Project Number:	**IST-2001-32603**
Project Title:	**6NET**
CEC Deliverable Number:	**32603/Partner/DS/6.1.2/A1**
Contractual Date of Delivery to the CEC:	31 June 2002
Actual Date of Delivery to the CEC:	31 December 2002
Title of Deliverable:	Management Architecture Specifications
Work package contributing to Deliverable:	6
Type of Deliverable*:	R
Deliverable Security Class**:	PU
Editors:	Georgios Koutepas
Contributors:	Jerome Durand, Rob Evans, Olivier Festor, Bartosz Gajda, Robert Szuman, Bernard Tuy, Ralf Wolter

* 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 document is the final specification of the management architecture of the 6Net network. It enumerates the requirements towards the management framework, provides a description of all entities contributing to the management activity and specifies their interaction. Especially it defines the 6NCC which is the entity at the heart of the management architecture which ensures coordination among all other participants.

Keywords: Network management architecture, 6NCC, Network management requirements

Table of Contents

1   Introduction

Being able to provide an integrated solution to the management of a large multi-domain IPv6 network is one of the key factors to the wide acceptance and deployment of IPv6. Providing the community with such a management solution is the objective of this work package of the 6net project. This work is very challenging because :

(1) No commercial integrated platforms exist today for managing IPv6 networks as compared to IPv4 available solutions,

(2) IPv6 introduces new functions (like auto-configuration, transition mechanisms, large scale network mobility, etc.) and it is not yet clear what specific management and monitoring functions have to be implemented for these.

(3) the 6Net is a very specific network that needs to support at the same time advanced operations related to new services experimentation together with normal operation and,

(4) because 6Net network must support extensive tests, it will be necessary to specify dedicated management procedures to this purpose.

Another challenge the management of the 6Net network will have to face is that the network will evolve very fast throughout the project from an almost completely experimental status to a full-fledged operational network with advanced service level quality. WP6 addresses all these challenges through various initiatives at all levels, from basic level instrumentation to high level business processes and interaction among management domain boundaries. This domument is buildt from the knowledge acquired by the various partners in managing IPv4 networks as well as their experience with various management platforms.

This document completes the first Management Architecture Specification document (D6.1.1) taking into consideration the first months of the network operation. It primarily focuses on presenting the components of a generic management architecture and the motivations behind those components and their interactions. It provides the description of the organisational and functional decomposition of the management of the network taking into account procedures already defined at the Core NOC level as well as all additional requirements emerging from the multi-domain, experimental nature of the network. The results of this work should be usable by any multi-domain IPv6 network.The document is organized as follows: Section 2 places this deliverable in the context of all other work packages. Section 3 defines the management functions that form the basic requirements towards the 6Net management architecture. Section 4 defines the various entities that contribute to the management of the 6Net network. It provides a first assignment of responsibilities and identifies the various interfaces that must be defined among the entities to perform efficiently the management and monitoring tasks. Section 5 provides a complete description of the different information flows inside the 6NCC and from/to external bodies. Section 6 goes into the details of the FCAPS operations which have to be supported by the platform. Section 7 summarizes the different phases through which the management organisation will go and which services it will integrate. In section 8, a brief status of current standardisation activities around the management of IPv6 networks is given. Section 9 is the conclusion of this document.

2   Relationship to other deliverables and work packages

Management is by nature an activity transversal to all other activities in the design, deployment and operation of a network and the services offered over this network. In the context of the 6Net project this means management related information will be found in all work packages and their respective

deliverables. Within WP6, the document has two main goals. First it aims at providing a global view of management architecture and requirements thus collecting all management aspects spread among other deliverables. Based on the knowledge aquired through the global view, a second goal is also to propose alternative management approaches and thus architectural evolutions of solutions or rules defined elsewhere.

Finally, new technologies – ie. Transition mechanisms, IP mobility, ...- may have their own requirements in terms of network or service management and monitoring. Therefore relevant WPs will be asked to provide us with this information so that an appropriate evolution can be proposed and performed.

The policy taken by the editors of this document towards content found in other deliverables is as follow : whenever the proposed procedures are supported by the current architecture, we explicitly refer to the location of these procedures in their respective deliverable (e.g. [5] for test management) rather than rewriting the entire procedure in this document. All additional information related to management requirements and procedures not defined in other WP deliverables are detailed in this document. To retrieve the complete information about network management architecture and operational procedures, please read the relevant cookbook, provided as a separate deliverable (D6.3 series).

3   General management requirements and information flows

Within this section, we define the requirements that are expected to be fulfilled by the 6Net envisioned management architecture. These are initially based on both benchmarking principles defined in [1] and management functions defined within the TeleManagement Forum with additions that are specific to the 6Net environment and its operational context, e.g. test planning, scheduling and performance.

3.1   Customer care

A unique access point must be provided to 6Net partners for interactions related to the operation and usage of the network and related services.

Due to the nature of the 6Net network, an entity responsible for the network and its management had to be created, involving some representatives, partners of the project. The 6NCC (6Net Network Coordination Center) has this responsability and is fully described in section 4.2.1.

This defines a two way information flow over which the following functions will be performed:

- Partner to 6Net management entity (6NCC) :
  - o   submit trouble reports including hardware failures,
  - o   submit change request,
  - o   submit test requests,
  - o   request for assistance,
  - o   request for information.

- 6Net management (6NCC) to partners :
  - o   proactive notification of planned network outages and changes,
  - o   notification of network failures,

- o answer to problem reports and change requests,

- o dissemination of detailed trouble tickets to concerned partners,

- o propagation of network status and configuration,

- o proposals for test set up and performance,

- o response to requests for information.

The above functions and tasks are those typically provided by the Customer Care function that needs to be made available within the 6Net management architecture. In the context of 6Net and especially in the area of network management the Customer Care function also holds a specific role in being used to enable partners to gain knowledge about how to manage such a network. This specific interaction will be detailed in section 5.4 of this document.

3.2 Publicizing Network management data

While network management is essentially oriented towards the users and customers of the network , data and information flows related to the operation of the network (e.g. usage statistics) are almost never made publicly available.

Within the 6Net WP6, like in other similar networks, the issue has been raised on whether network statistics should be made available outside the project or not, e.g. on a public Web page like it is done for the IPv6 Pilot in France [6] or for the Abilene IPv6 backbone [2]. This information can be very useful to present to the outside world the "life" of the network and the applications available for reporting and managing the network.

Providing a simple access to network statistics is recommended and selected as one of the management functions to be provided by the 6Net management framework. Thus the architecture must offer statistics collection services and securely disseminate them to appropriate components under the responsibility of the other WPs (e.g. WP7 for the public interface).

3.3 Operations support

Each part 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 to day operation of the network. It is responsible for the following services :

- Problem Management :
  - o collect trouble reports from 6Net participants,
  - o disseminate and archive outages information via a trouble-ticket system,
  - o track discovered faults,
  - o report discovered faults to impacted entities and appropriate bodies,
  - o resolve problems,
  - o disseminate procedures used to track and resolve the faults,
  - o notify resolved problems to the concerned parties.

- Configuration management :
  - o maintain an accurate configuration of every equipment of the network,

- maintain an updated set of maps of the current network topology, links status, etc.

- provide all necessary information that a partner can easily set-up the necessary hardware and software to connect to the network,

- plan and record software updates of the network,

- maintain software version control and history,

- manage name and address assignments.

- 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 the test as been completed

  - if specific measurement requirements 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 equipments and software and disseminate them on web pages if possible,

  - observe availability and performance of required network functions (e.g. DNS, routing daemons, ...)

- Security management :

  - ensure limited access to network components (access control and authentication)

  - provide authenticated means of collecting statistics from devices (SNMPv3 is one way of offering this facility),

  - provide authentication between network components (like BGP MD5 authentication)

  - set up tools to detect dynamically and protect against malicious attacks.

- Changes management :

  - while being part of the configuration management function, management of every change has a major role in the 6Net management architecture. In fact, due to its experimental nature, software changes are expected to occur on a much higher frequency than in standard networks. Hardware changes are also part of this function.

All these management services apply to both the network and related services (routing, DNS, etc.) Network operations support will be available under the same conditions as those defined for the core network by the NOC (see [4] for the details). These services will be further detailed in the context of the 6Net management architecture and related functions in section 6.

Concerning security management issues, the architecture will rely on the guidelines issued by WP3 as part of their work on the network security. As soon as the deliverable concerning this issue is available within WP3, the current text will be updated to check which features will be supported by the management architecture. Then implementation of these security recommendations – or a subset of - will be achieved.

3.4 New functions and protocols management

New functions (mobility, transition, multicast) will be installed, tested and made operational within the 6Net network throughout its lifetime, as soon as the standardisation process reaches a steady state. The 6Net network management architecture must provide support for these new services in terms of monitoring and management. This support includes :

- configuration and maintenance of the functions,

- monitoring and reporting for the services,

- definition of the management requirements for these functions in coordination with the concerned work package leader,

- study the impact of these functions on the existing management environment,

- provide management procedures and technical solutions to the addressed service.

It is the responsibility of those in charge of the management and development of 6NET to co-ordinate this activity and to contribute to the integration of these network functions within the set of managed entities. For example, when considering the deployment of mobile-IP support one has to consider in addition to the system update and deployment strategy, the services that need to be provided to monitor the activity of this service, the procedures related to trouble reporting, the statistics that need to be collected, MIBs to be implemented and so on. Establishment of this list, and implementation of related management components will be done in coordination between the 6Net management team and the WP leader responsible for the targetted service.
According to these needs, the management organization must also be able to evolve and change according to the specific functions needs.

4   Management domains and participating entities

Within this section, we identify the various components of the 6Net management environment, we define their roles in the management process and identify the interactions that must be defined.

4.1 Management domains

The 6Net network is divided in three main components (see figures 1 & 2):

- the backbone, composed of the 6Net core routers,

- the NREN networks,

- the 6Net partners, connected to 6Net via their National Research and Education Network.

This composition is illustrated in Figure 1 with the core network, the various NREN networks and the 6net partner networks (called CSite in the picture). External (EXNET) networks can be directly connected to 6Net via NRENs. The management of these links is under the responsibility of the concerned NREN.
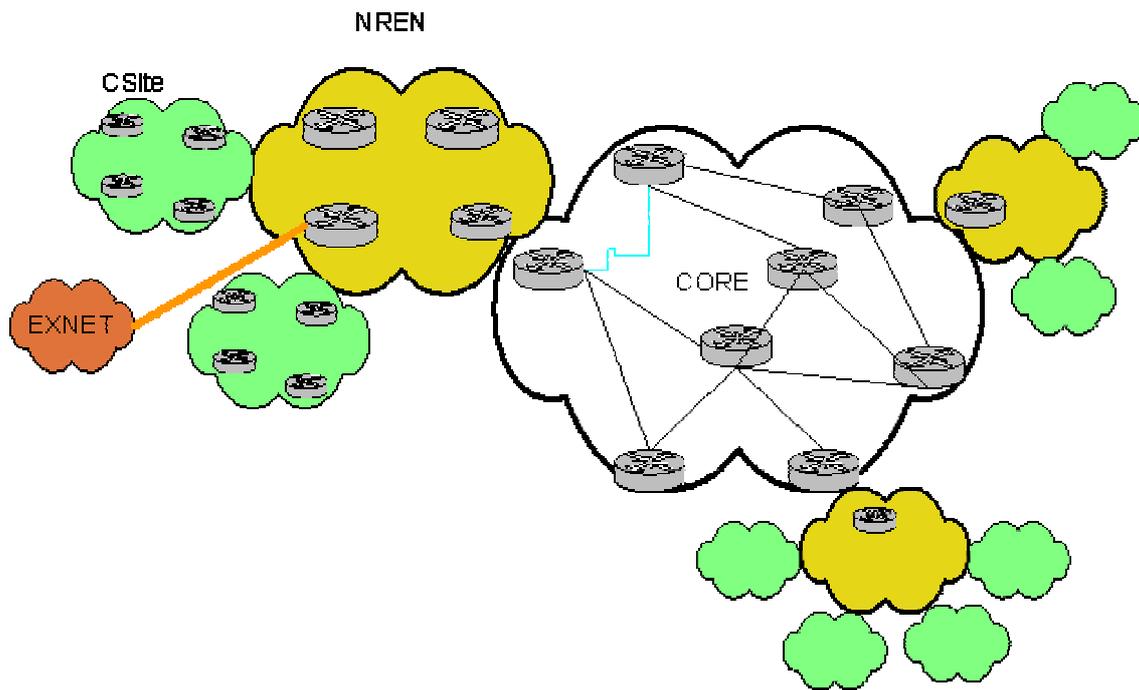
Figure 1: Network partitioning

From a management point of view, access routers to the 6Net play a specific role in the architecture. They are illustrated in figure 2 and belong to the so-called access area.
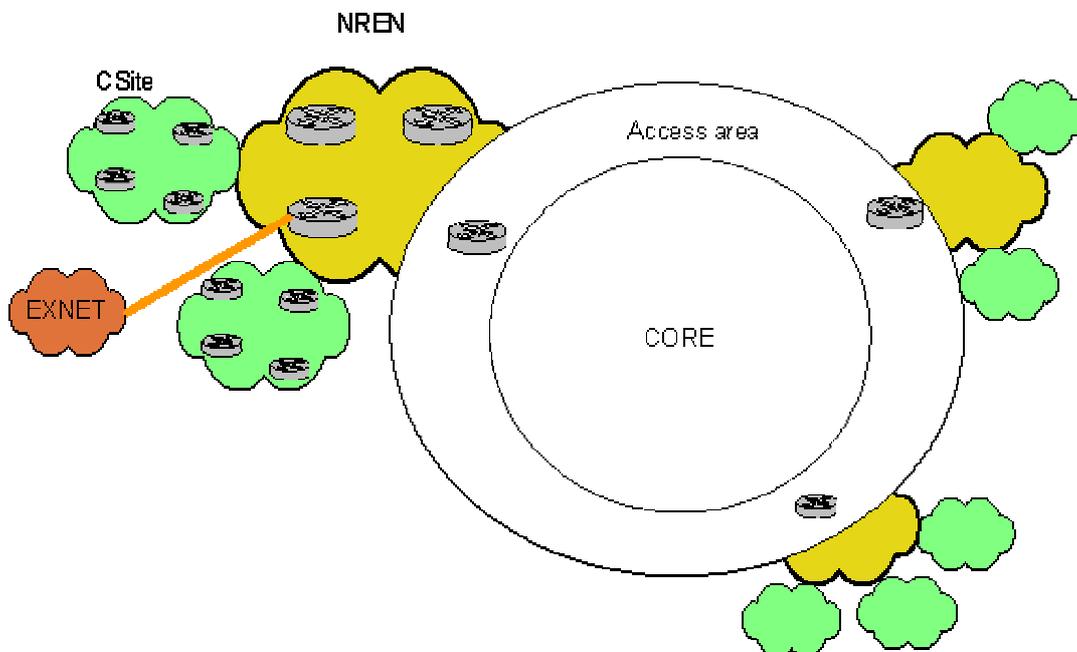

Figure 2: Access area components

Based on the above logical network distribution the management domains will, for the basic management services, be defined to match the physical boundaries across contributing networks. According to this statement, management domains are:

- the management domain covering the 6net backbone, formed with the PoP routers of the core,

- one management domain for each NREN including the corresponding access router,

- one management domain for each partner site beyond their respective NREN.

The access area is not in itself a specific management domain. However in this area, information exchange between both 6NOC –the entity responsible for the core management- and the NREN NOCs is required. A read-only access to statistics and configuration information needs to be provided on relevant interfaces.

4.2   Managing entities and information flows

This section describes the different entities involved in 6Net management.

4.2.1   6Net Network Coordination Centre (6NCC)

The 6NCC (6Net Network Coordination Center) is a federative structure gathering 6NOC and 6TAC and other participants. The 6NCC should act as a coordination entity responsible for the network and service management decisions related to 6Net network and services. Its composition is illustrated in figure 3.
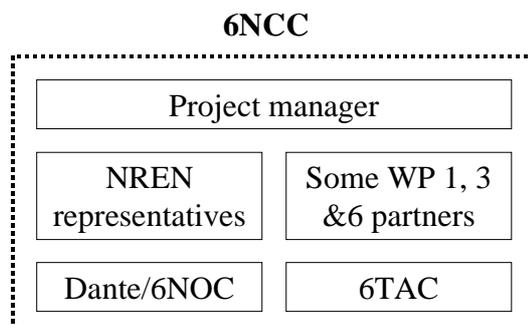
6NCC

Project manager	
NREN representatives	Some WP 1, 3 &6 partners
Dante/6NOC	6TAC

Figure 3: 6NCC components

As illustrated in figure 3, the following entities are involved in the 6NCC :

Entity	Represented by	Primary function
Project manager	CISCO	Responsible of 6Net project
6NOC	DANTE	Day to day operation and control
NRENs	Representatives	In charge of transferring their management experience in the 6Net project to their respective NREN NOC.
6TAC	Cisco TAC	Technical support for the 6NOC for software and harware related issues
Some WP1, 3 & 6 partners	Some WP1, 3 & 6 partners	Design the overall management architecture, provide operational procedures for each stage of the network, select and produce appropriate tools for monitoring, reporting ... implement and validate these tools (subset of, at least).

The 6NCC has the following main roles:

- Discusses all processes which cross management domain boundaries or involve several entities

- Discusses and validates the operational procedures submitted by WP6

- Discusses and validates any change of the network (IOS, topology, hardware) submitted by WP1 or WP3

- Discusses and validates tests preparation and scheduling

- Informs the partners about the current state of the network

- Provides access to all information related to management to the 6Net partners,

- Proposes which management information can be made available outside the project and, in coordination with WP7, provide the necessary tooling to enable this information availability.

- Overall, its role is to be the regulatory body for all acting entity activities in the 6Net management (6NOC, 6TAC, etc.).

The *6ncc@6net.org* mailing list is a closed list (limited to the ncc participants) provided for intra NCC communication.

4.2.2   6TAC

The Cisco Technical Assistance Center (TAC) [7] provides the technical support services for the Cisco products and technologies to all Cisco users. It treats submitted cases according to a 4-level priority model (from a severe network degradation case to a request for configuration or technical issue with no or little impact on network operations). The TAC also provides many technical information online which provides direct responses to most low priority level problems. Additional information concerning the TAC can be found at http://www.cisco.com/tac/ .

In the context of the 6Net project it has been agreed the 6TAC support is available only to the 6NOC as a second level support.

4.2.3   6NOC

The detailed management procedures related to the 6Net NOC are provided in Deliverable D.1.2 [3]. In this section we briefly summarize its goals and obligations.

In view of the management boundaries it is agreed for the 6Net project that the 6Net NOC will be responsible for the core network. That means it is not responsible for the end to end connectivity (it's not a global NOC) but for all problems, which are related to the core. For the NRENs whose access links have been ordered by DANTE, it is the responsibility of the 6NOC to solve the problem together with the carrier in case of link outages.

4.2.4   Network Operation Centres

In order to define the respective roles and interactions between the domains, a network operations center is associated to each managed domain (see figure 3):

- the 6NOC ensures operations support for the domain that covers the IPv6 backbone (described in the previous section) or core domain,

- the NREN-NOCs provide the operations support for the NREN network,

- the Partner NOC is dedicated to the management of one or more customer networks.

Each NOC has full management authority over its domain. Access across domains is specified on a peer to peer basis. This applies to the interfaces of the routers of the access area and the core POP routers.

As proposed above, this organization has the following advantages :

- it allows every domain to implement its own management and monitoring architecture, functions and tools….Each domain can use its own and/or shared tools and procedures and thus a broader set of management tests can be performed and more tools can be experimented and validated,

- it builds on a known management architecture, thus facilitating the initial set up of a management environment,

- it facilitates future transition of the network to an operational phase by already having authoritative separation.

It also has the following limits :

- management domains are not necessarily based on technical ones (e.g. multicast management may require a domain that spans all the above defined administrative boundaries),

- it requires more interface definitions than a flat architecture to enable end-to-end management of network services (domain boundary interfaces).

The management architecture group also recommends that, for specific services such as multicast and transition mechanisms, the logical organization of domains may be redefined for operational purposes and thus that the above defined architecture be open enough to enable a service specific domain decomposition as already expressed in the previous section.

4.3   Cross-domain information access policies

Monitoring facilities and read only access to network element configuration and/or state may be required in various situations, e.g. problem tracking or performance monitoring. Each time this need

appears, a mutual read-only access to the specific data will be provided on a peer-to-peer basis. Cross-domain access will be provided through looking glass services.

This facility has the advantage of providing almost all information other parties could need without direct access / connection to the equipment. Thus administration is simplified and security enhanced.

5   Information flows and Management interfaces

We can identify different management information flows relative to different actions:

- Problem reporting
- Problem handling
- Network change/test requests
- Request for information

5.1   Problem reporting

When a 6Net partner has any problem related to the network, he should be able to report it someway so that the problem can be solved. This part details the procedures to report a problem to the 6Net NOC (6NOC). We can identify two major phases during the project that are leading to 2 different approaches for reporting a problem.

5.1.1   Before the NREN-NOCs are IPv6 trained

At the time the 6Net project started, almost all the NREN NOCs were not IPv6 trained and no NOC was able to treat any request related to IPv6. One of the missions of 6Net project is to train the NOCs to IPv6 so that they are prepared for their future role concerning IPv6 management. The training organization is part of WP7 activity and the training content will be prepared by all relevant workpackages.

The following scheme gives the different management information flows related to problem reporting, when the NREN NOCs are not yet IPv6 trained.
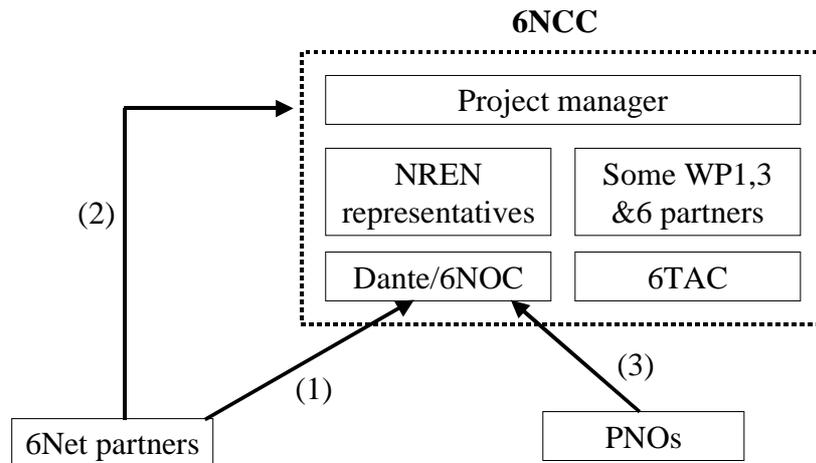
Figure 4: Problem report (phase 1)

1. Problem report from a partner

During this first phase, every 6Net partner is allowed to submit a problem to the 6NOC using the *trouble@6net.org* mailing-list. This corresponds to the interaction (1) on the scheme above. Before doing this, the 6Net partners have the responsibility to check that the problem really comes from the 6Net core. For this, the partners can use the facilities provided that makes it possible to see the current state of the network (e.g. looking-glass)

2. Escalation process

If the 6NOC does not resolve the problem, and the 6Net partner feels like no real action is taken by the 6NOC, then the 6Net partner can submit the trouble to the 6NCC using the 6ncc@6net.org mailing-list. This escalation procedure is shown by interaction (2) on the figure 4.

3. Problem coming from a PNO (Public Network Operator)

The PNO can schedule some outages and encounter problems. They have to contact 6NOC every time there is an interruption of service. For this purpose, the PNOs can use the *trouble@noc.6net.org* mailing-list. This is the interaction (3) on the figure 4.
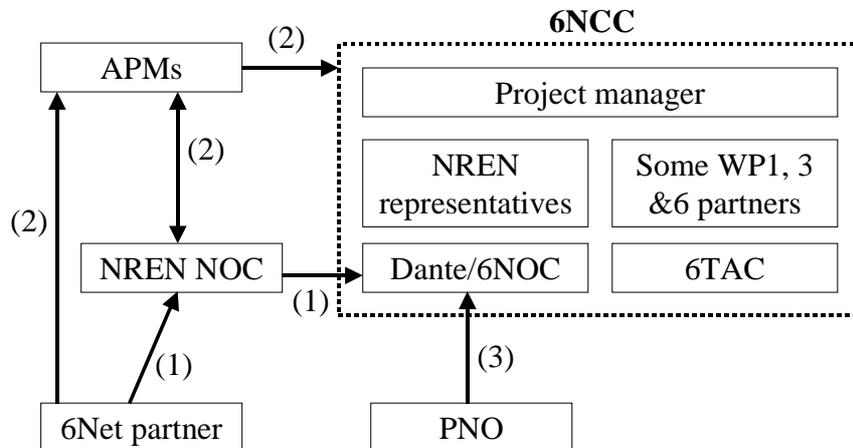
5.1.2 The NREN NOCs are IPv6 trained

Figure 5: Problem report (phase 2)

1. Problem report from a partner

After the NREN-NOCs are trained, then the partners have to submit any trouble to their NREN NOC. The NREN NOC can submit then the problem to the 6NOC if the investigation performed clearly showed that the problem comes from the 6Net core. For this, the NREN NOC must use the *trouble@6net.org* mailing-list. This process correponds to the flow (1) on the figure 5.

2. Escalation process

The other mission of the 6Net project is to ensure that people responsible of the NRENs can understand all the actions related to IPv6 and take their decisions and actions accordingly as they already do for IPv4. It is not suitable to have different APMs for IPv6 than the already existing ones for IPv4.

If the 6Net partner receives no information regarding his problem report, or if the problem handling takes too much time, or overtakes the NREN-NOC responsability, then the APM can be asked to handle the problem report as an escalation process. Then the APM can contact directly the 6NCC using the *6ncc@6net.org* mailing-list. This escalation process is shown by interaction (2) on the previous diagram

3. Problem coming from a PNO

The same situation than in § 5.1.1/3 applies. PNOs must contact 6NOC every time there is an interruption of service. For this purpose, the PNOs can use the *trouble@noc.6net.org* mailing-list. This is the interaction (3) on the figure 5.

5.2 Problem handling

Problem handling is resulting from a problem reporting. The following scheme shows the different management information flows related to problem handling.
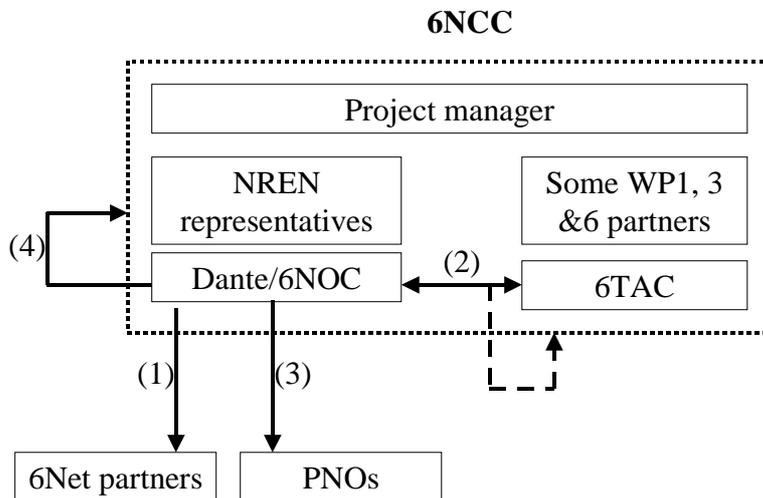
6NCC

Figure 6: Problem handling

Three different flows can be identified corresponding to different situations that can occur. When receiving any problem report, the 6NOC has to open a new trouble ticket. This trouble ticket will be updated while the problem is solved. Each time a trouble ticket is open, closed or modified, the *tickets@6net.org* mailing-list has to be informed. When the NOC foresees an outage, it has to open a ticket at least three days before so that the partners can schedule their tests on the network accordingly.

1. Informing the 6Net partners

When a trouble ticket is open, updated or closed, the 6NOC has to inform the project partners. This is done using the *tickets@6net.org* mailing-list. Only the 6NOC is allowed to send an email to this list.

All the 6Net partners are automatically subscribed to this mailing-list but can ask to be removed.

2. Difficulties to troubleshoot the problem

This is the only interface between the 6Net management entities and Cisco services. It is used by the 6NOC to report and invoke Cisco technical support every time a problem needs the 6TAC assistance. No interface to the 6TAC is available outside the 6NOC.

There are 2 channels to contact the 6TAC : a phone line and a Web (Mail) access.

The phone access number is already known by the 6NOC

Online case submission has to be done at the following URL : http://www.cisco/com/tac/caseopen

To open a case, the 6NOC must provide following information:

- the service and support contract number **(known by the 6NOC too)**

- the serial number of the product which is supposed to expose a failure,

- the network topology and the detailed problem explanation,

- relevant output information collected from the device,

- software version and types of equipment.

Based on this information, the 6TAC starts its internal procedures to solve the problem. The submitted case can go through 4 states :

- pending (problem currently under investigation at the 6TAC),

- closing (the 6TAC provided a solution. An assigned engineer can be contacted if doubt remains on the trouble),

- customer pending (information has been required by the 6TAC from the 6NOC or directly from the APM/partner and the 6TAC is awaiting a response),

- development pending (6TAC has submitted a development engineering request and forwarded it to Cisco Development Engineering for investigation).

Every time the 6TAC is invoked, the 6NCC has to be informed of the difficulties that the 6NOC encountered and the solutions provided by the 6TAC. This is done simply by adding the 6NCC mailing-list (*6ncc@6net.org*) in the 6TAC alias.

This management information flow is shown by the interaction (2) on figure 6.

3. Problem involving a PNO.

In this case, the 6NOC contacts the involved PNO to take the appropriate actions. This is the interaction (3) on the diagram of this section.

4. Problem that cannot be solved by the 6NOC

If the problem cannot be solved by the 6NOC, because it is not its responsibility, or needs a more general discussion, then the 6NOC has to inform 6NCC about it. This is done using *6ncc@6net.org* mailing-list. This is the interaction (4) on the figure 6.

5.3   Network change/test requests

This section explains the procedures to be followed to submit a network change request, or to ask for a test on the core network equipment(s).

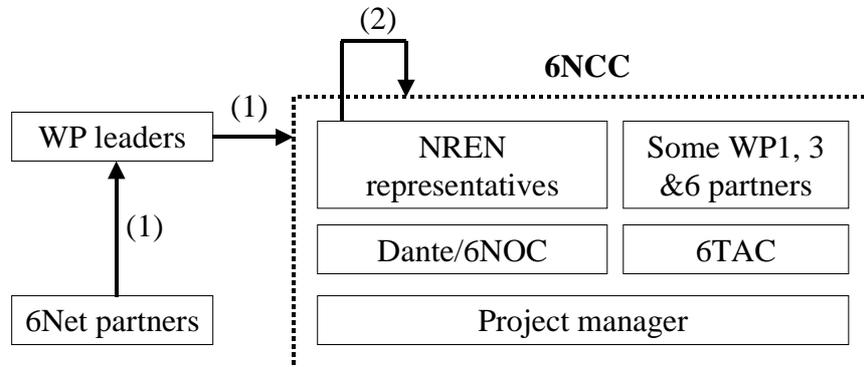Here is the scheme that will be explained in this part.

Figure 7: Network change/test request

1. Request from a partner

We can identify 3 types of request represented by interaction (1) on the diagram above:

- *Network change request*. When a partner (or a group of partners) requests for a change on the 6Net backbone (like a software upgrade, or a change of configuration)

- *Test request*. A partner can also ask for a test timeslot on the 6Net core.

- *Management procedure request*. There will also be management procedures for the 6NOC that will be submitted by 6Net WP6.

These requests must be done to the appropriate WP leader, responsible for transmitting it to the 6NCC using the *6ncc@6net.org* mailing-list.

The 6NCC then decides during meetings or via the mailing-list the relevance of the requests and notify the requester with the final decision.

2. NREN requests

Most of the time, the network change requests will come from the NREN, that have facilities to test software and hardware equivalent to the ones used in the core. The NREN representatives can ask for changes directly to the 6NCC mailing list (*6ncc@6net.org*) as shown with interaction (2) on the figure 7.

Action following a request

After the request from the 6Net partner has been discussed and is accepted by the 6NCC, then the 6NOC is asked to perform a set of actions by the test coordinator. This is done using the *trouble@6net.org* mailing-list. This is represented by the interaction (3) on figure 7.

5.4   Request for information

The identities involved in 6Net project (6Net partners, PNOs, NRENs etc.) can ask for information about the 6Net network (configuration tips, IOS versions, hardware specifications, etc.)

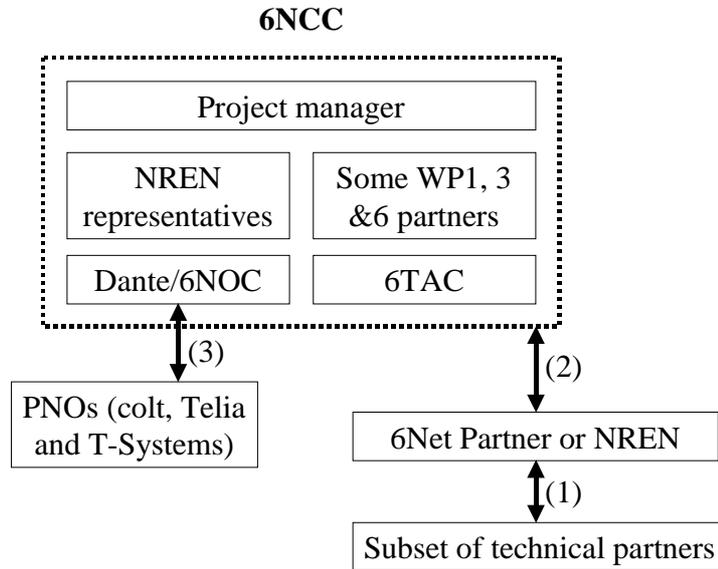This section describes the different management flows to achieve this action.

6NCC

Figure 8: Request for information

1. Request from a 6Net partner or NREN for general technical question

When a 6Net partner or NREN needs information about configuration tips, it can contact a subset of technical people volunteer for helping people debugging some situations using the *advice@6net.org* mailing-list. Then the people on the list will answer directly to the partner or NREN. This is the interaction (1) on the scheme above.

2. 6NCC - 6Net partners interaction

When a 6Net partner (which can be an NREN) needs information needs information about the network configuration and evolution, it has to check on the 6Net web page if the information is published in the network section (see section 5.6 for this). If no relevant information is found, then the partners can contact the 6NCC using the *6ncc@6net.org* mailing-list. Then the people on the list will answer directly to the partner. The 6NCC can contact directly every partners in case it needs. For this purpose it sends an email to the *technical-leaders@6net.org* mailing-list. This is the interaction (2) on the figure 8.

3. Request from a PNO

If a PNO needs information, it can contact the 6NOC using the *advice@noc.6net.org* mailing-list. The 6NOC answers directly to the PNO as shown by interaction (2) on the figure 8.

5.5 Mailing-lists reminder

- trouble@6net.org : is only dedicated to report operational problems. This list is ready and should be used by every 6net partner as long as 6Net APMs have been nominated and have their own communication mean.
- advice@6net.org : is relevant for all other needs of information about the 6Net network (configuration tips, IOS versions, hardware specifications …)
- tickets@6net.org : is a mailing list used by the 6NOC to inform the Consortium about a specific problem management. No one else is allowed to send email to this list.
- trouble@noc.6net.org : is a mailing-list used by the PNOs to report to the 6NOC operational problems.
- advice@noc.6net.org : is a mailing-list used by the PNOs to request the NOC information about the network.
- 6ncc@6net.org : is used to contact the 6NCC. It is not private mailing-list but should be used only in the cases described in this chapter.
- technical-leaders@6net.org : all the partners of the 6Net project.

5.6 Other interactions between the 6NCC and the project

This section gives a general overview of the interaction existing between the 6NCC and the rest of the 6Net project
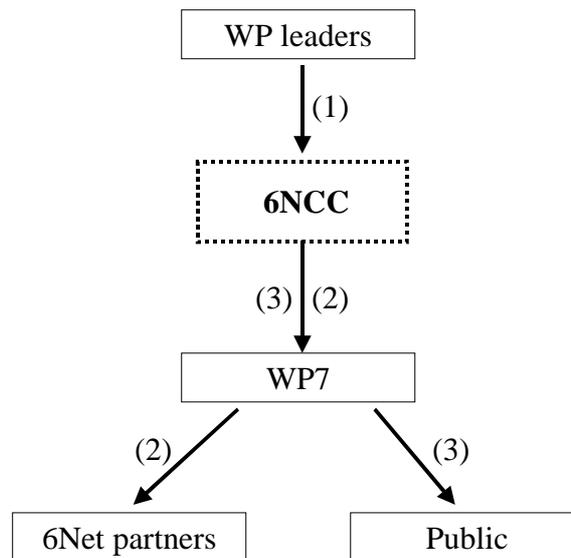

Figure 9: Interaction between 6NCC and the project

1. Requests to the NCC

These requests (like change or tests requests described in the section 5.3) are coming from the WP leaders to the 6NCC using the *6ncc@6net.org* mailing-list. (interaction (1) on the scheme above)

2. Provide information to the project partners

An important mission of the 6Net project is to let the partners (and if possible everybody) know what is the state of the network (software and hardware used, tests being performed)

6NCC has to provide some content to WP7 for this purpose and WP7 has to disseminate it to the appropriate people using regular communication schemes (mailing-list, 6Net newsletter, private or public web site...) This is interaction (2) on the scheme above.

3. Provide information to the public

Another goal is to let everybody know some particular information about the network. The 6NCC will have to provide to the WP7 some public information and WP7 will be in charge of disseminating it, using the appropriate medias (web site, 6Net newsletter...). This is interaction 3 on the figure 9

6   Additionnal management functions details

6.1   Configuration management

In addition to the standard functions related to configuration management, a network map needs to be provided offering following features :

- Layer 2 and layer 3 connectivity,

- Connectivity status.

6.2   Accounting management

While accounting is not the major topic within the project, continuous measurement of usage statistics is useful and existing tools will be adapted to this end.

6.3   Security management

In coordination with the security policies and services that will be defined in WP3, the network management strategies and procedures which enforce these policies need to be defined. For example, if only limited routes announcements are allowed on the network, the monitoring service of the management framework needs to regularly dump the routing tables of all 6Net routers to check that their content is consistent with the security policy in force. Within the architecture, only secure access to network equipment can be allowed. Additional security policies will be set up in the architecture as soon as they are fully specified within WP3. The detailed policies will be included in the cookbook.

6.4   Problem management

Problem handling defines the process that is executed when a fault is detected on the network. The detection itself can be either through an incoming problem report through the problem report procedure or through an incoming alarm or monitoring activity. In both cases, the detected problem enters the trouble-ticket system and is distributed to concerned partners as described in section 5.

6.5   Test planning and execution

Due to its experimental nature, enabling tests to be planned and performed over the network by various work packages is a major requirement towards the management activity. Since tests can have many impacts on the network behavior, they must be carefully planned and provide a clear structure of the actions before getting executed.

The activities linked to test management are under the responsibility of the 6NCC in strong coordination with the 6NOC and Cisco Professional Services. 6NCC is responsible for the scheduling of the tests and tracking the evolution from test procedures submission to their effective execution and reporting.

The procedure defined within the 6NOC is described in details in [5]. While protocols are standard targets for tests, management components and software components are also subject to test in the 6Net framework. Such function may require an additional degree of openness of the network like full Read-Write access to variables of the SNMP agents under test within core routers. These scenarios must be supported by the test function.

6.6 Transition management

The deployment of transition mechanisms will generate specific requirements towards the management of the network. These mechanisms need to be supported by the platform, e.g. having both IPv4 and IPv6 SNMP agents and access to management information. The transition mechanism for the management purposes (SNMP) is being performed within the work package 6 of the 6NET project and described in [8]. The details of the requirements towards the management architecture concerning other transition mechanisms will be defined in coordination with WP2.

The transition mechanism for the management protocol implemented as the "SNMP Transition Tool" will cause some additional requirements for other management tools and platforms concerning their network configuration. E.g. an IPv4 SNMP manager will access IPv6 network devices using the set of predefined IPv4 addresses. All these IPv4 addresses have to be configured on the IPv4 network interface of the transition tool system. It is suggested to use the IPv4 addresses space for private internets (10.0.0.0 - 10.255.255.255, 172.16.0.0 - 172.31.255.255, 192.168.0.0 - 192.168.255.255) on the transition tool system, but it is not mandatory. Notice that using the IPv4 addresses for private internets requires valid routing of these addresses between network management station and transition tool proxy server. The case of transition of IPv6 to IPv4 is similar to the transition of IPv4 to IPv6, but the IPv6 address space is sufficient enough. Another requirement for network management tools which will use the SNMP transition mechanism is the need for the reconfiguration of the DNS service for SNMP managers. It can be done by adding to the DNS server the appropriate IPv6 addresses representing the network devices from the IPv4 environment and the IPv4 addresses assigned to the IPv6 native devices. It is not a obligatory requirement but it will be very desirable for the users' convenience.

The SNMP Transition Tool will be tested under the Linux environment for the interoperability with existing network management platforms and various tools mentioned in [9]. The results of these tests can produce some additional demands towards the management architecture which can not be expected today. These new requirements will be included into the future revisions of this document if needed.

6.7 Mobility management

Like for management entities related to transition or security, mobility will provide additional management requirements. A request is made to the WP dealing with mobility to define those requirements that will be evaluated towards the hierarchical multi-domain management architecture of 6Net.

6.8   Universal functions

Monitoring and reporting are standard functions used in almost all FCAPS areas. In this section we define their usage in the specific context of the 6Net network management architecture.

6.8.1   Monitoring

Monitoring of equipment status and several network statistics need to be performed. Moreover the architecture needs to support proactive Service Level Agreement monitoring since this feature is one of the major requirements in todays networks. An important part of the monitoring environment is the recording of collected data. Within the 6Net management architecture, a service dedicated to monitoring data recording and access is required . Grouping and nature of collected data is still open for definition, e.g. per NREN, per user, per service, ... Note that this data access is very important for enabling reporting (see next section) as well as for providing data collected during a test execution for offline analysis.

6.8.2   Reporting

Reporting is a major feature regarding the life of the 6Net network and a strong requirement is made on pushing as much information as possible in reports related to the network.

First of all, reporting is used to inform about the processing staus of trouble submissions. In the context of 6Net, this reporting channel will contain much more data than today's standard trouble tickets. Especially, it is required that the firt trouble-ticket issued in response to a trouble report contains the complete data (text and attachments) that was in the original trouble report. This enables both 6NCC partners to contribute to problem solving and to acquire knowledge in the processing of troubles in the IPv6 network, knowledge acquisition required for the second phase of the 6Net management where NRENs NOCs will be in charge of managing their part of the 6Net network.

Reporting is also used to transfer results of test campaigns.

6.8.3   Out of band or prioritized access to 6Net routers

Remote access to an equipment is often necessary in case of network outage. To enable management operations to operate when the network runs in a degraded mode, two facilities are recommended by the management architecture group :

- All equipment must offer an out-of-band access to enable remote management when in-band secured access is not possible. This can be via a modem connection, or any other channel outside the normal in-band vehicle. This feature is already planed for the core routers (see [4], section 4 pp 24). In the global management architecture, this must be extended to access routers as well.

- Network offers a prioritized access to part of the management traffic.

7   Management phases

The network must be managed from the beginning. To this end, both basic monitoring and configuration interfaces need to be available before the first traffic occurs. In the initial phase (initial deployment), IPv4 based management solutions will be supported. In a second phase, the management platform must integrate the management of all basic services. In a third phase, test planning, transition and value-added services will be integrated in the management platform. By the end of the project, all management tools used must support native IPv6 functionality.

This three-phase approach is also setup concerning the involvement of NREN NOCs and customer sites in the management of the 6Net network. As already described in sections 4 and 5, the initial management of the network is under the responsibility of the 6NOC, while in the second phase, operations related to access routers and services will be delegated to each NREN willing to perform management on these functions. Within the third phase universities and participating organizations will be allowed to contribute directly to the cooperative management with their local NRENs.

These three phases and their impact on the mailing lists and information exchange are depicted [3] (version 6).

8   Standardization issues

Standardization plays a major role in delivering management interfaces to management applications and protocols. While the management architecture described in this report does not depend on any specific management protocol or approach, several interfaces and/or management information will be available only if they can be accessed through a standard management interface. The possible standards are SNMP, COPS provisioning and/or outsourcing and WBEM for the most probable ones and OSI CMIS or CORBA IDL for some telcos.

Of major interest to standard platforms integration is SNMP. The introduction of IPv6 was initially (back in 1996) treated in the management community like any other new protocol in the SNMP community, namely it was under the responsibility of the group that defines the protocol to come up with a MIB module that provides the information model describing the management view of the new protocol. This process was followed by the group that defined IPv6 and led to the information model defined in [RFC 2465]. The outcome is a portion of MIB-2 that provides the instrumentation of IPv6, ICMPv6, UDP over IPv6 and TCP over IPv6 that is compatible with the 128 bits size of IPv6 addresses.

To avoid multiple incompatible representations of IP addresses. An IPv6 MIB Revision design team was formed within the IETF IPng working group. The first challenge this working group had to face, was to define a textual convention for IP addresses that was generic enough to represent all types of existing addresses namely IPv4, IPv6 and DNS names. This new representation of network layer addresses has been initially published in [RFC 2851] and has been regularly enhanced to finally leed to [RFC 2851U6]. This specification which has recently been accepted to enter the standard track provides both a specification for generic internet addresses in MIB-modules and a set of guidelines on how these components should be used in new MIB modules.

Based on this new representation, a revision of all MIBs using IP addresses is necessary. This was first done for MIB-2 and led to a couple of drafts for ICMP, IP, TCP, UDP and Forwarding Table. Now, this has to be done for all MIBs and propagated to all implementations. This may take some time to be achieved and in the early stages of 6Net, the most common access to management information will be through the command line interface.

9   Conclusion

6Net is a wide international IPv6 network built mainly by a lot of academic organizations, therefore it is an open network in term of experimentations, tests an trials. Its design should be able to evolve quickly and more or less all along the project life. Then, the 6Net network management activities are very challenging and attractive. Because almost all scenarios are possible in such a network, management boundaries can be set up for some services in a conventional domain approach whereas other services should be built in a more transversal way : for multicast management, for

instance, the Rendezvous Point and groups management cannot deal with the domain management approach. Multiples frameworks will be used and combined to be able to provide an adaptive management facility being needed by all activities and services implemented during the 6Net project life.

This deliverable focuses on the management architecture description, taking into account the first months of the operational status of the 6Net network. In this management architecture, the 6Net Network Coordination Center (6NCC) is the masterpiece of the overall organization. It is a federative entity and information interfaces between these 6Net components are described in details. It is specified too who can contact the 6NCC and for what purposes, referring to the evolutionary status of the ability of the external entities regarding IPv6 operation and management. The 6NCC implementation is the result of a year of 6Net operation, showing a centralized and federative structure is needed to perform an efficient coordination among all operation activities. To this respect, the 6NCC is also a discussion forum for all technical issues related to network operation, and evolution. It is proposed that the 6NCC becomes the place where tests and trials are discussed and scheduled before being implemented by the 6NOC.

If the 6NCC concept is discussed, regularly presented in 6Net meetings and encounters no formal objection, its implementation has to be achieved as an extension of the existing management architecture. It is a challenge that all related parties will have to face in the coming weeks/months.

10 Bibliography

[1] Terplan, K., Benchmarking for Effective Network Management, McGraw-Hill Series on Computer Communications, 1995.

[2] The Abilene Network Operation Center, http://www.abilene.iu.edu/noc.html

[3] 6NET Deliverable 1.2 : "Operational Procedures to be followed by 6NET NOC", april 2002.

[4] 6NET Deliverable 1.1: "Design and Implementation of the Testbed infrastructure", version 1.c, april 2002

[5] 6NET Deliverable 1.4: "Procedures for the approval and scheduling of 6Net tests", version 1.a, april 2002.

[6] Renater, "Renater IPv6 Pilot Service", http://sem2.renater.fr/

[7] Cisco, "Cisco Technical Assistance Center : Quick Reference Guide", http://www.cisco.com/tac

[8] PSNC "6NET WP6 SNMP Transition Tool Specification",

http://www.ipv6.man.poznan.pl/6net/6NET_WP6_SNMPTransitionToolSpecyfication.pdf

[9] 6NET Deliverable D6.2.1: "6NET Management Tools Requirements", June 2002