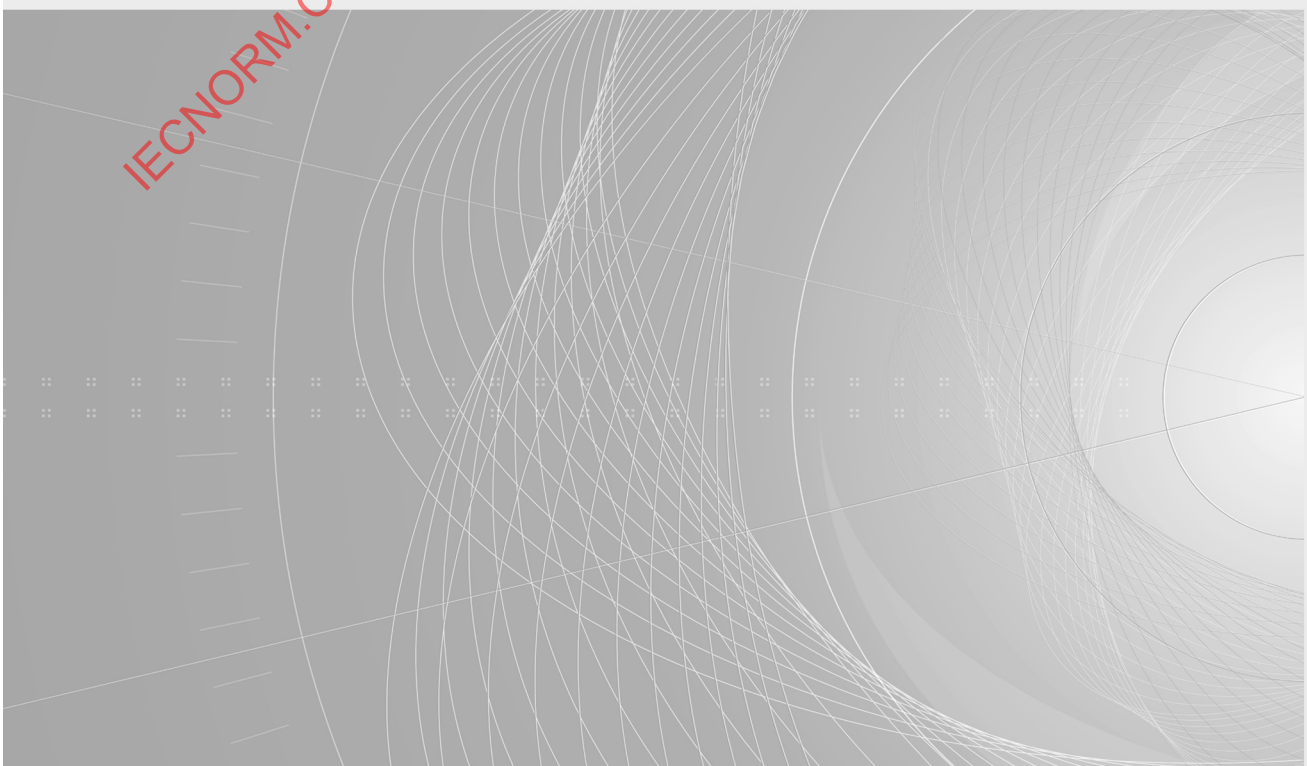
IEC TR 62357-200

Edition 1.0 2015-07

TECHNICAL REPORT

colour inside

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 TR 62357-200:2015-07(en)

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

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

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

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

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

IEC publications search - www.iec.ch/searchpub
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 It also gives information on projects, replaced and withdrawn publications.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 also once a month by email.

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

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

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

IEC TR 62357-200

Edition 1.0 2015-07

TECHNICAL REPORT

colour inside

Power systems management and associated information exchange – Part 200: Guidelines for migration from Internet Protocol version 4 (IPv4) to Internet Protocol version 6 (IPv6)

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 33.200

ISBN 978-2-8322-2795-4

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

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE –

Part 200: Guidelines for migration from Internet Protocol version 4 (IPv4) to Internet Protocol version 6 (IPv6)

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 62357-200, which is a technical report, has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

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

Enquiry draft	Report on voting
57/1563/DTR	57/1580/RVC

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

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

A list of all parts in the IEC 62357 series, published under the general title *Power systems management and associated information exchange*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC website under "http://webstore.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.

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

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

INTRODUCTION

This Technical Report provides definitions, guidelines, and recommendations for migration of data communication protocols which are today using the Internet Protocol version 4 (IPv4) to the Internet Protocol version 6 (IPv6).

This Technical Report addresses data communication for power systems at all voltage levels, from transmission level down to the low voltage. It is in addition useful for any other application domain which specifies the use of IP transport.

This Technical Report starts with a tutorial on the aspects of IPv4 and IPv6 technologies that are relevant for the migration.

This Technical Report addresses issues such as motivation for migration, migration strategies in general and specific application in power systems communications.

This Technical Report contains recommendations for the device manufacturers, network engineers and for standardization bodies.

This Technical Report defines a time table for the standard bodies defining data communication in power systems, as follows:

- All new or revised IEC documents support IPv6 as an option for projects that mandate it, starting in 2015.
- All IEC documents request both IPv6 and IPv4 support, while use is not mandatory, until 2030.
- All IEC documents consider IPv4 as deprecated after 2050.

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE –

Part 200: Guidelines for migration from Internet Protocol version 4 (IPv4) to Internet Protocol version 6 (IPv6)

1 Scope

This part of IEC 62357, which is a Technical Report, applies to information exchange in power systems including, but not restricted to, substations, control centre, maintenance centre, energy management systems, synchrophasor-based grid stability systems, bulk energy generation (including fossil fuel plants), distributed energy generation (renewables, wind and solar), energy storage, load management (demand side management and demand response for distribution level consumers or producers).

This Technical Report addresses the issues encountered when migrating from Internet Protocol version 4 (IPv4) to the Internet Protocol version 6 (IPv6). It describes migration strategies, covering impact on applications, communication stack, network nodes, configuration, address allocation, cyber security and the related management.

This Technical Report considers backward compatibility and show concepts as well as necessary migration paths to IPv6 from IPv4 where necessary, for a number of protocols in the IEC 61850 framework.

Following a review of IEC standards and technical reports according to the reference architecture for power system information exchange (IEC 62357-1), this Technical Report supports modifications caused by the introduction of IPv6 for revision of these documents, considering the impact of permitting or requiring IPv6.

This Technical Report does not impose the use of the IPv6 technology in utility communications.

2 Normative references

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

IEC 60050 (all parts), *International electrotechnical vocabulary (available at: <http://www.electropedia.org/>)*

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

IEC 61850-6:2009, *Communication networks and systems for power utility automation – Part 6: Configuration description language for communication in electrical substations related to IEDs*

IEC 61850-8-1:2011, *Communication networks and systems for power utility automation – Part 8-1: Specific communication service mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3*

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

IEC 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, *Communication networks and systems for power utility automation – Part 90-2: Using IEC 61850 for the communication between substations and control centres*[1]

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

IEC TR 61850-90-5, *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 TR 61850-90-12, *Communication networks and systems for power utility automation – Part 90-12: Wide area network engineering guidelines*

IEC 62351 (all parts), *Power systems management and associated information exchange – Data and communications security*

ISO 9506-1, *Industrial automation systems – Manufacturing message specification – Part 1: Service definition*

ISO 9506-2, *Industrial automation systems – Manufacturing message specification – Part 2: Protocol Specification*

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

IEEE 1815, *IEEE Standard for Electric Power – Systems Communications – Distributed Network Protocol (DNP3)*

RFC 0768, *User Datagram Protocol*

RFC 0791, *Internet Protocol (IPv4)*

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

RFC 0793, *Transmission Control Protocol, Protocol Specification*

RFC 0826, *An Ethernet Address Resolution Protocol*

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

RFC 0959, *File Transfer Protocol (FTP)*

---

1 To be published.

RFC 1142, *OSI IS-IS Intra-domain Routing Protocol",* February 1990

RFC 1191, *Path MTU Discovery*

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

RFC 1305, *Network Time Protocol (Version 3)*

RFC 1918, *Address Allocation for Private Internet*

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

RFC 2131, *Dynamic Host Configuration Protocol (DHCPv4)*

RFC 2147, *TCP and UDP over IPv6 Jumbograms*

RFC 2401, *IPsec*

RFC 2328, *OSPF Version 2*

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

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

RFC 2473, *Generic Packet Tunneling in IPv6 Specification*

RFC 2529, *Transmission of IPv6 over IPv4 Domains without Explicit Tunnels*

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

RFC 2766, *Network Address Translation – Protocol Translation (NAT-PT)*

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

RFC 3056, *Connection of IPv6 Domains via IPv4 Clouds (6to4)*

RFC 3315, *DHCP for IPv6 (DHCPv6)*

RFC 3416, *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*

RFC 3931, *IETF Network Working Group, Layer Two Tunneling Protocol – Version 3 (L2TPv3)*

RFC 4038, *Application Aspects of IPv6 Transition*

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 4302, *IP Authentication Header*

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

RFC 4380, Teredo: *Tunneling IPv6 over UDP through Network Address Translators (NATs)*

RFC 4443, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*

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

RFC 4554, *Use of VLANs for IPv4-IPv6 Coexistence in Enterprise Networks*

RFC 4632, *Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan*

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

RFC 4919, *IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)*

RFC 4944, *Transmission of IPv6 Packets over IEEE 802.15.4 Networks*

RFC 4966, *Reasons to Move the Network Address Translator – Protocol Translator (NAT-PT) to Historic Status*

RFC 5214, *Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)*

RFC 5569, *IPv6 Rapid Deployment on IPv4 Infrastructures (6rd)*

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

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

RFC 5905, *Network Time Protocol Version 4: Protocol and Algorithms Specification*

RFC 5942, *IPv6 Subnet Model: The Relationship between Links and Subnet Prefixes*

RFC 5952, *A Recommendation for IPv6 Address Text Representation*

RFC 5991, *Teredo Security Updates (Updates RFC 4380)*

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

RFC 6081, *Teredo Extensions*

RFC 6144, *Framework for IPv4/IPv6 Translation (NATs after RFC 4966)*

RFC 6145, *IP/ICMP Translation Algorithm*

RFC 6146, *Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers*

RFC 6282, *Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks*

RFC 6333, *Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion*

RFC 6535, *Dual-Stack Hosts using the "Bump-in-the-Host" Technique (BIH)*

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

RFC 6775, *Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)*

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

RFC 7059, *A comparison of IPv6-over-IPv4 Tunnel Mechanisms.*

RFC 7230, *Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing*

3 Terms, definitions, abbreviated terms, acronyms and conventions

3.1 Terms and definitions

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

3.1.1
application-level gateway
network device that converts the application payload received over a first protocol into an application payload over a second protocol, using application knowledge of the transmitted information

3.1.2
bridge
network device that connects network segments at the data link layer (Layer 2) of the OSI model

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

3.1.3
decapsulation
extraction of the data elements belonging to a first network protocol from a second network protocol used to transport the first protocol

3.1.4
DHCP server
network server that assigns an IP address to a host for a given period of time (lease)

3.1.5
domain name server
DNS
network server that resolves the IP address given the unique resource location (URL) of a communication partner

3.1.6
encapsulation
embedding of the data elements belonging to a first network protocol into a second network protocol that is used to transport it

3.1.7
host
network node aware of the IP protocol

3.1.8
public address
globally administrated, unique address

3.1.9
private address
locally administrated address that can be reused in another, separate network

3.1.10
router
network device that connects network segments at the network layer (Layer 3) of the OSI model

3.1.11
translation
process of converting a first protocol into a second protocol such that both partners are unaware of the other protocol

3.1.12
translator
device that translates the packets from one protocol into another protocol without using additional information from the communicating partners

3.1.13
transport-level gateway
network device that converts the payload received over a first protocol into a second protocol, using transport knowledge of the transmitted information

3.1.14
tunneling
transport of packet between two entities using a first protocol over a second protocol.

3.1.15
tunneler
device at each end of a tunnel that encapsulates /decapsulates the packets

3.2 Abbreviations

6LoWPAN	IPv6 over Low power Wireless Personal Area Network (RFC 4919)
A-record	32-bit IPv4 address record from DNS
AAAA	128-bit IPv6 address record from DNS
ALG	Application-Level Gateway
API	Application Programming Interface
AH	Authentication Header (RFC 4302)
ARP	Address Resolution Protocol (RFC 0826)
AS	Autonomous System
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol (successor of EGP in Internet)
BIH	Bump In the Host (RFC 6535)
CIDR	Classless Inter-domain Routing (RFC 4632)
CPE	Customer Premise Equipment (any terminal in the subscriber location)
DER	Distributed Energy and Renewable energy
DF	Don't Fragment bit (IPv4)

DMZ	DeMilitarized Zone
DNP3	Distributed Network Protocol version 3 (IEEE 1815)
DNS	Domain Name Server
DHCP	Dynamic Host Configuration Protocol
DHCPv4	DHCP version 4 (RFC 2131)
DHCPv6	DHCP version 6 (RFC 3315)
ESP	Encapsulating Security Payload (RFC 4303)
EUI-64	Extended Unique Identifier (IEEE Registration Authority)
FTP	File Transfer Protocol (RFC 0959)
GOOSE	Generic Object Oriented Substation Events (IEC 61850-8-1)
HTTP	Hypertext Transfer Protocol (HTTP) (RFC 7230)
HSR	High-availability Seamless Redundancy (IEC 62439-3)
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol (RFC 0792)
ICMPv4	ICMP version 4 (RFC 0792)
ICMPv6	ICMP version 6 (RFC 4443)
ID	IDentification
IGP	Interior Gateway Protocol
IED	Intelligent Electronic Device (IEC 61850)
IETF	Internet Engineering Task Force
IP	Internet Protocol (RFC 0791)
IPv4	Internet Protocol Version 4 (RFC 0791)
IPv6	Internet Protocol Version 6 (RFC 2460)
IPsec	Internet Protocol network layer security (RFC 2401)
IS-IS	Intermediate System to Intermediate System (RFC 1142, ISO/OSI 8473)
ISP	Internet Services Provider
LAN	Local Area Network
L2TP	Layer 2 Tunneling Protocol (RFC 3931)
LLDP	Link Layer Discovery Protocol (IEEE 802.1AB)
MAC	Medium Access Control (IEEE 802.1)
MF	More Fragment (IPv4)
MMS	Manufacturing Messaging Specification (ISO 9506)
MPLS	Multi-Protocol Label Switching
MTU	Maximum Transmission Unit (RFC 0791, RFC 2460)
NAT	Network Address Translation (RFC 3022)
NDP	Neighbor Discover Protocol (RFC 4861)
NERC	North-american Electricity Reliability Corporation (USA)
NIST	National Institute of Standards and Technology (USA)
NPDU	Network Protocol Data Unit (ISO/OSI)
NTP	Network Timing Protocol (RFC 1305)
OMB	Office of Management and Budget (USA)
OSI	Open Systems Interconnection (ISO)
OSPF	Open Shortest Path First (RFC 2328)

OSPFv4	OSPF version 4 (RFC 2328)
OSPFv6	OSPF version 4 (RFC 5340)
PDU	Protocol Data Unit (ISO/OSI)
PRP	Parallel Redundancy Protocol (IEC 62439-3)
PTP	Precision Time Protocol (IEC 61588)
RIR	Regional Internet Registry
RPL	Routing Protocol for Low-power and lossy networks (RFC 6550)
RTU	Remote Terminal Unit
SCADA	Supervisory Control And Data Acquisition
SCD	System Configuration Description (IEC 61850-6)
SCL	System Configuration Language (IEC 61850-6)
SDH	Synchronous Digital Hierarchy (ITU-T)
SED	System Exchange Description (IEC 61850-6)
SIIT	Stateless IP/ICMP Translation algorithm (RFC 6145)
SLAAC	StateLess Address AutoConfiguration (RFC 4862)
SNMP	Simple Network Management Protocol (RFC 3416)
SNTP	Simple Network Time Protocol (RFC 5905)
SONET	Synchronous Optical NETwork
SMV	Sampled Measurement Values (IEC 61850)
TCP	Transmission Control Protocol (RFC 0793)
UDP	User Datagram Protocol (RFC 0768)
ULA	Unique Local unicast Address (IPv6)
URL	Uniform Resource Locator (RFC 3986)
USGv6	United States Government internet protocol version 6 initiative (NIST)
VID	VLAN ID (IEEE 802.1Q)
VLAN	Virtual Local Area Network (IEEE 802.1Q)
VLL	Virtual Leased Line
VPN	Virtual Private Network
WAN	Wide Area Network
XML	eXtended Markup Language
XMPP	eXtensible Message and Presence Protocol (RFC 3921)

3.3 Conventions

3.4 Network diagram symbols

This Technical Report uses the symbols shown in Figure 1 in an effort to provide diagrammatic consistency. Combinations of these symbols create symbols that are more complex.

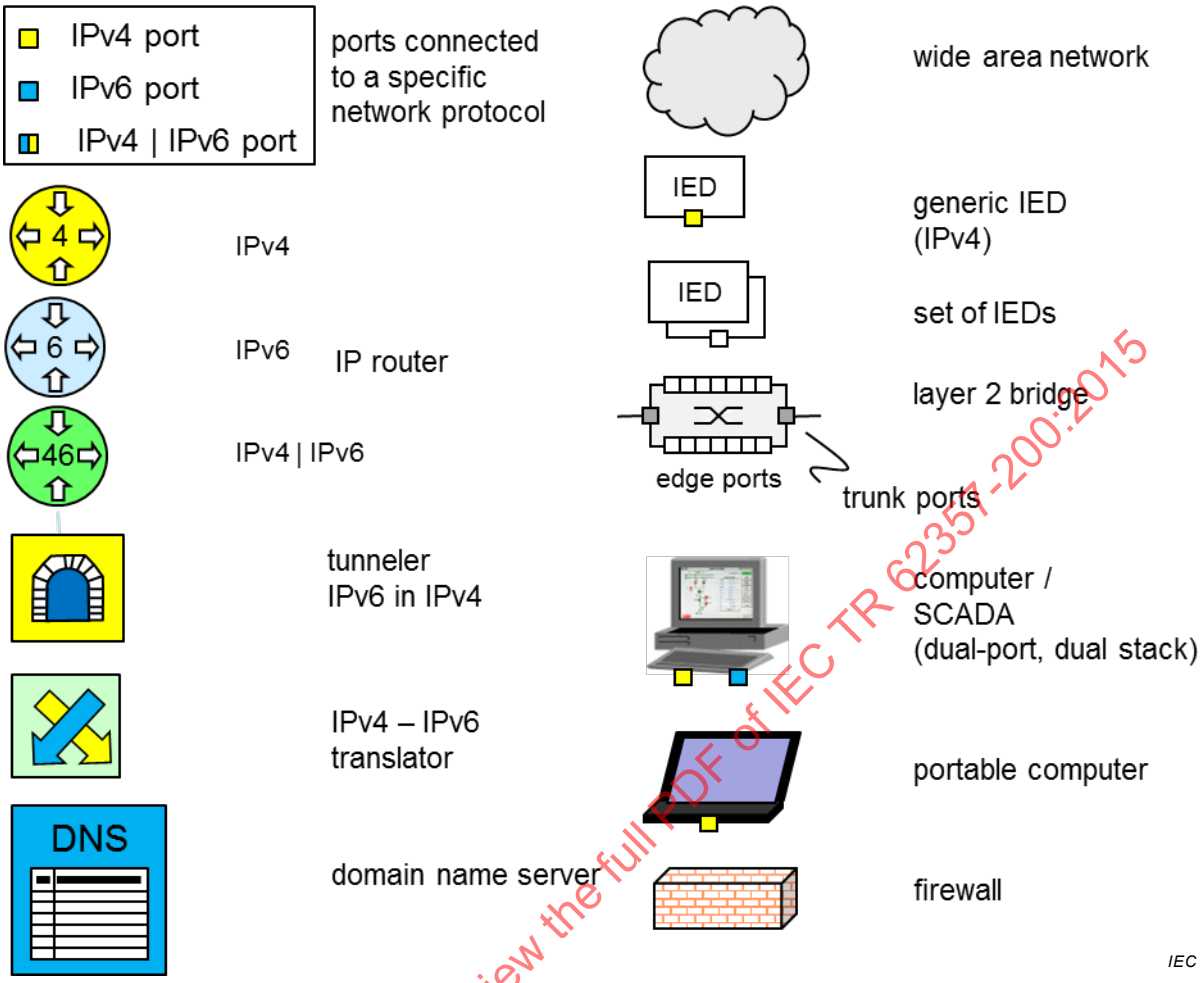


Figure 1 – Symbols

4 Internet technologies

NOTE This Clause has been copied from IEC TR 61850-90-12, to provide a self-contained document. It will not be maintained in future versions of this document.

4.1 Internet Protocol Version 4 (IPv4)

4.1.1 Origin

The Internet Protocol version 4 (IPv4) (RFC 0791) has been the base for the Internet since 1980 and is still the most widely used network protocol in 2015. Its main characteristics are:

- IPv4 is connectionless, i.e. routers retain no knowledge of previous messages;
- IPv4 operates with 32-bit network source and destination address;
- IPv4 is supported by a suite of routing protocols.

4.1.2 IPv4 packet transmission over Ethernet

RFC 0894 defines the transmission of IPv4 packets in Ethernet frames. The Layer 3 header comes just after the Layer 2 header (see Figure 2).

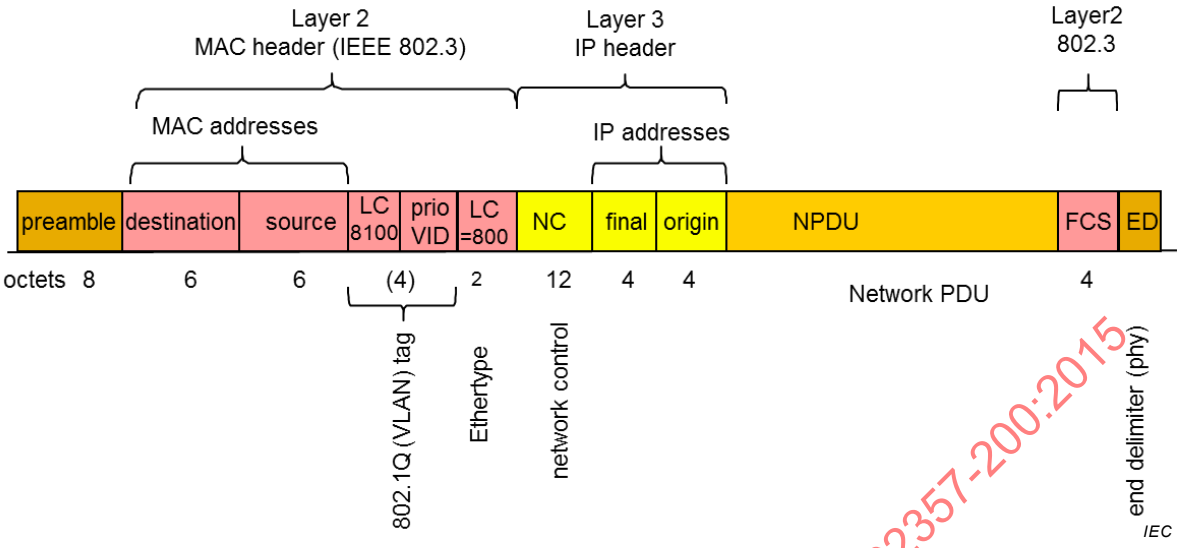


Figure 2 – Ethernet frame with IP network header

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

4.1.3 IPv4 header

The IPv4 network header carries the two 32-bit IP addresses and a protocol type indicating which kind of payload – called a Network Protocol Data Unit (NPDU) follows (see Figure 3).

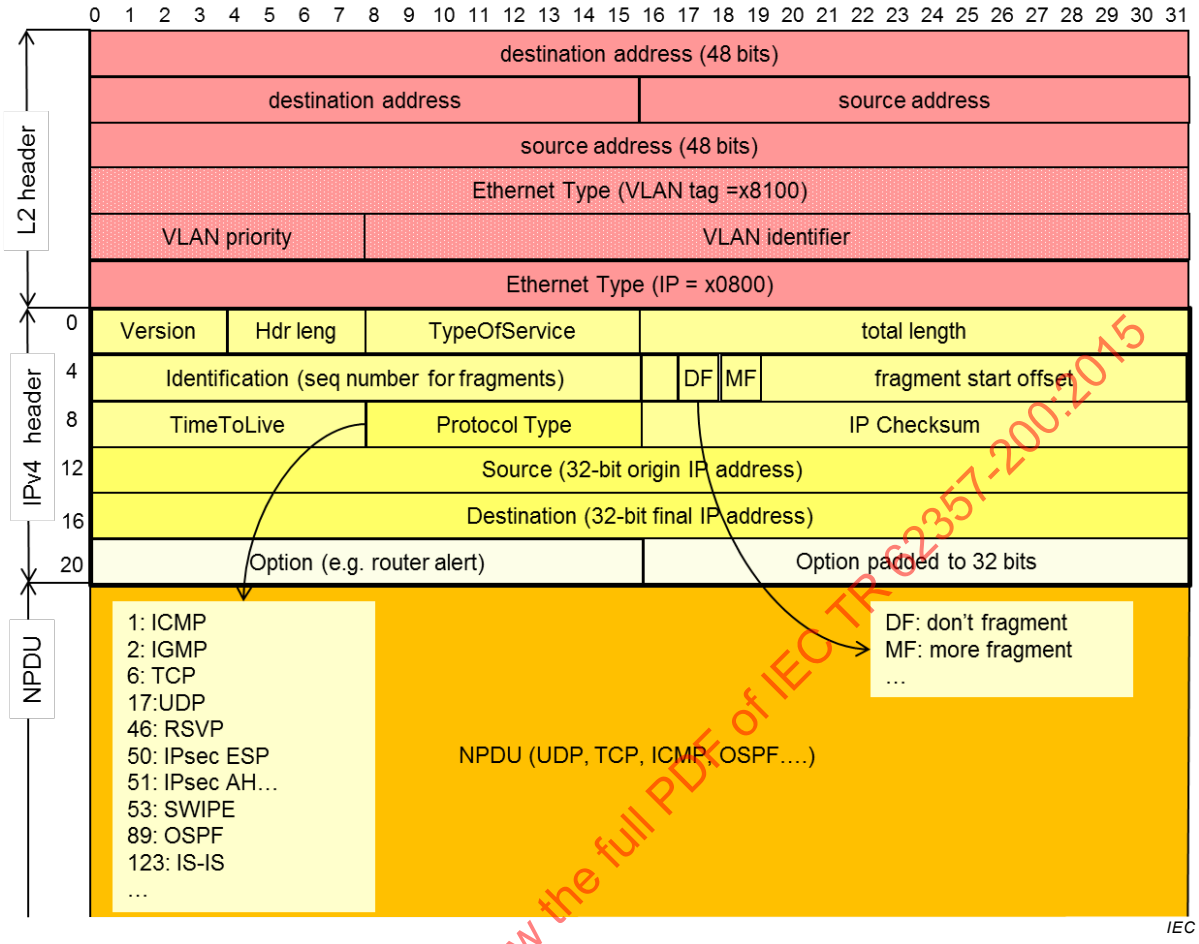


Figure 3 – Mapping of IPv4 header to Ethernet frames

4.1.4 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 1 "10.12.127.4" translates as "00001010'00001100'01111111'00001000"b.

The IP addresses are divided into a public address space (unique worldwide and administrated by the Internet Assigned Numbers Authority (IANA) through Regional Internet Registry (RIR) and a private address space (which can be reused, for instance be the same in different companies, industrial plants or internet service provider domains). RFC 1918 gives guidelines on the allocation of IPv4 addresses.

The public IPv4 addresses are exhausted (see 4.1.1), but this does not concern networks that operate with private addresses or that are separated from the public internet.

The router at the boundary of a private address subnet may translate from an internal to an external address or vice-versa as standardized in the Network Address Translation (NAT) (RFC 2663/RFC 3022). NAT allows at the same time to multiplex the IP addresses by the port identifiers in UDP and TCP traffic. NATs helped stretching the life of IPv4 by reusing addresses in private networks and translating them to public addresses.

The IPv4 addresses are structured into subnets, which are of varying size, as the Classless Inter-domain Routing (CIDR) (RFC 4632) defines.

EXAMPLE 2 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.

4.1.5 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 host may fragment if DF is not set, and if it cannot forward a received NPDU without fragmenting, it returns an error message through ICMP. The sending host must then reduce its MTU size until the other host accepts it. IPv4 hosts 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 packets over Ethernet use an MTU value of 1 500 octets.

More details are available in RFC 6864 and RFC 4459.

4.1.6 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 host to obtain the Layer 2 MAC addresses knowing the IPv4 address of the partner. To this effect, a host 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 a host asking about the presence of a remote host 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) allows a host asking the IP address of a remote host by submitting its Uniform Resource Locator (URL). 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.

4.1.7 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.

4.2 Internet Protocol Version 6 (IPv6)

4.2.1 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.

The address shortage does not immediately affect utility networks, since they have sufficient private addresses with IPv4 and tools and hardware should support IPv4 for a long time.

However, IETF will not support IPv4 anymore and network providers could stop support. It is therefore advisable to start the migration process the soonest possible.

4.2.2 IPv6 packets on Ethernet

RFC 2464 defines the transmission of IPv6 packets over Ethernet frames as Figure 4 shows.

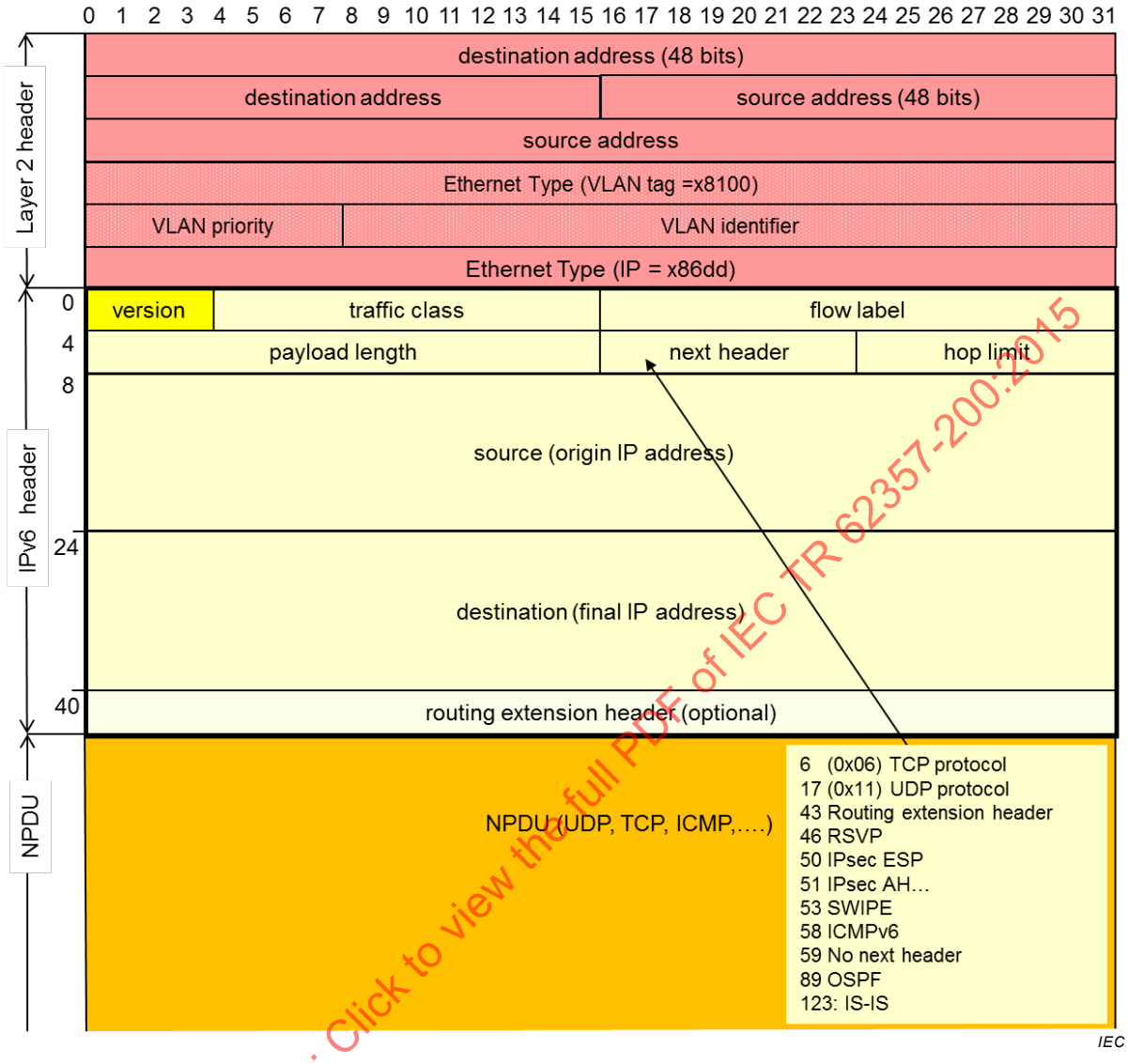


Figure 4 – Transmission of an IPv6 packet in an Ethernet frame

The Ethertype “0x86dd” identifies the IPv6 packets.

The IPv6 header has a fixed size of 40 octets. The only field retained from the previous IPv4 header is the Version Number. Extension headers allow appending parameters for routing, security, tunneling, etc.

This means that IPv4 and IPv6 are not compatible, but distinguishable through the Ethertype at Layer 2 and the Version Number at Layer 3.

4.2.3 IPv6 addresses

4.2.3.1 IPv6 address representation

RFC 4291 structures the human readable representation of IPv6 addresses in a different way from IPv4. Rather than using “dotted decimals”, it expresses the 128-bit addresses as eight groups of four hexadecimal (lowercase) digits, separated by colons.

EXAMPLE 1 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 it may occur at only one place in the address.

EXAMPLE 2 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 3 192.0.2.1 -> 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.

4.2.3.2 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 5).

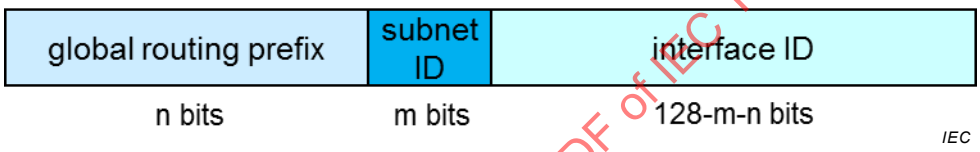


Figure 5 – IPv6 unicast address structure

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.

4.2.3.3 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”.

4.2.3.4 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 6):

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

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

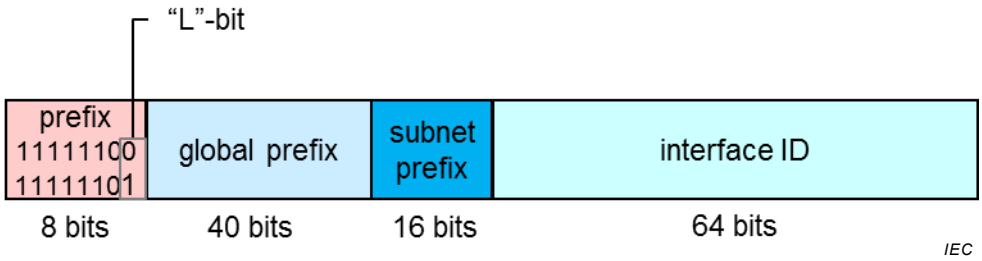


Figure 6 – IPv6 ULA address structure

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.

4.2.3.5 IPv6 local addresses

The link-local IPv6 address (Figure 7) has a prefix of fe80::/10 according to RFC 4291.

Figure 7 – IPv6 link local address structure

Link-local addresses are for use on a single link, they are not routable.

4.2.4 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 at the same level as UDP or TCP.
- Neighbor Discovery Protocol for IPv6 (NDPv6) (RFC 4861) provides StateLess Address AutoConfiguration (SLAAC). NDP replaces IPv4's ARP and ICMPv4 and it is part of ICMPv6.
- DHCPv6 (RFC 3315) and DHCPv6lite (RFC 3736) extend DHCP.
- Internet Protocol Security (IPsec) (RFC 2401) 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.

4.2.5 IPv6 fragmentation and packet size

IPv6 allows MTUs well in excess of the Ethernet frame size, called jumbograms (RFC 2147) on a hop-to-hop basis, but IEC TR 61850-90-5 rules them out.

The minimum frame that all IPv6 hosts must be capable to accept has a size of 1 280 octets.

IPv6 allows fragmentation only at hosts (including tunnelers), not at the intermediate routers as IPv4 does (RFC 4944).

IPv6 requests that a host be 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 hosts will not agree on an MTU that is smaller than 1 280 octets.

4.2.6 IPv6 routing

IPv6 uses the same protocols as IPv4 for routing, for example OSPF or IS-IS, adapted for IPv6.

4.3 Comparison IPv4 and IPv6

4.3.1 Main differences

Table 1 summarizes the main differences between IPv4 and IPv6:

Table 1 – 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)

4.3.2 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 NATs extend IPv4 addresses by including the port addresses, but this works only for TCP and UDP (nevertheless nearly all Internet traffic).

Table 2 compares the addresses in IPv4 and IPv6.

Table 2 – 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)

4.3.3 Address representation in IEC 61850

The System 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) as the following example shows:

```
<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>
```

5 Transition from IPv4 to IPv6

5.1 IPv6 migration necessity

Due to the exhaustion of the 32-bit IPv4 addresses, the public Internet is moving towards IPv6, which offers a practically unlimited address space of 128 bits.

IPv6 is growing rapidly and most new devices support it. A large number of servers still operate with IPv4.

Figure 8 shows the probable evolution of the IPv6 traffic in the public internet. Around the year 2030, there should be only a few IPv4-only nodes around, many of them in private networks.

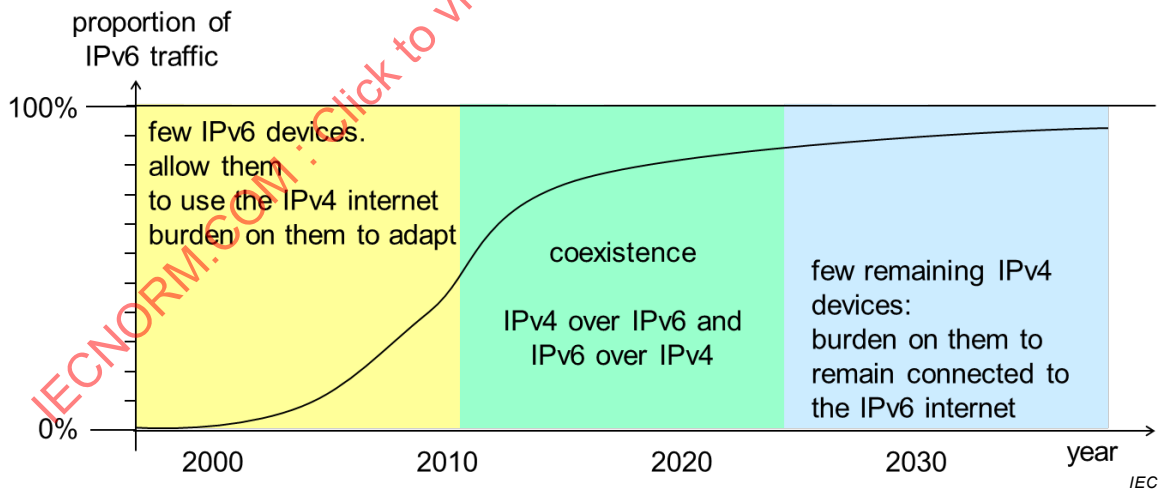


Figure 8 – IPv6 evolution

5.2 Migration types

IETF devised migrations strategies (RFC 4213).

Two different migrations are considered:

a) application migration:

applications currently written for IPv4 are migrated to IPv6, while possibly preserving compatibility with IPv4 devices. Examples are engineering tools, debug and traffic monitoring tools, telecontrol applications. This involves reprogramming and re-engineering of devices while preserving the application code.

b) device and system migration:

- new IPv6 devices must be able to operate over the IPv4 infrastructure;
- installed IPv4 devices, including routers, must be able to interoperate with IPv6 devices;
- installed IPv6 devices must not disturb the operation of already installed IPv4 devices;
- new devices should access both IPv4 and IPv6 devices (dual-stack);
- IPv4-only devices must be accessible over an IPv6-only network (tunnel or translator).

5.3 IPv6 migration impact on power systems communications

For power systems communications, the urgency of migrating to IPv6 depends on the application.

- within a substation, there is no exhaustion of addresses since substations use only private IPv4 addresses, as IEC TR 61850-90-4 describes;
- substation-to-substation communications and substation to control centre communications only need private IPv4 addresses (and possibly other communication means than IP) since they remain on a utility-managed network;
- maintenance access to devices in the substation will most likely take place over a Virtual Private Network that uses only private addresses and needs only a few public addresses to access the VPN edge device;
- control centres need access to market and weather information that is increasingly available only over IPv6;
- distributed energy networks can use and reuse private IP addresses, since their network is under control of the DSO;
- smart metering, distributed generation, demand side management, electric vehicles, etc. will need a larger address space and other services offered by IPv6, they are using IPv6 already today;
- sensor devices such as 6LowPan are IPv6-only.

Although power systems communications do not depend on IPv6, a migration should be prepared since:

- technology evolution will phase out IPv4 and the burden of maintaining IPv4 alive will remain with the utilities after 2025 to 2035, i.e. well within electrical equipment lifetime;
- all new developments in IETF will be based on IPv6, IPv4 will be ignored;
- operating system and router manufacturers could start to increase price to support IPv4 or discontinue support at a specific date;
- maintaining dual-stack devices will be costly, especially when the number of IPv4 devices is low;
- personal will lack training in IPv4 and will tend to consider this protocol as a potential source of insecurity;
- parts of the Smart Grid will operate with IPv6 and parts with IPv4, requiring a conversion or tunneling at every border;
- government regulations (USGv6, OMB, NIST, NERC, etc.) require using IPv6.

Therefore, a migration strategy should be devised already today so that a future transition needs less effort.

The migration strategy must in the first place respect the installed IPv4 base (and those installed until migration starts). Indeed, the installed base of IEC 61850 with IPv4 will continue to increase before an IPv6 migration becomes necessary.

At the same time, migration to IPv6 is an opportunity to address other issues.

The IPv4 – IPv6 migration is not an easy endeavor and needs careful planning.

6 Migration methods

6.1 Migration principles

A large number of legacy IPv4 devices will need communication with IPv6 devices. The first hurdle is the difference in size of the IP addresses. The second hurdle is how to map one address into another.

RFC 6144 defined about a dozen of IPv6 transition mechanism. These transitions mechanisms aim primarily at introducing the IPv6 protocol into existing IPv4 networks, but do not intend to preserve the operation of IPv4 once IPv6 is widely introduced.

RFC 4213 defined three basic transition strategies:

1) Dual-stack devices
2) Tunneling
3) Translation

6.2 Address mapping

6.2.1 Address mapping from IPv4 to IPv6

IPv4 did not foresee any mechanism to increase the address size (neither does IPv6). This makes the handling of the different address sizes a difficult issue in the migration from IPv4 to IPv6.

RFC 6052 defines several mappings from IPv4 to IPv6, but SIIT (RFC 6145) recommends to use "::ffff:0:0/96" (bottom address in Figure 9).

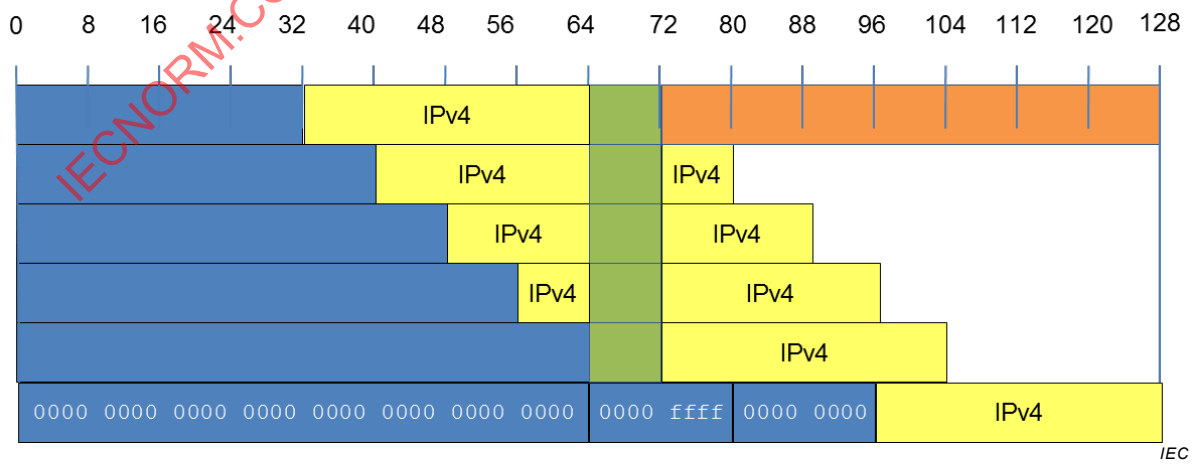


Figure 9 – Mapping of IPv4 to IPv6 addresses

However, 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
```

This checksum neutral address is only useful in the case of translators, to avoid recomputing the checksums. It is not useful when the former IPv4 address should become the least significant part of an IPv6 address.

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.

6.2.2 General application impact of IPv6 addresses

Applications that currently operate with IPv4 addresses should be migrated to IPv6 with as little modification as possible. Although applications should be independent of IP addresses, this is not stringent. The larger IPv6 address needs consideration just because of its larger size.

Examples:

- size of the display for the entry of IP addresses and netmask;
- representation of IP addresses in programs: from Int32 to Array [4] [2] of Int32 (today’s processors easily handle 32-bit, but do not support 128-bit arithmetic);
- size of tables and memory requirements;
- use of hard coded addresses (e.g. 127.0.0.1, “localhost”);
- handling of AAAA-records (IPv6 address) received from a domain name server;
- network service calls such as getnameinfo / getaddrinfo.

RFC 4038 makes recommendations on how to detect potential problems in the existing code.

6.2.3 Address migration in IEC 61850

6.2.3.1 General

In IEC 61850, the devices affected are not only the IEDs, but also all other application such as SCADA, engineering tools, debugging tools, network monitors, etc.

6.2.3.2 A proposal for IPv6 mapping in IEC 61850-8 and IEC TR 61850-90-4

All current substations use IPv4 private addresses belonging to the groups:

---

2 Numbers in square brackets refer to the bibliography.

10.xx.xx.xx /8,
172.32.xx.xx /11,
192.168.xx.xx /16

To remain non-routable over a public IPv6 network, these addresses should be mapped to IPv6 ULA addresses “fd00::/8” or “fc00/8” (conserving the checksum over the TCP/UDP pseudo-header).

The IPv6 address space affects engineering of a network. The network partition becomes flexible, i.e., there are no subnet masks any more. The selection of prefixes replaces subnetting.

NOTE In substation automation, the established static assignment of IPv4 addresses based on the physical topography relative to a plant, as defined in IEC TR 61850-90-4 can be kept with IPv6, provided a suitable prefix is used before the topography suffix.

When the devices are IPv6-enabled, they no longer need NATs.

A utility can segment its private address space (ULAs) geographically for the operational network, for instance as:

<operational><region><substation><voltage level><bay><IED>

The IPv6 address plan is related to the network part of the addresses (64 most significant bits). The host part is always 64 bit long. There is no address plan defined for the host part.

The amount of bits for the least significant part of the network address part can be identical to that of IPv4 address 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 (carrying e.g. email, file transfer, etc.) can be segmented differently from the operational network (carrying teleprotection, telecontrol, SCADA, etc.)

6.2.3.3 Addresses in other power systems protocols

Neither IEC 61400-25 nor IEC 60870-5-104 define an address assignment scheme.

NOTE Other protocols have not been investigated.

6.2.3.4 Addresses in configuration and management

Some applications embed IPv4 addresses in the payload. This is already a problem with TCP, whose checksum includes the IP addresses. It becomes even more of an issue with versions of File Transfer Protocol (FTP) that carry the IPv4 address in the payload.

Any application protocol that conveys addresses is affected. This applies specially to the transmission of SCL files in IEC 61850 that may contain IPv4 addresses that the destination cannot use.

6.2.3.5 Addressing migration evaluation

Implementation	Cumbersome, as legacy source code needs inspection
Impact	All application software
Special devices	None
IPv6 benefits	Replace NAT by a router, end-to-end connectivity
Difficulties	Test and extended certification
Recommendation	Inspect all applications for IP-address dependencies and abstraction from IP-addresses in all software. Manufacturers should start already now to care about the IPv6 enabling of their products. To keep backward compatibility, parsers should accept uppercase characters in IPv6 addresses, but transform then to lowercase characters for further use.

6.3 Dual-stack devices

6.3.1 General

A dual-stack device has both an IPv4 stack and an IPv6 stack, as Figure 10 shows. Routers were the first devices to use a dual stack since they should route messages according to the IP version they receive.

In end devices, the choice of using one or the other is an application issue.

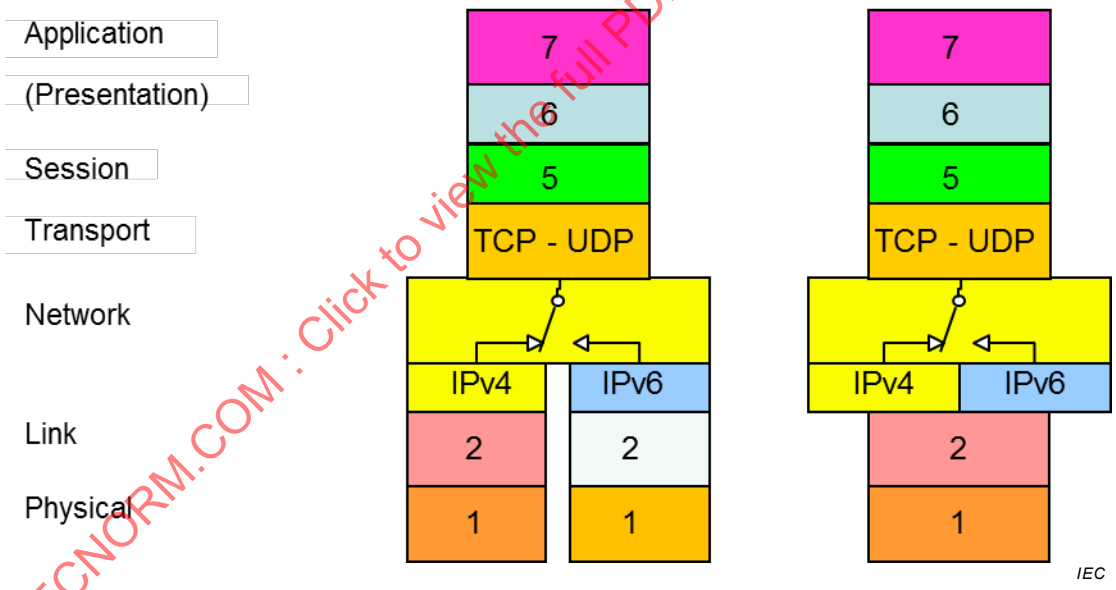


Figure 10 – Dual-Stack devices (with two and one port)

A dual-stack device has both an IPv4 address set and an IPv6 address set. The network layer uses the IPv4 or IPv6 connection depending on the address of the destination. Dual-stack applications can receive the correct IP address and protocol within a substation using preconfigured addresses obtained e.g. from the Substation Configuration Description (SCD) (IEC 61850-6) file (Figure 11).

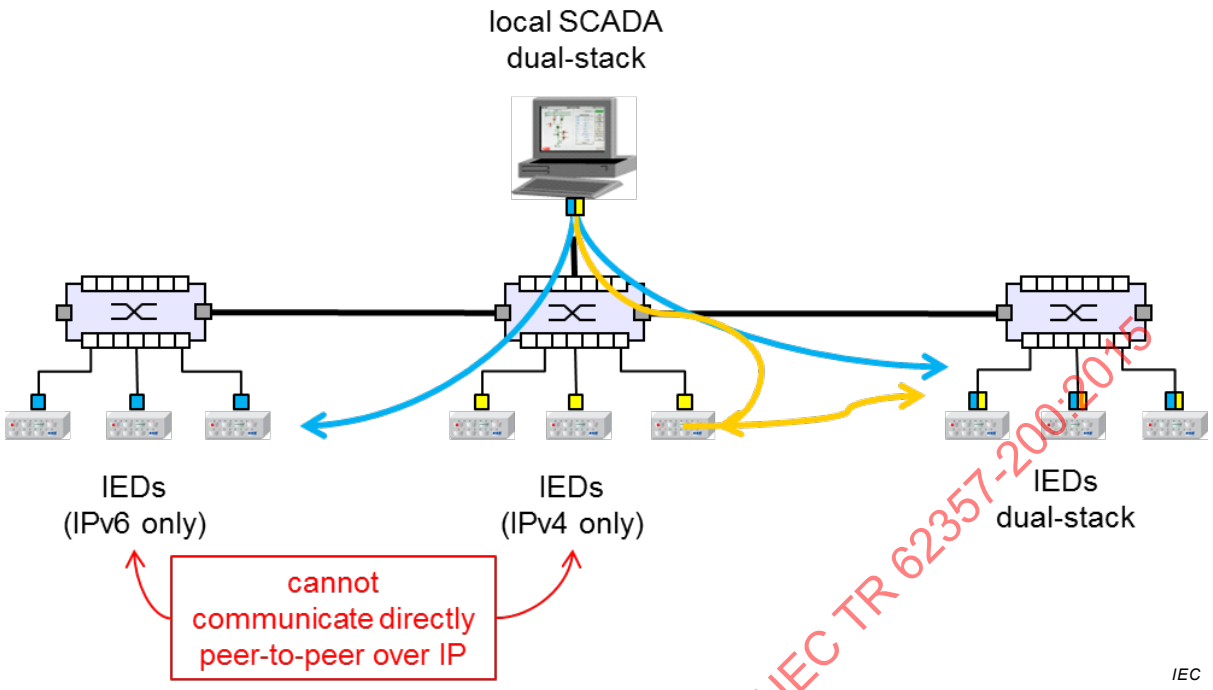


Figure 11 – Dual-Stack devices in a mixed domain

Dual-stack servers in a WAN could register to a DNS so the client knows over which interface to access them (Figure 12).

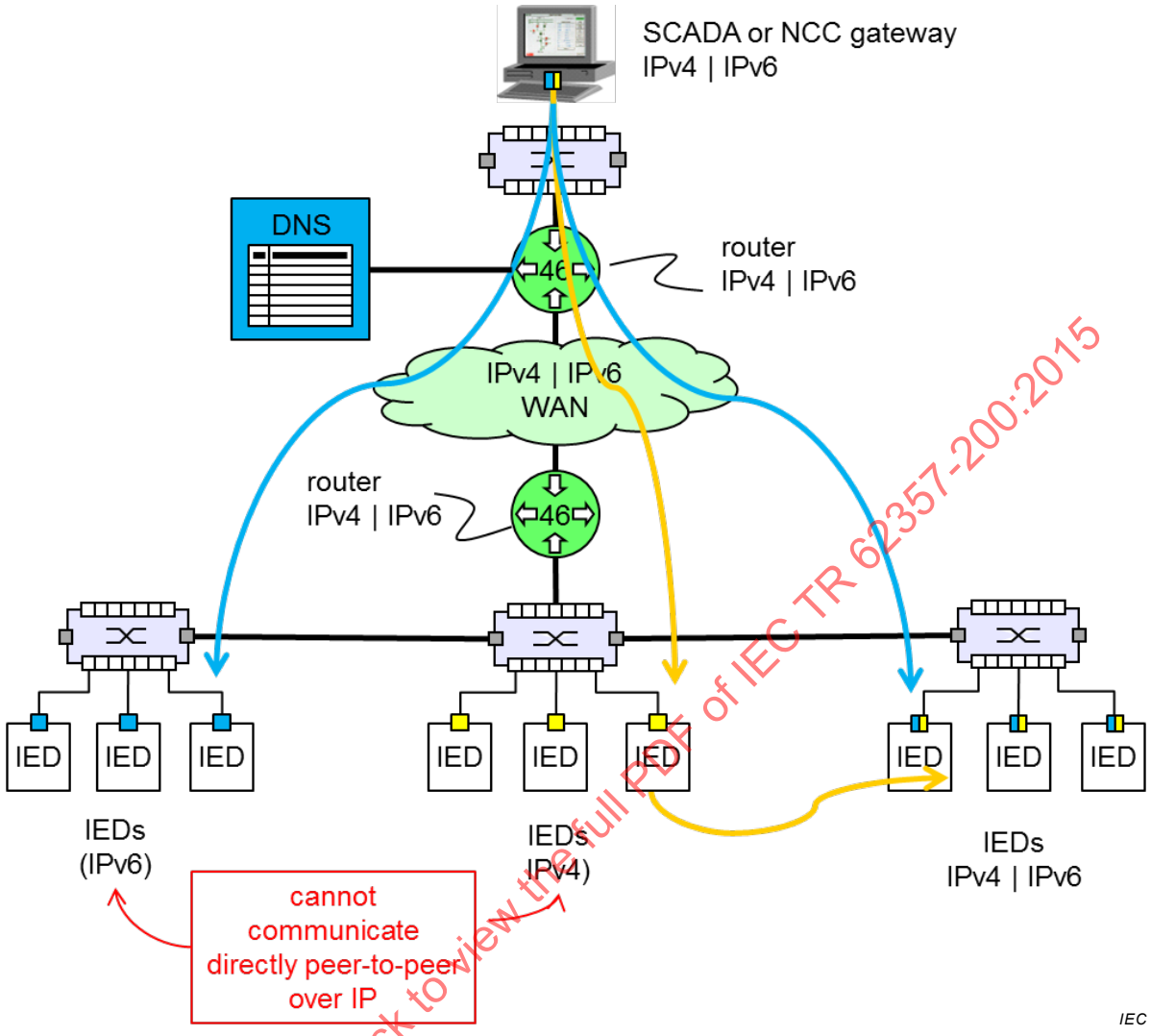


Figure 12 – Dual-Stack devices across routers

6.3.2 Standard dual-stack

Dual-Stack hosts use both IPv4 and IPv6 addresses.

IETF defined two dual-stack methods: Dual Stack and Dual-Stack Lite.

The "Dual-Stack Lite" (RFC 6333) mechanism uses routable, global IPv6 addresses. It uses only private IPv4-Addresses in the LAN of the client (similarly to a NAT). Instead of performing a NAT translation, the IPv4 are encapsulated into IPv6 packets in the Customer Premises Equipment (CPE). The CPE uses its global IPv6 addresses to transport the packets.

Using a DNS allows automating: the DNS responds with the IP address of the partner, which may be IPv4 (A-record) or IPv6 (AAAA-record). The dual-stack device uses the corresponding stack for the duration of the session. This method is useful for clients, such as personal computers or smartphones, but it is not recommended.

Table 3 compares the methods.

Table 3 – Dual-stack comparison

Method	Principle	Assumptions
Dual Stack	IPv4 and IPv6 are used in parallel	All interfaces have both an IPv4 and an IPv6 address; both stacks are independent.
Dual Stack Lite	Like Dual-Stack, but with global IPv6 and Carrier-NAT local IPv4 addresses	Although this should be the rule for all new devices, this method assumes that the whole path between devices is capable of dual-stack operation.

RFC 4554 (and [3]) informally propose to use Virtual Local Area Network (VLAN) tagging to segregate IPv4 and IPv6 devices. This is not necessary, since the Ethertype uniquely distinguishes IPv4 from IPv6 packets. VLANs serve to bundle and reduce traffic in parts of the network, as IEC TR 61850-90-4 recommends.

6.3.3 IEC 61850 stack with IPv4 and IPv6

Figure 13 shows the location of IPv4 and IPv6 in the IEC 61850 stack. In principle, the protocols on top of IPv4 or IPv6 should not be aware of the communication stack used and of the layers below IP (link layer, PRP, HSR) and in particular all hard real-time protocols (GOOSE, SMV, PTP) are not affected.

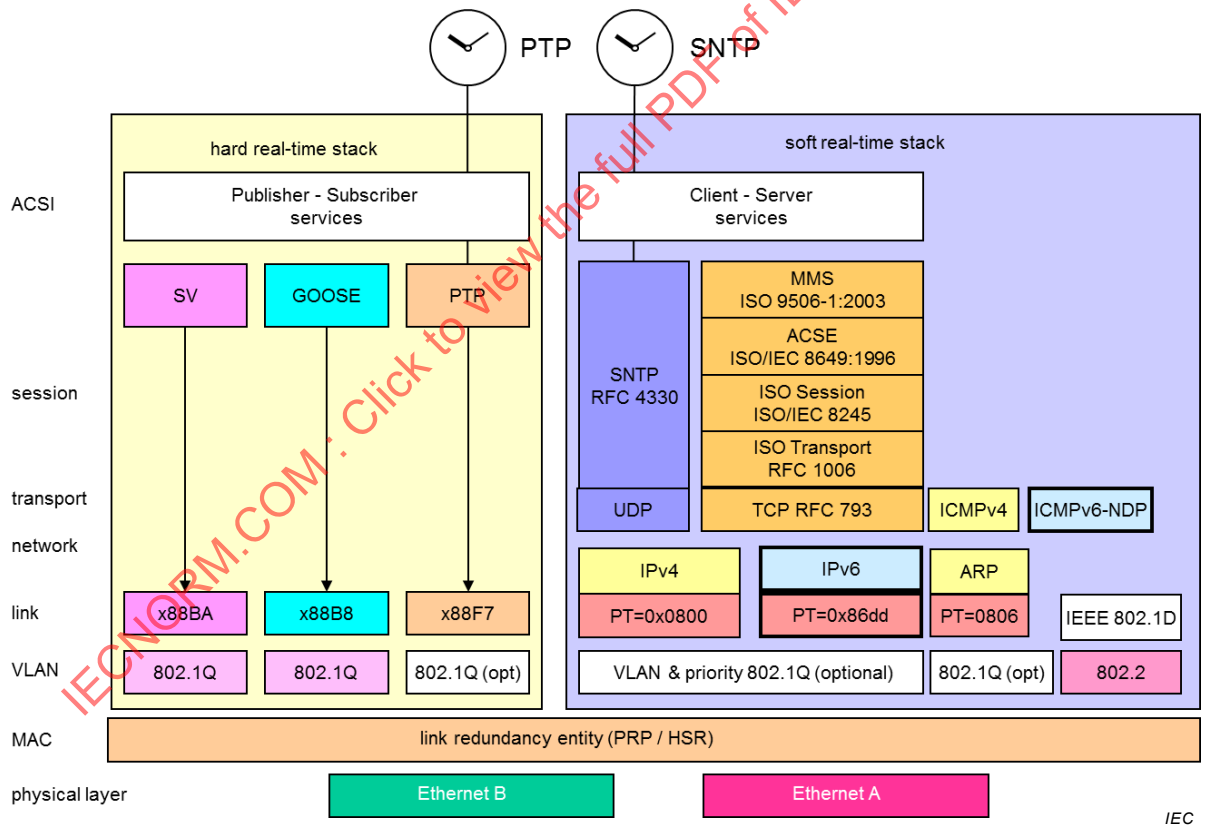


Figure 13 – IEC 61850 stack with IPv4 and IPv6 (doubly attached)

6.3.4 Migrating applications in dual-stack by Bump-in-the Host

The “Bump in the Host” (BIH) (RFC 6535) method allows migrating applications that are based on IPv4. BIH intercepts the IPv4 function calls at the Application Programming Interface (API) or socket level and directs them to IPv6 sockets using IPv6 addresses taken from a pool of IPv6 addresses to communicate with IPv6 hosts (see Figure 14).

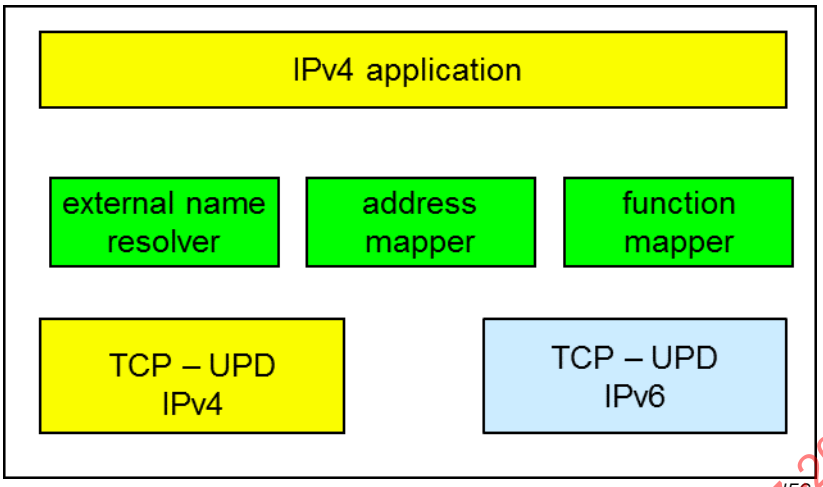


Figure 14 – Bump-in-the-host migration method

BIH obsoletes former methods such as “bump-in-the-stack” (RFC 2767) and “bump-in the-API" (RFC 3338).

However, applications that benefit from this method are restricted to those that:

– use DNS for address resolution;
– are agnostic to the IP address used by the destination;
– can perform “NAT transversal”.

This method is therefore not applicable to substation traffic, which does not use DNS and has no embedded “NAT transversal” facility in the nodes.

It only allows migrating the application, while requesting the nodes to be re-implemented.

6.3.5 Dual-stack recommendations

Dual-stack devices do not solve the migration of legacy IPv4 devices to IPv6.

Dual-stack is a coexistence technique for already deployed IPv4 devices.

Dual-stack makes sense for new devices, since devices will not change from IPv4 to IPv6 in a single step and the same hardware device can serve both.

Dual-stack should first be used for gateways and routers, especially since most operating systems offer today dual stack (Windows, Linux, etc.).

For (new or upgraded) devices, dual-stack may imply:

- redesign of the application to remove dependencies on addresses;
- ability to configure dual-stack (exists already in many real-time operating systems), but possibly only using one stack at a time for memory space reasons;
- ability to configure communications depending on the IP address of the partner.

Dual-stack devices (e.g. SCADA system, newly deployed devices) provide coexistence between legacy IPv4-only devices and new deployed or upgraded devices or systems.

6.4 Tunneling

6.4.1 Tunneling principle

Tunneling is the encapsulation of one protocol payload in another protocol. There are at least two tunnelers, one at each end of the tunnel, but there can be branches to other IPv4 domains, as Figure 15 shows. The first protocol could be IPv4 and the second IPv6.

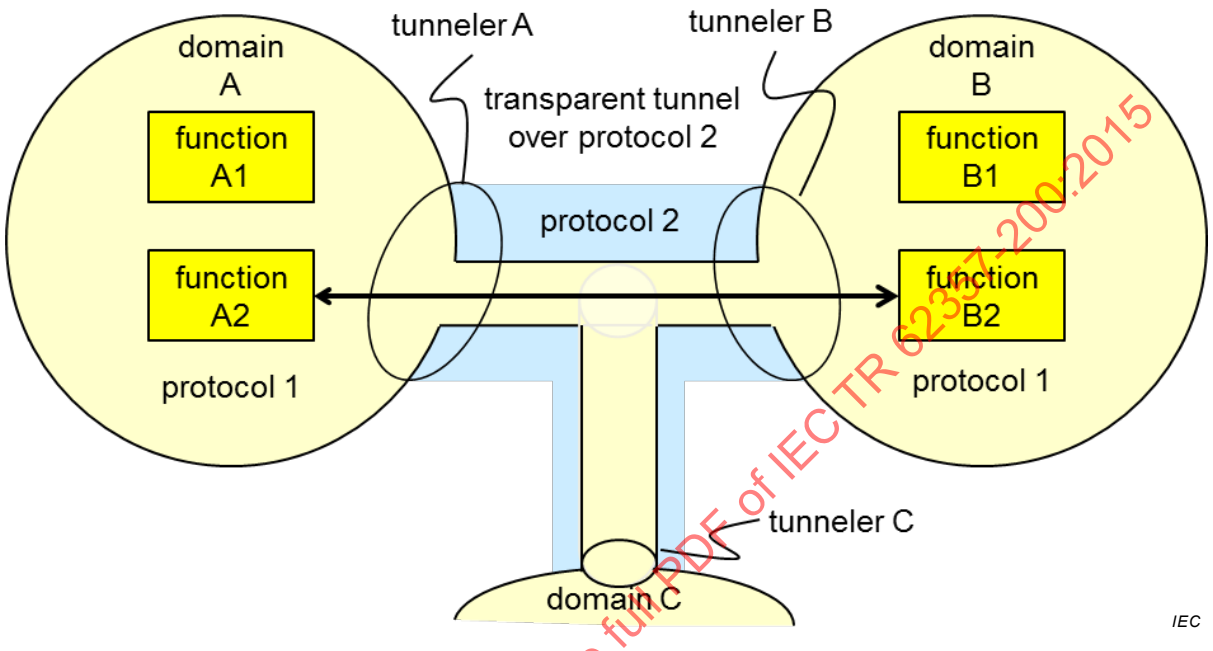


Figure 15 – Tunneling principle

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

6.4.2 Standardized tunneling protocols

IETF specified numerous tunneling protocols for IPv6. RFC 2473 (Generic Packet Tunneling in IPv6 Specification) summarize the general concepts.

RFC 7059 gives a list of the IETF tunneling mechanisms:

- Configured Tunnels (Manual Tunnels / 6in4)
- Automatic Tunneling
- IPv6 over IPv4 without Explicit Tunnels (6over4)
- Generic Routing Encapsulation (GRE)
- Connection of IPv6 Domains via IPv4 Clouds (6to4)
- 6to4 Provider Managed Tunnels
- Anything In Anything (AYIYA)
- Intra-Site Automatic Tunnel Addressing (ISATAP
- Tunneling IPv6 over UDP through NATs (Teredo)
- IPv6 Rapid Deployment (6rd)
- Native IPv6 behind NAT44 CPEs (6a44)
- Locator/ID Separation Protocol (LISP)

- Subnetwork Encapsulation and Adaptation Layer (SEAL)
- Peer-to-Peer IPv6 on Any Internetwork (6bed4)

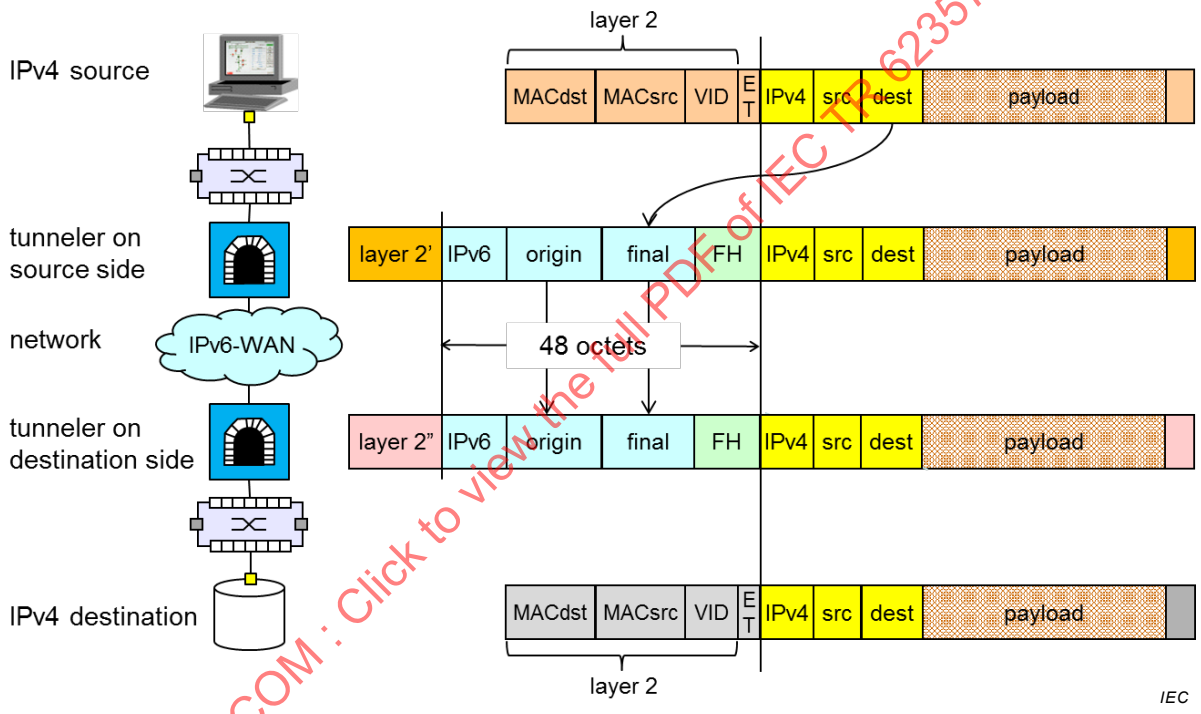
A comparison of the tunneling protocols appears in Table 4 and Table 5.

6.4.3 Tunneling IPv4 over IPv6

6.4.3.1 Tunneling principle

IPv4 nodes communicate with IPv4 nodes over an IPv6 network. The IPv6 network is in principle invisible to the end devices. Routing is IPv4-based and the routers must identify the corresponding partners and domains. The burden of encapsulating / decapsulating relies on the tunnelers.

Figure 16 shows an example of frame format.



Key

MACdst	MAC address destination;
MACsrc	MAC address source;
VID	VLAN ID;
origin	IPv6 source;
final	IPv6 destination;
src	IPv4 source;
dst	IPv4 destination;
IPv4	IPv4 header;
FH	fragment header.

Figure 16 – Tunneling IPv4 over IPv6

Figure 16 shows that the Layer 2 addresses on the IPv4 side are not preserved on the IPv6 side.

6.4.3.2 Tunneling and packet size

As Figure 16 shows, the frame size on the IPv6 network is larger than the frame size on the IPv4 network. Because the Ethernet maximum frame size dictates the frame size on the IPv6 network, the packet size on the IPv4 network, including the IPv4 header cannot exceed:

MTU size ≤ 1 232 octets (1 280 minus 40 for the IPv6 header and 8 for the fragment header).

The adjustment of the frame size is a challenge for existing IPv4 devices. Indeed, legacy devices do not necessary support MTU size reduction. If a legacy device transmits the frames with the DF bit set (see 4.1.5), the tunnel will not forward, but just return an error message to the originator.

In IPv4, the routers and not the end hosts usually perform fragmentation. If needed, tunnelers can fragment IPv4 packets before encapsulation into IPv6 packets. This reduces efficiency since the overhead is large.

If IPv4 devices intend to prevent fragmentation in the network by setting the DF bit, they themselves must be able either of:

- fragmentation of packets (the device itself fragments) or
- negotiation of the MTU size (which is only an optional feature of IPv4 nodes);
- manual adjustment of the MTU size in the source code (which may involve recompilation of their code).

Permanent setting of the DF bit is not advisable. RFC 4459 and RFC 6864 give instructions how to handle fragmentation.

6.4.3.3 Tunneler and VLANs

While a Layer 2 tunnel (such as L2TP) preserves the VLAN tags, a Layer 3 tunnel does not preserve VLAN tags, since VLANs base on Layer 2 addresses.

If the tunneler supports it, the VLAN ID can be coded into the tunneler header or reconstituted at the other side by configuration. The VLAN ID may be the same or a different one.

Instead of coding the VID into the IPv6 payload, it can be encoded into the source and destination IPv6 address (i.e. using a set of IPv6 addresses for the remote substation), but this restricts engineering.

Figure 17 shows a tunneling system that preserves the VLAN identification on both sides.

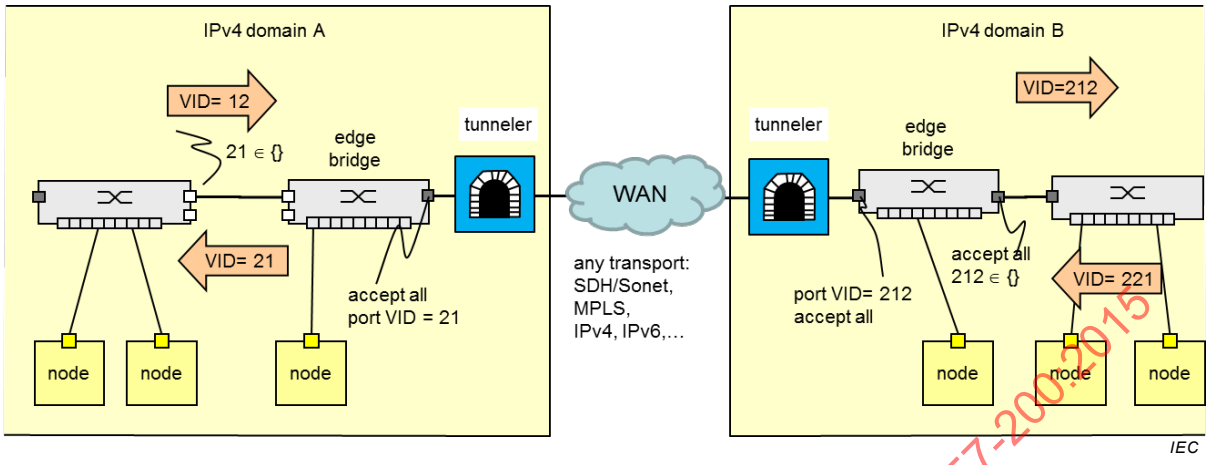


Figure 17 – Tunneling IPv4 over IPv6 and VLANs

In Figure 17, the traffic is running untagged between the edge bridges and the VID is re-established by the port VID at destination edge bridge. This works only for one VID. In the more general case, the edge bridge on the source side will not remove the VLAN tag, but deliver it to the source tunneler as a tunnel selector.

At the destination side, the tunneler will reconstructed or map the VID. This way multiple VLANs can be interconnected.

NOTE This method works also in MPLS with VLL and VPLS, in which case the tunnel and corresponding VID are identified by the inner MPLS label.

6.4.3.4 Tunneler operation

A tunneler packs the incoming IPv4 packets into IPv6 packets. If possible, it adjusts the packet size for the transport over the IPv6 link. Not all IPv4 devices support remote adjustment of the packet size.

The tunneler can map each internal IP address (also private addresses) to an external IPv6 address, allowing choosing among several other tunnelers.

The objects required for a tunneler is a tunneling table configured by system management. At the same time, the tunneler can serve as a NAT, converting the private addresses to public addresses on the other side.

6.4.3.5 Standardized IPv4 over IPv6 tunneling protocols

These tunneling methods are useful for communication from an IPv4 island to another IPv4 island over IPv6. This is useful for all scenarios where the external network must be IPv6, and presents little interest when the whole network is dual-stack.

IETF defined IPv4 over IPv6 tunnels, see Table 4.

As for the protocols in Table 5, the end device should be unaware of the tunneling.

Table 4 – IPv4 over IPv6 tunnels

Method	Mode of operation	Particularities
4in6 (RFC 2473)	Generic Packet Tunneling in IPv6, Clause 5	Tunneling von IPv4 in IPv6
4over6 (RFC 7040)	Public IPv4-over-IPv6 Access Network	Tunneling using global IPv4 addresses, transition strategy for internet service providers

6.4.3.6 Automatic tunneling

The objective of automatic tunneling is to avoid a static configuration of addresses. 6in4 (RFC 4213) defines an automatic tunneling mechanism, while a more general mechanism is specified in 6to4 (RFC 3056) which gives each node a global IPv4 address with a /48 IPv6 prefix which is sufficient for all applications.

6.4.3.7 Configured tunneling

Most of the mechanisms do not specify how to obtain the IPv6 or the IPv4 address pool. In IEC TR 61850-90-1, the tunnel is configured in the SED file. Such an SED file is loaded into the IEC TR 61850-90-1-aware router.

6.4.4 Standardized IPv6 over IPv4 tunneling protocols

Most of the tunneling protocols defined by IETF (see Table 5) consider transport of IPv6 packets over IPv4 tunnels, as a mean to facilitate the introduction of the IPv6 technology.

The objective is that the end devices should be unaware of the tunneling method.

There are various tunneling techniques applicable to specific network scenarios: host-to-host, host-to-gateway and gateway-to-gateway mechanisms. Static and automatic tunnels are distinguished.

For power systems communications, gateway-to-gateway techniques transparent to the end devices and systems are considered, so the protocols in Table 5 are not relevant.

Static gateway-to-gateway tunnels are the most transparent and generic approach from end device's perspective for interconnecting IPv6 islands over the IPv4 ocean. The only drawback is that static tunnels are not scaling well, so dynamic tunnels are a future option.

Therefore, it is not advisable to use IPv6 addresses with special formats (e.g. special prefixes, embedded IPv4 addresses) as it is required in many cases for automatic tunneling.

Table 5 – IPv6 over IPv4 tunnels

Standard	Mode of operation	Particularities
6in4 (RFC 4213)	Tunneling of IPv6 in IPv4 RFC 2473	Protocol type 41, +20B static configured
6over4 (RFC 2529)	address translation Transmission of IPv6 over IPv4 Domains without Explicit Tunnels between Dual-Stack nodes over an IPv4-Network	Uses IPv4 multicast virtual link layer using FE80::/10 e.g. 192.223.16.85 =>(FE80::C0DF:1055
6to4 (RFC 3056)	Stateless transport of IPv6-packets over an IPv4-Network.	automatic router-to-router tunneling based on a particular global address prefix and embedded IPv4 address Connection of IPv6 Domains via IPv4 clouds
Teredo (Meredo in Linux) (RFC 4380) (RFC 5991) (Security Updates) (RFC 6081) (Extensions).	Tunneling IPv6 over UDP through NATs	Encapsulation of IPv6-packets in IPv4-UDP-packets
ISATAP (RFC 5214)	Intra-Site Automatic Tunnel Addressing Protocol	
6rd (RFC 5569)	IPv6 Rapid Deployment on IPv4 Infrastructures	
Tunnel Brokers		

These protocols are not relevant for the utility automation scenarios in the short term since today no IPv6-only devices are integrated into an IPv4 utility network. This will change if 6LoWPAN-based sensor networks are deployed which need end-to-end connectivity with an IPv4 legacy information system

6.4.5 Tunneling conclusion

Tunneling is a coexistence method, but not a migration method on its own.

End devices should be unaware of tunneling.

Host-to-host and host-to-gateway tunnelers should not be used.

Tunnels do not allow IPv6 devices to communicate with IPv4 devices and vice-versa.

IPv4 devices may need to be able to reduce the MTU size according to the MTU size of the tunnel to avoid obliging the tunneler to fragment.

All newly developed devices should be able to operate at a reduced MTU size allowing tunneling.

6.5 Translation

6.5.1 Translation principle

With translation, IPv4 nodes communicate directly with IPv6 devices. In this case, the router to the IPv6 network should mimic an IPv4 network for the nodes in the IPv4 domain and mimic an IPv6 netowk for the nodes in the IPv6 domain, as Figure 18 shows.

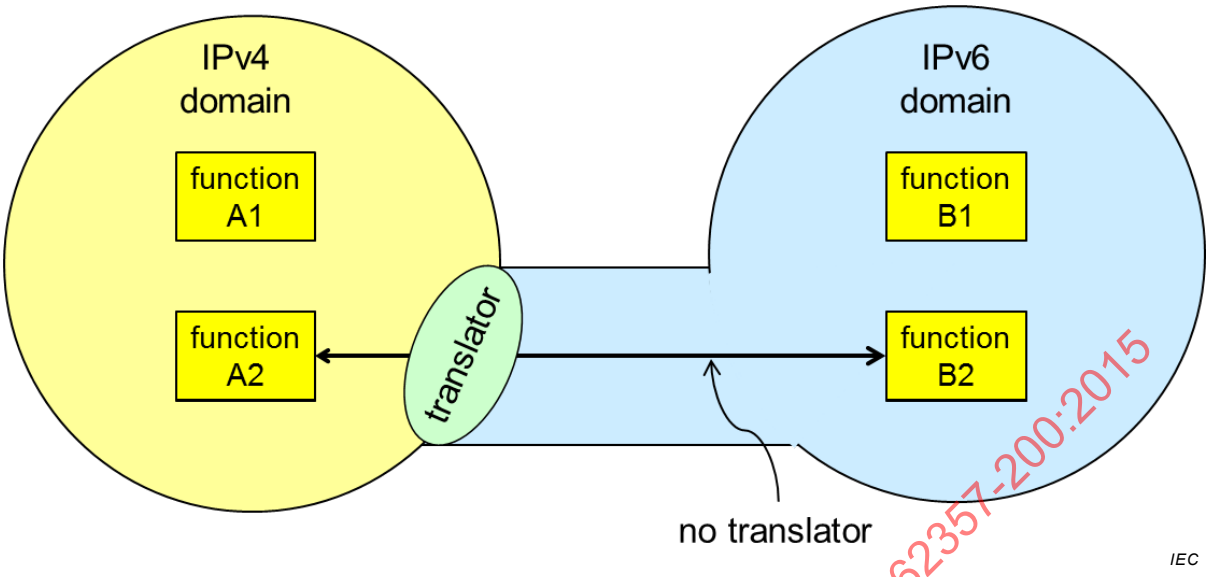


Figure 18 – Translator principle

6.5.2 Translation from IPv4 to IPv6

Figure 19 shows the packets exchanged between an IPv4 client and an IPv4 server over an IPv6 network when using a translator. The translator allows the IPv4 client to access IPv6 servers in the same way, and allows an IPv6 client to access the IPv4 server or to respond to request from the IPv4 client. The translator translates IPv4 addresses to longer IPv6 addresses. Since the IPv6 header is larger than the IPv4 header, the frame size on a LAN can exceed the maximum size.

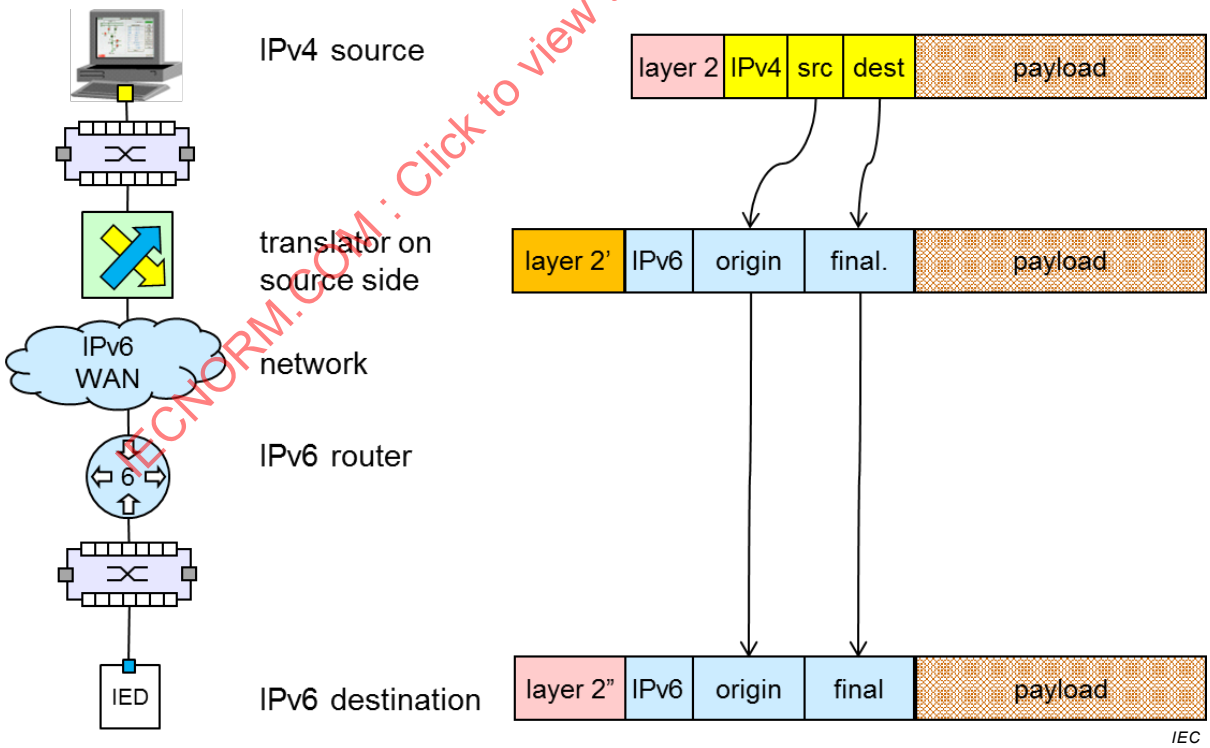


Figure 19 – Translation of IPv4 to IPv6

The first task of the translator is the mapping of the short IPv4 addresses to the long IPv6 addresses and vice versa.

Figure 20 shows the reverse translation. The IPv4 network behind the translator appears to be IPv6 when seen from the IPv6 network.

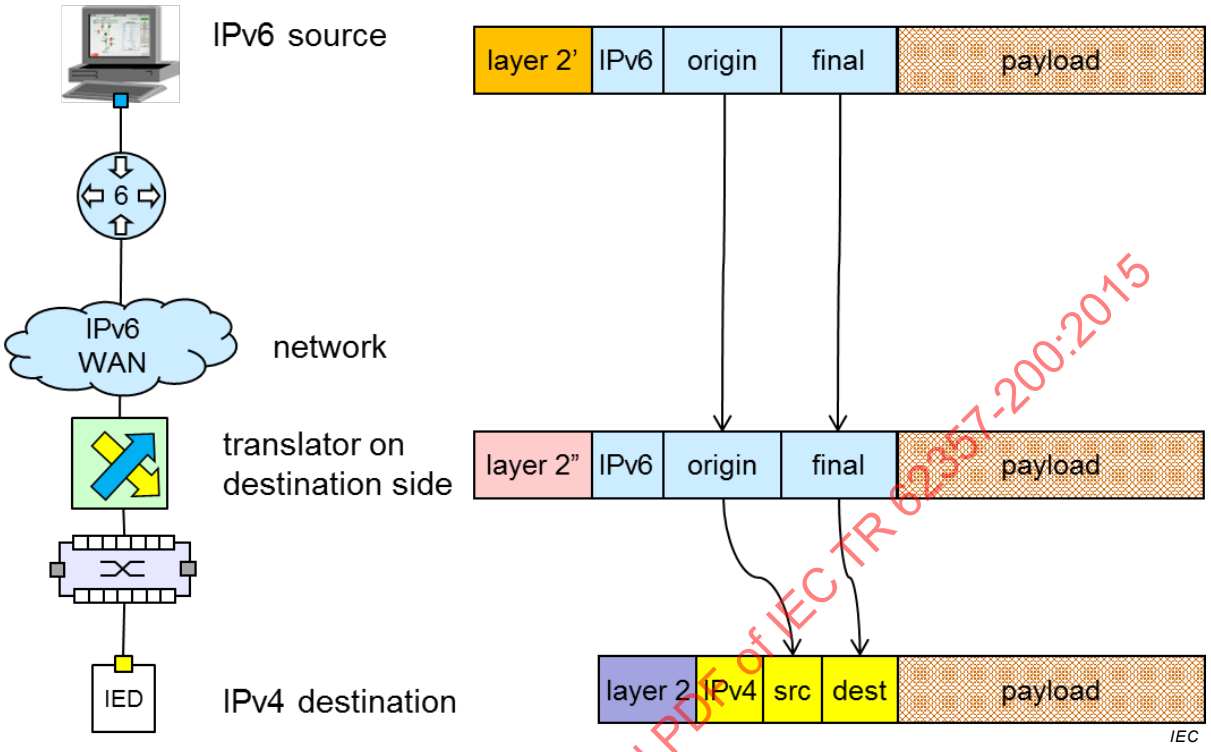


Figure 20 – Translation of IPv6 to IPv4

6.5.3 Translation implementation

There exist several translators, which have the same principle, shown in Figure 21.

The DNS plays an important role since it allows dynamic assignment of IP addresses rather than static configuration of the translators.

However, there are a number of pitfalls, in particular due to dependencies between the layers (which should in principle not exist in a layered ISO approach). In particular, TCP-UDP breaches the layering by embedding parts of the IP header into their checksums (this is known as “hidden header”, see 6.2.3.4). Therefore, the checksums must be recomputed.

Fragmentation in translators presents the same issue as for tunneling (see 6.4.3.2).

Finally, some semantics get lost in the process since some options have no equivalent in the other protocol.

NOTE Wireless devices with small packet size fragment and reconstruct at Layer 2.

There exist stateless and stateful translators. A stateful translator establishes a network session to allocate temporarily addresses, i.e. the network layer ceases to be the connectionless IP as originally designed.

The translator owns a pool of IPv6 addresses in one direction and of IPv4 addresses in the other that it can add dynamically.

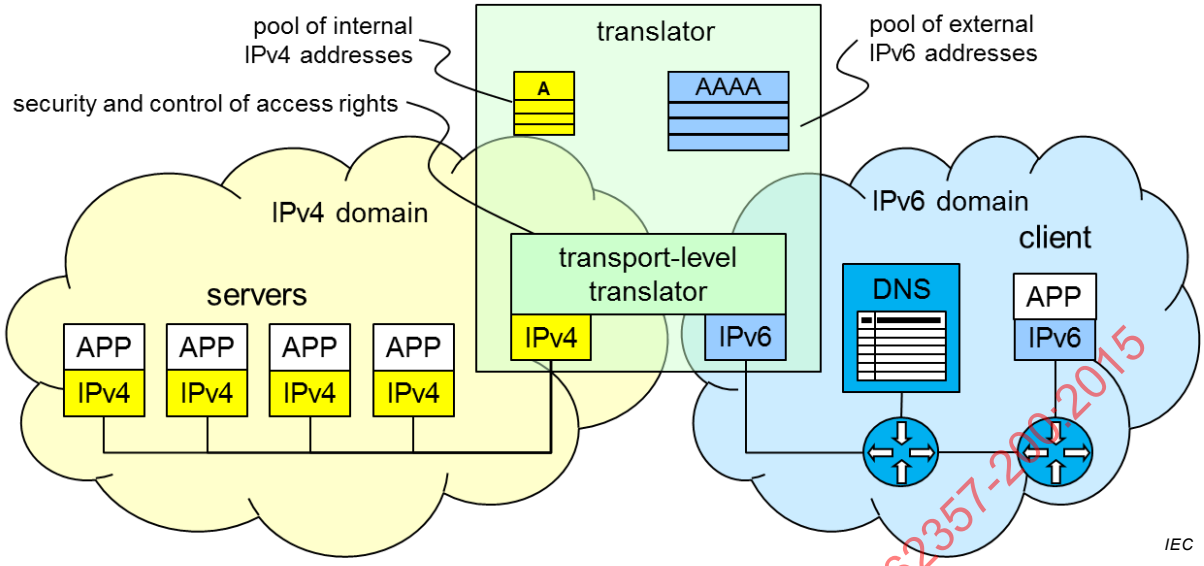


Figure 21 – Translator principle of IPv4 to IPv6

A session is established by the DNS, which resolves the URL and assigns a temporary IPv4 address to remote IPv6 nodes, and conversely assigns an IPv6 address (only visible to itself) to the IPv4 node.

In the opposite direction, mapping longer addresses to shorter IPv4 addresses requires network address translation, as is already used on IPv4 at the boundary between private and public networks.

6.5.4 Standardized translators

IETF defined several translator mechanisms (some are still in development):

- NAT-PT (RFC 2766) (deprecated by NAT64)
- NAT64 (RFC 6146)
- Stateless IP/ICMP Translation Algorithm (RFC 6145)
- TRT
- MAP-T (draft-ietf-softwire-map-t)
- Application Layer Gateway (ALG) translation

NOTE The practical hurdles with NAT-PT were so numerous that IETF decided to deprecate RFC 2766 (RFC 4966) and to propose NAT64 (RFC 6146) instead.

6.5.5 Translator conclusion

Translator is not properly a migration scenario.

The only scenario that justifies translators is when all new devices are IPv6-only. One can however expect that dual-stack devices will only disappear after the last islands of IPv4 devices will be decommissioned.

6.6 Migration plan

6.6.1 Procedure

No special migration plan is proposed, as there are very different scenarios.

In essence, IPv6-preparation should be in the project plan over every change to the networking infrastructure, to the devices requirement specification and to the tools specifications.

This includes the testing.

6.6.2 Security considerations

During the migration, several security issues can be raised.

The translation mechanism is able to infiltrate packets into a system bypassing the firewall, when the firewall does not do an analysis in depth of the packets. Therefore, a tunneler or a translator should be protected accordingly, in particular by a firewall with deep packet inspection, preferably located within the same device.

Security is challenging during migration through the necessity of conducting in parallel different security mechanisms and policies, increasing complexity.

7 Utility protocols based on the Internet Protocol

7.1 Utility protocols on Layer 3

Utility communication protocols carry a number of application data, in particular:

- IEC 60870-5-104 (telecontrol)
- IEEE 1815, previously called Distributed Network Protocol version 3 DNP3 (RTU)
- IEC 61850-8-1 (substation internal client-server communication with MMS)
- IEC TR 61850-90-1 (substation-to-substation)
- IEC TR 61850-90-2 (substation to control centre)
- IEC TR 61850-90-5 (from Phasor Measurement Unit to Phasor Data Concentrator)
- IEC 61400-25 (wind turbines)
- IEC 61588 based on Layer 3 (time synchronization in WANs)

These protocols use explicitly or implicitly protocols of the Internet Protocol suite such as:

- ARP;
- ICMP;
- FTP;
- Simple Network Management Protocol (SNMP) (RFC 3416);
- Network Time Protocol (NTP) (RFC 1305);
- Simple Network Time Protocol (SNTP) (RFC 5905);
- Hypertext Transfer Protocol (HTTP) (RFC 7230).

The application level protocols are however unaware of the network transport protocol used. For the purpose of the IPv4 to IPv6 migration, only the addressing capability and possible network layer support matters.

NOTE Utility protocols based on Layer 2, such as GOOSE (IEC 61850-8-1), SMV (IEC 61850-9-2), Precision Time Protocol (IEC 61588), Link Layer Discovery Protocol (LLDP) are not concerned.

7.2 Layer 3 communication in IEC 61850

7.2.1 Direct Layer 3 communication

IEC 61850-8-1 specifies Layer 3 communication for the Manufacturing Management Specification (MMS) and for SNTP. Other protocols cited that use Layer 3 communication are FTP (file transfer), SNMP (network management), HTTP (web interface) and the Layer 3 related protocols such as ICMP.

A Layer 3 protocol allows in principle direct access from the network external to the substation to all substation devices, as Figure 22 shows for the substation-to-substation communication.

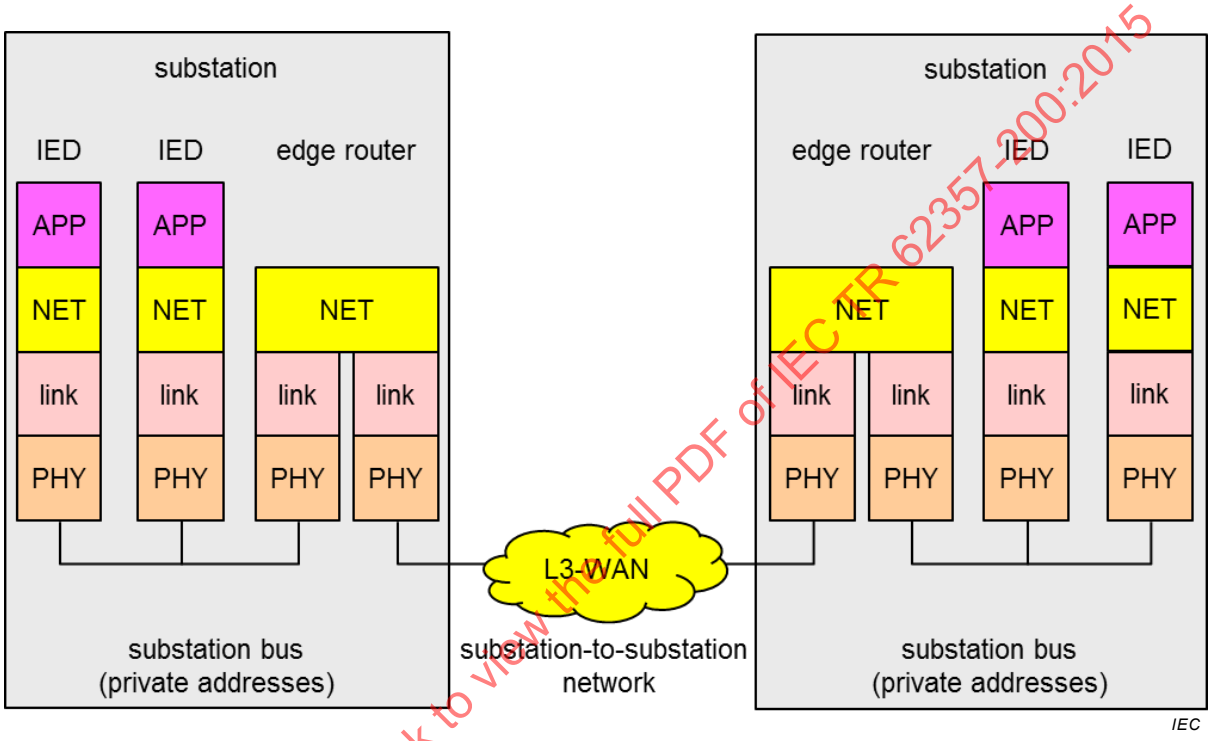


Figure 22 – Layer 3 direct connection

However, within a substation, devices use a private address space as proposed in IEC TR 61850-90-4. This scheme allows assigning statically an IP address to the different IEDs according to their position in the substation. The same IP address may appear in different substations, so these IP addresses cannot be used for direct substation-to-substation communication (see 7.2.2).

Private IPv4 addresses are not routable on the Internet. Therefore, the scheme of Figure 22 is only applicable in substations managed jointly.

7.2.2 Layer 3 communication by Network Address Translator (NAT)

For access outside of the substation, a NAT (RFC 2663) allows to map the internal addresses to external addresses. The edge router is responsible for address translation.

To this purpose, the edge router disposes of a pool of external IPv4 addresses that it will map to internal, private IPv4 addresses. In addition, it uses the port numbers of the transport protocol (TCP and UDP) to extend the address (this is how Internet Service Providers (ISPs) extend the life of IPv4 networks).

The network engineer can allocate external IPv4 addresses to the internal addresses. This involves more than just address translation, as Figure 23 shows. There is no need for a NAT at the SCADA site since the SCADA is aware of the NAT at the other end.

For instance, the SCADA can belong to a 10.x.x.x/8 subnet and each substation to a 192.168.x.x /16 subnet – only the substations need a NAT).

IEDs can in principle use the NAT to access external devices via an external IPv4 address.

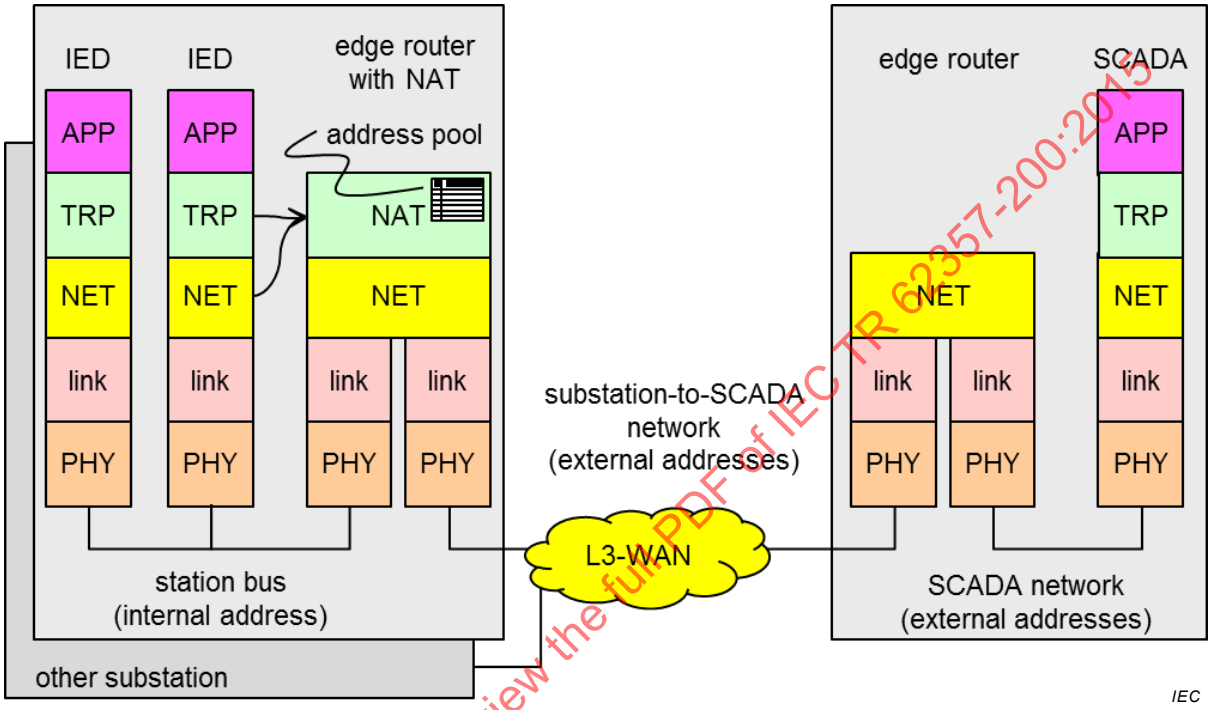


Figure 23 – Layer 3 connection over NAT

A dynamic allocation of IPv4 (private or public) addresses to IEDs is not advisable since the IEDs are by definition servers that need a known address. In a substation, the SCD file assigns the addresses, since tying the IP address to the device address would cause problems when exchanging the device hardware.

NOTE This statement does not apply to a communication scheme in which the IEDs are all clients, such as in an XMPP-like infrastructure.

7.2.3 Layer 3 communication by Application-Level Gateway (proxy)

Direct access to substation-internal devices from an external network 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 is expected.

NOTE 1 Complete physical separation of public internet from utility-owned networks cannot guarantee protection, as long as devices exist that are attached to both networks simultaneously or sequentially.

In applications where a direct access to the IEDs is not desirable (e.g. for security reasons) proxies 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 24, which shows the connection of a remote SCADA or engineering station to a substation.

The substation is visible only through the ALG that manages a pool of public IPv4 addresses. The ALG mimics an individual access to the IEDs, but the structure of the substation as seen from the outside can be different from the inside view and the ALG can block information that

should not be known outside. The SCADA side (or maintenance side) does not need an ALG since it operates only as client.

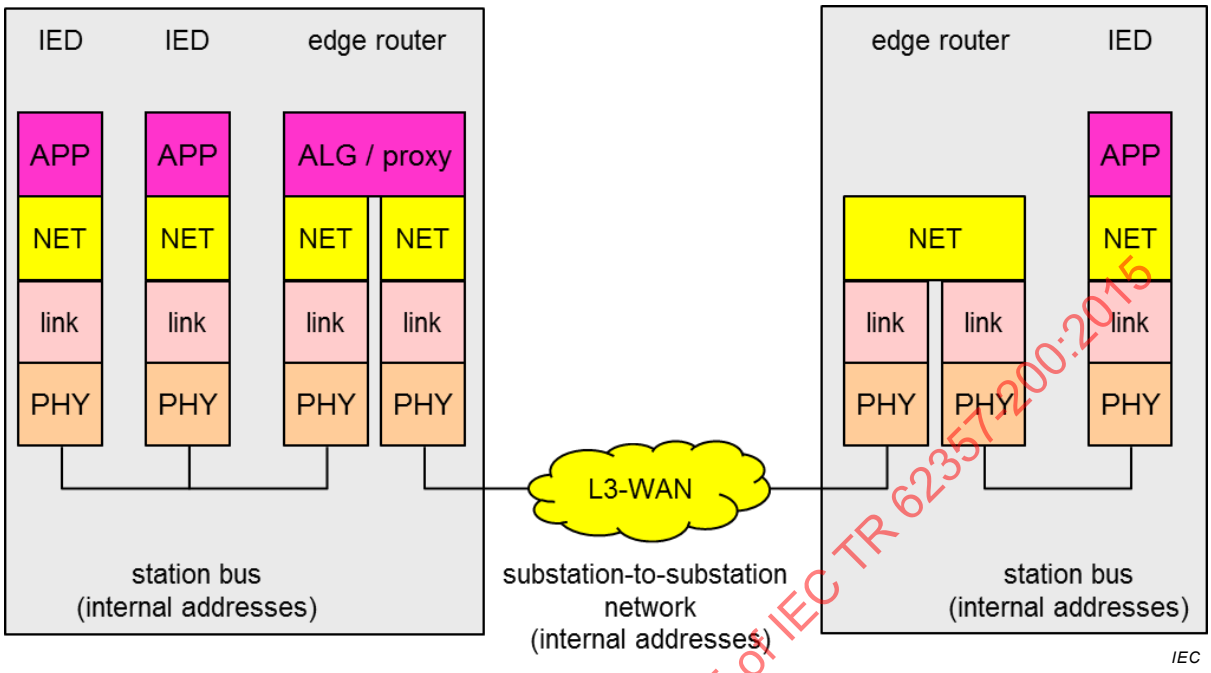


Figure 24 – Layer 3 connection via ALG

NOTE 2 The ALG does not need to be co-located with the edge router. It could be implemented on another device, e.g. a substation controller.

7.3 IEC 61850 Layer 3 communication for Layer 2 traffic

IEC TR 61850-90-1 foresees that substations exchange Layer 2 protocols over a tunnel. It does not however specify the type of the tunnel protocol (it can be an IP network, an SDH/SONET or a VLL / VPLS over MPLS), but suggest to use for Layer 2 tunneling L2TP (RFC 3931, RFC 5641), which also provides authentication and bases on UDP (Figure 25).

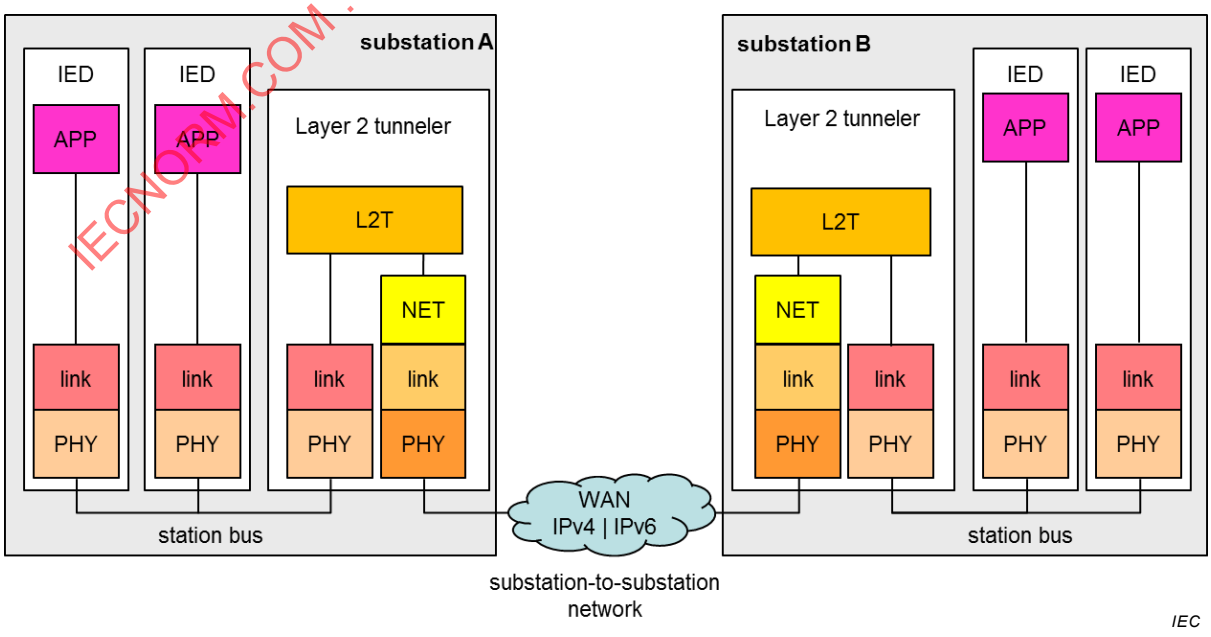


Figure 25 – Layer 2 tunneling over Layer 3 WAN or other transport

IEC TR 61850-90-1 also specifies a communication over ALG / proxy similar to 7.2.3.

IEC TR 61850-90-5 specifies how to transport Layer 2 traffic (SMV and GOOSE) over IPv4 or IPv6. For this, it uses the ITU X.234 (OSI connectionless transport) and RFC 1240 (OSI Connectionless Transport Services on top of UDP) to generate the corresponding session header (see Figure 26). IEC TR 61850-90-5 does not however disclose how to map the traffic to the IP addresses.

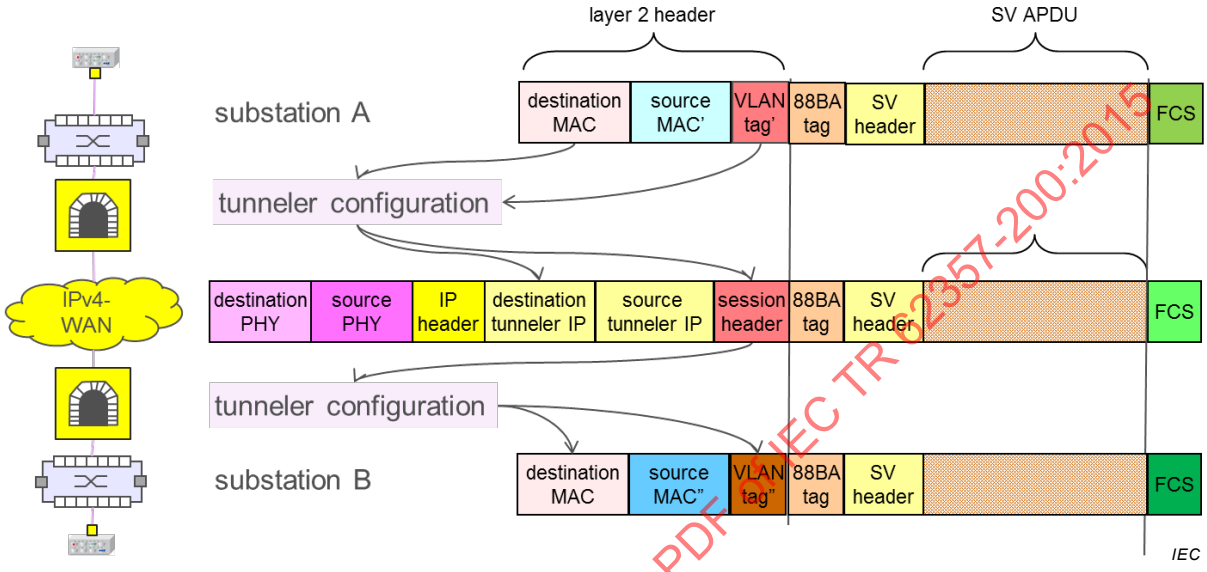


Figure 26 – Layer 2 frames tunneled over IPv4 in IEC TR 61850-90-5 (simplified)

7.4 Other utility protocols

IEC 61400-25 uses the same IP protocols as IEC 61850-8-1. It extends them with security features.

IEC 60870-5-104 uses IPv4 today, but there is no restriction to use IPv6.

IEEE 1813 (“DNP3 over IP”) uses IPv4 and IPv6.

7.5 Virtual Private Network and overlays

IP serves as a support for VPN services. These may for instance be implemented in IPsec “tunnel” mode that allows obfuscating also the IP addresses of the partners (the IP addresses for routing within the WAN are of course in clear).

On top of a VPN, a number of virtual connections exist, e.g. to support voice services and video telesurveillance. These protocols are not concerned by the IPv6 migration since for them, the underlying protocol is invisible.

8 Scenarios for substation automation

8.1 Scenario overview

The following scenarios are considered:

Case	SS	Network	CC | SS	Method	Example	Clause
1.1	4	6 | 4	SS 4	Tunneler IPv4 VPN	IEC TR 61850-90-1 GOOSE and SMV tunneling over IP, MMS uses the same channel	8.2.2
1.2	4	6	CC 4	Tunneler IPv4 VPN	Legacy substation, legacy SCADA and engineering GOOSE and SMV traffic tunneled over IPv6 and IPv4.	8.2.3
2.1	4	6	6 or 4 | 6	Dual-stack local computer as ALG	Access to legacy substation by remote desktop over dual-stack, dual port	8.3
2.2	4	6	6 or 4 | 6	Proxy edge router as ALG	Legacy substation, IPv6 control centre No access to devices	8.3.2
2.3	Dual-Stack	IPv6-only	4 | 6	Proxy edge router, translator	Legacy substation, IPv6 SCADA and >Engineering access to devices by translator	8.3.3
3	IPv4	IPv6	IPv6-only	gateway proxy translator	Partial migration of an existing IPv4 substation to IPv6 (total migration as a particular case)	8.4
4	IPv4 and IPv6	IPv4 and IPv6	IPv6	Use concentrators or intermediate servers as ALGs	Synchrophasor information distributed over both IPv4 and IPv6 networks, depending on the customer IPv4 devices within a domain access servers in an external IPv6 network, e.g. XMPP servers	8.5.1 8.5.2
5	IPv6	IPv6	IPv4	Translator at CC (unlikely since CC will be dual-stack for a long time)	A large amount of IPv6 (typically 6LoWPAN) devices such as sensors or actuators have to communicate with an IPv4 legacy SCADA or over an IPv4 network.	8.6.1 8.6.2

8.2 Scenario 1: Substation-external communication over IPv6 only

8.2.1 Scenario 1: Description

All communications outside of the substation are IPv6-based (by design or regulations).

8.2.2 Scenario 1.1: Substation to substation Layer 2 tunneling IPv4 over IPv6

IEC TR 61850-90-1 and IEC TR 61850-90-5 propose tunneling for communication from substation to substation and from PMU to PDC that already allow to use IPv6.

IEC TR 61850-90-1 proposes to use L2TP (see 7.3), L2TPv3 offers communication over IPv6.

IEC TR 61850-90-5 proposes for synchrophasor to use UDP and the OSI adaptation layer for ITU X.234 (ISO/IEC 8602) with an own tunneling protocol, which also supports IPv6.

In addition, any Layer 2 tunneling protocol that works over IPv6 would serve, as Figure 27 shows.

IEC TR 61850-90-1 foresees that the tunneler can be configured as IEC 61850 objects.

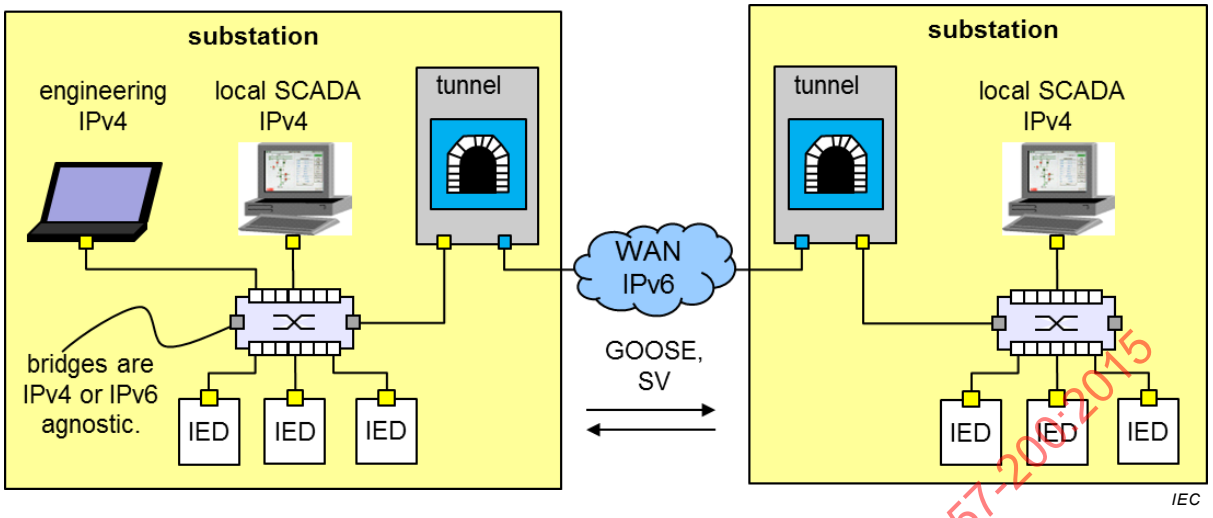


Figure 27 – IPv4 substation to substation over IPv6

8.2.3 Scenario 1.2: substation to control centre: tunneling IPv4 over IPv6

When the partners on both ends are IPv4-only devices, Layer 3 tunneling offers a simple solution (Figure 28).

The same tunneler used for GOOSE or SMV could be used to let remote clients access the substation internal IEDs, acting as a NAT (see Figure 28).

IEC TR 61850-90-1 does not yet consider the configuration of the tunneler as a collection of IEC 61850 objects.

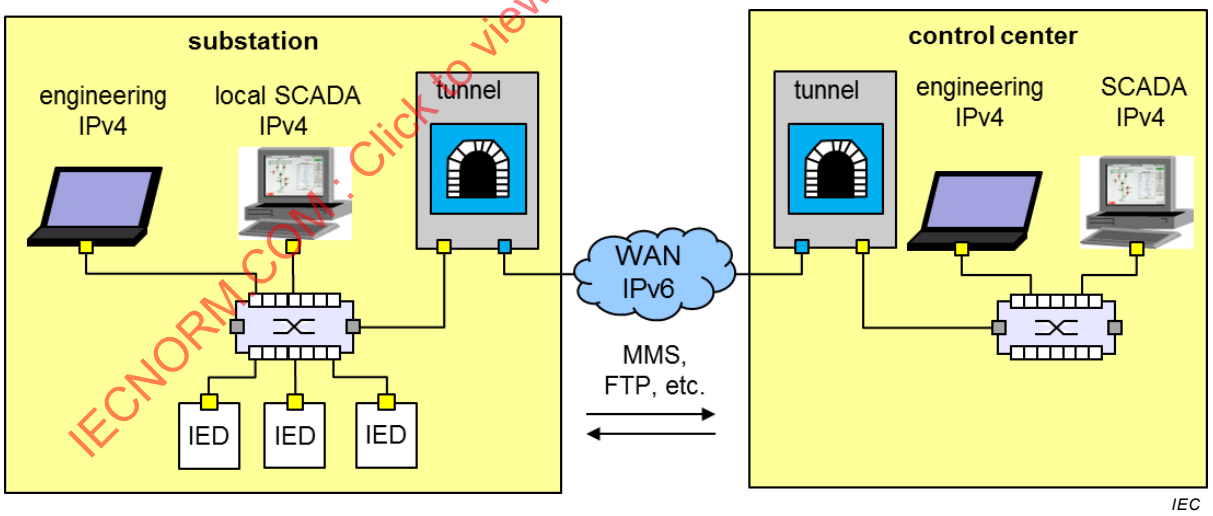


Figure 28 – IPv4 substation to external IPv6 over tunnel

8.2.4 Scenario 1: Evaluation

Implementation	Simple
Impact	Engineering
Costs	Moderate
Special devices	Tunnelers
IPv6 benefits	Devices outside of the substation can be IPv6-only

Difficulties	Network engineering, static configuration
Recommendation	Only use standardized solutions.

8.3 Scenario 2: Access from IPv6 devices through ALGs and translators

8.3.1 Scenario 2.1: substation to engineering over dual-stack engineering

When one party consists of IPv6-only devices, several solutions are possible.

If remote access over IPv6 is the only objective, a dual-stack, dual port engineering station can serve as remote access gateway. To access the individual IEDs, the engineering client uses the remote desktop of the engineering station, which executes the management locally (Figure 29).

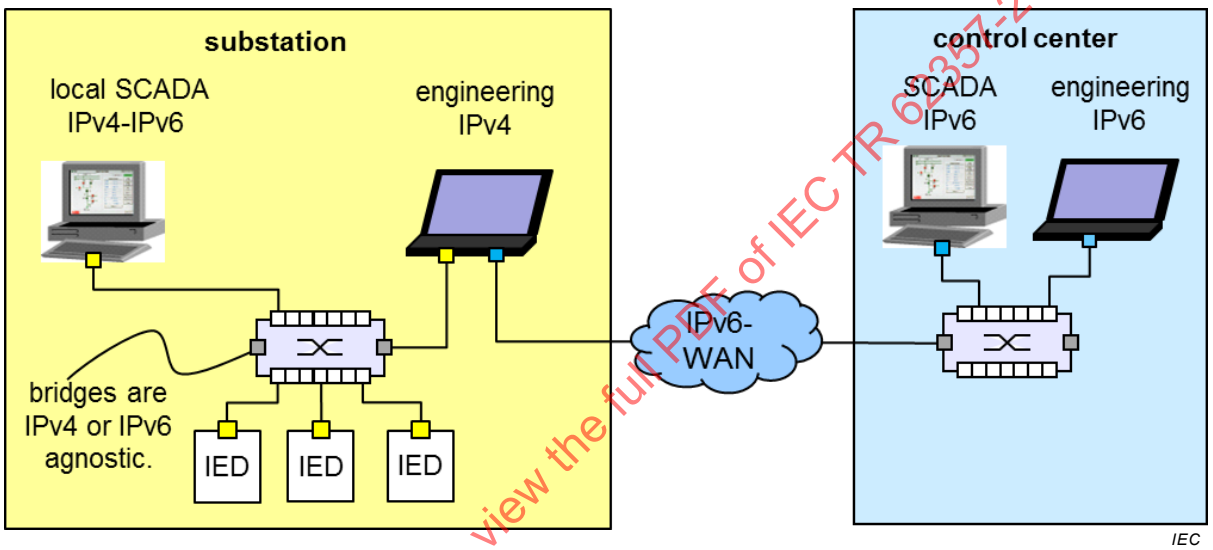


Figure 29 – IPv4 substation to external IPv6 client for engineering

8.3.2 Scenario 2.2 substation to control centre by ALG

If the only objective is access to IEC 61850 objects in the substation, without caring from which device they come, an application-level gateway acts as a proxy and presents the IED objects over an IPv6 interface. The access to the gateway's database can be MMS over IPv6 (Figure 30).

IEC 61850-8-1 does not yet define MMS over IPv6.

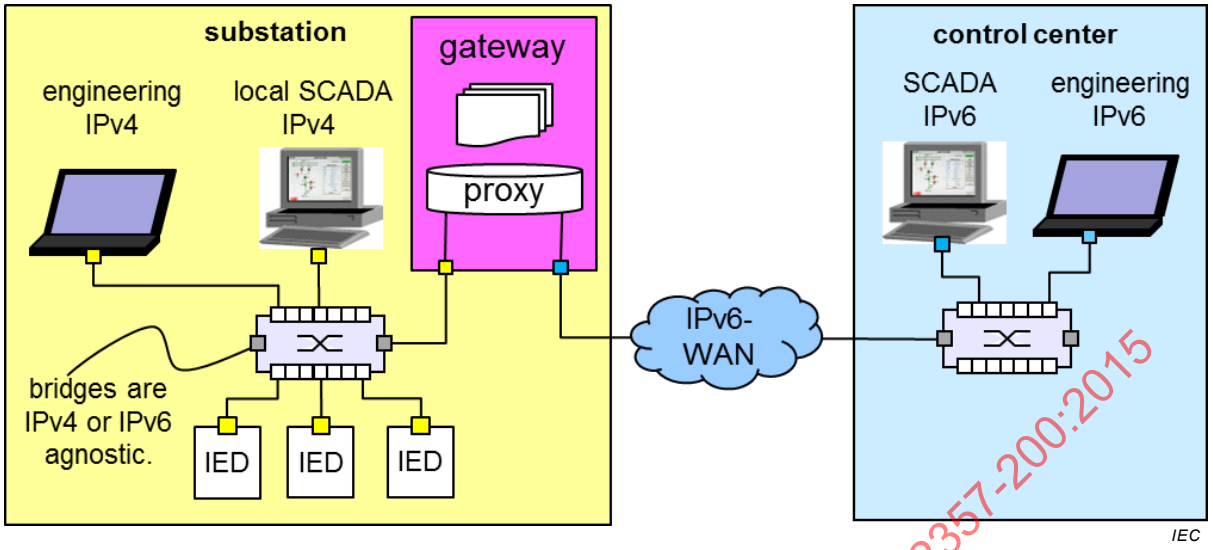


Figure 30 – IPv4 substation to external IPv6 over gateway

The gateway can be implemented in the current NCC-gateways that connect the substation to the regional or national control centre.

8.3.3 Scenario 2.3: substation to SCADA / engineering by translator/proxy

To support both the operational traffic and engineering traffic, a dual-stack, dual port proxy provides access to operational data using the proxy, and access to engineering data and devices using a translator. This allows using IPv6-only engineering tools (Figure 31).

The proxy/translator is however not a commercially available component. Therefore, this scenario has limited used.

Therefore, engineering tools should remain dual-stack as long as there will exist IPv4 legacy devices.

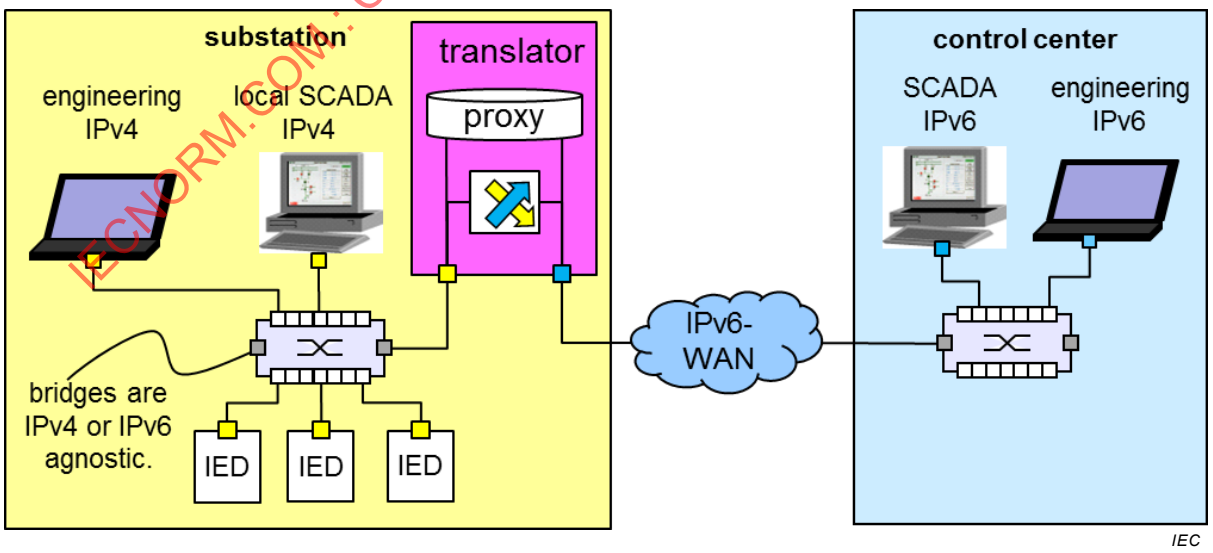


Figure 31 – IPv4 substation to external IPv6 over translator / proxy