INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2017-2020

SG20-TD613/GEN

STUDY GROUP 20

Original: English

Question(s): 3/20 Geneva, 24 January 2018

TD

Source: Editor

Title: Output of Draft Recommendation Y.IPv6RefModel “Reference model of IPv6 subnet addressing plan for Internet of things deployment” from Q3/20 e-meeting December 2017

Purpose: Discussion

Contact: Sébastien Ziegler
Mandat International
Switzerland

Tel: +41227744222
E-mail: s.ziegler@mandint.org

Editor note: This document contains the Draft Recommendation Y.IPv6RefModel discussed during the Q3/20 e-meeting held in December 2017. It also includes the editorial notes collected during the Q3/20 e-meeting.

Keywords: IPv6 Addressing Plan, Internet of Things, Global Routing Prefix Allocation

Abstract: This document incorporates the main discussion points for the Draft Recommendation Y.IPv6RefModel from the ITU-T SG20 meeting in September 2017. It also includes the main updates to the title of the Draft Recommendation from the September meeting.

Editor Note: The keywords mentioned in the document need to be consistent.

Keywords: IPv6 Addressing Plan, Internet of Things, Global Routing Prefix Allocation

Recommendation ITU-T Y.IPv6RefModel specifies an optional reference model of an IPv6 addressing plan for Internet of things (IoT) deployment by smart cities, public administrations and companies. It takes into account the growing importance of the Internet of things and IPv6. The specified addressing plan is provided as a reference model that can be adapted and customized by the end-user. It intends to simplify IPv6 addressing plan management and consistency and takes into account scalability requirements and the need to ease the transition from IPv4 to IPv6.

Y.IPv6RefModel

Reference model of IPv6 subnet addressing plan for Internet of things deployment

Summary

Recommendation ITU-T Y. IPv6RefModel specifies an optional reference model of an IPv6 addressing plan for Internet of things (IOT), whose deployment by smart cities, public administrations and companies is of the utmost importance. It addresses the needs, in terms of large-scale deployments and the transition from IPv4 to IPv6.

Introduction

Editor Notes: The meeting suggested to review the role of ICANN in the text below.

The Internet transition towards Internet Protocol version 6 (IPv6) is accelerating. As an illustration, by December 2017, Google servers received up to 21% of Internet traffic based on IPv6, from only 14% one year earlier. IPv6 has a direct impact on many Internet of things (IoT)-related standards. IPv6 is the de-facto protocol impacting the complete Internet architecture as it becomes more and more available. IPv6 provides a very large addressing capacity, enabling, potentially, the provision of a unique address to each and every IoT device. In parallel, it appears that several emerging IoT standards are converging towards IPv6 at the networking layer. In addition, the Internet Engineering Task Force (IETF) is working on extending IPv6 integration and interoperability with existing IoT standards.

The IPv6 standard has been properly defined by the IETF, which has assumed the primary and leading role in standardizing the Internet Protocol. Moreover, the IPv6 Forum and other relevant forums and consortia are playing a critical role in the evolution and promotion of IPv6 by improving market and end-user awareness. An IPv6 address is composed of several segments, including a global routing prefix (similar to the subnet in IPv4) and an interface ID. By adopting IPv6, end-users receive large ranges of IP addresses. Discussing IPv6 address assignment to end sites, IETF RFC 6177 [1]states that *"The exact choice of how much address space to assign end sites is an issue for the operational community."* ICANN and the Regional Internet Registries (RIRs) play an important role in managing address space allocation to Internet service providers (ISPs). The current ISPs practice tend to allocate /48 or /64 prefixes to regular customers (e.g., homes) and up to /29 for companies registered at RIRs. When receiving IPv6 addresses from their ISPs (or directly from their RIR), end-users will usually get enough address space for configuring and manage many IPv6 subnets. It will lead to the creation of an IPv6 subnet address plan by the end-user. Designing an IPv6 subnet address plan may consume a lot of time and resources if not properly structured since the beginning. The related learning curve has a cost for the end-user.

The emergence of the Internet of things has a disruptive impact on network design, deployment and management. The increasing number of end nodes tends to mechanically increase the size and complexity of addressing plans. Internet of things motes are often constrained and more fragile to cyberattacks, which may require specific firewalling and routing rules. Manageability is another important issue: increasing the size and scope of an addressing plan requires to adopt some logical and structured plan. Finally, the transition from IPv4 to IPv6 with a dual stack environment can end up in conflicting addressing plans and discrepancies.

Last but not least, another important challenge is the digital divide emerging between industrialized countries and developing countries. While the former group of country is evolving towards IPv6 adoption of their Internet traffic, the latter group of countries is predominantly focused on IPv4 only network environment. The Recommendation intends to ease the adoption and transition to IPv6 by end-users in developing countries and to reduce the risks of a digital divide in terms of IPv6 adoption. A reference model for proper IPv6 addressing plans is intended to produce the following benefits and advantages:

- enabling end-users to benefit from generic addressing plans as a basis that can be easily adopted and customized to address specific needs and requirements;
- providing a methodology and reference model that will reduce the risks of fragmented and difficult to manage addressing plans, or require costly reconfiguration due to unanticipated development of the IoT domain;
- easing the deployment, management and evolution of networks for the IoT, with a direct impact in minimizing the deployment and maintenance costs;
- enabling distinct entities to share a common addressing plan, easing interoperability and shared maintenance, including third party services;
- providing a resource for large public and private entities to define and adopt consistent addressing plans across various locations;
- providing a reference model for subnet addressing plan that can ease the adoption of IPv6 in developing countries.

Considering the scale and potential of such addressing space, defining and proposing a reference model for an IPv6 addressing plan for IoT deployment by smart cities, public administrations and companies is of the utmost importance.

This Recommendation has been carried out in consultation with the IETF, the IPv6 Forum, ETSI and other relevant stakeholders and academic partners working on IPv6-based IoT deployment. The proposed Recommendation is expected to take into account the ongoing and future evolution of IPv6-related RFCs and the IoT domain. It is expected to serve as a reference model to be adapted and customized by end-users in order to address their specific needs and requirements.

Table of Content

Keywords

Addressing plan, Internet of things, IPv6, public administrations

1 Scope

Editor Notes: It was suggested to replace "end-users" with "all relevant stakeholders" in this draft recommendation (including abstract), or to define end-users in future contributions. The editor should use consistent terminology when referring to the intended users of the draft recommendation.

Editor Notes: It was suggested to include reference to the actual IPv6 adoption statistics. Highlight what the problem is and what is the role of the various bodies such as RIRs.

This Recommendation designs and provides a reference model for an IPv6 addressing plan for Internet of Things (IoT) deployments by smart cities, public administrations and companies. The work solely focuses on end-user side IPv6 subnet addressing plans. More specifically, this Recommendation:

1) collects relevant information considering the on-going activities on IPv6-based IoT deployments;
2) provides a reference model of IPv6 subnet addressing plan for IoT deployment by smart cities, public administrations and companies (directed towards the benefit of end-users).

2 References

Editor Notes: The Meeting suggested to check and not to mention in this section IETF RFCs that are deprecated (such as RFC 2460 and RFC3513), even if they are mentioned in the IPv6 historic introduction.

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.2051] Recommendation ITU-T Y.2051 (2008), *General overview of IPv6-based NGN.*

[ITU-T Y.2052] Recommendation ITU-T Y.2052 (2008), *Framework of multi-homing in IPv6-based NGN.*

[ITU-T Y.2053] Recommendation ITU-T Y.2053 (2008), *Functional requirements for IPv6 migration in NGN*

[ITU-T Y.2054] Recommendation ITU-T Y.2054 (2008), *Framework to support signalling for IPv6-based NGN*

[ITU-T Y.4000] Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things*

[IETF RFC 760] RFC 760 (1980), *DoD standard Internet Protocol.*

[IETF RFC 791] RFC 791 (1981), *Internet Protocol, DARPA Internet Program, Protocol Specification.*

[IETF RFC 2460] RFC 2460 (1998), *Internet Protocol, Version 6 (IPv6) Specification.*

[IETF RFC 3587] RFC 3587 (2003), - IPv6 Global Unicast Address Format.

[IETF RFC 3513] RFC 3513 (2003), - Internet Protocol Version 6 (IPv6) Addressing Architecture.

[IETF RFC 8200] RFC 8200 (2017), *Internet Protocol, Version 6 (IPv6) Specification.*

2 Definitions

Editor Notes: The IETC RFC Numbers are to be updated.

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

Internet of things (IoT) [ITU-T Y.2060]**:** A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies.

Device [ITU-T Y.2060]**:** With regard to the Internet of things, this is a piece of equipment with the mandatory capabilities of communication and the optional capabilities of sensing, actuation, data capture, data storage and data processing.

Internet Protocol: The Internet Protocol refers to the protocols of communication specified by the IETF to enable data routing on the Internet and designed for use in interconnected systems of packet-switched computer communication networks. Two main versions exist: IPv4 ([IETF RFC 791)] and IPv6 ([IETF RFC 8200)].

Global Routing Prefix: As stated in [IETF RFC 3513] and [IETF RFC 3587], the Global Routing Prefix is a (typically hierarchically structured) value assigned to a site (a cluster of subnets/links). *The Global Routing Prefix corresponds to the segment of the IPv6 address assigned to a site.*

Subnet: A subnet in IPv6 is the part of the routing address (the first half of the IPv6 address) which is delegated by the ISP and managed by the site administrator [(IETF RFC 917 - Internet subnets)]. *It can be technically defined as the part of the IPv6 address comprised between the Global Routing Prefix and the Interface ID.*

Subnet ID: As stated in [IETF RFC 3513] and [IETF RFC 3587], a Subnet ID is an identifier of a link within a site. *It corresponds to the segment of the IPv6 address identifying the Subnet of an IPv6 address.*

Interface identifier or Interface ID: As stated in [IETF RFC 3513], Interface identifiers are used to identify interfaces on a link. *It corresponds to the part of the IPv6 address used to identify the interface or end node, and which, in the IoT, usually corresponds to the last 64 bits of the IPv6 address. The IPv6 Interface ID is often generated on the basis of the MAC address of the interface.*

~~**End-User: A human being, organization, or telecommunications system that accesses the network in order to communicate via the services provided by the network. [ITU-R]**~~

~~**An end-user is an entity (typically a user), associated with one or multiple subscriptions through identities (e.g., IMSIs, MSISDNs, IMPIs, IMPUs and application-specific identities). In the 3GPP system an end-user is characterised by an end-user identity. [ITU-T]**~~

End-User: The actual user of the products or services. [ITU-T Y.1910 (09/2008)]

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CoAP	Constrained Application Protocol
DMZ	Demilitarized Zone (part of the network directly connected to the Internet)
IAB	Internet Architecture Board
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communication Technologies
ID	Identifier
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
LAN	Local Area Network
MAC	Media Access Control
PAN	Personal Area Network
RFC	Request For Comments
RIR	Regional Internet Registry
SME	Small and Medium-sized Enterprise
WAN	Wide Area Network
WSN	Wireless Sensor Network

5 Conventions

In this Recommendation:

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords "can optionally" and "may" indicate an optional requirement which is permissible, without implying any sense of being recommended. These terms are not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Introduction to Internet Protocol version 6

Editor notes: The editor should provide future plan to the RIR communities to invite comments. Progress of the coordination with RIRs should be reported in the future.

In general, internet Protocol (IP) addresses refer to the unique numbers assigned to every computer network interface, or device that is connected to the Internet. Among other important functions, they identify every device connected to the Internet, whether it is a web server, smartphone, mail server, or laptop. There are currently two different versions of IP addresses in use—IPv4 and IPv6 [b-ICANN]. The IPv4 serves as the fourth version in the development of the IP. It is the first version of the protocol to be widely deployed. With a 32-bit address format, IPv4 can handle a maximum 4.3 billion unique IP addresses [b-CISCO].However, there are a limited number of addresses that can be assigned using IPv4 and the supply of these addresses is getting exhausted.

In line with the exhaustion of IPv4 addresses (as a result of the exploding demand for IP addresses), in recent years, there has been an evident transition from IPv4 to IPv6.

There are currently two different versions of IP addresses in use—IPv4 and IPv6

The introduction of IPv6 provides a much larger address pool than IPv4. IPv6 has a 128-bit address format. It can support 3.4 x 10^{38} or 340,282,366,920,938,463,463,374,607,431,768,211,456 unique IP addresses [b-CISCO].

IPv6 was initially designed and specified by the IETF to address IPv4 limitations. IPv4 was specified in 1980 by the IETF (as [IETF RFC 760] and later [IETF RFC 791]) at a time when the global adoption and the successful evolution of the Internet was not yet foreseen. Anticipating the scalability requirements and the limited address space of IPv4, the IETF developed the Internet protocol version 6 (IPv6), originally specified as [b-IETF RFC 1883] and later replaced by [IETF RFC 2460] and updated by [IETF RFC 8200]. IPv6 offers a highly scalable addressing capacity with 128-bit addresses, as well as several enhancements compared with IPv4.

The IETF has further developed a set of RFCs to better address the IoT requirements. New IETF standards, such as IPv6 over low power wireless personal area networks (6LoWPAN), constrained application protocol (CoAP), IPv6 routing protocol for low power and lossy networks (RPL), and IPv6 over time slotted channel hopping (6TiSCH), have been specified to specifically adapt IPv6 to constrained devices and IoT networks.

Other standards developing organizations (SDOs) have also progressively aligned their own IoT standards towards IPv6 as addressing layer. Several examples include but are not limited to:

- oneM2M, which is fully IPv6 compliant[b-oneM2M];
- lightweight M2M (LWM2M) developed by OMA, which is fully IPv6 and CoAP compliant [b-openmobile];
- ZigBee with its ZigBee IP version, which is natively IPv6 compliant [b-ZigBee]];
- Bluetooth low energy, which can be mapped on IPv6 [b-Bluetooth];
- standards using non-IP buses, such as KNX, that have developed IPv6 versions and specified application programming interfaces (APIs)[b-KNX].

The potential and relevance of IPv6 for the IoT has been researched and confirmed by several research projects, such as IoT6.[1]

- they highlight some key benefits related to IPv6 properties, including inter alia: A high scalability in terms of addressing, with 2^{128} unique addresses;
- auto-configuration mechanisms;
- availability of open source stacks and implementations;
- worldwide availability;
- availability of security and encryption enablers, such as IPSec.

In 2012, the IETF adopted the [b-IETF RFC 6540] requesting that all IP-capable nodes support IPv6, positioning IPv6 as the default IP protocol for the future.

In November 2016, the Internet Architecture Board (IAB) followed the IETF by adopting an official statement mentioning that "*the IAB expects that the IETF will stop requiring IPv4 compatibility in new or extended protocols. Future IETF protocol work will then optimize for and depend on IPv6."* The IAB formally recommended that *"all networking standards assume the use of IPv6, and be written so they do not require IPv4. We [the IAB] recommend that existing standards be reviewed to ensure they will work with IPv6, and use IPv6 examples."* The IAB also formally encourages "*the industry to develop strategies for IPv6-only operation***.** [b-IAB]

7 Preventing a New Digital Divide

IPv6 deployment is becoming largely adopted in many industrialized countries. As an illustration, in December 2017, Internet traffic on Google servers was up to 21% IPv6-based. However, there was a strong unbalanced between adoption in developing countries and industrialized countries. According to Google IPv6 statistics, while countries such as Belgium (49.8% IPv6 traffic), Greece (33.9% IPv6 traffic), Germany (33.6%IPv6 traffic), and US (33.1% IPv6 traffic) are actively adopting IPv6, most developing countries are lagging behind. There are a few remarkable regional exceptions such as Uruguay, India, Brazil, Peru, Malaysia and Saudi Arabia, but the vast majority of developing countries are close to 0% of IPv6 adoption. The risk of a new digital divide is real.

Despite the decision of the IAB and the promising numbers relating to IPv6 adoption in some countries, complete transition from IPv4 is not devoid of challenges. There are multiple factors that will affect the future IPv6 adoption mainly related to end-user awareness and adoption.

The address allocation is jointly managed by ICANN and the Regional Internet Registries (RIRs). In general, the RIRs have developed clear policies regarding IP address allocations to their members and ISPs in general. However, they did not specify how end-users should plan and structure their subnets. The proposed Reference Model of IPv6 subnet addressing plan for IoT deployment described

---

[1] This is a 3 year FP7 European research project on the future IoT. It aims to explore the potential of IPv6 and related standards (6LoWPAN, CORE, COAP, etc.) to overcome the current shortcomings and fragmentation of IoT.

in this Recommendation intends to complement and support the existing IPv6 allocation policies adopted by the RIRs. It provides the potential end-users with a reference model that can ease the adoption, planning and deployment of IPv6 in a way that anticipates the Internet of Things development and expansion.

8 Use cases and usability

IPv6 is likely to be used as an addressing protocol for large scale IoT deployments in the infrastructure of smart cities, public utilities, companies and smart buildings. In this context, a strategic issue is to adopt an IPv6 addressing plan that is able to address the evolving nature and growing number of IoT systems to be deployed in the future, as well as to take into account the progressive transition from IPv4 to IPv6.

Below are some examples of large scale IPv6-based IoT deployments:

- Bechtel, a global company with a presence in over 140 countries, has adopted and used IPv6 to connect all its information and communication technology (ICT) infrastructure all over the world through an integrated IPv6 network, enabling the company to remotely access any IP connected resource. It enabled Bechtel to interconnect together resources and communicating devices located in distinct countries. The adoption of IPv6 enables the company to simplify its network management and to benefit from features such as auto configuration and to leverage on IPv6 addressing capacity to ease the integration of distributed resources with SaaS solutions. Such evolution was driven by economies of scales and a need to simplify their network deployment and management [b-Microsoft].
- Chinese authorities, during the 2008 Olympic Games, adopted and deployed IPv6 to manage public lightings and video monitoring around the main stadiums. The deployment was led by the China Education Research Network (CERNET). CERNET built an IPv6 only network, CNGI-CERNET2, connecting 25 core node points in 20 major cities of China [b-Campbell] [b-BeijingOlympic].
- IPv6 deployment is gaining momentum in China. China will increase its investment in information infrastructure construction in accordance with the National Strategically Emerging Industries Development Planning in the 13th Five-Year Plan and the National Information Planning in the 13th Five-Year Plan. This being done to facilitate the healthy development of new generation information technology. Moreover, during the 13th Five-Year Plan, new generation Internet and other network infrastructure will be deployed and applied in succession, which will give a significant boost to the development of IPv6, especially within the EXCITING project, under the Horizon 2020.
- The IoT Lab European research project adopted IPv6 to remotely interconnect and federate several IoT testbeds together, including testbeds located outside of Europe. The use of IPv6 enables to aggregate heterogeneous and geographically distributed IoT resources together and to simplify their management. The same model is currently used by the IoT lab to aggregate IoT resources from various smart cities into a consistent addressing plan. [b-IoTlab].

This Recommendation is intended to provide interested ITU members with some guidance and a reference model that can be customized to the specific needs of each user. It is of particular interest for entities that are expected to handle large scale IoT deployments, but may be used for smaller Internet of things deployments as well.

9 IPv6 address structure

An IPv6 address is 128 bits long. As illustrated in Figure 1, an IPv6 address is composed of several segments:

- The routing address, which is split into two parts:
    - global routing prefix assigned to a site;
    - The subnet ID which is managed by the site and enables to differentiate several subnetworks.
- The interface ID, which corresponds to a specific interface of end-node.

The following diagram in Figure 1 summarizes the structure of the IPv6 address structure, in which the regular IPv6 Interface ID is 64 bits long.

n bits	64-n bits	64 bits
Global Routing Prefix	Subnet ID	Interface ID (or Host ID)

Figure. 1 IPv6 address structure

This structure and format of an IPv6 address enables hierarchical address allocation.

[b-IETF RFC 3177] initially specified a /48 routing prefix to be allocated to end-consumers. It has been updated by [b-IETF RFC 6177], which provides more flexibility by recommending to give home sites "significantly more than /64. /56 allocations are likely to become a mainstream practice for individual end-users (homes), while /48 allocations are likely to be the mainstream model for small and medium-sized enterprises (SMEs) and administrations. The policy for global routing prefix length allocation may vary from one region to another. It is handled by the Regional Internet Registries (RIRs) and the ISPs in order to address their end-user needs. Larger networks owners, such as large companies, can get up to /32 global routing prefixes.

For public administrations and large companies, it may be relevant to obtain a routing prefix directly from a RIR in order to become provider independent. It gives them the flexibility to use several ISPs or simply to change their ISPs without impacting their internal network configuration. In such a case, the minimum routing prefix size supported by RIRs is /48.

In the Recommendation, we will consider various length of global routing prefix allocations. RIRs adapt the size of the Global Routing Prefix to the variable needs of their clients. As an example, in 2016, ARIN allocated 48% of /48, 24% of /44, 22% of /40, and 5% of /36. We may consider the /48 global routing prefix as the prevalent routing prefix for SMEs and local public administrations, which leaves 16 bits to be used by the site administrator for configuring and managing subnets. In formal IPv6 notation, the default 16 bits are represented by 4 hexadecimal digits of the IPv6 address.

The Reference Model of IPv6 Subnet Addressing Plan is compatible with the use of current IPv6 transition mechanisms, such as the Stateless IP/ICMP Translation (SIIT), Nat 64, and others Basic Transition Mechanisms for IPv6 Hosts and Routers specified in IETF RFC 4213. The use of encapsulation mechanisms and tunneling solutions such as Teredo ("Tunneling IPv6 over UDP through NAT" specified in IETF RFC 4380) for deploying IPv6 over IPv4 networks have been designed in order to be transparent to both ends of the transmission and they don't affect the addressing of the end nodes, and *a fortiori* the subnet addressing plans. Moreover, it has to be noted that according to IAB statement, transition mechanisms should progressively disappear and be replaced by IPv6 only networks.

Editor Note: The meeting suggested to simplify the wording of the above paragraph.

10 Subnet address requirements,

Editor notes: there are a large number of ipv4-ipv6 transition and migration strategies: Teredo, 6to4, etc. In dual stack environments, it will be essential to develop an ipv6 addressing scheme which is appropriate to the transition or migration schemes that may be adopted. The cost/benefit analyses of these approaches and addressing schemes will need careful consideration. That work should be developed in consultation with those who have operational expertise in running such networks vis the RIR policy making fora.

A subnet addressing plan should take into account the following requirements:

- Scalability: The number of IoT connected devices is expected to substantially grow over time, with tens of Billions communicating devices. [b-Ericsson] Hence, a single company or public administration can quickly reach several tens of thousands IoT devices.
- Future proof: New IoT devices and technologies are expected to emerge over time, leading to the inclusion of new subnetworks.
- Manageability: The growing number of IoT connected devices will require the use of logical and well-structured subnets to simplify maintenance and control of IoT networks.

Moreover, during the transition phase from IPv4 and IPv6, the IPv6 subnet addressing plans in dual stack network environments should enable the coexistence of consistent addressing plans between IPv4 and IPv6 as much as possible.

Planning, deploying and configuring an address plan consume resources. The proposed Reference Model is flexible and can be adapted to end-user needs, while enabling them to benefit from a model that is optimized to anticipate the development of Internet of Things. Such a model is expected to save time and cost to the end-user by:

- easing the structuring of their subnet addressing plans;
- enabling the end-users to adopt a smooth transition from IPv4, to dual stack environment (IPv4 and IPv6) and finally to IPv6 only deployments;
- benefiting from an address plan that anticipates the expected expansion of Internet of Things deployments and will avoid costly ulterior adaptations when deploying their Internet of Things.

11 Reference model for IPv6 subnet addressing plan

As previously mentioned, the IPv6 address plan is split in distinct segments controlled by distinct entities. The ISP is in charge of allocating the global routing prefix and the interface ID is usually determined by the connected device. The end-user is ultimately able to control the subnet ID. With a /48 allocation, the subnet ID is 16 bits long, which translates into 65,536 available subnet IDs.

To enable mapping between and consistency between IPv4 and IPv6 subnet addressing plans, a dual strategy is proposed, with part of the IPv6 subnet addressing plan designed to map corresponding IPv4 addresses, with the possibility to extend the IPv6 subnet addressing plan and benefit from its scalability where this constraint is not required.

The reference model for the IPv6 subnet addressing plan is structured as follow:

A first hexadecimal digit (A), equivalent to 4 bits, is used to identify buildings and locations. It can identify up to 16 distinct locations. One or several hexadecimal digits can also be reserved for subnets that are not linked to any specific building or location.

A second hexadecimal digit (B), equivalent to 4 bits, is used to classify subnetworks among distinct categories:

- demilitarized zone (DMZ) category: used for public servers for the segment of the network directly connected to the Internet and to external interactions;
- internal servers category: reserved for the internal servers, backups and storing capacities;
- regular local area network (LAN) category;
- Internet of things category;
- other category: reserved for any other specific allocation, and which may also be used to extend one of the previous categories. For instance, it can be used to extend the IoT category to 50% of the subnets.

A third (C) and fourth (D) hexadecimal digits, equivalent to 4 bits each, are used to specify specific subnets. However, when IPv4 addresses require mapping with IPv6, the first and the fourth hexadecimal digits are set to 0, as indicated in Figure 2.

	A	**B**	**C**	**D**
Dual IPv6 - IPv4	0	Category	Subnet	0
Pure IPv6	Prefix	Category	Subnet	Subnet

Figure. 2 Subnet ID structure

The proposed model enables a direct mapping between IPv4 and IPv6 addresses. It facilitates a smooth transition from IPv4 to IPv6 and simplifies the coexistence of IPv6 and IPv4 addressing plans, while facilitating the transition towards IPv6 only networks (in line with the Internet Architecture Board recommendation). Where IPv4 is still required, it enables bidirectional mapping and translation of IPv4 addresses to IPv6 addresses and vice versa.

Figure 3 shows an example of reference model for the IPv6 subnet ID addressing plan based on [b-WAINA] (shared with support of Institute of Electrical and Electronics Engineers (IEEE) courtesy). The proposed model defines a two-stage addressing plan:

1. A dual IPv6-IPv4 addressing plan, with a perfect mapping of IPv6 addresses to IPv4 addresses, enabling a smooth transition from IPv4 to IPv6 with a consistent addressing plan.
2. An IPv6 only addressing plan, with the possibility of extending the addressing plan towards a larger number of end-nodes.

Network engineers can also combine addressing plans, by first reserving the IPv6 addresses used in the dual IPv6-IPv4 plan (A) for the legacy during the transition period, and in a second stage by using and allocating the additional IPv6 addresses available in the IPv6-only addressing plan for new IPv6-enabled devices and resources.

	Dual IPv6 - IPv4						Pure IPv6				
	IPv6				IPv4		IPv6				
Allocation	**A**	**B**	**C**	**D**	**octet**	**Nb**	**A**	**B**	**C**	**D**	**Nb**
DMZ	0	**0**	0-f	0	0 - 15	32	0-f	**0**	0-f	0-f	16 x 8'192
	0	**1**	0-f	0	16 - 31		0-f	**1**	0-f	0-f	
Internal Servers	0	**2**	0-f	0	32 - 47	32	0-f	**2**	0-f	0-f	16 x 8'192
	0	**3**	0-f	0	48 - 63		0-f	**3**	0-f	0-f	
Regular LAN	0	**4**	0-f	0	64 - 79	64	0-f	**4**	0-f	0-f	16 x 16'384
	0	**5**	0-f	0	80 - 95		0-f	**5**	0-f	0-f	
	0	**6**	0-f	0	96 - 111		0-f	**6**	0-f	0-f	
	0	**7**	0-f	0	112 - 127		0-f	**7**	0-f	0-f	
IoT & Building Automation	0	**8**	0-f	0	128 - 143	64	0-f	**8**	0-f	0-f	16 x 16'384
	0	**9**	0-f	0	144 - 159		0-f	**9**	0-f	0-f	
	0	**a**	0-f	0	160 - 175		0-f	**a**	0-f	0-f	
	0	**b**	0-f	0	176 - 191		0-f	**b**	0-f	0-f	
Others	0	**c**	0-f	0	192 - 207	64	0-f	**c**	0-f	0-f	16 x 16'384
	0	**d**	0-f	0	208 - 223		0-f	**d**	0-f	0-f	
	0	**e**	0-f	0	224 - 239		0-f	**e**	0-f	0-f	
	0	**f**	0-f	0	240 - 255		0-f	**f**	0-f	0-f	

Figure. 3 Subnet ID addressing plan

The proposed addressing plan exploits several properties:

- The addressing plan enables a direct and simple mapping of IPv6 addresses on IPv4 addresses;
- The specified segmentation enables to use bit-based filtering mechanisms to consistently differentiate IPv6 addresses according to their subnet category allocation;
- A fourth of the addressing plan is reserved either for other subnetworks or to extend one of the previous subnetwork categories. This enables for instance to allocate up to half of the addresses to IoT devices for entities with large IoT deployments and up to half of the addresses to the regular LAN for entities with limited foreseeable IoT deployments;

The proposed addressing plan enables to create and manage up to 65,536 subnetworks, including 32,768 subnetworks for the IoT. Subsequently, each IoT subnetwork could handle up to 16 Billion of Billions of unique end nodes and unique host ID. This is far larger than the whole Internet with each and every server on earth. This capacity is expected to be largely sufficient to address industry and public administrations requirements. For entities requiring a larger number of subnets, the possibility remains to extend the Global routing prefix to dramatically extend the number of subnets.

The proposed model has the advantage of enabling users in taking full advantage of their IPv4 addressing potential for dual stack deployments, while benefiting from the full IPv6 addressing potential for devices and nodes that can emanate from IPv4.

The proposed addressing plan enables network administrators to easily allocate addresses in a structured manner, and to identify and manage end nodes accordingly. Such structure also eases cybersecurity management by enabling the configuration of differentiated firewall rules according to the IPv6 addresses.

The addressing plan described above is illustrative. It can be customized to specific needs and requirements. The address ranges allocated to each category of subnetworks can be adapted accordingly.

112 Adaptation of the reference model to variable global routing prefix allocations

The following section presents variable models adapted to distinct lengths of global routing prefix allocation.

12.1 /56 global routing prefix allocation

In case of a /56 allocation, the size of the subnets is smaller and more limited than for the /48. The mapping is highly simplified as a direct and complete bidirectional mapping between IPv4 and IPv6 subnet addresses can occur. As an implicit consequence, there is no specific range for IPv6 only subnet allocation. Figure 4 presents the adaptation for such /56 global routing prefix allocations.

In this case, the hexadecimal digit used to filter and dissociate the addresses per category is the column corresponding to the first hexadecimal digit A.

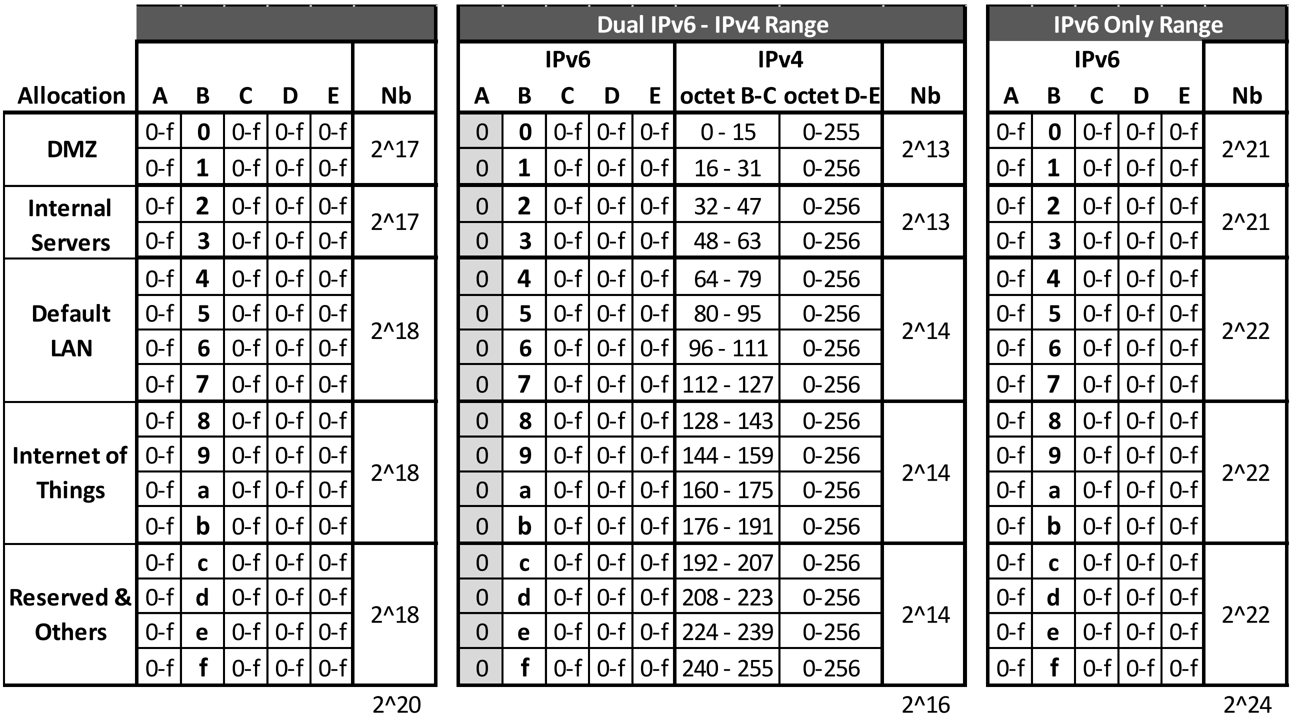
	Range			**Dual IPv4 IPv6 Range**			
Allocation	**A**	**B**	**Nb**	**A**	**B**	**IPv4 octet**	**Nb**
DMZ	**0**	0-f	32	**0**	0-f	0 - 15	32
	1	0-f		**1**	0-f	16 - 31	
Internal Servers	**2**	0-f	32	**2**	0-f	32 - 47	32
	3	0-f		**3**	0-f	48 - 63	
Default LAN	**4**	0-f	64	**4**	0-f	64 - 79	64
	5	0-f		**5**	0-f	80 - 95	
	6	0-f		**6**	0-f	96 - 111	
	7	0-f		**7**	0-f	112 - 127	
Internet of Things	**8**	0-f	64	**8**	0-f	128 - 143	64
	9	0-f		**9**	0-f	144 - 159	
	a	0-f		**a**	0-f	160 - 175	
	b	0-f		**b**	0-f	176 - 191	
Reserved & Others	**c**	0-f	64	**c**	0-f	192 - 207	64
	d	0-f		**d**	0-f	208 - 223	
	e	0-f		**e**	0-f	224 - 239	
	f	0-f		**f**	0-f	240 - 255	
			256				256

Figure 4.Model for a /56 global routing prefix allocation

12.2 /44 global routing prefix allocation

In case of a /44 allocation, the size of the subnet becomes larger than quite larger than a /48. As a consequence, the user can add a higher level of segmentation of the addressing plan. **Error! Reference source not found.** presents the adaptation for such allocations.

In this case, the hexadecimal digit used to filter and dissociate the addresses per main category is the column corresponding to the second hexadecimal digit B. It enables network engineers to address larger deployments with more locations to be identified with digit A, and more end-nodes to be identified with the additional digits E and F.



							Dual IPv6 - IPv4 Range								IPv6 Only Range					
							IPv6					IPv4			IPv6					
Allocation	A	B	C	D	E	Nb	A	B	C	D	E	octet B-C	octet D-E	Nb	A	B	C	D	E	Nb
DMZ	0-f	**0**	0-f	0-f	0-f	2^17	0	**0**	0-f	0-f	0-f	0 - 15	0-255	2^13	0-f	**0**	0-f	0-f	0-f	2^21
	0-f	**1**	0-f	0-f	0-f		0	**1**	0-f	0-f	0-f	16 - 31	0-256		0-f	**1**	0-f	0-f	0-f	
Internal Servers	0-f	**2**	0-f	0-f	0-f	2^17	0	**2**	0-f	0-f	0-f	32 - 47	0-256	2^13	0-f	**2**	0-f	0-f	0-f	2^21
	0-f	**3**	0-f	0-f	0-f		0	**3**	0-f	0-f	0-f	48 - 63	0-256		0-f	**3**	0-f	0-f	0-f	
Default LAN	0-f	**4**	0-f	0-f	0-f	2^18	0	**4**	0-f	0-f	0-f	64 - 79	0-256	2^14	0-f	**4**	0-f	0-f	0-f	2^22
	0-f	**5**	0-f	0-f	0-f		0	**5**	0-f	0-f	0-f	80 - 95	0-256		0-f	**5**	0-f	0-f	0-f	
	0-f	**6**	0-f	0-f	0-f		0	**6**	0-f	0-f	0-f	96 - 111	0-256		0-f	**6**	0-f	0-f	0-f	
	0-f	**7**	0-f	0-f	0-f		0	**7**	0-f	0-f	0-f	112 - 127	0-256		0-f	**7**	0-f	0-f	0-f	
Internet of Things	0-f	**8**	0-f	0-f	0-f	2^18	0	**8**	0-f	0-f	0-f	128 - 143	0-256	2^14	0-f	**8**	0-f	0-f	0-f	2^22
	0-f	**9**	0-f	0-f	0-f		0	**9**	0-f	0-f	0-f	144 - 159	0-256		0-f	**9**	0-f	0-f	0-f	
	0-f	**a**	0-f	0-f	0-f		0	**a**	0-f	0-f	0-f	160 - 175	0-256		0-f	**a**	0-f	0-f	0-f	
	0-f	**b**	0-f	0-f	0-f		0	**b**	0-f	0-f	0-f	176 - 191	0-256		0-f	**b**	0-f	0-f	0-f	
Reserved & Others	0-f	**c**	0-f	0-f	0-f	2^18	0	**c**	0-f	0-f	0-f	192 - 207	0-256	2^14	0-f	**c**	0-f	0-f	0-f	2^22
	0-f	**d**	0-f	0-f	0-f		0	**d**	0-f	0-f	0-f	208 - 223	0-256		0-f	**d**	0-f	0-f	0-f	
	0-f	**e**	0-f	0-f	0-f		0	**e**	0-f	0-f	0-f	224 - 239	0-256		0-f	**e**	0-f	0-f	0-f	
	0-f	**f**	0-f	0-f	0-f		0	**f**	0-f	0-f	0-f	240 - 255	0-256		0-f	**f**	0-f	0-f	0-f	
						2^20								2^16						2^24

Figure 5.Model for a /44 global routing prefix allocation

12.3 /40 global routing prefix allocation

In case of a /40 allocation, the size of the subnet becomes quite larger than a /48. As a consequence, the user can add a higher level of segmentation of the addressing plan. **Error! Reference source not found.**6 presents the adaptation for such allocations.

In this case, the hexadecimal digit used to filter and dissociate the addresses per main category is the column corresponding to the third hexadecimal digit C. It enables network engineers to address larger deployments with more locations to be identified with digits A and B, and more end-nodes to be identified with the additional digits E and F.

	Dual IPv6 - IPv4 Range									**IPv6 Only Range**						
	IPv6						**IPv4**			**IPv6**						
Allocation	**A**	**B**	**C**	**D**	**E**	**F**	**octet C-D**	**octet E-F**	**Nb**	**A**	**B**	**C**	**D**	**E**	**F**	**Nb**
DMZ	0	0	**0**	0-f	0-f	0-f	0 - 15	0-255	2^13	0-f	0-f	**0**	0-f	0-f	0-f	2^21
	0	0	**1**	0-f	0-f	0-f	16 - 31	0-256		0-f	0-f	**1**	0-f	0-f	0-f	
Internal Servers	0	0	**2**	0-f	0-f	0-f	32 - 47	0-256	2^13	0-f	0-f	**2**	0-f	0-f	0-f	2^21
	0	0	**3**	0-f	0-f	0-f	48 - 63	0-256		0-f	0-f	**3**	0-f	0-f	0-f	
Default LAN	0	0	**4**	0-f	0-f	0-f	64 - 79	0-256	2^14	0-f	0-f	**4**	0-f	0-f	0-f	2^22
	0	0	**5**	0-f	0-f	0-f	80 - 95	0-256		0-f	0-f	**5**	0-f	0-f	0-f	
	0	0	**6**	0-f	0-f	0-f	96 - 111	0-256		0-f	0-f	**6**	0-f	0-f	0-f	
	0	0	**7**	0-f	0-f	0-f	112 - 127	0-256		0-f	0-f	**7**	0-f	0-f	0-f	
Internet of Things	0	0	**8**	0-f	0-f	0-f	128 - 143	0-256	2^14	0-f	0-f	**8**	0-f	0-f	0-f	2^22
	0	0	**9**	0-f	0-f	0-f	144 - 159	0-256		0-f	0-f	**9**	0-f	0-f	0-f	
	0	0	**a**	0-f	0-f	0-f	160 - 175	0-256		0-f	0-f	**a**	0-f	0-f	0-f	
	0	0	**b**	0-f	0-f	0-f	176 - 191	0-256		0-f	0-f	**b**	0-f	0-f	0-f	
Reserved & Others	0	0	**c**	0-f	0-f	0-f	192 - 207	0-256	2^14	0-f	0-f	**c**	0-f	0-f	0-f	2^22
	0	0	**d**	0-f	0-f	0-f	208 - 223	0-256		0-f	0-f	**d**	0-f	0-f	0-f	
	0	0	**e**	0-f	0-f	0-f	224 - 239	0-256		0-f	0-f	**e**	0-f	0-f	0-f	
	0	0	**f**	0-f	0-f	0-f	240 - 255	0-256		0-f	0-f	**f**	0-f	0-f	0-f	
									2^16							2^24

Figure 6.Model for a /40 global routing prefix allocation

12.4 /36 global routing prefix allocation

In case of a /36 allocation, the size of the subnet becomes very large. As a consequence, the user can add a higher level of segmentation of the addressing plan. Figure 7 presents the adaptation for such allocations.

In this case, the hexadecimal digit used to filter and dissociate the addresses per category is the column corresponding to the third hexadecimal digit C (in yellow in the table).

	Address Range							
	IPv6							
Allocation	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**Nb**
DMZ	0-f	0-f	**0**	0-f	0-f	0-f	0-f	2^25
	0-f	0-f	**1**	0-f	0-f	0-f	0-f	
Internal Servers	0-f	0-f	**2**	0-f	0-f	0-f	0-f	2^25
	0-f	0-f	**3**	0-f	0-f	0-f	0-f	
Default LAN	0-f	0-f	**4**	0-f	0-f	0-f	0-f	2^26
	0-f	0-f	**5**	0-f	0-f	0-f	0-f	
	0-f	0-f	**6**	0-f	0-f	0-f	0-f	
	0-f	0-f	**7**	0-f	0-f	0-f	0-f	
Internet of Things	0-f	0-f	**8**	0-f	0-f	0-f	0-f	2^26
	0-f	0-f	**9**	0-f	0-f	0-f	0-f	
	0-f	0-f	**a**	0-f	0-f	0-f	0-f	
	0-f	0-f	**b**	0-f	0-f	0-f	0-f	
Reserved & Others	0-f	0-f	**c**	0-f	0-f	0-f	0-f	2^26
	0-f	0-f	**d**	0-f	0-f	0-f	0-f	
	0-f	0-f	**e**	0-f	0-f	0-f	0-f	
	0-f	0-f	**f**	0-f	0-f	0-f	0-f	
								2^28

	Dual IPv6 - IPv4									
	IPv6							IPv4		
Allocation	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**octet C-D**	**octet E-F**	**Nb**
DMZ	0	0	**0**	0-f	0-f	0-f	0	0 - 15	0-255	2^13
	0	0	**1**	0-f	0-f	0-f	0	16 - 31	0-256	
Internal Servers	0	0	**2**	0-f	0-f	0-f	0	32 - 47	0-256	2^13
	0	0	**3**	0-f	0-f	0-f	0	48 - 63	0-256	
Default LAN	0	0	**4**	0-f	0-f	0-f	0	64 - 79	0-256	2^14
	0	0	**5**	0-f	0-f	0-f	0	80 - 95	0-256	
	0	0	**6**	0-f	0-f	0-f	0	96 - 111	0-256	
	0	0	**7**	0-f	0-f	0-f	0	112 - 127	0-256	
Internet of Things	0	0	**8**	0-f	0-f	0-f	0	128 - 143	0-256	2^14
	0	0	**9**	0-f	0-f	0-f	0	144 - 159	0-256	
	0	0	**a**	0-f	0-f	0-f	0	160 - 175	0-256	
	0	0	**b**	0-f	0-f	0-f	0	176 - 191	0-256	
Reserved & Others	0	0	**c**	0-f	0-f	0-f	0	192 - 207	0-256	2^14
	0	0	**d**	0-f	0-f	0-f	0	208 - 223	0-256	
	0	0	**e**	0-f	0-f	0-f	0	224 - 239	0-256	
	0	0	**f**	0-f	0-f	0-f	0	240 - 255	0-256	
										2^16

	Pure IPv6							
	IPv6							
Allocation	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**Nb**
DMZ	0-f	0-f	**0**	0-f	0-f	0-f	0-f	2^25
	0-f	0-f	**1**	0-f	0-f	0-f	0-f	
Internal Servers	0-f	0-f	**2**	0-f	0-f	0-f	0-f	2^25
	0-f	0-f	**3**	0-f	0-f	0-f	0-f	
Default LAN	0-f	0-f	**4**	0-f	0-f	0-f	0-f	2^26
	0-f	0-f	**5**	0-f	0-f	0-f	0-f	
	0-f	0-f	**6**	0-f	0-f	0-f	0-f	
	0-f	0-f	**7**	0-f	0-f	0-f	0-f	
Internet of Things	0-f	0-f	**8**	0-f	0-f	0-f	0-f	2^26
	0-f	0-f	**9**	0-f	0-f	0-f	0-f	
	0-f	0-f	**a**	0-f	0-f	0-f	0-f	
	0-f	0-f	**b**	0-f	0-f	0-f	0-f	
Reserved & Others	0-f	0-f	**c**	0-f	0-f	0-f	0-f	2^26
	0-f	0-f	**d**	0-f	0-f	0-f	0-f	
	0-f	0-f	**e**	0-f	0-f	0-f	0-f	
	0-f	0-f	**f**	0-f	0-f	0-f	0-f	
								2^28

Figure 7. 36/ global routing prefix allocation

Bibliography

[b-ITU-T RES-T.64] Resolution RES-T.64 (2008), Resolution 64 – IP address allocation and encouraging the deployment of IPv6.

[b-IETF-RFC 6177] T. Narten, G. Huston, et S. University, IPv6 Address Assignment to End Sites. https://tools.ietf.org/html/rfc6177.

[b-IETF RFC 3587] R. M. Hinden et S. E. Deering, IPv6 Global Unicast Address Format. https://tools.ietf.org/html/rfc3587.

[b-IETF RFC 917] J. C. Mogul, Internet subnets (1984). https://tools.ietf.org/html/rfc917.

[b-CISCO] Routing and Bridging Guide, Cisco ACE Application Control Engine (2011)

[b-ICANN] Beginner’s Guide to Internet Protocol Addresses

[b-oneM2M] oneM2M. http://www.onem2m.org/.

[b-openmobile] OMA LightweightM2M (LWM2M) », Open Mobile Alliance. http://www.openmobilealliance.org/release/LightweightM2M/.

[b-ZigBee] ZigBee IP Specification », The ZigBee Alliance. http://www.zigbee.org/download/standard-zigbee-ip-specification/.

[b-Bluetooth] Bluetooth Low Energy. https://www.bluetooth.com/what-is-bluetooth-technology/how-it-works/low-energy.

[b-KNX] KNX Association. https://www.knx.org.

[b-IETF RFC 6540] C. Liljenstolpe, W. George, C. Donley, et L. Howard, IPv6 Support Required for All IP-Capable Nodes. https://tools.ietf.org/html/rfc6540.

[b-IAB] Morgan, IAB Statement on IPv6 , Internet Architecture Board, https://www.iab.org/2016/11/07/iab-statement-on-ipv6/.

[b-Microsoft] Bechtel Well Positioned to Serve Customers Using Microsoft & Cisco IPv6 Solution, Cisco and Microsoft (2007).

[b-Campbell] Dan Campbell, IPv6 gets a workout at Olympics », CGN, 20-août-2008. https://gcn.com/articles/2008/08/20/ipv6-gets-a-workout-at-olympics.aspx.

[b-BeijingOlympic] Beijing2008.cn leaps to next generation Net », Official website of the Beijing Olympic Games 2008, 31-2008. http://en.olympic.cn/08beijing/bocog/2008-05-31/1485914.html.

[b-IoTlab] IoT Lab, FP7 European Research project on IoT and Crowdsourcing. http://www.iotlab.eu/.

[b-IETF-RFC] IESG et IAB, IAB/IESG Recommendations on IPv6 Address Allocations to Sites. https://tools.ietf.org/html/rfc3177.

[b-Ericsson] L. M. Ericsson, More than 50 billion connected devices (2011).

[b-IEEE] S. Ziegler et L. Ladid, « Towards a Global IPv6 Addressing Model for the Internet of Things », in 2016 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA) (2016) p. 622- 627, DOI: 10.1109/WAINA.2016.178.

[b-O'Reilly Media] N.R Murphy, Malone.D. IPV6 Network Administration (2016).