

INFORMATION SOCIETY TECHNOLOGIES (IST)
PROGRAMME



Large Scale Monitoring of BroadBand Internet Infrastructure
Contract No. 004336

D3.3: Deployment - second phase

Abstract:

This document describes the deployment of LOBSTER probes by the project partners and organizations outside the project.

Contractual Date of Delivery	30 June 2007
Actual Date of Delivery	2 July 2007
Deliverable Security Class	Public

The LOBSTER Consortium consists of:

FORTH	Coordinator	Greece
VU	Principal Contractor	The Netherlands
CESNET	Principal Contractor	Czech Republic
UNINETT	Principal Contractor	Norway
SYMANTEC	Principal Contractor	United Kingdom
ALCATEL	Principal Contractor	France
FORTHnet	Principal Contractor	Greece
TNO	Principal Contractor	The Netherlands
TERENA	Principal Contractor	The Netherlands



Contents

1	Introduction	5
2	Deployed monitoring probes by project partners	7
2.1	ALCATEL	7
2.2	CESNET	11
2.3	FORTH	14
2.4	Forthnet	14
2.5	TNO	15
2.6	UNINETT	16
3	Deployed monitoring probes by organizations outside the project	19
3.1	Technical University of Catalonia	19
3.2	South-Eastern European Research & Education Network	19
3.3	Bulgarian Academy of Sciences	21
3.4	Columbia University (NY)	21
3.5	Institute for Infocomm Research (I ² R) – Singapore	21
3.6	National Technical University of Athens	22
3.7	Aristotle University of Thessaloniki	22
3.8	University of Crete	23
3.9	Cretan Health Network	23
3.10	Cretan School Network	24
3.11	Cooperation with the GN2 Project	25
3.12	Dissemination to ISPs	26
4	Summary	27

CONTENTS

Chapter 1

Introduction

This deliverable describes the current deployment status in the LOBSTER project. As of June 2007, the project partners have deployed 33 passive monitoring sensors across Europe, all of which are operational at the time of this writing, monitoring live network traffic. Furthermore, 14 LOBSTER sensors have been installed in eight different countries from organizations outside the project, monitoring production networks using LOBSTER's performance and security monitoring applications. Figure 1.1 presents the overall geographical distribution of the 47 LOBSTER sensors.

One of the main reasons for the increased deployment of LOBSTER sensors is the availability of several ready-to-use monitoring applications which take full advantage of LOBSTER's passive monitoring middleware and the Monitoring API (MAPI). The monitoring applications developed within LOBSTER, presented in Deliverable 3.3b, provide immediate benefits to network administrators and researchers, since they enable novel network measurement and attack detection possibilities.

The availability of the LOBSTER Live CD, which can be freely downloaded from the project's website, has also been of key importance to the dissemination of the LOBSTER software to the broader networking community. By just inserting the CD to a typical PC, the user can have a first-hand experience of the LOBSTER software. The procedure requires minimal effort, since MAPI is already configured and ready for use, while key monitoring applications are automatically started and the user can immediately see monitoring results from his own production network.

Finally, the project has set up Task Forces with the purpose of bringing the LOBSTER technology closer to organizations outside the project. The ISP Task Force helps the dissemination of LOBSTER to ISPs, and has already received positive feedback from several ISPs in Europe. The JRA1 Task Force ensures the interoperability of LOBSTER applications with the PerfSONAR framework of GN2, and promotes the use of passive monitoring within the GN2 network. Within this activity, a first passive monitoring deployment proposal has already been approved by the GN2 project.

This document consists of two main parts: Chapter 2 provides a detailed description of the passive monitoring sensors deployed by the project's partners, while Chapter 3 provides an overview of the deployed monitoring probes by organizations outside the LOBSTER project.

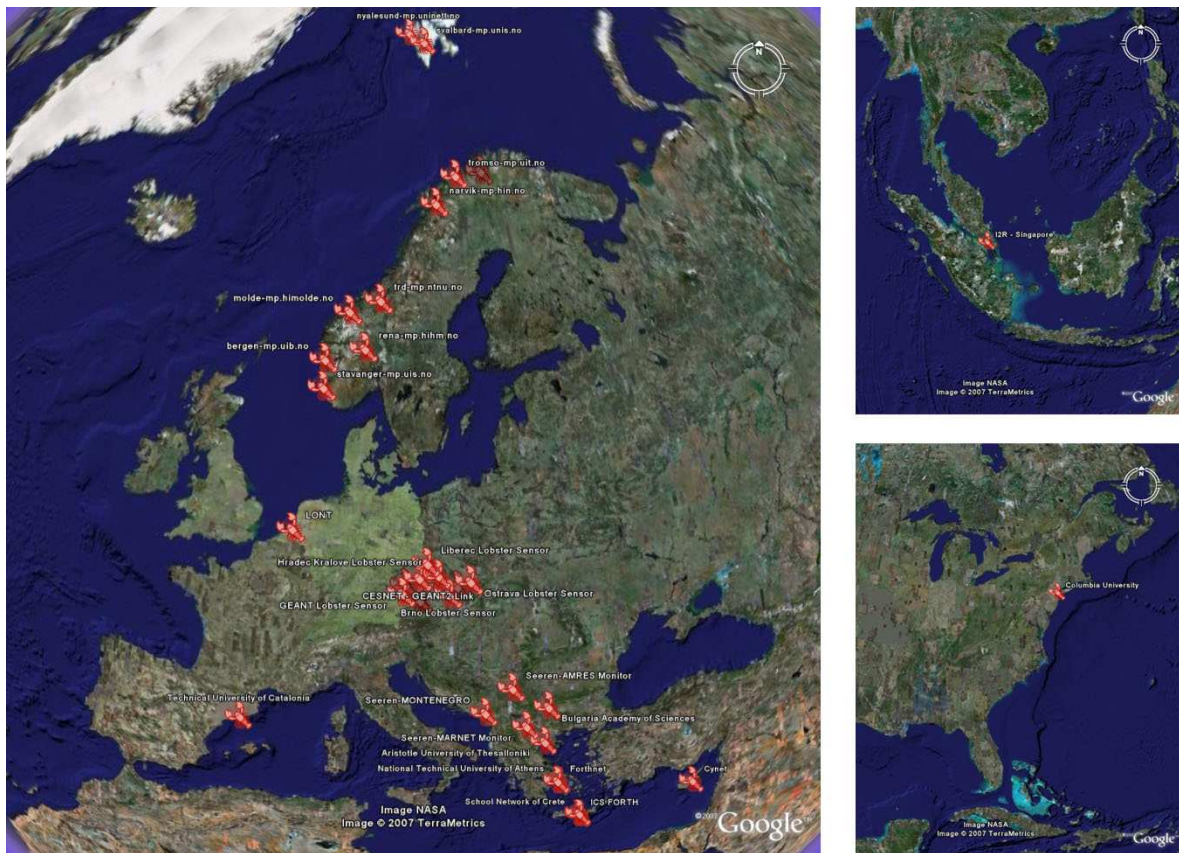


Figure 1.1: Deployed LOBSTER passive monitoring sensors around the globe.

Chapter 2

Deployed monitoring probes by project partners

This section provides a detailed description of the deployed monitoring probes by partners of the LOBSTER Project, as of June 2007. Each partner describes the location and type of monitoring probes that are deployed and gives some information about what the probes are currently being used for.

2.1 ALCATEL

2.1.1 Deployed sensor

Alcatel has one sensor, located in the Alcatel lab in Marcoussis. It is accessible via the Internet, at IP address 83.206.133.241. A web interface, available at <http://83.206.133.241> allows testing, checking and administrating this equipment. Test and check options are available to LOBSTER partners, using the same login name and password as those used to access the private pages of the LOBSTER website. Administration pages are only available for Alcatel, as they include options possibly impacting the sensor running state.

The Status and Admin interface are identical, but access to control options is removed from the Status page.

Admin and Status pages can be used to view the flows currently defined and the functions these flows are using. Global packet counters for each monitoring boards are also provided. The Admin interface also provides some basic administration options, available only to Alcatel staff.

With the Test interface a user can define a flow and get the results of the applied functions. This interface uses the DiMAPI APIs to access the sensor, using `localhost:atca0` as the parameter of the `mapi_create_flow` function.

Sensor can also be directly used via its DiMAPI interface. This usage is currently discouraged as some MAPI functions available on the sensor are not fully protected against wrong usage (bad parameters).

Monitored traffic is not real Internet traffic but comes from an Ethernet packet generator. This makes testing the sensor easier as, knowing the incoming traffic, we can accurately check the results of MAPI functions. Monitoring real traffic raises administrative and legal issues. It also implies a reliability level our prototype has not yet reached.



Figure 2.1: Web interface: main page

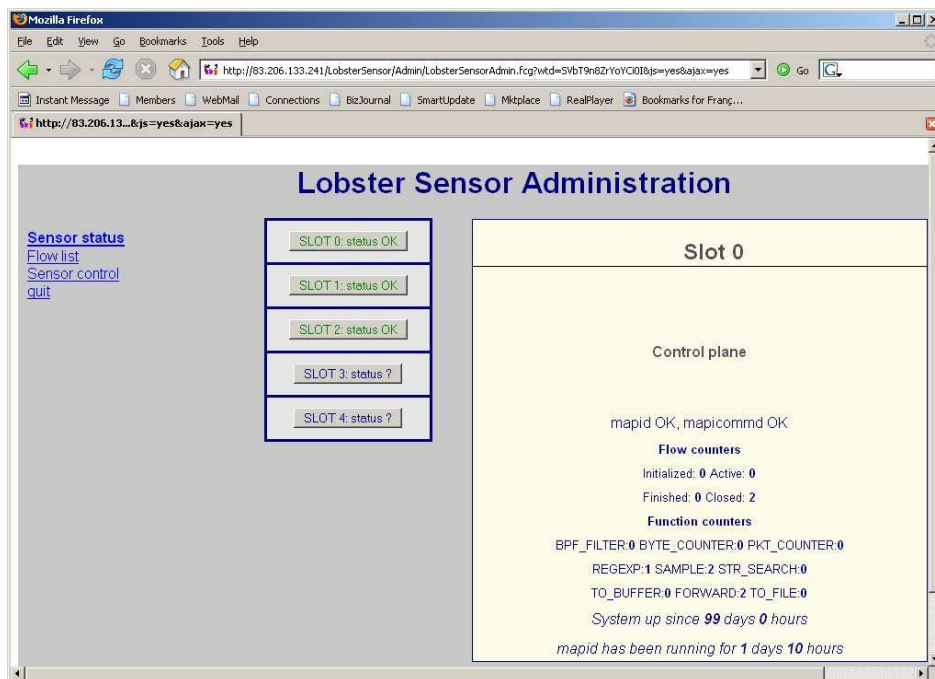


Figure 2.2: Web interface: Admin page

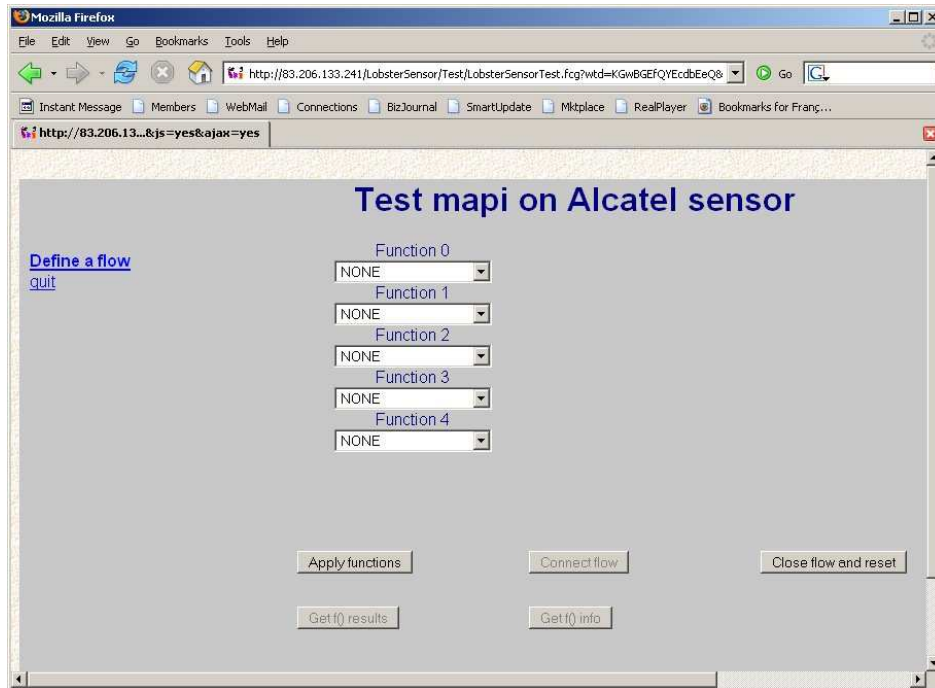


Figure 2.3: Web interface: Test page

The sensor and the web interface are still under development and test. Access to the Alcatel sensor can be denied at any time for example when a new version is installed, or when Alcatel does not want a test or a demo to be disturbed by external usage of the equipment.

2.1.2 Hardware description

The hardware architecture of the Alcatel sensor has been designed to be easily embedded in telecommunication equipments. It is also flexible and additional processing power could easily be added by plugging additional blades in the shelf. Figure 2.4 shows the current hardware:

1. Control plane: this blade is a PC board, running linux. The `mapidcomm` and `mapid` daemons run on this processor.
2. Main monitoring blade: this is an Octeon based board, developed by Alcatel. This is a prototype.
3. Secondary monitoring blade: this blade is a PC board, used to support MAPI functions which would be too difficult to port to the main monitoring board or which would have a too heavy impact on the main monitoring processor performance.
4. AdvancedTCA switch: this is a standard component of the AdvancedTCA architecture.
5. Ethernet connections to monitored networks: Up to 4 Gigabit Ethernet cable can be plugged to the main monitoring board.

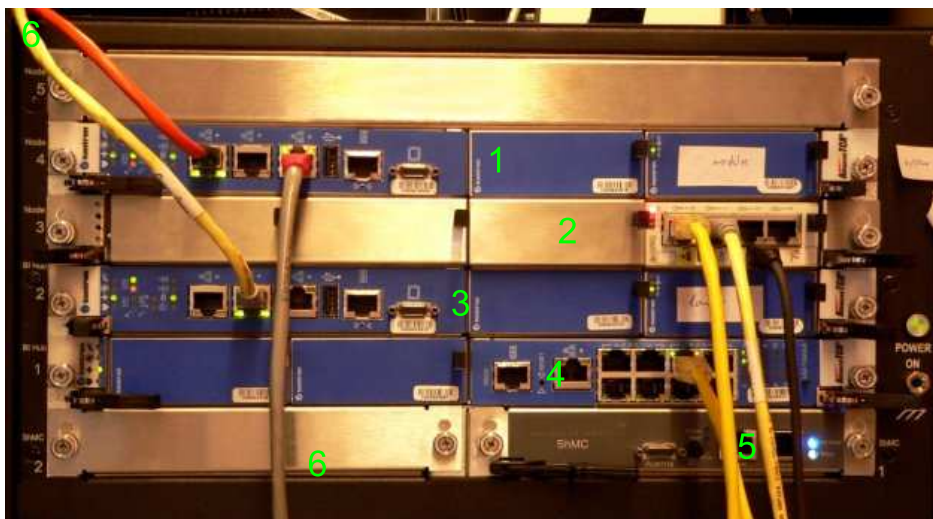


Figure 2.4: Alcatel sensor: picture of the hardware

2.1.3 Software specificities

Due to its specific hardware, the Alcatel sensor uses a modified version of the MAPI software. A specific MAPI library and a specific MAPI driver have been developed for interfacing with the Alcatel hardware. Monitoring blades runs their own specific software, the secondary monitoring blade uses a specific daemon which loads a modified versions of MAPI libraries.

The following MAPI APIs are supported and have been tested:

- `mapi_create_flow`
- `mapi_apply_function`
- `mapi_connect`
- `mapi_read_results`
- `mapi_get_next_pkt`
- `mapi_get_function_info`
- `mapi_close_flow`

The `mapi_authenticate` function and all the `mapi_get_xxx_info` have not been tested but they should work because they are implemented on the control plane, in the MAPI daemons, and do not involve any communication with monitoring boards. Support for the offline functions could also be easily provided, on the control plane. It is currently not provided because it would impact control plane performance. A solution to support offline flows on the secondary monitoring board would be preferable.

Currently the main monitoring board supports the following MAPI functions:

- `PKT_COUNTER`

- BYTE_COUNTER
- REGEXP
- STR_SEARCH
- BPF_FILTER
- SAMPLE
- TO_BUFFER
- TO_FILE
- TO_TCPDUMP

An additional function, FORWARD, has been introduced to allow forwarding packets from the main monitoring board to another slot. It takes one integer parameter, the slot number to forward the packet to.

The track library has been ported to the secondary monitoring board, it provides all the TRACK_XXX functions, as available in the 2.0 beta1 MAPI release.

2.1.4 Known issues and restrictions

- It is not possible to forward packets from a secondary monitoring board to the main monitoring board. Using a function from the main monitoring board after a function of the secondary monitoring board is impossible. For example, today the only way to get results from a TRACK_XXX function is to use the `mapi_get_function_info` call, which returns the number of packets which matched the filtering function.
- The REGEXP function uses a regular expression compiler delivered with the Oceon Software Development Kit. The syntax used for regular expressions is different from the one used in the MAPI standard delivery.
- The TO_FILE function creates the result file on the control plane. It is scheduled to give access to these files through the sensor web interface, but this option is not yet available.
- The STR_SEARCH function cannot search for string longer than 8 characters. The REGEXP function can be used when this STR_SEARCH limitation is a problem.
- The sensor cannot support more than 64 active flows. Today this limit is even set to 10, using a sensor configuration parameter.

2.2 CESNET

CESNET has deployed 12 LOBSTER monitoring stations in the Czech NREN (National Research and Educational Network).

- One 10 Gbit/s station monitors the GN2 – CESNET link
- One 10 Gbit/s station monitors the most heavily loaded Prague – Brno link

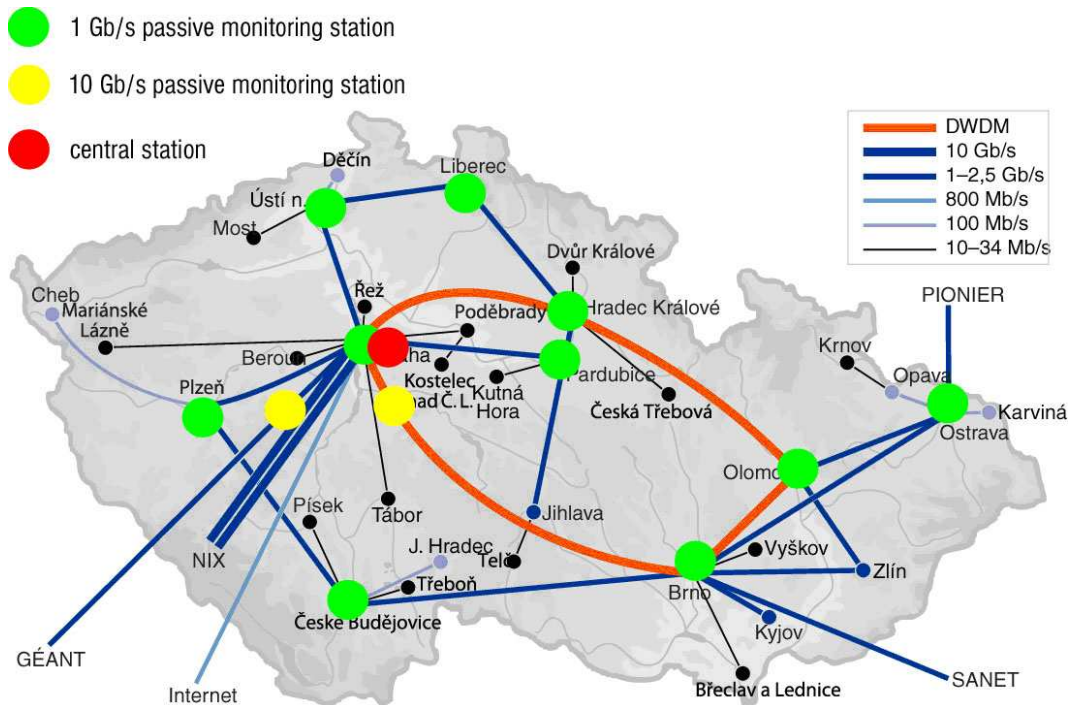


Figure 2.5: Passive monitoring stations in CESNET’s network.

- The remaining stations monitor traffic in major backbone nodes of the CESNET network.

All stations run continuously and their status is being monitored by the CESNET NOC (Network Operation Center). The geographical position of the monitoring stations is illustrated in Fig. 2.5.

The configuration of the monitoring stations is summarized in Table 2.1. We plan to monitor complete traffic entering and leaving our backbone network. Most access links to our backbone use 10 Gigabit Ethernet. We currently cannot afford to buy 10 Gb/s monitoring cards for all access points. Therefore, we use port mirroring on CISCO routers that can convert the link technology (particularly 10GE to 1 GE). There is a maximum of two port mirroring sessions on a router, which are both required for full-duplex monitoring. As we need to leave at least one session for network troubleshooting and the load on our links is increasing, we plan to upgrade stepwise to 10 Gb/s cards.

Each monitoring station runs MAPI and the ABW application for passive bandwidth usage monitoring. ABW is an application written on top of MAPI and the trackflib library. It was developed as part of the JRA1 activity of the GN2 project. The trackflib library was developed by FORTH as part of the LOBSTER project. Primary advantages of monitoring bandwidth usage by ABW when compared to using SNMP to read router interface byte counters are the following:

- We can distinguish bandwidth used by different protocols at different layers (L2, L3, L4 or application protocols)
- We can monitor bandwidth usage in short intervals (e.g., 1 second) in order to detect short peaks

ABW can use any network adapter to capture packets that is supported by MAPI. Currently it can be a DAG card, a COMBO card or a regular NIC card. We developed a first version of hardware-

# probes	Adapter	CPU	Memory	Linux distr.	DiMAPI access	MAPI version	GPS	Monitored Traffic
1	DAG 6.2SE (10 Gbit/s) + DAG 4.3 (1 Gbit/s)	Xeon 3.0GHz	1GB	Debian	Private	Devel.	Yes	CESNET backbone ↔ GN2 network
1	2× DAG 8.2X (10 Gbit/s)	2× Dual-Core Xeon 3.0GHz	2GB	Debian	Private	Devel.	Yes	CESNET node in Prague ↔ Brno (two major Universities)
10	2× Intel PRO/1000	Xeon 3.0GHz	512MB or 1GB	Debian	Private	Devel.	All except Liberec	CESNET backbone ↔ local PoPs

Table 2.1: CESNET monitoring probes

supported dagflib library that provides some of the MAPI functions implemented with hardware filters and counters in DAG cards. We support DAG4.3GE (1 Gb/s) card with coprocessor and one counter only also in newer 1 Gb/s and 10 Gb/s DAG cards with DSM classification (DAG4.5, 6.2 and 8.2). We are working on extended hardware support of MAPI functions.

Live measurements of bandwidth usage by ABW are available at the following address: <https://perfmon.cesnet.cz/abw-intro.html>

Monitoring of the GN2 - CESNET link is available to the public. Monitoring of CESNET backbone links requires authorization by username and password. An example graph produced by the application showing distribution of L4 protocols, presence of multicast and IPv6 including average and maximum values over specified time intervals is in Fig. 2.6.

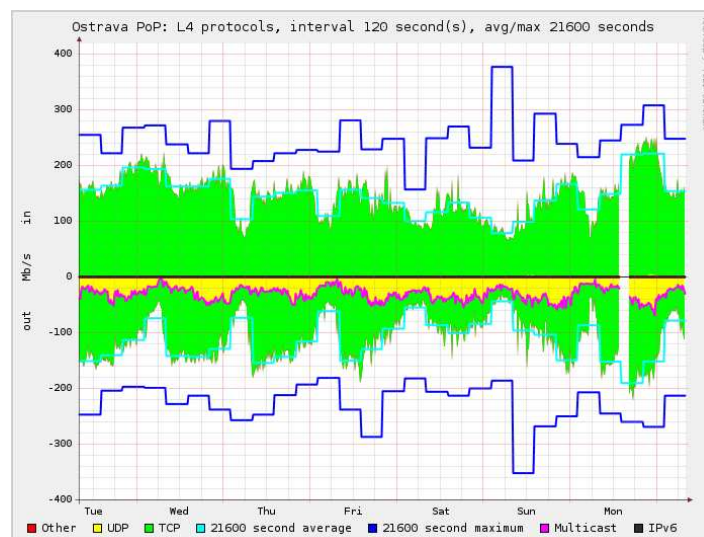


Figure 2.6: Example graph produced by ABW.

# probes	Adapter	CPU	Memory	Linux distribution	DiMAPI access	MAPI version	GPS
1	Intel 82546 Dual Port GigE Controller	Xeon 3.2GHz	1GB	Debian Testing	Private	Development	No
1	Intel 82546 Dual Port GigE Controller	Dual Xeon 3.4GHz	2GB	Scientific Linux 3.0.5	Private	Development	No
1	Intel 82546 Dual Port GigE Controller + Ethernet Tap	2× Pentium D 2.8GHz	2GB	Debian Testing	Private	Development	No

Table 2.2: Monitoring sensors deployed in FORTH’s network.

# probes	Adapter	CPU	Memory	Linux distribution	DiMAPI access	MAPI version	GPS
1	110 Embedded NC7782 dual-port Gigabit, Lights-out mgmt card	ProLiant DL360 G4 2×3.60GHz	2GB	RedHat Enterprise Linux AS 4	Private	Stable	No

Table 2.3: Characteristics of Forthnet’s operational LOBSTER sensor.

2.3 FORTH

FORTH, as of June 2007, has deployed three monitoring sensors running MAPI in FORTH’s network, summarized in Table 2.2.

- The main sensor, shown in Figure 2.7, monitors all incoming and outgoing traffic of FORTH’s campus in Heraklion, Crete.
- The second sensor, shown in Figure 2.8, monitors the traffic of the local EGEE-II GRID node: a large cluster-based parallel computer comprising 128 processors. The node participates in the EGEE (Enabling Grids for E-scienceE) infrastructure, and thus is heavily used by scientists all over Europe. Both sensors monitor 1 Gbit Ethernet links.
- Finally, the third sensor, a Dell PowerEdge 860 1U rack-mounted server, monitors the traffic of FORTH’s web server through an Ethernet Tap.

All probes are operational and monitor full payload traffic. The `appmon` application for real-time application traffic characterization is constantly running on all sensors. Most of the sensors are also used for security-related applications, such as `nemu` and `EAR`.

2.4 Forthnet

Since January 2007, a LOBSTER sensor has been installed and is being operated in Forthnet’s data-center. The sensor, located in the Point of Presence (PoP) in Athens, Greece, is equipped with a regular Gigabit NIC card. The network traffic mirrored to the sensor comes from Forthnet’s customers with leased lines (mercantile companies, maritime enterprises, insurance offices, internet cafes, etc.). Currently, part of customers traffic is mirrored (about 50–60 Mbps on average) for sensor evaluation and tuning, with perspective to add more traffic later.



Figure 2.7: FORTH's main LOBSTER sensor. The sensor monitors all traffic between FORTH's campus and the Internet.

# probes	Adapter	CPU	Memory	Linux distribution	DiMAPI access	MAPI version	GPS
1	DAG 4.3GE (1 Gbit/s)	Xeon 2.4GHz	768MB	Debian	Private	Stable	No

Table 2.4: Characteristics of TNO's operational LOBSTER sensor.

The probe is fully operational and the Appmon application (Figure 2.10) is constantly running at the sensor for providing accurate traffic categorization of the customer's traffic.

2.5 TNO

TNO has deployed one LOBSTER sensor installed at one of the edges of the TNO network. The sensor is based on a DAG4.3GE network monitoring card (see Table 2.4). The sensor itself is not available for DiMAPI access from people outside TNO. The LOBSTER Network Telescope (LONT) application which has access to the sensor can be shared with other organisations.



Figure 2.8: FORTH's GRID cluster. One of the 60 nodes is actually a LOBSTER sensor that monitors the traffic of the whole cluster.

2.6 UNINETT

UNINETT currently has 15 monitoring probes that are operational as summarized in table 2.5. An additional 7 monitoring probes will be deployed at universities and colleges during 2007, and 2 active monitoring probes will be upgraded with DAG cards for passive monitoring.

The OC48 DAG cards are installed on the main backbone link between Trondheim and Oslo. The gigabit Ethernet cards are installed in cooperation with Universities and Colleges in Norway and are located at the main access link of each institution. The deployment of the gigabit Ethernet probes are part of the GigaCampus project and the deployment is shown in figure 2.11.

There are two monitoring probes installed in Spitsbergen, one at the The University Centre in Svalbard and one in Ny-lesund, the northernmost permanent settlement in the world. This last probe

# probes	Adapter	CPU	Memory	Linux distribution	DiMAPI access	MAPI version
6	DAG4.3GE	Xeon 3.2GHz	2GB	Debian Sarge	Private	Development
6	DAG4.5G2	Xeon 3.2GHz	2GB	Debian Sarge	Private	Development
1	DAG4.2E	Xeon 3.4GHz	2GB	Debian Sarge	Private	Development
1	2xDAG4.3S OC48 w/coprocessor	Xeon 3.2GHz	3GB	Debian Sarge	Private	Development
1	DAG4.3GE	Xeon 3.2GHz	2GB	Debian Sarge	Private	Development

Table 2.5: UNINETT monitoring probes



Figure 2.9: Forthnet's operational LOBSTER sensor.

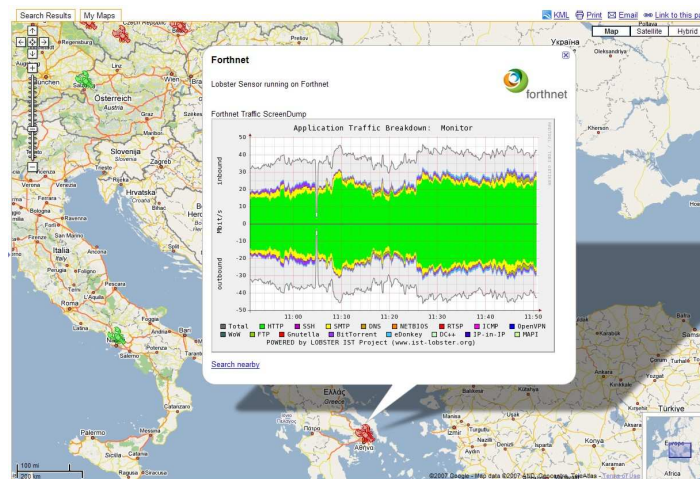


Figure 2.10: Appmon running on Forthnet's LOBSTER sensor in Athens.

is mainly used for monitoring and debugging e-VLBI¹ transfers between the radio telescope at Ny-lesund and the Haystack project at MIT.

The rest of the monitoring probes are used for monitoring QoS, security and for research. The Appmon application is running at the colleges at Narvik and Rena, and at the Universities of Troms and Stavanger. The MAPI IPFIX probe is used for exporting flow records extended with QoS parameters. Other Lobster applications will soon be in full production.

10 of the probes are equipped with Trimble Acutime 2000 GPS for time synchronization. Reliable operation of these units is proving a challenge, however. We have seen several instances of failures both in the GPS units and in the cabling.

The probes are currently closed for all DiMAPI access from people outside of UNINETT. This might change in the future, but until then general statistics from several Lobster applications will be made available through other interfaces or applications like Stager and perfSONAR.

¹Electronic Very Long Baseline Interferometry



Figure 2.11: UNINETT deployment

Chapter 3

Deployed monitoring probes by organizations outside the project

In this section, we provide an overview of the deployed monitoring probes by organizations outside the LOBSTER project. As of June 2007, a total of 14 operational LOBSTER sensors have been installed in eight different countries. The number of deployed sensors is expected to increase through the cooperation of LOBSTER with the GN2 project, as well as due to the increasing popularity of the LOBSTER monitoring software.

We should note that here we list only sensors deployed by organizations that had some contact with partners of the LOBSTER project, and for which we have confirmed that they maintain operational sensors. However, based on the software download statistics, the activity of the MAPI support mailing list, and personal feedback and questions to members of the consortium, several other researchers and administrators have been using the LOBSTER software, so we conjecture that there are probably more operational installations in production networks that we are not aware of.

3.1 Technical University of Catalonia

A LOBSTER sensor has been installed and is operational since January 2007 at the Technical University of Catalonia. The sensor, equipped with a Gigabit Ethernet monitoring interface and dual Xeon 2.4GHz CPUs, monitors all traffic of the backbone link between the University and the Spanish NRN. The sensor is dedicated for running `appmon`, the accurate traffic categorization application developed by the LOBSTER project. The application classifies the traffic of the whole Class B subnet of the University, with an average utilization of the monitored link around 400-500 Mbit/s.

The web interface of the application is publicly accessible from `http://loadshedding.ccaba.upc.edu/appmon/` (IP address information has been anonymized).

Further information: `http://www.upc.edu/`.

3.2 South-Eastern European Research & Education Network

The South-East European Research and Education Networking project (SEEREN), funded by the European Commission, aims at expanding the European research network in South-East Europe by providing GEANT connectivity to non-GEANT countries. SEEREN has employed LOBSTER technology for both network performance monitoring, through the `appmon` application, as well as for

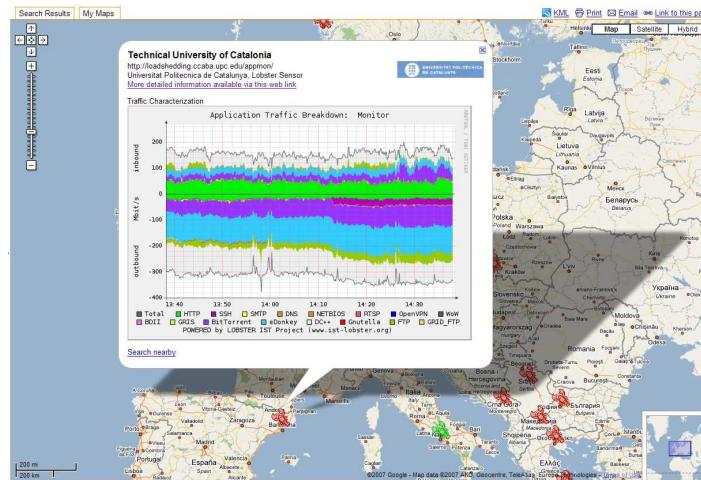


Figure 3.1: Appmon running at the Technical University of Catalonia.

network attack detection, using LOBSTER's polymorphic attack detection application (*nemu*). Three different parts of the SEEREN network are being monitored since early 2007.

3.2.1 Academic & Research Network of Serbia & Montenegro (AMREJ)

The Academic & Research Network of Serbia & Montenegro (AMREJ) is the main network operation center (NOC) of the education and research network in the country, coordinating the international cooperation and technical network development. The network operations center of AMREJ uses both *appmon* and *nemu* for performance and security monitoring.

Further information: <http://www.seeren.org/seeren1/index.php?op=modload&modname=Sitemap&action=sitemapviewpage&pageid=20>

3.2.2 MARNet (FYROM)

MARNet, FYROM's NREN, established in 1995, provides connectivity for academic and research organizations in FYROM. MARNet's NOC uses both *appmon* and *nemu* for performance and security monitoring.

Further information: <http://www.seeren.org/seeren1/index.php?op=modload&modname=Sitemap&action=sitemapviewpage&pageid=19>

3.2.3 MREN (Serbia and Montenegro)

The Montenegro Research & Education Network (MREN), established in 2005, support the communication and information network of the education and research community in Montenegro. MREN's NOC uses both *appmon* and *nemu* for performance and security monitoring.

Further information: <http://www.mren.cg.ac.yu/>.

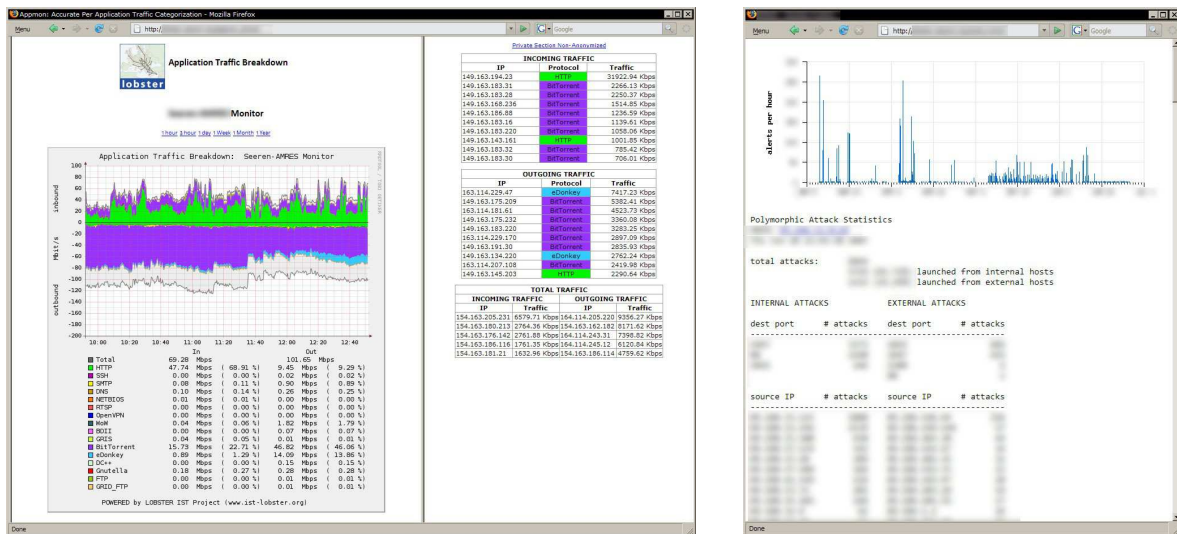


Figure 3.2: The LOBSTER appmon and nemu applications running at the SEEREN network. The IP addresses reported by appmon have been anonymized, while sensitive attack information reported by nemu has been sanitized.

3.3 Bulgarian Academy of Sciences

LOBSTER software has been installed on the monitoring sensor of the Bulgarian Academy of Sciences, which monitors the traffic of Bulgaria's National Research and Education Network. Specifically, the sensor runs the ABW application, which provides live bandwidth usage measurements.

The web interface of the application is accessible from: <http://selena.acad.bg/perfmon/abw>.

Further information: <http://www.bas.bg/>.

3.4 Columbia University (NY)

The Columbia University in the City of New York, USA, has recently installed a passive monitoring sensor based on LOBSTER software. The sensor monitors all traffic of the Network Security Lab of the Computer Science Department, with the sole purpose of performing application-level traffic categorization using the appmon application.

Further information: <http://nsl.cs.columbia.edu/>.

3.5 Institute for Infocomm Research (I²R) – Singapore

The Institute for Infocomm Research (I²R) was established in 2002, with the mission to advance infocomm technologies in Singapore. The Systems and Security Department in I²R has recently installed and operates a LOBSTER sensor that monitors the traffic of the public wireless network of the Institute, which consists of tens of wireless access points. Currently, its main use is to provide traffic categorization measurements using the appmon application.

Further information: <http://www.i2r.a-star.edu.sg/>.

CHAPTER 3. DEPLOYED MONITORING PROBES BY ORGANIZATIONS OUTSIDE THE PROJECT

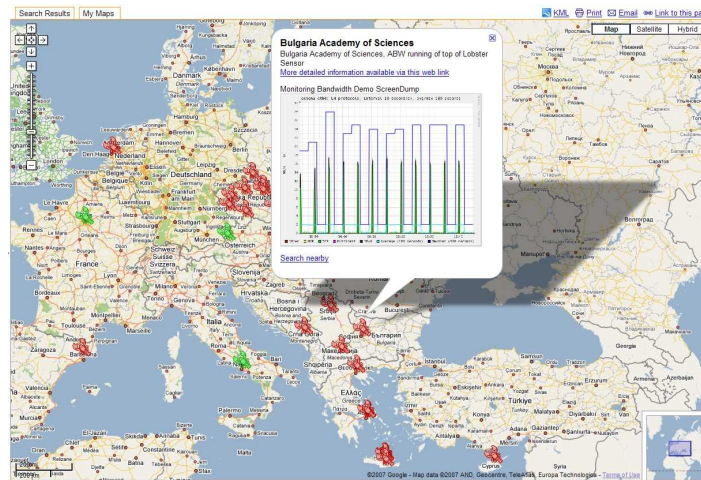


Figure 3.3: ABW running at the Bulgarian Academy of Sciences.

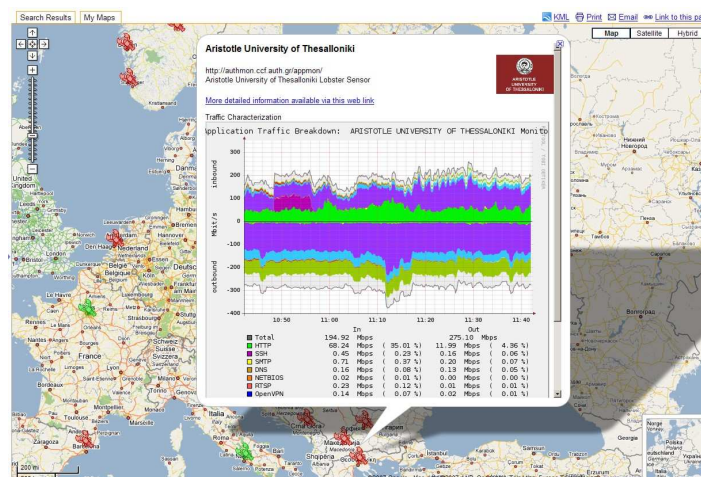


Figure 3.4: Appmon running at the Aristotle University of Thessaloniki.

3.6 National Technical University of Athens

The National Technical University (NTUA) is the oldest and most prestigious educational institution of Greece in the field of technology. The Network Operations Center of NTUA installed a LOBSTER sensor in December 2006, which has been continuously operational since then. The sensor, a Dell 1420SC server equipped with a DAG 4.2GE Gigabit optical passive monitoring card, monitors the almost fully utilized backbone Gigabit link of the campus. The monitored traffic is mirrored directly from the edge router to the DAG monitoring card.

Further information: <http://www.ntua.gr/>, <http://noc.ntua.gr/>.

3.7 Aristotle University of Thessaloniki

The Aristotle University of Thessaloniki (AUTH) is the largest university in Greece. The University Campus covers some 23 hectares close to the centre of Thessaloniki in Northern Greece. The Network

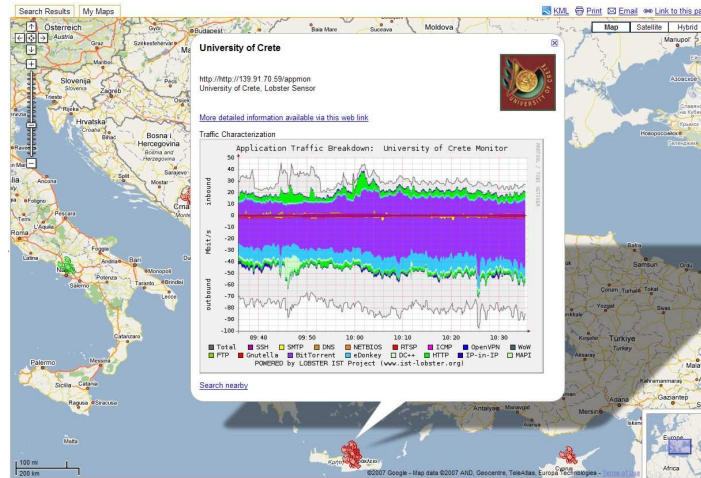


Figure 3.5: Appmon running at the University of Crete.

Operations Center of AUTH has installed a LOBSTER sensor (a Dell SX620 PC) that runs appmon for providing traffic categorization measurements of the campus' traffic (see Figure 3.4).

Further information: <http://www.auth.gr/>, <http://noc.auth.gr/>.

3.8 University of Crete

The University of Crete (UoC) is a multi-disciplinary, research-oriented Institution located in the cities of Rethymnon and Heraklion in Crete, Greece. UCnet, the Network Operations Center of UoC, has installed a LOBSTER sensor at the Heraklion campus, which monitors the traffic of the backbone link that connects the campus to GRNET, the Greek Research and Technology Network. The traffic is mirrored directly to the Gigabit Ethernet monitoring interface of the sensor from the campus' edge router.

The primary use of the sensor is traffic categorization using appmon (see Figure 3.5), which continuously runs on the sensor, while it is also spontaneously being used for security applications.

Further information: <http://www.uoc.gr/>, <http://www.ucnet.uoc.gr/>.

3.9 Cretan Health Network

The network administrators of the Cretan Health Network, which connects all major hospitals and health centers in Crete have installed several LOBSTER sensors for network performance and security monitoring.

3.9.1 Venizelio Hospital in Heraklion

The sensor is located at the second largest hospital in Heraklion, and monitors the 10 Mbps link that connects the local network to the internet. Traffic monitoring is performed using a passive Ethernet Tap which mirrors the traffic to the Ethernet monitoring interface of the LOBSTER sensor. Both appmon and nemu are continuously running on the sensor.

Further information: <http://www.venizeleio.gr/>.



Figure 3.6: The LOBSTER sensor at the Cretan School Network. Note the Gigabit Ethernet Tap used for traffic mirroring under the sensor's 1U server.

3.9.2 Charakas Health Center

The sensor monitors the access link that connects the Health Center of Charakas, located in the southern part of Crete, to the Internet. The primary use of the sensor is for traffic categorization using `appmon`.

3.9.3 Chania Hospital

Chania is the largest city of the Western Crete. A LOBSTER sensor has been installed at the Hospital of the city. The sensor monitors the access link that connects the hospital to the Internet, and its primary use of the sensor is for traffic categorization using `appmon`.

Further information: <http://www.chaniahospital.gr/>.

3.10 Cretan School Network

The Cretan School Network provides Internet connectivity to educational school institutions across Crete. A LOBSTER sensor has been installed at the network edge and monitors the Gigabit link that connects the whole school network to the Greek Research and Technology Network (GRNET). The monitored traffic is mirrored to the sensor using a Gigabit passive Ethernet Tap. Each direction of the full-duplex link is mirrored separately to the two interfaces of the dual Gigabit Ethernet adapter of the 1U server (see Figure 3.6).

Both `appmon` and `nemu` constantly run on the sensor. In fact, recently the new (still under development) version of `appmon` over `Stager` was installed in parallel with the stable version for real-world testing purposes.

Further information: <http://www.sch.gr/>.

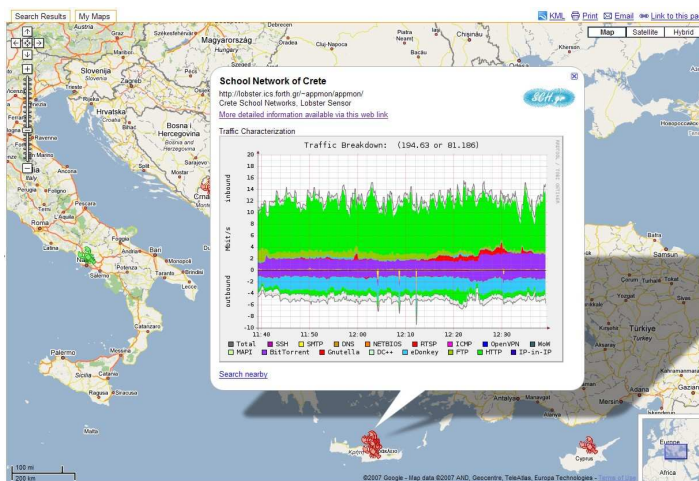


Figure 3.7: Appmon running at the Cretan School Network.

3.11 Cooperation with the GN2 Project

LOBSTER actively cooperates with the European GN2 project developing and operating a European academic network. A JRA1 activity within the GN2 project is responsible for the development of performance monitoring for the GN2 network. A comprehensive monitoring system called perfSONAR is being developed within JRA1. An SA3 activity is then responsible for deployment of the system developed by JRA1.

We have established a JRA1 task force within LOBSTER in order to:

- Make sure that selected LOBSTER applications can provide data to perfSONAR (this is being implemented by MP - Measurement points and by storing data in RRD files accessible to perfSONAR)
- Promote use of passive monitoring within the GN2 network

A passive monitoring deployment proposal was prepared in the SA3 activity and has already been approved by the GN2 project Exec. Under this proposal, several 10 Gb/s passive monitoring stations based on LOBSTER middleware technology at the cost of almost 200.000 Euro will be installed to monitor the main GN2 access links of the following partners:

- ACAD (Bulgaria) - 1 Gb/s sensor
- PSNC (Poland) - 1 Gb/s sensor
- LITNET (Lithuania) - 10 Gb/s sensor
- SWITCH (Switzerland) - 1 Gb/s sensor

A second phase of passive monitoring deployment with additional four or five partners is preliminary considered depending on the success of the first phase.

3.12 Dissemination to ISPs

The project has set up a Task Force with the aim to promote and help the dissemination of LOBSTER technology to ISPs. The following ISPs from South-East Europe countries and have been contacted invited to look and install LOBSTER sensors.

- Cytanet (Cyprus) - <http://www.cytanet.com.cy/>
- SpectrumNet (Bulgaria) - <http://www.spnet.net/>
- UNet (FYROM) - <http://www.unet.com.mk/>

Also, the LOBSTER monitoring software and tools have been proposed to Gnet (<http://www.gnet.gr/>), the largest Greek internet cafe chain, as a solution for their needs for categorization and management of its traffic. Currently they are in process of evaluation of such tools.

Chapter 4

Summary

As of June 2007, the number of operational passive monitoring sensors deployed by LOBSTER's partners and organizations outside the project has increased substantially, reaching 47 sensors across many European countries, USA, and Singapore. The number of deployed sensors is expected to increase further in the near future, since project's partners have already planned to install more sensors during 2007, the collaboration with the GN2 project has already resulted to a deployment plan, while the project's dissemination activities continue with an increasing pace.