Title:	Document Version:
Deliverable D3.6.2 – E-Government Generic Services with IPv6	1.1

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

Contractual Delivery Date:	Actual Delivery Date:	Deliverable Type* - Security**:
31/08/2013	18/12/2013	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, Uwe Holzmann-Kaiser	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)

Abstract:

This document is the second one 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

Revision History

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

Revision	Date	Description	Author (Organization)
v0.1	19.08.2013	Document creation	Carsten Schmoll (FRAUNHOFER)
v0.2	05.09.2013	Revised TOC	Carsten Schmoll (FRAUNHOFER)
v0.3	31.10.2013	added content for Spanish partners	Carlos Gómez Muñoz (MINHAP)
v0.5	04.11.2013	added more content for Spanish partners	Carlos Gómez Muñoz (MINHAP)
v0.6	04.11.2013	some editorial clean-up	Carsten Schmoll (FRAUNHOFER)
v0.35	09.10.2013	added Citkomm contributions	Timo Baumgart (Citkomm)
v0.45	10.10.2013	Revision of Citkomm contributions	Gerold Gruber (Citkomm)
v0.55	26.10.2013	Additional Chapters	Martin Krengel (Citkomm)
v0.65	05.11.2013	Completion of Citkomm contributions	Gerold Gruber (Citkomm)
v0.7	08.11.2013	Merge of contributions from German and Spanish partners	Carsten Schmoll (FRAUNHOFER)
v0.8	10.11.2013	Editorial corrections and smaller additions	Carsten Schmoll (FRAUNHOFER)
v0.9	18.11.2013	Addition of Turkish contributions	Emre Yuce (ULAKBIM) Onur Bektas (ULAKBIM)
v1.0	06.12.2013	Merging and editing and revision of the deliverable	Carsten Schmoll (FRAUNHOFER)
v1.1	18.12.2013	Final changes after QC from partner UL	Carsten Schmoll Uwe Holzmann-Kaiser

Disclaimer

Executive Summary

This document gives an updated overview of the current state of three national GEN6 pilots. For each pilot it describes its approach on the network service level (DNS, DHCP, …) to the transition, including address and network planning, and the envisaged transition process. This approach affects how services can be delivered inside the networks. Furthermore each pilot provides information on affected components, experiences gained during the transition process and some description of the obtained results and if available some tests to verify a successful transition.

This deliverable is the second snapshot of a living document. It focuses on generic network service elements, including network security elements and their transition to IPv6. Its successors (D3.6.4, D3.6.4) will cover higher-level service aspects and service details as the pilots evolve.

All these deliverables will be grouped into D3.6, showing commonalities and differences of the pilots so that it becomes most useful for a government audience. GEN6 can be taken as a starting point to introduce IPv6 based on the best practises of the variety of documented pilots.

Table of Contents

1 INTRODUCTION

This document belongs to 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. After the first year report (see document D3.6.1) the national pilots are now reporting about their concluding experiences when upgrading generic and network related services from IPv4 to dual-stack.

The 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 network or service.

The suggested approach is to build an IPv4-only test bed first, instead of doing “open heart surgery” by performing the process right from the start on the real components. The test bed needs to resemble the real environment as closely as possible. This way, transition work inside this test bed can then also emulate the challenges and pitfalls of the real networks. The steps of the transition work have to be documented well. The knowledge gained during this process is of invaluable help when the real server and service is going to be transitioned later on.

By reading this document, governments can learn from the experiences of three GEN6 government projects: It is important to understand the steps involved in switching a data centre, a government portal or a government backbone network to IPv6, and to start the planning for such a project and its realization in due time.

The following sections of this document are structured according to the necessary steps of a transition (address planning, transition strategies, components to change, experiences with components like routers, firewall, etc.) with contributions of each pilot. This allows a technical reading through transition steps and is not a transition story of the pilots.

2 NETWORK ARCHITECTURES AND STRUCTURES

2.1 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
- 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:

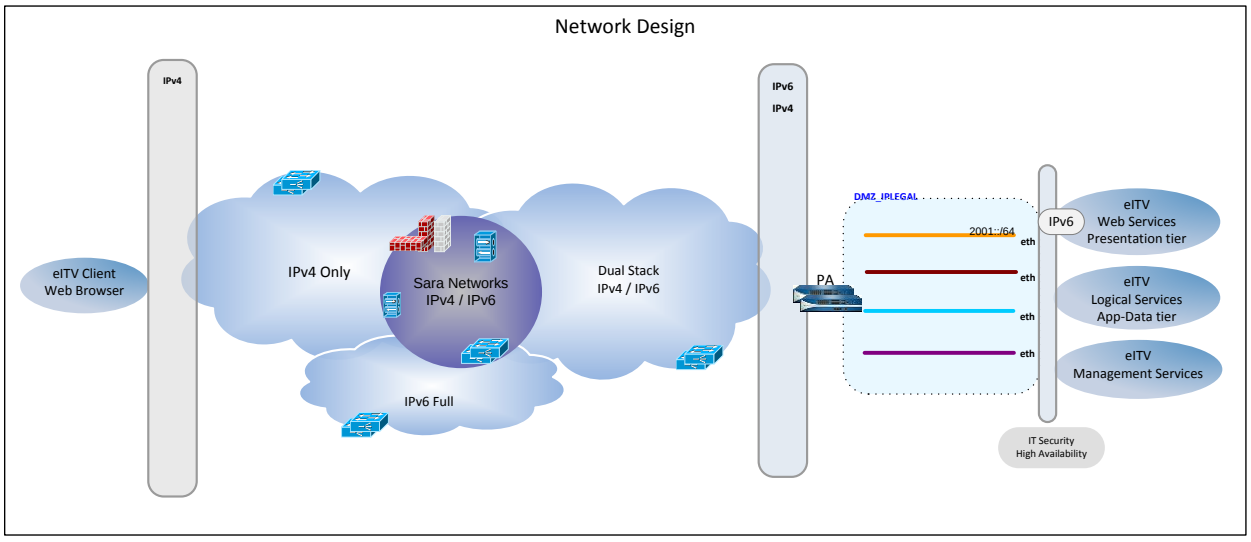

Figure 1 – Spanish Pilot Architecture (RED SARA)

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 441[1]) 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.

[1] Version 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:

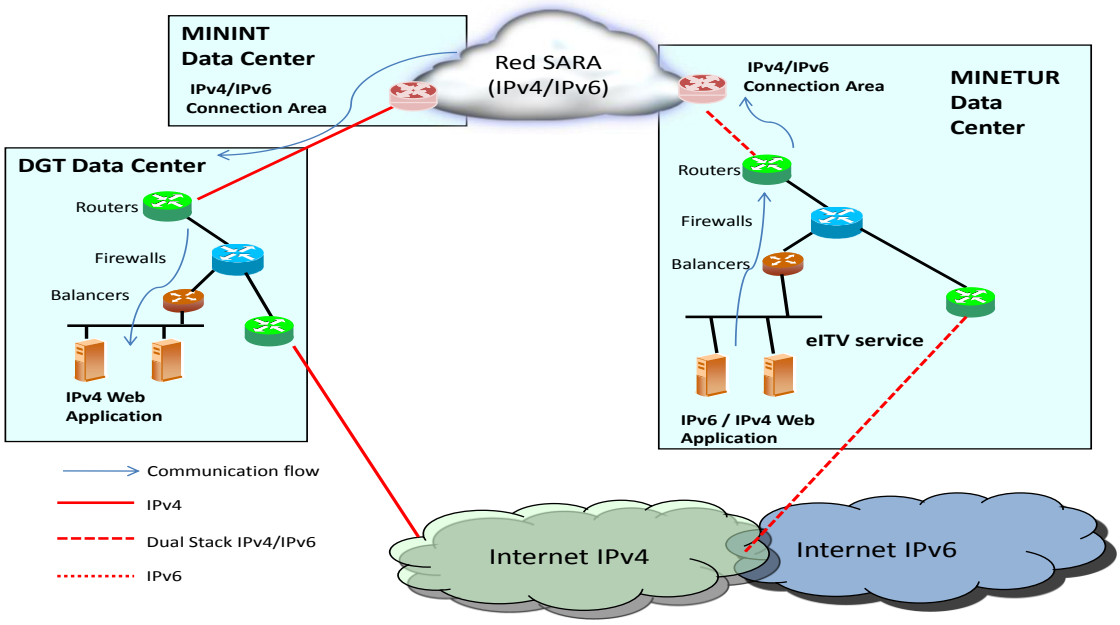

Figure 2 – Spanish Pilot - eITV Service Architecture

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 then 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 3.4.3 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 testbed was installed for application tests. The experiences gained in this testbed 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, containing 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:

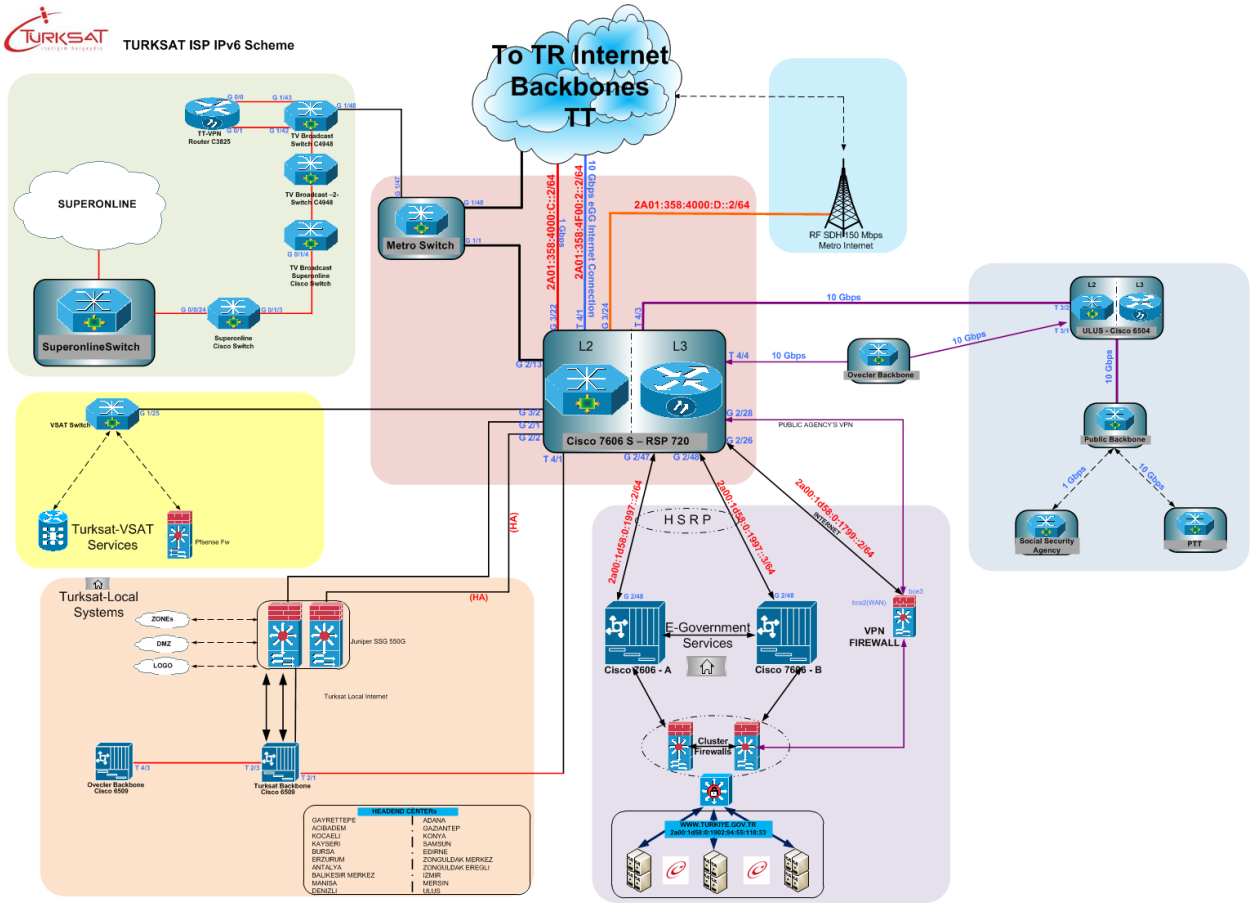

Figure 3 – Turkish Pilot Architecture

2.2 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.

2.2.1 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. Red SARA has already been registered as a LIR and is in conversations with RIPE-NCC to get the IPv6 addressing space. However, it is not foreseen to have this addressing space ready for GEN6, due to the need of justification for prefixes larger than /29. Such justification must include information from three levels of government, which implies a long process.

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 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).

TurkishPilot:

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

- TURKSAT network.
- 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.

2.2.2 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	Usedfor
2A00:2000:40A0:1::/64	18.446.744.073.709.500.000	2a00:2000:40a0:1:0:0:0:1	2a00:2000:40a0:1:ffff:ffff:ffff:fffF	DMZ
2A00:2000:40A0:FFFF::/64	18.446.744.073.709.500.000	2a00:2000:40a0:ffff:0:0:0:1	2a00:2000:40a0:ffff:ffff:ffff:ffff:ffff	Router-FW Segment
2A00:2000:40A0:FFFE::/64	18.446.744.073.709.500.000	2a00:2000:40a0:fffe:0:0:0:1	2a00:2000:40a0:fffe:ffff:ffff:ffff:ffff	NAT64 Segment

Table 1 – Spanish Pilot: IPv6 Adressing 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 assigment	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:

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 …

- 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.

2.2.3 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.

2.2.4 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 used 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.

2.3 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 migration 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 migration 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 Citkomm 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 Citkomm network.

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

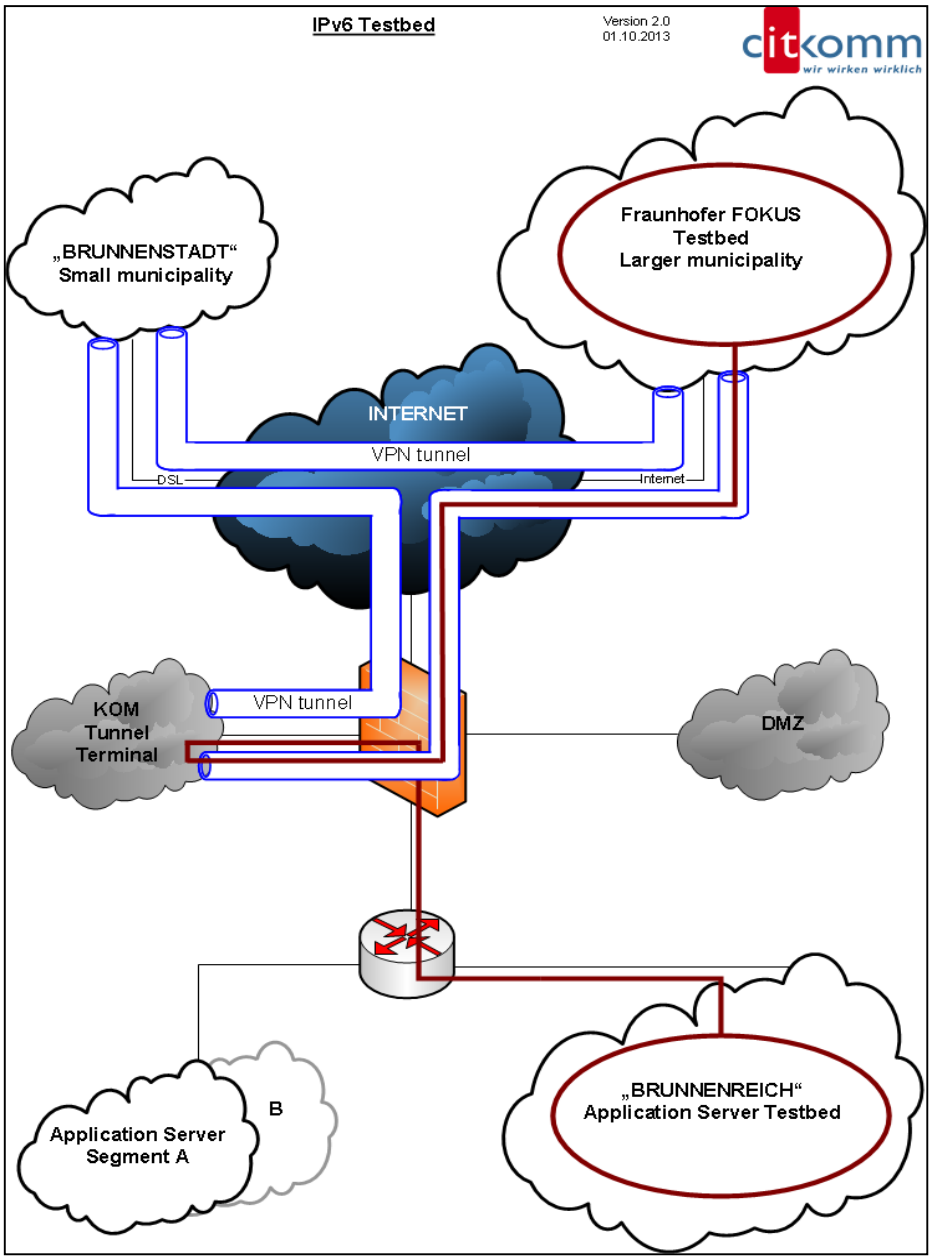

Figure 4 – German Pilot Testbed Architecture

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.

3 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.

3.1 Chosen Approach

Spanish Pilot:

The Spanish pilot envisages 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 ANS of the service.

Regarding IPv6 addressing, as it has been mentioned in section 2.2.1, 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 2.2.2), will be kept so that the renumbering of the networks can be made easily and with little effort.

<u>German Pilot:</u>

- 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 testbed 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.

3.2 Planned Order of Changes due to Transition

Spanish Pilot:

In the case of the Red SARA network, the changes required by the transition have been planned and will be performed in the following order:

- First, the platform for providing shared services for IPv6 access to e-government web sites is 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, is 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 is 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 is 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.

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 testbeds 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 testbed.

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 fileservers 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) **DB (MS SQL Server)**	Ubuntu 12.04 LTS 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.

3.3 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.

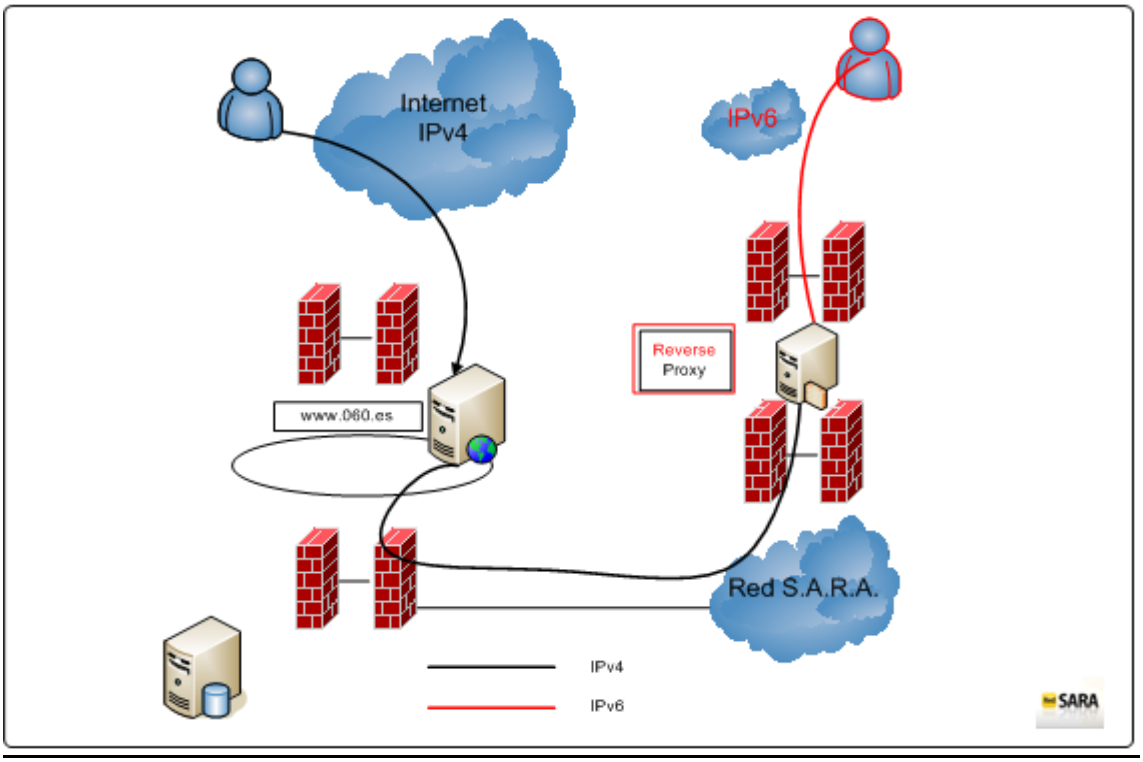

Figure 5 – Spanish Pilot: Reverse Proxy Approach for IPv6 Enablement

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, five Web Portals from the MINHAP have been made IPv6-enabled so far:

- e-government Portal: www.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

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 vSwitch would be

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

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 testbed. Their network interface cards work 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 testbed. 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 2.2.2. 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 testbed 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-AAAA	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 AAAA 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 (1.0.0.0.0.7.0.0.8.2.1.0.0.0.0.0.2.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-AAAA	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 AAAA 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 (1.0.0.0.0.7.0.0.8.2.1.0.0.0.0.0.2.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_Iserlohn_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_Arnsberg	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 - 2916 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 3.4.3.

- 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 testbed 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.

<u>Turkish Pilot:</u>

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).

3.4 Enabling IPv6 in Components

3.4.1 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 behavior 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.

Thee 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 thee 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.

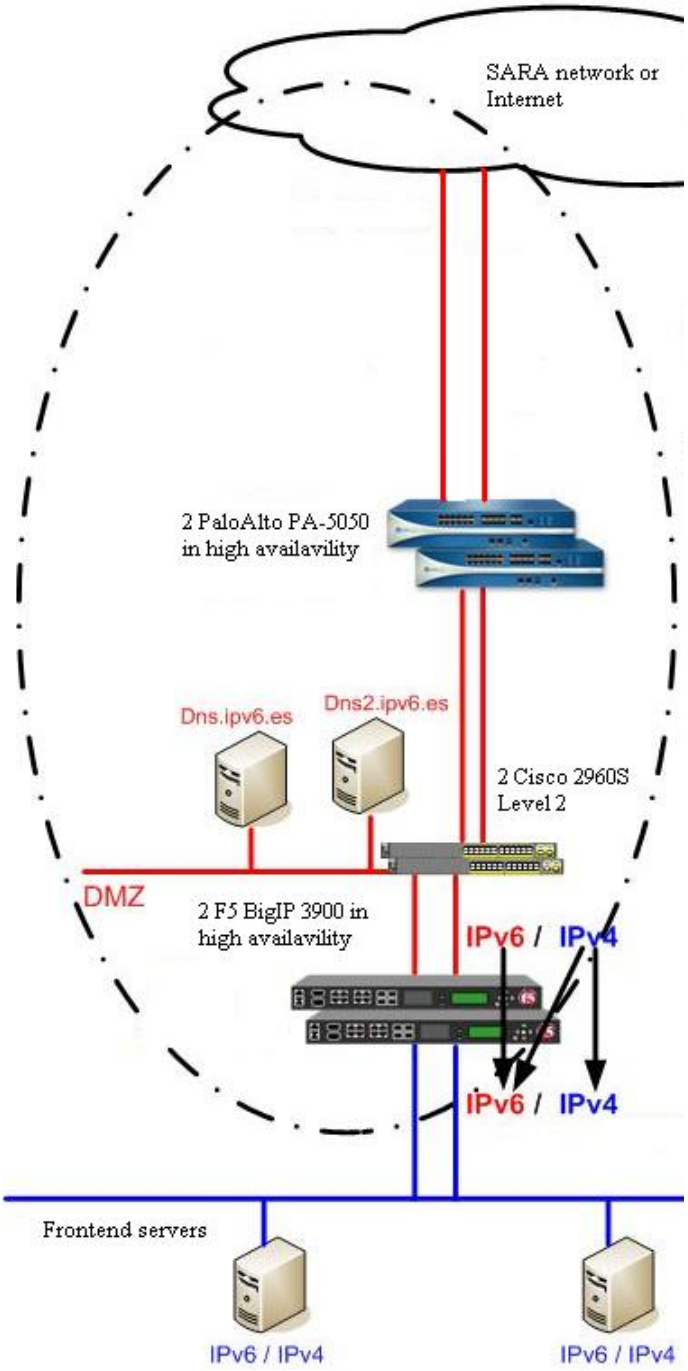

Figure 7 – Spanish Pilot: MINETUR's Network Configuration

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 build 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 Citkomm 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).

3.4.2 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 5.

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 a 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.

3.4.3 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 set up 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.

<u>Turkish Pilot:</u>

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.

4 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 migration 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 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 Center (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.

4.2 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 testbed 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.

4.2.1 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 it has been included the necessary AAAA records to allow the access of the clients using IPv6. 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 testbeds 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.

4.2.2 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. Testbeds 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 3.4.3.

Turkish Pilot:

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

5 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 areas[3], and it reports data to CCN-CERT through the logging aggregator. This new version is able to analyze 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 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.

[3] For more information, see http://www.snort.org/

5.1 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 fulfill the needs.

As it was mentioned previously, firewall configuration has been changed to fulfill 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.

5.2 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.

5.3 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 3.1.8[4], 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.

5.4 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.

[4] For more information, see http://www.squid-cache.org/

6 OUTLOOK

In 2013 and beyond, the GEN6 project's national pilots continue to work on migration of additional parts of their infrastructure to IPv6. This section gives an outlook on the most prominent migration work done and planned for each pilot.

6.1 Spanish Pilot

As it has been described previously, the Spanish pilot envisages three complementary action lines, all of them based on the role of Red SARA as the core network for the interconnection of the Spanish public administrations:

- The upgrade of Red SARA so that it can transport IPv6 natively, therefore allowing IPv6 communications between administrative units.
- 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.
- 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).

For the remaining time of the project, the work foreseen in the Spanish pilot in each of these lines is the following:

- Upgrading of Red SARA to support IPv6 services provision between public administrations. Being the upgrade completed in its most part, the work will be focused on monitoring and support of the IPv6 communications.
- IPv6 enablement of public administrations Web Portals through shared services. The implementation plan for this activity is based on several iterative cycles, so that sets of web portals were made IPv6 available in each interaction. It is therefore intended that in the future more iterative cycles will take place, aiming to increase significantly the number of IPv6-enabled portals by the end of the project. This will include the IPv6 enablement of the Spanish PEPS (the interoperability node for mutual recognition of electronic identities developed in the STORK project) to support the cross-border pilot.

- Adaptation of MINETUR services to IPv6. In the future months, development works to IPv6 enable eITV application will continue, as well as the preparation of the MINETUR network to support IPv6 connections to this service. Once the development has ended, the IPv6 compatible version of eITV will be deployed and operated.

6.2 German Pilot

During the next months, the application testbed will allow the use of more and more real-world use cases related to several products. These tests (and their results) will provide up-to-date information about the IPv6-readiness of the different vendors.

These municipal applications include:

- MACH governmental ERP System
- Votemanager publishing of election results
- Advis management of foreign citizens
- MESO citizen management

When the applications reach the “running” state, a prototypical monitoring and testing system will be upgraded with check routines to monitor the availability of these services over IPv6 connections.

Several security approvals are on Citkomm’s To-Do list, because the IPv6 protocol includes features that require additional attention compared to IPv4. The infrastructure will receive more in-depth analysis (and improvements) based on the knowledge acquired during the pilot.

At the same time, more and more customer websites will be made available over IPv6, accessible to the public. The productive infrastructure is completely available as of October 2013; and as the customers have agreed, after testing their websites will become visible in the IPv6 world too.

The network connection to the German governmental network DOI is already IPv6-enabled but the used applications are not yet enabled with IPv6. At first DNS and e-mail interchange services will become productive over IPv6 during the next quarter.

Finally yet importantly, Citkomm started the IPv6 transition planning for their LAN landscapes (additionally to keeping IPv4 support). The Citkomm LAN and a customer LAN will be enabled for

IPv6 in Q1/2014. This will show how future-proof the testbeds have been built and what issued might have been overlooked in the test cases. The knowledge transfer to technicians not directly involved in the tests up to this point will show which sections of the setup and how-to documentation needs to be extended.

6.3 Turkish Pilot

The Turkish pilot has successfully deployed IPv6 through TURKSAT and made the EGG Web portal IPv6-enabled in first year of the project. In other words, citizens are able to use the EGG Web portal either over IPv4 or over IPv6. In 2013, the backend of the EGG has been made IPv6-enabled. For this purposes, the connection between TURKSAT and other participating agencies are made IPv6-enabled. In this process, bureaucratic procedures are on-going as well as technical issues. At the end of the project it is planned that EGG is IPv6-enabled for both the backend and the frontend.

7 CONCLUSIONS

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 migration 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.

8 FIGURE INDEX

9 TABLE INDEX