ETSI GR IP6 008 V1.1.1 (2017-06)

IPv6-based Internet of Things
Deployment of IPv6-based Internet of Things

Disclaimer

The present document has been produced and approved by the IPv6 Integration (IP6) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
DGR/IP6-0008

Keywords
IoT, IPv6

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) IPv6 Integration (IP6).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

The present document summarizes the advantages and benefits of IPv6 in the deployment of IoT solutions.

It first analyses the IoT landscape, its evolution and its principal characteristics. It then focuses on the principal motivations for IPv6 in this environment both from a technical standpoint as well as from a standardization effort.

The next step is to underline the impact of the IoT toward the IPv6 specifications and its necessary evolutions.

The present document also describes an existing very large deployment of IPv6 in the Smart Grid area (multi-millions of devices).

1 Scope

The present document outlines the motivation for IPv6 in IoT, the technical challenges to address IoT on constrained devices and networks, the impact on the IPv6 technology and protocols, the technology guidelines, the step by step process, the benefits, the risks, as applicable to IoT domains including: M2M, Energy, Industrial, Mining, Oil and gas, Smart city, Transportation (including EVs), etc.

IPv6-based IoT in this context refers to the connectivity network layers needed to support the communication between things. It is understood that a complete IoT system may use of an IoT architecture including but not necessarily an abstraction layer part of an IoT platform. The description of such IoT platform is out of the scope of the present document.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] IEEE 802.15.4™: "IEEE 802.15 WPAN™ Task Group 4 (TG4)".

NOTE: Available at http://www.ieee802.org/15/pub/TG4.html.

[i.2] IEEE 1901.2a™-2015: "IEEE Standard for Low-Frequency (less than 500 kHz) Narrowband Power Line Communications for Smart Grid Applications - Amendment 1".

NOTE: Available at https://standards.ieee.org/findstds/standard/1901.2a-2015.html.

[i.3] IETF RFC 6296: "IPv6-to-IPv6 Network Prefix Translation".

NOTE: Available at https://tools.ietf.org/html/rfc6296.

[i.4] IETF RFC 4291: "IP Version 6 Addressing Architecture".

NOTE: Available at https://tools.ietf.org/html/rfc4291.html.

[i.5] IETF RFC 4193: "Unique Local IPv6 Unicast Addresses".

NOTE: Available at https://tools.ietf.org/html/rfc4193.

[i.6] IETF RFC 6690: "Constrained RESTful Environments (CoRE) Link Format".

NOTE: Available at https://tools.ietf.org/html/rfc6690.

[i.7] IETF RFC 7252: "The Constrained Application Protocol (CoAP)".

NOTE: Available at https://tools.ietf.org/html/rfc7252

[i.8] IETF RFC 7390: "Group Communication for the Constrained Application Protocol (CoAP)".

NOTE: Available at https://tools.ietf.org/html/rfc7390.

[i.9] IETF RFC 7641: "Observing Resources in the Constrained Application Protocol (CoAP)".

NOTE: Available at https://tools.ietf.org/html/rfc7641.

[i.10] IETF RFC 4861: "Neighbor Discovery for IP version 6 (IPv6)".

NOTE: Available at https://tools.ietf.org/html/rfc4861.

[i.11] IETF RFC 2460: "Internet Protocol, Version 6 (IPv6) Specification".

NOTE: Available at https://tools.ietf.org/html/rfc2460.

[i.12] IETF RFC 4944: "Transmission of IPv6 Packets over IEEE 802.15.4 Networks".

NOTE: Available at https://tools.ietf.org/html/rfc4944.

[i.13] IETF RFC 6282: "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks".

NOTE: Available at https://tools.ietf.org/html/rfc6282.

[i.14] IETF RFC 6775: "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)".

NOTE: Available at https://tools.ietf.org/html/rfc6775.

[i.15] IETF RFC 7428: "Transmission of IPv6 Packets over ITU-T G.9959 Networks".

NOTE: Available at https://tools.ietf.org/html/rfc7428.

[i.16] IETF RFC 6437: "IPv6 Flow Label Specification".

NOTE: Available at https://tools.ietf.org/html/rfc6437.

[i.17] IETF RFC 5072: "IP Version 6 over PPP".

NOTE: Available at https://tools.ietf.org/html/rfc5072.

[i.18] IETF draft-ietf-roll-applicability-ami-15: "Applicability Statement for the Routing Protocol for Low Power and Lossy Networks (RPL) in AMI Networks".

NOTE: Available at https://tools.ietf.org/html/draft-ietf-roll-applicability-ami-15.

[i.19] IEEE 802.11™: "IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[i.20] IEEE 802.15.4g™: "IEEE Standard for Local and metropolitan area networks--Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 3: Physical Layer (PHY) Specifications for Low-Data-Rate, Wireless, Smart Metering Utility Networks".

[i.21] IETF RFC 3027: "Protocol Complications with the IP Network Address Translator".

[i.22] IEEE 802.15.4e™: "IEEE Standard for Local and metropolitan area networks--Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1: MAC sublayer".

[i.23] IEC 62357-200:2015: "Power systems management and associated information exchange - Part 200: Guidelines for migration from Internet Protocol version 4 (IPv4) to Internet Protocol version 6 (IPv6)".

[i.24] IETF RFC 7668: "IPv6 over BLUETOOTH(R) Low Energy".

[i.25] Recommendation ITU-T G.9959: "Short range narrow-band digital radiocommunication transceivers - PHY, MAC, SAR and LLC layer specifications".

[i.26] IEEE 802.11ah™: "IEEE Standard for Information technology--Telecommunications and information exchange between systems - Local and metropolitan area networks--Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 2: Sub 1 GHz License Exempt Operation".

[i.27] Recommendation ITU-T G.9903: "Narrowband orthogonal frequency division multiplexing power line communication transceivers for G3-PLC networks".

[i.28] Recommendation ITU-T G.9905: "Centralized metric-based source routing".

[i.29] draft-ietf-6lo-nfc: "Transmission of IPv6 Packets over Near Field Communication".

[i.30] draft-ietf-6tisch-architecture: "An Architecture for IPv6 over the TSCH mode of IEEE 802.15.4".

[i.31] IEEE 802.3™: "IEEE Standard for Ethernet.

[i.32] IETF RFC 6272: "Internet Protocols for the Smart Grid".

[i.33] IEEE 802.16™: "IEEE Standard for Air Interface for Broadband Wireless Access Systems".

[i.34] IEC 61968: "Application integration at electric utilities - System interfaces for distribution management".

[i.35] IEC 61850: "Communication networks and systems for power utility automation".

[i.36] IEC 60870: "Telecontrol equipment and systems".

[i.37] ANSI C12.22: "Protocol Specification For Interfacing to Data Communication Networks".

[i.38] IEEE 802.1X™: "IEEE Standard for Local and metropolitan area networks--Port-Based Network Access Control".

[i.39] IEEE 802.11i™: "IEEE Standard for information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements".

[i.40] IETF RFC 2464: "Transmission of IPv6 Packets over Ethernet Networks.

[i.41] draft-ietf-6lo-dect-ule: "Transmission of IPv6 Packets over DECT Ultra Low Energy".

[i.42] draft-ietf-6lo-6lobac: "Transmission of IPv6 over MS/TP Networks".

3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	Third Generation Partnership Project
AAA	Authentication, Authorization, and Accounting
AMI	Advanced Metering Infrastructure
ANSI	American National Standards Institute
API	Application Programmable Interface
ARIN	American Registry for Internet Numbers
ATM	Asynchronous Transfer Mode
AVB	Audio Video Bridging
B2B	Business-To-Business
BACNET	Building Automation and Control Networks
BT-LE	Bluetooth - Low Energy
CapEx	Capital Expenditure
CoAP	Constrained Application Protocol
CoRE	Constrained Restful Environments

COSEM	Companion Specification for Energy Metering
CPU	Central Processing Unit
DA	Distributed Automation
DAD	Duplicate Address Detection
DCC	Data Communications Company
DECT	Digital Enhanced Cordless Telephone
DECT-ULE	DECT Ultra Low Energy
DHCP	Dynamic Host Configuration Protocol
DLC	Data Link Control
DLMS	Device Language Message Specification
DNS	Domain Name System
DPI	Deep Packet Inspection
DR	Demand Response
DSO	Distribution System Operator
DTLS	Datagram Transport Layer Security
E-IGRP	Extended - Interior Gateway Routing Protocol
ETSI	European Telecommunications Standards Institute
ETX	Extended Transmission metric
EV	Electric Vehicle
FA	Factory Automation
FAN	Field Area Network
FAR	Federal Acquisition Regulation
FAR	Field Area Router
FR	Frame Relay
GPRS	General Packet Radio Service
GSM	Global System for Mobile (communications)
HAN	Home Area Network
HTTP	HyperText Transfer Protocol
IANA	Internet Assigned Number Association
ICMP	Internet Control Message Protocol
ICT	Information and Communication Technology
IDS	Intrusion Detection Service
IEC	International Electro technical Commission
IEEE	Institute of Electrical and Electronic Engineers
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IoT	Internet of Thing
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPX	Internetwork Packet eXchange
IS-IS	Intermediate System to Intermediate System
ISP	Internet Service Provider
IT	Information Technology
ITU	International Telecommunication Union
LLN	Low Power and Lossy Network
LORA	LOng RAnge
LPWA	Low Power Wide Area
LPWAN	Low Power and Wide Area Networking
LTE	Long Term Evolution
LTE-MTC	LTE-Machine Type Communication
LTN	Low Throughput Network
M2M	Machine to Machine
MAC	Media Access Control
MDMS	Meter Data Management System
MP2P	Multi-Point-to-Point
MP-BGP	Multi Protocol-Border Gateway Protocol
MS/TP	Master-Slave/Token-Passing
MTC	Machine Type Communication
MTU	Maximum Transmission Unit
NAN	Neighbour Area Network
NB-IoT	Narrow Band-IoT

NB-PLC	Narrow Band-Power Line Communications
NFC	Near Field Communication
NMS	Network Management System
NOC	Network Operation Centre
NPT	Network Prefix Translation
OMB	Office of Management and Budget
OPEX	OPerational EXpenditure
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
OT	Operational Technology
P2P	Point-to-Point
PC	Personal Computer
PD	Prefix Delegation
PDR	Packet Delivery Ratio
PHY	PHYsical layer
PIM	Protocol Independent Multicast
PLC	Power Line Communications
PNNI	Private Network to Network Interface
QoS	Quality of Service
RAM	Random Access Memory
RF	Radio Frequency
RFC	Request For Comments
RIP	Routing Information Protocol
RIR	Regional Internet Registry
RoLL	Routing over LLN
RPL	Routing Protocol for LLN
RS	Recommended Standards
SAE	Society of Automotive Engineers
SEP	Standard Energy Profile
SMB	Standard Management Board
SNA	Systems Network Architecture
SNMP	Simple Network Management Protocol
SSH	Secure SHell
TC	Technical Committee
TCP	Transport Control Protocol
TSCH	Time Slotted Channel Hopping
TSN	Time Sensitive Networking
UDP	User Datagram Protocol
UNB	Ultra Narrow Band
VPN	Virtual Private Network
WAN	Wide Area Network
WG	Working Group
WIA	Wireless Industrial Automation
WI-SUN	Wireless-Smart Ubiquitous Network
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
WSN	Wireless Sensor Network

4 User defined clause(s) from here onwards

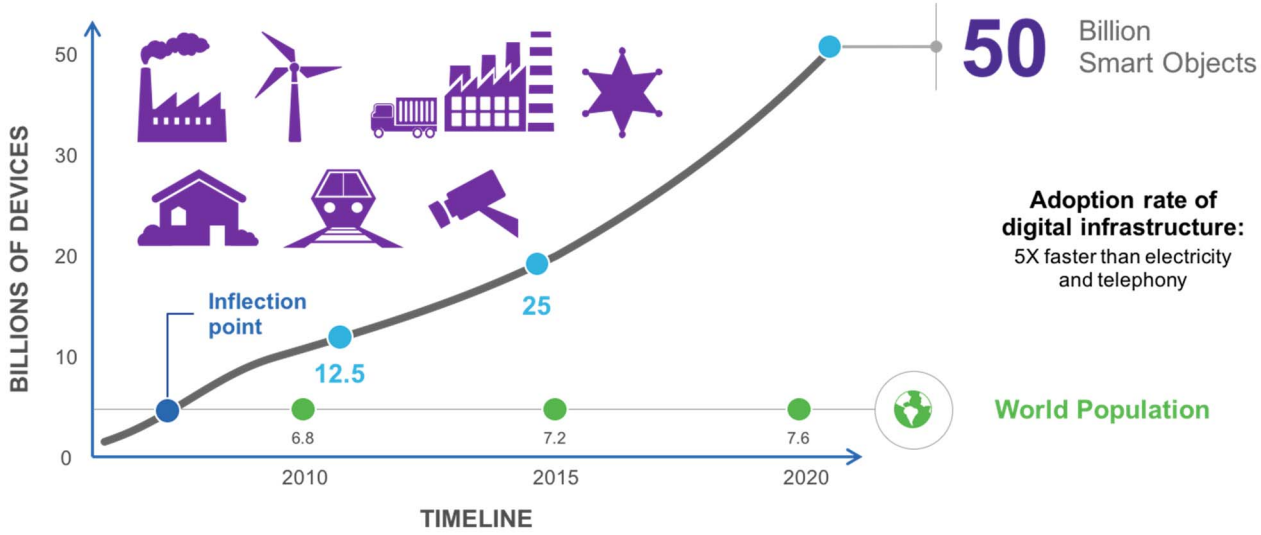
4.1 Introduction

4.1.1 The IoT in 2020: 50 Billion of connected devices

The number of Internet Connected devices will cross the incredible total of 50 billion by 2020.

The connectivity fabric of IP is used to enable more and more efficient context exchange with a broader range of devices and things. Thus, results the Internet of Things.

Projected to increase device counts by orders of magnitude over the next few decades, IoT's impact cannot be overstated. Already enabling a rich set of new capabilities in Smart Cities, Smart Grid, Smart Buildings, and Smart Manufacturing, IoT stands to transform virtually every part of modern life that automation or visibility may improve.



Source Cisco

Figure 1: IoT growth

4.1.2 IoT connectivity: Wired and Wireless

No matter the precise forecast, the sheer tsunami of devices coming online in the next months, years, and decades ensures that the future is not exclusively, or even significantly, wired.

Wireless with its adaptability and ease will inevitably dominate the IoT landscape. Exactly which wireless technology or technologies will be used remains relatively unclear, as many new technologies are still emerging, while others are still early in the standards process.

The challenges IPv6 poses to high bandwidth wireless networks are well-known. However, low bandwidth links, like LPWAN (Low Power Wide Area Network), do require optimization and broadly adapt and adopt techniques like IPv6 header compression.

Clause 4.4 is describing the IETF technologies to adapt IPv6 to different constraint media. This problem is not specific to the use of IPv6 but due primarily to the scale of IoT deployment.

The following list summarizes the main different wireless technologies used for IOT:

- IEEE 802.15.4 [i.1] WPAN: The IEEE 802.15 TG4 was chartered to investigate a low data rate solution with multi-month to multi-year battery life and very low complexity. It is operating in an unlicensed, international frequency band. Potential applications are sensors, interactive toys, smart badges, remote controls, and home automation.
- IEEE 802.11 [i.19] WLAN (Wireless Local Area Network).
- LPWAN (Low Power and Wide Area Network).
- Cellular Networks (NB-IoT, 5G).

New PLC (Power Line Communications) technologies are also emerging like IEEE 1901.2a [i.2]. These technologies offer the capability to use the same wire for power supply and communication media.

4.1.3 Constraint devices and constraint networks

4.1.3.1 The Unique Requirements of Constrained Networks

Devices deployed in the context of Neighbour Area Networks (NANs) are often constrained in terms of resources and often named IP smart objects. Smart-object networks are also referred to as low-power and lossy networks (LLNs) considering their unique characteristics and requirements.

As a contrast with typical IP networks, in which powerful routers are interconnected by highly stable and fast links, LLNs are usually interconnected by low-power, low-bandwidth links (wireless and wired) operating between a few kbps and a few hundred kbps and forming a meshed network for helping to ensure proper operations. In addition to providing limited bandwidth, it is not unusual to see on such links the packet delivery ratio (PDR) oscillating between 60 % and 90 %, with large bursts of unpredictable errors and even loss of connectivity at intervals. Those behaviours can be observed on both wireless (such as IEEE 802.15.4g [i.20]) and Power Line Communications (PLC) (such as IEEE 1901.2a [i.2]) links, where packet delivery variation may happen during the course of one day.

4.1.3.2 Energy consumption in the IoT

Some estimates of IoT have placed the number as high as 50 %, the devices that will be constrained by battery power and also require long-range, wide-area connectivity. Managing these volumes of batteries is no small task, especially given requirements from end-users in utilities and manufacturing asking for 10 to 20 years of battery life.

The sheer size of IoT market and associated communications infrastructure intensifies the importance of energy efficiency awareness. Without significant thought and effort, it is easy to reach very high levels of aggregate power consumption with these technologies. Normalizing the interface fabrics to IPv6 architectures and eliminating needless protocol translation functions is an enormous step towards overall efficiency and prudence.

4.2 The IoT landscape

4.2.1 The Convergence of IT and OT

Converging Networks for the Industrial Internet

Operational Technology (OT) often refers to industrial networks, which focus on highly reliable, secure and deterministic networking. In OT environments, deterministic networks are characterized as providing a guaranteed bandwidth with extremely low packet loss rates, bounded latency, and low jitter. OT networks are typically used for monitoring systems and supporting control loops, as well as movement detection systems for use in process control (i.e. continuous manufacturing) and factory automation (i.e. discrete manufacturing), and protection systems in the SmartGrid.

Due to its different goals, OT has evolved in parallel but in a manner that is radically different from Information Technology/Information and Communications Technology (IT/ICT), which relies on selective queuing and discarding of IP packets to achieve end-to-end flow control over the Internet.

The motivation behind the so-called Industrial Internet is that a single percentile point of operational optimization may save billions of dollars across multiple industries. This optimization requires collecting and processing of huge amounts of missing measurements utilizing widely distributed OT sensing and IT analytics capabilities.

In order to avoid skyrocketing operational costs, the Industrial Internet should share the same infrastructure (network and management) as the deterministic OT flows. This means that the Industrial Internet vision can only be achieved through the convergence of IT and OT, whereby the network becomes capable of emulating the properties of deterministic OT circuits in the same fabric that serves traditional best effort IP applications.

This convergence is made possible by for example the newly introduced open standards for Deterministic Networks that are developed to enable traffic that is highly sensitive to jitter, requires bounded latency in the worst case scenario, and has a high degree of operational criticality so that packet loss should be reduced dramatically, over a converged switched packet fabric.

The first generation of these open standards, called Audio Video Bridging (AVB), was developed at the IEEE 802.1 and tailored for professional Audio/Video networks. The work is now generalizing with Time Sensitive Networking (TSN) is as the particular effort focusing on Ethernet bridging whereas the forthcoming DetNet work in the IETF should enable end-to-end deterministic paths across layer-2 technologies.

4.2.2 The market segmentation

The IoT market is very broad and necessitates a segmentation as not every domain will have the same type of communication requirements.

The following markets or verticals are commonly used in the industry:

- Industrial Internet
- Energy
- Smart Home
- Connected Healthcare
- Oil and Gas
- Mining
- Wearables
- Transportation/Connected Vehicles
- Industrial/Factory automation
- Smart City
- Smart building

4.3 Motivation for IPv6 in the IoT

4.3.1 Technical Motivation

4.3.1.1 Main driver

The main driver is probably the large address space that IPv6 is providing but it is not the only aspect: Auto-configuration, security and flow identification bring huge advantages to IoT systems as well as being a future proof technology.

4.3.1.2 Addressability

Global, public, and private address space have been defined for IPv6; therefore, a decision has to be made regarding which type of IPv6 addressing scheme should be used. Global addressing means you should follow the Regional Internet Registries (RIR) policies (such as ARIN https://www.arin.net/policy/nrpm.html) to register an IPv6 prefix that is large enough for the expected deployment and its expansion over the coming years. This does not mean the address space allocated to the infrastructure has be advertised over the Internet allowing any Internet users to reach a given device.

The public prefix can be advertised if representing the entire corporation - or not - and proper filtering mechanisms are in place to block all access to the devices. On the other end, using a private address space means the prefix not be advertised over the Internet, but, in case there is a need for Business-to-Business (B2B) services and connectivity, a private address would lead to the deployment of additional networking devices known as IPv6-IPv6 NPT (Network Prefix Translation, IETF RFC 6296 [i.3]) gateways.

Once the IPv6 addressing structure (see IETF RFC 4291 [i.4] and IETF RFC 4193 [i.5]) and policies are well-understood and a prefix is allocated to the infrastructure, it is necessary to structure the addresses according to the number of sites and endpoints that would connect to it. This is no different to what an ISP or a large enterprise has to perform.

Internal policies may be defined by the way an IPv6 address is assigned to an end device, by using a global or private prefix.

Three methods to set an IPv6 address on an endpoint are available:

- **Manual configuration:** This method is appropriate for headend and NMS servers that never change their address, but is inappropriate for millions of end-points, such as meters, because of the associated operational cost and complexity.
- **Stateless auto configuration:** This mechanism is similar to Appletalk, IPX, and OSI, meaning an IPv6 prefix gets configured on a router interface (interface of any routing device such as a meter in a mesh or PLC AMI network), which is then advertised to nodes attached to the interface. When receiving the prefix at boot time, the node can automatically set up its IPv6 address.
- **Stateful auto configuration:** Through the use of Dynamic Host Control Protocol for IPv6 (DHCPv6) Individual Address Assignment, this method requires DHCPv6 server and relay to be configured in the network. It benefits from strong security because the DHCPv6 process can be coupled with authentication, authorization, and accounting (AAA), plus population of Domain Name System (DNS) available for headend and NMS applications.

The list above is the minimum set of tasks to be performed, but as already indicated, internal policies and operational design rules should also be established. This is particularly true when considering security and management tasks such as registering IPv6 addresses and names in DNS and in NMSs or establishing filtering and firewalling across the infrastructure.

4.3.1.3 Security Mechanism

In the past, it was sometimes claimed that the use of open standards and protocols may itself represent a security issue, but this is overcome by the largest possible community effort, knowledge database, and solutions available for monitoring, analysing, and fixing flaws and threats - something a proprietary system could never achieve.

Said otherwise, a private network, IP-based architecture based on open standards has the best understood and remedied set of threat models and attack types that have taken place and have been remedied against, on the open Internet. This is the strongest negation of the now deprecated concept of "security by obscurity" that argues that the use of nonstandard networking protocols increases security and which is unanimously rejected by the network security expert community.

4.3.1.4 IP up to the end device/end to end principle

The past two decades, with the transition of protocols such as Systems Network Architecture (SNA), Appletalk, DECnet, Internetwork Packet Exchange (IPX), and X.25, showed us that such gateways were viable options only during transition periods with smaller, single-application networks. But proprietary protocol and translation gateways suffer from well-known severe issues, such as high capital expenditures (CapEx) and operating expenses (OpEx), along with significant technical limitations, including lack of end-to-end capabilities in terms of QoS, fast recovery consistency, single points of failure (unless implementing complex stateful failover mechanisms), limiting factors in terms of innovation (forcing to least common denominator), lack of scalability, vulnerability to security attacks, and more. Therefore, using IPv6 end to end (that is, IP running on each and every device in the network) will be, in many ways, a much superior approach for multiservice IoT networks.

See IETF RFC 3027 [i.21] as an example of protocol complications with translation gateways.

4.3.1.5 Flow identification

The usage of the 3-tuple of the Flow Label, Source Address, and Destination Address fields enables efficient IPv6 flow classification, where only IPv6 main header fields in fixed positions are used.

See IETF RFC 6437 [i.16] - IPv6 Flow Label Specification - IETF Tools.

4.3.2 Standardization

4.3.2.1 IETF standardization effort (IPv6 for the IoT)

Beside the regular standardization activity, the IETF has established a specific directorate for the IoT:

The IoT directorate will provide three primary functions within the IETF. First, the IoT directorate will improve coordination between these working groups. Second, the directorate will provide review for IoT-related specifications for any area director or work group chair requesting such a review. Third, the directorate will provide insight on IoT work advancing outside of the IETF (SDOs, initiatives, product development, etc.) to the IoT-related working groups and to the IESG.

The most important IETF Working Groups for the IoT are the followings:

core: Constrained RESTful Environments (core https://datatracker.ietf.org/wg/core/charter/)

6lo: IPv6 over Networks of Resource-constrained Nodes (6lo https://datatracker.ietf.org/wg/6lo/charter/)

6tisch: IPv6 over the TSCH mode of IEEE 802.15.4e [i.22] (6tisch https://datatracker.ietf.org/wg/6tisch/charter/)

lpwan: IPv6 over Low Power Wide-Area Networks (lpwan https://datatracker.ietf.org/wg/lpwan/charter/)

roll: Routing Over Low power and Lossy networks (roll https://datatracker.ietf.org/wg/roll/charter/)

homenet: Home Networking (homenet https://datatracker.ietf.org/wg/homenet/charter/)

ace: Authentication and Authorization for Constrained Environments (ace https://datatracker.ietf.org/wg/ace/charter/)

ipwave: IP Wireless Access in Vehicular Environments (ipwave https://datatracker.ietf.org/wg/ipwave/charter/)

dice: DTLS In Constrained Environments (dice https://datatracker.ietf.org/wg/dice/charter/)

4.3.2.2 IEC and other SDOs

The IEC has recognized that the transition to IPv6 is an important step that needs to be carefully planned.

The Technical Committee 57 which focuses on Power automation has issued a technical report on the transition to IPv6: IEC 62357-200 [i.23].

The IEC SMB (Standard Management Board) is looking at transitioning all the other IEC domains to IPv6 as well.

4.4 Impact of the IoT on the IPv6 technology and protocols

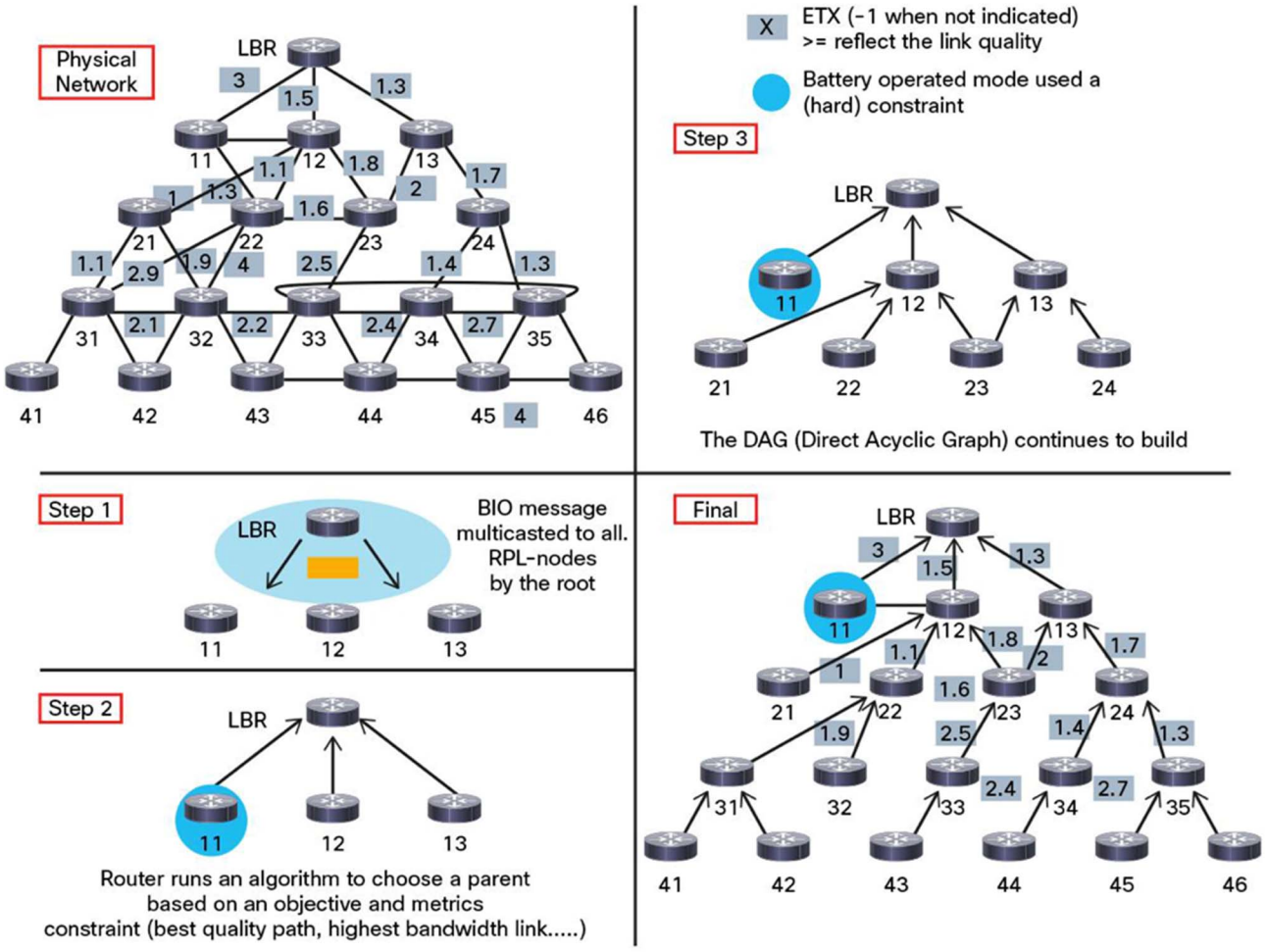
4.4.1 Routing Protocols: Roll

Proprietary systems originally developed for application-specific sensor networks usually neglect the architectural aspect of a scalable networking architecture. In most of these systems, it is not rare to find non-layered architecture, despite the lack of flexibility and scalability, with a layer violation. Routing is no exception.

Where should routing take place?

Several closed systems place the routing function at the data link layer (Layer 2). The consequence is that the network limits itself to a single data link layer technology. It therefore becomes impossible to mix or add data link layer technologies, which is a fundamental requirement of FANs (as previously discussed, mixing low-power RF, PLC, or even cellular is a use-case requirement). In Layer 2 routing networks, the support of multiple types of links would require superposing two routing protocols (both at the IP layer and the link layer; this is for example the case when the NAN becomes a multiservice network, a transit network to other networks), which is an architecture that has proven to be extremely complex, expensive, and difficult to manage even in an unconstrained classic network (IP over ATM (Private Network-to-Network Interface (PNNI)) is one of the notorious examples). Adding this level of complexity to AMI networks hurts the requirements for scalability, ease of operations, and support for long device lifecycles.

Therefore, performing routing at the network layer, as fundamentally adopted in the layered IP architecture is an appropriate choice. To that end, the IETF formed in 2008 the Routing over Low Power and Lossy Networks Working Group (RoLL WG) chartered to specify an IPv6 routing protocol for constrained large-scale networks such as FAN. Tasked with designing a routing solution for IP smart objects, the RoLL WG initially specified four standard documents, spelling out in detail the technical routing use-case requirements for urban networks, including smart-grid, industrial, and home and building automation networks. A protocol survey conducted to determine whether an existing routing protocol (OSPF, etc.) could be used for IP smart objects, given the characteristics and requirements of these networks (including table scalability, loss response, cost control, support of cost routing for links and nodes) led to the consensus that a new routing protocol had to be specified. Being re-chartered, and after almost two years of intensive work performed by numerous industry routing experts, RoLL WG published a new distance-vector routing protocol, called IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL).



Source Cisco

Figure 2: RPL routing protocol

RPL provides support for a large number of technologies and features that matches all service requirements reviewed in the introduction. One of the key characteristics of RPL is that the protocol is highly flexible and dynamic; it has been designed to operate in harsh environments with low-speed links potentially experiencing high error rates, while generating very low control plane traffic. RPL offers numerous advanced features, such as trickle timers limiting the chattiness of control plane, dynamic link (hop count, throughput, latency, link and path reliability, link colours) and node (node state or attribute, node power levels) routing metrics for constraint-based routing useful for combined AMI and DA deployment, multi topology routing, and loop detection or ability to avoid oscillations in case of transient failures (local repair mode and global repair mode).

Today, RPL is an approved international standard with various implementations, extensive simulations, and testing underway. This led several alliances such as ZigBee/IP (and more explicitly as part of Smart Energy Profile (SEP) 2.0), ZWave, and others to adopt routing at the network layer, and particularly RPL, into their evolution to the IP architecture. While offering a fairly sophisticated set of functionalities, RPL has been tailored to fit in few kilobytes of memory footprint and should become the IPv6 routing protocol of choice for FANs as documented in the applicability statement [i.18]. In combination with more traditional IP routing techniques, such as route redistribution, load balancing through multiple IP edge routers and dynamic rerouting in case of hardware or WAN failures, RPL deployment meets all the capabilities required by large and scalable FAN infrastructure.

It is worth stressing the fact that the use of multiple routing protocols all operating at the IP layer is not an issue in contrast with the coexistence of multiple routing protocols at different layers (link layer and IP), as pointed out at the beginning of this clause.

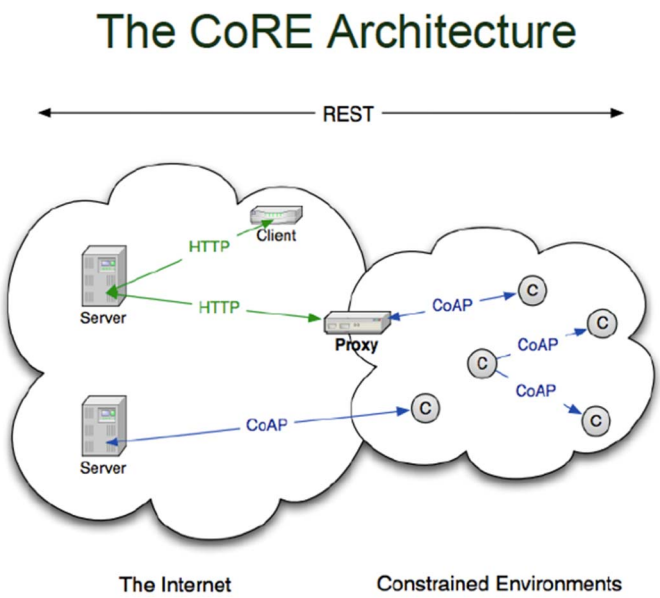
4.4.2 Transport protocols: CoRE

CoRE is providing a framework for resource-oriented applications intended to run on constrained IP networks. A constrained IP network has limited packet sizes, may exhibit a high degree of packet loss, and may have a substantial number of devices that may be powered off at any point in time but periodically "wake up" for brief periods of time. These networks and the nodes within them are characterized by severe limits on throughput, available power, and particularly on the complexity that can be supported with limited code size and limited RAM per node. More generally, constrained networks are defined whenever at least some of the nodes and networks involved exhibit these characteristics. Low-Power Wireless Personal Area Networks (LoWPANs) are an example of this type of network. Constrained networks can occur as part of home and building automation, energy management, and the Internet of Things (IETF CoRE charter).

Core has defined several standards including CoAP (Constraint Application Protocol). The list of RFCs is the following:

- IETF RFC 6690 [i.6] *(was draft-ietf-core-link-format)*
- IETF RFC 7252 [i.7] *(was draft-ietf-core-coap)*
- IETF RFC 7390 [i.8] *(was draft-ietf-core-groupcomm)*
- IETF RFC 7641 [i.9] *(was draft-ietf-core-observe)*

The CoRE architecture is based on a Restful approach. Figure 3 is describing the overall architecture view:



Source Zach Shelby

Figure 3: CoRE Architecture

4.4.3 IPv6 Neighbour Discovery

The IETF work in IPv6 over Low-power Wireless Personal Area Network (6LoWPAN) defines 6LoWPANs such as IEEE 802.15.4 [i.1]. This and other similar link technologies have limited or no usage of multicast signalling due to energy conservation. In addition, the wireless network may not strictly follow the traditional concept of IP subnets and IP links. IPv6 Neighbour Discovery was not designed for non- transitive wireless links, as its reliance on the traditional IPv6 link concept and its heavy use of multicast make it inefficient and sometimes impractical in a low-power and lossy network.

IETF RFC 6775 [i.14] defines optimization to Neighbour Discovery to cope with the new IoT requirements.

This specification introduces the following optimizations to IPv6 Neighbour Discovery IETF RFC 4861 [i.10] specifically aimed at low-power and lossy networks such as LoWPANs:

- Host-initiated interactions to allow for sleeping hosts.
- Elimination of multicast-based address resolution for hosts.
- A host address registration feature using a new option in unicast.
- Neighbour Solicitation (NS) and Neighbour Advertisement (NA) messages.
- A new Neighbour Discovery option to distribute 6LoWPAN header compression context to hosts.
- Multihop distribution of prefix and 6LoWPAN header compression context.
- Multihop Duplicate Address Detection (DAD), which uses two new ICMPv6 message types.

4.4.4 Adaptation Layers: 6Lo

IPv6 protocol is defined in IETF RFC 2460 [i.11] and it was defined at the time when there was no concept of Internet Of Things. Thus IPv6 protocol was mainly designed for wired Ethernet networks for which minimum MTU is 1 280 bytes, IPv6 header size is 40 bytes and the address resolution, duplicate detection and Router advertisements use Multicast messaging to reduce the notion of 'broadcast' in the local network. However, IEEE released the IEEE 802.15.4 [i.1] low power wireless personal area network standard in 2003 as the stepping stone for global low power radio standard for small embedded devices.

IETF defined 'IPv6-over-IEEE 802.15.4' (6LoWPAN WG) in order to integrate IP on the sensor devices with IEEE 802.15.4 [i.1] radio. Given the special requirements for low power devices with limited processing, bandwidth, radio power etc. the 6LoWPAN had a set of unique requirements that are quite different from regular IPv6 standardization on the standard PC or IP-enabled devices - one of them was the need for a simple and stateless compression mechanism for the IPv6 header (40 bytes) which was perhaps carrying only 10 - 20 bytes of IoT data over the low power and lossy networks.

The choice of IPv6 addressing over IPv4 on the IoT devices are clear as IPv6 naturally offers a large range of IP-addresses over a subnet considering the billions of such interconnected devices. 6LoWPAN produced the basic framework of IPv6-over-IEEE 802.15.4 devices and produced three main documents - IETF RFC 4944 [i.12], IETF RFC 6282 [i.13] and IETF RFC 6775 [i.14]. IETF RFC 4944 [i.12] describes the frame format for IPv6 packets, methods of forming the IPv6 addresses on the IEEE 802.15.4 [i.1] networks and the 6LoWPAN adaptation layer frames. IETF RFC 6282 [i.13] followed IETF RFC 4944 [i.12] describing the compression technique for 6LoWPAN packets while IETF RFC 6775 [i.14] provides a set of optimizations for saving Neighbour Discovery control messages and making the booting process reliable in the lossy and low power radio network. 6LoWPAN stack is widely accepted in the industry for IEEE 802.15.4 [i.1] networks.

The popularity of 6LoWPAN stack continues its adoption on many different link-layers (Bluetooth-low-energy, Zwave, Dect-ule, PLC, etc.). A new working group **'6lo'** is formed at IETF which defines IPv6 over constrained nodes networks that use IETF RFC 4944 [i.12], IETF RFC 6282 [i.13] and RFC 6775 [i.14] as base-line stack with necessary modifications to fit the L2-specific requirements. The charter of this work group can be found at https://datatracker.ietf.org/wg/6lo/charter/.

6lo includes IPv6 on IEEE 802.15.4 [i.1] and other supported L2 technology devices as described below. **6lo** is continuing further optimization and necessary enhancements of the 6LoWPAN stack and other new areas such as privacy and security at the network layer.

Benefits of running IPv6-on-IoT is multi-fold ranging from application portability to manageability with existing Network Management Operations using standard IP protocols.

Bluetooth Low Energy

IETF RFC 7668 [i.24] specifies the IPv6 over Bluetooth-Low Energy (BT-LE). The standard Bluetooth radio has been widely implemented and available in mobile phones, notebook computers, audio headsets, and many other devices. The low-power version of Bluetooth is a specification that enables the use of this air interface with devices such as sensors, smart meters, appliances, etc.

DECT Ultra Low Energy

The transmission of IPv6 packets over DECT Ultra Low Energy (DECT-ULE) is in progress towards standardization at 6lo WG currently (draft-ietf-6lo-dect-ule [i.41]). DECT-ULE enjoys benefits from its parent DECT technology such as long range, worldwide reserved frequency band and interference-free communication. The technology is also used for sensors, smart meters and home networking devices.

Zwave

IETF RFC 7428 [i.15] describes the frame format for transmission of IPv6 packets as well as a method of forming IPv6 link-local addresses and statelessly auto-configured IPv6 addresses on Recommendation ITU-T G.9959 [i.25] networks. Zwave is also used in home devices.

PLC

An individual IETF draft has been written on transporting IPv6 packets over IEEE 1901.2a [i.2] Power Line Communications (PLC) technology, but it is actually specified in ITU-T standards (Recommendations ITU-T G.9903 [i.27] and G.9905 [i.28]) G3-PLC networks for smart meters and other low power electrical devices.

Near Field Communications

Draft-ietf-6lo-nfc [i.29] specifies the transmission of IPv6 packets over the NFC L2 technology which is a very low range (~10 cm) communication identifying the IPv6 header compression, address formation, Neighbour Discovery optimizations for this short range but useful for many social and home applications via smartphones and other devices.

BACNET

Master-Slave/Token-Passing (MS/TP) is a medium access control method for the RS-485 physical layer, which is used extensively in building automation networks. Draft-ietf-6lo-6lobac [i.42] defines the IPv6 address formation and transmission of packets over MS/TP networks.

802.15.4e TSCH

The IEEE 802.15.4e [i.22] Timeslotted Channel Hopping (TSCH) is an amendment to the Medium Access Control (MAC) portion of the IEEE 802.15.4 [i.1] standard. TSCH is the emerging standard for industrial automation and process control LLNs. IPv6 over TSCH also uses 6lo/6LoWPAN protocols. (draft-ietf-6tisch-architecture [i.30]).

802.11ah

The IEEE 802.11ah [i.26] amendment defines a WLAN system operating at sub 1 GHz license-exempt bands designed to operate with low-rate/low-power consumption. This amendment supports large number of stations and extends the radio coverage to several hundreds of meters. IEEE 802.11.ah [i.26] technology presents a trade-off between energy consumption and bitrates. Thus, it is beneficial to run a 6lo defined IPv6 specification in order to save energy in the packet transmission in the IEEE 802.11ah [i.26] supported topology, stateless address auto configuration and Neighbour Discovery defined in the 6lo charter. Use case of IEEE 802.11ah [i.26] ranges from smart meters, appliances, home devices to the Industrial applications/monitoring devices.

4.4.5 LPWAN

Low-Power Wide-Area Network (**LPWAN**) is a type of wireless telecommunication network designed to allow long range communications at a very low bit rate among things (connected objects), such as sensors operated on a battery. (Wikipedia).

Battery life time is expected to be measured in decades.

LPWA has specific characteristics which defer from current communication technologies.

Table 1: LPWA characteristics

Characteristic	Order of magnitude	Typical value
Spectrum	Licensed (3GPP) vs Unlicensed	Sub-GHz, 2.4GHz
Range	Long in star topology	From 1 to +10 kms (urban/rural)
Objects	Many	Many thousands
Data volume	Small (upstream vs downstream)	Few kBytes per day (mostly upstream)
Data rate	Low (upstream vs downstream)	From 60bs to few 100kbs
Data payload	Small	From 10 to few 100 bytes
Latency	Low to high	Up to minutes
Battery life	Long	From months to +20 years
Module cost	Low	<$5
Service cost	Low	<$10 per year

Several technologies are competing for this market:

- LoRa
- Cellular based technologies (defined by 3GPP):
  - LTE-MTC
  - NB-IoT
  - EC-GSM-IoT
- UNB Ultra Narrow Band (defined by ETSI LTN)
- WI-SUN

The IETF Working Group **lpwan** is focussing on enabling IPv6 connectivity over a selection of Low-Power Wide-Area technologies.

The group is currently working on:

1) Producing an Informational document describing and relating some selected LPWA technologies. This work will document the common characteristics and highlight actual needs that the IETF could serve; but it is not intended to provide a competitive analysis. It is expected that the information contained therein originates from and is reviewed by people who work on the respective LPWA technologies.

2) Producing a Standards Track document to enable the compression and fragmentation of a CoAP/UDP/IPv6 packet over LPWA networks. This will be achieved through stateful mechanisms, specifically designed for star topology and severely constrained links. The work will include the definition of generic data models to describe the compression and fragmentation contexts. This work may also include to define technology-specific adaptations of the generic compression/fragmentation mechanism wherever necessary.

4.5 Specific market deployment considerations

4.5.1 Industrial Internet: *Deterministic Networking* DetNet/6TiSCH

In order to avoid collisions and ensure the transmission of a packet at an exact time, Wireless Deterministic Networking requires fully scheduled radios such as the TSCH mode of 802.15.4, and LTE/5G. Both ISA100.11a and WirelessHART™ use variations of the TSCH MAC, which is optimized for ultra-low power activities and is a natural match to transport low-frequency periodic flows, such as control loops, over a fully scheduled network.

A Controller called system manager, or network manager, respectively, computes all routes in the mesh network. Those routes are generally multipath, so as to augment the spatial diversity that is offered to the transported flows and to route around interferences dynamically. A third protocol, WIA-PA, was developed in parallel in China for process automation applications. Interestingly, WIA offers a faster FA version for Factory automation, using an 802.11 physical layer (aka Layer-1 or PHY layer).

Due to the necessity of a centralized computation to solve the NP-complete problem of multipath route optimization, those networks do not generally scale to large configurations and are too costly to efficiently address large scale monitoring applications such as required for the Industrial Internet.

Another major limitation is the siloed approach taken for all these standards. They were defined from the PHY layer up to the application, with no desire to interconnect with other networks and at bets the regulatory capabilities to share the spectrum with other technologies. This contrasts with eth end-to-end principle that guides the Internet designs, with a network that is agnostic to the applications and can be shared between multiple existing and any upcoming ones.

The work at 6TiSCH may ultimately enable the convergence of the lower layers of the stack to the end-to-end principle. This would allow significant OPEX savings in operational networks.

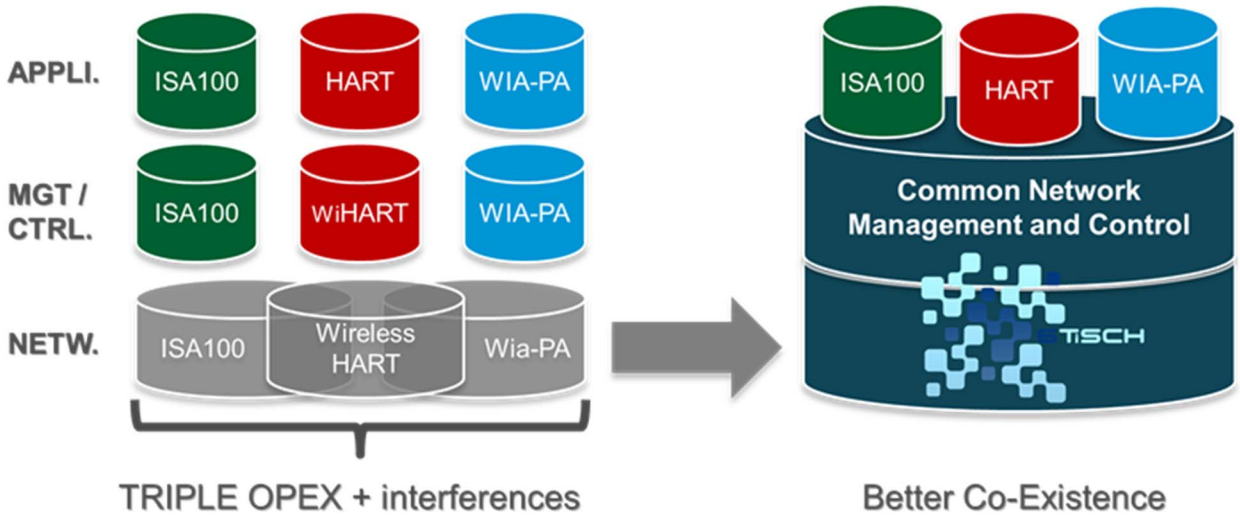


Figure 4: 6tisch model

But the Industrial Internet is also - and a lot - about reporting non-critical data such as diagnostics and for which the incumbent protocols are not a cost-efficient solution. Users are now after a wireless technology that would coexist transparently with the operational wireless network and scale to large numbers of devices at lower costs. The next problem for industrial wireless is thus to extend highly predictable WSN technologies to share bandwidth and other physical resources with non-deterministic traffic, reaching higher scales at lower costs.

6TiSCH addresses this additional challenge and allows for a mix of stochastic (best effort) IPv6 flows with such well-known deterministic flows while preserving the deterministic properties regardless of the load imposed by other flows. While the work on best effort is well on the way at the IETF, and though the vision is clearly to apply the methods defined at the IETF DetNet Working Group, there is still a lot to do at the time of this writing to enable deterministic traffic on 6TiSCH networks. It remains that the way a path is computed for a wired network may not fit the wireless medium well. This work proposes new approaches for wireless path computation.

4.6 Lesson learned: IPv6 for the Smart Grid

4.6.1 Power Automation use case

Beside the smart metering use case which will be described in clause 4.6.2, the utility industry is looking at IPv6 as the next communication protocol for power automation. This means communications between electric substations (around several thousand depending on the size of the utility) and communications within the substations.

One of the main driver to transition to IPv6 is the investment cycle which is very long in such a domain. Utilities need to plan for future proof architecture and technologies as equipment that will be installed in 2017 may stay operational for 30 years.

The Technical Committee 57 of the IEC has worked on a transition plan to IPv6. This Technical Report document is referenced IEC TR 62357-200 [i.23]. The scope of this report is the following:

"IEC TR 62357-200:2015(E) 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, distributed energy generation (renewables), energy storage, load management. It addresses the issues encountered when migrating from Internet Protocol version 4 (IPv4) to 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." https://webstore.iec.ch/publication/22943.

4.6.2 Field Area Network use case for Electric Distribution Network and smart metering

4.6.2.1 A Standardized and Flexible IPv6 Architecture for Field Area Networks: Smart-Grid Last-Mile Infrastructure

This clause is intended to provide a synthetic and holistic view of open-standards-based Internet Protocol Version 6 (IPv6) architecture for smart-grid last-mile infrastructures in support of a number of advanced smart-grid applications (meter readout, demand-response, telemetry, and grid monitoring and automation) and its benefit as a true multiservice platform.

Last-mile networks have gained considerable momentum over the past few years because of their prominent role in the smart-grid infrastructure. These networks, referred to as neighbourhood-area networks (NANs) in this clause, support a variety of applications including not only electricity usage measurement and management, but also advanced applications such as demand/response (DR), which gives users the opportunity to optimize their energy usage based on real-time electricity pricing information; distribution automation (DA), which allows distribution monitoring and control; and automatic fault detection, isolation and management. NANs also serve as a foundation for future virtual power plants, which comprise distributed power generation, residential energy storage (for example, in combination with electric vehicle (EV) charging), and small-scale trading communities.

Field Area Networks (FANs), which is the combination of NANs and local devices attached to a Field Area Router (FAR) offering the backhaul WAN interface(s), have emerged as a central component of the smart-grid network infrastructure. In fact, they can serve as backhaul networks for a variety of other electric grid control devices, multitenant services (gas and water meters), and data exchanges to home-area network (HAN) devices, all connected through a variety of wireless or wired-line technologies. This has created the need for deploying the Internet Protocol (IP) suite of protocols, enabling the use of open standards that provide the reliability, scalability, high security, internetworking, and flexibility required to cope with the fast-growing number of critical applications for the electric grid that distribution power networks need to support. IP also facilitates integration of NANs into end-to-end network architecture.

One application being run over FANs is meter reading, where each meter periodically reports usage data to a utility headend application server. The majority of meter traffic was thus directed from the meter network to the utility network in a multipoint-to-point (MP2P) fashion. With the emergence and proliferation of applications such as DR, distributed energy resource integration and EV charging, it is expected that the traffic volume across FANs would increase substantially and traffic patterns and bidirectional communication requirements would become significantly more complex. In particular, FANs are expected to support a number of use cases that take advantage of network services:

- **Communication with an individual meter:** On-demand meter reading, real-time alert reporting, and shutdown of power to a single location require point-to-point (P2P) communication between the network management system (NMS) or headend and the electric meter and conversely.

- **Communication among DA devices:** Subsets of DA devices need to communicate with each other to manage and control the operation of the electric grid in a given area, requiring the use of flexible communication with each other, including peer to peer in some cases.

- **HAN applications:** HAN applications typically require communication between home appliances and the utility headend server through individual meters acting as application gateways. For example, a user may activate direct load control (DLC) capabilities, empowering the utility company to turn off or turn down certain home appliances remotely when demand and/or the cost of electricity is high.

- **EV charging:** Users need to have access to their individual vehicle charging account information while away from home in order to be able to charge their vehicles while on the road or while visiting friends. Verifying user and account information would require communication through the meter to the utility headend servers from potentially a large set of nomadic vehicles being charged simultaneously from dynamic locations.

- **Multitenant services:** Combining information at the customer side and differentiating information into several services at the other side creates a complex multipoint-to-multipoint network (MP2MP). For example, this could be a converged network connecting devices from multiple utilities as suggested by the U.K. national multi-utility telecom operator DCC or Germany multi-utility communication box as specified in open meter systems.

- **Security:** Strong authentication mechanisms are needed for validating devices that connect to the advanced metering infrastructure (AMI) network, as well as encryption for data privacy and network protection.

- **Network management:** As the FAN carries increasingly more traffic and is subject to stringent service level objectives (SLOs), managing network-related data becomes critical to monitoring and maintaining network health and performance. This requires the communication of grid status and communications statistics from the meters to the NMS or Headend in a MP2P fashion.

- **Multicast services:** Groups of meters may need to be addressed simultaneously using multicast, for example to enable software upgrade or parameters updates sent by a NMS to all meters using multicast requests, and multicast queries for meter readings of various subsets of the meters.

4.6.2.2 The Key Advantages of Internet Protocol

One of the differences between information and communications technology (ICT) and the more traditional power industry is the lifetime of technologies. Selecting the IP layered stack for AMI infrastructure can support future applications through smooth evolutionary steps that do not modify the entire industrial workflow. Key benefits of IP for a distribution system operator (DSO) are:

- **Open and standards-based:** Core components of the network, transport, and applications layers have been standardized by the Internet Engineering Task Force (IETF) while key physical, data link, and application protocols come from the usual industrial organizations, such as the International Electrochemical Commission (IEC), American National Standards Institute (ANSI), Device Language Message Specification (DLMS)/Companion Specification for Energy Metering (COSEM), SAE International, Institute of Electrical and Electronic Engineers (IEEE), and the International Telecommunication Union (ITU).

- **Lightweight:** Devices, such as smart meters, sensors, and actuators, which are installed in the last mile of an AMI network, are not like personal computers (PCs) and servers. They have limited resources in terms of power, CPU, memory, and storage. Therefore, an embedded networking stack works on few kilobits of RAM and a few dozen kilobits of Flash memory. It has been demonstrated over the past years that production IP stacks perform well in such constrained environments.

- **Versatile:** Last-mile infrastructure in smart-grid networks has to deal with two key challenges. First, one given technology (wireless or wired) may not fit all field deployment criteria. Second, communication technologies evolve at a pace faster than the expected lifetime of a smart meter, or 15 to 20 years. The layered IP architecture is well-equipped to cope with any type of physical and data link layers, making it ideal as a long-term investment because various media can be used in a deployment now and over time, without changing the whole solution architecture and data flow.

- **Ubiquitous:** All recent operating system releases, from general-purpose computers and servers to lightweight embedded systems (TinyOS, Contiki, etc.), have an integrated dual (IPv4 and IPv6) IP stack that gets enhanced over time. This makes a new networking feature set easier to adapt over time.

- **Scalable:** As the common protocol of the Internet, IP has been massively deployed and tested for robust scalability. Millions of private or public IP infrastructure nodes, managed under a single entity (similarly to what is expected for FAN deployments) have been operational for years, offering strong foundations for newcomers not familiar with IP network management.

- **Manageable and highly secure:** Communications infrastructure requires appropriate management and security capabilities for proper operations. One of the benefits of 30 years of operational IP networks is its set of well-understood network management and security protocols, mechanisms, and toolsets, which are widely available. Adopting IP network management also brings an operational business application to the utility. Utilities can use network-management tools to improve their services, for example, when identifying power outage coverage through the help of the NMS.

- **Stable and resilient:** With more than 30 years of existence, it is no longer a question that IP is a workable solution considering its large and well-established knowledge base. More important for FANs is the benefit from the years of experience accumulated by critical infrastructures, such as financial and defence networks, as well as critical services, such as voice and video, which have already transitioned from closed environments to open IP standards. It also benefits from a large ecosystem of IT professionals who can help design, deploy, and operate the system solution.

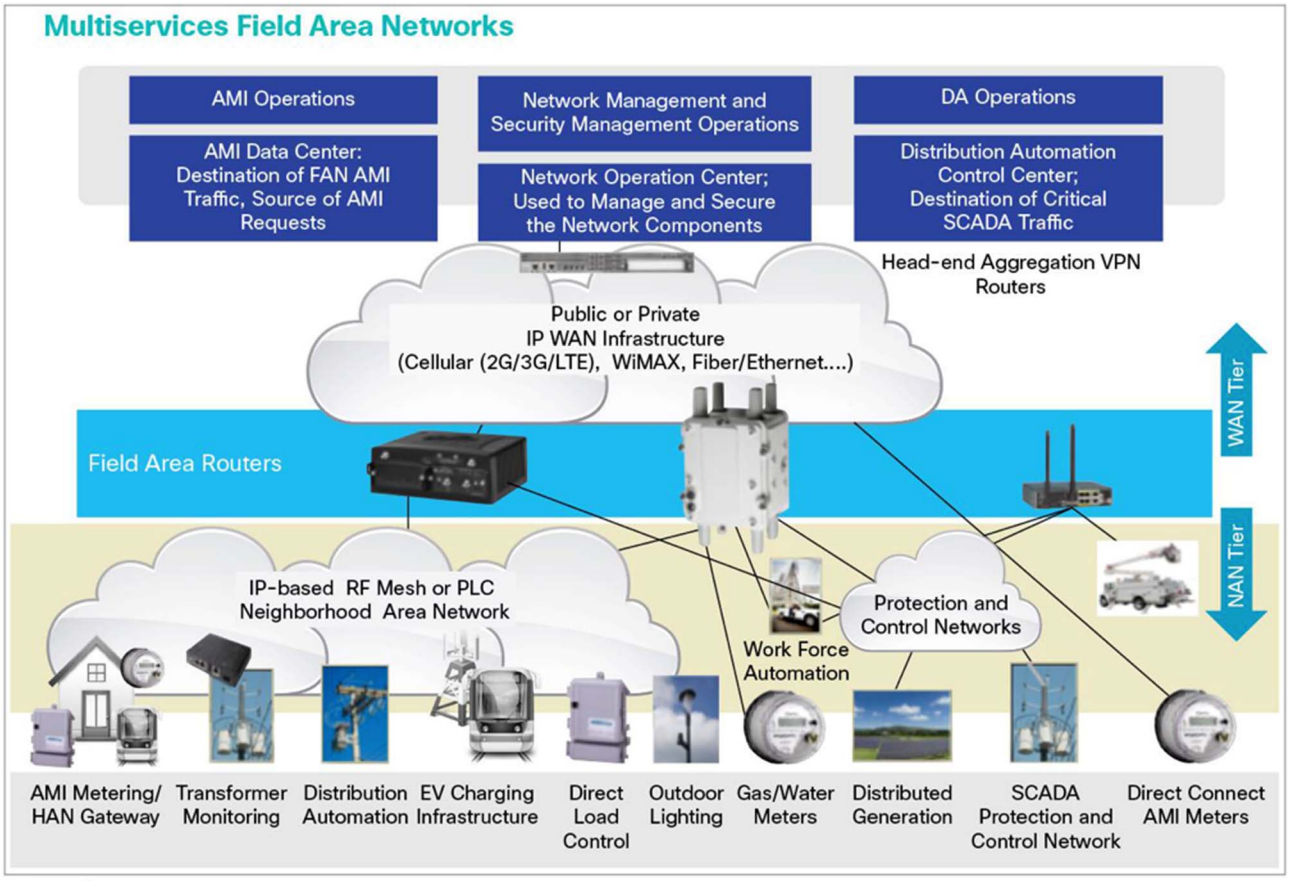
- **End to end:** The adoption of IP provides end-to-end and bidirectional communication capabilities between any devices in the network. Centralized or distributed architectures for data manipulations are implemented according to business requirements. By using protocol translation gateways, the efficiency of end to end communication might be impacted.

4.6.2.3 An IPv6 Distribution Network Architecture

The networking requirements for NANs have been extensively documented: cost efficiency, scalability (millions of nodes in a network is common), robust security, reliability, and flexibility are absolute requirements. Technologies based on open standards and with the flexibility to be relevant for 15 to 20 years are minimum expectations from utilities. This explains why the IPv6 suite was the initial protocol of choice, although new IPv6 protocols have been designed to address the unique requirements of such networks, as discussed in the next clause.

The adoption of IPv6 facilitates a successful transformation to connected energy networks in the last mile. The next clauses describe in greater detail IPv6 networking components such as IP addressing, security, quality of service (QoS), routing, network management and the use of end-to-end IPv6. After all, IPv6, as with any other technology, requires appropriate education to the whole workforce, from technicians to the executives evaluating vendors, subcontractors, and contractors.

One of the major steps in favour of building the momentum around using IP end to end in the last mile of smart-grid networks was to demonstrate that IP could be light enough to be used on constrained devices with limited resources in terms of energy, memory, and processing power. Thus, FANs were seen as single-application, stub networks with end nodes (such as meters not running IP) that could be reached through IP through protocol-translation gateways, with each gateway being tied to a dedicated service and/or solution's vendor.



Source Cisco

Figure 5: Multiservice Infrastructure for Last-Mile Smart-Grid Transformation

4.6.2.4 The Technical Components of IPv6 Smart-Grid Last-Mile Infrastructure

The industry has been working on IPv6 for nearly 15 years, and the adoption of IPv6, which provides the same IP services as IPv4 (Figure 5), would be fully aligned with numerous recommendations (U.S. OMB and FAR, European Commission IPv6 recommendations, Regional Internet Registry recommendations, and IPv4 address depletion countdown).

Moreover, all new developments in relation to IP for smart objects and LLNs, as discussed above, make use of or are built on IPv6 technology. Therefore, the use of IPv6 for smart-grid FAN deployments benefits from several features:

- A huge address space to accommodate any expected millions of meter deployments (AMI), thousands of sensors (DA) in the hundred-thousands of secondary substations, and, additionally, all standalone meters. Its address configuration flexibility helps it adapt to the size of deployments as well as the time-consuming process of installing small devices. The structure of the IPv6 address is also flexible enough to manage a large number of subnetworks that may be created by future services such as EV charging stations or distributed renewable energy.

- IPv6 is the de facto IP version for meter communication over open RF mesh wireless (IEEE 802.15.4g [i.20], DECT Ultra Low Energy) and PLC infrastructures (IEEE 1901.2a [i.2]) using the IPv6 over low-power wireless personal-area network (6LoWPAN) adaptation layer that only defines IPv6 as its protocol version.

- IPv6 is the de facto IP version for the standardized IETF Routing Protocol for Low-Power and Lossy Networks (RPL). RPL is an IPv6-only protocol.

This goes without forgetting all well-known IP feature sets, which help enable design variations for the deployment of highly available and highly secure communications infrastructure tying a network operations centre (NOC) and all NANs through public and/or private WAN links.

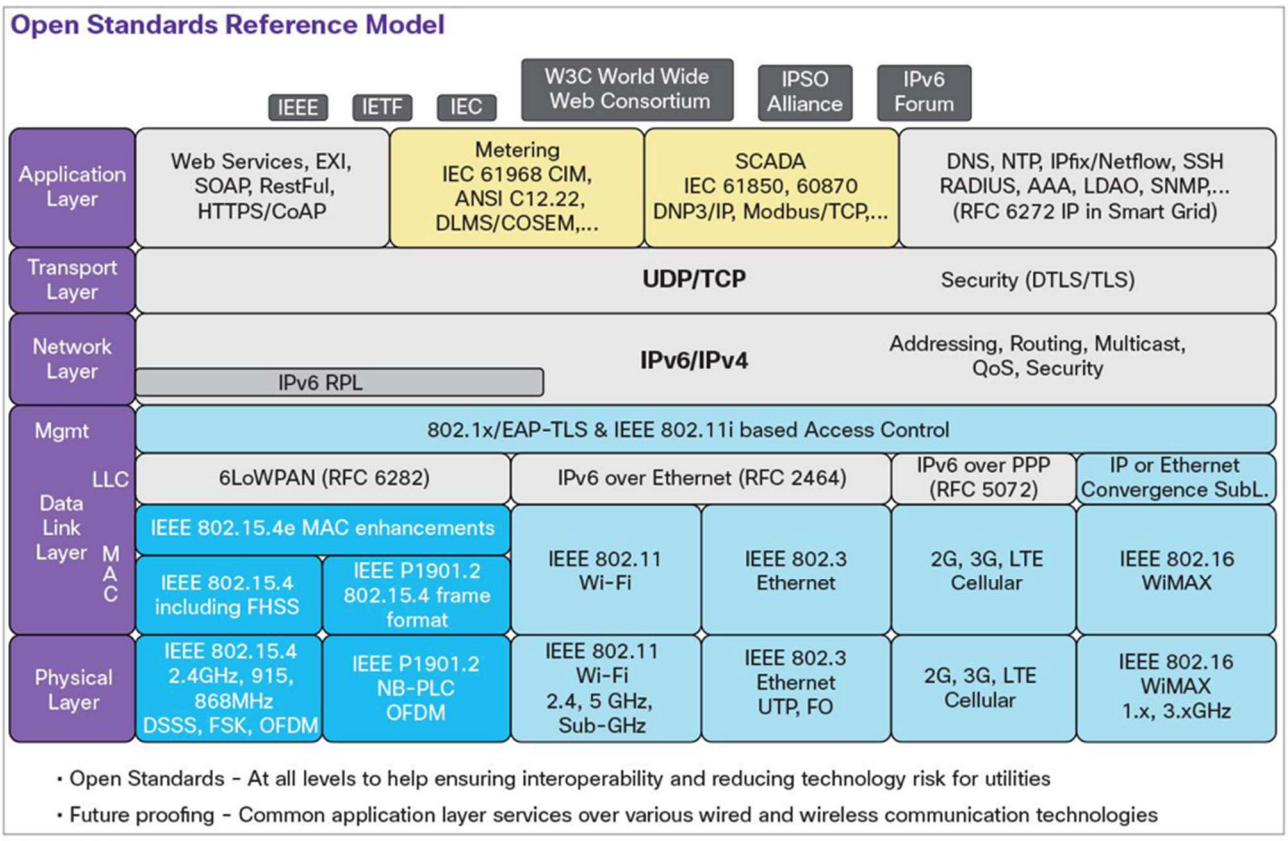
DSOs require redundancy as a means to improve communication reliability in the LLNs, as well as to measure against vendor lock-in and technology lock-in because of incompatibility in lifetime expectancies between communication and metering technologies. Redundancy can be achieved at several levels through mesh capabilities in the WAN and NAN, or by using multiple technologies simultaneously.

Routing is transparent from end to end and independent from the technology. For example, the WAN connection of the IP edge router is established by a private, highly reliable, fibre connection or by public, flexible, cellular communication technology, such as GPRS, 3G, or LTE. An IP edge router can be collocated with a metering node or located as a separate entity in a substation, while the majority of the metering nodes communicate over a meshed NAN through 6LoWPAN, IPv6, or RPL over RF or PLC technologies, or both. The possibility of multiple IP edge routers enabled by dynamic IP routing protocols is important to prevent single points of failure, typically introduced by concentrators as used today for proprietary PLC and RF mesh.

Dynamic routing would allow for transportable NAN nodes, such as electric vehicles, field tools, or pagers. IP edge routers capable of routing traffic over different NAN technologies and cooperating with other IP edge routers over the backbone for global connectivity are key elements to prevent vendor lock-in and technology lock-in, since alternative WAN and NAN communication technologies can easily be adapted. This is in contrast with IP (non-IP) gateway connecting the NAN with the rest of the network, where the failure of one piece of equipment that handles states and translates protocol unavoidably leads to communication failure.

This allows DSOs also to optimize on CapEx and OpEx, both in time and place. Take for example the situation with GSM/GPRS in some countries. While this mature technology is readily available for rollout and has low cost, it might be at the end of its lifecycle and a risk to deploy. However, using it for WAN access only easily mitigates this risk and supports placing more advanced 3G/LTE modems in (some of) the IP edge routers from the start or exchanging them gradually when coverage and prices are right.

Another concern for DSOs on optimizing costs is dispersed rollout. NAN technologies (RF or PLC mesh) typically need sufficiently dense node groupings to achieve mesh capabilities (that is, to see its neighbour). When starting a rollout in a location, an IP edge router has to be installed first, close enough from a first meter, to help ensure the WAN communications. Later, it will serve as a foundation for a larger NAN that will grow as soon as more neighbour nodes are deployed.



Source Cisco

Figure 6: An IPv6 Networking Stack for Smart-Grid FANs

Figure 6 summarizes the whole proposed IPv6 end-to-end architecture for FANs and clearly shows the power and flexibility provided by a layered architecture. First, the layers are independent from each other, still allowing cross-layer optimizations made possible by the application-programming interface (API) between the layers. For example, new link types can be added without having to revisit the network-addressing scheme, or new applications can be supported without affecting the rest of the stack. As another example, the routing function taking place on Layer 3 helps enable new link layers to be added without affecting the routing architecture. The rest of this clause describes in greater detail technical aspects related to the networking stack for FAN, knowing that a plethora of existing IP protocols are reused without requiring any change.

4.6.2.5 Network Management for Smart Meters

Today, use-case solutions, such as AMI or DA, handle most, if not all, services at the application layer. By adopting IPv6 for the last mile (and therefore enabling bidirectional IP end-to-end communications) there is the opportunity of using well-known services from the open-standards IP architecture, decreasing complexity, and supporting many required services of smart-grid applications, which could stay focused on utility data and application requirements, help to achieve modularity and scalability, and deal with security at all levels. However, to be able to use all services, some features would not only require proper configuration on the last mile, but may also need an evolution of the information system, which is due in any case because IPv6 adoption for the last mile requires changes on the headend system and Meter Data Management System (MDMS) to deal with IPv6 address of meters. For example, the use of DNS may allow devices to automatically register their names and the services they offer which can simplify add/move/change operations on the last-mile infrastructure.

When focusing on the particular use case of AMI, with millions of endpoints with constrained resources and subnets built with low bandwidth, it is important to stress that gathering network statistics for network management can be achieved through a pull model (for example, Simple Network Management Protocol (SNMP)), as well as a push model (for example, IPfix). The push model represents a key feature to scale network management to millions of nodes that have scarce CPU resources.

Therefore, although not restricted to IPv6, the overview of network services as shown in Table 2 is an opportunity to introduce a new protocol called Constrained Application Protocol (CoAP) designed by the IETF Constrained Restful Environments (CoRE) WG. CoAP is a new lightweight application protocol for constrained devices such as those deployed in IPv6/6LoWPAN FAN infrastructures. Although CoAP can be used end to end, the architecture also supports proxies performing a mapping function between CoAP and HTTP representational state transfer (Rest) API, independent of the application. CoAP supports various modes of caching and traffic flow (UDP binding with optional reliability supporting unicast and multicast requests, asynchronous message exchanges, etc.), which can be useful in AMI. Although CoAP is not yet fully mature and widely deployed as a protocol, its progress is significant with about a dozen companies having implemented CoAP with several successful interoperability tests. It will definitively be a key protocol of an IPv6-based FAN deployment.

The adoption of IP-based networking for all smart-grid services allows all devices involved in the delivery of these services to be managed through a single network view. All devices and the relationships between them at the IP level can be defined in the network management application and the impact of a failure of communication to any given device can be instantly evaluated and displayed.

Table 2: Taking Advantage of IPv6 Network Services when deploying IoT

Network Services	Layers and Services	Benefits
Unique device's addressing (Network Layer)	From IPv4 (32-bit address space, now deprecated at IANA) to IPv6 (128-bit address space), including multiple scopes (global, private, link)	Large address space able to cope with the IoT evolution. Private or public infrastructure
Address auto-configuration (Network Layer)	Manual (IPv4/IPv6), stateless (IPv6) and stateful (DHCP for IPv4 and IPv6), Prefix Delegation (DHCPv6 PD)	Centralized or distributed address management. Additional DHCP options Zero Touch Provisioning
Media independency (PHY & MAC layers)	IEEE 802.3 [i.31] Ethernet, IEEE 802.11 [i.19] Wi-Fi, IEEE 802.16 [i.33] WiMAX, IEEE 802.15.4g/e [i.20], [i.22] RF 6LoWPAN, IEEE 1901.2a [i.2] NB-PLC 6LoWPAN Serial, ATM, FR, SONET/SDH	Media diversity for local and backhaul communications Smooth evolution over long lifetime period (see note)
Routing (Network Layer)	Static, RIP, OSPF, E-IGRP, IS-IS, MP-BGP, RPL (IPv6 only)	Dynamic reactivity to communication and network device failures. Scalability of deployment
Data Integrity and Confidentiality, Privacy (all layers)	Layer-2 (MAC specific), Layer-3 (IPSec IPv4/IPv6), Layer-4 (TCP/TLS, UDP/DTLS) and Layer-7 (application dependent authentication & Encryption) Packet filtering, Deep packet inspection (DPI), Intrusion Detection Service (IDS), Flow monitoring	Multi layered secure networking
Multicast (Network layer)	IPv4/IPv6 multicast protocols: IGMP/MLD, PIM, MP-BGP	Scalable software upgrade, group commands
Quality of Services (QoS)	Specific MAC layers Class of Services (CoS), i.e. Ethernet, WiMAX IPv4/IPv6 QoS Differentiated Services architecture	Multi services field area networks Prioritization of data traffic Service Level Agreement
Network Segmentation and isolation	Virtual Private Networks (Layer-3), i.e. IPSec VPN, VRF-Lite	Shared infrastructures but dedicated and isolated traffic paths for critical applications
Time Distribution	Layer-3, i.e. Network Time Protocol version 4 (NTPv4)	Secure NTP4 for both IPv4 and IPv6
Management	DNS, IPFix, SNMP, CoAP, SSH, Telnet, XML/Netconf, etc.	Push and Pull management models Scalable end-point management
NOTE: IPv6/6LoWPAN is the only IP protocol version defined for IEEE 802.15.4g/e [i.20], [i.22] and IEEE 1901.2 [i.2].		

4.7 Conclusions

IPv6 can enable and sustain the growth rate of the IoT. It offers a future proof solution.

More and more SDOs (Standardization Development Organization) have decided to either transition to IPv6 or to develop new standards only based on IPv6. This is specifically the case for IoT related standards.

IPv6 does not only enable the scalability required by the IoT but also provides enhancement from IPv4 in the field of mobility support, stateless address auto-configuration, support of constraint devices and security to mention only a few of them.

Annex A:
Authors & contributors

The following people have contributed to the present document:

Rapporteur:
Patrick Wetterwald - IoT Architecture and Standards - CTAO Cisco

Other contributors:
Mr. Latif Ladid, Chair, ETSI IP6 ISG, University of Luxembourg

Mr. Pascal Thubert, CTAO Cisco

Ms. Samita Chakrabarti, IETF 6lo chair

Annex B: Bibliography

IETF RFC 6550: "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks".

NOTE: Available at https://tools.ietf.org/html/rfc6550.

History

Document history		
V1.1.1	June 2017	Publication