Title: **Deliverable D3.2** **Definitions of Statistics, Management and Security Control Systems**	**Document Version:** 0.5

Project Number: IST-2001-32161	**Project Acronym:** Euro6IX	**Project Title:** European IPv6 Internet Exchanges Backbone

Contractual Delivery Date: 31/12/2002	**Actual Delivery Date:** 23/05/2003	**Deliverable Type* - Security**:** R – PU

* 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: Carlos Ralli	**Organization:** TID	**Contributing WP:** WP3

Authors (organizations):

Peter Hovell (BT), Jordi Palet (Consulintel), Eduardo Azañón (TID), Aurora Ferrándiz (TID), Jesús López (TID), Francisco Romero (TID), Ruth Vázquez (TID), Mario Morelli (TILAB).

Abstract:

This deliverable summarizes the work done in the first year of Euro6IX project inside the WP3 in the context of A3.3 activity, regarding the definition and proposal of the architecture of systems to perform managing, monitoring, statistics reports and security control activities of each IPv6 Internet Exchanges and IPv6 networks.

The main goals of this deliverable are the analysis of available software and the A4.2 software developed for this activities in order to establish the management, operation and monitoring basics in Euro6IX IPv6 networks.

Keywords:

Euro6IX, IPv6, Management, Monitoring, Security network tools.

Revision History

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

Revision	Date	Description	Author (Organization)
v0.1	18/12/2002	Document creation	Carlos Ralli (TID)
v0.2	20/12/2002	BT contributions TID contributions	Peter Hovell (BT) Aurora Ferrándiz (TID)
v0.3	28/01/2003	TILAB contributions	Mario Morelli (TILAB)
v0.4	30/02/2003	TID changes	Carlos Ralli (TID)
v0.5	23/05/2003	Final Review and corrections	Jordi Palet (Consulintel)

Executive Summary

This document describes the first proposals regarding network management, statistics monitoring and security control issues in the context of Euro6IX IPv6 Exchangers and IPv6 networks.

All these proposals will be deeply discussed in next Euro6IX meetings in the context of activity A3.3, looking for their implementation. At least, a minimum set of them should be installed in their simpler manner by M15.

Table of Contents

Table of Figures

1. INTRODUCTION

During the first year of life of the project, the main goal has been to deploy the network. Now once this is done, and the network is running, it is time to develop new systems to control and operate the network.

In this document several proposals are presented to do this function in Euro6IX networks.

There are some important aspects of network management and control:

- Network Usage Statistics. This is a very useful because it helps us to control the amount of traffic, which services are the most used in the network and it serves as the input of D3.3.X documents, every month.
- Management and Operation of the Network. It is necessary to have systems to control and manage the network in order to prevent and solve any problem. At this point, TID proposal, Magalia provides a new point of view and a new concept of design in network management tools as it is explained in chapter 2.
- Security.

All of the developments in each of those aspects, made by any partner, are reflected in this document. They are also available in the repository to all the consortium members.

An interesting aspect of these developments is that at least two partners must have every system installed and running.

2. EURO6IX STATISTICS SYSTEMS PROPOSAL

Each one of the statistics systems described below should be installed and tested by at least two partners.

2.1 TILAB's Ping Tool System

Ping-view tool provides some information about the connectivity towards a specific set of destinations in the Internet (host or routers). The reachability information for every monitored site includes the packet loss (the number of echo replies not received back versus the number of echo requests transmitted) and the response time (RTT, Round Trip Time). The data is collected sending fixed length ICMP echo requests sequences (one per second) towards all the selected destinations using the ping program. The answer to the first echo request of every sequence is always rejected because it is usually slower than the others (due to e.g. caches priming). High values of packet loss and Response Time indicate low connection performances. 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 collected 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 statistics towards different destinations may be combined or grouped to show an estimation of the "network" performance. Groups of destinations defined to put together destinations belonging to given "parts" of the network may be used to show aggregated reachability statistics towards these "parts" of the network. Ping-view provides an aggregated view for custom defined groups, showing a summary table containing an estimation of the overall "group of connections" behavior ("RTT70% - last 7 days") together with an indication of the medium term trend (time-scale of days).

"RTT70% - last 7 days" is a performance parameter defined as the minimum response time within which the 70% of replies to the transmitted echo requests are received back during the last 7 days of data acquisition, in order to provide a "single value" indication of the network performance. If the overall ping success towards a specific site during the period of time chosen for the calculation of "RTT70% - last 7 days" is less than 70% this parameter can not be calculated and a not rated (n.r.) indication is shown. Higher values of "RTT70% - last 7 days" or the n.r. indication show lower communication performance.

Inside the statistics related to the aggregate views (as e.g. South America) two parameters are used: The Quality Factor and the Service predictability. The quality parameter called Quality Factor 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.

A measure of variability of service (or ping predictability) may be obtained 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.

2.2 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").

2.2.1 General Network Architecture

The operation of the statistics system has a very simple handling and installation. In the Management Box there is a machine with 'ping_stat' tool that is in charge to send "pings" to the IPv6 nodes that are included in the list of nodes to follow for generating the statistics results.

The results of these "pings" are stored in the Management Box and they are gathered with "wget" by the web servers, which uses the 'webstat' tool to generate an image file that will be shown in the statistic web page.

This architecture is represented in the following figure:

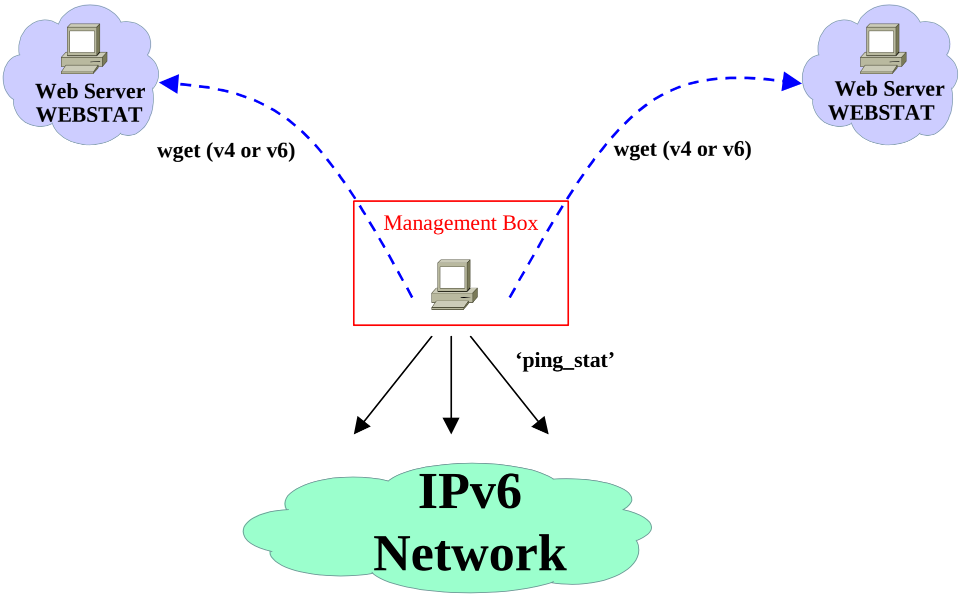


Figure 2-1: General Network Architecture

2.2.2 Euro6IX Implementation

2.2.2.1 Initial Statistics System (September 2002 - November 2002)

Initially, the statistics system was made up of three boxes mainly, all into LONG network. These boxes are:

- “Cocodrilo” which is a web server accessible from Internet, with restricted access, where the results of the statistics system are shown.
- “Che” is another web server where the results of the statistics system are shown but not accessible from Internet.
- “Mortadelo” which is the machine where ‘ping_stat’ is launched to obtain the result of statistics. Using the "wget" IPv6 enabled tool “cocodrilo” and “che” gather this results and are show in their respective web servers.

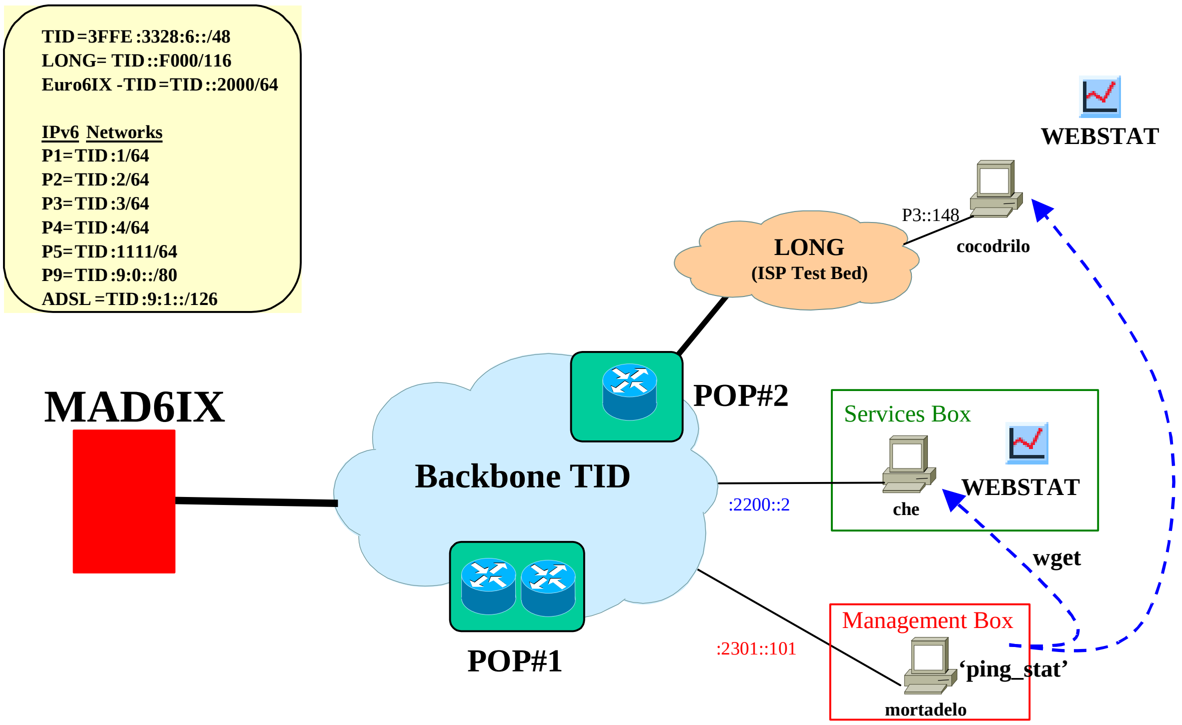


Figure 2-2: Euro6IX Implementation of the Statistics System

Nodes followed/monitored by the statistics system (http://stat6.tid.euro6ix.org/euro6ix-stats.html) will be into the configuration files of 'ping_stat'. This nodes are accessible through MAD6IX node in Alcobendas (Madrid) and they are shown in the following figure:

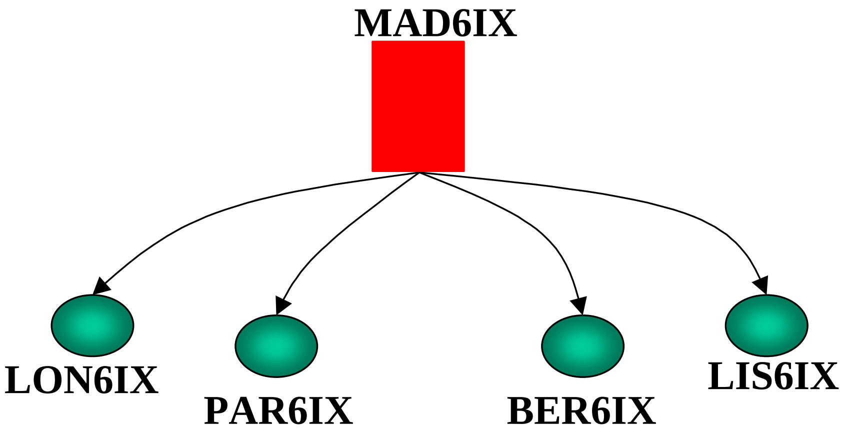


Figure 2-3: Nodes Verified by the Statistic System

2.2.2.2 Statistics in the Euro6IX Web Server (January 2003)

After the initial statistics system, the next step is to obtain Euro6IX's statistics so that they can be shown in the Euro6IX's main Web Server at Consulintel. In order to achieve this task, another machine with the 'ping_stat' tool will be installed in the MAD6IX node. After this, from Consulintel, using "wget" IPv6 enabled tool the result of statistics system will be transferred to generate the graphics in the web server. The new results generated by 'ping_stat2' will also be shown in the same web servers ("cocodrilo" and "che") as in the initial stage.

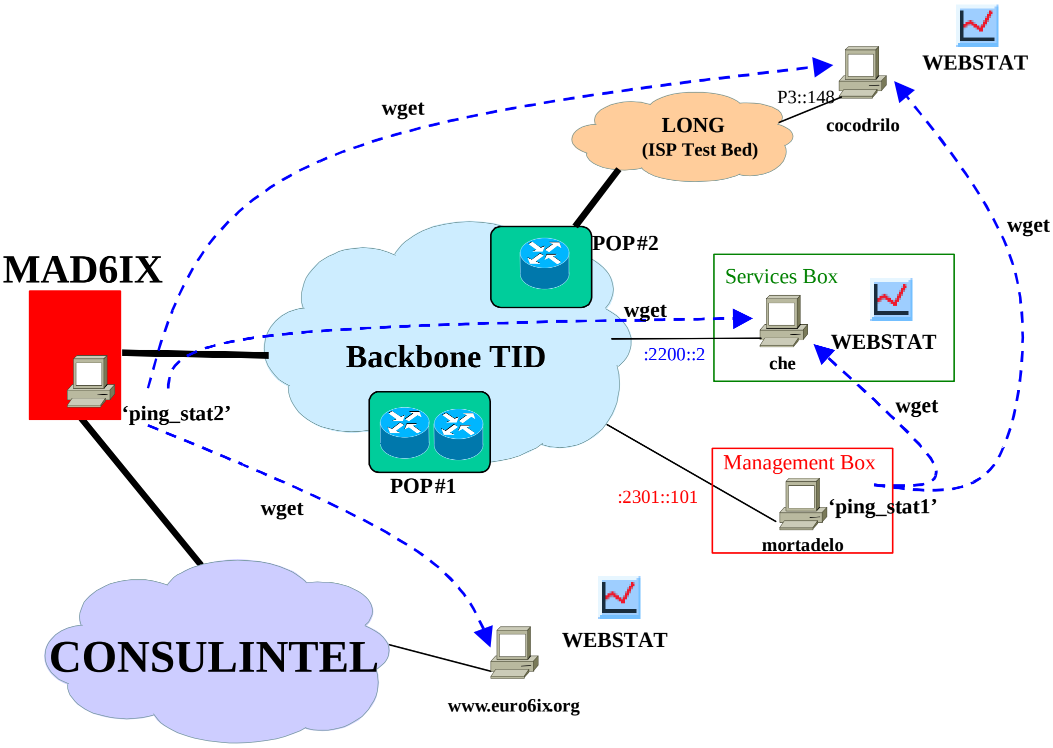


Figure 2-4: Statistics in the Euro6IX Web Server

2.2.2.3 Redundant Statistics System

This section includes a proposal where other IX uses this system, displays the measures and also sends the statistics measures to Euro6IX's main Web Server at Consulintel.

At least, BT has expressed interest in testing this system in this way.

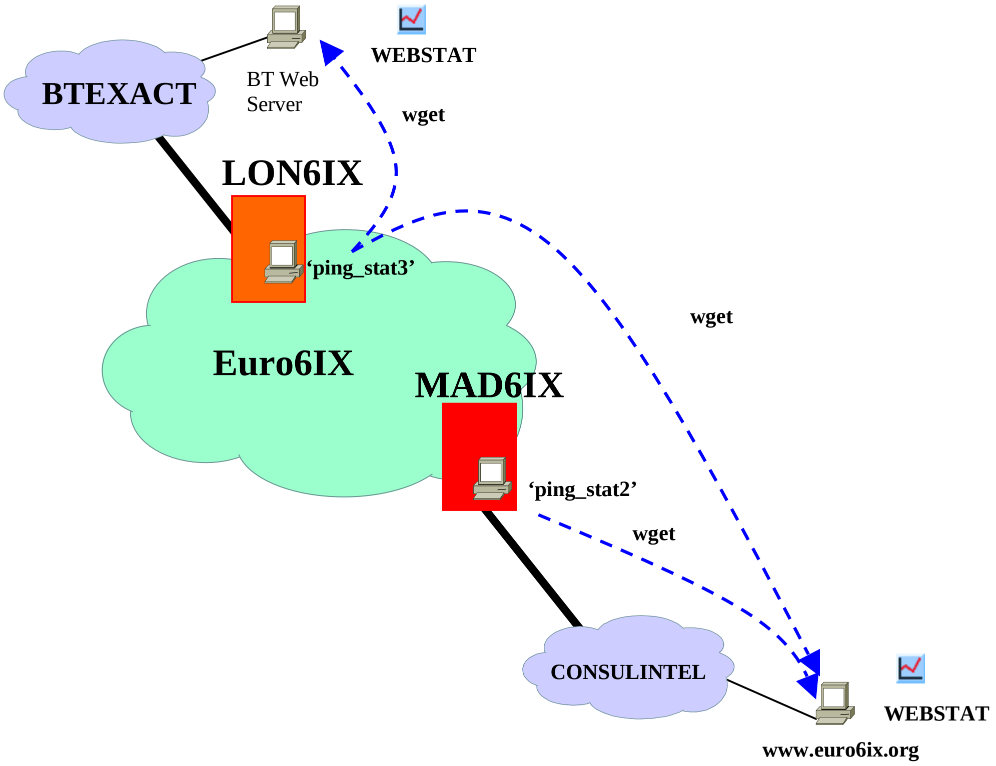


Figure 2-5: Redundant Statistics System

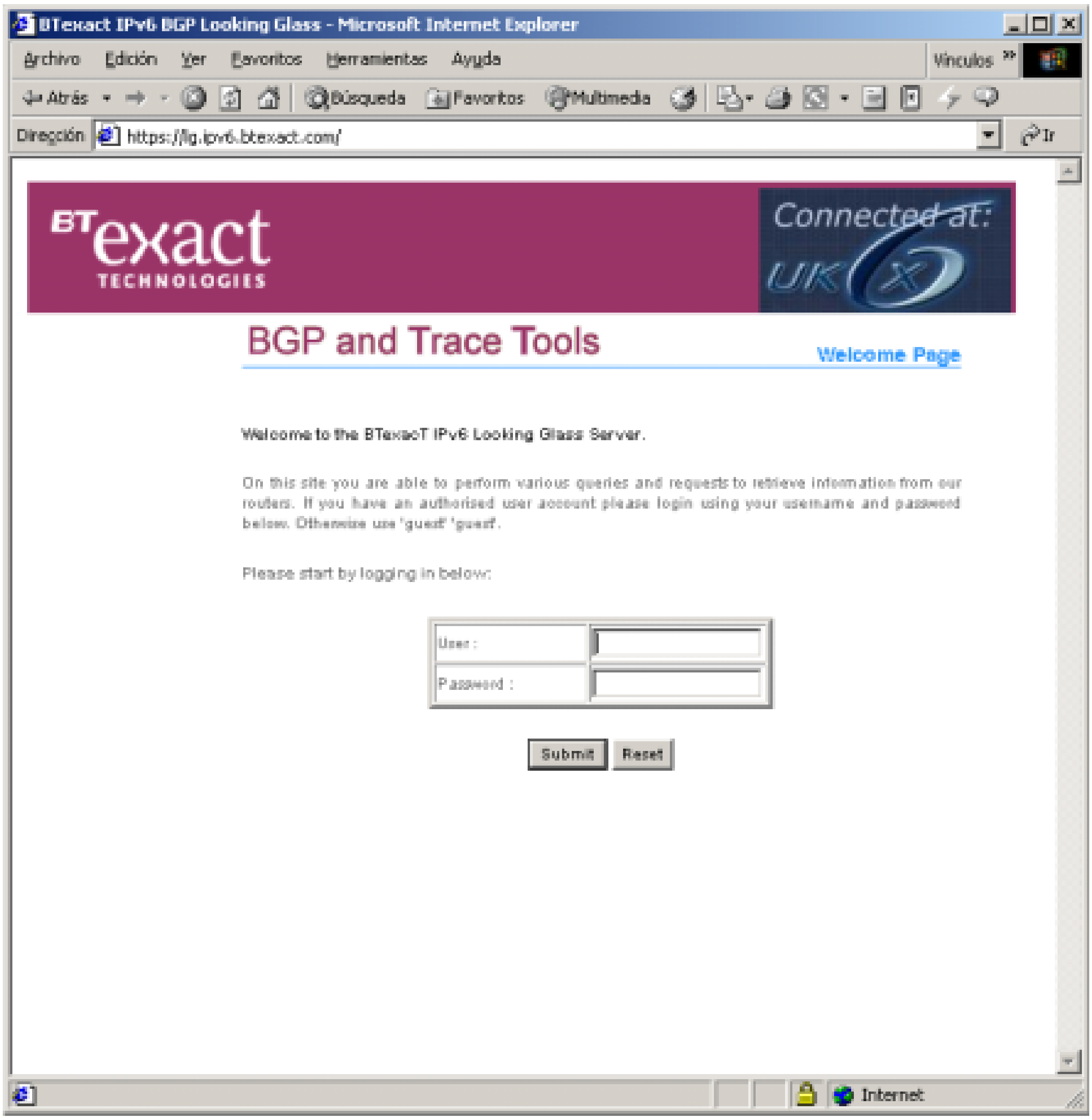
2.3 "BT Looking Glass" System

The Looking Glass is a software tool provided by BTexact at the UK6x IPv6 Internet Exchange that provides a secure web based interface to a number of common IP tools.

Security is provided via two mechanisms: Firstly you can be sure you are communicating with the BTexact Looking Glass because it has a secure certificate issued by VeriSign, and secondly the use of https ensures that the data to and from the users www browser and the Looking Glass server is encrypted and hence is virtually impossible to alter.

Via these mechanisms and the fact that the Looking Glass is built on a well-managed secure platform security and authentication is achieved.

The Looking Glass can be found at https://lg.ipv6.btexact.com/, the welcome page looks like Figure 2-6 where the use of https and certificate (lock) can clearly be seen.


BTexact IPv6 BGP Looking Glass - Microsoft Internet Explorer
Archivo Edición Ver Favoritos Herramientas Ayuda
Vínculos
Atrás
Búsqueda Favoritos Multimedia
Dirección https://lg.ipv6.btexact.com/
Ir
BTexact TECHNOLOGIES
Connected at: UK X
Welcome Page
Submit
Reset
Internet

BGP and Trace Tools

Welcome to the BTexacT IPv6 Looking Glass Server.

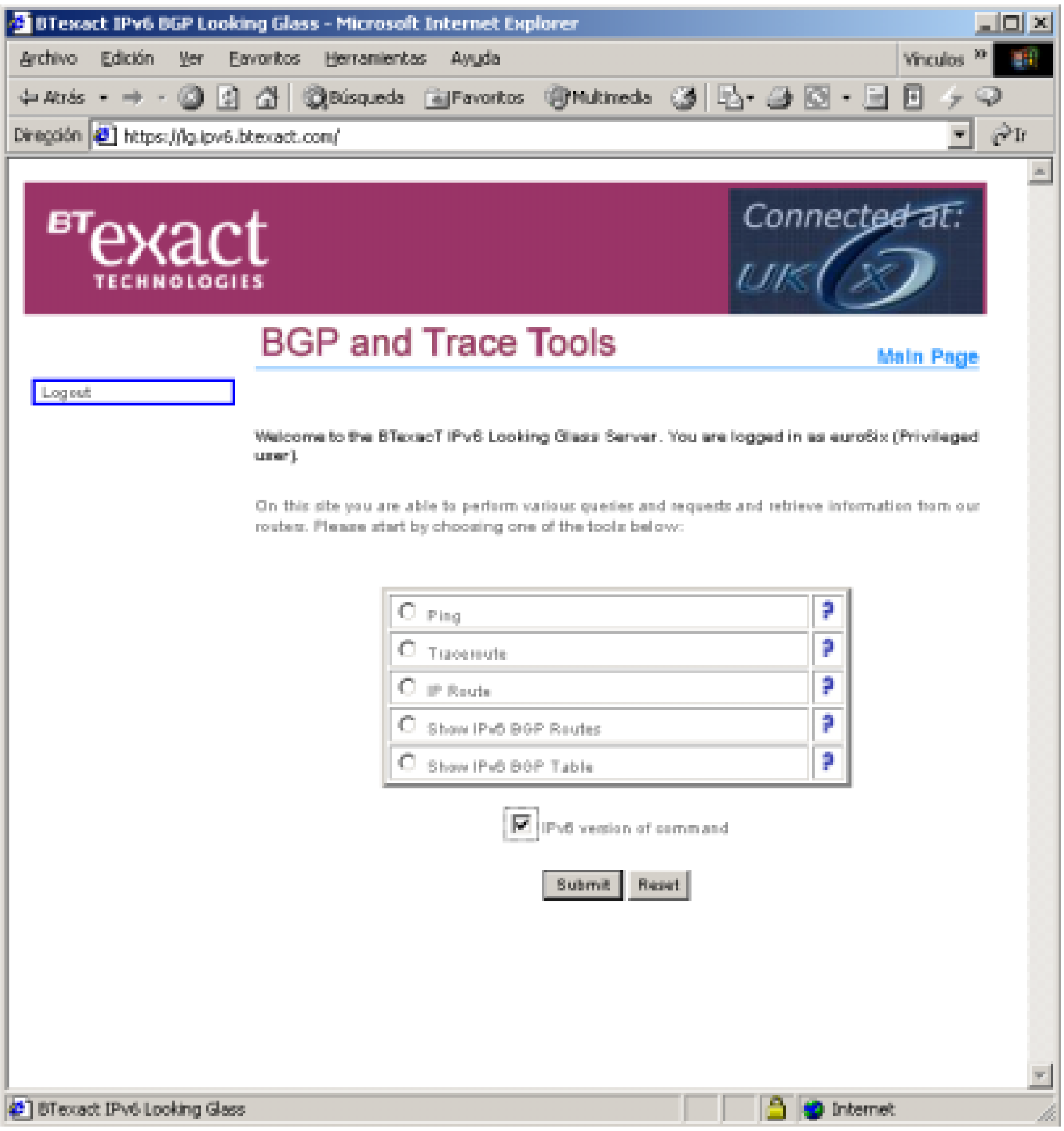
On this site you are able to perform various queries and requests to retrieve information from our routers. If you have an authorised user account please login using your username and password below. Otherwise use 'guest' 'guest'.

Please start by logging in below:

User :	
Password :	

Figure 2-6: BT exact IPv6 Looking Glass System Welcome Page

The services offered by the Looking Glass vary depending upon the users access rights. For the Euro6IX project, a default user and password has been set up and the details distributed to the parties. Once logged on the following several tools are available, as shown in Figure 2-7.


BTexact IPv6 BGP Looking Glass - Microsoft Internet Explorer
Archivo Edición Ver Favoritos Herramientas Ayuda
Vínculos
Atrás
Búsqueda
Favoritos
Multimedia
Dirección
https://lg.ipv6.btexact.com/
Ir
BT exact TECHNOLOGIES
Connected at: UK6X
Main Page
Logout
Submit
Reset
BTexact IPv6 Looking Glass
Internet

BGP and Trace Tools

Welcome to the BTexacT IPv6 Looking Glass Server. You are logged in as euro6ix (Privileged user).

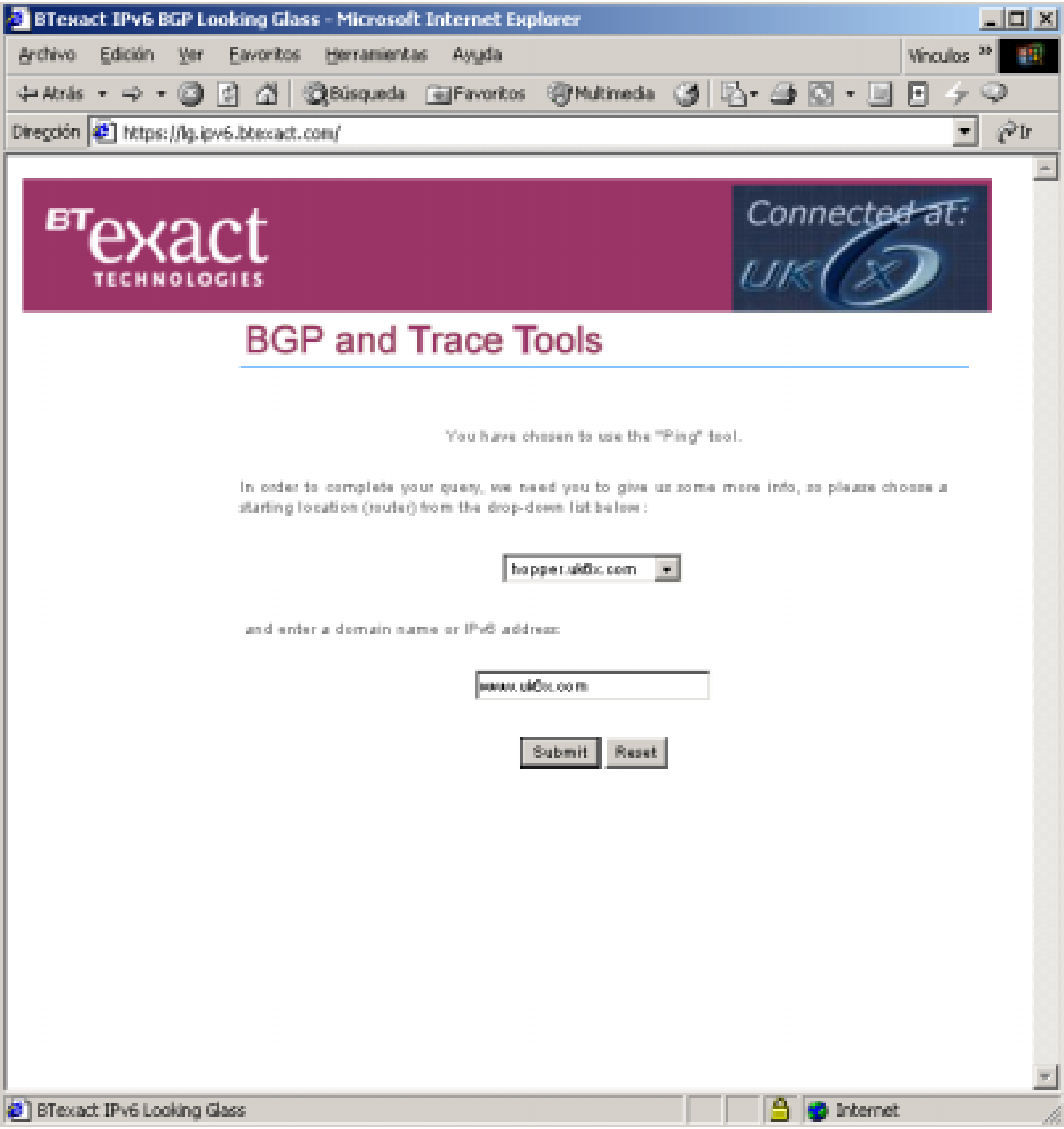
On this site you are able to perform various queries and requests and retrieve information from our routers. Please start by choosing one of the tools below:

○ Ping ?
○ Traceroute ?
○ IP Route ?
○ Show IPv6 BGP Routes ?
○ Show IPv6 BGP Table ?

☑ IPv6 version of command

Figure 2-7: Selection of the Tool

To access, for instance the ping command, just mark the ping box. The “?” icon gives a short explanation. You can request the command to be submitted in IPv4 or IPv6. Once the submit button is clicked the screen at Figure 2-8 is displayed.


BTexact IPv6 BGP Looking Glass - Microsoft Internet Explorer
Archivo Edición Ver Favoritos Herramientas Ayuda
Vínculos »
Atrás
Búsqueda
Favoritos
Multimedia
Dirección
https://lg.ipv6.btexact.com/
Ir
BT exact TECHNOLOGIES
Connected at: UK6X
BTexact IPv6 Looking Glass
Internet

BGP and Trace Tools

You have chosen to use the "Ping" tool.

In order to complete your query, we need you to give us some more info, so please choose a starting location (router) from the drop-down list below :

hopper.uk6x.com

and enter a domain name or IPv6 address:

www.uk6x.com

Submit Reset

Figure 2-8: Location of the Router

Here the router at which the command is to be run is selected, hopper.uk6x.com, is located at the UK6x Internet Exchange and finally the domain or IPv6 address, in this case to ping6, is entered. Once the command is submitted the Looking Glass securely (via SSH) logs onto the router, request that the command is performed and then displays the result back to the user.

It should be noted that because the UK6x infrastructure (including the router Hopper) uses the RIPE allocated Internet Exchange infrastructure addresses that are not globally routable, commands that require global IPv6 routability i.e. ping, traceroute, etc should, in general, not be performed from Hopper but from the router Asterix that has globally routable interface addresses. The reachability of the non globally routable IPv6 interface addresses on Hopper cannot be guaranteed.

At the moment a limited set of 5 commands are available to the Euro6IX users but additional commands can easily be added as well as additional routers.

In practice the Looking Glass with the additional commands and statistics available with other user rights has been found be to a very user friendly convenient tool to monitor and diagnose faults at the UK6x. It is hoped that the Euro6ix account will enable some of these benefits to be available to the Euro6IX partners.

2.4 TILAB's AS Path Tree

ASPath-tree is a tool to perform IPv6 network operation analysis based on the snapshots of the BGP routing table on IPv6 routers running BGP. Originally was 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 functions useful within any operational IPv6 networks, which make use of BGP.

ASPath-tree was developed inside the TILAB's IPv6 laboratory. It was tested on several Solaris (up to 8) and FreeBSD (up to 4.5) platforms, and it should work without problems on any Unix platform (FreeBSD, etc.) with Perl (version equal or greater than 5.0) installed (if there is no a Perl interpreter installed on the system it is possible to download it from the official Perl home page).

Based on a single snapshot of the IPv6 BGP table, it 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 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 TILAB, ASPath-tree is being currently used to monitor TILAB's IPv6 BGP routing configuration and the pages are automatically updated every 5 min.

3. EURO6IX MANAGEMENT SYSTEM PROPOSAL

3.1 Euro6IX Management System based on Magalia

Magalia is a network monitor and management developed at TID labs for Euro6IX project.

It is free binary distribution software between consortium members.

Magalia has been made from scratch to provide a modular design and a distributed architecture model for network management.

In this document several proposals will be given to establish a shared management system between Euro6IX partners of the Euro6IX backbone.

As Magalia is in development phase, its functionality can change according to the results obtained in sub-activity A3.3 of WP3.

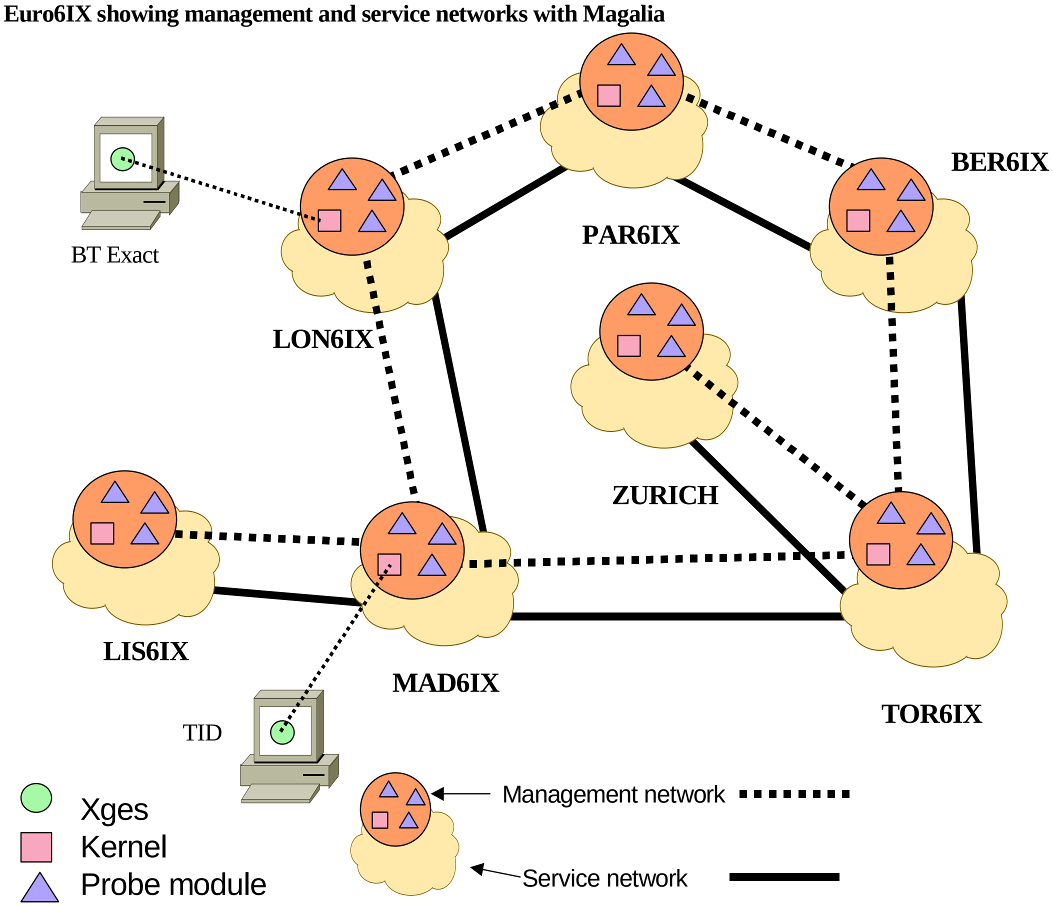


Figure 3-1: Euro6IX Backbone Management and Service Networks

Magalia’s design is represented in the next scheme:

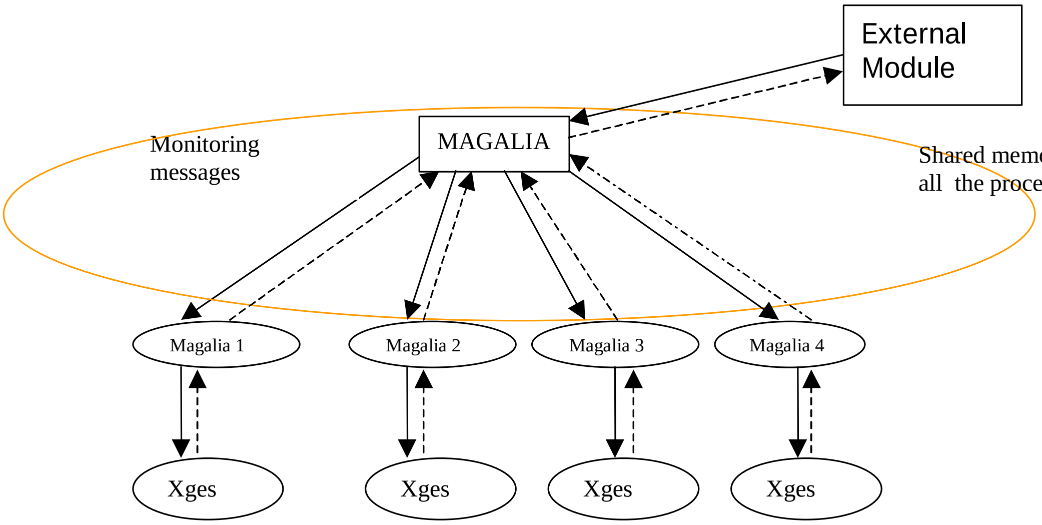


Figure 3-2: Magalia Modular Design

- **Xges**, graphical interface: Reads and interprets the FTR (it is the acronym for Network Topology File, in Spanish) and represents it graphically. It also manages the interaction between the application and the network operator.
- **Magalia,** kernel of the application: Receives notifications of external modules, process them (modifying the FTR if that's the point) and notifies Xges if there have been modifications in the FTR.
- **Plugins**: They are libraries of functions linked dynamically to Xges. They modify the behaviour of the graphical interface. Basically they are translators of Magalia's messages to Xges' low-level messages, and functions that extends Xges' API.
- **External Modules**: They accomplish a very concrete and well-defined operation over certain elements of the net, generally by means of SNMP consultations.

The distribution of each process explained above in Euro6IX network is like the one represented in next scheme:

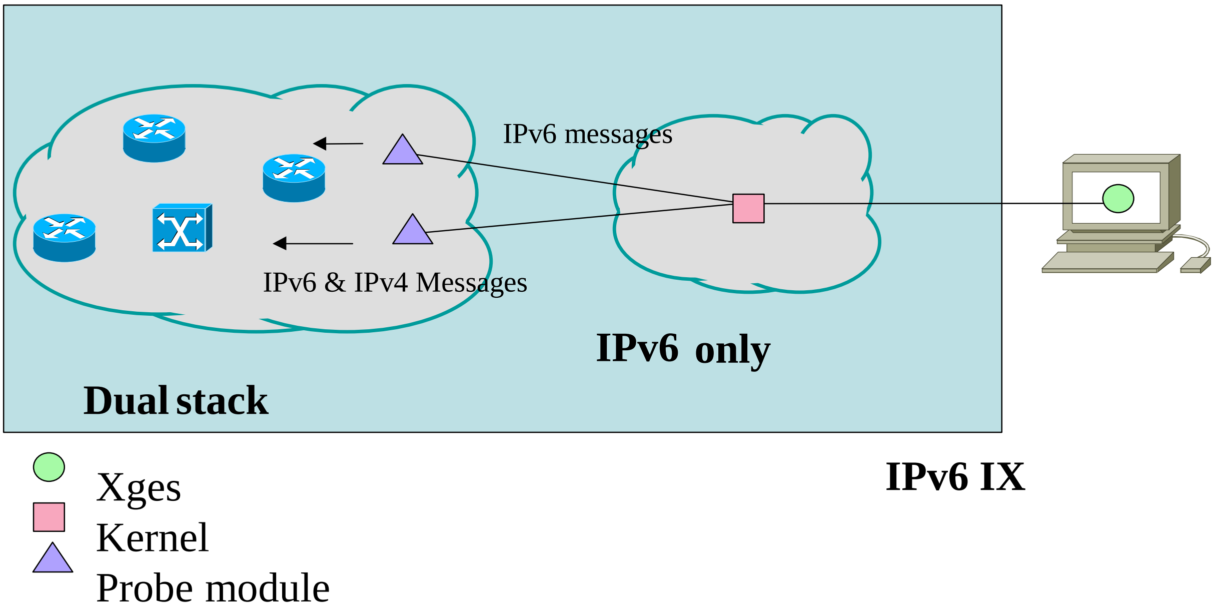


Figure 3-3: Basic Network Architecture

- A Linux PC runs Xges, which connects to Magalia kernel.
- Magalia Kernel is running in other Linux PC in management network of an IX.
- External Modules can run in any PC of the same network, even in the same PC where Magalia Kernel runs. The Modules connect to the server.
- In SNMP-module case, only IPv4 queries can be implemented because there are no routers performing SNMP queries in IPv6 yet. So, the IPv4 query must be done from a PC with IPv4 connectivity with routers.

  This PC has also IPv6 connectivity with Magalia server. This way the communication between Magalia server and SNMP-module is made using IPv6, but the SNMP query is made using only IPv4.
- Magalia Kernel sends this information to Xges terminal through an IPv6 connection.

3.1.1 Architecture of Magalia Advanced Distributed Management System

The objective of this development is to get this full-feature situation:

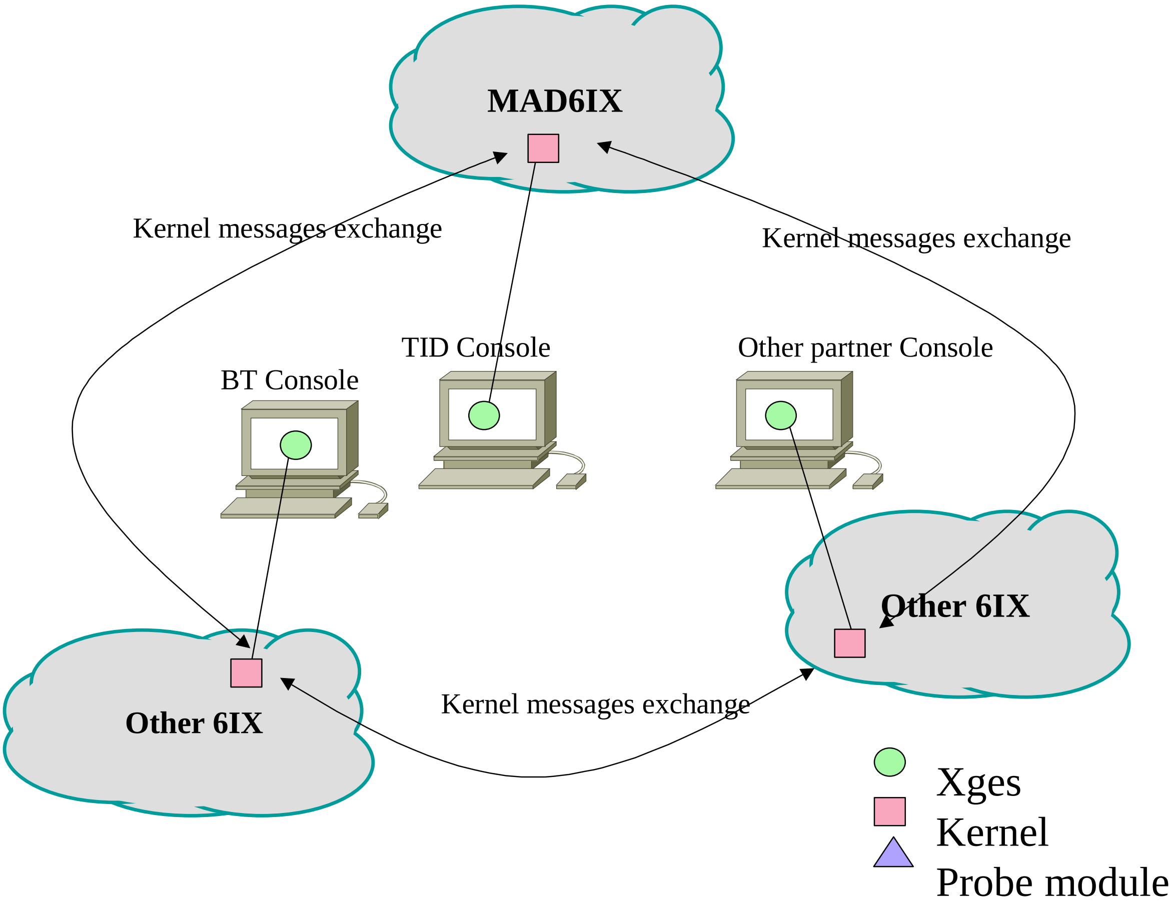


Figure 3-4: Full Vision of the Network

In this case, a global vision of the network is achieved by means of communication between the kernels.

This scheme intends to share public information of other IXs, for example, the state of a link out of local IX reach.

3.1.2 Today's Management Solution/Proposal based on Magalia

With at least two networks running Magalia (ALC6IX and TID) today, this solution is the one implemented:

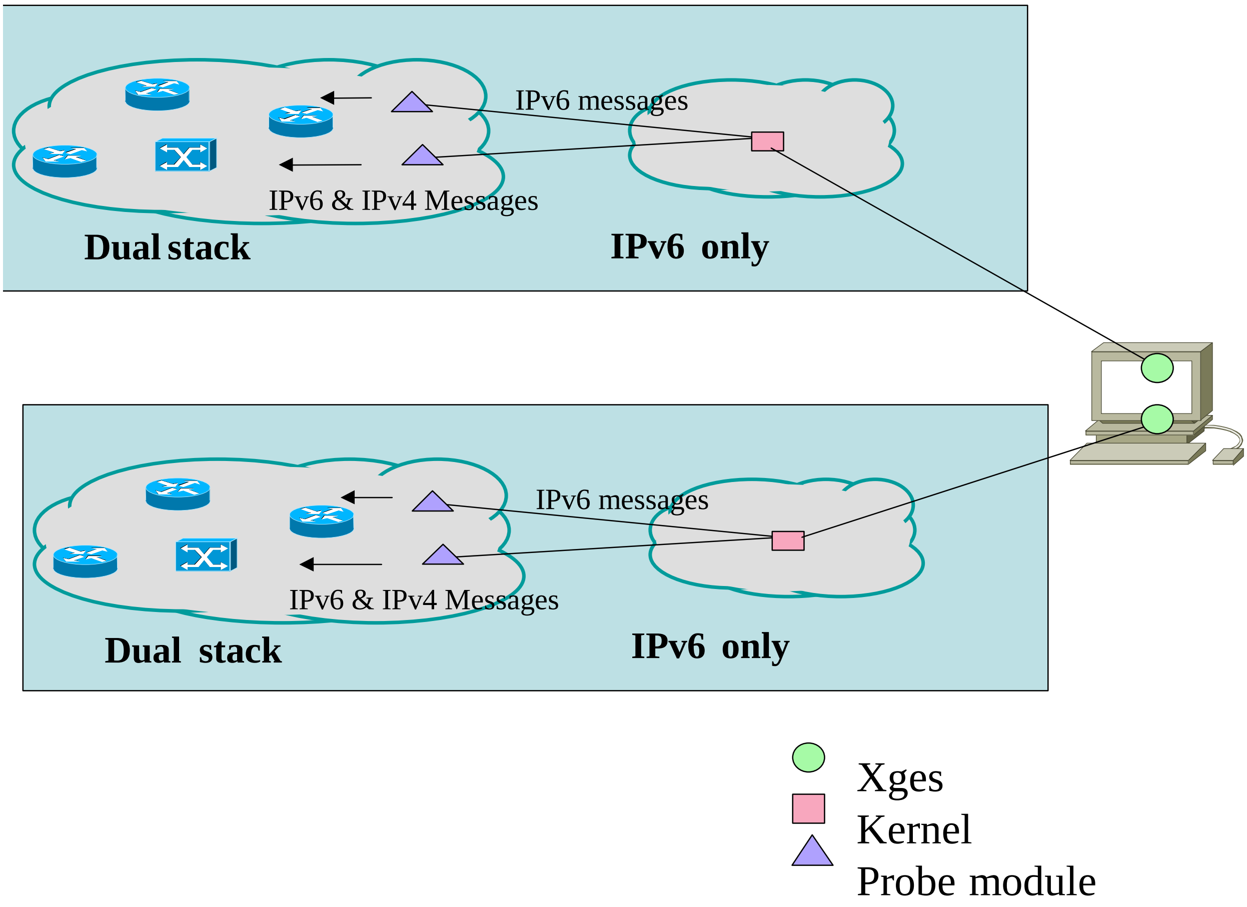


Figure 3-5: Today's Situation as of December 2002

This means that two views, each one with partial information about the state of the network, are available.

An Xges session must be started for each autonomous Magalia system to be monitored, so that each IX can configure their own management solutions, i.e. a user profile for the IX owners and a temporal profile for others (until solution 3.1.4 works).

This scheme was the one used in 31st October review at FT premises.

3.1.3 Management Proposal based on Magalia for the 2nd Year

During the second year, a transitional solution will be implemented in TID labs.

In this case, the vision of the network is still a fragmented one. Xges will connect to every Magalia kernel running in different IXs so that the whole information provided by all Magalia kernel instances could be seen with different connections.

The result of all of this is one only view of Euro6IX network.

This will be possible thanks to the management of users profiles, and the creation of a generic user in every IX called “Euro6IX” (Euro6IX/members) in order to assure a trustworthy access to every IX.

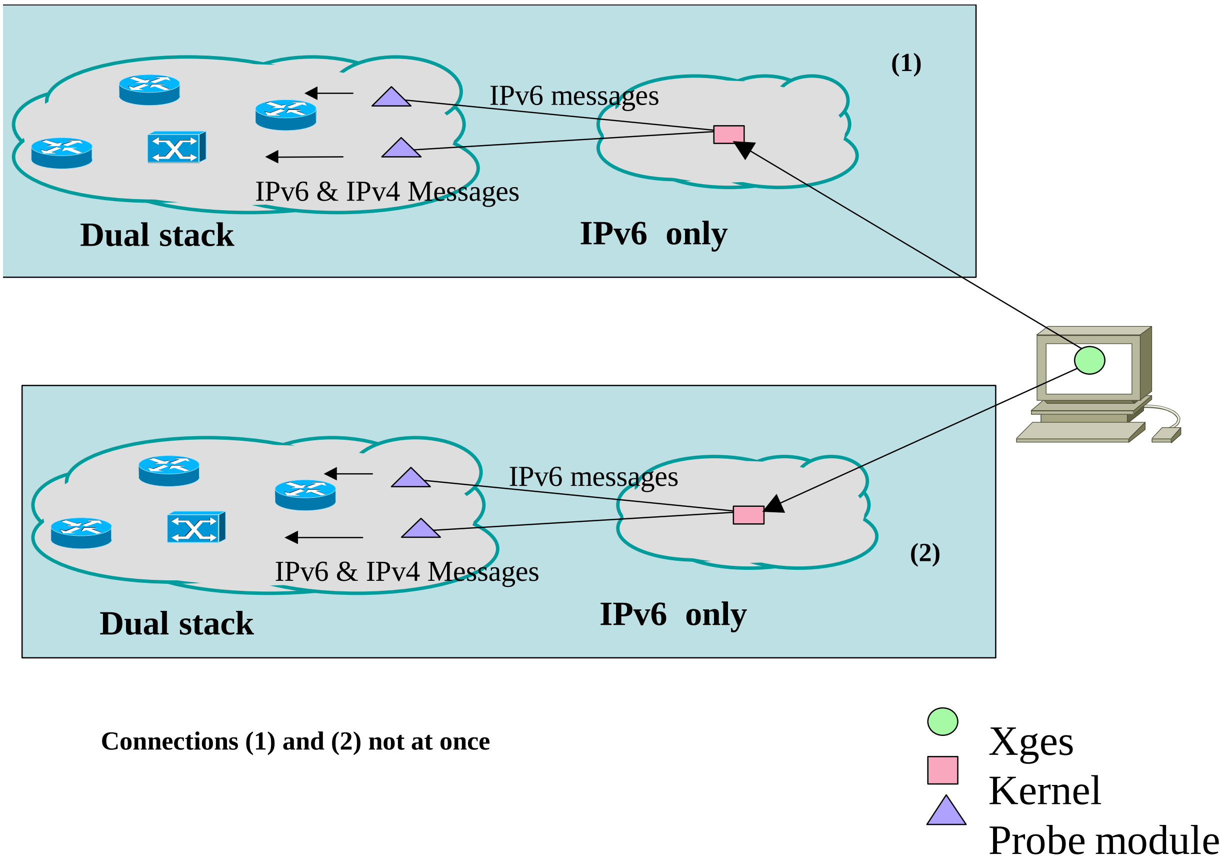


Figure 3-6: Transitional Proposal

This solution will be tested at March 2003 involving MAD6IX and LON6IX.

It is important to remark that this is a temporal solution since it is not expected in the future a telco allowing another one accessing their management kernel (even with user profiles). For a commercial situation, other solutions should be applied, as the described in next section.

3.1.4 Basic Distributed Management System Proposed

A beta version of Magalia including the full-feature scenario with communication between kernels (which implies full vision of the network) will be available in June 2003.

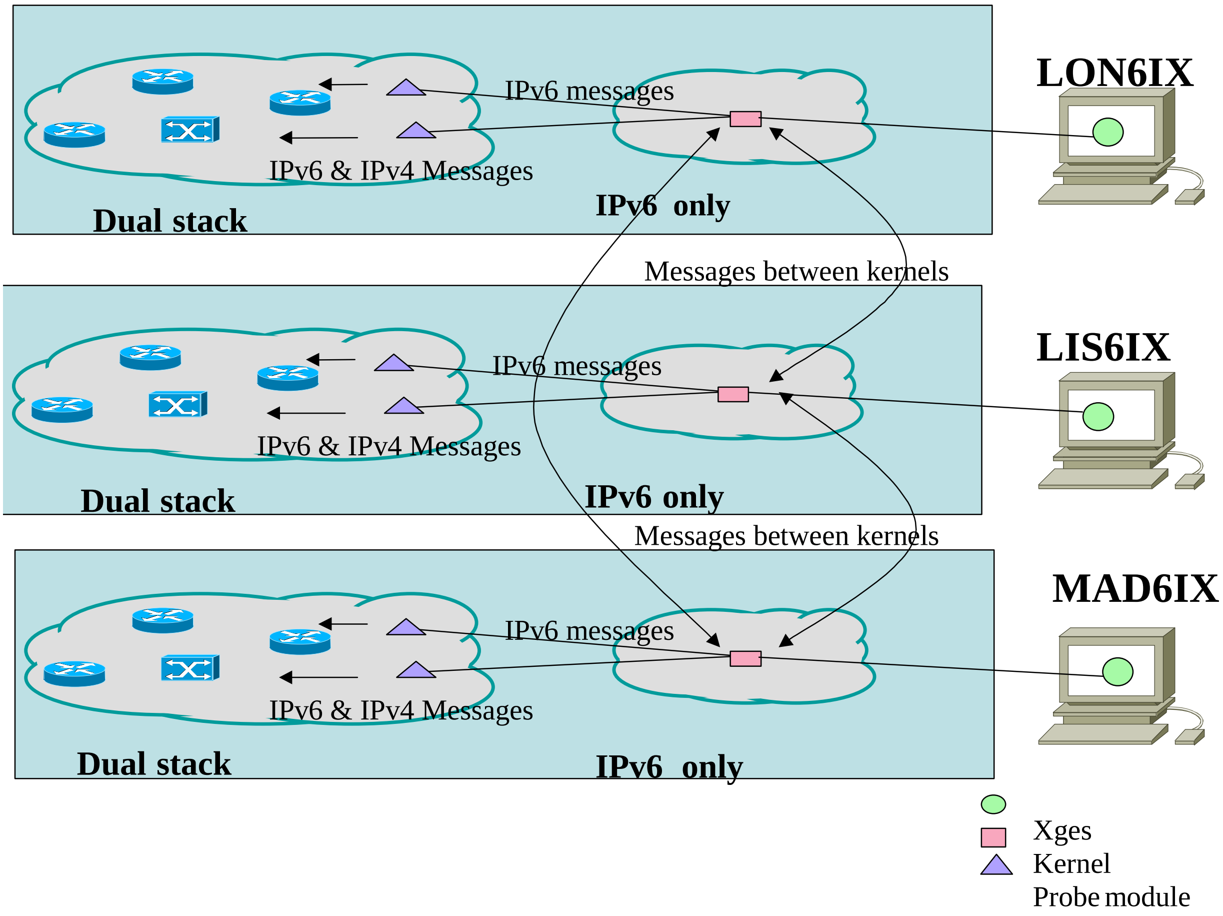


Figure 3-7: Solution for Full Vision

The test of this situation will involve MAD6IX, LIS6IX and LON6IX.

4. EURO6IX SECURITY CONTROL SYSTEMS PROPOSAL

4.1 Topaz: An IDS Tool

In order to detect attacks, TID labs are developing Topaz. Topaz will be tested in the following scenario:

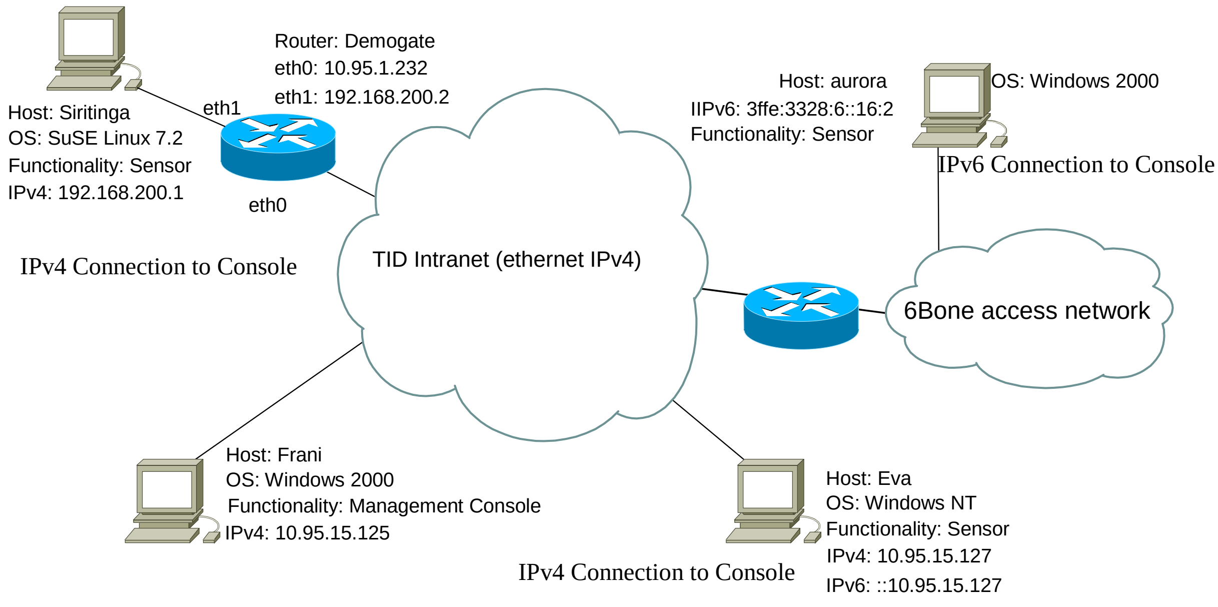


Figure 4-1: Topaz IDS Tool Test Scenario

This scenario is a IPv4/IPv6 network. The sensors are located in dual stack hosts. IPv6 addresses are IPv4 compatible addresses.

Tests in Euro6IX network (IPv6 native networks) will begin in first semester of 2003.

Management Console is executed in a Windows 2000 host with dual stack. The management console is able to receive requests from both IPv4 and IPv6.

Three hosts with three different Operating Systems (Linux, Windows 2000, and Windows NT) and three different network configurations (IPv4 only, IPv6, and IPv4/IPv6) compose the Sensors System

One of them, *Siritinga*, is connected to the *Management Console* through a router. *Siritinga* is dual stack.

The tests made in this environment are satisfactory. It has been demonstrated the establishment of connections to the *Management Console* both in IPv4 and IPv6, and the operation of the sensors in different platforms.

The *sensors system* detect two attacks implemented:

- ICMP attacks to restricted hosts.

- Connection limits to a port.

When a sensor detects an attack, it notifies about it to the *Management Console*.

The communication between Sensors and Management Console is carried out by means of a protocol specifically developed for this purpose.

5. SUMMARY AND CONCLUSIONS

This document has presented all the developments done during first year related to the network management and statistics control and presented a first scenario of how to test these systems.

Efforts done in adaptation of IPv4 network control systems to obtain reliable statistics, show how important is to every exchanger the statistics of the network. Any new system developed will be included in the final version of this document.

Related to the network management, a new concept has been introduced, the “Shared Network Management”, i.e., the possibility to see what is happening in the whole network, not just in a local place or IX. This will be done thanks to the sharing of information with a new protocol that has to be approved by all the partners. The final version will include this protocol and the results of the test of this new concept.

Another important point to assure the control of the network is the security. In the context of A4.2, an IDS is being developed. In the final version, the final scenario in TID test-bed and some indications of where to install this tool in any partner will be included. Also will include a brief description of new attacks implemented.