

ANNEX

IPv6-first open-standard European Internet foundational Stack strengthening the Digital Single Market

Recognising the Internet latest IPv6-based Open-Standards as EU Strategic Digital Infrastructure Pillars



Open standards • interoperability • resilience • competitiveness • technological autonomy

Contribution from European IPv6 experts and national IPv6 councils

POLICY CONTEXT

IPv6-first as a foundational open-standard layer for European digital sovereignty.

As the European Union advances its Sovereignty Act to strengthen technological autonomy, resilience, and competitiveness, attention has rightly been given to the promotion of open-source software as a foundation for a transparent, secure, and innovation-driven digital ecosystem. However, digital sovereignty depends not only on open software, but also on open and globally interoperable Internet standards.

Among these open-standards, IPv6-first represents a critical pillar for ISOC and IETF Internet standardization bodies and thus Europe's digital future. As the successor to IPv4 and the native protocol of the modern Internet, IPv6 is an open, vendor-neutral standard developed through transparent international processes and implemented by all major technology ecosystems, corporations and public bodies worldwide. It enables scalable connectivity, reduces dependence on increasingly scarce IPv4 resources, simplifies network architectures, and supports the growth and innovations of strategic sectors such as cloud computing, artificial intelligence, industrial digitalisation, 5G/6G networks, and the Internet of Things.

Promoting IPv6 adoption aligns with the objectives of technological sovereignty by ensuring that Europe's digital infrastructure remains interoperable, globally connected, and free from unnecessary dependencies on proprietary networking solutions or scarce legacy resources.

The Union and Member States shall take the necessary measures to encourage Union entities and public sector bodies to use and facilitate an IPv6-first open-standard and subsequent innovative protocols released by Internet Standardization authorities' strategy. It is critical to ensure this strategy for key and emerging IT sectors and therefore within the Cloud and AI Development Act (CADA), Internet of Things EU roadmap and High-Performance Computing (HPC) instruments and actions.

Implementing vs. Ignoring IPv6 Consequences

This submission proposes that IPv6 be explicitly integrated into the Tech Sovereignty Package framework as a foundational, harmonising measure.

Modern data exchange between public institutions, Member States and enterprises requires a secure, interoperable foundation, and IPv6 is now the only standard protocol capable of supporting that scale, as stated by the relevant Internet standardisation fora (IETF)[0].

Without an IPv6-first architecture, the EU cannot truly integrate fibre, 5G/6G, Wi-Fi and satellite into a unified digital backbone, nor remain competitive against regions that have already adopted national IPv6 strategies.

Emerging technologies reinforce this urgency: 6LowPAN for Internet of Things mesh networks, SRv6-enabled, programmable networks — essential for AI datacenters and high-performance cloud infrastructures — simply cannot operate on legacy IPv4.

At the same time, security risks are escalating. Since 2022, Chinese threat actors have exploited unmonitored IPv6 pathways while European organisations remain largely unaware of IPv6-specific exposures, leaving shadow assets invisible to existing tools.

Europe's fragmented IPv6 deployment further prevents seamless participation in the rapidly forming global IPv6-based Digital Market.

Compounding this, the shortage of IPv6 training and operational skills has become a critical barrier, even though coordinated capacity-building would greatly reduce cost, complexity and security risk. Transitional mechanisms such as NAT have reached their limits: they cannot sustain the scale required by IoT, AI systems, cloud-native services or networks.

If Europe fails to act while other major powers continue advancing their national IPv6 strategies, it risks becoming increasingly dependent on external technologies, operating under higher costs and security risks, and losing influence over the future evolution of the Internet itself. The choice is therefore strategic, not technical: an open-standard IPv6-first strategy adoption will help secure Europe's sovereignty, resilience and competitiveness, while inaction will gradually erode them.

Today's Major Powers IPv6-First Market Decision

As of 2026, IPv6 is not optional anymore. It is the only scalable addressing system and Internet base layer that can support Europe's digital ambitions for the next 30 years.

Today, IPv6 is no longer a future technology: billions of users worldwide access the Internet using IPv6, representing over 50% of global end users. Several European leading nations[1]—including France, Germany, Belgium, Greece, Hungary, and the United Kingdom—already report IPv6 adoption rates well above 50%.

In line with the historical evolution of the Internet—where new technologies typically reach end users first and are subsequently adopted by enterprises and large-scale infrastructures—IPv6 adoption has now become a priority for public infrastructures and enterprises. Today, IPv6 is quickly becoming a foundational technology embedded across the entire digital value chain, encompassing devices, connectivity, platforms, security capabilities, applications and innovative architectures.

In response to this priority, several leading digital economies[2]—including China, India, Japan, Malaysia, UAE (United Arab Emirates) and the United States—have implemented explicit national strategies and mandates to advance IPv6-first and IPv6-only adoption across administrations, cloud platforms and critical public and private infrastructures. These efforts position IPv6 as a core enabler of digital scale, resilience, and security.

Aligning European Commission Programmes with an IPv6-First Internet Reality

The Tech Sovereignty Package is foreseen in the first Semester of 2026.

The Package represents a generational opportunity to rebuild Europe's connectivity and digital sovereignty framework, designed to modernise Europe's digital networks, create modern and unified Sovereign Cloud base layers, AI and HPC ready infrastructures and Internet of Things ecosystems while boosting cybersecurity and strengthen technological sovereignty and ensure fair cost-sharing between digital players.

In order to enhance strategic goals, the European Commission may work in existing and new partnerships, policies, incentives, instruments, actions and packages ensuring IPv6 open-standards as core enablers resulting in Europe long-term Internet technologies autonomy, eliminating IPv4 scarcity costs and address markets, enabling efficient connectivity deployment, improving cybersecurity and network manageability, strengthening the Single Market through cross-border interoperability and providing a future-proof foundation for European AI and cloud sovereignty strategies.

In this preliminary formulation, the following six refocusing measures are suggested:

Foster IPv6 Deployment. All electronic communications modern networks (including fibre, 5G/6G and Satellite constellations), platforms and services should evolve to support IPv6 end-to-end cross-border operation by default.

Ensure IPv6-first strategies within Emerging Critical Economy IT sectors. Particularly, within the CADA (Cloud and AI Digital Act), HPC and IoT ecosystems related actions and instruments.

Promote and create incentives to foster European engineers', marketing professionals' and executives' awareness, knowledge and skills to ensure Europe develops the expertise required to deploy, operate and innovate on IPv6-based infrastructures independently and at scale.

Develop IPv6 Requirements to Cybersecurity and Resilience Provisions.

Set IPv6-Only Operation target for 2030 with phase out IPv4 (maintained only through transitional gateways) **plans** by 2032.

Europe's IPv6-first Digital Economy Implementation Measures

Building on the approach set out above, the Union and its Member States shall incorporate corresponding IPv6-readiness obligations into their respective national assignment frameworks and shall operationalise them through an actionable implementation plan comprising, at a minimum, the following elements:

IPv6-first Cybersecurity. All IPv6 deployments shall comply with Union cybersecurity requirements, including secure-by-design IPv6 configurations, routing security, DNSSEC-enabled services and incident-response readiness. Operators shall integrate IPv6-specific risks and controls into their security audits and resilience plans. ENISA shall issue guidance on IPv6 security baselines applicable across the entire connectivity ecosystem.

Capacity Building: Member States, in cooperation with ENISA, the IPv6 Forum and the national chapters of the IPv6 Forum shall implement capacity-building programmes to develop IPv6 expertise in public administrations, regulators and private economic sectors. Training initiatives shall prioritise IPv6-secure operations, network automation and migration planning. The Union shall support common curricula, knowledge exchanges and technical workshops to strengthen human capital across the digital networks sector.

Improve University computer science/telecommunication programs including IPv6-first as a cornerstone of Digital infrastructures knowledge, otherwise we have graduates with obsolete knowledge entering the labour market.

Funding and Incentives for Upgrades, Innovation and Hands-on. Union funding instruments shall prioritise IPv6-native investments supporting AI infrastructures, cloud and edge data centers, and industrial IoT ecosystems leveraging 6LoWPAN and Wi-SUN-based profiles. Financial support shall also promote SRv6 and related technologies, enabling fully programmable, end-to-end network architectures. Funds may be directed to pilot deployments, innovation actions, and upgrades, accelerating the shift toward IPv6-only, software-defined connectivity across the Union. A key condition for funding must be that the pilots will become IPv6 production too.

A good reference is CERN recent IPv6-only deployment at the Worldwide Large Hadron Collider Computing Grid (WLCG)[4] as Dual-stack is not, however, a viable long-term solution.

Europe's IPv6-First Policies' potential impact on strategic Sectors

Internet technologies constitute essential infrastructure for communications, economic activity, and the delivery of public services across the Union. International standardisation bodies increasingly mandate the adoption of IPv6 as the current and future protocol of the Internet.

The implications of this transition for key European Economic and strategic sectors shall be considered, covering:

The European Cybersecurity Industry and Safety: IPv6 will enhance European security by avoiding IPv6-specific threats and vulnerabilities, improved European tools and more traceability by avoiding public IP address sharing.

The Financial Sector. IPv6 will allow financial institutions to operate simpler, more scalable, resilient and low-latency infrastructures, essential for real-time transactions and AI-driven analytics. It will reinforce cybersecurity and fraud-prevention, routing security and stronger isolation of sensitive services.

The Utilities Sectors. IPv6 will facilitate massive device connectivity for smart grids, supply-chain monitoring and automated retail systems, improving operational efficiency and service continuity. It will enable more secure, real-time control of industrial assets and distribution networks. These capabilities will reduce outages, optimise resource usage and enhance customer experience.

Smart Cities and Smart Agriculture ecosystems. IPv6 will unlock large-scale, interoperable IoT deployments required for mobility management, environmental monitoring and precision agriculture. It will improve data flows across sensors, devices and edge platforms, enabling more efficient and sustainable urban and rural services. Its built-in scalability and security will support advanced automation and decision-making across these ecosystems.

The Retail sectors: IPv6 will enable retailers to deploy large-scale sensor networks for inventory tracking, loss-prevention systems and real-time supply-chain visibility, improving operational efficiency and reducing stock-outs. Its expanded addressing capacity will allow seamless integration of smart shelves, connected POS terminals and customer-experience technologies such as personalized in-store services and automated checkout.

Final Remarks

Europe must recover the spirit of Internet leadership that helped give the world the World Wide Web through CERN in the early 1990s. Today, a similar opportunity exists to shape the next generation of digital infrastructure by ensuring that Europe is not only a consumer of digital technologies, but also a leader in their deployment, operation and evolution.

Achieving this objective requires coordinated policies, sustained investment and clear political commitment at both EU and Member State level. Strategic support for open standards, digital skills development, research, innovation and infrastructure modernisation will be essential to strengthen European competitiveness, accelerate digital transformation and enhance cybersecurity resilience.

Digital sovereignty cannot be achieved solely through sovereign cloud services, artificial intelligence or semiconductors. It also depends on the underlying Internet open-standards architecture that connects citizens, enterprises, governments and critical infrastructure. A resilient, scalable and interoperable Internet foundation is a prerequisite for Europe's technological independence.

IPv6 is not merely a network upgrade; it is a strategic enabler of Europe's future digital economy. It provides the addressing scale, operational efficiency and architectural simplicity required for AI, cloud computing, IoT, advanced telecommunications and future digital services. By embracing an IPv6-first approach, Europe can reduce strategic dependencies, strengthen cybersecurity, foster innovation and ensure its continued ability to compete on equal terms with other global digital powers.

The choice facing Europe is therefore strategic rather than technical: to lead the future Internet or to depend on infrastructures and decisions shaped elsewhere. A strong commitment to IPv6 deployment will help ensure that Europe's digital future remains open, secure, innovative and sovereign.

References

[0] IETF, Internet Engineering Task Force.

[1] APNIC IPv6 adoption statistics

[2] Include references of China, USA, India, etc.

[3]

[4] Towards an IPv6-only WLCG: More successes in reducing IPv4

Contributing Organisations

This document has been prepared with the sole purpose of contributing to the objectives of European technological sovereignty, digital resilience and long-term competitiveness.

It reflects the collective expertise and shared concerns of independent IPv6 experts, engineers and Internet practitioners from multiple European Union Member States. Drawing on operational experience across public administrations, telecommunications operators, cloud providers, enterprises and research communities, the contributors have worked together to identify common challenges and harmonised recommendations for Europe's digital future.

This contribution is guided by core European values: openness, interoperability, technological independence, diversity, innovation, security and cross-border cooperation. Its objective is to support policymakers in building a resilient, future-proof and globally competitive digital ecosystem based on open Internet standards.

The authors believe that IPv6 is not merely a technical evolution, but a strategic enabler of European digital sovereignty, cybersecurity, competitiveness and innovation. The recommendations presented in this document are intended to help ensure that Europe remains an active leader in shaping the future of the global Internet rather than a passive consumer of technologies and architectures defined elsewhere.

The following organisations have participated in its preparation (listed in alphabetical order):

IPv6 Council Belgium,

IPv6 Task Force France

IPv6 Council Germany

IPv6 Council Ireland

IPv6 Council Spain