ETSI GR IP6 010 V1.1.1 (2017-12)

IPv6-based SDN and NFV; Deployment of IPv6-based SDN and NFV

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/IP6-0010

Keywords
IPv6, NFV

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 motivation for the deployment of IPv6-based Cloud Computing, the objectives, the technology guidelines, the step-by-step process, the benefits, the risks, the challenges 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 6333: "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion", A. Durand, R. Droms, J. Woodyatt et al., August 2011.

[i.2] IETF RFC 6877: "464XLAT: Combination of Stateful and Stateless Translation", M. Mawatari, M. Kawashima, C. Byrne, April 2013.

[i.3] IETF RFC 6535: "Dual-Stack Hosts Using "Bump-in-the-Host" (BIH), B. Huang, H. Deng, T. Savolainen, February 2012.

[i.4] IETF RFC 6146: "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", M. Bagnulo, P. Matthews, I. van Beijnum, April 2011.

3 Abbreviations

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

ALG	Application Layer Gateway
API	Application Programming Interface
CAPEX	Capital Expenditure
CGN	Carrier-Grade NAT
DS-Lite	Dual Stack Lite
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
lw4over6	lightweight IPv4 over IPv6
MAP	Mapping of Address and Port
NAT	Network Address Translation
NAT44	Network Address Translation IPv4 to IPv4
NAT64	Network Address Translation IPv6 to IPv4
NFV	Network Functions Virtualisation
NFVI	Network Functions Virtualisation Infrastructure
OPEX	Operations Expenditure
OSS	Operations Support System

QoS	Quality of Service
SDN	Software Defined Networking
SUPA	Simplified Use of Policy Abstraction
TDP	Transition Data Plane

4 IPv6-based SDN & NFV Deployment

4.1 Introduction

The exhaustion of the IPv4 address space has been a practical problem that providers are facing today. The migration to IPv6 is ongoing and picking up steam throughout the world.

Depending on the amount of technology debt and legacy present in the existing infrastructure, the IPv6 transition might require significant upgrades and different approaches to the roll-out in order to maintain efficiency. Instrumentation and operational tools, back-end systems and processes will also need to be updated for the new protocol. Therefore, operators might have to upgrade network devices to support different transition strategies but more importantly to support different visions of the future infrastructure. The transition will increase the OPEX and CAPEX needs during the transition. The increase will be determined by the specifics of the provider and particularly by the speed with which the provider chooses or is forced to execute the transition.

One option is to consider managing the transition by using SDN/NFV concepts and technologies. A unified Transition Data Plane (TDP) enables DevOps in IT environment by providing extensibility via programmability, by integrating deployment and operation into the implementation, and by streamlining OSS. The IPv6 transition can be viewed as another service enablement exercise managed by TDP. In a TDP enabled environment, an IPv6 transition powered by SDN could lower the deployment and operational costs by decoupling the data plane and control plane, and by providing unified data plane devices. It also nurtures the development of native IPv6 services through the availability of open Northbound APIs. An Open IPv6 can reduce the operational complexity and risk via the unified data plane which adapts to different transition scenarios.

4.2 Unified Openv6 Use case

4.2.1 Evolve from one Scenario to Another

During the IPv6 transition period, the network will go through three stages: IPv4-only network, dual-stack network and IPv6-only network. The network should support both IPv4 services and IPv6 services at each stage.

There are multiple IPv6 transition technologies for different network scenarios (e.g. IPv4 network for IPv4/IPv6 user access, IPv6 network for IPv4/IPv6 user access, IPv4 servers for IPv6 visitors, etc.). Different network scenarios will co-exist during IPv6 transition which means the IPv6 transition device should support multiple IPv6 transition technologies. The following are possible flow scenarios over the IPv6 transition period:

1) Scenario 1: IPv6 hosts visit IPv6 servers via IPv4 access network.

2) Scenario 2: IPv4 hosts visit IPv4 servers via IPv4 NAT Dual-stack network.

3) Scenario 3: IPv6 hosts visit IPv6 servers via IPv6 network.

4) Scenario 4: IPv4 hosts visit IPv4 servers via IPv6 access network.

5) Scenario 5: IPv6 hosts visit IPv6 servers via IPv4 access network.

6) Scenario 6: IPv4 hosts and IPv6 hosts interaction.

It is not necessary that all operators will go through each scenario one by one. For example, some operators may start from scenario 1, and some may start directly from scenario 2 or scenario 4. However, since the final stage (target) is the IPv6-only access network, one still needs to cover several scenarios that deal with legacy and transition.

To execute its transition strategy the operator might have to either upgrade existing devices to support new features, or replace them with new ones that enable its IPv6 plans. When the operator's network consists of devices from different vendors, it becomes more difficult to orchestrate the feature support across all areas of the infrastructure in order to deliver IPv6 as planned.

4.2.2 Multiple Transition Mechanisms Co-Exist

Various technologies involved in the transition process will impact in different ways the overall user experience. For example, DS-Lite negative impact could be due to address sharing. On the other side, 6rd mechanisms, and NAT64 negative impact might be due to penalties paid while transiting the ALG. Operators may prepare a fall-back mechanism to guarantee the same level of user experience when there are complaints from subscribers. Therefore, it is required to support multiple transition mechanisms in the footprint.

Another use scenario is that alongside IPv6 transition mechanism deployed in a domain, IPv4 address exhaustion mitigation mechanisms might be deployed as well. For example, if there are both IPv6-only devices and IPv4-only devices in the same area with limited public IPv4 address, both NAT64 and NAT44 (or DS-Lite) are required to achieve IPv4 service connectivity.

Current implementations normally use separate instances for each mechanism, with additional policies on the same device for each mechanism. Some devices have limitations on the number of policies which can be configured, while other have restrictions regarding the resources availability (e.g. one transition instance will occupy a static amount of memory). The coexistence of multiple transition mechanisms is costly and can add significant complexity to an already complex environment.

4.2.3 Scattered Address Pool Management

When operators are facing address shortage problem, the remaining IPv4 address pools are usually very fragmented. It is quite complicated for an operator to manage fragmented address pools in many transition devices. The situation will become even worse when multiple transition mechanisms in the same device need to be configured from different address pools. Moreover, the utilization of the address pools may vary during different transition periods. As there are not many IPv6-enabled services and IPv6-enabled devices, IPv4 traffic still occupy a great portion of the total traffic, while in the later stage of IPv6 transition, IPv4 traffic will decrease and the amount of IPv4 address pools will decrease accordingly.

The ideal would be to manage the address pools centrally. Different transition mechanisms can access the address pools on-demand. For example, when one transition mechanism is running out of the current address pools, it may request an additional address pool. It can also release the address pools which is no longer used. That way, operators do not need to configure the address pools one by one manually and it also helps using the address pools more efficiently.

4.2.4 Extensibility

During migration from IPv4 to IPv6, different scenarios usually need different solutions. Although IETF has already invented some mechanisms including DS-Lite IETF RFC 6333 [i.1], 464XLAT IETF RFC 6877 [i.2], BIH IETF RFC 6535 [i.3], NAT64 IETF RFC 6146 [i.4], etc., the current solutions have solved the following scenarios only in a limited way:

- IPv4 client communicates to IPv6 server.
- IPv4 client communicates to IPv6 peer.

It is possible that new technologies are invented in the future. In addition, some mechanisms are still evolving from a session-based solution (e.g. DS-Lite) to a more scalable way (e.g. lw4over6, MAP). It might be possible that operators who have already deployed one solution may upgrade to a better one in the future. Besides, IPv6 transition can also be regarded as a virtualised network function which can be offered to a third-party.

Therefore, it is required to offer an open and programmable way to easily add new features without modifying existing device hardware.

4.3 Open IPv6 Architecture: Powered by SDN

4.3.1 Overall Architecture

The key features of Open IPv6 are:

- Decoupling of the data plane and control plane.
- The presence of Northbound APIs for services needed to manipulate the traffic.
- In addition, the approach is flow-based and IPv6 routing compatible.

The overall architecture (figure 1) of Open IPv6 is depicted in the following.

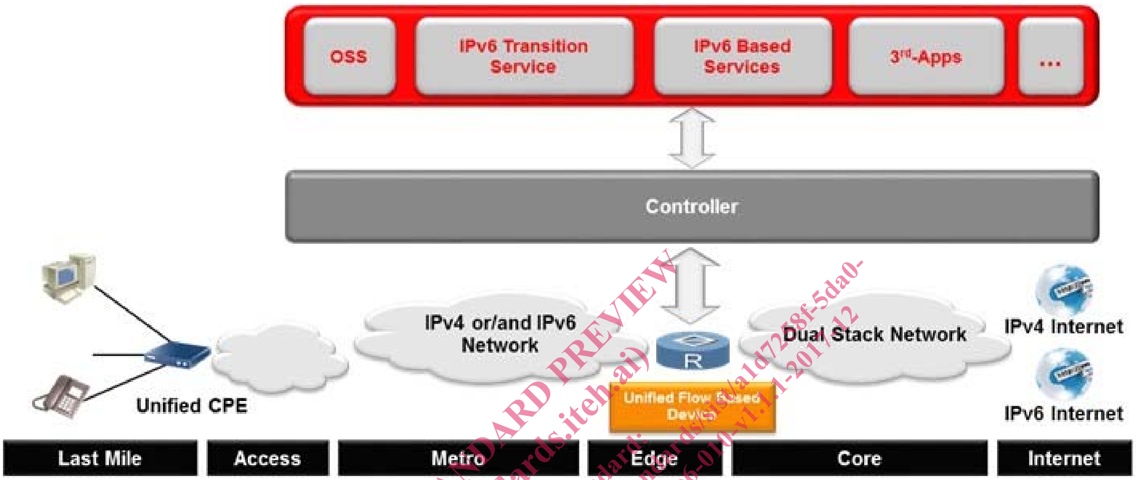

Figure 1: Overall Architecture of IPv6-based SDN solution

The edge device in the data plane is flow based, and the control plane and the network services are removed from the device. These two factors help unifying the data plane and improving its extensibility.

Services such as OSS and IPv6 transition services are deployed at the application layer. All of these features bring multiple important benefits to DevOps organizations who implement this architecture:

- Different IPv6 transition scenarios can be supported.
- IPv6 based services, and different scenarios, are supported by uniform equipment.
- Open IPv6 will accommodate future IPv6 services.
- And the architecture is unified with any IPv6 migration path.

The Open IPv6 architecture, powered by SDN, offers the promise of greatly reducing the complexity and cost of an IPv6 transition.

In this architecture, the unified flow-based device handles incoming packets basing on the flow table. Examples of Forwarding Nodes can include:

- A router that has an extended function module. The extended module handles incoming packets based on the flow table of the module.
- A server that runs vRouter or vSwitch.
- A CGN that runs NAT, Tunnel En/De-capsulation functions.

The unified flow table is used for handling incoming packets of the forwarding node. The flow table can be updated by the application. If an incoming packet does not match any entry of the flow table, the packet will be delivered to the agent for generating new entries.

The Open IPv6 agent interacts with the forwarding node to provide specified behaviour for incoming packets via the flow table.

4.3.2 How Open IPv6 works

The following figure 2 depicts how Open IPv6 works powered by SDN technology.

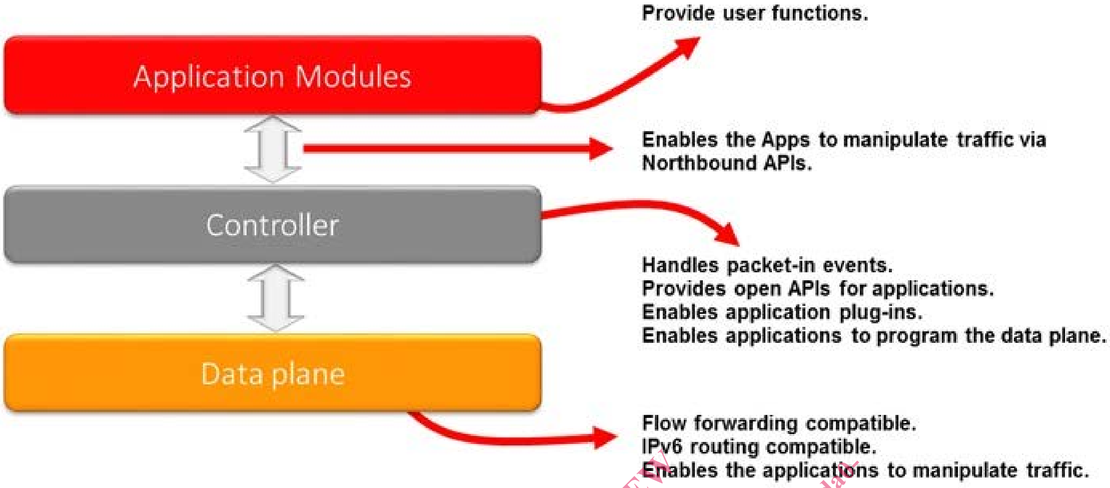

Figure 2: Layered Architecture of IPv6-based SDN solution

Starting from the bottom, the data plane is flow forwarding and IPv6 routing compatible. It enables the applications to manipulate the traffic.

In grey, the controller handles packet-in events, it provides open APIs for applications, and it enables applications plug-in and enables applications to program the data plane.

The Northbound Interface represented by the arrow enables the applications to manipulate traffic via Northbound APIs.

Finally, at the top, the application modules provide user functions such OSS, 3rd-Apps, and IPv6 services.

4.3.3 Processing Flow-Based Services

The following depicts the processing of flow-based services.

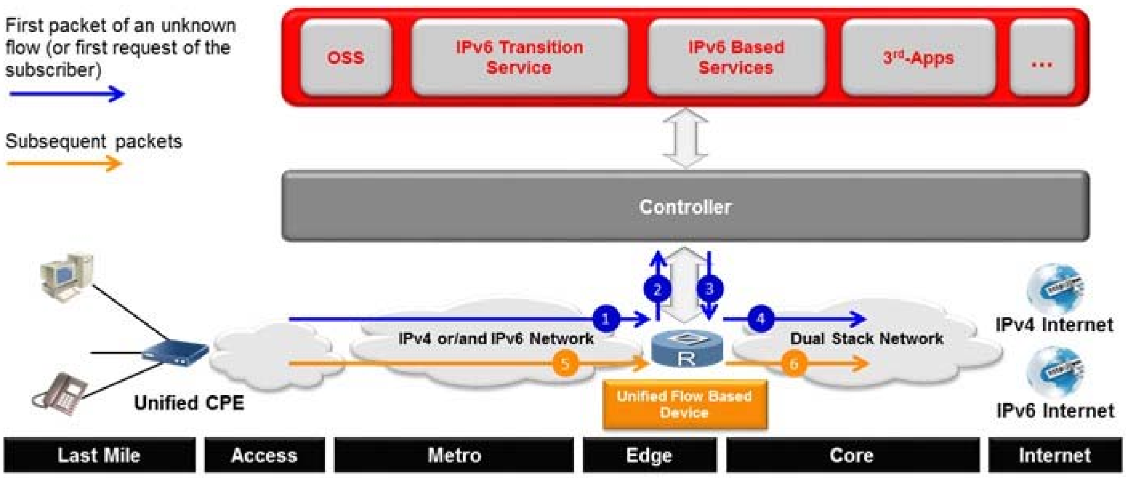

Figure 3: Process flow-based service

The blue line represents the first packet of an unknown flow, or first request of the subscriber. The first packet of an unknown flow is sent to the controller and triggers policies delivered to data plane. The subsequent packets do not need to send to the controller.