GOVERNMENTS ENABLED WITH IPv6

GEN6

WHY ARE GOVERNMENTS ON IPV6?

START YOUR IPV6 PROJECT RIGHT NOW

This project has received funding from the European Union´s

European Commission

BE READY FOR IPV6

There is nothing more important in the contemporary world than to be a step ahead. On the contrary, getting one step behind can cause serious problems.

The Internet and nearly all local computer networks make use of the Internet Protocol. Due to the success and the penetration of the Internet in nearly every part of modern life, the initially used Internet Protocol Version 4 (IPv4) is running out of address space. In Europe, the Internet registry ran out of IPv4 address blocks in February 2012. To solve this shortage, the Internet Protocol Version 6 (IPv6) was developed. IPv6 offers hugely more addresses to identify endpoints.

Network providers with a growing customer base are forced to use the Internet Protocol Version 6 (IPv6) to get new customers connected. Connecting ever more networked machines to the Internet ("Internet of things") requires a huge number of additional IP addresses.
Leading content providers in the Internet world such as Facebook and Google are already running on the new version of IPv6. Some governments have already followed their success story, too. Not supporting IPv6 can cause connection problems and information lack on a web site to visitors connecting from an IPv6-enabled network.

If public and private sector will introduce IPv6 in their policies, nobody will be excluded in future from the benefits of the information society. When implementing IPv6, one has to remember to "think globally and act locally". No citizen must be withdrawn from the convenience of an ever improving information society.

Now it's your turn to join them!

This booklet describes some aspects of IPv6 transition based on the experiences of the national pilots of the GEN6 project.

Things we have to face

On the following pages we list some facts and observations happening around IT, services and networks - often being neglected, pushed to some point of time in the future or even be feared. The arguments you may hear are ‚That's the problem of my provider' or ‚There is still enough time before this will affect my business'. It doesn't matter whether you belong to the economic or government sector or are a private person. Why can delaying IPv6 rollout be a wrong conclusion? Read on and act before you see the taillights of your competitors.

Roll out for citizens is on its way

Providers are using IPv4 addresses for customer connections until now. Most providers that have been in business for many years have significant IPv4 resources available. On the other hand, competitors joining the market in the last years could not claim a huge amount of IPv4 addresses. Due to the shortage of IPv4 addresses they were forced to think about the step towards IPv6 in their access networks. Nowadays, several providers connect new customer only with IPv6 and connections to the 'legacy' world of IPv4 are implemented by tunnelling and network address translation in IPv4 or 6to4-solutions. In both cases, expensive carrier grade gateways must be implemented. This results in increasing costs for the providers and in consequence for the citizens and businesses.

With IPv6-enabled server/service and access connections, one can use IPv6 without any gateways. Use of those expensive gateways can be minimized and therefore some costly investments can be avoided.

Loss of communication

To give availability of 6to4-gateways to all customers, most of the time the number of parallel connections per customer is limited. When web sites with a high information density, e.g. city map services, use many several parallel connections to speed up the transmission, some transmissions may get blocked – with an incomplete site presentation as a result on the customer side.

Websites and Internet services providing IPv6 connectivity will not be hurt by those connectivity issues, because they communicate directly with IPv6 without such gateway limitations.

Stagnation on eGovernment evolution

The continuous growth of electronic communication demands more connectivity and more hosts. Each node requires its own IP address. As described above, IPv4 addresses have become very limited nowadays. New large address blocks are no longer available from the regional registration authorities. Addresses can often only be acquired from someone that still has an existing claim on IPv4 addresses (but does not use all of them). This approach causes delays for new projects and businesses up to a total stop due to unavailability of IPv4 resources.

Shadow market on IPv4 addresses

Up to now IPv4 addresses were not traded on a market – but this starts to change with the upcoming shortage. The implementation of further services may require the costly acquisition of IPv4 addresses, as they have become a limited asset. Each additional large project requiring additional IPv4-addresses may cause an extra growth in IPv4 address costs.

IPv6 addresses on the other hand are available in great number via the Regional Internet Registries (RIRs). This guarantees a non-market for allocation fees for further IPv6-addresses. Introducing IPv6 and moving traffic to IPv6 can result in overall lowered acquisition costs for IP addresses.

(Re-)Enabling the end to end communication

Today's local networks mostly operate with so-called "private IP addresses". Their use was not originally planned when the Internet was designed. In the public Internet only packets with public IP addresses will be routed, therefore an address translation between the address types must be established. This so called network address translation (NAT) is located at the Internet gateway of one's local network. Due to cooperation between governments, private organizations and companies sometimes multiple networks must be interconnected. Usually, at each network's edge a NAT gateways is in use. This inhibits the end to end view of the IP communication. At every point of the transmission even the network administrators only have a clear track up to the next NAT gateway. Everything behind is hidden and hard to reach – even where it should be reachable. In effect, this results in huge administration efforts in implementation and in troubleshooting of all those connection paths.

Furthermore, real-time communication profiles such as voice or video do not operate across NATs without special network appliances, causing additional costs in implementation and operation.

In IPv6, the former end to end paradigm of the Internet communication has been re-injected. The NAT mechanism with private IP addresses is not available anymore in IPv6. Therefore, every communication is clearer and more direct. This reduces administrative efforts and operational risks by increased transparency in the transport services.

Why the loss of NAT is no evil

In marketing material of the gateway vendors network address translation (NAT) evolved into a security feature. However, the security effects of NAT are a result of stateful ingress packet filtering and application layer gateways – features that are also available without address translation. The advertised hiding of local endpoint addresses behind a NAT firewall is a myth for many use cases, as for example the local IP address of a client can be read in every http-based browser session on the server side.

In IPv6, the strength of the public-to-private network border is in the strength of the gateway configuration with suitably customized, well deliberated rule sets – just like with IPv4 today. However, due to the absence of the address confusion due to NAT, rules can be defined more clearly and therefore with less risk of misconfiguration.

What we want to avoid?

- Digital darkness
- Broken connections
- Stagnation of eGovernment services due to address shortage
- Costs for gathering additional IPv4 resources

What we want to achieve?

- Available e-services
- Direct communication
- Secure network configuration

Stay connected = Be IPv6 ready!!!

Policy background

The support of the new Internet Protocol Version 6 has been implemented by some governments into their national policies. However, in the era of the global Internet, using IPv6 is not only a national issue, but European as well. Policy support for IPv6 has been mentioned first in 2002 within the Communication called “Next Generation Internet – priorities for action in migrating to the new Internet protocol IPv6”. However, today’s Digital Agenda for Europe is much more important for current decision makers and policy creators. These key European strategies called within the Action 89 the Member States to make eGovernment services fully interoperable while overcoming organisational, technical or semantic barriers and supporting IPv6. The need to provide electronic services via IPv4 plus IPv6 is highlighted also within the European eGovernment Action Plan 2011-2015.

Recommendation for policy-makers

Based on analysis and long-term experiences from the GEN6 project, the following recommendations can be made in order to improve the provisioning of electronic services as well as the implementation of IPv6:

- *Involve* support for improvement of electronic services and IPv6 in strategic documents and policies.
- *Require* IPv6 support when renewing infrastructures and electronic services, preferably in the RFP (Request for Proposal) documentation.
- *Communicate* on a regular schedule with national domain registries since they are usually the ones who informs about various ways of IPv6 implementation.
- *Follow* awareness-raising and information events in order to learn about possible ways to upgrade software and hardware that needs to be transformed to IPv6.
- *Maintain* permanent discussions among IT experts, politicians and civil servants to exert pressure on the implementation of IPv6 and related current standards.
- *Provide* practical workshops for IT experts in order to learn and work with IPv6 and spread technical as well as organisational best common practices.

How to get informed?

Transition efforts exist in the public sector as well as in the private sector. In order to fulfil the European Competitiveness and Innovation Framework Programme we have do our best to extend the European knowledge society. Transitioning to IPv6 requires learning and being familiar with best practices. Be inactive! Get involved! Learn and make sure you're keeping track. Information and ongoing discussions will prevent underestimation of this important issue and will help to avoid possible mistakes in the future. The private and non-profit sector needs to be involved, too.

PRIVATE SECTOR

Very positive role in the deployment of IPv6 represents national domains registry. By promoting and informing about necessity of new protocol, national domain registry can facilitate decision makers as well as IT experts to create a strategy for IPv6 deployment.

PUBLIC SECTOR

Several national Ministries launched a strategic plan for IPv6 deployment. Their web sites in common offer several support and best practice within the government transition to IPv6, as well as short tutorials.

→ Further reading: http://www.gen6-project.eu/links/

Best practices in government policy

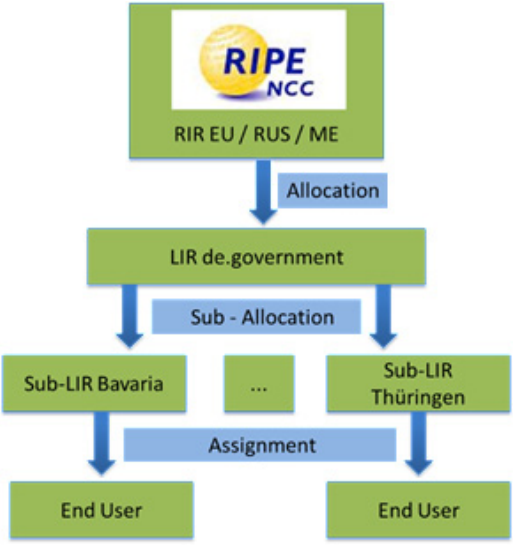
In the Czech Republic legislation made implementation of IPv6 obligatory for central government institutions. This government resolution, prepared by the Ministry of Industry and Trade in 2009 and extended in 2013, had a positive impact on IPv6 that resulted in considerable higher rank of IPv6 deployment. During the last one and half year, the IPv6 support on web-servers has increased from 36% to 57% by ministries and from 50% to 82% by other central government institutions. Meanwhile national average in the Czech Republic is 19.5% (January 2013) and by TOP100 companies only 5%! The example shows that mandatory deployment of IPv6 can be an efficient tool to increase the readiness for IPv6 and public sector can give a positive example to private sector!

Especially in relation to the net neutrality there are interesting examples of policy implementation *"General rules and recommendations for the use of data traffic management in the provision of Internet access service"* adopted by the Czech Telecommunication Office (CTU). According to these guidelines, "the access to the Internet" means a service enabling to connect all end user points connected via IPv4 or IPv6. This definition is related to the **net neutrality and CTU clearly states that net neutrality means also a freedom to choose an Internet protocol** – IPv4 or IPv6 and same rights are granted for IPv4 and IPv6 users as well.

Best practices in government address allocation

The routing between governmental networks over rented lines and the improvement of security by transparent routing can be significantly supported by using a homogenous IPv6 addressing space for the national government. For a central management of domestically used governmental IP addresses, an institution of a country needs to become a Local Internet Registry (LIR), registered with the RIPE NCC (see figure below). This way has been chosen in Germany, and it is currently under discussion in Spain. Germany set up its central LIR called „de.government“ in 2009. Upon extensive requests, the RIPE NCC allocated one /26 prefix for this LIR.

Beneath the LIR de.government a set of Sub-LIRs was founded to organize the IPv6 address deployment in Germany. Based on the /26 prefix, the LIR takes care of the (top level) management of the IPv6 addresses for the public administrations in Germany. A domestic address plan determines the use of the next six bits, after the /26 prefix. This way, one or more /32 prefixes are allocated to sub-LIRs as the basis for /48 site prefixes they hand out on request to their customers.



⟶ Further reading: http://www.gen6-project.eu/publications/booklets/

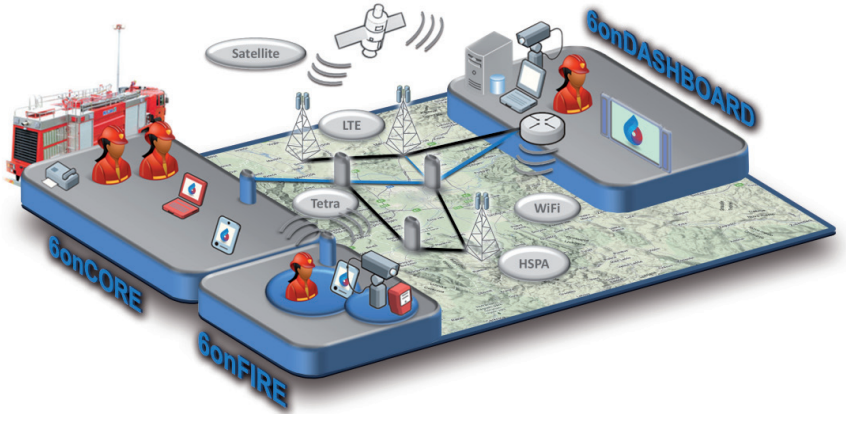
Best practices in energy and green IT

The Greek pilot in GEN6 aims to influence the behaviour of the local school communities by raising their energy awareness. The pilot provides real-time energy efficiency services over IPv6-enabled grids to the local educational community, providing students with information on their energy consumption patterns and raising awareness among them on the energy savings that behavioural changes may bring. Through the implementation of the Greek IPv6 pilot, the deployed infrastructure has been extended and many problems that are related with the use of IPv4 for access to the smart energy meters have been solved. This extension provides a signal to European stakeholders that IPv6 technology can be an enabler for green IT.

⟶ Further reading: http://www.gen6-project.eu/publications/booklets/

Best practices in emergency response systems

The aim of the advanced emergency response communications pilot - A-ERCS - is to clearly demonstrate the state-of-the-art IPv6-enabled features in emergency response environments.



More specifically, the A-ERCS pilot demonstrates:

- A scalable and robust overlay system for data transport and rich multimedia service built across both professional (e.g. DMR, TETRA, and Satellite), commercial networks (e.g. UMTS/HSPA, LTE) and ruggedized alternative commercial-of-the-shelf (COTS) systems (mesh Wi-Fi and ad-hoc WiMax).
- The ability of such a system to deliver seamless connectivity from targeted/affected areas across heterogeneous technologies and public networks, locally as well as on national and cross-border levels.
- Capabilities of the IPv6 technology to assist in deployment of automatic network planning and deployment capabilities, vital to all PPDR systems.
- IPv6 support for advanced features, such as network, node and host auto configuration, and self-organization and self-healing characteristics.
- The ability of such a system to assure secure and QoS-enabled transmission of data, voice and multimedia-rich services system by relying upon modern professional and commercial telecommunications networks and IPv6-based technologies and features.

The A-ERCS pilot is part of 6inACTON, a broader PPDR communications and intervention management solution. More information is available at: www.6inaction.net

⟶ Further reading: http://www.gen6-project.eu/publications/booklets/

Best practices in backbone transition

The Spanish IPv6 transition pilot within the GEN6 project is implemented by the Ministry of Finance and Public Administration (MINHAP) and the Ministry of Industry, Energy and Trade (MINETUR), with the collaboration of the University of Murcia. It aims to foster the IPv6-readiness of e Government services, with a pragmatic approach based on the following principles:

- building upon the infrastructure already in place, making the most of the IPv6 capabilities of the existing hardware, software and networks,
- relying on the use of shared services, to increase efficiency in the use of the existing resources, and avoid divergence in technologies and solutions,
- providing enough flexibility so that it can accommodate the different transition paths of the different administrative units (IPv4 and IPv6 coexistence), and
- assuring that the experience from the transition to IPv6 of the early adopters is shared and used by the administrative units that follow, so that their own transition can be softened.

The pilot takes advantage of the existence of Red SARA (SARA network), operated by MINHAP, which connects all Spanish Public Administrations, as well as the shared services that Red SARA provides.

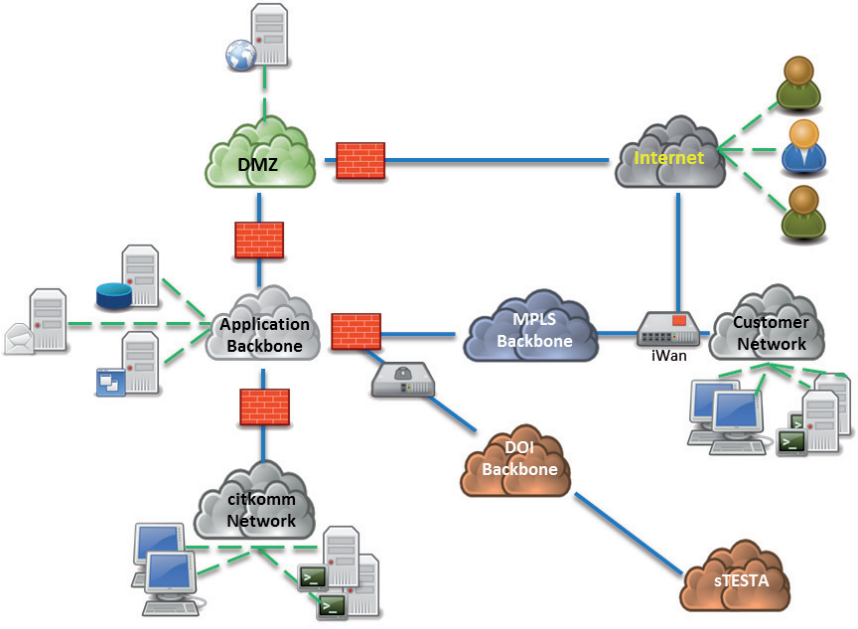
⟶ Further reading: http://www.gen6-project.eu/publications/booklets/

Best practices in data centre transition

The German pilot aims to the transition of the Citkomm data centre infrastructure in the municipality Iserlohn, transitioning several applications to an IPv6-enabled dual-stack scheme. The local IPv6 infrastructure will be implemented in the “de.government” IPv6 address space and will be connected to the DOI network of German administrations.

Besides the specific applications themselves, this requires the network and the local infrastructure including all clients to be IPv6 enabled as well. The work on the application backbone differentiates between the inner backbone, providing specific application services

to the employees of the local government, and the outer backbone – commonly known as de-militarised zone (DMZ) – offering e-government services, portal applications and web presentations to the citizens.



The transition of a data centre encompasses the following areas:

- Network Infrastructure
- Application Backbone Infrastructure
- Customer Environment
- Migrating from TLS/SSL to IPsec

⟶ Further reading: http://www.gen6-project.eu/publications/booklets/

Best practices in eGovernment service transition

The eGovernment Gateway (EGG) is an existing service and offers a central access to around 200 e Government services to more than 13 million registered users in Turkey. Around 50,000 new wcitizens subscribe to EGG every day. These numbers point out the public interest on this service and reveal possible wide impact of enabling IPv6 on such a service. The experience to be gained by the realization of such a big-scale pilot project in the scope of the GEN6 project allows to derive best practices, guidelines, methodologies and toolkits for the transition of e-Government services all around Europe. The main goal throughout the pilot was to make the EGG portal and candidate EGG services IPv6-enabled.

⟶ Further reading: http://www.gen6-project.eu/publications/booklets/

All these pilots are showing why the transition to IPv6 is unavoidable! They can give you inspiration about where to start your transition, what might happen during this phase and inform you about the things you need to do and to avoid. However, in the light of your own project think of one of Fleetwood Mac's greatest hits and

„Go your own way!"

DISCLAIMER

This booklet is powered by

This work was part-supported by the European Commission as part of the project “Governments Enabled with IPv6” - GEN6. GEN6 is about stimulating EU-wide deployment of IPv6 by means of best practices and guidelines in existing eGovernment infrastructures.

Authors:
Zuzana Duračinská (CZ.NIC, Czech Republic)
Uwe Holzmann-Kaiser (FhG FOKUS, Germany)
Martin Krengel (Citkomm, Germany)
Jiří Průša (CZ.NIC, Czech Republic)

Contact:
To get in contact with the GEN6 project or the partners please contact us in:
info@gen6-project.eu
www.gen6-project.eu

This booklet is part of a series of information on IPv6 transition in eGovernment. See www.gen6-project.eu/publications/booklets/ for further available booklets. Booklets already published:

- Government motivation for IPv6 transition
- Smart communication solutions in emergency situations
- IPv6 Application in the road domain
- IPv6 Address Planning and Transition
- Requirement Analysis for eGovernment Services with IPv6