



IST-2000-32603	Deliverable 6.3.2. Interim report on the implementation of tools and operational procedures	
----------------	---	--

<b>Project Number:</b>	IST-2001-32603
<b>Project Title:</b>	6NET
<b>CEC Deliverable Number:</b>	32603/ DANTE/DS/D6.3.2/A6.2
<b>Title:</b>	Interim report on the implementation of tools and operational procedures
<b>Work Package:</b>	WP6
<b>Type of deliverable*:</b>	R
<b>Deliverable security class**:</b>	PU
<b>Editors:</b>	Ana Romero
<b>Contributors:</b>	Isabelle Astic, Frank Aune, Wojbor Bogacki, Arnaud Brucy, Tim Chown, Lorenzo Colitti, Lucas Dolata, Jérôme Durand, Olivier Festor, Bartosz Gajda, Martin Kaminski, Ioannis Kappas, Radoslaw Krzywania, Olav Kvitem, Roman Lapacz, Simon Leinen, Janos Mohacsi, Wiktor Procyk, Tomasz Szewczyk, Robert Szuman, Christian Schild, Andre Stolze, Tina Strauf


<b>Abstract:</b>
<p>This document gives a detailed overview of</p> <ul style="list-style-type: none"> <li>- Implementation of management, measurement and monitoring tools in 6net</li> <li>- Operational procedures in 6net</li> </ul>

<b>Keywords:</b>
IPv6, research, connectivity.

IST-2000-32603	Deliverable 6.3.2. Interim report on the implementation of tools and operational procedures	
----------------	---	--

## **Interim report on the implementation of tools and operational procedures**

<b>INTERIM REPORT ON THE IMPLEMENTATION OF TOOLS AND OPERATIONAL PROCEDURES.....</b>	<b>2</b>
<b>1 INTRODUCTION.....</b>	<b>3</b>
<b>2 RELATION WITH OTHER DELIVERABLES.....</b>	<b>3</b>
<b>3 IMPLEMENTATION OF TOOLS IN 6NET.....</b>	<b>3</b>
3.1. TOOLS USED.....	3
3.2. ARGUS.....	4
3.3. AS-PATH-TREE.....	4
3.4. CRICKET.....	6
3.5. ETHEREAL.....	7
3.6. IPFLOW.....	7
3.7. 6NET LOOKING GLASS.....	8
3.8. IPV6 MANAGEMENT GATEWAY (OLD NAME: SNMP TRANSITION TOOL).....	8
3.9. IPV6 SUPPORT FOR NETFLOW V9 IN IOS.....	10
3.10. MPING.....	10
3.11. MRTG.....	11
3.12. MULTICAST BEACON.....	12
3.13. NAGIOS.....	13
3.14. NETFLOW/IPFIX.....	14
3.15. NETSNMP.....	14
3.16. PCHAR.....	15
3.17. RANCID.....	16
3.18. RIPE TT SERVER.....	16
3.19. WESTHAWK SNMP STACK.....	17
3.20. TOOLS USED BY 6NET NOC.....	19
3.21. SUMMARY.....	20
<b>4 OPERATIONAL PROCEDURES USED IN 6NET.....</b>	<b>20</b>
4.1. OPERATIONAL PROCEDURES BY 6NET NOC.....	20
4.2. OPERATIONAL PROCEDURES FOLLOWED BY 6NET PARTNERS.....	22
4.3. OPERATIONAL PROCEDURES DURING TEST PERIODS FOR 6NET NOC AND 6NET PARTICIPANTS.....	22

IST-2000-32603	Deliverable 6.3.2. Interim report on the implementation of tools and operational procedures	
----------------	---	--

## 1 INTRODUCTION

Deliverable 6.3.2. ‘Interim report on the implementation of tools and operational procedures’ gives a description of the real usage of the tools in 6net network including the 6net core and each National IPv6 tests/pilot network. This document continues the work done in Deliverable D6.3.1. ‘6net IPv6 Network Management Cookbook’ which covers a set of recommendations for managing and monitoring networks.

D6.3.2 also summarises the operational procedures followed by 6net NOC and 6net partners and updates the information given in deliverables D1.2. and D1.3.

## 2 RELATION WITH OTHER DELIVERABLES

Part 3 ‘Implementation of tools in 6net’, concerning tools used in 6net continues the work done in D6.3.1 which documents design, features, recommendations and tools that may be used to manage and monitor a wide area IPv6 network more concisely. D6.3.2 describes the tools used in 6net to manage and monitor the network.

D6.3.2 is related with ‘D.6.2.3. Interim report on development and test’ which describes the development and test of tools done by 6net partners. Deliverable 6.3.2. describes the tools which has been really used and explains how 6net partners are using them.


Part 4 ‘Operational procedures used in 6net’ summarises the procedures to be followed by 6net NOC which are described in detail in D1.2 and D1.3. already submitted to EC.

## 3 IMPLEMENTATION OF TOOLS IN 6NET

There are many tools to manage and monitor networks nowadays. Here, in this part, it is presented a description of the tools used by 6net participants in order to manage and monitor 6net network. For each tool, it gives an explanation of how they are used and some examples of current implementation in 6net network.

### 3.1. Tools used

Argus  
AS-path-tree  
Cricket  
Ethereal  
Infovista  
Intermapper  
IPFlow

IST-2000-32603	Deliverable 6.3.2. Interim report on the implementation of tools and operational procedures	
----------------	---	--

6net Looking glass  
 IPv6 management gateway  
 IPv6 support for Netflow v9 in IOS  
 Mping  
 MRTG  
 Mcast Beacon  
 Nagios  
 Netflow/IPFIX  
 NetSNMP  
 PCHAR  
 RANCID  
 RIPE TT server  
 Westhawk SNMP Stack

### 3.2. *Argus*

Argus is a system and network monitoring application which includes IPv6 support since version 3.2. It will monitor nearly anything you ask it to (TCP and UDP applications, IP connectivity, SNMP OIDS, etc). It comes with a nice and clean, easy to view web interface that will keep both the managers and the technicians happy. Argus contains built-in alert notification via email and pager (qpage) but is easily extendible to use any other program like i. e. winpopup etc. It will automatically escalate alerts until they are acknowledged by resending the alert at different intervals while optionally switching to other methods of notification or other recipients. Due to the fact that most of the testing modules are written in perl IPv6 functionality is included in most of them.

For installation one has to fulfill a few prerequisites to use the program with IPv6. Other than a running an operating system that supports IPv6 one also has to have both Socket6.pm and fping6 installed. The standard fping is only IPv4 capable but the fping sources at fping.com can be compiled to either work with IPv4 or use IPv6. One binary only works with one protocol at a time. For configuration there is really nothing IPv6 specific to do. If you specify an IPv6 address or hostname that resolves to an IPv6 address, IPv6 will be used for the test.

For further documentation and downloading the program itself please refer to the project's homepage at <http://argus.tcp4me.com>.


#### **Example of running implementations available in 6net**

An example of a running implementation of the program is publicly available within 6net at:

<https://www.join.uni-muenster.de/cgi-bin/arguscgi?func=login> (user:6net password:<any>)

### 3.3. *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 Aspath-tree designed to be used by an IPv6 site involved in

IST-2000-32603	Deliverable 6.3.2. Interim report on the implementation of tools and operational procedures	
----------------	---	--

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.

The tool currently supports Cisco/Juniper/Zebra routers. Based on a single snapshot of the IPv6 BGP table, 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 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 neighbours (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

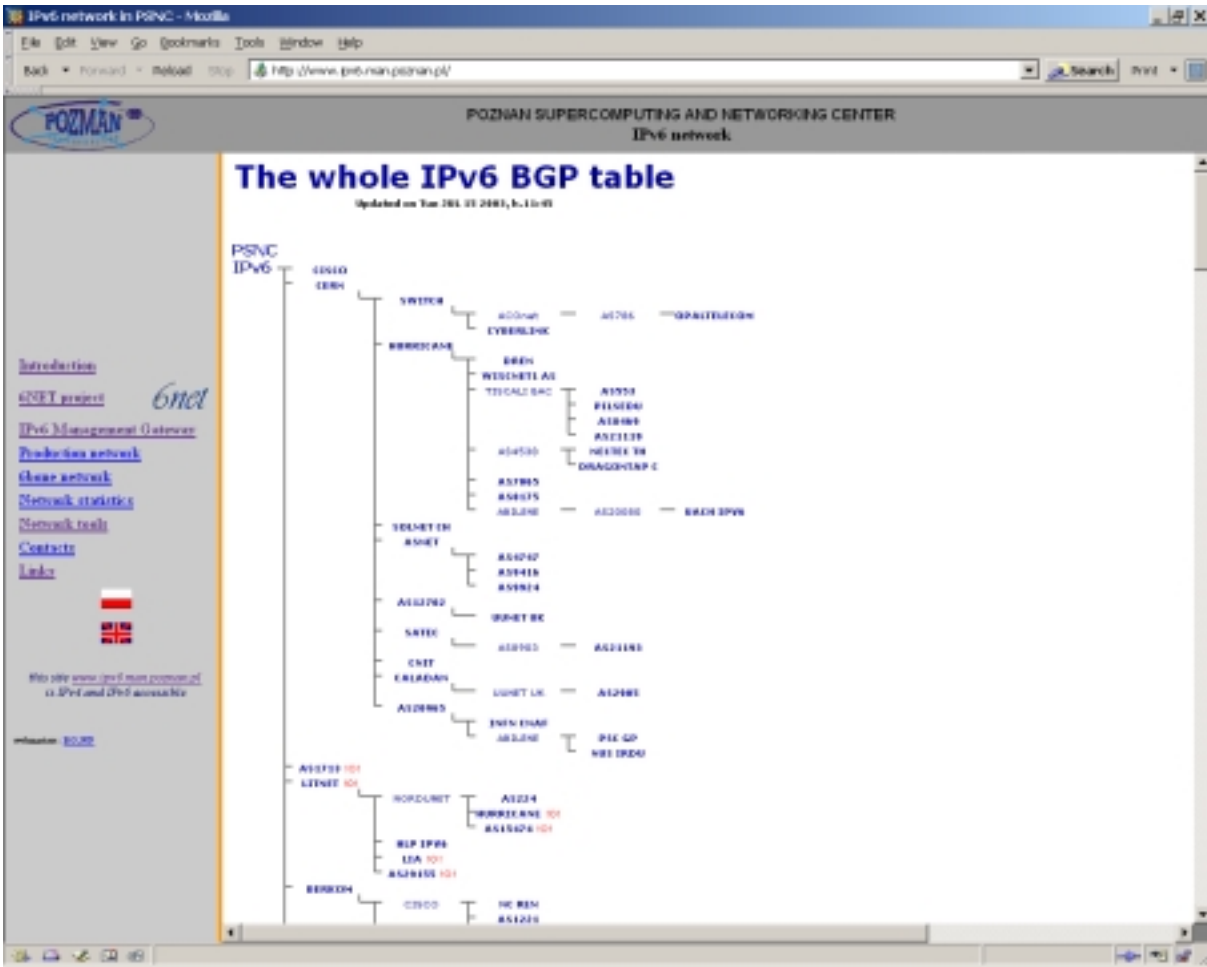
Application domains in the 6Net management framework ASpath-tree will be very useful to verify routing tables of the backbone, to check every configuration and to have some statistics about the backbone routers.

ASpath-tree is very useful for network routing engineering. It makes it possible for a network administrator to clearly see what is the routing map and if the announcements are coherent. In this period, while more and more sites are moving to IPv6, network administrators have to check often their routing policy to be sure routing is optimal.


### Example of running implementations available in 6net

- 6NET backbone: <http://6nettools.dante.net/ASpath-tree/bgp.html> (version 3.3)
- CERN: [http://www-ipv6.cern.ch/ASpath-tree-v3\\_3/htdocs/bgp/bgp.html](http://www-ipv6.cern.ch/ASpath-tree-v3_3/htdocs/bgp/bgp.html) (version 3.3)
- NIIF/HUNGARNET: <http://6net.iif.hu/6netaspathtree/> (version 4.2)
- JOIN/DFN: <http://www.join.uni-muenster.de/bgp/bgp.html> (version 4.1)
- SWITCH: <http://www.switch.ch/network/ipv6/bgp/> (version 3.3)
- UNINETT: <http://drift.uninett.no/ipv6/bgp/bgp.html> (version 4.1)
- RENATER: <http://supervision-ipv6.renater.fr> (for both IPv6 unicast and IPv6 multicast BGP trees)
- PSCN: <http://www.ipv6.man.poznan.pl/> (version 4.1.)

The following figure is a snapshot taken from PSCN running implementation:



### 3.4. Cricket

IST-2000-32603	Deliverable 6.3.2. Interim report on the implementation of tools and operational procedures	
----------------	---	--

Cricket is a high performance, extremely flexible system for monitoring trends in time-series data. Cricket was expressly developed to help network managers visualise and understand the traffic on their networks, but it can be used all kinds of other jobs, as well.

Network operators require awareness of how well their network performs. Every node in the network keeps statistics on many attributes that affect its performance. The operators would like to constantly monitor these attributes over time and keep track of their intensity. The tool can be used by anyone who wants to monitor and plot value variations of network attributes inside their management domain.

### **Example of running implementations available in 6net**

<http://6net.iif.hu/cricket/grapher.cgi> (HUNGARNET: same user ,6core‘ from tools.6net.org)

### **3.5. *Ethereal***

Ethereal is a packet analyser with a graphical (GTK) front-end that supports drill-down. Ethereal fully supports the basic IPv6 protocols, and all TCP- and UDP-based application protocols running over IPv6. It is widely used to develop and troubleshoot IPv6 applications and protocols.

Proposed extensions Protocols that are used or developed within 6NET could be supported with additional or improved dissectors if required.

### **Example of running implementations: PSCN**


Ethereal is a useful network protocol analyzer for Unix and Windows. Because it is free, it is IPv6 enabled and it runs on many system platforms; PSCN often use it when they need to examine the network flows. Ethereal offers a graphical interface and allows to set up different filters. In case of Linux systems, PSCN more often use a standard tool – tcpdump, which is build in the system and it is generally sufficient in its functionality. But in case of windows system, there is no build-in tool for analyzing packet, so Ethereal is very useful.

### **3.6. *IPFlow***

IPFlow is a collector for Netflow version v1, v5, v6, v7, v8 and v9. It supports logging flow data to disk, data aggregation according to configuration, port scan detection, storage of aggregated data in RRDtool, and graphical display of flow statistics. The author is Christophe Fillot.

### **Example of running implementations**

SURFnet

IST-2000-32603	Deliverable 6.3.2. Interim report on the implementation of tools and operational procedures	
----------------	---	--

HUNGARNET.

### 3.7. *6net looking glass*

Looking Glass is a tool available for the 6net core. It is a CGI script which allows to connect to a remote router from a simple web page, to run some commands on the router and to show the result on another web page. Its pre-requisite is a simple user login on the router.

#### **Example of running implementations available in 6net**

<http://6nettools.dante.net/diafaneia/> (user 6core, password available in [www.6net.org](http://www.6net.org) private area)

- Some commands about the BGP4+ protocol:

- Retrieve BGP status
- Retrieve BGP peer status
- List routing table

- Multicast services

- Multicast PIM topology
- Multicast RPF check
- List multicast routing table


- Some other services:

- ping
- traceroute

### 3.8. *IPv6 management gateway (old name: SNMP Transition Tool)*

The main purpose of the developed IPv6 Management Gateway is to enable the existing IPv4 network management platforms to monitor, configure and manage the native IPv6 network. The IPv6 Management Gateway translates SNMP and ICMP protocol messages between IPv4 and IPv6 networks.



IST-2000-32603	Deliverable 6.3.2. Interim report on the implementation of tools and operational procedures	
----------------	---	--

**Example of running implementations available in 6net**

The IPv6 Management Gateway is being used to support the monitoring of 6NET core routers and “ping hosts”. Monitoring is performed using [Ipswitch, Inc.](#) WhatsUp Gold (Fig.1, Fig.2), which supports only IPv4.

IPv6 Management Gateway translates SNMP and ICMP protocol messages between WhatsUp Gold (IPv4) and 6NET network (IPv6).

WhatsUp Gold is accessible at <http://chives.man.poznan.pl>; IPv6 Management Gateway works on [plum.man.poznan.pl](http://plum.man.poznan.pl).



Fig. 1



Fig. 2

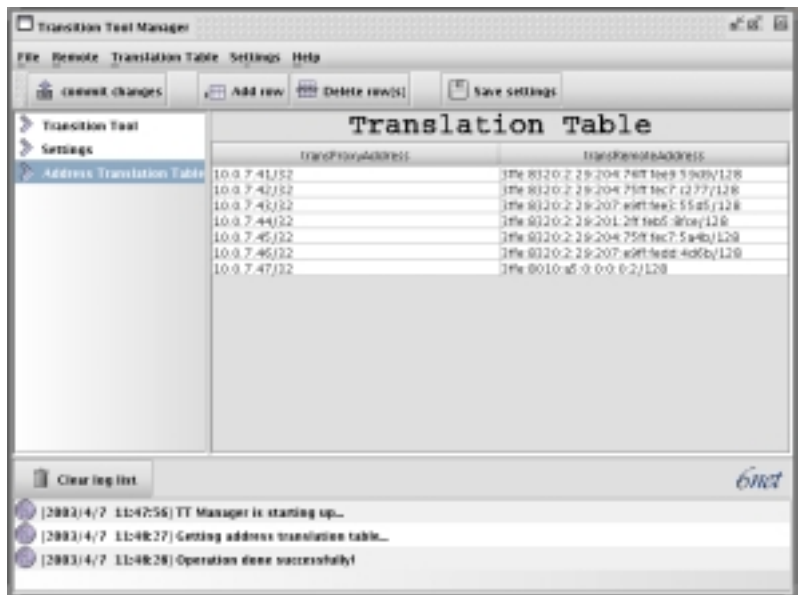



Fig. 3

Configuration has been made using the IPv6 Management Gateway Configurator (Fig.3).

# Configuration file for the mg6gateway

IST-2000-32603	Deliverable 6.3.2. Interim report on the implementation of tools and operational procedures	
----------------	---	--

# Syntax:

# <ip address of proxy> <ip address of agent>

```

150.254.160.130 2001:798:10::1
150.254.160.131 2001:798:12::1
150.254.160.132 2001:798:14::1
150.254.160.133 2001:798:16::1
150.254.160.134 2001:798:17::1
150.254.160.135 2001:798:20::1
150.254.160.136 2001:798:22::1
150.254.160.137 2001:798:25::1
150.254.160.138 2001:798:28::1
150.254.160.139 2001:620:0:1:208:2ff:fea0:bab9
150.254.160.140 2001:718::8
150.254.160.141 2001:638:0:500::1
150.254.160.142 2001:648:0:1000:a00:20ff:fea7:83e5
150.254.160.143 2001:738:0:402::2
150.254.160.144 2001:760:fff:1::1
150.254.160.145 2001:610:1:800b:260:8ff:fe5a:b397
150.254.160.146 2001:700:0:501:230:48ff:fe21:d805
150.254.160.147 2001:630:0:5:a00:20ff:fe77:e773
150.254.160.148 3ffe:8010:a5::2
150.254.160.149 2001:628:402:1:210:dcff:fef1:23f8
150.254.160.150 2001:808::1
150.254.160.151 3ffe:8320:2:29:207:e9ff:fee3:55d5

```

### 3.9. *IPv6 support for Netflow v9 in IOS*


The metering/exporting side of Netflow v9 has been implemented in Cisco IOS. Currently, 3640 and 7200/7500 routers are supported. This tool is used by SWITCH, RENATER, SURFnet and DANTE.

### 3.10. *Mping*

Mping collects ping statistics for multiple hosts at the same time. Making a mping on all the hosts from a traceroute command would give more statistical information than the traceroute itself. It can do percentiles and SDV statistics, sorted reports, histograms and curves. It does accumulation over days and months.

The Mping service consists of two parts: The Mping client, written in C, and the web interface extension, written in PERL. Unless otherwise specified, in this document when referring to Mping we are referring to the Mping C-client.

Mping is a tool for measuring round-trip delay and packet loss, using the ICMP echo feature, in a TCP/IP based network. Multiple hosts - up to 500, both IPv4 and IPv6 at the same time - can be pinged in a round-

IST-2000-32603	Deliverable 6.3.2. Interim report on the implementation of tools and operational procedures	
----------------	---	--

robin order. At runtime, the user can set the wait time between each packet sent, number of packets sent and the size of the packets. For each host specified, information about packet loss and minimum/average/maximum response time is displayed. Mping can also display the collected data as median, cube-sum, standard deviation or 10/50/90-percentile at the users request.

Several techniques are implemented into the Mping service, to make sure that the collected data is “statistically” correct:

- Mping by default do not send more than 10 ICMP packets per second, thus measured data is independent from the time of measuring.
- Mping do not send all ICMP-packets to one 'Gateway' at the same time, rather Mping tries to spread it out in a Round-Robin fashion, thus avoids temporary network characteristics.
- Mping starts the pingsweeps at asynchronous intervals. We use a Poisson-distribution, thus avoiding periodic network variance.

Technique 1 and 2 are Mping C-client features, while 3 is implemented in the PERL web interface extension.

A web interface is used for browsing the collected data and for generating reports, graphs and traceroutes for the different hosts we measure. The PERL code is modularised and easily extended to suite other needs. As an example, the language support is modularised and thus adding support for new languages is very easy.

### Example of running implementations available in 6net

UNINETT: <http://mping.uninett.no>

### 3.11. MRTG

The Multi Router Traffic Grapher (MRTG) is a tool to monitor the traffic load on network-links. MRTG generates HTML pages containing graphical images which provide a LIVE visual representation of this traffic. It does support SNMP over IPv6 in Linux, but it is used only in IPv4.

MRTG is already widely used to monitor the traffic on network links, CPU usage on routers, and other network and host parameters.


It is a very popular tool to monitor the traffic load on network-links. The results are presented as images on web pages, which are frequently regenerated to show – up-to-date network statistics.

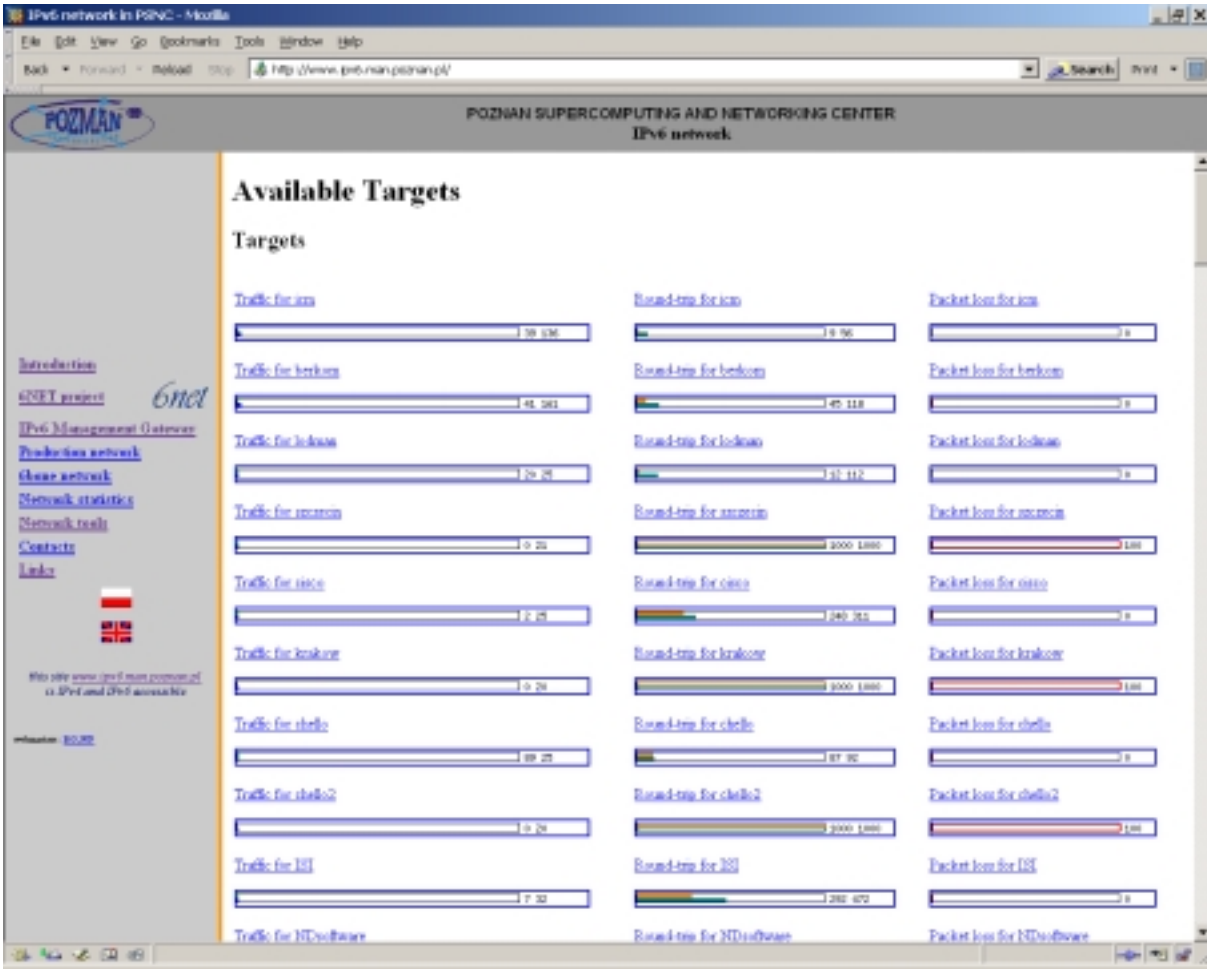
### Example of running implementations available in 6net

GARR: <http://www.uniroma3.6net.garr.it/mrtg/graphs/gsr.html>

RENATER: <http://supervision-ipv6.renater.fr>

In PSNC, they use MRTG based on IPv4 MIBs (IPv6 MIBs are not implemented yet). They monitor all IPv6/IPv4 network tunnels outgoing from our 6bone router. These statistics are available on public web server: <http://www.ipv6.man.poznan.pl/> under the “network statistics” link.

IST-2000-32603	Deliverable 6.3.2. Interim report on the implementation of tools and operational procedures	
----------------	---	--




PSCN also monitor their connections to the 6NET network outgoing from our access router and also additional routers parameters like i.e. CPU usage. However, because of the security issue these statistics are not publicly available.

**3.12. Multicast Beacon**

Multicast Beacon is the application for monitoring the parameters of multicast traffic. These parameters are: loss, delay, jitter, duplicate, order. The application consists of two parts: server and clients. The role of the server is collecting information received from clients and presenting them by means of a stand-alone GUI tool or HTTP interface. The second approach is very usable for a large number of users interested in the collected results. They can observe the parameters via web browser, like Internet Explorer or Netscape Navigator

Beacon can be useful in multicast traffic monitoring in IPv6 networks

IST-2000-32603	Deliverable 6.3.2. Interim report on the implementation of tools and operational procedures	
----------------	---	--

### Example of running implementations available in 6net

<http://beaconserver.lan.switch.ch:8888/> (for 6NET scope)

<http://beaconserver.m6bone.pl/> (M6Bone scope global)

In PSNC, they are using Beacon server to monitor IPv6 multicast network called m6bone. This network was used for IPv6 multicast tests before enabling multicast transmission in 6net core. Now multicast beacon server can be used as monitoring tool during interoperability tests between 6net and other “tunnel based” IPv6 multicast networks.

## Multicast Beacon

[\[Loss\]](#) [\[Delay\]](#) [\[Jitter\]](#) [\[Order\]](#) [\[Duplicate\]](#)      [\[Clients Info\]](#) [\[History\]](#) [\[Mtrace\]](#)

Time: **Thu Dec 05 10:47:21 CET 2002**

Target: **ff0e::8320:1:56465**

Nr of Beacon clients: 7

Page refresh: **60 seconds**


Loss [%]	S0	S1	S2	S3	S4	S5	S6
R0 Hiof	0.0	0.0	2.0	2.0	5.0	0.0	2.0
R1 LIP6	10.0	0.0	2.0	0.0	0.0	0.0	2.0
R2 Renater	10.0	0.0	2.0	0.0	0.0	0.0	2.0
R3 uninett	10.0	5.0	12.0	2.0	2.0	5.0	2.0
R4 SURFnet	17.0	0.0	0.0	2.0	0.0	0.0	2.0
R5 PSNC	10.0	0.0	0.0	2.0	0.0	0.0	2.0
R6 UCL	10.0	0.0	0.0	2.0	0.0	0.0	0.0

---

romradz@man.poznan.pl (new features in the Beacon), PSNC, <http://noc.man.poznan.pl>  
 NLANR/DAST (original version of Beacon), <http://dast.nlanr.net>

### 3.13. Nagios

Nagios is a host and service monitor designed to inform network operators about the network problems. The monitoring daemon runs intermittent checks on hosts and services you specify using external "plugins" which return status information to Nagios. When problems are encountered, the daemon can send

IST-2000-32603	Deliverable 6.3.2. Interim report on the implementation of tools and operational procedures	
----------------	---	--

notifications out to administrative contacts in a variety of different ways (email, instant message, SMS, etc.). Current status information, historical logs, and reports can all be accessed via a web browser.

### **Example of running implementations available in 6net**

NAGIOS software is used at NIIF/HUNGARNET for monitoring networking services. They set up a separate NAGIOS station for monitoring IPv6 network service of HUNGARNET and 6NET also.

NIIF/HUNGARNET: <http://6net.iif.hu/nagios/> (same user ,6core' from tools.6net.org)

### **3.14. Netflow/IPFIX**

Netflow is a flow-based traffic accounting protocol defined by Cisco Systems. It is widely used to support various applications such as usage-based charging, traffic analysis, or capacity planning. The latest version, Netflow v9, will be used as a basis for the IPFIX (IP Flow Information eXport) protocol that is currently being standardized in the IETF. An initial router implementation of IPv6 support for Netflow v9 is now available as an IOS EFT (Early Field Test, [NetFlowIos](#)). A few collectors have added IPv6 support, mostly in experimental status ([NetFlowUtc](#)).

It is being used at 6net by SWITCH, SURFnet, HUNGARNET and DANTE.

### **Example of running implementations available in 6net**

Public available URL where one can check running software, for example for MRTG and RRDBAR:

<http://www.ipv6.man.poznan.pl/cgi-bin/14.cgi?cfg=tunele.cfg>

### **3.15. NetSNMP**

#### **Example of running implementations available in 6net**


NetSNMP (<http://www.netsnmp.org>) version 5.0.6 is used in PSNC in the following areas:

- libnetsnmp library is used in the IPv6 Management Gateway project
- snmpd agent is used in the IPv6 SNMP transport tests

The IPv6 Management Gateway is a project of PSNC (<http://www.ipv6.man.poznan.pl/>), one of its tasks is to translate SNMP messages between IPv4 and IPv6 networks. Libnetsnmp is used to assemble and disassemble SNMP messages. This library is required to properly build and use the IPv6 Management Gateway.

Snmpd is a standalone SNMP agent from the NetSNMP package. One of its features is IPv6 transport support. PSNC uses this feature to test other tools, like the IPv6 Management Gateway or the MUVI MIB Browser. The lack of IPv6 MIBs on the Linux version of NetSNMP unfortunately forbids using it in research areas like network topology discovery.

The NetSNMP package also contains ready tools like snmpget and snmpwalk, which are used in tests.

IST-2000-32603	Deliverable 6.3.2. Interim report on the implementation of tools and operational procedures	
----------------	---	--

### 3.16. PCHAR

Pchar is a tool to characterise the bandwidth, latency, and loss of links along an end-to-end path through the Internet. It is based on the algorithms of the pathchar utility written by Van Jacobson, formerly of Lawrence Berkeley Laboratories.

Pchar measures the characteristics of the network path between two Internet hosts, on IPv4 or IPv6 network. The program measures network throughput and round trip time by sending varying sized UDP packets into the network and waiting for ICMP messages in response. It modulates the IPv4 time to live (TTL) field or the IPv6 hop limit field to get measurements at different distances along a path.

Pchar for each hop in the trip shows the following details:

- the number of partial lost datagrams and percentage of probe packets that were lost during the probes for that hop
- the estimated round trip time from the probing host through the current hop
- estimates of the round trip time and bandwidth for the current hop
- estimate of the average queuing along the path, up to and including the current hop

After the last hop (usually the target host), pchar prints statistics in the entire path, including the path length and path pipe (the latter is an estimate of the delay bandwidth product of the path).

In the other/second mode of operation called trout (short for “tiny traceroute”). Pchar sends packets of random sizes (one packet per hop diameter) along the path to a destination. This mode is extremely fast but no attempt at estimating link properties is made.


#### Example of running implementations available in 6net

In PSNC, Pchar is running on a host called plum.man.poznan.pl and it can also be accessible directly using the following link: <http://plum.man.poznan.pl/cgi-bin/pchar.cgi> . The user-friendly web interface for the Pchar tool is implemented as a Perl script written in PSNC. Their implementation is IPv4 and IPv6 enabled and publicly available through the links mentioned above. They use only basic options for this tool to simplify the user interface. During the testing phase and every day use PSCN have noticed that Pchar can return quite accurate results for the nearest neighbours, but for far-end hosts it can give incorrect results. Generally, Pchar can estimate the correct bandwidth for the near neighbours before it reaches the bottleneck of this link. Unfortunately, it can then propagate any limitations and approximations caused by the link’s bottleneck giving inexact and unreliable results.

An example of results given by our Pchar implementation is presented below:

```
[ plum.man.poznan.pl → ipv6-gw.man.poznan.pl ]
```

```
pchar to 3ffe:8010:a5::2 (3ffe:8010:a5::2) using UDP/IPv6
Using raw socket input
Packet size increments from 52 to 1000 by 32
31 test(s) per repetition
3 repetition(s) per hop
0: 2001:808::2 (2001:808::2)
```

IST-2000-32603	<p style="text-align: center;">Deliverable 6.3.2. Interim report on the implementation of tools and operational procedures</p>	
----------------	--	--

Partial loss: 0 / 90 (0%)  
 Partial char: rtt = 0.867730 ms, (b = 0.000988 ms/B), r2 = 0.763518  
                   stddev rtt = 0.110532, stddev b = 0.000104  
 Partial queueing: avg = 0.000204 ms (206 bytes)  
 Hop char: rtt = 0.867730 ms, bw = 8099.441136 Kbps  
 Hop queueing: avg = 0.000204 ms (206 bytes)  
 1: 2001:808::7 (2001:808::7)  
 Partial loss: 17 / 90 (18%)  
 Partial char: rtt = 1.177978 ms, (b = 0.001347 ms/B), r2 = 0.800236  
                   stddev rtt = 0.138020, stddev b = 0.000140  
 Partial queueing: avg = 0.000123 ms (206 bytes)  
 Hop char: rtt = 0.310248 ms, bw = 22252.042978 Kbps  
 Hop queueing: avg = -0.000081 ms (0 bytes)  
 2: 3ffe:8010:a5::2 (3ffe:8010:a5::2)  
 Path length: 2 hops  
 Path char: rtt = 1.177978 ms r2 = 0.800236  
 Path bottleneck: 8099.441136 Kbps  
 Path pipe: 1192 bytes  
 Path queueing: average = 0.000123 ms (206 bytes)  
 Start time: Mon Jul 14 15:48:24 2003  
 End time: Mon Jul 14 15:49:56 2003

### 3.17. RANCID

RANCID, "Really Awesome New Cisco config Differ", is a tool to automatically retrieve configuration files from a router and store it in a CVS environment. With CVS, changes over time in these configurations can be tracked. There are various frontends to watch these changes, e.g. "cvsweb" or "viewcvs". Rancid is a program written in perl, which uses external programs to connect to a router (telnet, ssh, rsh, expect) and to store the retrieved data (CVS). When these external programs are IPv6-ready, we will show that it is easy to use rancid in an IPv6 environment.


#### Example of running implementations available in 6net

It can be used for router configuration management. It is used in 6Net by 6net NOC and HUNGARNET.

### 3.18. RIPE TT server

RIPE TT server allows statistics to be gathered between any pair of deployed TT servers. The statistics include packet delay and loss, as well as a historical view of observed traceroutes. The system is available as a "black box" shipped from RIPE-NCC. It requires a roof-mounted GPS to be deployed for time synchronisation. Statistics are gathered at the RIPE NCC site and presented for views there by RIPE-NCC TT server owners (once you own a box, you can view any details). There is a purchase fee and maintenance fee – these fees are currently under review and likely to be lowered (purchase is around 3,000 Euros, maintenance is likely to fall to 1,000 Euros p.a.).



IST-2000-32603	Deliverable 6.3.2. Interim report on the implementation of tools and operational procedures	
----------------	---	--

IPv6 functionality was added to the existing RIPE NCC TT server after discussion between 6NET and the RIPE NCC which started in Q1 2002. It was decided that RIPE NCC rather than 6NET would develop the new IPv6 functionality so that expertise could be gathered and maintained in RIPE NCC.

6NET project is running live TT server boxes on many project partner sites. These tools are being used actively for monitoring the backbone performance and routing paths.

There are at least 14 IPv6-enabled RIPE NCC TT servers as of July 2003, of which six are located at 6NET project partner premises. They are:

- tt13: Surfnet, Utrecht
- tt42: NTUA, Greece
- tt73: University of Vienna, Austria
- tt76: University of Southampton, UK
- tt77: DFN, Germany
- tt85: SWITCH, Switzerland

Other NREN sites include HEAnet (Ireland) and FCCN (Portugal).

All new TT servers shipping now have IPv6 support in them.

There is ongoing work in addressing additional IPv6 issues, including IPv6 NTP. The progress of the TT server porting will be tracked in 6NET, with the tool used by partners for inter-site testing.

6NET will also seek to find international (e.g. US and Japan) sites that may host TT server systems for network performance analysis on international links.

### **3.19. Westhawk SNMP Stack**

The Westhawk SNMP Stack version 4.13 is used in the Multicast Visualisation Tool (MUVI) project (<http://muvi.man.poznan.pl>). It uses the SNMP protocol to examine router statuses and retrieve information about multicast traffic. Although MUVI operates on the IPv4 routers (because the appropriate multicast MIBs for IPv6 are not defined yet), it can communicate with the IPv6 routers. There is a simple MIB Browser integrated with MUVI that allows to send requests either to the IPv4 or IPv6 routers. The results of an example GET\_NEXT request sent to the one of our IPv6 SNMP agents are visible on the Fig.4. MUVI uses the SNMP protocol either in version 1 or 2, depending on the configuration. In version 2 the GET\_BULK request is used to obtain values of MIB tables. The Westhawk SNMP stack handle it quite well. Unfortunately a problem was encountered for the GET\_BULK request when the number of maximal repetitions is quite big (e.g. 50). According to the reported exception the received packet length differs from the received bytes.

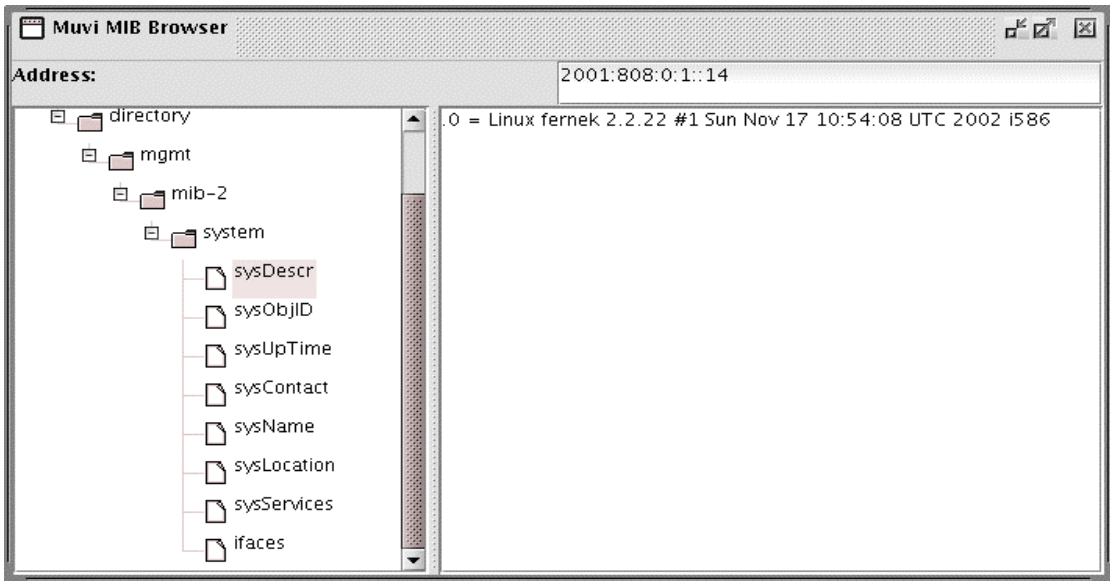


Fig. 4 The result of a GET\_NEXT request for an IPv6 router using the MUVI MIB Browser

### 3.20. Tools used by 6net NOC

#### 3.20.1. Infovista

The IP performance of the 6NET Core Network is monitored using InfoVista, a commercial network monitoring application, which is configured to gather information from all the relevant routers at regular intervals using SNMP GET-requests. In order to avoid problems with 32-bit SNMP counters wrapping during the polling cycle on high speed links, 64-bit SNMP counters are used instead. The routers are all monitored for the same information, which enables the 6NET NOC to provide uniform reporting across the entire 6NET network. The traffic measurement is based on samples of the MIB variables ifHCInOctets and ifHCOutOctets, which give traffic at the physical or logical interface level. The 6NET links are mainly POS (Packet Over Sonet) but there is still some ATM VC (Virtual Channel). Infovista generates data based on a 15 minutes polling interval.

#### 3.20.2. Intermapper

Intermapper network monitoring and alerting tool provides a real time view of traffic flows through and between critical networks routers and links. It also provides a viewing of the state of 6net network. It also have utilization statistics which show up traffic, errors and outage information which help to troubleshooting the problems that may occur.

The network map is displayed in web page where you can find different information about it. Below it is shown a snapshot of the current state of the 6net network.

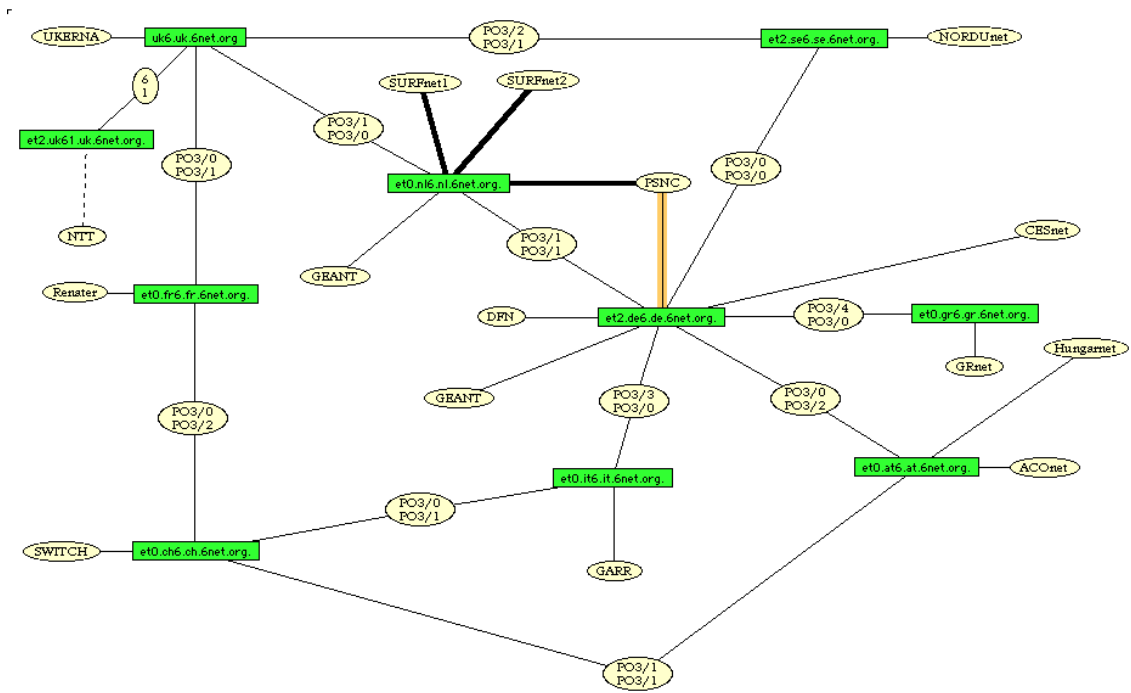



Fig. 5

The following table presents a summary of the tools that are being used by the 6net NOC.

IST-2000-32603	Deliverable 6.3.2. Interim report on the implementation of tools and operational procedures	
----------------	---	--

Tool	Monitor	Protocol	Frequency	Alert
<b>In-House – Network Monitor</b>	<input type="checkbox"/> Physical Link on Backbone Circuits	SNMP	<input type="checkbox"/> Every 5 minutes (an outage of more than 10 minutes is detected)	<input type="checkbox"/> Email (describing the alarm) <input type="checkbox"/> Pager (describing the alarm)
<b>Infovista</b>	<input type="checkbox"/> Traffic on links.	SNMP	<input type="checkbox"/> Poll every 5 minutes.	<input type="checkbox"/> None
<b>Rancid</b>	<input type="checkbox"/> Configuration changes on the routers.	SSH	<input type="checkbox"/> Everyday.	<input type="checkbox"/> Email (indicating the changes)
<b>In-House – Syslog</b>	<input type="checkbox"/> Syslog messages	Syslog	<input type="checkbox"/> Received in real-time on the server but processes and archived on an everyday basis.	<input type="checkbox"/> Email (giving a summary of the syslog messages which have a severity level of error and above)
<b>Intermapper</b>	<input type="checkbox"/> Visual Check		<input type="checkbox"/>	<input type="checkbox"/>

### 3.21. Summary

D6.3.2. describes and explains tools which are being used by 6net partners. All of them are included in D6.2.3. Interim report on development and test. This document covers in detail how NREN have improved or even develop each tool. Around 65% of the tools presented in D6.2.3. are being used in NREN networks. All of them have been tested before starting to use.

Managing and monitoring is a critical part in every network based in IPv4 or in IPv6. Standards for MIBs and its transport protocol SNMP for IPv6 are still under development. The continuous work on that will give several improvements in short-term to the management of IPv6 networks.


## 4 OPERATIONAL PROCEDURES USED IN 6NET

### 4.1. Operational procedures by 6net NOC

#### 4.1.1. Introduction

This part describes the management of the 6net network done mainly by 6net NOC and its responsibilities and tasks. It summarises Deliverable 1.2. Operational procedures to be followed by 6net NOC, which was submitted last year but still is up-to date regarding operational procedures.

#### 4.1.2. 6net Management

IST-2000-32603	Deliverable 6.3.2. Interim report on the implementation of tools and operational procedures	
----------------	---	--

The 6NET network is considered to consist of three management areas, which define different domains of responsibility and control:

1. 6NET core routers are co-located to the GÉANT PoPs and are under the responsibility and control of the 6NET NOC with support of the NCC (Network Co-ordination Centre).
2. 6NET access routers, directly connected to the 6NET core routers, are under the control of the NRENs with support for the NCC.
3. The user routers, connected to the access router, are under control of the NRENs and/or Universities. This management hierarchy has been defined to allow the NRENs and end user to gather their own experiences by managing and controlling their part of the IPv6 network themselves. In the following paragraph the 6NET core infrastructure is described in short which is operated and managed by the 6NET NOC.

#### 4.1.3. 6net core infrastructure

6NET core network consists of a ring of native/dedicated STM-1 connections provided by COLT between the core routers UK, FR, CH, IT, DE and NL. In addition to the ring configuration the SE PoP (providing connectivity to the Nordic countries Norway, Finland and Sweden via NORDUnet) is connected to UK and DE supplied by Telia and AT is connected to CH and DE provided by T-System circuits. GR is connected to DE via L2 tunnelling using the GÉANT infrastructure.

Each 6NET core PoP is equipped with Cisco 12404. Each of them contains a 16 port STM-1 Engine-3 (or new name ISE) interface card. Each router have: dual AC power supplies, one GSR card with a Fast Ethernet and a Serial Port interface for management purposes, an integrated switch and alarm engine. In the Netherlands an additional 3 port GE card is provided, which is used for resilient local-loop with different paths. The Cisco router in Sweden is equipped with an additional STM-16 card for local-loop purposes.

For the purpose of management and monitoring, the 6NET core routers are connected with the GÉANT network to allow:


- Out of band management using the console port on 6NET core router connected to the GÉANT terminal server.
- IPv4 telnet access to the management Fast Ethernet port of the router processor via the GÉANT network.

#### 4.1.3. 6net NOC

The GÉANT Network Management Service is provided by DANTE. 6NET NOC has been defined to be a part of the GÉANT Network Management Service, but to treat the 6NET network separated from there is a dedicated group of people dealing with aspects of the 6NET core network.

In general the 6NET NOC provides the day to day operational management, covering the central fault reporting point for the Services, issuing trouble tickets, the management of the Services, the management of gateways to external networks, and planning for changes to the network configuration. It has responsibility for monitoring and reporting on the performance of the network and it collects data for the monthly reports on the Service, which are primarily intended for the NRENs.

The 6NET NOC is especially responsible for all problems related to IPv6 protocol while operational problems (hardware failures, connectivity problems) will be solved in interaction with other entities like Carriers, Cisco TAC, GÉANT NOC and DANTE as network management co-ordination centre for the GÉANT network

IST-2000-32603	Deliverable 6.3.2. Interim report on the implementation of tools and operational procedures	
----------------	---	--

## ***4.2. Operational procedures followed by 6net partners***

### *4.2.1. Introduction*

This part summarises the procedures followed by 6net partners to connect to 6net core. See Deliverable 1.3 Operational procedures to be followed by organisations connected to 6net for more details. D1.3 was submitted in June 2002, but it still contains up-to-date information.

### *4.2.2. Access circuits*

Access circuits for the connection of the NREN to the 6NET core were ordered by the NREN or via DANTE. The process of obtaining a new or upgraded Access Port involved discussions with WP1 by the 6NET partner, and finally approval by the 6NET Project Management Committee.

The access circuits for Janet, DFN, Aconet, RENATER, GARR, SWITCH, NORDUnet and SURFnet to get connected to 6net core were done via local-loops in each country in the first part of the project. Subsequently, Cesnet was connected to DE and HUNGARNET to AT via dark fiber provided by T-Systems. NTT, Asian ISP was directly connected to 6net core in UK via COLT provider.

## ***4.3. Operational procedures during test periods for 6net NOC and 6net participants***

The complete procedures for approval and scheduling test in 6net which involves configuration and deployment of the 6net routers are described in detail in D1.4. Updated. This part explains the differences of responsibility tasks during test period.


6NET network itself is not a production network, but an IPv6 test network. This means that service disruption and degradation is possible. But the participants should know the tests that might cause problems.

6NET NOC keeps the baseline configuration of the 6NET core routers. They are responsible of the configuration work and they always know which configuration should be used for operating the router (baseline configuration). 6NET NOC is responsible to configure the first state of the router needed for the test. During the running of the test, any needed configuration change would be done by the responsible of the test. For that, temporal RW access must be enable for the responsible of the test to be able to change the configuration of the routers for test purposes. In case of any IOS upgrade/downgrade, this should be done by 6NET NOC.

The configuration changes during the running of the test must be left in the core router and the 6NET NOC will be responsible to roll back to last configuration in case needed and RW access for testers will be removed.

A special Trouble Ticket will be raised at the beginning of the running to inform about the core routers affected during the test. The life of this ticket will last until the end of the running of the test and it will be closed after rolling back to the last configuration.

As testers will be able to change the router configuration during the running of the test, no Trouble Ticket would be raise in the event of any outage in the affected routers during the tests since 6NOC would not be

IST-2000-32603	Deliverable 6.3.2. Interim report on the implementation of tools and operational procedures	
----------------	---	--

able to keep track of the problems. 6NOC is not responsible of debugging problems that may occur in the affected routers during the test.