


IST-2000-32603	Deliverable D	
----------------	---------------	---

Project Number:	<b>IST-2001-32603</b>
Project Title:	<b>6NET</b>
CEC Deliverable Number:	<b>32603/Partner/DS/631./A1</b>
Contractual Date of Delivery to the CEC:	30/9/2002
Actual Date of Delivery to the CEC:	
Title of Deliverable:	6Net IPv6 Network Management Cookbook
Work package contributing to Deliverable:	6
Type of Deliverable*:	R
Deliverable Security Class**:	PU
Editors:	Duncan Rogerson
Contributors:	Isabelle Astic, Tim Chown, Jérôme Durand, Robert Evans, Fulvio Risso, Duncan Rogerson, Bernard Tuy

\* Type: P - Prototype, R - Report, D - Demonstrator, O - Other

\*\* Security Class: PU- Public, PP – Restricted to other programme participants (including the Commission), RE – Restricted to a group defined by the consortium (including the Commission), CO – Confidential, only for members of the consortium (including the Commission)

**Abstract:** This deliverable documents design, features, recommendations and tools that may be used to manage and monitor a wide area IPv6 network.

**Keywords:** Network management, network monitoring, network management tools

## Table of Contents

<b>1</b>	<b><u>INTRODUCTION</u></b> .....	<b>3</b>
<b>2</b>	<b><u>RELATIONSHIP TO OTHER DELIVERABLES</u></b> .....	<b>3</b>
<b>3</b>	<b><u>MANAGEMENT PROTOCOLS AND MIBS IN THE STANDARDISATION PROCESS</u></b> .....	<b>3</b>
3.1	<u>SNMP FOR IPV6</u> .....	3
3.2	<u>MIBS</u> .....	4
3.2.1	<u>The Textual Conventions</u> .....	4
3.2.2	<u>The Evolution of the MIBs</u> .....	4
3.3	<u>THE OTHER STANDARDS</u> .....	6
3.4	<u>THE EXPECTED ACHIEVEMENTS</u> .....	6
<b>4</b>	<b><u>NETWORK MANAGEMENT ARCHITECTURE</u></b> .....	<b>7</b>
4.1	<u>INTRODUCTION</u> .....	7
4.2	<u>MANAGEMENT ARCHITECTURE</u> .....	7
4.3	<u>CUSTOMER CARE</u> .....	8
4.4	<u>OPERATIONS SUPPORT</u> .....	9
4.5	<u>NETWORK MANAGEMENT AS A PROMOTIONAL SERVICE</u> .....	10
4.6	<u>NEW FUNCTIONS AND PROTOCOL MANAGEMENT</u> .....	10
<b>5</b>	<b><u>GENERAL MANAGEMENT RECOMMENDATIONS</u></b> .....	<b>11</b>
5.1	<u>INITIAL DEPLOYMENT REQUIREMENTS</u> .....	11
5.2	<u>OPERATIONAL REQUIREMENTS</u> .....	11
5.2.1	<u>Network Communications Links</u> .....	11
5.2.2	<u>Routing Status</u> .....	12
5.2.3	<u>Network Equipment</u> .....	13
5.2.4	<u>Change Management</u> .....	13
5.2.5	<u>Protocols and Services</u> .....	14
5.2.6	<u>Hosts and LANs</u> .....	14
5.2.7	<u>Applications</u> .....	15
<b>6</b>	<b><u>NETWORK PERFORMANCE AND TRAFFIC MEASUREMENT</u></b> .....	<b>15</b>
6.1	<u>BASIC TRAFFIC ACCOUNTING</u> .....	15
6.2	<u>TRAFFIC FLOWS</u> .....	15
6.3	<u>NETWORK LATENCY AND JITTER</u> .....	15
6.4	<u>EQUIPMENT STATUS</u> .....	16
6.5	<u>THRESHOLDS AND ALARMS</u> .....	16
<b>7</b>	<b><u>MANAGEMENT, MEASUREMENT AND MONITORING TOOLS</u></b> .....	<b>16</b>
7.1	<u>LINK MANAGEMENT</u> .....	16
7.2	<u>TRAFFIC MANAGEMENT</u> .....	16
7.3	<u>EQUIPMENT MANAGEMENT</u> .....	16
7.4	<u>CONFIGURATION MANAGEMENT</u> .....	16
7.4.1	<u>LAN and host management</u> .....	16
<b>8</b>	<b><u>TOOL SUMMARY</u></b> .....	<b>18</b>
<b>9</b>	<b><u>CONCLUSION</u></b> .....	<b>19</b>
<b>10</b>	<b><u>BIBLIOGRAPHY</u></b> .....	<b>19</b>
	<b><u>GLOSSARY</u></b> .....	<b>20</b>

---

## 1 Introduction

Network management and monitoring is a critical part of operating any production quality network, whatever the nature of the network. It is one of the essential building blocks of the 6net network, and must be so for any IPv6 public network, especially in the Internet service provider area. If IPv6 backbone networks are not subject to the same (or even an improved) standard of management and monitoring as existing IPv4 networks, the existing IPv4 user base will be unwilling to migrate.

This activity covers many areas of the network. From straightforward monitoring of link status, to traffic statistics gathering and analysis, both for future network planning and for use in other situations, such as early detection of denial of service (DOS) attacks.

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 function. The end result should be that this deliverable will be both a useful guide to designers of new IPv6 networks, and as a reference for more experienced network managers.

This document draws from experiences on the 6net backbone network, and from individual 6net partners and their experiences managing and monitoring their own IPv6 networks.

Most of the 6Net WP6 partners have also got experience in managing IPv4 production networks. This experience is a common background to contribute to the WP6 activity and mainly to 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. Nevertheless we are still in a period of time where standards by the IETF are not completed and MIBs for IPv6 equipment are largely implemented by vendors to their own proprietary standards

In this transition period one can see commercial ISPs deploying and offering IPv6 services to their customers. In order to manage their service (i.e. their network) they still have to rely on home-made tools; some of them even relying on using the IPv4 transport of information from and about IPv6 devices. This Cookbook will be updated throughout the 6Net project life, as more experience is gained with IPv6 network management and monitoring.

## 2 Relationship to other deliverables

As noted in other WP6 documents, network management and monitoring are activities that are used across an entire network. This may be at the network level, providing basic traffic counts and availability, or testing the performance of a network, so it can be tuned to support the requirements of particular applications. Additionally, as this document is a "cookbook", it will touch on and reference many, if not all, other deliverables in WP6 and in other WPs.

## 3 Management protocols and MIBs in the standardisation process

As the main management standard used for IPv4 networks was SNMP, this section starts with a summary of the evolution of the SNMP standard, and its associated MIBs. Later on, the section covers the evolution of other standards towards IPv6 support.

### 3.1 SNMP for IPv6

One implementation of SNMP over IPv6 is now in existence, since March 2002, from the net\_snmp Open Source project. The reason that no other implementations currently exist is most likely

because most IPv6 networks were/are running dual stack with IPv4. It is possible to manage IPv6 networks via SNMP over IPv4, if MIBs are defined for using SNMP over IPv4.

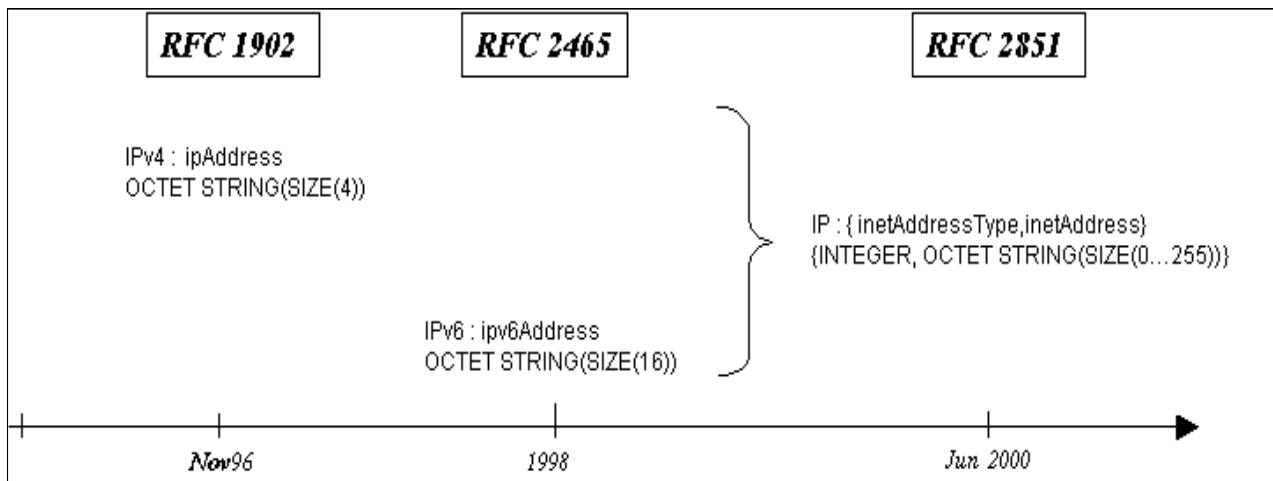
Now that IPv6 native networks exist, the need for SNMP over IPv6 increases but, as far as we are aware, there is no other implementation available as of the time of writing this first version of this cookbook.

### 3.2 MIBs

There are almost one hundred MIBs to check, to verify if they could be used to manage IPv6 networks. Some will have to be further developed to support IPv6. Effort is currently only being made on MIB II, although since the specification of IPv6 in 1995, the definition of a MIB II table to manage IPv6 networks has changed twice.

#### 3.2.1 The Textual Conventions

Figure 1 represents the evolution of the textual convention since the last “IPv4 MIB II” updates in 1996. In 1998, a textual convention was defined for IPv6 addresses only. But this implied the partition of IPv4 and IPv6 management. That is why the latest textual convention for IP address is an unified convention, able to manage both types of addresses.



**Figure 1: Evolution of the IP Address textual convention**

This new convention defines an IP address as a structure {inetAddressType, inetAddress}, where

- *inetAddressType* is an INTEGER which specifies if the following address is, for example, an IPv4 or IPv6 one, and
- *inetAddress* is defined as an OCTET STRING(SIZE(0...255)), in order to be able to save the value of an IPv4 or IPv6 address, as the value of a DNS name (cf. RFC 2851 updated by RFC 3291).

#### 3.2.2 The Evolution of the MIBs

The definition of this textual convention implies associated modification of the MIB II.

In 1996, the MIB II was updated in order to manage IPv4 networks. It was defined by the RFC 2096, RFC 2011, RFC 2012, RFC 2013. Three groups were defined: ip, tcp and udp. Each group contains simple objects and tables (see figure 2).

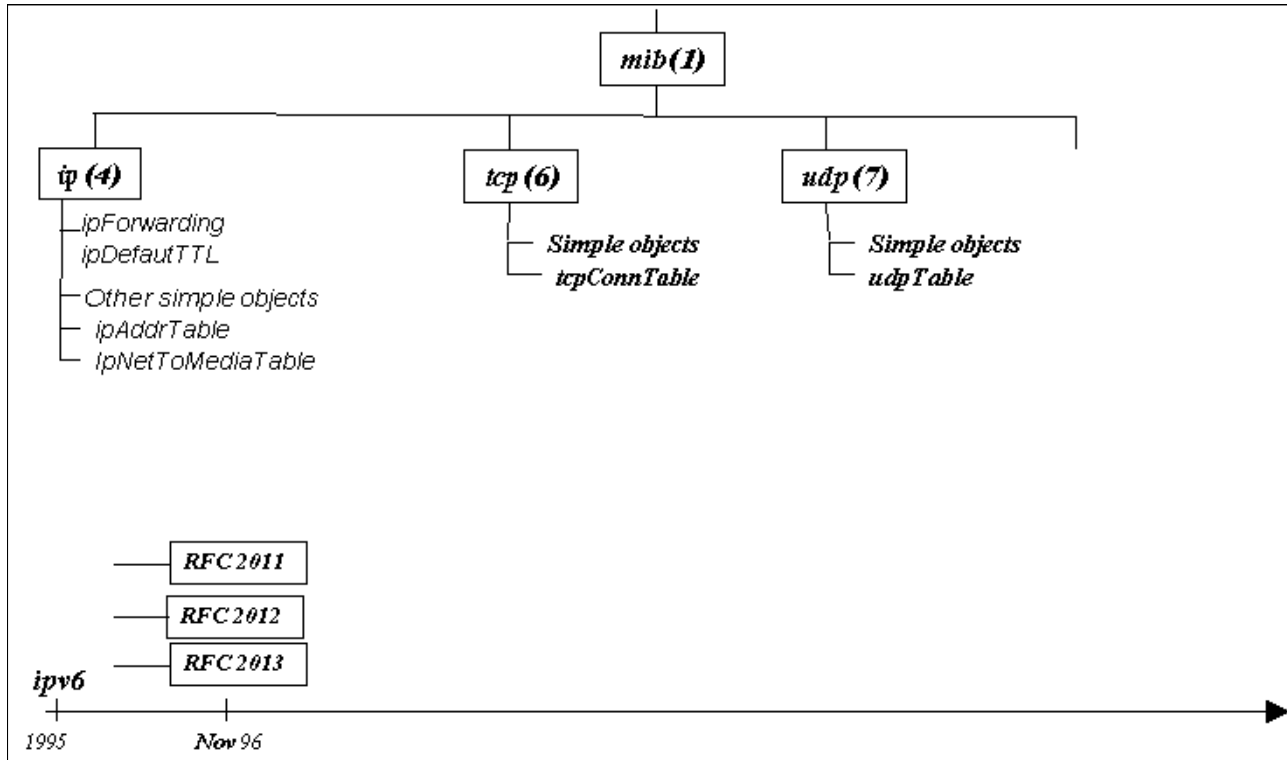


Figure 2 : The MIB II in 1996

In 2002, the unified approach, illustrated in Figure 3, unified all the tables : ipAddrTable became ipAddressTable, ipNetToMediaTable became ipNetToMediaTable, all the simple objects defined into the IPv4 MIB II became the ipIfStatsTable. The same with tcpConnTable which became tcpConnectionTable, and with udpTable, which became udpListenerTable. It must be noticed that, in addition to this table, issued from the IPv4 management architecture, new tables were defined like the ipv6InterfaceTable.

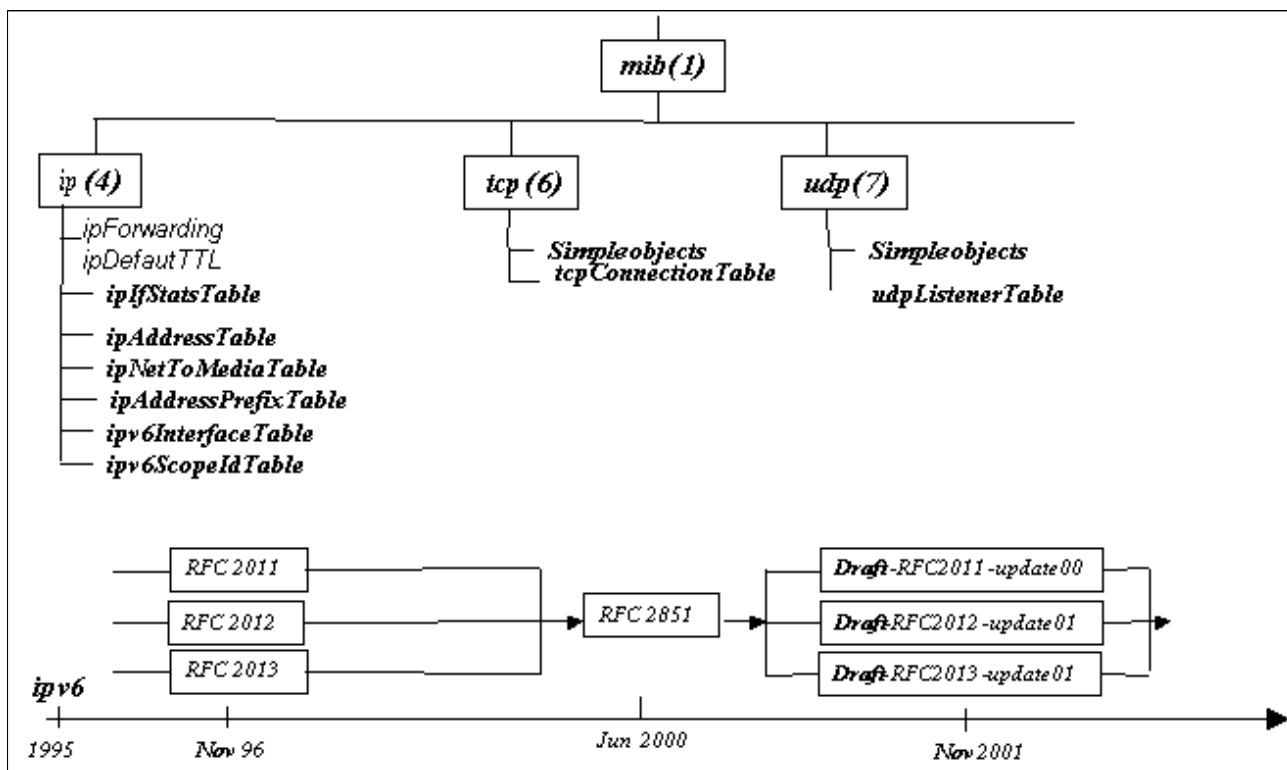


Figure 2 : The unified MIB II

### 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, Authorisation and Accounting). Those standards are COPS, WBEM for the configuration point of view, RADIUS and Kerberos V 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 (see RFC 3162). But as experience has shown that it can not 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 is not currently defined into a RFC but only into a Internet draft (the last version (the 13<sup>th</sup>) is dated of October 2002), but an implementation already exists, due to SUN, based on the 7<sup>th</sup> version of the draft. A new one is under development into the IST Moby Dick project, defined upon the 10<sup>th</sup> version of the draft.

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

### 3.4 The Expected Achievements

As we could see, in a short-term, the main problem to solve is the absence of similar management standards available for IPv4 for IPv6 networks as well (except for the AAA where work is more in advance).

---

To a configuration point of view, standards upon IPv6 are available, only misses their implementation.

The problem is bigger for monitoring and fault management where SNMP standard is not available for the moment. It becomes really urgent to have at least a standardized MIB II and several implementations of the SNMP protocol over IPv6.

## **4 Network Management Architecture**

### **4.1 Introduction**

In this section we describe the basic ideas of network management architecture design. It is aimed at giving help to anyone starting an IPv6 network, to help understand how to set-up its management entities and information flows between these entities. 6Net deliverable 6.1.1 sets out the suggested network management architecture for the 6Net network. This architecture is quite usual in splitting the network management into several areas and defining the boundaries of every entity's responsibility. In some peculiar situations though a different, and more unified, model could be implemented, having a single entity responsible for the all components of the network. From experience, this kind of situation is quite rare in large networks, such as 6Net, spreading over several European countries.

### **4.2 Management architecture**

We can draw a scheme of the different management domains of a network. We basically have three different domains, or management areas : the site area, to which the end-users are connected, the access domain, connecting a set of sites to the core, and the core area itself. Ideally, one entity should exist for each domain, responsible for the network management and monitoring of that particular domain.

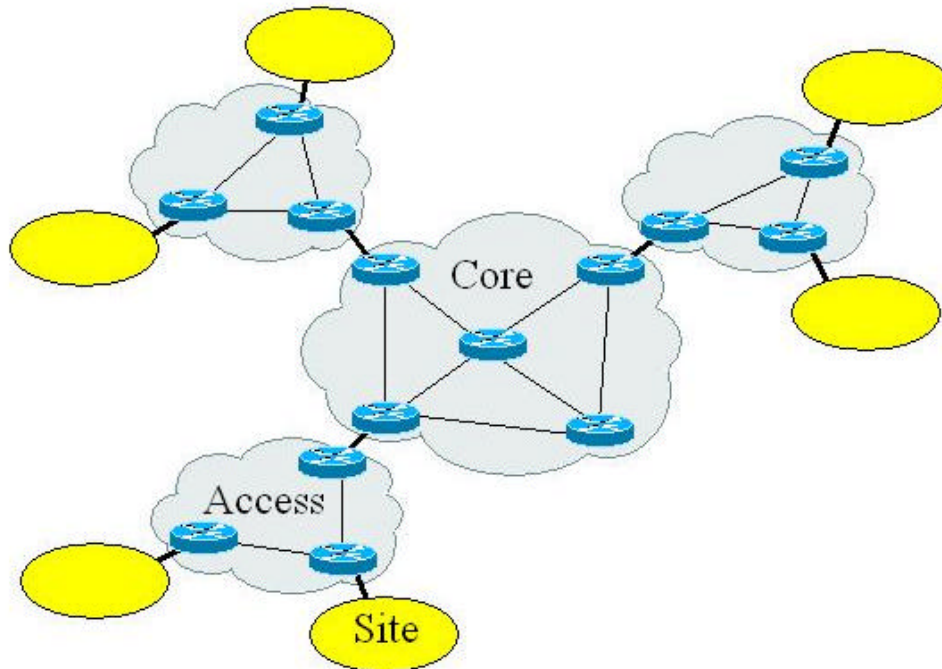


Figure 4.2

It is important to coordinate all these entities and to describe the different flows of information between these entities. D6.1 chapters 4, 5 and 6 describe the entities and the different flows designed for 6NET. Responsibility boundaries between the management domains have to be defined too. Usually, the operation of the links is in the charge of the entity closer to the core, with every entity being responsible for its interfaces which are connected to links which have terminations in different domains.

### 4.3 Customer care

A unique point of contact should be provided to any customer for reporting problems related to the operation and usage of the network and related services. This defines two-way information flows between the user and the customer care management entity, over which the following functions could be performed :

- Customer to network management entity:
  - submit trouble reports including hardware and link failures,
  - submit change request,
  - submit test requests,
  - request for assistance,
  - request for information.



- Network management entity to customers:
  - proactive notification of planned network outages and changes,
  - notification of network failures,
  - answers to problems reported and change requests,
  - dissemination of detailed trouble tickets to concerned customers and entities,
  - propagate network status and configuration,
  - provide proposals for test set up and performance,
  - respond to information requests.

#### 4.4 Operations support

Each domain / area of the network must be under the control of an operations support system which is linked to the customer care process. Operations support ensures the day by day operation of the network. It could be responsible for the following services :

- Basic network management activity
  - Link monitoring (see §5.2.1)
  - Network equipments monitoring (see §5.2.3)
  - Fault reporting, via trouble ticket systems (see Problem management below)
- Problem Management :
  - collect trouble reports from customers,
  - disseminate trouble-tickets,
  - track discovered faults,
  - report discovered faults to impacted entities,
  - resolve problems,
  - disseminate procedures used to track and resolve the faults,
  - notify resolved problems to the concerned entities.
- Configuration management :
  - maintain an accurate configuration of the network,
  - provide a map of the actual network state,
  - provide all necessary information to enable a partner to easily set-up the necessary hardware and software to connect to the network,
  - plan and track software update across the network,
  - maintain software version control,
  - manage name and address assignments
  - implement routing policy
  - register all IP resources into related appropriate Internet Registry Databases.
- Test Management :
  - backup configuration data to enable restoration,
  - configure the network for a given test purpose,
  - enable the test and monitor the activity of the considered test,
  - restore the network configuration after test performance,
  - if specific measurements are defined as part of a test, provide the entity performing the tests with the information obtained from the test monitoring activity.
- Performance & accounting :
  - collect continuous usage statistics from the network through monitoring,
  - observe availability and performance of required network functions (e.g. DNS, routing daemons, bandwidth utilisation...)
- Security management :

- ensure limited access to network components (access control and authentication, looking glasses for the use of users or other management entities from other areas)
- provide authenticated means of collecting statistics from devices (SNMPv3 is one way of offering this facility),
- detect and protect against malicious attacks.
- All this management services apply to both the network and related services (routing, DNS...)

#### 4.5 Network management as a promotional service

While network management is essentially oriented towards the users and customers of the network and the provider, data and information flows related to the operation of the network (e.g. usage statistics) are sometimes not made publicly available.

Whilst the general feeling in the 6net community is that publishing management and monitoring statistics is useful, the decision for a network to publish will depend upon individual commercial or political circumstances.

If the decision is made to publish any (or all) of the network management information, it can be very useful to show to the outside world the “life” of the network. e.g. the web page for the IPv6 Pilot in France<sup>1</sup>, or for the Greek Research and Technology Network<sup>2</sup>.

#### 4.6 New Functions and Protocol Management

As IPv6 is a new protocol and many services are being deployed, the network management entity has to be cautious of the impact on network management when deploying new services. For instance, transition mechanisms between IPv4 and IPv6 are new facilities and at the moment nobody clearly understands how they have to be managed. Even from a security point of view, experience with these mechanisms has to be gained. A more detailed set of recommendations will be inserted in this Cookbook, as and when experience is gained

To this respect, WP2 activities should provide us with a set of first recommendations since at this stage of the network deployment, only intellectual activity has been undertaken.

Here is a brief list of transition mechanisms being studied in WP2 for which we need to be confident that the interfaces, traffic levels and perhaps in some cases state information should be monitored, but where some metrics are certainly not defined in any MIB drafts. A brief description of the operation of each method is given to provide a flavour of the information that may need to be monitored for each mechanism.

- IPv6-in-IPv4, IPv6-in-IPv6, IPv4-in-IPv6 tunnels: standard tunnels, manually configured, tied to physical interfaces.
- ISATAP: has an ISATAP IPv6-in-IPv4 tunnel interface on the client, with site ISATAP router(s) having a tunnel end-point. ISATAP clients may use anycast or a well-known name to discover the ISATAP router.
- 6to4: has an automatic IPv6-in-IPv4 tunnel interface on routers (or in some cases hosts) using the method, and also has an associated 6to4 relay that is generally discovered by using IPv4 anycast to 192.88.99.1, to which traffic directed towards to “native” IPv6 links is tunnelled. The relay may be open (and thus be subject to relay (D)DoS attacks).

---

<sup>1</sup> <http://lookingglass.imag.fr/>

<sup>2</sup> <http://netmon.grnet.gr/lgv6.shtml>

- 6over4: not being considered in WP2 (likely to be declared HISTORIC). It uses IPv4 multicast to carry IPv6 traffic.
- Teredo: unclear at present - no implementations.
- DSTM: requires dynamic IPv4 client stack configuration, then encapsulation of the data (IPv4-in-IPv6) is performed from the client to the Tunnel End Point router (TEP) located on the boundary of the local IPv6-only network. The TEP then decapsulates the data and deliver it to the destination in the IPv4 Internet. This mechanism requires that an IPv4 address pool is managed (DSTM server) for the IPv6 clients need via DHCPv6 or an equivalent mechanism.
- Tunnel broker: clients connect to a broker web server to establish the IPv6 prefix/address to use, and the address of the tunnel broker server, plus a script to (de)activate the tunnel. State information for active tunnels should probably be available.
- NAT-PT: translates IPv6 to/from IPv4 packets/headers. Maintains state in the NAT-PT device, thus state information should probably be monitored to assess/predict problems with overloading.
- BIS/BIA: not currently being considered in WP2 (little use of the tools at present).
- TRT/SOCKS: translation occurs at the socket level, thus not probably directly monitored at network layer; may be monitored by other means.
- ALGs: web proxy, SIP proxy, FTP proxy, not directly managed at the network layer, but can be monitored for use/traffic in other ways.

## 5 General Management Recommendations

There are many different pieces of equipment and functions within an IPv6 network that will, or may, require monitoring and managing. These will vary as the state of the network progresses from initial implementation to full deployment.

### 5.1 Initial Deployment Requirements

At the start of deployment, network management requirements are very different from those needed during normal network operation. Much of the initial network management activity is centred around planning, tracking delivery of equipment and links, and ensuring that network engineering and operations staff have access to all physical locations on the network. This may be both physical, for example, for site surveys and physical installation of equipment, and logical such as out of band access via PSTN or ISDN, to enable equipment configuration before the actual network links are delivered. In the aim of setting up the management entities, an important process has to be started as soon as possible : choosing the people who will run the management entity, and their training needs in the new technologies.

### 5.2 Operational Requirements

After the network is brought into service, the following should be managed and monitored:

#### 5.2.1 Network Communications Links

We should be able here to verify that the connectivity between two elements of the same link is available, and be able to archive this information. Any link between two devices needs to be

considered in terms of each visible physical link in the path. For example, the end-to-end link between two routers may contain:

- A link from router A to a local ATM switch
- A link from the ATM switch into another operator's network
- An operator's network (of which the local network has no internal visibility)
- A link from the operator's network into the local network
- An internal link across the local network
- A link from the terminating ATM switch to router B

The connectivity state between two interfaces on router A and B depends on:

- The interface of router A
- All physical links between A and B
- All equipment between A and B
- Other operator's networks (where used)

So we here need to be able (for each part of the end to end link):

1. To verify the configuration of each interface in the path for which we have visibility (IP addresses, link layer protocol used, link layer configuration protocol) and to be able to track any changes in it. In the specific context of IPv6, we should be able to verify, for example, which kind of configuration was used for the IP addresses (stateless auto-configuration, stateful auto-configuration, manual configuration), and if the protocols involved into the configuration process (DHCPv6, Neighbour Discovery) are well-configured.
2. To test the integrity of a link (for example, with statistics about the link layer traffic: high CRC errors could be a damaged physical link or broken patch cable).
3. To test the integrity of a switch (for example, damaged power supplies supplying out of range electrical current can cause strange problems on a switch or router)
4. Date of last repair, number of repairs since the link has been put into operation.
5. The status of any transit paths through other operator's networks.

### 5.2.2 Routing Status

In the case of connectivity problems, and if there is no communication between a sender and a receiver, the routing process must be verified.

A routing may occur due to a malfunction of:

- The sender or receiver interface
- Any of the routers involved in the transmission of the packet from the sender to the receiver
- The routing protocol (e.g. RIPng, BGP4+, ISIS, ...)
- The redistribution between several routing protocols is not correctly configured

So here, we need to be able to:

1. Verify the configuration and state of the sender and receiver interfaces (see above)

2. Verify the configuration and state of all the routers involved in forwarding the data from the sender to the receiver
3. Define and verify the behaviour of a router. For example, we should be able to define the routing policy as tightly as possible, notably to manage multi-homed routers. We should be able to verify also, as precisely as possible, the reason why a packet is refused or discarded by a router. As IPv6 creates new headers and thus new reasons for discarding packets, this should be managed.
4. Verify the interconnection (configuration, state, behaviour) of the multiple routing protocols involved into the routing process between the sender and the user. For example, is there a good interconnection between a BGP4+ and the intra-routing protocol, like RIPng.
5. Check for bugs in the version of operating software
6. Verify that IP prefixes are accurately registered in the Internet Registries

### 5.2.3 Network Equipment

Manage and monitor equipment means:

- To verify the integrity of all equipment on the network
- To configure the equipment and to keep track of any changes in this configuration. At least, choose between a stateless auto-configuration, a stateful one or a manual one for the end hosts.
- To archive all the useful information about them
- To verify the data modelling this equipment and to keep trace of any of their change
- To track date of last repair, number of repairs since the equipment has been put into operation
- To track inventory status of equipment (original, backup, replacement loan, ...)

### 5.2.4 Change Management

Tracking and scheduling changes to the network is vital in operating a stable network. Scheduling the changes in advance allows notice to be given to users and other management entities of any potential disruption in service that might be caused as part of implementing the change. If the change fails, backing out the change should be easily possible from consulting the tracking logs.

To manage and monitor the changes occurring on the network, we must be able to:

- Detect these changes if they are not notified and described to all management entities in advance
- Archive change information
- Recreate the exact same changes for analysis, particularly if the changes had previously caused problems
- Monitor and archive equipment configurations
- Maintain an inventory of equipment and the version numbers of operating software in use

### 5.2.5 Protocols and Services

The previous sections define the architecture for managing the basic transport network itself – for example, in 6net, the ability to transmit an IPv6 packet from one network host to another. However, the information carried in those packets has not been considered – troubleshooting network problems may require the ability to inspect these packets more closely.

A protocol is mainly a set of rules that allow applications to talk together, with a specific packet format. It might be configured with special features like the size of a waiting queue, value of temporisation.

To manage and monitor protocols we will need to:

1. Verify the content of the packets sent by the particular protocol. Specifically, for the IPv6 protocol, this should include the reading of the header to be able to verify how they are defined.
2. Verify the way the protocol sequences the packets
3. Define, test, change, save and verify periodically the configuration of the protocol

[1] gives this definition of a service : “a particular logical function that may be invoked via some network protocol, such as printing, storing a file on a remote disk”. With IPv6 and its auto-configuration, special needs appear in the services discovery. This should be taken into account here.

So, the availability of the service rely on the connectivity of course, but also on:

- The availability of the protocol needed
- The availability of the service itself
- The availability of the equipment needed for the service itself (ex: the printer)
- The availability of the protocol allowing the services discovery, if any

This means that to manage and monitor a service, we should be able to:


1. Manage its configuration
2. Configure, define, verify and monitor the underlying protocol
3. Configure, define, verify and monitor its underlying discovery protocol
4. Verify and monitor the status of the service itself
5. Verify and monitor the status and the use of the equipment needed for the service

### 5.2.6 Hosts and LANs

Although the 6Net project focuses particularly on the network infrastructure, edge Local Area Networks are an important part of the overall infrastructure. The main problem we envision is that hosts cannot be queried by means of SNMP tools because they usually do not have SNMP installed; therefore a different set of tools is needed to assure their manageability.

The most important management operations that have to be done on LANs are:

- Capture traffic with the ability to specify custom filters
- Monitor node activity (if a node is currently active, whether it is

IST-2000-32603	Deliverable D	
----------------	---------------	--

- Sending traffic, what amount of traffic is currently sent/received)

### 5.2.7 Applications

The network may choose to provide some network infrastructure services, such as DNS, mail relays or a centrally managed IP videoconferencing or VoIP services. The availability and verification that these, and other network management applications such as statistics gathering is desirable to be managed.

There are many possible ways to do this – at the most basic level, checking that a connection to a TCP port on a server may verify that a service is actually running (although this does not guarantee correct configuration of the service, of course).

As and when suitable experience is gained on 6net, this section will be expanded in future revisions of this document.

## 6 Network Performance and Traffic Measurement

The management and monitoring activities take care of the basic function of the network. They establish whether communications links are up, and if the basic physical building blocks of the network, such as routers and switches, are running and available. This provides a network manager with basic reachability and availability information, but does not offer any further detail on the performance of the network itself, or the amount of traffic being carried.

To allow for future planning for network expansion and/or introduction of new services on the network, it is essential to have information about the amount of traffic running over the network, and the actual performance of the network. Performance in terms of latency and jitter can be important for many applications, particularly real time multimedia activities such as voice and video conferencing.

The following items should be monitored and measured:

### 6.1 Basic Traffic Accounting

Simple byte counts of traffic across the links on the network should be gathered, analysed and archived. This information immediately helps to identify areas on the network which may be experiencing, or soon to experience, congestion problems. It can also serve as a guide for future capacity planning, or more immediate traffic engineering.


### 6.2 Traffic Flows

Measurement and analysis of traffic flows allows a network manager to visualise network traffic at a higher level than simple byte counts. Flow measurement can identify the source and destination of an IP connection, the port/service being accessed, and the amount of traffic sent between the two hosts. Simple traffic statistics may identify a busy link, but flow statistics can be an easy way of identifying who is using the link, and what the link is being used for.

Flow analysis can be a great help in network planning and provisioning, and can be invaluable in detecting denial of service (DOS) attacks if a real-time flow measurement/monitoring tool is available. As with basic accounting, analysis of traffic flows could aid traffic engineering on the network.

### 6.3 Network Latency and Jitter

As already discussed, many real-time applications are sensitive to delay and jitter on the network. This delay and jitter can occur on even relatively unloaded networks, due to short bursts of traffic

IST-2000-32603	Deliverable D	
----------------	---------------	---

briefly overloading a link or the buffer space on an interface. Once aware of such a problem, network engineering staff may be able to tune queues, buffers or other configuration in the router to fix the problem.

Latency measurements are also useful in identifying some types of routing problems. For example, traffic may start to route over a back-up satellite link because of a routing table problem, even though the regular terrestrial link is still up and available. Availability monitoring will not detect this, as the link is up and reachable. However, measurements of latency will show significant increases, alerting operations staff to the problem.

#### **6.4 Equipment Status**

Simple availability monitoring shows whether a piece of equipment, such as a router, is reachable and functioning. However, many pieces of networking equipment are now capable of monitoring their own environment, such as temperature, power supply status and the failure of any or some of their modules or cards.

Environmental information is particularly useful for "lights-out" operation of equipment in remote locations, where no staff are physically present. If many of the pieces of equipment in the same location report increasing operating temperatures, this may indicate a failure in the local environment. Once network operations staff are alerted, it may be possible to fix the problem before the remote equipment fails.

Equally, in the case of equipment with resiliency features such as redundant CPU cards, it is very useful to know if a CPU card has failed, so that it can be replaced immediately. Otherwise the redundant card may fail too, causing the equipment to shut down.

#### **6.5 Thresholds and Alarms**

Most equipment and software can be set to generate alarms when a certain threshold is reached (such as 70% utilisation on a link). Such alarms may indicate either that capacity on a link needs to be increased, or the presence of undesired/unusual traffic such as a misbehaving application or some form of DOS attack.

Alarms can often also be generated for other events, such as environmental conditions and latency.

## **7 Management, Measurement and Monitoring Tools**

This section details tools, or groups of tools, and how they may be used to manage, monitor and measure an IP network. Information about whether the tool is currently IPv6 capable, and if the tool is being used on the 6net backbone, or in 6net partner IPv6 networks is also provided.

### **7.1 Link Management**

### **7.2 Traffic Management**

### **7.3 Equipment Management**

### **7.4 Configuration Management**

#### **7.4.1 LAN and host management**



---

This work is usually done by tools like network sniffers. The most important products we envision are:

- Ethereal (<http://www.ethereal.com>), a well known protocol analyser, whose main characteristics are the platform compatibility (it exists on several UNIX and Win32 platforms), the large number of supported protocols, and high-level feature like the "follow TCP flow"
- analyzer (<http://analyzer.polito.it>), another well known protocol analyser, which is able to monitor LAN nodes activity and offers a completely customisable protocol decoding engine by means of dynamically parsed XML files. This tool is currently under development at Politecnico di Torino where it is experimented.

## 8 Tool Summary

Monitoring Task	Tools	IPv6 Status	Used in 6net
	ping	Y	Y
	traceroute	Y	Y
Link availability	SNMP poll	Y	?
	SNMP trap	?	?
	commercial package		
Equipment availability	ping	Y	Y
	traceroute	Y	Y
	SNMP poll	Y	?
	SNMP trap	?	?
	commercial package		
Overall Network Status	weather map		
	intermapper		
Network performance	ping	Y	Y
	ttcp		
	Cisco SAA		
Configuration management	rancid		
	commercial package		
Traffic statistics	SNMP poll		
Routing status	SNMP poll		
	ASPATH tree		
	Looking glass		
Service/applications status	ping		
	TCP/UDP connection		
	Looking glass		
Reporting	commercial package		
LAN and Host management	ethereal	Y	Y
	Analyzer	Y	N

## 9 Conclusion

This cookbook try to gather relevant information about general IPv6 network management and monitoring in a single place.

Basic concepts are identical to what is used within IPv4 networks management (management entities and information flows, most of the tools have just to be ported for being used with IPv6 applications).

Nevertheless, differences are focused on new mechanisms and facilities (e.g. transition mechanisms, router renumbering, auto-configuration ...)

Today some tools are available and make it possible to offer basic management services (looking-glass, SNMP polls, ...) both over IPv4 or IPv6 transport. Part of these tools are deployed in the 6Net core.

But there are still a lot of missing facilities for the IPv6 network management: mainly MIBs implementation, and commercial integrated platforms.

There is still a standardization effort to be done in the IETF community. This area should speed up drastically when the IPv6 protocol and networks will become more used.

## 10 Bibliography

[1] «Requirements for Automatic Configuration of IP Hosts », draft-ietf-zeroconf-reqts-12.txt A.Williams, Motorola, 19 September 2002. (Note that this is a limited lifetime draft document of the IETF and may be published as an RFC or superceded).

---

### **Glossary<sup>3</sup>**

COPS	Common Open Policy Service, define in RFC 2748, “a simple client/server model for supporting policy control over QoS signaling protocols”
WBEM	Web Based Enterprise Management

---

<sup>3</sup> to be completed in future releases