D23 - Report on Integrated Test Scenarios

Abstract

Deliverable D23 is a joint deliverable of work package 1 and work package 2. The possibility of mobilising synergistic effects between IST projects, which would produce Integrated Test Scenarios, is explored. For this purpose, a new survey among MOME Cluster projects was sent to projects. This document analyses the results of the survey and other related activities of work package 1 and work package 2.

Keywords

MOME, Deliverable D23, IST, Measurement Tools Database, Measurement Database

Table of Contents

Index of Figures

Index of Tables

List of Acronyms

BPF	Berkeley Packet Filter
GUI	Graphical User Interface
CLI	Command Line Interface
GPL	General Public License
IPFIX	Internet Protocol Flow Information Export
IPPM	Internet Protocol Performance Metric
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
MAC	Medium Access Control
NREN	National Research and Education Network
NSIS	Next Steps in Signalling (IETF Working Group)
OWD	One Way delay
QoS	Quality of Service
RTT	Round Trip Time
RTP	Real Time Protocol
SLA/SLS	Service Level Agreement / Service Level Specification
SLAC	Stanford Linear Accelerator Centre
SNMP	Simple Network Management Protocol
UWB	Ultra Wide Band
WP	Workpackage

Executive Summary

Deliverable D23 is the result of joint work of Workpackage 1 and Workpackage 2. Once the MOME database was implemented and launched (see Deliverable D22 [5]), the project has started to explore the possibilities of sharing measurement and monitoring activities and results between IST projects in what could be described as Integrated Test Scenarios.

An integrated OWAMP test was conducted, building on the lessons learnt in the MOME Interoperability Event held in Paris, France on 28-30 July 2005 (see Deliverable 13 [4]) regarding possibility of sharing measurement and monitoring tool development activities between projects. In this case, the MOME and EuroNGI projects brought together different research groups working on the one way active measurement protocol. In addition to checking the interoperability of different protocol implementations, the measurement results have been published and the corresponding entries in the MOME database were created.

In order to fully formalise an Integrated Test Scenario as a monitoring and measurement process, the concept of the measurement chain is introduced. Using this concept, MOME has conducted between September and October 2005 a second project survey, including an electronic mailing, requesting information about current and closed measurement and monitoring activities from IST projects. Identifying monitoring and measurement tools for wireless and IPv6 networking environments was one of the decisive issues, given their importance in the near future of the Networking World.

While the situation regarding tools for these environments is, generally speaking, good, it is not that encouraging regarding the availability of network traces for both environments. The main factors which explain the situation are:

- **technological:** research projects dealing with wireless communication in the IST realm are working on the physical layer (i.e. Radio communications). MOME is working at the IP layer.

- **legal reasons**: there is no legally sound framework which could give the researchers the confidence to publish the data without facing legal consequences (i.e. Violation of data privacy)

- **marketplace**: mobile operators monitor and measure their network, but these data are highly confidential, since they reflect the strengths and weaknesses of their network and could be used against them by competing operators.

This conclusions are corroborated by similar studies carried out by other projects (i.e. LOBSTER) in the past and shows the degree of progress achieved in the area. In order to better explore these limiting factors, a second questionnaire for Internet Service providers targeting their inter-domain measurement and monitoring activities was prepared.

The study unveils overlaps in different areas within the IST Programme, analyses the real benefits of such overlapping and formulates some recommendations for future programmes in order to foster and promote Monitoring and Measurement Activities and the exchange of measurement data among EU funded projects.

1   Introduction

The Monitoring and Measurement Cluster MOME has contacted a lot of research projects in Europe, which have some activities related to it.

One of the interfaces of the Monitoring and Measurement MOME Cluster to IST projects is through the MOME Database, which is accessible through the MOME Web page. This database was launched at the beginning of 2005. This database is a knowledge exchange point for experts in Monitoring and Measurement and has two sections, one dedicated to Monitoring and Measurement tools and one to traces. This database offers an interesting insight on activities in the area of Monitoring and Measurement in IST projects and outside them.

In the process of gathering significant data for the MOME Database, the project contacted projects from the IST framework. Through a questionnaire (See appendix A.1 "Questionnaire to IST projects monitored by MOME"), each project was asked about measurement and monitoring activities it conducted and the use and the final destination of the raw measurement data obtained by it.

In order to formalise the full monitoring and measurement process, the concept of the measurement chain (see chapter 2 "Monitoring and Measurement Chain") was introduced, which starts with the formal definition of the measurement (or monitoring) scenario. The scenario, in turn, defines the objectives. Finally, the objectives define which measurement or monitoring tasks have to be performed and which tools are needed to perform the measurements and to process the measurement results to meaningful data.

Using this concept, MOME has conducted between September and October 2005 a second project survey, including an electronic mailing, requesting information about current and closed measurement and monitoring activities from IST projects. The survey was crafted around the concept of the measurement chain. The results were sorted into four main categories:

- Tools
- Protocols
- Approaches
- Scenarios

In addition, a second questionnaire for Internet Service providers targeting their inter-domain measurement and monitoring activities (see appendix A.2) was prepared.

During the period of activities documented in this deliverable, WP1 and WP2 have concentrated their efforts in identifying monitoring and measurement tools for wireless and IPv6 networking environments. The results are quite encouraging, because a plethora of tools could be identified. The situation is not that encouraging regarding the availability of network traces for both environments. The main factors which explain the situation are:

- **technological:** research projects dealing with wireless communication in the IST realm are working on the physical layer (i.e. Radio communications). MOME is working at the IP layer.

- **legal reasons**: there is no legally sound framework which could give the researchers the confidence to publish the data without facing legal consequences (i.e. Violation of data privacy)

- **marketplace**: mobile operators monitor and measure their network, but these data are highly confidential, since they reflect the strengths and weaknesses of their network and could be used against them by competing operators.

This document is structured as follows:

Chapter 1 provides an overview of the document

Chapter 2 introduces an abstraction used to categorise measurement and monitoring experiments in the context of the MOME project known as the Measurement Chain.

Chapter 3 shows the integrated test scenario prepared by MOME and EuroNGI to test implementations of the One Way Active Measurement Protocol (OWAMP) and gather measurement data for the MOME Database.

Chapter 4 uses the Measurement Chain as the main tool to analyse the result of the survey made with the questionnaire sent to IST projects targeting their monitoring and measurement activities.

Chapter 5 analyses the current status of wireless measurement and monitoring scenarios in the world, showing the restrictive practices with regard to sharing traffic traces and the reasons behind them.

Chapter 6 gives an overview of the activities related to measurement and monitoring in the IPv6 world, including the different IPv6 specific traffic repositories.

Chapter 7 analyses the Interoperability Event held in Paris (see Deliverable D13 [4]) linking project participation in the event with the MOME Database.

Chapter 8 presents the conclusions after evaluating the questionnaire output and comparing it with similar activities in other projects (i.e. Lobster) and the different tests carried out by MOME.

Appendix A includes the questionnaires sent to IST projects targeting their monitoring and measurement activities and to Internet Service Providers targeting their inter-domain monitoring and measurement practises.

Appendix B shows the project by project results of the survey made with the questionnaire sent to IST projects targeting their monitoring and measurement activities. These results are used in Chapter 4.

Appendix C shows the freeware and commercial wireless tools referenced in chapter 5.

Appendix D lists IPv6 ready monitoring and measurement tools and the operating systems they run on.

Appendix E is the table of references.

2   Monitoring and Measurement Chain

"Monitoring and Measurement Chain" is the formal concept which will be used in this Deliverable to provide a common grounds to study and categorise the different measurement and monitoring approaches proposed by the different projects which fall under the scope of the MOME coordination action.

All projects which have to measure parameters of an IP network or monitor its evolution, do it with a specific scientific objective in mind. They also have to consider the networking environment they are going to observe with their measurements in order to determine which tools are appropriate and which are not. At this stage, a set of appropriate post-processing tools, which convert the measurement data into results which are significant for the project can also identified. The scientific objective and the networking environment will determine the measurement scenario which is more appropriate for each project.

The measurements proper will be determined by the measurement scenario and by the measurement tools which the project finally decides to use. Their outcome will be the measurements performed by the project on the measurement scenario.

The measurements results are nothing else than a more or less bulky amount of collected data. In a last step, the project will use a series of available analysis tools to post-process these data and obtain the scientific results they outlined in their scientific objective.

This process is normally repeated with the same tools in different measurement campaigns to obtain a significant amount of data. In some cases, the measurement cycle has to be repeated with different tools in order to identify the best suited tools. In other cases, different analysis strategies are applied to the measurement data to identify the most suited tools.

The following figure illustrates the whole process:
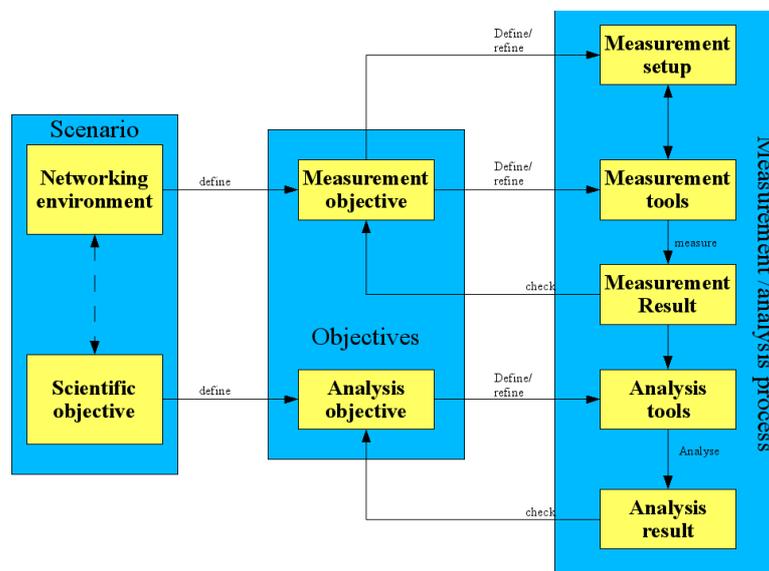
Figure 2-1: The measurement process

The figure also shows the current best practise where the networking scenario is defined as the networking environment in which the measurements take place and the scientific objective to be achieved by the measurements. This networking scenario provides then the objectives for the measurements and the analysis, which, in turn, define the measurement and analysis tools to be used

and also help refine the measurement and analysis processes in order to achieve the most accurate and useful results.

3 OWAMP Interoperability Testing Event

The OWAMP interoperability testing event was an integrated test event between members of the Euro-NGI and the MOME project.

3.1 Motivation

There are different implementations of the One-Way Active Measurement Protocol OWAMP. Bringing them together and test the interoperability was the main goal of this remote event. OWAMP is a draft standard of the IP Performance Measurement IPPM Working Group. Information can be found on http://www.ietf.org/html.charters/ippm-charter.html.

The OWAMP interoperability event aimed on the following objectives and benefits:

- Bringing together the involved institutes and researchers

- To show the possibilities of OWAMP

- To improve and debug implementations

- To check the interoperability of implementations

- To check the performance of implementations

3.2 Event Description

The remote OWAMP interoperability event focused on the possibility to use this protocol over a wide range of active measurement scenarios. The different implementations of the protocol should be tested against each other. Basic measurement infrastructure was provided by MOME. Other participants can include their own equipment for initiating tests. Also, participants were invited provide Internet access to their OWAMP system.

3.3 Test Scenario

Currently known available protocol implementations:

- Internet2 OWAMP Version 1.6f (beta): http://e2epi.internet2.edu/owamp/

- J-OWAMP 1.0 http://www.av.it.pt/jowamp/

4 measurement hosts with the following roles and tools installed were provided. For OWAMP Test-Sessions, the ports UDP 21164-21174 were used:

> 212.183.10.186 (anc-test.salzburgresearch.at), Salzburg, Austria:
>
> - OWAMP Results database incl. simple web interface
>
> - OWAMP Server @ port 22368 & Session-Receiver (CMToolset 2 using j-owamp)
>
> - NTP (Stratum 2, taking time from a GPS-Receiver host in the same subnet)
>
> 161.24.3.17 (R03S230P013.ele.ita.cta.br), Sao Paulo, Brazil:
>
> - OWAMP Server @ port 22368 & Session-Receiver (CMToolset 2 using j-owamp)
>
> - NTP (Stratum 2, sync to ntp.cais.rnp.br)
>
> 152.66.247.72 (malna.tmit.bme.hu), Budapest, Hungary:
>
> - OWAMP Server @ port 22368 & Session-Receiver (CMToolset 2 using j-owamp)
>
> - NTP (Stratum 2, sync to clock1.redhat.com)

193.136.92.121 (ares.av.it.pt), Aveiro, Portugal:

- OWAMP Server @ port 22368

- OWAMP Session-Sender (J-OWAMP http://www.av.it.pt/jowamp/)

- OWAMP Session-Receiver (J-OWAMP http://www.av.it.pt/jowamp/)

- NTP (currently unknown)

User Measurement Point, e.g.:

- OWAMP Session-Sender

- OWAMP Control-Client

- Arbitrary measurement points in the Internet can initiate OWAMP tests from their location by e.g. using Internet2 OWAMP Version 1.6f with the following example command:

  - owping -t -c 20 -P 21164-21174 152.66.247.72:22368
    …initiates an OWAMP-Test between your local Session-Sender and the Budapest Session-Receiver, sending 20 test packets.

- Note: J-OWAMP Session-Senders and -Receivers cannot communicate with Internet2-OWAMP Servers (and vice versa), because this communication is not standardized in the OWAMP Protocol.

Results from CMToolset 2 Session-Receivers (Sao Paulo, Budapest and Salzburg) are available via a simple web-interface and can be retrieved at: http://anc-test.salzburgresearch.at/owamp.php
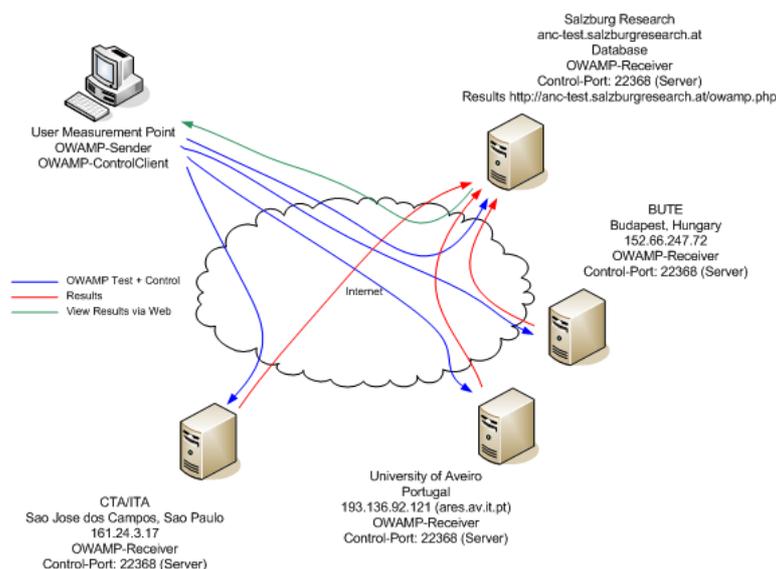
Figure 3-1: OWAMP interoperability testbed

3.4   Related Links

OWAMP related IETF activities are reflected in RFC3763 [24] and an Internet Draft [25], which led to the implementations, checked during this experiment:

- Internet2 OWAMP Version 1.6f (beta) - http://e2epi.internet2.edu/owamp/

- J-OWAMP 1.0 - http://www.av.it.pt/jowamp/

• CMToolset - http://cmtoolset.salzburgresearch.at

3.5   Test Results

The main goals of the OWAMP tests were:

• to test the communication functionality between J-OWAMP and Internet2 OWAMP

• to test the integration of J-OWAMP and CMToolset

The results are summarised as follows:

• Parts of J-OWAMP were successfully integrated to the CMToolset Architecture.

• CMToolset supports the functionality to start J-OWAMP Sever and SessionReceiver (similar to owampd from the Internet2 OWAMP implementation).

• Therefore "owping -t" was needed as SessionSender and ControlClient.

• To fully implement the functions of a Server, CMToolset needs to be extended to report the results to a FetchClient

• CMToolset directly stores the results to its database.

• The port of the Session Receiver is not correctly updated by the CMToolset implementation

• J-OWAMP suits to the CMToolset architecture, therefore the integration of new version (J-OWAMP 2.0) to CMToolset is planned

Raw data of the measurement results have been published in the MOME database (http://www.ist-mome.org/database/). To extract the meta-data from the J-OWAMP measurements, the mapping listed in Table 3-1 has been applied.

MOME meta-database tag	J-OWAMP-extracted value
Dataset name	OWAMP interop test, 21/11/2005 <number of test>
Data type	QoS
File size	<File size of the result table>
File compression	none
Start time	<Send time of first packet>
End time	<Send time of last packet>
Description	A short description on the reason of testing
Dataset location	The URL to the result table
Tool	J-OWAMP, resp. OWAMP
Network Type	WAN, public Internet
Measurement Type	active
Metrics	OWD, loss, throughput, duplications
Sender Location	<location of sender, incl. IP address>
Receiver Location	<location of receiver, incl. IP address>
Sender Platform	Linux PC
Receiver Platform	Linux PC

MOME meta-database tag	J-OWAMP-extracted value
Timestamp Synch.	NTP, GPS
Number of Values	<the number of single packet data values>
Data Format	HTML

Table 3-1 Mapping of J-OWAMP results to MOME meta-database structure

For these initial tests, the results have been entered to the MOME database using the provided web interface. In future the metadata of the J-OWAMP tests should be extracted automatically after the tests have been executed.

The following open issues need to be addressed in future tests:

- testing of J-OWAMP 2.0 and OWAMP2.0

- evaluation of delay measurement accuracy

- performance tests

- Extending the functionality of CMToolset Architecture to support also the functions of SessionSender, ControlClient and FetchClient.

4 Survey of Monitoring and Measurement IST projects

4.1 Project survey

MOME started its first questionnaire in 2004, where an initial list of projects dealing with monitoring and measurements was selected and analysed. During the runtime of these projects more information became available from the projects describing details about their approaches in monitoring and measurement.

The activities of the projects have been continuously followed by MOME, and new projects have been investigated with respect to the monitoring and measurement topic by analysing the project web-pages and deliverables. Another questionnaire (see appendix A.1) to the projects was necessary to get further details, especially to the measurement chain, which was done in fall 2005. Table 3-1 shows the full list of projects investigated and addressed by the MOME project.

The information gathered was structured to cover the following topics:
- Objectives
  - Scientific Objective
  - Measurement objective
- Networking environment
- Measurement Process
  - Measurement set-up
  - Measurement tools
  - Measurement results
- Analysis
  - Analysis tools
  - Analysis results

The project by project results are included in Appendix B.

4MORE	6QM	ACE	AMBIENT NETWORKS	ATHENA	B-BONE
BREAD	BROADWAN	CAPANINA	COCOMBINE	COSIN	COST279
COST290	DAIDALOS	DEISA	DELIS	DIADEM FIREWALL	DMRG-PAN
Diligent	E-Next	E2R	EGEE	ENTHRONE	EUQOS
EVEREST	EVERGROW	Euro NGI	Euro6IX	EuroLabs	FLEXINET
GANDALF	GEANT/ DANTE	GEANT2	GRIDCC	IPv6 TF-SC	LASAGNE
LIAISON	LOBSTER	LONG	MAESTRO	MAGNET	MESCAL
METAWIN	MMAPPS	MOCCA	MOME	MOSSA	MUPBED
MUSE	NEWCOM	NGN-LAB	NOBEL	OBAN	OPERA
PAN-NET	PHOENIX	PULSERS	SABA2	SATLIFE	SATNEX
SCAMPI	SEE-GRID	SEINIT	SIDE-MIRROR	SIMPLICITY	SPECTRUM
SWAMI	U-BROAD	UBISEC	WIDENS	WINDECT	WINNER
WWI	E-PHOTON/ ONE				

Table 4-2: Monitoring and measurement projects investigated by MOME

4.2   Detected overlaps

During the runtime of the MOME project more than 70 IST-projects have been identified in related areas, out of which 20 can be said to have a strong or very strong relation to monitoring and measurement objectives.

4.2.1   Tools

In order to analyse where similar activities lead to the use of the same tool or set of tools this information has been reviewed and overlaps have been identified by inspecting the project web-pages and deliverables.

Table 4-3 lists the outcome of this inspection.

Project	Tools
6QM	OpenIMP, Mgen, trpr, pathchirp, tcpdump, tcptrace
ATHENA	DVB-MHP, DVB sender and receiver, IPSec software
BROADWAN	Tcpdump, Chariot, Sniffer Pro, Ethereal, Cisco SAA, IPANEMA, NIMI, Rude/Crude, Netmate
DAIDALOS	OpenIMP, IPProbe, netfilter, Linux tc (traffic control), Ethereal, Monitoring Platform for Mobile IPv6 flows
DIADEM FIREWALL	Netfilter, different modules (one per known attack will be developed)
ENTHRONE	Passive meters (MIBv2 from SNMP Linux router software), IP/DVB-T gateway.
EUQOS	NetMeter (active), MGen traffic generator (active), Trace-based Traffic Generator (TrTG) for traces re-playing, End-to-end Test Tool (E2ETT), Link Load Measurement Tool (LLMT), Topology Acquisition Tool (TAT), ORENETA, Chariot
Euro6IX	Cisco Netflow, ping_stat, IPv6 snmp monitoring, IDS software, stat6, looking glass, nagios, mrtg
EuroNGI	Distributed Passive Measurement Infrastructure (DPMI), Saturne, J-OWAMP
EVEREST	Oreneta, iptables, Linux tc (traffic control)
EVERGROW	DAG Cards for traffic monitoring
GEANT/Dante	Ping, Traceroute, Inter-mapper, for link monitoring using SNMP, Cricket (SNMP), Taksometro (for long-term network monitoring), Multicast beacon (active), Multicast per group monitoring tool, Looking Glass (for executing queries on remote routers), Nagios, (for monitoring different parameters, creating reports and alarms) Mezeuon, for monitoring traffic on router interfaces
LOBSTER	DAG cards for traffic monitoring, MAPI (Monitoring API), Stager (a system for aggregating and presenting network statistics)
MESCAL	Smartbits (hardware), MGEN (active), TG (traffic generator), QARobots (SW, for BGP messages)
METAWIN	DAG cards for passive monitoring
SCAMPI	DAG cards, SmartBits Traffic generator, Ntop, Snort, Mapi
DEISA	Iperf, Ping, MRTG, Netscout NGenius PM

Table 4-3: Use of monitoring and measurement tools in MOME projects

The following projects have not provided to MOME nor produced any publicly available documentation regarding the measurement tools they use:

- MUPBED, NOBEL, PAN-NET, SATLIFE, and SATNEX

This most often is the case when measurement and monitoring is only a minor part of the project's work and not in their main scope of research.

We have found three main categories for the tools:

- Custom project developments

- Commercial tools

- Well-known open source tools

Table 4-4 groups the tools used in two or more projects into these categories:

Tool Category	Tool
Custom Project developments	Openimp
	Oreneta
Well-known open source tools	Mgen
	Tcpdump,
	Ethereal
	Netfilter
	Linux traffic control (tc)
	Looking glass (cf e.g. here)
	MRTG (or its predecessor RRDTool)
	ping, traceroute, (also Unix wget)
	Nagios
Commercial products	SmartBits
	DAG boards

Table 4-4: Popular monitoring and measurement tools

Some solutions like the DAG boards and Linux netfilter/traffic control (tc) are quite popular and used in many projects. The line of high speed DAG boards offer convenient traffic capture and line-speed analysis functions, while the Linux traffic control software offers an easy (and low cost) way to implement an IP router with traffic shaping capabilities for realisation of QoS and differentiated services.

In addition numerous open source (mostly Linux-based) tools are in use in different projects to realise testbed services such as differentiated and integrated service, IP routing, mobile Ipv4 and IPv6 support, as well as implementing WLAN access points with novel features, and for setting up test server applications (web server, video server, DNS).

From our experience and the observations we made we can conclude that for the goal of fostering the common use of monitoring and measurement tool four preconditions are vital:

- a clearly targeted (and limited) application area for each tool

- clear, accurate documentation (function, installation, configuration, use)

- a company or community which keeps this tool up-to-date and provides support

- dissemination, i.e. public accessibility of tools, their documentation, and preferable use case examples. It is strongly suggested to publish such tools information clearly on project websites and to make use of open program databases for registering own developed tools, e.g. MOME, Souceforge, Freshmeat, Sourcewell.

If such preconditions are met then reuse or common use of monitoring and measurement tools can be facilitated no matter what their originating source is.

4.2.2   Protocols

A plethora of protocols are in common use within the approached projects. This information is even more complex to obtain than the list of tools as it is often not clearly stated in project deliverables. In addition to the common transport protocols (UDP, TCP, SCTP) we found the following list of non-proprietary protocols in use in the observed IST-projects:

Type	*Protocols*
Signalling	SIP, RTSP, RSVP, NSIS
Configuration	COPS, SNMP, LDAP, RMON
Data Transfer	Radius, Diameter, IPFIX, RTP, H.323
Remote Process/Function Invocation	RMI, XML-RPC, Unix named pipes, SOAP
other	Flute, SLP, PANA, OWAMP

Table 4-5: Non-proprietary protocols used in IST projects

Several projects are actively participating in work on upcoming protocols (such as IPFIX) and extensions to current protocols (i.e. Diameter, RSVP and new SNMP MIBs). This includes contributions to work of standardisation bodies such as IETF, ETSI, TISPAN, IEEE, ISO/IEC, TIA, 3GPP, ITU-T, and W3C. There is a two-way communication in place:

- IST project work gives incentives for new protocols requirements and protocol extensions

  and

- Protocols being standardized are implemented, deployed and tested by IST project participants during their work on prototypes and system solutions.

4.2.3   Approaches

From analysing the projects the following three main approaches to monitoring and measurement in the projects have been identified:

1 **Developing Monitoring and/or Measurement tools & architectures**: These projects are developing new measurement tools and measurement architectures. Synergies in these projects can be exploited mainly by contributing to new standards in the Monitoring and Measurement

area. These projects are important from the MOME viewpoint, because they can contribute information about their new developments to the MOME database.

2 **Applying Monitoring and/or Measurement for evaluation & validation**: These kind of projects don't develop measurement tools and architectures themselves, but use them to evaluate or validate QoS architectures or similar.
   They can make use of the MOME database by getting information about measurement tools. These projects are important from the MOME viewpoint, because they have the possibility to deliver measurement data and results taken during the evaluation and validation procedures, if they make it publicly available and contribute information to the MOME database

3 **Building infrastructures & testbeds**: These projects either design infrastructures or include the design of a project specific testbed. Infrastructures usually can be used by other projects, while testbeds are project internal environments, where the evaluation & validation of the project approaches take place. These projects are important from the MOME viewpoint, because they can provide the environment for testing measurement tools and retrieving measurement results.

Some projects can be assigned to more than one approach. Figure 4-1 shows in which areas each project[1] is active.
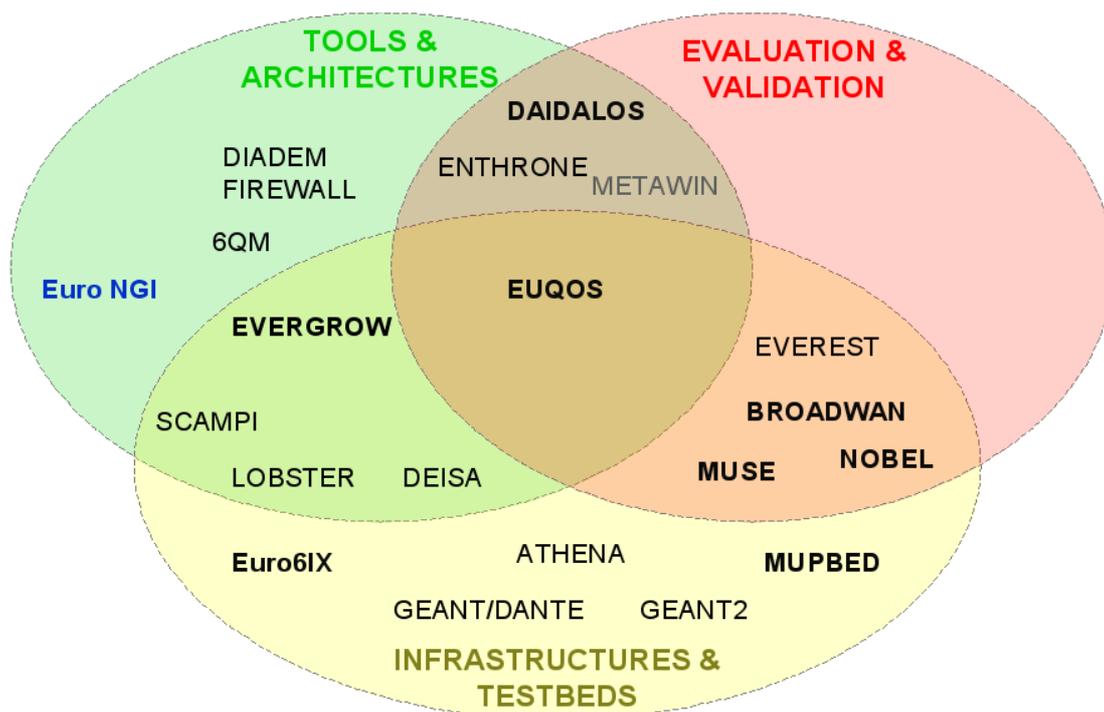
Figure 4-1: Approaches to monitoring and measurement from the projects

Projects in the same areas have overlaps in their approaches and therefore they have potential to co-operate in these issues. This doesn't imply that they have to e.g. share all their testbeds or measurement tools, but being aware of the activities of projects with related approaches can help to harmonise them and get comparable results. Projects addressing more than one of these generic approaches are placed in the overlapping areas.

---

1 Integrated projects appear in bold black font in Figure 4-1, while NoE appear in blue characters

4.2.4   Scenarios

The measurement scenario is determined by the scientific objective of the project. The main component of the scenario is the networking environment in which the measurements take place. From this point of view, the measurement scenarios assumed by the investigated projects can be broadly divided into two categories:

- **Measurements in testbed**, which are performed according to carefully planned scenarios in fully controlled environment. Such measurements usually aim at testing specific solutions proposed by particular project. Thus, the possibility to re-use raw results obtained by different projects is rather limited. The cooperation between projects should focus on re-using the tools and increasing the interoperability of tools in order to improve the comparability of obtained results.

- **Measurements in the operational network**, where the obtained results (like e.g. packet- or flow- level traces) correspond to the actual traffic observed in real-life scenarios. In this case, raw results might be especially interesting for other researchers and sharing the results is an interesting possible area of cooperation between projects.

Furthermore, another classification criterion is related to the layer on which the project performs the measurements. Taking this into account we can distinguish between:

- **IP-layer measurements**, which are in the main focus of MOME, and

- **Lower-layer measurements** like e.g. measurements of physical link characteristics.

The classification of investigated projects taking into account the above criteria[2] is presented in the figure below:
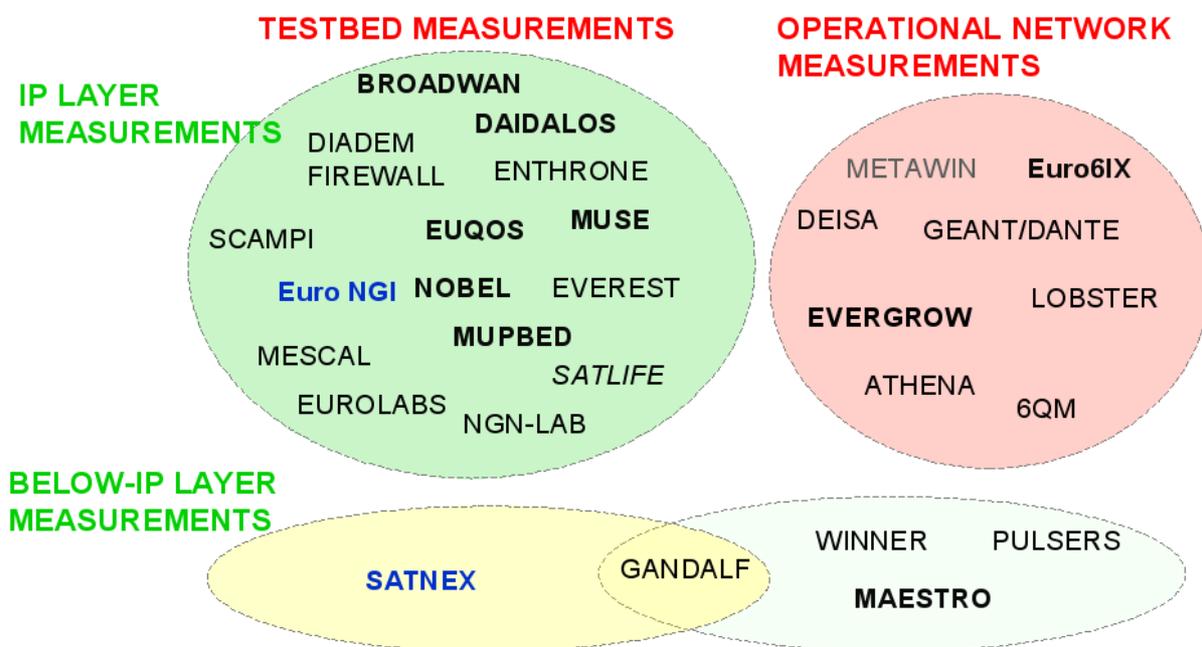
Figure 4-2: Measurement scenarios assumed by associated projects

---

2 Integrated projects appear in bold black font in Figure 4-2, while NoE appear in blue characters.

4.3   Recommendations

The study shows that there are some areas in which overlaps exist. Overlaps in protocols are easily justifiable, since the protocols can carry data with quite different semantics. This is the main area for inter-project collaboration.

Certainly, the exchange of information between European projects about measurement tools and assumed test scenarios is highly desirable. The analysis of the questionnaire answers and project deliverables allows us for pointing several projects that produced especially valuable results that could be studied by other projects working in similar or complementary research areas.

In particular, the projects that build networking testbeds and apply measurements for network evaluation and validation, should consider the outcomes of the projects that develop measurement tools and architectures. Several of such projects have provided us with a clear and well-documented measurement chain, including description of developed tools (see Table 4-6, more details can be found in Appendix B).

Projects developing QoS measurement tools	*Projects developing traffic measurement tools*	*Projects developing topology and routing acquisition tools*	*Projects developing data analysis tools*
6QM (OpenIMP) EuroNGI (Saturne, J-OWAMP) EuQoS (Netmeter, Oreneta) EVERGROW (ETOMIC) DAIDALOS (OpenIMP)	EuroNGI (DPMI) EuQoS (LLMT) LOBSTER (Traffic Monitoring Infrastructure)	EuQoS (TAT) EVERGROW (DIMES)	EuroNGI (TSTAT) LOBSTER (data anonymisation tools)

Table 4-6: Selected projects developing measurement tools

From our experience and the observations we made we can conclude, that three preconditions are vital for the goal of fostering the common use of monitoring and measurement tools:

- a clearly targeted (and limited) application area for each tool
- clear, accurate documentation (function, installation, configuration, use)
- a company or community which keeps this tool up-to-date and provides support
- public accessibility of tools through open program databases

If such preconditions are met then reuse or common use of monitoring and measurement tools can be facilitated no matter what their originating source is.

Overlaps in protocols are easily justifiable, since the protocols can carry data with quite different semantics. This is the main area for inter-project collaboration. Parallel implementation for newly developed protocols is valuable since different programmers can detect other protocol pitfalls and shortcomings. This approach also avoids a software "monoculture", i.e. only relying on one specific realisation of a protocol. Such approach can increase overall computer system safety.

On the other hand, among the projects that focus on using measurement tools in testbeds for network evaluation and validation, we note the following ones that provided us with complete information about their measurement chain (see Appendix B for more details):

- EuQoS that develops the QoS architecture for heterogeneous multi-domain networks and uses measurements for architecture validation, supporting the system functions and performing QoS monitoring,

- EVERGROW that uses the developed monitoring infrastructure for conducting real-time measurements of public Internet traffic and topology,

- GEANT/GEANT2/DANTE that operates the European research network and uses measurements for monitoring the current load and QoS parameters between selected points,

- LOBSTER/SCAMPI that deploys a pilot passive traffic monitoring infrastructure,

- BROADWAN that develops architecture for providing broadband services for fixed and nomadic users and uses measurements for architecture validation and system debugging,

- DAIDALOS that deploys heterogeneous network technologies giving users access to personalised voice, data and multimedia services, and uses measurements for charging, session monitoring and SLA verification,

- DEISA that deploys a dedicated network for connecting the supercomputers and uses measurements for network usage monitoring and SLA verification,

- Euro6IX that deploys IPv6 infrastructure to research, test and validate IPv6-based applications and services, and uses measurements for monitoring and tracking the IPv6 network traffic.

The measurement objectives and requirements worked-out by these projects might be considered as valuable input for projects working on developing new measurement tools and architectures.

MOME has also found some examples of IST projects which perform measurements as part of their infrastructure monitoring activities, but have no clear policy regarding the dissemination of these measurement results. This ambiguity is the result of the lack of a clear measurement dissemination policy in the IST FP6 and previous programmes.

Setting a clear policy, which mandates dissemination of measurements performed in future framework programmes, with the appropriate anonymisation procedures to assure no civil rights concern is raised, should promote measurement exchange and reuse among projects. More research is needed in this field, to provide IST projects with information about anonymisation methodologies, techniques, and the effect of different anonymisation strategies. Only with a common basis in those techniques and well-know tools a wide-spread level of dissemination of trace data can be reached.

The use of specific tools and especially information about own developed tools should be made clearly available on a projects web page and/or inside open tools repositories. This will enhance effectiveness of dissemination, increase cooperation and finally can lead to joint development and work instead of double work on new tools inside multiple projects.

When interoperability between different IST projects can be foreseen due to partial overlaps or work in clearly adjacent areas then such cooperation should be strongly encouraged if not mandated inside the projects' technical annexes. Such work could cover foreseen common tools development, common demonstrations, or joint work on upcoming standards (e.g. for protocols). An early commitment to such joint work would enhance project interoperation as well as cooperation with coordinating actions and willingness to provide input.

We also suggest to prepare and hand out guidelines for functionality of web presence of ongoing projects and to mandate certain base features to common projects. This would enhance the effectiveness of IST-projects' web presence and allow other researcher a much more effective way of accessing and searching for data about other projects which they potentially like to cooperate with. Finally the EC might want to think about giving extra monetary incentives for successfully proven cooperation between projects. Yet, clear definition of the targets of such cooperative work need to be stated and disseminated by the EC for having such practice to be really effective.

5   Wireless measurement and monitoring scenarios

5.1   Wireless measurement and monitoring tools in the MOME tools database

The MOME tools database contains a set of Wireless LAN tools useful on the 802.11a/b/g protocol.

Traditional traffic monitoring and measurement tools used in Ethernet (802.3) are also valid for use in WLANs despite the fact that 802.11 and 802.3 protocols are different at the physical and data link layers. Those tools can be used at the transport (e.g. IP) and above application layers.

Nevertheless WLAN dedicated tools are required to fulfil WLAN specificities, such as detecting WLAN networks and checking signal strength or channel quality.

The MOME tools database search results for wireless tools show WLAN monitoring and measurement tools which fall in the two categories open source and commercial tools.

Usually all-round monitoring and measurement tools applied to use in wireless networks such as WLAN can be used to measure standard metrics such as connectivity, used and available bandwidth, jitter, delay, loss, and application specific attributes.

In addition wireless-specific tools are often able to obtain attributes only available on this medium such as WLAN SSID, number and type of channels present, radio signal strength, used transmission mode and encryption scheme (if applicable). Applications cover a wide range including accounting, QoS measurements, trouble shooting, fraud prevention and detection and infrastructure planning.

Whilst almost all open source tools in the wireless sector are targeted at WLAN measurements, the commercial tools also cover the GSM (GPRS, HDSC, EDGE) and UMTS sector.

Wireless-targeted tools listed in the MOME tools database can be found by using the search dialog
    http://www.ist-mome.org/database/MeasurementTools/?cmd=toolssearch
and entering "wireless" in the 'Description' field.

The most well-known set of command line tool in the Linux world are the Wireless Tools (WT), a set of command-line tools that give access to (installed) WLAN cards via the Wireless Extensions API. They use a textual interface and are rather crude, but aim to support the full Wireless Extensions. There are many other tools which use the Wireless Extensions, however the Wireless Tools are the reference implementation.

Appendix C shows a selection of wireless monitoring and measurement tools that are also available in MOME database. For a better overview, the tables have been separated depending on the status of the tools. Table C-1 lists open source tools. Table C-2 lists commercial tools.

Many more wireless tools can be found at: http://www.networkintrusion.co.uk/wireless.htm

5.2   Wireless measurement traces in the MOME database

At the moment there are no wireless measurement and monitoring activities from IST projects documented in the MOME database. This is a result of not being able until now to obtain any IP layer measurements from IST projects which capture traffic over wireless technologies. This does not directly imply that such activities are not performed. In section 5.4 "IST wireless networking projects and measurements" references to IST projects working on and measuring different layers of the networking reference model in wireless environments are listed.

5.3   Wireless measurement traces not covered by MOME

Outside the scope of IST, the MOBILIB project [1] has published a limited amount of traces from different universities, mainly located in the United States of America.

Many wireless traces have serious limitations, mainly due to legal concerns regarding privacy issues. Some campuses offer access to their trace database in very restrictive terms. In some cases , the published data are heavily filtered to preserve the privacy of the users. The Dartmouth Wireless Traces [2] web page specifically states:

> "I do not have,
>
> - Any authentication data. I make the assumption that a MAC address identifies a user, although some people have multiple cards and some cards may be used my multiple people.
>
> - Any packet headers above the TCP layer. A typical packet has Ethernet, IP, and TCP headers. The exception is the VoIP data from the 2003/4 trace, where we provide the RTP header for those devices that use RTP (the Cisco devices).
>
> - Any packet data: thus you cannot see inside the http protocol, for example."

The MOME project has concentrated on finding and contacting IST projects involved in this kind of activities. Unfortunately, projects dealing with wireless scenarios have not been able to contribute any data, mainly due to the same or harder restrictions to preserve the privacy of the monitored users.

A project which uses real time monitoring data from a mobile network to show the evolution of a city has been found. Led by the MIT, the mobile landscape [3] project shows the real time evolution of the mobile network of Mobilkom Austria (A1) in the town of Graz. Despite the final objective of this project being artistic and not scientific, the restrictions imposed on the project on anonymisation and use of trace data are quite heavy.

Also in Austria, the Austrian national project METAWIN [20] aims at collecting and analysing packet-level traces from a commercial UMTS network operator (Mobilkom Austria). The project has collected large amount of anonymised traces, which are stored in a proprietary format. However, the traces are not available for public, since the data is regarded as business critical by the operator.

Outside the scope of IP layer measurements, several IST projects have measurement activities, but are only publishing measurement analysis results and not the traces used to generate them.

5.4   IST wireless networking projects and measurements

Several IST projects in the wireless world are performing measurements. After contacting partners within them, no relation between their activities and the scope of the MOME Database could be found. In some cases, measurements on layers of the networking protocol stack other than IP are performed.

For example, the WINNER [14] project has performed a series of measurements to characterise the radio frequency channel in their experimental scenarios and some bulk measurements of traffic generated by the applications they selected for their demonstrator. These traffic measurements were tailored specifically to the simulation tools developed in the STRIKE [15], an earlier IST-project.

Measurements to characterise the radio channel are performed with specific RF measurement equipment, which is out of the scope of MOME. They include:

- Statistical distribution of the number of parallel radio paths

- Statistical distribution of the number of clusters without temporal dispersion

- Statistical distribution of the mean & maximal delay

- Relationship between delay and attenuation

- Characterisation of fast fade-out (Doppler)

All these measurements are completely out of the scope of the MOME project.

Another example could be the IST-PULSERS [16] project, which has provided measurements to study the coexistence of Ultra Wide Band (UWB) systems with the current and future mobile networks. This task was accomplished by measuring the bit error rate (BER)on commercial GSM/GPRS and UMTS terminals for different levels of UWB interference.

In the scope of the IST-EuQOS project [19] measurements are performed in testbeds build using different network technologies, among them wireless networks WiFi and UMTS. The experiments are performed in a controlled testbed environment. They are aimed mainly at validating the prototype of the EuQOS System, which is designed and implemented by the project for providing services with assured QoS level in different access network technologies and on end-to-end basis. Since the goal is to measure QoS parameters on the IP packet level, no tools specific to wireless environment are currently used or developed by the project. The processed and analysed results will be published in the project deliverables.

6   IPv6 measurement and monitoring scenarios

Although some IST projects have planned and carried out IPv6 measurement and monitoring activities, the results were not always completed or fully documented.

With the development of the Internet Protocol version 6, tools used to monitor and measure IPv4 traffic are adapted to interpret IPv6 packets. FP5 and FP6 projects such as 6net, MobyDick, Euro6IX have designed their own tools and/or modified tools to meet their needs in IPv6 management and monitoring.

6.1   IPv6 measurement and monitoring tools in the MOME tools database

Most monitoring and measurement tools were designed for the Internet Protocol version4 IPv4. In order to support the new Internet Protocol, IPv6, tools require advanced extensions. Many developers and projects have contributed to this evolution by extending and porting measurement tools. For example, IPv6 extensions to the Berkeley Packet Filter (BPF), libcapv6, and extensions to BPF based tools such as tcpdump have been developed.

The following list shows monitoring and measurement tools that are included in the MOME database and have been designed for or ported to IPv6. The tools are listed according to the project that used them:

- The JOIN[6] project uses AS Path Tree to monitor and output activities of the JOIN 6bone node. The AS-Path tools generally look at BGP4+ status. They provide graphic displays and all route entries within the IPv6 BGP backbone.

- The 6WIN [7] project uses IPv6 Route Looking Glass for BGP traffic summary and to monitor advertised-routes.

- The 6net [8 project is maintaining a repository of monitoring tools (http://tools.6net.org) which have been used in their network. Some have been ported to IPv6.

- The LONG [17] project has ported a number of applications to IPv6 and also released a guidelines documentation [18] for doing so.

Below is a selected set of tools suitable for IPv6 monitoring and measurement that are also available in MOME database

- Analyzer
- Argus
- AS Path Tree
- CISCO Works Campus Manager (CiscoWorksCM)
- Cricket
- dbeacon
- Ethereal
- HP OpenView Network Node Manager
- IPv6 Management Gateway
- Jnettop
- JOIN-TV
- MRTGv6

- Multicast Beacon

- Nagios

- PCHAR

- Ripe NCC Test Traffic Tools

The GÉANT [9] project uses a number of these tools to monitor its traffic.

RIPE NCC test traffic measurement is used within GEANT to provide delay summaries (incoming and outgoing delays and packet losses), delay overview plots and graphs showing delay and losses, as well as Jitter or IPDV plots and IP Tunnel Detection.

The DFN IPPM devices are installed on GÉANT and within a few National Research and Education Networks (NRENs) in order to measure the OWD, the jitter and the packet loss between those points. The visualisation of the result is also provided.

All these tools are also listed in the MOME database.

6.2   IPv6 measurement traces in the MOME database

The current overall traffic volume of IPv6 communications is still quite low compared to IPv4 traffic on the Internet. Most IPv6 traffic is run in experimental networks like testbeds or NRENs .

The MOME database does not provide IPv6 measurement traces coming from the IST realm, because the observed IST projects with activities in IPv6 measurements and monitoring at the IP layer did not make traces publicly available. However, the MOME database references some of the MAWI traces [11].

6.3   IPv6 measurement traces not covered by MOME

The 6bone[10] network, an early IPv6 testbed, collects daily traces from IPv6 line connected to the WIDE-6Bone network. The majority of traffic recorded is BGP and ICMPv6 packets. The Measurement and Analysis Work Group (MAWI) of the Widely Integrated Distributed Environment (WIDE) project [11] from Japan provides traffic data from their backbone and makes it publicly available through their traffic repository for download and analysis. These traffic traces are in the tcpdump raw format and IPv6 traffic is also recorded.

The NLANR AMP[12] is collecting IPv6 performance data between a mesh of twelve active monitors, mainly in USA. Three additional monitors are placed in Australia (AARnet), in Japan (APAN), and in the Netherlands (SURFnet). Traces could be made available on request.

It is expected that IPv6 traffic will increase in the near future with router and operating systems vendors starting to provide IPv6 support in their base systems. This will increase the volume of IPv6 traffic traces recorded. It is therefore important, that the MOME database is kept alive to register these traces in the future.

The RIPE Routing Information Service (RIPE-RIS) [13] has a repository of raw routing information base and BGP-4 update files. With the introduction of IPv6 services, the routing beacons and collectors where migrated to support the multi-service extensions to BGP-4 and more recent files include IPv6 routing information.

7   IETF related activities

7.1   Interoperability event

The Interoperability Event organized by MOME was held in Paris, France on 28-30 July 2005, just before the IETF meeting. 44 people from 18 companies attended, and 14 implementations covering IPFIX, NSIS, and NETCONF implementation work were tested.

Several attendees visited this event on behalf of EU funded projects or projects funded by national research programmes in the EU:

Attendee	*Protocol*	*Project*	*Framework*
France Telecom	IPFIX	6QM	FP5 IST
Fraunhofer Fokus	IPFIX	Daidalos	FP6 IST
NEC	IPFIX, NSIS NETCONF	EuroLabs	FP6 IST
University Coimbra	NSIS	EuQoS	FP6 IST
University Tübingen/Erlangen	IPFIX	DIADEM	FP6 IST
University Göttingen	NSIS	ENABLE VIDIOS	FP6 IST EC EUREKA CELTIC

Table 7-1: Projects attending the MOME Interoperability Event

Deliverable D13 [4] documents the event, including the detailed test specifications and results.

The Interoperability event showed, that several projects are implementing the same protocol. This parallel work is beneficial for the overall protocol standardisation process because different views and interpretations of the protocol specification are confronted and grey areas can be clarified.

7.2   Inter-Domain Questionnaire

This survey has been created to raise the question of inter-domain measurements and data exchange between ISPs. Its goal is to find out what the main concerns are, and whether and how an inter-domain collaboration would be beneficial for the community.

With the feedback from ISPs, which has not yet been received as of the time of writing this deliverable, the MOME team targets to gather practical knowledge about provider's needs which can be valuable input for IST projects when practically applying their work in life operating network environments. The feedback results will be documented in future MOME deliverables.

The Inter-domain web-based questionnaire can be found at

   http://www.ist-mome.org/surveyor/quest-interdomain.html .

It is based on the document "Inter-domain Data Exchange Questionnaire" [21] which has been submitted as IETF draft.

8   Conclusions

This deliverable documents the different activities around the MOME Database since its deployment. The project has provided a rationalisation of the whole process of collecting and processing of raw measurement data in order to produce scientific data for further study. This process has been formalised in the Measurement Chain concept.

Our measurement and monitoring project survey on IST projects showed, that there are some areas in which overlaps exist. Overlaps in protocols are easily justifiable, since the protocols can carry data with quite different semantics. This is the main area for inter-project collaboration and leads to improvements and extensions to those protocols which are still in draft status.

For the common use of monitoring and measurement tools we can conclude from our experience and the observations the following three vital preconditions:

- a clearly targeted (and limited) application area for each tool

- clear, accurate documentation (function, installation, configuration, use)

- a company or community which keeps this tool up-to-date and provides support

If such preconditions are met then reuse or common use of monitoring and measurement tools can be facilitated no matter what their originating source is. This does imply some information exchange between projects if the tool in use has been developed by one of the IST projects using it.

Generally speaking, we have seen quite some resistance to publishing network traces. From the factors which explain the situation, the two main are:

- **legal reasons**: there is no legally sound framework which could give the researchers the confidence to publish the data without facing legal consequences (i.e. Violation of data privacy). These concerns exist in fixed and wireless networking environments.

- **marketplace**: mobile operators monitor and measure their network, but these data are highly confidential, since they reflect the strengths and weaknesses of their network and could be used against them by competing operators.

This conclusions are aligned with the results of a survey conducted by the LOBSTER project [22]. As part of the requirement analysis phase for their measurement equipment, they conducted a survey, targeted among others, at the National Research and Education Networks of the European Community and ISP's [23]. This study points out that on the one hand, there is interest in having access to raw network data as opposed to highly processed results and on the other, there is a lack of willingness to share these data. The study also points out, that anonymisation can be a way to encouraging data sharing and that it should be directly done by the capturing device, to minimise the risk of leaking real user information.

MOME has detected the lack of a clear measurement dissemination policy in the IST FP6 and previous programmes. Setting a clear policy, which mandates dissemination of measurements performed in future framework programmes, with the appropriate procedures to assure no civil rights concern is raised, should promote measurement exchange and reuse among projects.

From the point of view of protocols supporting monitoring and measurement, some parallel work in the implementation has been detected and confirmed at the MOME Interoperability event. The event helped the projects to check the interoperability of their respective implementations. The fact that there are several projects implementing in parallel can be justified, because the phrasing of some standards leave space for interpretation, which can only be harmonised by contrasting implementations in events like the MOME Interoperability event.

Appendix A Questionnaires used for surveys

A.1   Questionnaire to IST projects monitored by MOME
Dear IST programme participant,

```
We are contacting you on behalf of the IST co-ordination action
for Monitoring and Measurement (MOME, http://www.ist-mome.org).

Objective of MOME is to find synergies between active IST projects
which are (partially) active in the area of network monitoring,
measurements, and analysis.

Therefore we analysed the project web-sites and deliverables and
now would like to get a few more detailed information.

Please take a few minutes to answer a small set of questions
(or delegate this to the most appropriate person in your project).

The answers will be summarised and published in the upcoming
MOME Deliverable D23 which will show the diverse measurement and
analysis approaches of current IST projects in the area of
monitoring and measurement in comparison.

Please send us your answers in reply to this email not later than
*October 14th*. Thank you.

In case you have further questions please do not hesitate to contact me.

Sincerely,
<name of sender> on behalf of the MOME-Team.


(1) Is your project concerned with network monitoring and doing measurements and
analysis on these data? If yes, please proceed.
Note: In case your project already took part in the MOME questionnaire in 2004 then
please proceed, if changes apply.

(2) Which standardised or upcoming protocols do you make use of?
e.g. IPFIX, PSAMP, OWAMP, NSIS, NETCONF, DIAMETER, other?)

(3) Has your project developed own tools? If yes, for which purpose?
Are they available (URL)? Under which license?
(4) How are the tools you use connected and transfer data to form a
 complete chain from data gathering to processing and analysis:
 - What are your objectives with this measurement?
 - What is your measurement set-up/scenario?
 - What kind of raw measurement data do you capture?
 - What tools to you use to capture them?
 - What kind of processed measurement results do you use for your work?
 - What tools do you use to obtain them from them raw data?

(5) Do you collect and store raw measurement results, e.g. full traffic
 traces, in your project as well? If yes:
 - In what format are they stored?
 - Are they publicly available? If not, why not?

(6) Do you have contacts for interworking with other monitoring and measurement
related IST projects? If yes, what are the common goals of both projects?

Thanks a lot for your answers. To get informed about the published results,
please subscribe to the mome-announce mailing list at:
http://www.ist-mome.org/announcements/

PS: if you have output (papers, posters) from your project which you would like to
```

present you might want to take a look at the Call for Papers of the IPS-MoMe 2006
workshop (http://www.ips2006.org/cfp/)

A.2   Questionnaire to Internet Service Providers on Inter-domain Data Exchange

Inter-domain Data Exchange Questionnaire

0 - Contact Information

You may specify here your contact information so that we can contact you in case of further cooperation. These fields may be left blank. The contact information will be kept confidential and will not be visible in the overall survey results.

0.1: Name:

Please write your answer here:

0.2: Occupation:

Please write your answer here:

0.3: Company:

Please write your answer here:

0.4: eMail:

Please write your answer here:

1 - Measurement

1.1: Are you in general interested in measurements across domains?

Please choose **only one** of the following:

Yes

No

1.2: What kind of data (i.e. traffic metrics) from other ISPs are you interested in?

Please write your answer here:

1.3: Would you have a use for a protocol (or application) that would allow you to demonstrate to your customers that your network is performing well?

Please choose **only one** of the following:

Yes

No

1.4: How do you handle the lack of precise methodology to attribute performances to specific path segments?

Please write your answer here:

1.5: Do you have a motivation for end-to-end measurements which span multiple domains and which can be reliably partitioned into segments of single domains?

Please choose **only one** of the following:

Yes

No

1.6: Have you ever been blamed for problems that were outside of your network (due to bad or non-existing measurements)?

Please choose **only one** of the following:
Yes
No

1.7: From your point of view, for which application/reason would the use of passive measurement be most applicable?

Please choose **all** that apply
Resource Usage
Resource Allocation
Traffic Accounting
Security
Network Quality
Fault Diagnosis
Trouble Shooting
ISP Privacy
Long Term Network Planning
Other:

1.8: From your point of view in which application would you consider active measurement the most applicable solution to use?

Please choose **all** that apply
Resource Usage
Resource Allocation
Traffic Accounting
Security
Network Quality
Fault Diagnosis
Trouble Shooting
ISP Privacy
Long Term Network Planning
Other:

2 - Protocols and Tools

2.1: Would you develop/use a (STANDARDIZED) tool for handling the inter-domain data exchange?

Please choose **only one** of the following:
Yes
No

2.2: Would you like to participate in the development process of an inter-domain information exchange software/platform/framework?

Please choose **only one** of the following:
Yes
No

2.3: Would you like to let other entities set up active measurements that originate/terminate in your domain by using tools under your administrative responsibility and control?

Please choose **only one** of the following:

Yes
No

3 - Measurement Information Exchange

3.1: Which aspect of the information exchange is most important to you?

Please choose **all** that apply
Access Control
Accuracy of the information
Prompt availability of the results
Information usability in contracts
Reliability of data exchange
Machine to machine communication
Other:

4 - Privacy

4.1: What information are you allowed, through measurements, to collect about your users?

Please write your answer here:

4.2: What information are you allowed, through measurements, to reveal to other ISPs about your users?

Please write your answer here:

4.3: What information are you allowed to reveal to other ISPs about your network (e.g. topology)?

Please write your answer here:

4.4: To which data/information would you never grant others access?

Please write your answer here:

4.5: Would you, using appropriate policies, allow researchers to collect data in your network (e.g. number of different flows, mean number of packets per flow, mean packet size), or would you share collected data with researchers? If yes, under which conditions?

Please write your answer here:

5 - Anonymisation

5.1: Do you use any kind of anonymisation on the collected data (e.g flow information, traffic traces, packet data)?

Please choose **only one** of the following:
Yes
No

5.2: If you do not use any kind of anonymisation on the collected data, why is this so?

Please choose **all** that apply
Anonymisation is still a research topic, not a mature field
It is not needed
Concerns on the vulnerabilities of some anonymisation

Other:

5.3: If you do make use of anynomisation techniques, which do you use?

Please choose **all** that apply
Hash functions (one-way hashing)
Masking
Truncation
Random permutations
Other:

5.4: Which items are targets of anonymisation?

Please choose **all** that apply
IP (v4 or v6) source addresses
IP (v4 or v6) destination addresses
Source Port
Destination Port
Entire Application Level Payload
Part of Application Level Payload
Other:

5.5: Do you use an anonymisation tool? If yes which one?

Please choose **all** that apply
Tcpdpriv
Crypto-PaN
Ip2anonip
Ipsumdump
Anonymizer
A proprietary one
Other:

6 - General Information

6.1: Have you started a business coalition with other ISPs? Why or why not?

Please write your answer here:

6.2: Do you have close relationships or contracts with other ISPs?

Please choose **only one** of the following:
Yes
No

[Only answer this question if you answered 'Yes' to question '6.2 ']
6.2.1: Of what nature are these contracts with other ISPs?

Please write your answer here:

7 - Feedback

7.1: What final questions and/or remarks do you have on this survey?

Please write your answer here:

Submit Your Survey
Thank you for completing this survey. Please fax your completed survey to: .

Appendix B Project by project results of the survey

The project by project results are presented in the following sections of this appendix. Our main information gathering tools was the MOME questionnaire. A second information source was the information published by the different projects in their respective Web sites and public project deliverables. All projects are studied using the following structure:

- Objectives
  - Scientific Objective
  - Measurement objective
- Networking environment
- Measurement Process
  - Measurement set-up
  - Measurement tools
  - Measurement results
- Analysis
  - Analysis tools
  - Analysis results

When no reliable information could be gathered neither through the question nor from the project's publications, the point is skipped.

B.1   6QM (Project No. IST-37611)

Objectives

Scientific Objective

The project 6QM is devoted to research and development of measurement technologies for Quality of Service in IPv6 networks.

Measurement objective

the project has created create a comprehensive system integrating the various required functions for QoS measusurement, such as packet capturing, precise time-stamping, data collection, QoS metrics derivation (delay, loss, jitter etc.) and result presentation. Main objectives are network monitoring, and active and passive IP QoS measurements.

Networking environment

IPv6-enabled fixed IP networks, e.g. 6Net, 6-Bone

Measurement Process

Measurement setup

The setup is comprised of active traffic sender, receiver, intermediate routers and two monitoring probes along the path. This represents a setup with active probes at the network edges, and passive probes listening on dedicated links.

Measurement tools

FOKUS OpenIMP, mgen, trpr, pathchirp, tcpdump, tcptrace

Measurement results

Packet and volume counters, packet traces, packet Ids

Analysis tools

For Analysis 6QM has used the developed qos computation server (openimp), as well as tcptrace, tcpdump, and trpr tools.

Analysis results

IP QoS for measured traffic for metrics such as one-way delay and jitter. Basic packet and volume accounting as well.

B.2   *DIADEM FIREWALL (Project No. IST-2154)*

Objectives

Scientific Objective

The goal of Diadem is to develop security solution for secure broadband services, by combining flexible high-speed packet processing, algorithms for intrusion detection, and policy-based techniques for automated configuration and decision-handling.

The project aims for the development and deployment of network components that enable service providers to offer to their customers secure broadband services in an effective and cost-efficient way. This includes the following objectives:

- Design and implementation of an architecture for provider-controlled distributed high-speed edge firewall devices with policy-based control
- Develop and deploy enhanced techniques capable of detecting a wide range of security violations, in particular detecting DDOS (Distributed Denial of Service) attacks
- Support enhanced detection capabilities using distributed monitoring of application traffic
- providing an effective protection against DDOS attacks
- Ensure fair, coherent, and efficient enforcement of security policies

The proposed architecture shall ensure high performance in combination with functional flexibility using programmable hardware for classification, filtering, sampling and measurements.

Measurement objective
- high speed network monitoring
- sampling
- intrusion and attack detection (IDS)

Networking environment

A testbed set-up is proposed for ISP/enterprise scenario and for firewalls operating between operator networks. Fixed IP based networks are the target.

Measurement Process

Measurement set-up
The setup includes a router and different firewall solutions (free (netfilter) + commercial)

Measurement tools
Different modules, one per known attack will be developed.

Measurement results
results of IDS system are input for decision of policy engine which controls the behaviour of the firewall

Analysis results
- detected attacks

- alarms signals

- firewall configurations

B.3   EUQOS (Project No. IST-4503)

The key objective of EuQoS is to research, integrate, test, validate and demonstrate end-to-end QoS technologies to support the infrastructure upgrade for advanced QoS-aware applications over multiple, heterogeneous network domains, belonging to research, scientific and industrial communities.

The project will deliver the EuQoS system which will support the delivery of end to end QoS. As QoS is primarily a challenge for the access network, the EuQoS system will be developed and trialed on various types of research access networks with the GEANT core providing Pan European support. This heterogeneous infrastructure, which models the production networks of the future, requires a QoS technical solution that has not been synthesised to date. The EuQoS project will propose and develop new QoS mechanisms which build upon the state of the art and incorporate the following mechanisms: Monitoring and Measurements, Admission Control, Failure Management, Signaling & Service Negotiation, Security and AAA, Charging and Traffic Engineering & Resource Optimisation.

Objectives

Scientific Objective

The EuQoS project develops the architecture for providing end-to-end QoS in heterogeneous networks. The design and implemented system will be tested by performing measurements in the trial network, build based on different access network technologies. In addition, measurements are performed for supporting some network functions, in particular traffic engineering and admission control.

Measurement objective

The role of the Monitoring and Measurement System in EuQoS is threefold:

- to provide measurement facilities for trials – to validate QoS provided by EuQoS architecture and to assess scalability of the solution,

- to support Traffic Engineering and Connection Admission Control functions in EuQoS system,

- to support network operators by performing on-line QoS monitoring.

Networking environment

The EuQoS project will build an European wide research testbed to deploy the EuQoS solution over the access network infrastructure testbeds interconnected by the GÉANT backbone network. The tesbeds will be build based on different access network technologies: LAN, WiFi, xDSL, UMTS, inter-connected by the IP core consisting of GEANT and the NRENs.

Measurement Process

Measurement setup

The monitoring and measurement tools will be deployed in all EuQoS testbeds. The measurements are performed only at the IP layer, following the specified measurement plan. The Measurement Points (MPs) are located in the points, where the EuQoS Classes of Service begin and end to operate. The measurements will be performed in carefully designed artificial trial scenarios, using traffic generators and EuQoS applications to produce packet traffic.

Measurement tools

The EuQoS Monitoring and Measurement System is based on tools, which were developed by the project partners and are further enhanced to take into account specific requirements of the project. In particular, for supporting the trials the following tools were developed:

- NetMeter tool for measuring QoS parameters using the active method,

- Background Traffic Generator Script (BTG) to generate an arbitrary amount of flows through the MGen traffic generator,

- Trace-based Traffic Generator (TrTG) for re-playing the packet-level traces produced with the help of EuQoS packet level simulator (SIM-EuQoS-PTL),

- End-to-end Test Tool (E2ETT) for allowing users to test the QoS in UMTS network.

The following tools were developed for supporting EuQoS system functions:

- Link Load Measurement Tool (LLMT) for measuring the average traffic throughput on the inter-domain links,

- Topology Acquisition Tool (TAT) for collecting from border routers the information about available QoS paths established by EQ-BGP protocol.

The following tool will be used for QoS monitoring:

- OreNETa for on-line passive monitoring of the EuQoS Classes of Service.

In addition, the following commercial tools are used:

- Chariot for measuring QoS using the active method.

Measurement results

Following the main objectives of measurements in EuQoS, the following measurement results will be collected:

- Measured QoS parameters (off-line), for prooving the correct design of EuQoS Classes of Service,

- Link load measurements, for supporitng long-term Traffic Engineering function,

- Inter-domain routing information for supporting end-to-end Connection Admission Control function,

- Measured QoS parameters (on-line), as support for netowrk operators.

Analysis tools

Currently, additional analysis of measurement results is not planned.

Analysis results

Currently, additional analusis of measurement results is not planned.

B.4   Euro NGI (Project No. IST-507613)

EuroNGI's main target is to create and maintain the most prominent European centre of excellence in Next Generation Internet design and engineering, leading towards a leadership in this domain.

Objectives

Scientific Objective

The project WPs deal with different research areas related with future IP-based networks. Among them, the WP JRA4.3 aims to deploy a measurement platform and to process the results in order to optimize measurement point's location and measurement traffic. On the other hand, the goal of WP JRA5.1 is to perform research on traffic characterisation and modelling.

Measurement objective

IPAM project (Integration of Passive and Active Measurement Platforms) is a Euro-NGI internal project. This project aims at the investigation of solutions for an effective integration of passive and active measurements. As a step towards this end, the project have developed platform to integrate the various traffic tools under development by the partners. This platform has been called EMP (Euro-NGI Measurement Platform) public available in http://193.136.92.121/emp/emp.php. Fortunately, these tools cover already all the elements required for a complete and integrated traffic monitoring solution, i.e., infrastructures for both active and passive measurements and statistical analysis tools. In particular, it includes an infrastructure for passive measurements, called DPMI (Distributed Passive Measurement Infrastructure), a tool for the statistical analysis of measured data, called Tstat (TCP Statistic and analysis tool), and infrastructures for active measurements, called Saturne and J-OWAMP (Java Implementation of OWAMP) respectively.

Networking environment

The project deals with different research areas related with future IP-based networks.

Measurement tools

DPMI (http://inga.its.bth.se/projects/dpmi/)is a framework designed to allow for efficient use of measurement equipment on network links. Currently there is no other technology that provides the service that the DPMI provides (to the best of our knowledge), the closest would be a wiretap attached to a hub. The DPMI does however provide more functionality than this; for instance filtering, selective distribution of measurement data and time synchronization. The DPMI framework is focused on passive network measurements and as such it does not provide any analysis or visualization of measurement data.

J-OWAMP (http://www.av.it.pt/jowamp/) is a Java implementation of the

One-Way Active Measurement Protocol (OWAMP) to perform active measurements

of one-way delays and losses between hosts.

Saturne evaluates the One Way Delay (OWD) and the losses of packets in a network. Saturne is either an active or a passive measurement tool. It can introduce a dedicated flow for measurements that will be aggregated to applications flows during its routing in the network, giving a precise approximation of the delays and the losses observed by application packets. On the other hand, Saturne can also measure the IPv6 application packets one way delays and losses by introducing a timestamp in the packets themselves.

The IPAM project also includes a research activity with the objective of developing a Peer-to-peer measurement architecture that integrates traffic measurements and traffic analysis.

Measurement results

The project develops a measurement infrastructure but does not perform actual measurements.

Analysis tools

Tstat (http://tstat.tlc.polito.it/) analyzes traces in real time, using common PC hardware, or starting from previously recorded traces in various dump formats, such as the one supported by the libpcap library, and the DAG systems used to monitor Gigabit speed links. It is written in standard C, and runs on Linux systems, and should run also on other UNIX-like operating systems.

Besides common IP statistics, derived from the analysis of the IP header, Tstat also rebuilds each TCP connection status looking at TCP headers in the forward and backward packet flows.

Analysis results

The project uses the packet level traces for extensive studies on traffic characterisation and modelling.

B.5   EVERGROW (Project No. IST-33234)

The EVERGROW project measurement activities are handled by the WP Measurement and modelling which conduct real-time measurements of network traffic and topology. It consists of the ETOMIC et DIMES projects. European Traffic Observatory Measurements Infrastructure (ETOMIC) is a paneuropean measurement platform which consists of measurement nodes synchronized by GPS and using Endace DAG cards (transmission in the range of nanoseconds), and a management kernel which handles software upload and experiment execution. DIMES (Distributed Internet Measurements and Simulations) is a distributed scientific research sub-project, aimed to study the structure and topology of the Internet.

Objectives

Scientific Objective

ETOMIC sub-project builds a measurement infrastructure to carry out high temporal resolution, globally synchronized, active measurements between measurement boxes. The system generates maps and track internet dynamics over time.

Measurement objective

Performing real-Time IP monitoring of the internet is the objective of the project. The active and passive measurements provide:

1. a picture of the fast changes of the Internet enabling a new kind of network tomography

2. and aim to visualise the Internet topology.

The measurement objectives are to estimate path parameters, like physical bandwidth, utilization, traffic granularity, internal link queuing delay with end-to-end active probing

Networking environment

The measurement infrastructure consists of measurement nodes with hardware components, installed in various european research centers

Measurement Process

Measurement setup

The paneuropean traffic measurement infrastructure consists of 1) SW-based measurement clients (DIMES), for topology discovery 2) and HW-based measurement nodes (ETOMIC boxes): In the nodes are installed DAG cards to capture the traffic, network interfaces/probes to generate traffic, and GPS synchronised nodes. These equipments and software are installed in various sites over Europe. For the ETOMIC sub-project, the measurement setup is as follow: the sender node injects packet pairs into the network with a given input spacing, while the receiver node measures the output spacing between the probe pair. The estimation is based on the analysis of the output spacing - input spacing function.

Measurement tools

DAG Cards for monitoring the traffic are used in the ETOMIC subproject. The Evergrow project developed some tools to send and capture packets with the DAG monitoring card provided by Endace. They developed an end-to-end bandwidth parameter estimation tool and a measurement tool to perform network tomography. It is planned to make public license to the bandwidth estimation tool under GPL license.

Measurement results

The project has built a distributed data repository where traffic measurement data is publicly available. Raw measurements results: back-to-back packet-pairs (with different destination) are used to measure one way delay data to their different destination, which are decomposed to a queuing delay of a given link.

Analysis tools

Self developed tools based on the DAG C API provided by Endace, some original Endace tools, and some standard software like tcpdump.

Analysis results

Processed measurement results: UDP probe packets,captured at the receiver node, are used in the measurements.

It is free of charge to register (request an account) to the Central Management System of the Etomic Infrastructure where any registered user can share their raw or processed measurement data. In that way any registered user can use the publicly shared data.

The results of the monitored traffic are displayed in realtime and presented into maps.

B.6   GEANT/DANTE

The GÉANT project is a collaboration between 26 National Research and Education Networks representing 30 countries across Europe, the European Commission, and DANTE. Its principal purpose has been to develop the GÉANT network - a multi-gigabit pan-European data communications network, reserved specifically for research and education use. The project also covers a number of other activities relating to research networking. These include network testing, development of new technologies and support for some research projects with specific networking requirements.

Objectives

Scientific Objective

GEANT is a working network. Therefore, the main objective of performing measurements is to support the network operations by monitoring the carried load, as well as the packet-level QoS parameters between selected measurement points.

Measurement objective

Measurements are perfomred with several goals, among them:

(1) supporing traffic engineering,

(2) monitoring QoS parameters,

(3) supporitng security functions, i.e. intrusion detection,

(4) SLA/SLS monitoring,

(5) supporting failure management and troubleshooting of network problems.

Networking environment

GEANT operates a pan-European backbone network, interconnecting the National Research Networks (NRENs).

Measurement Process

Measurement setup

The measurement tools are deployed in the Measurement Points important from the point of view of monitoirng network traffic and QoS parameters. In particular, MPs are located on the Points of Presece (PoPs) and in the NRENs.

Measurement tools

GEANT uses freely available measurement tools, as well as the tools specially developed for GEANT. Among them the following tools are used:

- Ping, for connectivity and RTT measurements,

- Traceroute, for checking connectivity and routing state,

- Inter-mapper, for link monitoring using SNMP,

- Cricket, for monitoring equipment interfaces using SNMP,

- Taksometro, for long-term network monitoring,

- Multicast beacon, for active measurements of QoS in multicast trees,

- Multicast per group monitoring tool,

- Rancid looking glass, for executing queries on remote routers,

- Nagios, for monitoring different parameters, creating reports and alarms,

- Mezeuon, for monitoring traffic on router interfaces.

Measurement results

GEANT collects a large number of measurement results. In addition, monthly reports are created. Most of the results are related with on-line monitoring of the operational network and are available only to the network admisnistrators.

Analysis tools

Several tools are used for analysing the raw measurement results. Among them the following tools are used:

- Wheathermap, for visualisation of results obtained by taksometro tool,

- Purgatorio, for analysing traffic statistics and creating long-term traffic matrices,

- DoS detection tool, for detecting abnormal patterns in the carried traffic.

Analysis results

The measurements results are analysed for providing additional information usefull for the network operators. The analysis results include results visualisation, estimation of traffic matrices, as well as detecting attacks and other abnormal situations.

B.7   GEANT2 (Project No. R1-2003-511082)

GEANT2 is the successor network to the pan-European GEANT network. It will provide researchers across Europe with a much enhanced service, focusing on performance and user support. It will employ a new 'hybrid architecture' encompassing optical transmission and switching technologies to cater for the different types of traffic that are an increasing feature of network usage as researchers exploit the exceptional performance that GEANT has made available. The network itself is complemented by a targeted programme of research activities and publicity and dissimination.

For measurement and monitoring activities refer to the description of GEANT in the previous paragraph.

B.8   LOBSTER

Objectives

Scientific Objective

The overall objectives of the LOBSTER project are the following 1) to deploy a pilot advanced European Internet Traffic Monitoring Infrastructure based on passive monitoring sensors at speeds starting from 2.5 Gbps, and possibly up to 10Gbps; 2) to realize the appropriate data anonymizing tools that will prohibit unauthorized tampering with the original traffic data; 3) to provide anonymized data traffic information on a regular basis.

Measurement objective

The main goal of LOBSTER is to create a measurement infrastructure that can be used for all types of passive measurements. The measurements aim for building a collaborative passive monitoring. With extended IPFIX, extra attributes are added to the IPFIX record to get a

better overview of the quality of flows on the network. Some of the extra attributes that are available are histograms of packet size and

distance between consecutive packets and minimum and maximum bit rate during the lifetime of the flow.

Networking environment

The LOBSTER infrastructure is deployed across NRENs and ISPs in Europe and is comprised of testbeds and operational networks.

Measurement Process

Measurement setup

To better compare results multiple Lobster probes are used to generate the extended IPFIX. These monitoring probes send extended IPFIX to a collector that processes them and inserts high level reports into Stager. In this example, IPFIX records is the raw measurement data. In other Lobster applications, packets or the header of packets can be the raw measurement data.

Measurement tools

Lobster does not create any new tools from scratch, but improves on

several open source tools:

MAPI, http://mapi.uninett.no , GPL

NERDD, http://www.nerdd.org , Apache license

Stager, http://software.uninett.no/stager/ , GPL Lobster created a small script that reads the raw IPFIX records, processes them and inserts reports into the Stager application for presentation.

The project makes use of HW and SW tools including

1. DAG cards

2. MAPI, or Monitoring API, a multi-user programming interface designed to simplify the development of network monitoring software and allows users to express their monitoring needs in a device-independent way;

3. Stager, a system for aggregating and presenting network statistics.

MAPI now has full support for IPFIX. tcpdump/libpcap was used for capturing the raw data which was then pre-prosessed with ethereal.

Measurement results

Lobster supports the storing of raw measurements, but it is up to the owner of each monitoring probe to decide what he actually want to store. MAPI can store full packet traces in either pcap or DAG ERF format.

The project plans to provide periodic summaries of anonymized traffic data at regular intervals.A distributed version of MAPI, DiMAPI, is used for generating the extended IPFIX records. The raw data is processed to create reports that for example give information about average jitter in flows or distribution of jitter.Lobster contain an advanced anonymization framework for easier sharing of data.

Analysis tools

e.g. an application, that can run on top of LOBSTER, is extended IPFIX which presents reports in the Stager application.

B.9   METAWIN

The METAWIN project is funded by mobilkom austria, Kapsch CArrierCom and co-funded by the Austrian research programm "K-plus".

The aim of the project is to extensively monitor traffic in Mobilkom Austria's live GPRS and UMTS network using non intrusive packet capturing methods. Based on traffic traces network performance can be evaluated and models for user- and control plane traffic can be derived. Traffic models will be used as an input to traffic generation. Realistic traffic generators are in turn an important pre-requisite to perform meaningful measurements with GPRS and UMTS equipment and simulations allowing optimization of the Mobilkom Austria network based on sound engineering guidelines.

Objectives

Scientific Objective

The main objectives of METAWIN measurements are: to analyse traffic patterns, to gain quantitative understanding of network

performances and to detect network anomalies. Based on traffic traces from operational UMTS network, network performance can be evaluated and models for user- and control plane traffic can be derived. Traffic models will be used as an input to traffic generation. Realistic traffic generators are in turn an important pre-requisite to perform meaningful measurements with GPRS and UMTS equipment and simulations allowing optimization of the Mobilkom Austria network based on sound engineering guidelines.

Measurement objective

The project collects packet-level traces with the aim of further statistical analysis.

Networking environment

The project aims at monitoring traffic in operational UMTS and GPRS network in Austria. The following interfaces are monitored: Gn, Gi,

Gb, IuPS.

Measurement Process

Measurement setup

The project has developed a large-scale passive monitoring system, inlcuding a parser of the whole protocol stack of the 3G Core Network. All core network interfaces (Gi, Gn, Gb, IuPS) are monitored using the DAG cards.

Measurement tools

The project uses the DAG cards for passive monitoring of selected links. The project has developed a tool for real-time large-scale monitoring

and analysis of the whole 3GPP protocol stack (user data + signaling) in the core network of 3G. The tool is proprietary (commercial exploitation is under consideration).

Measurement results

The project collects anonymized packet-level traces, which are stored in a proprietary format. The traces are not available for public since the data is regarded as business critical by the operator (Mobilkom Austria).

Analysis tools

The project uses specially modified version of TCPSTAT tool for statistical post-processing of the collected traces. In addition, IDS tools Snort and Bro are used.

Analysis results

One of the research goals is to evaluate the RTT times of TCP connections in the UMTS network. This is done by appropriate post-processing of packet-level traces collected at selected capture points. The objective is to provide in-depth analysis of effects contributing to performance of TCP traffic in the UMTS network.

B.10   MUPBED (Project No. IST-511780)

The main goal of MUPPET is to integrate and validate, in the context of user-driven large-scale test beds, ASON/GMPLS (Automatically Switched Optical Network / Generalised Multi Protocol Label Switching) technology and network solutions as enablers for future upgrades to European research infrastructures.

Objectives

Scientific Objective

The objectives of the project are (1) to identify service and network requirements of high-end applications for European research environments, (2) to define the ASON/GMPLS features matching the above requirements and enabling the penetration of broadband services in Europe, (3) to find and experimentally validate solutions for interoperability between different network domains, (4) to assess the ability of ASON/GMPLS solutions to support demanding research applications, such as Grid computing, through lab and field trials with a large user community (including NRENs), and (5) to develop guidelines for the introduction of ASON/GMPLS technologies and ultra-broadband services in future European research infrastructures

Measurement objective

SDI-over-SDH and other advanced

protocols will be evaluated, as well as QoS parameter enforcement (delay, jitter, loss) in the IP

stack for applications such as transmission of uncompressed video, high quality video conference for distributed collaborative work and education, massive data transfer, grid platform and virtual Organisations.

Networking environment

Mainly optical networks (IP/MPLS, ASON/GMPLS)

Measurement Process

Measurement setup

The MUPBED test-bed consists of two

ASON/GMPLS network test-beds (T-Systems, TILAB), a GMPLS network (ACREO), an Ethernet

based network (PSNC) and an IP/MPLS network test-beds (TID), and participating and supporting

NRENs (from Denmark, Sweden, Germany, Poland, Spain, Italy)

Measurement tools

Measurement results

Analysis tools

Analysis results

B.11   NOBEL (Project No. IST-506760)

The main goal of NOBEL is to carry out analysis, feasibility studies and experimental activities on innovative architectures, technologies solutions and for core and metro networks supporting broadband services.

Objectives

Scientific Objective

The objectives of the project are (1) to define network architectures, evolutionary guidelines and a roadmap for core and metro optical transport networks towards intelligent data centric solutions (based on optical and electrical switching, e.g. ASON/GMPLS); (2) to identify main drivers for the evolution of core and metro optical networks supporting end-to-end broadband services, and to derive technical requirements in accordance to this; (3) to study efficient traffic/network engineering and resilience strategies in multi-layer/domain/service networks and interworking issues; (4) to assess and describe social and techno-economic aspects regarding the deployment of network solutions and technologies for intelligent and flexible optical networks; (5) to evaluate solutions for providing end-to-end Quality of Service;

(6) to identify network architectures, concepts and solutions for advanced packet/burst switching; (7) to propose simplified strategies for the end-to-end management and control of intra/inter-domain connections in multi-layers networks (e.g. IP over Optics); (8) to find enhanced solutions and technologies for physical transmission in transparent optical networks; (9) to identify the key functional requirements from the architectural, management, control and transmission viewpoints and translate them into specifications, feasibility studies and prototype realizations for multi-service/multi-layer nodes with flexible client and adaptable transport interfaces;

(10) to assess existing technologies, components and subsystems in terms of efficiency and cost-effectiveness, deriving requirements and specifications for next generation components and subsystems, with respect to the network solutions identified; and (11) to integrate the prototype solutions of for multi-service/multi-layer nodes into existing test beds for experiments on advanced functionalities.

Measurement objective

The goal of the measurements is to validate the integration of testbeds.

Networking environment

Mainly optical network (IP/MPLS, ASON/GMPLS)

Measurement Process

Measurement setup

The upper layer of the NOBEL testbed is composed of IP/MPLS routers. The optical GMPLS layer is divided into three domains, that have different transparency capability and dynamic routing capabilities. There is also a management layer, which allows the assessment of the network management and control aspects.

Measurement tools

Measurement results

The measured properties include inter-arrival time, holding time, total traffic, BER.

Analysis tools

Analysis results

B.12   SCAMPI (Project No. IST-32404)

Objectives

Scientific Objective

SCAMPI objectives are: 1) to develop a scaleable monitoring platform for the Internet 2) to develop a network adapter, initially at 10 Gbps speeds, tailored to the needs of monitoring tools 3) to develop monitoring and measurement tools for denial-of-service detection, SLS auditing, quality-of-service, traffic engineering, traffic analysis, billing and accounting.

Measurement objective

The tests validate the correctness of measured QoS characteristics: one-way delay, jitter and packet loss, in a controlled environment.

Smartbits network performance analysis system, generate the traffic with random payload.

Networking environment

The infrastructure consists of testbeds and operational environments.

Measurement Process

Measurement setup

Testing is carried out in a controlled environment.

Measurement tools

The measurement tools used and developed are DAG cards, traffic generators (SmartBits,...), Ntop, Snort.

Measurement results

Measurement results are published on the project web site. Traces are stored on a web repository or are available on request from project partners.

Analysis tools

Analysis results

B.13   ATHENA (Project No. IST-507312)

This project considers that if proper decision will be taken for the digital switchover (taking into account the networking aspect of the new television) it will also provide a solution for the second problem (the broadband access for all citizens). It presents an approach towards the solution of the digital switchover that comprises the use of the DVB stream for interconnecting next generation network (NGN) nodes, by the use of regenerative configurations. The utilisation of regenerative configurations enables for the realisation of a virtual common Ethernet backbone that can be exploited by 3G/UMTS and B3G operators and broadcasters, besides enabling for broadband access for all citizens. Such a configuration enables for multi-service capability, as the regenerative DVB-T creates a single access network physical infrastructure, shared by multiple services (i.e. TV programmes, interactive multimedia services, Internet applications, etc.). Validation of such a broadband access for all citizens infrastructure, based on the proper adoption of digital switchover, will be realised in a real condition trial in a medium-sized city (Heraklion city, Crete, Greece).

The above trial includes the implementation, testing and validation of a spectrum efficient real time dynamic management of the available bandwidth, for supporting the variety of heterogeneous bit rate services, and of a traffic policy mechanism, for UMTS users on the move, for seamless reception of IP data when transition from one UHF channel (DVB-T stream) to another is required.

Objectives

Scientific Objective

The objective of this project is the validation of a broadband access for all citizens infrastructure based on the proper adoption of digital switchover.

Measurement objective

The measurement objectives are to perform functional tests of the system

Networking environment

UHF channel in Heraklion, Crete

B.14   BROADWAN (Project No. IST-1930)

BROADWAN encompasses a total solution for universal hybrid broadband access networks for fixed and nomadic users. This will be achieved through many innovations within global coverage architecture, new generation adaptive equipment and automatic network planning and management software. The 25 BROADWAN partners comprise operators, industry, academia, and consultancy from 10 countries representing all parts of Europe. The significant numbers

Objectives

Scientific Objective

BROADWAN has three major goals:

1) Develop an economical realistic network architecture to provide true broadband services for all citizens in Europe.

2) Bring European industry in the lead for next generation wireless solutions.

3) Motivate advanced utilisation of broadband services at all levels of the society by performing wireless demonstrations and trials in rural areas.

Measurement objective

The measurement objectives concentrate on functional tests and measurements for debugging. Communication flows are analysed with respect to service evaluation and validation. The services and applications to be tested as well as the demonstration platforms and testbeds are described in D11 "A multi-service validation procedure"

Networking environment

The BROADWAN test environment has 3 demonstration platforms. France for VoD, EoD, P2P; Spain for satellite access/DVB-RCS solutions; Norway for IPv6-multicast video streaming). Further a testbed interconnecting two sites in Austria and UK is available. The testbed focusses are on All-IPv6 and ad-hoc networking, video multicast and service discovery.

Measurement Process

Measurement setup

BROADWAN deploys exsiting measurement tools in testbeds and demonstrators

Measurement tools

The project makes use of existing measurement tools. The following tools are planned to be used: tcpdump, Chariot, Sniffer Pro, Ethereal, Service Assurance Agent (CISCO), IPANEMA, NIMI, Rude, Netmate

Measurement results

From the tools used, traces and QiS parameters will be available. The final results will be reported in deliverable D25 "Summarised conclusions from trials and demonstrations, and final recommendations on how to provide full coverage"

Analysis tools

Trace analysis tools like Ethereal are planned.

Analysis results

Analysis result will be the validation of the broadband networking architecture.

B.15   DAIDALOS (Project No. IST-506997)

Objectives

Scientific Objective

The Daidalos vision is to seamlessly integrate heterogeneous network technologies that allow network operators and service providers to offer new and profitable services, giving users access to a wide range of personalised voice, data, and multimedia services. These goals include an implementation of seamless and fast handover between mobile clients, terminal and session mobility, AAA and auditing, QoS support and SLA verification.

Measurement objective

The measurement objectives in Daidalos are manifold and involve passive as well as active measurement tasks for:

- volume accounting for charging

- session monitoring (service duration) for charging and for checking traffic reservations

- monitoring of router queues for traffic shaping optimization

- SLA verification purposes

Networking environment

The project will test its solution in a rich heterogeneous networking environment including mobile IPv6 with fast handover, fixed and wireless (WLAN) access, DVB-T broadcast, AAA, multimedia and multicast services, SIP, and VoIP applications active in the network.

Measurement Process

Measurement set-up

Daidalos features multiple software meter probes (one per access router), controlled by one management server per domain.

Measurement tools

The OpenIMP measurement platform from Frauhofer FOKUS including project specific extensions is used. Data export from the measurement probes to a central database features the IPFIX protocol.

Measurement results

From the probes accounting, session and QoS records are transferred using the IPFIX protocol via an accounting gateway to the AAA server, or to an SLA-Verification component, or to the QoSBroker component which governs the router queues on each access router.

Analysis tools

For the analysis an accounting gateway, impd measurement probes (part of openimp), and an SLA verification component are in use.

Analysis results

Result flow records are comprised of packet and byte counters and QoS data records. Analysis tools convert these data into accounting records (Diameter), and decisions for the traffic shaping process.

B.16   DEISA (Project No. RI-2002-508830)

DEISA is a consortium of leading national supercomputing centres that currently deploys and operates a persistent, production quality, distributed supercomputing environment with continental scope. The purpose of this FP6 funded research infrastructure is to enable scientific discovery across a broad spectrum of science and technology, by enhancing and reinforcing European capabilities in the area of high performance computing. This becomes possible through a deep integration of existing national high-end platforms, tightly coupled by a dedicated network and supported by innovative system and grid software.

Objectives

Scientific Objective

DEISA has deployed a dedicated network for the coupling of supercomputers, completely isolated from the intranets of the participating sites.

Measurement objective

The measurement objectives are to give DEISA-participants a view onto the actual network usage, availability and reliability of the dedicated network and to give the network staff some hints on arising problems as well as to monitor the SLAs.

Networking environment

The DEISA-network is up and running with some major sites for about 15 month now. It is designed as a dedicated network for the coupling of supercomputers and completely isolated from the intranets of the participating sites and, of course, the internet. It is deployed by using virtual leased lines with guaranteed bandwidth of the national research network providers (NRENs) and DANTE/GEANT/GEANT2. The technique that is used for bandwidth reservation differ from NREN to NREN (separated physical links, VCs, Qos/CoS).

Measurement Process

Measurement setup

For monitoring end to end network parameters like throughput and packet loss, probe-applications, like iperf and some ping-variations, are running at every participating site and gathering and presenting these informations at a DEISA-internal accessible web-server. Furthermore this server is presenting consolidated network parameters and statistics that are available for DEISA from the different participating NRENs and partner-sites as well as some major status information regarding the availability of different hosts at the participating sites. For problem analysis, especially at the setup phase of the network, the provider test equipment is located "in the middle" of their cloud of responsibility.

Measurement tools

The project has developed some probe-tools consisting of basic network-tools and -applications in combination with the gathering and visualization by some free or GPL available software of the measured performance data.

Measurement results

TCP and UDP throughput measured by iperf, packet loss by iperf and ping, router and switch interface statistics by SNMP (mrtg) and RMON (Netscout NGenius PM).

Analysis results

Statistics aggregated over time.

B.17   ENTHRONE

The provision of an integrated management based on the end-to-end QoS over heterogeneous networks and terminals is considered to be a key element for the successful mass market provision of audio-visual services, that would produce revenues for the content/service providers and network operators. The ENTHRONE project proposes an integrated management solution which covers an entire audio-visual service distribution chain, including content generation and protection, distribution across networks and reception at user terminals.

Objectives

Scientific Objective

The scientific objective of the project is to deliver audio-visual services to Content Consumers in different receiving conditions (mobile, stationary,…) over a variety of networks.

Measurement objective

The goal is to measure the QoS perceived by users when receiving audio and video services over different types of networks.

Networking environment

The project proposes an integrated management

solution which covers an entire audio-visual service distribution

chain, including content generation and protection, distribution

across a variety of networks and reception at user terminals.

Measurement tools

Perceived Quality (passive) Meters will be used in the ENTHRONE end-to-end QoS architecture (source D25).

B.18   Euro6IX (Project No. IST-32161)

Objectives

Scientific Objective

The project main objective is to deploy IPv6 IX infrastructure to research, test and validate IPv6-based applications and services.

Measurement objective

Measurements are performed for monitoring and tracking of the IPv6 network traffic. The measurement objectives are to control routers operation, get network usage statistics and therefore control the amount of network traffic, and to identify the most used services.

Networking environment

The Euro6IX infrastructure is organised in three levels: 1) IX-level: Regional native IPv6 exchanges;

2) Backbone-level: Pan-European core network that interconnects the regional exchanges;

3) Node-level: Service providers.

Measurement Process

Measurement tools

Some of the tools used are MRTG, Looking Glass, TID Pingstat tool, Topaz the IDS tool . MRTG has been ported to support IPv6 and tested to show IPv6 network reachability of the Euro6IX POPs; monitoring and tracking of the IPv6 network traffic.

Measurement results

Some results might be available at project partners, but the project hasn't established a uniform measurement result publishing policy.

B.19   EVEREST (Project No. IST-1858)

The objective of the EVEREST project is to devise and assess a set of specific strategies and algorithms for access and core networks, leading to an optimised utilisation of scarcely available radio resources for the support of mixed services with end-to-end QoS mechanisms within heterogeneous networks beyond 3G.

Objectives

Scientific Objective

The objective of the projects is to measure end-to-end QoS in a network scenario where a B3G heterogeneous access network interfaces with a DiffServ core network.

Measurement objective

The measurements should allow comparing performance metrics (throughput, delay, jitter, packet loss) of a flow in different points of the network.

Networking environment

The testbed uses a network emulator for the UMTS and IP core networks and it consists of an application

server (to generate a streaming or videoconferencing flow), the network emulator and a client. All PCs used in the testbed have Linux as operating system (source: D12, January 2005).

Measurement Process

Measurement setup

Packets are captured with the Oreneta tool in different points of the network. The info is then sent to an analyser, which is part of Oreneta.

Measurement tools

Oreneta is a platform for real-time network analysis developed in UPC (Technical University of Catalonia). Oreneta has two components, a meter and an analyzer.

Analysis tools

The analysis of measurement results is also performed with the Oreneta tool.

B.20   MUSE (Project No. IST-507295)

The overall objective of MUSE is the research and development of a future low-cost, full-service access and edge network, which enables the ubiquitous delivery of Broadband services. The project addresses the network architecture, techno-economics, access nodes, solutions for the first mile, and interworking with the home network. Solutions will be evaluated in end-to-end lab trials and promoted in standardisation.

Objectives

Scientific Objective

Research on access and edge network architecture, access and edge node functionality, innovations of first mile solutions, and the interworking with the home and SOHO network.

Measurement objective

QoS testing. Parameters examined for Video conference and Streaming Video services: Delay, Jitter, Packet loss, Throughput; For Web browsing and bulk data transfer: Response Time,

Download Time; For Interactive Gaming: Delay, Packet loss, Throughput

Networking environment

The networking environment is a hybrid access network of ATM and packet (Ethernet, IP) network elements and CPE with embedded service awareness and application enablers.

B.21   PAN-NET

Objectives

Scientific Objective

Analysis and Design of Advanced Multiservice Networks supporting Mobility, Multimedia and Internetworking:

(1) Internet topology (VTT), (2) Traffic Engineering in IP networks (HUT), (3) QoS mechanisms for the Internet (HUT), (4) Queueing theory for fractal traffic (VTT), (5) GPRS and other traffic measurements (VTT), (6) Multicast in mobile communications systems (HUT)

Networking environment

PAN-NET does research in multiple areas

B.22   SATLIFE (Project No. IST-507675)

Satellite R&D project using the first multimedia on-board processor, the AMERHIS system, based on the satellite standards DVB-RCS and DVB-S.

Appendix C Wireless tools

This appendix shows a compilation of freeware and commercial wireless tools. All these tools were examined when preparing chapter 5.

Tool	OS	Description
Aerosol	Win32	Aerosol is a prism2 chipset wireless access point detecting application.
AirSnort	Linux	AirSnort is a wireless LAN (WLAN) tool which recovers encryption keys. AirSnort operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered.
Dstumbler	BSD	Dstumbler is a wardriving/netstumbling/lanjacking utility for the BSD operating system that attempts to provide features similar to netstumbler in a fast and easy to use curses-based application. It is part of the bsd-airtools package released by Dachb0den Labs, which provides a complete BSD based tool set for 802.11b penetration testing.
MacStumbler	MacOSX	MacStumbler is a utility to display information about nearby 802.11b and 802.11g wireless access points. It is mainly designed to be a tool to help find access points while travelling, or to diagnose wireless network problems. Additionally, MacStumbler can be used for "wardriving", which involves coordinating with a GPS unit while travelling around to help produce a map of all access points in a given area. MacStumbler requires an Apple Airport Card and MacOS 10.1 or greater. MacStumbler doesn't currently support any kind of PCMCIA or USB wireless device.
NetStumbler	Win32	NetStumbler is a tool for Windows that allows you to detect Wireless Local Area Networks (WLANs) using 802.11b, 802.11a and 802.11g. It has many uses: Verify that your network is set up the way you intended. Find locations with poor coverage in your WLAN. Detect other networks that may be causing interference on your network. Detect unauthorized "rogue" access points in your workplace. Help aim directional antennas for long-haul WLAN links.
MiniStumbler	WinCE	MiniStumbler is a tool for Windows CE that allows you to detect Wireless Local Area Networks (WLANs) using 802.11b, 802.11a and 802.11g. It has many uses: Verify that your network is set up the way you intended. Find locations with poor coverage in your WLAN. Detect other networks that may be causing interference on your network. Detect unauthorized "rogue" access points in your workplace.
WaveStumbler	Linux	WaveStumbler is console based 802.11 network mapper for Linux. It reports the basic AP stuff like channel, WEP,

Tool	OS	Description
		ESSID, MAC etc. It has support for Hermes based cards Compaq, Lucent/Agere, and others). It still in development but tends to be stable. It consist of a patch against the kernel driver, orinoco.c which makes it possible to send the scan command to the driver via the proc/hermes/ethX/cmds file. The answer is then sent back via a netlink socket. WaveStumbler listens to this socket and displays the output data on the console.
Wellenreiter	Linux	Wellenreiter is a wireless network discovery and auditing tool. Prism2, Lucent, and Cisco based cards are supported. It is the easiest to use Linux scanning tool. No card configuration has to be done. The whole look and feel is pretty self-explaining. It can discover networks (BSS/IBSS), and detects ESSID broadcasting or non-broadcasting networks and their WEP capabilities and the manufacturer automatically. DHCP and ARP traffic are decoded and displayed to give you further information about the networks. An ethereal/tcpdump-compatible dumpfile and an Application save-file will be automatically created. Using a supported GPS device and the gpsd you can track the location of the discovered networks.
Airscanner Mobile Sniffer	WinCE	Airscanner Mobile Sniffer is a full featured packet sniffer/analyzer for the PocketPC device. It offers support for Ethereal packet capture, real-time packet statistics, filtering and more. It allows a WLAN audit, including password and intruder detection. The program can decode UDP, TCP, Ethernet, DNS, and NetBios packets. Results can be saved to a file, viewed in real-time and exported to Ethereal format for further inspection. Free for home or personal (non-commercial) use.
Airtraf	Linux	AirTraf 1.0 is a wireless sniffer that can detect and determine exactly what is being transmitted over 802.11 wireless networks. This open-source program tracks and identifies legitimate and rogue access points, keeps performance statistics on a by-user and by-protocol basis, measures the signal strength of network components, and more.
BSD-AirTools	NetBSD, OpenBSD, FreeBSD	bsd-airtools is a package that provides a complete toolset for wireless 802.11b auditing. Namely, it currently contains a bsd-based wep cracking application, called dweputils (as well as kernel patches for NetBSD, OpenBSD, and FreeBSD). It also contains a curses based acces point detection application similar to netstumbler (dstumbler) that can be used to detect wireless access points and connected nodes, view signal to noise graphs, and interactively scroll through scanned ap's and view statistics for each. It also includes a couple other tools to provide a complete tool-set for making use of all 14 of the prism2 debug modes as well as do basic analysis of the

Tool	OS	Description
		hardware-based link-layer protocols provided by prism2's monitor debug mode.
Ethereal	*NIX, Win32	Ethereal is a program for troubleshooting, analysis, software and protocol development, and education. It offers a large variety of protocol analyser functions. Ethereal can capture packets on-line or read them from a file. On-line packet capturing is supported for Ethernet, FDDI, PPP, Token-Ring, IEEE 802.11, Classical IP over ATM, and loopback interfaces. Captured network data can be browsed via a GUI or CLI.
Kismet	Linux, BSD, MacOSX, Cygwin	Kismet is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. Kismet will work with any wireless card which supports raw monitoring (rfmon) mode, and can sniff 802.11b, 802.11a, and 802.11g traffic. Kismet identifies networks by passively collecting packets and detecting standard named networks, detecting (and given time, decloaking) hidden networks, and inferring the presence of nonbeaconing networks via data traffic.
KisMAC	MacOSX	KisMAC is a free stumbler application for MacOS X, that puts your card into the monitor mode. Unlike most other applications for OS X it has the ability to run completely invisible and send no probe requests. KisMAC supports several third party PCMCIA/PCCards cards with Orinoco and PrismII chipsets, as well as Cisco Aironet cards. Original Airport Cards are supported too. The newer Airport Extreme Cards are only supported in a limited active mode.
Packetyzer	Win32	Packetyzer is a Windows user interface for the Ethereal packet capture and dissection library. Packetyzer can decode more than 483 protocols. Packetyzer also works together with the Neutrino Sensor for 802.11 packet capture and analysis.

Table C-1: Open Source Wireless Monitoring and Measurement Tools

Tool	Platform	Description
AirMagnet Laptop Analyzer	Win32	The AirMagnet Laptop Analyser is an advanced stand-alone solution for wireless security and troubleshooting. Built from the ground up to meet the challenges of 802.11a/b/g WLANs, the AirMagnet Laptop provides a direct automated analysis of any WLAN, proactively detects over 120 network problems, and delivers a set of active wireless troubleshooting tools that simply aren't available anywhere else. The result, is an invaluable network management tool that gives IT professionals a transparent view into Wi-Fi and provides everything they need to quickly pin down any network problem.
AirMagnet Handheld	WinCE	Built from the ground up for wireless, the AirMagnet

Tool	Platform	Description
Analyzer		Handheld Analyser provides a highly mobile set of tools to enforce zero tolerance network security policies, quickly eliminate connection problems, maintain network performance levels, and to survey and deploy the wireless network.
Berkeley Varitronics Systems Yellowjacket	WinCE	Yellowjacket® is a wireless receiver module designed to work with HP's iPAQ® PDA in sweeping, analysing and optimizing 2.4 GHz W-LANs and WISPs. The receiver measures all 14 DSSS network channels operating on the IEEE 802.11b standard allowing the user to determine the AP (Access Point), PER (Packet Error Rate), Signal-to-Noise ratio, Delay Spread, Multipath (Ec/Io), SSID and RSSI (narrow and wideband) signal levels of any Access Point and Client STA. Other features include W.I.S.P. Antenna Alignment and Direction Finding. Yellowjacket® allows those familiar with the iPAQ's PocketPC® interface a unique advantage over "software only" products currently available because Yellowjacket® functions as a complete WLAN analysis system combining the elegant PocketPC® Windows CE® environment along with Berkeley's precision calibrated receiver technology. Yellowjacket® is also fully compliant with Hive Indoor Mapping Software so users may also create, edit and analyse indoor W-LANs where GPS reception is not possible.
LinkFerret Network Monitor and Protocol Analyzer	Win32	LinkFerret network monitoring products for LAN and wireless topologies provide you with a comprehensive set of monitoring utilities and packet sniffers for capture, statistical analysis, and protocol decoding. The LinkFerret network monitor is a complete and reliable Windows-based monitoring solution available at a truly affordable price
Fluke Networks OptiView Series II Integrated Network Analyzer	N/A	Complete network vision in seconds. Combines seven layer protocol analysis, active discovery, SNMP device analysis, RMON2 traffic analysis and physical layer testing into a mobile solution. Design and user interface equally effective whether the unit is carried as a portable device or placed semi-permanently on a network link. Web enabled remote analysis allows up to seven users to access a single unit simultaneously. Wireless, WAN, VLAN and Expert Analysis options available.
Javvin Network Packet Analyzer	Win32	Network Packet Analyser is an advanced network traffic monitoring, analysis and reporting tool, based on Windows operating systems (all versions). It captures and analyses all traffic transport over both Ethernet and WLAN networks and decodes all major TCP/IP and application protocols. With Network Packet Analyser, you can easily filter the network traffic to focus on the information that you are looking for. The comprehensive reports and graphic views allows you to understand network performance and bandwidth usage quickly, to check network health and identify problems in simple steps.
Network General Sniffer Wireless	Win32	Sniffer® Wireless Intelligence, a component of Sniffer Portable LAN, helps you manage network applications and

Tool	Platform	Description
		deployments on wireless LAN 802.11a/b/g networks to deliver the best possible performance. It spots security risks in real time, identifies network problems quickly and helps to maximize network investments. Sniffer Wireless Intelligence provides a wireless-specific Expert analysis system that enhances visibility into network anomalies and facilitates automatic problem-solving — helping to ensure that performance problems are corrected, rogue wireless equipment is removed and unauthorized mobile users are discovered.
Network Instruments Observer	Win32	A network monitor and protocol analyser for Ethernet, Wireless 802.11b/a/g, Token Ring and FDDI networks. Observer provides metrics, capture and trending for both shared and switched network environments.
TamoSoft CommView for Wi-Fi	Win32	CommView for WiFi is a powerful wireless network monitor and analyzer for 802.11 a/b/g networks. Loaded with many user-friendly features, CommView for WiFi combines performance and flexibility with an ease of use unmatched in the industry.
Tektronics WCA11G Signal Analysis	N/A	Features: Automatically Controls the WCA300 Series to Evaluate Transmission Characteristics of IEEE 802.11a, b, and g RF Signals Precisely as Defined in the Standard, Ensuring Conformance. Automatically Detect Data format and Bit Rate of Specified Standard. Simple, Familiar Configuration - Uses Standard External PC to Control the Analyser and to Acquire, Store and Analyse Data Offline in a Standard Windows Environment, Eliminating Tedious set-ups and Uncertainties. Frequency Domain Triggering Can Be Set to Capture Transient Events and Intermittent Signal Fluctuations, No Matter when They Occur. Powerful Spectrum Mask Testing Automatically Detects Out-of-Limit Conditions and Captures Signals to Help Identify and Troubleshoot the Causes.
WildPackets AiroPeek NX	Win32	Expert Wireless LAN Analyser: AiroPeek NX, WildPackets' expert wireless LAN analyser, provides network engineers with the expert diagnostics they need to deploy, secure, and troubleshoot wireless LANs. AiroPeek NX covers the full spectrum of wireless LAN management requirements, including site surveys, security assessments, client troubleshooting, WLAN monitoring, remote WLAN analysis, and application layer protocol analysis.
WildPackets AiroPeek SE	Win32	Wireless LAN Protocol Analyser: AiroPeek SE, a comprehensive packet analyser for IEEE 802.11 wireless LANs, is designed to identify and solve wireless network anomalies. It quickly isolates security problems, fully decodes all 802.11 WLAN protocols, and analyses wireless network performance with accurate identification of signal and noise strengths, channel and data rates. Analysis.
WildPackets AiroPeek VX	Win32	Expert Voice over Wireless LAN Analyser: AiroPeek VX, WildPackets' Expert Voice over Wireless LAN analyser, offers both wireless and VoIP diagnostics in real time.

Tool	Platform	Description
		AiroPeek VX provides real-time expert analysis, Application Response Time (ART) analysis, full 7-layer decodes, alarms, triggers, comprehensive graphs and reports, and more. In addition to its advanced wireless network analytics, AiroPeek VX offers per-call analysis and supports multiple signalling protocols. The media plane analysis looks at packet-level details of RTP and RTCP streams and evaluates packet delay variations, packet loss, jitter, and provides MOS scores as well as R-Factor values for each call.

Table C-2: Commercial Wireless Monitoring and Measurement Tools

Appendix D IPv6 tools

This appendix shows a list of IPv6 tools, and tools that are being currently ported to IPv6 and tested.

A complete list of IPv6 tools is detailed in the MoMe database.

Tool	*OS*	*Description*
Analyzer	Win32	Analyzer is an advanced network sniffing and monitoring tool.
Argus	Linux	Argus is a system and network monitoring application which includes IPv6 support since version 3.2. It monitors TCP and UDP applications, IP connectivity, SNMP OIDS, etc. It comes with a nice and easy to view web interface. Argus contains builtin alert notification via email and pager (qpage) but is easily extendible to use any other program like e.g winpopup. 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.
ASpath-tree	Solaris FreeBSD Linux w/ Perl interpreter	ASpath-tree is a tool which allows displaying graphically the BGP4+ routing paths managed by the CISCO/Juniper/Zebra routers of a backbone.
CISCO Works Campus Manager	MS Windows Solaris	Campus Manager, a member of the Cisco Works family of products, is a suite of web-based network management tools that enable administrators to obtain various types of graphical views of their network topology and end-user information. Campus Manager is based on a client/server architecture that connects multiple web-based clients to a server on the network. The Cisco Works Server supplies tools and services to the Campus Manager applications, including the Asynchronous Networks Interface (ANI) Server. The ANI Server discovers information about network devices and saves it in the ANI database for Campus applications, to access.
Cricket	UNIX systems	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 all kinds of other jobs, as well.
dbeacon	UNIX systems	'dbeacon' stands for Distributed Beacon. dbeacon is a Multicast Beacon written in C++. The main purpose of a beacon is to monitor other beacon's reachability and collect statistics such as loss, delay and jitter between beacons. dbeacon support both **IPv4** and **IPv6 multicast**, collecting information via ASM and SSM. Used for monitoring multicast connectivity. Similar to other multicast beacons

Tool	OS	Description
		except that there is no centralized server, and it also checks SSM on systems supporting SSM.
HP OpenView Network Node Manager	HP-UX 11.0 for Workstations and Servers HP-UX 11.11 for Workstations and Servers Windows 2000 Windows XP Solaris 8.0 Solaris 9.0 Linux Red Hat AS 2.1 operating system	HP OpenView Network Node Manager Extended Topology discovers the existence of IPv6 devices, creates a map showing layer 3 IPv6 device connectivity, then monitors the status of each device. To monitor the address status of a device, Extended Topology uses an IPv6 ping rather than using SNMP requests. Extended Topology considers a device to be down if it doesn't respond to an IPv6 ping.
Jnettop	Unix/Linux	Jnettop is a Network traffic visualiser that captures traffic coming across the host it is running on and displays streams sorted by bandwidth they use. Result is a listing of communication on network by host and port, how many bytes did this communication transport and the bandwidth it is consuming. Jnettop allows administrators of routers to watch online traffic coming across the network in a fashion similar to the way top displays statistics about processes. It is useful for quickly evaluating the state of the network. It is console application without web interface.
JOIN-TV	Unix/Linux	JOIN-TV (JOIN Traffic Visualizer) visualizes the Traffic-flow within a network by interpreting the log-files of the MRTG-Tool written by Tobias Oetiker. JOIN-TV was developed for the 6WiN (http://www.6win.de) – a native IPv6 backbone in Germany – and the tunnel endpoints of the connected members of DFN. Therefore all tests of the tool were done within the 6WiN.
Looking Glass	Unix/Linux	Looking Glass is a tool available in its IPv6 version on www.traceroute.org. It is a CGI script which allows connecting to a remote router from a simple web page, to run some commands on the router and to show the result on another web page. Its pre-requisit is a simple user login on the router.
MRTGv6	Linux	MRTG is already widely used to monitor the traffic load on network links, CPU usage on routers, and other network and host parameters. IPv6 support to MRTG was added in version 2.10.0.
Multicast Beacon	Unix systems	Multicast Beacon is a tool for monitoring traffic parameters of multicast network. Its architecture is

Tool	OS	Description
		client/server. Clients exchange data between themselves using multicast technology and measure parameters of such generated traffic. Server receives measure reports from clients and display to users' current values.
RIPE NCC Test Traffic server	Unix systems	RIPE NCC TT servers allow estimates for properties of network links (e.g. one-way delay and packet loss) to be made, between pairs of participating TT server sites. The code is claimed to adhere to the RFC standards under the IETF IP Performance Metrics WG.

Appendix E References

[1]   MobiLib: Community-wide Library of Mobility and Wireless Networks,
        http://nile.usc.edu/MobiLib/
[2]   The Dartmouth Wireless Traces, http://cmc.cs.dartmouth.edu/data/dartmouth.html
[3]   Mobile landscape; Graz in real-time; http://senseable.mit.edu/projects/graz/graz.htm
[4]   MOME Deliverable D13: MOME Interoperability Event
[5]   MOME Deliverable D22: MOME Workstation
[6]   The Join Open InterNetworks Project (JOIN): http://www.join.uni-muenster.de/
[7]   6WIN, IPv6 Network of DFN, German NREN: http://www.6win.de/
[8]   IST 6NET project: http://www.6net.org
[9]   The GÉANT project, the pan-European research and education network:
        http://www.geant.net/
[10]   The 6Bone project: http://www.6bone.net
[11]   WIDE project: http://www.wide.ad.jp/ and
        the MAWI WG: http://www.wide.ad.jp/wg/mawi/;
        the traffic data repository: http://tracer.csl.sony.co.jp/mawi/
[12]   The Active Measurement Project (AMP) http://amp.nlanr.net
[13]   RIPE Routing Information Service RIPE-RIS: http://www.ripe.net/ris
[14]   IST-WINNER: WINNER - Wireless World Initiative New Radio; https://www.ist-
        winner.org/
[15]   STRIKE- IST project IST-2001-38354; http://ist-strike.org/
[16]   IST-PULSERS: Pervasive Ultra-wideband Low Spectral Energy Radio System
        http://www.pulsers.net/main.shtml
[17]   IST-LONG: Laboratories over Next Generation Networks
        http://long.ccaba.upc.es/
[18]   "Porting applications to IPv6 HowTo" (part of the IST-LONG project)
        http://jungla.dit.upm.es/%7Eecastro/IPv6-web/ipv6.html
[19]   The IST-EuQoS project (End-to-end Quality of Service support over heterogeneous
        networks), www.euqos.org
[20]   The METAWIN project, http://www.ftw.at/ftw/research/projects/ProjekteFolder/N2/
[21]   Inter-domain Data Exchange Questionnaire http://www.ietf.org/internet-drafts/draft-boschi-
        data-exchange-quest-01.txt
[22]   IST-LOBSTER: Large Scale Monitoring of Broadband Internet Infrastructures
        http://www.ist-lobster.org/
[23]   IST-LOBSTER. D0.1 - Requirement collection and analysis http://www.ist-
        lobster.org/deliverables/d0.1.pdf
[24]   RFC 3763 - One-way Active Measurement Protocol (OWAMP) Requirements
[25]   A One-way Active Measurement Protocol (OWAMP) (draft-ietf-ippm-owdp-08.txt, draft-
        ietf-ippm-owdp-15.txt)