



Title:	Deliverable D3.6 – eGovernment Services with IPv6 Compilation	Document Version:
		1.0

Project Number:	Project Acronym:	Project Title:
297239	GEN6	Governments Enabled with IPv6

Contractual Delivery Date:	Actual Delivery Date:	Deliverable Type* - Security**:
31/06/2014	10/10/2014	R – CO

*Type: P – Prototype, R – Report, D – Demonstrator, O – Other

** Security Class: PU- Public, PP – Restricted to other programme participants (including the Commission), RE – Restricted to a group defined by the consortium (including the Commission), CO – Confidential, only for members of the consortium (including the Commission)

Responsible and Editor/Author:	Organization:	Contributing WP:
Carsten Schmoll	FRAUNHOFER	WP3

Authors (organisations):

Antonio Skarmeta (UMU), Pedro J. Fernández (UMU), Kamil Seyhan (TURKSAT), Timo Baumgart (Citkomm), Gerold Gruber (Citkomm), Martin Krengel (Citkomm), Carlos Gómez Muñoz (MINHAP), Uwe Holzmann-Kaiser (Fraunhofer), Carsten Schmoll (Fraunhofer), Emre Yuce (ULAKBIM), Onur Bektas (ULAKBIM), Juan José Rodríguez Moreno (MINETUR), Miguel Ángel Rodríguez Ramos (MINETUR), Gabriela Gheorghe (UL)

Abstract:

This document is the final, concluding document in a series of deliverables documenting the progress of three national pilot projects within GEN6. The national pilots are located in Germany, Spain, and Turkey. Their goal is the transition of selected, public sector services from IPv4 to IPv6 networks.

Keywords:

IPv6, e-government, IPv6-enabled services, Public Sector, Pilot Projects

Revision History

The following table describes the main changes done in this document since its creation.

Revision	Date	Description	Author (Organization)
v0.1	01.05.2014	Document creation	Carsten Schmoll (FRAUNHOFER)
v0.2	25.05.2014	Document extension	Carsten Schmoll (FRAUNHOFER)
v0.3	25.06.2014	Document extension	Carsten Schmoll (FRAUNHOFER)
v0.4	01.07.2014	Document extension	Carsten Schmoll (FRAUNHOFER)
v0.5	17.07.2014	Document extension, for German pilot	Timo Baumgart (Citkomm)
v0.6	18.07.2014	Document extension, integration of D3.6.x material	Carsten Schmoll (FRAUNHOFER)
v0.7	31.07.2014	Document extension, for Spanish pilot	Carlos Gómez Muñoz (MINHAP) Juan José Rodríguez Moreno (MINETUR) Miguel Ángel Rodríguez Ramos (MINETUR)
v0.8	20.08.2014	Editorial document overhaul, formatting, etc.	Carsten Schmoll (FRAUNHOFER)
v0.9	22.08.2014	Document extension and Turkish pilot addition.	Emre Yüce (ULAKBİM)
v0.91	30.09.2014	Extension by German Pilot	Timo Baumgart (Citkomm)
v1.0	10.10.2014	Document revision and finalisation	Carsten Schmoll (FRAUNHOFER) Uwe Kaiser (FRAUNHOFER)

Disclaimer

The GEN6 project (number 261584) is co-funded by the European Commission under the ICT Policy Support Programme (PSP) as part of the Competitiveness and Innovation framework Programme (CIP). This document contains material that is the copyright of certain GEN6 partners and the EC, and that may be shared, reproduced or copied “as is”, following the Creative Commons “Attribution-NonCommercial-NoDerivs 3.0 Unported”(CC BY-NC-ND 3.0) licence. Consequently, you’re free to share (copy, distribute, transmit) this work, but you need to respect the attribution (respecting the project and authors names, organizations, logos and including the project web site URL “<http://www.gen6.eu>”), for non-commercial use only, and without any alteration, transformation or build upon this work.

The information herein does not necessarily express the opinion of the EC. The EC is not responsible for any use that might be made of data appearing herein. The GEN6 partners do not warrant that the information contained herein is capable of use, or that use of the information is free from risk, and so do not accept liability for loss or damage suffered by any person using this information.

Executive Summary

This document gives a final overview of the current state of three national GEN6 pilots, and the progress therein. Towards that goal this document summarizes on a high level the findings and technical improvements that were achieved in the three pilot projects.

This deliverable is the final instance of documents in the GEN6 D3.6.x series. As such it less represents new technical details, yet more summarises these D3.6.x deliverables and can be used as a reference or guide to find out where to look up details (if needed) in the other deliverables. To some degree it adds new knowledge, gained from work on the three pilots done after the last D3.6.x deliverable, i.e. D3.6.4.

The three national pilots working inside the GEN6 project are located in Turkey, Spain and Germany. Their targets are similar: examining existing e-government services currently based on IPv4 and building a pilot for selected services to ease the transition to IPv6. This of course needs the transition of basic networking equipment first. The environments in which the pilots are being implemented (technical and administrative responsibilities, existing infrastructures, pre-existing addressing plans, administrative level, etc.) are rather diverse. So are the challenges encountered and possible solutions. On the technical side, there are some overlaps to be exploited when common infrastructure components are migrated, such as Switches, routers, operating systems, and DNS, e-Mail, and firewall systems. All these need to have a sustained IPv6 support, working in a real-live environment, to make the transition of e-government applications and services possible on top.

Apart from the value of the individual experiences gained in the pilots, the summary of insights allows for a good overview of the broad range of tools, techniques and solutions available when moving e-government Services to IPv6. This range of possibilities is further evaluated and described as the pilots' progress. See chapter 5 for the lessons learned by the pilots.

Table of Contents

1	<i>Introduction.....</i>	9
2	<i>GEN6 Networking Services with IPv6</i>	10
2.1	Network Architectures and Structures	10
2.1.1	Upgrade of External Connectivity	10
2.1.2	IP Addresses	16
2.1.3	Network Planning and/or (Re-)Design	25
2.2	Transition to IPv6	28
2.2.1	Chosen Approach	28
2.2.2	Planned Order of Changes due to Transition	32
2.2.3	Successfully Migrated Components	37
2.2.4	Enabling IPv6 in Components	45
2.3	Affected Network Components	56
2.3.1	Routers and Routing.....	56
2.3.2	Affected Central IT Systems	58
2.4	Security Aspects of Using IPv6	61
2.4.1	Firewalls	62
2.4.2	Application Layer Gateways (ALGs).....	63
2.4.3	Proxies	64
2.4.4	Other Security Aspects	65
3	<i>GEN6 Generic Services With IPv6</i>	66
3.1	Transition to IPv6	66
3.1.1	Chosen Approach	66

3.1.2	Planned Order of Changes due to Transition	68
3.1.3	Successfully moved components until now	71
3.1.4	Enabling IPv6 in Components.....	73
3.2	Affected Network Components	81
3.3	Routers and Routing.....	81
3.4	Affected Central IT Systems	82
3.4.1	DNS.....	83
3.4.2	DHCP	83
3.5	Further Affected Systems/Components.....	84
3.5.1	VPN.....	84
3.5.2	Load Balancing	85
3.5.3	Monitoring	86
3.5.4	Management.....	87
3.5.5	SNMP.....	88
3.6	Security Aspects of Using IPv6	89
3.7	Firewalls	90
3.8	Intrusion Detection/Prevention Systems.....	91
3.9	Application Layer Gateways (ALGs)	91
3.10	Proxies	92
3.11	Other Security Aspects.....	92
4	<i>GEN6 Specific Services With IPv6</i>	<i>93</i>
4.1	German Pilot	93
4.1.1	IPv6-Testbed.....	93
4.1.2	Test Setup.....	95

4.1.3	Results	97
4.1.4	Evaluation of the Results	98
4.2	Spanish Pilot	99
4.2.1	eITV application description	100
4.2.2	Security policies	105
4.2.3	Evaluation of the Results	106
4.3	Turkish Pilot	106
4.3.1	Certification	106
4.3.2	Logging	107
4.3.3	Testbed	107
4.3.4	Public Integration Box	107
4.4	Luxembourg Pilot	108
4.4.1	Description of the service	108
4.4.2	Transition to IPv6	110
4.4.3	Monitoring considerations	111
5	<i>Summary of Lessons Learned</i>	117
5.1	Network Design and Structural Level	117
5.1.1	Spanish Pilot	117
5.1.2	German Pilot	117
5.1.3	Turkish Pilot	120
5.1.4	Common to all	120
5.2	Network Devices Level	121
5.2.1	Spanish Pilot	121

5.2.2	German Pilot	122
5.2.3	Turkish Pilot.....	122
5.2.4	Common to all	122
5.3	Network Base Services Level	123
5.3.1	Spanish Pilot	123
5.3.2	German Pilot	124
5.3.3	Turkish Pilot.....	124
5.3.4	Common to all	124
5.4	Application Level	125
5.4.1	Spanish Pilot	125
5.4.2	German Pilot	126
5.4.3	Turkish Pilot.....	126
5.4.4	Common to all	126
6	Figure Index.....	128
7	Table Index.....	130

1 INTRODUCTION

This document gives a final overview of the current state of three national GEN6 pilots dealing with existing e-government infrastructures, and the progress therein. Towards that goal this document summarizes on a high level the findings and technical improvements that were achieved in the three pilot projects.

This deliverable is the final instance of documents in the GEN6 D3.6.x series. As such it less represents new technical details, yet more summarises these D3.6.x deliverables and can be used as a reference or guide to find out where to look up details (if needed) in the other deliverables. To some degree it will also add new knowledge, gained from work on the three pilots done after the last D3.6.x deliverable.

The single most important aspect of the transition of an existing government service to IPv6 (or dual stack support) is business continuity. Therefore, and depending on the technical environment, different techniques are advisable to add IPv6-support to an e-government service. For the three GEN6 pilot projects, IPv6 has been enabled in addition to the existing IPv4 support. In effect that meant that all projects have mainly chosen the “dual stack” approach whereby each involved, networked component is configured to run IPv4 plus IPv6 at the same time. In Red SARA (Spain) and in Citkomm (Germany) premises some servers have been made available via IPv6 to the outside by adding an HTTP reverse proxy “in front” of them, too.

All pilot projects have chosen to build an IPv4-only test bed initially, which resembles the environment of the real (business) applications as closely as possible, and to work on the transition of this test bed. The steps of this work have been documented in the D3.6.x deliverable series. Knowledge gained in this process is now of invaluable help for the transition of real servers or services later on.

2 GEN6 NETWORKING SERVICES WITH IPV6

2.1 Network Architectures and Structures

2.1.1 Upgrade of External Connectivity

This subchapter documents which steps have been taken or will be taken by the national pilots in order to get external IPv6 connectivity, either from an existing, already used provider or a new provider. This section shall also explain which types of IPv6 addresses (provider dependent or provider independent) were acquired and how access is realized technically (e.g. native or via an MPLS tunnel). Where a pilot uses multiple providers for increased availability of external connectivity, this chapter also shortly highlights how the newly acquired IPv6 connectivity will integrate into the existing multi-provider setup.

Spanish Pilot:

The external IPv6 connectivity of the pilot lies in two points:

- the connection point between Red SARA and the Internet and
- the connection point between MINETUR and the Internet

Regarding Red SARA, Internet connectivity is required in order to allow the access to IPv6-enabled e-government services using the shared service platform foreseen in the pilot. The following figure shows a high-level overview of the connectivity of Red SARA networks:

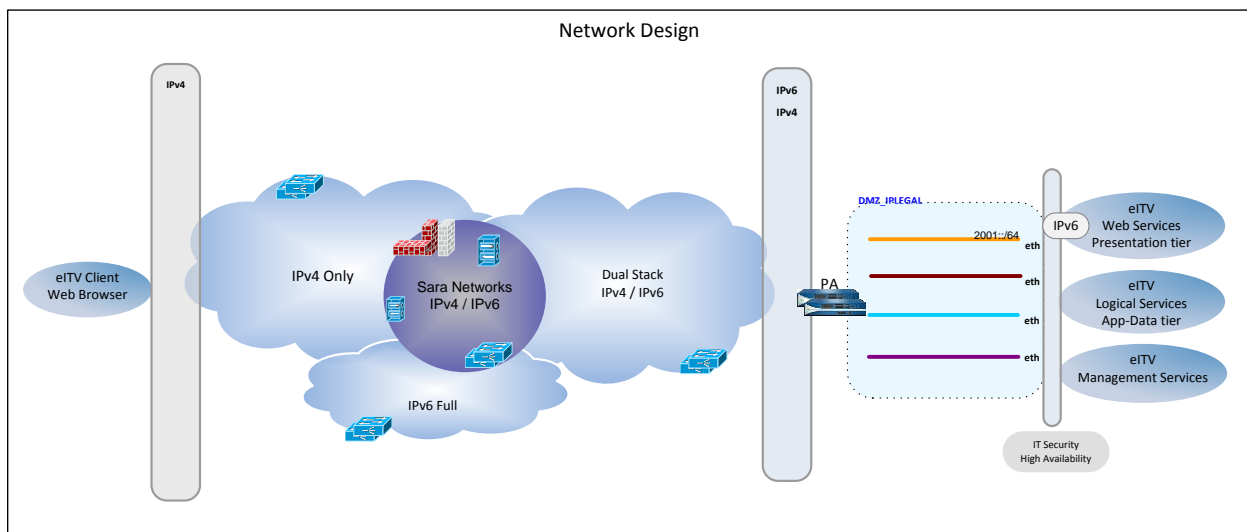


Figure 1– Spanish Pilot Architecture (Red SARA)

Currently this connection point is IPv6-enabled natively by means of the IPv6 service provided by the current telecommunications provider of Red SARA. This provider has assigned Red SARA a /48 prefix (2a00:2000:40a0::/48) from the pool delegated to them by the RIPE-NCC.

The connection is configured for high availability, achieved by means of different redundancy layers:

- Two data centres connected to the Internet, located in different sites
- Two physical links in each data centre
- Two different paths to two different points of presence (POPs) with two AS

The same equipment used previously only for IPv4 (Cisco 3825, 3845, 2851 routers) has been configured now with dual-stack supporting at the same time IPv4 and IPv6 traffic. To achieve this goal, the main change needed was to upgrade firewall software versions (Fortigate 4.0 to Fortigate 4.0MR3 with the patch 441¹) while maintaining the same network appliances.

In the case of MINETUR, the access to the eITV service that will be part of the pilot is different depending on the type of user: Internal users from MINETUR access it through the corporate network, other government units (DGT) access it through Red SARA, and external users (automotive industry) access it through Internet.

¹Version 5.0 allows "policy routing", "DNS64" and "NAT64" but the Fortigate currently installed in Red SARA does not support this version (a hardware upgrade, not foreseen, would be required)

The following figure shows these three ways of access to the eITV service:

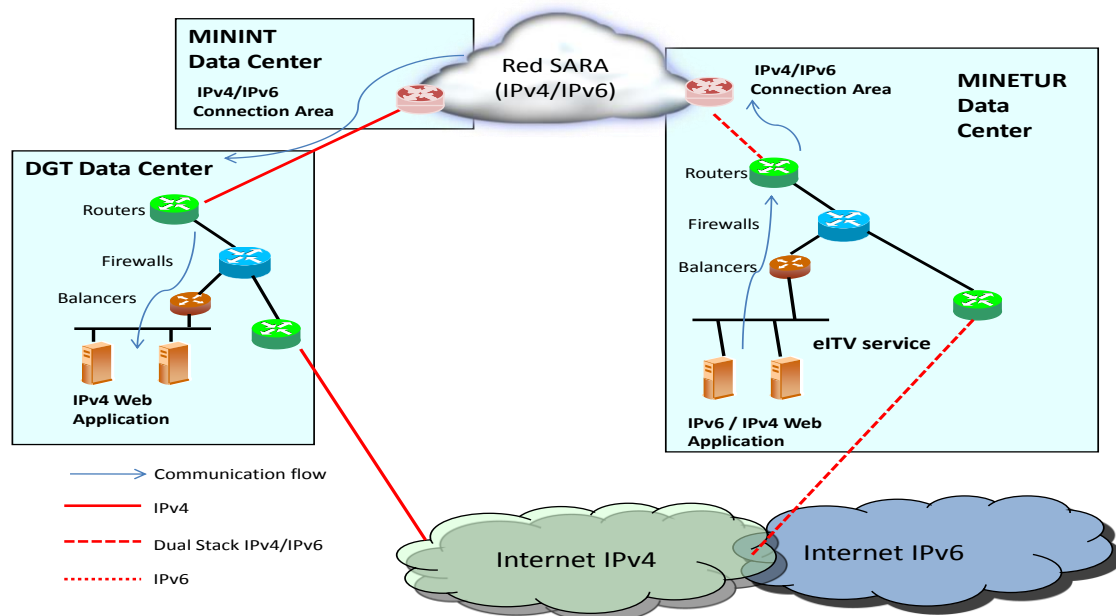


Figure 2 – Spanish Pilot - eITV Service Architecture

Internet connectivity is required so that automotive industry users can access the eITV service that will be part of the pilot. MINETUR has already adapted its external infrastructure to IPv6 and is now able to offer its services over the Internet by means of the native IPv6 connection provided by the ISP of MINETUR, RedIRIS, who has assigned MINETUR the IPv6 addressing space 2001:0720:0438::/48.

German Pilot:

Citkomm is connected to external networks in different flavours. First, there are regular Internet access connections delivered from commercial providers. For obvious reasons of redundancy, two providers are contractors. Initially, Citkomm had gotten “normal” provider dependent (IPv4) addresses from them, in completely different networks of course. This implied several interesting constructions to keep all services reachable from the Internet, in case of an uplink failure of one provider. The decision to move to provider-independent addresses and an own Autonomous System (AS) was even older than the participation in the GEN6 project. Therefore, the contracts with the external providers became of type “IP transit”. Asking them for IPv6 connectivity returned different results: Deutsche Telekom could provide IPv6 and connect Citkomm with IPv6 connectivity after the required route objects in the RIPE database had been created (see the next

chapter on how to obtain IP addresses). The second provider is a smaller one, operating more locally to Citkomm, named DOKOM21. It has been a fresh challenge for this company to route IPv6 traffic through their backbone. Finally, after several months they could provide IPv6 transit, too.

Finally, Citkomm now has its own Autonomous System with provider-independent IPv4 and IPv6 addresses, connected to the Internet via two independent providers.

The second type of connection is a link to the German national governmental Backbone, DOI (“Deutschland Online Infrastruktur”, formerly called TESTA). This link has been enabled with IPv6 in a project of the German Ministry of Interior, independently of GEN6. Chapter 2.2.4.3 contains more information about upgrading Citkomm’s link to DOI.

There also exist MPLS connections to or from different providers. Those will remain as they are for the near future, i.e. use IPv4 with private RFC1918 addresses. Finally, all data traffic from customers runs via OpenVPN tunnels, which can carry IPv6 inside IPv4 packets, besides other combinations. Tunnelling is a possible solution for getting IPv6 traffic across non-IPv6 capable infrastructures for company networks. This approach also turned out to be a working solution for the cross-border pilot from GEN6.

The forth variety of external connections are VPN connections for home workers. The use of either IPv4 or IPv6 connections across the Internet to the VPN concentrators in the data centre is working as planned. However, the IPv6 data connection through the VPN for a single PC or notebook in the home office is still on the to-do list.

Last but not leased there are some remains of the leased line and dialup connection area in the “historic corner” of the data centre. These will stay untouched until they are replaced during the regular exchange cycle.

Note on the Structure of the German Pilot Documentation:

Citkomm describes their information in the same style (same four subsections) for each chapter. This way the reader can have a look on all levels Citkomm has worked on and get a simple outline of the progress. In addition, each chapter will be easier to read because the sub-items are always in the same order. The structure for each Citkomm chapter is as follows:

- General

First, some information of general interest for the topic is given that enables the reader to get an idea of the environment and the described challenges. As Citkomm's business case is to run applications, host data, and provide network connectivity for the municipalities that founded the company, this will be reflected for the areas affected by IPv6.

- Application backbone infrastructure

Therefore, the second sub-item covers pilot results concerning the enabling of IPv6 in existing applications and on the servers they run on.

A separate test bed was installed for application tests. The experiences gained in this test bed as well as those made in the real production infrastructure are documented in this sub-item.

- Network infrastructure

The network infrastructure contains all necessary basic network components to make IPv6 communication possible across the different parts of the network. This includes wide area networks as well as the Internet access network or the connections to other networks, such as the national government backbone DOI or the European sTESTA.

- Customer Environment / LAN

The fourth sub-item is about IPv6 enabling in the Local Area Networks of Citkomm and towards the governmental customer. It is primarily concerned with the office networks for the end-users, i.e. the employees of the governments. This sub-item deals with experiences from the transition of basic local networks as well as basic office applications. It is focused heavily on Microsoft Windows solutions.

Citkomm and Fraunhofer FOKUS established a test environment for working on the pilot that span different networks and locations as shown in Figure 4.

Turkish Pilot:

Two different cases are considered regarding the external connectivity of the Turkish pilot:

- the connection between TURKSAT and the Internet
- the connection between TURKSAT and the participating governmental institutions

The first case is the external connectivity of the central Web portal to the global IPv6 network to provide IPv6 access to the citizens. This connection has been established through the current service provider Turk Telekom by using a native IPv6 connection.

The second case is the connection between TURKSAT and the participating governmental agencies (SGK, PTT and ULAKBIM). Connections to SGK and PTT have been established via VPN on top of the current connection. For this purpose, a Public Integration Box (PIB) has been deployed in remote institutions. Connection to ULAKBIM is also made via VPN. Turk Telekom is the service provider for these connections, too.

The following figure shows the connectivity between the Turkish network entities:

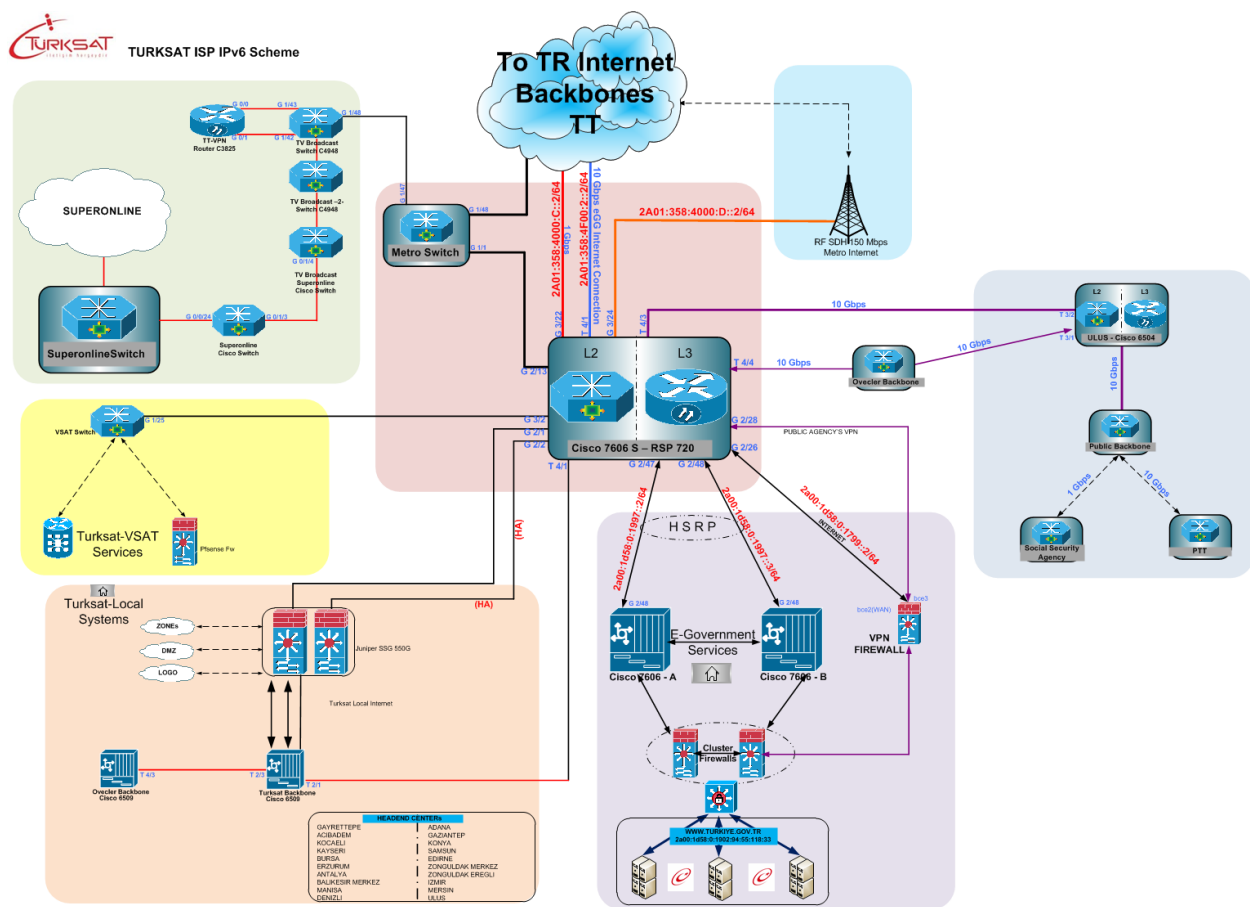


Figure 3 – Turkish Pilot Architecture

2.1.2 IP Addresses

This subsection documents how IPv6 addresses are allocated, distributed across the internal networks, configured to local devices and servers and managed in each national pilot.

2.1.2.1 Allocation and Assignment

Spanish Pilot:

In the Spanish pilot two different levels of addressing plans are required:

- The Spanish Public Administration Interconnection and Addressing Plan defines a common addressing scheme for public administration entities connected through Red SARA. At this level, the addressing plan allocates different prefixes to the connected entities, and gives guidelines regarding address distribution. There is therefore only one Public Administration Interconnection and Addressing Plan.
- An organization's addressing plan distributes the allocated prefixes and assigns addresses to the different elements connected to the organization's network, according to guidelines provided by the Public Administration Interconnection and Addressing Plan. At this level, there are therefore as many addressing plans as entities connected to Red SARA.

Since the current version of the Spanish Public Administration Interconnection and Addressing Plan foresees only IPv4 addresses, an updated version including also IPv6 addresses is under development. The intended approach is based on Red SARA becoming a Local Internet Registry (LIR) and receiving a /26 to /24 block to distribute it among the entities connected to Red SARA, so that these entities can use the assigned public addressing space for developing their own specific addressing plans covering all the IPv6 addressing needs of their networks. Because the update of the Spanish Public Administration Interconnection and Addressing Plan involves national, regional and local governments, its approval is taking more time than what was initially expected, and it will not be probably available in the timeframe of the GEN6 project.

So far, Red SARA has already been registered as a LIR and is in conversations with RIPE-NCC to get the IPv6 addressing space. However, due to the need of justification for prefixes larger than /29, obtaining that IPv6 addressing space is not straightforward.

After the initial conversations with RIPE-NCC, it has been agreed that, not being feasible to provide detailed information of all the entities that may require IPv6 addresses from the common addressing space to support the justification (since it involves the three levels of government: national, regional, local), a simplified approach would be followed. With this approach, Spain

would provide detailed examples of three regions, one of large size, one of medium size, and one of small size, and three ministries, also large, medium and small, being the overall addressing space calculated by extrapolating these examples to the rest.

At the moment of writing this document, a first set of justification documents, one for a ministry and one for a region, has been prepared and sent to RIPE for validation, with positive result, so the process is continuing with the other two examples requested.

Hence, the Spanish pilot will not initially use the addressing space from the Spanish Public Administration Interconnection and Addressing Plan, but it will use the IPv6 addressing space allocated by the current ISP of MINHAP and MINETUR.

In the case of Red SARA, as it was previously mentioned, it has received a /48 block from its ISP to be used in the pilot (2a00:2000:40a0::/48). This block of addresses is of the “Provider Aggregatable” (PA) type, so, in case Red SARA decides to change its Internet Service Provider, all of the addresses assigned to the different elements at the interconnection point and first DMZ should be changed, as well as all the entries at DNS level for the different services.

In the case of MINETUR, and due to the fact, as it has been previously mentioned, that there are different means of access depending on the type of user, there are two addressing spaces allocated:

- The addressing space allocated by RedIRIS, the ISP of MINETUR, 2001:0720:0438::/48, for the connections to eITV service through Internet
- The addressing space allocated by Red SARA to MINETUR, for the connections to eITV service through Red SARA (which is described in the following section).

German Pilot:

Citkomm operates with a subset of the central address space, claimed by the German government from RIPE NCC. From the view of a provider, this address space has to be handled as provider independent.

Based on the national address plan, Citkomm received a /48 prefix for its own infrastructure. The allocated subnet is fully (i.e. as one block) announced to the Internet. Further address spaces outside of Citkomm’s /48 will be made usable later for the customer networks. This is related to Citkomm’s role as municipal data centre. There are some questions still to answer regarding the provider independence of the networks from the German government address space. These discussions are ongoing and Citkomm is a leading participant not at least resulting from the engagement in the GEN6 project.

Citkomm reorganised its Internet access network independently from GEN6. Internet access was changed from two independent links with two completely separated provider-assigned IPv4-address ranges to an autonomous system with Citkomm's provider independent IPv4 network. With a reorganisation of the IPv4 addresses, a new infrastructure was installed with dual-stack capabilities to enable the Internet access for IPv6.

One after the other, the providers were able to route Citkomm's IPv6 addresses, so IPv6 connectivity was given in the beginning on one of the two uplinks of Citkomm only and later on the second uplink, too. Considering the small share of IPv6 traffic from the public Internet, it seemed acceptable to start with a not redundant IPv6 connectivity (compared to IPv4).

Turkish Pilot:

IP address allocation and assignment in the Turkish pilot is considered for

- TURKSAT network and for
- participating institutions (SGK, PTT and ULAKBIM).

Firstly, the 2a00:1d58::/32 IPv6 subnet has been allocated from RIPE NCC in order to be used by TURKSAT. The subnet 2a00:1d58::/36 is reserved for the e-government Gateway Network and is announced to the Internet as AS47524 autonomous system.

Secondly, participating institutions have allocated their own IPv6 address spaces to be used in their inner networks. For the connection between TURKSAT – SGK and TURKSAT – PTT, IPv6 addresses from TURKSAT IPv6 address space have been assigned since there has been a direct connection (dark fibre).

ULAKBIM is the Turkish NREN and the leading institution for IPv6 deployment in Turkey. Hence, ULAKBIM has its own IPv6 address space as 2001:a98/32. This address space is used both for ULAKBIM services and to assign universities and research institutions IPv6 address space of /48.

2.1.2.2 Planning for Internal Subnets

Spanish Pilot:

In the case of the Spanish pilot, there are two plans to be considered:

- The plan for Red SARA
- The plan for the internal network of MINETUR

The plan for Red SARA covers the addressing needs of the connection areas, which act as interfaces for the connections of the entities linked to Red SARA with the backbone, as well as the data centres where the shared services supported by Red SARA are located (among them, the platform for IPv6 shared access to e-government web sites).

The plan for the internal network of MINETUR covers, in the context of the pilot, the addressing needs of the eITV service.

In the case of the Data Centres of Red SARA, IPv6 addressing for the equipment required for IPv6 Internet connectivity has been planned as follows:

Network	Number of hosts	1st Host	Last Host	Used for
2A00:2000:40A0:1::/64	18.446.744.073.709.500.00 0	2a00:2000:40a0:1:0:0:0:1	2a00:2000:40a0:1:ffff:ffff:ffff:ffff	DMZ
2A00:2000:40A0:FFFF::/64	18.446.744.073.709.500.00 0	2a00:2000:40a0:ffff:0:0:0:1	2a00:2000:40a0:ffff:ffff:ffff:ffff:ffff	Router-FW Segment
2A00:2000:40A0:FFFE::/64	18.446.744.073.709.500.00 0	2a00:2000:40a0:fffe:0:0:0:1	2a00:2000:40a0:fffe:ffff:ffff:ffff:fff	NAT64 Segment

Table 1 – Spanish Pilot: IPv6 Addressing for Red SARA

Inside the DMZ, the addressing assignment is as follows:

IP assignment	Equipment
.1	External FW,
.21	DNS,
.22	Mail Server,
.23	PROXY,
.24	REVERSE PROXY,
.30	Secondary DNS

Table 2 – Spanish Pilot: IP Assignment for Servers

While inside the Router-FW Segment, the addressing assignment is as follows:

IP assignment	Equipment
.1, .2, .3 .4	Router
.5	HSRP,
.6	FW iptable ipv6,
.7	NAT64,
.FF	Fwfortigate

Table 3 – Spanish Pilot: IP Assignment for Gateways

Regarding the range reserved for NAT64, the addressing depends on the used IPv4 addresses. The IPv6 address is formed joining the IPv6 prefix and the IPv4 address to which we are doing NAT. For example, IPv4 address 212.163.27.141 (ips.060.es) would be associated with IPv6 address 2a00:2000:40a0:fffe::d4a3:1b8d (d4a3:1b8d is 212.163.27.141 in hexadecimal format).

In the case of the connection areas of Red SARA, a /56 has been assigned to all the Ministries of the National Administration.

2A00:2000:40A0:0000::/56	Ministerio de Hacienda y Adm Púb - SEAP
2A00:2000:40A0:0100::/56	Ministerio de Cultura
2A00:2000:40A0:0200::/56	Ministerio de Industria, Energía y Turismo
2A00:2000:40A0:0300::/56	Ministerio de Asuntos Exteriores
2A00:2000:40A0:0400::/56	Ministerio de Justicia
2A00:2000:40A0:0500::/56	Ministerio de Hacienda
2A00:2000:40A0:0600::/56	Ministerio del Interior
2A00:2000:40A0:0700::/56	Ministerio de Trabajo
2A00:2000:40A0:0800::/56	Ministerio de Fomento
2A00:2000:40A0:0900::/56	Ministerio de Educación
2A00:2000:40A0:0A00::/56	Ministerio de Medio Amb., M. Rural y Marino
2A00:2000:40A0:0B00::/56	Ministerio de la Presidencia
2A00:2000:40A0:0C00::/56	Ministerio de Sanidad y Consumo
2A00:2000:40A0:0D00::/56	Ministerio de Defensa
2A00:2000:40A0:0E00::/56	Ministerio de Economía y Competitividad
2A00:2000:40A0:0F00::/56	AEAT-Agencia Tributaria
2A00:2000:40A0:1000::/56	GISS - Seguridad Social
2A00:2000:40A0:1100::/56	INEM
2A00:2000:40A0:1200::/56	Gabinete de Crisis

Table 4 – Spanish Pilot: IPv6 Assignments to Ministries

From this /56 network, different sub-ranges have been defined for the different network elements, keeping the same structure in all the connection areas. In the case of MINETUR, for example, these sub-ranges are the following:

297239	GEN6	D3.6: e-government Services with IPv6 Compilation
--------	------	---------------------------------------------------

2A00:2000:40A0:0200::/56	Ministerio de Industria, Energía y Turismo	2A00:2000:40A0:0201::/64 LAN MINETUR
		2A00:2000:40A0:020E::/64 DMZ AC MINETUR
		2A00:2000:40A0:020F::/64 RT-FW MINETUR

Table 5 – Spanish Pilot: /64 Ranges Assigned to the Elements of the Connection Area

Additionally, regarding MINETUR internal subnets, MINETUR plans to use a private address range, in case of needing a confidential network without access to public networks for the internal management of the service.

German Pilot:

Citkomm has started structuring the received address space of /48. Planning IPv6 addresses along existing network structures was only in part a viable approach.

A big difference between IPv4 and IPv6 address planning is the completely flexible host part of an IPv4 address since the introduction of CIDR. So transfer networks with also a /64 prefix can take an unexpected big part of the IPv6 address range, if all those interfaces shall be equipped with public routable addresses (versus link local addresses, which would be possible technically spoken). Due to the role of Citkomm, where the secure connection between many customer locations is a central service, there are numerous transfer networks between network components and premises.

Moreover, the structure of the server segments, often based on a /24 dimension in IPv4, can be restructured with an addressing capacity of 64 bits for each network segment.

To be able to use aggregatable address ranges (e.g. in firewall configurations) Citkomm decided to give the fourth word of the IPv6 addresses (bit 48 to 63) a structure as follows:

- The first four bits code the premise where the network is in use. Segments that are available in multiple locations are included in the concept.
- The next four bits (second nibble of the fourth word of the address) encode the usage of the network, e.g. transfer networks, server segments, DMZ, management network or LAN ranges.
- The last 8 bits of the network address simply are used for a sequential number of the network.

Server segments, LAN and Customer Network

In addition to the definitions above for the local area networks, additional restrictions have been made. At this point, the following schema was introduced for the host part of the IPv6 addresses:

- The first word is used to encode a device category, e.g. router, server, client, loopback address, printer, phone, etc.
- The second and third word of the address carries the 3rd and 4th Byte of the IPv4 address of the system. This was strongly requested by the network administrators as they look into firewall logs and try to recognise their packets and the affected systems.
- The last byte is usually set to 1. If there are several virtual machines running on the same hardware or a user has several VMs on his client PC this last byte will be counted up and can be used to distinguish them.

Turkish Pilot:

TURKSAT consists of four large networks, namely:

- e-government Gateway
- Satellite Operations (VSAT, TV and radio streaming, etc.)
- TURKSAT Local Network Operations
- Cable TV and Internet

For the business level and the different Network Operation Centres, the IPv6 prefix has been divided into four subnets of different sizes as follows:

1. for e-government Gateway Datacentre (2a00:1d58:0::/36)
2. for VSAT (2a00:1d58:2000::/36)
3. for TURKSAT Local Services (2a00:1d58:1000::/36)
4. for Cable TV and Internet (2a00:1d58:8000::/33)

SGK and PTT used TURKSAT IPv6 addresses with /64 prefix in order to deploy the Public Integration Box.

2.1.2.3 Address Configuration

Spanish Pilot:

In the case of Red SARA, the equipment to be configured includes a limited set of hosts running network services such as DNS, proxy, etc. Due to this, IPv6 addresses in Red SARA network will be assigned using manual/static configuration. Since there is no end user architecture, which needs IPv6 access, configuring any kind of router advertisement or DHCP service is not required.

In the case of MINETUR's network, address assignment will be performed statically in two steps:

- Initial assignment using auto-configuration
- Final allocation with static IP address assigned in the previous step

German Pilot:

- General:

Citkomm differentiates between static addresses for servers and dynamic assigned addresses for clients. Clients get an IPv6 address by a DHCPv6 server (stateful DHCP). A route to the local /64 network is announced from the default gateway via router advertisement.

- Application backbone infrastructure

The servers have a fixed static IPv6 address from obvious reasons.

The routers distribute the router-advertisements only for possible clients. In this case, they provide in addition to the DHCP server the prefix for the client interfaces to complete the stateful address configuration.

- Network infrastructure

Router systems are configured statically.

- Customer Environment/LAN

Servers get static addresses; clients receive a stateful DHCP configuration.

Static assignments are possible and in use. How to ease and automate the process of getting the Interface Association Identifier (IAID) and DHCP Unique Identifier (DUID) needed for the identification of Windows clients will have to be figured out during this project.

Turkish Pilot:

Address configuration for e-government gateway (EGG) web portal has been made using static IPv6 addressing. This part has included IPv6 addressing of layer-3 devices that need static IPv6 addressing such as load balancers, firewall and web servers.

For SGK, PTT and ULAKBIM address configuration is needed at the point where Public Integration Box is connected. Also at this point static addresses have been deployed.

Due to legislations in Turkey, IP addresses of hosts should be logged. Static addressing makes logging and management of IPv6 addresses feasible. Hence, it is observed that static address configuration is the first choice of system and network administrators in general.

2.1.2.4 Address Management

Spanish Pilot:

At this stage of the pilot, and since the number of addresses to be supervised is not high, address management is being made through Excel sheets, both in the case of Red SARA and MINETUR.

However, in the case of Red SARA, due to the limitation of the Excel sheets for a production environment, and foreseeing a wide adoption of IPv6 in the public administrations in the midterm that will increase the number of addresses to be managed, the use of an IP Address Management (IPAM) tool is being explored, such as Infoblox.

German Pilot:

No tool has yet been planned for address management. The IPv4 addressing plan of the networks is documented in Excel tables, and so is the IPv6 address use. The subnets themselves are documented in sheets concerning one or a few subnets each.

Turkish Pilot:

There is no commonly defined address management scheme in Turkey for IPv6. In general, governmental institutions manage their IPv6 address blocks in parallel to their IPv4 address blocks. Also in this phase, institutions may consult with more experienced institutions such as ULAKBIM.

ULAKBIM currently makes use of excel sheets when assigning new IPv6 address blocks to NREN

members (universities and research institutions). In addition, ULAKBIM has developed and is using a custom application that monitors IP and service status of NREN members.

2.1.3 Network Planning and/or (Re-)Design

Spanish Pilot:

Apart from addressing, new planning or re-designing has not been required in the Spanish pilot, since all the transition to IPv6 has been devised with the aim of maintaining the current architecture and use dual-stack as the intended transition mechanism. New services are located in the same VLANs used previously for Internet connection, adding the new IPv6 stack to the same hardware infrastructure and trying to reflect the previous IPv4 addressing plan structure into the new IPv6 addresses when possible.

It has to be noted that the range used to implement NAT64 did not exist previously (not even the concept), so the creation of a new range has been required (the FFFE for the NAT64 segment mentioned in the planning for the internal subnets section).

German Pilot:

- General:

The GEN6 project started coincidentally when Citkomm reorganised its public addresses for other reasons. The basic structure of the local data centre networks has not been changed. Recommendations on how to structure IPv6 networks found application mainly in the definition of IPv6 address ranges (subnets partitioning) and network access rules. Nevertheless, the IPv6 address scheme embeds the “old” IPv4 addresses in the addresses’ interface identifier part. This way it is easier for administrators to verify that a system has the correct IPv6 address.

- Application backbone infrastructure

One so-called “backbone segment” was chosen be the pioneer for the IPv6 transition of server landscapes of Citkomm’s infrastructure. It received the working title “BRUNNENREICH” in the style of the test municipality called “BRUNNENSTADT”. Citkomm prepares a workflow for easy planning and transition of server infrastructures to enable them for IPv6. The pilot team has evaluated many ideas for a redesign of the existing network segmentation during the introduction of IPv6. Finally, all participants agreed that there would be confusion if a different network segmentations would be used in IPv6 addressing than in IPv4. This is caused by the dual-

stack approach, which is unavoidable from our point of view. There will be no IPv6-only systems for a reasonable period. For this reason – and to keep the network transparent, manageable and understandable by humans – all existing network segments keep their current IPv4 structure.

- Network infrastructure

At the WAN level, the transition to IPv6 did not force any redesigns. At the LAN and server backbone area, the design concept could be modified, especially due to greater subnet dimension. Because this will affect further issues, especially security, we are currently only in the phase of considering a subnet redesign.

Fraunhofer and Citkonn use an OpenVPN connection between their IPv6 test areas over the Internet. In a first step, the channel was established over IPv4. With the availability of IPv6, also an “outside IPv6” tunnel will be tested. This is today’s approach to protect the data on their way through the Internet. OpenVPN is preferred over IPsec because of much fewer problems with firewalls on the way, and for home user setups. Over the years, OpenVPN has become the standard VPN application in the Citkonn network.

The following figure shows a schematic overview of the constructed test bed and its connectivity:

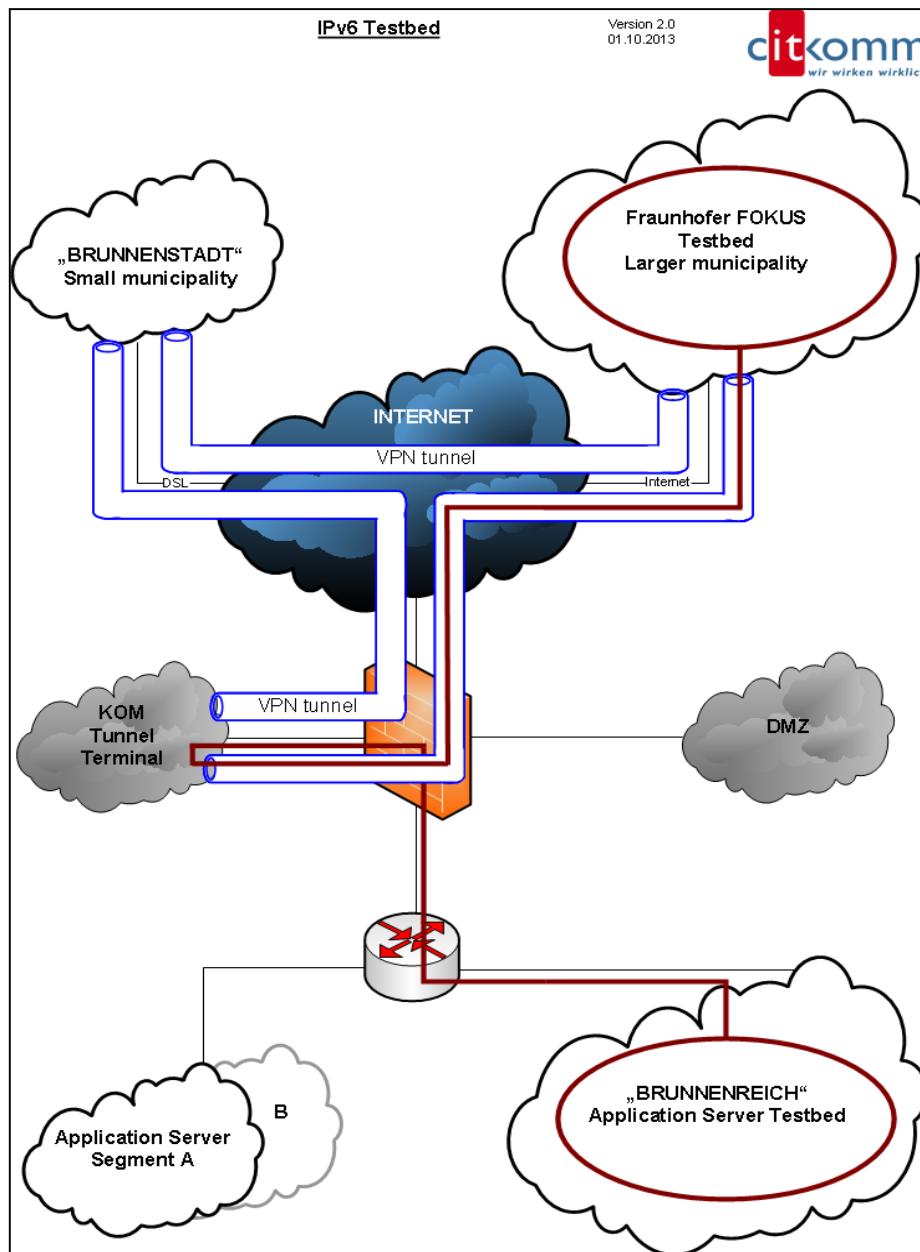


Figure 4 – German Pilot Testbed Architecture

The effects of the use of IPv6 on an ongoing cooperation with a neighbouring data centre will show up later in the future. Regarding the Internet access, the main concern is the source of the used addresses (how or where to get them).

The used general schema or address pool for the administration and authorities of a country seems to be a good approach. If this will really lead to provider independent addresses taken from a central schema for each municipality ongoing talks with the providers will show.

- Customer Environment / LAN

After testing of the address assignment to clients and the operation of the services IPv6 will be rolled out into the LAN of Citkomm and to a pilot customer. Essential is the capability of server and client systems to deal with IPv6. The network design can be left intact.

Turkish Pilot:

In the TURKSAT network, no major network changes were needed since the L3 network devices used in TURKSAT supports dual-stack. Only a software update was required for load balancers in order to deploy a dual-stack network. As the first step, this software update has been implemented successfully.

ULAKBIM, as the leading IPv6 institution in Turkey, has been working as dual-stack since 2003. Hence, no network re-design or planning is needed for ULAKBIM as well.

2.2 Transition to IPv6

This chapter documents the overall chosen high-level decisions concerning the introduction of IPv6 in each national pilot. Per pilot it will motivate the taken decision on how IPv6 will be introduced (e.g. in parallel, new networks, or inside existing ones), what are the steps taken to do so, from a top-down perspective and which aims have already been achieved (and how). In this part of the deliverable also the already found pitfalls in these works performed are documented.

2.2.1 Chosen Approach

Spanish Pilot:

The Spanish pilot envisaged initially three complementary lines of action with different approaches:

- The upgrade of Red SARA so that it can transport IPv6 natively, allowing therefore IPv6 communications between administrative units. This line is approached by means of dual-stack compatibility of elements in Red SARA.
- The implementation of a transition mechanism that allows public administrations to offer online services accessible by means of IPv6, based on a shared service approach. This line is being tackled by means of IPv6-to-IPv4 translation, using reverse proxy and NAT64 equipment located in Red SARA's Internet access.

- The evolution of the MINETUR network so that it can provide native IPv6 services (eITV application) to be consumed by other administrative units (DGT, Directorate General for Traffic). Building an IPv6-native infrastructure is approaching this line.

In this way, three different approaches are being performed and expertise about all of them is being acquired.

Specifically, in the case of MINETUR's network the proposed solution consists of a dual-stack system, allowing both IPv4 and IPv6 address publication. In a first stage, native IPv6 will be deployed, being accessible only through IPv6. This stage foresees an access only through the SARA network as an IPv4-only way of communication.

In a second stage, the architecture will be based on dual-stack. It will allow access through both protocols and publish them to outside public networks. This will be a restricted access by way of a failover system in case the DGT is not able to reach internally the IPv6 address through the SARA network.

The functional design achieves high availability and accessibility needs, key requirements demanded by MINETUR for a critical access system, with a high availability of 99.9999 % defined in the SLA of the service.

In the case of MINHAP, during the implementation of the project there has been an evolution in the chosen approach for offering its own IPv6 ready e-government services. Though initially it was planned that MINHAP's services would be made IPv6 available through the shared service based on IPv6-to-IPv4 translation, the option of having some of these services in dual stack has also been considered. Thinking of potential scalability problems with the shared service if the number of portals integrated with it grows quickly, a mid-term scenario in which the shared service is used by other ministries, while the services operated by MINHAP are using dual stack, was deemed to be foreseen.

In that sense, an initial feasibility assessment covering the STORK service involved in WP4 has been performed, being the result positive, and some other services were evaluated in order to make them IPv6 enabled by means of dual stack: EUGO (Spanish Single Point of Contact for the Service Directive), @firma (eID and e-signature validation platform), Plataforma de Intermediación de Datos (Data Exchange Brokering Service).

Currently, the focus is on those services oriented to the citizens running in the PHP platform, such as the e-invoicing portal and the transparency portal, since they that have been considered more

appropriate for the IPv6 transition than the services oriented to public administrations in the Java platform, such as the eID and e-signature validation platform and the Data Exchange Brokering Service initially planned.

Regarding IPv6 addressing, as it has been mentioned in section 2.1.2.1, the chosen approach to transition involves using initially IPv6 addressing space allocated by the current ISP of MINHAP and MINETUR. Later on, once the Spanish Government has obtained its own IPv6 addressing space from RIPE-NCC, and the new Spanish Public Administration Interconnection and Addressing Plan has been approved, there will be a change in the addressing, renumbering the networks according to the new addressing space. However, the current scheme planned for the addressing of the internal subnets (changing the bits from 49 to 64, as described in section 2.1.2.2), will be kept so that the renumbering of the networks can be made easily and with little effort.

German Pilot:

- General:

Currently, all network components are chosen to allow a dual-stack approach. Because most applications are running on a single server, it would be a complete waste of resources to have a separated IPv6 system. To avoid further effort separating or duplicating the systems on the application level, these servers are best running dual-stack.

IPv4 will survive for a longer time hidden behind proxies, in closed networks or backend connections.

Several activities started independently: Getting IPv6 addresses and Internet connectivity, the tests with network and infrastructure components and the creation of test bed islands that were connected with direct tunnels to other islands. Later the connection between IPv6 islands could be rearranged as more parts of the network became available for IPv6 traffic.

- Application backbone infrastructure

The IT infrastructure is based on dual-stack infrastructure for clients and servers. The implementation of applications in the dual-stack test bed took much longer than expected in the beginning due to migration to a new generation of servers and active directory. This test landscape was designed independently of GEN6 activities but many problems showed up during its installation.

An Icinga server is installed to watch all servers and services. This is a prototype for dual-stack monitoring and development and approval of checks.

- Network infrastructure

The network should not be separated between IPv4 and IPv6. Both communications shall be handled on the same interface, using corresponding routing tables. This can be reached best using a dual-stack solution.

For the access to web applications hosted for citizens in the Citkomm data centre a reverse proxy solution is established as application level gateway. This was done do to security considerations and to save public IPv4 addresses. It has the side effect that applications can be presented over IPv6 that are not IPv6 ready natively. Nevertheless this solution requires some detailed testing, because in rare cases even simple web sites may show problems when clients come along with IPv6. The whole field of log file analysis comes into focus during the next months.

As an early step, an external system was set up to monitor the availability of the public services on both protocols. Therefore, this system must be IPv6 respectively dual-stack connected.

- Customer Environment / LAN

For the local networks, dual-stack is also chosen, because it will not be possible to migrate all existing applications. DNS will decide if a connection is made via IPv4 or v6.

Turkish Pilot:

The Turkish pilot consists of critical systems that should support high availability. At the beginning of the project, EGG has been actively working over IPv4. The chosen approach should be the one that would affect the system at the minimum level. Moreover, although there was a test environment, it was not possible to simulate the whole working system there. Consequently it was decided to make the network dual-stack approach which will least affect the currently running system.

Following the requirement analysis in TURKSAT network, it is observed that all L3 network devices have IPv6 support. This leveraged TURKSAT to use dual-stack as the transition approach for the frontend. The only problem had been the software update for load balancers. The update process has been detailed in the upcoming sections. For TURKSAT, no IPv6 only network is needed.

On the other hand, the situation for the connection between TURKSAT and the participating governmental agencies (SGK, PTT and ULAKBIM) is less complex. At the beginning of the project, there was already a direct connection between TURKSAT – SGK and TURKSAT – PTT. Hence, the plan for these connections was to complete the research and development work on a Public Integration Box (PIB) in order to achieve the backend communication over IPv6.

2.2.2 Planned Order of Changes due to Transition

Spanish Pilot:

In the case of the Red SARA network, the changes required by the transition were planned and performed in the following order:

- First, the platform for providing shared services for IPv6 access to e-government web sites was set up. This involves ensuring external IPv6 connectivity with Internet, and the configuration of the network devices, hosts and applications located in Red SARA data centre belonging to this shared services platform, so that the IPv6 to IPv4 translation can be performed properly.
- Second, the backbone of the network, as well as the links connecting the institutions' sites to this backbone, was upgraded to transport IPv6 traffic. This is a task to be carried out by Red SARA telecommunications provider, under the guidance and supervision from MINHAP. Currently, most of the backbone and the links are already IPv6-enabled, with only a few connections to second tier sites, not involved in the pilot, pending.
- Third, the equipment located in the connection areas of the entities linked to Red SARA was turned into dual-stack, so that it can handle both IPv4 and IPv6 traffic. This includes the connection areas of MINETUR and MININT (which DGT, the administrative unit that uses the eITV application belongs to), what will allow the IPv6 only connection between both Ministries required by the eITV application, as it is foreseen in the pilot.
- Finally, since Red SARA provides connectivity through the s-TESTA network to the whole of the Spanish public administrations (by means of the s-TESTA connecting point located in the Remote Access Centre of Red SARA), the equipment responsible for managing the information exchange between Red SARA and s-TESTA was upgraded. This is required to support the cross-border pilots envisaged in WP4. Once this upgraded is completed, MINETUR will also configure its network in order to reach s-TESTA through Red SARA using IPv6.

Additionally, after all those changes were implemented in Red SARA, MINHAP began to work in

the transition of some of its e-government services from the shared service for IPv6 access to the dual stack approach mentioned before.

In the case of MINETUR's network, the changes to be made in large blocks are as follows:

Adaptations by the development team

1. Set up a complete IPv6 development environment.
2. Develop a new component of environment adaptation that allows the access to the service in a transparent way in any of both protocols IPv4 and IPv6. The development will be done using .NET.
3. Modify the access components to the Service through the component of environment adaptation.

Adaptations by the network team

4. Define and install network devices for IPv6 access.
5. Define security policies for the IPv6 network perimeter.
6. Configure DNS.
7. Install and configure devices for high availability

Systems adaptation

8. Adapt end systems to IPv6.

German Pilot:

- General:

The planned order of changes for the German pilot had been as follows:

The pilot touches different networking areas. These areas may have different priorities. These areas are planned and migrated independently in the first phase of the pilot. After finalizing the activities in one segment, it can be connected with other areas already finished. Therefore, the

transition is most often done in a button-up fashion, i.e. migrating the layer-2 and layer-3 devices first, then end systems and servers, and last but not least the active applications.

When the network infrastructure is IPv6-enabled and WAN tunnels can connect IPv6 networks then the test beds get connected in a production-like manner. When test clients can work with test servers over IPv6 (or dual-stack) then in a next phase production systems can be migrated. This refers to the pilot customer LAN as well as to production servers.

The different segment areas for the pilot are:

- Internet connection
- WAN gateways and internal networking
- DMZ servers
- Backbone servers with many different applications
- Local network (customer and Citkomm)

The first phase is focused on the Internet connection, the WAN gateways and first web servers as prototypes for many DMZ systems. In Q4/2012, the work on all further segments started in parallel.

- Application backbone infrastructure

As an example for the steps of the transition, the setup of the Citkomm network for application testing is described in detail. This may be used as a practical reference:

The basic idea for testing and migrating production applications has been to have a separated network that should be connected to the Citkomm world by a dedicated router. Therefore, the first steps could be performed without the danger of influences on the existing production systems. When these new systems are tested and known as working, the segment should be connected to the meanwhile available IPv6 infrastructure that has been built by another team.

This test-network named "BRUNNENREICH" is a so-called backbone subnet purely for testing purposes. It contains several servers that make up a basic infrastructure (DNS, DHCP, and Active Directory for user management) and others that provide the applications. As long as no connectivity to other network segments is available, some clients are planted into this segment. Therefore, during the first levels of the setup no influence on other systems has to be worried about. This idea turned out as a good one during the installations in the test bed.

This subnet is fully virtualized on a VMware hypervisor. So provisioning of new systems is easy as long as the resources CPU, RAM and Storage are available. The next sections explain the workflow design. At first, the virtual environment has to be prepared. Citkomm uses a VMware ESXi 5.1 hypervisor. Network addresses for IPv4 and IPv6 must be chosen.

In the next step the first virtual machine is installed which is the router for the subnet. The typical Citkomm router it is a software appliance based on Ubuntu Linux with Long-Term-Support (LTS). It has three interfaces in this configuration. On the one logical side, there are two connections to the backbone rings that give connectivity to other network segments and towards the Internet or tunnel terminals, and on the other side there is a connection to the application server subnet. Routing, a firewall and a router advertisement daemon have to be installed and configured on this router, too. As the system represents standard technologies (except IPv6), it can be used to provide the test servers with network connectivity easily. This is useful for patch installations and to have access to the file servers where common tools are found. This saves a lot of time-consuming copying of ISO images. In the third step, the virtual machines for infrastructure and application servers are installed. They run different operating systems and get static IPv4 and IPv6 addresses. See the following list for more information:

Components	OS Version
Router	Ubuntu 12.04 LTS
ADDS (Active Directory, DNS) & DHCP	Windows Server 2008 R2
Java Application Server and Deployment System for Glassfish (as Java Application Server)	Ubuntu 12.04 LTS
DB (MySQL)	Ubuntu 12.04 LTS
DB (MS SQL Server)	Windows Server 2008 R2
DB (Oracle)	SLES 11.3
WEB	Ubuntu 12.04 LTS SLES 11.3 Windows Server 2008 R2

Windows Terminal Server	Windows Server 2008 R2
Fileserver	Windows Server 2008 R2
Other Application Server	Windows Server 2012

Table 6 – German Pilot: Table of Systems in the “BRUNNENREICH” Domain

- Network infrastructure

Citkomm’s own routing appliance iWAN, which is the fundament of the Citkomm network, can be installed as a virtual machine. Based on Ubuntu Linux 12.04 LTS it can be expected that IPv6 only has to be enabled. OpenVPN as core application shall support IPv6 inside the tunnel out of the box. Other components like radvd can be installed from the standard repositories. Most applications (DNS, Proxy ...) only need additional entries in the configuration files to run on IPv6 in addition.

- Customer Environment / LAN

The operation of the basic components for a client network should be proven in the basic cell of the backbone network. There, the basic components for a LAN are installed and tested. Due to progress in the network area, connections to the application servers are now available. This will also speed up the testing of the LAN environment.

Turkish Pilot:

The Turkish pilot has two main areas of activity for the transition. First, TURKSAT listed the requirements for the EGG frontend to be made IPv6-enabled. For this purpose, L3 devices in the TURKSAT network have been investigated. Fortunately, it was observed that all devices in the TURKSAT network support a dual-stack approach except the operating system of load balancers that have been deployed as the gateway for the web server farm of EGG. Hence, the first step for the transition was to update the operating system of load balancers. No hardware upgrades were needed in the TURKSAT network. Following the completion of the operating system update of load balancers, layer three network devices, firewalls and load balancers have been configured respectively to work as dual-stack.

The second area of the activity for the Turkish pilot is the IPv6 support of the EGG backend. This includes the connection between TURKSAT and the participating governmental agencies. There

exists a direct connection between TURKSAT – SGK and TURKSAT – PTT. Communication through this connection has been achieved by deploying the Public Integration Boxes (PIBs) at the end points. PIB has been developed through the project. It provides VPN connection over IPv6. ULAKBIM has its own IPv6 infrastructure since 2003. Hence the connection between TURKSAT and ULAKBIM is planned to be achieved using IPsec over the public IPv6 network.

To summarize, the Turkish pilot has been divided in two parts namely: EGG frontend and EGG backend. Firstly EGG frontend infrastructure has been made IPv6-enabled from outside to inside. After a successful completion of the EGG frontend's IPv6 support, the EGG backend (connection between TURKSAT and participating governmental agencies) has been made IPv6-enabled.

2.2.3 Successfully Migrated Components

Spanish Pilot:

Two versions of the shared service platform for providing IPv6 connectivity to e-government Web Portals have been implemented.

In the initial solution, enabling IPv6 access was achieved by means of a Reverse Proxy (IPv6 clients connect to this proxy and the proxy acts as a gateway to IPv4 servers). In cases where the use of a Proxy is not possible due to the need of an electronic certificate validation, NAT64 was used, mapping the IPv6 addresses requested by the client application to the IPv4 addresses. In this solution, Squid is used as Reverse Proxy (more details in section 5.2), with the connection being split into two sections, as it is shown in the figure:

- In the first case, IPv6 traffic goes from the client to the Reverse Proxy.
- In the second one, IPv4 traffic goes from the Reverse Proxy to the web server to obtain the page demanded from the client.

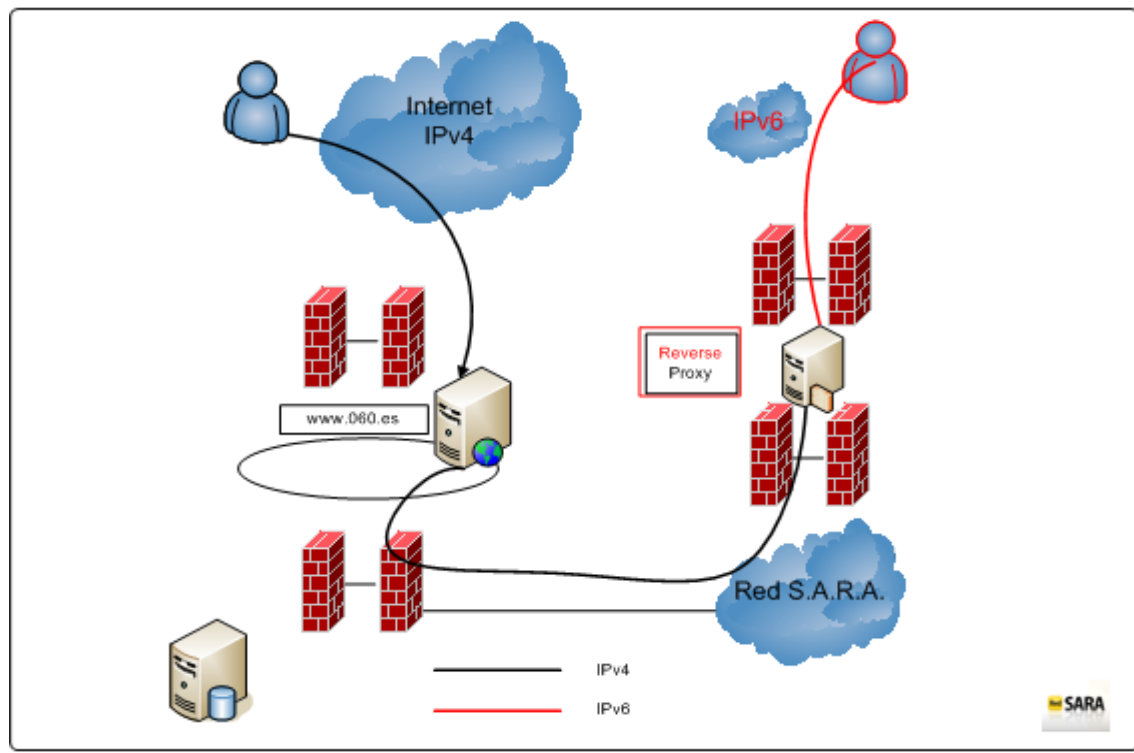


Figure 5 – Spanish Pilot: Reverse Proxy Approach for IPv6 Enablement

In the current solution, not only services requiring user's digital certificate validation are deployed using NAT64, but also all the services are implemented via SSL. Since it has been found that the reverse proxy approach created some difficulties when using SSL connections, due to the need of installing the original server certificate of the end service in the reverse proxy, the NAT64 approach, which does not require duplicating the certificate in an external server, has been considered more appropriate when using SSL.

Therefore, in the current configuration, http connections go through the proxy server, and https connections go through NAT64.

Using this platform, several Web Portals from the MINHAP have been made IPv6-enabled so far:

- e-government Portal: www.administracionelectronica.gob.es
- e-government observatory: dataobsae.administracionelectronica.gob.es
- Forge of the Technology Transfer Centre: forja-ctt.administracionelectronica.gob.es
- Common Electronic Registry for the Spanish National Administration:
<https://rec.redsara.es>
- Portal to communicate address changes to public administrations:

<http://cambiodomicilio.redsara.es>

- Electronic Signature Validation Service “Valide”: <http://valide.redsara.es>
- Preproduction environment of the Spanish PEPS used in STORK platform: <http://prespanishpeps.redsara.es>
- Production environment of the Spanish PEPS: <https://spanishpeps.redsara.es/>

As well as some portals from the Ministry of Justice:

- Web portal of the ministry: <http://www.mjusticia.gob.es>
- Electronic headquarters of the ministry (for access to electronic administrative procedures): <https://sede.mjusticia.gob.es>
- Map of Civil War graves: <http://mapadefosas.mjusticia.es>
- Publications portal: <http://publicaciones.mjusticia.es>
- Access to the corporate mail: <https://correoweb.mjusticia.es/exchange>

Additionally, an inventory of IPv6 capabilities of elements connecting to the SARA network has been performed. There are three types of connection areas, depending on the entity in whose network they are deployed Ministry Offices, Autonomous Communities (regions) and Singular Institutions. The elements in the connection area are basically the same, but the concrete equipment depends on the type of connection area (e.g., in the Ministries Juniper ex3200-24t and Cisco C3825 routers are used, whereas in the Autonomous Communities the routers are Cisco C385 and C2851).

Regarding these routers, all the connection areas of the Ministries have been configured to support IPv6. To implement the new protocol it has not been necessary to change in any form the VPLS infrastructure. New pseudo interfaces for IPv6 have been configured on the routers (WAN and LAN networks) but over the same VLAN at VPLS level. Thus, it is possible now to process IPv6 native traffic between these connection areas through the VPLS backbone of Red SARA.

Additionally, MINETUR is adapting the eITV service to IPv6 as defined in the project. This has two distinct parts: the IPv6 infrastructure and the modification, to support IPv6, of the application that makes use of that infrastructure. To achieve this goal, both development and systems departments of MINETUR are involved, working on the basis of a coordinate effort.

Regarding the eITV infrastructure, the preproduction environment already deployed and

connected to Red SARA and the Internet has been tested, verifying successful IPv6 connectivity from Red SARA and from the Internet.

German Pilot:

- General:

As one of the first visible steps, the Internet connection of Citkomm was enabled to route IPv6. Afterwards the Citkomm website www.citkomm.de was made available over IPv6 using a reverse proxy, based on the open source “nginx”². The Citkomm web service went online in time for the IPv6 launch day in June 2012.

Afterwards one working group started implementing and testing the enabling of the very common OpenVPN tunnel connection for IPv6. Their work schedule also included all the essential parts of the internal network infrastructure like routing protocols, DNS and firewalling. The corresponding paragraph below contains more details.

Another team started dealing with LAN and application server structures. BRUNNENSTADT and BRUNNENREICH were built as prototypical test networks. For the local network, all central servers were implemented using dual-stack from the beginning on. The tests did not show any significant problems regarding the basic network services so far.

Therefore, in the last two months talks with customers of Citkomm started to find a volunteer for enabling a municipality’s LAN for IPv6. Preparations are on the way and during the first months of 2014, the first workstations in the field will connect to IPv6 servers.

- Application backbone infrastructure

When the installation of the first systems in BRUNNENREICH started this island was not yet connected to an IPv6 infrastructure. However, the hosts linked together on a virtual switch would be able to exchange IPv6 packages among themselves. Therefore, Citkomm started to install new separate domain controllers. To keep the new domain separated from the productive one, a router was installed between the application test area and the backbone network. Two Windows Server 2008 R2 systems represent the heart of the test bed. Their network interface cards work

²Citkomm uses reverse proxy systems as strategic components for load balancing, caching and accounting and for saving resources in IPv4.

in dual-stack mode. On both servers, the “Active Directory Domain System” service has been installed, so they act as domain controllers of the application test bed. The DNS service on these domain servers is used to relate a unique name to a host in the local network. This is done by an AAAA-record, which relates a name to an IPv6-Address, in addition to A-records and IPv4 addresses. Due to the length of an IPv6 address, it is much easier to address a server by its name instead of a hexadecimal address. On the other hand, the use of exactly the intended protocol requires a little more effort. Surely, the use of IPv6 is forced when a client gets no IPv4 address at all. The use of additional DNS entries, e.g. v6.my.server with an according AAAA record, also makes it possible to select one protocol by intention. However, this is not intended for configuring applications. Practical experiences will show what helps best when troubleshooting network problems in a dual-stack network effectively.

Reverse entries in DNS called PTR records allow the assignment of names to addresses. The opinions about the need of such entries vary here.

Furthermore, a DHCP server is installed on one of the domain controllers to allocate IPv4 and IPv6 addresses for clients in the application subnet. Normally there would not be any client in an application server subnet, but as already stated, the application network was not connected to an IPv6 network in its beginning. Therefore, the cheap and fast solution was to have some clients locally.

The Windows DHCP server defines IPv6 address pools in a different way than IPv4 addresses. In fact, that IPv4 address space is defined by setting a start and an end IP address. The address space of an IPv6 pool is allocated the other way. At least, if the address concept is as Citkomm’s, see chapter 2.1.2.2. To set up such a limited IPv6 pool (in relation to the available 2^{64} host addresses in the network segment) all address spaces which should not been used for dynamic assignment have to be defined as “do not use” to the DHCP server. This will be done by setting a start and end address, too.

To get a working IPv6 client using stateful DHCP another component is needed: the radvd distributes information about the subnet mask and the default gateway to the DHCP clients.

To use statically assigned but dynamically configured addresses, newer standards for IPv6 autoconfiguration do not rely on the MAC address for building the unique interface identifier of a NIC, but use two parameters called DHCP Unique Identifier (DUID) and Interface Association Identifier (IAID). These have to be grabbed from the client by reading them manually or by assigning a pool address first and watching the protocols on the DHCP server attentively.

When the first systems had received their addresses, first applications could be tested: RDP can be used to receive a terminal service session from a server on a client, and SSH connections can be tested to access typical Linux servers. All this worked unspectacular.

Next, an application system that consists of several components has been installed. One key component is the single-sign-on application “CAAS”, developed at Citkomm. For testing purposes two Ubuntu servers were built up, one running a glassfish environment for the application itself and another with a MySQL database. The latter will take more databases when the tests continue. The communication between application server and database runs fine on IPv6. This application landscape is currently extended to host a complete production like setup for applications called “ADVIS”, “WinBIAS” and “Mach”.

- Network infrastructure

Before making available the Citkomm website on IPv6, the WAN gateway components had been enabled for IPv6 connectivity. The most important gateways used in Citkomm networks are the iWAN gateways. These appliances are based on Linux open source components, namely the Ubuntu LTS distribution. They implement several services, apart from the VPN connectivity over different IP transport platforms like DSL lines, Internet access over cable TV infrastructure, private radio links or MPLS access networks. The ability for IPv6 has been successfully implemented for the tunnel interface and the in-tunnel traffic first because of the missing IPv6 infrastructure for the outer connection. At this point, the pilot gateway implementation is able to support full network connectivity for IPv4 and IPv6. To check the functionality, one gateway was located in the IPv6 test bed of Fraunhofer FOKUS in Berlin. While in the beginning and for the first tests only connected to a test island at the Citkomm site named “BRUNNENSTADT” this gateway now keeps a permanent connection to a central gateway at Citkomm. The connection to BRUNNENSTADT represents now a cross connection as is quite common in Citkomm’s network.

As far as Citkomm’s Internet connection is concerned the transition to an own autonomous system (AS) has passed the halfway milestone but is still in progress. The final topology for the components to represent a high available infrastructure for the connection to the autonomous system uplinks had first been planned and tested for IPv4 only. After successful implementation and approval in a test area, the production systems were enabled with IPv6, too. They are operating in dual-stack mode since then. The test series performed for the legacy Internet protocol had been successful repeated for IPv6 connections. The validity of this concept could be confirmed finally as of Q4/2012. An external validation of the whole concept was performed.

In addition, of course the firewalls had to be made aware of IPv6 traffic. A new, upgraded version of the fwbuilder tool is used on a new management system. Some issues with this will be mentioned in the next chapter.

After enabling the central Internet access infrastructure successfully with IPv6, the basic infrastructure services DNS and e-mail have been set up in dual-stack. Therefore, these services are available to the public via IPv6 since spring 2013.

At the same time, an external monitoring system went online. This system is located at a hosting services providing company's data centre and has a look from outside at the Citkomm network. It is used to monitor the availability of the typical public available services like DNS, SMTP gateway and different websites and gateways. It is built as an Icinga server with adapted tests to be able to check services or systems via either IPv4 or IPv6 intentionally.

Host ▲▼	Service ▲▼	Status ▲▼	Last Check ▲▼	Duration ▲▼	Attempt ▲▼	Status Information
AS41052	AS_Status_v4	OK	2013-11-06 12:03:27	6d 20h 54m 58s	1/4	HTTP OK: HTTP/1.1 200 OK - 30989 bytes in 0.804 second response time
	AS_Status_v6	OK	2013-11-06 11:59:55	1d 20h 18m 31s	1/4	HTTP OK: HTTP/1.1 200 OK - 30989 bytes in 0.825 second response time
ENNS.CITKOMM.NET	DIG4-PTR	OK	2013-11-06 12:16:36	41d 23h 29m 8s	1/4	DNS OK - 0.018 seconds response time (69.128.216.91 in-addr.arpa. 86400 IN PTR mx2.kdvz.net.)
	DIG6-A.A.A.A.	OK	2013-11-06 12:14:03	8d 18h 54m 27s	1/4	DNS OK - 0.025 seconds response time (www.citkomm.de. 30 IN A.A.A.A. 2a02:100e:befc:8cd1:0:203:11:1)
	DIG6-PTR	OK	2013-11-06 12:16:17	12d 6h 52m 11s	1/4	DNS OK - 0.021 seconds response time (1.0.0.0.7.0.0.8.2.1.0.0.0.0.2.d.c.4.c.f.e.b.e.0.0.1.2.0.a.2.ip6.arpa. 86400 IN PTR smtp2.kdvz.net.)
	DNS4	OK	2013-11-06 12:18:03	21d 14h 50m 23s	1/4	DNS OK - 0.019 seconds response time. www.citkomm.de returns 91.216.128.221,91.216.128.231
	DNS6	OK	2013-11-06 12:16:37	14d 6h 56m 48s	1/4	DNS OK - 0.018 seconds response time. www.citkomm.de returns 91.216.128.221,91.216.128.231
EVENTSONLINE.KDVZ.DE	HTTP4	OK	2013-11-06 12:15:43	3d 21h 17m 44s	1/4	HTTP OK: HTTP/1.1 200 OK - 2386 bytes in 0.090 second response time
MX1.KDVZ.NET	smtp4	OK	2013-11-06 12:18:07	42d 6h 3m 31s	1/4	SMTP OK - 0.050 sec. response time
MX2.KDVZ.NET	smtp4	OK	2013-11-06 12:15:32	40d 20h 51m 42s	1/4	SMTP OK - 0.051 sec. response time
	smtp6	OK	2013-11-06 12:13:46	21d 14h 16m 10s	1/4	SMTP OK - 0.061 sec. response time
MYCITKOMM.KDVZ.DE	HTTPS4	OK	2013-11-06 12:16:07	0d 6h 27m 18s	1/4	HTTP OK: HTTP/1.1 200 OK - 7102 bytes in 0.263 second response time
NS2.HANS.HOSTEUROPE.DE	DIG4-A.A.A.A.	OK	2013-11-06 12:13:48	38d 6h 51m 46s	1/4	DNS OK - 0.014 seconds response time (www.citkomm.de. 30 IN A.A.A.A. 2a02:100e:befc:8cd1:0:203:11:1)
	DNS4	OK	2013-11-06 12:15:45	39d 13h 23m 23s	1/4	DNS OK - 0.015 seconds response time. www.citkomm.de returns 91.216.128.221,91.216.128.231
NS8.KDVZ.NET	DIG4-PTR	OK	2013-11-06 12:16:58	12d 6h 51m 27s	1/4	DNS OK - 0.019 seconds response time (69.128.216.91 in-addr.arpa. 86400 IN PTR mx2.kdvz.net.)
	DIG4-PTR6	OK	2013-11-06 12:14:34	95d 12h 52m 27s	1/4	DNS OK - 0.017 seconds response time (1.0.0.0.7.0.0.8.2.1.0.0.0.0.2.d.c.4.c.f.e.b.e.0.0.1.2.0.a.2.ip6.arpa. 86400 IN PTR smtp2.kdvz.net.)
WAHLEN.CITKOMM.DE	Startseite_Jserlohn_HTTP4	OK	2013-11-06 12:17:56	2d 11h 45m 29s	1/4	HTTP OK: HTTP/1.1 200 OK - 1710 bytes in 0.040 second response time
	Startseite_HTTP4	OK	2013-11-06 12:14:45	3d 21h 18m 40s	1/4	HTTP OK: HTTP/1.1 200 OK - 1710 bytes in 0.048 second response time
WEB1.WAHLEN.CITKOMM.DE	HTTP4	OK	2013-11-06 12:15:34	47d 22h 42m 5s	1/4	HTTP OK: HTTP/1.1 200 OK - 1709 bytes in 0.024 second response time
WEB2.WAHLEN.CITKOMM.DE	HTTP4	OK	2013-11-06 12:15:45	47d 22h 42m 5s	1/4	HTTP OK: HTTP/1.1 200 OK - 1710 bytes in 0.025 second response time
WEBOPAC.KDVZ.DE	WebOPAC_Amsberg	OK	2013-11-06 12:13:32	0d 7h 4m 53s	1/4	HTTP OK: HTTP/1.1 200 OK - 2911 bytes in 0.872 second response time
	WebOPAC_Balve	OK	2013-11-06 12:14:03	0d 8h 9m 22s	1/4	HTTP OK: HTTP/1.1 200 OK - 2896 bytes in 0.216 second response time
	WebOPAC_Burscheid	OK	2013-11-06 12:16:47	0d 7h 1m 38s	1/4	HTTP OK: HTTP/1.1 200 OK - 2816 bytes in 0.215 second response time
	WebOPAC_Kierspe	OK	2013-11-06 12:17:36	0d 7h 50m 49s	1/4	HTTP OK: HTTP/1.1 200 OK - 2906 bytes in 0.233 second response time
	WebOPAC_Leichlingen	OK	2013-11-06 12:13:14	0d 8h 0m 11s	1/4	HTTP OK: HTTP/1.1 200 OK - 2926 bytes in 0.267 second response time

Figure 6 – Screenshot from Citkomm-external Monitoring System

The external connection to the German government backbone “Deutschland Online Infrastruktur – DOI” was finally enabled for IPv6 in February of 2013. At this moment the interface is – deviating from the general transition of Citkomm – not generated as dual-stack, but as two separated, tagged VLANs. This is due to restrictions of the crypto gateway of the DOI, which offers the

customer site interface and does not support IPv6 in dual-stack until mid-2014. A real dual-stack interface shall be provided with the next release of the firmware in first half of 2014.

The final setup was successful only after several problems and more or less unsuccessful tries, resulting from problems with the components of the DOI network. Details are outlined in chapter 2.2.4.3.

- Customer Environment / LAN

A test network similar to a typical customer's network is established. This test network is called BRUNNENSTADT and aims to act like the administration network of a small community. Like such small municipalities, it is connected over DSL, an iWAN, and an OpenVPN connection to the Citkomm data centre and contains typical client and server systems. For some weeks, an IPv6-enabled DSL connection can now be used for tests.

The test bed at FOKUS looks more like a larger administration network. The connection from there to Citkomm is also established via "Soft-iWAN" (virtual iWAN Appliance) and OpenVPN. The Internet connection is dual-stacked. Several systems allow for tests with different client systems. A connection via tunnel and the IPv6-enabled Citkomm network have made possible tests with application servers in BRUNNENREICH for a few weeks.

When only the first experimental tunnel between the FOKUS testbed and BRUNNENSTADT was established, the first connections between clients and servers via ssh and RDP Clients were used. Tests with a simple web application revealed already columns in a session table that had been too small to hold IPv6 addresses. This could be fixed very quickly. In addition, after setting up mail servers in both networks and putting according MX records into DNS successful mail transfer over IPv6 could be filed.

Turkish Pilot:

On the TURKSAT side of the project, load balancers, which have a non-IPv6-enabled OS, have been updated. This enabled to continue working on IPv6 support of EGG frontend. After updating load balancers' operating systems, TURKSAT started working to deploy IPv6 in its own network. For this purpose, TURKSAT configured IPv6 addresses and routing protocols (BGP, OSPFv3 and static routes) on network devices starting from outer-most devices. This work continued with the configuration of inner network devices, which include firewalls, load balancers and servers (web servers, monitoring appliances). In addition, clients in TURKSAT have been configured as dual-stack. These components have been successfully moved to IPv6 within the first year of the

project. Because of this work, the EGG frontend, which is the Web portal (www.turkiye.gov.tr), has been made IPv6-enabled. Hence, currently EGG frontend is working dual-stack.

By the second year of the project, project staff started working on the IPv6 support of EGG backend. This work included enabling IPv6 communication of TURKSAT and the participating governmental agencies. This work has been achieved by deploying Public Integration Boxes, which establishes VPN connections over IPv6, at the end points of the communication. These boxes have been successfully deployed at the participating agencies (SGK and PTT).

2.2.4 Enabling IPv6 in Components

2.2.4.1 Practical Tests

Spanish Pilot:

As it has been mentioned before, at this moment the connection areas of the Ministries are IPv6 capable. To achieve this goal, tests were conducted in three ways:

- Traffic processing through VPNs
- HTTP traffic between two connection areas
- DNS IPv6 capabilities

Traffic processing through VPNs

All the traffic processed through the VPLS backbone of Red SARA is encrypted using the IPsec capabilities offered by the edge firewalls located in the connection areas. This is true for IPv4 traffic and must be configured in the same manner for IPv6 traffic. To do so, new tunnels have been defined on the devices included in the test scenario and IPv6 native traffic has been injected between these connection areas. The result was successful and, as expected, IPv6 tunnel behaviour was so similar to that of IPv4. At this moment, native IPv6 traffic can be processed between Ministries sites and this traffic is encrypted on the edge firewalls. As IPsec connections are defined between networks (tunnel mode), in fact the only IPv6 traffic that can be seen in the backbone is the ESP traffic between edge firewalls.

HTTP traffic between two connection areas

More or less half of the traffic processed in Red SARA is HTTP, so it was considered, as the best

functionality test, to install an HTTP server in one connection area and try to navigate from another. The chosen connection area to host the HTTP server was the one owned by the Ministry of Industry Energy and Tourism (MINETUR). Navigation was performed from several locations, in different Ministries, using native IPv6. No differences were found while using IPv6 and user experience was similar (speed, latency ...).

DNS IPv6 capabilities

To implement IPv6 services infrastructure one key point is DNS. It is necessary to define new DNS entries for direct and reverse resolution using IPv6 addresses (AAAA records for direct resolution and ip6.arpa zones for reverse resolution). The server chosen was the one located at the Central Services connection area (where the e-government shared services provided by Red SARA are hosted) and the new entries were added at the zones involved in the test. This server was configured in dual-stack, and it had no problems in answering queries related to IPv6 services neither when connecting through IPv4 nor connecting through IPv6.

In the case of MINETUR eITV service, access tests via IPv6 with a private address range have been made in the MINETUR laboratory.

A first line of perimeter security has been designed. It defines the access to the DMZ service and it will be delimited by two Cisco 2960S, level 2, systems.

A /64 prefix will be used. The IPs to be used are those obtained automatically when auto-configuring the equipment. Once the IP is obtained, it will be configured manually on the equipment.

This process will be the same for the HSRP virtual IP's required for the Cisco equipment.

Three IPs will be used for each HSRP, two physical and one virtual.

In the perimeter security equipment, Palo Alto PA-5050, the same procedure will be used to obtain the IPs and the high availability system, allocating three IPv6 addresses, two physical and one virtual.

The configuration of the load balancing equipment, F5 3900, will use the same mechanism as in the previous equipment, with three IPs (two physical and one virtual).

Two DNS servers will be used, dns.ipv6.es and dns2.ipv6.es and they are using the same procedure to obtain their IP addresses.

This configuration will be the same as in the production environment and is represented in the following figure.

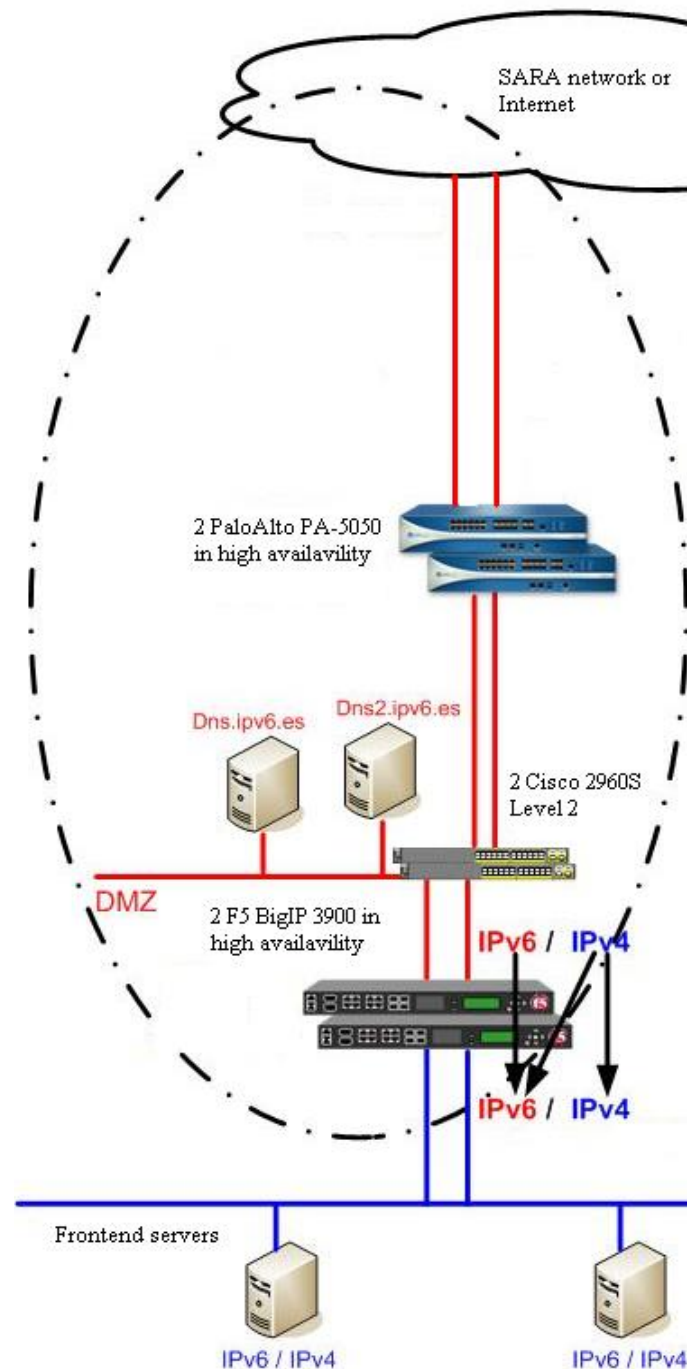


Figure 7 – Spanish Pilot: MINETUR's Network Configuration

German Pilot:

- General:

According to the progress in the pilot different components were involved in the IPv6 enabling process and had to proof their IPv6 capabilities. On the network level the basic functionality does not cause harms but when it comes to real applications or more complex setups the one or other issue has to be solved.

Typical test commands for low-level operations are

`ipconfig / ifconfig / ip a` (to check the validity of the local configuration)

`Ping / ping6` and `tracert / traceroute / traceroute6` with options to select sender addresses or interfaces to check the connections to targets

`Route / ip r / ip -6 r` to check the routing tables

- Application backbone infrastructure

Citkomm and Fraunhofer have built up three IPv6 test areas with more than 30 virtual servers and clients. Recent operating systems like Windows Server 2008 R2, Windows7, Ubuntu LTS 12.04 or SLES11 SP3 work out of the box with IPv6. Some minor things want to have paid attention, see next chapter. Also basic services DHCP, DNS and Mail work. Web services also cause not so much trouble. If there are issues then they are related to the applications that are not aware of the longer addresses with another syntax.

- Network infrastructure

The core interconnect network at Citkomm uses Linux based routers as basic systems. On the perimeter, some Cisco systems are in use. From these the Internet uplink routers are in the focus of the project as they provide the connectivity to the world and interact via OSPF routing protocol with the interior Linux routers. This routing interaction between Cisco and Linux systems works as well as the OSPF routing information exchange with the Quagga package on Linux.

For the wide area network, Citkomm uses the self-developed appliance iWAN. All tests are performed with the current iWAN generation based on Ubuntu LTS 12.04. The OpenVPN implementation supports IPv6 also on under laying network as also inside the tunnel. All communications could be tested successful with IPv6 and combinations of IPv4 and IPv6. The

scripts that generate routing information dynamically when a tunnel comes up were adapted to take care of IPv6 routes. This is required as the Citkonn infrastructure includes redundant tunnel terminal systems and so there must be taken care of correct routing info regardless if the iWAN at customer's side has chosen the one or the other terminal. Therefore, for this setup the correct established routes had to be checked carefully.

The generation and distribution of firewall rules in an automated way is an action point for the next period, as well as the automated setup of an iWAN system with respect of an IPv6 configuration.

- Customer Environment / LAN

The infrastructure of typical client networks is based on Windows server technology. The setup of address assignment and basic network configuration distribution via stateful DHCP was described before. The correct setup of Windows and Linux clients was verified successfully.

The tested applications are web browsers, mail clients, RDP and Ssh for connections to servers at this moment. As soon as the server systems for native client/server applications are available, they will be tested.

Turkish Pilot:

Practical tests for Turkish pilot may be investigated under two main headlines, which are tests for EGG frontend and tests for EGG backend. For the EGG frontend (Web portal), TURKSAT had already built a test environment. The test environment used the same configuration as the production environment and updated respectively. A new feature is first tested in this test environment and if it succeeds, it is ported to the production environment. Although every new update has been tested, deployment of the feature in the production environment may give different performance results as EGG Web portal serving over 15 million registered citizens.

In addition, performance and conformance tests had been run for the EGG frontend over IPv6 in the test environment. These tests included access and penetration tests over IPv6. After completing the tests successfully, the new configuration had been moved to the production environment. Load balancer tests were critical for the Turkish pilot.

As the second headline, connection and performance tests (including throughput, jitter etc.) were made while setting up the connections between TURKSAT and the participating governmental institutions (SGK and PTT).

2.2.4.2 Security Considerations

These considerations are taken from the view of the three pilots and their special needs with respect to transition, operating environment and implementation. Common security aspects for introducing IPv6 can be found in section 2.4.

Spanish Pilot:

In the case of Red SARA, the main security considerations have been:

- Implementing the changes in the firewall rules to deal with IPv6
- Configuring the IPsec tunnels that link the connection areas so that the traffic that crosses the network always travels encrypted

These considerations are explained in more detail in the following sections.

In the case of MINETUR, the main security considerations have also been related to the firewall rules, which have been changed to allow only http and https traffic to the IPv6 DMZ hosting the eITV service.

German Pilot:

- General:

Citkomm has an established security policy for its productive environment. This was designed in an IPv4 world but can and must be extended to the IPv6-enabled network. As a dual-stack approach was chosen, the network paths for the permitted traffic are the same for both protocols. To be able to use the known graphical interface for defining firewall rules a new version of fwbuilder had to be set up and was installed and a new base system consequently. Deeper investigations of specific IPv6 issues are scheduled.

- Application backbone infrastructure

The application servers themselves are treated as located in a safe area. Nevertheless, the router to the application segment has firewall rules on it that restrict the access to the servers.

- Network infrastructure

Of course, for the network infrastructure the general rules are applied. In addition, the firewalls

and application layer gateways (proxies and reverse proxies) have to be watched.

- Customer Environment / LAN

These networks are protected by iWAN systems. The basic security considerations are the same as for the network infrastructure above. In addition, a customer interface will have to be updated. This allows for instance the customer's administrators to add exception rules to the proxy rule sets. This application has to be extended to allow the handling of client IPv6 addresses.

Turkish Pilot:

The Turkish pilot consists of critical systems that hold citizenship information. Hence, security policies were already prepared for IPv4 before the project. These policies include access control rules (firewall rules, access control list rules etc.) and performance criteria in order to protect the whole system from DDoS like attacks. These policies have been successfully adapted to IPv6 as well and the system has been made dual-stack. After IPv6 transition, security tests are performed by an external information security company in order to check confidentiality, integrity and availability of the whole system.

For the EGG backend, which consists of the connection between TURKSAT and the participating governmental agencies, there exists a direct connection. This connection has been made over IPsec VPN so that this communication has been secured by encryption.

2.2.4.3 Lessons Learned (Experiences and Pitfalls)

Spanish Pilot:

As it was described, one of the main issues has been determining the actual compatibility of the existing equipment and services with IPv6. In the case of Red SARA connection areas, it has been found that not all existing services support IPv6. Though some of them can be easily upgraded, there are others whose updating would require considerable investments. This has led to clearly differentiate between those services that are essential to provide IPv6 transport capabilities and those that support network operation, focusing on the first ones. Therefore, it has been decided not to act on those support services that are not compatible with IPv6 and cannot be made compatible easily, such as the High Availability service, leaving them out of the scope of the pilot.

After the practical tests, the main lesson learnt is that the main concepts of IPv6 are not so different from the concepts used in IPv4: The main concepts of routing, firewalling, tunnels, etc.

are similar to IPv4, though special care needs to be taken not to make mistakes due to the new addressing scheme. Not caring enough for details can also become a problem when it comes to handling DHCPv6 traffic, the new methods for IPv6 autoconfiguration, and correct network protection with firewalls in the absence of network address translation with IPv6. Once compatibility of the different elements has been ensured, the way to implement security, services and so on is similar to that of IPv4.

German Pilot:

- General

During the tests and the implementation of IPv6 in the Citkomm infrastructure, additional technical challenges surfaced. Until now, solutions or workarounds could be found and established so that there are no showstoppers for the use of IPv6. Nevertheless, it is sure that in the depth of the real applications, there will be some flaws and pitfalls that will prevent the use of the new protocol in the one or other way. However, we expect to be able to find a way to provide access to these legacy applications via IPv6. The last resort seems the use of terminal services in which case the backend communication is of no interest from the viewpoint of the client.

Windows systems in a stateful DHCP environment require some special settings. For static configurations, some settings of the IPv6 protocol on the interface card have to be changed by netshell commands:

```
netsh interface ipv6 set interface "Interfacename" routerdiscovery=disabled
netsh interface ipv6 set interface "Interfacename" managedaddress=disabled
netsh interface ipv6 set interface "Interfacename" otherstateful=disabled
```

This prevents additional autoconfiguration of the interfaces and obtaining dhcp leases.

Clients get an IPv6 address by a DHCPv6 server (stateful DHCP). A route to the local /64 network is announced from the default gateway via router advertisement.

One more word regarding the Windows DHCP server from 2008 R2 server: In Citkomm's addressing schema only a subset of the address space of the /64 network segment is intended for use by typical DHCP clients. So the first word of the host part is fixed. In a way different to the IPv4 scope, you have to exclude the ranges that you do not want to use for dynamic IPv6 addresses from the whole network segment address range. At IPv4, you create the scope by

setting up a start and end address. At IPv6, you create the dynamic scope by setting it up the other way around, i.e. you have to exclude all ranges you do not want to assign.

- Application backbone infrastructure

By installing an application to test some IPv6 transmissions, Citkomm found out that `ip6tables` did not support port redirection. This technique is used in IPv4 to make a non-root running application available on the privileged port 80 (which normally only applications with root permissions can open).

The application to be tested is deployed on the glassfish node server and contains a website with a login. To make the login page reachable on standard ports for access from outside networks the application requires port-redirection from port 80 and 443 to ports above 1024. Using unusual ports would produce the need to add special rules in firewalls and/or proxies for the users of this portal, so the portal operator wants to use standard ports. However, the java application shall not run with root privileges from security reasons. This means, it cannot open ports below 1024 for listening. Using a reverse proxy is one possible solution, but this is a little heavy weight.

Therefore, the *NAT* table of the *iptables* for IPv4 is extended by some rules that exactly perform this port translation. In case of the reachability of the login page over IPv6, `ip6tables` was to add the according redirection rules. As a problem it turned out that `ip6tables` did not support such redirections. Normally redirections are entered in the NAT table, but NAT is generally not supported with IPv6.

Investigating the issue Citkomm found out that the Linux kernel 3.9 should support this feature. However, Citkomm's Linux Ubuntu server uses 12.04 LTS distribution with backport packages. As of September 2013, only kernel 3.8 was available. Hopefully, the backported kernel from the Ubuntu 13.10 release will bring some progress. Otherwise, a fall-back to the proxy solution has to be considered.

A couple of websites hosted at the Citkomm data centre base on typo3 as content management system. The websites were made available for IPv6 access by use of a reverse proxy system. After successful implementation on this way, it was planned to make such servers available natively on IPv6 in a next step. Typo3 gives full IPv6-support just since November 2012. The version containing this is no long-term support version. Because of the strategy of Citkomm to use long-term supported versions as far as possible a new version giving unrestricted IPv6 support will be available in Citkomm productive infrastructure not before middle of 2014.

A minor problem was found in another web application that claimed to be completely independent of IPv4 or IPv6. It turned out that the IP address of the client was stored in a database for session management purposes. Moreover, for the longer IPv6 addresses that table column was too small, which lead to an application error. A small change in the database layout corrected that problem.

- Network infrastructure

One of the very first things that must be available for an IPv6 transition is a provider uplink to the Internet. Why? It may turn out as not so easy to bring a production environment with official addresses to the public Internet.

Because several providers offer IPv6 solutions since years Citkomm assumed that there will be no problem to get IPv6 connectivity on their existing uplinks or at minimum with parallel access products. First requests at the sales departments of the contracted provider confirmed this assumption. Getting deeper it could be seen, that IPv6 connectivity is not always easy available. In case of Citkomm the Internet connection was operated by two providers and still based on an autonomous system. Therefore, the uplinks were “transit” products. For this access, IPv6 was available at no problem from Deutsche Telekom. The second uplink was from a local city carrier, the DOKOM21. The people from DOKOM were willing to cooperate with Citkomm in configuring the network access router. However, IPv6 connectivity through their backbone was not available in 2012. The enabling of this uplink needed at least one more year to be finalized.

For further test Citkomm requested in Q2/2013, a simple Internet access solution (DSL) with IPv6 support at Deutsche Telekom. They announced the support for IPv6 on new installed access in December 2012 so we expected no problems. Surprisingly the sales agent from business sales replied that there is still no business product on IPv6 available. On DSL access there is none. On fixed line it may be possible, but only if he could get us into a running pilot. At this point in time, no regular market offer including IPv6 was available. So it must be checked in detail, if there is a provider that really supports IPv6 on a given solution. We satisfied our requirement in this case finally by ordering a new DSL access using the consumer channel - with a specific product, that is known as supporting IPv6.

There are still problems investigated with ospf6d from the Quagga project. On area border routers routes appeared only in one direction on the other side. This work is in progress.

Just as additional information, here are some notes about the introduction of IPv6 in the German governmental network: In a first plan the German government backbone network “Deutschland

Online Infrastruktur – DOI” should be enabled for IPv6 in Q4/2010. Pilots set up with some governments resulted in several problems. These problems were so massive that even a single “ping” could not be transmitted successful to another site. The problems seemed to have occurred of the crypto gateway used in the DOI. Due to these fundamental problems, the transition was set out for nearly one year. The next pilot in end of 2011 resulted in basic communication. Nevertheless, from the operator site further problems could be identified in the firmware of the crypto gateway. Therefore, a second patch phase had to be introduced. After that the approval for the roll out was given. For a structured roll out, at first the central services of the DOI had to be established with IPv6. At this point problems with the installed firewall at this central site occurred. Due to fixed change processes, the setup of the final firewall fix took further three month. At the end, the first customer location could be set up with IPv6 in Q4/2012. In the next time further problems came up, those were based on a problem in interoperation between the new full IPv6 supporting firmware and the former version on the productive crypto gateways. To get this issue clear the roll out was interrupted another time. Finally it could be seen, that

1. IPv6 implementation should be tested seriously and not only claiming on the point that it is “just another IP protocol in parallel”.
 2. IPv6 implementation in large scaled infrastructures can be a problem simply to the fact, that some details may not be seen in the pre testing. In addition, due to a strict scheduled change timetable in those infrastructures the final successful set up may take several attempts.
- Customer Environment / LAN

There is not so much to mention here in this moment besides the general sayings about Windows systems. With the availability of application servers and more intensive testing from the clients, probably more content will appear here.

Turkish Pilot:

One of the experiences gained through the project and IPv6 research is that one of the reasons for an institution not to be IPv6-enabled may be an ISP that does not have IPv6 support. Another reason is that institutions do not want to modify their already working systems. In Turkish pilot, it is observed that besides the technical issues, one should investigate the administrative and human resource issues in IPv6 transition. In other words, in some situations institutions may need to be convinced about IPv6 transition.

There had been no major IPv6 connectivity problems experienced in the Turkish pilot. Turkish ISP (Turk Telekom) provides native IPv6 connectivity, so by having IPv6-enabled devices, institutions are able to connect to global IPv6 networks preferably using dual-stack.

Open source tools are commonly deployed in institutions in Turkey. A disadvantage has been discovered that open source tools may be problematic in IPv6 support. In other words if you do not own a commercial support, IPv6 support will not be prioritized in code development.

Another issue may be IPv6 misconfiguration of third party servers. There are major issues in the case that your clients have IPv6 support but the destination network has a misconfigured IPv6 web server.

On the other hand, it is observed that network and security appliances may be problematic in terms of IPv6 deployment. There is no clear and common definition of “IPv6-enabled” for network and security appliances. Therefore, institutions that require getting an IPv6-enabled appliance should list their requirements and level of support such as QoS or mobility support.

2.3 Affected Network Components

This chapter takes a deeper, more technical look at certain network elements and servers of an IT infrastructure which are affected by a transition of e-government services from IPv4-only to running IPv4+IPv6 support (from their users’ point of view). These systems include network-level devices such as routers, plus auxiliary services like electronic mail and DNS, which are in direct or indirect use of the migrated e-government services.

2.3.1 Routers and Routing

Spanish Pilot:

Regarding Red SARA, at present:

- All Internet routers are capable to route IPv6 traffic. This implies that both the two routers located in the main Data Centre (Cisco 3825) and the two routers located in the back-up data centre (Cisco 3845 and Cisco 2851), are already configured to do so.
- In addition, the routers involved in the backbone infrastructure (located in the connection areas) are IPv6 capable as it was mentioned before. So far, only those routers involved in the connection between Ministries have been configured to support IPv6, but the extension of IPv6 to the rest of connected bodies (Autonomous Communities and Singular

Entities), not involved in the pilot, should not be a problem, based on the experience acquired with the Ministries.

- Regarding switches, they are Switch Cisco Catalyst 3750E and 3750G, and they have no specific requirements for IPv6 management, since the use of IPv6 for managing devices is out of the intended scope of the Spanish pilot, as the network will keep dual-stack capabilities and management can still be achieved by means of IPv4. On other hand, switches in connection areas have Cisco IOS c3750e-universalk9-mz.122-44.SE6, which is not IPv6 capable, so an update of the IOS is required to make them support IPv6 natively. This means that an important investment in new licenses is required to manage switches using IPv6.

Regarding MINETUR's network, routers affected in the service consist of those to access the Ministry's secure network perimeter. These routers will be configured in redundancy using the HSRP protocol. 3 IPs will be used for each HSRP, two physical and one virtual.

German Pilot:

As part of the autonomous system implementation tests, all relevant routers have been enabled for IPv6. All relevant routers under control of Citkomm are implemented as Linux-based software routers. The provider edge routers are based on Cisco technology. For the routing static and dynamic routing is implemented. For the dynamic routing OSPF is used. The IPv6 implementation did not raise any significant problems, with the exception of ospf6d on Linux.

OpenVPN from Ubuntu 12.04 (v2.2.1) is considered as operational as far as the tests are performed until now.

Turkish Pilot:

Throughout the pilot process, the next step after the addressing plan was configuring routers with IPv6 support. Since routers in the TURKSAT network (as well as other L3 devices) had IPv6 support, this step was not a challenging experience, as the routing protocols for external routing BGP has been configured for the defined networks. The address range 2A01:0358:4F00:0002::/64 has been allocated from Turk Telekom for interface connectivity and BGP configuration. BGP connectivity was established and the address range 2A00:1D58:0::/36 has been announced to the Internet. Similarly for the internal routing static routing had been deployed where necessary.

Static routing had been deployed on the connection between TURKSAT and the participating

governmental agencies.

2.3.2 Affected Central IT Systems

Spanish Pilot:

Regarding the Red SARA network, a comprehensive inventory of the different services mentioned has been conducted, and a deep analysis of the software is being performed to ensure compatibility with IPv6 services.

Public IP addresses have been configured in Internet firewalls to offer IPv6 services natively with associated IPv6 addressing. As it has been mentioned, it has been necessary to upgrade the software used on the Internet firewalls, though the appliance itself has been kept.

To offer the IPv6 services it has been necessary to deploy a new infrastructure dedicated only to support this service, which could be used as a shared service platform. A new cluster of servers based on Linux has been installed on the DMZ of Red SARA to host the different servers:

- NAT64 gateway
- Reverse Proxy
- DNS server
- Mail server

Firewalls located on the connections areas have also been configured to process IPv6 traffic, not only routing and filtering but also ciphering.

Currently, the IPv6 DNS service is provided through the SARA network, so accessing resources published on the network in IPv6 is possible.

German Pilot:

- General:

All central systems of the Citkomm network will be affected by the project. Due to the fact that until now the focus of the project was on the network environment none of the following mentioned central systems have been transitioned productive until now.

- Application backbone infrastructure

Application servers are tested in the test bed currently. A timeline for enabling production systems with IPv6 is not fixed now.

- Network infrastructure

Most of the routers of the central distribution network are in productive dual-stack mode. For VPN terminal systems and the routers to the application server segments test system are placed on production equivalent positions. Therefore, the routing scenarios are being tested currently to approve them for production use finally.

The complete preparation of a new iWAN generation that is fully IPv6-enabled is on schedule for 2014. However, it is possible to use IPv6 with the current Ubuntu 12.04 based generation. This will usually not give the customer's admin full access to all the features he can control, but can be already used to connect a customer's network with the IPv6 world and the Citkomm data centre network.

- Customer Environment / LAN

The typical basic LAN servers (Directory, DNS, DHCP, and Mail) are counted as tested and ready for being configured in a pilot customer's network. This will take place in the beginning of 2014.

Turkish Pilot:

Main central IT systems for the Turkish pilot can be considered as the DNS and the logging systems, which are deployed and maintained within TURKSAT network. These systems had been already working before the project over IPv4. These systems are affected by the IPv6 transition as expected. These items are investigated and updates have been done as defined in the following sections.

2.3.2.1 DNS

Spanish Pilot:

The DNS service in each of the connection areas is provided by means of BIND version 9.3.4-6, and BIND 9 fully supports all currently defined forms of IPv6 name to address and address to name lookups. It will also use IPv6 addresses to make queries when running on an IPv6 capable system.

To allow the access from pure IPv6 clients to DNS service, an IPv6 capable DNS server has been installed in the DMZ of Red SARA. This server has been configured as a slave for the different zones for which we are offering IPv6 services (that is, the zones where the IPv6-enabled e-government services, such as `administracionelectronica.gob.es`, belong to). This server receives the zone files from the master servers used previously to serve these domains (that of course have had to be configured to do so). In these zone files the necessary AAAA-records to allow the access of the clients using IPv6 have been included. At this moment, each domain using IPv6 services from Red SARA has its original name servers plus another one IPv6 capable, the one provided by Red SARA. To do so it has been also necessary to modify the list of NS entries at the registration authority (usually `red.es`).

Regarding MINETUR network, the DNS service is provided also by means of BIND. As it has been mentioned before, two ranges of IPv6 address are used to provide access through SARA network and from the Internet.

German Pilot:

The operation of DNS Servers in a dual-stack IPv6-enabled environment is considered as production grade proven. The Citkomm primary DNS is productive and public available since Q1/2013. The Windows DNS is also ok as the tests in the LAN and application backbone test beds acknowledged.

Turkish Pilot:

IPv6 support was added to the DNS servers by configuring IPv6 addresses and reverse DNS records in the respective NIC.TR servers.

2.3.2.2 DHCP

Spanish Pilot:

In connection areas, IPv6 is assigned statically, so DHCP is not used in Red SARA.

In the case of MINETUR, IPv6 is assigned through autoconfiguration so DHCP is not used either.

German Pilot:

Most of the network areas and components affected are working with static IP addresses. DHCP will be relevant for the local networks. Test beds for such local networks have been installed and

the DHCP service was one of first investigation points to get these networks ready for operation. See also chapter 2.2.4.3.

Turkish Pilot:

IPv6 address configuration is being made statically in Turkish pilot for the time being. Hence, DHCPv6 is not deployed.

2.4 Security Aspects of Using IPv6

This chapter documents the security aspects of running an IPv6-capable network for e-government services. Some of these aspects originate from the involved devices (e.g. firewalls), others from the use of IPv6 addresses. Finally, we emphasize that also non-technical aspects such as training for technicians as well as other employees are needed to keep the same level of security, as exists nowadays in an IPv4-only network environment.

Spanish Pilot:

As far as Red SARA is concerned, regarding systems and components referred to in this section, one point to highlight is the deployment of the new 2.9 version of Snort. Snort is the open-source IDS/IPS used in Red SARA connection areas³, and it reports data to CCN-CERT through the logging aggregator. This new version is able to analyse IPv6 traffic.

Additionally, as it was previously mentioned, it has been necessary to change the configuration in all the firewalls involved in the deployment of IPv6. New interfaces, rules and VPNs have been created to support the new protocol.

German Pilot:

The IPv6 implementation of OpenVPN is very similar to that in IPv4. This means that all routes and tunnels can be configured for IPv6 the same way that was used for IPv4.

Turkish Pilot:

In the case of the Turkish pilot, IPv6 support means there will be a dual-stack network over which both IPv4 and IPv6 traffic will be flowing. It is assumed that security and performance issues will

³For more information, see <http://www.snort.org/>

increase in a dual-stack network since the network will be a target both for IPv4 and IPv6 attacks. In addition, routers and L3 devices should be able to deal more traffic when they are run in dual-stack mode. It is sure that all security and monitoring appliances should be IPv6-enabled and rules and access control lists should be updated appropriately.

Recently several different types of attacks have been observed over IPv6. For the time being, simple attacks like SYN flood are the most common types.

2.4.1 Firewalls

Spanish Pilot:

As expected, firewalls have been one of the elements more impacted in the deployment of IPv6 in Red SARA. In some cases (border firewalls accessing Internet) it has been necessary to upgrade software versions (Fortigate 4.0 to Fortigate 4.0MR3 with the patch 441), while in others (connection areas) it has been enough to define new rules and elements to fulfil the needs.

As it was mentioned previously, firewall configuration has been changed to fulfil the new requirements in two areas:

- Addressing and rules
- IPsec tunnels

The actual IPv6 *stack* (implementation) is completely separate from the IPv4 one even if the protocols often behave identically. If the firewall needs to process IPv6 traffic, it is necessary to translate the IPv4 rules used previously to the new addressing schema (if not all, at least those related to IPv6 traffic). Depending on the product used to implement the firewall service this translation can be tedious. In the case of Red SARA, where all the traffic crosses the network encrypted using IPsec tunnels, it is also necessary to define new tunnels to accommodate the new networks.

In the case of MINETUR, one firewall rule has been added to allow IPv6 traffic only through HTTP and HTTPS to eITV service.

German Pilot:

Of course, the firewalls had to be made IPv6 aware. In the case of Citkomm's Linux based firewalls this was an issue of updating the firewall management system running fwbuilder. Then new

definitions and rule sets with IPv6 sections had to be created. The proper operation of the rule sets had to be verified.

The new protocol with its new special options and features will for sure need more attention as it comes wider in use. It can be expected that many new issues show up on the security level as IPv6 traffic will make up a greater share of the whole Internet traffic.

Fortunately, all rule sets are managed centrally. Therefore, the maintainers for the firewalls will have to be trained before the rollout of IPv6 to more than pilot customers is started.

Turkish Pilot:

Through the pilot, all security devices (firewalls, IDS/IPSs etc.) have been configured to support IPv6. Rules and lists defined in these devices have been updated according to the TURKSAT IPv6 network structure.

2.4.2 Application Layer Gateways (ALGs)

Spanish Pilot:

Application Layer Gateways (ALG) are being used in the Spanish pilot in the shared service platform for providing IPv6 access to e-government websites, by means of reverse proxy servers.

To implement this access to web services using IPv6, Red SARA has installed a reverse proxy server with dual-stack. The proxy is listening in IPv6, waiting for connections from Internet. Once it receives a connection, it finds in the HTTP 1.1 header "Host:" the final service the client is trying to connect to. It uses this information to connect to the correct original server ("parent") using IPv4 via Red SARA. Once it has received the information, it returns that information to the original client using IPv6. That way, an IPv6 client (who is not aware of all the technical procedures involved) can connect to a service offered only by means of IPv4.

German Pilot:

As far as this is related to Citkomm, ALGs and Proxies are considered as one class of devices. See in the next section.

Turkish Pilot:

For the status of the Turkish pilot, there is no deployment of ALGs.

2.4.3 Proxies

Spanish Pilot:

Red SARA provides proxy services to the institutions that are connected to its network. To achieve this, there are proxy servers running in the service cluster located in the connection areas between the institution and Red SARA, which can act both as direct and as reverse proxies.

These services are provided by means of the open-source software Squid 3.1.8⁴, which supports IPv6.

Squid is also used as gateway for IPv6 clients to IPv4 world (see previous section about ALG). This software, among its capabilities, has the option to act as reverse proxy or accelerator, and it is installed in the Internet access DMZ of Red SARA with dual-stack configuration, using:

- an IPv6 address to communicate with IPv6 Internet clients, and
- an IPv4 address to talk to e-government web portal servers.

In this way, as has been described before, it is able to act as bridge between IPv4 portal servers and IPv6 requests from citizens.

German Pilot:

All affected proxies have to be approved for IPv6 operation with or without possible IPv4/IPv6 translations. Subsystems like virus scanners must be included in these tests.

Moreover, especially all filter rule sets have to be checked for IPv6-awareness.

A special point is the Citkomm created local administrator interface of the iWAN systems. This GUI has to be extended to become IPv6-enabled and to offer the same opportunities for IPv6 as in IPv4.

Turkish Pilot:

No proxies have been deployed in Turkish pilot as an administrative decision.

⁴For more information, see <http://www.squid-cache.org/>

297239	GEN6	D3.6: e-government Services with IPv6 Compilation
--------	------	---------------------------------------------------

2.4.4 Other Security Aspects

Spanish Pilot:

Regarding NAT64 security issues, a security policy forbids any kind of traffic from the Internet to go through SARA network. Therefore, when using NAT64 to enable IPv6 connection to web portals, traffic from the Internet is routed to IPv6 public addressing, so no data is transmitted through the SARA network in this case.

3 GEN6 GENERIC SERVICES WITH IPV6

3.1 Transition to IPv6

This chapter documents the chosen high-level decisions for the introduction of IPv6 in each national pilot. It describes the chosen approach for each pilot, how IPv6 has been introduced (e.g. in parallel, new networks, or inside existing ones), which steps were taken to do so (from a top-down perspective) and which goals have already been achieved (and how). In this part of the deliverable, also the pitfalls found during this work are documented.

3.1.1 Chosen Approach

German Pilot:

For the German pilot, it was decided to start all IPv6 transition work on a dual-stack strategy. The most important reason for this decision was that the real existing infrastructures were very heterogeneous, this fact being related to the applications in use. Up to now, there is no realistic way to implement an IPv6-only infrastructure on the client side. On the server side it is also not useful to separate the IP traffic by protocol version. In this case, the application data would have to be kept in a synchronous state, for both IP worlds. To avoid this additional effort and increased technical complexity, the dual-stack approach was chosen as the basic concept. Wherever possible, a testbed landscape was used first.

The activation of IPv6 was then executed step by step.

Initially, the used network infrastructure components were reviewed. Switches turned out to be non-critical as they are used as simple layer 2 devices in the Citkomm network, and *managing* them via IPv6 was no goal of the project. This results from the use of a separated out-of-band management network with no connection to customer services related traffic.

Then, the basic enabling of IPv6 on the involved servers and clients was considered. To avoid unwanted and therefore uncontrolled communication, IPv6 was deactivated at first in all relevant networks and systems. Then IPv6 was enabled on server side first, and after successful tests on the client side, too. Until this point still all services and applications used IPv4, as all DNS requests resolved to IPv4 addresses only. Afterwards, IPv6 could be enabled application by application, after testing with some clients with specific host-entries overruling, respectively replacing DNS resolution during initial test.

Following the same basic principle, network segments were enabled for IPv6 one by one. This way, IPv6 connectivity could be tried in small steps. This was also easy to handle in backbone segments with dynamic routing, because on the installed routers the IPv6 routing is handled by a separate daemon, which is independent from the IPv4 routing service.

This approach gave birth to the opportunity to make an IPv6 roll-out in single steps, allowing possible functional errors to be identified and fixed easily.

Spanish Pilot:

As it has been mentioned previously, the Spanish pilot combines two different approaches to the IPv6 transition:

- Dual-stack, as the chosen mechanism for transitioning to IPv6 in the connection areas of Red SARA, and in the infrastructure that supports the eITV service provided by MINETUR. Additionally dual-stack is also being considering for some services operated by MINHAP, as an evolution from the IPv6 availability achieved by means of the shared service based on IPv6 to IPv4 translation.
- IPv6 to IPv4 translation, using reverse proxy and NAT64 equipment located in Red SARA's shared services data centre, for providing a transition mechanism that allows public administrations to offer IPv6-enabled online services.

These two approaches are complemented by the use of tunnelling techniques required by the cross-border pilot (due to the lack of IPv6 native support in sTESTA), which helps the Spanish partners to acquire a solid expertise in deploying IPv6 which other government units can benefit from.

Turkish Pilot:

The Turkish pilot has been in production over IPv4, and the transition should be seamless for the end users (Turkish citizens). Considering this issue, the pilot participants have decided to implement dual-stack through the network.

As stated previously, the Turkish pilot consists of two parts: Frontend and backend transition. The frontend transition includes the IPv6 enabling of the e-Government gateway (EGG) portal while backend transition includes the establishing of IPv6 communication between TURKSAT and the participating governmental institutions (SGK and PTT). Both cases were suited to work on the dual-stack implementation. Most of the planned IPv6 transition in the Turkish pilot is complete, and participants have observed that dual-stack is the right solution for the pilot. Still, another

important observation is: One should keep in mind that dual-stack increases management workload for the network since the administrators are responsible for the security and monitoring of two different protocols.

3.1.2 Planned Order of Changes due to Transition

German Pilot:

IPv6 was always activated step by step. Due to the global dual-stack approach, the enabling of the new protocol could be started in different subnets at the same time.

To make sure that there will not occur any unwanted side effect from one IPv6 transition area to its legacy neighbour segments, as a very first step all router and gateway systems were checked for their IPv6 state – and IPv6 was strictly deactivated. This way, we made sure that enabling IPv6 in a single network segment was limited to this segment alone and there would be no IPv6 communication happening to other network areas.

After that, the first network areas were enabled with IPv6. We started with the local Internet uplink. Starting from the provider uplink router down through the access components and gateways, the DMZ and the internal gateway routers were enabled with IPv6. As Citkomm uses a fully redundant access network, several failover mechanisms had to prove their IPv6 capability. Because of the used router systems and the separated IPv6 routing daemon this could be performed in the productive environment after passing the testbed successfully without affecting IPv4 in the production networks.

In parallel, the WAN/VPN network with its specific components has been enabled for IPv6. It is based on different VPN solutions, using Internet or MPLS networks as underlying transport facilities. The necessary testing was done with a testbed that represents a typical customer access infrastructure. IPv6 ability could be enabled for the transport layer (if available) as well as for the inside tunnel communication for the VPN solutions.

After finishing the work on the Internet uplink, the first services in the DMZ have been enabled for IPv6. An early adopter was the public Citkomm website. The existing architecture uses reverse proxy servers for all accesses from the Internet to the vast majority of the web servers. IPv6 only had to be enabled on the public side of each reverse proxy. Afterwards, additional services have been enabled with IPv6, namely the public DNS and SMTP servers.

Moving these areas to production state required the monitoring system to be IPv6-aware.

Externally available services should be monitored from an external probe. The provider for this system has to be capable of offering IPv6 services, namely connectivity for the monitoring appliance. The latter had to be enabled for IPv6 with its longer addresses, and checks had to be adapted manually in many cases.

The work on the implementation of IPv6 in the local area networks (LAN) – has been started independently from the work described before. In the Citkomm pilot work on the LANs started after the server transition due to the involvement of the same staff. The LAN consists of "Linux enhanced" Windows networks, meaning it is based on an Active Directory with integrated Exchange and MS SQL Servers and some Linux servers for additional services, like e.g. Wikis. The clients are Windows systems (mostly Windows7), and some Linux desktops. As part of the German pilot, also a transition for a Linux-based network has been started. Due to strategic decisions, the former Linux server based environment of the Citkomm LAN was migrated to Windows. Inside the LAN, servers were enabled for IPv6 first. In this state they started to use IPv6 with link local addresses to other machines reachable on IPv6. All Windows-internal communication switched to IPv6 in this scenario - more or less automatically. To get into the chosen addressing concept, the addresses from the Citkomm range of the national government address scheme have been configured on the servers. Additional auto-configured addresses have been suppressed. DHCPv6 has been used to provide clients with IPv6 addresses. The router advertisements for the network were supplied from the segment's router that connects the LAN to other network areas. By using static address assignments with DHCP, it was possible to get the clients in production step by step. The further roll out of IPv6 could be grouped and sorted by application use and the criticality of the touched workstations.

In the beginning, external communication to other governmental institutions using the national government backbone was thought to be the first area for transition. However, the enabling of the external network link itself had been delayed for many months. Furthermore, the use of real IPv6 communication needs active IPv6-enabled paths to internal server segments when passing the backbone of Citkomm. Due to load and change rate related issues with the IPv4 routing daemons, the central backbone was one of the last components brought into an IPv6 production state. In fact the services in the national government backbone for DNS and SMTP had not been IPv6-enabled until the writing of this document. Yet, recent success notifications have stirred new optimism in this work area.

Spanish Pilot:

As it has been described before, in the Spanish pilot, the planned order of changes has been:

1. Setting up the platform for providing shared services for IPv6 access to e-Government web sites. This involves ensuring external IPv6 connectivity to Internet, by configuring the network devices, hosts and applications located in Red SARA data centre.
2. Upgrading the backbone of the network of Red SARA to IPv6, as well as the links connecting the institutions' sites to this backbone, carried out by Red SARA's telecommunications provider, under the guidance and supervision from MINHAP.
3. Configuring the equipment located in the connection areas of the entities linked to Red SARA to operate in dual-stack, including the connection areas of MINETUR and MININT involved in the eITV service.

In parallel, the adaptation to IPv6 of the eITV service has been carried out.

Turkish Pilot:

The Turkish pilot has prioritised the frontend IPv6 transition. Hence the first phase of the pilot focused on the IPv6 support of e-Government gateway portal. At first, the local ISP has been queried for an IPv6 uplink. After the receipt of a positive answer on having an IPv6 uplink from the current ISP, the internal network infrastructure components had been analysed, and requirements regarding the internal network had been enlisted. This list was made, starting from the outmost network components and continuing with the inner ones. To be more precise: The EGG portal backbone router, layer 3 switches, firewalls, load balancers and web servers have been checked if they are IPv6 ready in the sense that they can have basic IPv6 capabilities like identifying and routing IPv6 packages and running IPv6 routing protocols (OSPFv3, BGP). In other words: At this stage, more advanced IPv6 support such as IP mobility was not considered a must for the IPv6 support of network appliances. After being sure that every network appliance on the EGG's road was IPv6-capable, an IPv6 address plan has been created and implemented in the same order: Starting from the outermost level.

The first phase had been completed throughout the first year of the pilot. As the first result of the pilot, the EGG web portal had been IPv6-enabled.

The second phase of the pilot focused on the IPv6 transition of the communication between TURKSAT and the other governmental institutions which provide the backend services. In this phase IPv6 was working over either dedicated lines or by deploying VPNs between the

institutions. For the pilot VPNs, tunnels for secure communication have been deployed between the institutions. For this purpose, public integration boxes have been developed and deployed on the end points of the communication. These boxes create a VPN tunnel over IPv6 to secure the communication. Currently they have been successfully deployed in SGK and PTT.

3.1.3 Successfully moved components until now

German Pilot:

At this point in time, most components and areas of Citkomm are enabled for IPv6. In detail these are:

WAN Network

The WAN routers are Linux-based appliances, using OpenVPN for tunnelling. A recent version of OpenVPN was tested successfully with IPv6 on both, the outer and the inner side of the tunnel tube. Basic services like NTP, DNS and proxy are enabled for IPv6 in dual-stack use. The approved design has not been integrated in the default setup procedure for the network components so far. But it has been tested in several installations extensively and it expected to make its way into the next release of the routing appliances.

Internet Access

The Internet Access network of Citkomm is fully IPv6-enabled. All components run in dual-stack mode. All fail-over mechanisms of the high availability design support IPv6 and IPv4. Several servers with connections to the public Internet are enabled for IPv6. Most IPv6-enabled Web servers use the reverse proxy as IPv6 termination point, due to security considerations. Servers such as DNS or SMTP use IPv6 directly, but are protected by firewalls.

Local Area Networks

In the local networks, the IPv6 transition has been successful implemented in different test beds, covering a variety of server systems. In productive networks of a customer and Citkomm itself, the implementation has just started.

Other Networks

The connection to the national government backbone is IPv6-enabled. No services are in production so far due to the outstanding IPv6 empowering in the core backbone.

Spanish Pilot:

As it has been described in section 2.2, in the Spanish pilot several components have been successfully moved to IPv6 so far.

Regarding the shared service platform for providing IPv6 connectivity to e-Government Web Portals, it has been implemented using two different approaches:

- Initially, based on a Reverse Proxy, combined with NAT64 for services in which the validation of the user's electronic certificate was required
- After operating the service for some time, and adding new portals, the solution was evolved, having NAT64 not only for the cases in which there is involved a user's electronic certificate validation, but also for all the services based on SSL, since this simplifies the management of the server certificates used in SSL connections.

Using this platform, several Web Portals operated by MINHAP and the Ministry of Justice have been made IPv6-enabled.

Additionally, a feasibility assessment for moving to a dual-stack platform some of the services operated by MINHAP that currently make use of the IPv6 enablement shared service has been performed, with positive results. This assessment has been considered in order to provide an alternate solution for enabling IPv6 portals, in case scalability problems are found when increasing the number of portals in the shared service platform based on the IPv6-IPv4 gateway. With this approach, e-Government services operated by MINHAP would be made IPv6 ready by means of this dual-stack platform, while the IPv6-to-IPv4 gateway would provide IPv6 readiness to the e-Government services operated by other government units, as a shared service in Red SARA.

Regarding the backbone of Red SARA, all the connection areas of the Ministries have been configured to support IPv6, enabling dual-stack in the equipment. New pseudo interfaces for IPv6 have been added on the routers (WAN and LAN networks) but over the same VLAN at VPLS level, so no change in the VPLS infrastructure has been required.

Additionally, MINETUR is adapting the eITV service to IPv6 as defined in the project. This has two distinct parts: the IPv6 infrastructure and the modification, to support IPv6, of the application that makes use of that infrastructure. To achieve this goal, both development and systems departments of MINETUR are involved, working on the basis of a coordinate effort.

Regarding the eITV infrastructure, the production environment already deployed and connected to Red SARA and the Internet has been tested, verifying successful IPv6 connectivity from Red SARA and from the Internet.

Due to the need to test the eITV service before offering it to the real users, now we have two environments: preproduction and production. The production environment is IPv6-full while the pre-production environment use IPv4/IPv6 dual stack mode because it is necessary to access to it from the development department computers that use IPv4 protocol.

Turkish Pilot:

For the Turkish pilot, currently TURKSAT and the participating institutions have active IPv6 uplinks from their current service providers. In addition, the EGG portal, which is managed by TURKSAT, is IPv6-enabled for more than a year now. For the time being, TURKSAT is monitoring the activities and requests in EGG portal made by citizens. Monitoring activity is being made for both security purposes and for reporting on the usage of EGG services.

On the other hand, backend infrastructure has been enabled with IPv6 for SGK and PTT services. This means that queries made for services that are provided by SGK (e.g. social security records) or PTT (e.g. postal service records and activities) are being transmitted to them over IPv6, and the answers to these queries are being sent to TURKSAT over IPv6 similarly on the backend.

3.1.4 Enabling IPv6 in Components

3.1.4.1 Practical Tests

German Pilot:

- General:

According to the progress in the pilot, different components were involved in the IPv6-enabling process and had to prove their IPv6 capabilities. On the network level, the basic functionality does not cause any harm, however, when it comes to real applications or more complex setups some issues had to be resolved.

Typical test commands for low-level operations are:

`ipconfig / ifconfig / ip a` (to check the validity of the local configuration)

ping / ping6 and tracert / traceroute / traceroute6 with options to select sender addresses or interfaces to check the connections to targets

route / ip r / ip -6 r to check the routing tables

- Application backbone infrastructure

Citkomm and Fraunhofer have set up three IPv6 test areas with more than 30 virtual servers and clients. Recent operating systems such as Windows Server 2008 R2, Windows7, Ubuntu LTS 12.04, or SLES11 SP3 support IPv6 “out of the box”. Some minor issues needed extra attention (see also the next chapter for details). The basic services DHCP, DNS, and electronic mail operate as expected. Web services also cause not much trouble. If there are issues, then they are related to the applications that are not aware of the longer addresses and the different literal IP address syntax.

- Network infrastructure

The core interconnect network at Citkomm uses Linux-based routers as node systems. On the perimeter, some Cisco systems are in use. From these, the Internet uplink routers are in the focus of the project as they provide the connectivity to the world and interact via OSPF routing protocol with the interior Linux routers. The routing interaction between Cisco and Linux systems works well as well as the OSPF routing information exchange with the Quagga package on Linux. Due to Quagga problems when using a large number of routes and frequent topology changes (and some missing features), BIRD has been tested as an alternative package. The observed problems are not related to the GEN6 project activities. They were observed, coincidentally at the time of the project as a side effect of some centralisation, homogenisation and expansion of the Citkomm network and appeared only in IPv4. Quagga seems to work well for small environments with only a few number of changes per time. For heavier use, alternatives can better fight the admin’s headaches.

For the wide area network, Citkomm uses the self-developed appliance “iWAN”. All tests are performed with the current iWAN generation, based on Ubuntu LTS 12.04. The distribution includes an OpenVPN implementation that supports IPv6 on the underlying network as well as inside the secure tunnel. Not surprisingly, the use of IPv6 inside the tunnel does not require the outside tunnel to be IPv6-aware. All communication could be tested successfully with IPv6 and with combinations of IPv4 and IPv6. The scripts that generate routing information dynamically when a tunnel comes up, were adapted to take care of IPv6 routes. This is required as the Citkomm infrastructure includes redundant tunnel terminal systems. Therefore, care must be

taken for using the correct routing information, regardless whether or not the iWAN at the customer side has chosen one or the other terminal. Therefore, for any such setup the correctness of the established routes have to be checked carefully.

The generation and distribution of firewall rules in an automated way is an action point for the next period, as well as the automated setup of an iWAN system with respect to IPv6 configuration.

- Customer Environment / LAN

The infrastructure of a typical client network is based on Windows server technology. The setup of address assignment and basic network configuration distribution via stateful DHCP has been described before. The correct setup of Windows and Linux clients was verified successfully.

The tested applications are web browsers, mail clients, RDP and ssh for connections to servers, at this moment. As soon as the server systems for native client/server applications are available, they will be tested, too.

Spanish Pilot:

The test performed to make the connection areas of the Ministries IPv6 ready have been described in section 2.2.4, implying three different kinds of tests:

- Traffic processing through VPNs
- HTTP traffic between two connection areas
- DNS IPv6 capabilities

Additionally, as it has been mentioned before, MINHAP has also performed some test to assess the feasibility of moving to a dual-stack platform some of the applications that currently make use of the IPv6 enablement shared service. These tests were made with the Spanish PEPS (Pan-European Proxy Service), the interoperability node of the STORK platform, by setting a dual-stack path (involving routers, firewalls, reverse proxies and load balancers) between Internet and the PEPS servers, which have been configured also in dual-stack. Though some problems regarding the configuration of the maximum transfer unit (MTU) were initially found, after solving them the results of the tests were positive, confirming that the designed solution can work properly and can be extended to other services.

297239	GEN6	D3.6: e-government Services with IPv6 Compilation
--------	------	---------------------------------------------------

In the case of MINETUR eITV service, access tests via IPv6 with a private address range have been made in the MINETUR laboratory.

A first line of perimeter security has been designed. It defines the access to the DMZ service and it is delimited by two Cisco 2960S, level 2, systems.

An IPv6 /64 prefix is used. The IP addresses to be used are those obtained automatically when auto-configuring the equipment. Once the IP is obtained, it has been configured manually on the equipment.

This process is the same for the HSRP virtual IP's required for the Cisco equipment.

Three IPs are used for each HSRP, two physical and one virtual.

In the perimeter security equipment, Palo Alto PA-5050, the same procedure is used to obtain the IPs and the high availability system, allocating three IPv6 addresses, two physical and one virtual.

The configuration of the load balancing equipment, F5 3900, uses the same mechanism as in the previous equipment, with three IPs (two physical and one virtual).

Two DNS servers are used, dns.ipv6.es and dns2.ipv6.es and they are using the same procedure to obtain their IP addresses.

This configuration will be the same as in the production environment and is represented in the following figure.

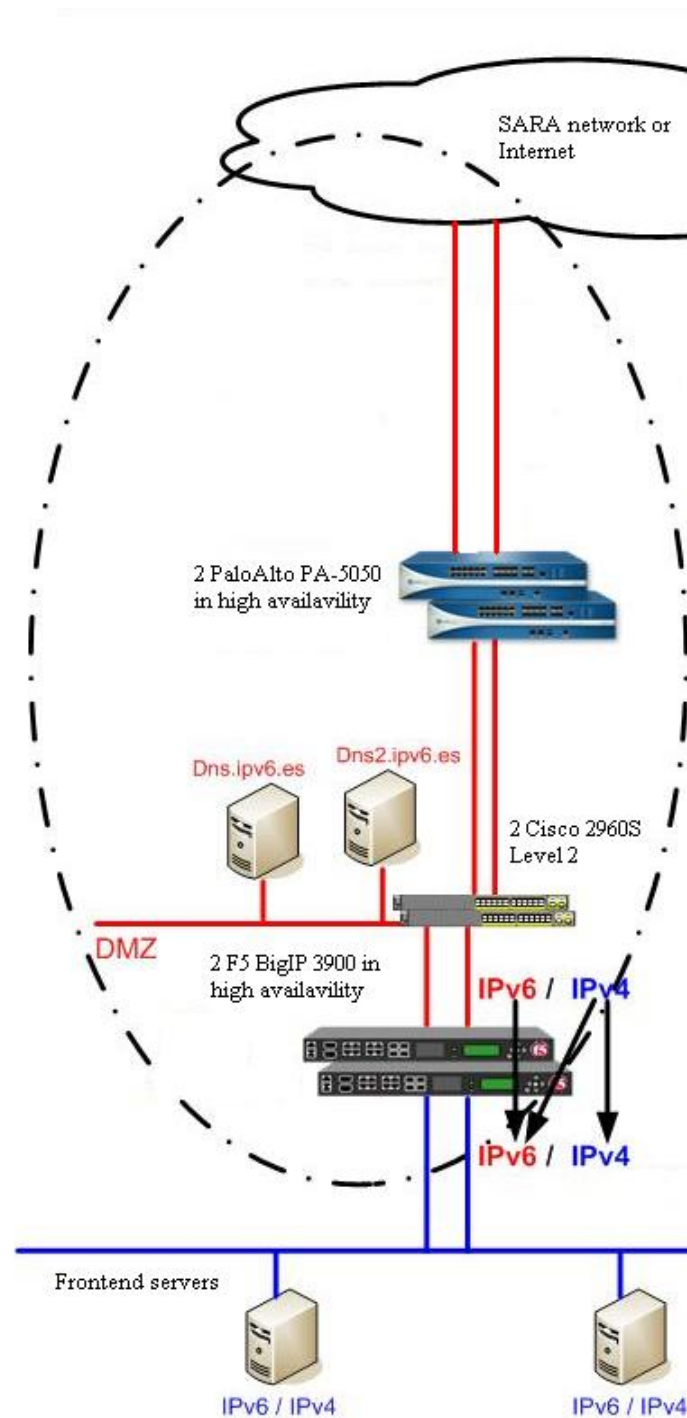


Figure 8 – Spanish Pilot: MINETUR's Network Configuration

Regarding the evolution of the implementation of eITV service, it is installed in the pre-production environment. Preliminary tests have been done having obtained a satisfactory result. Access to the application is successful. Users are validated in the application in two different ways:

- The traditional system of user and password
- By means of digital certificate.

Both validation methods have been tested with successful results.

Turkish Pilot:

Turkish pilot consists of two sub phases namely the frontend and the backend as stated previously. As a highly available infrastructure both the frontend i.e. EGG, and the backend communication has been tested for various scenarios.

Practical tests focusing on the network connection have been described at Section 2.2.4 in this document. In addition to these tests, other performance and usability tests have been implemented on generic services such as DNS, load balancing and EGG Web portal. For instance in the case of EGG Web portal is accessible via username/password or e-signature. Both access methods have been tested and successful results were observed.

3.1.4.2 Security Considerations

German Pilot:

- General:

Citkomm has an established security policy for its productive environment. The policy has been designed in an IPv4 world but can and must be extended to the IPv6-enabled world, too. As a dual-stack approach was chosen, the network paths for the permitted traffic are the same for both protocols. To be able to use the known graphical interface for defining firewall rules a new version of the “fwbuilder” tool had to be set up and was installed and a new base system consequently.

More in deep investigation for specific IPv6 issues is on the schedule.

- Application backbone infrastructure

The application servers themselves are treated as being located in a safe area. Nevertheless, the router to the application segment has firewall rules on it that restrict the access to the servers.

- Network infrastructure

For the network infrastructure the general security rules are applied. In addition, the firewalls and application layer gateways (proxies and reverse proxies) must be tested and watched.

- Customer Environment / LAN

These networks are protected by iWAN systems. The basic security considerations are the same used for the network infrastructure above. In addition, a customer administration interface will have to be updated. Among other things, it allows the customer's administrators to add exception rules to the proxy rule sets. This application has to be extended to allow the handling of client IPv6 addresses.

Spanish Pilot:

As it has been mentioned in section 2.2.4.2, in the case of Red SARA, the main security considerations have been related to the firewalls and the IPsec tunnels.

In the case of MINETUR, the firewall is the main security system. As there are two environments: preproduction and production, two rules have been enabled in the firewall to allow access to these environments only by http and https protocols.

Turkish Pilot:

As stated in 2.2.4.2 security policies; including access control rules (firewall rules, access control list rules etc.) and performance criteria in order to protect the whole system from DDoS-like attacks, have been updated in order to filter the IPv6 traffic.

In addition to the security considerations for the network level, generic services are also reviewed as well. Thus DNS, load balancer and EGG Web portal access filters have been added to the system. Also necessary configurations have been updated to keep the access logs for these services over IPv6.

3.1.4.3 Lessons Learned (Experiences and Pitfalls)

German Pilot:

The Linux kernel supports port mapping in iptables only in latest versions: As a consequence of

the lack of NAT in IPv6, the port mapping at a gateway was not implemented until recent Linux kernel versions. For a test scenario and a customer approval check for implemented services it was required to forward an IPv4 connection to a machine that then used IPv6 for the further communication to a final test object.

No packet for Nagios / Icinga nrpe client with IPv6 support available: For monitoring in the well-known Nagios / Icinga monitoring system the nrpe remote node is required. At this moment no nrpe-client with IPv6 support is available for Ubuntu LTS distributions. In consequence, it is necessary to compile the source code with adequate options. This can lead to a fitting package in a local repository or even to a contribution to the Ubuntu project. Maybe newer technical approaches will make the current nrpe obsolete. But the wide-spread established base justifies the extra efforts in Citkomm's heterogeneous infrastructure where several Linux distributions have to be served.

Spanish Pilot:

Apart from the lessons learned described in section 2.2.4.3, there have been also some lessons learned after the tests for assessing the feasibility of a dual-stack platform for MINHAP services, where some problems with the MTU in the reverse proxies were encountered. These reverse proxies are used for security reasons. Since direct access to the services from the Internet is not allowed, they are located in front of the application servers. Because VPN are used in Red SARA for connecting different sites, a header is introduced in the IP packet that increases the MTU above the defined limit. When these packets go through the reverse proxies, a fragmentation request is generated so that the reverse proxies decrease automatically the MTU. However, this was not working properly, so the adopted solution was decreasing the MTU of the interfaces of the reverse proxies manually.

Regarding MINETUR, initially, the eITV application was developed for an IPv4 environment. Therefore, the transition to an IPv6 environment has required the review and adaptation of the source code.

Although laborious, the problems have been similar to those of IPv4. The difficulties found have not been too great provided some basic considerations as, for example, exclude IPv4 addresses in the program code and always use stable identifiers to connect to other nodes (host names, for example).

Thus, delegating the resolution of the IP addresses to the name resolution system, there will be no problem to access to other hosts.

Turkish Pilot:

Turkish pilot participants have gained a considerably high amount of hands-on experience and know-how on IPv6 through the pilot. Some of the high-level ones have been described in Section 2.2.4.3.

Security is one of the hot topics that the participants had hard times. It is observed that one should watch out for IPv6 prefixes announced through the VLANs and should keep track of the IPv6 addresses that a server or a device has. If a router or a layer 3 switch is configured accidentally (or because of the default configuration) to announce IPv6 prefix to a VLAN, this would cause servers and devices, which have autoconfiguration setting is on, to get new IPv6 addresses without your notice. As the result you would see strange IPv6 addresses in your logs and flow data. This is a case especially for the MS Windows hosts and servers.

3.2 Affected Network Components

This chapter takes a deeper, more technical look at certain network elements and servers of an IT infrastructure which are affected by a transition of e-Government services from IPv4-only to running IPv4+IPv6 support (from their users' point of view). These systems include network-level devices such as routers, plus auxiliary services like electronic mail and DNS, which are in direct or indirect use of the migrated e-Government services.

3.3 Routers and Routing

German Pilot:

The router support for IPv6 caused no problems besides the Quagga issue, see above. Most of the routers in the Citkomm network are Linux based. Some systems are Cisco routers. In none of these systems any kind of problem regarding especially to IPv6 occurred. Also the used dynamic routing protocols resulted in no specific problems. Helpful is the fact, that in Linux software routers the OSPF6 daemon is fully separated from the IPv4 daemon. This gives good control for soft transition scenarios, but finally it has to be watched for IPv6 routing independently of IPv4 in either case.

Spanish Pilot:

As it has been described in section 2.3.1, regarding Red SARA, at present, all Internet routers, as well as the routers involved in the backbone infrastructure (located in the connection areas) are

capable to route IPv6 traffic.

In the case of MINETUR, the IPv6 networks are directly connected to the firewall PaloAlto PA-5050 which acts as a router, redirecting the traffic to the Cisco 3750 or 2960S switches (depending on the environment) where a VLAN is created only for IPv6 servers .

Turkish Pilot:

Router and routing configuration details have been described in 2.3.1 stating the external and the internal routing protocol details. As buying IPv6 enabled devices is obliged by law in Turkey, all routers and L3 devices in TURKSAT network were IPv6 enabled.

3.4 Affected Central IT Systems

German Pilot:

Out-of-band management networks can remain on IPv4 when systems with connections to the public internet become IPv6-enabled from obvious reasons.

Core infrastructure components cause harm only under rare circumstances when running the IPv6 protocol.

Monitoring systems like our beloved Icinga require often more than less work to have checks IPv6 aware, or to be able to differentiate between the operational state in IPv4 and IPv6. Several approaches for a unified setup of bilingual tests were found but not yet a take-this-and-forget-the-problem solution could be identified.

Security with IPv6 is expected to become a challenge as the use of the protocol increases. The design has some features that can give a new flexibility. The practical usefulness of these features will have to show that it is worth the risks of non-watertight implementations. The re-established respectively possible end-to-end connectivity requires new attention in security and network design. Ease-of-use functions like stateless DHCP or router advertisements also contain a misuse potential. Many more remarks can be given in the security field.

Spanish Pilot:

As it has been mentioned in section 2.3.2, a new infrastructure dedicated to support the shared

service for IPv6 availability has been deployed in Red SARA, consisting on a cluster of servers based on Linux located on the DMZ.

Turkish Pilot:

DNS, logging/management and load balancing systems are considered as the affected central IT systems in TURKSAT network through the Turkish pilot. The logging and load balancing systems are considered as one of the most critical systems as they play an important role for the high availability of the system.

3.4.1 DNS

German Pilot:

The operation of DNS Servers in a dual-stack IPv6-enabled environment is considered as production grade proven. The Citkonn primary DNS is productive and public available since Q1/2013. The Windows DNS is also ok as the tests in the LAN and application backbone test beds acknowledged.

Spanish Pilot:

The DNS service has been described in section 2.3.2.1. Both in the case of Red SARA and MINETUR it is based on BIND.

The domain eitv6.mitycia.es has also been created to access the test environment of the eITV application with IPv6 protocol. It can be accessed only through the internal network and Red SARA.

Turkish Pilot:

IPv6 support was added to the DNS servers by configuring IPv6 addresses and reverse DNS records in the respective NIC.TR servers.

3.4.2 DHCP

German Pilot:

Most of the network areas and components affected so far are working with static IP addresses.

DHCP will be relevant for the local networks. Test beds for such local networks have been installed and the DHCP service was one of first investigation points to get these networks ready for operation. See also chapter 11.

Spanish Pilot:

Not applicable in the case of the Spanish pilot.

Turkish Pilot:

IPv6 address configuration is being made statically in Turkish pilot for the time being. Hence, DHCPv6 is not be deployed.

3.5 Further Affected Systems/Components

3.5.1 VPN

German Pilot:

The Citkomm WAN network uses VPN services as central infrastructure. Therefore, VPN is vital for the German pilot. The iWAN gateway has been enabled for IPv6 connectivity. These appliances base on Ubuntu Linux LTS distributions and use OpenVPN as one core component. The combination of used packages is performed in a manner useful for the special demands in the Citkomm wide area network and for the connected customers. The ability for IPv6 has been successful implemented for both: the network interface and the tunnel interface. So at this point, the pilot gateway implementation is able to support fully network connectivity for IPv4 and IPv6. To check the functionality even under WAN and productive conditions one gateway was installed in the test bed at Fraunhofer FOKUS in Berlin. This gateway now keeps a permanent connection to a central gateway at Citkomm.

When such a tunnel is brought up (or when it is finished from whatever reason) some scripts must be executed to publish the route to the OSPF system (or to revoke it). These scripts got extensions so they are now IPv6 aware.

Spanish Pilot:

In the Spanish pilot, Red SARA hosts a set of different VPNs. Among them, only the VPN that connects Ministries (National Government), Autonomous Communities (regional Governments) and singular entities (constitutional bodies and such) is within the scope of the pilot.

This VPN must be capable of establishing connections between the entities linked to Red SARA in both IPv6 and IPv4 protocols.

VPN tunnels between different entities connected to Red SARA are created by means of IPsec. VPN endings are located in external Firewalls of connection areas. These firewalls are based on Stonegate version 5.3.3, which support IPv6. IPsec tunnels for IPv6 are defined in a similar way as those of IPv4. It is needed to define both ends and the networks involved in the connection. As there is only one manager which centralise the configuration of all the equipment used in Red SARA, using only this centralised information the firewalls are capable to agree on the different encryption schemas and to negotiate the different IPsec Security Associations (SAs) needed for the communication to take place. Since the procedure is identical to that of IPv4, no significant problem has been found.

Turkish Pilot:

A VPN connection has been deployed in the backend implementation of the Turkish pilot between TURKSAT and other governmental institutions. VPN connections are finalized at the VPN box placed on the public institution side. NETAS CO. worked on this box as an R&D project. The work finished in 2013. VPN connection was being made over IPv4 IPsec before the deployment of PIB. By deploying PIB, IPv6 IPsec has been used natively.

3.5.2 Load Balancing

German Pilot:

Citkomm does not operate load balancer as special solution. Load balancing features are implemented in some server installations, e.g. WTS farms, but have not been investigated until now.

Round robin DNS as poor man's load balancer is considered as working, but not for WTS gateways on Windows 2012 server.

Spanish Pilot:

Regarding the Spanish pilot, in Red SARA load-balancers are not used. In the case of IPv6 access to web portals of public administrations, an IPv6 load balancing function is performed by the firewalls located in the DMZ of the connection between Red SARA and the Internet, so that incoming requests are sent to the appropriate server in one of the two data centres that host

Red SARA Internet services. After going through the IPv6-IPv4 gateway, there are load balancers before the servers that host the e-Government web portals, but this balancing is performed in IPv4, once the IPv6 to IPv4 translation has been completed. This will be the approach used initially in the pilot to balance IPv6 traffic; reassessing it can be considered when the IPv6 traffic through Red SARA becomes increasingly significant.

In the case of the tests performed to assess the feasibility for a dual-stack platform, the load balancers before the PEPS servers (F5) were actually configured in dual-stack and therefore are able to do IPv6 balancing. Though there were initially some problems with the setting up of the system, and it was thought that they were caused by a wrong configuration of the balancers, at the end the problem was due to the MTU in the reverse proxies, as it has been previously described.

In the case of MINETUR, load-balancers are needed to send IPv6 traffic to the server farm and to act as IPv6/IPv4 gateway to the backend servers inside the internal network, and have been configured accordingly.

Turkish Pilot:

Load balancers have a critical importance in Turkish pilot since all servers are deployed behind them. Load balancers provide security and performance measurements for EGG. In the scope of GEN6 project, load balancers were updated successfully to support IPv6.

3.5.3 Monitoring

German Pilot:

Citkomm uses central monitoring services based on Icinga. Icinga offers IPv6 support, but most of the job is done by the actual test programs and scripts. Quite a bunch of them is contributed by the community. Fortunately, many of them are already IPv6 aware. Additional efforts in the form of more configurations as well as more tests to be performed leading to more load on the Icinga server result from the approach to check to operation of services per protocol separately.

One bad point is the fact, that the well-known remote probe nrpe on the monitored server is not available as packets supporting IPv6 in the Linux distributions used at Citkomm site. This results in additional effort, because the packets have to be compiled from the sources each time until the pain leads to IPv6-enabled package in the Citkomm package repository. This is expected by the end of Q1/2014.

Spanish Pilot:

Red SARA performs the monitoring of its systems using two platforms: Nagios as general purpose platform and CISCO works for CISCO devices.

Because currently the IPv6 traffic to be monitored is very low (restricted only to the external connections to IPv6-enabled web portals), monitoring systems have not been fully adapted yet. IPv6 traffic is being supervised, as a temporary means, using the IPv6 logging capabilities of the firewalls.

Additionally, the reverse proxy service, required by the shared service platform for providing IPv6 connectivity to e-Government Web Portals, is also being monitored by means of Nagios.

Regarding MINETUR, the PaloAlto firewall records the traffic to both IPv6 environments created: pre-production and production. Logs are recorded in real time and will be further processed.

Turkish Pilot:

TURKSAT has been monitoring IPv4 networks and services using different tools such as Nagios, NfSen and Microsoft Scm. These tools are also IPv6-enabled. Required configuration has been made for these tools such as IPv6 addresses for services on monitoring tools. No challenge has been experienced during this process.

In addition, there exists a management room where the network and the servers are being monitored 7/24. For instance, PIBs have on their own alert systems for physical intrusion.

3.5.4 Management

German Pilot:

The management for Citkonn data centre operates as far as possible out-of-band, using an own physical infrastructure. This infrastructure is out of the scope of the project and shall be continued with IPv4 only. Due to the isolated character of the network, this will not affect the pilots other activities.

Spanish Pilot:

Regarding servers in connection areas, central management services are provided by means of Dell Remote Access Controllers (DRAC) version 4. This version does not support IPv6 since it was

included in version iDRAC6. They are not intended to be updated within the scope of the pilot, since they do not affect the capability of the network to support the provision of e-Government services in IPv6.

In the case of MINETUR, as the number of servers is not very big, they are managed locally.

Turkish Pilot:

TURKSAT network supports IPv6 for the time being. Servers and network appliances in the Turkish pilot are configured dual-stack. Therefore, the management of these devices can be made over both IPv4 and IPv6. Also monitoring software such as Nagios is deployed to ease the management of devices.

3.5.5 SNMP

German Pilot:

SNMP is not so much used in the Citkomm network. In the out-of-band management network IPv6 will not be seen during the next months.

And in this sense is the whole SNMP thing in this project: as no IPv6 only network is to be seen on Citkomm's horizon SNMP data can be fetched via IPv4 further on. The content of the SNMP data was not yet reviewed in relation to IPv6. Functional tests in the monitoring do not use SNMP for obtaining IPv6 service related information so far.

Spanish Pilot:

SNMP is currently used in Red SARA, together with other tools, to monitor the network and therefore all the nodes belonging to it support SNMP. By means of SNMP, different HW parameters (disk status, temperature, power supply, etc.) are controlled, as well as some services running in the servers, such as the clustering SW.

Within the scope of the Spanish pilot it is not expected to use SNMP over IPv6, so the IPv6 support required for the hardware regarding SNMP is the capability to provide information about IPv6 parameters when it is queried by the monitoring system using IPv4 as transport protocol.

Though the configuration of the SNMP systems to deal with IPv6 parameters has not been done yet, once the upgrading of the connection areas has been completed, it is intended to assess the current operation procedures based on SNMP in order to determine which modifications would

be required in the SNMP configuration due to the use of IPv6 traffic.

Regarding MINETUR, no SNMP management is used in IPv6 environments.

Turkish Pilot:

SNMP is currently used within TURKSAT network, where EGG is deployed, for monitoring the IPv4 network. SNMP is planned to be used for the IPv6 network as well.

On the backend communication which has been established between TURKSAT and the service provider institutions SNMP is not being used and it is not planned to be deployed within the pilot.

3.6 Security Aspects of Using IPv6

This chapter documents the security aspects of running an IPv6-capable network for e-Government services. Some of these aspects originate from the involved devices (e.g. firewalls), others from the use of IPv6 addresses. Finally, we emphasize that also non-technical aspects such as training for technicians as well as other employees are needed to keep the same level of security, as exists nowadays in an IPv4-only network environment.

German Pilot:

The autoconfiguration features of IPv6 will require some more attention for the things going on at the network level. Router discovery and address autoconfiguration may produce unexpected results and security holes in environments with unattended but IPv6 capable and enabled systems. Many systems deployed over the last years came with IPv6-enabled out of the box. In addition, there might be some test systems that received not so much attention so far as they could not connect to the world via IPv4. That could change with an IPv6 router on the network segment and SLAAC in operation.

Also the by default enabled IPv6 tunnels from Microsoft system attract more attention now. Other areas are better known from IPv4 and covered in the next sections.

The IPv6 implementation of OpenVPN is very similar to that in IPv4. This means that all routes and tunnels can be configured for IPv6 in a similar way as for IPv4.

In fact the dual-stack approach minimizes the effort for transition of security concepts, as in the process all security considerations can be transferred to IPv6 as a one to one image. As for IPv6 sometimes other tools and syntax must be used this lowers the risk of confusion and therefore

for security gaps.

Spanish Pilot:

The main security aspect of using IPv6 is the need of configuring properly the IDS/IPS systems and the firewalls. This is explained in more detail later.

Turkish Pilot:

Some points regarding the security aspects of using IPv6 have been described in Section 2.4. In this section security aspects regarding the generic services including DNS, load balancer systems and EGG Web portal will be shared.

3.7 Firewalls

German Pilot:

Of course, the firewalls had to be made IPv6 aware. In the case of Citkomm's Linux based firewalls this was an issue of updating the firewall management system running fwbuilder. Then new definitions and rule sets with IPv6 sections had to be created. The proper operation of the rule sets had to be verified.

The new protocol with its new special options and features will for sure need more attention as it comes in wider use. It can be expected that many new issues show up on the security level as IPv6 traffic will make up a greater share of the whole Internet traffic.

Fortunately, all rule sets are managed centrally. Therefore, the maintainers for the firewalls will have to be trained before the rollout of IPv6 to more than pilot customers will start.

Spanish Pilot:

As described in section 2.4.1, firewalls have been one of the elements more impacted in the deployment of IPv6 in Red SARA. Since IPv6 stack is completely different from the IPv4 one, the work of translating IPv4 rules to IPv6 can be tedious in some firewall products. Apart from the rules, it is also required to define new IPsec tunnels to accommodate the new IPv6 networks.

In the case of MINETUR, two firewall rules have been added (one per environment) to allow only IPv6 traffic through HTTP and HTTPS to the eITV service.

Turkish Pilot:

As stated previously all security devices (firewalls, IDS/IPSs etc.) have been configured to support IPv6 deployed in the TURKSAT network.

An increase in security incidents is expected as the IPv6 traffic increases. An important point is that network and system administrators should be aware of this fact.

3.8 Intrusion Detection/Prevention Systems

German Pilot:

Not to be published

Spanish Pilot:

As far as Red SARA is concerned, one point to highlight is the deployment of the new 2.9 version of Snort. Snort is the open-source IDS/IPS used in Red SARA connection areas⁵, and it reports data to CCN-CERT through the logging aggregator. This new version is able to analyse IPv6 traffic.

In the case of MINETUR, PaloAlto firewall has IDS capabilities. We are using these capabilities to block threats although no specific changes have been made for IPv6 environments.

Turkish Pilot:

Several IDS/IPS instance have been deployed within TURKSAT network. These include both hardware and software solutions. All instances are IPv6-enabled and the rules are updated to identify anomalies and attacks on the IPv6 network.

3.9 Application Layer Gateways (ALGs)

German Pilot:

As far as this is related to Citkomm, ALGs and Proxies are considered as one class of devices. The remarks to the proxies can be found there.

⁵For more information, see <http://www.snort.org/>

Spanish Pilot:

See description in section 2.4.2.

Turkish Pilot:

For the status of the Turkish pilot, there is no deployment of ALGs.

3.10 Proxies

German Pilot:

All affected proxies (squid, nginx, apache in proxy mode) had to be approved for IPv6 operation with or without possible IPv4/IPv6 translations. Subsystems like virus scanners must be included in these tests.

Moreover, especially all filter rule sets have to be checked for IPv6-awareness.

A special point is the Citkomm made local administrator's interface of the iWAN systems. This GUI still has to be extended to become IPv6-enabled and to offer the same opportunities for IPv6 as in IPv4.

Spanish Pilot:

See section 2.4.3.

Turkish Pilot:

No proxies have been deployed in Turkish pilot as an administrative decision.

3.11 Other Security Aspects

Spanish Pilot:

Regarding NAT64 security issues, a security policy forbids any kind of traffic from the Internet to go through SARA network. Therefore, when using NAT64 to enable IPv6 connection to web portals, traffic from the Internet is routed to IPv6 public addressing, so no data is transmitted through the SARA network in this case.

In the case of MINETUR, a log analyser has been installed. The firewall logs are sent to this system and are analysed and correlated to detect threats and attacks.

4 GEN6 SPECIFIC SERVICES WITH IPV6

4.1 German Pilot

This chapter takes a deeper, more technical look at certain network elements and servers of an IT infrastructure which are affected by a transition of e-Government services from IPv4-only to running IPv4+IPv6 support (from their users' point of view). These systems include network-level devices such as routers, plus auxiliary services like electronic mail and DNS, which are in direct or indirect use of the migrated e-Government services.

4.1.1 IPv6-Testbed

The test bed of Fraunhofer FOKUS allows testing of infrastructure devices in an IPv4-only, dual-stack and IPv6-only environment. The main goal of the performed tests lies in realistic end-to-end test scenarios.

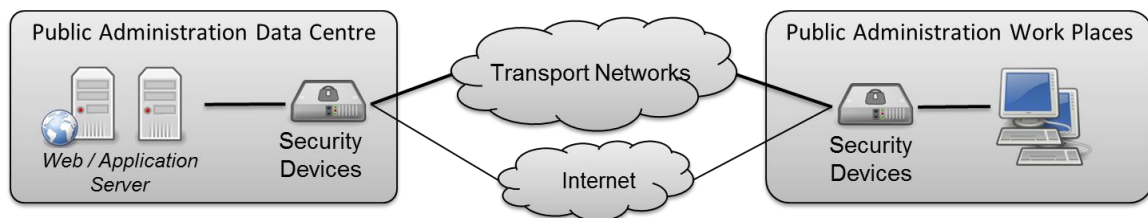


Figure 9 – Reference Architecture

The locally used test bed adheres to our reference architecture that is used to provide an environment similar to the ones used by public administrations in the field. In the practice of the test bed this includes not only the network structure and network elements but also typical end systems and installed software. This is shown in the following Figure 10.

Based on the performed application scenarios, one side of the setup will “play” the role of a public administration while the other side will play the “remote data centre” role. In this data centre we run the domain-specific applications that are accessed by the administration’s desktop computers. In this setup we can realistically evaluate hardware appliances as well as software applications in IPv4-only, IPv6-only and dual-stack environments.

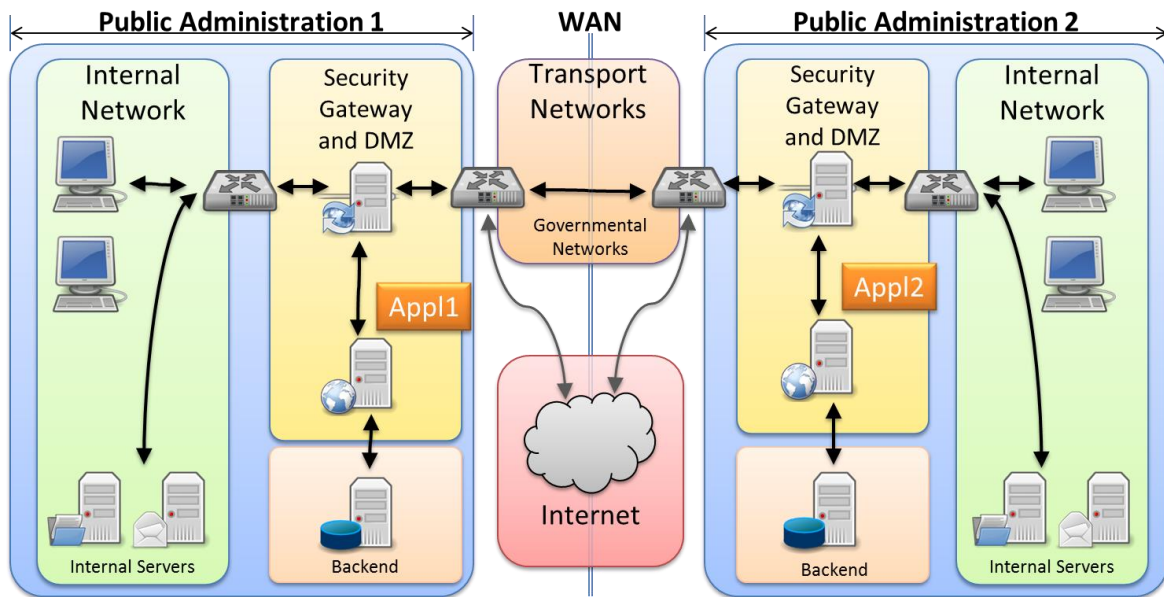


Figure 10 – Reference Architecture

4.1.1.1 Basic Use Cases

In our test environment we systematically performed the analysis of different communication patterns, depending on the device type, as there are:

- Inside to outside
 - Connecting from workplace systems to the Internet
- Outside to inside
 - Connecting from external clients to internal services (e.g. servers in the DMZ)
- Network Services
 - Communication to network infrastructure services (e.g. DNS)
- Management interfaces
 - Administrative access for configuration and management of devices
- Configuration of (Security-)Policies
 - Adaptation of existing policies and/or creation of new policies

4.1.1.2 Basic Approach

Our tests of hardware and software have been typically split into the following phases:

- Configuration IPv4-only
 - Where the starting point is the currently existing configuration
- Partial transition to IPv6
 - Transition of parts the network infrastructure; e.g. with IPv6 connections over IPv4-VPN-Tunnels
- Dual-Stack operation
 - Using IPv4 plus IPv6 across the whole network infrastructure as far as possible; with the mix of applications also using IPv4 and IPv6 in parallel in the network
- IPv6-only
 - Using no IPv4 traffic whatsoever in the network infrastructure

4.1.2 Test Setup

4.1.2.1 Adapted Use Cases

This work performs an analysis of application-relevant communication aspects, also tailored to the specific device type under test (where the device in our case is a special „VPN-box“ used by German administrations for secure LAN-to-LAN tunnels). This work consisted of:

- Installation and Base configuration of the VPN system via its management interface
 - Including network services such as LDAP and NTP
- VPN system management: Configuration of security relations between local and remote subnets
 - Including adaptation of existing policies or adding new policies (management permissions, filter rules, group policies) to reflect the current policies on IPv6
- Connectivity tests across the configured VPN

4.1.2.2 Approach

The following steps were taken while integrating the VPN systems into the FOKUS IPv6 test bed:

1. Configuration IPv4-only

Configuration of IPv4 addresses and communication relationships between IPv4 networks plus integration of VPN systems into the test bed

2. Dual-Stack operation

All active network interfaces and services (as far as possible) inside the test bed network are activated with IPv6 in addition to the above IPv4 configuration

3. IPv6-only

Disabling of IPv4 on all test bed components (hardware and software)

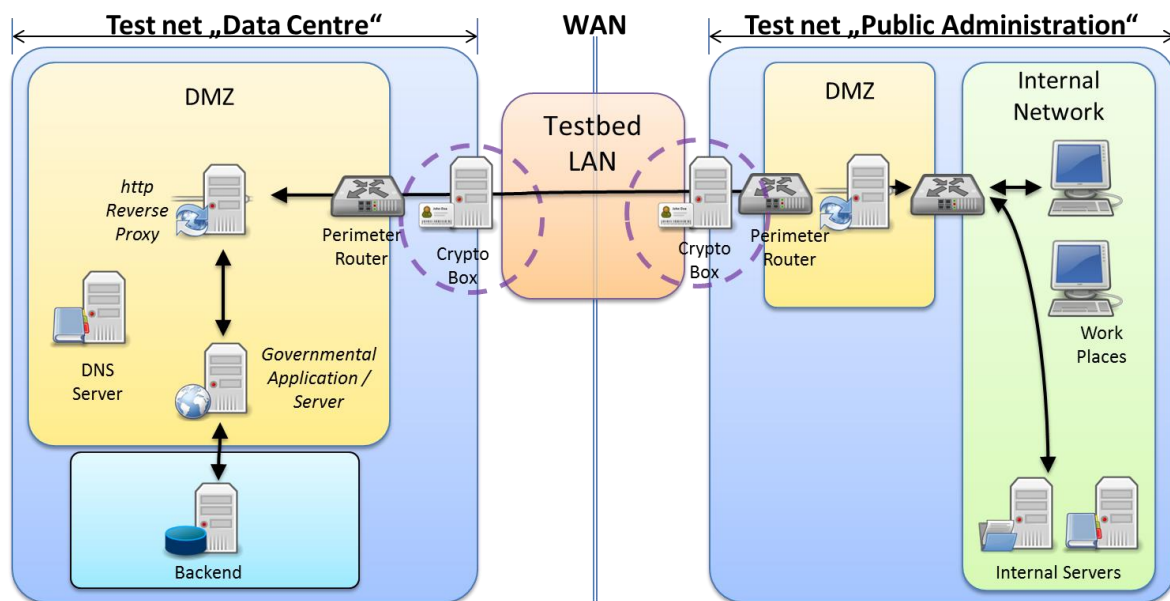


Figure 11 – Logical view of VPN systems and their management inside the FOKUS IPv6 testbed

4.1.2.3 Application scenarios

The following application scenarios were tested after each phase of configuration (see previous section). The focus of the testing is on the typical use of these VPN solutions with the German public administration's LAN-to-LAN VPN coupling.

The goal of the tests is running secure connections from one premise to another (remote one), across possibly insecure networks. The VPN system connects a LAN subnet on one side to another LAN subnet on the other side (contrary to e.g. VPN-secured dial-in connections). Therefore the main focus of our tests lies on the connectivity between these subnets, as well as application connectivity and performance between clients on one side and servers on the other side, across the encrypted VPN connection (using IPsec in tunnel mode). The allowed connections were guarded by the configuration of the security policies on the VPN systems on both ends of the secured connection. In these tests we did not check connectivity to or from the Internet, only government to government (G2G) use cases.

4.1.2.4 Management Interface

The VPN system is configured only using its own management software. This software has been installed in our test bed on a dedicated virtual PC (with IPv6 support). As part of the setup process, the used smart cards have been enabled by writing the target configuration on them. Those smart cards are the secure way of transferring the final configuration to the VPN systems. When booted with the correct configuration on the smart cards, the VPN systems could be enabled with online management functionality, which then allows for remote management using the VPN system's console.

4.1.2.5 Configuration of security policies

During the configuration and test of the different application scenarios, we also checked the usability of the management interface with regards to IPv4 versus IPv6 configuration. This means checking whether IPv6 rules will be added automatically, or a place-holder will be generated (and values asked from the operator) in the case of dual stack operation, or if IPv6 rules have to be added manually later on, after the configuration of the IPv4 rules.

4.1.3 Results

The results will be described in the following text, based on the different application scenarios. Since we are not going to describe in detail the concrete VPN system here from a specific manufacturer, these results should be viewed by the reader as a set of best-practices and what-to-take-care-of findings to be taken into account in general when running VPN systems' setup in an IPv4 plus IPv6 environment.

Note: To be sure whether IPv4 or IPv6 connections were used in our tests (e.g. by a web browser

application), we have used only literal IP addresses (IPv4 and IPv6) instead of host names.

4.1.3.1 Management Interface

Initially, the VPN system's management software had been installed inside a virtual Linux machine in the FOKUS IPv6 test bed. During installation it needs to be made sure that the machine's operating system, network configuration and the management application for the VPN system are IPv6-aware. Check with the manufacturer whether this is already the case (and just needs to be configured), or a newer version of the VPN system's management software is needed. With our system we noted that the documentation for the management software did not cover IPv6 configuration in a way that was fully consistent with the real software. So, some practical probing of the effective features of software for IPv6 configuration is always recommended, before recommending it to others. To our experience, the actual software is usually ahead of its documentation, i.e. can do more than is documented.

However, in our concrete case we could not setup a dual-stack configuration of the management interface using the graphical management software – if only because of the fact that only one IP-Address (IPv4 or IPv6) could be given in the configuration menu. If the management interface of the VPN system is indeed dual-stack reachable then the actual upload of configurations tries connecting via IPv6 first and then (if IPv6 fails) via IPv4.

4.1.3.2 Configuration of (Security) Policies

For configuring security policies (and security associations between coupled subnets) we also tried a partial transition, i.e. coupling networks with IPv6 traffic across IPv4 networks (IPv6 in IPv4 packets), and vice versa (IPv4 over IPv6 networks). In our experience this works quite as expected, in both cases. We only noticed that the user interface one could also try to couple an IPv4 subnet with an IPv6 subnet, which will not work due to the incompatibility of the IP protocols. Only when the configuration of all coupled networks was set to final, the user interface would issue an error message. Sometimes, also the default selection of a subnet on the other side of a VPN tunnel was suggesting a network of the wrong IP type. This could be fixed easily during the configuration, but could be avoided by the user interface in the first place.

4.1.4 Evaluation of the Results

The used VPN system's tunnelling functionality has been proven capable for IPv4-only, IPv6-only and dual-stack operation mode in our tests in the FOKUS test bed.

Yet, all its functions are configured over its proprietary management software – and this software (not the VPN box itself) showed some drawbacks, mainly related to dual-stack configurations, e.g. the fact that management server could not be configured over the user interface with IPv4 and IPv6 addresses. Secondly, the automatic selection for IP subnets on the remote side would always default to selecting an IPv4 subnet, even in the local subnet was an IPv6-only network.

Finally, the installation process of the management software was somewhat tricky, due to somewhat dated installation documentation. When running such systems one should always contact the manufacturer and ask (or download) the very latest documentation for it, since the (possibly printed) documentation that is delivered together with the system may not yet reflect all the features of the system with regards to IPv6, especially when the IPv6 support in the system is much “younger” than the IPv4 support, as it is the case with most systems (to our experience).

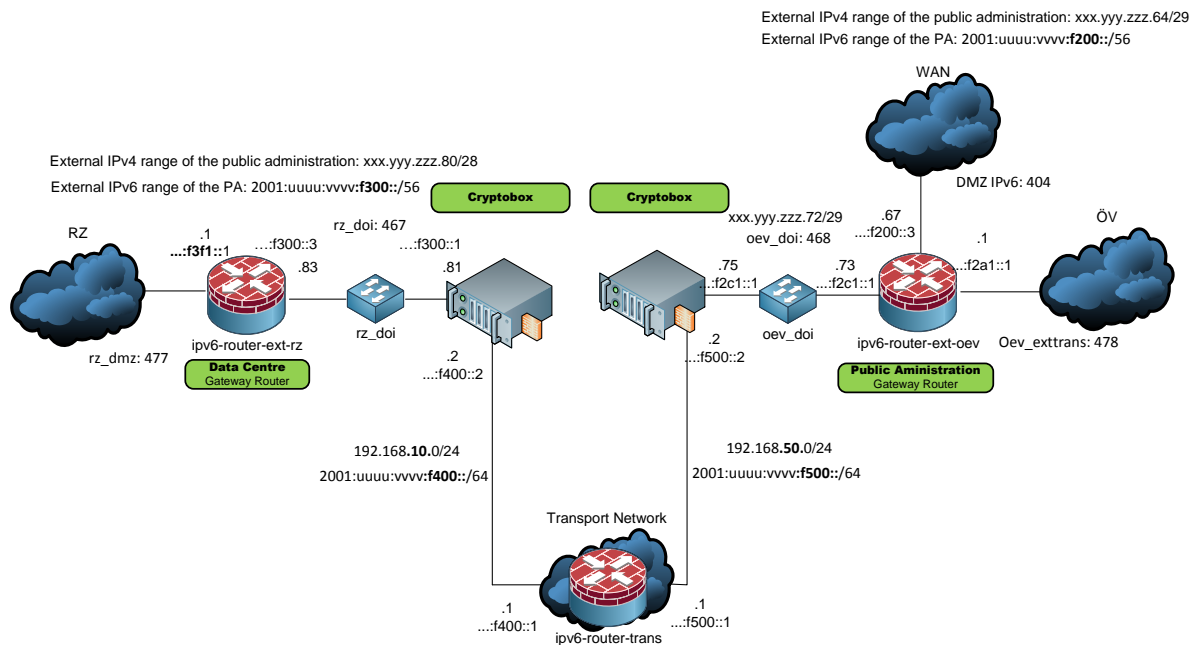


Figure 12 – Testbed configuration

4.2 Spanish Pilot

One of the purposes of the Spanish pilot is the use of IPv6 connections between different government departments. All these departments communicate with each other through a network called RedSara (SARA Network), which has been updated to transport IPv6 natively.

In this pilot, as a demonstration of enabling IPv6 e-government services between different government units, eITV application, related to the registration of a motor vehicle, has been

selected. The Ministry of Industry, Energy and Tourism (MINETUR) provides eITV application to another administrative unit of another ministry, the DGT (Directorate General for Traffic) as well as vehicle manufacturers.

4.2.1 eITV application description

eITV replaces the traditional paper-based ITV card (Vehicle Technical Inspection card) with an electronic card and all face-to-face procedures required for registering a motor vehicle by electronic procedures.

The eITV application consists of the management of eITV cards made by the Ministry of Industry, Energy and Tourism. The Ministry provides the necessary tools to vehicle manufacturers and DGT for the request and query of the eITV cards.

It is a web application with public and private part and a web service for data exchange that uses digital signatures to ensure authentication, integrity and non-repudiation. The information sent is stored in electronic records.

The necessary steps are:

- ITV electronic cards are requested and created.
- The Ministry authorization process is fully electronic.
- The eITV card is electronically sent to all stakeholders (Ministry, DGT, vehicle manufacturers, etc.)
- The electronic matriculation procedure includes the acquisition by manufacturers of electronic cards issued by the Ministry. These cards are filled with information of the vehicle by the manufacturer and send to MINETUR and DGT for further registration.
- The matriculation process by the DGT is fully electronic.

The flow of data exchanged for the registration of a vehicle is as follows:

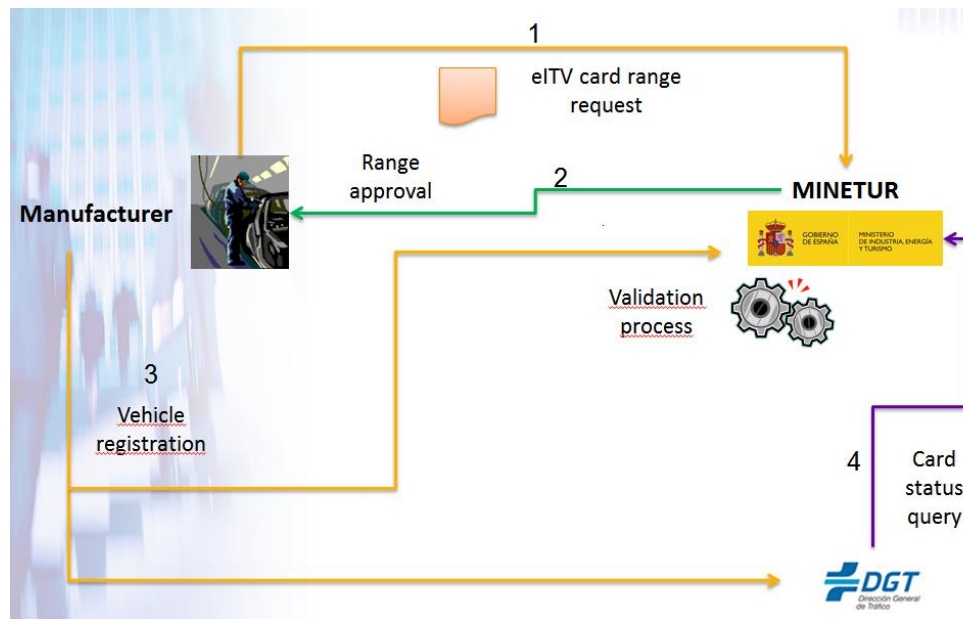


Figure 13 – eITV application data flow

1. eITV card range request. Manufacturers ask MINETUR for eITV cards ranges.
2. MINETUR grants eITV cards ranges.
3. eITV cards are filled by manufacturers with vehicle information and data are sent to MINETUR and DGT simultaneously.
4. Both MINETUR and DGT check the cards sent. For that reason, DGT will query the MINETUR data.

As a result of the fully electronic procedure, the following benefits occur:

- Saving time and money in the process of registration.
- Safety in the transmission of the data (errors and fraud are avoided).
- Quality of data stored for query and reference.

4.2.1.1 eITV application users

You can access the application in two ways: through the classic user / password system and using digital certificate as shown in the following screen:

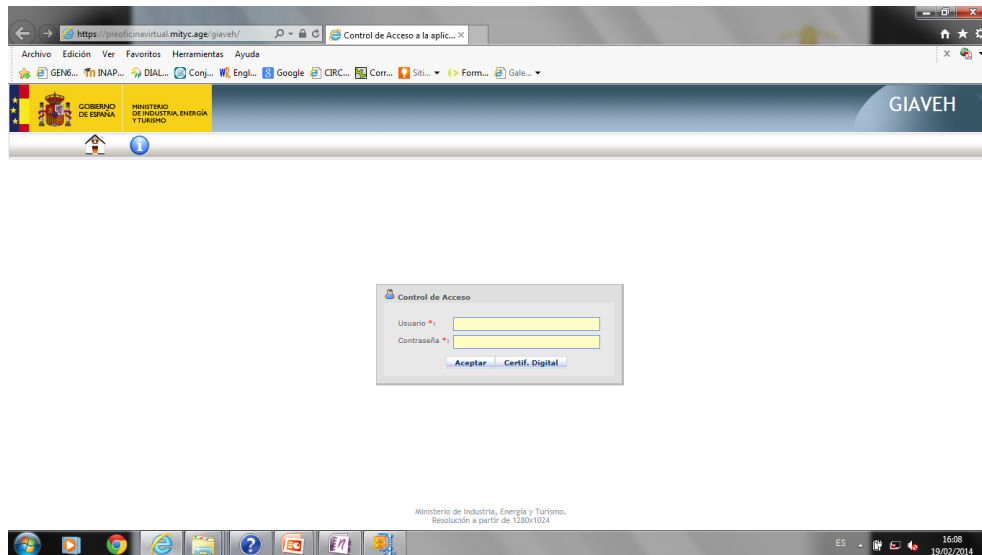


Figure 14 – eITV access screen

Once inside, the processes are different for each type of user:

- External users (vehicle manufacturers). They may request eITV cards, check the status of cards requested and send data with information of the vehicles for registration to MINETUR and DGT.

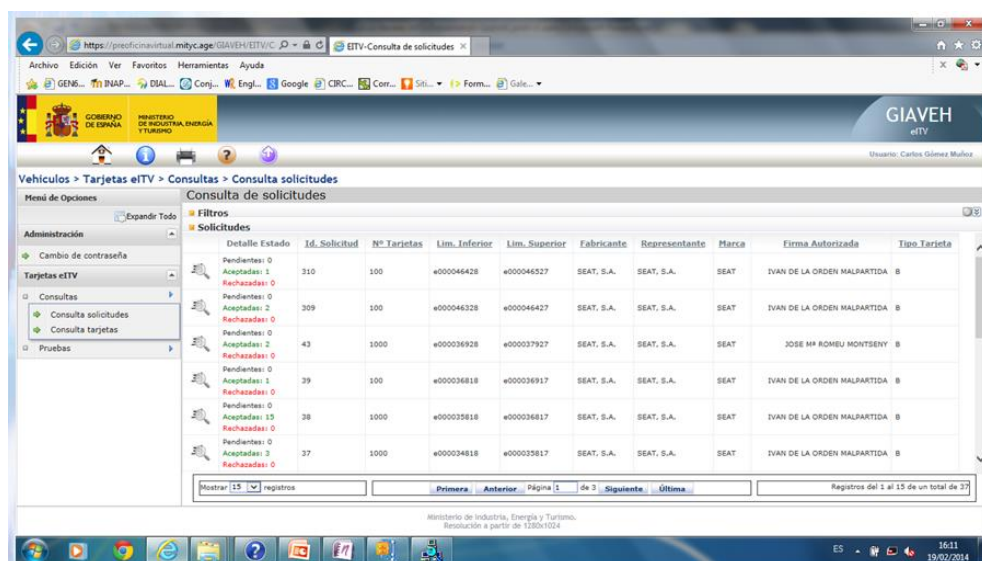


Figure 15 – eITV card range query

- Internal users (MINETUR). They will access management options and application control as well as validation of electronic cards requested by the manufacturers.

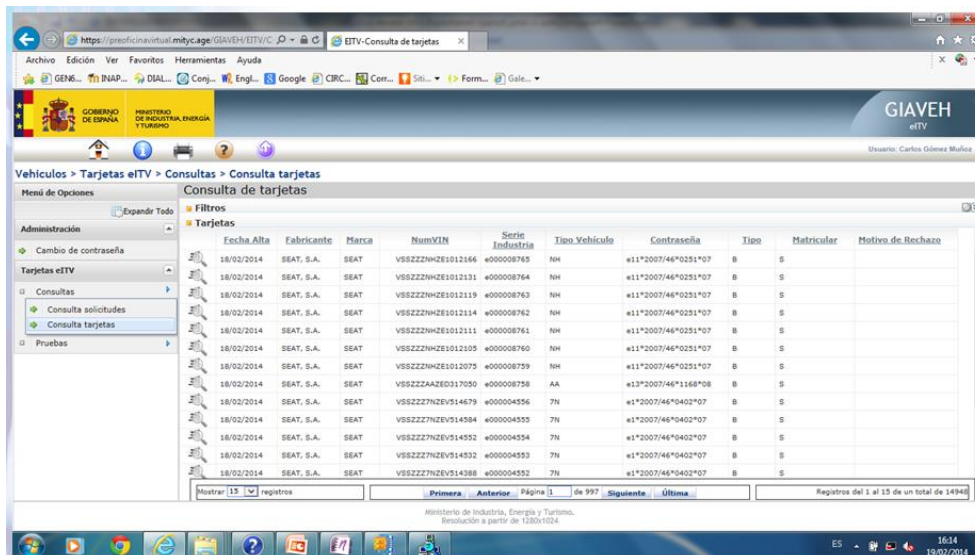


Figure 16 – eITV card authorization query

- Government users (DGT). They can check the status and data of the electronic cards sent by the manufacturers.

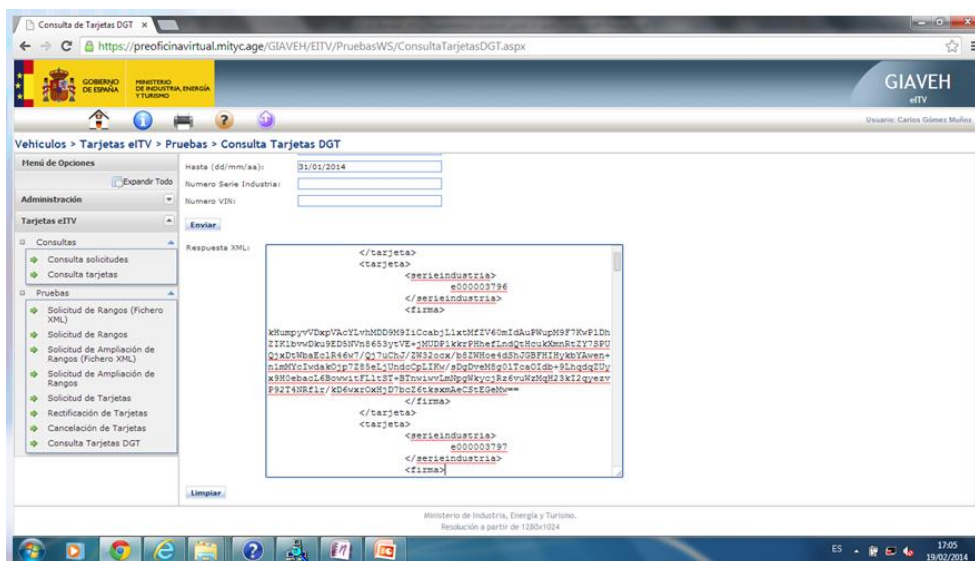


Figure 17 – eITV card status query for DGT

The following figure shows where the different types of users are located within the scheme of the infrastructure required by the application and the different protocols used by each of them to access the system.

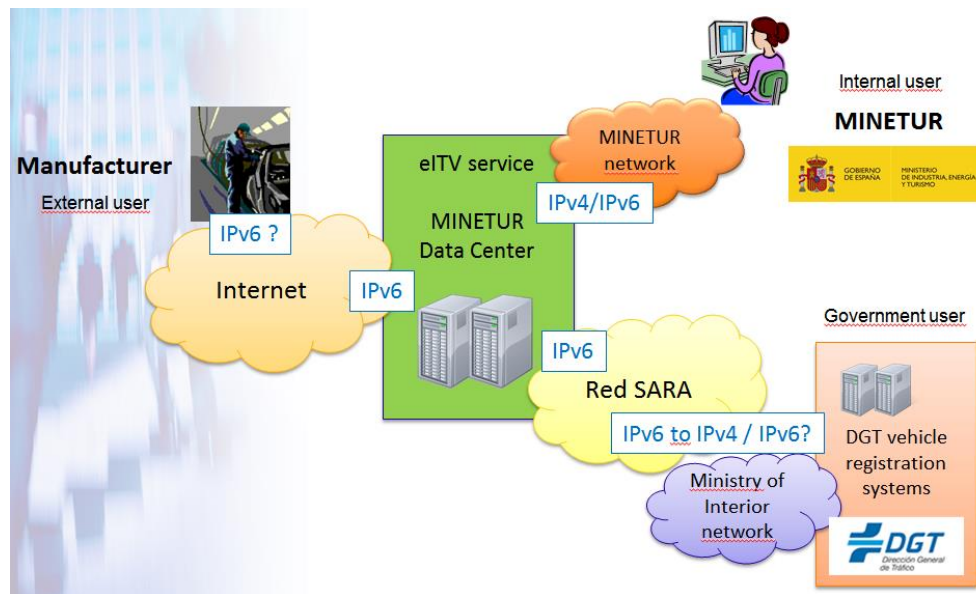


Figure 18 – Users of the system and protocols used

As seen in the figure, we have no certainty whether the manufacturers are going to use IPv6 protocol or not. It is not in our hands but we are having contacts so that they use this protocol.

Regarding the internal users, our internal network is IPv4. The users are able to access eITV using IPv6 only from specific subnets on our data centre or by means of a portable computer configured with IPv6 and connected through our Wi-Fi connection that is able to serve IPv6 addresses with DHCPv6.

Concerning the DGT users, this department belongs to another Ministry and the data must pass through a network where IPv6 is not implemented. We are in contact in order to use IPv6 end-to-end connections.

4.2.1.2 Infrastructure and software used by eITV

The general outline of the infrastructure used by the eITV application is:

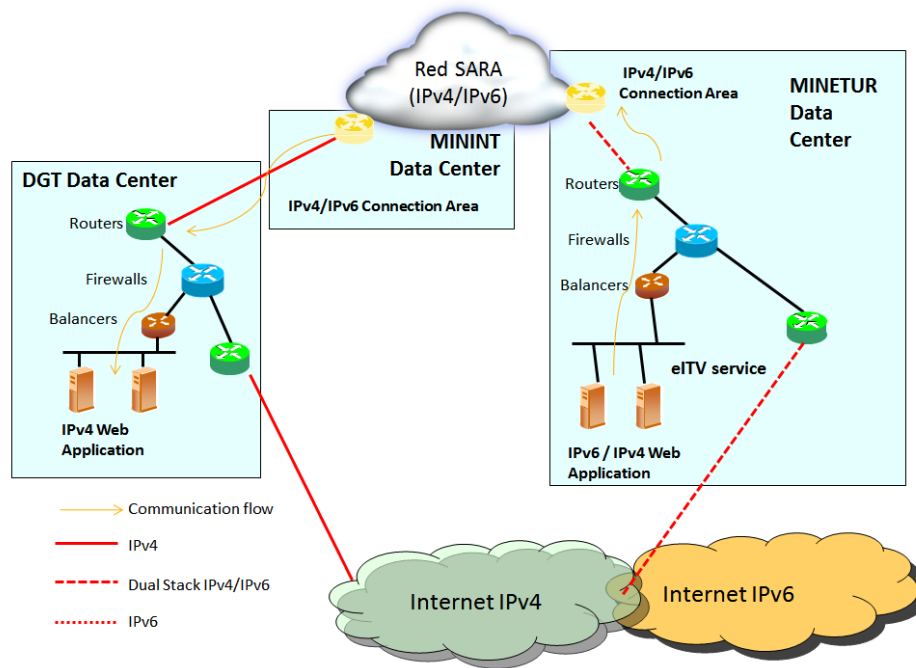


Figure 19 – Reference architecture

As we can see in the figure, the communication between the data centre of DGT and MINETUR will use the connecting areas between ministries that SARA Network provides.

The connections from the Internet will be made by vehicle manufacturers to communicate with MINETUR and DGT.

eITV is a web application with a web service for data exchange. It uses .NET Framework 4.0 and the database is Oracle 11 G R2. The application servers are Windows 2008 Server 64bit with IIS 7.0.

4.2.2 Security policies

Our security policies relays mainly in our firewall. Firewall rules have been added to allow only IPv6 traffic through HTTP and HTTPS to the eITV service.

We have taken advantage of the IPS capabilities of the firewall as well as the malware and antivirus detection. We are using these capabilities to block threats although no specific changes have been made for IPv6. The firewall logs are also analysed and correlated to detect threats and attacks.

The use of digital certificates when data is exchanged between different users of the application guarantees the integrity and security of data.

4.2.3 Evaluation of the Results

No problem with commercial products needed to implement eITV application. They all are adapted to IPv6.

Initially, eITV application was developed for an IPv4 environment. Therefore, the transition to an IPv6 environment has required the review and adaptation of the source code.

The problems have been similar to those of IPv4. The difficulties found have not been too great since some basic considerations have been taken into account as the exclusion of IPv4 addresses in the program code and the use of stable identifiers to connect to other nodes (host names resolved by DNS).

4.3 Turkish Pilot

Turkish e-government Gateway (EGG) is composed of a web portal which is serving approximately 1000 services to more than 18 million citizens and the backend connections to the respective governmental institutions. Hence, Turkish pilot consists of two main phases. First phase of the Turkish pilot includes the IPv6 transition of EGG portal which is the frontend of EGG. This phase has been successfully completed through the first year of the project. Second phase of the project is to make the backend communication between TURKSAT and the selected service provider governmental institutions IPv6-enabled.

Turkish EGG is designed to serve millions of users via high available architecture. This brings many different challenges and complexity to be managed so usage of industry standard equipment and software is important. Hence, vendor produced and licensed applications are preferred rather than in-house produced scripts and applications which will be programmer dependent.

4.3.1 Certification

One of the main components of the Turkish pilot is the EGG web portal which should comply with standards defined for W3C Web Content Accessibility Guidelines and Ergonomics of human-system interaction. For this purpose TURKSAT has applied for the following standards and Turkish EGG web portal has been approved for satisfying the appropriate standards.

- ISO 9241-151:2008 Ergonomics of human-system interaction -- Part 151: Guidance on World Wide Web user interfaces
- ISO/IEC 40500:2012 Information technology -- W3C Web Content Accessibility Guidelines

(WCAG) 2.0

Tests have been carried out by Human-Computer Interaction Research and Application Laboratory (<http://hci.cc.metu.edu.tr/>) in Middle East Technical University which is one of the leading universities of Turkey. Through accessibility tests communication over IPv6 has been tested and the results are successful.

4.3.2 Logging

In EGG, logging is one of the building blocks in order to keep the system secure, manageable and accountable. Enabling IPv6 on services and portal caused the upgrade of commercial logging server solution to support IPv6

Throughout the Turkish pilot security configurations has been updated to support IPv6 as well. In general these configurations include firewall rules or access control lists. Specifically for Turkish pilot user access logs are kept for forensics purposes. Through the Turkish pilot these logs have been made IPv6-enabled. Small in-house developed web scripts are also patched to support IPv6 like script that shows the users last 3 login IP addresses on login web page.

4.3.3 Testbed

As Turkish EGG has a complex structure it is difficult to make a testbed to represent all the operations taking place. Besides, as most of the institutions do not have a test service that TURKSAT test service can interact, simulating communications between TURKSAT and remote institutions and setting up a production level testbed for EGG is not feasible. However TURKSAT has setup a local testbed where tests have been launched for new applications, software and hardware.

4.3.4 Public Integration Box

On the backend of the Turkish pilot there exist VPN connections between TURKSAT and the remote instructions. In order to decrease the setup effort TURKSAT has developed a plug-and-play hardware which enables VPN tunnels (both IPv4 and IPv6) between end points. These boxes (aka Public Integration Boxes) have been deployed in the remote sites throughout Turkish pilot. During the development progress, the box was designed to be IPv6 enabled.

4.4 Luxembourg Pilot

4.4.1 Description of the service

The University Of Luxembourg (UL) has developed a pilot together with Citkomm in order to support local elections in Germany. This pilot is the first of its kind to combine cloud computing and IPv6, and moreover to integrate a cloud deployment into a production infrastructure in order to serve peak traffic. It has successfully managed to serve IPv6 traffic on the first election round on May 25th: 5% of the total traffic was over IPv6 and it passed through the IPv6-only cloud servers at UL during the initial Election Day. The same setup was used in a second election round on June 15th 2014, and it served up to 2% of the total traffic.

The service that is supported by the pilot is the election website presentation. Throughout the election days, citizens of various municipalities in North-Rhine-Westphalia could access the current voting count on a Citkomm-hosted website (<http://wahlen.citkomm.de/>). The backend web server for this website has traditionally been IPv4-only, and with this pilot the intention was to showcase two novelties at the same time:

- IPv6 enablement of website needed especially by those citizens accessing it from premises that are IPv6 connected.
- Cloud computing assurance (availability, resilience and scalability) when it comes to handling large amounts of user traffic.

In terms of the implementation, this pilot featured several elements:

- The use of the OpenStack Havana open-source cloud computing distribution that was fully adapted to support IPv6. Note here that IPv6 support is not yet official.
- Intensive testing phase that covered heavy load generation.
- QoS monitoring during test and production phase, complemented by extensive data collection of different kinds:
 - User-level data elicited from monitoring web site performance from various locations in Europe and abroad.
 - Hypervisor data, elicited from monitoring the way the hosting cloud platform reacts to increasing loads on the resources allotted to the application running on

top of it.

- Hardware data, elicited from monitoring the load of the bare metal resources hosting the cloud operating system that in its turn hosts the high-level application.

The architecture of the testbed is shown in Figure 20. The lower part of the diagram shows the cloud infrastructure as a private virtual network hosting several Ubuntu virtual machines (VMs), of which two are Citkomm’s website servers. These two VMs have IPv6 addresses and are hence reachable from the outside, and can be configured from within the Citkomm backend network. The middle part of the diagram shows the physical servers at UL that host the virtual network in the cloud, and their connection with the outside world via dual IPv4-IPv6 connectivity.

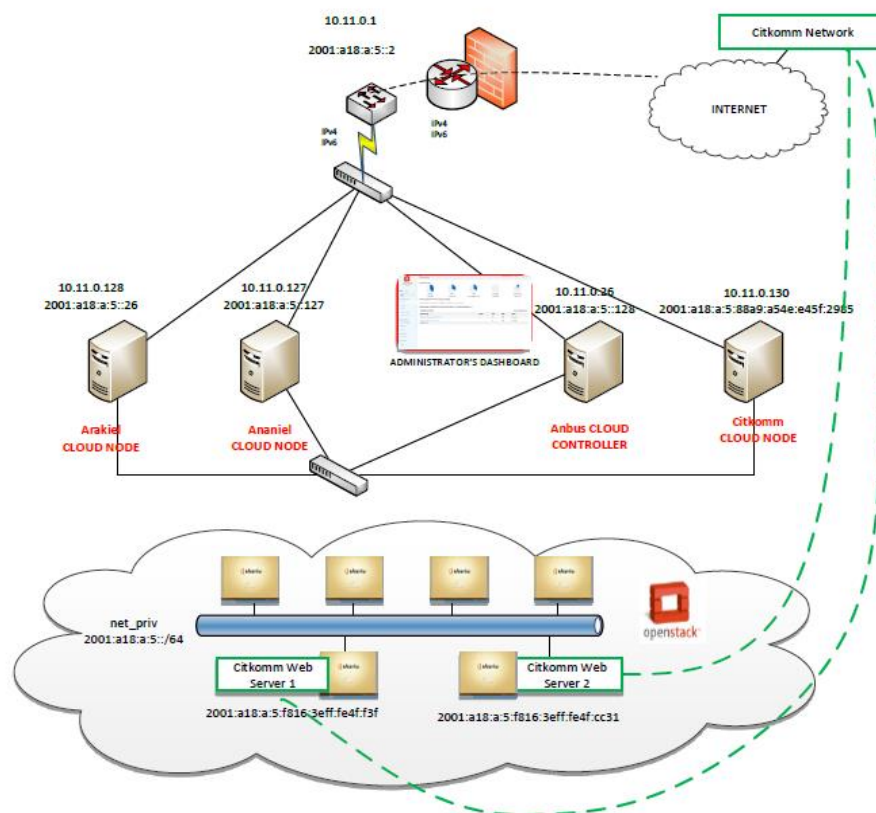


Figure 20 – Reference architecture for UL-Citkomm pilot

In Figure 21 we can see the integration of the two sites – one in Germany (hosted at QSC) and the other one in Luxembourg – within the same infrastructure used in the election presentation. As mentioned before, the Luxembourg infrastructure was IPv6 only, and it was fully integrated in the DNS entry with a central URL (wahlen.citkomm.de) for all servers. All citizens accessing this URL via IPv6 were directed to the Luxembourg servers, while all the others, to the QSC site.

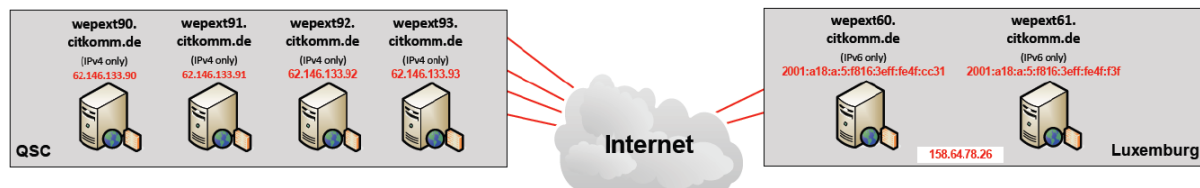


Figure 21 – Integration of the machines in Luxembourg and Germany in the same testbed

The two main pilot objectives – to enable existing e-government services with IPv6, and to handle peak loads on existing applications with the support of cloud computing – have been achieved so far.

4.4.2 Transition to IPv6

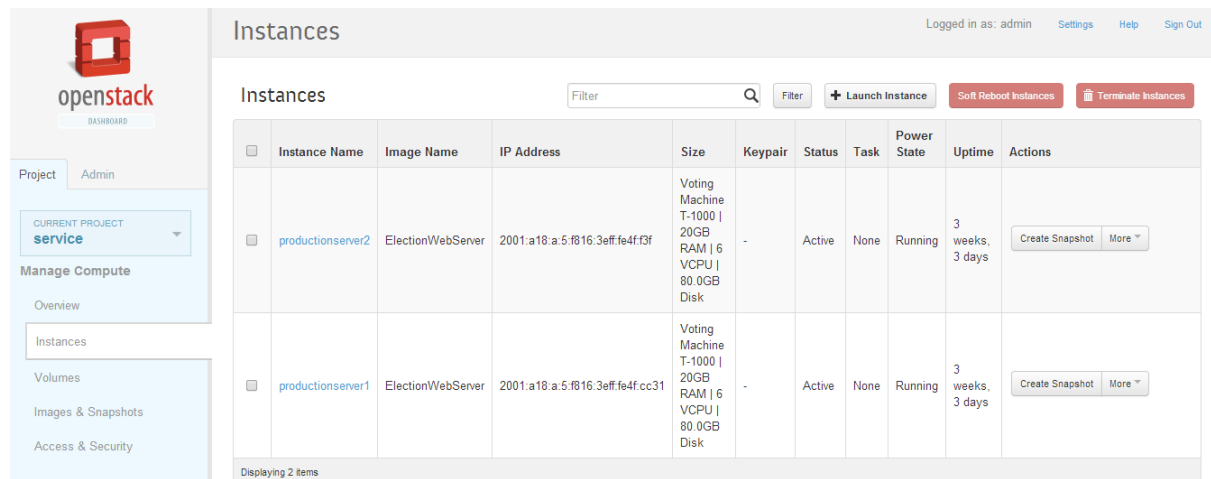
There are clear advantages of cloud infrastructures on IPv6. The addressing space being large, there is more room for addressability of resources in the cloud. Virtual networks and resources can be managed easier, because they can be added, removed or changed easily.

As mentioned earlier, the integration of IPv6 in OpenStack is not yet officially achieved in the open-source community. At UL, the OpenStack Havana testbed has been patched for full IPv6 support with the help from Nephos6, a company in the US. All details of the patch can be found in a previously published whitepaper⁶, while here we only give a few pointers on the biggest shortcomings that were addressed by the patch:

- Router advertisements were not being sent properly between routers and virtual networks, and consequently traffic from virtual networks would not reach IPv6 routers but rather OpenStack's DHCP servers.
- Duplicate address detection had to be turned off at interface level, to bridge a potential kernel bug generating "IPv6 duplicate address detected" messages in the VMs running Ubuntu 13.10 / 64 bits.
- Generation of SLAAC IPv6 addresses and configuring IP6Table rules

With the patch in place, we could launch virtual machine instances with native IPv6 addresses, as shown in the screenshot below.

⁶ <http://www.nephos6.com/pdf/OpenStack-Havana-on-IPv6.pdf>



Instances

Logged in as: admin [Settings](#) [Help](#) [Sign Out](#)

Instances

<input type="checkbox"/>	Instance Name	Image Name	IP Address	Size	Keypair	Status	Task	Power State	Uptime	Actions
<input type="checkbox"/>	productionserver2	ElectionWebServer	2001:a18:a:5:f816:3eff:fe4f:f3f	Voting Machine T-1000 20GB RAM 6 VCPU 80.0GB Disk	-	Active	None	Running	3 weeks, 3 days	<input type="button" value="Create Snapshot"/> <input type="button" value="More"/>
<input type="checkbox"/>	productionserver1	ElectionWebServer	2001:a18:a:5:f816:3eff:fe4f:cc31	Voting Machine T-1000 20GB RAM 6 VCPU 80.0GB Disk	-	Active	None	Running	3 weeks, 3 days	<input type="button" value="Create Snapshot"/> <input type="button" value="More"/>

Displaying 2 items

Figure 22 – Instances with IPv6 addresses in OpenStack Havana (UL testbed)

4.4.3 Monitoring considerations

It is essential for the infrastructure/service provider (e.g. the administration) to have detailed and timely control over the system, in order to be able to react to events as soon as possible. Activity and traffic monitoring are essential, in that sense, for event management and advanced reaction: For example, identification of denial for service attacks needs to be done as soon as possible and an appropriate system mitigation to be taken, in order to minimize the impact of the attack and suppress further exploitation. Recognizing security events as soon as possible implies runtime monitoring of the infrastructure: for example, is the DNS handling the load now? Are the virtual machines hosting the election website handling the load? If they are not, is it a web server problem? Is the hypervisor or the network service overloaded?

Monitoring of the runtime system is already provided in OpenStack since versions earlier than Havana. The cloud administrator can use the dashboard offered by Horizon, the presentation server in OpenStack. The figure below shows what the administrator can see in the dashboard of the managed project: an overview, in this case, of the instances (number of virtual machines currently deployed), virtual CPUs of the compute server, the current amount of RAM used of the total available amount, the security groups and the virtual IPs (called “floating IPs”) if any were used in the project by the instances.

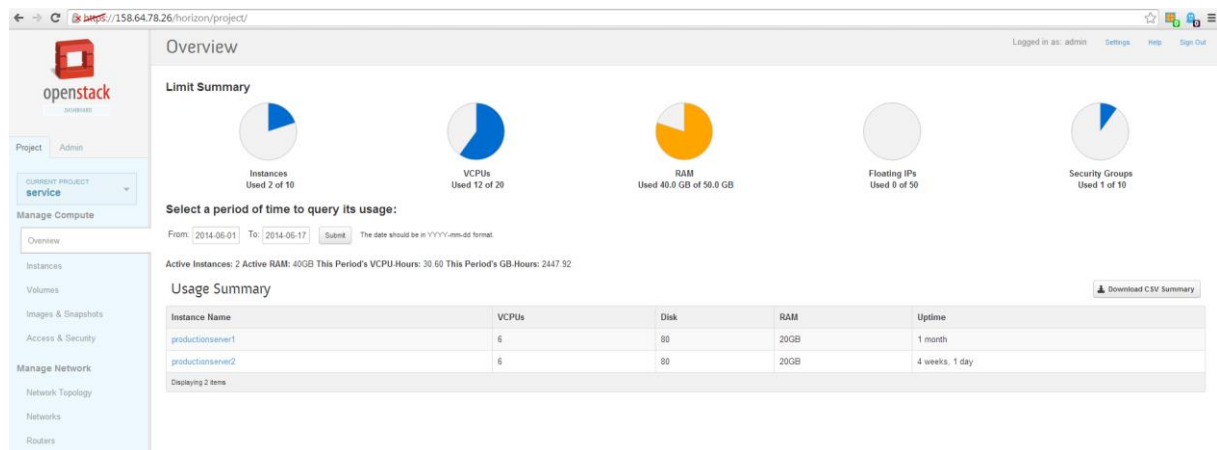


Figure 23 – The dashboard in OpenStack's Horizon

Equally, this graphical interface can show the network topology for the virtual networks hosted by OpenStack, some security features related to the firewall (see Figure 24 Firewall rules in the OpenStack election setup) as well as the access control to the projects, graphical interface, VMs and OpenStack resources.

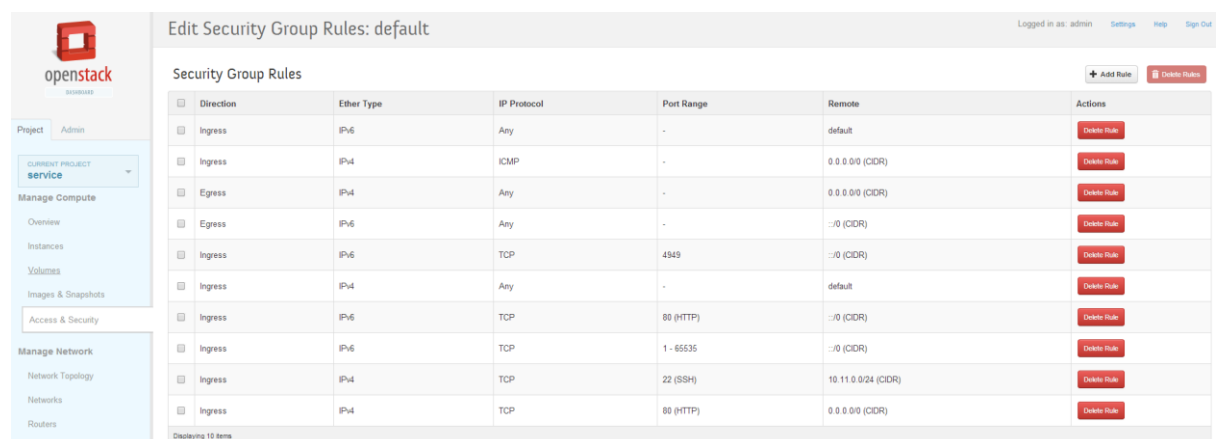


Figure 24 – Firewall rules in the OpenStack election setup

For a better idea of the actual resource usage, runtime monitoring for the current cloud infrastructure was done at several layers:

- Infrastructure-wide for the entire election infrastructure, done by Citkomm.
- Hypervisor level from OpenStack's resource statistics service, for the UL cloud setup, which was part of the Citkomm election infrastructure. This is shown in Figure 27 and Figure 28.
- Virtual Machine level, from Munin running in the election VMs on top of OpenStack. See

Figure 29 for this information.

- End-user level, running from the Internet and measuring the user-perceived performance of the application. See Figure 25 and Figure 26.

The end-user monitoring involved the use of v6sonar agents provided by colleagues from Nephos6, a set of scripts running at several locations: one in Luxembourg, and two in Germany. Thanks to Nephos6's dashboard specially adapted for this setup, Figure 25 shows how potential end-users could experience the election website on May 25th, between 1:20 pm and 2:15 pm. The performance measurement agents would look at ping and http requests when retrieving the election website index. The election website was periodically updated throughout the Election Day, in order to show the current voting count per each municipality included in the elections. The VMs had only IPv6 addresses, as mentioned earlier. Their overall performance before and around May 25th is shown in Figure 26. In our setup it is also possible to separate how the traffic was split to the virtual machines.

We believe that by providing detailed data at different levels at application runtime, we can provide valuable monitoring information that the infrastructure provider/administrator can use to identify security events, together with their causes and possible suitable remediation.

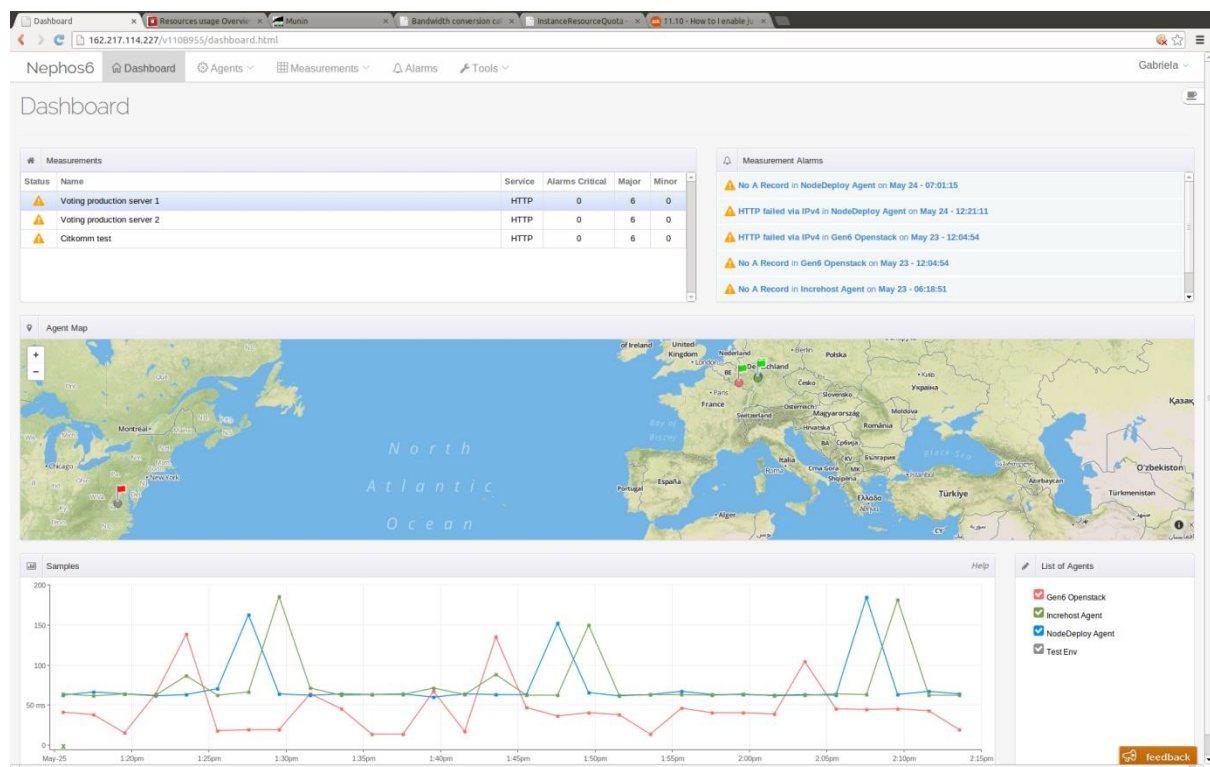


Figure 25 – User-perceived performance (blue and green lines) against local performance (red line)

The previous figure showed the user-perceived performance (blue and green lines) against local performance (red line) of the election website on the Election Day. The website was hosted on two virtual machines using an OpenStack setup hosted at UL.

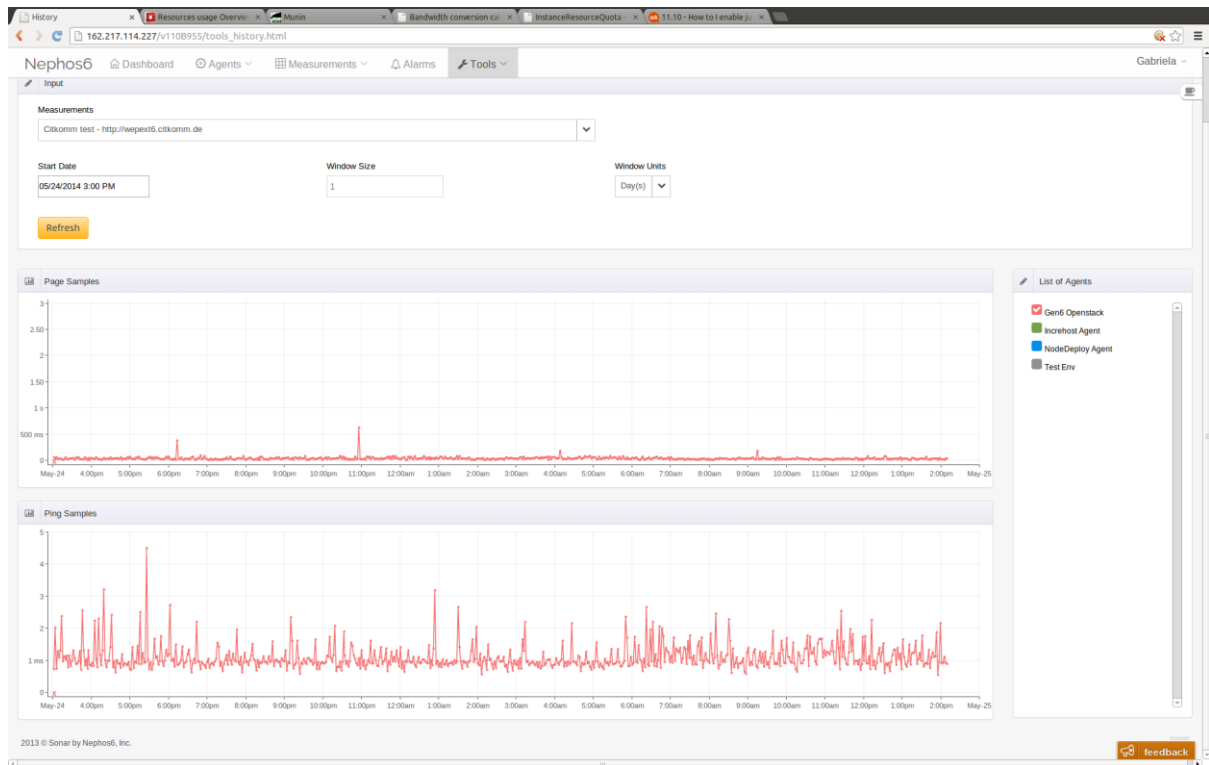


Figure 26 – Performance of the election website on IPv6, for one day starting from May 24th at 3pm

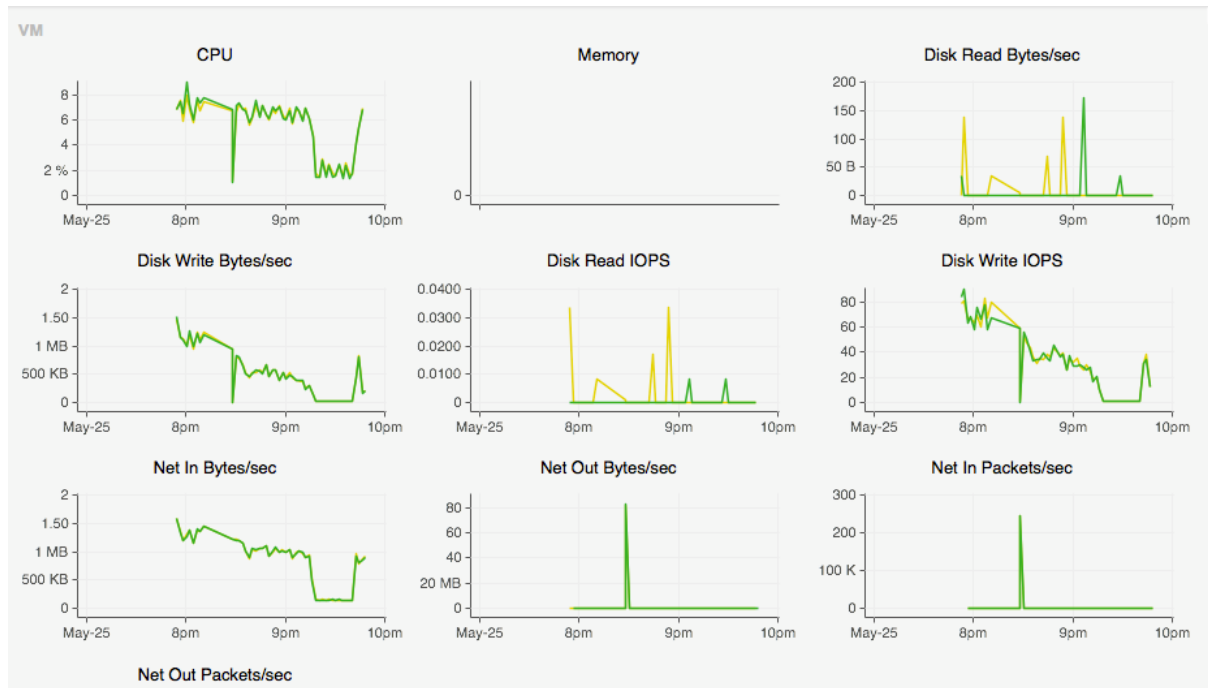


Figure 27 – Parameters of two VMs hosting the website on IPv6, on the evening of the Election Day

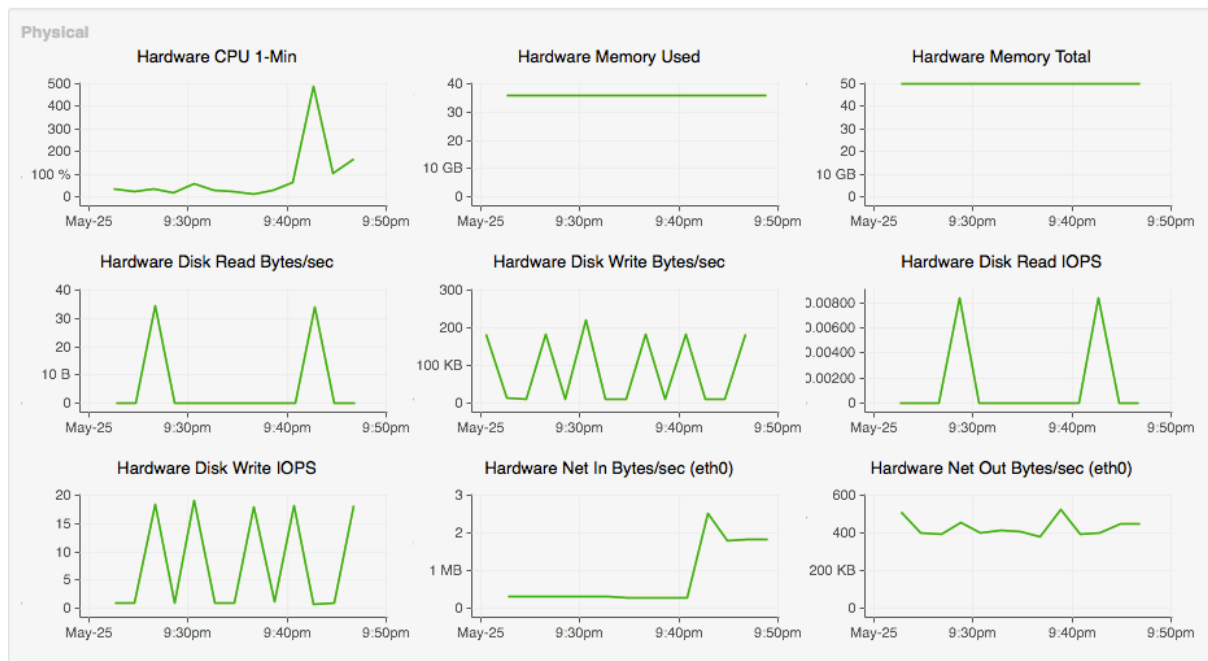


Figure 28 – Hardware resource usage for the testbed at UL, on the election evening

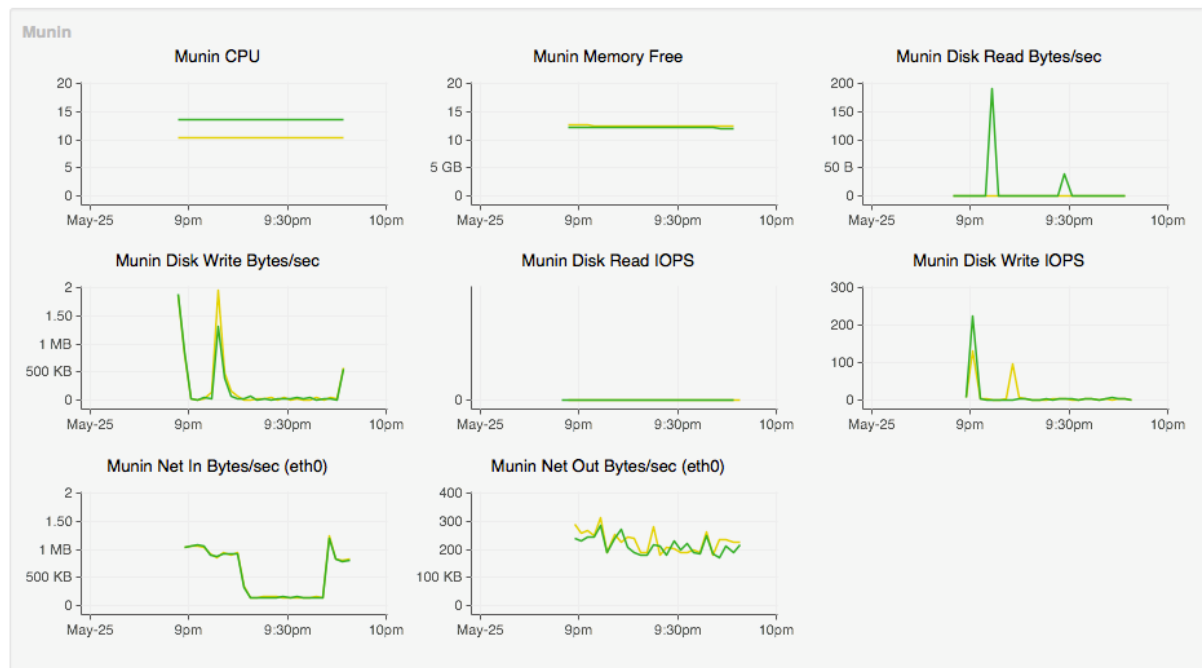


Figure 29 – The evolution of the VM performance for two VMs on the election evening

The figures above show various graphs that a system administrator or manager can see in the dashboard. The information covers the following performance aspects of the cloud infrastructure:

- Per each virtual machine (one drawn in green and another in yellow⁷), the amount of CPU, memory, disk read and disk writes, network in and network out bytes or packets (Figure 27)
- Hardware resource usage (CPU, memory, disk read, disk write, network in and out) at the level of the hypervisor of OpenStack (Figure 28)
- Internal to each virtual machine, another set of statistics on the CPU, Memory, disk read and write, and network in and out. These statistics are gathered by means of Munin⁸, a known system monitoring tool (Figure 29).

⁷Sometimes the green line covers up the yellow one in the drawing so that just the green one is visible.

⁸Munin, an open-source networked resource monitoring tool, <http://munin-monitoring.org/>.

5 SUMMARY OF LESSONS LEARNED

5.1 Network Design and Structural Level

5.1.1 Spanish Pilot

Since a significant part of the Spanish pilot is focused on the deployment of IPv6 not in the network of one governmental unit, but in Red SARA, the network that connects the different Spanish administrations and provides shared services to them, one of the main lessons learned has been that there are important differences in the transition to IPv6 between both cases. These differences are not so related to technical issues as to organizational and coordination issues. In that sense, addressing is one of the key elements, due to the complexity of obtaining large IPv6 spaces, so planning for temporary IPv6 assignments while managing the process of getting the permanent ones may be a good practice for fostering the transition.

Maintaining the current network architecture and trying to reflect the previous IPv4 addressing plan structure into the new IPv6 addresses has proved to be a good approach to reduce the complexity of the transition in this initial stage.

It is also good to consider in advance that probably different transition mechanisms will have to be deployed in order to have the services ready in IPv6. Though dual stack should be the preferred approach, tunnels cannot be avoided in some cases when networks must connect through non IPv6 ready infrastructures, something that it is not unusual since many telecom operators do not offer IPv6 transport yet in all their networks. IPv6-to-IPv4 translation, on the other hand, can be an effective means of achieving IPv6 visibility from the outside world without devoting too much effort, and should be evaluated as an option, at least in the beginning.

Finally, it is also important to define clearly which equipment and software that does not support IPv6 should be really upgraded or replaced in the transition. A reasonable approach is focusing initially on those elements that are essential to provide IPv6 transport capabilities, while leaving in IPv4 the ones that do not, such as those that support network operation.

5.1.2 German Pilot

As the German pilot aims the transition of an existing network no changes in network design have been implemented in the first transition phase. As there always was a dual stack solution implemented this approach had the essential advantage, that the IPv4 network could be operated as before. The IPv6 roll out was independent to this operation as it handles on a

different protocol, that sometimes is still handled by different daemons. There are still considerations for a redesign of some network areas, but as this always needs a redesign of the operational IPv4 environment those have been postponed so far.

From our experience the rollout of IPv6 in a government network, and similar in all other business networks, should start “from the edge”. This means that at first on the one hand side the Internet exposed networks have to be taken in account. At the moment the share of IPv6 in the Internet traffic is growing rapidly. As on the end user site often transition technologies like DSLite are in use the end-user may recognize quality loss for web sites, not supporting IPv6 natively. This is reasonable e.g. due to a limitation of the parallel IP sockets on a carrier grade gateway for DSLite installations.

As next steps one has to continue network by network down in the back end area. This approach is necessary to set up Global Unicast Addresses on all devices and enable connectivity up to all connected networks.

For some reason one may not be able to continue with the backbone and then stepping forward to the backend segments. A possible reason may be a necessary upgrade of some core components, which have not been in budget yet and therefore cause heavy delay. In this case the back end networks should be focussed nevertheless. In this case it is not possible to have a direct roll out of the Global Unicast Addresses, but still IPv6 can be enabled and set into managed on the link local level. We are aware that this approach is in conflict with common transition models. But this is once to not get the transition project in heavy delay, second for another priority reasons:

In the back end network segments commonly the private servers and clients are located. Microsoft sees IPv6 as a mandatory part of its operating system since 2008. Initially, new Windows services are implemented IPv6 only. Microsoft still no longer does quality checks for its operating systems disabled IPv6-support in an installation⁹. Therefore, IPv6 is unavoidable in the local network, if not already now, then in the near future. To operationally ensure this mandatory “new” protocol (“new” from the view of the operation management), it must be integrated in all implementation and operation processes and structures. Most of the time it will be possible to isolate the IPv6 in one or a few backend network segments as a first step, so link local connectivity satisfies the connectivity requirements so far. With this approach IPv6 can be set in management

⁹ <http://technet.microsoft.com/en-us/magazine/2009.07.cableguy.aspx>

and a fully supported environment is enabled for the Microsoft operation systems and their new services. The unlovely aspect of this approach is the fact that the distribution of Global Unicast Addresses and the uplink connectivity must be initiated as a separated later transition phase.

Therefore, this approach of starting “from the edge” is a worthwhile approach, giving the opportunity to enable IPv6 first where it is really needed. IPv6-enabled islands can be connected in later steps. This approach also takes care of possible investments for upgrades in network components that can be performed during the transition of the edge networks. Take care: this approach does not mean “think from the edge”, it means “think (and prepare) about the whole, yet start work from the edges”.

For enabling the “Internet edge”, the Internet uplink and the demilitarised zone, especially the website(s) are most relevant. Initially, the need of a connection to the IPv6 Internet is more crucial than the transition of the internal infrastructure, as here the customer front end is located. Besides the transition of the web-servers and web-services is also easy because the infrastructure of the demilitarised zone is commonly not as complex as the subnets of the backend network.

After resolving the sources of error and getting a stable IPv6 connection to the public servers, the backend subnets of the network can be taken into account. A good starting point would be the local area network which is the subnet for the employees. The transitioned subnet should be separated from the rest of the network infrastructure by a router. Before you enable IPv6 in your network you should be certain that your router

- If it has an existing IPv6 uplink: Gets an IPv6 prefix and is able to forward it.
- If it has *no* existing IPv6 uplink: Blocks IPv6 traffic qualified

Besides, there should be only one router acting as IPv4- and IPv6-gateway for the subnet. The reason for this network design is to keep the network infrastructure as simple as possible. Of course the subnet infrastructure can be structured into more than one network, e.g. a client subnet and a separated server subnet, in case of IPv4, NAT and the private address range for IPv4 addresses are used. However, using IPv6 implicates a new way of subnetting. So you should think of the length of the IPv6 prefix. For an IPv4 subnet with client systems in it, an IPv6 prefix with the length of 64-Bits must be used, always.

At the end of the transition IPv6 availability has to be given from outside to inside and backwards. So take a deeper look at firewall rules when forwarding IPv6 through the network infrastructure

to connecting each subnet with IPv6. Be careful: some elder firewalls do not support IPv6 as required and therefore sometimes show unwanted behaviour to the network and its security.

5.1.3 Turkish Pilot

Network design is one of the most important steps for a successful IPv6 transition. First step for the IPv6 transition is the IPv6 address allocation and address assignment. For the address allocation the crucial point is to guess the IPv6 prefix length. The institution may leverage the current IPv4 address space used, considering there will be no NATs i.e. no private IP addresses in IPv6 network. In other words the network administrator should keep in mind that each device will be assigned a real IPv6 address. After address allocation the institution should plan the assignment of the IPv6 addresses to the sub-networks. The critical point here is that it is advised that at least /64 prefix should be used for a subnet in an IPv6 network. Similarly one may guess how many IPv6 addresses will be required at each subnet by looking at the current IPv4 setup and logs.

Basic communication over IPv6 may be considered as the next step of the network design. The initial communication should be established between the backbone routers of the ISP and the institution. Some connectivity problems have been observed while trying to establish this communication sourcing from the Maximum Transmission Unit (MTU) values. After this communication established it is advised to create a separate IPv6 test VLAN in order to test devices, configuration and security policies.

It is observed through the Turkish pilot that implementing the transition phases step by step as described above makes things simpler. For instance debugging an issue gets easier. However it may sometimes get complicated while moving to the production environment.

5.1.4 Common to all

Due to the address shortage when using IPv4, subnets with public IP addresses were often structured in a way to make them only as big as needed, e.g. using a /28 IPv4 network for a DMZ subnet for around a dozen of servers.¹⁰ For IPv6 subnets, such restriction does not apply.¹¹

¹⁰ A /28 IPv4 subnet is able to host $2^4 - 2 = 14$ IPv4 endpoints, including its upstream gateway router.

¹¹ As each IPv6 subnet may host up to $2^{64} - 1$ networked endpoints.

Unfortunately, in a dual stack environment, the restrictions of IPv4 still play a role (not so in an IPv6-only subnet). Still, a transition project with the goal of running IPv4 and IPv6 together in a dual stack setup should be seen as a chance to (a) document, (b) re-think, and (c) possibly restructure one's own local networks (or parts thereof) before the actual transition takes place. "Cleaning up" one's long-grown, and possibly sub-optimal, network structures before going dual stack is a much less tedious task than doing it at the same time or afterwards.

With the introduction of IPv6 into the local networks one also needs to think about the local address scheme (how to number subnets and endpoints) as well as how addresses get configured (static vs. dynamic; with stateless or stateful techniques; with or without privacy extensions). Chapter six in the transition guidelines document¹² gives extensive help on these questions.

The good news on network structure is, that the overall layout of your local networks (inside / outside, security zones, DMZ, etc.) can stay the same as before, since all the concepts which led to this structural design are independent from the IP version used. Still, many configurations for e.g. routes, access control lists, and filter rules must be extended so that the same functionality and level of security is provided by the network, after the addition of IPv6 to it.

5.2 Network Devices Level

5.2.1 Spanish Pilot

The compatibility assessments performed have shown that nowadays most of the network devices used in Red SARA support IPv6 as they are or after an upgrade of the software versions, so probably it is reasonable not to expect big issues on this in other deployments.

Practical tests have also shown that the main concepts of IPv6 are not so different from the concepts used in IPv4, so its implementation should not be difficult for most of the network staff. The most relevant point is to take special care of not forgetting things or making mistakes due to the new addressing scheme. This is especially important when thinking of security, since security elements must be configured to handle both protocols.

¹²http://www.bva.bund.de/DE/Organisation/Abteilungen/Abteilung_BIT/Leistungen/IT_Beratungsleistung/en/IPv6/best_practice/ipv6migrationsleitfaden_EN/download/fue_migrationsleitfaden.html?nn=4482170

5.2.2 German Pilot

On the switching level of the network no problems for IPv6 operation have been seen so far. Only the management level of the switches still has no common support for IPv6. On the Layer three – the routing level - the Citkonn network bases on software routers mostly. So therefore network device level is similar to the server operating system experiences.

For some older operating systems, such as e.g. SUSE Linux 11.3 or Microsoft Windows XP, IPv6 support is not technically mature. There is even more work to do to enable IPv6 so that it stays enabled across reboots and also becomes the preferred internet protocol. Since Windows Server 2008, the IPv6 protocol is enabled by default. For the Windows desktop versions, all base functions of IPv6 are implemented since Windows Vista.

The support of Linux operating systems is available since Ubuntu 12.04 LTS and the SUSE version above. From our experiences with these Linux versions IPv6 works well in everyday practice.

5.2.3 Turkish Pilot

Through the Turkish pilot it is observed that most of the current devices and operating systems are IPv6 enabled. One of the reasons for this was a governmental circular stating that governmental institutions are obliged to buy IPv6 enabled devices after 2012. At this point there exists a strange experience that IPv6 enabled is not well defined among vendors. Although it does not differ too much for the basic functionalities such as packet forwarding, routing etc., for the advanced features such as flow exporting, mobility or multicast the definition of IPv6 enabled may differ.

Another point to be considered for the administrators is that by the deployment of dual stack networks, devices will be forced to deal with two different protocols. This forces administrators to be more careful both in means of monitoring the performance and the security of devices.

5.2.4 Common to all

All networked devices in an IPv6-enabled network (think: dual stack network) should be checked on their IPv6-readiness. Some devices, such as e.g. routers, *must* be able to support IPv6 in such an environment. Other devices, such as end systems, may well run as IPv4-only in such dual stack network. However, switching on IPv6 in their local network may have unknown side effects to their connectivity – therefore every devices should be checked.

For the most crucial devices (routers, switches, and security devices) their administrators should check the IPv6 support in detail, depending in their needed functionalities. For this purpose it can be helpful to check their features one by one by e.g. consulting the IPv6 readiness standards (gold or platinum version), or the publicly available IPv6 profiles tables¹³. Especially for IP routers not only the IP packet forwarding engine(s) must be able to handle IPv4 plus IPv6, but any existing and used routing functionality (exchange of routing information and computation of routing tables) must also support IPv6. This can demand switching to a newer version of the used routing protocol, too, and therefore must be planned with care not to disturb the working IPv4 routing.

One should not forget that in addition to running the “core” functions (e.g. packet forwarding) of a network device on IPv6, sooner rather than later the device should also be able to be configured over IPv6, i.e. its management interfaces should support both IP protocol versions, too. The same applies to the ability to provide monitoring information, e.g. packet counters. Esp. for routers, IPv4 and IPv6 counters, and the respective SNMP MIBs, should be available. If needed, devices must be upgraded with a newer firmware version, which may add newer IPv6 features to a device (or IPv6 support at all).

Probably the most crucial checks must be made when enabling IPv6 security devices with IPv6, as its features for IPv6 may not be on par (yet) with those for IPv4. Also, do not forget to extend their configuration in order to represent the same rules for IPv6 which were already configured for IPv4 – such rules are usually *not* applied automatically for both protocol versions.

5.3 Network Base Services Level

5.3.1 Spanish Pilot

Preparing network base services for IPv6 has not been especially problematic, since the products used in Red SARA and MINETUR (BIND for DNS, Squid for reverse proxy, Stonegate and PaloAlto for the firewalls, Snort for the IDP/IPS) support IPv6.

¹³http://www.bva.bund.de/DE/Organisation/Abteilungen/Abteilung_BIT/Leistungen/IT_Beratungsleistung/en/IPv6/best_practice/ipv6profile_EN/download/fue_profilmatrix.html and companion document http://www.bva.bund.de/DE/Organisation/Abteilungen/Abteilung_BIT/Leistungen/IT_Beratungsleistung/en/IPv6/best_practice/ipv6begleitdokument_EN/download/fue_profildokument.html

5.3.2 German Pilot

As of mid-2014 all basic network services of the pilot run with IPv6. Tested services include DNS, DHCP, Active Directory, FTP, RDP, and SMTP server. These services were mostly tested under Microsoft Windows Server 2008 R2.

Some business applications later investigated regarding their IPv6 ability, such as MACH or ADVIS Linux server, are used which managed databases, mail daemons, web-servers and so on. These services run great with IPv6, too.

5.3.3 Turkish Pilot

The most crucial network based services in the Turkish pilot were DNS, monitoring services, load balancers and security services. These services have been upgraded in parallel to the currently deployed IPv4 infrastructure. For instance DNS server has been configured to answer queries over IPv6 and AAAA records for the respective domain names have been added to the zone files. Monitoring and security services have been made functional before the public services (e.g. EGG Web portal) in order to prevent the production environment from unauthorized access and adversaries.

5.3.4 Common to all

For all basic network services inside a local network an upgrade is needed to support the transition to IPv6. "Upgrade" will at least mean to slightly modify the configuration of an existing service. It can mean the installation of a newer version of the service (plus configuration), or, in the extreme case, switching to a completely different tool for the purpose altogether. It is highly recommended to verify the IPv6 capabilities of used network services before actually starting the transition (consult handbooks, Internet, manufacturer, support).

Affected base network services include servers for:

- DHCP (plus, if used, DHCP relays)
- DNS (support for AAAA records, plus connectivity via IPv6)
- NTP
- Directory services, such as LDAP
- SMTP mail servers (MTAs)

Additional network-related servers include, but are not limited to:

- Network monitoring and surveillance solutions
- Proxies, reverse proxies and load balancers
- Firewall and intrusion detection systems
- gateways and tunnelling appliances (e.g. VPN concentrator)
- management tools, and managed entities (e.g. IPv6 support for SNMP agents)
- IP address management solutions (IPAM)

Special care must be taken when transitioning “NAT boxes”, i.e. middle-boxes that perform IPv4 source address rewriting (also called masquerading), since NAT is not available for IPv6. The lack of source NAT for outgoing IPv6 connections means that desired properties of NAT such as hiding network structure or endpoint identifiers (if needed) must be obtained by other means, e.g. by using an HTTP proxy for outgoing connections. This decision must be part of the structural decisions mentioned in chapter 2 of this document.

5.4 Application Level

5.4.1 Spanish Pilot

Regarding commercial products used to support business applications, no issues with IPv6 have been detected, since all of them are adapted to the new protocol. Regarding the specific developments carried out for the eITV application, there have not been major issues once the best practices for development, such as abstracting the network layer from upper layers, increasing the length of IP address fields, and using host names instead of IP addresses have been followed.

5.4.2 German Pilot

At this point, Citkomm's basic experience made with applications running with IPv6 can be summarized as this: Either the installed application works with IPv6 out-of-the-box - or a deep error analysis is needed (i.e. more work than just enabling IPv6 in the application's configuration). Unfortunately easy to fix reasons for not supporting IPv6 out-of-the-box are rare. A more detailed analysis often has to investigate the network connections traffic of the application. Detailed information on how to take a deeper look at the error correction, based on the experiences of Citkomm, is given in Chapter 4.1.

Because Citkomm is the hosting provider of the applications for several municipalities but does not write the software itself, there is no way for Citkomm to directly change any existing program code. In theory for the majority of applications the transition to IPv6 should be handled without many problems. But at the end of the practical tests, Citkomm found out that just a small number of the applications have the possibility to be set up with IPv6 - and in this case are available to communicate over IPv6. Citkomm took a deeper look at this problem; results are described in chapter 4.1. There we talk about the difference between the IPv6-availability of the network protocols on server and applications.

5.4.3 Turkish Pilot

In the Turkish pilot applications are mostly either written in-house or open source solutions are deployed. In-house applications do not constitute a problem for the IPv6 support, however problems are observed with some open source projects. Briefly if you do not own a commercial support, IPv6 support may not be prioritized in code development of a project.

5.4.4 Common to all

Finally, the use-case-specific applications software (user clients as well as server software) that uses IP network connectivity must be checked for their operation with IPv6. This is true for use in an IPv4/IPv6 dual stack environment, and even more so in an IPv6-only environment – being able to work in an IPv6-only environment will become important in the future, for sure. "Application software" can be anything in this context, from web servers and web browsers to specific governmental applications, and, also, used apps running on mobile devices.

We have seen in our tests, that applications built on a high level language (and runtime) are often less dependent on the version of IP being used for network connectivity. This is because with a high level language setting up an IP connection uses a higher abstraction. When only speaking

hostnames are used instead of literal IP addresses, a program can be completely unaware of the IP version that is available and used by the system underneath, as e.g. in some function call such as `openConnectionTo(www.example.com)`. Programs that are programmed in a language with less abstraction, such as e.g. C, often explicitly handle IP addresses and connections for IPv4, and IPv6 support has to be enabled first by configuration, or even by re-compilation of the program. Also, transparent support for IPv4 and IPv6 is less of an issue with scripting languages, due to their high level of abstraction. Some programming languages provide both, explicit and implicit IP version selection, e.g. by allowing to write both, `new IPv4Connection()` / `new IPv6Connection()` and `new IpConnection()` in the source code.

In addition to software listening for incoming connections or connecting to services itself, related systems can be IPv6-unaware. This can e.g. cause problems with (sub-)systems for IP address logging, log analysis and/or existing solutions for IP address storage in databases. One more issue with tool that log IP addresses is, that even if they are able to handle literal IPv6 addresses, the written form of an address may differ for the same IPv6 address, due to the options for writing an abbreviated form of an IPv6 address, in case that it contains a series of zeroes. It is therefore now a best common practice, to either normalise all logged literal IPv6 addresses, or to store any logged IP addresses in binary form (suggested in case they are stored in a relational database).

To avoid these pitfalls, it is therefore recommended to test business-critical applications at first in a laboratory environment, in different setups (IPv4-only host/server, dual-stack host/server, IPv6-only host/server), with literal and with textual endpoint identifiers, and thoroughly check auxiliary systems for monitoring, logging, and analysis of data containing IP addresses, as well.

6 FIGURE INDEX

<i>Figure 1– Spanish Pilot Architecture (RED SARA)</i>	10
<i>Figure 2 – Spanish Pilot - eITV Service Architecture</i>	12
<i>Figure 3 – Turkish Pilot Architecture</i>	15
<i>Figure 4 – German Pilot Testbed Architecture</i>	27
<i>Figure 5 – Spanish Pilot: Reverse Proxy Approach for IPv6 Enablement</i>	38
<i>Figure 6 – Screenshot from Citkomm-external Monitoring System</i>	43
<i>Figure 7 – Spanish Pilot: MINETUR’s Network Configuration</i>	47
<i>Figure 8 – Spanish Pilot: MINETUR’s Network Configuration</i>	77
<i>Figure 9 – Reference Architecture</i>	93
<i>Figure 10 – Reference Architecture</i>	94
<i>Figure 11 – Logical view of VPN systems and their management inside the FOKUS IPv6 testbed</i>	96
<i>Figure 12 – Testbed configuration</i>	99
<i>Figure 13 – eITV application data flow</i>	101
<i>Figure 14 – eITV access screen</i>	102
<i>Figure 15 – eITV card range query</i>	102
<i>Figure 16 – eITV card authorization query</i>	103
<i>Figure 17 – eITV card status query for DGT</i>	103
<i>Figure 18 – Users of the system and protocols used</i>	104
<i>Figure 19 – Reference architecture</i>	105
<i>Figure 20 – Reference architecture for UL-Citkomm pilot</i>	109

Figure 21 – Integration of the machines in Luxembourg and Germany in the same testbed	110
Figure 22 – Instances with IPv6 addresses in OpenStack Havana (UL testbed)	111
Figure 23 – The dashboard in OpenStack's Horizon	112
Figure 24 – Firewall rules in the OpenStack election setup.....	112
Figure 25 – User-perceived performance (blue and green lines) against local performance (red line) ...	113
Figure 26 – Performance of the election website on IPv6, for one day starting from May 24th at 3pm.	114
Figure 27 – Parameters of two VMs hosting the website on IPv6, on the evening of the Election Day ..	115
Figure 28 – Hardware resource usage for the testbed at UL, on the election evening	115
Figure 29 – The evolution of the VM performance for two VMs on the election evening	116

7 TABLE INDEX

<i>Table 1 – Spanish Pilot: IPv6 Addressing for Red SARA.....</i>	<i>19</i>
<i>Table 2 – Spanish Pilot: IP Assignment for Servers</i>	<i>19</i>
<i>Table 3 – Spanish Pilot: IP Assignment for Gateways</i>	<i>19</i>
<i>Table 4 – Spanish Pilot: IPv6 Assignments to Ministries</i>	<i>20</i>
<i>Table 5 – Spanish Pilot: /64 Ranges Assigned to the Elements of the Connection Area</i>	<i>21</i>
<i>Table 6 – German Pilot: Table of Systems in the “BRUNNENREICH” Domain.....</i>	<i>36</i>