security – Part 6: Security for IEC 61850*

IEC TS 62351-7:2017, *Power systems management and associated information exchange – Data and communications security – Part 7: Network and System Management (NSM) data object models*

IEC TS 62351-8:2011, *Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control*

[3] In preparation. Stage at the time of publication: IEC TR/PWI 61850-90-2:2019.

IEC TS 62351-9:2017, *Power systems management and associated information exchange – Data and communications security – Part 9: Cyber security key management for power system equipment*

IEC TR 62351-10:2012, *Power systems management and associated information exchange – Data and communications security – Part 10: Security architecture guidelines*

IEC TR 62351-11:2016, *Power systems management and associated information exchange – Data and communications security – Part 11: Security for XML documents*

IEC TR 62357-200, *Power systems management and associated information exchange – Part 200: Guidelines for migration from Internet Protocol version 4 (IPv4) 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 62439-3:2015, *Industrial communication networks – High availability automation networks – Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR)*

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

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

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*

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

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

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.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 1981, *Path MTU Discovery for IP version 6*

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 Behaviour)*

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

RFC 3260, *New Terminology and Clarifications for DiffServ*

RFC 3261, *SIP: Session Initiation Protocol*

RFC 3315, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*

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 4443, *Internet Control Message Protocol (ICMP v6) for the Internet Protocol version 6 (IPv6) specification*

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 4862, *IPv6 Stateless Address Autoconfiguration*

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 6550, *IPv6 Routing Protocol for Low-Power and Lossy Networks*

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, abbreviated terms, acronyms, and symbols

3.1 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

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 (IEC 60050-192:2015, 192-01-24), recoverability (IEC 60050-192:2015, 192-01-25), and maintainability (IEC 60050-192:2015, 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 of IEC 60050-192:2015, *Availability related measures*.

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

3.1.1.2
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
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
core network

3.1.5
backhaul
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: ANSI/IEEE 802.1D:2004]

3.1.7
Carrier Ethernet
extensions to Ethernet that enable use of Ethernet 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
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], 192-01-22.

3.1.13
encapsulation
transport from end to end of protocol data over another protocol

3.1.14
enterprise traffic
data traffic supporting the enterprise, such as email, data servers, accounting, software updates, etc.

3.1.15
fault
abnormal electricity flow requiring reaction of a protection device

3.1.16
Frame Relay
1990 telephony technology providing permanent virtual circuits

3.1.17
grid
electrical interconnection

3.1.18
integrity

3.1.18.1
integrity
<of a data stream> probability of undetected errors in a data stream subject to a certain bit error ratio

3.1.18.2
integrity
<of a system> quality of a system not to produce undetected erroneous data

3.1.18.3
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.

3.1.19
jitter
variation of the latency, expressed in relative time (e.g. ±10 ms) or in percentage of the latency (e.g. ±0,1 %)

3.1.20
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 with "communication delay" or "network delay", but not to "transfer delay" (IEC 61850-5), which is the application to application delay.

3.1.21
network
data transmission system

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

3.1.22
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.

3.1.23
persistency
ability of a system to continue producing correct data in the presence of faults

3.1.24
pseudowire
emulation of a direct, not shared wire with constrained latency using a PSN

3.1.25
protection

3.1.25.1
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.

3.1.25.2
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.

3.1.25.3
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 "defence" instead. However, "protection" still appears in abbreviations and referenced documents.

3.1.26
private address
address belonging to an address range administrated by the network operator, reusable in another network

3.1.27
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

3.1.28
public address
address belonging to an address range allocated by IANA or IEEE, which is unique in the context of the network

3.1.29
public internet
worldwide network using public addresses

3.1.30
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

3.1.31
router
network node able to route traffic, either through dynamic paths (IP) or through pre-established paths (MPLS) at Layer 3

3.1.32
traffic engineering
allocation of network resources (prioritized queues, bandwidth, time slots, etc.) to achieve a certain QoS

3.1.33
unavailability
expression of availability as the time during which a system is not available over a time interval (e.g. 2 min/year)

3.1.34
virtual leased line
VLL
point-to-point connection overlaid on top of another network, also called VPC or VPWS

3.1.35
virtual private circuit
VPC
point-to-point connection overlaid on top of another network, also called VLL or VPWS

3.1.36
virtual private LAN service
VPLS
point-to-multipoint connection overlaid on top of another network

3.1.37
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

3.1.38
virtual private network
VPN
network overlaid on top of another network, which it possibly shares with other VPNs

3.2 Abbreviated terms and acronyms

3GPP	Third Generation Partnership Project (mobile networks standardization body)
5G	Fifth Generation (of mobile networks)
6LoWPAN	IPv6 over Low power Wireless Personal Area Network (RFC 4919, RFC 6775)
AAA	Authentication, Authorization and Accounting (security)
ACL	Access Control Lists(IP)
ADM	Add-Drop Multiplexer (SDH)
ADSL	Asymmetric Digital Subscriber Line
ADSS	All Dielectric Self-Supporting (optical fibre)
AF	Assured Forwarding (RFC 3260)
AH	Authentication Header (RFC 4302)
ALG	Application Layer Gateway
APLC	Analog Power Line Carrier
APS	Automatic Protection Switching
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 (RFC 5880)
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
BMCA	Best Master Clock Algorithm (IEC 61588)
BPL	Broadband Power Line carrier
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 Packet 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)
COSEM	Companion Specification for Energy Metering
COTS	Common, off-the-shelf software
CP	Control Plane
CPE	Central Processing Equipment (WAMPAC)
CPE	Customer Premises Equipment
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CWDM	Coarse Wavelength Division Multiplexing (ITU-T G.671, see WDM, DWDM)
D8PSK	Differential 8-Phase Shift Keying
DA	Distribution Automation
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)

DLMS	Device Language Message Specification
DMR	Digital Mobile Radio
DLC	Distribution Line Carrie
DMZ	Demilitarized Zone
DNP3	Distributed Network Protocol (IEEE 1815)
DNS	Domain Name Server
DoS	Denial of Service (security)
DPI	Deep Packet Inspection
DPLC	Digital Power Line Carrier
DQPSK	Differential Quadrature Phase Shift Keying
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)
DXC	Digital Cross Connect
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
eMBB	Enhanced Mobile Broadband (5G)
EMEA	Europe Middle East and Africa
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
EPL	Ethernet Private Line (MEF)
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)

EVC	Ethernet Virtual Connection
EVPL	Ethernet Virtual Private Line (MEF)
EVP-LAN	Ethernet Private LAN (MEF)
EVPT	Ethernet Private Tree (MEF)
EXP	EXPerimental (MPLS)
FAN	Field Area Network
FCC	Federal Communications Commission (USA)
FCAPS	Fault Configuration Accounting Performance Security
FCS	Frame Check Sequence
FDB	Filtering DataBase (IEEE 802.3)
FDM	Frequency Division Multiplexing
FDMA	Frequency Division Multiple Access
FDV	Frame Delay Variation (MEF)
FL	Fault Location
FLISR	Fault Location Isolation and Service Restoration
FRR	Fast Re-Route (MPLS)
FTP	File Transfer Protocol (RFC 959)
G-Ach	Generic Associated Channel
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 (2nd generation mobile network)
GPS	Global Positioning System
GSM	Global System for Mobile communications (2nd generation mobile network)
HAN	Home Area Network
HC	Hybrid Clock
HDSL	High-bit-rate Digital Subscriber Line
HES	Head End System
HES	Home Electronic Systems
HMAC	Hash-based Message Authentication Code (RFC 2104)
HMI	Human-Machine Interface
HSPA	High-Speed Packet Access (3rd generation mobile network)
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)
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol (RFC 3376)
IGP	Internal Gateway Protocol
IntServ	Integrated Services (RFC 2210)
IOT	Internet Of Things
IP	Internet Protocol (RFC 791)
IPFIX	IP Flow Information Export (RFC 7011)
IPLS	IP-only LAN-like Service
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)
ISM	Industrial Scientific and Medical radio bands
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)
LDAP	Lightweight Directory Access Protocol
LDP	Label Distribution Protocol (RFC 5036)
LER	Label Edge Router (MPLS)
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol (IEEE 802.1AB)
LMU	Line Matching Unit
LOADng	Lightweight On-demand Ad-hoc Distance-vector routing – next generation
LoRaWAN	LoRa (Alliance) Wide Area Network
LPWAN	Low Power Wide Area Network
LQI	Link Quality Indicator
LSP	Label Switching Path (MPLS)
LSR	Label Switching Router (MPLS)
LTE	Long-Term Evolution (4^{th} generation mobile network)
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)
MEC	Mobile Edge Computing (5G)
MEF	Metro Ethernet Forum

MEMS	Micro-Electro-Mechanical Systems
MF	More Fragment (IPv4)
MFA	MPLS Forum Association (now IPMPLS)
MIB	Management Information Base (SNMP)
MMS	Manufacturing Messaging Specification (IEC /ISO 9506)
mMTC	Massive Machine Type Communications (5G)
MP2MP	Multipeers-to-multipeers
MPLS	Multi-Protocol Label Switching (RFC 3031)
MPLS-TE	MPLS Traffic Engineering
MPLS-TP	MPLS Transport Profile
MSDP	Multicast Source Discovery Protocol
MSP	Multiplex Section Protection
MS-SPRing	Multiplex Section Shared Protection Ring
MSTP	Multiple Spanning Tree Protocol
MTBR	Mean Time Between Repairs
MTC	Machine Type Communications (5G)
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)
NB-IOT	Narrow Band IOT
NB-PLC	Narrow Band Power Line Carrier
NCD	Network Configuration Description (IEC 61850-6)
NDP	Neighbor Discovery Protocol (RFC 4861)
NERC	North-American Electricity Reliability Corporation
NFV	Network Function Virtualization (5G)
NG	Next Generation
NGMN	Next Generation Mobile Networks (5G Alliance)
NIC	Network Interface Controller
NIST	National Institute of Standards and Technology (USA)
NMS	Network Management Services
NPCC	Northeast Power Coordinating Council
NPDU	Network Protocol Data Unit (ISO/IEC 7498)
NSM	Network and System Management
NTP	Network Time Protocol (RFC 5905)
OAM	Operation, Administration and Maintenance
OC	Optical Carrier (SONET channel)
OC	Ordinary Clock
OFDM	Orthogonal Frequency Division Multiplexing
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 (IEEEE 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)
PAN	Personal Area Network
PANA	Protocol for carrying Authentication for Network Access (IETF)
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 Y.1541 (IP), ITU-T Y.1563 (Ethernet))
PE	Provider Edge (node)
PFD	Probability to Fail (dangerously) on Demand (IEC 61508)
PHB	Per Hop Behaviour (MPLS)
PHY	Physical layer
PIM-SM	Protocol Independent Multicast – Sparse Mode (RFC 4601)
PM	Performance Monitoring
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 μHz/Hz or μs/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
PSK	Phase Shift Keying
PSN	Packet Switched Network
PTP	Precision Time Protocol (IEC 61588)
PW	Pseudo-Wire (pseudo wire)
PWI	Proposed Work Item (IEC)
PWE3	Pseudo-Wire Edge-to-Edge (RFC 3985)
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying

RADIUS	Remote Authentication Dial In User Service
RAN	Regional Area Network (see page 102)
RAN	Radio Access Network
RAS	Remedial Action Schemes (referred to as WAMPAC in this document)
RAT	Radio Access Technology
RBAC	Role Based Access Control
RF	Radio Frequency
RIR	Regional Internet Registry
ROBO	Robust Operation (NB-PLC)
RP	Rendezvous Point
RPL	Routing Protocol for Low power and lossy networks (RFC 6550)
RSPEC	Reservation Characteristics in IntServ (RFC 2210)
RSSI	Received Signal Strength Indication
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)
SCD	System Configuration Description
SCL	System Configuration Language (IEC 61850-6)
SCP	Secure Copy (UNIX service)
SDH	Synchronous Digital Hierarchy (ITU-T)
SDN	Software Defined Networks
SDSL	Symmetric Digital Subscriber Line
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 High-speed Digital Subscriber Line
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)
SNCP	SubNetwork Connection Protection
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
SSU	Synchronisation Supply Unit (SyncE)
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
TDMA	Time Division Multiple Access
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)
TSPEC	Traffic description in IntServ
TSN	Time Sensitive Network (IEEE 802.1, 802.3)
TTL	Time To Live (IP, MPLS)
UDP	User Datagram Protocol (RFC 0768)
ULA	Unique Local unicast Address (RFC 4193)
UMTS	Universal Mobile Telecommunications System (3rd generation cell phone)
UNI	User Network Interface (MEF)
UP	User Plane
UPSR	Unidirectional Path Switch Ring
URL	Unique Resource Locator
uRLLC	Ultra-reliable and Low-latency Communications (5G)
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 Private Routed 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.

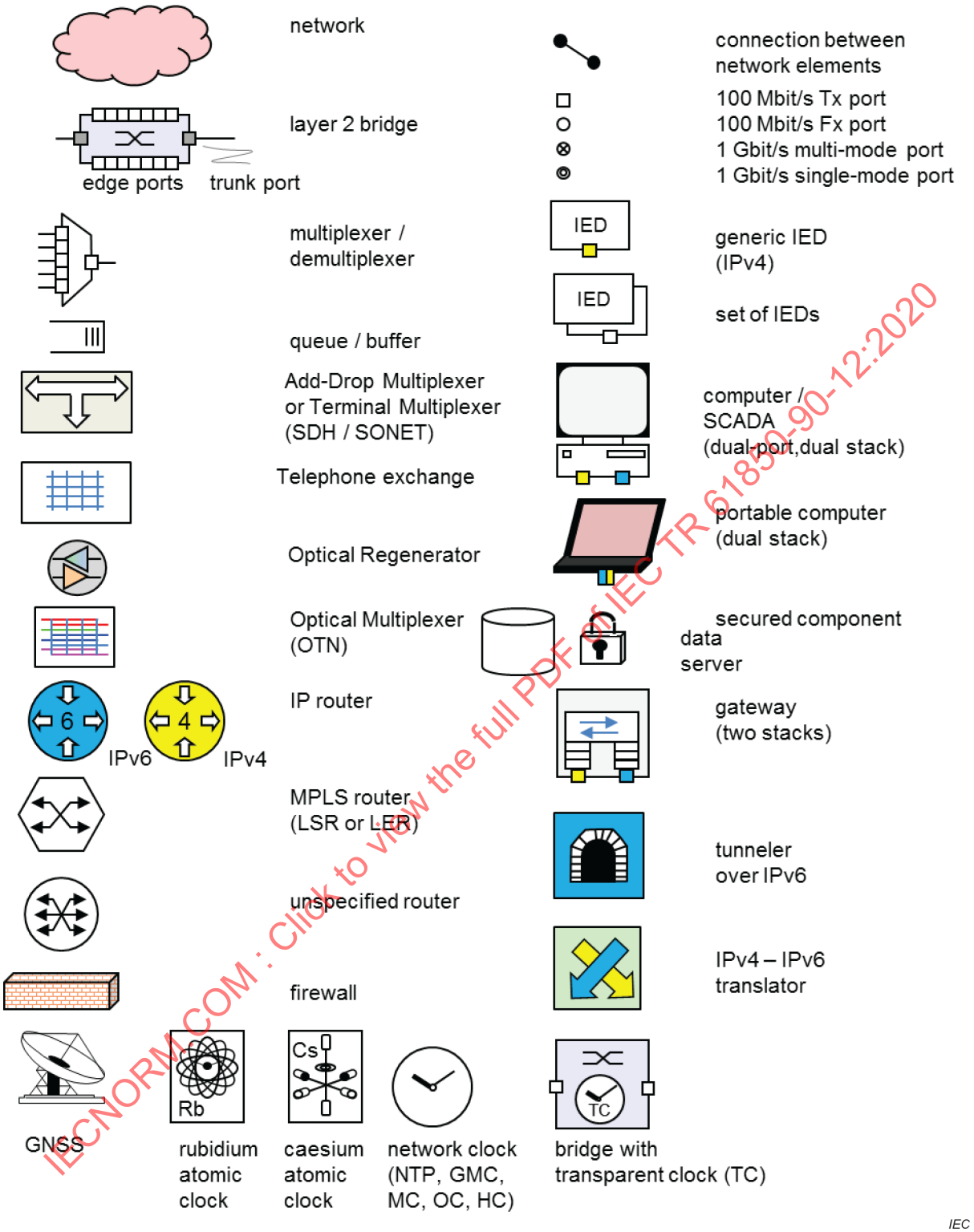


Figure 1 – Symbols

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 green field sites. 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 fibres 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 intend to give advice on the potential conflict points:

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

Clause 5 deals with network metrics such as latency, jitter, time accuracy and availability in order to describe communication requirements for use cases, network technologies and technology mappings in the following clauses.

Clause 6 consists of use case descriptions and WAN communication requirements derived from each of these use cases.

Clause 7 describes the communication 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 contains the mapping of appropriate communication technologies to the use cases described in Clause 6.

Clause 9 describes aspects of migration from legacy to modern communication network technologies and protocols.

The informative Annex A contains the description of some future promising or upcoming technologies.

4.2 Network and application example: 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).

Figure 2 – Substation locations in Andalusia

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

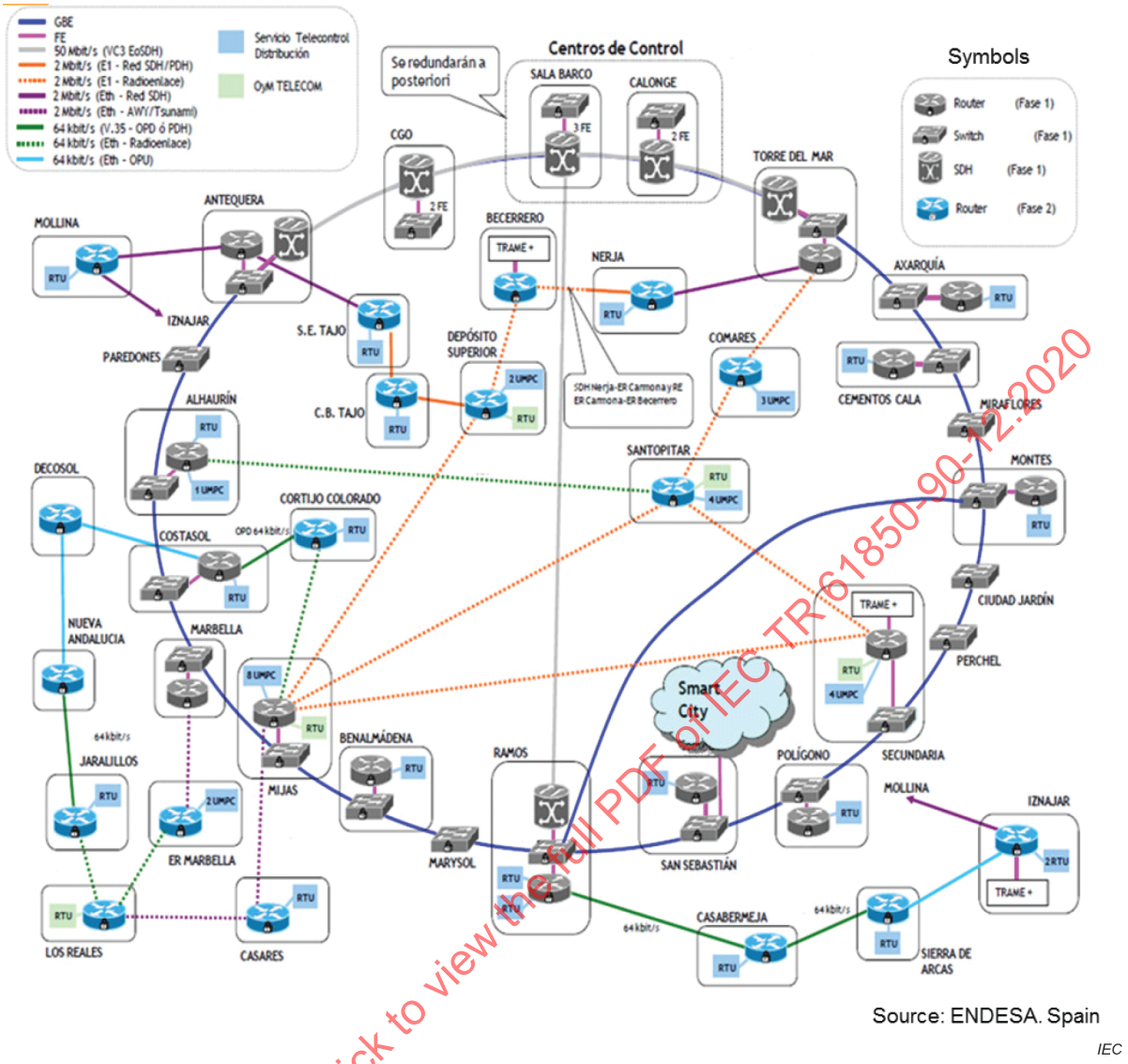


Figure 3 – Topology of the Andalusia network

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 is 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 a 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.

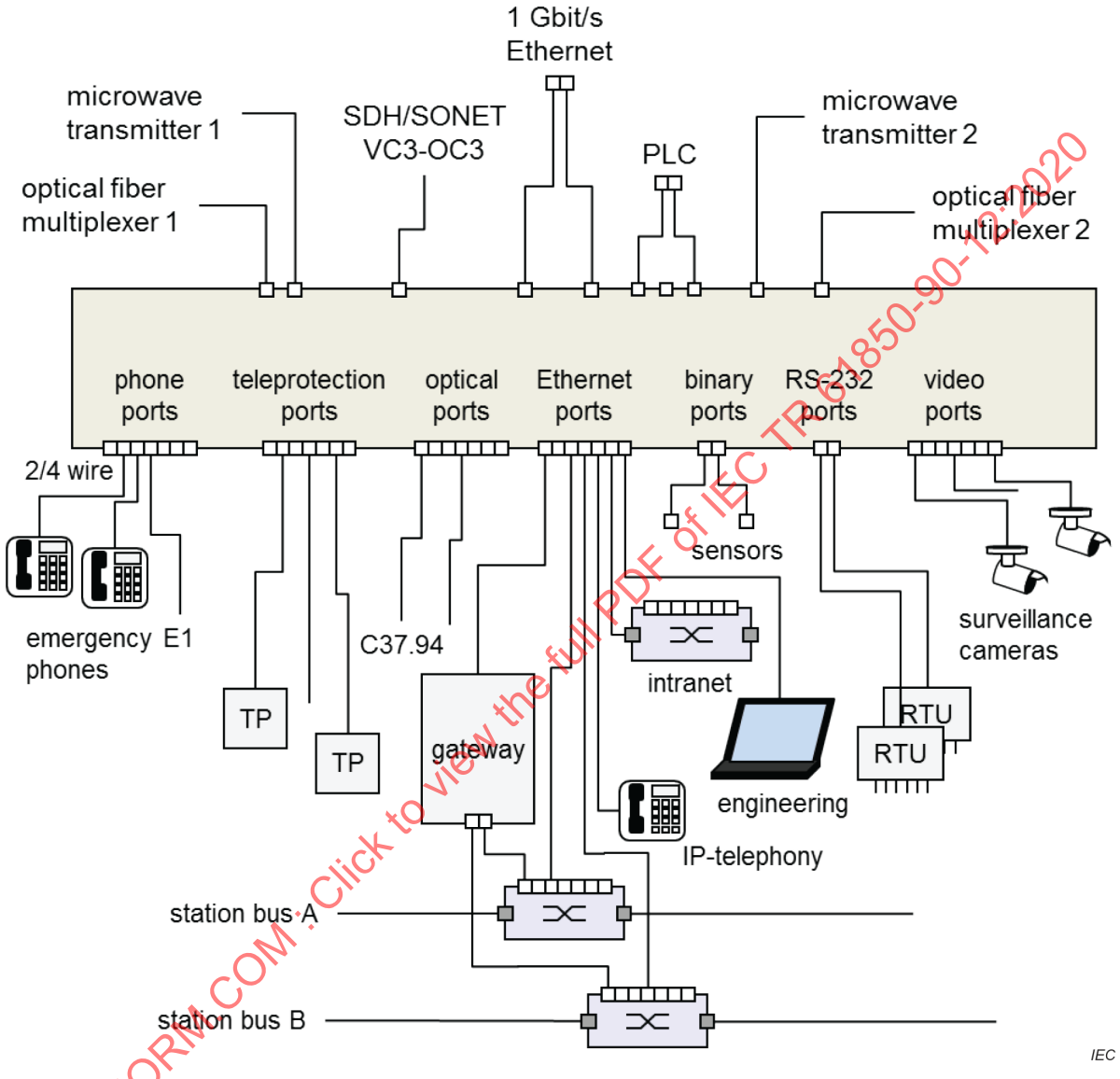


Figure 5 – Communication interfaces in a SEN

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.

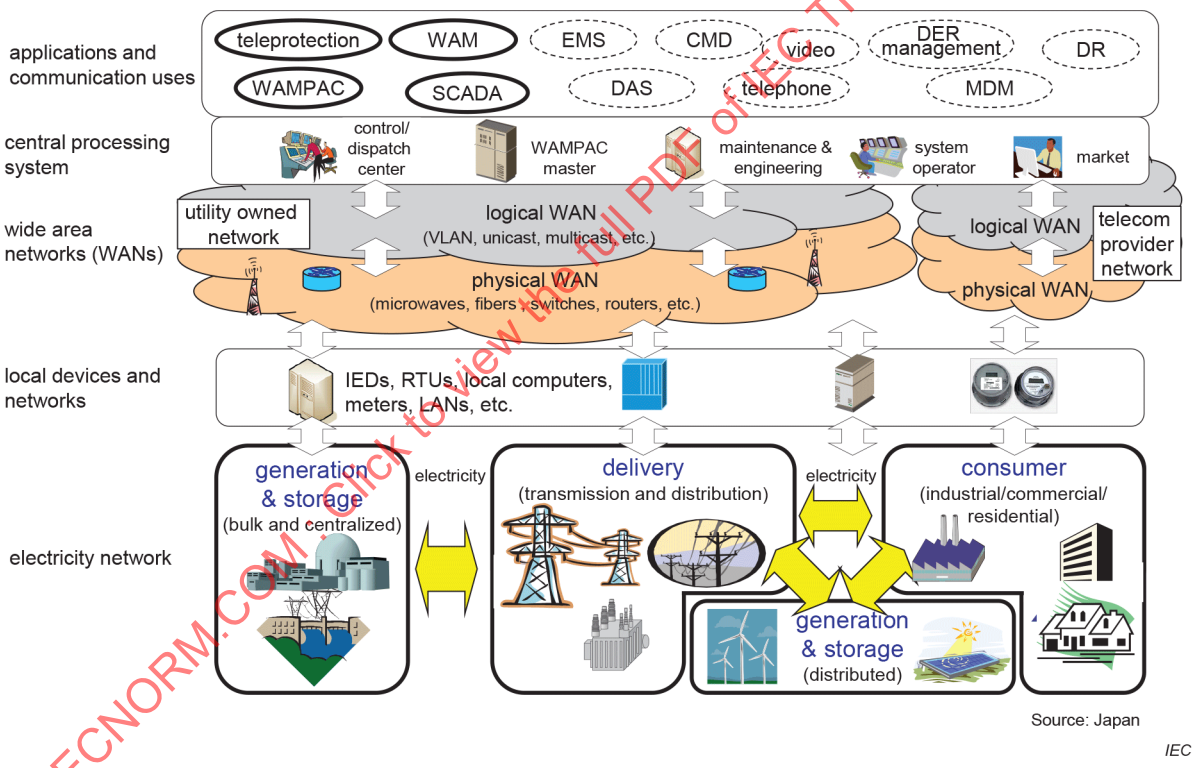


Figure 6 – Communicating entities

4.5 Smart Grid Architecture Model (SGAM) Mapping

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

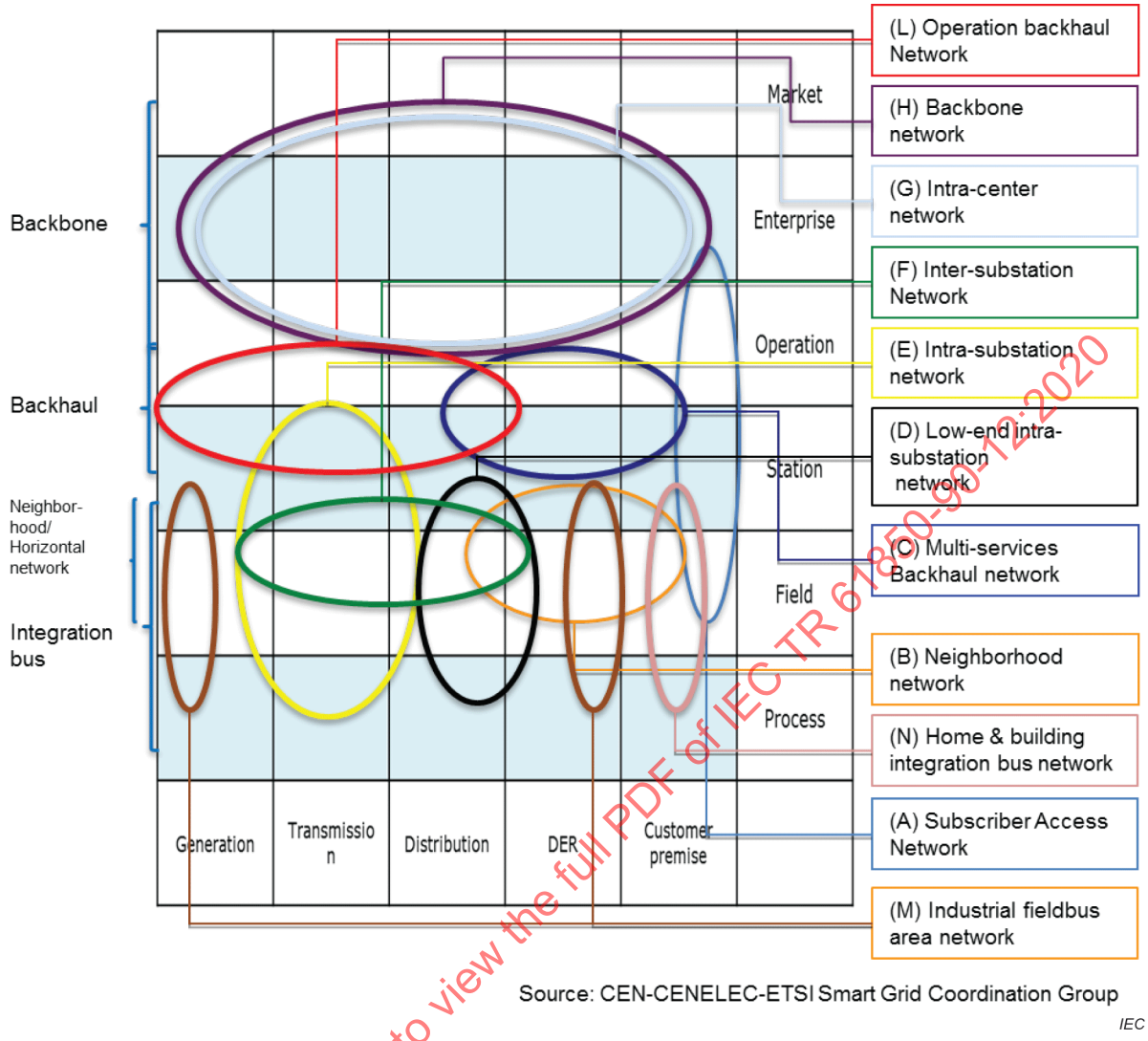


Figure 7 – SGAM communication model

SGAM defines a number of network types, in particular:

- subscriber access network;
- neighbourhood network;
- multi-services backhaul network;
- low-end intra-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:

- core network, which roughly corresponds to the SGAM backbone network
- 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 the National Institute of Standards and Technology (NIST), USA [36].

4.6 Network elements and voltage level

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

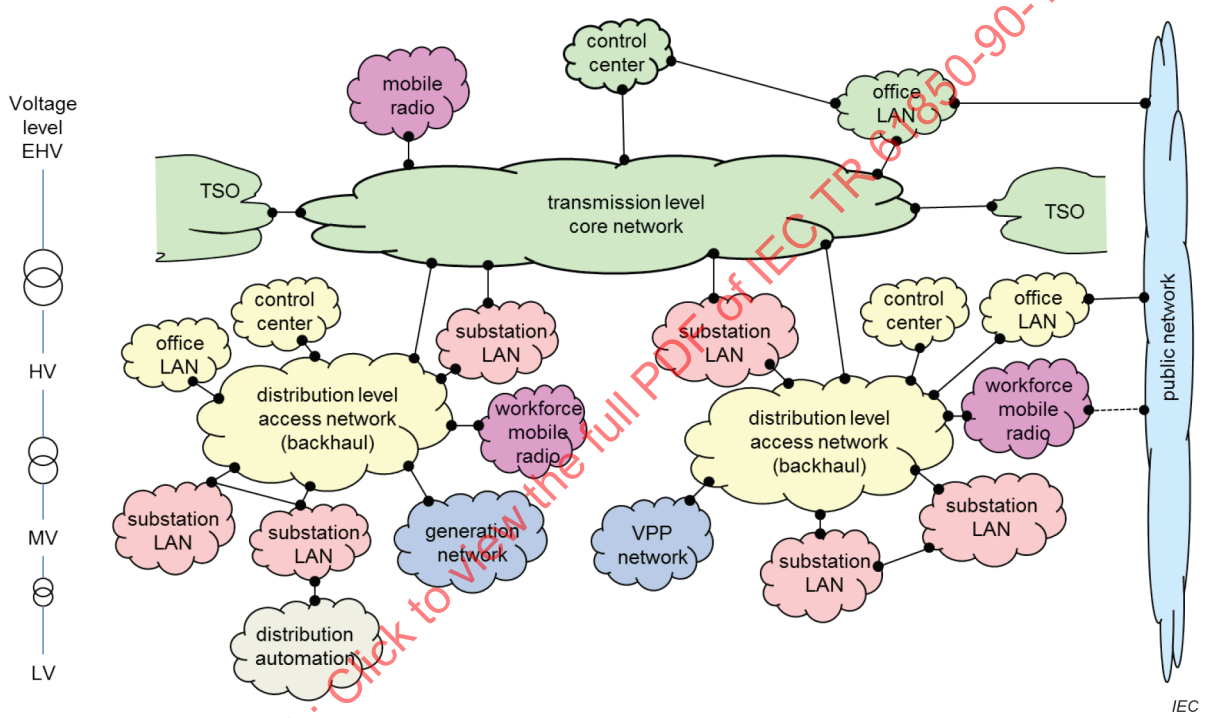


Figure 8 – Principle of grid voltage level and network technology

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 workforce 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 Figure 9 shows.

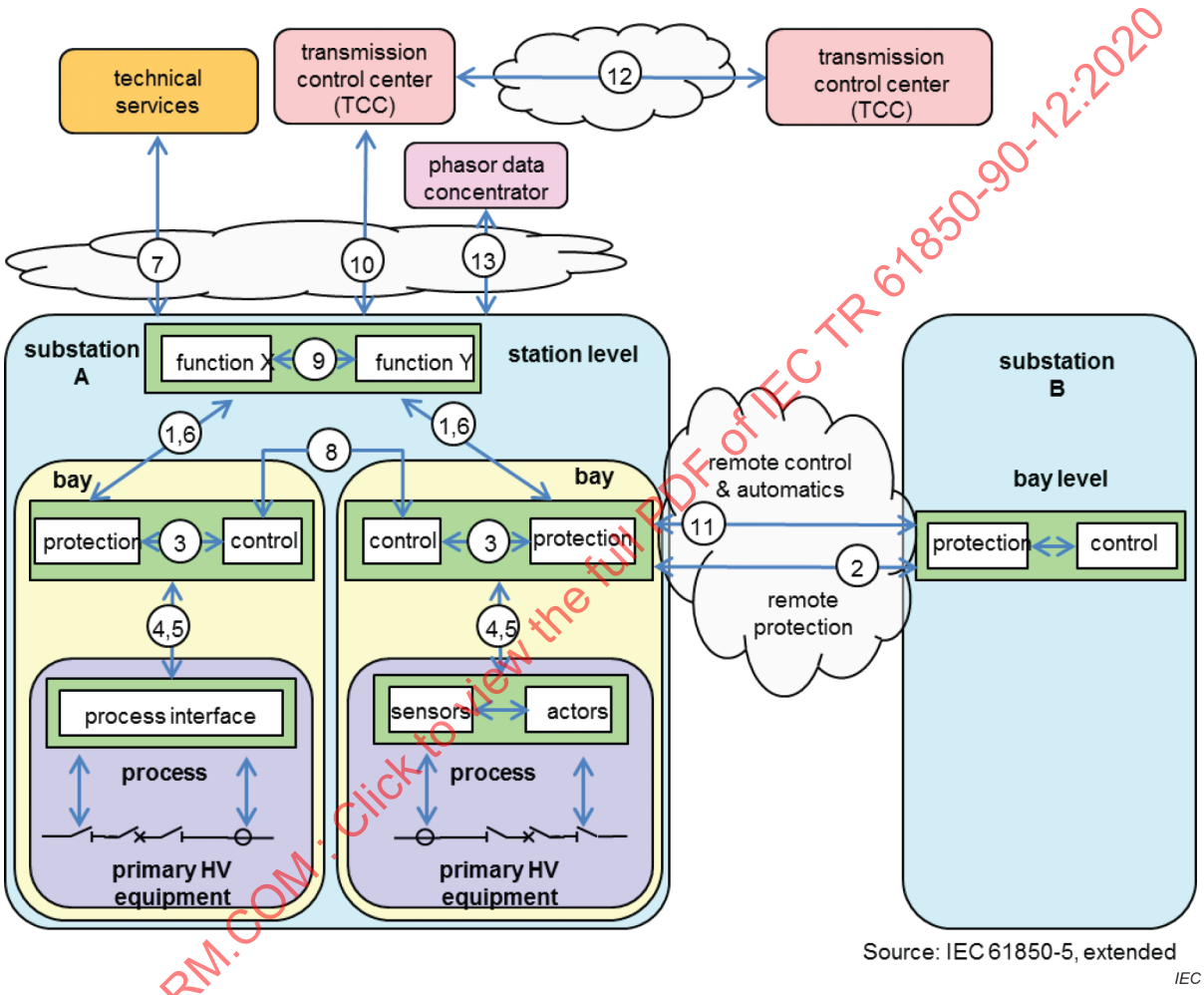


Figure 9 – Communication paths and interfaces

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 analogue 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 architecture in IEC TR 62357-200

IEC TR 62357-200 describes the logical interfaces for standardized applications (Figure 10). The boundary between what is in the substation and what is outside can vary.

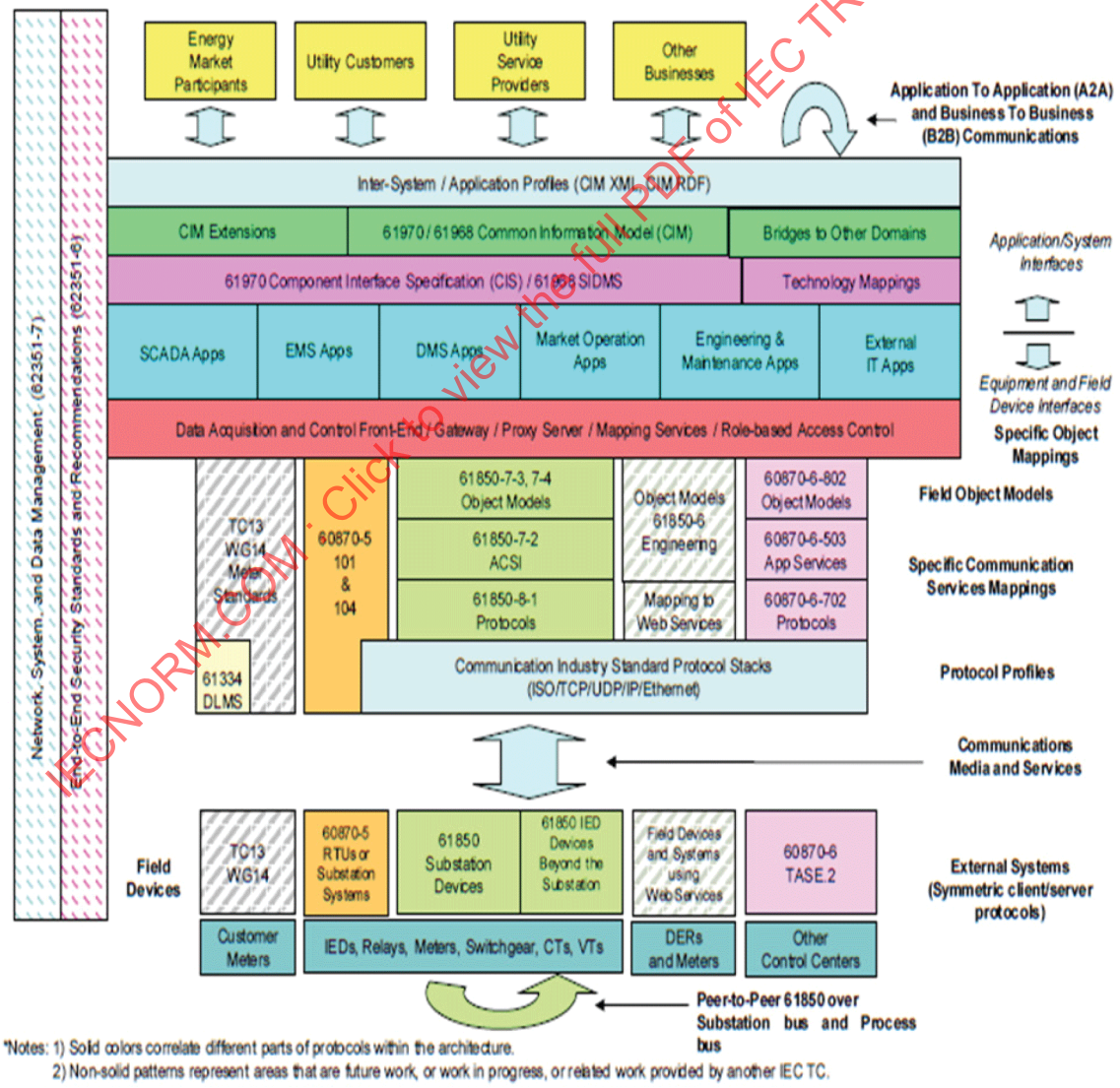


Figure 10 – IEC TR 62357 Interfaces, protocols, and applications

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 behaviour matter.

In all cases, engineering the different substations or terminals requires tools that generate the System Configuration Description (SCD) files of all participants and in addition the network information. These tools need to 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 fibres that they themselves do not need.

Owing 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 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 service level agreement (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. Therefore, PSNs have a variable average latency depending on the traffic load. In the worst case, the queue overflows and incoming messages are dropped because of overbooking or traffic bursts.

  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.

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 µs/km for copper cables or optical fibres, and 3 µs/km for radio links (Table 26). 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) packetization 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 µs.

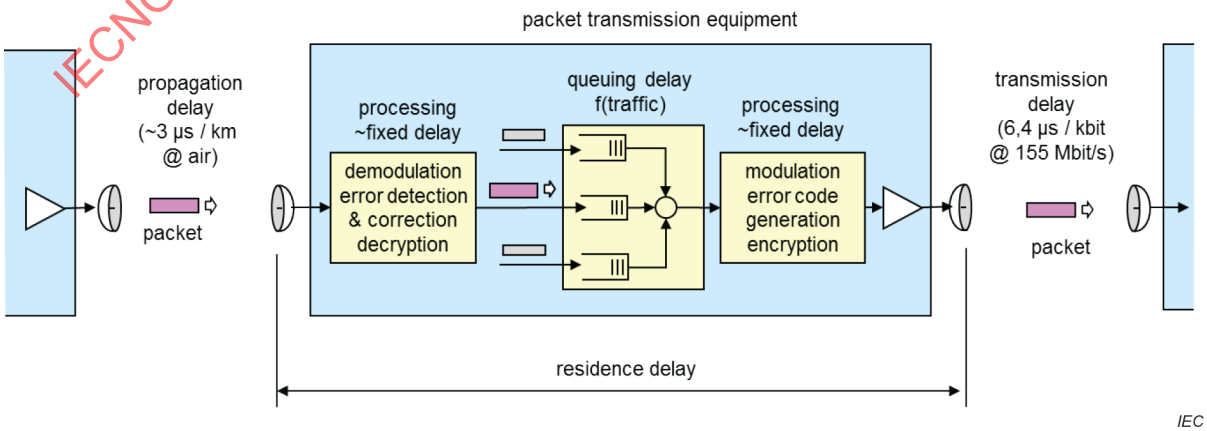


Figure 11 – Composition of end-to-end latency in a microwave relay

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 12a), 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 12a.

– In a non-deterministic transmission (Figure 12b), 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} in non-zero.

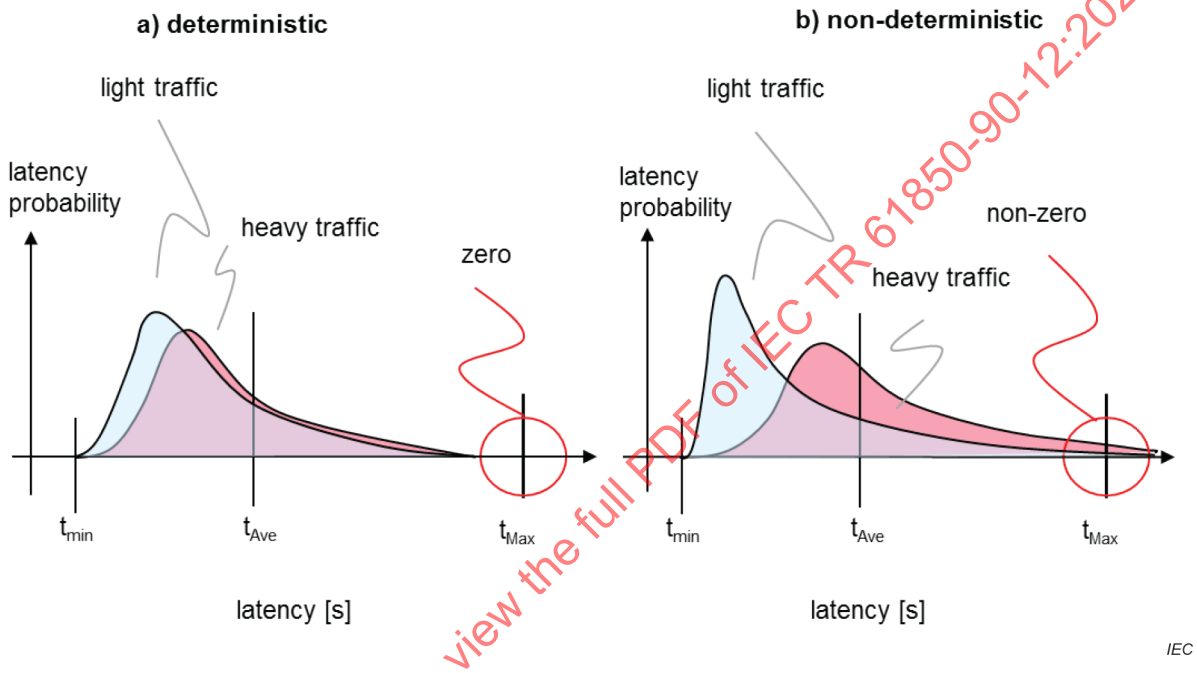


Figure 12 – Example of latency in function of traffic

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 neighbouring substation (analogue)
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	≤ 1000 ms	All other messages
TL300	(TT2)	≤ 300 ms	Operator commands
TL100	TT3	≤ 100 ms	Slow automatic interactions
TL30	(TT4)	≤ 30 ms	Fast automatic interactions
TL10	TT5	≤ 10 ms	Teleprotection
TL3	TT6	≤ 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).

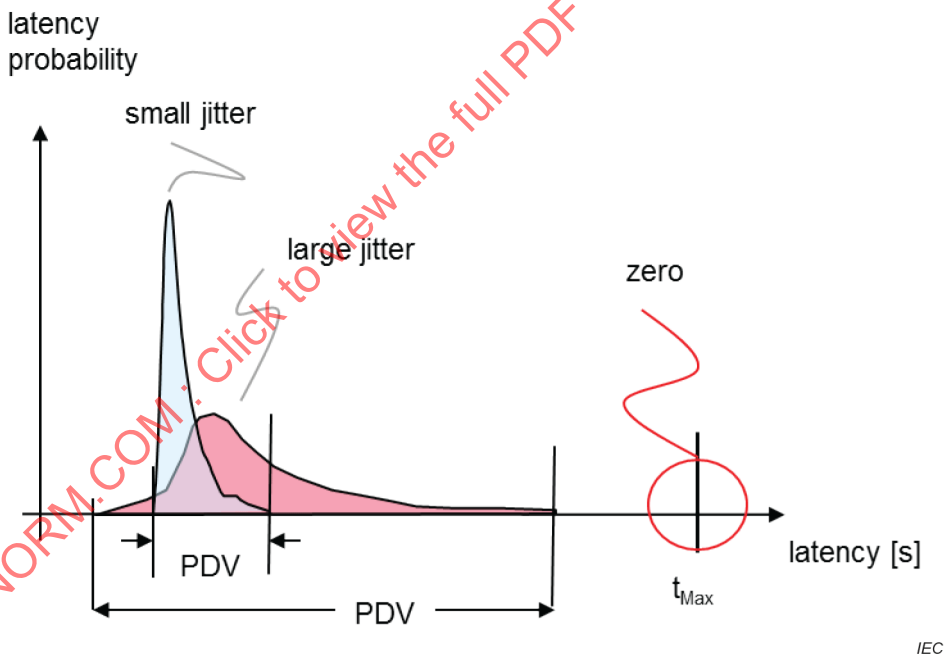


Figure 13 – Jitter for two communication delay types

Jitter produces unpredictable errors in differential (analogue) protection analogue 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" behaviour (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 behaviour 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 9.1.6.1.1.

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 (ΔTA) (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 fibres.

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/IEEE 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 Asymmetric Digital Subscriber Line (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 24.

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 62439-3:2015, Annex D).

Time accuracy is the deviation of a clock from the reference time, with a certain confidence, e.g. 3σ, as Figure 14 shows.

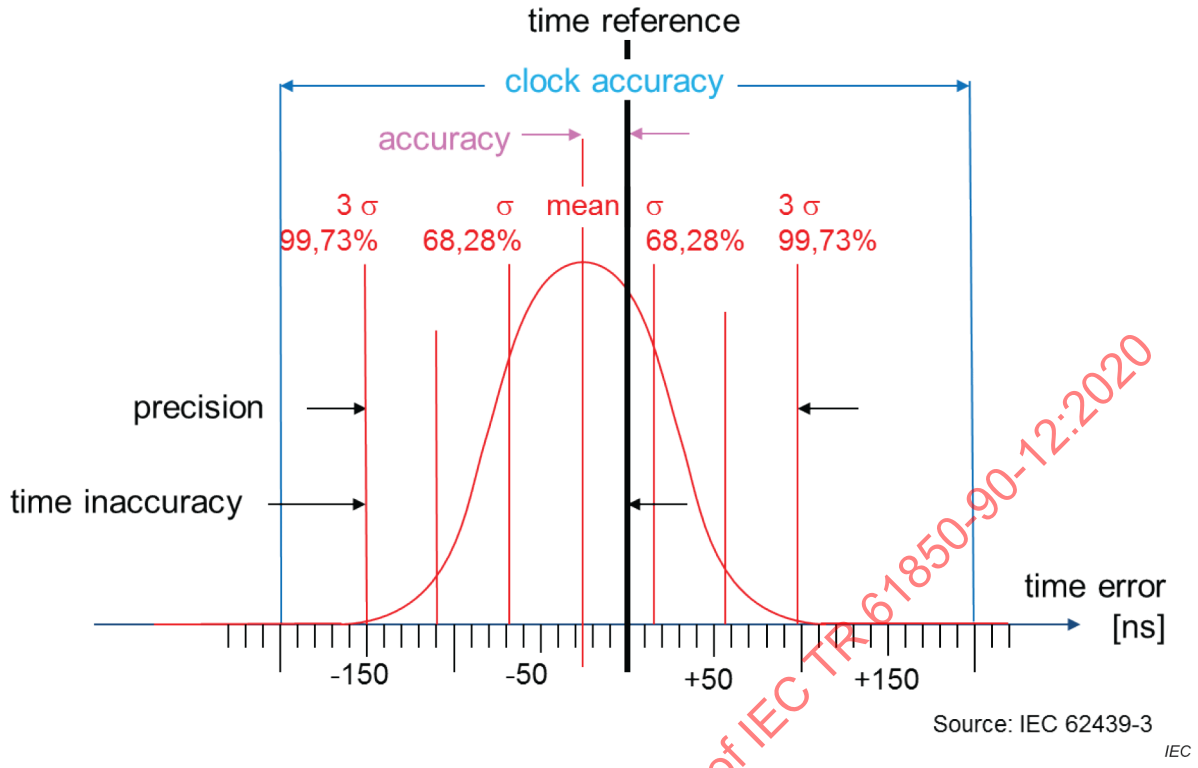


Figure 14 – Precision and accuracy definitions

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 analogue 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
TX25	T3	25	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 behaviour 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 fail (MTTF) for an element or a system, defined as:

$$MTTF = \int_0^\infty R(t)\,\mathrm{dt} \tag{1}$$

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 they are still up, they need seconds to resume carrying operational traffic after a severe failure.

  Standby methods are called "m:n", with the following special cases:

  "1:1 redundancy" one redundant element backs up one single working element,

  "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 type (e.g. different manufacturers) to avoid design or installation errors.

Figure 55 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 with repair will reliability be significantly increased. 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.

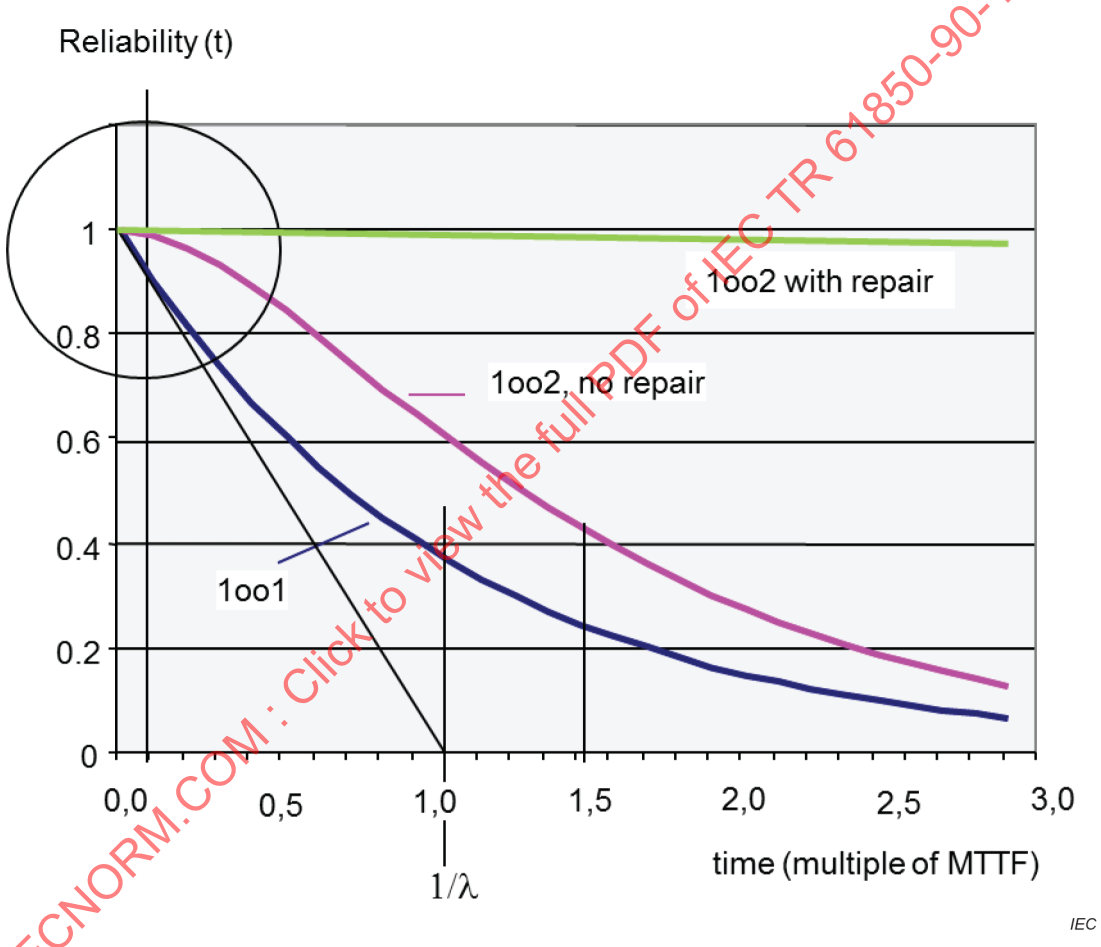


Figure 15 – Redundancy of redundant systems

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.

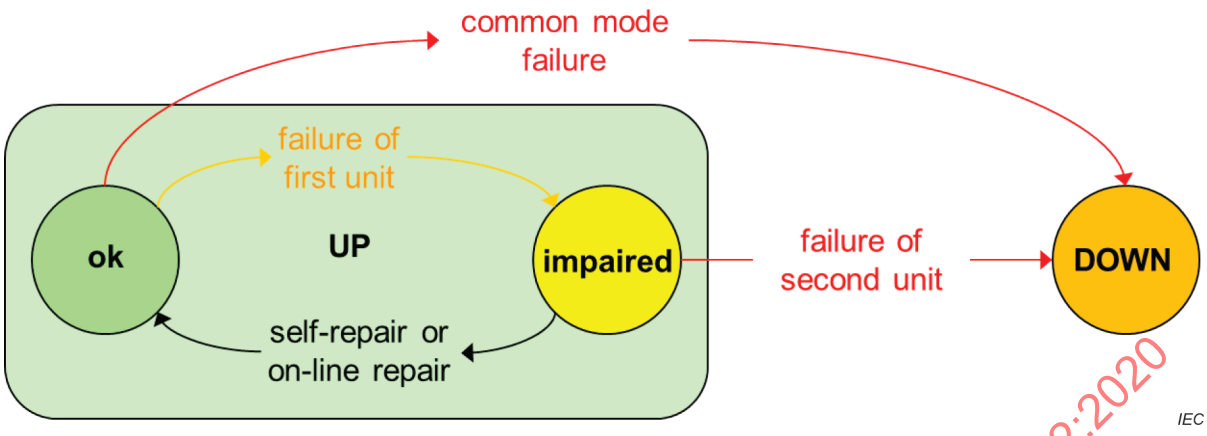


Figure 16 – Redundancy calculation

5.10.5 Redundancy checking

Redundancy is ineffective 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, R4 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.

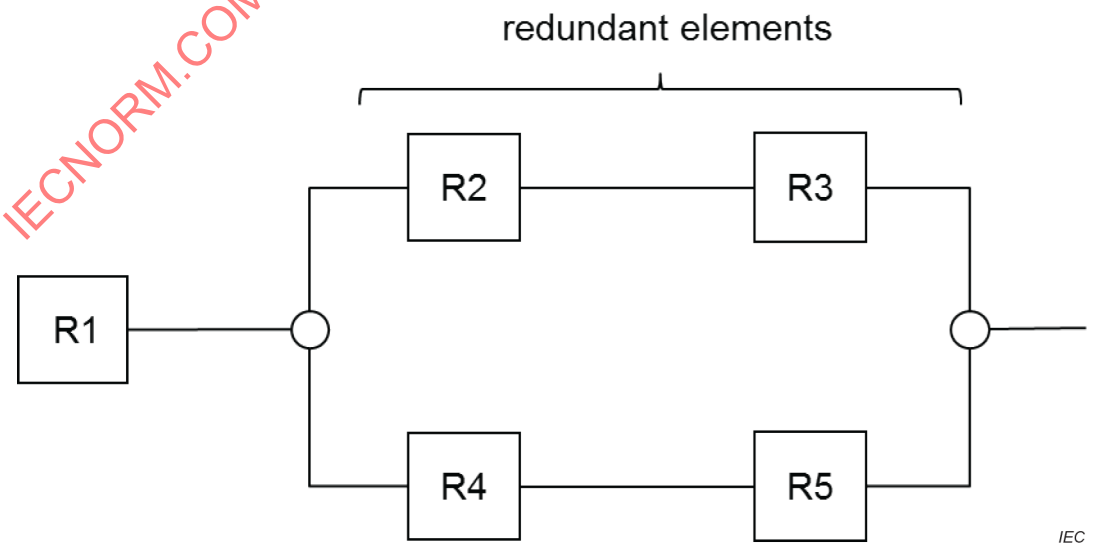


Figure 17 – Redundancy layout with single point of failure

In terms of 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 Northeast 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.

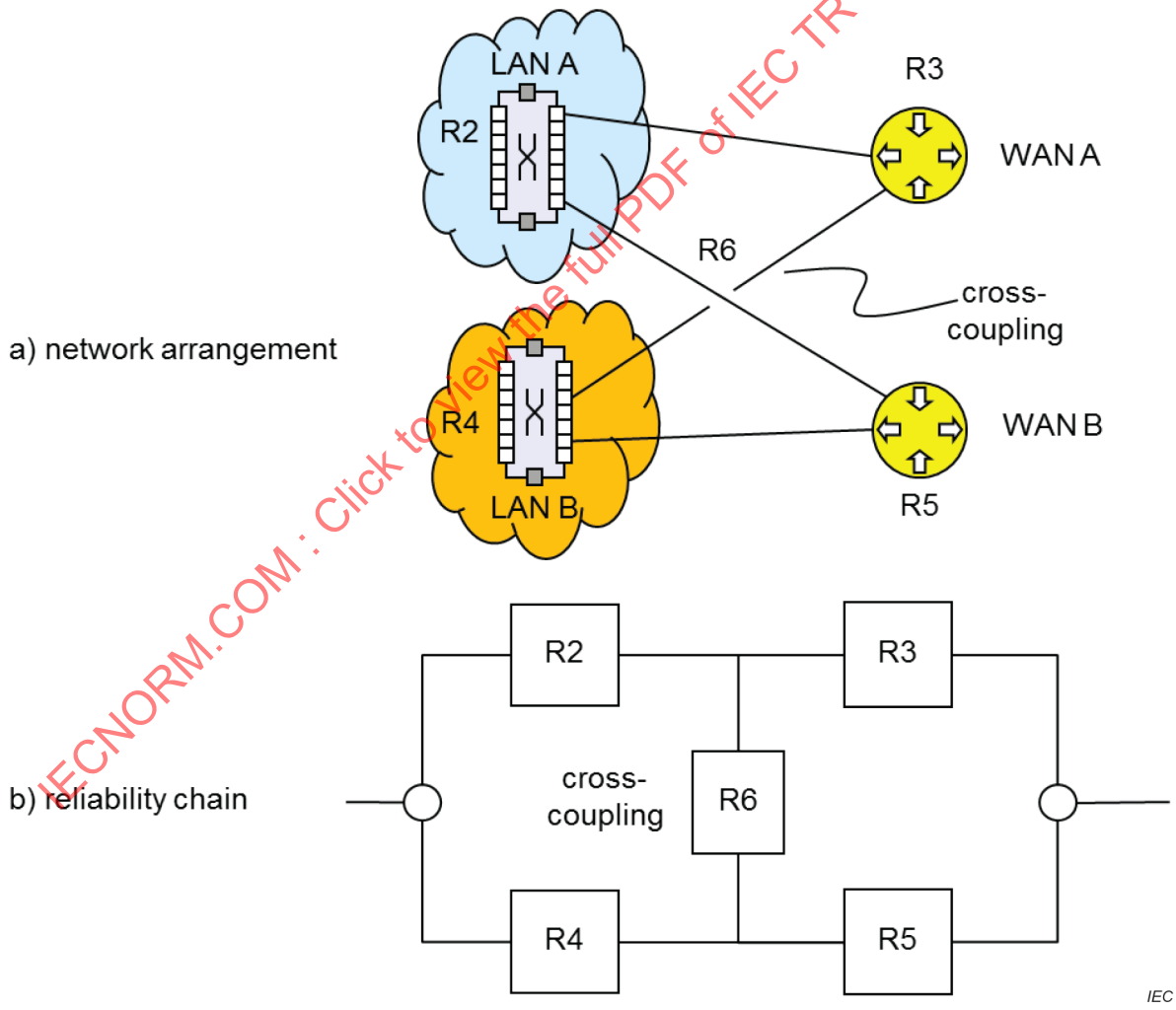


Figure 18 – Redundancy layout with cross-coupling

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.

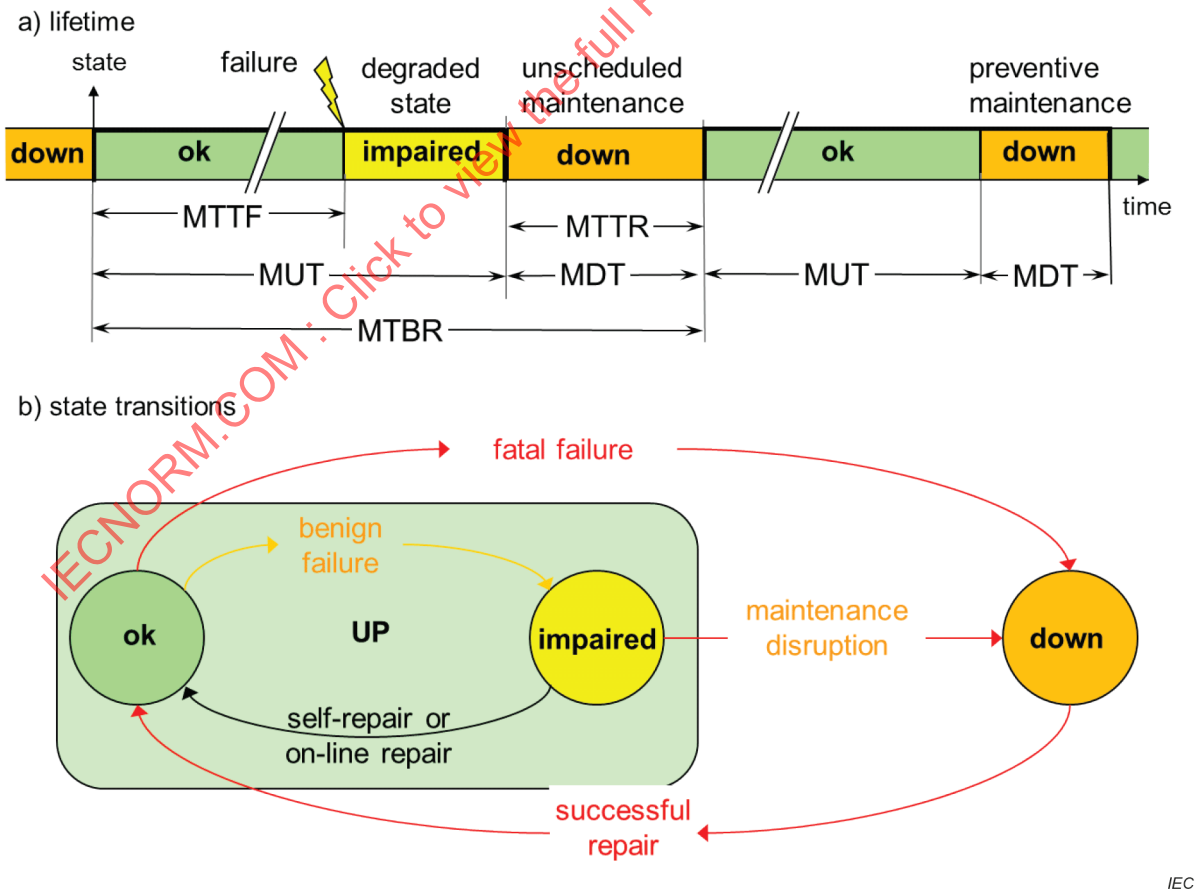


Figure 19 – Availability definitions

(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 correctly calculate 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 also includes the probability that the operation does not complete within the required time for it to be useful. 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, including security maintenance, influence the availability calculation, they should be considered in contracts since they depend on the 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 endeavour, 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 the term "integrity" instead of "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 60870-5-1 considers the residual error rate as a function of the BER, as Figure 20 shows.

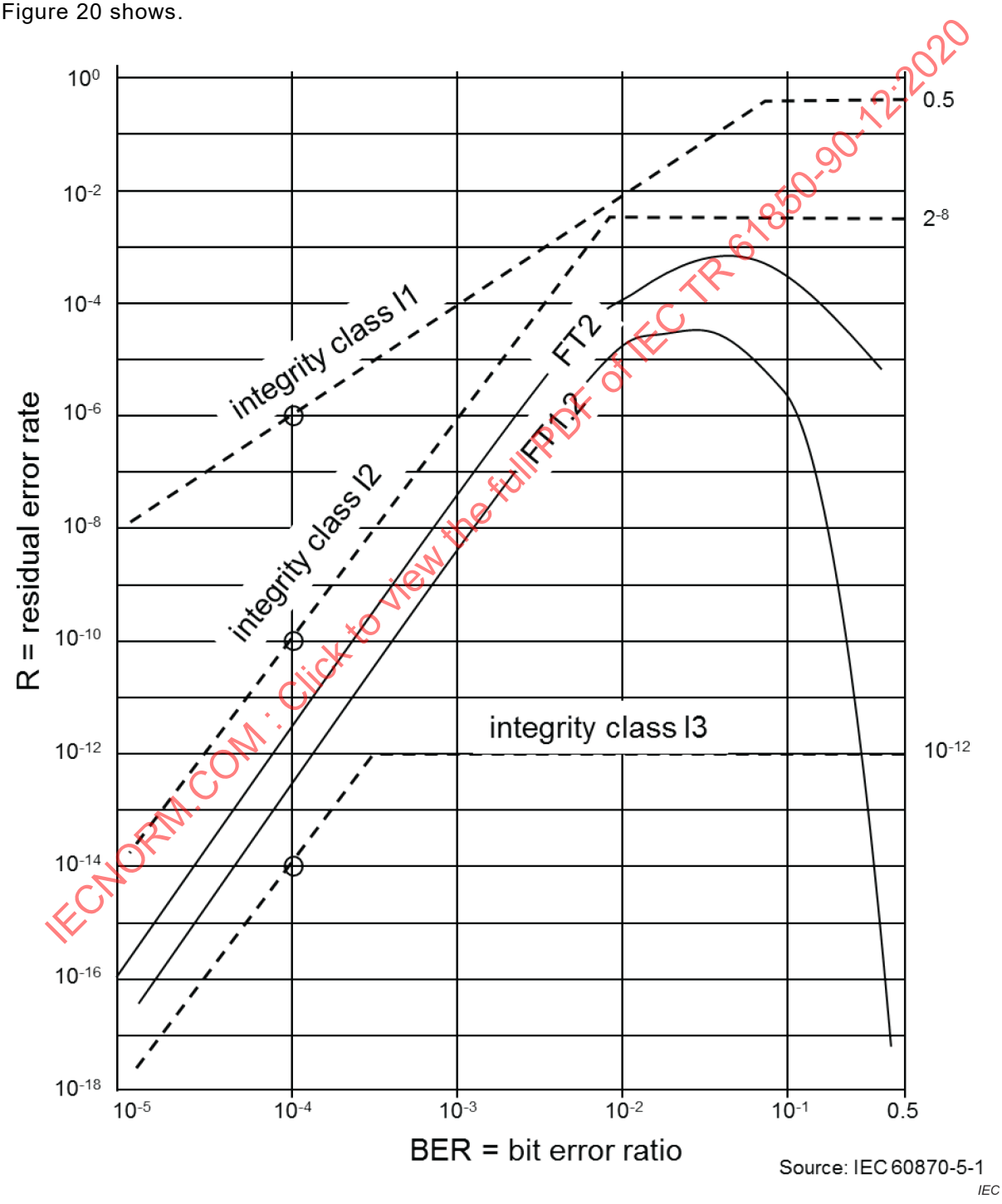


Figure 20 – Residual error rate as a function of BER

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 in 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 fibres 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 their geographic distribution, 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 will reject 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 would be aware – 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 IEC 61850-5 prescribes that trip signals should be received within 3 ms or 10 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 Use cases and WAN communication requirements

6.1 List of generic use cases

Engineering of a network is based upon 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;
2) enterprise traffic used by the utilities themselves; and
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 types of application are considered:

- (*) teleprotection (horizontal between SS); (IEC TR 61850-90-1);
- (*) telecontrol (including power plant SCADA); (IEC TR 61850-90-2);
- (*) wide area monitoring system (WAMS); (IEC TR 61850-90-5);
- (*) wide area monitoring, protection, and control (WAMPAC); (IEC TR 61850-90-5);
- (*) control centre to control centre;
- (*) fault location (FL);
- DISpatching (EMS, DMS), communication between CC;
- (*) condition monitoring and diagnosis (CMD) and asset management;
- (*) distribution automation (DA) (including FLISR);
- (*) smart metering;
- (*) others (DER monitoring and control, direct load control, etc.);
- 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 6.11 detail the requirements of the applications marked with "(*)" in the list above, 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, permissive 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 perspective, two main categories are apparent:

1) protections using analogue values, comprising:
   - phase comparison protection;
   - differential protection.
2) protection schemes utilising binary status/control values, 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) analogue 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 Current differential teleprotection for multi-terminal transmission line

6.2.3.1 Functional description

Figure 21 shows three types of logical configuration of current differential multi-terminal line protection (teleprotection) system where a four-terminal line is depicted as an example.

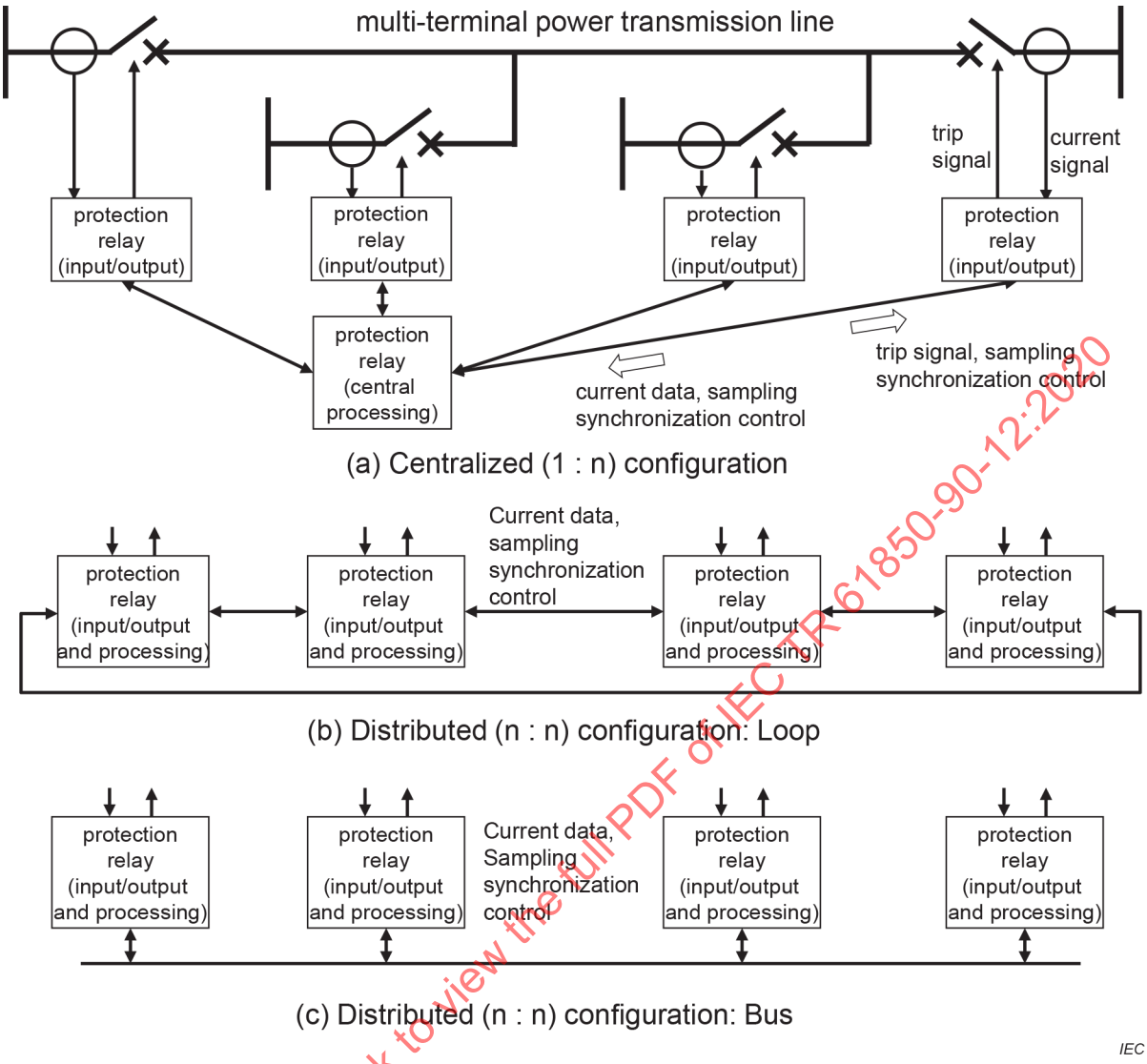


Figure 21 – Network configurations for multi-terminal line protection

In the centralized configuration, each terminal has an I/O-type protection relay that detects the current and transmits the data to the centrally processing protection relay via a communication channel. This configuration simplifies each terminal's protection relay and communication channels. Since the central protection relay receives the current data from all terminals, the fault locator function can be easily implemented using the data acquired.

In the distributed configuration where ring and bus types exist each terminal has a protection relay with I/O and processing functions as well as a signal transmitting function. Since each protection relay needs to collect all other terminals' data, their communications should be either multicast type or daisy-chain (hop-by-hop data accumulation and delivery) type.

6.2.4 Teleprotection communication requirements

6.2.4.1 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 also apply to the other traffic.

Table 10 – Latency for line protection

Teleprotection	Max. Latency	Transfer time class (IEC 61850-5)
Differential protection	< 3 ms to 10 ms	TT6 or TT5
Blocking	< 10 ms	TT5
Permissive tripping	< 10 ms	TT5
Transfer tripping	< 10 ms	TT5

6.2.4.2 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 × $\Delta\tau$ causes a sampling synchronization error of $\Delta\tau$.

The allowable two-way differential delay is around 200 µs 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 behaviour of a pilot-wire interconnection (pseudo-wire).

6.2.4.3 Teleprotection requirements for integrity

For generic telecontrol protocols, IEC 60870-5-1 defines the residual error rate for different integrity classes as a 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	> $1-10^{-5}$	> $1-(10^{-2}$ to $10^{-3})$	> $1-10^{-4}$
Integrity	> $1-10^{-6}$	> $1-(10^{-4}$ 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 [60], CIGRE 521 D2			

6.2.4.4 Teleprotection communication requirements 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

	Analogue comparison (Current differential)	Command	Transfer tripping
Direction	Bidirectional	Bidirectional	Unidirectional
Message (useful) size	50 bits to 100 bits[1)]	Few bits (On/off)	Few bits (On/off)
Message (frame) periodicity	3 to 12 times per cycle	Sporadic	Sporadic
Bit rate (Bandwidth) [2)]	9,6 to 64 kbit/s	< 10 kbit/s	< 10 kbit/s
Latency	< 3 ms to 10 ms (TT6 or TT5)	< 10 ms (TT5)	< 10 ms (TT5)
Jitter[3)]	< 100 µs	Not required	Not required
Latency asymmetry	< 200 µs[4)]	Not critical	Not critical
Time accuracy (relative)	< 100 µs	Not critical	Not critical
Bit 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 × Unit Interval (ITU-T G.823).

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

6.3 Wide area monitoring system (IF13)

6.3.1 WAMS overview

Wide area monitoring systems (WAMS) gather the values of current and voltage over a large area (a region or a country, sometimes 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, behaviour, and performance, as well as to anticipate, prevent, or respond to problems before disruptions arise [41].

6.3.2 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 a display together with WANs.

NOTE IEC TR 61850-90-5 calls the central processing equipment "central equipment", this term is not used here because of an abbreviation clash.

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

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

a) Decentralized PDCs (Figure 22a) 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.

b) Centralized PDC at the CPE (Figure 22b) 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.

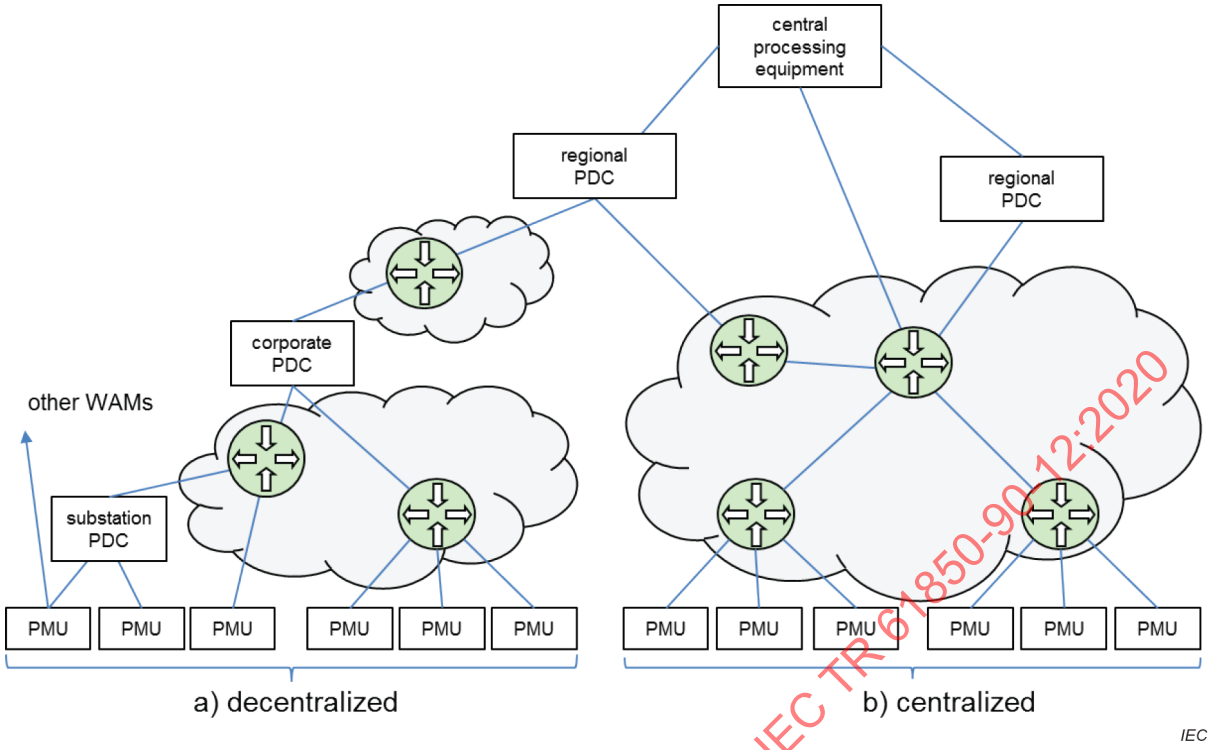


Figure 22 – Principle of synchrophasor transmission

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

NASPI [37] documented the synchrophasor distribution for North America, shown in Figure 23. Some 1000 PMUs were installed until 2014, March 19.

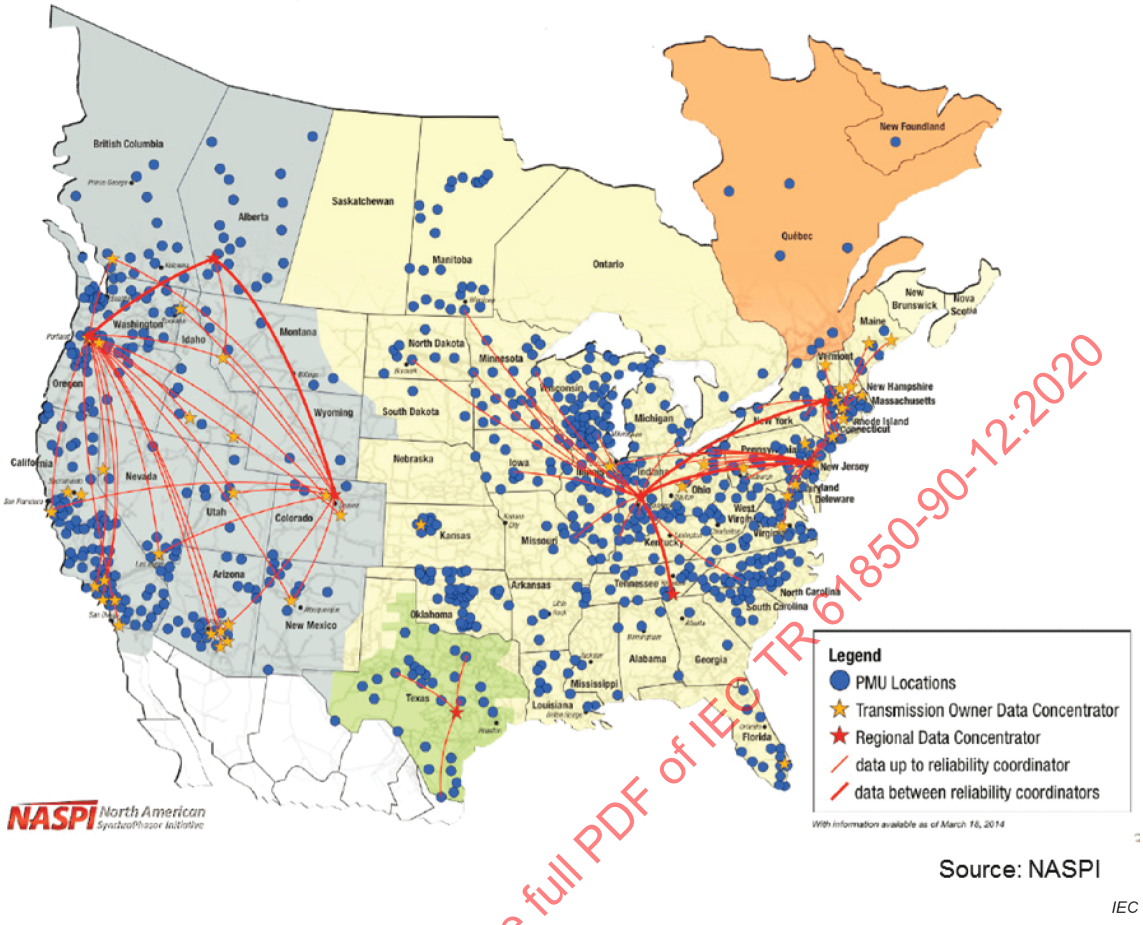


Figure 23 – PMUs and data flow between TSO and regional data hubs

6.3.3 WAMS communication requirements

Table 13 summarizes the communication requirements stipulated in IEC TR 61850-90-5.

Table 13 – 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 @ 50 Hz 30 to 120 @ 60 Hz	30	25	Medium	Medium	SMV service
Undervoltage load shedding	25 @ 50 Hz 30 @ 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						

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

The communication requirements for WAMS are summarized in Table 14.

Table 14 – Summary of communication requirements for wide area monitoring

	Class B (State estimation)	Class C (Visualization and monitoring)	Class D (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 (unavailability < 10^{-4}), redundancy needed	Not critical	Fairly critical (unavailability < 7×10^{-5})
NOTE The 50 µs 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 µs, see in particular 7.15.11.			

6.4 Wide area monitoring, protection, and control (WAMPAC) IF13

6.4.1 Functional description

WAMPAC systems are also referred to as system integrity protection scheme (SIPS), remedial action scheme (RAS) and grid stabilizing control.

Figure 24 categorizes the target phenomena for WAMPAC, each imposing its own communication requirements.

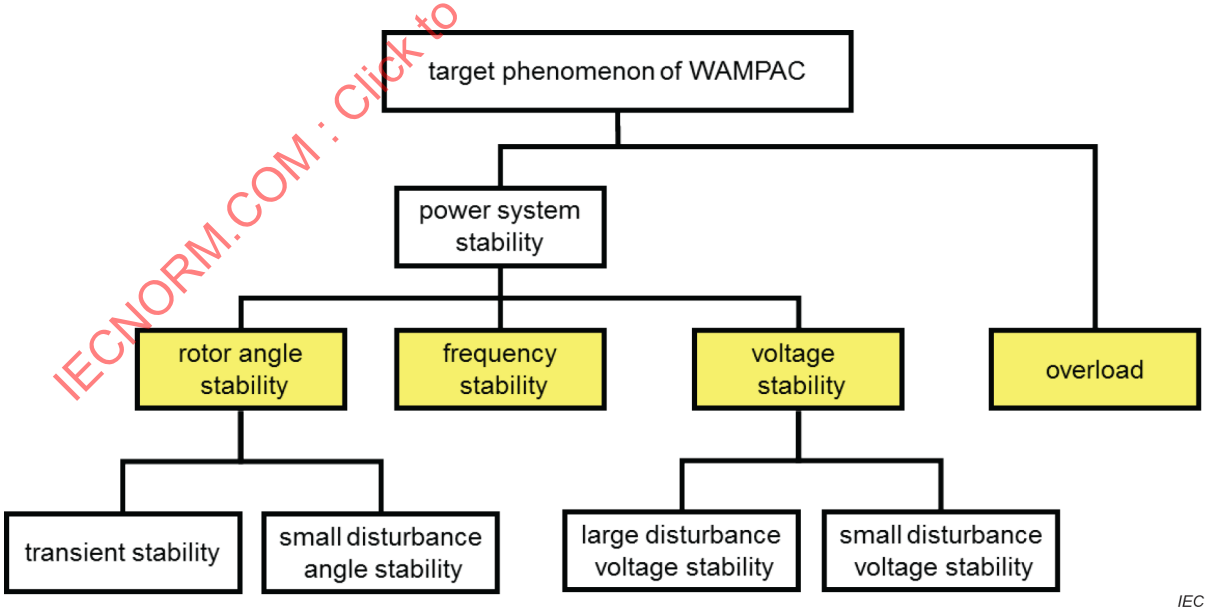


Figure 24 – Target phenomena for WAMPAC

NOTE More detailed typical use cases for WAMPAC are described in IEC TR 61850-90-1, *Use of* IEC 61850 *for the communication between substations* and IEC TR 61850-90-5, *Use of* IEC 61850 *to transmit synchrophasor information according to* IEEE C37.118.

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

Figure 25 shows an example of the general architecture, functions, and information flow.

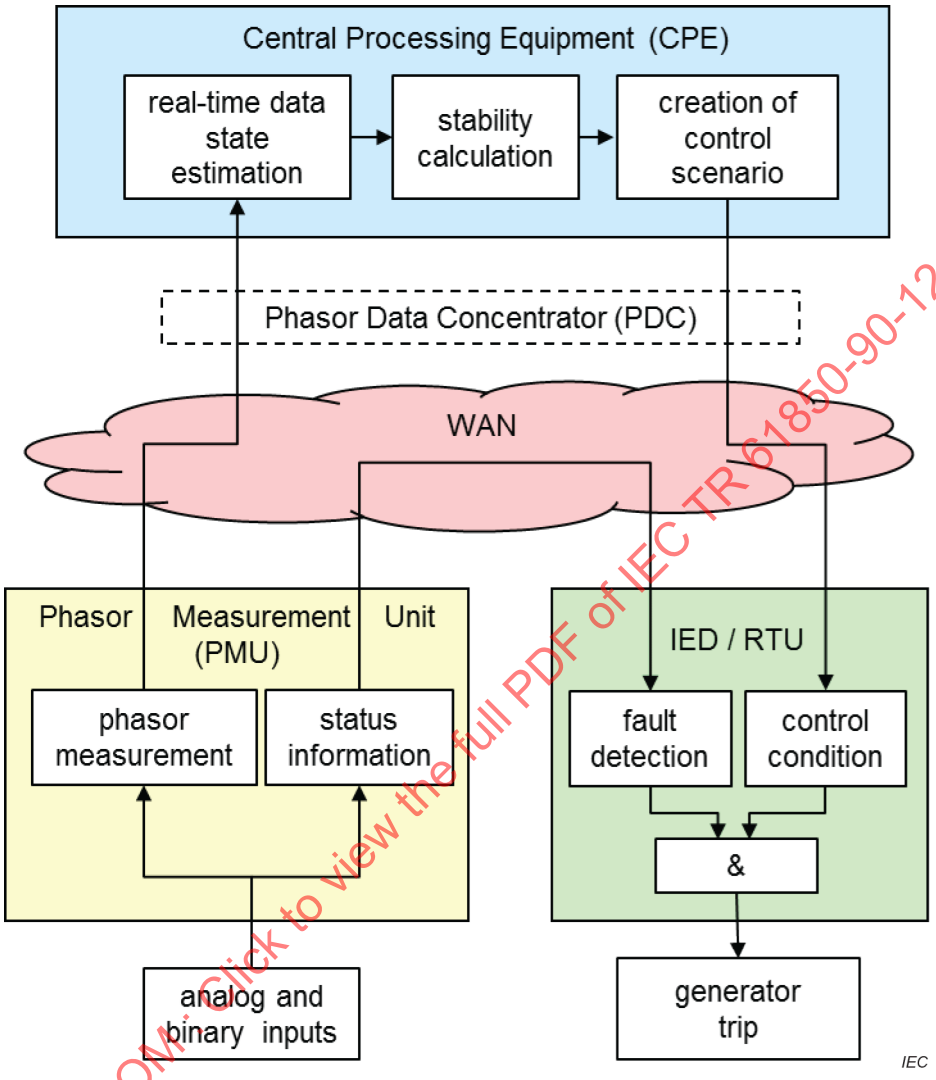


Figure 25 – Example of main function and general information flow

PMUs are installed at each of the measurement points in the grid. They send 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 participates in the stability control.

The CPE estimates the grid state using the data received from the PMUs. If it detects an instability phenomenon, it creates a countermeasure 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.

6.4.2 WAMPAC communication requirements

Table 15 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 15 also indicates the number of PMUs, the data size, and the transmission distance because these items are necessary for the engineering of practical WANs.

Table 15 – 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 µs	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 µs	20	1 / cycle	10	100	500
Frequency stability	200	PMU to IED	Phasor	50 µs	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]									

6.5 Fault Location

6.5.1 Functional description

Figure 26 shows a logical configuration for a fault locator (FL) system where while many FL systems are installed for two-terminal transmission lines, a three-terminal line is depicted as an example of more generic multi-terminal lines. A fault location terminal unit (FLTU) is installed at each terminal of a power transmission line, each FLTU is connected to the fault location calculation unit (FLCU) via a wide area network. The FLCU reports its fault location calculation result to an operation and maintenance (OAM) server via a wide area network.

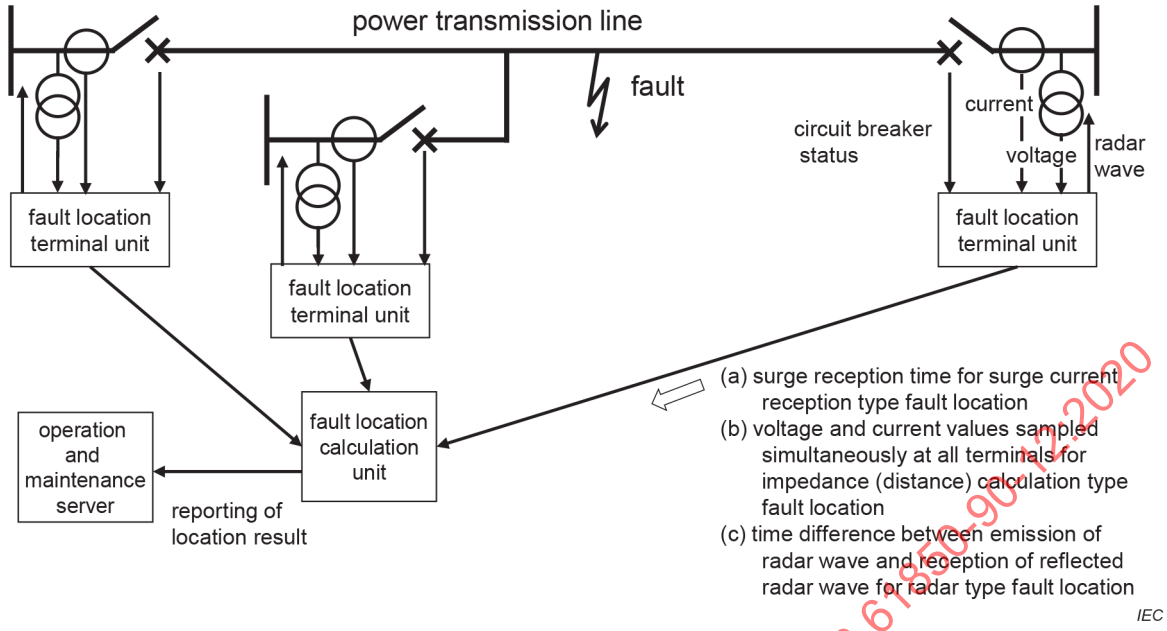


Figure 26 – Network configuration for a fault locator system

There are three types of FL system: (a) surge reception type, (b) impedance calculation type and (c) radar type.

(a) Surge reception type

When a fault occurs, its surge current propagates toward each terminal, and each fault location terminal unit receives the surge and records the reception time. There are two types of fault location calculation method: single-ended and double-ended methods (IEC/TR 61850-90-21). In the single-ended method, a FLCU at a terminal calculates the fault location by using the time difference between the first received and second received (reflected) surges, and reports the results to an OAM server. In the double-ended method, the surge reception time information of all FLTUs is collected by the FLCU and the location of the fault can be calculated from the reception time differences, the FLCU reports the result to the OAM server. Therefore, the double-ended FL system needs time synchronization among the FLTUs.

(b) Impedance calculation type

During a fault, the distance to the fault can be calculated by using the impedance calculated from the current and voltage values at the terminal (FLTU integrated with FLCU) similar to a distance relay. The calculated result is transmitted to an OAM server via a WAN as a form of "Remote access to substation equipment, log retrieval" mentioned in 6.1. This type of FL system can be integrated into a current differential teleprotection system.

(c) Radar echo (pulse or wave reflection) type

In a radar echo type FL system, each FLTU emits a pulse or frequency modulated continuous wave (FMCW) and receives a reflected pulse or wave from where the pulse or wave reaches the fault with the speed of a travelling wave. The elapsed time multiplied by the diffusion speed gives the distance to the fault. For multi-terminal lines, measurements at all of the terminals from which data is transmitted to the FLCU is via a WAN and the central calculation performed by the FLCU provides a more accurate result.

6.5.2 Fault location communication requirements

The communication requirements are shown in Table 16. Regarding redundancy, since fault location is not a protection, but used for transmission line surveillance and restoration, it is not critical compared with protection and does not necessarily need a redundant configuration. With a fault location error (inaccuracy) requirement of hundreds of meters, depending on utility's power transmission surveillance criteria, the surge reception type FL system requires a time synchronization error less than, for example, 1 µs to 3 µs. Time synchronization based on an intra-system clock is sufficient, rather than requiring a global clock. Depending on the time synchronization scheme applied, jitter and delay asymmetry requirements may be stipulated for achieving the time synchronization accuracy. While the impedance calculation type FL does not ordinarily need time synchronization, the sampling timing synchronization may be utilized to ensure the accuracy and efficiency of the calculations for multi-terminal lines.

Table 16 – Requirements for fault location

Item	Surge reception	Impedance calculation	Radar echo
Direction	Unidirectional (FLTU to FLCU)		
Bandwidth	1 to 10 kbit/s	1 to 10 kbit/s	1 to 10 kbit/s
Transmission rate	Event driven		
Latency (end-to-end)	≤ 20 to 40 ms	≤ 20 to 40 ms	≤ 20 to 40 ms
Jitter	N/A	N/A	N/A
BER	$< 10^{-6}$	$< 10^{-6}$	$< 10^{-6}$
Redundancy	Single	Single	Single
Unavailability	10^{-4}		
Time (sampling) synchronization	≤ 1 to 3 µs	N/A	N/A
Delay asymmetry	N/A		

6.6 Distribution Automation

6.6.1 Functional description

Figure 27 illustrates a system configuration for distribution automation including power quality monitoring, pole-top voltage regulators & capacitor bank monitoring, remote control of feeder switches, feeder voltage regulation, fault location isolation & service restoration (FLISR) and distribution substation SCADA. The actors include a distribution automation system (DAS) server located in a distribution control centre, IEDs at distribution substations, sensors, voltage regulators and switches situated along distribution feeders.

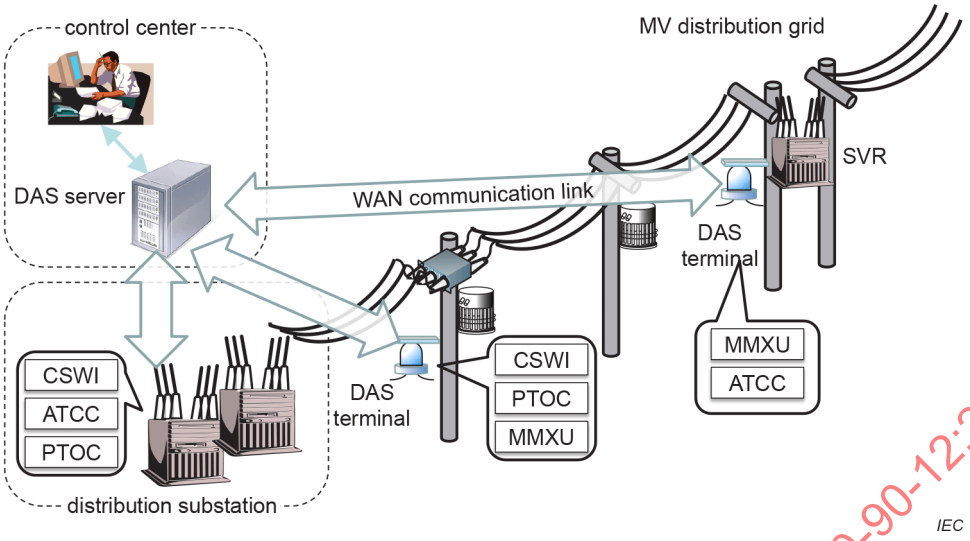


Figure 27 – System configuration for distribution automation

6.6.2 Distribution automation communication requirements

Table 17 shows the communication requirements for distribution automation. Regarding the time synchronization requirement, if an application utilizes synchrophasors, for example, for condition monitoring, fault detection and fault location in a distribution system, microgrid operation, etc. [55], it may need precise time synchronization when a WAN is used.

Table 17 – Requirements for distribution automation communication

Item	Requirement
Direction	Bidirectional
Bandwidth	A few to tens of kbit/s per monitored/controlled device
Transmission rate	Every 30 minutes to once a day for ordinary monitoring Every 0,5 s for monitoring applied for commands Event driven for commands
Latency (end-to-end)	0,5 s for commands 1 s for monitoring
Jitter	N/A
BER	< 5 % (PER)
Redundancy	Single
Unavailability	$< 10^{-4}$
Time synchronization	Depends on application requirement
Delay asymmetry	N/A
Cyber security	Low/Medium

6.7 Condition monitoring and diagnostics (CMD) and asset management (IF7)

6.7.1 Functional description

Condition monitoring and diagnosis systems includes video surveillance, on-line condition monitoring and field workforce voice communication. Figure 28 shows the logical configuration of a CMD and asset management system. In IEC 61850-5, the communication interface at a substation is referred to as IF7 (data exchange between substation (level) and a remote engineer's workplace).

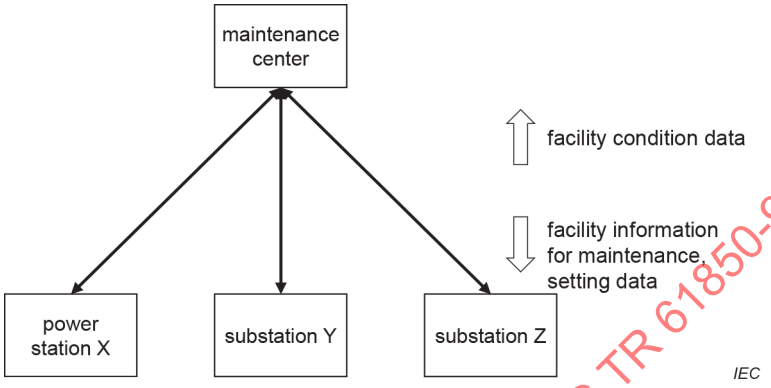


Figure 28 – Network configurations for CMD and asset management

WANs used for CMD and asset management provide communications from maintenance centres to power stations and substations, and vice versa transmitting facility condition data from power stations and substations to maintenance centres, and facility information for maintenance and setting data in the opposite direction. One power station or substation may be supervised simultaneously by multiple maintenance centres.

6.7.2 CMD communication requirements

On-line CMD requires almost the same as telemetry. Table 18 lists the communication requirements for condition monitoring of primary equipment.

Table 18 – Communication requirements for CMD

	Video surveillance	On-line condition monitoring
Direction	Bidirectional	Unidirectional (SS/PS to CC)
Message (frame) size (octets)	1000	160
Message (frame) rate (Hz)	1	0,3 to 1
Bit rate (kbit/s)	100 to 2 000	1 to 10
Latency (ms)	< 1 000 (TL1000)	< 1 000 (TL1000)
Transfer delay asymmetry	–	–
Time accuracy (µs)	–	–
Jitter	–	–
Bit error rate	–	$< 10^{-6}$
Recovery delay (s)	–	20
Unavailability	$< 10^{-4}$	$< 7 \times 10^{-5}$
NOTE A recovery delay of 18 s is compatible with a TCP recovery delay.		

6.8 Telecontrol (SCADA)

6.8.1 Functional description

This use case includes applications such as telemetry, supervision and telecontrol used to report state information of primary and secondary grid equipment to control centres and to control this equipment from control centres. Figure 29 shows the logical configuration of the telecontrol (SCADA) system.

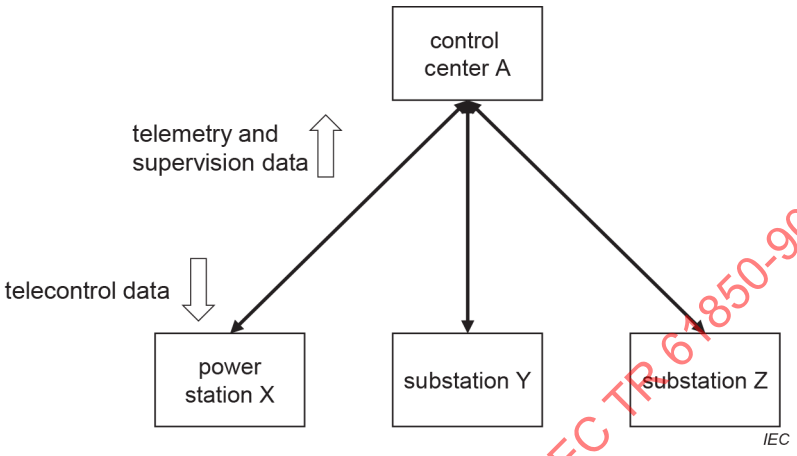


Figure 29 – Logical network configuration for telecontrol (SCADA)

WANs for Telecontrol (SCADA) provide communications from control centres to power stations and substations, and vice versa transmitting telemetry and supervision data from power stations and substations to control centres, and telecontrol data in the opposite direction. One power station or substation may be supervised simultaneously by multiple control centres.

6.8.2 Telecontrol communication requirements

IEC TR 61850-90-2 specifies the communication between control centres and substations/power stations as per IF10. Table 19 lists typical communication requirements.

Table 19 – 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[1)]	< 300 ms (TL300) < 2 s to 4 s[1)]	< 300 ms (TL300) < 0,5 s[1)]	< 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
Bit error rate	$< 10^{-6}$	$< 10^{-6}$	$< 10^{-6}$	$< 10^{-6}$
Recovery delay (s)	20	20	2	2
Unavailability	$< 7 \times 10^{-5}$	$< 7 \times 10^{-5}$	$< 7 \times 10^{-5}$	$< 2 \times 10^{-5}$
SOURCE: Japanese utilities NOTE MV and LV applications				

IEC TR 61850-90-2 specifies the latency and time classes for CC to SS /PS (Table 20).

Table 20 – 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.				

6.9 Control centre to control centre (IF12)

6.9.1 Functional description

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 (Figure 30). Other communications include load dispatch voice and meteorological information collection. IEC TR 61850-90-12:2015 refers to this communication interface as IF12.

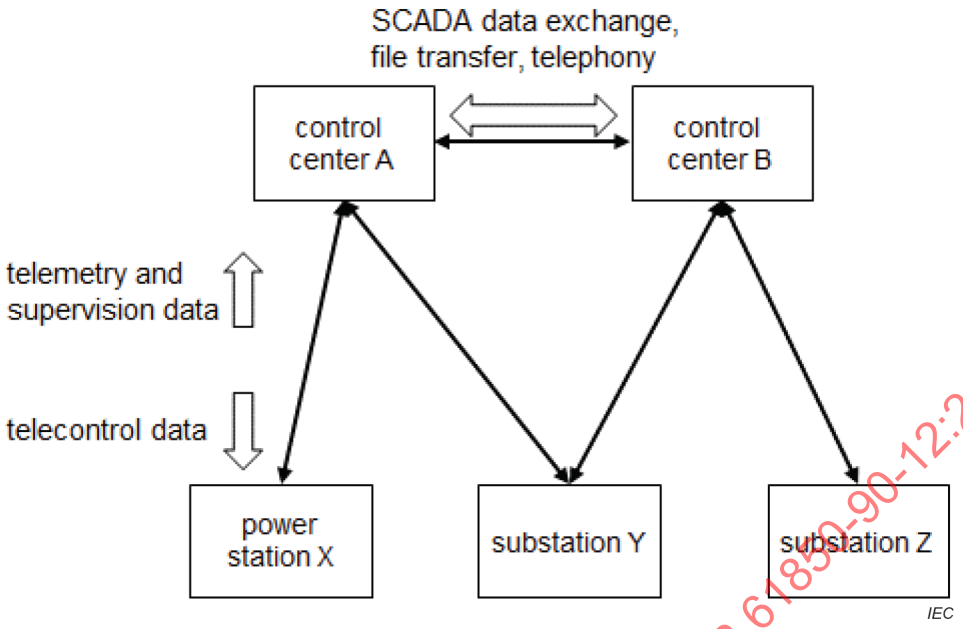


Figure 30 – Network configurations for inter-control centre

The ICCP / TASE-2 standard IEC 60870-6 makes recommendations on communication that are now obsolete as a consequence of technology progress. The CIM standard IEC 61970 makes no recommendation on the network topology or performance.

6.9.2 Inter control centre communication requirements

The required performance is summarized in Table 21.

Table 21 – 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			

6.10 Smart metering / advanced metering infrastructure

6.10.1 Functional description

Figure 31 shows a system configuration for smart metering or AMI (advanced metering infrastructure). A typical AMI system records customer consumption at least once an hour and transmits those measurements at least once a day. AMI requires a fixed communication network with stationary transmitters and receivers and must provide two-way communications. It enables automated periodic measurement of end user energy usage along with 2-way communication associated with remote control (connection/disconnection of electricity supply) capability. Its actors include the smart meter and data centre consisting of a meter data management system (MDMS) and head end system (HES) where in-line concentrators may exist as shown in Figure 31.

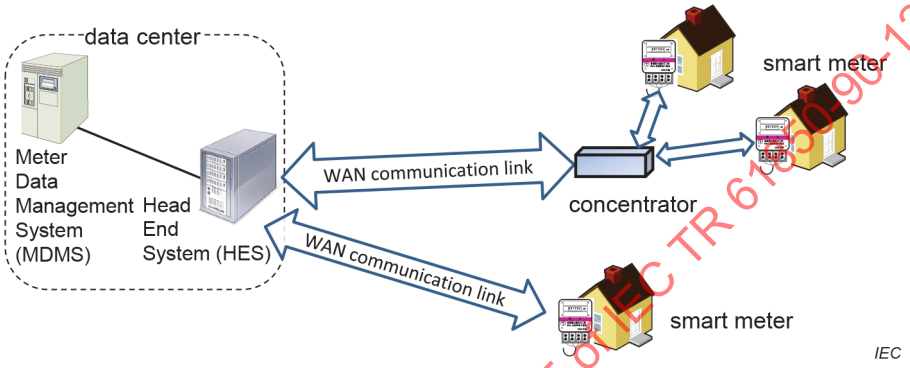


Figure 31 – System configuration for smart metering

6.10.2 Smart metering communication requirements

The communication requirements are shown in Table 22. Regarding the time synchronization requirement, since meter data is collected every 15 to 30 minutes, the time synchronization error required may be, for example, less than 10 ms.

Table 22 – Requirements for smart metering communication

Item	Requirement
Direction	Bidirectional
Bandwidth	20 kbit/s per meter
Transmission rate	Every 15 or 30 minutes to once a day for meter data Event driven for command
Latency (end-to-end)	1 min. for meter data 5 s for command
Jitter	N/A
BER	< 10^{-2} (packet error ratio)
Redundancy	Double
Unavailability	< 10^{-3}
Time synchronization	< 10 ms
Delay asymmetry	N/A
Cyber security	High

6.11 WAN communication requirements summary

Table 23 reduces the communication requirements to four distinct classes to which all requirements are mapped, with approximately one order of magnitude in between.

Table 23 – 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[1)]	100 µs	1 ms	10 ms	100 ms
Time accuracy[2)]	1 µs	10 µs	100 µs	10 to 100 ms
Bit error ratio	10^{-7} to 10^{-6}	10^{-5} to 10^{-4}	10^{-3}	
Unavailability	10^{-7} to 10^{-6}	10^{-5} to 10^{-4}	10^{-3}	
Recovery delay	zero	50 ms[3)]	5 s[4)]	50 s[5)]

1 The jitter requirement can be relaxed if common clock synchronization exists.

2 Applies to time distribution only.

3 Compatible with SDH/SONET, MPLS and IP (FRR).

4 Compatible with RSTP/MSTP.

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 24, but actual numbers may differ.

Table 24 – 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^{-6}	10^{-6}	0
State comparison line protection	SS-SS	< 10	10	0.1	–	1	10^{-6}	10^{-6}	0
Transfer tripping	SS-SS	< 10	3	0.3	–	1	10^{-6}	10^{-6}	25
WAMS	SS-CC	10 to 100	100	1	–	1	10^{-6}	10^{-6}	50
WAMPAC for transient stability	SS/PS-CC	10 to 100	10	0.1	–	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 General

Clause 7 describes the network technologies available for WANs used 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 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 32 illustrates an example in which the rings are explicit.

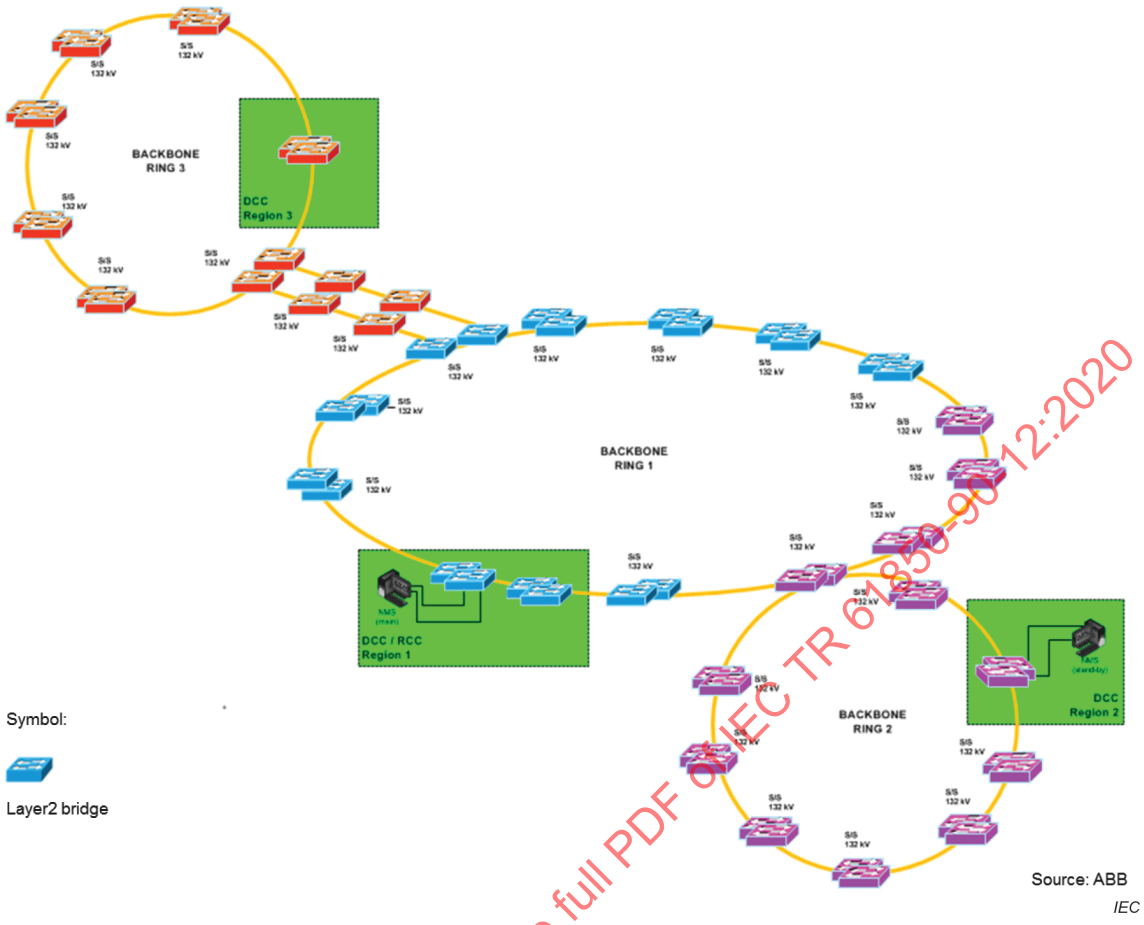


Figure 32 – Network ring topology example

7.3 Overview

Any network has:

- a data plane that switches the circuits or packets (corresponding to the old relays used in analogue telephony);
- a control plane that determines how data is routed from network element to network element (corresponding to the dialling pulses processing in analogue 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 25 summarizes the technologies for building WANs while providing the performance required.

Table 25 – 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	IEEE 802.3, ATM, PPP, Frame Relay	IEEE 802.3, ATM, PPP, Frame Relay
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	PTP, 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)	Automatic (OSPF, IS-IS, SNMP)	Automatic (LDP,RSVP-TE)	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
Observations	Obsolete	Widely used in utility networks	Widely used in metropolitan and access networks	Widely used in WANs	Possible migration path from SDH/SONET to PSN	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 26 list the media detailed in 7.4.3 to 7.4.6.

Table 26 – 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 fibre					
	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	> 100km	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)	A few kbit/s to 300 kbit/s	4,2 µs to13 µs per km	1000 km	IEC 60495 IEEE 1901 (TDM)
	MV, LV meshed	10 kbit/s to100 kbit/s, up to 30 Mbit/s	5 µs / km	Up to 2km 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 Ω.

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 a substation environment, it is not recommended to span copper cables over such distances; fibres are recommended instead.

Twisted pair cables are used not only for analogue 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 analogue 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 27 compares the different DSL technologies.

Table 27 – 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 28 details the trade-offs of copper cable communication.

Table 28 – 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)

7.4.4.1 General

The electricity grid is one of the most ubiquitous wire networks available throughout the world.

A power line terminal is equipment able to manage a telecommunication link over an electricity power line, mainly used to reliably transmit speech, data, and power system protection signals.

The power network is very diverse ranging from high voltage operating at the order of 100 kV and more, medium voltage at below 100 kV and low voltage below 1 kV. There are several power line communication technologies typically used by Power Utilities depending on the segment of the grid and the application to be supported.

Each power line can be used to simultaneously transmit both energy as well as signals.

The communication services offered by modern power line communication system are point-to-point and meshed links which enable a high efficiency of data transmission and therefore a low level of operational costs of automation equipment especially for long high-voltage power transmission lines.

Table 29 summarizes the advantages and disadvantages of PLC communication.

Table 29 – Power Line Telecommunication advantages and disadvantages

Advantages	Disadvantages
Electricity grid is ubiquitous and in general can easily reach areas where Telcos have no interest/coverage	Disaster susceptible (if high-voltage lines are damaged)
Communication independent of external provider	Very harsh environment for a communication channel
Uses existing power line utility assets	Needs access to the high-voltage line
Cost-effective and fast installation and maintenance	Low bandwidth (< 1 Mbit/s) with narrowband technology Low distance range with broadband technology
Robust, long-distance communication with HV PLC	Correlation between line fault and communication channel: not suited for analogue comparison schemes

NOTE The term "power line carrier" (PLC) refers specifically to narrowband transmission over high-voltage, and sometimes medium-voltage, powerlines for point-to-point communication.

Other technologies exploiting power lines as transmission medium are named distribution line carrier (DLC), MV high data rate and LV narrowband PLC. Medium- and low-voltage broadband power line communication or BPL. The latter in the majority of cases find their application within the access segment for metering and in-house, in-home related applications.

Typical use case scenarios for power line communication technologies include:

- operational speech;
- teleprotection in HV;
- data transmission for RTU-SCADA communication;
- grid to utility metering to establish an advanced metering infrastructure (AMI);
- grid automation, especially in distribution automation;
- communication between electric vehicles and charging stations;
- home area networking and automation;
- lighting infrastructure in buildings and outdoors (street lighting);
- solar panel power line communication and automation;
- smart grid application (demand response, home EMS, etc.).

7.4.4.2 Frequency bands for power line telecommunication systems

There are different spectrum allocations and associated channel plans for PLC communication systems depending on the level of voltage of the electrical power line used, international standards and local regulation, and type of transmission i.e. narrowband or broadband.

7.4.4.3 HV narrowband PLC frequency spectrum

Most of the multi-purpose systems require a bandwidth of 4 kHz for each direction of transmission; therefore, the available range of frequencies (24 kHz to 1 MHz) is divided into a number of channels each 4 kHz wide. Two of these will be required for each two-way carrier circuit but they need not necessarily be adjacent.

It is a good practice, in order to assure compatibility and coexistence with other systems in operation, that new digital and traditional systems will use basically the same channelling approach. Depending on the technology used, it is common to have adjacent, non-contiguous, and superimposed bidirectional transmission channel grouping a number of 4 kHz channels.

Other channel widths have also been adopted in some countries to suit their special needs.

The range of frequency for standards in Europe (CENELEC) and USA (IEEE) and other countries are shown in Table 30 .

Table 30 – HF spectrum allocated for HV/MV PLC systems

	IEC-CENELEC	USA	Other countries
Reference standard	IEC 62488-1	IEEE 643	-
Frequency range	40 kHz to 500 kHz	24 kHz to 1 MHz	24 kHz to 1 MHz
NOTE Frequency ranges are also provided in IEC 61334-3-1 (distribution line carrier systems frequency bands for distribution automation) and IEC 61000-3-8 (frequency range from 3 kHz up to 525 kHz to transmit information on low-voltage electrical installations).			

7.4.4.4 LV narrowband PLC frequency spectrum

Power line communication is mostly used over LV underground cables to establish narrowband communication using the frequency spectrum as shown in Table 31.

Table 31 – HF spectrum used for narrowband LV PLC and associated standards

	CENELEC (EUROPE)			USA	Other countries
Reference standard	**EN 50065-1**			**IEEE 643**	**-**
Frequency range	3 to 148,5 kHz	A band (3 kHz to 95 kHz)	Utilities access	50 kHz to 450 kHz	-
		B band (95 kHz to 125 kHz)	Consumer In-house in-home		
		C band (125 kHz to 140 kHz)			
		D band (140 kHz to 148,5 kHz)			

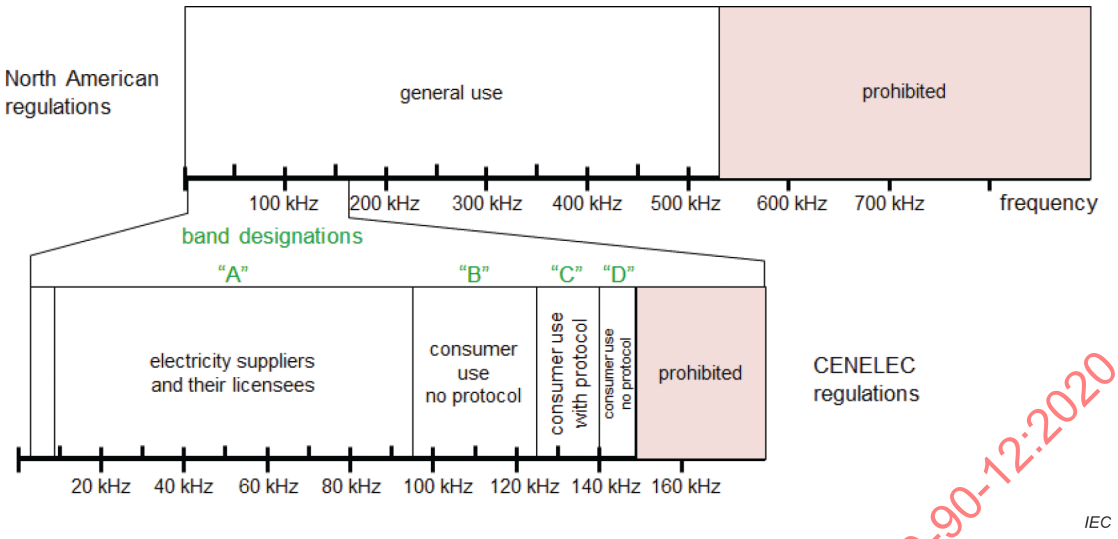


Figure 33 – Narrowband channel plans for LV PLC Europe vs. North America

Figure 33 shows the allocated spectrum in Europe and the USA for LV PLC.

7.4.4.5 LV broadband power line (BPL) frequency spectrum

Figure 34 shows the allocated frequency spectrum for low-voltage broadband power line telecommunication.

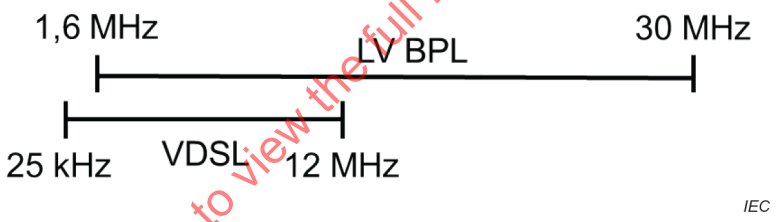


Figure 34 – HF allocated frequency spectrum plans for LV BPL

7.4.4.6 Reference standards for power line telecommunication systems

7.4.4.6.1 General

Narrowband HV PLC is well covered by the following standard:

- IEC 62488, *Power line communication systems for power utility applications*.

MV/LV Narrowband PLC is covered by several communication standards. In the following a list of some common standards is reported:

- IEC 61334:2001 is based on spread frequency shift keying (SFSK);
- IEEE 1901.2:2013 defines PHY & MAC including security and a northbound interface; supports all global bands and hence by definition, offers multiple modes of operation;
- ITU-T G.9902 G.hnm:2013 Narrowband orthogonal frequency division multiplexing power line communication transceivers for ITU-T G.hnem networks specifies MAC, LLC for OFDM PLC systems;
- ITU-T G.9903 G3:2008, this standard specifies MAC, PHY, LLC. It is also supported by G3 Alliance;
- ITU-T G.9904 PRIME:2008, this standard specifies PHY, MAC. It is also supported by PRIME Alliance;

- CLC/prTS 50568-4 and CLC/prTS 50568-8 standards in part adopted by Meters & More Alliance.

Typically, these standards operate in the frequency range below 500 kHz and make use of different channelling plans, according to the regulation established in each country and region.

Figure 35 shows the use of narrowband spectrum depending on the standards and regulation areas.

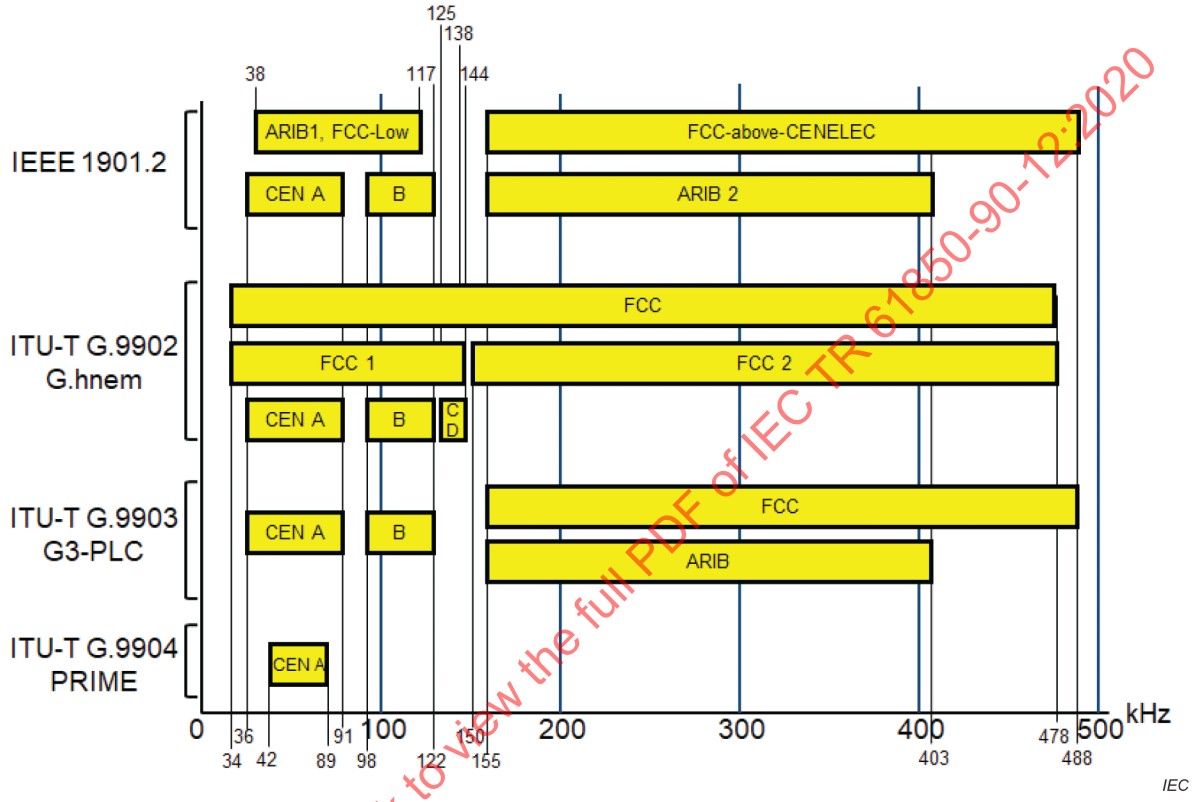


Figure 35 – Narrowband spectrum usage vs. standards and regulation areas [57]

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

Typically, these standards support several bands in this frequency range, established and regulated in different countries and regions. Typical use case scenarios for Narrowband-PLC are:

- grid to utility metering to establish an advanced metering infrastructure (AMI);
- grid automation, especially in distribution automation;
- communication between electric vehicles and charging stations;
- home area networking and automation;
- lighting infrastructure in buildings and outdoors (street lighting);
- solar panel power line communication and automation.

Narrowband PLC shares the medium, wires and cable, with electric power transmission or electric power distribution. The key advantage is that the existing infrastructure, the power grid, is used to establish a communication network as well. As power lines were originally designed and deployed for the distribution of power at 50-60 Hz AC, the use of PLC for communications at higher frequencies (3 kHz to 500 kHz) presents some technical challenges such as:

- signal losses due to reflections and frequency selective fading;
- cable transition can cause reflections and can change characteristic impedance resulting in multipath signal propagation;
- noise and interference can occur, typically background noise and impulsive noise caused by switching power supplies and halogen lamps.

Robust coding, interleaving and modulation techniques are needed to address these problems in harsh environments. Coexistence mechanisms (as for example defined in IEEE 1901.2) are important for flexible deployments. On the other hand, Narrowband PLC installations must comply with regulation requirements, i.e. regarding the limit on radiated and conducted emission (CENELEC EN 50065), disturbing other systems operating in the same frequency band. As an example, injection of a PLC signal in a power cable will result in radiation of an electromagnetic field, where power cables are acting as antennas.

Table 32 lists the key characteristics of specified and deployed Narrowband-PLC standards:

Table 32 – Characteristics of common NB-PLC standards

	IEEE P1901.2	G3-PLC	PRIME
Specifications	IEEE P1901.2-2013 (PHY & MAC)	ITU G.9903 (PHY, MAC, LLC, address allocation)	ITU G.9904 (PHY & MAC)
Frequency bands	CENELEC A & B FCC, ARIB Low & Medium Voltage support	CENELEC A & B FCC, ARIB Low & Medium Voltage support	CENELEC A FCC, ARIB
Coding and modulation	OFDM Super ROBO, ROBO, DBPSK, DQPSK or D8PSK – 16QAM FCC (optional)	OFDM ROBO, DBPSK, DQPSK or D8PSK	OFDM DBPSK, DQPSK or D8PSK ROBO
Maximum theoretical data rate	Dependent on modulation & frequency band – from +30kbs in CENELEC A band to +300kbs in FCC band above CENELEC	Dependent on modulation & frequency band – from +30kbs in CENELEC A band to +300kbs in FCC band above CENELEC	Dependent on modulation & frequency band – from +100kbs in CENELEC A band to +900kbs in FCC band
Maximum MAC payload size	Up to 1280 octets (aligned with IPv6 MTU size)	Up to 400 octets	Up to 2268 octets
IEEE 802.15.4 MAC frame format	Yes 15.4e Ack Sec & Information Elements	Yes No Ack Sec & 15.4e Information Elements	No
Convergence sub-layer	IPv6 6LoWPAN	IPv6 6LoWPAN	Null CS, IPv4, IPv6 Connection-oriented
IPv6 header Compression	Yes, 6LoWPAN RFC 6282	Yes, 6LoWPAN RFC 6282	Optional, 6LoWPAN RFC 6282 if supported
Packet forwarding and routing	Layer-3 Routing using IPv6 Routing – RPL (RFC 6550)	Layer-2 Mesh Switching using LOADng protocol	Layer-2 Switching defined in G.9904
Security	AES-128, CCMP	AES-128, CCMP	AES-128

7.4.4.6.2 Network and deployment considerations for MV/LV Narrowband PLC

Depending on the technology, the network topologies supported are different. PRIME supports tree based networks, while IEEE 1901.2 and G3-PLC specify meshed networks. Narrowband-PLC based technologies may implement layer-2 forwarding or layer-3 routing protocol mechanism. The IEEE 1901.2 standard contains a reference to RPL (IPv6 Routing), and is dedicated to so-called low power and lossy networks (LLNs), specified by a series of RFC documents. This layer-3 IPv6 routing protocol enables integration of narrowband-PLC subnets in an IP infrastructure. It is also used by other PHY and MAC layer specification such as IEEE 802.15.4g RF as well as by other IETF 6LO (working group) technologies. The alignment with the IEEE 802.15.4g/e RF Mesh profile based on 6LoWPAN (RFC 6282) as an adaptation layer and RPL (RFC 6550) for routing at the network layer enables a mix of PHY/MAC technologies in a single deployment. RPL specifies routing metrics that can be derived from the link layer quality such as RSSI and LQI, used by an objective function (i.e. RFC 6719, *Minimum rank with hysteresis objective function*), which can be adapted to any PHY/MAC technology. RPL routing information can be re-distributed in other IP dynamic routing protocols, i.e. OSPFv3, MP-BGP, ensuring end-to-end IPv6 reachability as well as filtering capabilities.

7.4.4.7 HV narrowband PLC Systems

The modulated High frequency (HF) PLC transmitted signal is injected into the power line by means of a coupling system (which basically includes a coupling capacitor, line trap and line matching unit or LMU).

At the receiving side, the attenuated signal is first decoupled and then demodulated by the PLC receiver as shown in Figure 36.

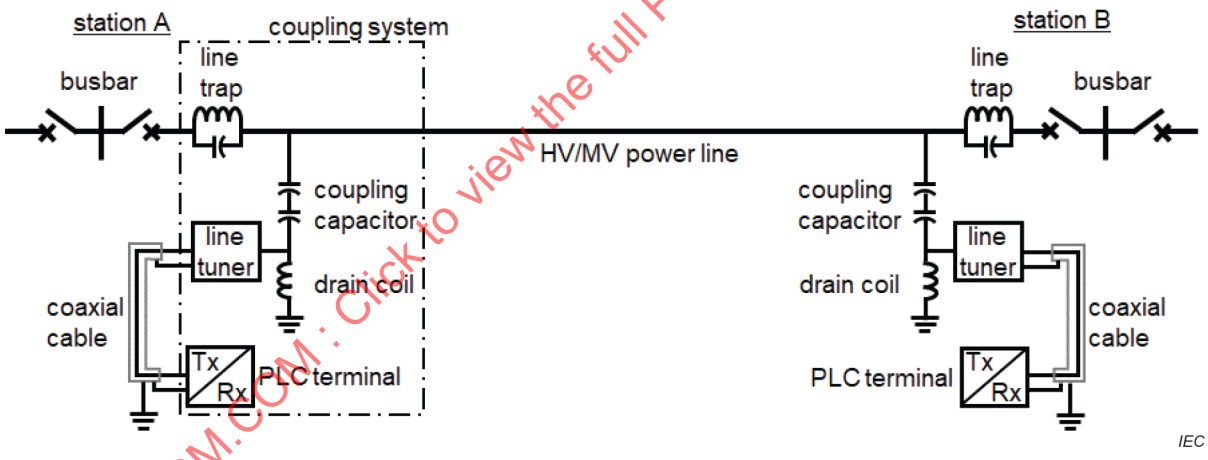


Figure 36 – HV PLC link building blocks

PLC terminals can be classified in accordance with the modulation technology they use, analogue PLC (APLC) or digital PLC (DPLC). A hybrid terminal is equipment that includes both APLC and DPLC.

All narrowband APLC and DPLC equipment maintain a compatibility channelling plan that fits the requirements of the coupling system present over the electricity grid (HV and MV) in order to reduce the overall cost of the assets and at the same time assuring the coexistence with other equipment in operation.

Phase-to-ground and phase-to-multiphase coupling/differential coupling may be used.

Figure 37 and Figure 38 show phase-to-ground coupling, which is the most commonly used in HV power lines.

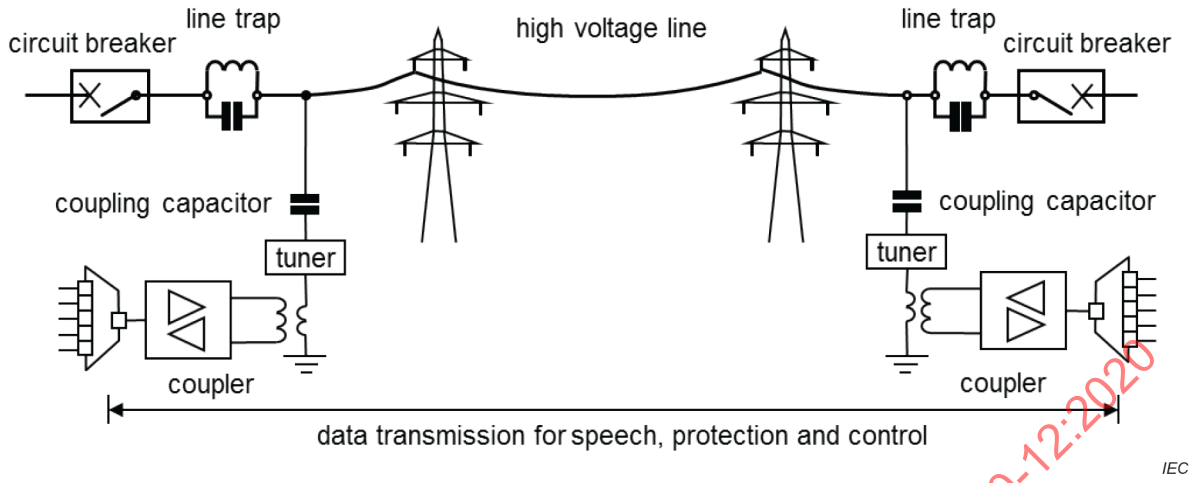


Figure 37 – Phase-to-ground coupling for PLC

Figure 38 – HV PLC coupling with suspended line traps

Signal coupling phase-to-phase is more expensive and is recommended when higher reliability is requested. This configuration maintains data transmission even with a power line phase down. In this case two coupling capacitors and two line traps are required at each coupling point. Figure 39 and Figure 40 show phase-to-phase coupling arrangements.

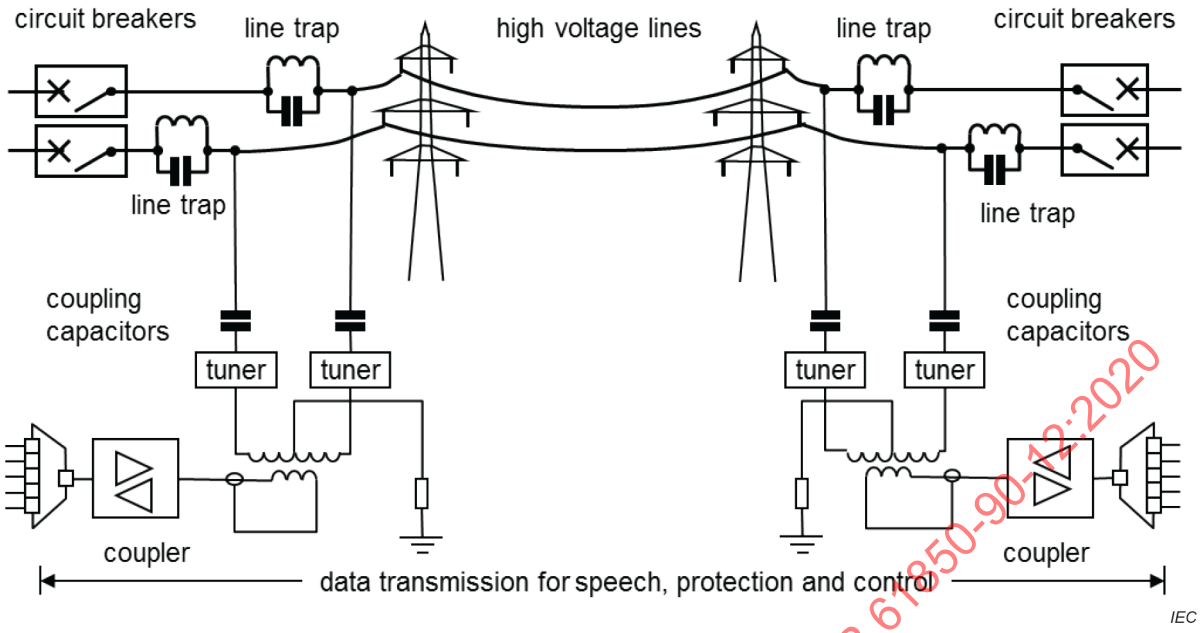


Figure 39 – Phase-to-phase signal coupling for PLC

Figure 40 – Phase-to-phase signal coupling

Figure 41 shows the installation of line traps.

Figure 41 – Power line carrier, line traps

7.4.4.8 APLC systems

APLC systems have been in use for many years by electricity utilities for their communication needs (teleprotection, telephony and data, fax) mainly on the EHV and HV electricity transmission grids.

The modulation scheme generally used for these systems is single sideband (SSB) amplitude modulation to carry one or several basic telephone channels in the carrier range from 20 kHz to 500 kHz (sometimes extended to 1 MHz).

When more than one service is required, the services are mixed using frequency division multiplexing (FDM). The main limitation of APLC systems is the data rate which is limited to some hundred bit/s per service because of the limited bandwidth and the nature of the modulation.

Some of the most commonly used technologies within APLC systems are listed below:

– frequency-division multiplexing;
– single sideband modulation;
– channel equalisation;
– FSK modem (rates ≤ 2400 bit/s);
– PSK or QPSK modem (rates > 600 bit/s).

7.4.4.9 DPLC systems

Today, the transmission speed of PLC has increased mainly due to the progress in the adopted encoding and digital modulation scheme. Thanks to the introduction of digital power line carrier (DPLC) equipment using single or multicarrier quadrature amplitude modulation (QAM, OFDM) data rates of up to 128 kbit/s and more have been allowed.

When more than one service is to be transmitted, DPLC makes use of time division multiplexing (TDM) to arrange the different services into a single stream.

The main advantages of DPLC links as compared to APLC links are the following:

1) Enhancing the transmission capacity compared with traditional APLC links for the same channel bandwidth:
   - more data channels (or data channels running at higher rates);
   - more speech channels using vocoding techniques.
2) Easy integration of the PLC network into a larger digital network (DPLC as an embedded component of a digital telecommunications network):
   - n × 64 kbit/s channel as a tributary channel of a digital telecom network;
   - digital data interfaces for lower speed data avoiding intermediate modems;
   - data rates of DPLC allow their use for LAN to LAN connection (typically through an Ethernet access);
   - a native network access provides an easy way to integrate the DPLC links in a network management system.
3) The use of TDM provides greater degrees of flexibility as compared to frequency-division multiplexing.

DPLC links can be used in access links or network internal links, for the transmission of speech, data and teleprotection related signals.

Some of the most commonly used technologies within DPLC systems are listed below:

– quadrature amplitude modulation (QAM);
– multicarrier modulation (OFDM);
– trellis coding modulation;
– echo cancellation;
– adaptive equalisation;
– time division multiplexing (TDM);
– speech compression.

7.4.4.10 APLC and DPLC performance

The propagation delay of PLC varies depending mainly upon the signal elaboration time within modems and upper layer interfaces. Quite a small contribution to delay is also a function of the geometry of the power line primary characteristics (F/m, H/m); it typically lies between 4 µs/km and 13 µs/km.

As shown in Table 33, power line telecommunication technology is often also used in MV distribution electricity grids.

Table 33 – HV/MV APLC/DPLC/BPL technology performance

Voltage level	Technology	Narrowband PLC	Broadband BPL
		24 kHz to 1 MHz	1,8 MHz to 30 MHz
		Low/medium data rate	High data rate
		0,2 kbit/s to >128 kbit/s	up to100 Mbit/s
High voltage >100 kV (WAN)			
	Range	> 200 km	
	Application	Teleprotection, utility communication, SCADA	
	Standards	IEC 62488	
Medium voltage > 20 kV (RAN)			
	Range	0,5 to 10 km	0,5 to 1,5 km
	Application	Distribution automation ripple control	Smart grid backbone
	Standards	IEC 62488 series, IEC 61334-5-4	IEEE 1901

7.4.5 Radio transmission

7.4.5.1 General

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

NOTE IEC 61850 does not define mapping to radio links yet.

Radio transmission features can be divided into:

- omnidirectional vs. directional depending upon the type of antenna;
- licensed bands (costly, difficult to obtain, but in principle interference-free) vs. unlicensed bands (free, but shared with unpredictable traffic);
- fixed vs. mobile – the latter being interesting for workforce communication;
- indoor units vs. 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, antenna directivity) and interference from other radio systems;
- transmitting power, this may be regulated in some countries;
- receiver sensitivity.

In general, radio transmission can be affected by higher error rate, limited radio range and lower throughput, compared to wireline communication. They are subject to security threats such as jamming, DoS attacks, spoofing and interception.

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

The radio range impacts the distance between relays. Higher radio range and worse radio conditions impact the battery lifetime due to the higher transmitting power required and higher number of retransmissions.

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.

NOTE Terrestrial fixed microwave radio usually requires licences and can be quite expensive. This means it is predominantly reserved for high-end use.

Microwave technologies are deployed in clear line-of-sight conditions and offer point-to-point connectivity, as shown in Figure 42.

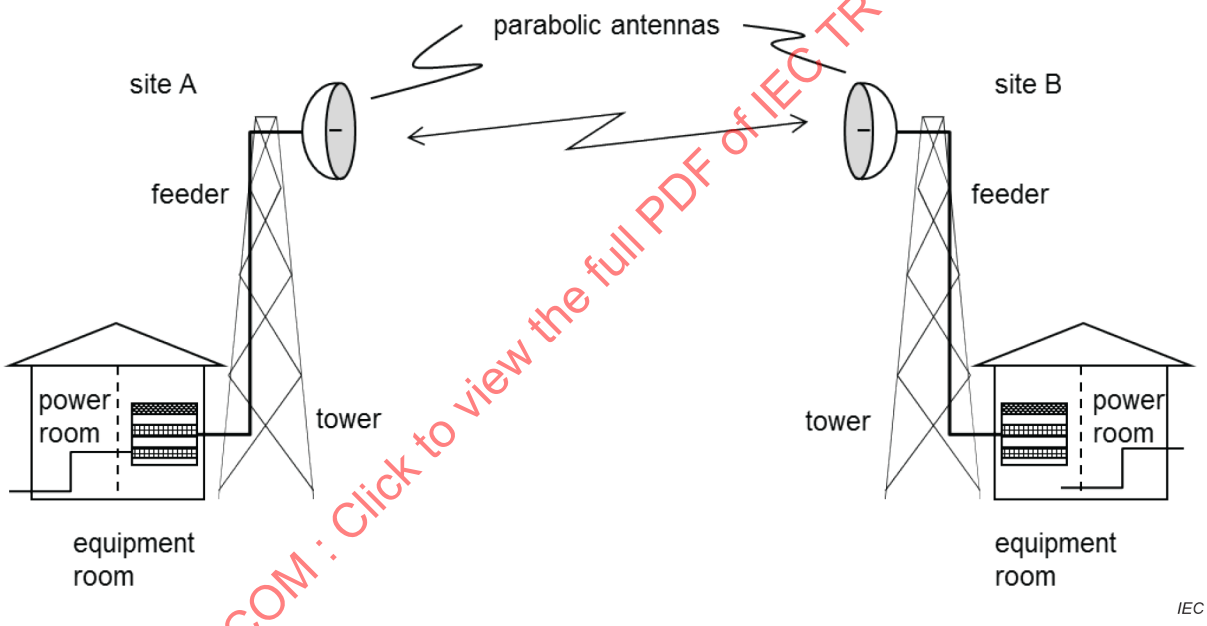


Figure 42 – Terrestrial microwave link

Figure 43 shows the different interface options for microwave radio systems. Digital microwave radio links transport Layer 2 PDUs via:

- PDH/SDH/SONET interfaces, T1 or E1 interfaces (see 7.6.1.2), including Ethernet over SDH (Figure 43 (a));
- native Ethernet interfaces (Figure 43 (b));
- TDM traffic converted to packet stream and all traffic handled as packets (Figure 43 (c)).

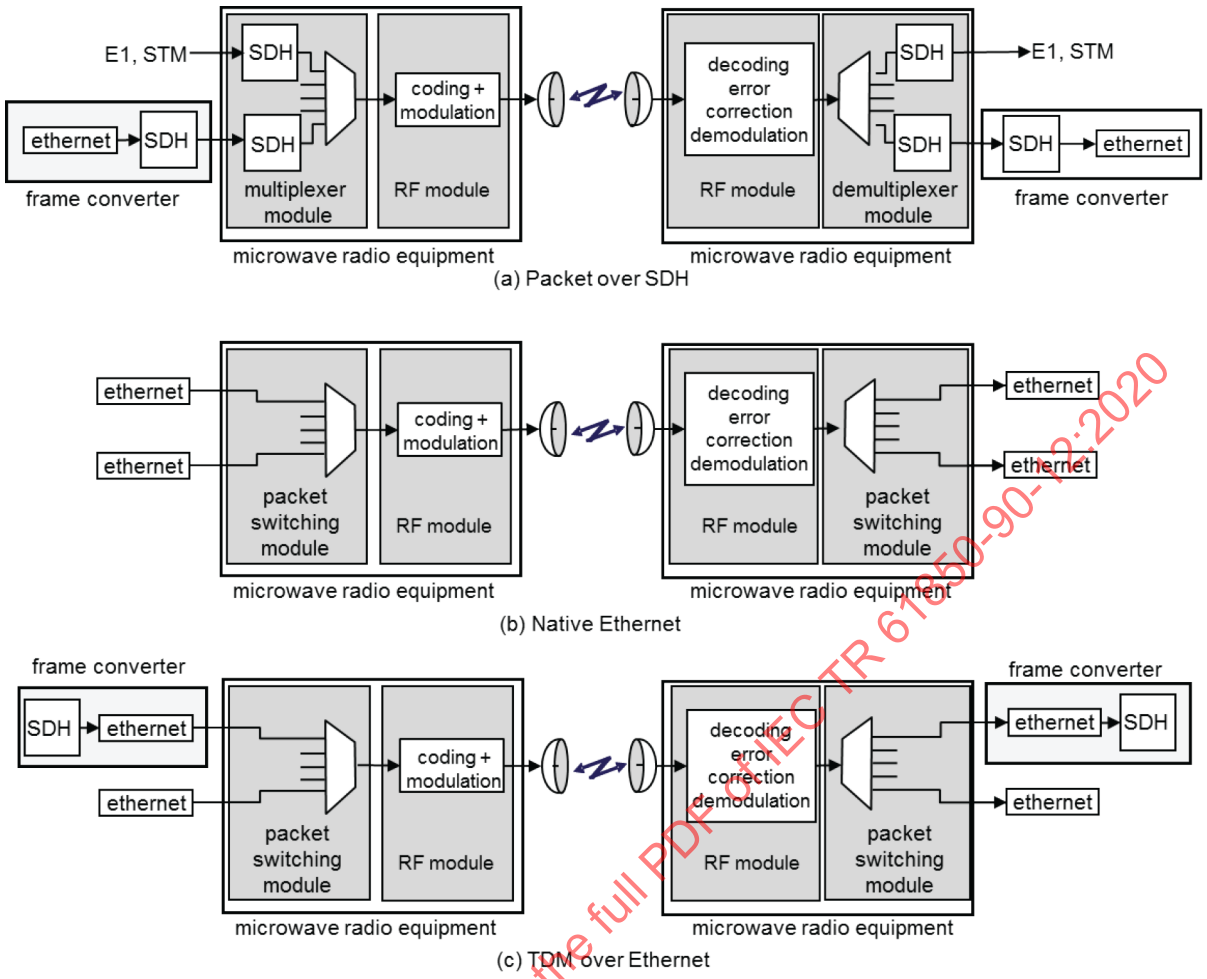


Figure 43 – Layer 2 transport on microwave radio systems

Table 34 shows typical microwave link performances.

Table 34 – Microwave link performance

Link type	Carrier	Radio range	Typical bandwidth per carrier	Channel configuration	Typical data rates
long-haul	4 GHz to 11 GHz	Tens of km, typically 30 km – 60 km	5 MHz, 10 MHz, 20 MHz, 30 MHz, 40 MHz	Multichannel 10+0	8-311 Mbit/s (34 Mbit/s, 140 Mbit/s, 155 Mbit/s, etc.)
short-haul	12 GHz to 42 GHz	A few tens of km	2,5 MHz, 3,5 MHz, 7 MHz, 10 MHz, 14 MHz	Multichannel 4+0.	34-140 Mbit/s
very short link	52 GHz to 90 GHz	A few km	3,5 MHz, 7 MHz, 10 MHz, 14 MHz, 28 MHz, up to 2.5 GHz	Single channel	Up to 1 Gbit/s and greater
NOTE Source ITU-R report F.2323-1. The distance covered depends on regulations (permitted transmission power).					

Table 35 shows the advantages and disadvantages of terrestrial microwave.

Table 35 – Terrestrial microwave advantages and disadvantages

Advantages	Disadvantages
Relatively cost-effective installation, no digging required.	Short period of outages during fading and/or attenuation in certain terrains and frequency bands, depending also on the weather and other meteorological phenomena.
In case of deploying dedicated microwave towers: little interference from power system asset failures (unlike optical fibres if using the power masts i.e. power line transmission towers)	Need of high elevation sites for microwave antennas. Disaster-sensitive if antenna located on power masts. (separate microwave towers are preferred)
Long haul communication capability.	Limitation to point-to-point communication.
	Need for license. High costs.

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 36 lists the major terrestrial mobile radio technologies. One should note that 2nd generation mobile radio technologies, such as GSM and GPRS, are about to disappear and not recommended for future use. However, GSM/GPRS can be replaced by LTE CAT-M for continuous control communication, such as IEC 60870-5-104, DNP3 and Modbus TCP and by NB-IOT for sensor-style, on-demand communication.

Table 36 – Terrestrial mobile radio technologies

Technology	Bands country dependent	Typical radio range	Typical data rate	Status
GSM	850 MHz to 1900 MHz	A few tens of km	9,6 kbit/s	2nd generation mobile network
GPRS	850 MHz to 1900 MHz	A few tens of km	80 kbit/s (downlink) 40 kbit/s (uplink)	2nd generation mobile network
UMTS	850 MHz to 2100 MHz	A few tens of km	384 kbit/s to 2 Mbit/s	3rd generation mobile network
UMTS WCDMA	850 MHz to 2500 MHz	A few tens of km	7,2 Mbit/s	3rd generation mobile network
UMTS – HSPA+	850 MHz to 2500 MHz	A few tens of km	28 Mbit/s to 42 Mbit/s (168 Mbit/s downlink)	3rd generation enhanced for IP data traffic
WiMAX (IEEE 802.16-2004)	2 GHz to 11 GHz	2 km to 10 km	Up to 70 Mbit/s	Obsoleted by LTE
LTE	700 MHz to 2600 MHz	A few tens of km	150 Mbit/s (300 Mbit/s (4G+))	4th generation mobile network

Technology	Bands country dependent	Typical radio range	Typical data rate	Status
Wi-Fi/WLANs (IEEE 802.11)	2,4 GHz, 5 GHz	100 m	4,3 Mbit/s to 3500 Mbit/s (netto)	Widespread use
NOTE The radio range does not depend so much on the mobile technology (2G, 3G, 4G) but on the frequency band that is used (e.g. 850/900 MHz, 1800/1900/> 2000 MHz) and the local geographical conditions. Furthermore, the mobile cell dimension is usually designed considering also the estimated number of mobile subscribers at that location. By rule of thumb, a radio range of up to approximately 30 km is achieved and used at 900 MHz in rural locations but only up to a few hundred metres are used in city locations at 1800 / > 2000 MHz.				

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 37).

Table 37 – Terrestrial radio advantages and disadvantages

Advantages	Disadvantages
Cost-effective and easy to install	Relatively short transmission range (< appr. 30 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 DMR (digital mobile radio)

The European Telecommunications Standards Institute (ETSI) defined DMR (digital mobile radio) in TS 102 361 (since 2005) as a complement to TETRA to replace analogue radio links for voice and data over the same two 12,5 kHz communication channels.

DMR comprises three profiles (tiers):

1) Tier 1 (unlicensed) for amateur or commercial applications operates in the 446,1 MHz to 446,2 MHz band with 500 mW power as a point-to-point communication in FDMA. Tier 1 is intended for direct communication between devices.
2) Tier 2 (licensed conventional) for industrial applications operates in point-to-point or uses a repeater station with a 2-slot TDMA and random access (listen before talk). Power can be increased to several watts in licensed bands, allowing ranges of kilometres. Tier 2 is used for direct communications between devices (walkie-talkie) and also for communication to a base station. There exists a tier 2 variant using FDMA.
3) Tier 3 (licensed trunked) for critical applications operates with a network of base stations and uses a 2-slot TDMA / 4FSK. It is a trunked technology, meaning that the base station permanently broadcasts a carrier to assign the time slots, avoiding collisions and carrier establishment delays, eases roaming and sets priorities. A station asks the base station for a transmission slot in the signalling channel.

For electrical utilities, only Tier 3 is relevant as it provides a high availability and long range (typical power is 5 W for hand-help devices and 25 W for a fixed station, including pole-mounted).

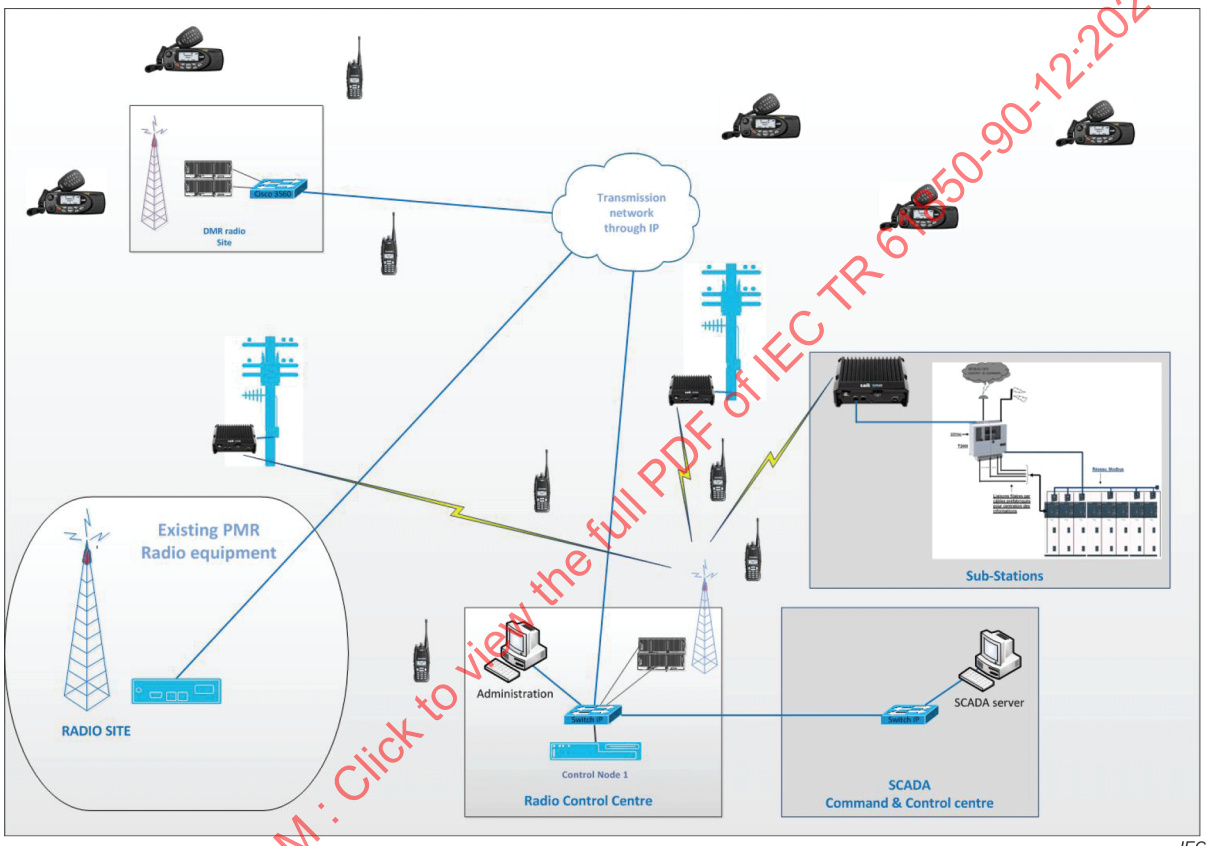
Although in principle applicable to the whole range 66 MHz to 960 MHz, DMR T3 mainly operates on the 380-440-470 MHz (upper) and 150 MHz (lower) bands. With about 5 W of power, transmission distances to the base station are several kilometres. Data quality is enhanced by forward error correction. Data may be protected by AES 256 encryption with corresponding reduction of the data rate.

While the payload data rate is low (typically 2,4 kbit/s), it is sufficient for voice communication between maintenance teams, demand response, remote operation of distribution grids, pole top devices and RTUs in rural areas. DMR networks operate independently from the grid and therefore can be used in wide-area emergency operations.

The ETSI standard TS 102 361 series describes the physical layer, the radio spectrum, the data protocol, and the trunking protocol.

(Source: TAiT GridLink, 2012)

Figure 44 shows typical use of DMR by electrical utilities.



(Source: TAiT GridLink, 2012)

Figure 44 – DMR (Digital Mobile Radio)

Table 38 shows the advantages and disadvantages of DMR.

Table 38 – DMR advantages and disadvantages

Advantages	Disadvantages
Infrastructure exists for maintenance teams and distribution grid.	Limited bandwidth
Robustness, can be used for back-up and disaster-recovery	
Reserved communication channels	
Simplicity	

7.4.5.6 Satellite radio

Satellite radios use microwave bands to communicate via geostationary or low-orbit satellites, see Table 39.

Table 39 – 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 fibres in high-voltage lines or ground cables)	Subject to jamming, DoS attacks, spoofing and interception

7.4.5.7 Low-Power Wide-Area Network (LPWAN)

7.4.5.7.1 General

Low-power wide-area networks (LPWAN) comprise wireless telecommunication network technologies that allow long range communication and deep indoor penetration by using special modulation and low bit rate encoding. LPWAN is a core network technology to connect a vast number (thousands) of objects (such as battery powered sensors) in an IoT (Internet of Things) environment. It fills the gap between local wireless and cellular wireless technologies; other characteristics are:

- end-device with battery life lasting longer than 10 years;
- over-the-air distance over 15 km;
- optimized for small and intermittent data burst;
- data payload from 10 to a few 100 octets;
- data rate from 60 bit/s to 100 kbit/s;
- operating in licensed and unlicensed spectrum;
- outdoor coverage and sufficient indoor penetration.

Exemplary use case scenarios for LPWAN are:

- water and gas metering;
- electric metering;
- location tracking;
- street lighting;
- smart parking;
- waste management;
- environmental monitoring;
- smart buildings.

LPWAN deployments are typically scattered and used to track, monitor, and manage assets.

A number of technologies are available, e.g.:

- LoRaWAN™ [4];
- UNB ultra narrow band (Sigfox-like technologies);
- cellular based technologies.

Some of these technologies operate in a licensed spectrum (e.g.: LTE), other technologies in an unlicensed spectrum (e.g.: LoRaWAN™).

7.4.5.7.2 LoRaWAN™ technology

The LoRa Alliance specifies the LoRaWAN™ protocol (above the PHY layer) as well as the overall network architecture for deployments in regional, national, or global scenarios. LoRaWAN™ defines classes of end-point devices to address the different requirement of the applications using this technology:

- CLASS A: very suitable for lowest powered devices with no latency constraint; the most energy efficient communication class which must be supported by all devices;
- CLASS B: suitable for battery operated devices; energy efficient communication class for latency controlled downlink;
- CLASS C: powered devices which can afford to listen continuously; no latency for downlink communication.

Figure 45 depicts the LoRaWAN™ stack.

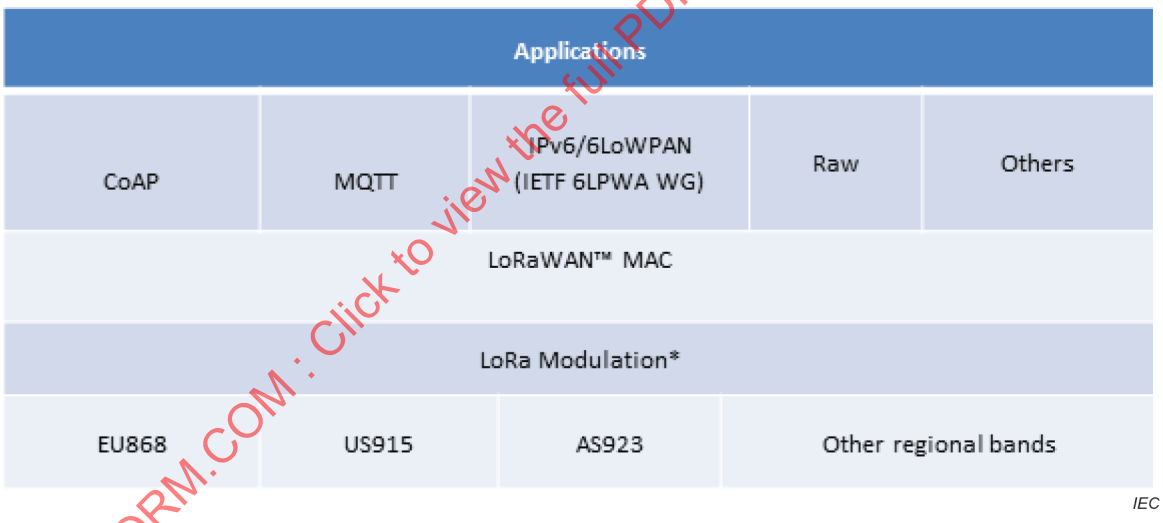


Figure 45 – LoRaWAN™ Protocol Stack

LoRaWAN™ operates in the ISM Band – 433/780/868/915 MHz, reaches up to 15km in rural and 3km in urban areas with an adaptive data rate (250 bit/s to 5,5 kbit/s – 50 kbit/s [FSK in EMEA]). Payload is adaptive, up to 250 octets.

A LoRaWAN™ architecture is typically built based on a stars-of-stars topology. A gateway is used to bridge networks and forward the messages from the end devices upstream (in a backhaul mode) to a central network server which might be connected to application servers in the data centre running the applications (e.g.: parking or meter data management). The network server performs critical operations such as MAC de-capsulation, security management, network

[4] LoRaWAN is the trademark of a product supplied by LoRa Alliance. This information is given for the convenience of users of this document and does not constitute an endorsement by the IEC of the product named. Equivalent products may be used if they can be shown to lead to the same results.

and radio management as well as message scheduling. The communication links between the gateways and the central network server are standard IP-based connections over a variety of media (3G, Wi-Fi, and Ethernet). For this backhaul connection, network security can be applied by using typical protection mechanisms such as IPSec. Geo-localization is available with the LoRaWAN® technology.

7.4.5.7.3 Sigfox technology

Sigfox™ [5] is a proprietary ultra-narrow band (UNB) technology and service provided by a French company of the same name with the following characteristics, among others:

- spectrum: ISM Band – 868 MHz/915 MHz;
- coverage: up to 50 km in rural and 10 km in urban;
- payload: fixed, 12 octets in uplink, 8 octets in downlink direction;
- limited number of messages per day (depending on contract);
- unconfirmed message sending (each radio message simply sent three times);
- security: authentication, integrity protection and payload encryption (latter optional);
- geolocation, private network service.

The Sigfox company cooperates with various chip and radio module manufactures and network service providers. The Sigfox network is available in many countries around the world. It appears as single, cross-country network. This is in contrast to LoRaWAN® and mobile LPWAN networks, which are operated by various service providers independently and require roaming capabilities.

7.4.5.7.4 Cellular-network based LPWAN technologies

Cellular based technologies for machine-to-machine (M2M) communication as typically defined in 3GPP provide various options to meet the LPWAN requirements. This comprises:

- LTE-MTC (machine type communication);
- NB-IOT;
- EC (extended coverage)-GSM-IOT;
- LTE CAT (Category)-M;
- weightless.

LTE CAT-M and NB-IOT are part of the LTE evolution to 5G. Together with EC-GSM-IOT, these cellular-based solutions could be operated as one network. NB-IOT is a pre-5G technology and will be implemented and deployed in existing 3GPP networks with the following characteristics:

- spectrum: LTE Band 1, 3, 5, 8, 12, 13, 17, 19, 20, 26, 28;
- bandwidth: 200kHz;
- each NB-IOT carrier can support 200K subscribers per base station (estimates);
- coverage: up to 35km;
- data Rate: up to 170 kbit/s.

5 Sigfox is an example of a suitable product available commercially. This information is given for the convenience of users of this document and does not constitute an endorsement by the IEC of the product named. Equivalent products may be used if they can be shown to lead to the same results

The protocol is based on OFDM technology and is specified in 3GPP Release 13. NB-IOT can be operated along with wideband LTE carriers using OFDM secured orthogonality and common resource utilization. The selection of a technology to deploy and operate a low-power wide-area network depends on requirements, availability of the technology, operational aspects etc. Table 40 provides an overview on current capabilities.

Table 40 – LPWAN technology capabilities

	LoRaWAN™	Sigfox™	LTE-M	NB-IOT
SDO / Alliance	LoRa Alliance	-	3GPP	3GPP
Band	433/780/868/915 MHz ISM	868/915 MHz	Cellular Bands	Cellular Bands
Total Band	3-26 MHz	2-26 MHz	500 MHz+	600MHz+
Radio range	10-20 km (rural) 3-8 km (urban)	30-50 km (rural) 3-10 km (urban)	2-5km (urban)	10-20 km (rural) 1-5 km (urban)
Packet Size	Flexible	12/8 octets (up/down-link)	Up to 1kB	Flexible
Topology	Star	Star	Star	Star
Roaming	Yes	N/A	Yes	Yes
SLA	Yes	Yes	Yes	Yes
Billing (native)	No	No	Yes	Yes

7.4.5.8 Wi-SUN Alliance and technology

The Wi-SUN Alliance is working to produce several standards based profiles for smart utility, IOT and smart city network applications running IP over IEEE 802.15.4e/g and IEEE 1901.2 NB-PLC networks. Interoperability and compliance certification programs for these profiles are also being developed. Currently, the main application profile under development is the one for field area networks (FAN). Field area networks provide wireless networking solution for a wide range of applications such as advanced metering infrastructure (AMI), distribution automation, connectivity for distributed energy resources, and infrastructure management. The Wi-SUN Alliance FAN solution utilizes IEEE 802.15.4g, a global wireless communications standard, IETF IPv6 protocols including UDP/TCP, 6LoWPAN adaptation + header compression, routing using RPL and IEEE 802.1x enterprise level security, to enable robust, high performance, low power, and long-range networks. Wi-SUN FAN defines the technical profile of a standards based, multi-service and secure field area network. The effort specifies the test and certification processes which enable interoperable implementations from multiple vendors.

The current Wi-SUN FAN stack definitions comprise the following building blocks, key features, and underlying protocols based upon various international standards from IETF, IEEE and ANSI/TIA supporting low power and lossy networks:

IPv6 protocol suite:

- (TCP)/UDP;
- 6LoWPAN Adaptation including header compression;
- DHCPv6 for IP address management;
- routing using RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks); RPL is independent from the data links but its metrics may be leveraging link layers information;
- ICMPv6;
- unicast and multicast forwarding.

Security as essential component comprises:

- 802.1X/EAP-TLS/PKI-based authentication;
- 802.11i group key management;
- optional ETSI-TS-102-887-2 node 2 node key management.

MAC based on IEEE 802.15.4e + information elements (IE) extensions:

- frequency hopping;
- discovery / join;
- protocol dispatch (IEEE 802.15.9);
- several frame exchange patterns;
- optional mesh-under routing;
- PHY based on 802.15.4g;
- various data rates and regions supported.

The FAN specification provides an application independent IPv6-based transport service for connectionless (UDP) and connection-oriented (TCP) services. On top of this architecture, the stack supports a variety of IP-based application and automation & control protocols such as DLMS/COSEM, ANSI C12.22, DNP3, IEC 60870-5-104, ModBus TCP, and CoAP based management protocols. From the architectural perspective, a Layer 3 routed FAN using RPL contains one or more personal area networks (PAN). Within PAN architecture, network nodes can fulfil one of three operational roles – each PAN contains a border router providing WAN connectivity to the PAN. (I) The border router maintains source routing tables for all nodes within its PAN, makes node authentication and key management services available, and provides PAN wide information (e.g. broadcast schedules). (II) Router nodes, which provide upward and downward packet forwarding within a PAN as well services for relaying security and address management protocols. (III) Leaf nodes with basic functions such as discovering and joining a PAN and sending/receiving IPv6 packets. The WAN north-bound connectivity provides all the services that are located in higher layers of the system architecture: security management, back end- , head end- and control centre services.

7.4.5.9 Technologies usable for smart metering

Table 41 shows wireless technologies used for customer-side communications in Japan.

Table 41 – Wireless technologies used for customer-side communications in Japan

Radio band	429 MHz	920 MHz	950 MHz	2.4 GHz	
System	Specified low power radio	Active low power radio	Active low power radio	ZigBee	WLAN (IEEE 802.11b)
Modulation method (primary/secondary)	FSK	MR-FSK	GFSK	O-QPSK/DSSS	BPSK, QPSK/ DSSS
Output power	<10 mW	<20 mW	<10 mW	<10 mW/MHz	<10 mW/MHz
Number of channels	40	38 (<20mW) 77(<1mW)	17 (<10mW) 33 (<1mW)	16	14
Channel space	12,5 kHz	200 kHz	200 kHz	5 MHz	5 MHz
Max. speed	2,4 kbit/s	400 kbit/s	250 kbit/s	250 kbit/s	11 Mbit/s

Radio band	429 MHz	920 MHz	950 MHz	2.4 GHz	
Int'l standard	–	IEEE 802.15.4g	IEEE 802.15.4d	IEEE 802.15.4	IEEE 802.11b
Multi-hop routing protocol	Vendor proprietary	Proprietary or SUN	Vendor proprietary	Standard (AODV)	Standard (HWMP by IEEE 802.11s)
Routing metric	Vendor proprietary	Vendor proprietary	Vendor proprietary	Received power, PER	Airtime link metric (IEEE 802.11s)

Wireless M-Bus or Wireless Meter-Bus (EN 13757-4) is the wireless variant of M-Bus or Meter-Bus (EN 13757). It is widely used in Europe for smart metering or Advanced Metering Infrastructure (AMI) applications. It is specified for the 169 MHz, 434 MHz and 868 MHz frequency bands which are licence-free in Europe and provide higher range and better penetration in buildings than the license free 2,4 GHz band, used e.g. for ZigBee. There are different forms of modulation and data rates. Modulation types include Manchester, non-return to zero (NRZ) and 3-out-of-6 encoding. Wireless M-Bus deploys a star network topology and a thin protocol stack (without IP). Wireless M-Bus is targeted to low-cost solutions.

7.4.6 Fibre optics

7.4.6.1 General

Optical fibres 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 operational communication. Since optical fibres 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 Manual 2009, *Optical fibers, cables and systems* [10] provides a comprehensive overview.

7.4.6.2 Fibre types

Fibres used within substations are usually multi-mode fibres (50/125 µm) operated at 1 300 nm wavelength (near infrared) and limited to distances of a few kilometres without repeaters.

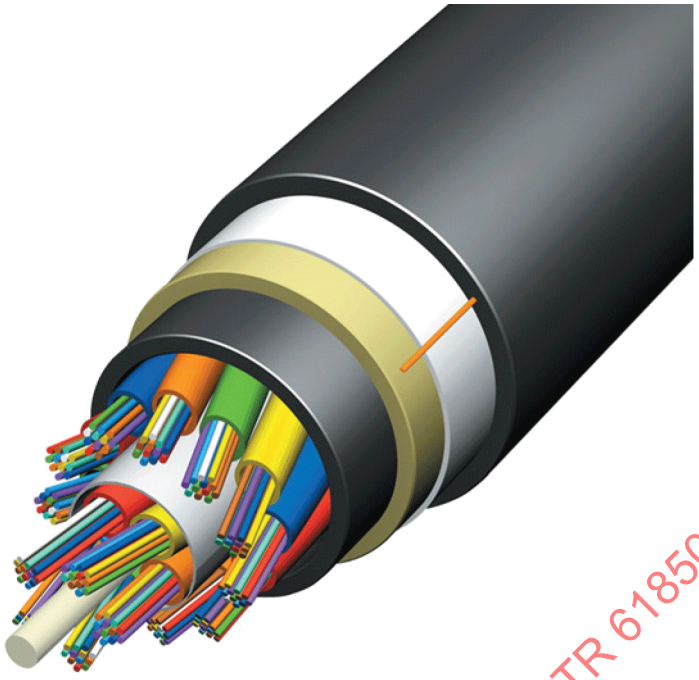
Fibres used in WANs are usually single mode fibres (9/125 µm) operated at 1 310 nm or 1 550 nm which present an attenuation of 0,3 dB/km plus 0,1 dB per splice and some 0,75 dB per connector. Single-mode fibres allow spanning more than 100 km without repeaters.

Fibres 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 fibres.

NOTE IEEE C37.94 standardizes a fibre optical interface between teleprotection and multiplexer equipment for 50 µm and 62,5 µm multi-mode optical fibres 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 Fibre in separate cable

All dielectric self-supporting (ADSS) optical cables are attached to high-voltage towers or poles (Figure 46). 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 fibres are therefore not shielded from the magnetic field of the line and this affects the optical characteristics and the dielectric of the fibre when the voltage exceeds 150 kV. ADSS cables are often used in 132 kV lines.



Source: AFL, USA

IEC

Figure 46 – ADSS fibre cable

Figure 47 shows a HV line with the retrofitted ADSS fibre 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 47 – ADSS installation with splicing box

7.4.6.4 Fibre in ground cable

Fibres are often and preferably embedded in the earthing cable of high-voltage power lines, called overhead power ground wire (OPGW), see Figure 48. As a result, the network topology closely follows the high voltage lines topology, with the data communication equipment located in the substations.

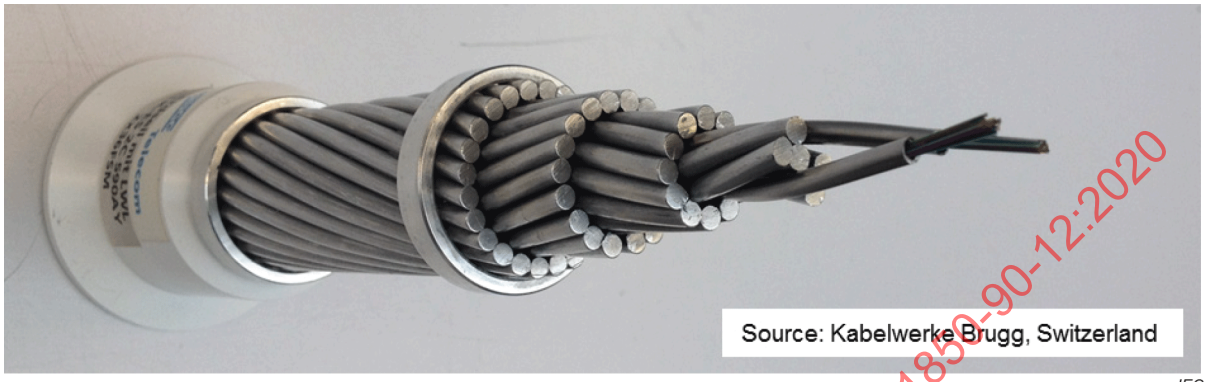


Figure 48 – OPGW in ground cable

The earthing cable contains one or more "C" tubes that each holds a bundle of fibres (Figure 49).

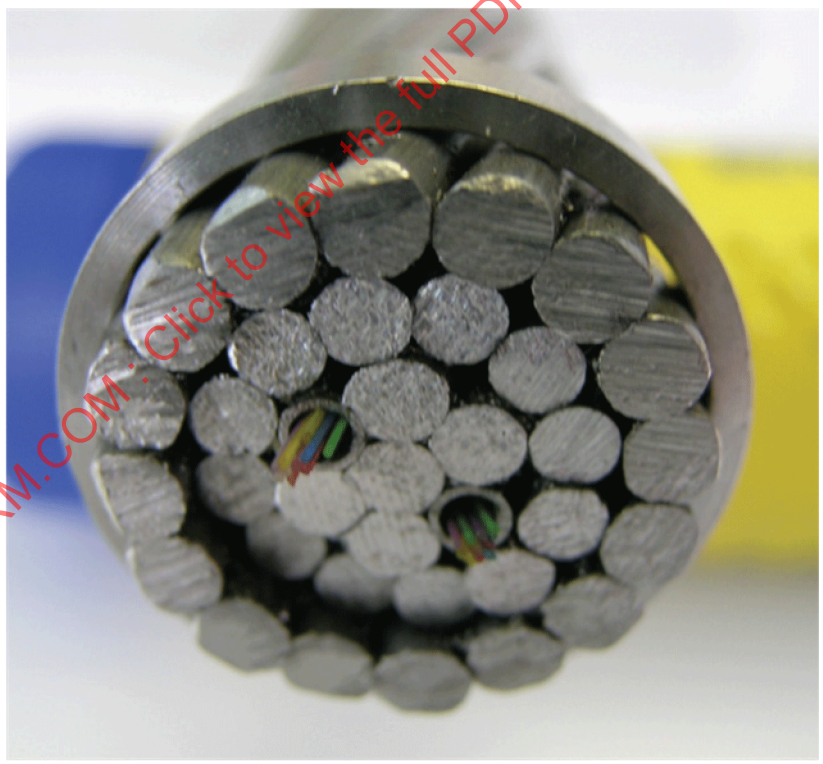


Figure 49 – OPGW with two "C"-tubes each with 32 fibers

NOTE Figure 49 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 fibres, a multitube can accommodate over 200 fibres (Figure 50).

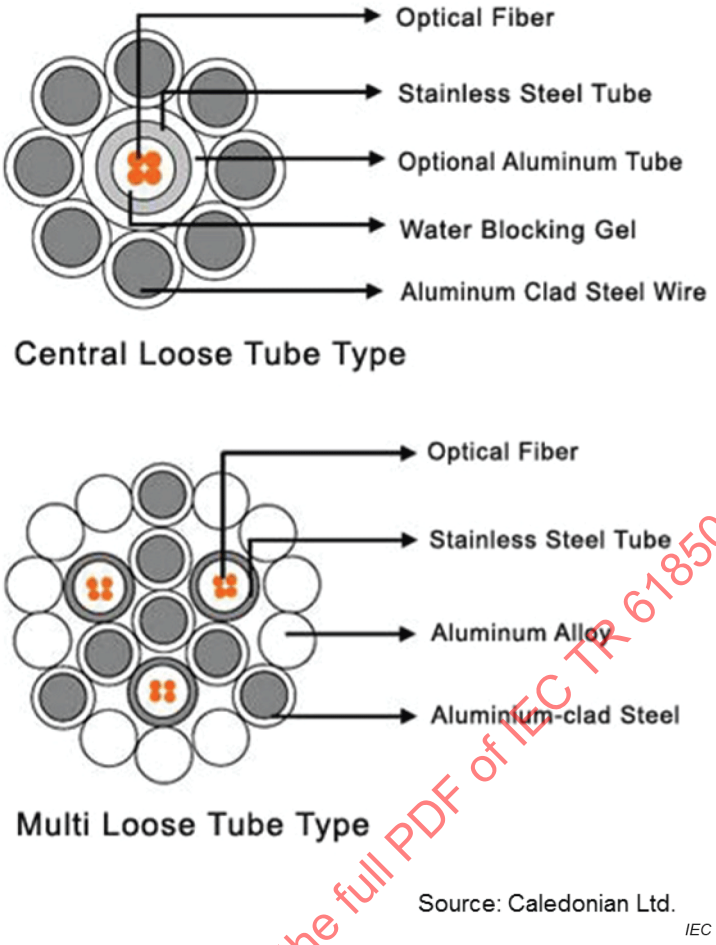


Figure 50 – OPGW fibers

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

7.4.6.5 Fibre splicing

The fibres 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 51), others install it at 3 m to 5 m above ground. Figure 51 shows the splicing cassette box at the right.

Source: LightCom, Switzerland

IEC

Figure 51 – Splicing box

The same kind of box shelters repeaters or communication equipment.

Fibres do not provide 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 fibre can carry multiple optical channels when multiplexed by WDM.

While multimode optical fibres (such as those used within a substation) are restricted to one wavelength only, single mode fibres allow sending simultaneously several optical beams with different wavelength, or "colour", as Figure 52 shows.

NOTE Colours in Figure 52 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).

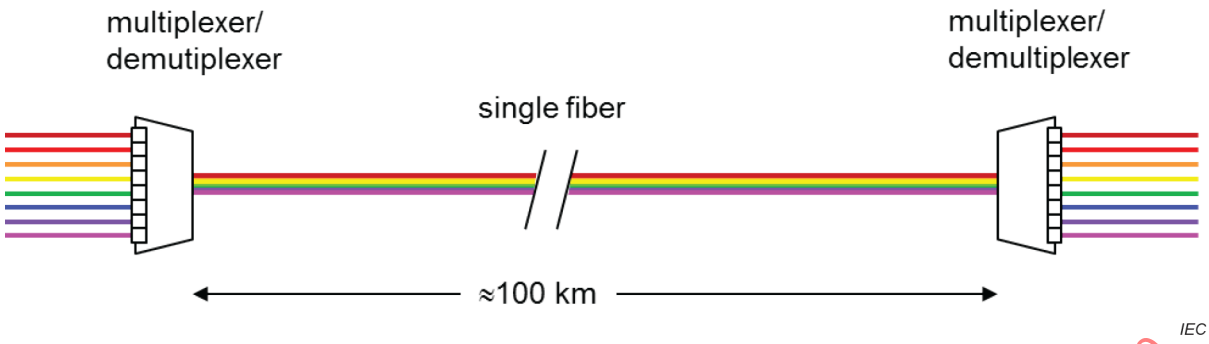


Figure 52 – WDM over one fibre

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

ITU-T standardized two multiplexing methods:

- coarse wavelength division 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 division 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 fibre 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 fibre amplifiers.

7.4.6.7 Optical transport network (OTN) OCh

OTN (ITU-T G.709) (7.6.2.10) specifies an optical channel OCh as a physical layer 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 fibres. It foresees optical regenerators and optical wavelength switching (Figure 53).

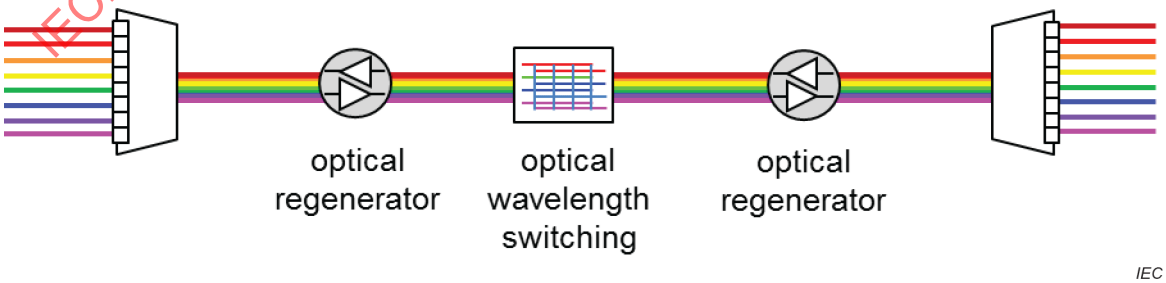


Figure 53 – OCh optical components

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 the splitting of one fibre signal into different fibres 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 was developed for the last mile and residential areas and has little importance in WANs.

7.4.6.9 Fibre reliability and supervision

Fibres present the highest reliability of all communication media.

The weak points are the transmitters.

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

Nevertheless, constant supervision of the fibres is necessary, and tools exist to provide 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 Fibre advantages and disadvantages

Table 42 summarizes optical fibre characteristics.

Table 42 – Optical fibres: 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 fibres and within a fibre	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 fibres	

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 fibres from the bundle and leases the rest. In some cases, utilities outsource the whole fibre communication to a telecom company with a SLA concerning the fibres indispensable for operation.

7.4.7 Layer 1 redundancy

To keep availability high upon failure or disaster, medium redundancy is applied, e.g. parallel fibres 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 neighbouring 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 ineffective. Therefore, non-active links need to be energized and exercised regularly. Better than occasional checking of redundancy is the parallel operation of a redundant medium, where energy consumption and service restriction permit.

The selection of the redundant medium is usually implemented at Layer 2 or Layer 3. Figure 54 illustrates an example of diverse redundancy through microwave towers separated from the OPGW transmission.

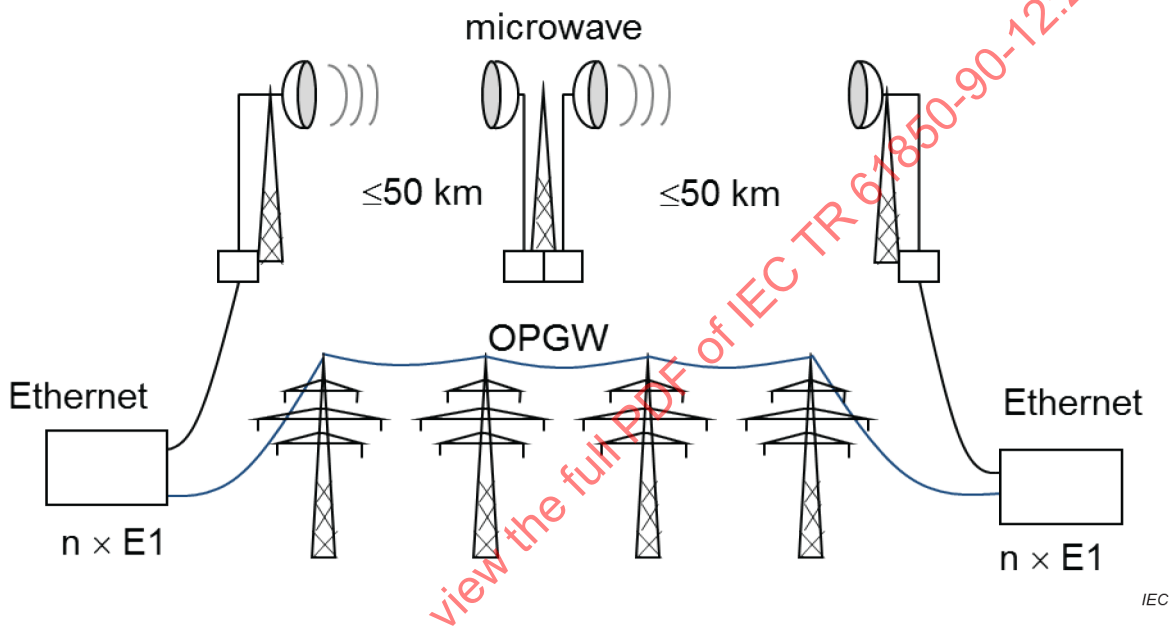


Figure 54 – Optical link with microwave back-up

7.4.8 Application example: 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 appropriate grid operations, provides one of the two circuits composing the teleprotection and SPS (SIPS) systems.

Figure 55 shows one of two high voltage transmission lines that 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 the 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 55 – Photograph of a partially destroyed 735 kV line

7.4.9 Layer 1 security

Layer 1 security mostly relates to physical security attacks such as the physical cutting of communication cables including optical fibres 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 fibre at a splicing box is possible with sophisticated equipment and disrupting the communication is 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. 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 takes place in a 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 techniques still use it (7.4.4.1).
- Wavelength division multiplexing (WDM), in which different light wavelengths are used to send signals in parallel over the same optical fibre. For instance, using CWDM, up to 16 channels can share the same fibre (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 analogue 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" behaviour.

The old modem communication over analogue 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 arrived with the PCM system, which samples the voice at 8 kHz with an 8-bit analogue-to-digital converter after proper shaping. The voice channel DS0 of 8 × 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 × 64 + 8 = 1,544 Mbit/s of raw bandwidth. The payload of 24 × DS0 is called DS1 (ANSI T1.403-1999).

The E1 frame (see Figure 56) 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, signalling and management.

The E3 frame (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.

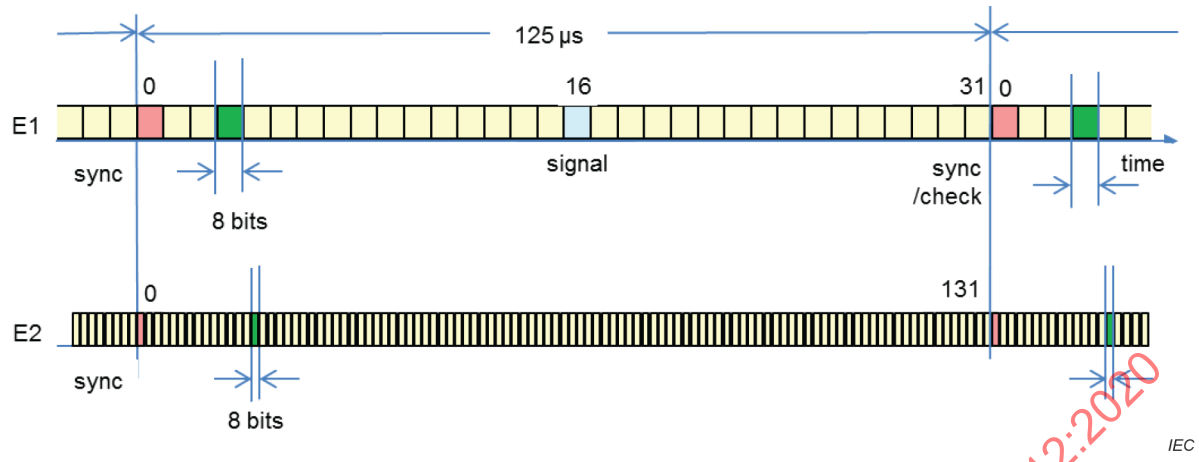


Figure 56 – E1 and E2 channels

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 behaviour through TDM based on basic DS0 circuits that offer each 8 bits at 8 kHz (64 kbit/s), originally intended for voice.

Figure 57 and Figure 58 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.

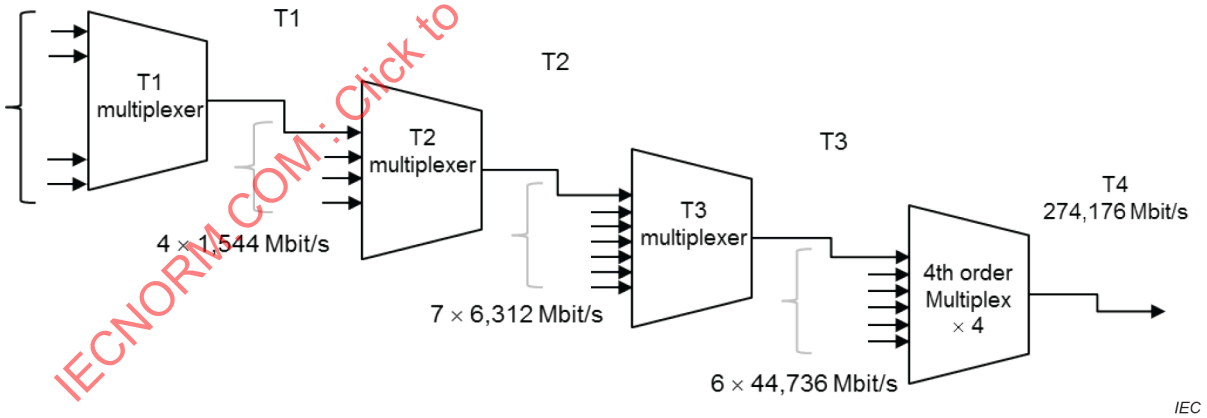


Figure 57 – Digital transmission hierarchy (T-standards)

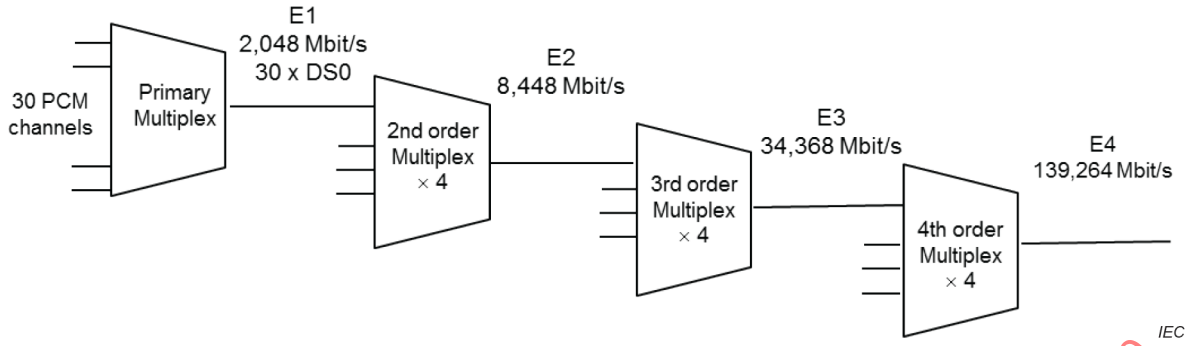


Figure 58 – Digital transmission hierarchy (E-standard)

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

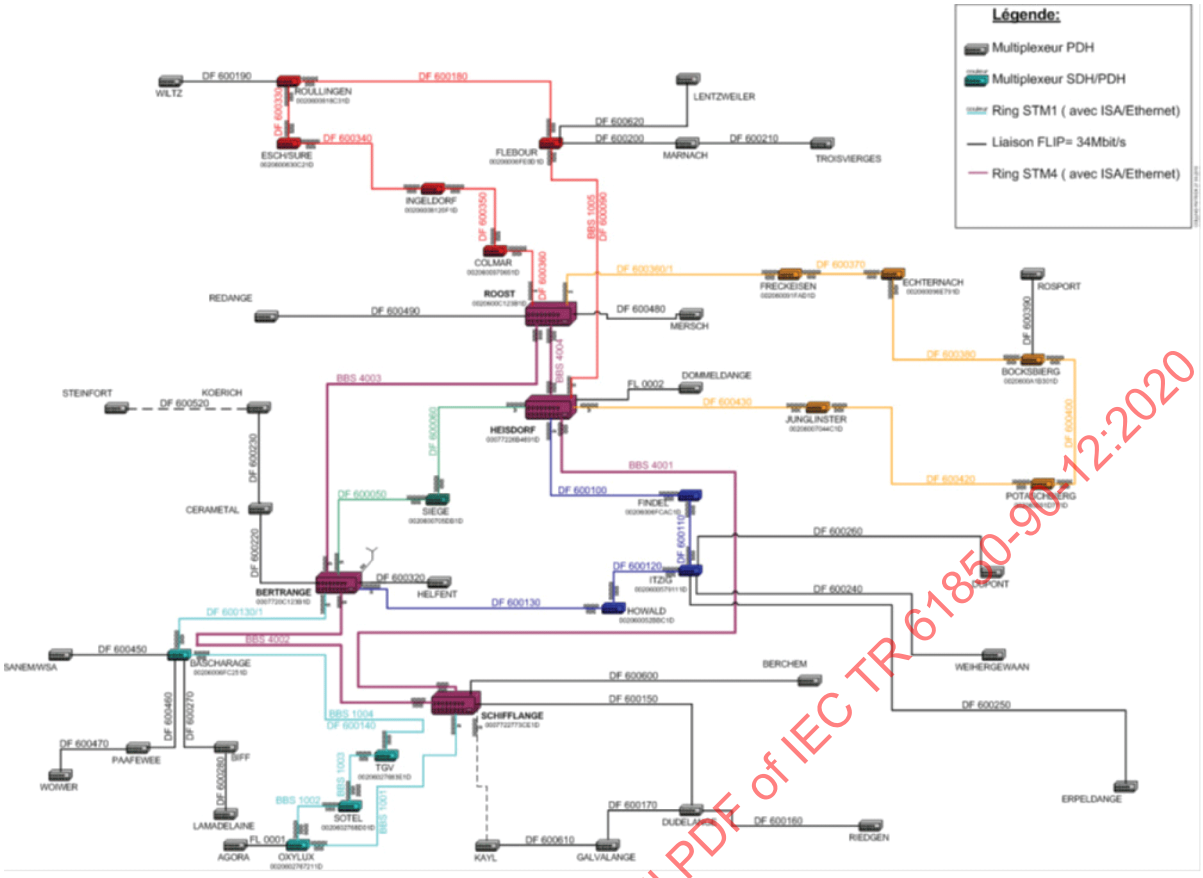


Figure 59 – Example of an SDH network for utilities

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 fibre (very long distances at high data rates possible) or microwave radio (for difficult topological environments, 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 60 shows the SONET digital transmission hierarchy (ITU-T G.803). Figure 61 shows the SDH hierarchy. Synchronous and non-synchronous line rates and the relationships between each appear in Table 43.

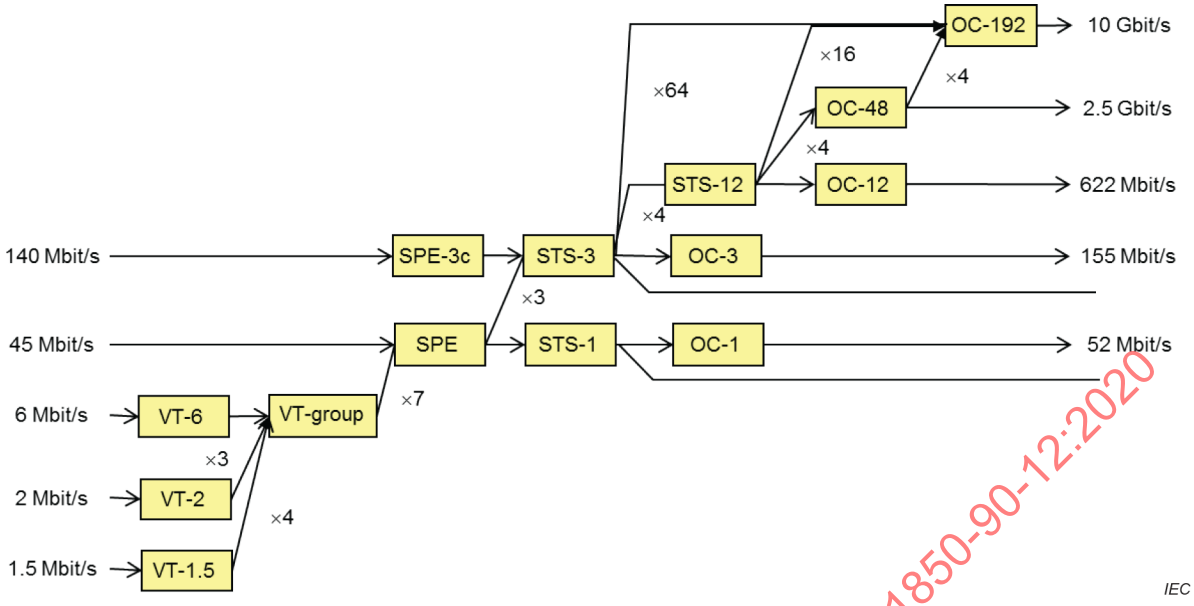


Figure 60– SONET multiplexing hierarchy

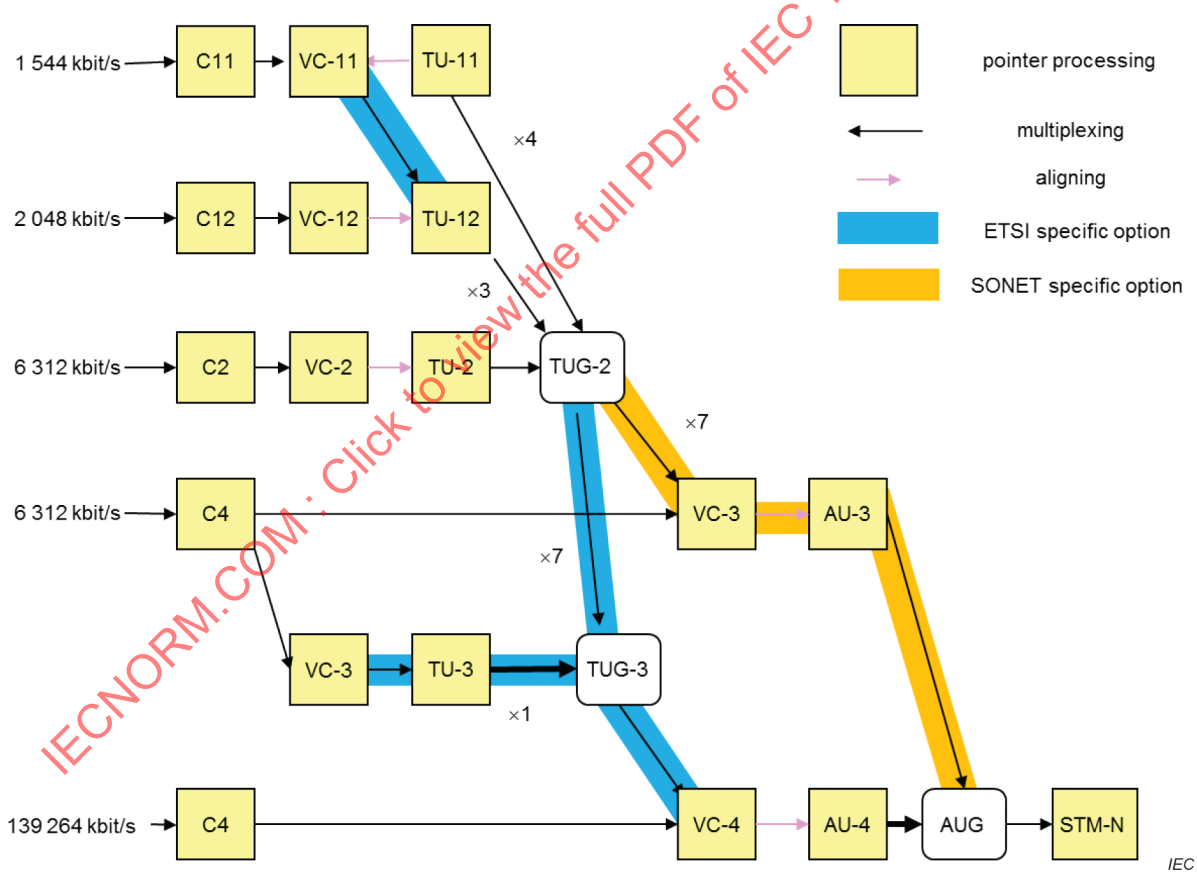


Figure 61 – SDH multiplexing hierarchy

Table 43 – 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 @ 64 kbit/s	
	E-1		2,048			32 × DS0 @ 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. This synchronization allows the networks to operate synchronously, 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. 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:

a) terminal multiplexer (TM), which multiplexes several low-speed channels on a high-speed path;

b) add-drop-multiplexer (ADM), which adds and drops tributaries at intermediate points along a path;

c) 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 62).

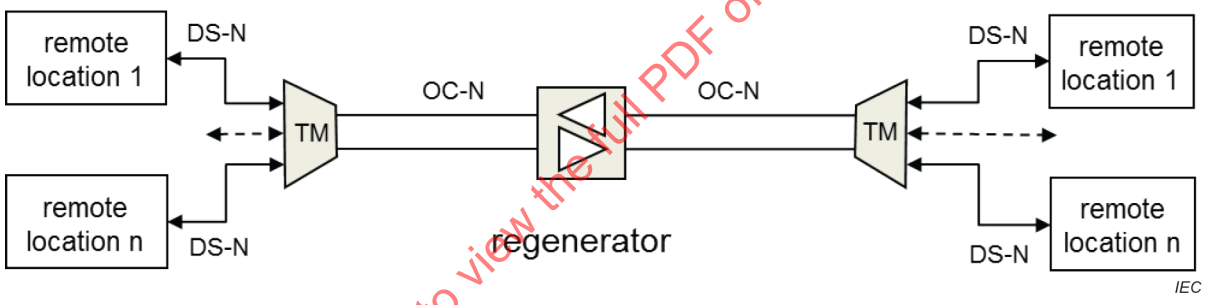


Figure 62 – SDH/SONET with point-to-point topology

7.6.2.5.2 Linear topology

A linear topology (Figure 63) uses ADMs and TMs placed along a SDH/SONET path. Service providers use this topology for medium and long-haul linear SDH/SONET architectures.

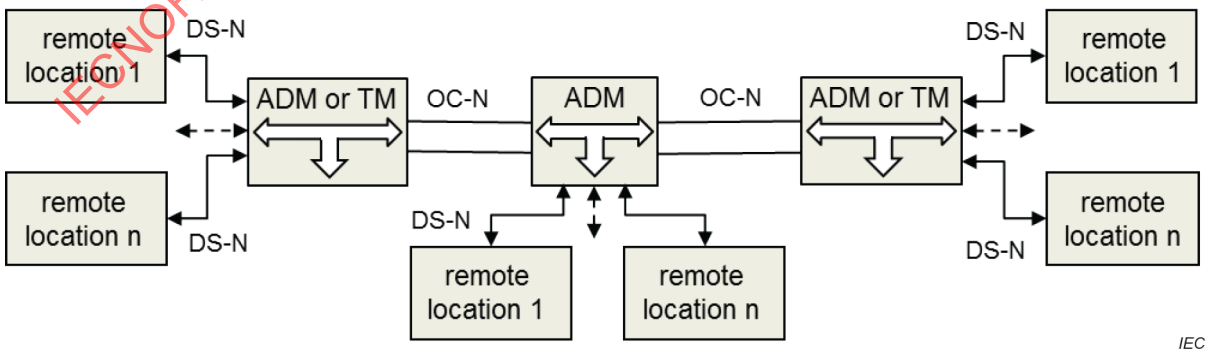


Figure 63 – SDH/SONET with linear topology

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 fibre 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

In the event of a failure SDH/SONET can provide switchover times below 50 ms. Depending on the mechanism used, switching can affect 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 fibre 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 to be bidirectional because both directions of transmission use the same set of nodes.

Redundancy against breaks 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 × VC-4 on STM-4 / 2 × STS-3 on OC-12) is used for working traffic, the other half is reserved for redundant traffic
- 4-fiber: 2 fibres are used for working traffic, another 2 fibres are reserved for redundant traffic (each fibre pair providing full capacity e.g. 4 × VC-4 / 4 × 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 64 shows how BLSR/BSHR works under normal conditions and Figure 65 shows the same under failure conditions.

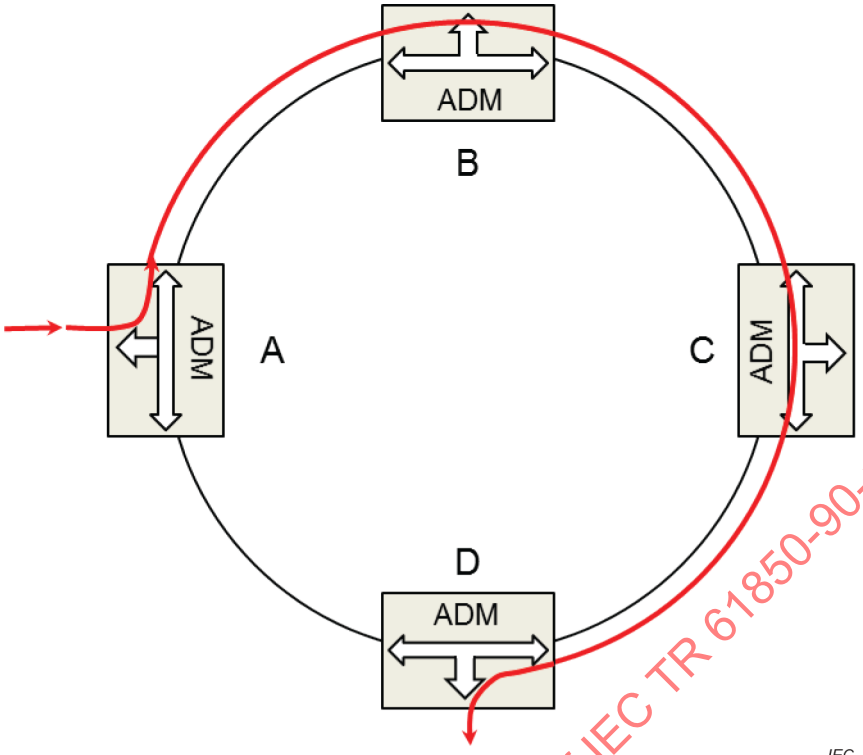


Figure 64 – BLSR/BSHR topology in normal conditions (from A to D)

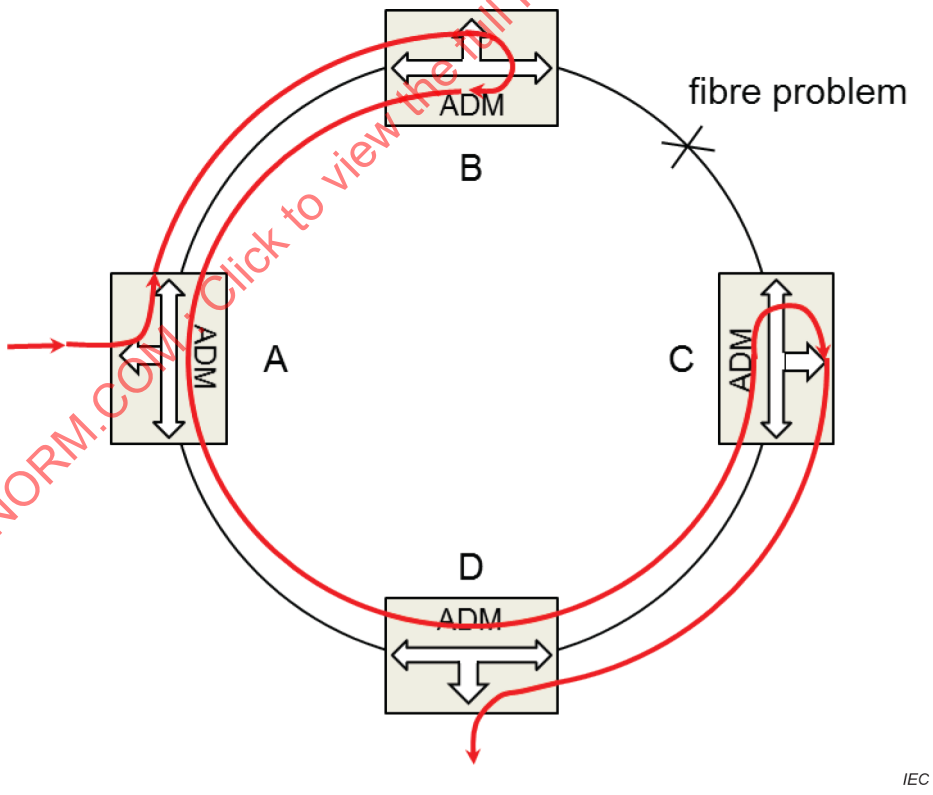


Figure 65 – BLSR/BSHR topology in failure conditions

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 anticlockwise 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 66 shows how SNCP/UPSR work in normal conditions and Figure 67 shows the failure condition.

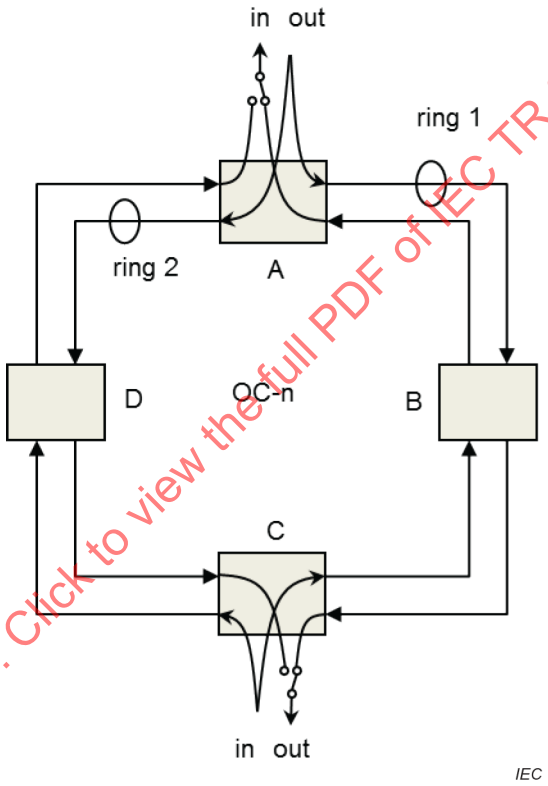


Figure 66 – SNCP/UPSR topology in normal conditions

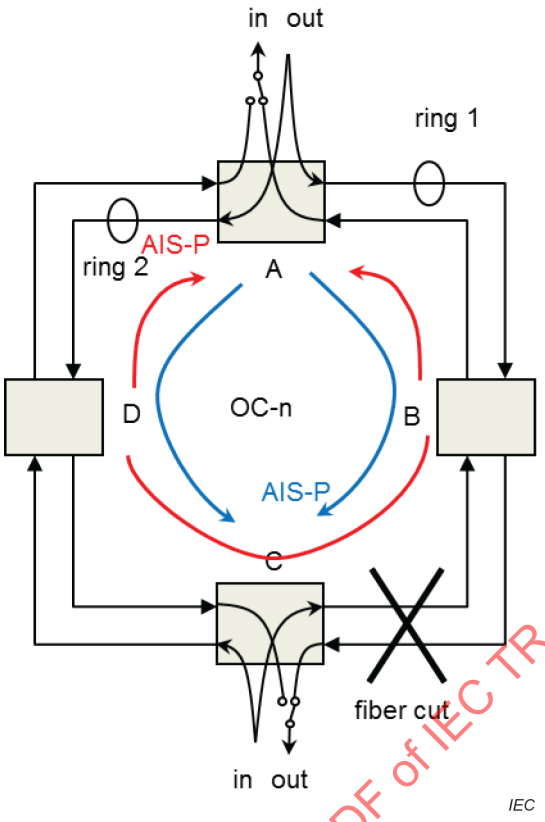


Figure 67 – SNCP/UPSR topology in failure conditions

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 the reliability of a network element, the redundancy methods 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 the grouping of 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 of the 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 elements and networks fulfil the criteria of 6.2.4.3.

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 virtual circuits/virtual tributaries (VCs/VTs) in the line, it is impossible to lock the switching of specific VTs as 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 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 into 2 diverse paths through the network which makes it difficult to interfere.

7.6.2.11 SDH/SONET summary

Table 44 summarizes SDH/SONET.

Table 44 – 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 is inefficient for packet switching due to resource 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 high-end links up to 100 Gbit/s. Figure 68 shows the structure of an OTN interface.

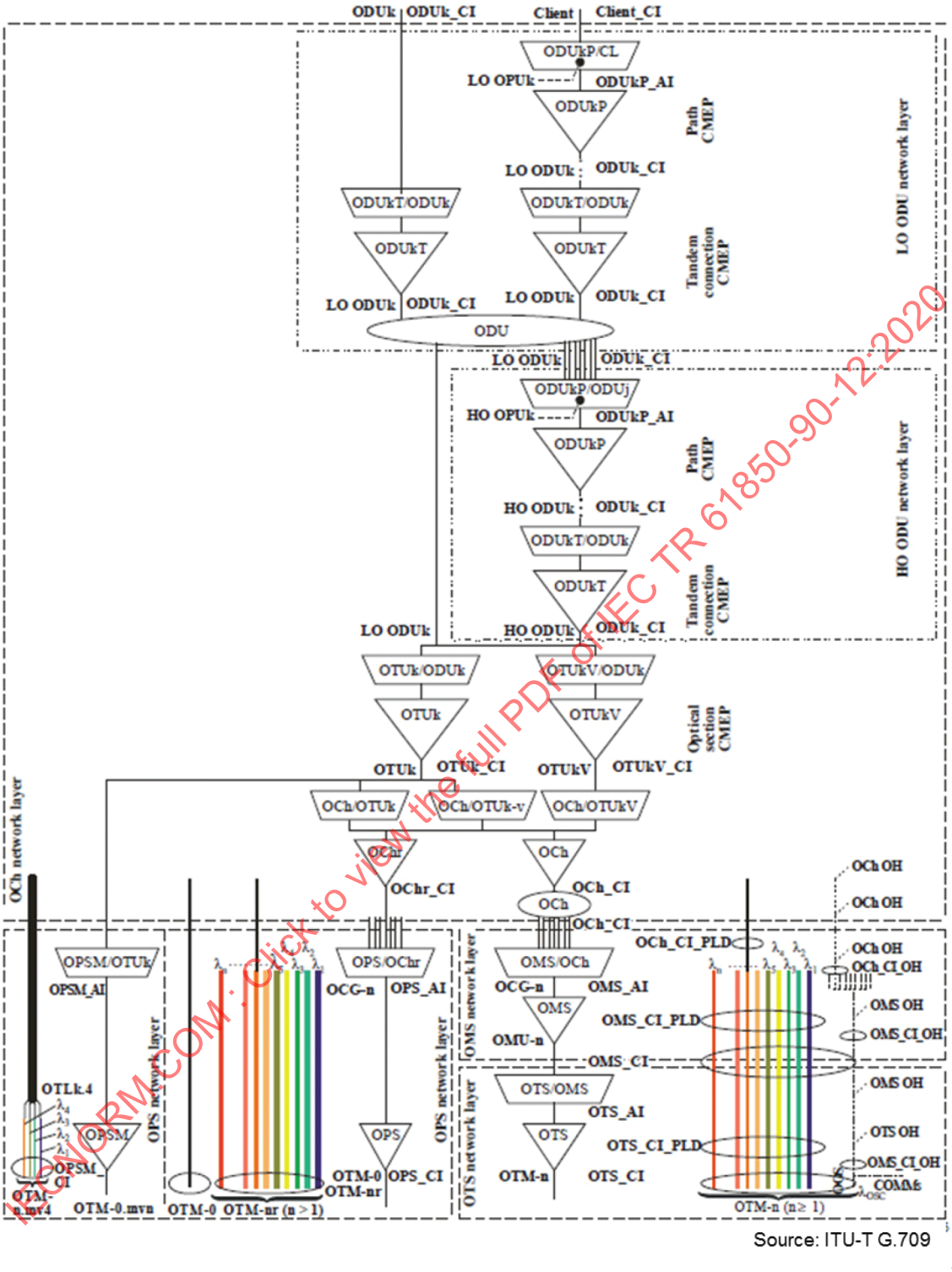


Figure 68 – Example of information flow relationship in OTN

OTNs are becoming increasingly interesting although no deployment in utilities is known.

7.6.4 Ethernet

7.6.4.1 Ethernet technology

Ethernet is originally a Local Area Network technology standardized in 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 fibres that overcame the former limitations. Optical fibres cover distances of several kilometres without repeaters, and hundreds of kilometres with repeaters. The total available bandwidth of an Ethernet network exceeds the bandwidth of a single link.

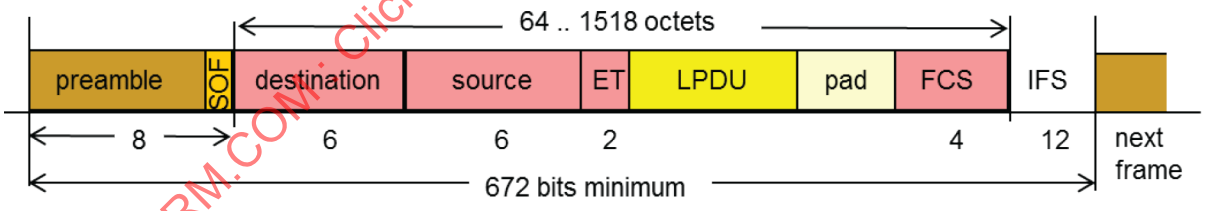
IEEE 802.3 specifies many physical layers; Table 45 lists the most important.

Table 45 – Ethernet physical layers

Standard	Rate (Mbit/s)	Medium	Properties
100Fx	100 Mbit/s	Multimode fibre single mode fibre	Most widely used in substations single mode little used
1000Fx	1 Gbit/s	Multimode fibre single mode fibre	Most widely used in WANs
LX-4	10 Gbit/s	CDWM 4 × 3,125 Gbit/s	WAN technology
SyncE	diverse	Optical fibres	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 69), which is really what makes "Ethernet". This frame format has become the common reference of WANs.



SOF Start of Frame
ET Length/Ethertype
LPDU Link Protocol Data Unit
pad padding bits to achieve minimum frame size
FCS Frame Check Sequence, 32-bit Cyclic Redundancy Check
IFS Interframe spacing

IEC

Figure 69 – 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 address or a logical address.

NOTE IEEE RAS 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 it is called "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 70).

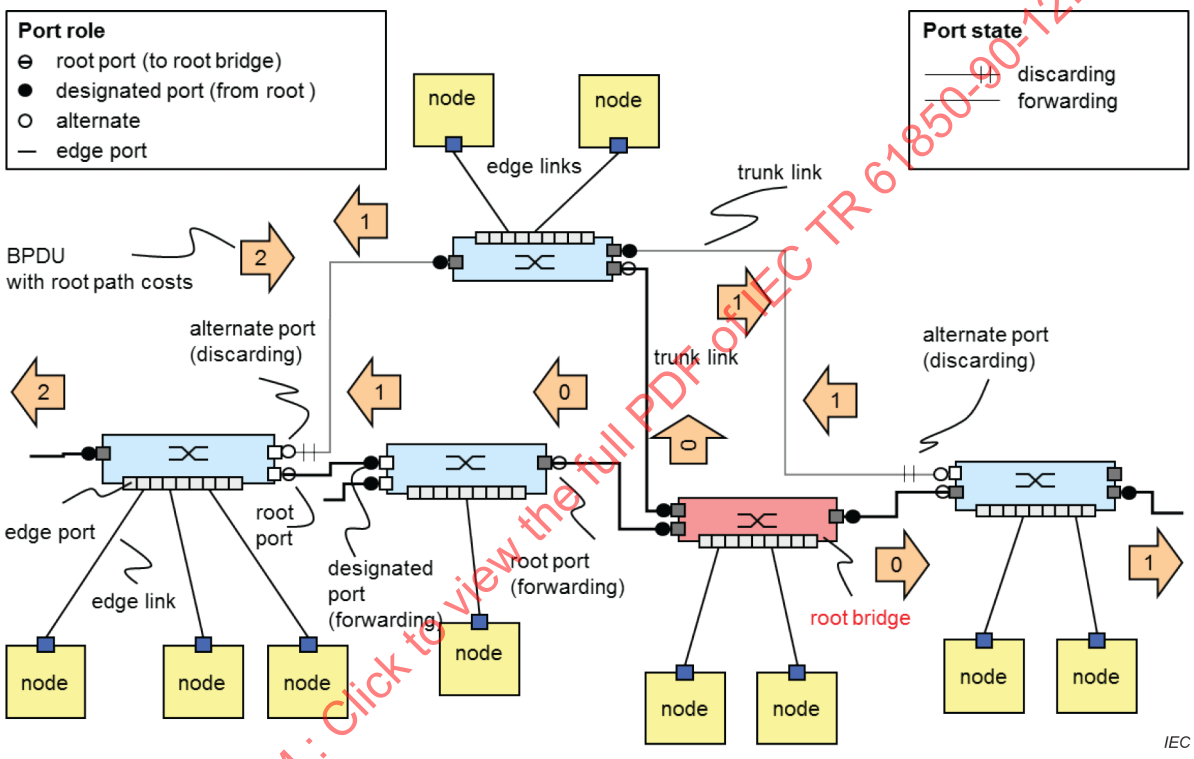


Figure 70 – IEEE 802.3 (Ethernet) topology with RSTP switches

Other technologies such as HSR (IEC 62439-3) and ERPS (G.8032) also prevent loops in meshed Ethernet networks, especially in rings (Figure 75).

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 the 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 71). Figure 71 shows only one 802.1Q tag, but several such tags may be stacked.

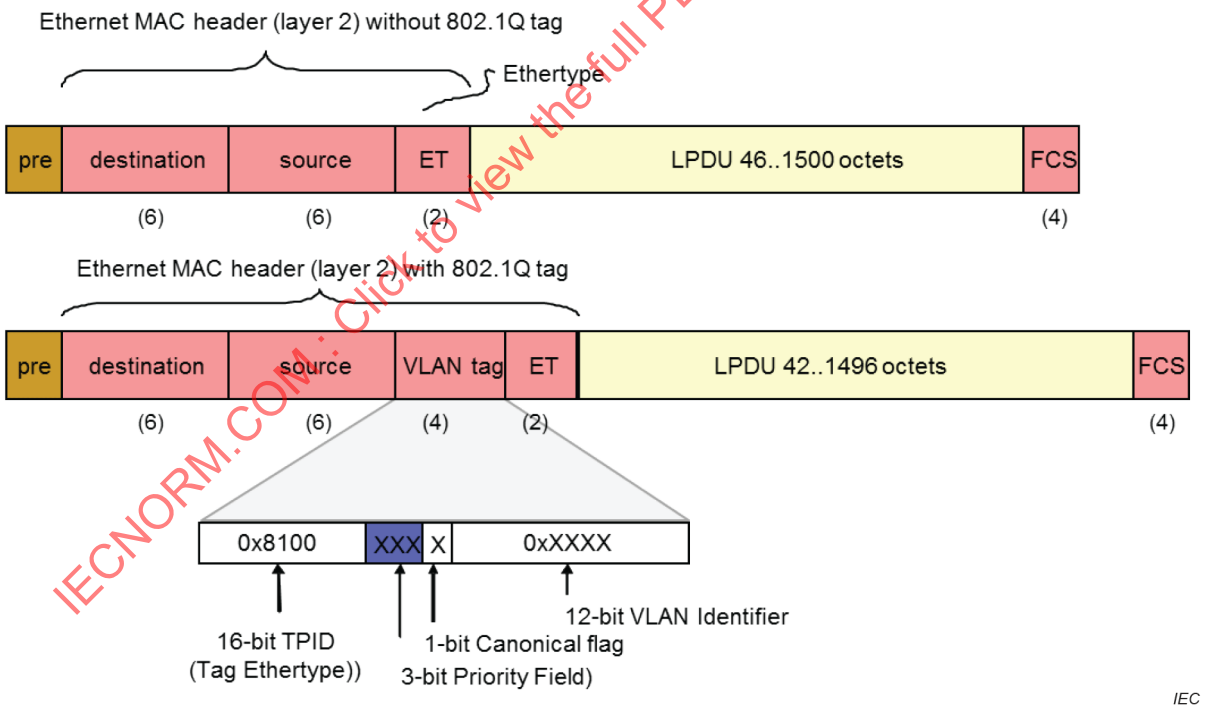


Figure 71 – IEEE 802.1Q-tagged Ethernet frame format

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 fibre or using a WDM channel. The arrangement of Figure 72 is well suited when optical fibres directly connect 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 72).

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 72, 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 Figure 72 shows. 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.

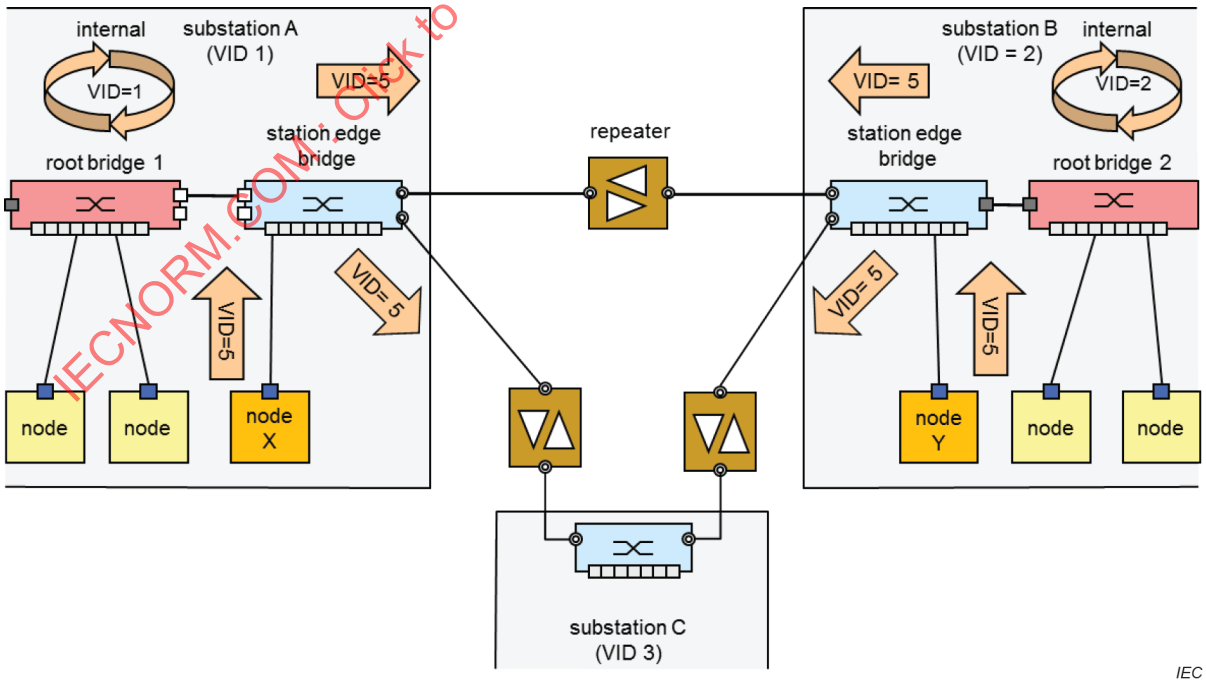


Figure 72 – Direct Ethernet with VLAN in substation-to-substation transmission

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 tunnelling GOOSE and SMV and IEC TR 61850-90-5 recommends for tunnelling 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 73). The situation is similar when the Layer 2 packets are tunnelled over a link that does not preserve the VLAN tags.

In the example of Figure 73, substation A sends the GOOSE messages intended for substation B with VID=12; the tunneller removes the tag; the link between the substations forwards the untagged frames; the tunneller at substation B retags the frames with VID=212. Conversely, substation B sends the GOOSE messages for substation A tagged as 212, the tunneller of substation A retags them to VID 12.

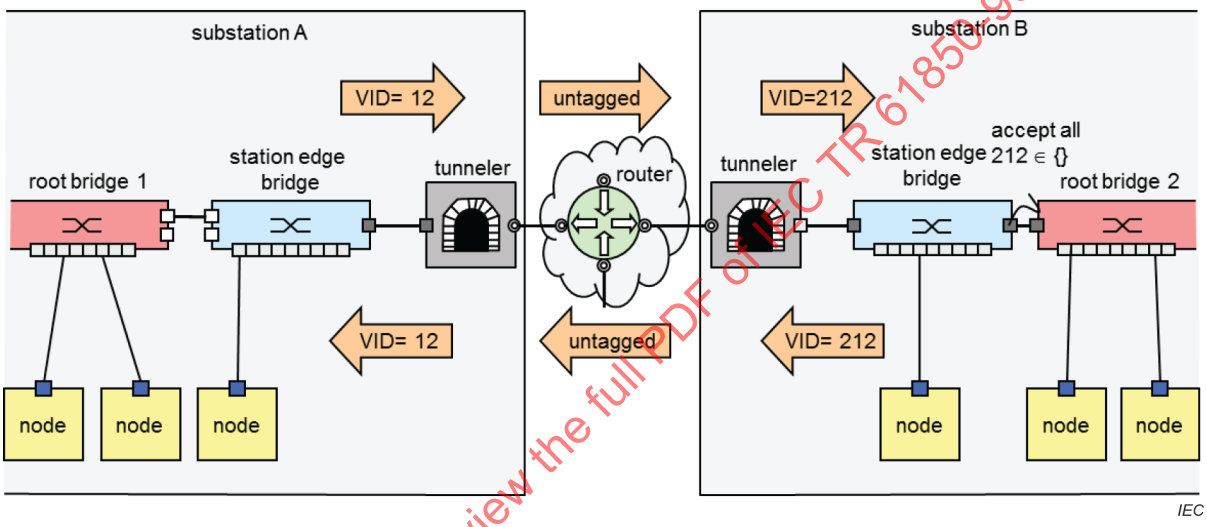


Figure 73 – Substation-to-substation Layer 2 transmission tunnelled over IP

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. Single RSTP domains are also limited in size.

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 62439-3:2015, 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 74).

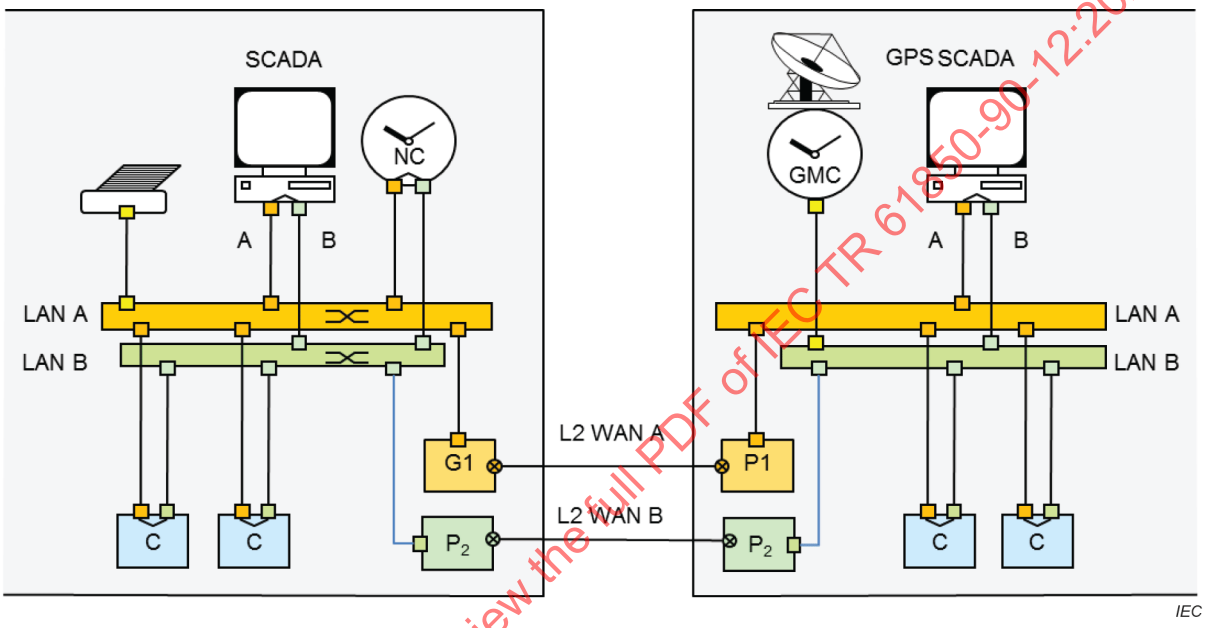


Figure 74 – PRP structure (within and outside a substation)

7.6.4.8.5 HSR

HSR (IEC 62439-3:2015, 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 75).

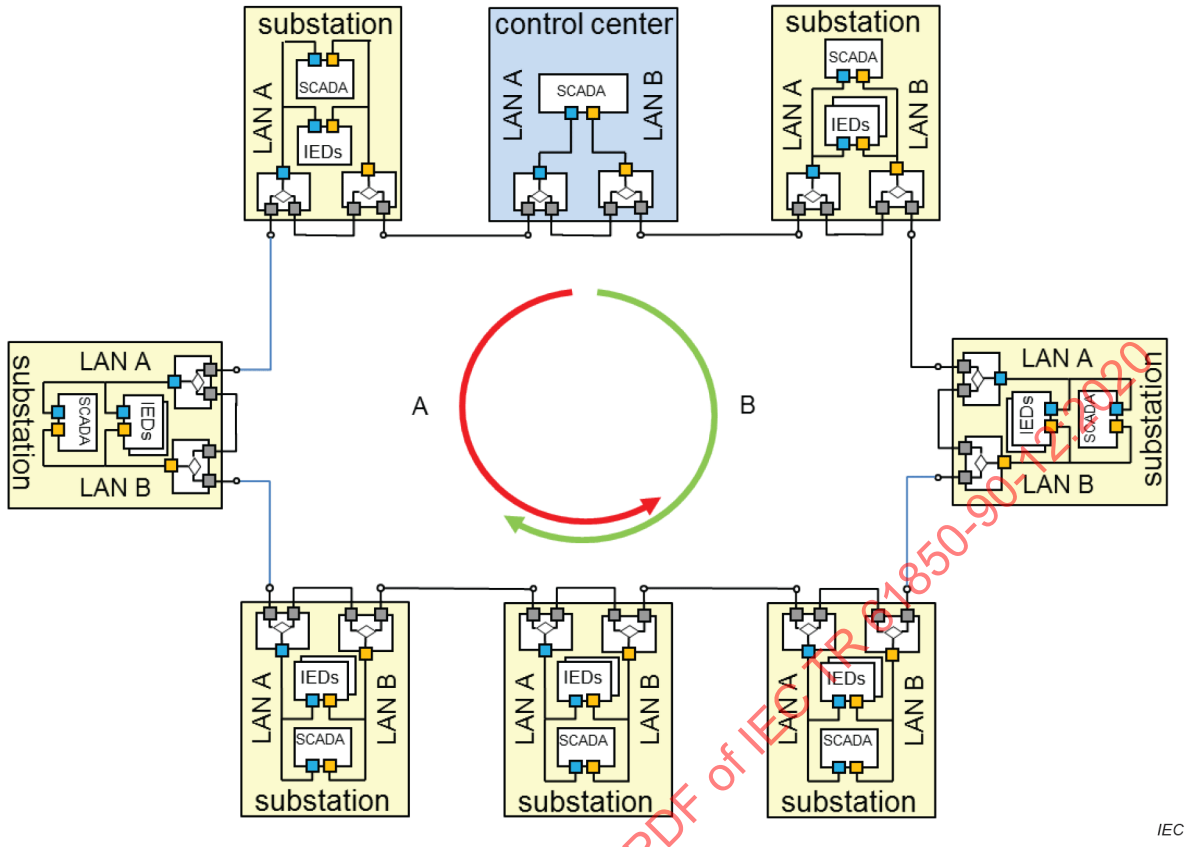


Figure 75 – HSR ring connecting substations and control centre

In HSR; the duplicate discard algorithm considers propagation delays, which amount to 5 µs/km (without repeaters), processing delays (some 5 µs/node) and transmission delays (at 100 Mbit/s, the minimum frame takes 6 µs 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 × (36 × 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 Class of Service 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 behaviour 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 a 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 76):

- Security Tag, which is an extension of the EtherType
- Authentication Code

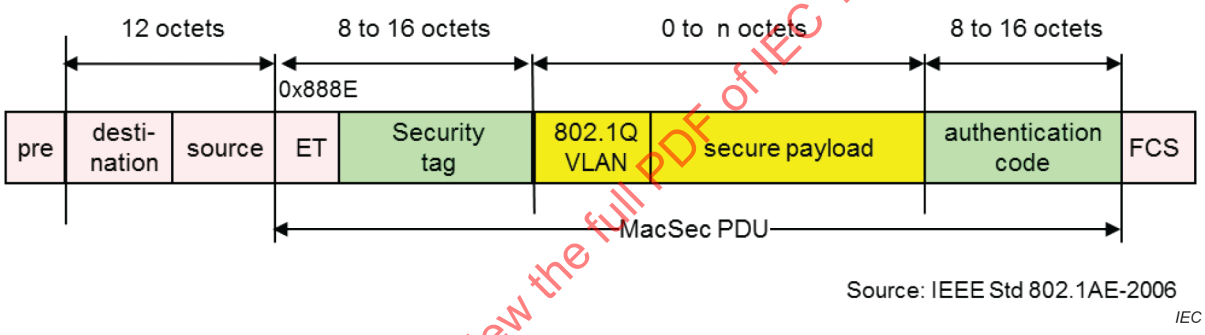


Figure 76 – MACsec frame format

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 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 77 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.

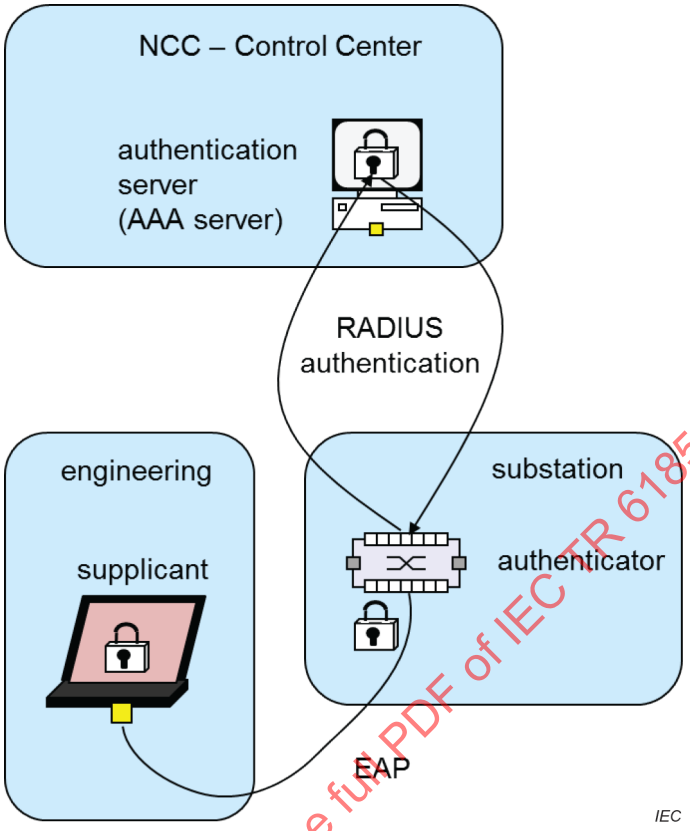


Figure 77 – IEEE 802.1X principle

IEEE 802.1X consist of three actors (Figure 77):

a) Supplicant: software component on the device or client machine used to request network access

b) Authenticator: the network node, typically a switch (e.g. in the substation automation network) which is placed between the supplicant and the authentication server

c) 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 bridges, SNMP can be used with dedicated MIBs, often depending on the manufacturer.

IEC TR 61850-90-4 allows the configuration of bridges and supervision of 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 PTP); 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 78).

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.

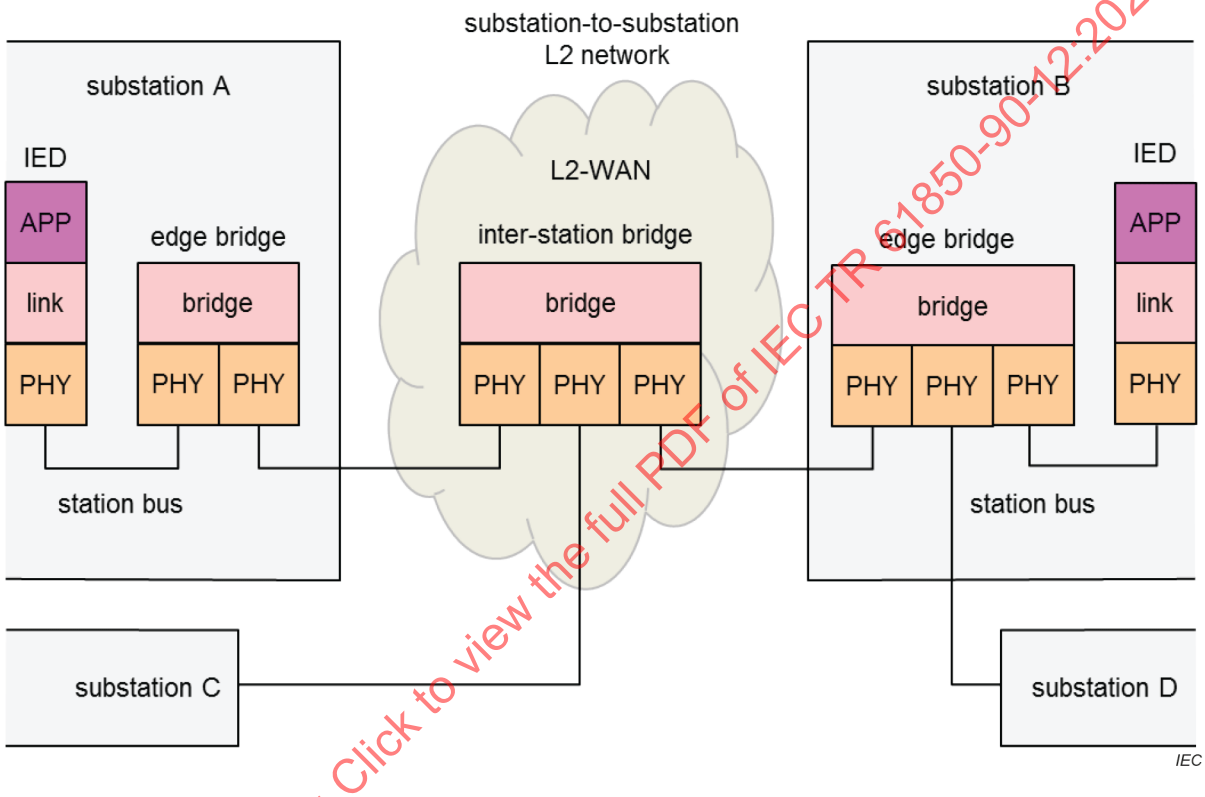


Figure 78 – Ethernet for substation-to-substation communication

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 systems 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 46 shows the differences in mapping Ethernet based payloads in SDH/SONET and the efficiency increase using Next Generation SDH / SONET with VCAT.

Table 46 – 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, fibre 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 79)

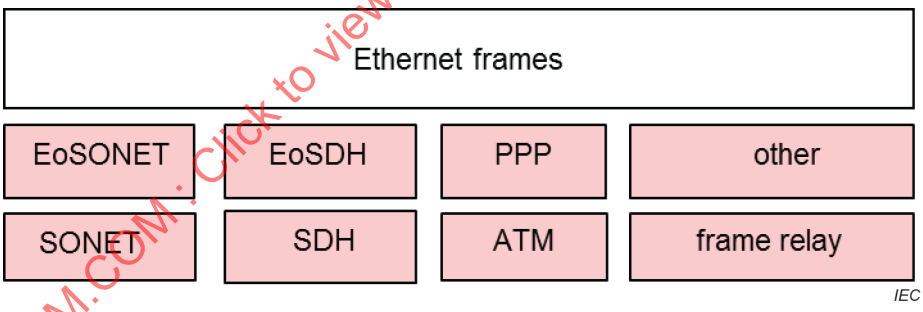


Figure 79 – Packets over TDM

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 to 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 Figure 112;
- E-tree emulates a point to multipoint communication;
- E-LAN emulates a multipoint to multipoint communication (see VPLS in Figure 112).

7.6.6.4 Carrier Ethernet summary

Table 47 summarizes Carrier Ethernet's characteristics.

Table 47 – 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 loops 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 varies
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 predicable 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 favour of MPLS (7.6.9). Since a number of utilities still use PBB, especially in Japan, a brief description follows in the next sub-clause.

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 80 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.

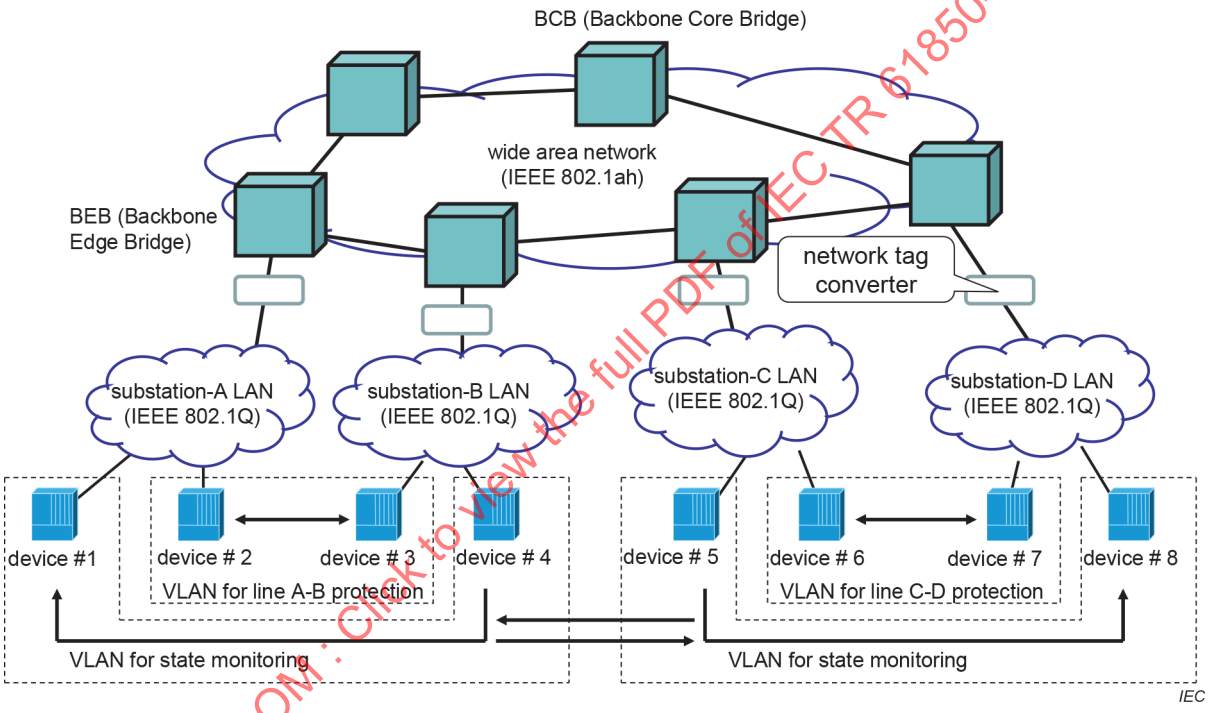


Figure 80 – IEEE 802.1Q/ad/ah network configuration

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.

7.6.9 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 allows multi-service transport over a wide variety of Layer 1 and Layer 2 technologies (fibre, 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 is based on labels inserted between the Layer 2 – and the Layer 3 headers hence the name "Layer 2,5" (see Figure 82 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 81):

- 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 substation edge node (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.

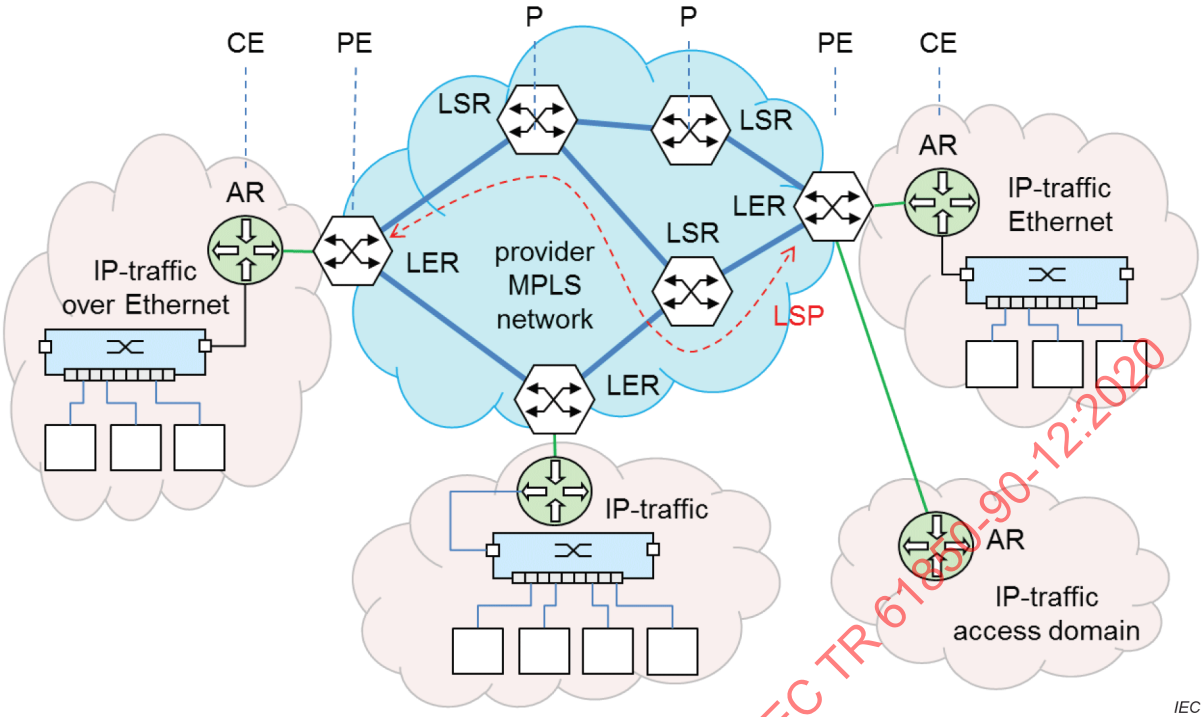


Figure 81 – Basic MPLS architecture

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 82 is based on Ethernet frames in which a label field replaces 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.

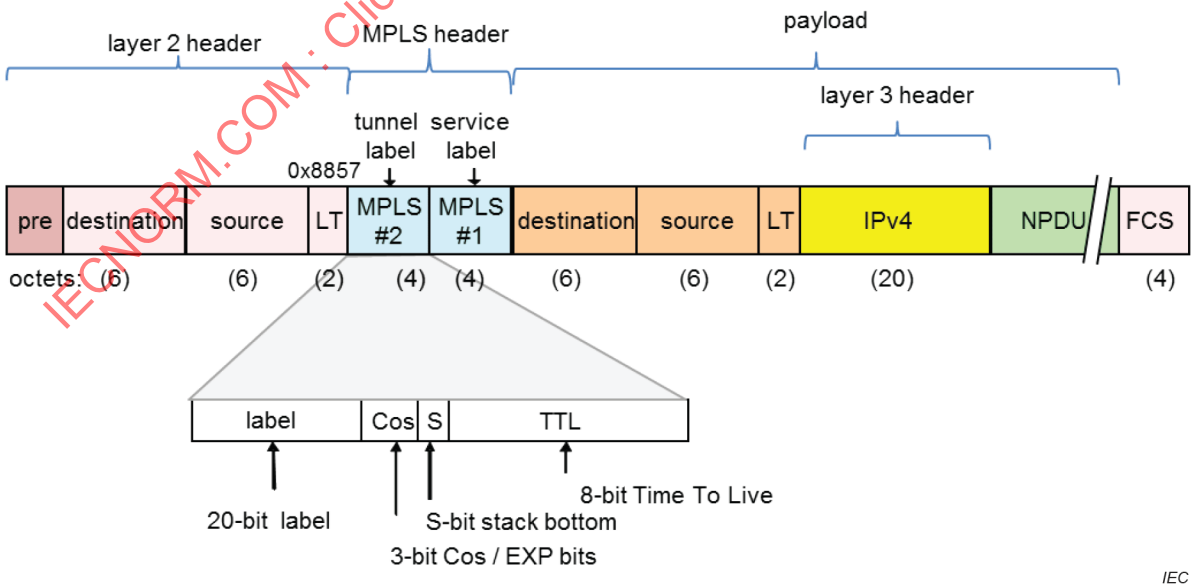


Figure 82 – Example of MPLS frame format with IPv4 payload

7.6.9.4 MPLS Services

MPLS networks support 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 83 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.

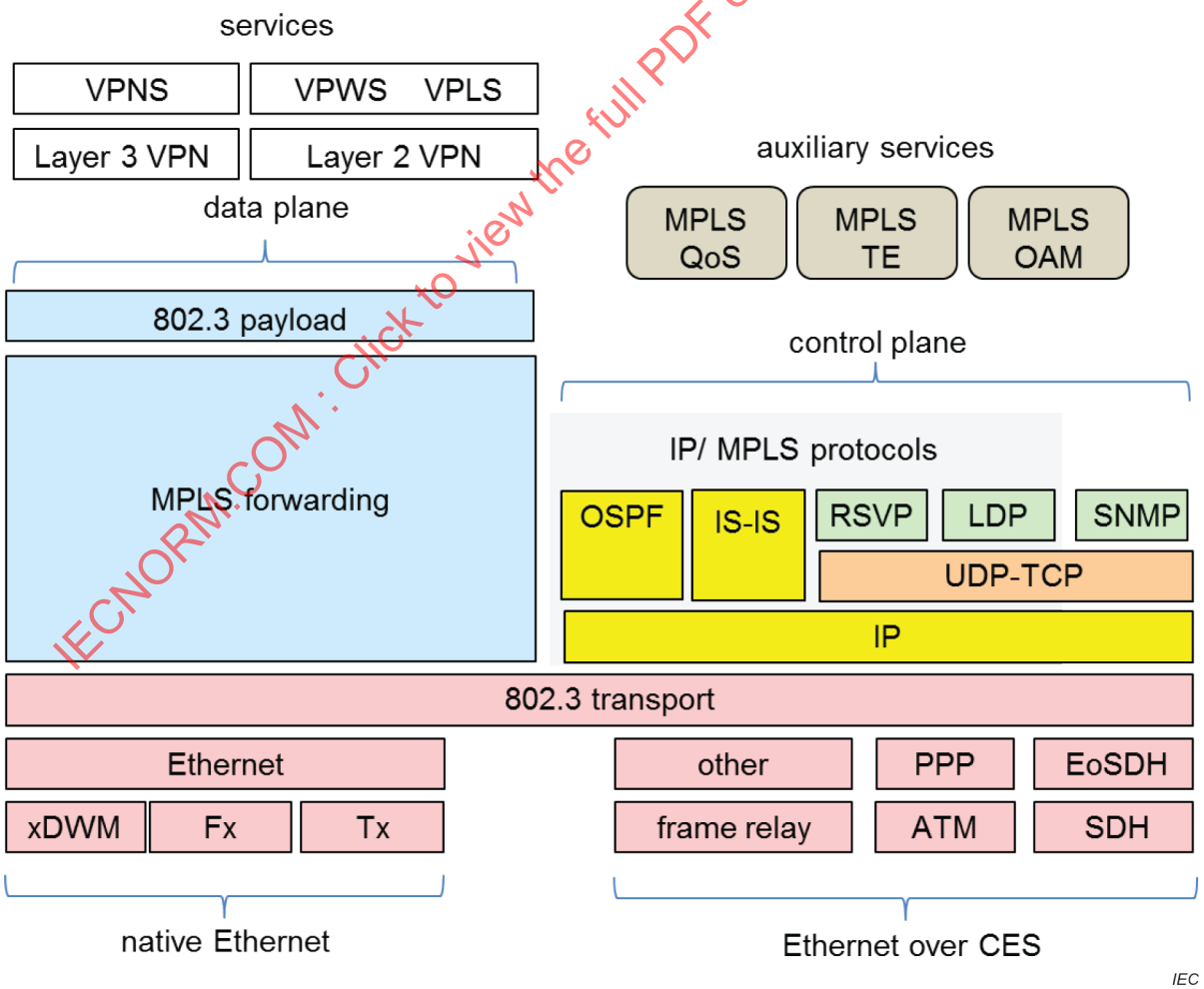


Figure 83 – MPLS building blocks

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 is based 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.

7.6.9.8 MPLS TE

Traffic engineering allows setting up the MPLS network. To this effect, the network engineer configures the different LSR and LER.

7.6.9.9 Use case: MPLS application in utility automation

Figure 84 depicts a generalized architecture in which an MPLS network establishes WAN communication between the main components of a power system. It addresses the main use cases:

- substation-to-substation (IEC TR 61850-90-1): multiple substations can be connected over a multi-service MPLS infrastructure (the intra-substation network consisting of station bus and process bus has no routing).
- substation-to-control centre (IEC TR 61850-90-2): the figure contains a primary and a secondary control centre.
- Remote engineering use cases are covered inherently.

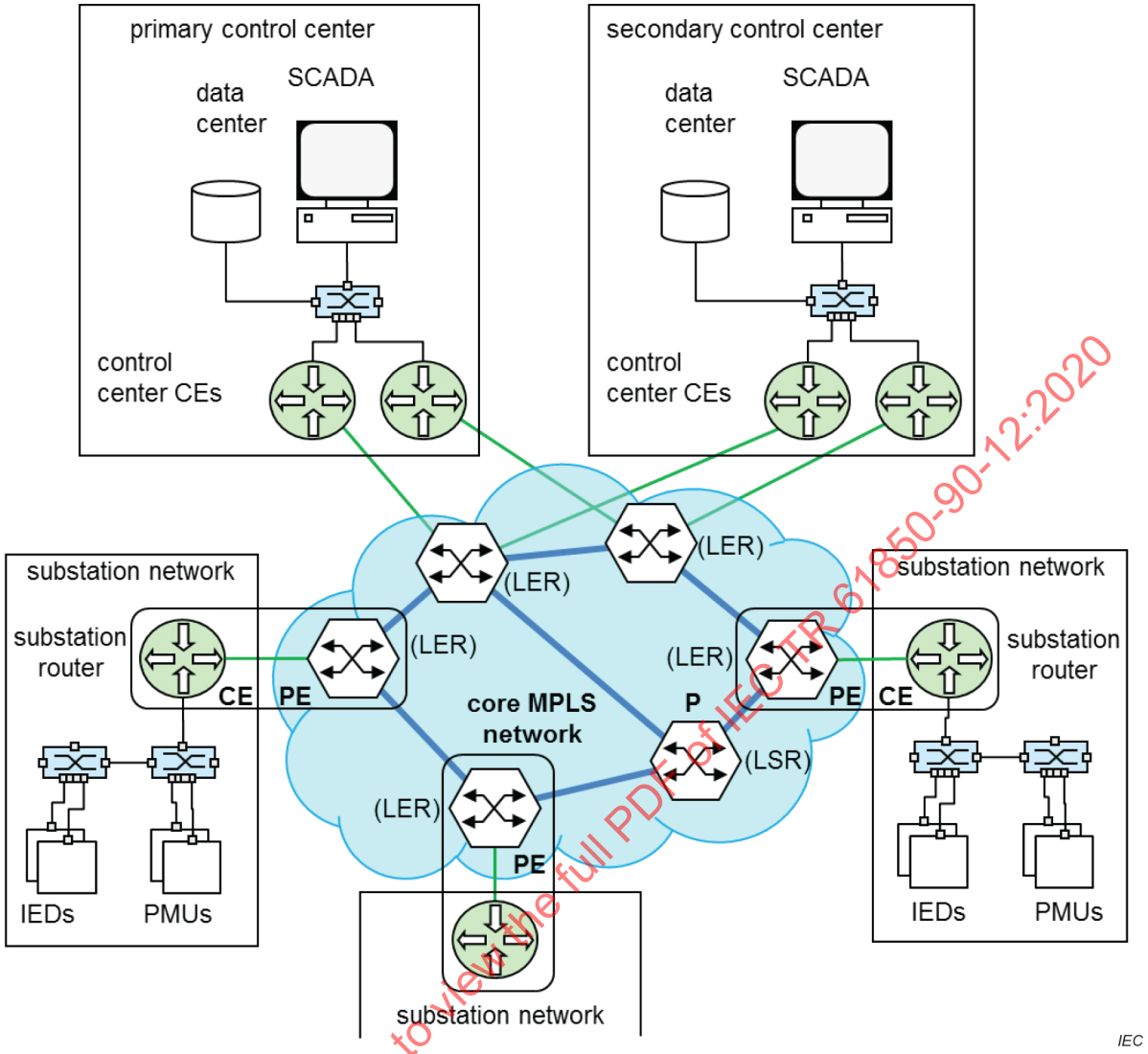


Figure 84 – MPLS network architecture for utilities

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 85 shows the differences and the overlapping features.

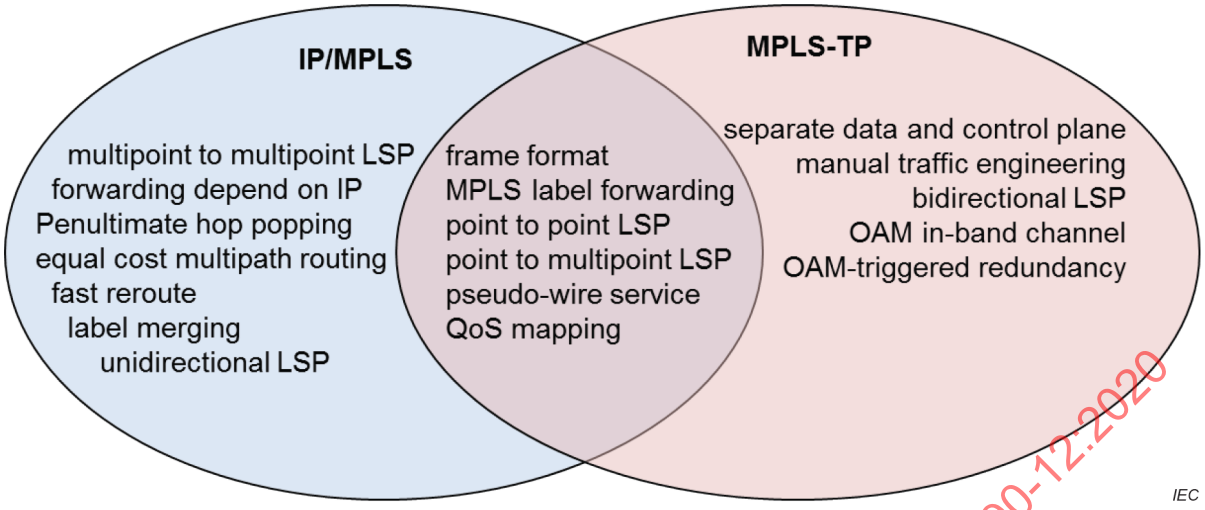


Figure 85 – IP/MPLS and MPLS-TP features

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 48.

Table 48 – IP/MPLS characteristics

Data plane	P2P, P2MP / MP2MP LSP forwarding ECMP (Equal-cost multi-path routing)
Control plane	Dynamic, by BGP and LDP
OAM (Operations, Administration, & Maintenance)	Based on LSP Ping, Trace Route, Trace Tree
Resiliency	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.
Traffic engineering	Bandwidth reservation with RSVP-TE, advertised by the IGP and maintained in the TE database stored on each node
Services	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 49 contains the basic characteristics of MPLS-TP; Figure 86 shows the basic architecture.

Table 49 – MPLS-TP characteristics

Data plane	P2P, P2MP (no MP2MP) Bidirectional P2P and unidirectional P2MP LSP (no LSP merging) In-band associated channel (G-Ach / GAL) Co-routed (same forward and reverse paths following exactly the same nodes) LSP contained within a tunnel acting as a container for LSP
Control plane	Static; does not need MPLS control plane capabilities Enables the management plane to set up LSPs manually Dynamic (in GMPLS)
OAM	Dedicated, In-band OAM channel (Generic Associated Channel (G-ACh)) which enables a rich set of OAM features Guaranteed resources for management Continuity check, remote defect indication Connectivity verification and route tracing Fault OAM (e.g. MPLS Lock Report) Performance management OAM does not need any IP layer functionalities
Resiliency/Fault tolerance	50 ms switchover (recovery) Path (Linear) fault tolerance – 1:1, 1+1, 1:N Ring fault tolerance
Services	VPWS (point-to-point) and VPLS (multicast).

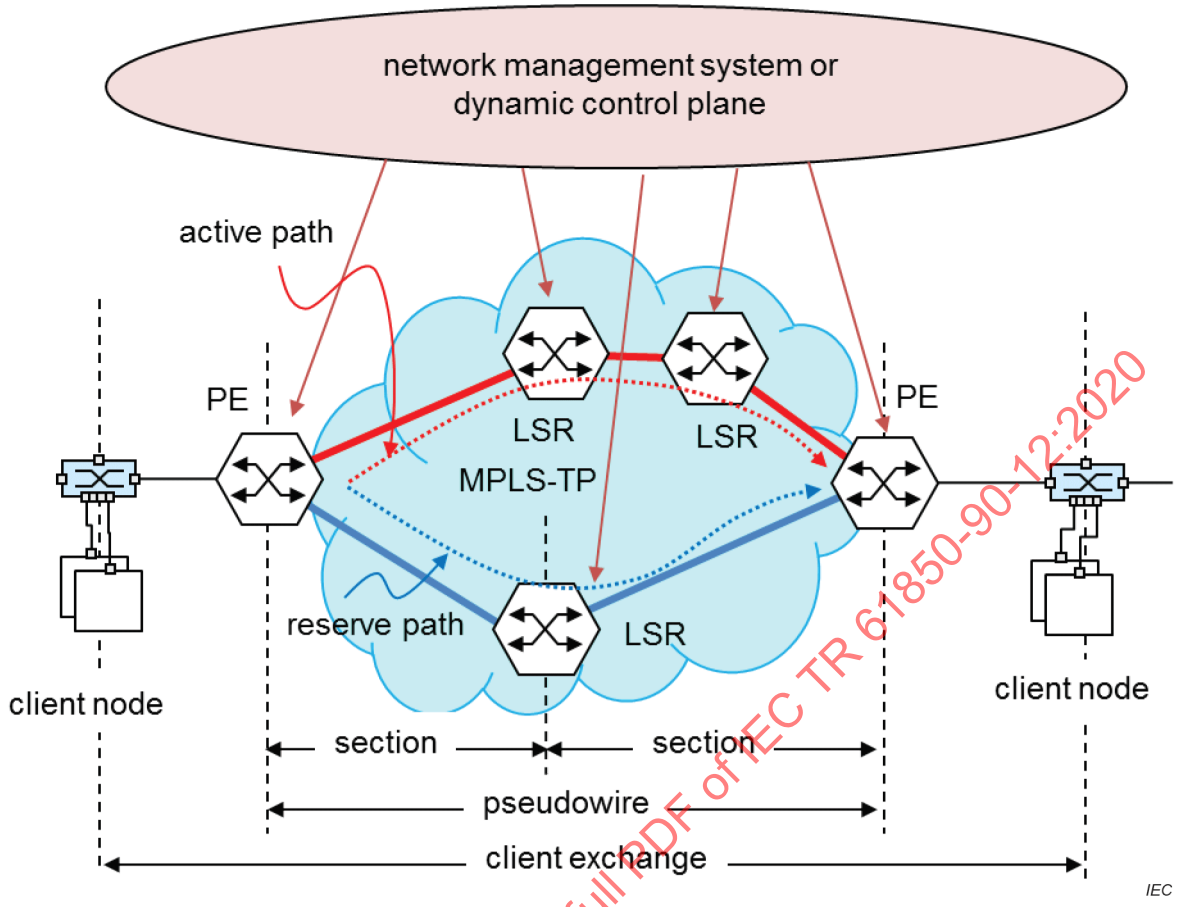


Figure 86 – MPLS-TP redundant routing

7.6.9.10.4 MPLS summary

Table 50 summarizes MPLS.

Table 50 – 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 involves 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 Subclauses 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 2019. 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 87).

NOTE GOOSE and SMV frames do not carry a network header within a substation, but often an IEEE 802.1 Q tag.

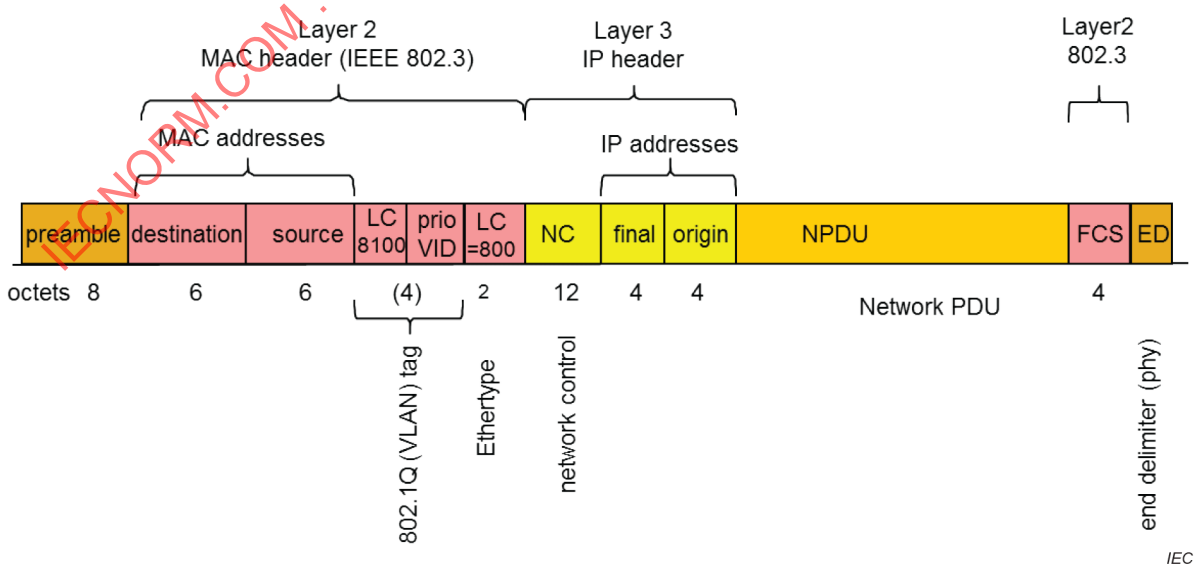


Figure 87 – Ethernet frame with IP network header

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 88).

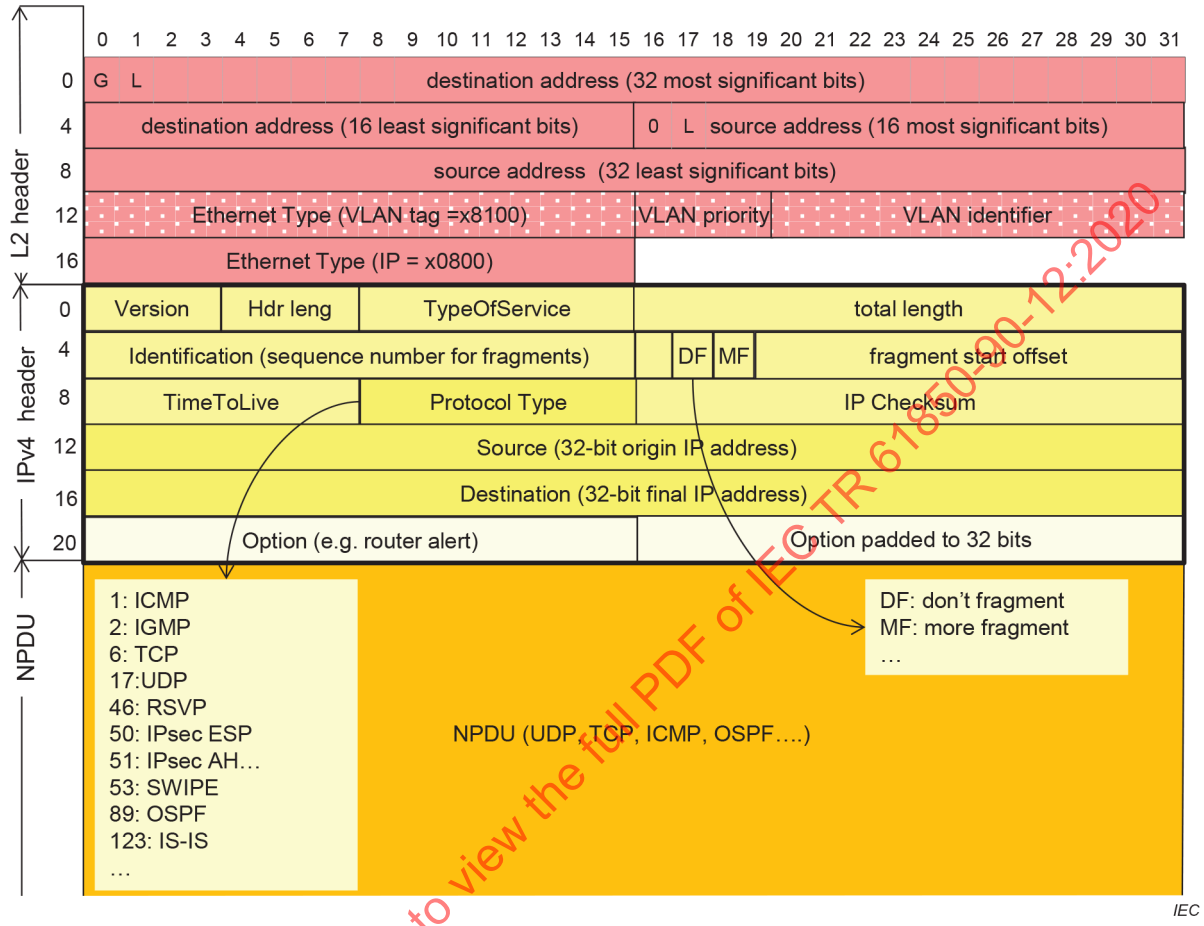


Figure 88 – Mapping of IPv4 to Ethernet frames

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 "00001010'00001100'01111111'00000100"b.

The IP addresses are divided into a public address space (unique worldwide and administrated by the Internet Assigned Numbers Authority (IANA) through the 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 to stretch the life of IPv4 since they allowed the reusing of 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 NPDUs, 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 no longer support IPv4 and network providers may stop their support. It is therefore advisable to commence with the migration process, as 9.2 recommends.

7.7.1.3.2 IPv6 header

RFC 2464 defines the mapping of IPv6 to Ethernet frames as Figure 89 shows.

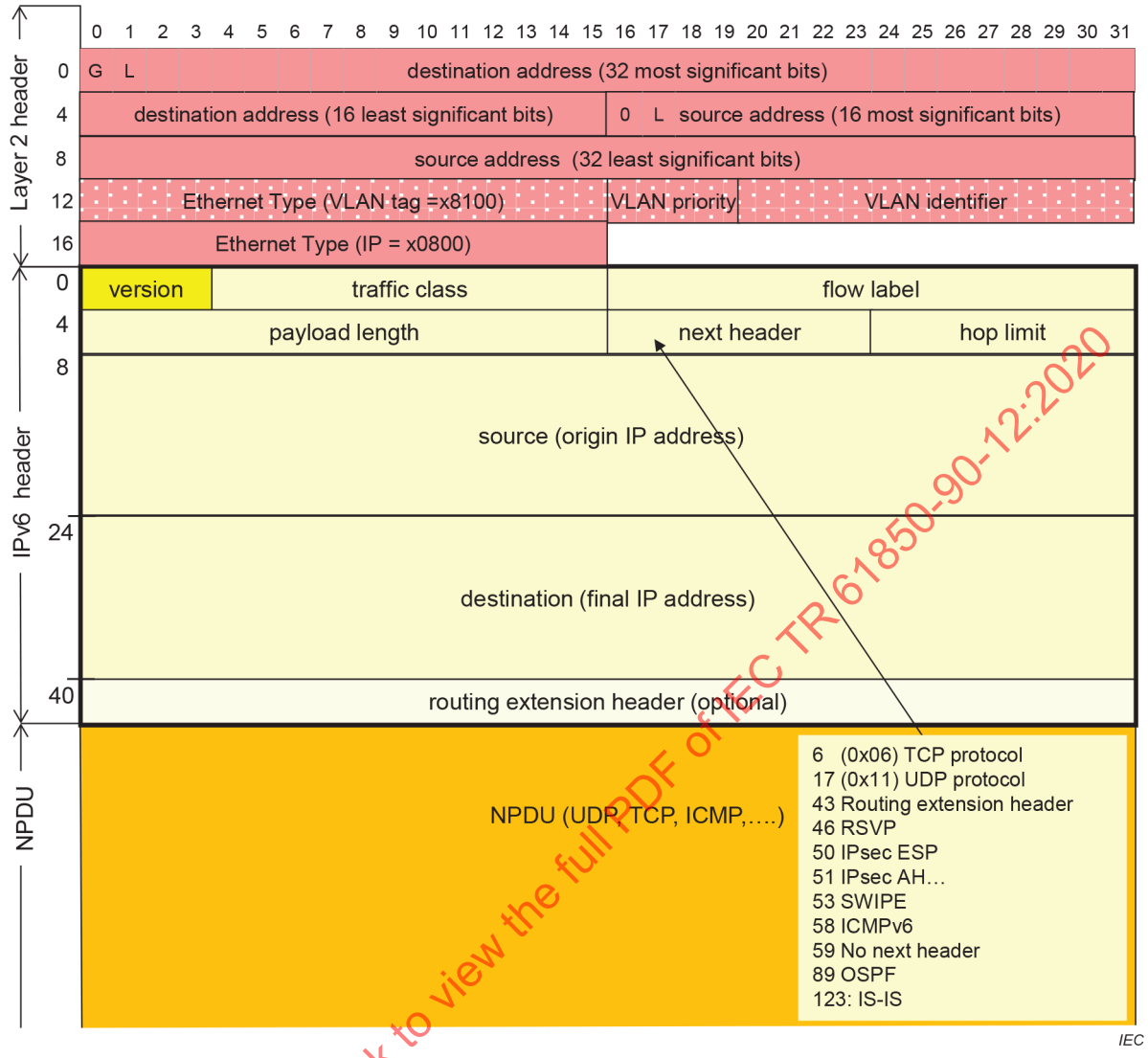


Figure 89 – Mapping of IPv6 to Ethernet frames

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, tunnelling, 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 90).

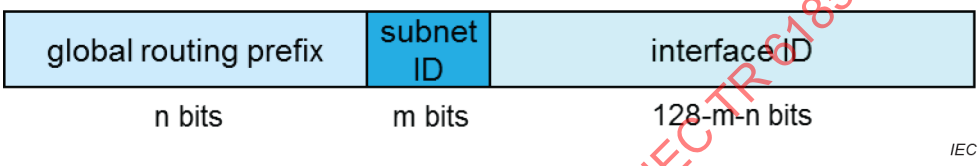


Figure 90 – IPv6 unicast address structure

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 91):

fc00::/8 ("L-flag" bit set to ‘0’); or

fd00::/8, ("L flag" bit is set to ‘1’).

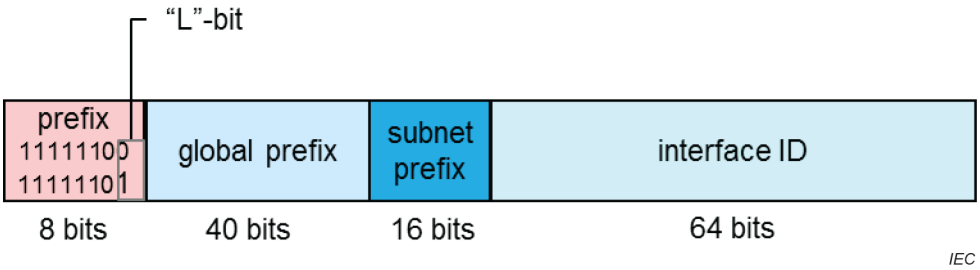


Figure 91 – IPv6 ULA address structure

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 92) has a prefix of fe80::/10 according to RFC 4291.

Figure 92 – 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 tunnellers), not at the intermediate routers as IPv4 does (RFC 4944).

IPv6 requests that a node is capable of MTU path discovery (RFC 1981), 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) (RFC 4862). 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 (RFC 4919) provides IPv6 support over low power and lossy networks.
  - RFC 6550 provides the routing protocol for 6LoWPAN (RPL)
  - RFC 4944 specifies the 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 51 summarizes the main differences between IPv4 and IPv6:

Table 51 – 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 52 compares the addresses in IPv4 and IPv6.

Table 52 – IPv6 vs 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>
```

NOTE The IPv6 address is represented using lowercase hexadecimal characters, but uppercase characters were previously used, so a parser should accept both uppercase and lowercase.

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 93) that RFC 2765 recommends.

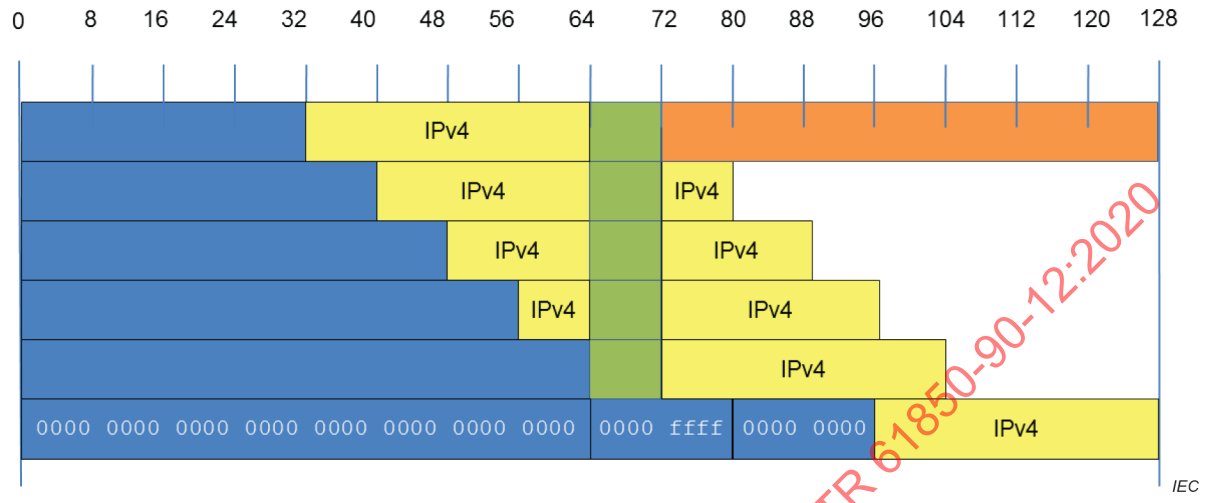


Figure 93 – Mapping of IPv4 to IPv6 addresses

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 anymore. 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 number 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.

7.7.2 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 in a timely manner, 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 the requests of the end devices.

Routers can give a higher priority to some kinds 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 upon 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 88) from the 3-bit IP-precedence to a 6-bit DSCP field (see Figure 94), allowing to distinguish 64 classes of traffic.

The packet classification determines the router's treatment of the packet as per-hop behaviour (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 53).

For example, the codepoint "101110" designates EF. The codepoint "000000" designates "best-effort traffic".

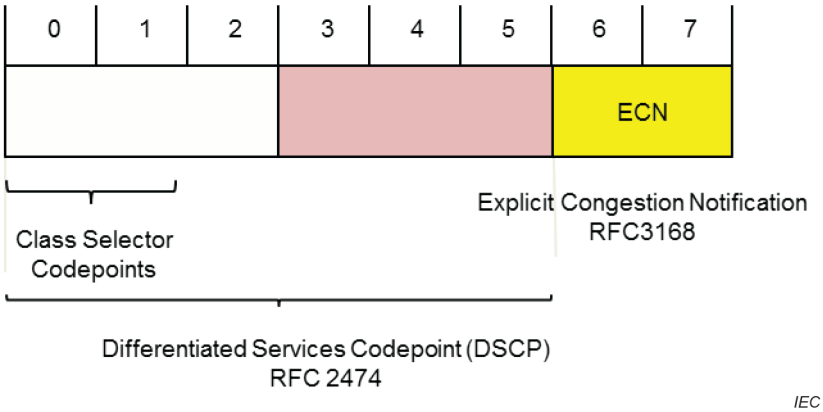


Figure 94 – DiffServ codepoint field

Table 53 – 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 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 95).

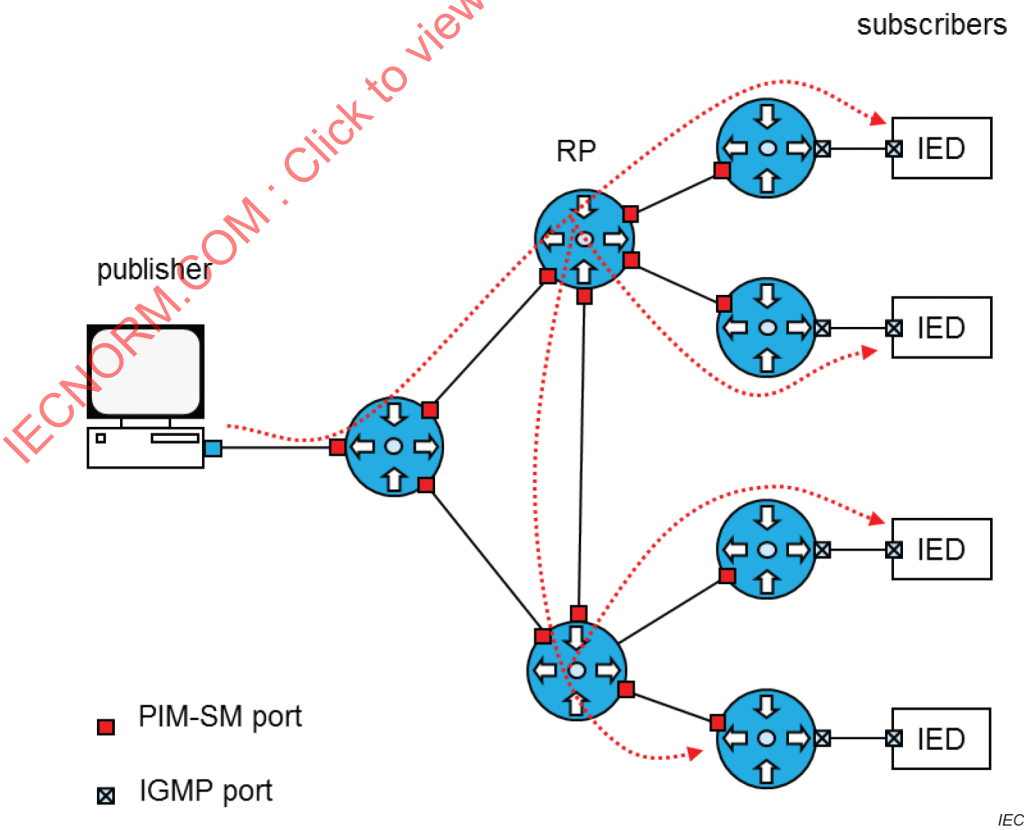


Figure 95 – Unidirectional protocol independent multicast

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 96).

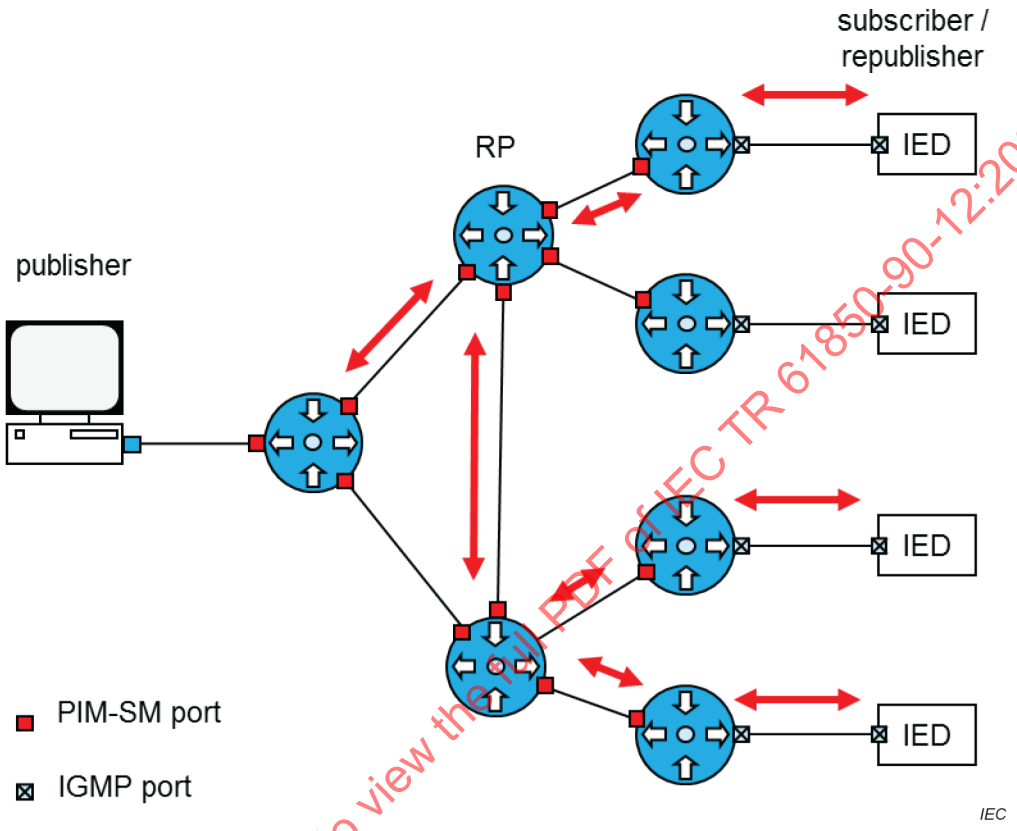


Figure 96 – Bidirectional protocol independent multicast

7.7.4 IP redundancy

IP provides redundancy against router failures or link failures by rerouting the packets.

If IP is based upon 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 a 50 ms recovery period 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) or both.

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 97 shows the frame format for authentication.

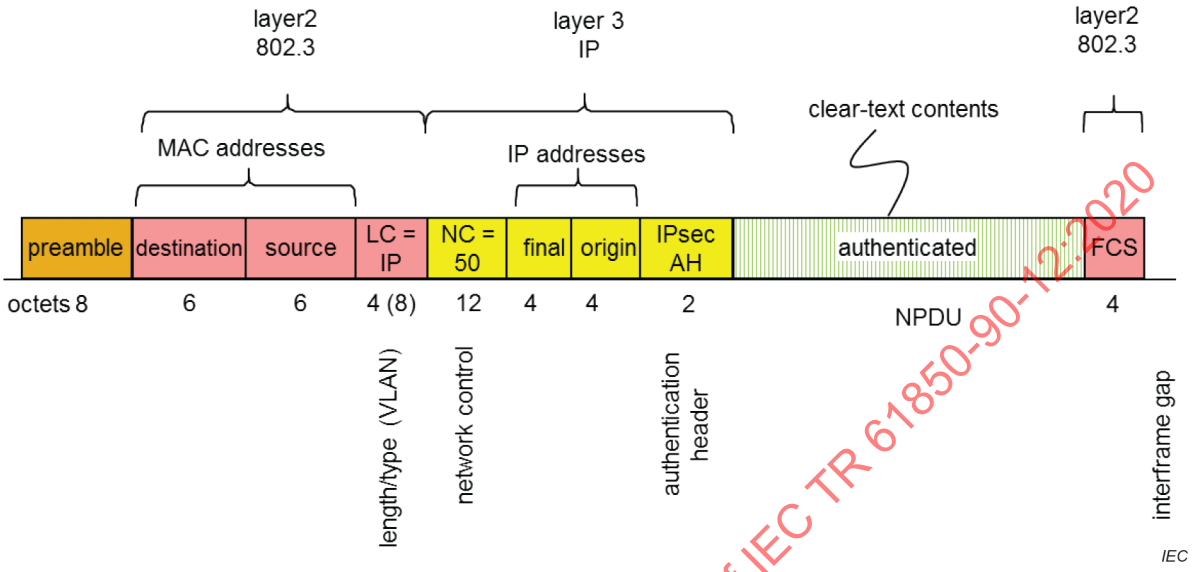


Figure 97 – Frame format for IPsec (authenticated)

- 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 NPDU contains a whole IP packet with origin and final IP addresses which are distinct from the IP addresses used for transport over the IPsec-defended segment (Figure 98). This way, the IP addresses of the end user remain hidden. IPsec in tunnel mode implements a VPN, see 7.11.

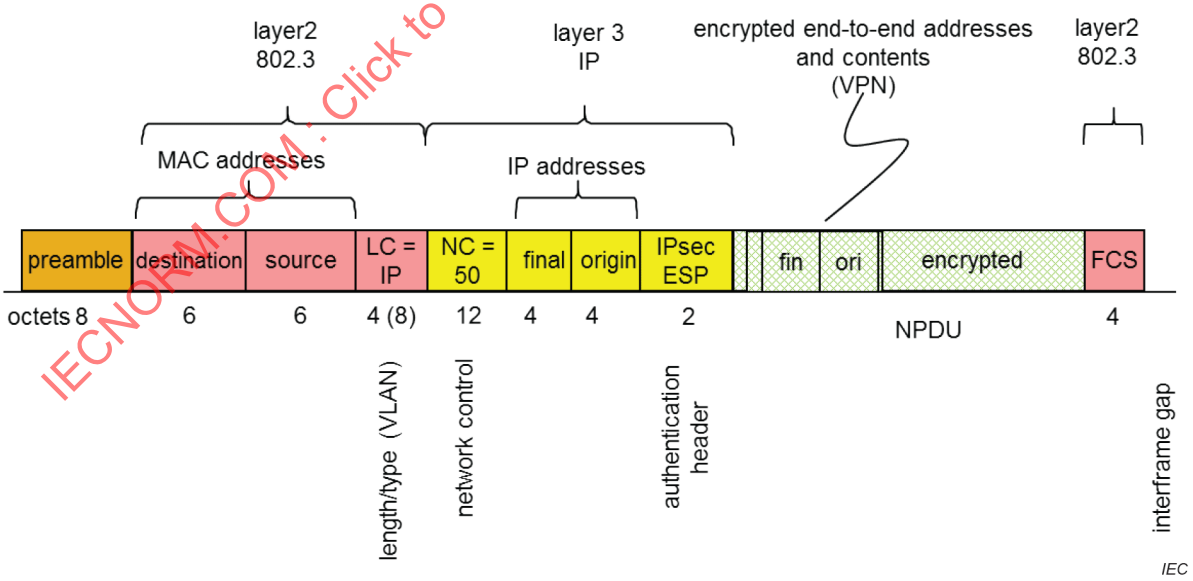


Figure 98 – Frame format for IPsec (encrypted)

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 is based on DNP3 or IEC 60870-104, which also use TCP/IP. However, this traffic does not necessarily 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 99).

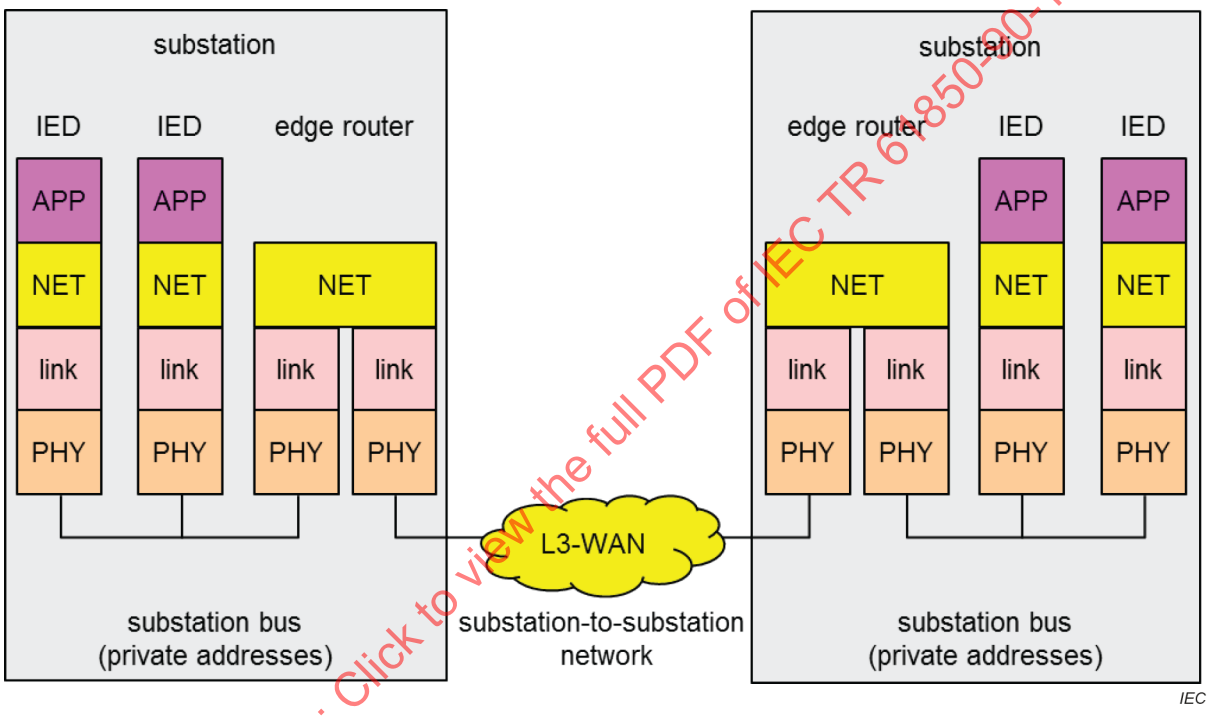


Figure 99 – Layer 3 direct connection within same address space

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.

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 an NAT that owns a pool of global addresses. These addresses are not necessarily public internet addresses, in most cases, they will be enterprise addresses taken from the company's address space (e.g. 10.x.x.x). Only a few communications go to the public internet. There will be another NAT in the network connected to the public internet, probably with stricter security policies.

Figure 100 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.

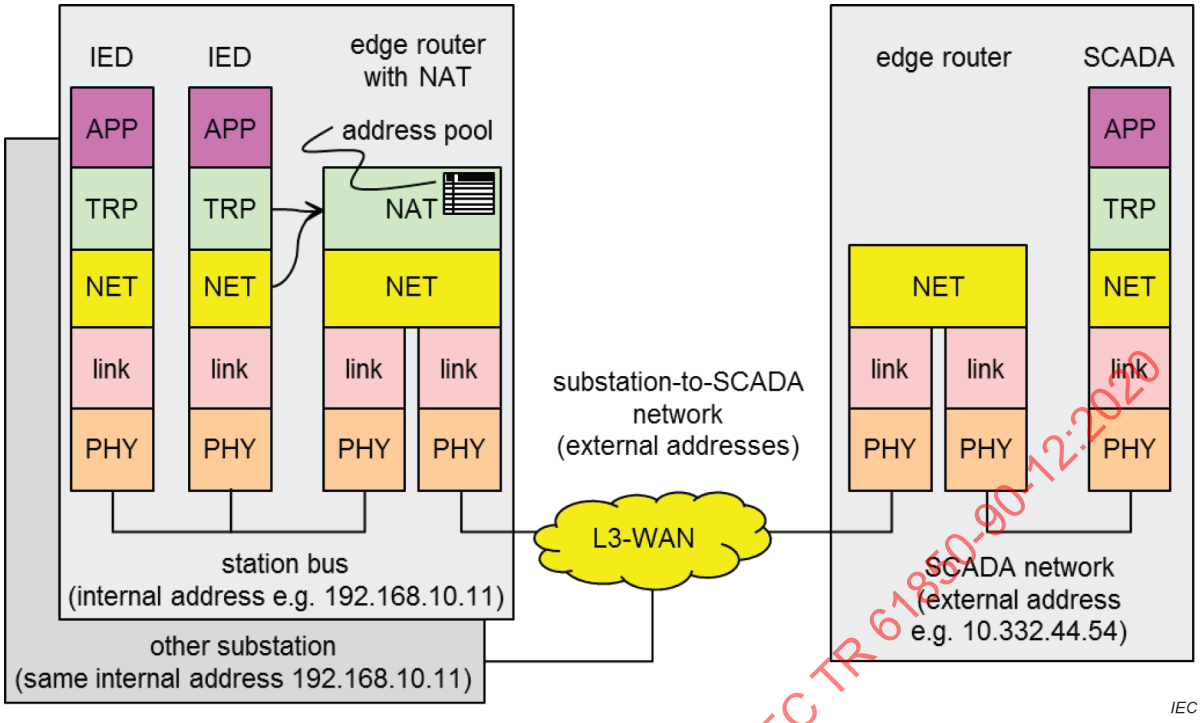


Figure 100 – Connecting substations to SCADA by a NAT

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 9.2.3.

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 auto configuration which 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 101, which shows the connection of a remote SCADA or engineering station to a substation.

The substation is visible only through the Application Layer Gateway (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.

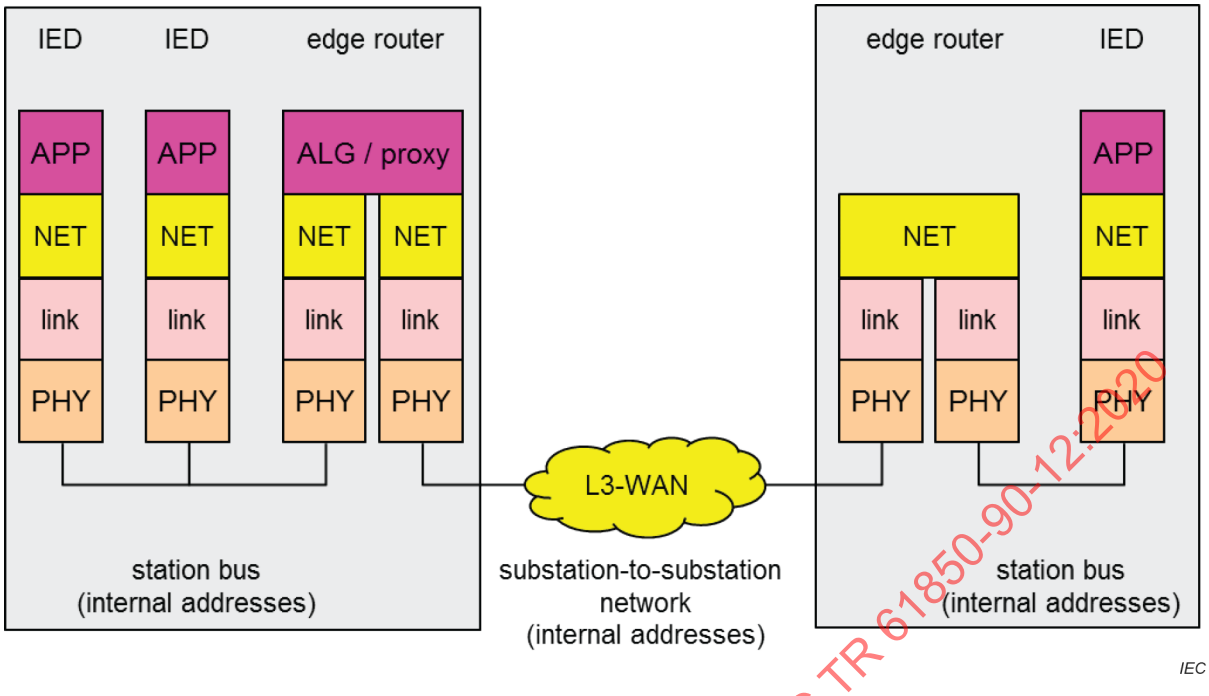


Figure 101 – Substation to SCADA connection over ALG

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 54 summarizes the IP technology.

Table 54 – IP Summary

Feature	Comments
Acceptance	Well known and understood, used for 40 years
Bandwidth Efficiency	In general high – bandwidth can be shared over different paths; medium efficiency for small data packets due to relatively high packet header overhead
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 caters for end-to-end flow control and error recovery. The transport header follows the network header and precedes the transport payload (TPDU) (Figure 102).

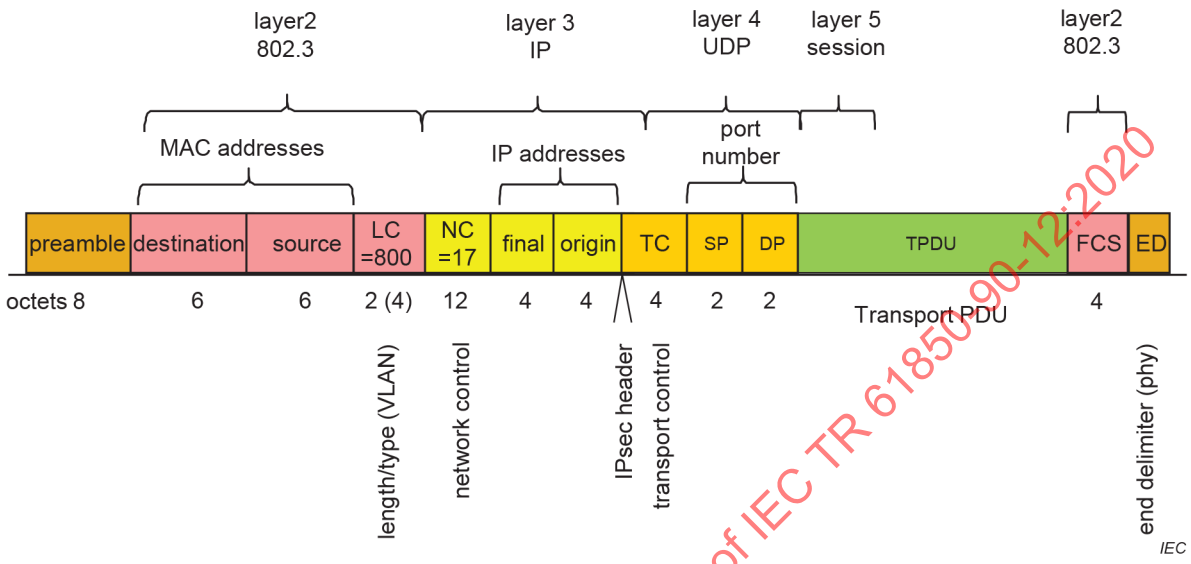


Figure 102 – Ethernet frame with UDP transport layer

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 103).

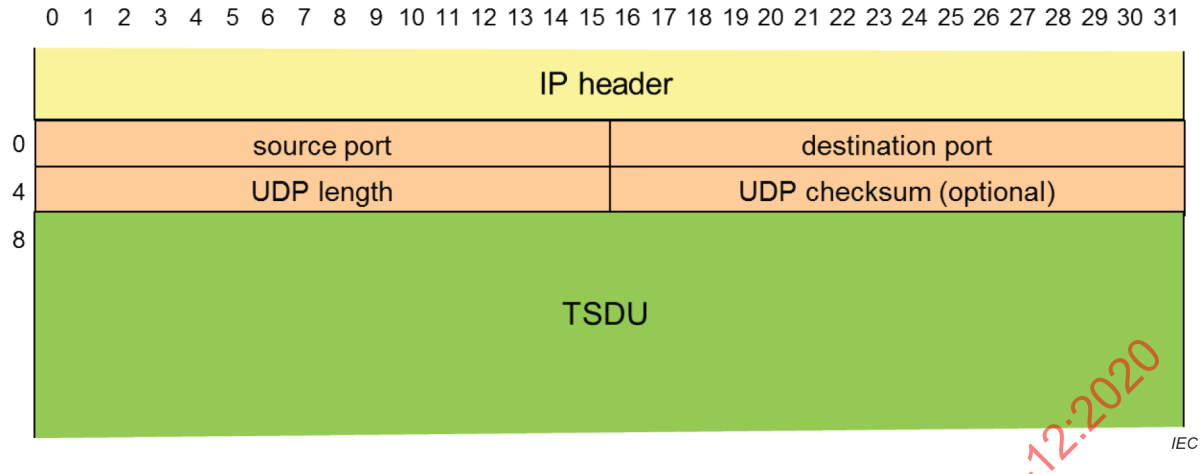


Figure 103 – UDP header

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 104).

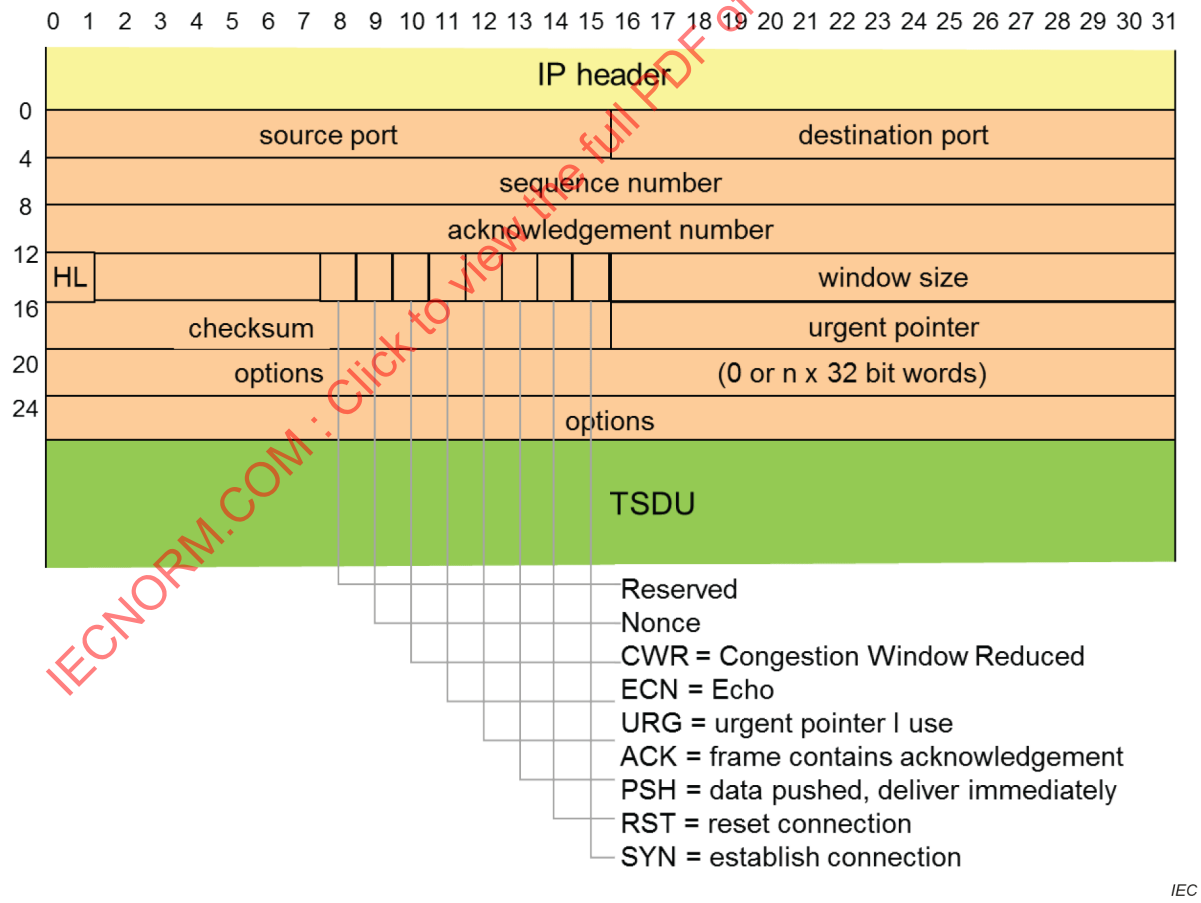


Figure 104 – TCP header

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 1 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 cater for possible duplicates.

NOTE 2 IP provides 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 1 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 systems and devices that employ web based applications.

NOTE 2 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 is originally based on ISO/OSI and ITU-X protocols. To maintain 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 105).

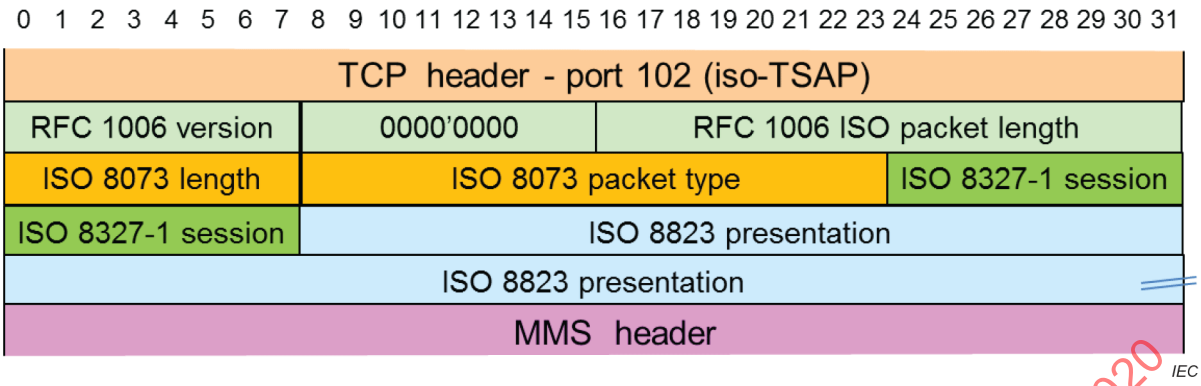


Figure 105 – Session and presentation layers for MMS

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 106).

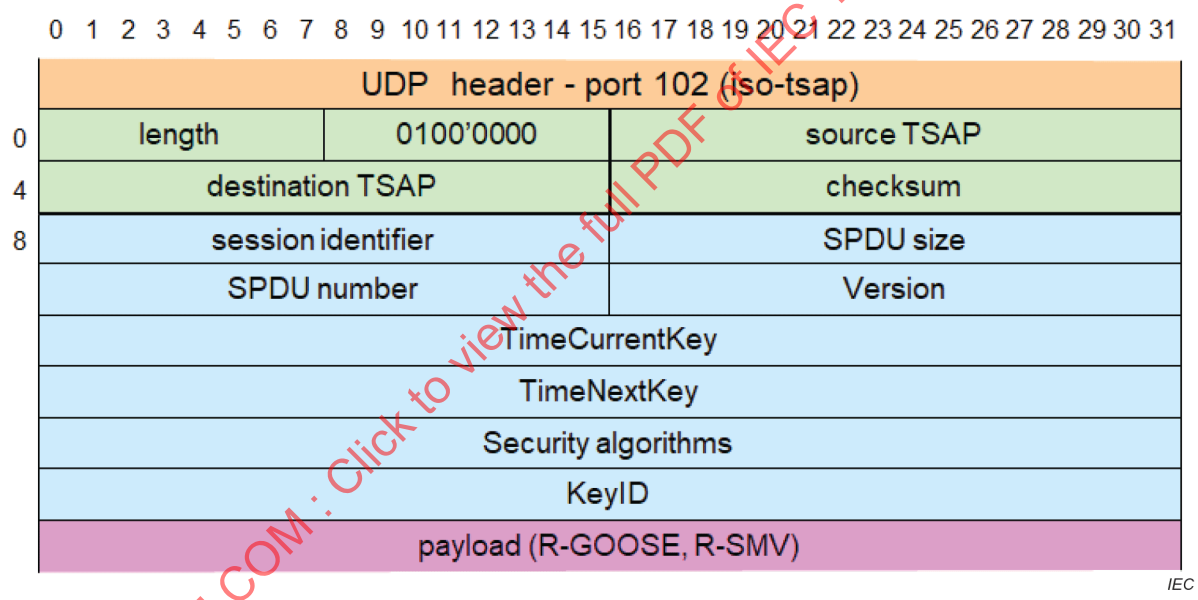


Figure 106 – Session and presentation layers for R-GOOSE

Both RFC 1006 and RFC 1240 are protocol overlays as will be further developed in 7.10.

IEC TR 61850-90-5 supports both a direct and a tunnel mode (see Figure 111).

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 107 shows the frame format in case of IEEE C37.118 transmission over UDP/IP.

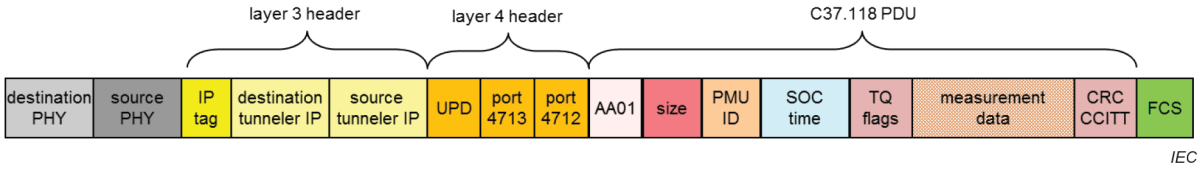


Figure 107 – IEEE C37.118 frame over UDP

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 in widespread 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 illustrates examples of application interface redundancy, in which the application choses explicitly between the different communication paths available to it.

Figure 108 shows an example of redundancy in the end-to-end application layer using multicast duplicate transmission and retransmission mechanisms.

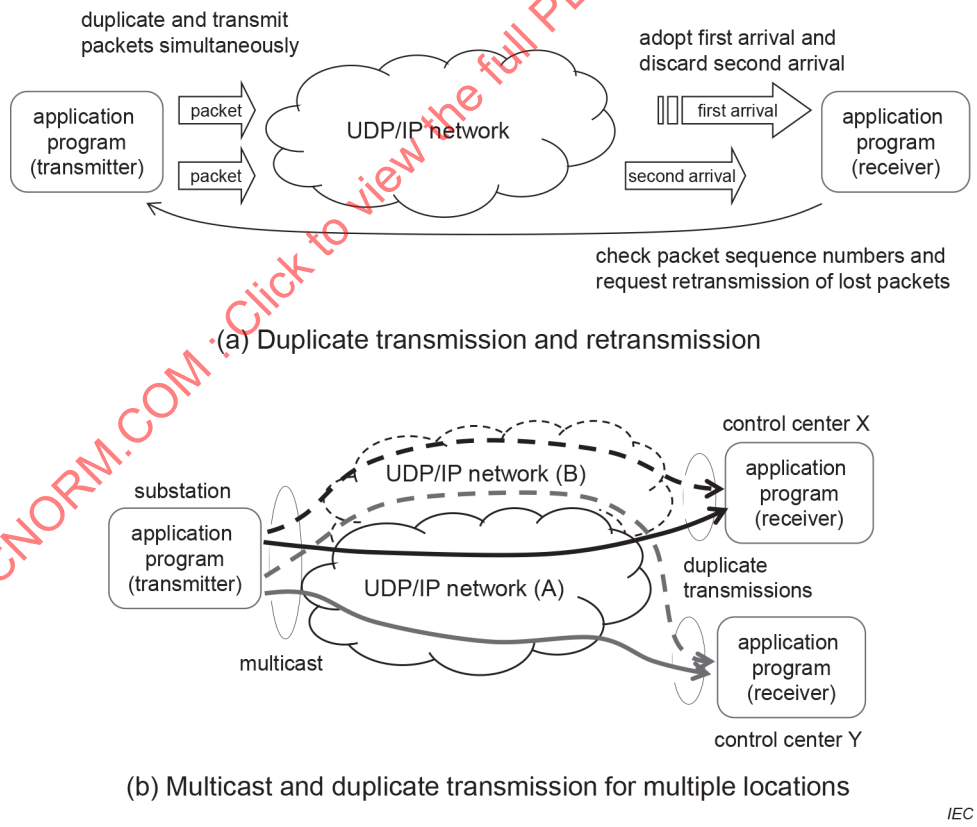


Figure 108 – Redundant network transmission handled by the application layer

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 address pairs is clumsy. When several applications share the same hardware, it makes little sense to let every application with different criteria 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 – tunnelling

7.10.1 Definitions

Protocol overlay is the transport of one protocol over another, also called tunnelling.

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 tunnelling.

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

7.10.2 Tunnelling principle

Tunnelling is the encapsulation of one protocol payload in another protocol. There are at least two tunnellers, one at each end of the tunnel, but there can be branches to other IPv4 domains, as Figure 109 shows. The first protocol could be IPv4 and the second IPv6.

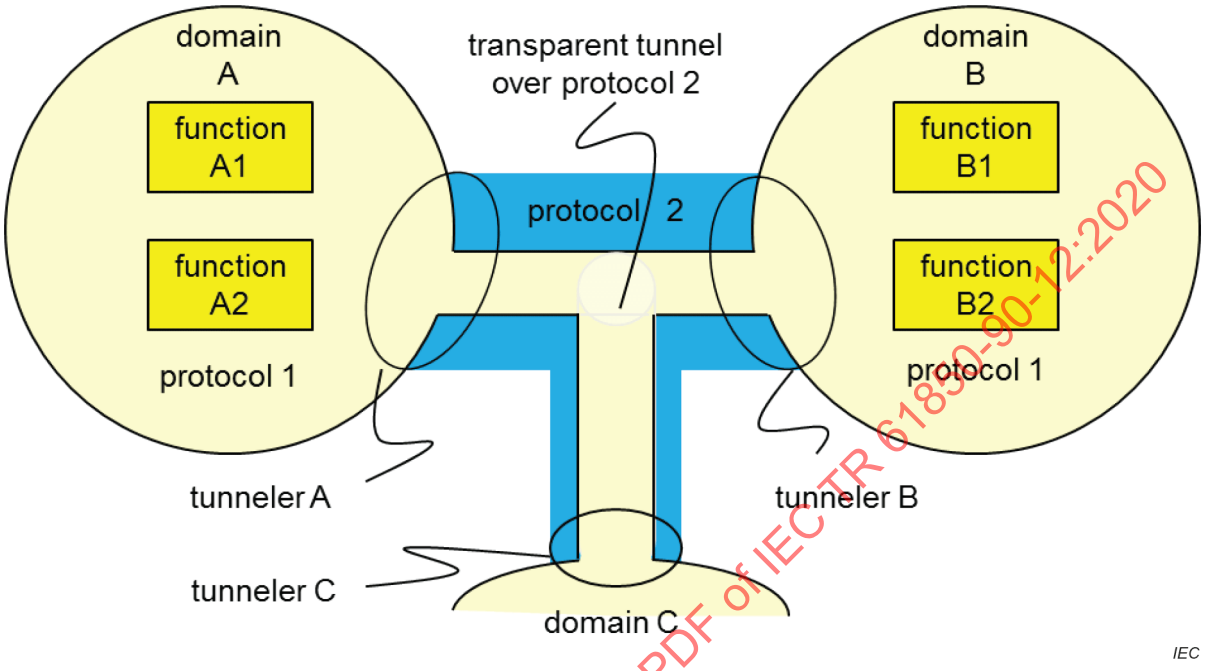


Figure 109 – Tunnelling in IEC TR 61850-90-1

The tunneller is aware of the characteristics of the second protocol; the domains at the end are not aware of it, except that the tunneller can ask to limit the frame size.

7.10.3 Tunnelling Layer 2 over Layer 3

Sending Layer 2 (Ethernet) frames over an IP network is a common way to implement virtual private networks.

IETF standardized numerous tunnelling protocols over IP, among them the Layer Two Tunnelling Protocol (L2TP) (RFC 5641).

Figure 110 shows the protocol layers involved in L2TP tunnelling of GOOSE messages between two substations connected by a Layer 3 WAN.

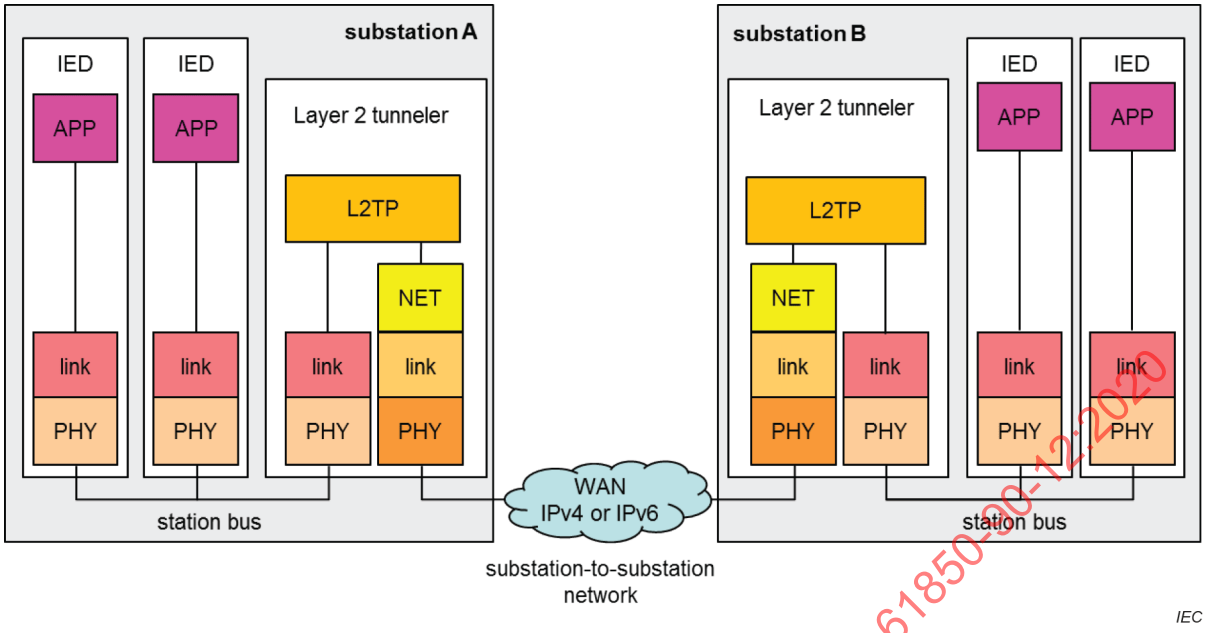


Figure 110 – L2TP transporting Layer 2 frames over IP

7.10.4 Application Example: Tunnelling 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 PTP and LLDP.

These Layer 2 protocols operate with MAC addresses, they may include a VLAN tag as an 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:

d) Forward directly the Layer 2 messages from one terminal to the others over a Layer 2 link (Figure 72), with a Layer 2 being:
   - a Layer 2 direct link (e.g. a dark fibre in an earth cable), or
   - a switched Ethernet network or
   - a Layer 2 emulation over another network.

e) Encapsulate Layer 2 information at one terminal into Layer 3 packets in a Layer 2 tunneller 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 tunneller 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 tunneller.

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 111). The tunneller is particular to the IEC 61850 protocols.

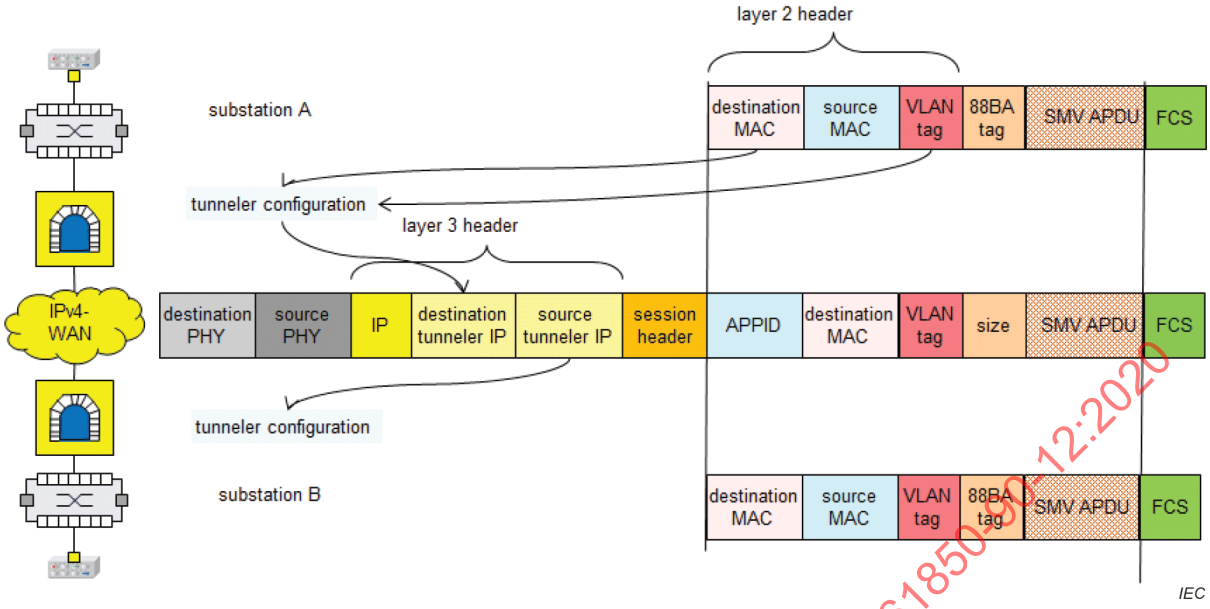


Figure 111 – Tunneling SMV over IP in IEC TR 61850-90-5

7.11 Virtual private networks (VPNs)

7.11.1 VPN principles

Virtual private networks span several completely disjointed 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.

Disjointed 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 the 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.

Tunnelling 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 112 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.

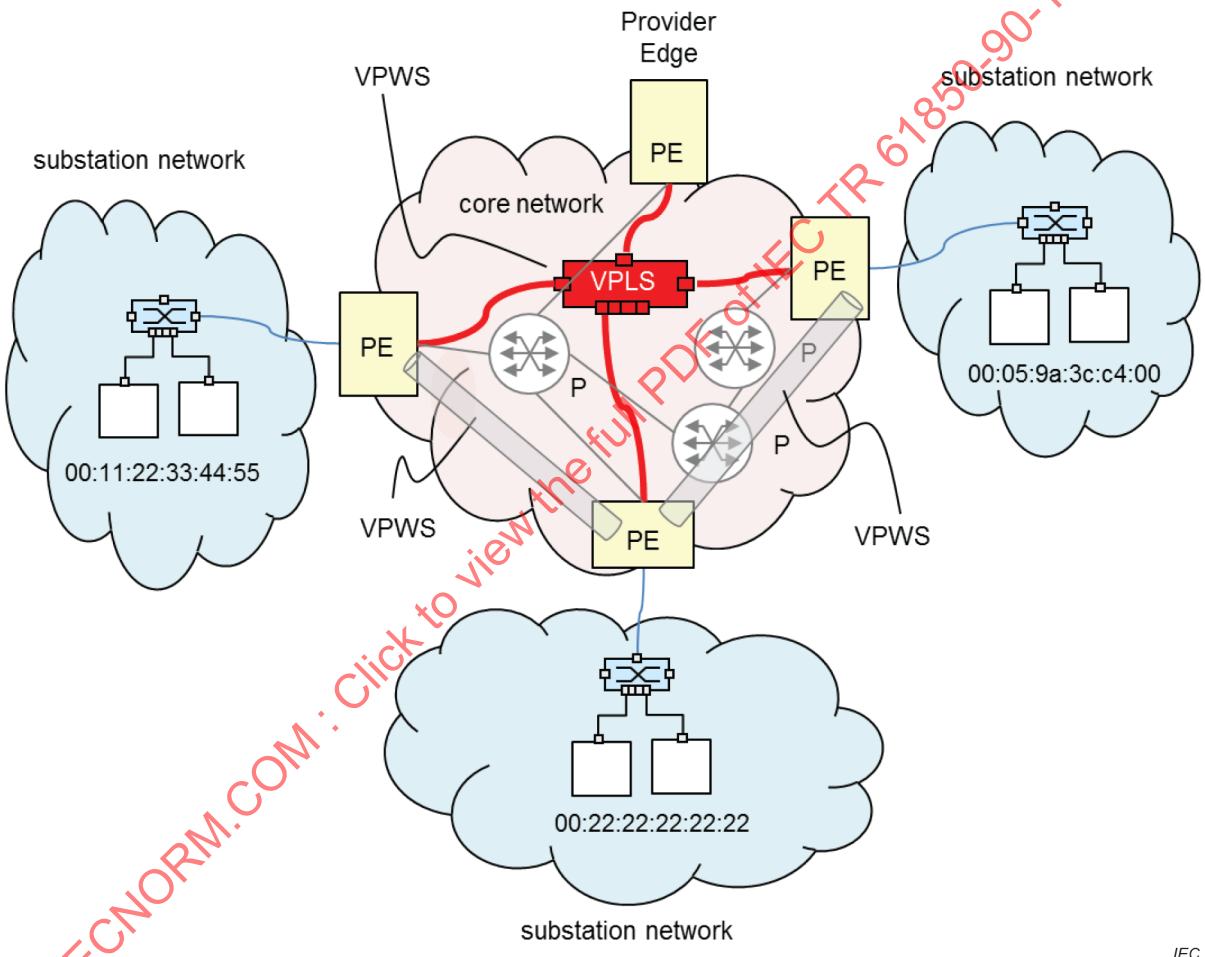


Figure 112 – L2VPNs VPWS and VPLS

L2VPNs make it possible to operate private, multipoint, and point-to-point LANs through wide area networks. L2VPNs usually provide 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 based upon the IP addresses and does not forward the MAC addresses. Figure 113 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.

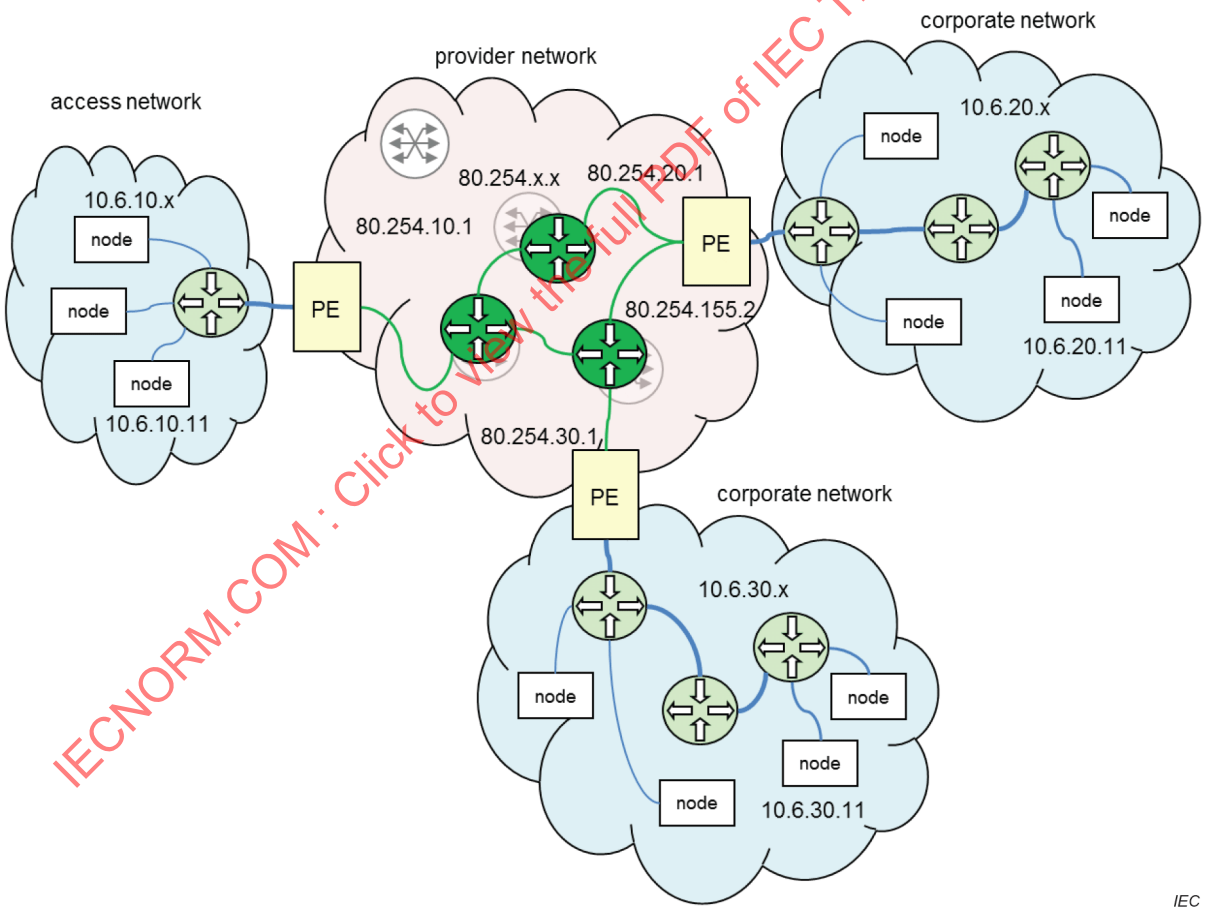


Figure 113 – L3VPN

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).

VPRN 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 behaviour 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 114 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.

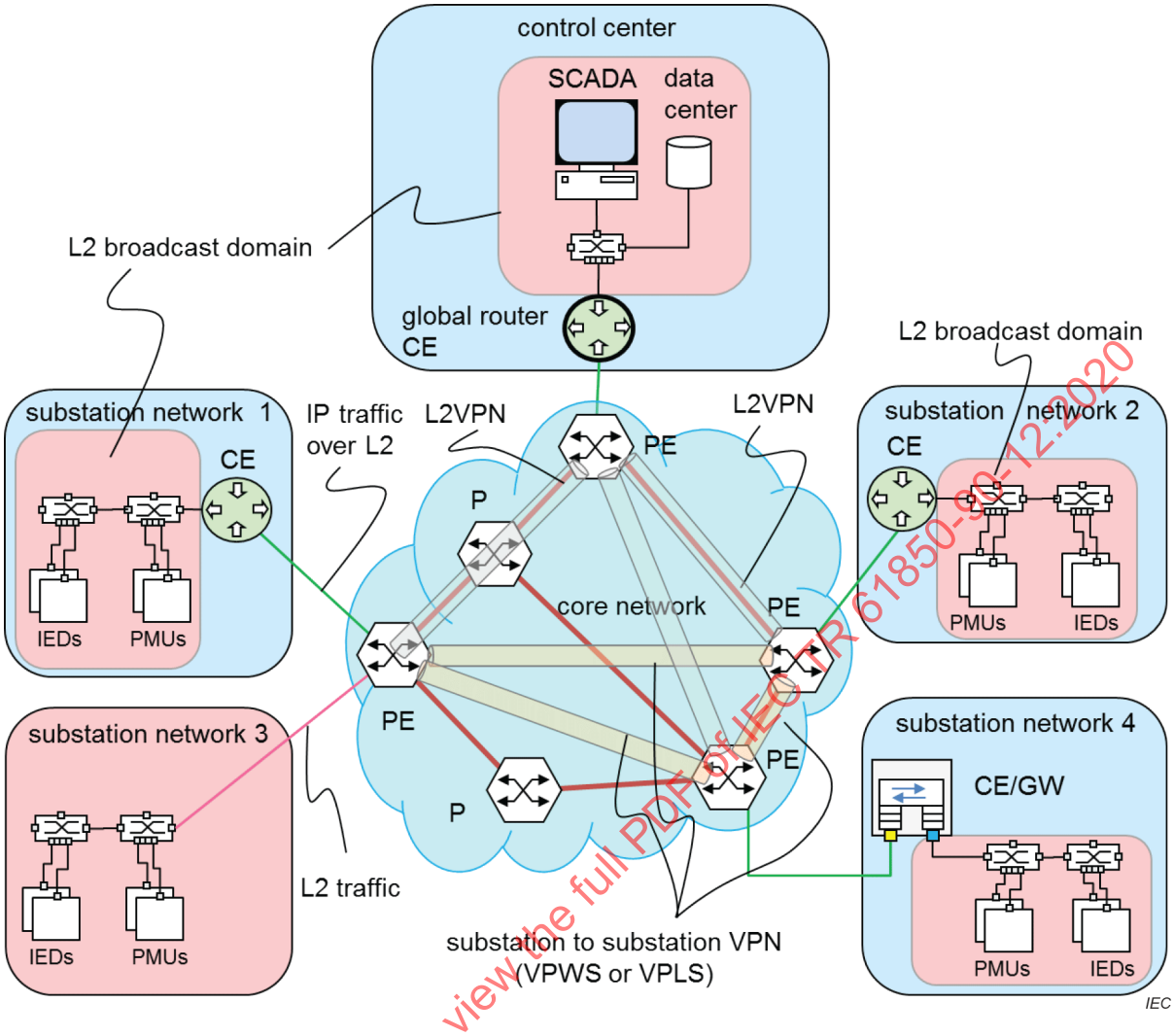


Figure 114 – Emulation of L3VPN by L2VPN and global router

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

VPNs 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 tunnelling 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 55 shows the application cases with the recommended VPNs and QoS.

Table 55 – 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-VPRN	4	GOOSE, SV, raw C37.118 R-SV, IEC 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 115).

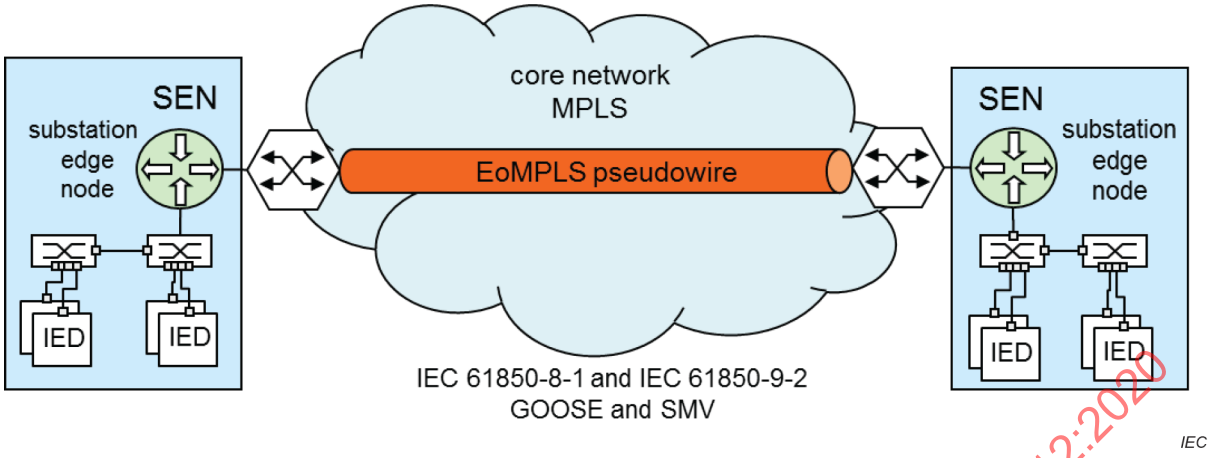


Figure 115 – Tele-protection over VPWS

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 116) to the Central Processing Equipment that computes grid stability conditions.

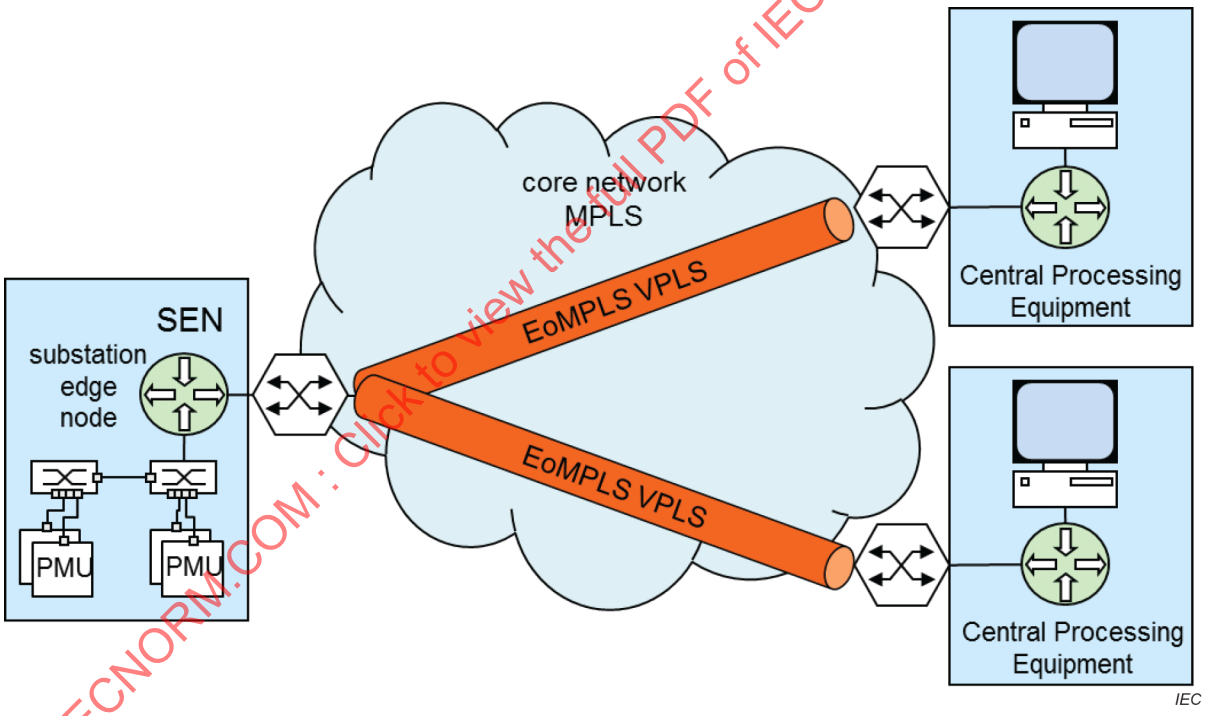


Figure 116 – WAMS over VPLS

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 tunnelled 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 117).

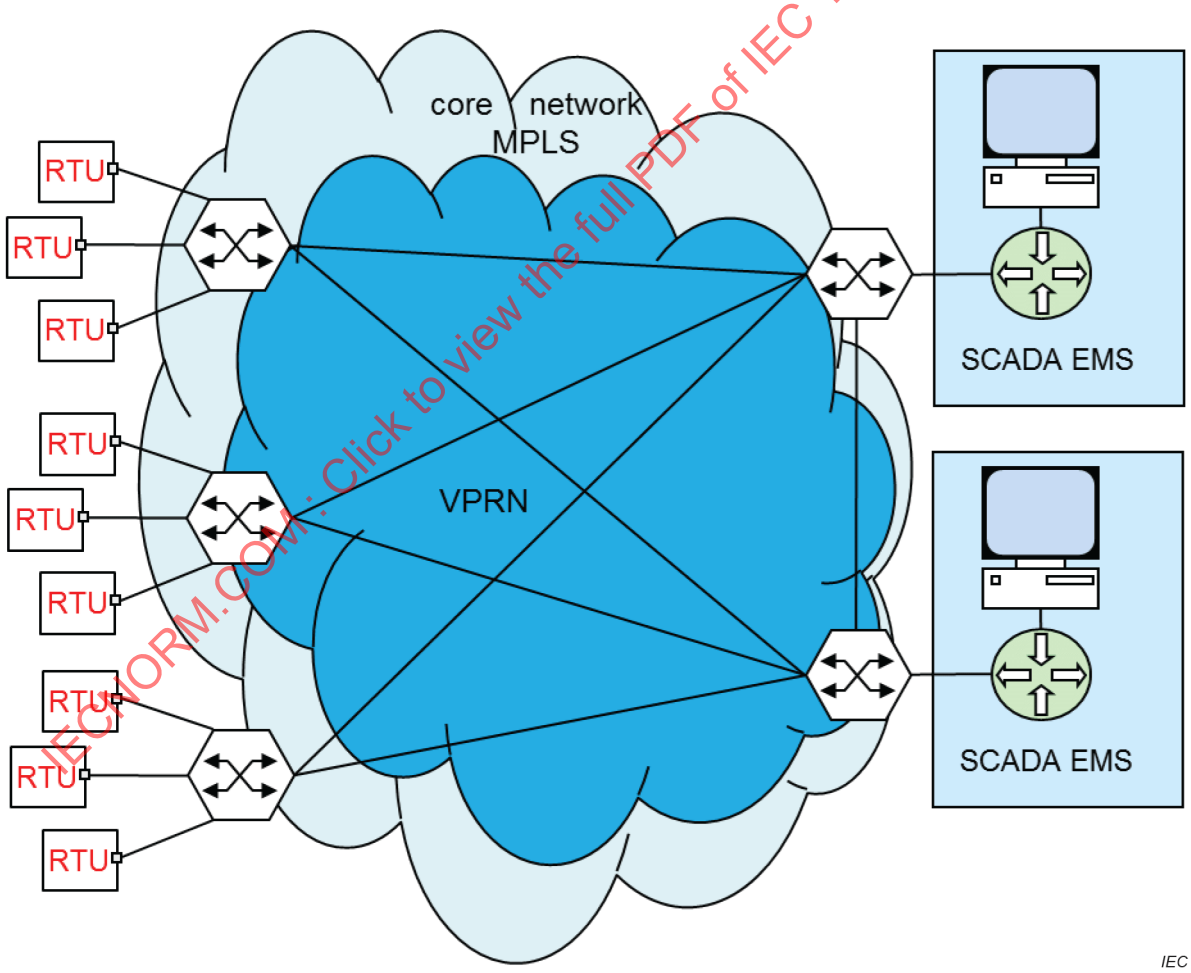


Figure 117 – VPN for IP-based SCADA/EMS traffic

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 entities into a false sense of security.

PSNs are much more vulnerable to 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 requirements. It has also to be considered that security related activities (e.g. updating security patches) must not interfere with utility operation or even interrupt operational traffic.

The IEC 62443 suite specifies a defence 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 or may not be applied.

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 "defence 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 defer 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 of the measures 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 system 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 which can generate considerable traffic;
- Layer 1 security (7.4.9) prevents unauthorized eavesdropping or traffic injection. It is requested when the media runs 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 defence-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 118 shows options 2 to 4.

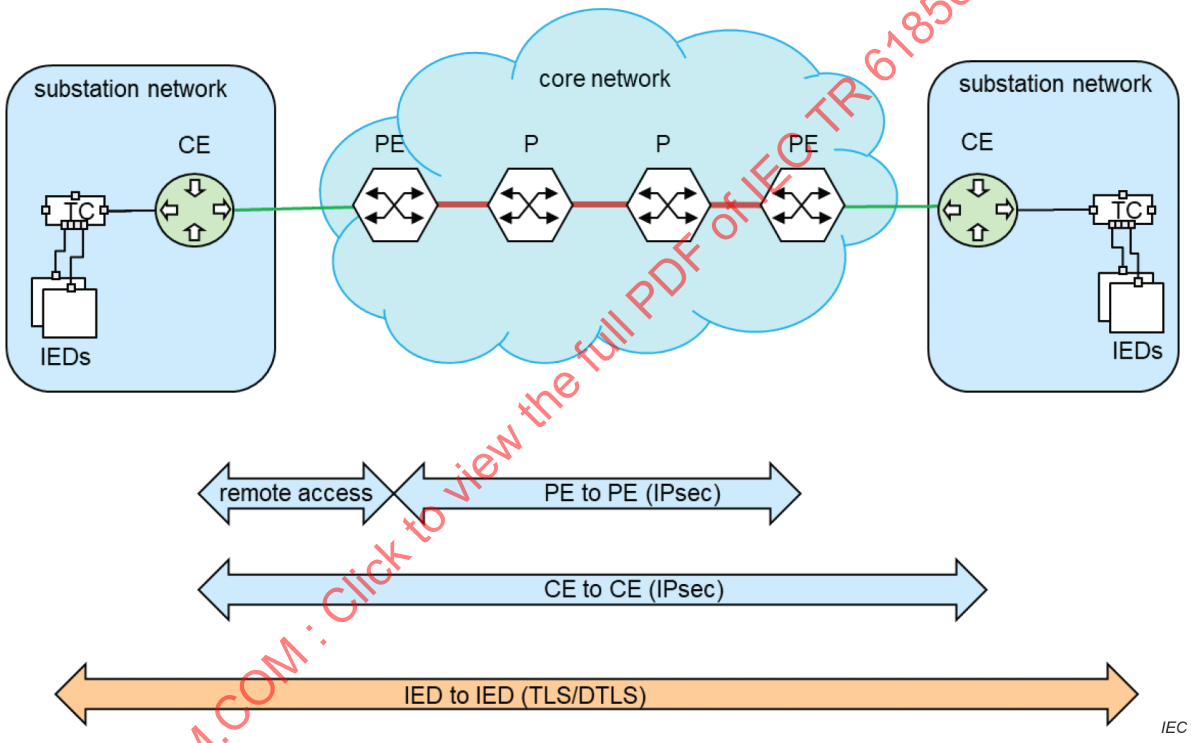


Figure 118 – VPN deployment options

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 defence for telecontrol and SCADA traffic, IP-based or serial (tunnelled). Furthermore, the security architecture for PMU networks in IEC TR 61850-90-5 considers GDOI-based VPNs as an optional security function. It is based on a defence-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 such 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 databases.

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 defence 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 119 shows is another measure.

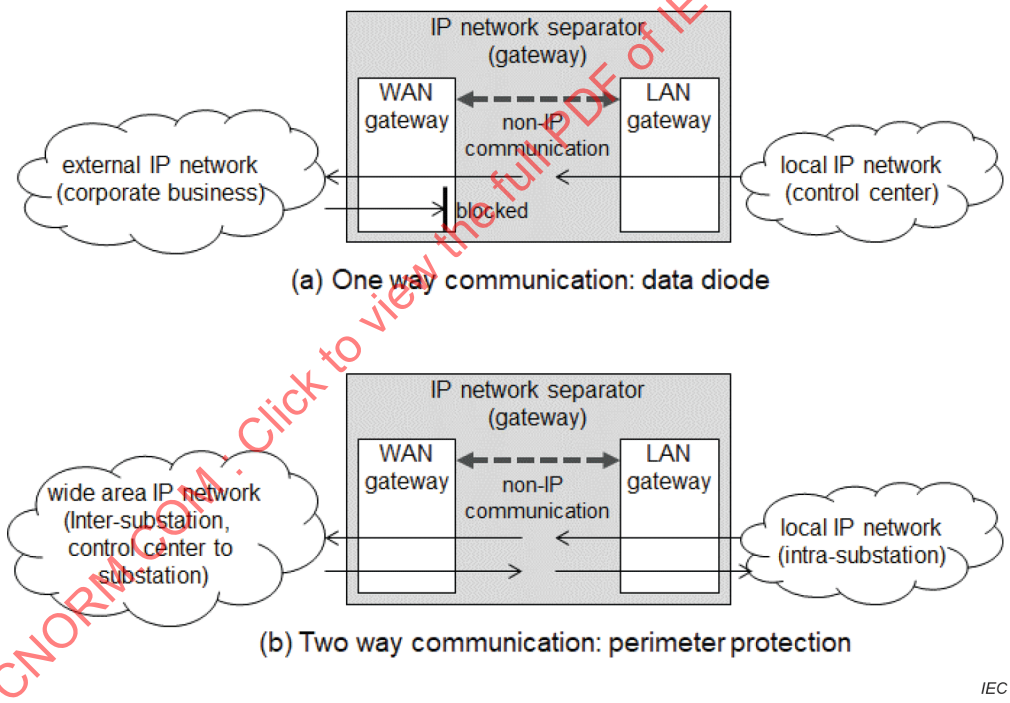


Figure 119 – IP network separator

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 on 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 a 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 to execute on critical system within control centres 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 120) 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 defence

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 defences, depending on the installation, as well as internal defences 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). An NMS typically supports the process of controlling access to networks and devices. An operator uses an NMS to configure and monitor the performance of the network deployment. An 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.
- QoS policies: QoS needs to be assured for critical data flows; DoS prevention by QoS policy:
  - control plane defence;
  - denial-of-service defence;
  - 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 defence-in-depth as well as general architectural quality attributes such as extensibility and scalability. A selection of security services as described in 7.12.1 to 7.12.5 need to be combined, depending on the individual utilities situation and requirements.

Figure 120 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.

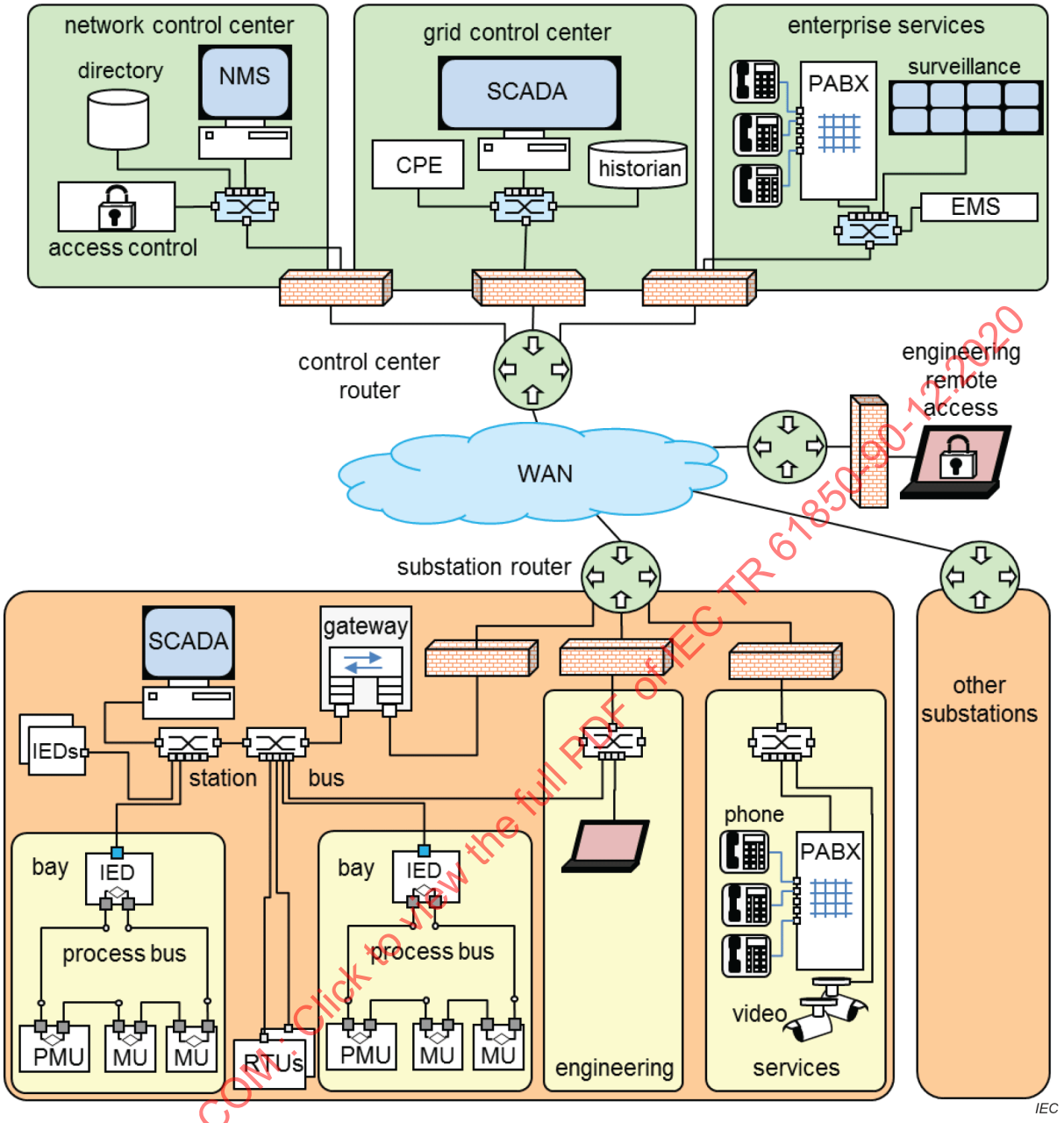


Figure 120 – Security architecture (using segmentation and perimeter security)

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 56 lists the parts of IEC 62351 with a brief overview of the content.

IPsec and TLS/DTLS provide the foundation for many secure tunnelling 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 56 – IEC 62351 series

Part	Content
IEC TS 62351-1:2007	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 62351-2:2008	Glossary – contains key terms and definitions used in the scope of IEC 62351
IEC 62351-3:2014/AMD1:2018	Profiles including TCP/IP – applies to: (IEC 60870-6 TASE.2, IEC 61850 over MMS, IEC 60870-5-104 & 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 62351-4:2007	Profiles including MMS – applies to: (IEC 60870-6 TASE.2, IEC 61850 over MMS)
IEC TS 62351-5:2013	IEC 60870-5 & Derivatives – applies to: (IEC 60870-5-104 & DNP3, IEC 60870-5-101,102,103 & Serial DNP)
IEC TS 62351-6:2007	Security for IEC 61850 – applies to: (IEC 61850 over MMS, IEC 61850 GOOSE, SMV)
IEC 62351-7:2017	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 62351-8:2011	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 62351-9:2017	Cyber security key management for power system equipment
IEC TR 62351-10:2012	Security architecture guidelines – describes guidelines for the security power systems based on essential security controls
IEC 62351-11:2016	Security for XML files
IEC TR 62351-12:2016	Resilience and security recommendations for power systems with DER
IEC TR 62351-13:2016	Guidelines on security topics to be covered in standards and specifications
IEC TR 62351-90-1:2018	Guidelines for handling role-based access control in power systems
IEC TR 62351-90-2:2017	Deep Packet Inspection (DPI) of encrypted communications (draft)
IEC TS 62351-100-1:2018	Conformance test cases for IEC TS 62351-5 and IEC TS 60870-5-7 (draft)
IEC TS 62351-100-3:2018	Conformance test cases for IEC 62351-3, the secure communication extension for profiles including TCP/IP (draft)

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 62351-6:2007 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 PTP) – 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 communications 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 network technology used; 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 57. 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 (if the service crosses 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 57 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 57 – 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 61850-90-5 (SS-CC)	5	EF, CS5
Streaming	IP telephony, video surveillance	4	AF41, AF42, AF43, CS4
Operation	SCADA, DNP-3, IEC 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 121 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 Ethernet or IP traffic, including IEC 61850, legacy and other traffic. The proxy-gateway sends the 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 Ethernet or 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 tunnelled 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.

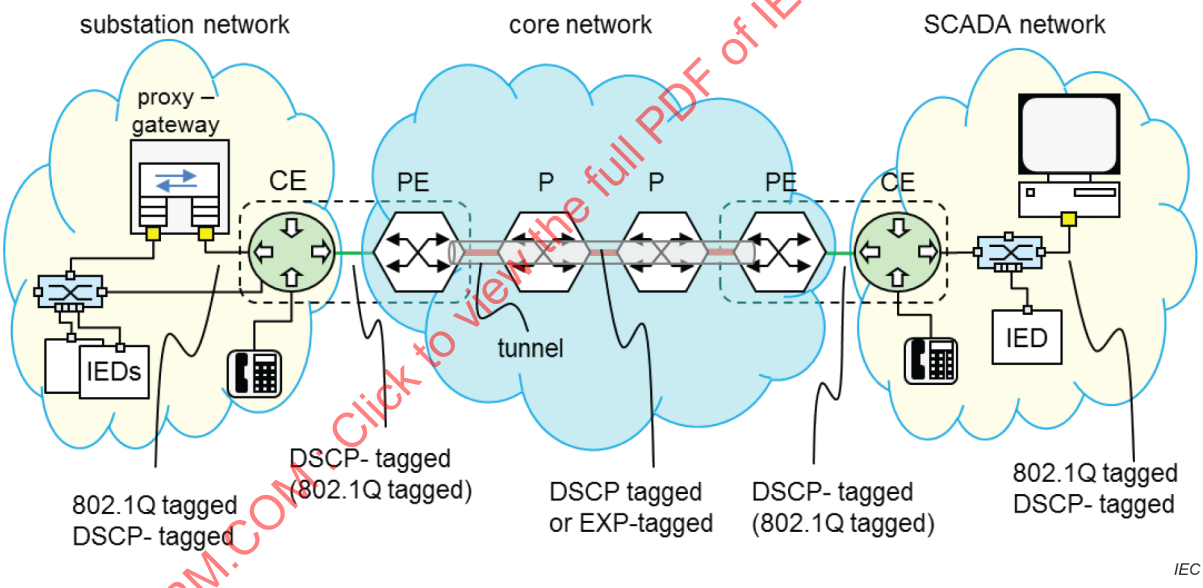


Figure 121 – QoS chain

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 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 57.

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 57.

7.13.7.3 PE-router engineering

At the entry of the core network, the PE-router in Figure 121 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 necessarily 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 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:

- 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;
- 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 Table 58 shows.

Table 58 – Typical oscillator stability

Type	Abbreviation	Suited for stratum (ANSI T1.101)[1)]	Drift (free-running)[2)]	Conditions
Hydrogen maser	–	1 Time and frequency definition	-	laboratory
Caesium 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 ±1 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 6.2.4.2.

Figure 122 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 9.1.6.1.1)

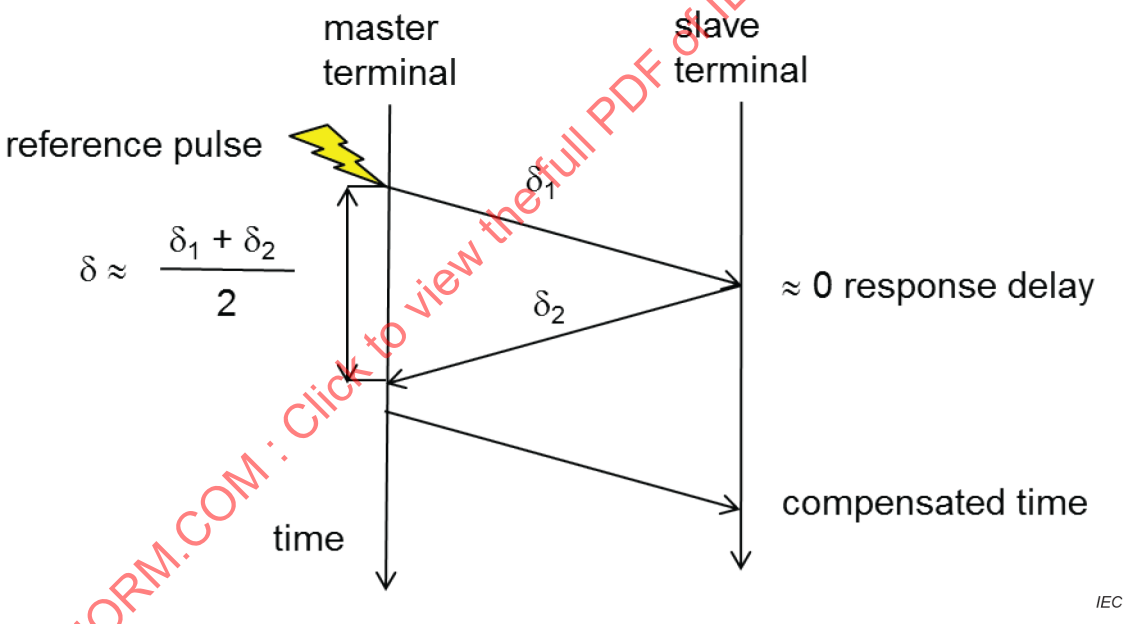


Figure 122 – Timing pulse transmission methods of legacy teleprotection devices

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 also allows distributing the time-of-day, also using a dedicated fibre. 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.