



IST-2000-32603	Deliverable 6.3.3. Final report on the implementation of tools and operational procedures	
----------------	--	--

Project Number:	IST-2001-32603
Project Title:	6NET
CEC Deliverable Number:	32603/ DANTE/DS/D6.3.2/A6.2
Title:	Final report on IPv6 management and monitoring architecture design, tools, and operational procedures. Recommendations.
Work Package:	WP6
Type of deliverable*:	R
Deliverable security class**:	PU
Editors:	Jérôme Durand
Contributors:	Isabelle Astic, Frank Aune, Wojbor Bogacki, Arnaud Bruzy, Tim Chown, Lorenzo Colitti, Lucas Dolata, Jérôme Durand, Robert Evans, Olivier Festor, Bartosz Gajda, Martin Kaminski, Ioannis Kappas, Radoslaw Krzywania, Olav Kvittem, Roman Lapacz, Simon Leinen, Janos Mohacsi, Wiktor Procyk, Duncan Rogerson, Tomasz Szewczyk, Robert Szuman, Christian Schild, Andre Stolze, Tina Strauf, Bernard Tuy


<p>Abstract:</p> <p>This document gives a detailed overview of</p> <ul style="list-style-type: none"> - Implementation of management, measurement and monitoring tools in 6NET - Operational procedures in 6net - Recommendations to operate/manage an IPv6 network from the experience gained.

<p>Keywords:</p> <p>IPv6, network management, monitoring tools, operational procedures.</p>
--


IST-2000-32603	Deliverable 6.3.3. Final report on the implementation of tools and operational procedures	
----------------	--	--

Final report on IPv6 management and monitoring architecture design, tools, and operational procedures. Recommendations

1.	Introduction.....	4
2.	Relation with other deliverables	5
3.	Management protocols and MIBs in the standardization process	6
3.1.	SNMP for IPv6	6
3.2.	MIBs	6
3.2.1.	The Textual Conventions.....	6
3.2.2.	The Evolution of the MIBs	6
3.3.	The Other Standards	7
3.4.	Flow monitoring (IPFIX, Netflow...)..	8
3.5.	Management of IPv6 new protocols and transition mechanisms	8
3.6.	The work to be done	8
4.	Network Management architecture.....	9
4.1.	Conceptual phase	9
4.1.1.	Network segments and boundaries	9
4.1.2.	Information flows	9
4.1.3.	Security aspects	9
4.1.4.	Maintenance.....	10
4.1.5.	Management information accessible to users	10
4.1.6.	Transition mechanisms and services	11
4.2.	Implementation phase - Management tools set	11
5.	Management tools deployed in 6NET	12
5.1.	Management tools for core networks (WAN)	12
5.1.1.	AS-path-tree.....	12
5.1.2.	6net looking glass	14
5.1.3.	IPFlow.....	14
5.1.4.	IPv6 support for Netflow v9 in IOS	14
5.1.5.	Mping.....	14
5.1.6.	RIPE TT server	15
5.1.7.	Cricket.....	16
5.1.8.	MRTG.....	16
5.2.	Management tools for end-sites (LAN).....	17
5.2.1.	Argus.....	17
5.2.2.	Ethereal	17
5.2.3.	Multicast Beacon	18
5.2.4.	PCHAR.....	18
5.2.5.	Iperf.....	19
5.2.6.	ntop	19
5.3.	Tools for all network parts.....	20

IST-2000-32603	<p style="text-align: center;">Deliverable 6.3.3.</p> <p style="text-align: center;">Final report on the implementation of tools and operational procedures</p>	
----------------	---	--

- 5.3.1. IPv6 management gateway (old name: SNMP Transition tool).....20
- 5.3.2. Nagios.....20
- 5.3.3. RANCID.....21
- 6. Recommendations for network administrators.....22
 - 6.1. Network management architecture.....22
 - 6.2. End-site networks.....22
 - 6.3. Core networks.....22
- 7. Tools used by 6net NOC.....24
 - 7.1. Infovista.....24
 - 7.2. Intermapper.....24
 - 7.3. Summary.....25
- 8. Operational procedures used in 6NET.....27
 - 8.1. Introduction.....27
 - 8.2. Operational procedures followed by the 6net NOC.....27
 - 8.3. Operational procedures followed by 6NET partners.....27
 - 8.3.1. Introduction.....28
 - 8.3.2. Access circuits.....28
 - 8.4. Operational procedures during test periods for 6NET NOC and 6net participants.....28
- 9. Conclusion.....29
- 10. References.....30

IST-2000-32603	Deliverable 6.3.3. Final report on the implementation of tools and operational procedures	
----------------	--	--

1. Introduction


Network management and monitoring is a critical part for operating any production quality network, whatever the nature and size of the network. Network management is one of the essential building blocks of the all the IPv6 networks in general, especially in the Internet service provider area. If IPv6 backbone networks do not have an improved or not even the same standard of management and monitoring as legacy IPv4 networks, the IPv4 provider will be unwilling to migrate or simply to deploy IPv6. To achieve the goal of providing the same or better network management for IPv6 networks the task for the 6NET management area is not only to check the protocols, tools and applications available to achieve all the management and monitoring functions, but to inventory every missing part too. It then becomes possible to effectively work on progressing standards in the relevant bodies and with manufacturers to help them build their roadmaps for providing customers with what they need to manage and monitor production quality IPv6 networks.

The network management activity covers many areas (also called network segments) of the network. Usual classification distinguishes Local area Networks (LAN) from Metropolitan (MAN) and Wide Area Networks (WAN). In this regard sets of very different functions have to be provided to the manager, from straightforward monitoring of link status, to traffic statistics gathering and analysis. These sets could roughly be classified in two categories: those needed for day to day network control operations and those dedicated to network behaviour analysis. The latter allows the manager to optimise the network or parts of it and to schedule the necessary evolutions.

This document brings together all the network monitoring and management work conducted by WP6 into a single document. The document is designed as a "cookbook", summarising the issues required for managing and monitoring an IPv6 network, and suggests appropriate tools that can be used to support the network management and monitoring functions. As a result this deliverable can be both a useful guide to designers of new IPv6 networks, and a reference for more experienced network managers.

Most of the 6NET WP6 partners have experience in managing IPv4 production networks. The WP6 activities and results could draw from this experience and greatly profit from it, especially for this cookbook. It is quite obvious that the management of an IP network is not that different from one version of the protocol to another one. Nevertheless we are still in a period of time where IETF standards for IPv6 management are not completed and MIBs for IPv6 equipment are still largely implemented by vendors with their own proprietary standards.

This is the final version of the cookbook. It benefits from the 2.5 years of experience from the 6NET partners on IPv6 network management but due to the fact that not all standards, MIBs and protocols have yet been finalized and uniformly implemented, there is still room for additional work.


IST-2000-32603	Deliverable 6.3.3. Final report on the implementation of tools and operational procedures	
----------------	--	--

2. Relation with other deliverables

This deliverable is the third version of the D6.3 series about management architecture, implementation of monitoring tools and operational procedures. The D6.3.1 deliverable [D6.3.1], written at the beginning of the 6NET project at a time when few management tools were available, focuses on the principles of network management and the management architecture. These principles were applied to the 6NET network itself to check their correctness. Deliverable D6.3.2 [D6.3.2], written when a first set of more sophisticated tools capable of managing IPv6 networks became available, deals with the tools deployed by the different partners for managing their infrastructure. This third version updates the information available in D6.3.1 about the current status of the standardization regarding IPv6 management; and also updates and classifies the tools deployed by the different partners. This deliverable therefore presents the latest recommendations for the management architecture and the monitoring tools to be deployed in different parts of the network, taking into account the experience gained in this project.

D6.3.3 is related to ‘D6.2.4. Final report on development and test’ [D6.2.4] that describes the development and test of tools performed by 6NET partners. Deliverable 6.3.3 only describes the tools that have really been used and explains how 6NET partners are using them. It is not an exhaustive list of all the available tools and their test report. A more complete list can be found in deliverable D6.2.4.

Parts 7 and 8 ‘Operational procedures used in 6NET’ summarizes the procedures to be followed by 6net NOC that are described in detail in D1.2 [D1.2] and D1.3. [D1.3] already submitted to the EC.

IST-2000-32603	Deliverable 6.3.3. Final report on the implementation of tools and operational procedures	
----------------	--	--

3. Management protocols and MIBs in the standardization process

As the main management standard used for IPv4 networks is SNMP (Simple Network Management Protocol), [RFC3416], it was an obvious goal to pursue to also make SNMP management available for and via IPv6. This section focuses on SNMP for IPv6, the corresponding MIBs (Management Information Base) and standardisation process and also gives a brief history on the evolution of the SNMP protocol in general.

3.1. *SNMP for IPv6*

Today many network equipments (6WIND, CISCO, HITACHI, JUNIPER...) support SNMP over IPv6 and can be monitored in an IPv6-only environment. One could note that equipments not supporting SNMP over IPv6 can be managed over IPv4 as most IPv6 networks are running dual stack.

The number of SNMP applications able to poll remote SNMP agents over IPv6 remains low. Most of the tools today use the netSNMP open source SNMP library. Recently however some integrated management platforms (HP Openview, Ciscoworks 2000) have also become or are in the process of becoming IPv6 capable and serious progress has been made towards the support of SNMP functions, even if the transport remains IPv4 in most cases.

3.2. *MIBs*

There is a large number of MIBs to check, to verify if they could be used to manage IPv6 networks. Some will have to be further developed to support it.


3.2.1. *The Textual Conventions*

In 1998, a textual convention was defined for IPv6 addresses only. But this implies the partition of IPv4 and IPv6 management information bases, that is to double the effort to get all MIBs ready for both versions of IP. Fortunately another approach is under way since then based on a “unified MIB convention” where the same MIB can handle both IPv4 and IPv6. To be able to achieve this, the address data structure had to be changed. But it is worth the effort.

3.2.2. *The Evolution of the MIBs*

In 1996, the MIB II was updated in order to manage IPv4 networks. It was defined by the RFC 2011 (IP MIB) [RFC2011], RFC 2012 (TCP MIB) [RFC2012], RFC 2013 (UDP MIB) [RFC2013] and RFC 2096 (IP forwarding MIB) [RFC2096]. Three groups were defined: ip, tcp and udp. Each group contains simple objects and tables (see figure 1).

In 2002, the approach, illustrated in Figure 1, unified all the tables. The RFC 2851 [RFC2851] (now updated with RFC 3291 [RFC3291]) describes textual conventions to represent both versions

IST-2000-32603	<p style="text-align: center;">Deliverable 6.3.3.</p> <p style="text-align: center;">Final report on the implementation of tools and operational procedures</p>	
----------------	---	--

of IP in MIBs. The existing MIBs (RFC 2011, 2012, 2013 and 2096) were updated following this new textual convention. They were recently accepted as proposed standards.

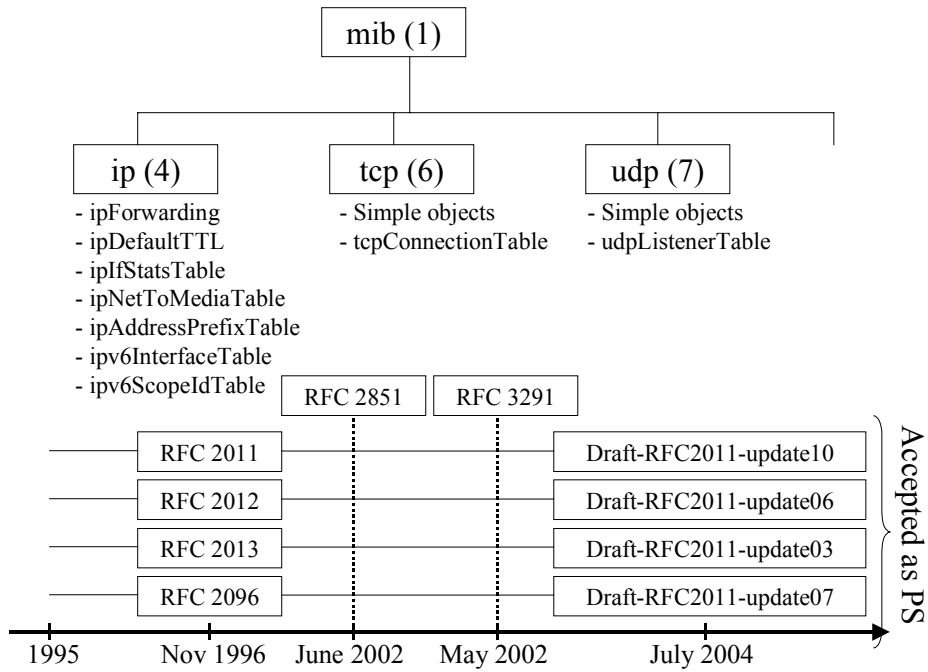


Figure 1 : The unified MIB II
(Numbers in parenthesis are oids)


3.3. The Other Standards

The SNMP standard was mainly used for the monitoring and fault management. Some other standards were defined to satisfy the need of configuration and AAA (Authentication, Authorization and Accounting) [RFC3539]. Those standards are COPS [RFC2748], WBEM (Web-Based Enterprise Manager) [WBEM] for the configuration point of view, RADIUS [RFC3162] and Kerberos V [RFC1510] for the AAA.

COPS and WBEM are available for IPv6 networks. The protocols themselves and their data models or policies are already defined to be able to manage such networks. But it seems that no implementation of those standards exist.

RADIUS was defined upon IPv6 in 2001 (RFC 3162). But as experience has shown that it cannot be used in large scale network, a new protocol was defined by the IETF called DIAMETER. That could explain that no implementation of RADIUS upon IPv6 exists.

DIAMETER has been published as RFC 3588 [RFC3588]. An implementation already exists, to SUN Microsystems, based on the 7th version of the draft. A new one is under development within the IST Moby Dick project, defined upon the 10th version of the draft.

IST-2000-32603	Deliverable 6.3.3. Final report on the implementation of tools and operational procedures	
----------------	--	--

KERBEROS V was partly implemented upon IPv6 since its 1.2 version, by the Massachusetts Institute of Technology.

3.4. Flow monitoring (IPFIX, Netflow...)

Netflow is a flow-based traffic accounting protocol defined by Cisco Systems. It is widely used to support various applications such as usage-based billing, traffic analysis, or capacity planning. The latest version, Netflow v9, is used as a basis for the IPFIX (IP Flow Information eXport) protocol that is currently being standardized in the IETF. Only version 9 of Netflow is designed to export IPv6 flows towards the Netflow collector.

IPv6 support in Netflow v9 is now available in 12.3T CISCO IOS train. But the transport used for the data export is still over IPv4 only. On GSR series Netflow v9 is implemented but is not yet able to export IPv6 flows.

Netflow Collectors are also available for IPv6 either from Cisco (NFCv5.0) or from academic organizations (UTC, France). See section 5.1.3 for further information.

3.5. Management of IPv6 new protocols and transition mechanisms

IPv6 is a new protocol and with it many services are being deployed. The network management entity has to be aware of the impact on network management when deploying these new services. For instance, transition mechanisms between IPv4 and IPv6 should be considered in the management infrastructure. Some work has already been done regarding the management of the IPv6/IPv4 coexistence protocols. A draft describes a MIB for tunnel management : draft-ietf-ipv6-inet-tunnel-mib-02 [TUNNELMIB].


The deliverable D6.2.2v2 [D6.2.2] also gives some recommendations for secured management of transition mechanisms but targets mostly security aspects of the different transition protocols rather than the management techniques.

Nevertheless, it should be noted that in general, there is little standardization effort made for the management of new services coming along with IPv6, as most of the work is concentrated on having the same level of management for IPv6 as for IPv4.

3.6. The work to be done

As we could see, for the short-term, the main problem is to get similar management standards for IPv6 than those for IPv4.

The implementation of the unified MIBs for TCP, UDP and BGP becomes more and more urgent. Today many manufacturers implement private MIBs based on RFC 2465 [RFC2465] or the drafts updating RFCs 2011, 2012 and 2013. The transport of SNMP over IPv6 is no longer a problem as most of the network equipment support this feature today.

IST-2000-32603	Deliverable 6.3.3. Final report on the implementation of tools and operational procedures	
----------------	--	--

4. Network Management architecture

4.1. Conceptual phase

4.1.1. Network segments and boundaries

Before deploying a new network –or part of- it is wise to think how to structure the network in order to facilitate the management. For instance in the 6net project, three network segments have been defined: a core network, access networks and user/site networks. Once the management boundaries are clearly defined, other elements can be added like VLANs, DMZ, intranets, ...

The other goal to achieve during this preliminary step is to clarify the domains responsibilities for every entity involved in the network management. For instance, in the example of 6NET above, the core network was under 6NET NOC responsibility, the access networks under the NREN responsibility and the user/site network under the responsibility of the network administrator of the site.


4.1.2. Information flows

After the preliminary planning stages it is useful to consider the information flows between the entities responsible for each domain to get a clear understanding on what information is needed to manage the domain, who is supposed to provide this information and who should receive it. From this information chart, operational procedures can be designed and written down (as an example, the reader can refer to deliverable D6.1.2 [D6.1.2], where this “theoretical exercise” has been applied to the 6NET network management). Looking back after two years it can be stated that the process was useful and efficient. For months nobody has complained for about the way the network – mainly the core network – is managed. Additionally, operational procedures for implementing test phases for experiments and tests have been identified and implemented. This was not easy since the goal was to accommodate requirements both for production-like traffic and test constraints.

4.1.3. Security aspects

Finally, one of the most complex things to decide is security of management information and procedures. There are several things to take into account in this area:

- The security of the management information itself and the priority of its traffic. The management information should stay under the network administrator’s control. Part of this information is usually not publicly available, it is reserved for administrators to control the normal network behaviour or to gather statistics data on the traffic flows... When there is congestion or an overload in (part of) the network, then it is efficient to have predefined the class of traffic the management information belongs to.

IST-2000-32603	Deliverable 6.3.3. Final report on the implementation of tools and operational procedures	
----------------	--	--

It is a good way to insure the management information remains available to the administrator when the traffic is slowed down for whatever reason.

- The security of the operational procedures.
Operational procedures are defined so the network management information and the access to the network resources are accessible almost at anytime. For general outage there is no real solution but these situations are becoming rare at least in developed countries. The operational procedures should be designed to take into account unusual events so the administrator knows in advance what he has to do (urgent actions to take, who to warn, ...). These procedures are usually only known by a restricted group of people and are written down.
- The security of the network equipments and their access.
Access to the network equipments is obviously not granted to anyone. Security measures have to be implemented adequately. Moreover, a backup way (or ways) to access the network equipments in case of outage have to be predefined (for instance the IPv4 connectivity can be used to access dual stacked equipments when IPv6 routing is broken). Usually, for critical resources, phones lines –or ISDN- allow access to the equipment in case of outage. These accesses are part of the network management; they should be considered during the conceptual phase of building the network and then be checked on a regular basis when the network has been put into operation.


4.1.4. Maintenance

Maintenance procedures and their reserved time slots should be defined in advance so a wide set of people knows about them. Regular maintenance is usually scheduled out of working hours, to avoid disturbing the production traffic. Other maintenance procedures are for emergency cases (outages, ...). They have to be foreseen in the operational procedures.

4.1.5. Management information accessible to users

Various experiences have shown that it is very important to provide the users of the network with some management information. It is efficient since the user (including an administrator from another network segment/domain) can quickly understand where a problem comes from and try to get in touch with the appropriate person or entity, instead of asking people that cannot help in solving a problem and wasting time unnecessarily.

For this use, tools to provide management information have to be chosen and a relevant subset of the information should be selected. To this respect, in the 6Net project a set of looking glasses, weather maps etc. have been implemented. They allow any user to understand with a simple click how the network performs and in case of problems in what part of the network the problem occurred. Obviously these facilities are not restricted to large networks, but can be applied to any LAN (Local Area Network) with real benefits. The only thing that changes in this case, is the nature of management information the users can obtain.


IST-2000-32603	Deliverable 6.3.3. Final report on the implementation of tools and operational procedures	
----------------	--	--

4.1.6. Transition mechanisms and services

Most of the above applies with no major differences to both IPv4 or IPv6 networks. What is specific to IPv6 are the so-called transition mechanisms. In fact they are means to provide internetworking between IPv4 and IPv6 resources. These mechanisms can be seen as services offered to the users. They need the administrator to pay attention to them depending on how they are implemented, managed and the secured. For instance, designing a 6to4 service requires decisions on which users should be allowed to use the service, where the 6to4 gateways are installed, whether there are any 6to4 relay available in the network or if other network's relays are allowed, ... At the present time, it is not yet completely clear how to manage such services and what information is relevant for the administrator. Since most of these mechanisms are based upon encapsulation techniques, the security issues are those associated with these kinds of well known mechanisms in IPv4. More information is available in 6Net deliverable D6.2.2v2 [D6.2.2] on operational procedures for secured management with transition mechanisms.

4.2. Implementation phase - Management tools set

Once all the steps of the conceptual phase have been clearly understood and executed it is time to select the appropriate tools to gather the information needed as defined during the planning. To this respect the reader can refer to D6.2.4 [D6.2.4] where the management and monitoring tools we gained experience with are documented. A subset of those tools used for the management in the different segments of the 6Net network, is described in the following section.

IST-2000-32603	Deliverable 6.3.3. Final report on the implementation of tools and operational procedures	
----------------	--	--

5. Management tools deployed in 6NET

There are many tools to manage and monitor IPv6 networks. The management needs are not the same in the different parts of the network as discussed in the previous section. For this reason this part of the document classifies the management tools according to the part of the network they best apply to (LAN or WAN).

In this section the following tools for wide area networks are presented:

- AS-path-tree (<http://carmen.ipv6.tilab.com/ipv6/tools/ASpath-tree/>)
- 6Net looking glass (<http://tools.6net.org> , <http://w6.loria.fr>)
- IPflow (<http://www.rrt.cr-picardie.fr/~fillot/nf6/>)
- IPv6 support for netflow v9 in IOS (<http://www.cisco.com/go/netflow/>)
- Mping (<http://mping.uninett.no>)
- RIPE TT server (<http://www.ripe.net/ttm/ttm-ipv6.html>)
- Cricket (<http://cricket.sourceforge.net/>)
- MRTG (<http://people.ee.ethz.ch/~oetiker/webtools/mrtg/>)

For local area networks the following tools are detailed::

- Argus (<http://argus.tcp4me.com>)
- Ethereal (<http://www.ethereal.com>)
- Multicast Beacon (<http://dast.nlanr.net/Projects/Beacon/> ; <http://noc.man.poznan.pl/noc/strony/aplikacje.html>)
- Pchar (<http://www.employees.org/~bmah/Software/pchar>)
- Iperf (<http://dast.nlanr.net>)
- Ntop (<http://www.ntop.org>)

At the end examples are presented of tools that can be deployed in any part of the network:


- IPv6 management gateway (<http://www.ipv6.man.poznan.pl>)
- Nagios (<http://www.nagios.org>)
- Rancid (<http://www.shrubbery.net/rancid/>)

The reader can refer to 6Net deliverable D6.2.4 [D6.2.4] for detailed test results for all the management tools known by the 6Net project partners.

5.1. Management tools for core networks (WAN)

5.1.1. 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 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 features useful within any operational IPv6 network, which makes use of BGP.

IST-2000-32603	Deliverable 6.3.3. Final report on the implementation of tools and operational procedures	
----------------	--	--

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

ASpath-tree is not a tool that monitors BGP peerings in the way that it does not send any kind of notification when peerings go down or up or when the number of routes received from a given peering is critical (too low or too large). Therefore it cannot be used for continuous operational monitoring of the routing in the network.

On the other hand, ASpath-tree is very useful to check that the routing table of the network matches the routing policy. It helps a lot 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 of IPv6 deployment, while more and more sites are moving to IPv6, network administrators have to check their routing policy frequently to be sure it 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 (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.)

IST-2000-32603	Deliverable 6.3.3. Final report on the implementation of tools and operational procedures	
----------------	--	--

5.1.2. 6net looking glass

A looking glass is available for the 6net core network. In essence a looking glass is a CGI script which allows to connect to a remote router from a simple web page, to run some predefined 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/>

5.1.3. 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 as well as a graphical display of flow statistics. The author is Christophe Fillot.

The following partners have deployed IPFlow :

SURFnet

HUNGARNET

5.1.4. 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 being used by SWITCH, RENATER, SURFnet and DANTE.

5.1.5. Mping

Mping collects ping statistics for multiple hosts at the same time. Performing an “mping” on all the hosts being listed by 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-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

IST-2000-32603	Deliverable 6.3.3. Final report on the implementation of tools and operational procedures	
----------------	--	--

the collected data as median, cube-sum, standard deviation or 10/50/90-percentile at the user's request.

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

- Mping by default does not send more than 10 ICMP packets per second, thus measured data is independent from the time of measuring.
- Mping does not send all ICMP-packets to one 'Gateway' at the same time, rather Mping tries to spread them out in a Round-Robin fashion, thus avoiding temporary network characteristics.
- Mping starts the pingsweeps at asynchronous intervals. A Poisson-distribution is used, 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 which are measured. 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 a running implementation available in 6NET :

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

5.1.6. RIPE TT server


RIPE TT servers allow 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 a maintenance fee – these fees are currently under review and likely to be lowered (purchase at the moment is around 3,000 Euros, maintenance is likely to fall to 1,000 Euros p.a.).

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.

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

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

- tt13: Surfnet, Utrecht
- tt42: NTUA, Greece
- tt73: University of Vienna, Austria

IST-2000-32603	Deliverable 6.3.3. Final report on the implementation of tools and operational procedures	
----------------	--	--

- 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 is followed 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.

5.1.7. Cricket

Cricket is a high performance, extremely flexible system for monitoring trends in time-series data. Cricket was expressly developed to help network managers visualize and understand the traffic on their networks, but it can be used for 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)

5.1.8. 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 the traffic on the links. MRTG is widely used, currently mostly over IPv4. IPv6 support has been tested on Linux only, but should work on other operating systems such as FreeBSD.

Example of running implementations available in 6NET:

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

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

PSNC : <http://www.ipv6.man.poznan.pl/>

IST-2000-32603	Deliverable 6.3.3. Final report on the implementation of tools and operational procedures	
----------------	--	--

5.2. Management tools for end-sites (LAN)

5.2.1. Argus

Argus is a system and network monitoring application, which includes IPv6 support since version 3.2. It will monitor nearly anything it is asked 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 fulfil 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 the Perl module 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 :

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

5.2.2. 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 extension protocols that are used or developed within 6NET could be supported with additional or improved dissectors if required.

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

IST-2000-32603	Deliverable 6.3.3. Final report on the implementation of tools and operational procedures	
----------------	--	--

5.2.3. Multicast Beacon

Multicast Beacon is the application for monitoring the parameters of multicast traffic. These parameters are: packet loss, delay, jitter, duplicate or 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. This 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

The beacon can be useful for multicast traffic monitoring in IPv6 networks. In PSNC a beacon server has been deployed to monitor an IPv6 multicast network called m6bone (<http://www.m6bone.net>). This network was used for IPv6 multicast tests before enabling multicast transmission in the 6NET core. Now the multicast beacon server can be used as monitoring tool during interoperability tests between 6NET and other “tunnel based” IPv6 multicast networks.

Example of running implementations available in 6net :

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

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

5.2.4. PCHAR

Pchar is a tool to characterize 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 an IPv4 or IPv6 network. The program measures network throughput and round trip time by sending UDP packets of varying size 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 presents the following details for each hop in the trip:

- the number of partial or 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 i6NET :

IST-2000-32603	Deliverable 6.3.3. Final report on the implementation of tools and operational procedures	
----------------	--	--

In PSNC, Pchar is running on a host called plum.man.poznan.pl. It can be accessed 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. Only basic options for this tool are used to simplify the user interface. During the testing phase and every day use PSNC 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.

5.2.5. *Iperf*

As Pchar described above, Iperf can be used to check the bandwidth available on an end-to-end path of the IPv6 Internet, as well as packet loss and latency. As the throughput that can be measured with Iperf is low compared to the link capacities of core networks, it is more likely that this tool better fits usage in end site networks that want to check the performance they can get on end-to-end paths.

The “-V” option can be used with Iperf to use the IPv6 protocol. This option has to be explicitly mentioned on the client and server side.

Server side:

```
$ iperf -s -V
```

Client side:


```
$ iperf -c <Server IPv6 Address> -V
```

5.2.6. *ntop*

ntop is a network traffic probe that shows the network usage, similar to what the popular top Unix command does for CPU usage of a system. ntop is based on [libpcap](#) and it has been written in a portable way in order to virtually run on every Unix platform and on [Win32](#) as well.

ntop now fully supports IPv6, thanks to the effort of INRIA within the WP6 framework of the 6NET project. ntop can collect and make stats available on IPv6 flows and hosts in the network. Moreover, IPv6 flows can be exported with netflow v9 from with the nProbe feature, merged with the ntop tool.

ntop can also act as a netflow v9 collector for IPv6 flows exported from other equipment (eg. a CISCO router or another ntop application)

IST-2000-32603	Deliverable 6.3.3. Final report on the implementation of tools and operational procedures	
----------------	--	--

5.3. Tools for all network parts

5.3.1. 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.

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.](http://www.ipswitch.com) WhatsUp Gold (Figure 2, Figure 3), which supports only IPv4.

IPv6 Management Gateway translates SNMP and ICMP and TCP protocol messages between WhatsUp Gold (IPv4) and the 6NET network (IPv6). WhatsUp Gold is accessible at <http://chives.man.poznan.pl>; The IPv6 Management Gateway is implemented on plum.man.poznan.pl.

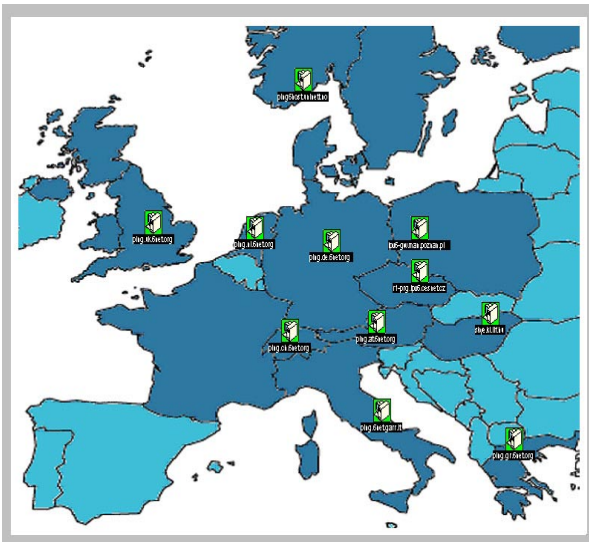


Figure 2

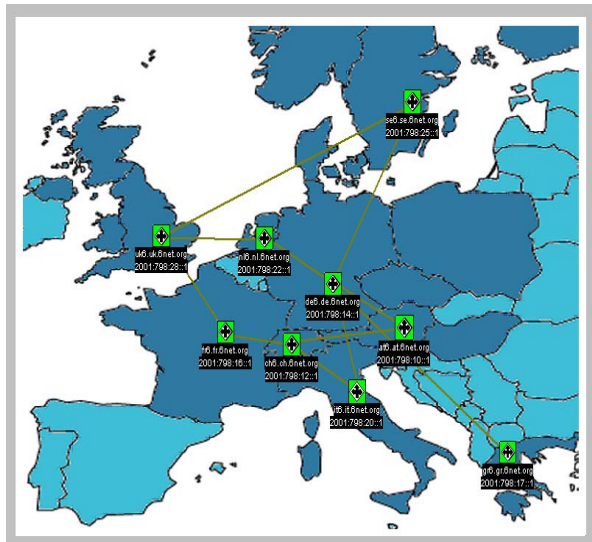



Figure 3

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

5.3.2. Nagios

Nagios is a host and service monitor designed to inform network operators about network problems. The monitoring daemon runs intermittent checks on hosts and services as specified in the configuration using external "plugins" which return status information to Nagios. When problems

IST-2000-32603	Deliverable 6.3.3. Final report on the implementation of tools and operational procedures	
----------------	--	--

are encountered, the daemon can send 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. A separate NAGIOS station for monitoring IPv6 network service of HUNGARNET and 6NET has been setup.

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


5.3.3. 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 front-ends 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, 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.

IST-2000-32603	Deliverable 6.3.3. Final report on the implementation of tools and operational procedures	
----------------	--	--

6. Recommendations for network administrators

6.1. Network management architecture

These recommendations are explained in section 4 of this document.

6.2. End-site networks


The following tools could be deployed for managing end-site networks:

- A single tool for traffic management, service availability (web, DNS, SMTP, IMAP...) and link/equipment status: Argus, Nagios or Ntop
- Optionally, one tool for evaluating end-to-end performance of the IPv6 network: Iperf or Pchar
- Rancid for managing the configuration of the equipment
- One tool for analysing packets on shared links for occasional troubleshooting: Ethereal or tcpdump
- One Multicast beacon for IPv6 multicast management


6.3. Core networks

The following tools could be deployed for managing core networks:

- For traffic management, the following tools could be deployed: MRTG, Cricket or Nagios
- Intermapper or Nagios can be deployed for monitoring and displaying equipment and link status.
- For routing management, two different tools can be deployed, which have completely different goals :
 - ASpath-tree can be deployed to monitor the routing policy and the global status of the routing table.
 - Home-made scripts have to be deployed for monitoring BGP peerings for two reasons. On one hand, very few routers have a MIB describing IPv6 BGP behaviour of the router. On the other hand, there are no clients available to perform the requests.

IST-2000-32603	Deliverable 6.3.3. Final report on the implementation of tools and operational procedures	
----------------	--	--

- For accounting management: IPflow can be used. But it appears that in most cases, network administrators prefer to deploy their own collector.
- Rancid for managing the configuration of the equipment

IST-2000-32603	Deliverable 6.3.3. Final report on the implementation of tools and operational procedures	
----------------	--	--

7. Tools used by 6net NOC

This section is an illustration of the set of tools that can be deployed for network management. This set of tools was deployed by the 6Net NOC for the 6Net core network management. It must be noted that the set of tools that is deployed also depends of the experience of the NOC staff regarding management tools.

7.1. 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.

7.2. 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 the 6NET network. It also presents utilization statistics, which show up traffic, errors and outage information, which helps troubleshooting the problems that may occur.

The network map is displayed as a web page where one can find different information about the network. Below a snapshot of the current state of the 6NET network is presented.

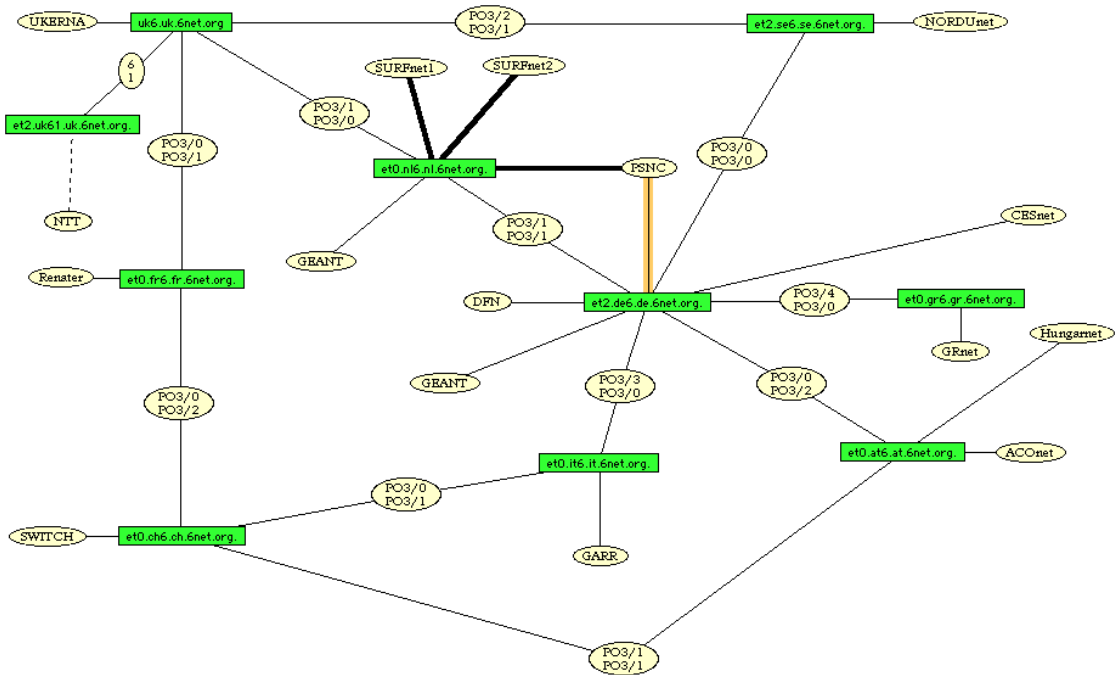


Figure 4


Table 1 summarizes the tools that are being used in 6Net NOC to monitor the core routers. More information about them can be found in the last version of the deliverable, D6.3.2 [D6.3.2].

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

Table 1: tools used by 6Net NOC


7.3. Summary

Section 5 describes and explains tools, which are being used by 6NET partners. All of them are included in D6.2.4 [D6.2.4] “Final report on development and test”. This document covers in detail

IST-2000-32603	Deliverable 6.3.3. Final report on the implementation of tools and operational procedures	
----------------	--	--

how NRENs have improved or even developed 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 production deployment.

Managing and monitoring is a critical part in every network, whatever the version of IP. Some standards for MIBs and are still under development. The continuous work on that will result in several improvements in short-term for the management of IPv6 networks.

IST-2000-32603	Deliverable 6.3.3. Final report on the implementation of tools and operational procedures	
----------------	--	--

8. Operational procedures used in 6NET

This section illustrates the management procedures for the 6NET network. More information about management in general can be found in section 4.

8.1. Introduction

This section gives an update of the procedures followed by the participants of the project i.e. partners and 6net NOC. The 6NET network was built mainly during the first year of the project and all the procedures were defined and described during that period. In the following year, there were some slight changes, which were described in D6.3.2 [D6.3.2] - mainly related to the procedures to propose and schedule tests which affect the 6NET core. All those procedures - described in detail in D1.2, D1.3 and D1.4 have been followed and implemented during the last part of the project.

8.2. Operational procedures followed by the 6net NOC

D1.2 describes more in detail the procedures to be followed by 6net NOC. This section presents first an overview of 6net NOC and the updates from D6.3.2.


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, 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, managing the services, managing gateways to external networks, and planning and executing changes to the network configuration. The 6NET NOC has responsibility for monitoring and reporting on the performance of the network and it collects data for the monthly reports on services, which are primarily intended for the 6NET partners.

The offices of the 6NET NOC have moved in Q3 2004, the new contact phone number is as follows:

Trouble email: trouble@6net.org
 Trouble desk phone: +33 141 28 85 59
 Fax number: +33 141 28 47 47

6NET NOC may receive or give reports by email, fax or telephone for urgent matters. The employees to receive trouble email include the GEANT NMS dedicated team, the DANTE operations team and Cisco, who are responsible for troubleshooting problems in the network and the equipment.

8.3. Operational procedures followed by 6NET partners

IST-2000-32603	Deliverable 6.3.3. Final report on the implementation of tools and operational procedures	
----------------	--	--

8.3.1. Introduction

This part of the document summarises the procedures followed by 6NET partners to connect to the 6NET core. See Deliverable 1.3 “Operational procedures to be followed by organisations connected to 6NET” for more details.

This section contains only the updates from the reported period between H2/2003 and H1/2004.

8.3.2. Access circuits

Access circuits for the connection of the NRENs to the 6NET core were ordered by the NRENs itself 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 were established via local-loops in each country in the first year of the project. Subsequently in Q1 2003, Cesnet was connected to DE and HUNGARNET to AT via dark fiber provided by T-Systems. NTT, Asian ISP was directly connected to the 6NET core in UK with E3 via COLT provider. PSCN and GRnet were also connected using a Layer 2 VPN connection throughout GEANT infrastructure.

During the last reported period H2 2003 - H1 2004, FCCN has been connected to the core in Q1 2004 via a Layer 2 VPN connection through GEANT. Also during the same period, the native link AT-HUNGARNET was decommissioned and replaced by a Layer 2 VPN using the same technology than in FCCN due to the low performance of the link. A new 1GB link Prague-Amsterdam is used to provide a second connection to CESNET and used for multicast only traffic.

More information about the network topology and changes is reported in D1.5.4 and D1.5.5.


8.4. Operational procedures during test periods for 6NET NOC and 6net participants

The complete procedures for approval and scheduling test in 6NET, which involve configuration and deployment of the 6NET routers, are described in detail in D1.4. The updated version of D6.3.2 also contains a brief explanation of the procedures. The full procedures were successfully applied during the multicast and CoS tests performed during 2003 and 2004 respectively.

IST-2000-32603	Deliverable 6.3.3. Final report on the implementation of tools and operational procedures	
----------------	--	--


9. Conclusion

This deliverable gives the reader some keys to manage an IPv6 network. The reader is first presented with an updated of the standardization status. After that the basics for building the management architecture are explained. The deliverable details clearly that successful network management consists of a combination of procedures to be defined, and management functions to fulfil. To assure these management functions, the network administrator has to deploy a set of appropriate tools, and this deliverable presents a non-exhaustive list of the tools deployed by most of the 6NET partners. To assist the reader in the choice of the appropriate tools to deploy, the recommendation section lists a set of tools that can be used, which satisfy most of the management scenarios (depending on whether the network is a LAN or a WAN). At the end, the management architecture for 6Net network is presented as an example, from procedures and policies to the tools deployed.

IST-2000-32603	Deliverable 6.3.3. Final report on the implementation of tools and operational procedures	
----------------	--	--

10. References

- [RFC 2011] “SNMPv2 Management Information Base for the Internet Protocol using SMIV2”, K. McCloghrie (ed.), November 1996
- [RFC 2012] “SNMPv2 Management Information Base for the Transmission Control Protocol using SMIV2”, K. McCloghrie (ed.), November 1996
- [RFC 2013] “SNMPv2 Management Information Base for the User Datagram Protocol using SMIV2”, K. McCloghrie (ed.), November 1996
- [RFC 2096] “IP Forwarding Table MIB”, F. Baker, January 1997
- [RFC 2465] “Management Information Base for IP Version 6: Textual Conventions and General Group”, D. Haskin, S. Onishi; December 1998
- [RFC 2748] “The COPS (Common Open Policy Service) Protocol”, D. Durham (ed.), J. Boyle, R. Cohen, S. Herzog, R. Rajan, A. Sastry; January 2000
- [RFC 2851] “Textual Conventions for Internet Network Addresses”, M. Daniele, B. Haberman, S. Routhier, J. Schoenwaelder; June 2000
- [RFC 3291] “Textual Conventions for Internet Network Addresses”, M. Daniele, B. Haberman, S. Routhier, J. Schoenwaelder; May 2002
- [RFC 3539] “Authentication, Authorization and Accounting (AAA) Transport Profile”, B. Aboba, J. Wood; June 2003
- [RFC 3588] “Diameter Base Protocol”, P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko; September 2003
- [RFC 3614] “Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)”, D. Harrington, R. Presuhn, B. Wijnen; December 2002
- [D1.2] “Operational Procedures to be Followed by the 6NET NOC”, October 2002
- [D1.3] “Operational Procedures to be Followed by Organisations Connected to 6NET”, July 2002
- [D1.4] “Procedures for the Approval and Scheduling of Tests”, June 2002 and March 2003
- [D1.5.*] “Six Months Usage Report”, June 2002, December 2002, June 2003, December 2003, June 2004,...
- [D6.1.2] “Management Architecture Specifications”, January 2003

IST-2000-32603	Deliverable 6.3.3. Final report on the implementation of tools and operational procedures	
----------------	--	--

- [D6.2.2] “Operational Procedures for Secured Management with Transition Mechanisms, 2nd Version”, May 2004
- [D6.2.3] “Interim Report on Development and Test”, July and December 2003
- [D6.2.4] “Final Report on Development and Test”, September 2004
- [D6.3.1] “6NET IPv6 Network Management Cookbook”, October 2002
- [D6.3.2] “Interim Report on the Implementaation of tools and operational procedures”, July 2003
- [TUNNELMIB] “IP Tunnel MIB”, draft-ietf-ipv6-inet-tunnel-mib, D. Thaler; August 2004
- [WBEM] “What is WBEM?”,
<http://www.win2000mag.com/Articles/Index.cfm?ArticleID=3568>, Greg Todd;
July 1998