



<b>Title:</b>		<b>Deliverable D 5.6.1</b>		<b>Document Version:</b>
		<b>Monitoring of IPv6 in Academic Networks-1</b>		1.0
<b>Project Number:</b>	<b>Project Acronym:</b>	<b>Project Title:</b>		
297239	GEN6	Governments ENabled with IPv6		
<b>Contractual Delivery Date:</b>		<b>Actual Delivery Date:</b>	<b>Deliverable Type* - Security**:</b>	
30/09/2014		15/11/2015	R – PP	

\* 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)

<b>Responsible and Editor/Author:</b>	<b>Organization:</b>	<b>Contributing WP:</b>
Fernando Mira da Silva	IST	WP5

**Authors (organisations):**

José Costa (IST), David Duarte (IST), Jorge Matias(IST), Fernando M. Silva (IST), Luis G. Silva (IST)

**Abstract:**

This deliverable presents a report on the work performed up to now in the scope of WP5 in order to monitor effective IPv6 usage access in academic networks.

**Keywords:**

IPv6, Governments, Academic IPv6, Monitoring Data, DNS support.

## Revision History

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

Revision	Date	Description	Author (Organization)
V0.1	10/09/2014	Document creation	José Costa (IST)
V0.2	15/10/2002	Document revised and preliminary results included	José Costa (IST)
V0.3	14/11/2002	Data updated	Jorge Matias (IST), David Duarte(IST)
V0.4	17/11/2002	Corrections and conclusions added	Fernando M. Silva (IST)
V1.0	18/11/2002	Final revision	Luis G. Silva (IST)

## Disclaimer

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

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

## Executive Summary

One of the main activities in the GEN6 project is the academic pilot which consists in collecting the experience and results, on IPv6 deployment scenarios, of the participating universities, namely KIT and IST, and monitoring the IPv6 deployment in Academia across Europe. This report addresses the work performed in the scope of monitoring the IPv6 deployment in Academia.

The goal of this activity is the development and installation, in highly accessed web pages, of a software sensor probe for monitoring the effective use of IPv6 at the user level in academic institutions. This activity requires the cooperation of several Universities across Europe, which will be asked to install a link to the developed sensor on their main websites, in order to enable the collection of a significant and geographically diverse number of access logs from within academic networks.

This report describes the methodology adopted for the sensor probe development and it presents preliminary results of IPv6 usage at the user level in academic networks. In order to achieve this goal, it was required to adapt previously existing sensor probes to the specific requirements of this monitoring activity and to perform adequate filtering and statistical processing of the collected log data in order to obtain relevant results and to test the developed system and underlying data processing methodology. Therefore, in the first phase of this activity, the sensor probe was installed and tested at IST, prior to a wider deployment in other academic institutions.

The results presented in this report cover the period from 28<sup>th</sup> of July, 2014 to 31<sup>st</sup> of October, 2014. During this period, the sensor probe was tested and improved, and the flow required to process the collected log data was developed. The log data enables the identification of the IP protocol used to access the test website and the collection of other relevant information. The sensor probe records the type of connection (IPv6, IPv4 or both), the university of origin, the country of origin and the local IPv6 DNS support. When both IPv6 and IPv4 are available, it also provides the preferred connection protocol used. The total number of connections to the test site in the reported period was 206,061.

Since in this test phase the sensor probe was only deployed at IST, there is a large number of Portuguese universities in the top 20, relative to the total number of accesses. As it would be expected, Universidade de Lisboa (Lisbon University, of which IST is part of) comes on top in the number of incoming connections. Nevertheless, several accesses from other European Universities were also identified and processed.

These very preliminary results show that IPv6 penetration in academic networks varies

significantly, depending on the university. One notable mention is the case of the Royal Institute Of Technology where almost 100% of the connections were made using IPv6. The number of IPv6-only connections is greater in countries like the Netherlands and Germany. However, if one takes into account the preferred access protocol, when both IPv4 and IPv6 are available, Finland and Portugal exhibit the highest number of native IPv6 accesses. Nevertheless, as stated before, these are preliminary results, which enable the validation of the adopted data collection and processing methodology, but still have reduced statistical significance. A wider deployment is required in order to achieve more meaningful results.

# Table of Contents

<b>1. Introduction .....</b>	<b>9</b>
<b>1.1 Context and Motivation .....</b>	<b>9</b>
<b>1.2 Contents Overview .....</b>	<b>10</b>
<b>2. Methodology.....</b>	<b>11</b>
<b>2.1 Approach used.....</b>	<b>11</b>
<b>2.2 Probe description .....</b>	<b>12</b>
<b>2.3 Probe deployment .....</b>	<b>14</b>
<b>2.4 Challenges .....</b>	<b>15</b>
<b>3. Preliminary Results.....</b>	<b>19</b>
<b>4. Discussion and future work .....</b>	<b>26</b>
<b>5. References.....</b>	<b>27</b>

## Figure Index

<i>Figure 1 – Percentage of connections using IPv6, IPv4 or both.....</i>	<i>19</i>
<i>Figure 2 – Percentage of connections using IPv6, IPv4 or both for the top 4 portuguese universities and the top 4 non-portuguese universities. ....</i>	<i>22</i>
<i>Figure 3 - Percentage of connections using only IPv6, only IPv4 or both for the top 7 countries. ....</i>	<i>24</i>
<i>Figure 4 - Evolution of IPv6, IPv4 and both connections during the period under study.....</i>	<i>25</i>

# Table Index

**Table 1 - Number of connections to IST website per university. .... 21**

**Table 2 - Number of connections to IST website per country..... 23**



## 1. INTRODUCTION

### 1.1 Context and Motivation

The academic pilot consists in collecting the experience and results on IPv6 deployment scenarios of the participating Universities, namely Karlsruhe Institute of Technology (KIT) and Instituto Superior Técnico (IST), and monitoring the IPv6 deployment in Academia across Europe.

One of the main goals of the pilot will be to assess the maturity level of IPv6 implementation and deployment on academic institutions and Universities across Europe, including both technological and non-technological schools, including the monitoring of the effective IPv6 use at the user level.

The GÉANT network is the pan-European research and education network that interconnects Europe's National Research and Education Networks (NRENs). The GÉANT backbone fully supports IPv6, as well as the majority of all NREN networks. However, IPv6 penetration at the institution and user level is quite variable, and strongly dependent on the local effort and commitment of CIO's and local network administrators.

The assessment of the effective IPv6 use in the academia at the user level is not an easy task, since it is hard to directly monitor the IPv6 usage at the user level. However, several indirect measures can be taken and complementary usage scenarios can be envisaged:

- Global IPv6 traffic at the academic level can be obtained from the GÉANT backbone infrastructure;
- Academic IPv6 traffic at the national level can also be collected from the several NREN;
- Through the installation of adequate software sensor probes in highly demanded web pages one may estimate the effective use of IPv6 at the user level in academic institutions. This requires the cooperation of representative universities, which will be asked to install a sensor probe that effectively points to a controlled page where access information can be collected and measured. Of course, the degree of implementation of this monitoring service will depend on the cooperation of target universities and content provider websites.

This document describes the methodology adopted for the sensor development and it presents preliminary results of IPv6 support at the user level in academic networks. In order to achieve this goal, it was required to adapt a previously existing sensor probe to the specific requirements of this monitoring activity and to develop an adequate filtering and statistical

processing flow of the collected raw data in order to obtain relevant results. Within the scope of this activity, it was also necessary to extensively test and tune the sensor probe and the methodology employed for processing the log data, in order to enable reliable results to be obtained. Therefore, in the first phase of this activity, the sensor probe was installed and tested at IST, prior to wider deployment in other test sites.

The preliminary monitoring results reported in this document describe the results collected by the test probe installed in the IST website in the period from 28<sup>th</sup> of July, 2014 to 31<sup>st</sup> of October, 2014. As stated before, these results still have reduced statistical significance at European level, but provide valuable information and a proof of concept about the data that can be gathered and reported when a wider deployment of the sensor probe is available.

## 1.2 Contents Overview

The structure of this document is as follows. Section 2 describes the overall methodology used for the monitoring activity. It describes the details of the software sensor probe, how it can be installed in a web pages, its output, and how this output can be used to gather statistics on IPv6 penetration in Academia across Europe. This chapter also discusses the major challenges that still need to be addressed in order to enable more reliable and accurate results to be achieved. In Section 3 we present the preliminary results obtained from the test sensor probe installed in IST. Finally, in Section 4, we discuss the achieved results and we describe the next steps to be taken in the scope of this activity.

## 2. METHODOLOGY

### 2.1 Approach Followed

The first step in order to monitor the IPv6 implementation level in the access network of target universities, was to create a specific probing web service and DNS service. When accessing a site with the sensor probe installed, the user is redirected to these services. Access logs to these services provide detailed information about IP source, supported protocols and further access information. All this raw data is recorded and subject to adequate filtering and statistical analysis in order to provide meaningful information about IPv6 penetration and support in the access network.

In order to achieve this goal, web and DNS services were configured to reply to requests assuming the following connectivity scenarios (in the following order):

1. HTTP address is available only in IPv4 and DNS service is available in dual stack;
2. HTTP address is available only in IPv6 and DNS service is available in dual stack;
3. HTTP address is available in dual stack and DNS service is available in dual stack;
4. HTTP address is available only in IPv4 and DNS is only available in IPv6;
5. HTTP address is available in several IPv6 addresses and DNS is available in dual stack.

These connectivity scenarios are intended to test the ability of the DNS resolvers to access other DNS servers, both when these are only available in IPv6 and when they are available in dual stack. The last test attempts to monitor the behavior of the service when a single domain name has a long list of IPv6 addresses associated (20, in the specific test performed). In this case, the reply is too long and the reply should be provided over TCP instead of UDP (RFC 1035 [1]). This scenario enables TCP support to be tested and firewall configurations that may block this reply to be identified.

In order to promote the access to the web/DNS service where this monitoring is performed, a small software probe was developed, implemented in Javascript, which was designed to be installed in websites frequently accessed by academic users. In practice, to reach this goal, it is planned to request the installation of the probe in the main website of several representative universities, since these are institutions open to research and that, by their own nature, do have a high number of accesses from the academic community. However, one must emphasize that the location of the probe itself is irrelevant for the tests to be performed in the scope of this activity. In fact, IPv6 support is tested between the user platform and the IST test server, irrespective of the sensor probe location. Therefore, any public site with a potentially high

number of accesses from academic networks would be a good candidate for installation of the sensor probe.

As stated before, the probe is just a small piece of Javascript code adapted from a previous version developed by the IPv6 observatory [2]. The goal of the probe is to force the user of the web browser to make several accesses to the web and DNS test services, installed at IST. The details of this probe are described in section 2.2.

In order to obtain specific data concerning IPv6 support in academic networks, it is necessary to identify if the source of each access to the test services is made from a university or academic institution, and filter out all other accesses. Since the source IP address is known, it should be easy to identify the source network. In order to identify the source network, the extensive use of the IANA *whois* service [3] and the RIPE database [4] is made. In practice, this mapping has proven to be a harder task than initially anticipated, and in fact some degree of error still exists regarding the identification of academic networks. This subject is addressed in deeper detail in section 2.4.

If the source IP address is identified as belonging to an academic network, for each access to the test services the following data is recorded:

- User source IP address;
- University name;
- Web server;
- Operating system and web browser;
- Access date.

In order to associate each test set to a single access, and to avoid counting repeated accesses from the same source, it was required to develop a method to enable the identification of a single access. We will detail this method in section 2.2.

## 2.2 Probe description

As we have mentioned, the developed probe is an updated version of the one originally developed by the IPv6 observatory [2], modified in order to perform the tests foreseen in the scope of this workpackage. The goal is to insert the probe in the HTML of several websites with popular academic content, so as to enable the Javascript code to be executed by the web browser of the user, and to identify accesses with source in academic networks. The most practical way to achieve this goal is to install the probe in the main website of large universities.

The reference to the probe is as simple as possible. The only requirement is to install the following Javascript code embedded in HTML in the target website:

```
<script type="text/javascript">
    document.write(unescape("%3Cscript src='" + document.location.protocol +
    "//static.gen6.tecnico.ulisboa.pt/gen6.js' type='text/javascript'%3E%3C/script%3E"));
</script>
```

The sensor probe was developed in such a way that minimizes load and latency overhead when the user accesses the corresponding website, keeping in practice the extra time unnoticeable at user level. Moreover, it is suggested that the cooperating sites install the probe code at the very end of the target page, just before the final tag `</body>`. While the overhead introduced by the probe is minimal, this option ensures that the test being performed does not affect the load time of the web content.

When the browser executes the probe code, one HTTP GET request is sent to each of five different virtual test websites installed at IST. Each one of these accesses simply downloads a small transparent image (1x1px). This small image is designed in order to trigger the effective access to the test sites, but in fact does not introduce any perturbation to the graphic content of the website, being unnoticeable by the end user.

As a result of this access, relevant access data is recorded. In practice, log data enables the following scenarios to be detected:

1. Access to the IST test site in IPv4 only;
2. Access to the IST test site in IPv6 only;
3. Access to the IST test site available in dual stack;
4. Access to the IST test site in IPv4 only, but for which the DNS only supplies an IPv6 reply;
5. Access to the IST test site in IPv6 only, and for which the DNS supplies a large reply with 20 IP addresses.

Overall, these tests provide two types of information:

- Connectivity tests in IPv4 and IPv6 between the user device and the IST test site;
- Connectivity tests to the local DNS resolver, performed by the user device.

In the scope of the above tests, the following information about the user access is collected:

- If the user is able to access to the test site in IPv4 (base test);

- If the user is able to access the test site in IPv6 and, if positive, which type of addressing is used (e.g. IPv6 native, Teredo tunneling, 6to4 tunneling, etc..);
- To identify the preferred access protocol chosen by the end user device (IPv4 or IPv6).

In the scope of the connectivity tests performed to the DNS server, the following information is collected:

1. If the resolver has IPv6 connectivity to obtain addresses from domain names;
2. If the resolver uses IPv6 over IPv4 tunnels in which MTU limits may prevent to resolve domain names in IPv6.
3. If there the local firewall configuration disables the resolver to receive TCP connections, which are required to resolve DNS replies of large dimension.

In order to identify accesses that were made by the same single user, a unique identifier is generated, which is added to each Full Qualified Domain Name (FQDN) retrieved from the access to the Web/DNS test servers. Moreover, in order to avoid that the same user repeats the tests whenever it accesses the probe in each site where it is deployed, it is generated a local Javascript cookie in the first access, which indicates whether the tests were already performed or not. This cookie times-out after 24 hours.

All requests to the Web and DNS test servers are stored in local log files. These log files are periodically processed in order to monitor the supported IP protocol from each source IP and to generate the desired statistics and access reports.

## 2.3 Probe deployment

The wide deployment of a probe with the features described above is a sensitive task, since it not only requires the voluntary cooperation of several test sites, as it is crucial that both the probe and the test sites are carefully designed in order to ensure that its inclusion in the cooperating sites do not harm regular behavior and performance. In order to achieve this goal, prior to wider deployment, the probe was initially installed in several IST websites and subject to extensive tests.

Currently, the probe is installed in the following sites:

- The homepage of the IST website, as well as in several secondary IST sites with relevant contents;
- In the official homepage of the IPv6 observatory;

- In the home page of the University of Murcia;
- The probe is currently being installed in the homepage of the Karlsruhe Institute of Technology (KIT);

As it is clear, in order to gather more significant and wider statistics, the probe will have to be deployed in many more websites. As stated in chapter 4, IST will attempt to obtain the cooperation of several European Universities in order to achieve a wider test universe and meaningful results at the European level.

As explained in section 2.2, a significant feature of this probe is that it does not require the local website where the probe is deployed to have any kind of IPv6 support. In fact, as explained above, the probe just redirects the user browser to the IST test site. All tests are performed between the end user device and the IST test site, and IPv6 support is only tested in the path between these two endpoints. Therefore, local IPv6 support at the probe installation site is in fact not required. As such, any website with a potentially high number of accesses from the European academic community is certainly a good target site for probe deployment, irrespective of local IPv6 support.

## 2.4 Challenges

The goal of this task is to monitor IPv6 support in academic networks. In fact, while we anticipate that the probe will be mainly deployed in academic websites, recorded data will include accesses both from academic and non-academic networks. Therefore, as explained in section 2.1, it is necessary to identify the source IP and to check if the access was performed from a University network. This requires performing a reverse look-up of the source IP address, and to use public services as the IANA *whois* database and the RIPE database to identify the IP owner and, from the data collected from these services, to identify if it belongs to an academic network.

However, this task proved to be much more difficult than previously anticipated. In practice, the following challenges were identified:

1. There is not a well established database which states whether a given IP block belongs or not to a University;
2. It is not easy to obtain a full list of all Universities and Higher Education Institutions in Europe;
3. When accessing the Whois and RIPE database, several difficulties arise:
  - The RIPE database is not uniform:

- Each University may have several IP blocks;
  - Each IP block often has a quite different text description;
  - The text description is in several different languages;
  - Given the three factors above, the automatic merge of different records is difficult and its association to a single University usually requires human supervision and manual processing.
- In several cases, IP blocks belong to Faculties or other institutions within a single University. In these cases, it is required to associate these institutions to the correct University in order to have a coherent set of results. This has proven a difficult and, in several cases, an almost impossible job;
  - The official owner of a given IP block is very often outdated. With the high number of institutional name changes, merge, fusion and split of Universities observed in the last few years, the official IP databases are plenty of outdated and noisy data, to say the least;
  - IP blocks belonging to the same University do not have any information that enables their association to that University;
  - The RIPE database has a daily limit of 1000 accesses.
    - In order to partially overcome this limitation, and in order to speedup the access to the RIPE database, IST developed a local cache database, where relevant information from RIPE replies is stored. In this local database the following data is stored:
      - The IP address block;
      - If it belongs or not to a University and, if yes, the name of the University.
4. In its current form, the probe is not able to identify if the user has already made any access to the test site through some other website. In fact, the existing probe avoids duplicated daily accesses through the same website by generating a unique cookie in the domain site where the probe is deployed. However, if the same user accesses two different sites where the probe is installed, a duplicated entry is generated. While up to now this is not a relevant problem, given the limited number of websites where the probe is currently deployed, the problem may become more relevant when the number of website increases.



In order to avoid this duplicated counting, the current probe must be modified in order to generate a global cookie in a single centralized domain (e.g., gen6.tecnico.ulisboa.pt) and to forward the local probe to this target domain during the tests. At the time of writing of this report, this is still work in progress, and its effective implementation will depend on the evaluation of access data and on the number of cooperating sites where the probe will be deployed.

297239	GEN6	D5.6.1: Monitoring of IPv6 in Academic Networks
--------	------	---

### 3. PRELIMINARY RESULTS

In this section we present some results obtained from the probe installed in the website of Instituto Superior Técnico / University of Lisbon. The results described here correspond to the period from 28<sup>th</sup> of July, 2014 to 31<sup>st</sup> of October, 2014. During that period we were able to obtain the type of connection supported by the users that accessed the website. The probe gave us information on the type of connection (IPv6, IPv4 or both), the university of origin and the country of origin.

The total number of connections to the website was 206061.

In Figure 1 we present the percentage of accesses done using only IPv6, only IPv4 or both, originating from university sites. When both IPv6 and IPv4 were available we also got the preferred connection used. The percentage of connections that support only IPv6 is small, but nevertheless much higher than it was anticipated. Further analysis of the recorded raw data is still being performed in order to identify if these IPv6 only accesses are due to some small glitches occurring during the corresponding IPv4 tests.

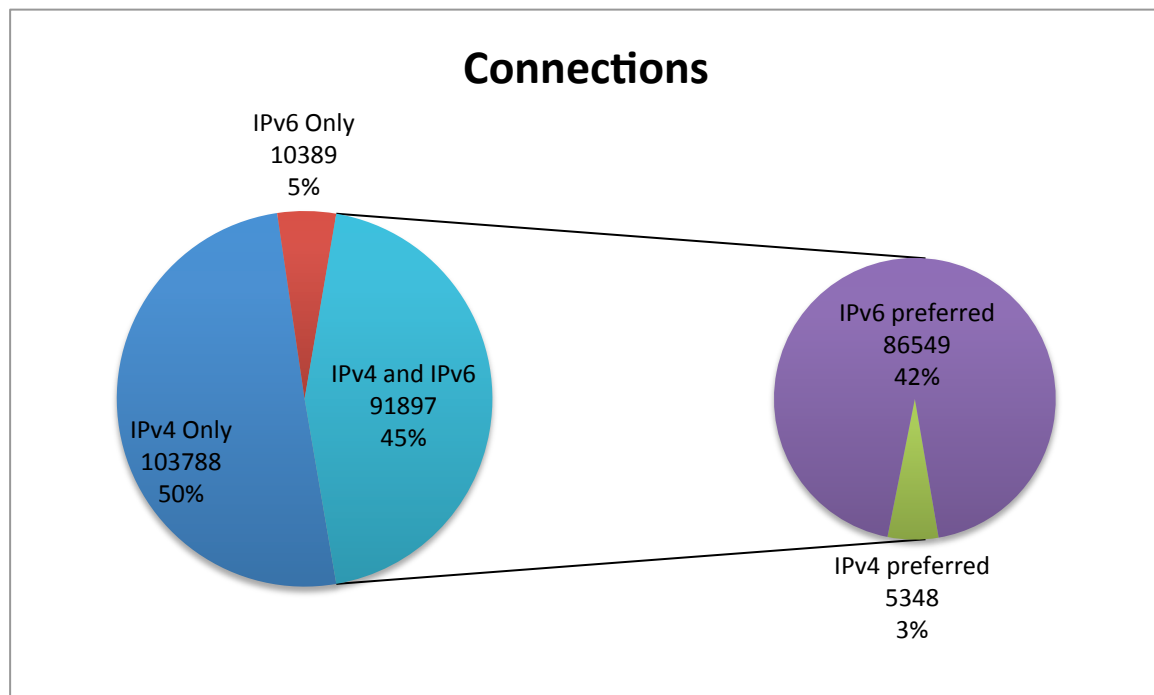


Figure 1 – Percentage of connections using IPv6, IPv4 or both.

In Table 1 we present the total number of connections made to the IST test service per university. We only list the top 20 universities, considering the number of accesses to the test site. The total number of universities that accessed the test site during the analysis period was 373. In this table we also present the number of connections made using only IPv6, only IPv4

and both. In the case where both connections could be used, we also present results of which connection type was preferred. As it would be expected, given the limited scope of the collected data, University of Lisbon (of which IST is part of) comes on top in the number of connections. Also, as it would be expected, there are several Portuguese universities in the top 20. These results will change significantly when the probe will be installed in websites of other Universities across Europe, but they show the kind of information that it is possible to collect with the developed methodology and the relevant statistical data that can be collected from this process.

While these results are quite preliminary and limited, they show that IPv6 penetration varies a lot depending on the university. One notable mention is the case of the Royal Institute Of Technology where almost 100% of the connections were made using IPv6.

Name	Country	Total	IPv6 Only	IPv4 and IPv6	IPv4 Only	IPv6 Preferred	IPv4 Preferred
Universidade de Lisboa	PT	198176	10069	91199	96908	85891	5308
Universidade Nova de Lisboa	PT	1289	0	0	1289	0	0
Universidade do Porto	PT	1259	0	198	1061	193	5
University of Coimbra	PT	548	4	44	500	40	4
Universidade de Aveiro	PT	545	12	4	529	4	0
Instituto Universitario de Lisboa	PT	441	0	0	441	0	0
Universidade do Minho	PT	375	2	105	268	97	8
Universidade da Beira Interior	PT	259	0	0	259	0	0
Universidade de Evora	PT	252	1	155	96	147	8
Universidade do Algarve	PT	232	0	0	232	0	0
Universidade Lusofona	PT	183	0	0	183	0	0
Delft University Of Technology	NL	150	0	2	148	0	2
Aalto University	FI	116	0	0	116	0	0
University Of Twente	NL	109	58	45	6	45	0
Universidade Tras-os-montes Alto Douro	PT	93	0	0	93	0	0
Karlsruhe Institute Of Technology	DE	88	10	25	10	24	1
Universidade Dos Acores	PT	86	0	0	86	0	0
Royal Institute Of Technology	SE	83	82	0	1	0	0
Katholieke Universiteit Leuven	BE	71	0	0	71	0	0

Table 1 - Number of connections to IST website per university



**Figure 2 – Percentage of connections using IPv6, IPv4 or both for the top 4 portuguese universities and the top 4 non-portuguese universities.**

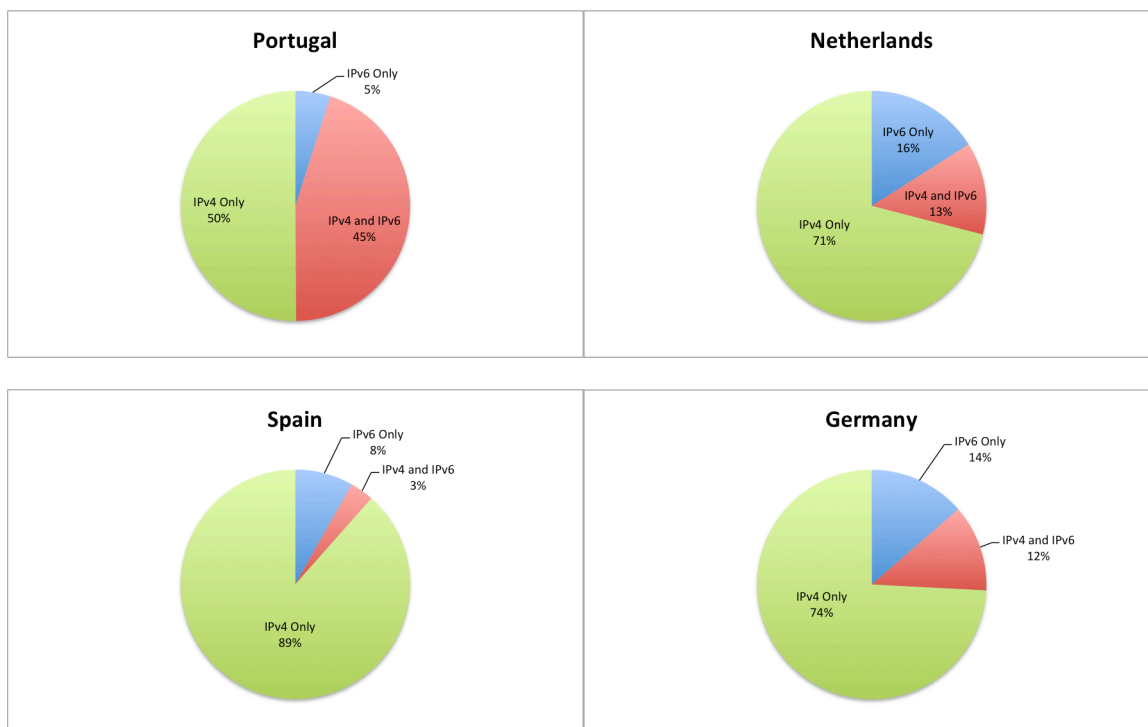
In Figure 2 we present the percentage of connections using IPv6, IPv4 or both for some universities. The universities represented in the figure are the Portuguese top 4 and the non-

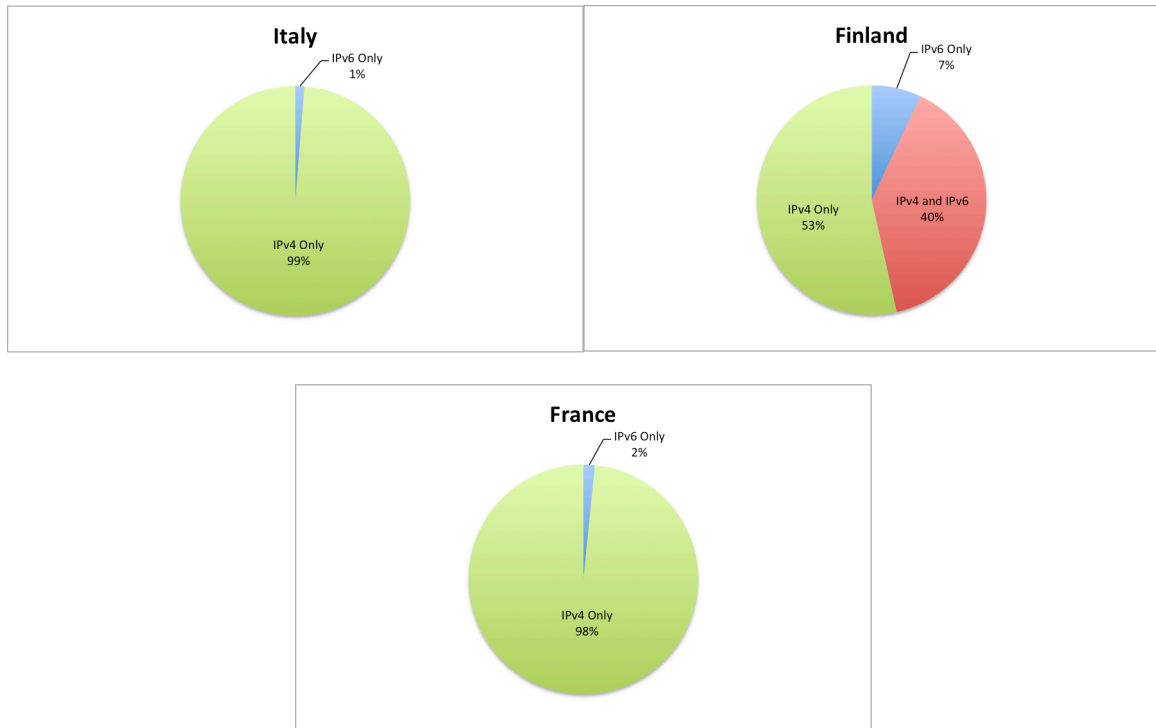
portuguese top 4. The percentage values were taken from Table 1. We can see that the values vary a lot depending on the university. With the exception of University of Lisbon, University of Twente and Karlsruhe Institute Of Technology in all others represented in Figure 2, IPv6 penetration is very residual.

**Table 2 - Number of connections to IST website per country**

Country	Code	total	IPv6 Only	IPv4 and IPv6	IPv4 Only	IPv6 Preferred	IPv4 Preferred
Portugal	PT	203973	10074	91755	102144	86416	5339
Netherlands	NL	362	58	47	257	45	2
Spain	ES	269	22	9	238	8	1
Germany	DE	213	29	26	158	25	1
Italy	IT	158	2	0	156	0	0
Finland	FI	129	9	51	69	49	2
France	FR	125	2	0	123	0	0

In Table 2 we present the total number of connections made to the IST website coming from academia per country. We only present the countries which had more than 100 accesses. In this table we also present the number of connections made using only IPv6, only IPv4 and both. In the case where both connections could be used we also present results of which connection type was preferred. As was expected, the majority of accesses were made from Portugal. This fact will change when we install the probe in more websites.

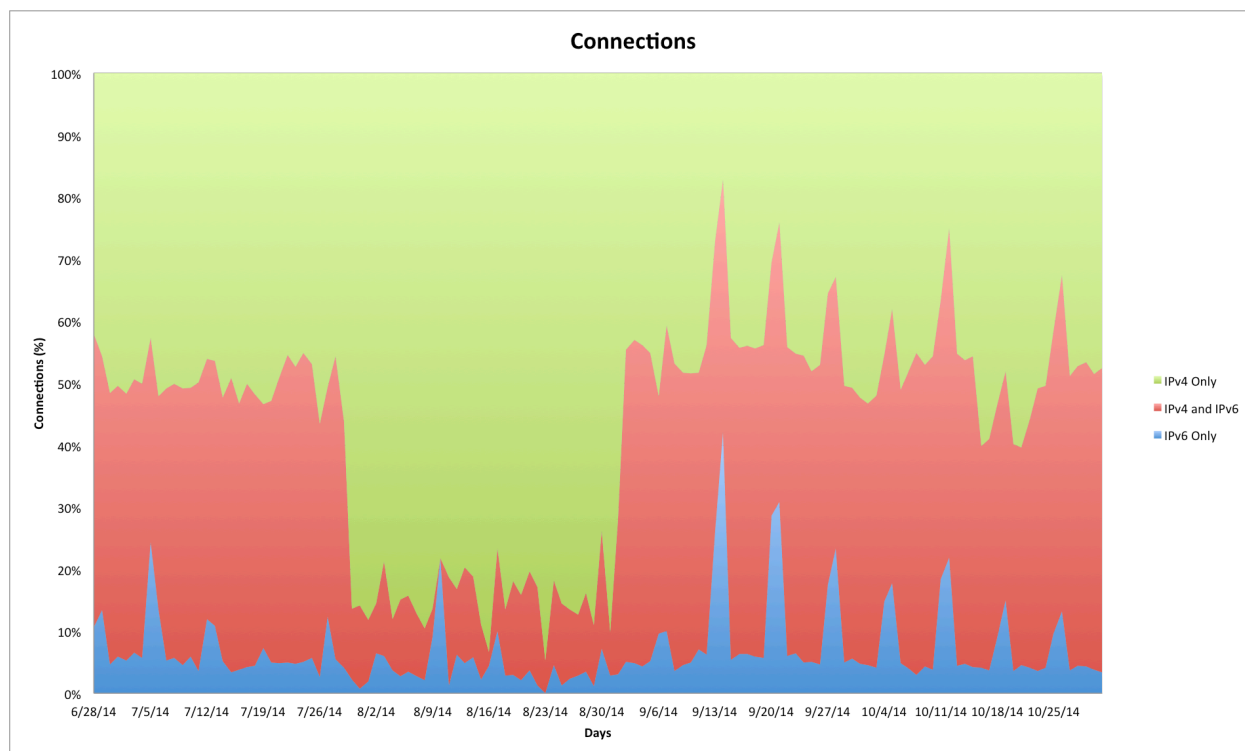




**Figure 3 - Percentage of connections using only IPv6, only IPv4 or both for the top 7 countries.**

In Figure 3 we present the percentage of connections using IPv6, IPv4 or both in academia for some countries. The countries shown are the ones with more than a 100 connections. The percentage values were taken from Table 2. We can see that the values vary significantly depending on the country. As stated before, the number of IPv6 only connections is surprisingly high and its source is still being investigated. Anyway Table 2 shows that, in this limited sample universe, the countries with more IPv6 connections are Finland and Portugal.





**Figure 4 - Evolution of IPv6, IPv4 and both connections during the period under study.**

In Figure 4 we can see the evolution in the type of accesses during the period from 28<sup>th</sup> of July, 2014 to 31<sup>st</sup> of October, 2014. In the Figure we have the percentage of accesses using only IPv6, only IPv4 or both. With the exception of the month of August (main holiday period in Portugal) the percentage of the different types of accesses were more or less constant.

## 4. DISCUSSION AND FUTURE WORK

This report describes the sensor and processing methods developed in the scope of the GEN6 project in order to assess and monitor effective IPv6 usage and support in Academic networks across Europe. As it was clear from the achieved results, the developed probe and processing methods may provide a high degree of granularity regarding the measure of IPv6 support at user level, as well as IPv6 DNS support at the user level.

The results achieved so far are quite limited in scope given that up to now most of the work was devoted to develop and test the probe capabilities and to define how to process collected data. Therefore, the probe was mainly tested and installed in IST websites. In order to obtain more meaningful results, it will be required a wide cooperation of Universities across Europe and to install the probe in the main websites of relevant Universities. This may prove to be a difficult task, since such cooperation will rely to a high degree on the goodwill of relevant officials and website administrators. While personal contacts may help on this regard, official support from a large number of institutions will be certainly difficult to obtain. In order to ease this task, it is planned to develop a GEN6 academic website, where relevant statistics will be displayed and updated in a regular basis. We expect that the launch of this site will help to promote the deployment of the sensor in the websites of relevant Universities.

Further, to achieve a wider deployment of the probe, one of the main challenges of this task is the correct mapping of IP addresses to Universities, as discussed in section 2.4. While we will attempt to be as extensive and accurate as possible, there will be always some identification errors, and it may be difficult to quantify the error margin of this approach.

Next steps for this task will include:

1. Development of the GEN6 academic website;
2. Promotion and dissemination of the probe;
3. Improvement of the statistical processing of the collected data, in order to report academic IPv6 support with deeper detail and granularity;
4. Try to improve the identification of IP blocks and its association with European Universities, in order to obtain a better and more accurate report of IPv6 usage and penetration, as well as better identification of the source Universities.

## 5. REFERENCES

[1]	RFC 1035 - DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION, <a href="https://www.ietf.org/rfc/rfc1035.txt">https://www.ietf.org/rfc/rfc1035.txt</a> . Accessed 15 sep. 2014.
[2]	IPv6 Observatoy Indicators, <a href="http://www.ipv6observatory.eu/indicators/">http://www.ipv6observatory.eu/indicators/</a> , accessed 15 Sep. 2014.
[3]	IANA whois service, <a href="https://www.iana.org/whois">https://www.iana.org/whois</a> , accessed 15 Sep. 2014.
[4]	Ripe database, <a href="http://www.ripe.net/data-tools/db">http://www.ripe.net/data-tools/db</a> , accessed 15 Sep. 2014.