IPv6 Deployment Status

draft-vf-v6ops-ipv6-deployment-01

Online, Nov 2020, IETF 109

Giuseppe Fioccola (Huawei)
Paolo Volpato (Huawei)
Nalini Elkins (Inside Products)
Sebastien Lourdez (Post Luxembourg)

Motivation

- IPv6 is becoming a priority again and a new wave of IPv6 deployment is happening [ETSI-IP6-WhitePaper]
- This document aims to investigate what is missing and how to improve the current IPv6 deployment strategies of the network operators and enterprises
- The objective is to give an updated view of the practices and plans already described in [RFC6036].
- The IPv6 incentives are presented but the general IPv6 challenges are also reported in particular in relation to Architecture, Operations, Performance and Security issues

A look at the ToC

- **The global picture of IPv6**
  - IPv6 users
  - IPv6 allocations and networks
- **Survey among Network Operators**
- **Considerations for Enterprises**
- IPv6 deployments worldwide
  - IPv6 service design for Mobile, Fixed broadband and enterprises (IPv6 introduction, IPv6-only service delivery)
- Findings of the IPv6 Survey
- **IPv6 incentives**
- **Call for action**
  - Transition choices (Service providers, Enterprises)
  - Network Operations
  - Performance (IPv6 latency, IPv6 packet loss, Router's performance)
  - IPv6 security (Protocols security issues, IPv6 Extension Headers and Fragmentation, Oversized IPv6 packets)

The global picture of IPv6

Different analytics have been made available by many agencies and institutions worldwide

IPv6 Users

	Jan 2015	Jan 2016	Jan 2017	Jan 2018	Jan 2019	Jan 2020	CAGR
World	74.24	179.42	290.68	513.68	574.02	989.25	67.9%

IPv6 allocations worldwide

Registry	Jan 2015	Jan 2016	Jan 2017	Jan 2018	Jan 2019	Cumulated	CAGR
AFRINIC	86	116	112	110	115	539	58%
APNIC	778	1,681	1,369	1,474	1,484	6,786	72%
ARIN	602	646	684	658	605	3,195	52%
LACNIC	1,061	1,010	1,549	1,450	1,618	6,688	58%
RIPE	2,206	2,141	2,051	2,617	3,105	12,120	53%
Total	4,733	5,594	5,765	6,309	6,927	29,328	58%

Allocations per address family

Address family	Jan 2015	Jan 2016	Jan 2017	Jan 2018	Jan 2019	Cumulated	CAGR
IPv6	4,733	5,594	5,765	6,309	6,927	29,328	58%
IPv4	11,732	9,787	9,440	10,199	14,033	55,191	47%

Percentage of IPv6-capable ASes

Advertised ASN	Jan 2015	Jan 2016	Jan 2017	Jan 2018	Jan 2019	Jan 2020	CAGR
IPv6-capable	9,182	10,744	12,663	14,506	16,440	18,623	15.19%
Total ASN	43,543	44,549	44,368	60,281	63,782	67,713	9.23%
Ratio	21.1%	24.1%	28.5%	24.1%	25.8%	27.5%	

Survey among Network Operators

IPv6 poll to more than 50 network operators about the status of IPv6 deployment

The main Questions asked are:

- Do you plan to move more fixed or mobile or enterprise users to IPv6 (e.g. Dual-Stack) or IPv6-only in the next 2 years? What are the reasons to do so? Which transition solution will you use?
- Do you need to change network devices for the above goal? Will you migrate your metro or backbone or backhaul network to support IPv6?

The result of this questionnaire highlights that major IPv6 migration will happen in next 2 years.

- **Dual Stack** is always the most adopted solution and the transition to IPv6-only is motivated in particular by IPv4 public/private addresses depletion
- The two stage approach is valid: (1) IPv6 introduction (**Dual Stack**) and (2) IPv6-only (**464XLAT**, **DS-Lite**)
- In general, it is possible to state that, when the Dual-Stack disadvantages outweigh the IPv6-only complexity, it makes sense to migrate to **IPv6-only**

IPv6 incentives

It is possible to state that IPv6 adoption is no longer optional, indeed there are several incentives for the IPv6 deployment:

- **Technical incentives**: all Internet technical standard bodies and network equipment vendors have endorsed IPv6 and new IETF protocols are optimized for and depend on IPv6.
- **Business incentives**: with the emergence of new digital technologies, such as 5G, IOT and Cloud, new use cases have come into being and posed more new requirements for IPv6 deployment.
- **Governments incentives**: governments have a huge responsibility in promoting IPv6 deployment within their countries. There are example of governments already adopting policies to encourage IPv6 utilization or enforce increased security on IPv4.

Call for action: Transition choice and Network Operations

Transition choices

There are some areas of improvement, that are often mentioned in the literature and during the discussions on IPv6 deployment.

- **Service providers**

From an architectural perspective, there are many technical alternatives available and transition choices. This is also related to the strategy adopted for CGNAT.

- **Enterprises**

Most of the enterprises have failed to adopt IPv6, especially on internal networks and their engineers and technicians are not well trained.

Network Operations

Network management applications and equipment need to be properly configured and in same cases also replaced. This may introduce more complexity.

Call for action: Performance

Despite their relative differences, people tend to compare the performance of IPv6 and IPv4, even if these differences are not so important for applications.

Latency

- APNIC constantly compares the latency of both address families. Currently, the worldwide average is still in favor of IPv4.
- An APRICOT document highlights that a difference in performance exists and it could be related to asymmetric routing issues. Other possible explanations for a relative latency difference lays on the specificity of the IPv6 header which allows fragmentation, EHs.

Packet Loss

- APNIC also provides the failure rate of IPv6. Two reports from RIPE and APRICOT discussed the associated trend, showing how the average worldwide failure rate of IPv6 worsened from around 1.5% in 2016 to a value exceeding 2% in 2020.

Router's performance

- Most of the routers showed a remarkably similar throughput and latency for IPv4 and IPv6. Only for smaller software switching platforms, some tests reported a lower throughput for IPv6

Call for action: IPv6 security (1/2)

The security aspects have to be considered to keep the same level of security as it exists nowadays in an IPv4-only network environment.

- Comparing IPv6 and IPv4 at the protocol level, one may probably conclude that the increased complexity of IPv6 results in an increased number of attack vectors

- **Protocols security issues**

In general there are security concerns related to IPv6 that can be classified as follows:

- Basic IPv6 protocol (Basic header, Extension Headers, Addressing)
- IPv6 associated protocols (ICMPv6, NDP, MLD, DNS, DHCPv6)
- Internet-wide IPv6 security (Filtering, DDoS, Transition Mechanisms)

In particular there are several security issues for NDP and in general for IPv6 First-Hop Protocols that need to be further analyzed to give a proper picture

Call for action: IPv6 security (2/2)

- **IPv6 Extension Headers and Fragmentation**

IPv6 Extension Headers imply some issues, in particular their flexibility also means an increased complexity.

Security devices and software must process the full chain of headers while firewalls must be able to filter based on Extension Headers.

- **Oversized IPv6 packets**

A lot of additional functionality has been added to IPv6.

All of the these expand the packet size and this could lead to oversized packets that would be dropped.

Call for action: What's missing?

We have proposed some areas of improvement (Call for action) based on the survey and on the existing literature

- Is it exhaustive? Maybe more contributions and inputs are needed from V6OPS here
- Which actions can we do to stimulate the IPv6 adoption?
- What are the additional issues on IPv6 deployment for Network Operators and Enterprise?
  - A Survey among Network Operators is included in the draft. Additional inputs from V6OPS are welcome.
  - INTC and IIESOC received grants from ARIN and APNIC to help with IPv6 Enterprise deployment. Support from V6OPS is welcome (contact Nalini Elkins or Dhruv Dhody).

Next Steps

- Get inputs from the Working Group
- Open to new contributors
- Comments are welcome

Thank you