

<b>Title:</b>	<b>Document Version:</b>
<b>Deliverable D3.2A</b> <b>Update on the Definition of Statistics, Management and Security Control Systems</b>	1.0

<b>Project Number:</b> IST-2001-32161	<b>Project Acronym:</b> Euro6IX	<b>Project Title:</b> European IPv6 Internet Exchanges Backbone
--	------------------------------------	--

<b>Contractual Delivery Date:</b> 30/03/2003	<b>Actual Delivery Date:</b> 01/09/2003	<b>Deliverable Type* - Security**:</b> 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> Aurora Ferrándiz	<b>Organization:</b> TID	<b>Contributing WP:</b> WP3
---	-----------------------------	--------------------------------

<b>Authors (organizations):</b> Eduardo Azañón (TID), Alberto Escolano (TID), Juan Fernández (UPM), Jesús González (TID), Gabriel López (UMU), Antonio Lucientes (TID), Mario Morelli (TILAB), Jordi Palet (Consulintel), Cristina Peña (TID), María José Perea (UPM), Álvaro Vives (Consulintel).
---

<b>Abstract:</b>  This document is an update of Deliverable D3.2.  It explains the deployment of systems to control, manage and secure Euro6IX networks.
--

<b>Keywords:</b> IDS, Looking glass, Magalia, Management of the Network, MRTG, Ping-based systems, Security, Statistics, Topaz.
--

# Revision History

The following table describes the main changes done in the document since created.

Revision	Date	Description	Author (Organization)
v0.1	31/07/2003	Document Creation	Aurora Ferrándiz (TID)
v0.2	31/07/2003	Euro6IX Management Proposal Contribution TID Ping_stat system contribution Webalizer and AWSTATS System at TID Contribution Topaz Contribution	Eduardo Azañón (TID) Aurora Ferrándiz (TID) Jesús López González (TID)
v0.3	05/08/2003	Consulintel Contribution on Smoke Ping System, Looking Glass, MRTG and AWSTATS.	Álvaro Vives (Consulintel)
v0.4	06/08/2003	UPM Contribution on Looking glass, AS-Path Tree, MRTG, Web access statistics and other Services Statistics (Nagios)	Juan Fernández (UPM) María José Perea (UPM)
v0.5	06/08/2003	TILAB Contribution	Mario Morelli (TILAB)
v0.6	07/08/2003	TID Contribution on Security Guidelines	Cristina Peña (TID)
v0.7	08/08/2003	TID Contribution on Looking Glass and MRTG	Alberto Escolano (TID) Antonio Lucientes (TID)
v0.8	11/08/2003	Summary and Conclusions	Aurora Ferrándiz (TID)
v0.9	01/09/2003	UMU Contribution	Gabriel López (UMU)
v1.0	01/09/2003	Final Review	Jordi Palet (Consulintel)

# Executive Summary

This document describes all the systems deployed by Euro6IX partners to control, manage and secure Euro6IX network.

It is also described all the systems to get statistics of the stability of the network and statistics of each partner's web service access.

# Table of Contents

<b>1.</b>	<b><i>Introduction.....</i></b>	<b>7</b>
<b>2.</b>	<b><i>Euro6IX Statistics Systems Used in Euro6IX Networks.....</i></b>	<b>8</b>
2.1	<b>Statistic Tools Based in IPv6 Ping .....</b>	<b>8</b>
2.1.1	TILAB's Ping Tool System.....	8
2.1.2	TID's Pingstat System.....	10
2.1.3	Smoke Ping at Consulintel .....	11
2.2	<b>Looking Glass System .....</b>	<b>13</b>
2.2.1	Loking Glass System at BT.....	13
2.2.2	Looking Glass System at Consulintel .....	13
2.2.3	Looking Glass System at UPM .....	14
2.2.4	Looking Glass System at TID .....	15
2.2.5	Looking Glass System at UMU .....	15
2.3	<b>TILAB's AS-Path Tree .....</b>	<b>17</b>
2.3.1	AS-Path Tree at TILAB .....	17
2.3.2	AS-Path Tree at UPM .....	18
2.4	<b>MRTG Statistics .....</b>	<b>19</b>
2.4.1	MRTG Statistics at Consulintel.....	19
2.4.2	MRTG Statistics at TID .....	21
2.4.3	MRTG Statistics at UMU.....	22
2.4.4	MRTG Statistics at UPM .....	23
2.5	<b>Web Access Statistics Implemented at Partner's Sites .....</b>	<b>24</b>
2.5.1	Webalizer .....	24
2.5.2	AWSTATS .....	25
2.5.2.1	AWSTATS at Consulintel.....	25
2.5.2.2	AWSTATS at TID .....	27
2.5.3	Web Access Statistics Implemented by UPM.....	27
2.6	<b>Other Services Statistics .....</b>	<b>28</b>
2.6.1	Nagios at UMU .....	28
2.6.2	Nagios at UPM.....	28
<b>3.</b>	<b><i>Euro6IX Management Proposal.....</i></b>	<b>30</b>
3.1	<b>Euro6IX Management System based on Magalia (MSIP) .....</b>	<b>30</b>
3.2	<b>Distributed Management Proposal to Test MSIP .....</b>	<b>31</b>
3.2.1	Objective of the Test .....	31
3.2.2	MSIP Test Description .....	31
3.2.3	MSIP Test Configuration Tips .....	31
3.2.3.1	Agreement about Naming of Nodes and Links.....	33
3.2.3.2	Message Paths .....	33
3.2.3.3	MSIP Nodes Behavior.....	33
3.2.3.4	Public and Private Maps.....	34
3.2.4	Distributed Management Proposal to test MSIP .....	34
<b>4.</b>	<b><i>Euro6IX Security Control Systems Proposal.....</i></b>	<b>35</b>
4.1	<b>Security Guidelines for Euro6IX Network .....</b>	<b>35</b>

<b>4.2</b>	<b>Topaz, an IDS Tool.....</b>	<b>37</b>
4.2.1	Topaz Application .....	37
4.2.2	Proposal of Installation of Topaz at TID Test-bed.....	39
4.2.2.1	Probably Intrusion Sources .....	39
4.2.2.2	Sensors Installation .....	39
<b>5.</b>	<b><i>Summary and Conclusions</i>.....</b>	<b>41</b>

# Table of Figures

<b>Figure 2-1:</b>	<b>TILAB Ping Tool System Web Page.....</b>	<b>9</b>
<b>Figure 2-2:</b>	<b>TID Pingstat System Web Page.....</b>	<b>10</b>
<b>Figure 2-3:</b>	<b>Other Utilities from TID Stat System.....</b>	<b>11</b>
<b>Figure 2-4:</b>	<b>MAD6IX Interfaces with Smoke Ping .....</b>	<b>12</b>
<b>Figure 2-5:</b>	<b>MAD6IX to TID Interface with Smoke Ping (I).....</b>	<b>12</b>
<b>Figure 2-6:</b>	<b>MAD6IX to TID Interface with Smoke Ping (II).....</b>	<b>13</b>
<b>Figure 2-7:</b>	<b>Consulintel's Looking Glass .....</b>	<b>14</b>
<b>Figure 2-8:</b>	<b>UPM's Looking Glass .....</b>	<b>15</b>
<b>Figure 2-9:</b>	<b>TID's Looking Glass .....</b>	<b>16</b>
<b>Figure 2-10:</b>	<b>UMU's Looking Glass.....</b>	<b>16</b>
<b>Figure 2-11:</b>	<b>TILAB's AS-Path Tree .....</b>	<b>18</b>
<b>Figure 2-12:</b>	<b>UPM's AS-Path Tree .....</b>	<b>19</b>
<b>Figure 2-13:</b>	<b>Consulintel's MRTG Statistics (I).....</b>	<b>20</b>
<b>Figure 2-14:</b>	<b>Consulintel's MRTG Statistics (II) .....</b>	<b>20</b>
<b>Figure 2-15:</b>	<b>TID's MRTG Statistics (I).....</b>	<b>21</b>
<b>Figure 2-16:</b>	<b>TID's MRTG Statistics (II).....</b>	<b>22</b>
<b>Figure 2-17:</b>	<b>TID's MRTG Statistics (III).....</b>	<b>22</b>
<b>Figure 2-18:</b>	<b>UMU's MRTG Statistics.....</b>	<b>23</b>
<b>Figure 2-19:</b>	<b>UPM's MRTG Statistics .....</b>	<b>24</b>
<b>Figure 2-20:</b>	<b>TID Statistics of Access to <a href="http://www.tid.euro6ix.org">www.tid.euro6ix.org</a> using Webalizer .....</b>	<b>25</b>
<b>Figure 2-21:</b>	<b>Home of Euro6IX Web Site Statistics .....</b>	<b>26</b>
<b>Figure 2-22:</b>	<b>Example of Euro6IX Web Site Statistics .....</b>	<b>26</b>
<b>Figure 2-23:</b>	<b>TID Statistics of Access to <a href="http://www.tid.euro6ix.org">www.tid.euro6ix.org</a> using AWSTATS .....</b>	<b>27</b>
<b>Figure 2-24:</b>	<b>UPM's Access Statistics .....</b>	<b>27</b>
<b>Figure 2-25:</b>	<b>UMU's Nagios Service.....</b>	<b>28</b>
<b>Figure 2-26:</b>	<b>UPM's Nagios Service.....</b>	<b>29</b>
<b>Figure 3-1:</b>	<b>Euro6IX Network Map Design.....</b>	<b>32</b>
<b>Figure 3-2:</b>	<b>MSIP Operation Through Euro6IX Network Map .....</b>	<b>34</b>
<b>Figure 4-1:</b>	<b>Traffic Control in the Carrier's Network .....</b>	<b>35</b>
<b>Figure 4-2:</b>	<b>Traffic Control in the ISP's Network .....</b>	<b>36</b>
<b>Figure 4-3:</b>	<b>Traffic Control in the IPv6 Internet Exchange.....</b>	<b>36</b>
<b>Figure 4-4:</b>	<b>Sensor Log messages.....</b>	<b>38</b>
<b>Figure 4-5:</b>	<b>Topaz Console Snapshot.....</b>	<b>38</b>
<b>Figure 4-6:</b>	<b>TID Test-Bed.....</b>	<b>39</b>
<b>Figure 4-7:</b>	<b>Topaz Installation Proposal at TID Test-Bed .....</b>	<b>40</b>

## 1. INTRODUCTION

During the second year of the project the work has been focused on the installation of services to generate traffic and the installation of system to control this traffic.

Web statistics systems have been installed on every web server to know whom and how many times has accessed the web.

Also, new statistics systems to control the stability of the network have been installed like Smoke Ping, MRTG and Nagios; TID ping-stat system has been improved with new functionalities.

Regarding Network Management, Magalia has become a reference in the development of applications to control New Generation Networks and other partners like UPM has installed it and they use it to control its network. Other partners like BT, Consulintel, PTIN, T-Nova, UMU, Vodafone have showed their interest in installing the application.

In this document, the Magalia Sharing Management feature it is explained and a proposal for testing with other partners it is formulated.

Another area of work of the project is the Security of the Network. Before opening the net to the rest of the rest of the world a security policy had to be defined. The results of this definition are the “Security Guidelines for Euro6IX Network” which are explained in chapter 4.

A tool that will help Euro6IX to make more secure networks is Topaz, a NIDS (Network Intrusion Detection System) developed at TID labs. This year Topaz developing team has been working with A4.1-1 in order to define the set of rules to be watched by the application. In this document, Topaz is presented with snapshots and a brief explanation of its features. There is also a proposal to test this application at TID labs.

## 2. EURO6IX STATISTICS SYSTEMS USED IN EURO6IX NETWORKS

### 2.1 Statistic Tools Based in IPv6 Ping

#### 2.1.1 TILAB's Ping Tool System

Ping-view (<http://net-stats.ipv6.tilab.com/6boneBB/index.html>) is a tool that provides some useful information about the connectivity towards a specific set of destinations in the Internet (both host and routers). The reachability information for every monitored site includes the packet loss (i.e. the number of echo replies not coming back versus the number of echo requests transmitted) and the response time (RTT, Round Trip Time). The basic mechanism used is the sending of ICMP packets (i.e. ping packets) and then, using the RTT and loss values obtained, some parameters are measured to evaluate the performances of the network. In particular, this tool sends fixed length sequences of ICMP echo requests, one per second, towards all the selected destinations using the ping program.

Note that the answer to the first echo request of every sequence is always rejected because it is usually slower than the others (caches priming, etc).

The acquisition of the reachability information towards all the monitored sites is repeated periodically (generally once an hour). At every data acquisition, the measured values (loss and response time) are recorded in an archive in order to be available for further analysis and elaborations. In particular, this information is used to create various kinds of graphic representations of the collected data (including loss and RTT versus time, loss and RTT frequency distributions, the Quality Factor and the Service Predictability) and some history-based parameters ("RTT70% - last 7 days" and trend).

Ping-view provides moreover an aggregated view, showing a summary table containing an estimation of the overall "group of connections" behavior together with an indication of the medium term trend (time-scale of days).

Using this tool is also possible to detect an occasional degradation in the performance of the communications looking at the summary table displaying the results of the latest measures. In order to provide some information about the medium term evolution of the network performance (i.e. if they are improving or if they are getting worse), it is compared an effective bit rate value calculated from loss and response time values measured over the last 7 days (medium term network performance) with the one calculated over the last 4 hours (short term network performance). The effective bit rate is calculated as follows:

$$(2 * \text{bytes in ping packet} * 8) * (\text{total packets} - \text{packets lost}) / \text{total packets} / \text{average response time}$$

An improved bit rate in the last last 4 hours is shown as a positive trend, while a slower bit rate in the last last 4 hours is shown as a negative trend. If on the other hand the two values are very close together an indication of substantial stability in the network performance is returned.



Thanks to the measures obtained with ping-tool, it is also possible to evaluate a quality parameter called “Quality Factor” that is an estimate of the probability of getting an answer to an ICMP Echo Request within a given RTT\* and is calculated as the number of Echo replies obtained back within RTT\* versus the total number of Echo requests sent to the destination(s). This parameter is calculated from the loss and RTT values collected during a given time frame.

The Quality Factor (QF) is a function of RTT\* and gets values in the range [0,1]. A low value of QF(RTT\*) indicates low connection performances while a value of QF(RTT\*) very close to 1 stands for good performances.

Moreover, this tool permits to obtain a measure of the variability of service (or ping predictability) by means of a scatter plot of the dimensionless variables (average ping data rate / maximum ping data rate) versus the (average ping success/maximum ping success) where:

- Ping success = (total packets - packets lost) / total packets).
- Ping data rate = (2 \* bytes in ping packet) / response time.

The service predictability parameter has been defined at SLAC (Stanford Linear Accelerator Center) by Les Cottrell, Warren Matthews and Connie Logg (see the SLAC tutorial on WAN monitoring). For short timeframes (up to 24 hours), the average ping success and data rate are evaluated for every data acquisition. For longer timeframes, they are averaged on a daily basis.

The following picture shows an example of aggregate and site-by-site view using ping-view tool.

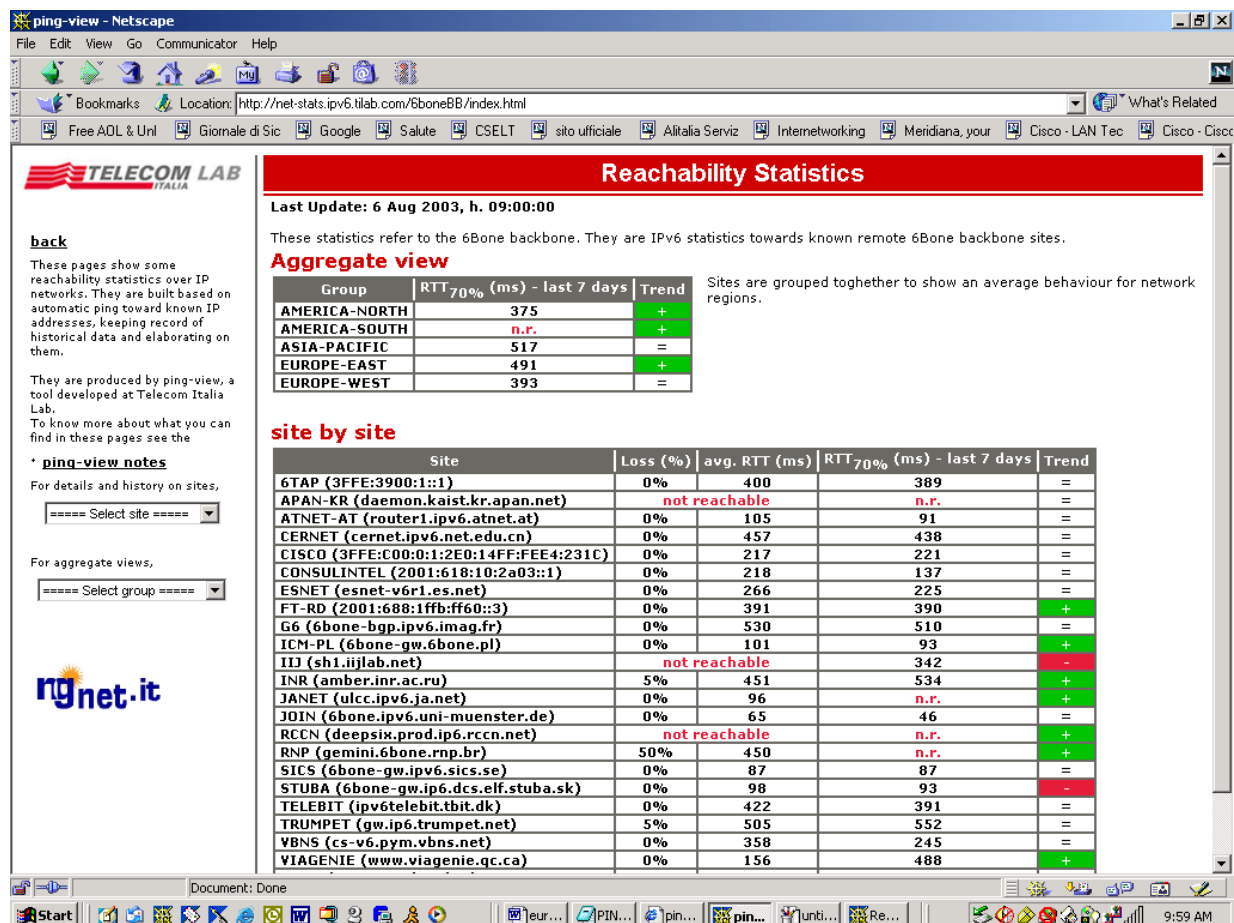


Figure 2-1: TILAB Ping Tool System Web Page

## 2.1.2 TID's Pingstat System

The 'ping\_stat' tool has been developed by TID in the context of the LONG project and allows checking the reachability of network elements by executing "ping" to a list of IPv6 addresses. The results will be transferred to a second machine using the "wget" IPv6 enabled tool. This second machine shows, through a WEB interface, the graphics generated using the information retrieved.

In the context of Euro6IX project, this statistics system has been improved adding new operation features and changes in the system architecture.

All local sites currently reachable from TID (Consulintel, UMU, UPM, ...) and IX nodes (MAD6IX, LIS6IX, LON6IX, PAR6IX, BER6IX) have provided a stable host/router interface, which is periodically checked by the "ping\_stat" tool. Each fifteen minutes a loss/delay measure is taken, although WEB server updates are made each hour to reduce traffic generated by "wget").

This system is used only by TID and the results are offered through this URL: <http://stat6.tid.euro6ix.org>.



Figure 2-2: TID Pingstat System Web Page

This URL offers the possibility to recover past statistics results of a concrete day, and every month it generates a graphic that represents an average of the data collected every day during the whole month. This average is created with the sum of the Nth values collected every day for a concrete node and dividing it by the number of measures taken for that node.

If there are no measures for a day, the represented value in this case in the DELAY graphic is 0%, in the case of LOSS graphic, is 100%.

This monthly statistics are included in Monthly Reports since March Report.

It also offers the possibility to make a ping or telnet to a host and to add a new host to be monitored by the system.



**Figure 2-3: Other Utilities from TID Stat System**

Next feature to be implemented is the sending of mail alerts to the Network administrator when a node controlled by the system is down.

During Madrid 2003 Global IPv6 Summit, this system controlled the demo router and the demo hosts stability and reachability.

### **2.1.3 Smoke Ping at Consulintel**

The SmokePing tool (<http://people.ee.ethz.ch/~oetiker/webtools/smokeping>) allows monitoring several IPv6 addresses, using a user-friendly web interface that organizes the ping points in a hierarchical way.

Consulintel have installed SmokePing to monitor several points within Euro6IX network. This way several partner's hosts and IX's interfaces are being monitored. Using this system, changes and breakdowns in the network are being detected in an easy and quick way.

Consulintel's SmokePing web site could be accessed, using project's user and password, in <http://www.consulintel.euro6ix.org>. Just click on Euro6IX Private and in Ping6 Statistics.

Following some snapshots are showed:

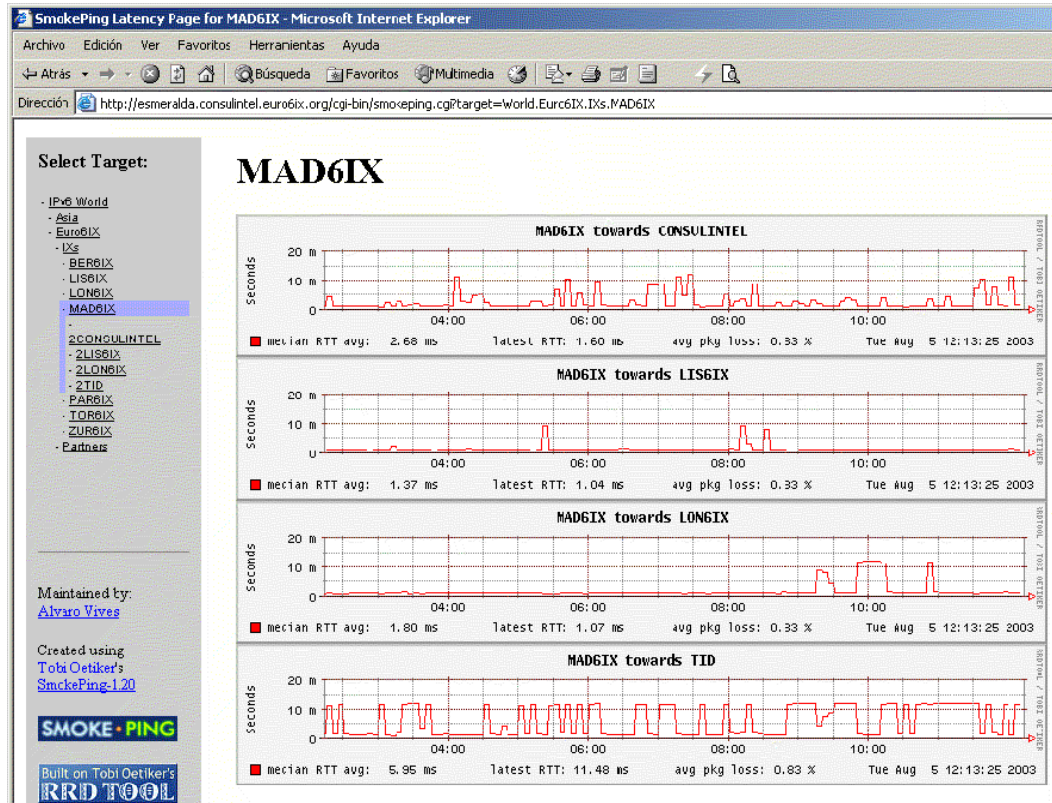


Figure 2-4: MAD6IX Interfaces with Smoke Ping

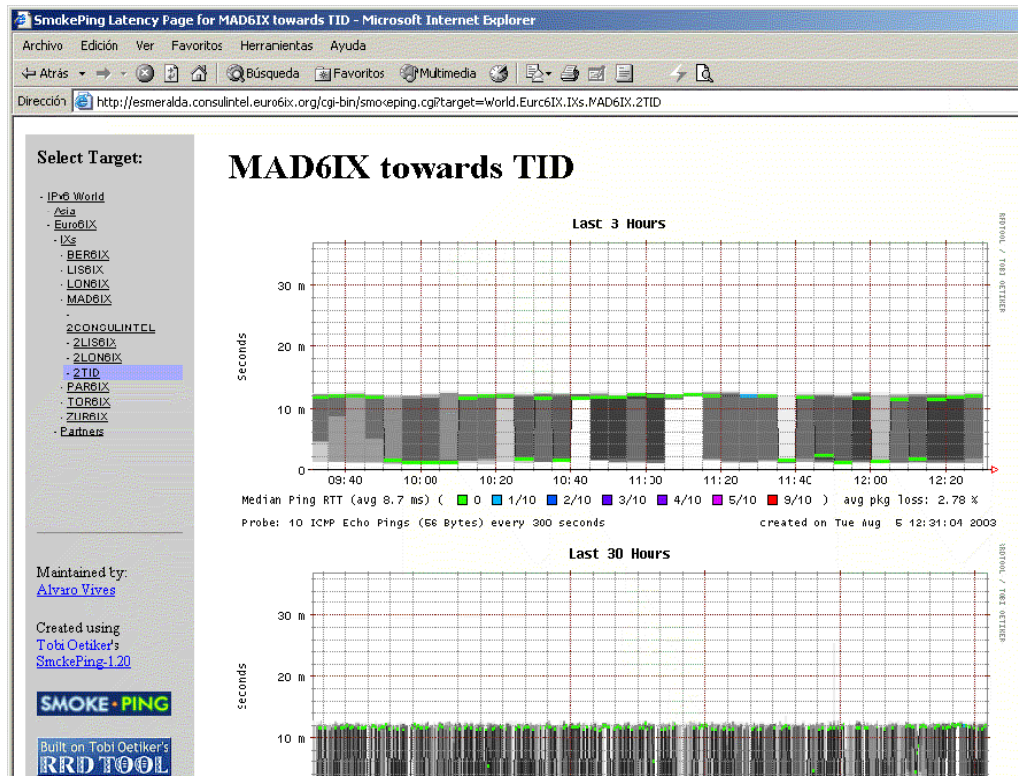


Figure 2-5: MAD6IX to TID Interface with Smoke Ping (I)



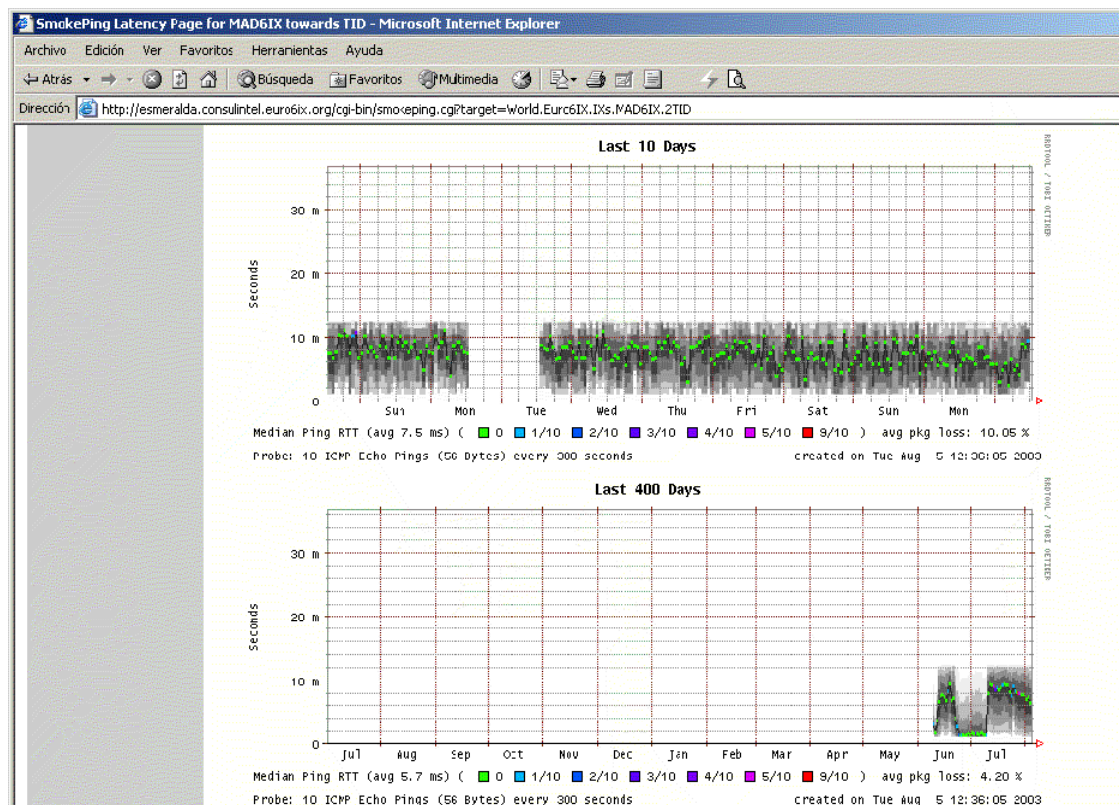


Figure 2-6: MAD6IX to TID Interface with Smoke Ping (II)

## 2.2 Looking Glass System

The Looking Glass is a software tool that provides a secure web based interface to a number of common IP tools.

### 2.2.1 Looking Glass System at BT

Looking Glass System at BT is already described in D3.2 “Definition of Statistics, Management and Security Control Systems” and more exactly its 2.3 section called “BT Looking glass System”.

### 2.2.2 Looking Glass System at Consulintel

Consulintel has developed its own Looking Glass software, within the project. It could be accessed in <http://www.consulintel.euro6ix.org> in the Public Services menu or just using <http://lg.consulintel.euro6ix.org>.

It provides ping and traceroute tools both with IPv4 and IPv6 functionalities, and also the dig tool to perform DNS queries.

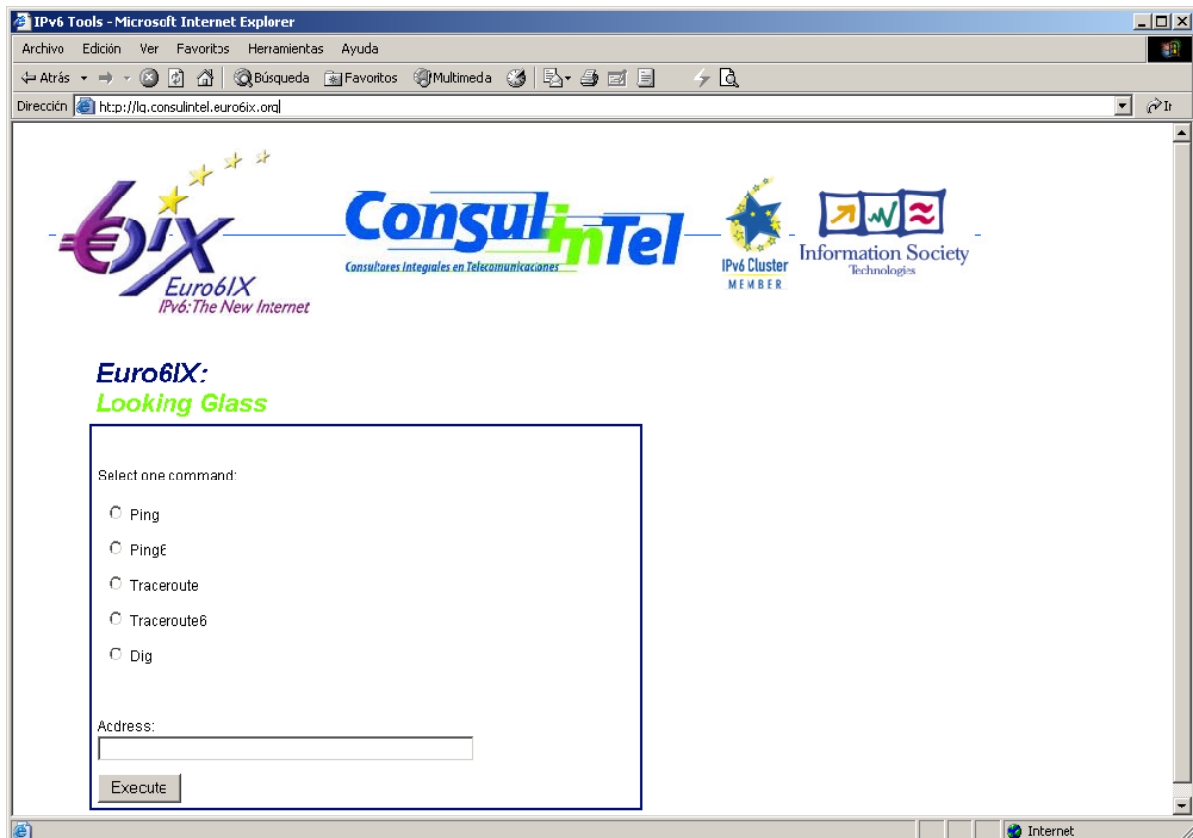


Figure 2-7: Consulintel's Looking Glass

### 2.2.3 Looking Glass System at UPM

This tool is available through the UPM Euro6IX Web page:

<http://www.upm.euro6ix.org/cgi-bin/looking-glass-upm-v0.6/ntools.pl>

The network tools provided by looking glass are divided in four sections:

- Network trace commands: This sections includes ping, traceroute and mrtg (IPv4 and IPv6).
- DNS commands: dig with all the possible options: ANY, A, AAAA, PTR, MX, NS, CNAME.
- BGP, BGP4+ diagnostic commands: sh bgp ipv6 summary, sh bgp ipv6, sh bgp ipv6, sh bgp ipv6 neighbours, sh bgp ipv6 advertised-routes, sh bgp ipv6 neighbour routes, sh bgp summary, sh bgp, sh bgp neighbours.
- Routing Display commands: sh ipv6 route (bgp, connected, local, rip, static, summary).

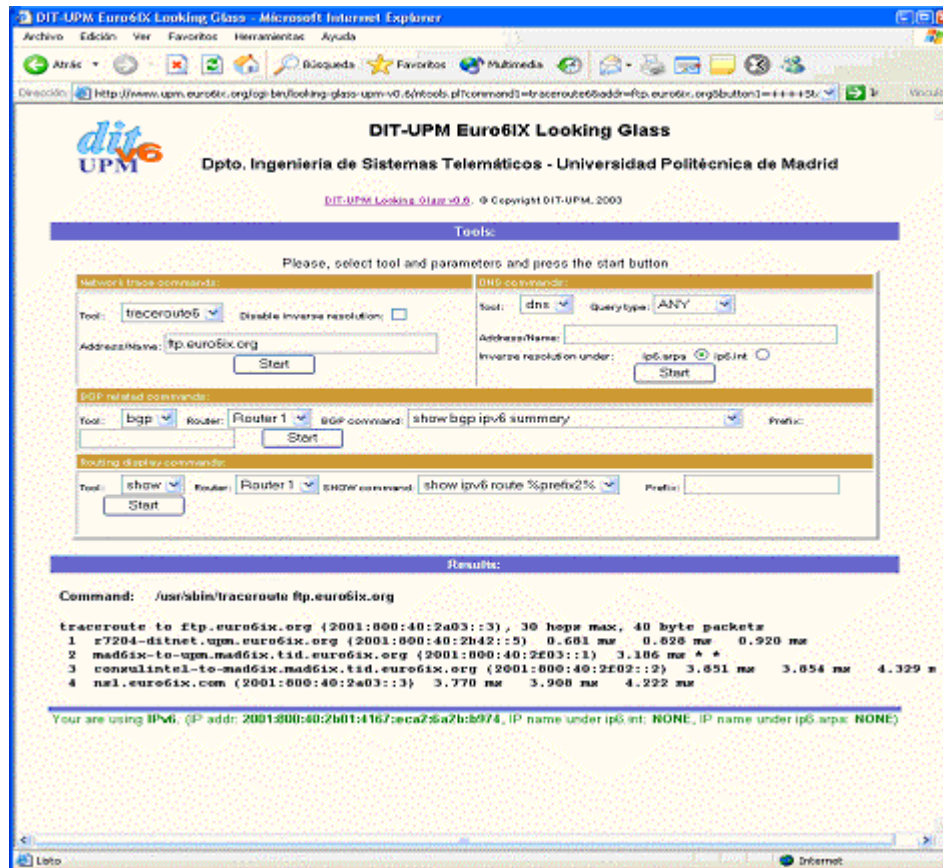


Figure 2-8: UPM's Looking Glass

## 2.2.4 Looking Glass System at TID

The Looking Glass system installed at TID (Telefónica R&D) is the one developed by the UPM.

This tool is accessible through the TID Euro6IX web page: <http://lg.tid.euro6ix.org/cgi-bin/ntools.pl>.

Include the same tools as in the UPM one.

## 2.2.5 Looking Glass System at UMU

The Looking Glass application installed at UMU is the one developed by the UPM.

This tool is available through the UMU Euro6IX Web page: <http://www.umu.euro6ix.org/cgi-bin/router-lan/ntools.pl>.

Include also the same tools as in the UPM one.

**TID-Euro6IX Looking Glass - Mozilla**

File Edit View Go Bookmarks Tools Window Help

Back Forward Reload Stop

http://tld.euro6ix.com/cgi-bin/tools.pl?command1=traceroute&addr=mrtg.tld.euro6ix.com&

Search Print

**Telefonica** Telefónica Investigación y Desarrollo

**TID-Euro6IX Looking Glass**  
TID - Telefónica Investigación y Desarrollo

DIT-UPM Looking Glass v0.6 Copyright DIT-UPM, 2003

**Tools:**

Please, select tool and parameters and press the start button

**Network trace commands:**

Tool: **traceroute6** Disable inverse resolution: ☐

Address/Name: **mrtg.tld.euro6ix.com** Start

**DNS commands:**

Tool: **dns** Query type: **ANY**

Address/Name: Inverse resolution under: **ip6.arpa** ☒ **ip6.int** ☐ Start

**BGP related commands:**

Tool: **bgp** Router: **6IXGATE** BGP command: **show bgp ipv6 summary** Prefix: Start

**Routing display commands:**

Tool: **show** Router: **6IXGATE** SHOW command: **show ipv6 route %prefix2%** Prefix: Start

**Results:**

Command: **/usr/sbin/traceroute6 mrtg.tld.euro6ix.com**

traceroute to mrtg.tld.euro6ix.com (2001:800:40:2301::101) from 2001:800:40:2301::102, 30 hops max, 16 byte packets

1 core1-cgc.tld.euro6ix.org (2001:800:40:2301::6) 0.84 ms 0.671 ms 0.655 ms

2 mrtg.tld.euro6ix.org (2001:800:40:2301::101) 1.196 ms 1.134 ms 1.073 ms

You are using IPv6. (IP addr: 2001:800:40:2200:201:2ff:feac:f45b, IP name under ip6.int: nemuru.tld.euro6ix.org., IP name under ip6.arpa: nemuru.tld.euro6ix.org.)


Document: Done (0.591 secs)

prueba@nemu emacs@nemu prueba@nemu prueba@nemu TID-Euro6IX L

prueba@nemu root@cocodril prueba@nemu prueba@nemu VLC (Gtk+ inte

19:18

Figure 2-9: TID's Looking Glass

 **UMU Euro6IX Looking Glass - Router LAN (HemIs)**

Dpto. de Ingeniería de la Información y las Comunicaciones - Universidad de Murcia

**Tools:**

Please, select tool and parameters and press the start button

**Network trace commands:**

Tool: **ping6** Disable inverse resolution: ☐

Address/Name: **www.euro6ix.org** Start

**DNS commands:**

Tool: **dns** Query type: **ANY**

Address/Name: Inverse resolution under: **ip6.arpa** ☒ **ip6.int** ☐ Start

**BGP related commands:**

Tool: **bgp** BGP command: **show bgp ipv6 summary** Prefix: Start

**Results:**

Command: **/usr/sbin/ping6 -c 5 -w 7 www.euro6ix.org**

PING **www.euro6ix.org**(ns1.euro6ix.com) 56 data bytes

64 bytes from ns1.euro6ix.com: icmp\_seq=0 hops=60 time=18.191 msec

64 bytes from ns1.euro6ix.com: icmp\_seq=1 hops=60 time=29.936 msec

Figure 2-10: UMU's Looking Glass



## 2.3 TILAB's AS-Path Tree

ASpath-tree is a tool to perform IPv6 network operation analysis based on the snapshot of the BGP routing table on IPv6 routers running BGP. Originally designed to be used by an IPv6 site involved in the experimentation of the BGP protocol inside the 6Bone network, it now supports a set of features useful within any operational IPv6 network, which makes use of BGP.

### 2.3.1 AS-Path Tree at TILAB

ASpath-tree is a tool developed by TILAB in order to collect information about routing inside an IPv6 network based on the snapshot of the BGP routing table on IPv6 routers running BGP. It was originally designed to be used by an IPv6 site involved in the experimentation of the BGP protocol inside the 6Bone network, and now it supports a set of features useful within any operational IPv6 network that makes use of BGP.

Based on a single snapshot of the IPv6 BGP table, ASpath-tree automatically generates, every 5 minutes, a set of HTML pages providing a graphical view of the routing paths towards the other IPv6 connected domains. Moreover it allows detecting anomalous route entries announced through BGP (invalid prefixes and unaggregated prefixes), anomalous AS numbers (i.e. reserved or private) and a set of summary information such as:

- The number of route entries (valid/total/suppressed/damped/history).
- The number of AS in table (total, originating only, originating/transit, transit only, private and reserved).
- The number of active AS paths.
- The number of active BGP neighbors (i.e. announcing routing information).
- An analysis of the network size, in terms of AS distances.
- The number of circulating prefixes (total, 6Bone pTLAs, sTLAs, 6to4, others).

Based on repeated snapshots of the IPv6 BGP table at different points in time, ASpath-tree automatically generates HTML pages reporting on BGP routing stability (last 24 hours) for:

- 6Bone pTLAs.
- RIR's assigned sTLAs.

The outputs are obtained elaborating the AS path information of all the BGP routing entries available on an IPv6 router.

In Telecom Italia Lab, ASpath-tree is being used in order to monitor TILAB's IPv6 BGP routing configuration. These pages are automatically updated every 5 min.

At the time of writing, the current version of the AS-Path tree tool is 4.2.

The following figure shows an example of the global IPv6 BGP table:

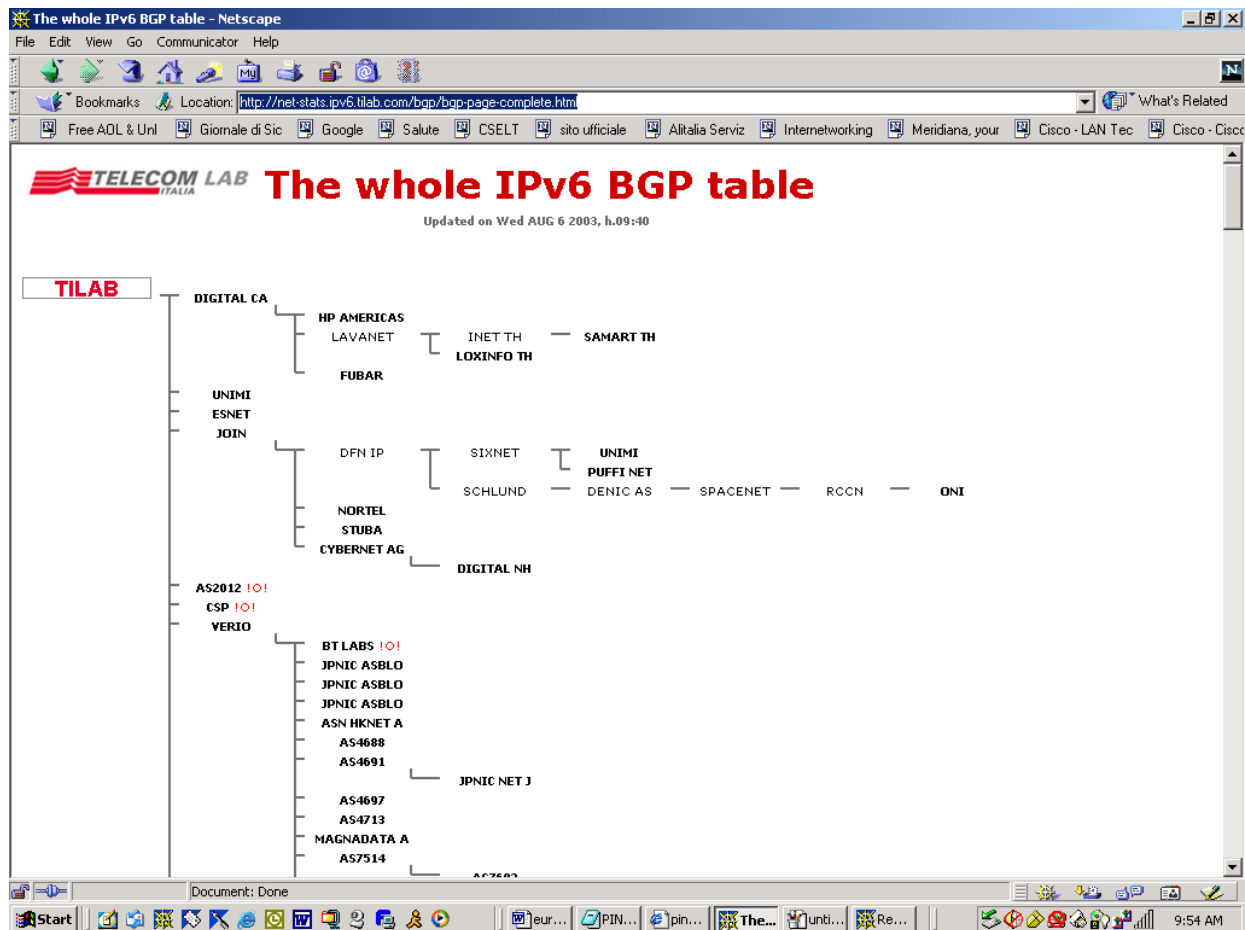


Figure 2-11: TILAB's AS-Path Tree

### 2.3.2 AS-Path Tree at UPM

This tool is available through the UPM Euro6IX Web page:

<http://www.upm.euro6ix.org/bgp/bgp.html>

ASpath-tree automatically generates a set of html pages providing a graphical view of the routing paths towards the other IPv6 connected domains. Additionally it provides pages for the detection of anomalous route entries announced through BGP (invalid prefixes and unaggregated prefixes), anomalous AS numbers (i.e. reserved or private) in use and a set of summary information.

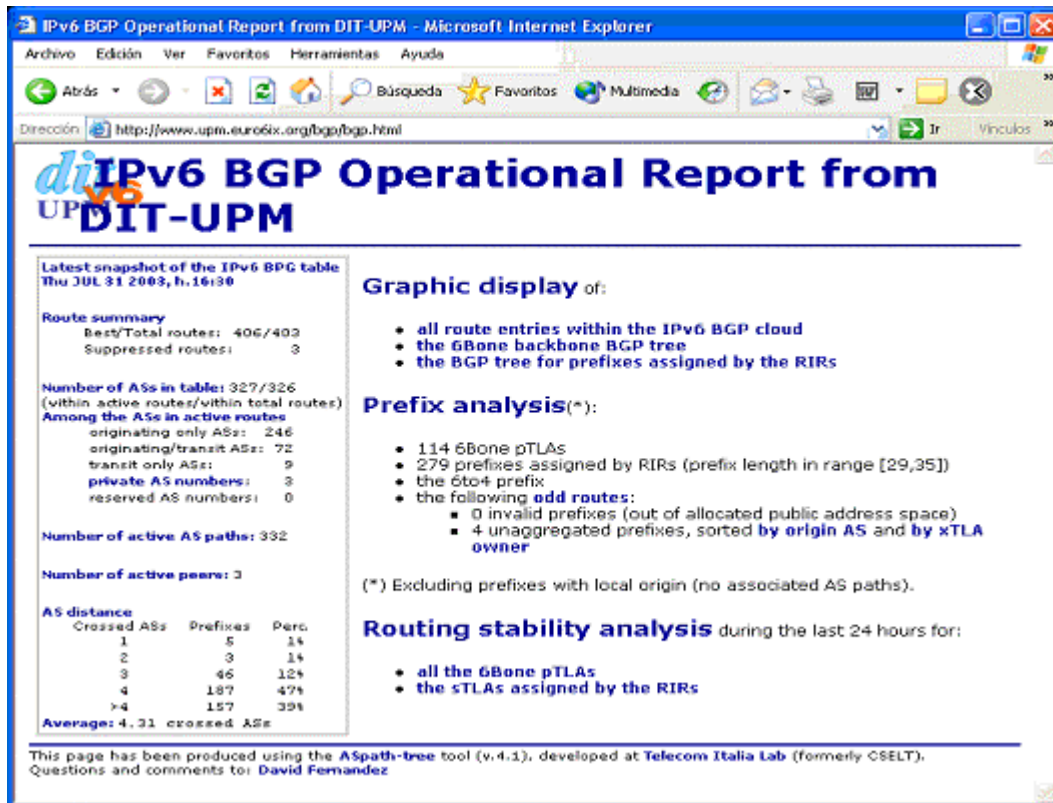


Figure 2-12: UPM's AS-Path Tree

## 2.4 MRTG Statistics

### 2.4.1 MRTG Statistics at Consulintel

Consulintel has MRTG statistics of its link towards MAD6IX. They are accessible through <http://www.consulintel.euro6ix.org> (Euro6IX Private menu, Traffic Statistics option). In order to access the MRTG graphics you need to know the project user and password.

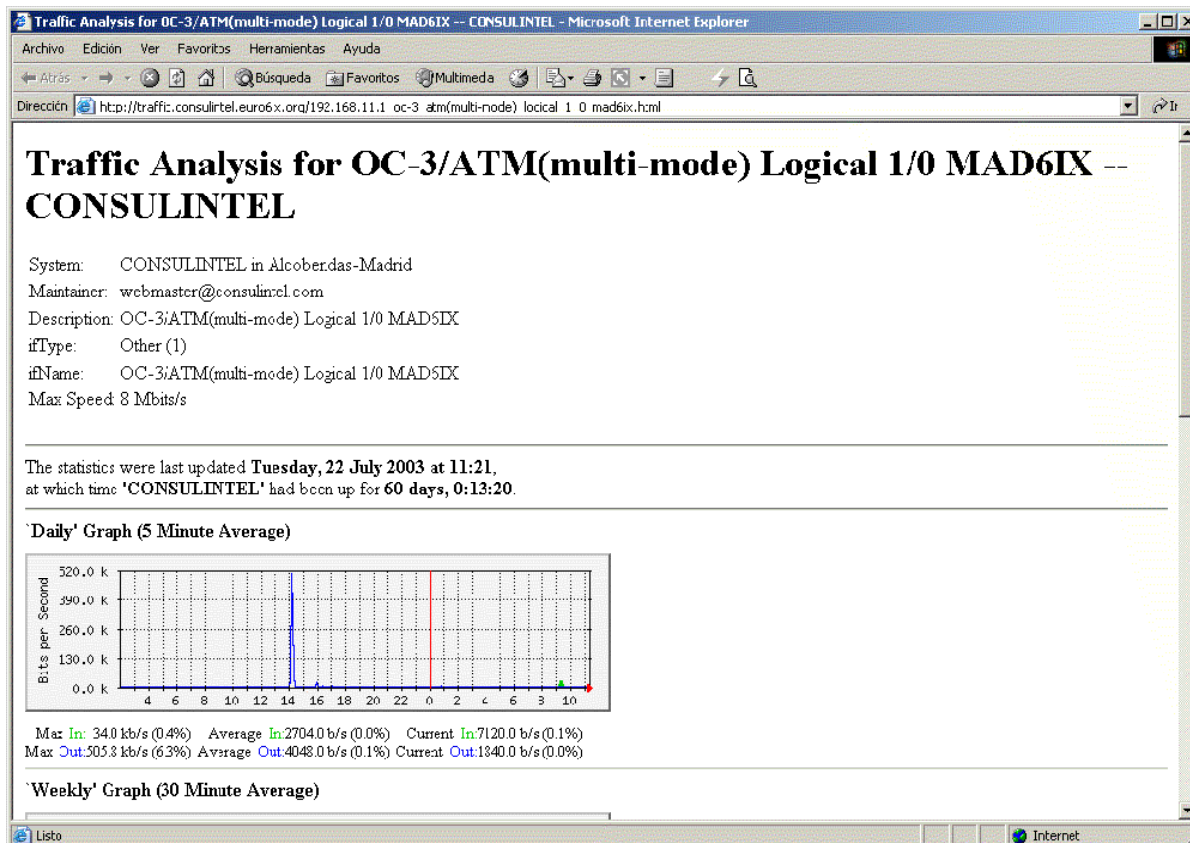


Figure 2-13: ConsulinTEL's MRTG Statistics (I)

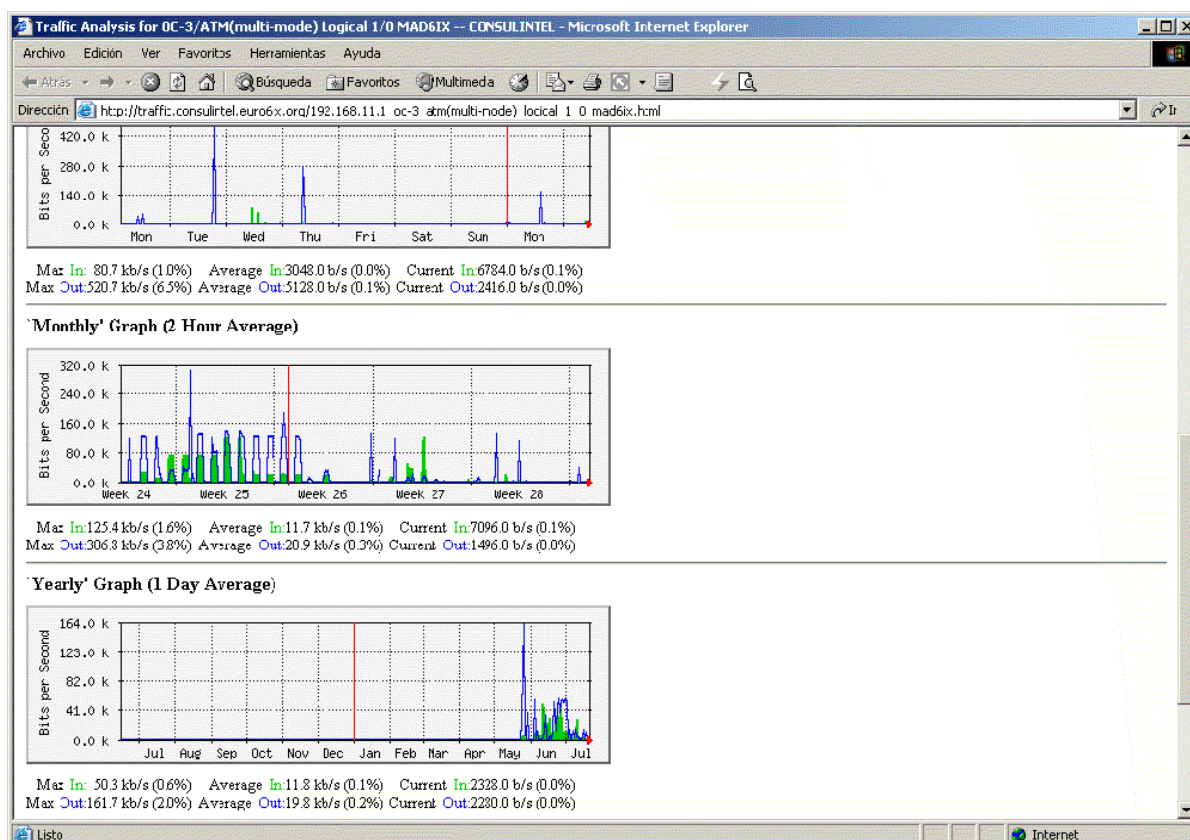


Figure 2-14: ConsulinTEL's MRTG Statistics (II)

## 2.4.2 MRTG Statistics at TID

The main MRTG web page where every link in Telefonica R&D premises can be monitored is accessible in this URL: <http://mrtg.tid.euro6ix.org/mrtg>.

Another way easier to see the MRTG statistics system installed at TID is accessible through the TID Euro6IX web page: <http://www.tid.euro6ix.org>.

To view the MRTG graphic for each link the user must pass the mouse pointer over the link to be monitored.

In the **Networks** section of the web page (<http://www.tid.euro6ix.org>), there are three different network levels:

- Euro6IX: Links from MAD6IX to LIS6IX and LON6IX.

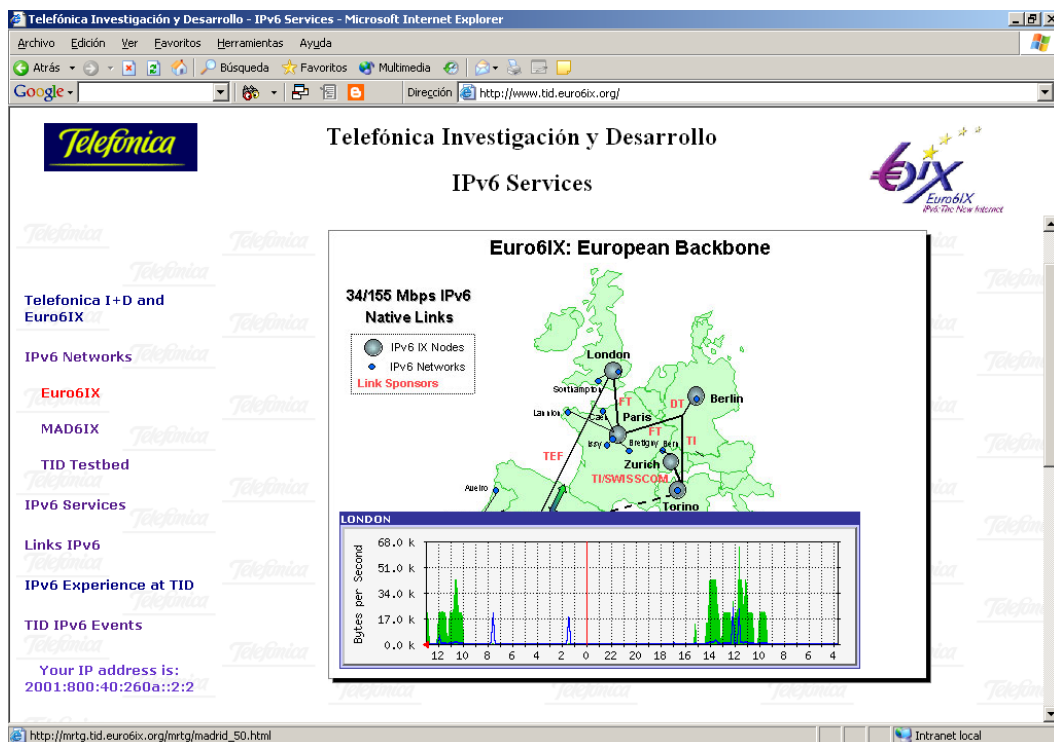


Figure 2-15: TID's MRTG Statistics (I)

- MAD6IX: Links inside MAD6IX with other national partners (Consulintel, UPM, TID, Vodafone).

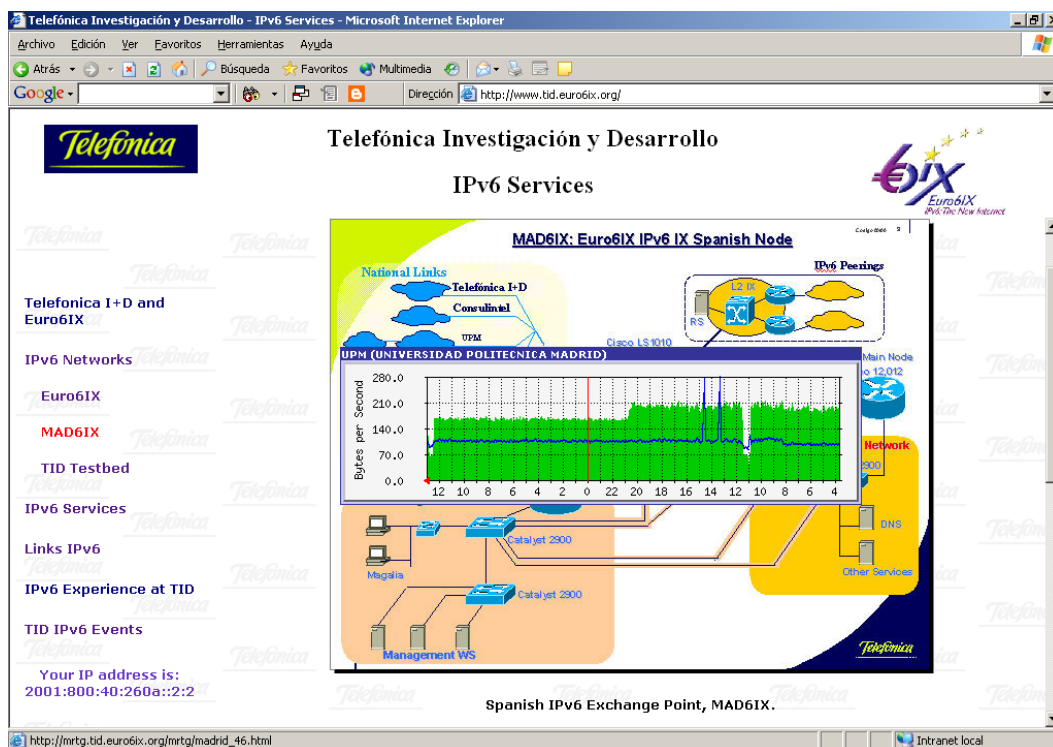


Figure 2-16: TID's MRTG Statistics (II)

- TID Test-bed: Links inside TID's IPv6 Network.

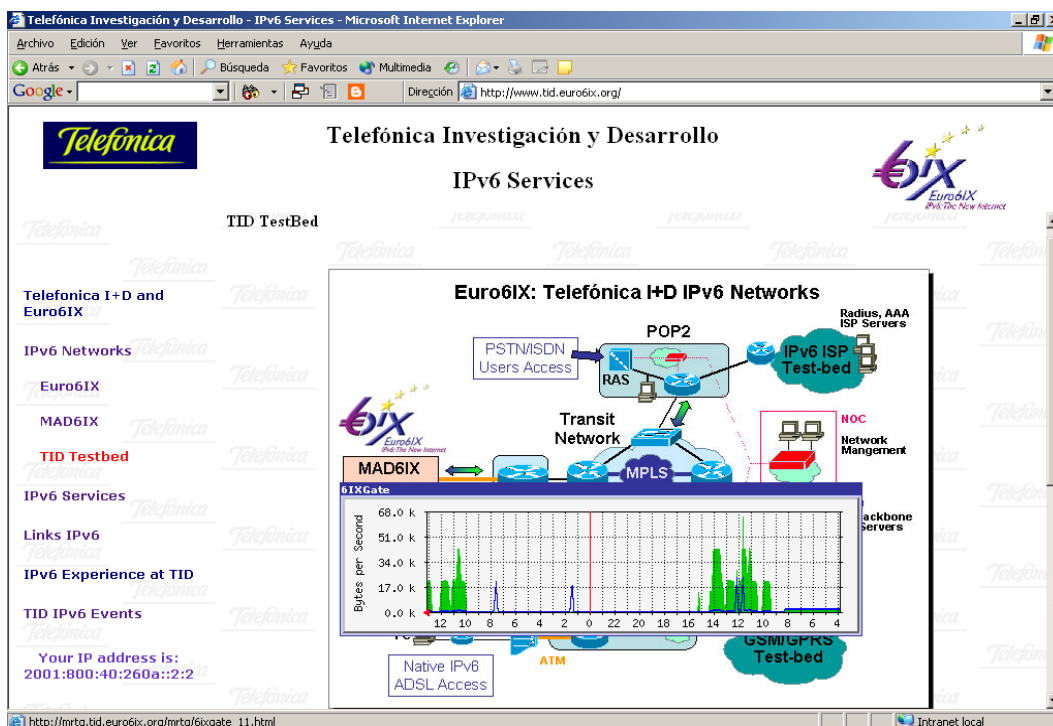


Figure 2-17: TID's MRTG Statistics (III)

### 2.4.3 MRTG Statistics at UMU

This tool is available through the UMU Euro6IX Web page:



<https://nagios.umu.euro6ix.org/mrtg6/>

To access it, you must present a valid Euro6IX Public Key Certificate, to get one go to <https://pki.umu.euro6ix.org/index.html>.

It shows MRTG statistics of all the UMU connection to the IPv6 world, including Euro6IX backbone.

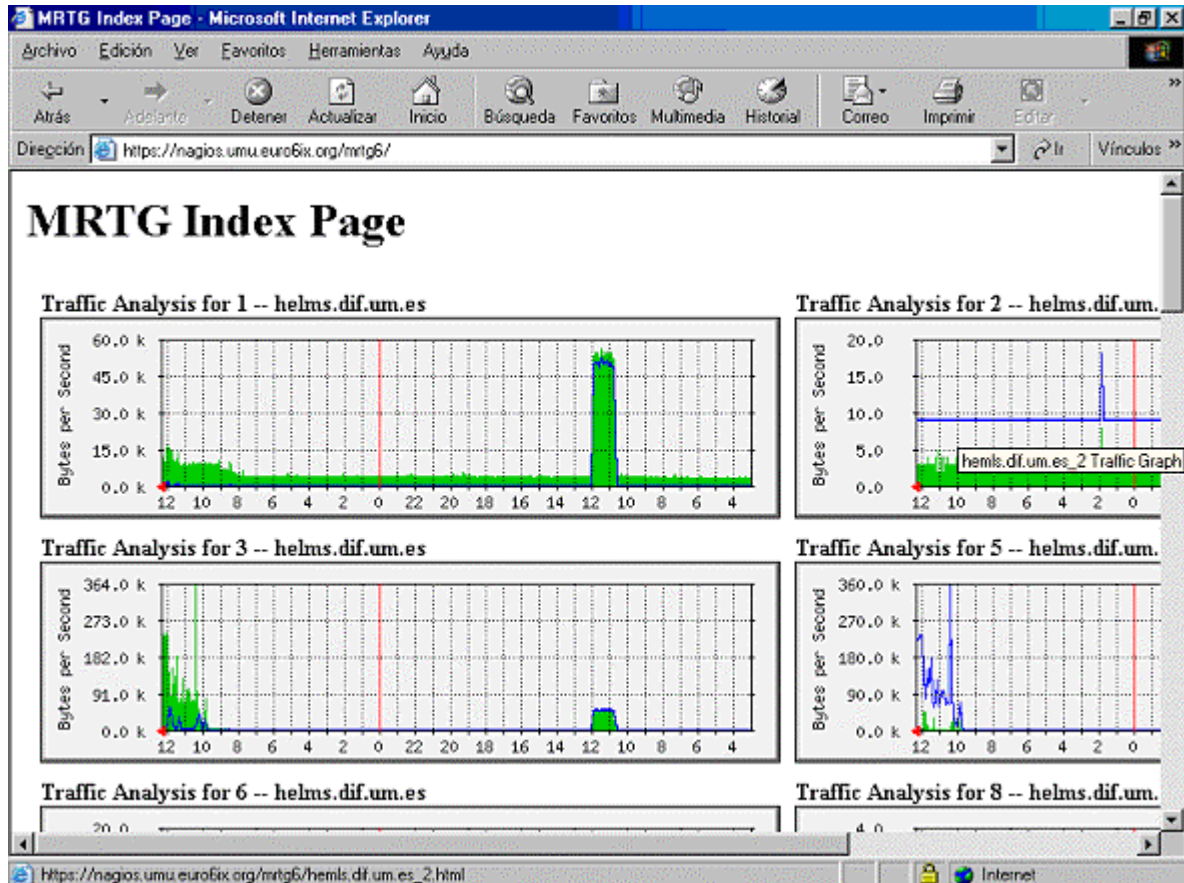


Figure 2-18: UMU's MRTG Statistics

## 2.4.4 MRTG Statistics at UPM

This tool is available through the UPM Euro6IX Web page:

[http://www.upm.euro6ix.org/mrtg/map\\_dit.html](http://www.upm.euro6ix.org/mrtg/map_dit.html)

It shows MRTG statistics of the three main IPv6 links available in UPM: MAD6IX, tunnel to m6bone, and tunnel to UMU, that are accessible through a network map.

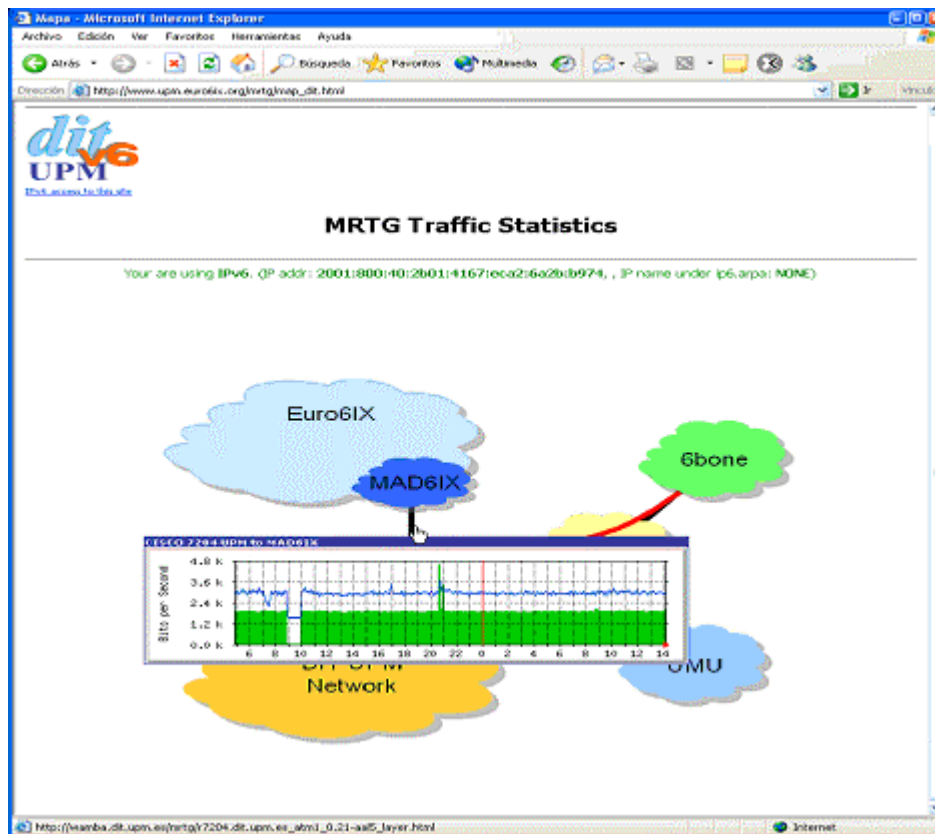


Figure 2-19: UPM's MRTG Statistics

## 2.5 Web Access Statistics Implemented at Partner's Sites

As part of the Web service, statistics of accesses should be installed to control and to be web and to have a measure of the accesses made by IPv6 users.

To get this goal, two modules of IPv6 web access statistics are suggested to get installed at Euro6IX partners web sites: Webalizer (<http://www.mrunix.net/webalizer/>) and AWSTATS (<http://www.mrunix.net/webalizer/>), both with IPv6 support.

UPM has installed a CGI access counter called `nph-count` in the main web server.

### 2.5.1 Webalizer

The **Webalizer** is a fast, free web server log file analysis program of Apache log file. It produces highly detailed, easily configurable usage reports in HTML format, for viewing with a standard web browser.

It provides information about the number of accesses, the IP of the user who has visited the web site and which pages have been visited.

The Webalizer server installed at TID Web Server is the one with IPv6 support.

The statistics generated about TID Web Server using Webalizer can be seen at: <http://www.tid.euro6ix.org/usage>.



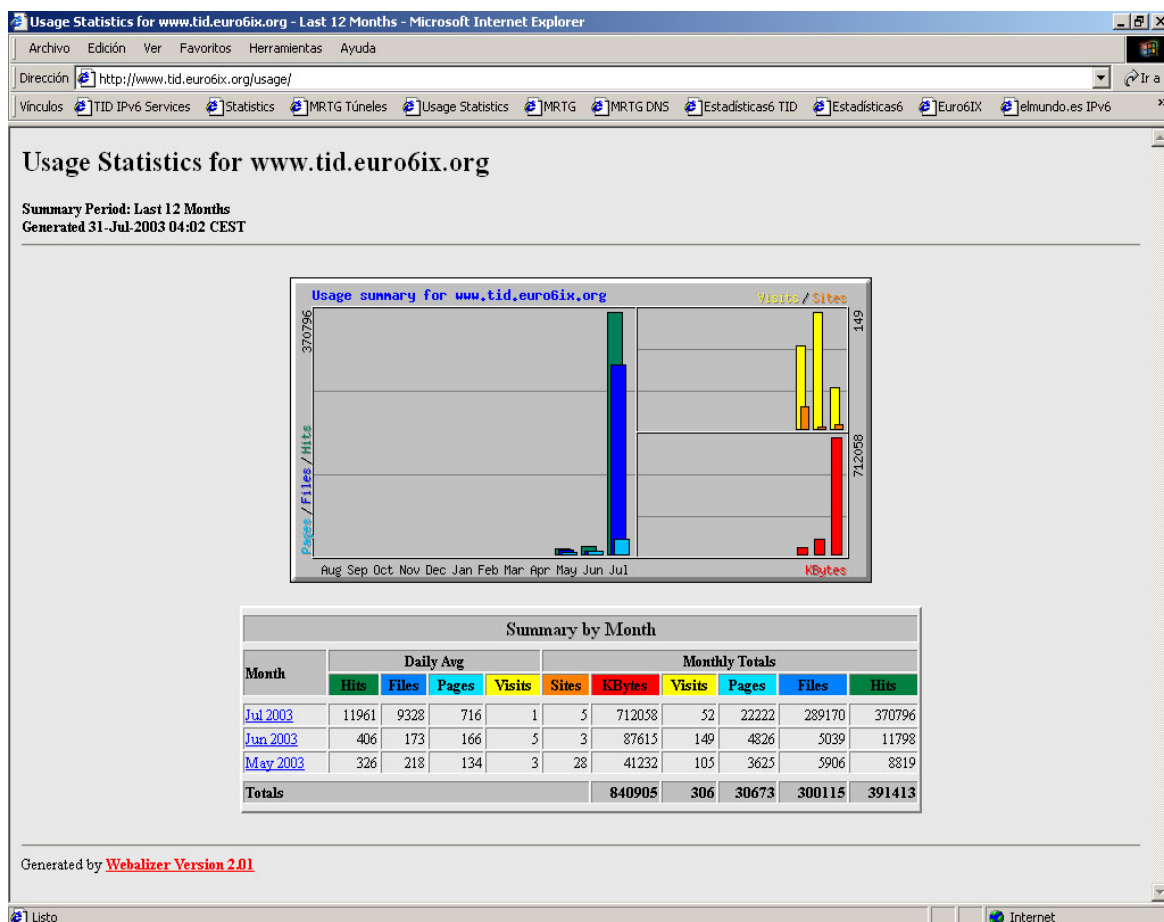


Figure 2-20: TID Statistics of Access to [www.tid.euro6ix.org](http://www.tid.euro6ix.org) using Webalizer

## 2.5.2 AWSTATS

AWStats (<http://awstats.sourceforge.net>) is a short for Advanced Web Statistics.

AWSTATS is a free powerful and plenty of features toolset that generates advanced graphic web server statistics. This log analyzer works as a CGI or from command line and shows you all possible information your log contains, in few graphical web pages.

It uses a partial information file to be able to process large log files, often and quickly. It can analyze log files from IIS (W3C log format), Apache log files (NCSA combined/XLF/ELF log format or common/CLF log format), WebStar and most of all web, proxy, wap, streaming servers (and ftp servers or mail logs).

Up to date (version 5.6), the IPv6 support is not total, as there is not the possibility to show IPv6 only statistics. What could be done is to show both IPv4 and IPv6 statistics, and using a new plugin, perform reverse IPv6 DNS lookups.

### 2.5.2.1 AWSTATS at Consulintel

At Consulintel, in order to have IPv6 only statistics some previous scripting over the access logs has been made. In <http://www.consulintel.euro6ix.org> within the Private Euro6IX menu web access statistics could be found. The project's user and password is required to access them.

Both combined (IPv4+IPv6) and IPv6 only statistics are available.

In the near future, Euro6IX code porting activity will solve this and provide a full featured IPv6 AWSTATS version.

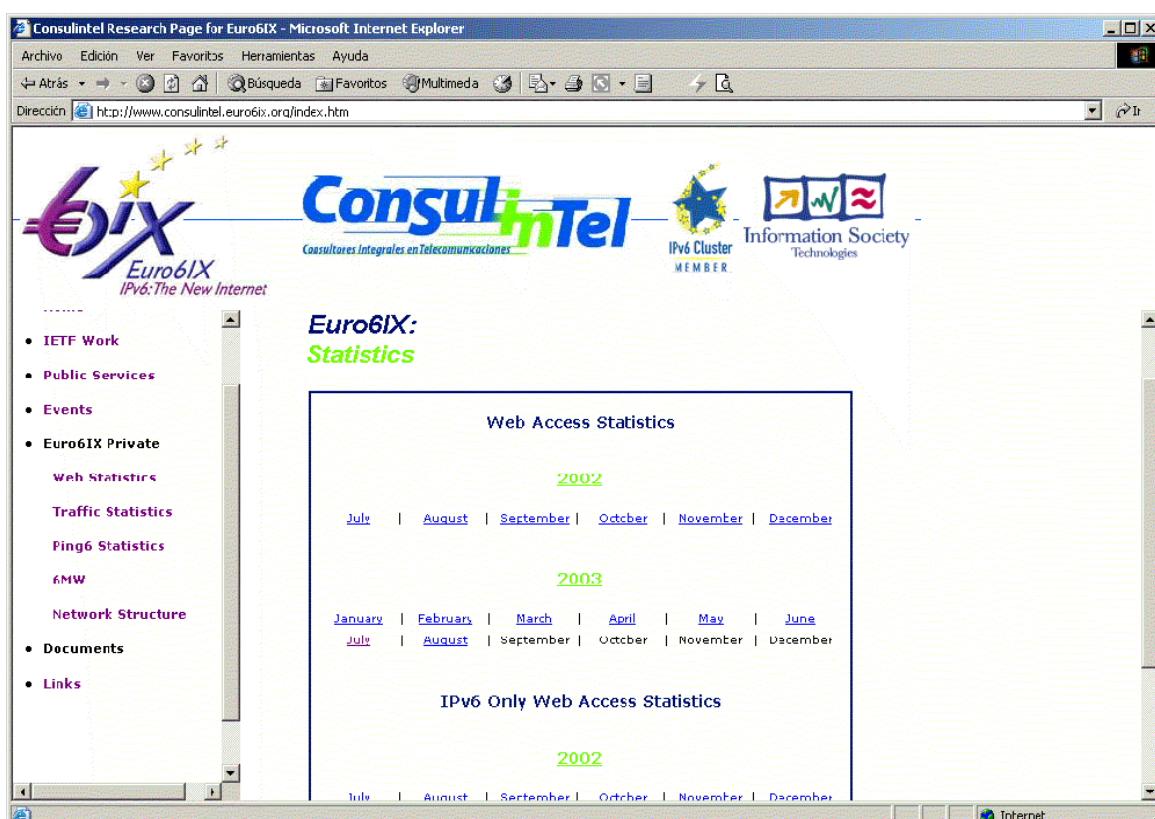


Figure 2-21: Home of Euro6IX Web Site Statistics

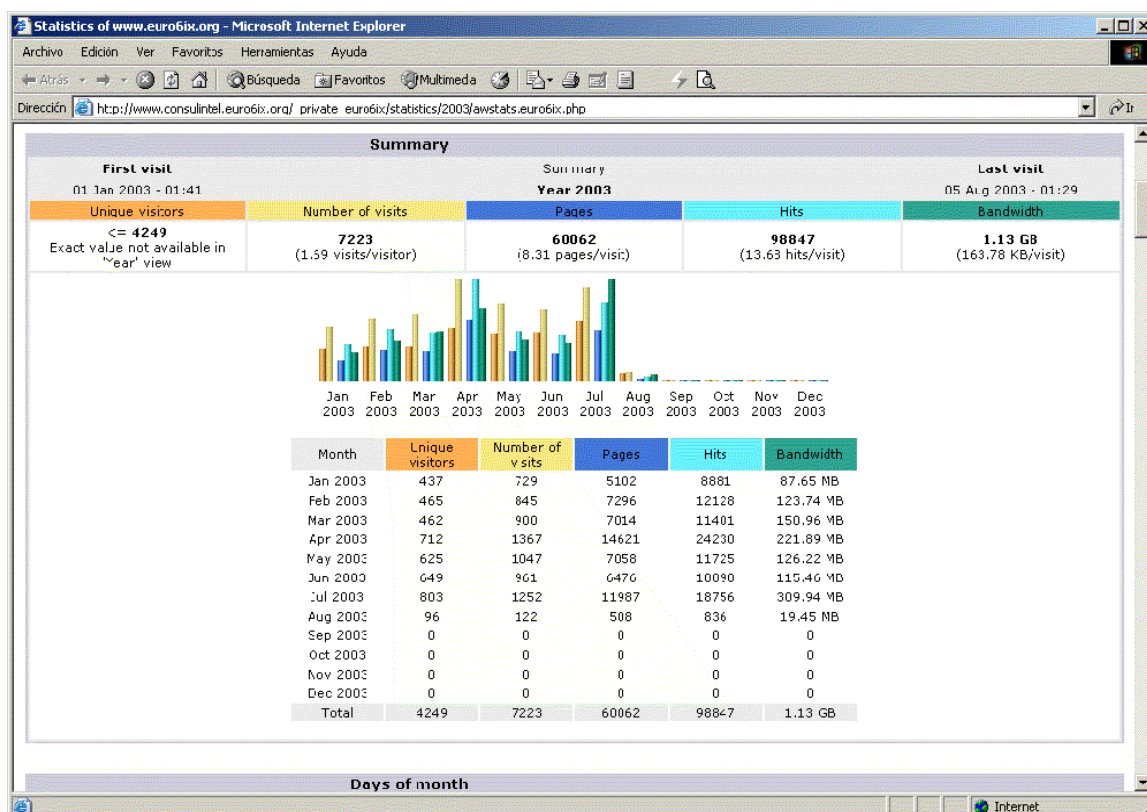


Figure 2-22: Example of Euro6IX Web Site Statistics

### 2.5.2.2 AWSTATS at TID

The statistics generated about TID Web Server using AWSTATS can be seen at: <http://www.tid.euro6ix.org/cgi-bin/awstats.pl?config=che>.

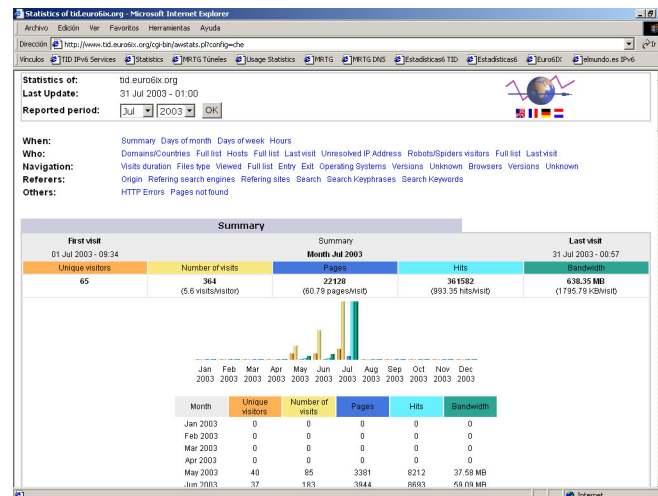


Figure 2-23: TID Statistics of Access to [www.tid.euro6ix.org](http://www.tid.euro6ix.org) using AWSTATS

### 2.5.3 Web Access Statistics Implemented by UPM

UPM has installed a CGI access counter called `nph-count` in the main web server. It shows IPv6 and IPv4 accesses to the web page (<http://www.upm.euro6ix.org>).



Figure 2-24: UPM's Access Statistics

## 2.6 Other Services Statistics

### 2.6.1 Nagios at UMU

UMU has installed the Nagios statistics system. This web service is accessible through:

<https://nagios.umu.euro6ix.org/nagios>.

To access it, you must present a valid Euro6IX Public Key Certificate, to get one go to <https://pki.umu.euro6ix.org/index.html>.

UMU services and Euro6IX backbone connections are monitored.

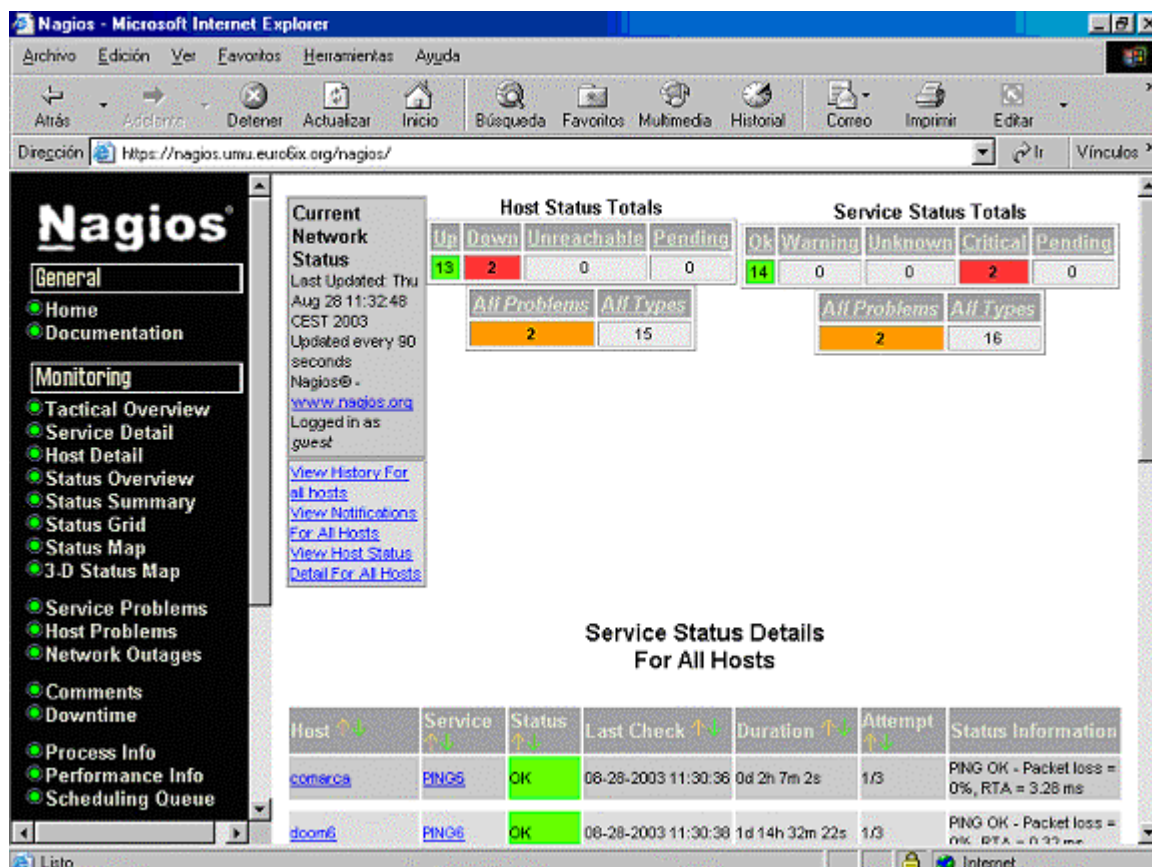


Figure 2-25: UMU's Nagios Service

### 2.6.2 Nagios at UPM

UPM has installed the Nagios statistics system, a network monitoring application that watches hosts and services specified, sending alerts when things go bad and when they get better. The plugin developed at TILAB has been also installed in order to enable IPv6 services monitoring.

This web service is accessible through: <http://nagios.upm.euro6ix.org/nagios>.

Main IPv6 links are monitored: UPM-MAD6IX and UPM-UMU. Also, most services available at UPM Euro6IX web page are monitored.



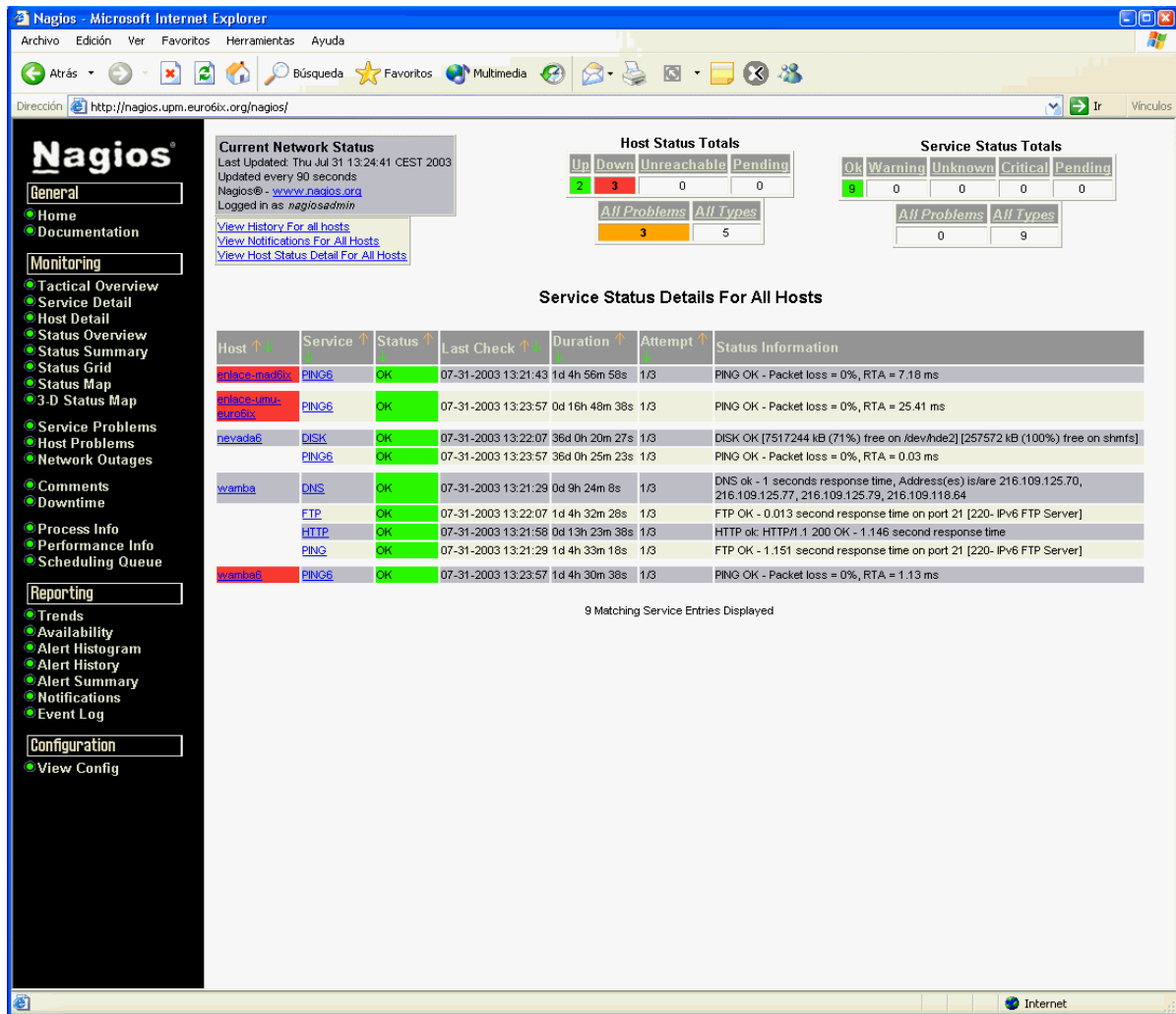


Figure 2-26: UPM's Nagios Service

### 3. EURO6IX MANAGEMENT PROPOSAL

#### 3.1 Euro6IX Management System based on Magalia (MSIP)

The Management of a big network, with nodes owned by different organizations, causes that nobody can know the global state of the network.

The solution to this problem is not very easy because organizations usually are very reluctant to allow SNMP accesses to their equipments, and even in the case that will be allowed this kind of accesses, the amount of monitoring traffic generated can produce a bandwidth waste.

To solve this situation, a new protocol called MSIP and a new Magalia module called IM have been created. The new Magalia interchange module (**IM**) and **MSIP protocol** have been designed to make possible the sharing of monitoring information.

This protocol will provide communication exchange of the public monitoring information of the IXs, isolating the private information of the IXs from the rest of the world.

With MSIP, each organization forwards to the rest only information pieces previously selected by the owner of this information.

These pieces of information aren't forwarded to everybody, the information is sent to a set of few organizations, and this information is relayed to others and so on, resulting in a significant saving of bandwidth and CPU usage.

Thanks to MSIP, each organization will have graphical information of the global state of the network.

This protocol is designed with the following features:

- Isolation of private information between MSIP partners.
- Loops and mesh network topologies working capable.
- Infinite loop avoidance mechanism.
- Spoofing protection.

With this protocol, a new set of concepts are introduced:

- **MSIN:** Magalia Shared Information Network. Is the set of “nodes” and “message paths” that compose the group of organizations that share the information.
- **IM:** Interchange Module. Magalia module that performs the exchange information between Magalia kernels.
- **MSIP:** Magalia Shared Information Protocol.
- **MP:** Message path. Virtual Path to be followed by MSIP messages.

For more information about MSIP protocol, see “Magalia\_EIP.doc” document at Euro6IX Repository.

## 3.2 Distributed Management Proposal to Test MSIP

This proposal is an example of installation of MSIN in Euro6IX network, which will give a global view of Euro6IX network state to all project partners.

### 3.2.1 Objective of the Test

The objective of the test is to verify the proper operation of MSIP, to detect possible errors in the protocol design, and to provide for the first time a global vision of the Euro6IX network status to all Magalia users.

### 3.2.2 MSIP Test Description

The test consists in the installation of Magalia package in various IXs of Euro6IX and the configuration of MSIP.

The information to be shared will be messages bearing information about the traffic load, and the state of the public links shared between different 6IXs.

The cooperation between the Euro6IX members is of vital importance in the success of this trial.

As a profit of the test, every participating partner will see the global link state of Euro6IX.

It is proposed that IXs involved in this test are: BER6IX, LIS6IX, LON6IX, MAD6IX, PAR6IX and ZUR6IX.

### 3.2.3 MSIP Test Configuration Tips

Because of the arbitrary nature of the information needed by MSIP to run, most of configuration criteria are arbitrary and they can be subject of negotiation.

Now take a look over the following picture of Euro6IX network to identify the topology of the network and design in Figure 3-1.

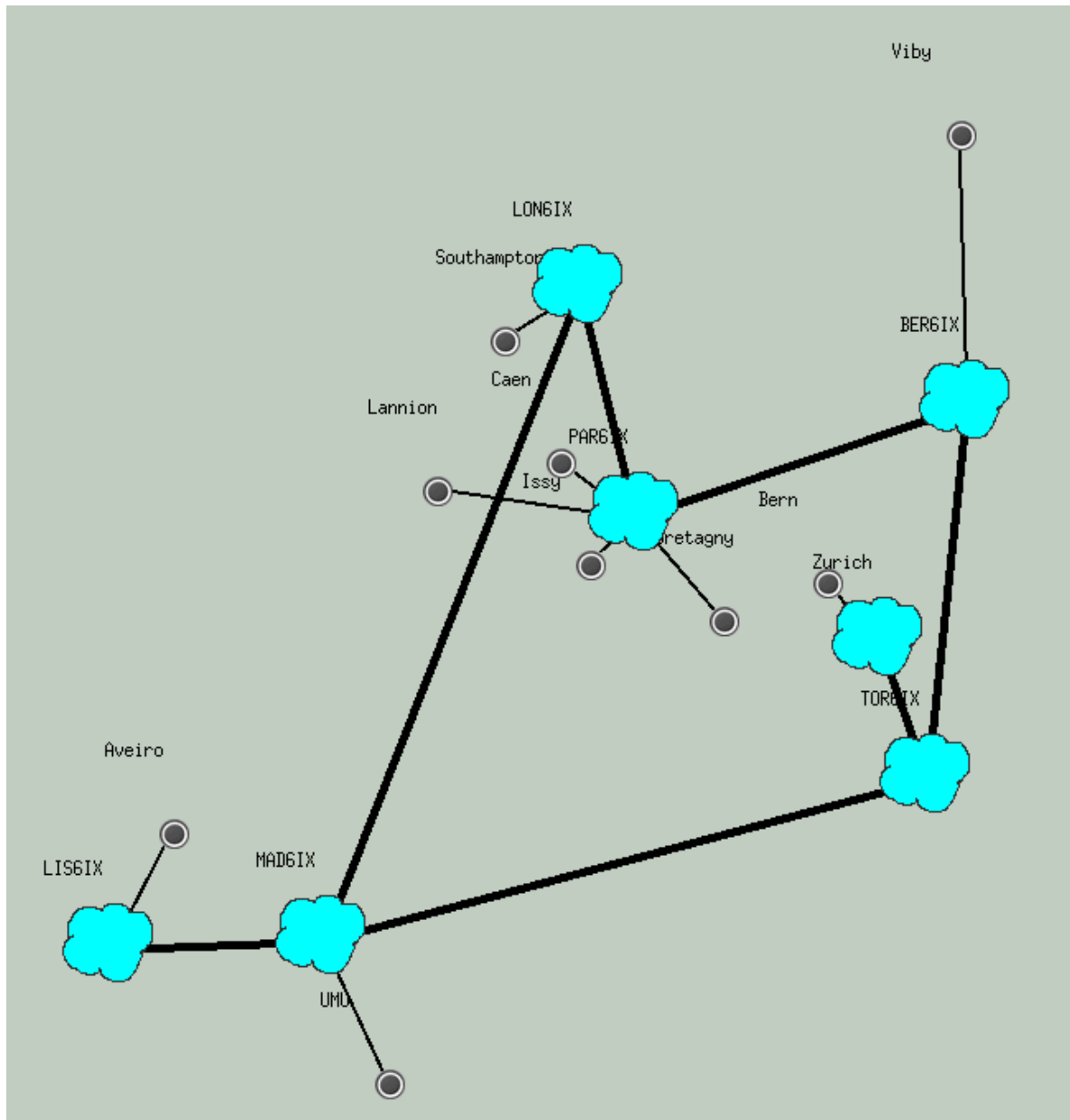
As it can be seen, this network has a big ring, with radial adjacencies.

The next part of the work is very political, and it consists in the establishment of regions of responsibility according to the weight of the nodes in the network.

A node is so much heavy in importance the nearer of the ring is located. This way, a hierarchy can be established: level 0 is assigned to the nodes lying down over the ring, level 1 is assigned to out of the ring adjacent nodes attached to level 0 nodes and so on.

If this hierarchy is applied to Euro6IX network, the result can be like this:

- **Level “0” nodes:** MAD6IX, LON6IX, PAR6IX, BER6IX and TOR6IX.
- **Level “1” nodes:** LIS6IX, Zurich, Southampton, Caen, Lannion, Issy, Bretagne, Viby and UMU.
- **Level “2” nodes:** Aveiro and Bern.



**Figure 3-1: Euro6IX Network Map Design**

Note that the hierarchical level has nothing to do with the importance of node itself, it only depends on the proximity to the ring.

Every node has the responsibility to forward MSIP messages from the deepest levels of its region to the upper level node. An influence region is the node and its low level hanging nodes.

For example, the region of MAD6IX is formed by MAD6IX (as head node) and the nodes LIS6IX, UMU and Aveiro. At the same time the region of LIS6IX is formed by LIS6IX (as head node) and Aveiro node.

When various nodes of the same level share a set of monitoring parameters, (in the case of Euro6IX the load and state of the ring links), the responsibility of monitoring must be distributed using a finger criteria.

What is the “finger criteria”? See Euro6IX ring as a steering wheel. In this wheel, the level zero nodes will monitor the adjacent links reached in clockwise.



Following this explanation:

- MAD6IX will monitor the link between MAD6IX and LON6IX.
- LON6IX will monitor the link between LON6IX and PAR6IX.
- And so on.

If a node can't be monitored is assigned link but the adjacent node can, exceptions will be accepted by mutual agreement.

### 3.2.3.1 Agreement about Naming of Nodes and Links

All organizations must agree in the naming of links and nodes because MSIP and Xges instances need it.

Here is TID proposal:

The names of level zero nodes will be MAD6IX, LON6IX (or UK6IX if London prefers), PAR6IX, BER6IX and TOR6IX, etc.

The **“ifz”** attribute of every link (see “Module\_snmp” properties in Magalia Handbook) in the ring will be **“<node a>-<node b>”** following the steering wheel criteria in clockwise. For example “MAD6IX-LON6IX”, LON6IX-PAR6IX”, “PAR6IX-BER6IX” and so on.

In the radial links, the criteria of naming links will follow the name of the nodes from the ringside toward the outside. For example “MAD6IX-LIS6IX”, “LIS6IX-Aveiro”, etc.

### 3.2.3.2 Message Paths

Two MP will be created inside the ring, **“LEVOGIRAL”** and **“DEXTROGIRAL”**, both are equal except in the sense of message circulation. In the first MP the messages screws left the ring, and the second screw right.

The radial MPs will be named following the criteria **“<name of the canton's head node>-out”** and **“<name of the canton's head node>-in”**, depending if the message leaves the ring toward radial MP, or ingress in the ring coming from the radial MP. The MP should be prolonged till the last node of the branch.

### 3.2.3.3 MSIP Nodes Behavior

All nodes must configured to comply these requirements:

- All level zero nodes must forward the messages coming from a concrete ring MPs to the next ring of the same MP node.
- If the node is a region-head, it must route the ring MP messages to all radial MPs, changing the destination MP to the radial MP and must change ORIGINATOR field to its node name and set the TTL field properly to allow the message to get every node in the radial MP.
- If a region-head node receives a message from any radial MP, the node must forward the message to the rest of the MPs, (ring and radial for its canton), and change ORIGINATOR and TTL fields properly.
- When, as a result of module activity, a new message is generated, the node (this node can be of any level) must send the message to all attached MPs, with the ORIGINATOR filled with its name, and the TTL field set to an adequate value for all.

### 3.2.3.4 Public and Private Maps

The configuration tips exposed along the preceding sections of this chapter must be configured in the public map. This map is the reference needed by the IM (information module) to work. This map must be accessible to all organizations.

The private map can be a copy of the public map, adding after the organization's private attributes, to permit the real surveying work to the rest of the modules, this map can have confidential information and mustn't be distributed to the rest of the partners.

### 3.2.4 Distributed Management Proposal to test MSIP

This map shows the proposal for testing MSIP. All partners involved.

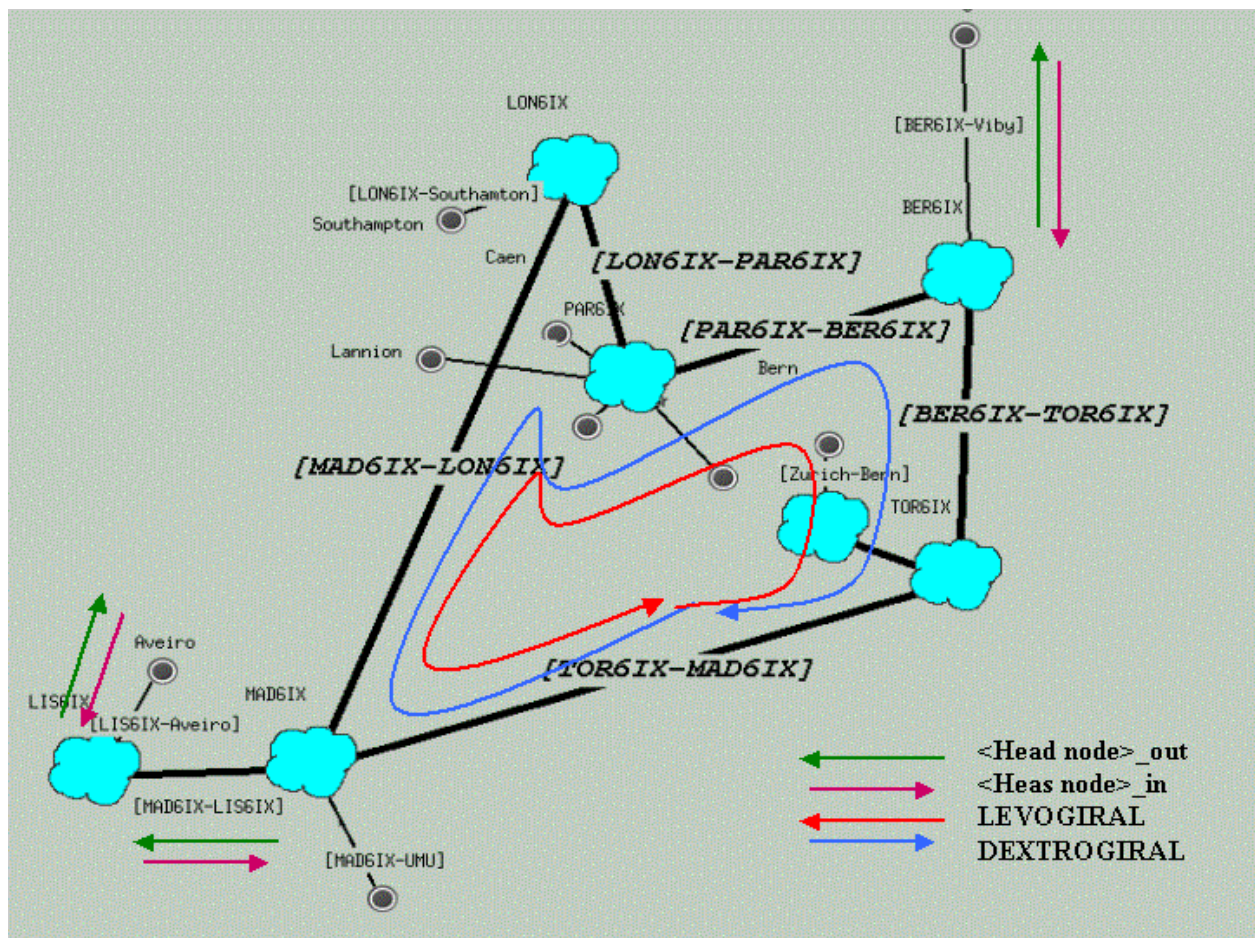


Figure 3-2: MSIP Operation Through Euro6IX Network Map

The **ifz** link attribute values come enclosed in square brackets.

## 4. EURO6IX SECURITY CONTROL SYSTEMS PROPOSAL

### 4.1 Security Guidelines for Euro6IX Network

Security guidelines for Euro6IX network have been defined in collaboration with research activities within WP4. The deliverable D4.4 “Report on the second year Network and Application Research Activities (draft)”, and more exactly its 2.1.6 section called “Network Security”, already contained a summary of these rules.

In order to provide an overall view the basics are presented again.

The basic security feature to consider is the Least Privilege principle. It states that every component should have only the privileges needed to carry out assigned tasks.

The Euro6IX network model has been divided into three different functional blocks:

- Internet Exchange Network.
- Carrier’s Network.
- ISP Network.

After that, traffic has been modeled for each kind of network in order to control it.

The following figure shows the Traffic Control in the Carrier’s Network.

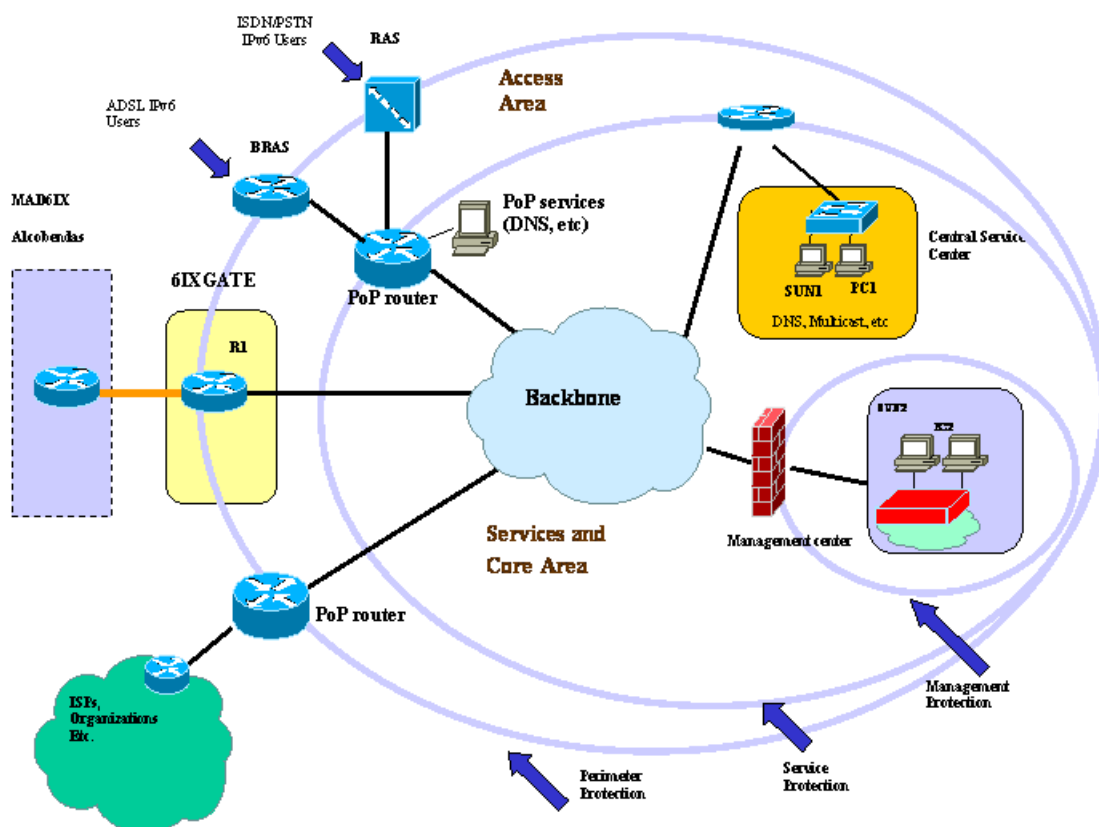


Figure 4-1: Traffic Control in the Carrier's Network

The following figure shows the Traffic Control in the ISP's Network.

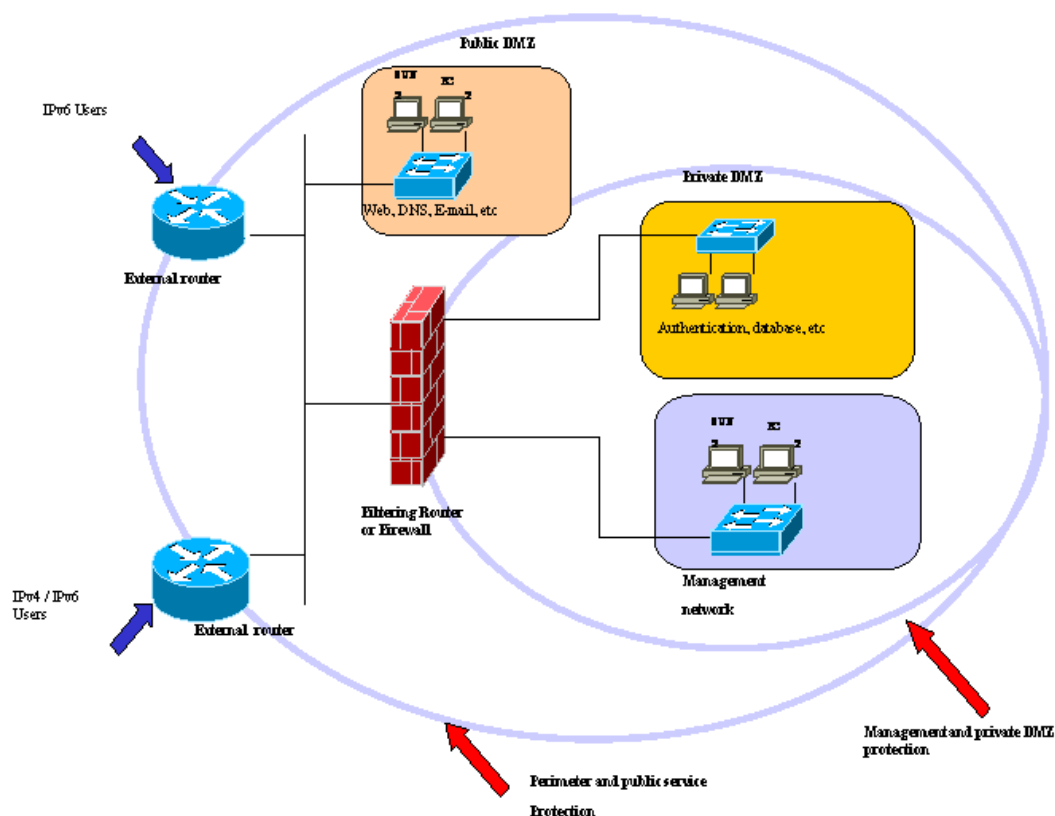


Figure 4-2: Traffic Control in the ISP's Network

The following figure shows the Traffic Control in the IPv6 Internet Exchange.

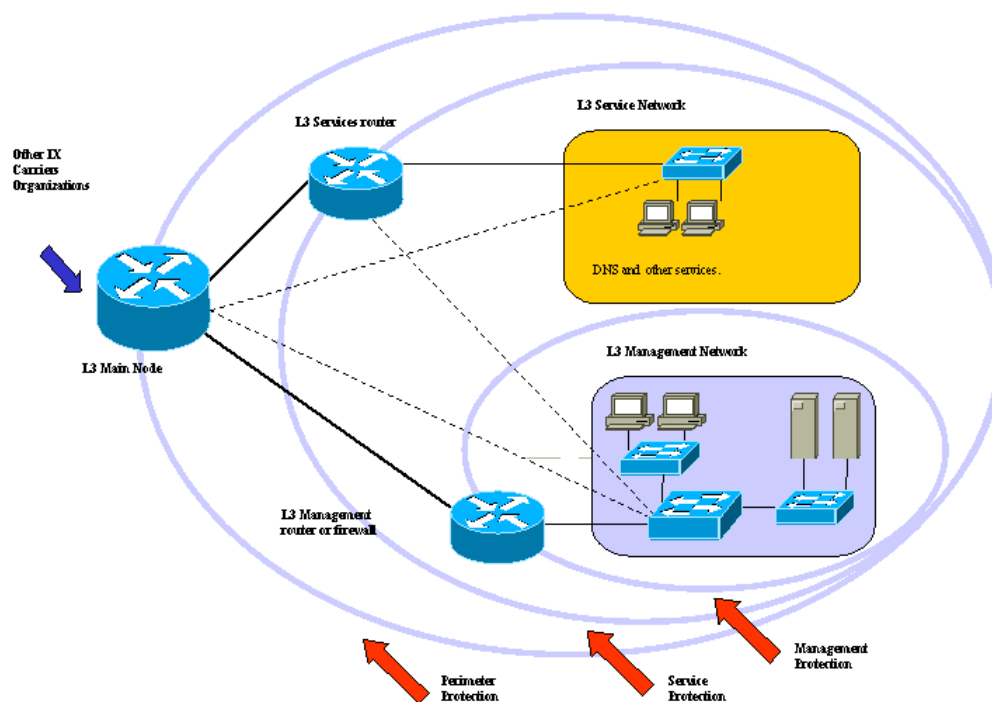


Figure 4-3: Traffic Control in the IPv6 Internet Exchange

From a security point of view, and if performance is not seriously affected, it is recommended that traffic flows from/to L3 Services and Management networks pass through its access element (like filtering routers/firewalls) for this parts of the networks.

For further information, it is recommended the reading of the whole document “Security Guidelines for Euro6IX Networks” that can be found in the Euro6IX repository. After the implementation stage in WP2, feedback will be provided to WP3 and WP4.

## 4.2 Topaz, an IDS Tool

Topaz is a NIDS (Network Intrusion Detect System) developed within Euro6IX in order to study and experiment new IPv6 attack patterns.

Topaz is an application to secure Euro6IX networks. Its relevance for IXs architecture and IPv6 is high, as its main objective is to detect possible IPv6 protocol vulnerabilities, and it offers a new point of view for implementing this kind of applications.

During 2003, Topaz development team at TID has been collaborating with sub-activity A4.1-3 in order to define the complete Detection Logic. The rules contained in this Detection Logic can be classified in three categories:

- **Forbidden Accesses:** Failed accesses detection, *root* access detection, and brute force attacks detection ...
- **Common Attacks:** DoS attacks detection, IP Spoofing detection, Critical Services scanning detection, shell executions detection, Specific Services attacks ...
- **IPv6 Specific Vulnerabilities:** Specific Attacks for IPv6 protocol.

Category 1 and 2 are defined and implemented. The collaboration with A4.1-3 continues to define and implement the set of rules in the category “IPv6 specific vulnerabilities”.

### 4.2.1 Topaz Application

Topaz is made of two components:

- The **Sensors**. Its function is the capture of Ethernet frames to get an analysis of the IP packets contained in every Ethernet frame and to get/send the messages from/to the *Management Console*.

Sensors have been developed in C++ programming language, in both Linux and Windows platforms.

In the snapshot at Figure 4-4, it can be seen the different log messages that a sensor exchanges with the Management Console.

- The **Management Console**. The Management Consoles centralizes and manages in a graphical way all the Sensors System and the reception of alerts.

The Management Console is a traditional Windows event-oriented application, adding graphical capabilities to alert analysis and trace presentation functionalities.

Features of the Management Console are:

- Add/delete a registered sensor.
- Add/delete a category of rules (in a graphical way).
- Add/delete a rule (in a graphical way).
- Presentation of alerts notifications.
- Updates of the list of sensors connected to the Management Console.



- Allow (or not) the registration of new sensors.
- Sending of mail alerts to the network administrator.
- Saving of the Alerts Buffer to a log file.

A snapshot of Topaz Console indicating elements follows below in Figure 4-5.

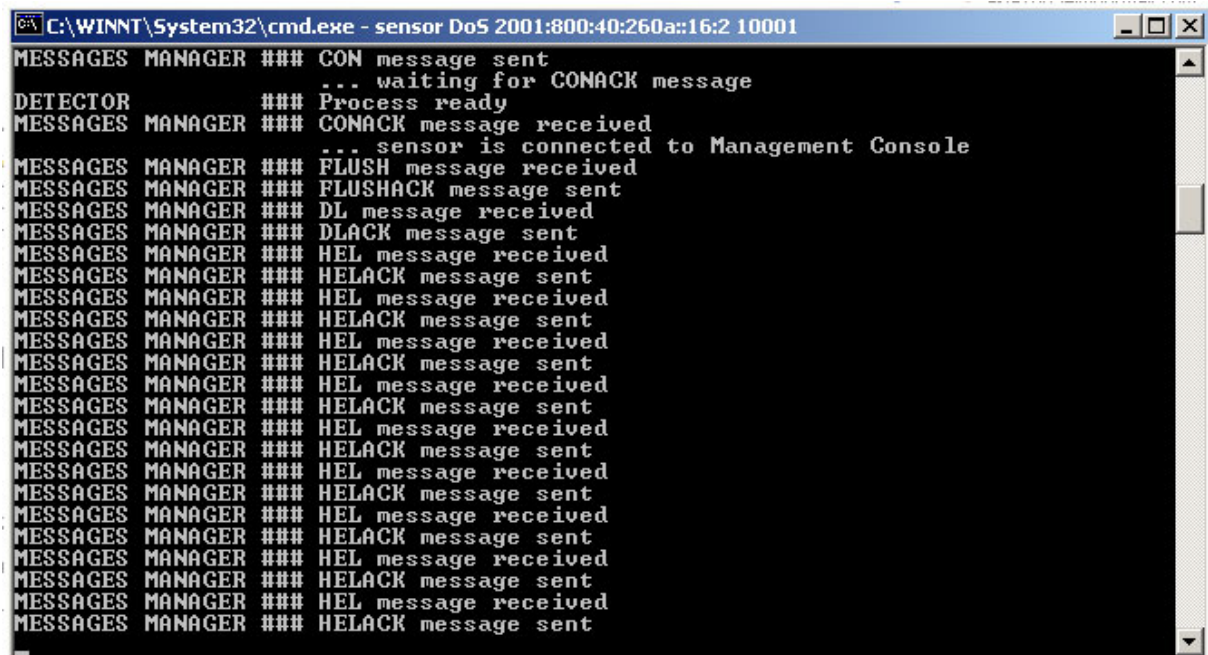


Figure 4-4: Sensor Log messages

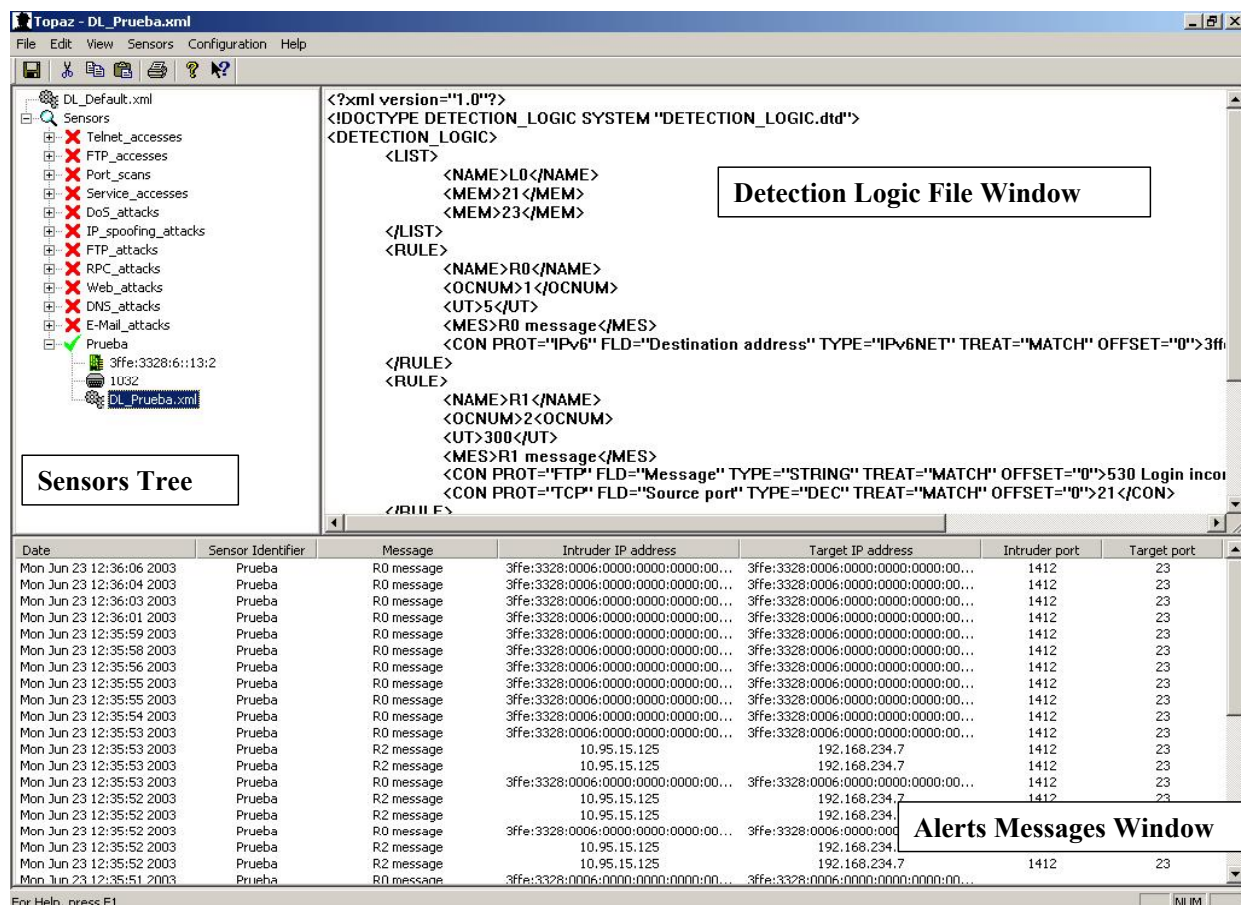


Figure 4-5: Topaz Console Snapshot

#### 4.2.2 Proposal of Installation of Topaz at TID Test-bed

This is a proposal to install and test Topaz Sensors System and Topaz Management Console at TID. In this proposal, it is analyzed which are Probably Intrusion Sources and which places are the bests to install Sensors system and Management Console in order to secure TID test-bed.

Today, any response mechanism of Sensors is implemented.

Firstly, let's take a look at TID Test-bed:

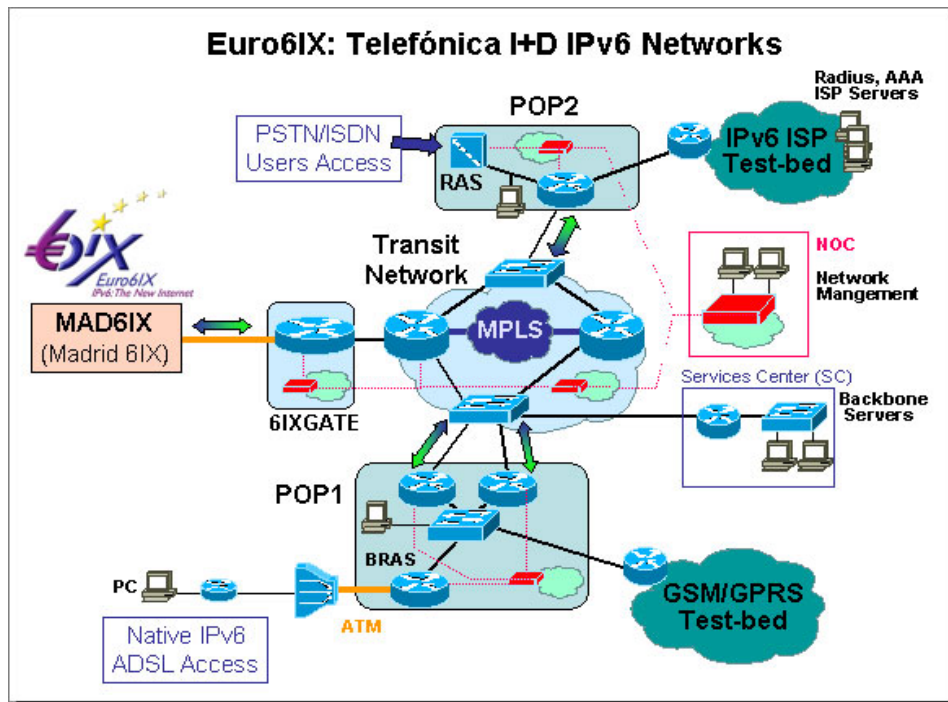


Figure 4-6: TID Test-Bed

##### 4.2.2.1 Probably Intrusion Sources

These are:

- Externally:
  - International Accesses through MAD6IX.
  - All other national organizations networks.
  - Access from ADSL and ISP users.
- Internally:
  - Incorrect use of resources by administrators and operators.

##### 4.2.2.2 Sensors Installation

The sensors system at TID will be composed by:

- 1 sensor controlling 6IXGATE incoming traffic.
- 1 sensor at POP#1 controlling clients incoming traffic.
- 1 sensor at POP#2 controlling ISDN IPv6 Users.
- 1 sensor at NOC.
- 1 sensor at Backbone Servers.

- 2 sensors at IPv6 ISP test-bed:
  - 1 in IPv6 Services network.
  - 1 after the IPv4/IPv6 tunnels from external users.

The Management Console is to be installed at Backbone Servers.

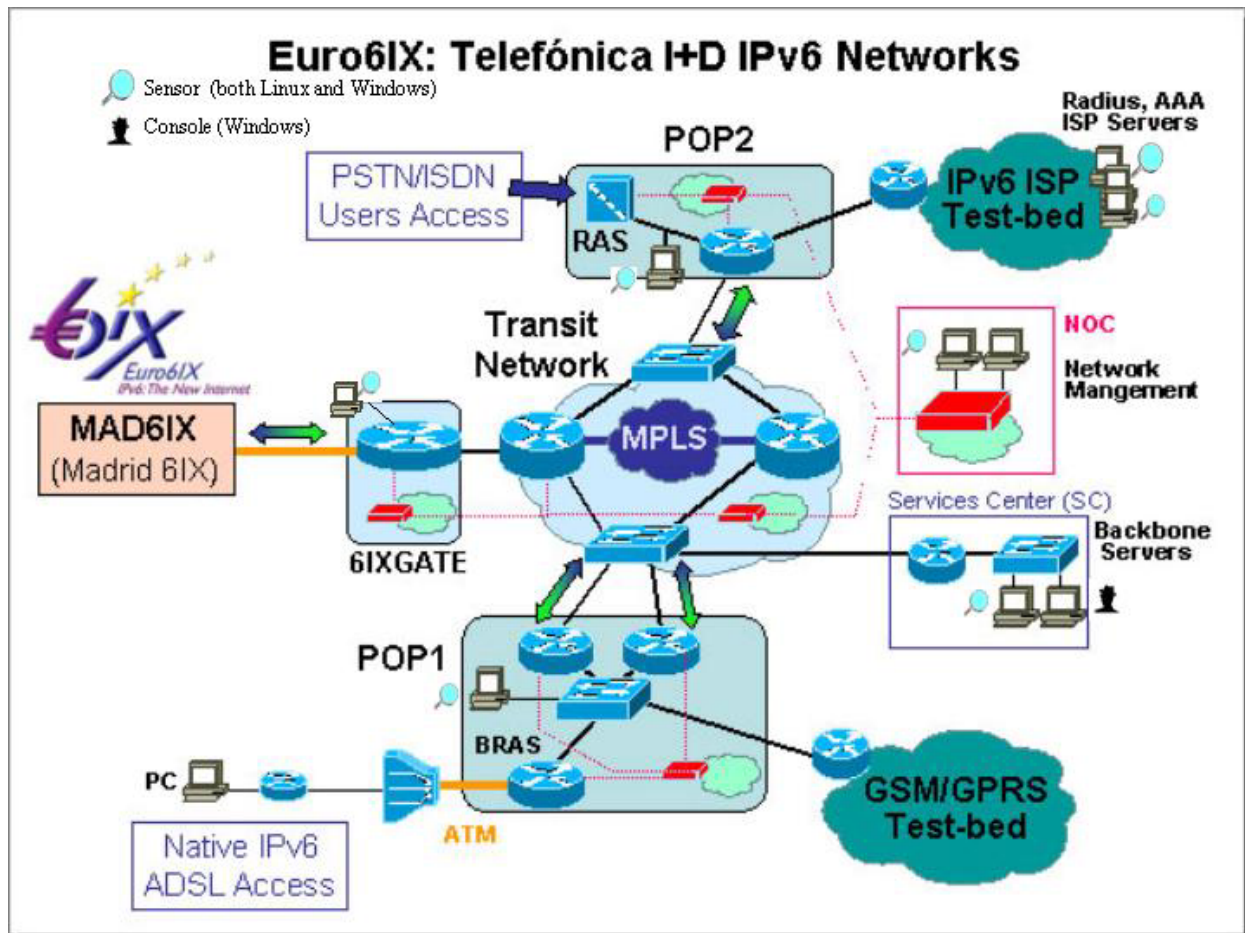


Figure 4-7: Topaz Installation Proposal at TID Test-Bed



## 5. SUMMARY AND CONCLUSIONS

This deliverable has presented the systems used by Euro6IX networks to control and monitor IPv6 traffic.

The results of A4.1-1 and the collaboration with A4.2-2 are explained in chapter 4. Up to now the most effort has been theoretical in the case of study of Security Guidelines and development effort in the case of Topaz.

The next lines of work in security are:

- To elaborate a plan to install and test Topaz in TID test-bed (a proposal is presented in this deliverable), and to install the application in every partner test-bed and every IX.
- The Security Guidelines are being installed and tested at TID test-bed.

The feedback about these two issues will be reported in Deliverable D3.3.

Another line of work is Magalia. The goal for next year is to have the functionality of Sharing Management running and being tested in every IX.

It is also very important that partners have installed this application in their own test-bed to have it controlled and communicated to the main Magalia node in the correspondent IX (level zero nodes in MSIP terminology). In D3.3, results obtained by partners (and IXs) that will install Magalia will be reported.

The systems to control traffic and to obtain statistics from it have become very important since the next step in the evolution of Euro6IX is the introduction of real beta-tester users. In this way, A4.2 has to make a big effort in order to make attractive final-users applications.

New systems (if any), implemented to control this new traffic, will be commented in D3.3.