ETSI GR IP6 001 V1.1.1 (2017-06)

IPv6 Deployment in the Enterprise

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/IP6-0001

Keywords

Internet, IoT, IPv6, Mobile, NFV, SDN

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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

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 outlines the motivation for the deployment of IPv6 within enterprises, the objectives, the benefits, the risks, the challenges, the technology guidelines, the different choices that arise when designing IPv6-only or dual-stack enterprise network, step-by-step process, the addressing plan, and the milestones.

With the growing number of users and the proliferation of smart devices and things, IPv4 address space exhaustion is a major Information and Communications Technology (ICT) issue. The current IPv4-based Internet can no longer sustain the explosive growth of ICT. Any organization that relies on the Internet to any extent need to be prepared, need to support IPv6. The move to IPv6 is inevitable, there is no alternative plan at this time. IPv6 is the cornerstone of our connected society. IPv6 offers important business and technical advantages. While all/most existing IPv4-based infrastructures will continue to work after the last IPv4 address is issued, enterprises may be tempted to put off transitioning to IPv6 till some later date. However postponing the inevitable can put an enterprise at a competitive disadvantage. The present document provides guidelines and recommendations on IPv6 deployment in the enterprise.

1 Scope

The present document outlines the motivation for the deployment of IPv6 in enterprises, the objectives, the benefits, the risks, the challenges, the technology guidelines, the different choices that arise when designing IPv6-only or dual-stack enterprise network, step-by-step process, the addressing plan, and the milestones.

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] IETF RFC 1918: "Address Allocation for Private Internets".

[i.2] IETF RFC 3493: "Basic Socket Interface Extensions for IPv6".

[i.3] IETF RFC 4193: "Unique Local IPv6 Unicast Addresses".

[i.4] IETF RFC 3531: "A Flexible Method for Managing the Assignment of Bits of an IPv6 Address Block".

[i.5] IETF RFC 3542: "Advanced Sockets Application Program Interface (API) for IPv6".

[i.6] IETF RFC 4193: "Unique Local IPv6 Unicast Addresses".

[i.7] IETF RFC 4380: "Teredo: Tunneling IPv6 over UDP through Network Address Translations".

[i.8] IETF RFC 5375: "The Locator/ID Separation Protocol (LISP)".

[i.9] IETF RFC 6146: "Stateful NAT64: - Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers".

[i.10] IETF RFC 6296: "IPv6 to IPv6 Network Prefix Translation".

[i.11] IETF RFC 6555: "Happy Eyeballs: Success with Dual-Stack Hosts".

[i.12] IETF RFC 7239: "Forwarded HTTP Extension".

[i.13] RIPE NCC: "Requirements for IPv6 in ICT Equipment".

NOTE: Available at https://www.ripe.net/publications/docs/ripe-554.

[i.14] IETF ID draft-troan-homenet-sadr-01: IPv6 Multihoming with Source Address Dependent Routing (SADR)".

[i.15] DomainKeys Identified Mail.

NOTE: Available at https://en.wikipedia.org/wiki/DomainKeys_Identified_Mail.

[i.16] IETF RFC 6145: "IP/ICMP Translation Algorithm".

3 Abbreviations

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

AAAA	DNS resource records (RRs) IPv6 address record
ACL	Access Control List
AFT	Address Family Translation
ARP	Address Resolution Protocol
ALG	Application-aware Logic
AV	Audio/Video
BCP	Best Current Practices
BGP	Border Gateway Protocol
BIND	Berkeley Internet Name Domain
BYOD	Bring your own device
CDN	Content Delivery Network
CG-NAT	Carrier-grade NAT (Network Address Translation)
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ERP	Enterprise Resource Planning
FQDN	Fully qualified domain name
GR	Group Report
HTTP	HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
ICT	Information and Communications Technology
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IoT	Internet of Things
IP	Internet Protocol
IPAM	IP Address Management
IPS	Intrusion Prevention Systems
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
ISC	Internet Systems Consortium
ISG	Industry Specification Group
IS-IS	Intermediate System to intermediate System
ISP	Internet Service Provider
LISP	Locator/Identifier Separation Protocol
LLMNR	Link-Local Multicast Name Resolution Protocol
LOB	Line of Business
MAC	Media Access Conrol address
MIB	Management information base
MiM	Man-in-the-Middle
MTA	Mail Transfer Agents
NAT	Network Address Translation
ND	Neighbour Discovery
NPTv6	Network Prefix Translation
OS	Operating System
OSX	Mac OS X™

NOTE 1: Unix-based graphical operating system developed and marketed by Apple Inc.

NOTE 2: Mac OS X™ is a trademark of Apple Inc., registered in the U.S. and other countries.

PA	Provider aggregatable
PI	Provider independent
RDNSS	Recursive DNS Server

RIPE	Réseaux IP Européens
RIR	Regional Internet Registry
RR	Resource Record
SADR	Source Address Dependent Routing
SIEM	Security Incident and Event Management
SLAAC	Stateless Address Auto Configuration
SLB	Server Load Balancer
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSDP	Simple Service Discovery Protocol
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
ULA	Unique Local IPv6 Unicast Addresses
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network

4 IPv6-enabled Enterprise

4.1 Introduction

When IPv4 emerged as the standard Internet protocol in the 1980s for the "Internet", the address space - some four billion IP addresses - seemed more than adequate. Today it is clearly no longer the case. The world has moved from IP enabled to IP dependent. As of 2015 more than 83 percent of the world's population no longer has access to a "public Internet address." In North America, Latin America, Asia, and Europe, the IPv4 address pool is already entirely depleted. With the growing number of users and the proliferation of smart devices and things, IPv4 address space exhaustion is a major Information and Communications Technology (ICT) issue. The current IPv4-based Internet can no longer sustain the explosive growth of ICT. Any organization that relies on the Internet to any extent needs to be prepared to support IPv6.

IPv6 needs to be adopted globally across all parts of the Internet ecosystem. Global service providers and mobile operators are already deploying IPv6 in order to keep the Internet growing. IPv6 is allowing them to continue to grow their businesses and deliver the services that all of today's e-commerce is based on.

The move to IPv6 is inevitable, there is no alternative plan at this time**.** IPv6 is the cornerstone of our connected society. IPv6 offers important business and technical advantages. Among them: higher performance, enhanced mobility, automated management, built-in multicasting for multimedia applications, enhanced security, simplified administration and many more. Indeed, many enterprises have already determined that IPv6 is a much better networking tool than its predecessor, and it offers much greater capabilities for future technologies developed for networking platforms.

Because all/most existing IPv4-based infrastructures will continue to work after the last IPv4 address is issued, enterprises may be tempted to put off transitioning to IPv6 till some later date. Postponing the inevitable, however, can put an enterprise at a competitive disadvantage. As more and more customers operate in an IPv6 world, companies supporting only IPv4 risk being shut out of high-growth markets because they are unable to reach, or be reached by, these customers. The fallacy in this position is that maintaining IPv4-only communications can put enterprises at a competitive disadvantage. Seamless, pervasive connectivity is an integral part of doing business today.

IPv6 enables the enterprise and the global Internet to keep growing in a secure and open manner, and to scale toward the demand of new applications and, literally, billions of connected devices, while streamlining operations and provisioning. Enterprises deploying IPv6-enabled services are in a better position to capture the market changes, be more competitive, increase their growth potential, and provide for improved business continuity.

Of particular note is the fact that regardless of an organization's IPv6 preference, its customer base is currently deploying it. As consumers and customers adopt IPv6, enterprises will need to ensure that their own technology assets align with how their customers prefer to do business. As the shift to online shopping has already shown, customers will continue to buy from companies that do business on their terms. Meeting the needs of the customer base (many of which already have an IPv6-connected device) should be an imperative for all organizations.

Today, enterprises should already have assessed their position toward IPv6 adoption, understood its challenges and opportunities, and drafted their own requirements and plans accordingly.

4.2 Guiding principles

There are many scenarios/variations to enable IPv6 within the enterprise, there is no "one size fits all" answer. The present document does not attempt to provide guidance for all possible networking situations. Enterprise network architects should each take the responsibility of choosing the best solution for their own case.

Enterprises should understand the impact of the IPv6 Internet on their services. Next, they should assess their own situations and requirements as early as possible, if they have not yet done so. This assessment includes network, security, and business applications. Enterprise priorities could be:

- IPv6 is strategic in order to achieve business continuity.
- IPv6 has its own value outside of IPv4 address exhaustion.

In each case, requirements demand a production-grade deployment within a two- to three-year horizon.

It is expected that for most enterprises adding IPv6 connectivity, the Internet presence will be the highest priority because enterprises should offer services and content to their IPv6 customers over the Internet. This is also the easiest part.

Deploying IPv6 across the core is also a relatively easy task and will provide the network staff with a solid working knowledge of the IPv6 protocol.

Providing IPv6 access to all internal users and applications is probably the next highest priority, especially if the enterprises move to the cloud computing paradigm or to web services.

The last step will probably be adding IPv6 in the intranet and in the data centre applications. This will take longer, as there is a clear impact on business applications.

Finally there are three core principles to shape IPv6 network development:

- The first principle is to maintain a standards-based approach and avoid proprietary technologies. Embracing open standards allows to use best-of-breed products for whatever needs arise.

  A network build on open standards will have interoperability with the broadest base of users and partners.

- The second principle is planning. Without proper planning, the transition will be plagued with rework and missteps.

- The third principle is repeatability of the network design across the network (a standard set of requirements, and a standard solution design to meet the enterprise network requirements).

  Such standardization increases efficiency in building out the network, and also makes it easier to troubleshoot the network in each location.

4.3 IPv6 Transition strategies

4.3.1 Setting the scene

The vast majority of devices, laptops, desktops, operating systems, switches, routers, content providers, carriers, and Internet service providers (ISPs) support native IPv6 today at no extra cost, which makes it possible to deploy network based on IPv6. However, enterprises typically purchased and configured their network to support IPv4 traffic only. And while most equipment can be software enabled, some may need to be replaced to add support for IPv6. Furthermore even if the capabilities to operate in a dual network configuration exist, additional planning steps and architecture design will most likely be required. Similarly management systems and security systems that can support both environments are necessary. Enterprises should also verify that applications they use can operate correctly and are IPv6-enabled.

Because IPv4 and IPv6 will coexist for some time, a phased deployment is recommended to minimize the impact of the transition and keep costs manageable. Recognizing that IPv4 and IPv6 will run parallel to each other for the foreseeable future, IETF established three standard transition mechanisms: Each of these techniques has advantages and trade-offs. The optimal solution will depend on a variety of factors, including the enterprise's current environment and long-term goals. It may also encompass all three transition mechanisms. It is important to understand that one method does not fit all.

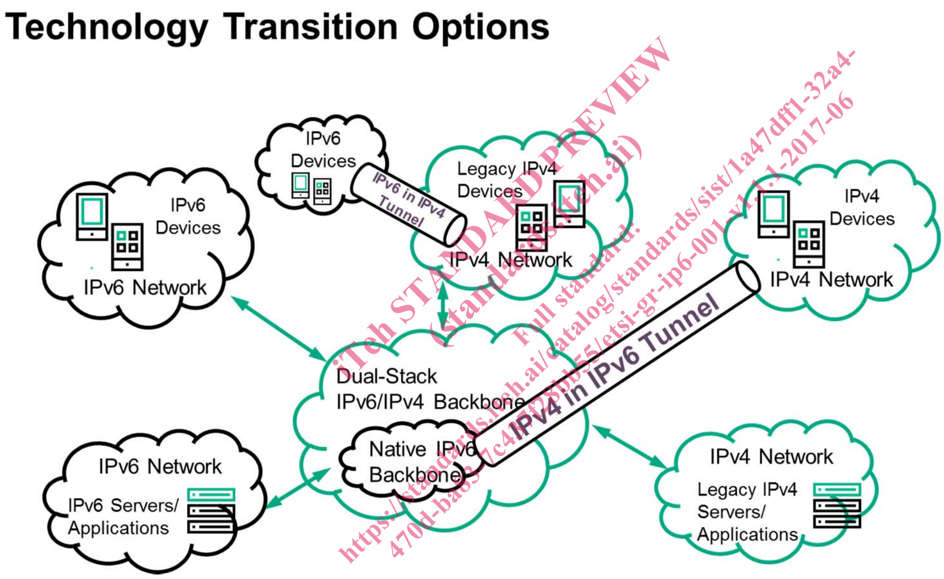

Figure 1: Technology Transition Options

In planning the IPv6 initiative, the following three key families of mechanisms enable the transition:

- **Dual-stack** - Provides support for both protocols on the same device to allow for communications with both IPv4-only and IPv6-only nodes.

  This mechanism is the most versatile. A dual stack transition strategy enables a very smooth transition and will likely remain a part of the worldwide Internet infrastructure for years to come, until IPv4 is fully retired.

- **Tunnelling** - Encapsulates IPv6 packets in IPv4 headers (or vice versa).

  Tunnelling enables the network team to create islands of IPv6 or IPv4 capabilities, and in the short term, to connect them over the existing IPv4 network. Tunnelling enables networks in transition to take advantage of IPv6 services while remaining connected to the IPv4 world.

- **Translation** - Between IPv4 and IPv6.

Enterprises should also implement a procurement policy to IPv6-ready the backbone so that IPv6 can be turned on without having to do a fork and replace the physical hardware.

The main IPv6 transition deployment models that are being discussed are listed below:

- **IPv4 only:** delays the introduction of IPv6 to a later date and remains an all-IPv4 network. Long term, it is expected that this migration strategy will lead to problems and increased costs. Due to the increase in traffic there will be an increased demand for IP addresses and the usage of NAT in the carrier's network, denoted as Carrier Grade Network Address Translation (CG-NAT). In particular, all traffic to and from the Internet will have to pass CG-NAT. Furthermore, growth in bandwidth demand can only be handled with increased CG-NAT capacity, which has a higher cost and single point of failure.

- **Coexistence of IPv4 and IPv6:** requires the use of a dual-stack, introducing IPv6 in the network next to IPv4. Please note however dual-stack networks are more complex to deploy, operate, and manage. Furthermore, this option also requires an address management solution for both IPv4 and IPv6 addresses.

- **IPv6 only:** introduces IPv6 in the network and removes IPv4 completely. This approach can provide benefits because IPv6-only networks are simpler to deploy, operate, and manage. Moreover, an address management solution is required only for IPv6 addresses. However, the problem with this approach is that many devices, websites, and applications still only work on IPv4. When moving to an IPv6-only network may lead to differences in network quality. That is why NAT64 with DNS64 should be offered in addition to offering IPv6 only.

4.3.2 Dual-Stack

Most enterprises will initially prefer the dual-stack model. All users, applications, and network equipment will be given address space from both IPv4 and IPv6. It is then up to the user's device to select which protocol version to use. Most common operating systems prefer IPv6 when a functional path is available.

The operating systems have specific checks in place to ensure quick and reliable connections when operating in dual-stack mode, based on IETF RFC 6555 "Happy Eyeballs" [i.11]. IETF RFC 6555 [i.11] tries to ensure that (where it is reliably available) IPv6 is usually preferred over IPv4. That is to say without IETF RFC 6555 [i.11] the first response back is preferred by default. Simply stated, parallel DNS queries are launched for IPv4 and IPv6 addresses for any website, and the first response back is preferred. IETF RFC 6555 [i.11] works with a slight bias toward IPv6 by giving the AAAA query a slight head start over the query for the legacy protocol address.

It is important to note that the dual-stack model will not be sustainable in the future when the available IPv4 space has been completely exhausted.

Dual-stack model also doubles the amount traffic at layer 2 for service discovery protocols like LLMNR and SSDP, as well as ARP and ND. This can have negative impact on CPU of some older network hardware. Additionally it is important to validate there is sufficient memory to store both IPv4 and multiple IPv6 addresses.

IPv6 traffic on Wi-Fi network requires additional consideration. IPv6 ND traffic and other IPv6 control plane traffic using multicast as the delivery mechanism may require optimizations over Wi-Fi network. Multicast over Wi-Fi network uses lowest management rates and mechanisms such as clients power save could impact timely delivery of multicast traffic over Wi-Fi. Typically Wi-Fi vendors convert multicast traffic to unicast to ensure robust and reliable delivery of multicast traffic. This also ensures that traffic is delivered to clients at the highest data rates possible and since the traffic is unicast, the standard power save mechanism for delivering multicast traffic does not apply.

IPv6 over Wi-Fi may require optimization techniques such as these to ensure reliable delivery of IPv6 control traffic.

4.3.3 IPv6 only

IPv6-only is the end goal of transitioning to IPv6. There have been numerous recent examples of large entities migrating to IPv6 after dual-stack transitions. Typical motivations are to avoid costs of translation equipment, reduce the cost of running a dual-stack infrastructure, reduce the attack surface to only one protocol, and simplify troubleshooting. It has deployed an IPv6-only infrastructure within its data centre.

The public-facing side of its Internet presence/WAN edge still presents a dual-stack interface to the global Internet, but it has completely removed IPv4 from the internal data centre infrastructure.

IPv6 only with NAT64/DNS64 is easy to implement and works well in a Client/Server model, there are challenges with peer-to-peer applications and IPv4 only clients. Application validation for enterprise peer-to-peer applications should be included in the scorecard.