TRANSITION to IPv6
Arcep publishes an account of the launch meeting of the Task Force on IPv6 in France

Paris, 18 December 2019

Following through on the workshops devoted to the transition to the IP♥6 protocol, Arcep created a task force, in concert with Internet Society France, to accelerate the transition to IPv6 by galvanising the forces of all of the willing internet stakeholders (operators, hosting companies, businesses, public sector players, etc.).

At a time when the announced shortage of IPv4 addresses is now a reality, Arcep played host to some 50 stakeholders at its headquarters, on 15 November 2019, to launch the task force and organise multi-stakeholder working groups:

- The first working group focused on the **impacts of the IPv4 address shortage**. The workshops explored alternatives to not making the transition to IPv6, technical solutions for making the transition and issues surrounding equipment, software and applications' compatibility with IPv6. The working group was preceded by a keynote from RIPE-NCC (the regional registry for IP addresses which is tasked with allocating IPv4 addresses in Europe and the Middle East) which provided a regional view of the current shortage of IPv4 addresses, and served to underscore how urgent it is to accelerate the transition to IPv6.
- The second working group addressed **IPv6 security issues**. Discussions tackled the topics of securing the local network, anonymisation and privacy issues as well as filtering challenges. A keynote from France's National Cybersecurity Agency, ANSSI, introduced this working group by focusing on the need to rethink security with IPv6.

The account of the work done by these groups is being published today. Between now and the next meeting of the IPv6 task force, which is scheduled for spring 2020, participants will continue to collaborate on deepening some of the identified work streams.

Press liaison
Anne-Lise Lucas
anne-lise.LUCAS@arcep.fr
Tel.: 01 40 47 71 37

Associated documents

Videos of the IPv6 Task Force launch meeting

• Workshop opening address by **Loïc Duflot**, Director of Arcep's Internet, Print media, Post and Users department, and by **Nicolas Chagny**, President of Internet Society France

• Presentation of the barometer of the transition to IPv6 in France by **Aurore Tual**, Open Internet Unit Chief, and Arcep policy officers**, Samih Souissi** and **Vivien Gueant**

• Keynote by **Xavier Le Bris**, RIPE-NCC

• Talk by Arcep Chair**, Sébastien Soriano**

• Keynote by **Arnaud Ebalard**, ANSSI

Arcep at a glance

The Regulatory Authority for Electronic Communications, Postal Affairs and Print Media Distribution (Arcep), a neutral and expert arbitrator with the status of independent administrative authority (IAA), is the architect and guardian of internet, fixed and mobile telecoms and postal networks in France

Account of the launch meeting of the Task Force on IPv6 in France

The different workshops helped to identify concrete proposals for actions to accelerate the transition.

The table in the annex details the different points that emerged from each working group.

1. Working group: impact of the IPv4 addresses shortage

a. Context and issues

- Need to keep IPv4 for as long as the transition to IPv6 has not been finalised on every link of the internet's technical chain;
- Problems created by alternatives to making the transition (buying or sharing IPv4 addresses);
- Existence of various options for making the transition: IPv6 in an IPv4-only network, dual-stack[1] or IPv4 in an IPv6-only network;
- Certain equipment, applications, software, services, etc. IPv6-compatibility issues;
- Management differences between IPv4 and IPv6, notably in the features deployed and in terms of performance;
- Need to increase the government's role in leading by example in the transition to IPv6.

b. Workstreams

- Communicate with businesses to encourage them to make the transition to IPv6;
- Include IPv6 activation in calls to tender, on top of IPv6 compatibility;
- Obtain testimonials from enterprises that have switched from IPv4 to IPv6 (at least in dual-stack) to estimate costs, benefits, technical conditions, etc.;
- In addition to these testimonials, draft an in-house development guide for IPv6 deployment;
- Identify the different categories of application, equipment and software for which malfunctions caused by Carrier Grade NAT (CGN)[2] have been observed;
- Inventory the different categories of application, equipment and software that cause IPv6 compatibility issues.

[1] Double pile IP: consists of assigning a piece of network equipment both an IPv4 and a an IPv6 address.

[2] Carrier Grade NAT: large-scale Network Address Translation mechanism, used in particular by ISPs to reduce the number of IPv4 addresses used.

2. Working group: IPv6 security issues and challenges

a. Context and issues

- Existence of several IPv6 network security aspects, similar to IPv4's but IPv6 requires a security rethink;
- Lack of available skilled labour and poor understanding of existing IPv6 security solutions;
- Several standards and RFC not updated,
- Taking anonymisation and privacy protection issues properly into account when implementing IPv6:
- Lack of knowledge of IPv6 filtering best practices.

b. Workstreams

- Inventory updated RFC and IPv6 security training resources;
- Compile the RIPE's existing resources as well as Internet Society initiatives, and update them;
- List the privacy issues caused by IPv6 and discuss the different countermeasures;
- Issue recommendations on how IPv6 filtering must be performed.

N.B. This account in no way constitutes Arcep's position on the relevance, feasibility or priority of the workstreams. Its only purpose is to describe the information that the different participants provided to the IPv6 Task Force. The courses of action to take will be prioritised in concert with the participants community.

Annex: Working group summaries

Working group	Workshop	Context and issues	Workstreams proposed by participants

Impact of the IPv4 addresses shortage	**Alternatives to making the transition: buy or share IPv4 addresses**	• Need for all players to keep IPv4 for several more years, regardless of whether or not IPv6 is offered.
		• Need for solutions to absorb growth, after having optimised the resource.
		• IPv4 address buying/renting: risk of blocking certain services that use location (VoD, financial services, government services, etc.).
		• IPv4 sharing: problem identifying the subscriber, many applications degraded by CGN.
			• Communicate with businesses to encourage them to make the transition to IPv6.
			• Develop IPv6 training programmes:
			  ○ Training for engineers, but also for managers;
			  ○ Training in engineering schools: heavier focus on IPv6 and concrete case studies.
			• Include IPv6 activation in calls to tender, on top of IPv6 compatibility.
			• Establish best practices for anti-spam rules for IPv6, to drive email's transition to IPv6.
			• Identify the different categories of application, equipment and software for which malfunctions caused CGN have been observed.

	Which option(s) for making the transition: IPv6 in an IPv4-Only network, dual-stack or IPv4 in an IPv6-only network?	• Need for the dual-stack solution to smooth the transition, the duration of this stage being tied to the transition of applications, software, etc. • Need for IPv6 for certain enterprise networks, to enable them to grow (including businesses' internal networks). • Need to promote the advantages of IPv6: offer beta testing for services in IPv6, provide at least the same level of support as exists for IPv4.	• Support the transition thanks to testimonials from enterprises that have switched from IPv4 to IPv6 (at least in dual-stack) to estimate costs, benefits, technical conditions, etc. • Accelerate software's transition: the migration must be massive enough to give software the incentive to deploy IPv6, which means a high enough quality of service for IPv6. • Encourage training and building skillsets: notably amongst young engineers. Dual-stack is one solution to enable an expansion of skills.

	IPv6 compatibility: equipment, applications, software, etc.	• Several IPv6 compatibility issues identified:
		  ○ Certain applications and business software manage IPv6 poorly, or not at all;
		  ○ Certain service platforms (notably voice ones) are not compatible with IPv6;
		  ○ Certain equipment has features that are not IPv6-compatible.
		• Lack of functional parity between v4 and v6:
		  ○ A number of compatible (or partially compatible) equipment are incapable of managing IPv6 with the same quality as with IPv4;
		  ○ Certain software performs poorly with IPv6.
		• Wi-Fi's IPv6 issues.
		• Need to increase the government's role in leading by example in the transition to IPv6.
			• Identify and inventory the different categories of application, equipment and software that cause IPv6 compatibility issues.
			• Define best practices and provide advice (including organisational) to guarantee IPv6 compatibility, for each technical category:
			  ○ Perform a structured inventory of v4/v6 parity, indicating the last holdout links;
			  ○ Make testimonials available in an in-house development guide for IPv6 deployment;
			  ○ Provide a management framework for the transition to IPv6: What to do ahead of time? What does the current regulation say? Who to involve? When?
			• Encourage IPv6 compatibility to be taken into account in public service contract tenders, taking a cue from the France numérique 2012 scheme.

Working group	Workshop	Context and issues	Workstreams proposed by participants
IPv6 security issues and challenges	**Securing the local network (enterprise, datacentre)**	• Existence of several IPv6 network security aspects, similar to IPv4's but IPv6 requires a security rethink. • Poor understanding of existing IPv6 security solutions. • Several standards and RFC not updated. • Lack of available skilled labour for existing IPv6 security solutions.	• Inventory businesses/hosting companies' main problems; ○ Compare v4 vs. v6 security. • Inventory updated RFC and IPv6 security training resources; • Collect analyse and compile RIPE's existing resources as well as Internet Society initiatives (Deploy 360, etc.), and update them.

	Anonymisation and privacy	• Presence of an identification and location bias when a MAC address is available in the IPv6 address.
		• Online tracking problems with IPv6:
		  ○ NAT66: Is it a solution that should be installed systematically?
		  ○ DoH: Is it an additional means for tracking users?
		• Existence of privacy solutions: privacy (rfc4941), opaque interface ID (rfc7217), CGA address (rfc3972), etc. extensions? Which ones to favour?
		• Lack of information on the way in which obsolete, uncontrolled or uncontrollable equipment (IoT, tablet or mobile whose OS is no longer supported) should be handled.
			• List the privacy issues caused by IPv6.
			• Discuss the different countermeasures and best practices to implement.
			• Specify the links on the chain where particular efforts are needed: terminal or intermediate equipment (router, DHCP server, etc.) ?
			  ○ Analyse the risks that are covered for each case, and specify residual risks.

	IPv6 filtering issues (box, inter-connection)	• Existence of several Pv6 filtering practise, and lack of consensus on how this filtering should be performed:
		  ○ Security at the peripheral level, to eliminate the need for an IPv6 firewall vs. need for a firewall given the difficulty some connected objects have in protecting themselves from and staying up to date against security breaches;
		  ○ Existence of privacy mechanisms to limit an IPv6 address's traceability. This is not a security mechanism, however. The fact that IPv6 addresses are hard to find and not permanent is no guarantee of security and protection;
		  ○ Some players' desire to adopt the NAT security support model by blocking incoming unsolicited IPv6 traffic by default, using a firewall.
			• Issue IPv6 filtering recommendations, and especially the following:
			  ○ Ability to increase existing IPv4 level security by combining:
			  - An IPv6 address that changes regularly, amongst the unused /64;
			  - a firewall that blocks incoming streams by default.
			  ○ Activate only the corresponding firewall for TCP and UDP, as some want the firewall not to block other protocols, to enable future innovations.
			  ○ Authorise the firewall's simple deactivation, with the ability to deactivate:
			  - Fully;
			  - Peripheral by peripheral;
			  - Port by port;
			  - IPv6 by IPv6.