ETSI GR IP6 006 V1.1.1 (2017-11)

Generic migration steps from IPv4 to IPv6

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/IP6-0006

Keywords
IPv4, IPv6, transition

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

Copyright Notification

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.

1 Scope

The present document outlines the generic transition steps from IPv4 to IPv6 [i.1], [i.2], including the transition necessity, principles and technology guidelines, generic transition steps, security implications and the generic step-by-step process.

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 791: "Internet Protocol", September 1981.

[i.2] IETF RFC 2460: "Internet Protocol, Version 6 (IPv6) Specification", December 1998.

[i.3] IETF RFC 1631: "The IP Network Address Translator (NAT)", May 1994.

[i.4] IETF RFC 1701: "Generic Routing Encapsulation", October 1994.

[i.5] Durand, A., Droms, R., Woodyatt, J., and Y. Lee: "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion".

[i.6] IETF RFC 5569: "IPv6 Rapid Deployment on IPv4 Infrastructures (6rd)", January 2010.

[i.7] IETF RFC 7597: "Mapping of Address and Port with Encapsulation (MAP-E)", July 2015.

[i.8] IETF RFC 7599: "Mapping of Address and Port using Translation (MAP-T)", July 2015.

[i.9] IETF draft-ietf-v6ops-ipv6-ehs-in-real-world-02: "Observations on the Dropping of Packets with IPv6 Extension Headers in the Real World", December 2015.

[i.10] IETF RFC 6555: "A. Happy Eyeballs: Success with Dual-Stack Hosts", April 2013.

[i.11] IETF RFC 7359: "Layer 3 Virtual Private Network (VPN) Tunnel Traffic Leakages in Dual-Stack Hosts/Networks", August 2014.

[i.12] LinkedIn® Case Study: "IPv6 at a Social Media Company". Schuller, S. 11th Slovenian IPv6 Summit, June 21, 2016, Ljubljana, Slovenia.

NOTE: Available at https://go6.si/wp-content/uploads/2016/06/LinkedIn-Case-Study.pdf.

[i.13] IETF RFC 1702: "Generic Routing Encapsulation over IPv4 networks".

[i.14] IETF RFC 5969: "IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) - Protocol Specification".

[i.15] IETF RFC 6751: "Native IPv6 behind IPv4-to-IPv4 NAT Customer Premises Equipment (6a44)".

[i.16] IETF RFC 5214: "Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)".

[i.17] IETF RFC 6343: "Advisory Guidelines for 6to4 Deployment".

[i.18] IETF RFC 4213: "Basic Transition Mechanisms for IPv6 Hosts and Routers".

[i.19] IETF RFC 6333: "Dual-tack Lite Broadband Deployments Following IPv4 Exhaustion".

[i.20] IETF RFC 6346: "The Address plus Port (A+P) Approach to the IPv4 Address Shortage".

[i.21] IETF RFC 7739: "Security Implications of Predictable Fragment Identification Values".

[i.22] Dan York: "Migrating Applications to IPv6", 2011.

3 Abbreviations

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

4464XLAT	Combination of Stateful and Stateless Translation
6a44	Native IPv6 behind NAT44 CPEs
6over4	IPv6 over IPv4 without Explicit Tunnels
6RD	IPv6 Rapid Deployment
6to4	Connection of IPv6 Domains via IPv4 Clouds
AAAA	An AAAA record points a domain or subdomain to an IPv6 address
API	Application Program Interface
AYIYA	Anything-In-Anything
CGN	Carrier Grade NAT
CPE	Customer-Premises Equipment
DNS	Domain Name Server
DoS	Denial of Service
DS-Lite	Dual-Stack Lite
GRE	Generic Routing Encapsulation
ICMP	Internet Control Messages Protocol
ICP	Internet Content Provider
IoT	Internet of Things
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
ISP	Internet Service Provider
MAN	Metropolitan Area Network
MAP	Mapping of Address and Port
MAP-E	Mapping of Address and Port - Encapsulation
MAP-T	Mapping of Address and Port - Translation
MSS	Maximum Segment Size
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NAT-PT	Network Address Translation - Protocol Translation
NBMA	Non-Broadcast Multiple Access
SIIT	Stateless IP/ICMP Translation Algorithm
TCP	Transmission Control Protocol
Teredo	Tunnelling IPv6 over UDP through NATs
TSP	IPv6 Tunnel Broker with the Tunnel Setup Protocol
UDP	User Datagram Protocol

4 Transition from IPv4 to IPv6

4.1 IPv6 transition necessity

For more than 35 years, IPv4 has been the core underlying technology enabling services such as the web, e-mail, and so forth. However, as a result of the unexpected growth of the Internet, the IPv4 32-bit address space has become a limiting factor to future Internet growth - that is, IPv4 will be unable to provide a globally routable unique IP address to each system to connect to the Internet. To overcome the exhaustion of IPv4 addresses, the Internet Protocol version 6 (IPv6) was developed, with 128-bit addresses that provide enough addresses to allow for the foreseeable future growth of the Internet.

IPv4 address exhaustion has accelerated IPv6 deployment. There are two complementary ways to ensure service continuity:

- Start introducing IPv6 and give new customers' IPv6 addresses.
- Implement IPv4 address sharing mechanisms to continue using IPv4 service.

Please note that IPv4 address sharing (using Network Address Translation (NAT) [i.3]) could only temporarily relieve the IPv4 address exhaustion problem, and that other challenges arise with massive deployment of IPv4 address sharing in the form of Carrier Grade NAT (CGN). CGNs not only result in more complicated networks and increased network management and operational costs, but also eventually introduce interoperability problems. Besides, due to address sharing, it results in loss of geo-location information, and difficult lawful intercept/abuse response. Therefore, transition to IPv6 is the only real solution to address the IPv4 address exhaustion problem.

Please note that the pressure resulting from IPv4 address exhaustion varies from one organization (e.g. ISP) to another due to many factors, such as the situation of address storage and Internet penetration. This results in a different pace for supporting IPv6.

Currently, there are a few applications or services only available in IPv6. And it is expected that it will take a long time for all IPv4-only services to be transitioned to IPv6. In fact, it is expected that many of such IPv4-only services will be "transitioned" to IPv6 when their corresponding systems are phased-out and replaced with IPv6-ready counter-parts. Therefore, it is expected that IPv4 and IPv6 will co-exist for a long time, and thus, even in the presence of IPv6-deployment, IPv4 provisioning needs to be taken care of.

4.2 Transition types

The original transition plan from IPv4 to IPv6 was based on the Dual Stack principle. Essentially, every node in the Internet would implement and enable IPv6 well before IPv4 address exhaustion. Unfortunately, such plan failed, and a number of transition technologies were subsequently implemented to allow for the incremental deployment of IPv6, and the co-existence of IPv4 and IPv6.

Transition technologies are employed for one of the following goals:

- Providing IPv6 connectivity
- Providing IPv4 connectivity (usually by multiplexing multiple devices in the same IPv4 address)

The following transition technologies are employed for providing IPv6 connectivity:

- Dual-stack
- Configured tunnels (6in4)
- Generic Routing Encapsulation (GRE)
- IPv6 Rapid Deployment (6rd) [i.6]
- Native IPv6 behind NAT44 CPEs (6a44)
- Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)

- Connection of IPv6 Domains via IPv4 Clouds (6to4)
- Tunnelling IPv6 over UDP through NATs (Teredo)
- IPv6 over IPv4 without Explicit Tunnels (6over4)
- Anything In Anything (AYIYA)
- IPv6 Tunnel Broker with the Tunnel Setup Protocol (TSP)

The following transition technologies are employed for providing IPv4 connectivity:

- Stateless IP/ICMP Translation Algorithm (SIIT)
- Stateful NAT64
- Combination of Stateful and Stateless Translation (4464XLAT)
- Dual-Stack Lite (DS-Lite) [i.5]
- MAP-E [i.7]
- MAP-T [i.8]

These transition technologies are discussed in clause 5.

5 Transition Principles and Technologies

5.1 Dual-stack

5.1.1 Dual-stack Principle

The dual stack principle was the original transition plan to IPv6. Essentially, every node on the Internet would implement and enable IPv6 before the IPv4 address space was exhausted. Thus, IPv4 support could start to be disabled at any time, since all communications could be performed over IPv6. Unfortunately, this plan failed, and the Internet hit IPv4 address exhaustion before widespread deployment of IPv6.

Nevertheless, Dual Stack is still the preferred transition technology for servers, since it allows IPv6-enabled clients to communicate with servers employing native IPv6 connectivity. Besides, the number of global IPv4 addresses required to provision servers is usually way smaller than the number of iPv4 addresses required to provision clients (compare the number of servers vs. clients in a usual Internet Service Provider).

Figure 1 illustrates the Dual Stack architecture.

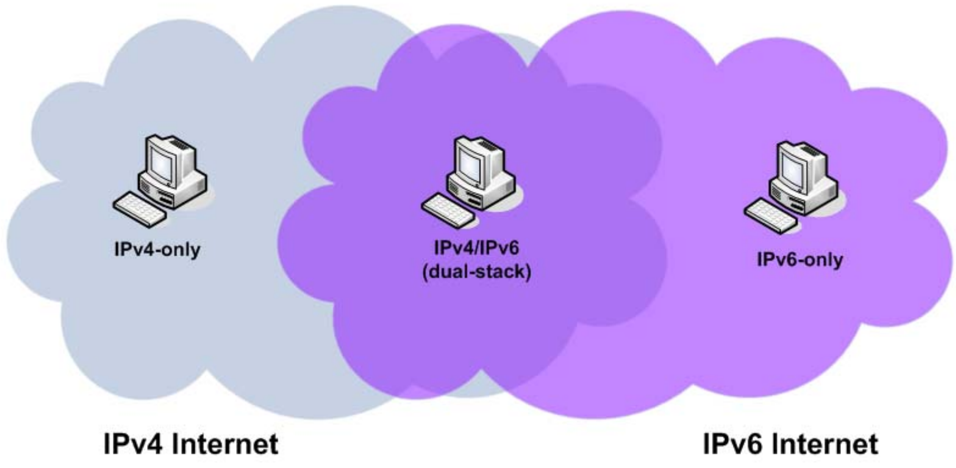

Figure 1: Dual Stack architecture

It is interesting to note that dual-stack essentially results in two separate networks. In principle, IPv4-only systems can communicate only with IPv4-only systems, while IPv6-only systems can only communicate with their counterparts. On the other hand, Dual Stack nodes can communicate with IPv4-only, IPv6-only, a Dual Stack (IPv6/IPv4) systems.

The DNS plays a key role in the IPv6 and the IPv4 world: for example, when a Dual Stack host means to browse the website www.example.com, it will typically query for both IPv4 and IPv6 addresses (A and AAAA records, respectively). Then it is up to the host (or host application) to use the available addresses.

5.1.2 Dual-stack Security Implications

The security implications of IPv6 transition technologies depend, for most part, on the specific paradigm being employed.

Dual-stack essentially implies that every node being transitioned will implement and operate with two different protocol stacks: an IPv6 stack and an IPv4 stack. Implementing, deploying, and operating an additional stack clearly increases the potential attack surface. In particular, since the maturity level of IPv6 implementations generally does not match that of existing IPv4 implementations, it is very likely that new bugs (possibly with security implications) will be discovered in the IPv6 code, and hence particular care should be taken to keep the operating system and applications up-to-date.

5.1.3 Dual-stack conclusion

Dual stack is generally the ideal mechanism for transitioning to IPv6, since it employs both native IPv6 and native IPv4 connectivity. The only drawback of this transition technology is that it requires the operation and management of two separate networks: an IPv6 network and an IPv4 network. In some scenarios, such as data centres, this issue may be considered enough of a motivation for employing SIIT, such that the server farm only implements IPv6, and IPv4 connectivity is provided via stateless translation.

5.2 Tunnelling

5.2.1 Tunnelling Principle

The tunnelling principle involves encapsulating packets of one internet protocol into packets of a (usually different) internet protocol. This is of use when "islands" of one internet protocol should be interconnected across a network that does not support the aforementioned internet protocol. For example, it can be employed to interconnect to IPv6 "islands" across the IPv4 Internet.