INFORMATION SOCIETY TECHNOLOGIES (IST) PROGRAMME

A Scaleable Monitoring Platform for the Internet
Contract No. IST-2001-32404

D3.1 "Experiment Definition and Infrastructure Requirements"

Abstract: This document describes the high-level tasks that need to be accomplished in order to assess both the development progress and the end results of SCAMPI. It defines the current environments in which the experiments are to be performed and will be used to identify the required infrastructure.

Contractual Date of Delivery	31 October 2002
Actual Date of Delivery	12 November 2002
Deliverable Security Class	Internal
Editor	Steven Van den Berghe
Contributors	IMEC, FORTH, LIACS-LU, NETIKOS, UNINETT, CESNET, FORTHnet, 4PLUS, TERENA

The SCAMPI Consortium consists of:

TERENA	Coordinator	The Netherlands
IMEC	Principal Contractor	Belgium
FORTH	Principal Contractor	Greece
LIACS	Principal Contractor	The Netherlands
NETikos	Principal Contractor	Italy
Uninett	Principal Contractor	Norway
CESNET	Principal Contractor	Czech Republic
FORTHnet	Principal Contractor	Greece
4Plus	Principal Contractor	Greece
Siemens	Principal Contractor	Germany

Contents

List of Figures

Chapter 1

Introduction

This document describes the high-level tasks that need to be accomplished in order to assess both the development progress and the end result of SCAMPI. For performing this task, tests will be made on the sites where components are developed and in wide-area environments. The first tests will allow to evaluate individual components or an interconnected set of components in an isolated environment, either based on artificially generated traffic or on stored packet traces. The goal of this phase is to allow functionality, stability and stress tests to continuously be fed back into the development cycle. Once the system (or an stand-alone part of it) is considered ready, further functional, usability and stability testing can be performed in the operational network. In the following section, the evaluation tasks will be outlined based on the functional decomposition of the SCAMPI architecture. After this, an overview will be made of the available equipment[1], both in the development environments and in the final operational testbeds. Finally, the resulting requirements will be summarized and an overview of additionally required infrastructure will be given.

[1] A detailed description of technologies and tools used can be found in [2]

Chapter 2

Evaluation tasks

2.1 Functional Decomposition of the SCAMPI Architecture

Figure 2.1 illustrates the SCAMPI architecture[1]. Each of the four layers in the architecture contains multiple functional components. Initial tests can be used to verify the correctness, performance and robustness of the individual components independent of other components. The input of such tests can be simulated in order to concentrate on the subjects of interest instead of influences of external parameters. The output will be analysed and compared with theoretical expected or required results. To test the Module Organiser for example, input such as monitoring configurations (as defined in the Module Organiser interface specification) can be generated. The output of the testing process will be examined in order to verify the correctness of the Module Organiser. Stress tests, performance tests and stability tests can also be performed on an individual component. In this case the measured performance will be compared to the expected or required performance to steer the development process. Several functional and operational limitations can be necessary during testing. In order to test component functionality's, scaled-down line-speeds such as 100Mbit/s instead of 10Gb/s can be preferred.

The monitoring hardware might include several types, like special purpose monitoring cards (such as DAG cards), monitoring cards based on network processors, commodity hardware such as fast (10 Gb/s) interfaces placed in promiscious mode, and "intelligent" routers/switches such as Juniper's switches.

When each component behaves as required, multiple components can be linked together. Instead of using a single trace-file, the MiddleWare can for example operate on real-time captured data. Performance and stress tests will validate the co-operability of the linked components. When the project evolves, the number of linked components will rise until the tests are running on the entire SCAMPI architecture.

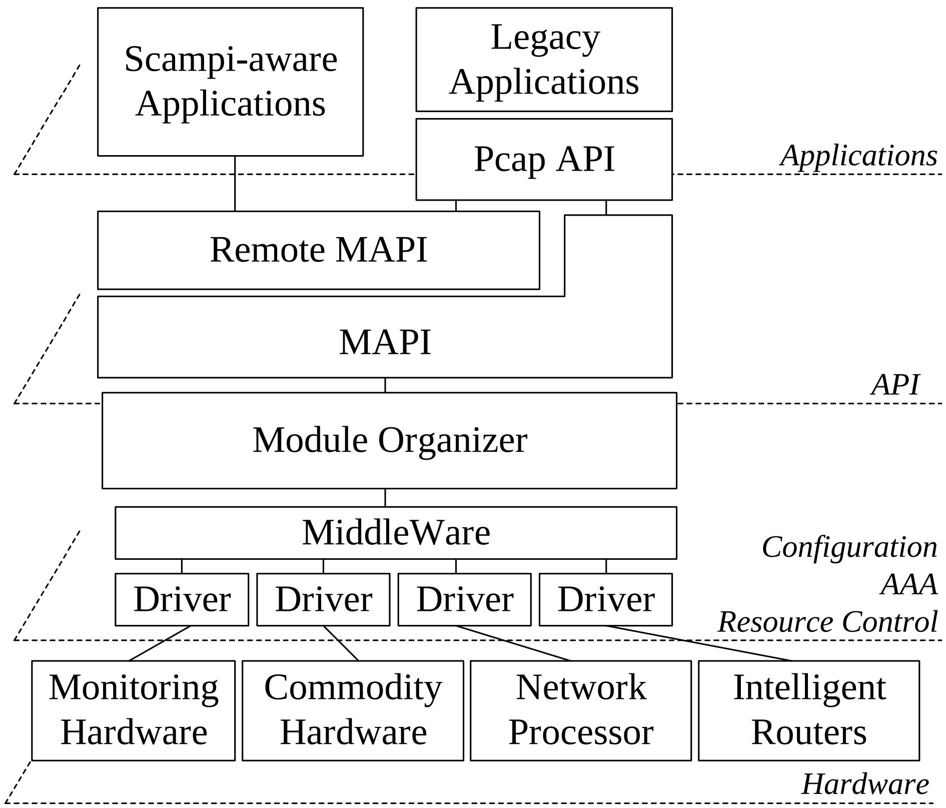

Figure 2.1: SCAMPI Architecture Overview

2.2 Requirements and Goals

Functional Testing Apart from optional small pieces of debugging software, for instance to manually provide artificial input for components, no specific requirements are currently forseen for performing this task. The goal of these tests is to evaluate the technical and semantic correctness of inter-component communication.

Stability Testing These tests will evaluate the correct behaviour of components and (sub-) systems over time. Possible memory leaking errors or other instabilities must be tested. The intermediate and final system tests on the operational environments are the main evaluations where this task will be performed.

Stress Testing For stress tests we need to generate testing traffic streams at congestion speeds. These streams could include patterns of various phenomena to be detected and measured by SCAMPI.

One possibility is to generate these streams directly using commodity network adapters. For example, Intel announced sampling of 10GBASE-LR adapters in near future. In order to achieve the required level of output, this adapter must by installed in an appropriately powerful PC, particularly in terms of bus speed and RAM speed.

Another possibility is to generate a slower testing stream, such as 1 Gb/s, and merge this testing stream with a set of background streams, each running at 1 Gb/s, using a switch with one 10 Gb/s port and multiple 1 Gb/s ports. For example, Cisco announced 10-Gigabit Ethernet adapters for Catalyst 6500 series switches. However, this technology is rather expensive for the purpose of SCAMPI evaluation. In both cases, the testing stream is supposed to be generated in software application, either replaying recorded traffic or generated synthetic streams.

Yet another possibility is to use a commercial traffic generator. However, currently it seems that possibilities to specify the required traffic patterns are rather limited on these generators.

Alternatively, pre-recorded network traces can be re-run at full speed, using a tool called tcpreplay (http://tcpreplay.sourceforge.net/), allowing close to real-life traffic to be generated for experiments in an isolated environment.

2.3 Application-level Experiments

Packet capture functionality The goal of this experiment is to verify that the packet capture functionality of the SCAMPI architecture works properly. It is not a goal of this experiment to verify the performance of packet capture, which will be tested in another experiment. Therefore, this experiment can be conducted on a scaled-down version of the SCAMPI architecture with 100BASE-TX commodity adapter for easier measurement.

Packet capture stress test This test will be performed with the final version of the SCAMPI adapter, operating at the target speed of 10 Gb/s. The purpose of the test is to check that the SCAMPI architecture can operate at the full speed, after its functionality was thoroughly tested at lower speeds on scaled-down adapters.

Packet capture has been selected as a service to be evaluated in this test because it is presumably the most resource demanding monitoring application.

Intrusion and DoS detection The purpose of this test is to check that the SCAMPI architecture correctly detects required intrusion and DoS attempts in a supplied testing traffic.

QoS and TE monitoring The purpose of this test is to check that the SCAMPI architecture can monitor required QoS characteristics with the required precision.

Network flow statistics The goal of this experiment is to verify that network flow statistics reported by the SCAMPI architecture correspond to the characteristics of the monitored network traffic.

Chapter 3

Development Environment

This section describes the environment available at sites where the SCAMPI system will be developed. As part of this development local testing will be done in order to assess the functional behaviour of the developed system. This document should contain the development environment and possible assisting assesement tools of all involved partners (e.g. Smartbits)

3.1 NETikos

Netikos development environment is located mainly in the second most important site, in Pisa. If it will be permitted, some tests will be done also at the University of Pisa to take the advantage of the high - speed connection among the university departments.

3.1.1 Network Equipment

The following equipment is available:

- Intel and AMD based PC's running Linux operating system; Sparc / Intel architecture pc's running Solaris operating system (Solaris 8) and also Mac's Pc's with MacOS-X as operating system as end - system;
- L2 network layer switches: Cisco catalyst clusters (series 3500 XL) with 10 / 100 baseT and 1000 base FX interfaces (VLAN);
- L3 network layer switch: both Cisco and Juniper router (series 2600 for Cisco and series M5-M10 for Juniper Networks) with ATM and 10/100/1000 Mbit Ethernet interfaces.

Further experiments: soon a 1000base FX interface will be available for Netikos M10 router in order to analyze the 1Gb backbone.

3.1.2 Test Tools

The following list describes all the tools available for testing:

- Ntop - based system with ethernet interfaces as network analyzer;
- Snort - based system with ethernet interfaces as above;
- Juniper firewall configuration as traffic sampler;
- Public domain network traffic generator (e.g. Rude);
- Multimedia equipment.

3.2 IMEC

The IMEC testbed is the Atlantis-laboratory located at INTEC premises in Gent, Belgium.

3.2.1 Network Equipment

The following equipment is available:

- Intel- and AMD-based experimental PC's, both in desktop and rack-mounted chases, running the Linux operating system. PC-based systems are used both as end-systems and routers. The available equipment can allow, for instance, for experimentation/development of a medium-size (5-20 hops) Linux-based network.
- Experimental 10/100-BaseT and 1000-BaseF Ethernet network and 155 Mbit multimode fibre ATM network, ADSL-test network
- Commercial network elements: ADSL-rack / DANA, IBM ATM-switches 8265 and 8285, NEC Atomis ATM switch, Cisco 7507 with 10/100Mbit interfaces and 155 Mbit ATM, 3Com Superstack-II with 155Mbit ATM uplink, 10/100/1000 Ethernet Switch The following hosts are available:
- Intel- and AMD-based experimental PC's, both in desktop and rack-mounted chases, running the Linux operating system
- Sun workstations running Solaris

3.2.2 Test Tools

The following test tools are available:

- HP BSTS broadband analyser with ATM/Ethernet interfaces
- SmartBits SMB-2000 traffic generator with 10/100Mbit Ethernet interfaces

- PAMS voice evaluation equipment (for evaluating quality of voice transmission, e.g VoIP) and multimedia equipment (camera's / Quicknet cards for VoIP / ...)

3.3 ICS-FORTH

ICS-FORTH's testbed is located at its premises, at the Science and TEchnology Park of Crete (STEP-C) in Heraklion, Crete, Greece.

3.3.1 Network Equipment

ICS-FORTH has two operational passive monitoring platforms:

- OC3mon-based traffic monitoring platform[1]: Passively captures traffic over an ATM OC3 optical link, with the use of optical splitters.

- 100 Mbps Ethernet-based traffic monitoring platform: Passively monitors traffic from a "port monitoring" port of a Cisco Catalyst 6500.

A third platform for monitoring traffic on a 1 Gbps Ethernet is currently under deployment.

Additionally, the following equipment is available:

- Intel-based PC's running the FreeBSD and Linux operating systems, and Sun workstations running the Solaris operating system.

- Experimental 10/100-BaseT Ethernet network, and 155 Mbps ATM fibre network. Partly experimental 1000-BaseF Ethernet network

- Network elements: Cisco 6500 Catalyst switch, Cisco 7500, 7200, and 4500 routers, Cisco and FORE ATM switches.

3.3.2 Test tools

- Cisco Switchprobe, and Cisco Traffic Director.

- A series of software traffic generators for voice, video, and http traffic.

3.4 LIACS

The LIACS lab development environment is located at the university of Leiden in The Netherlands.

[1] More information on this platform is available at `http://tracer.ucnet.uoc.gr`

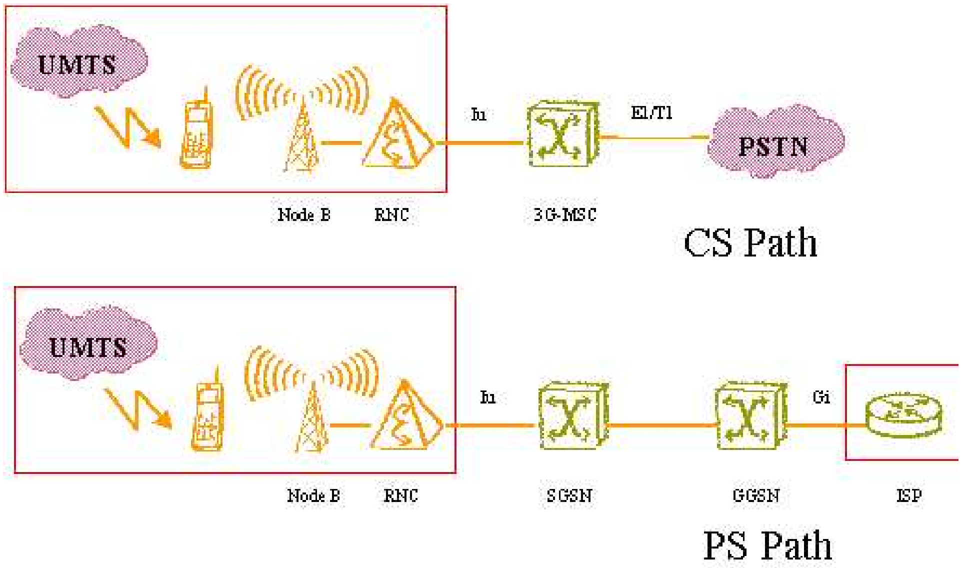

Figure 3.1: 4Plus-Siemens Networking Environment

3.4.1 Network Equipment

In addition to the commodity Linux-based routers and GigE cards, LIACS currentlyhas an IXP1200 evaluation board with 2 GigE ports (connected to a PC with GigE adapter). It's installed in a server with 3 64/66 PCI slots (which might be useful for experiments with fast cards and a lot of PCI traffic).

3.5 4PLUS

At company's premises, located in Athens, Greece, there is no networking environment to be used for SCAMPI tests. Alternatively, 4Plus maintains, jointly with Siemens ICM, a 3G UMTS testing environment (figure 3.1) in Munich, Germany, which may be used for the purpose of hosting some short of SCAMPI traffic experiments.

3.5.1 Network Equipment

The following equipment is available:

- GGSN gateway.
- SGSN gateway.
- Mobile switching controller (MSC).

3.5.2 Test tools

The following test equipment is available:

- Iu/Gi traffic generator and analyser capable of performing mobile subscribers simulation (both voice and IP services are available) on both c/u-plane stacks.
- Gi/Gn traffic generator and analyser capable of simulating SGSN and GGSN functionality.

3.6 UNINETT

UNINETT operates a National Research and Education Network (NREN) and a National Test Net in Norway. There is also a testbed available located at the premises in Trondheim, Norway.

3.6.1 Network Equipment

In addition to the production networks, the following equipment is available:

- Two DAG 3.5 cards. Passive monitoring cards capable of measuring at OC3 and OC12 speeds.
- Two DAG4Ge cards. Passive monitoring cards for Gigabit Ethernet. Will be available by the end of the year
- Intel based experimental PC's running Linux operating system. Other operating systems can be installed if needed.
- Various Cisco routers and switches.

3.7 CESNET

CESNET operates a National Research and Educational Network (NREN) in the Czech Republic. There is also a network research laboratory in CESNET promises.

3.7.1 Network Equipment

CESNET is primarily concerned with evaluation of the SCAMPI platform. For the development work that will be done in CESNET, the same equipment as described in section 4.1.1 can be used.

For laboratory experiments, CESNET can provide the following equipment. All the equipment is currently used for research purposes other than SCAMPI, but sharing the equipment with SCAMPI and in some cases dedicating the equipment to SCAMPI is possible.

- Various Cisco routers and switches, namely GSR12080 with 3-port Gigabit Ethernet adapter, 7507 router with two Gigabit Ethernet ports and four Fast Ethernet ports, 3660 router with two Fast Ethernet ports, 2600 router with two Fast Ethernet ports, 3550 switch with 12 Gigabit Ethernet ports.

- PCs with Gigabit Ethernet and Fast Ethernet adapters (currently three PCs)

Chapter 4

Evaluation Environment

Next to the in-lab testing that is an inherent part of the development cycle. Tests on realistic data/networks, must cross-check the functionality of the system and assess its performance. This can be done based on pre-recorded traces (which provides a constant, well-known input to SCAMPI, allowing to compare the system both with its different development stages, and with third-party products). In further steps, the evaluation can also be done with life traffic (both at low and higher speeds).

4.0.2 Network traces

The following traces are available

- ATM and TCP/IP layer packet-level traces containing traffic between ICS-FORTH and GRnet (Greek Research and Technology Network), and between the University of Crete and GRnet. These traces have been captured using the two monitoring platforms described above.
- Other publicly available traffic traces can be found at "Capture the Capture The Flag" (`http://www.shmoo.com/cctf/`) and "The Internet Traffic Archive" (`http://ita.ee.lbl.gov/`). ICS-FORTH has local copies of the traces in these archives, which are used for conducting performance evaluation tests.
- Sample "crack"-traces, available at `http://www.ethereasl.com/sampl`

Next to these and other publicly available traces, the partners might make other traces available captured on their own links.

4.1 Operational Network Environments

4.1.1 CESNET

The backbone of the Czech NREN operated by CESNET (fig. 4.1) is currently running at OC-48 and Gigabit Ethernet speeds. Upgrade of some circuits to 10

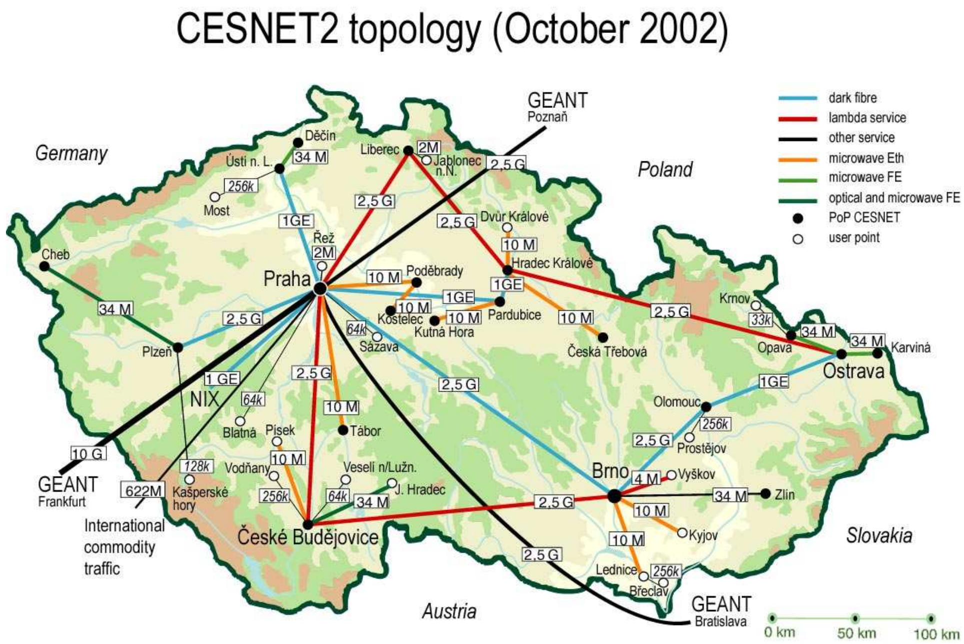

Figure 4.1: CESNET Operational Network

Gb/s is planned in the timeframe of the project. 10-Gigabit Ethernet currently seems to be more prospective technology for our network than OC-192 mainly due to its much lower cost.

The network can be used for SCAMPI evaluation provided that its production operation will not be disrupted in any way. Namely, we assume that optical splitters will be installed on some of the backbone circuits to connect SCAMPI adapters allowing evaluation on the real-world traffic. Privacy of network users must be guaranteed through proper technical and administrative measures.

4.1.2 UNINETT

The backbone of the Norwegian NREN operated by UNINETT (fig. 4.2) currently operates at speeds ranging from OC3 to OC48. Many of the slower network connections are planned upgraded to OC48 during the project timeframe. UNINETT also operates a National Test Network currently at OC3 speeds.

These networks can be used for SCAMPI evaluation provided that the production operation will not be disrupted and that the privacy of users are guaranteed through proper technical and administrative measures.

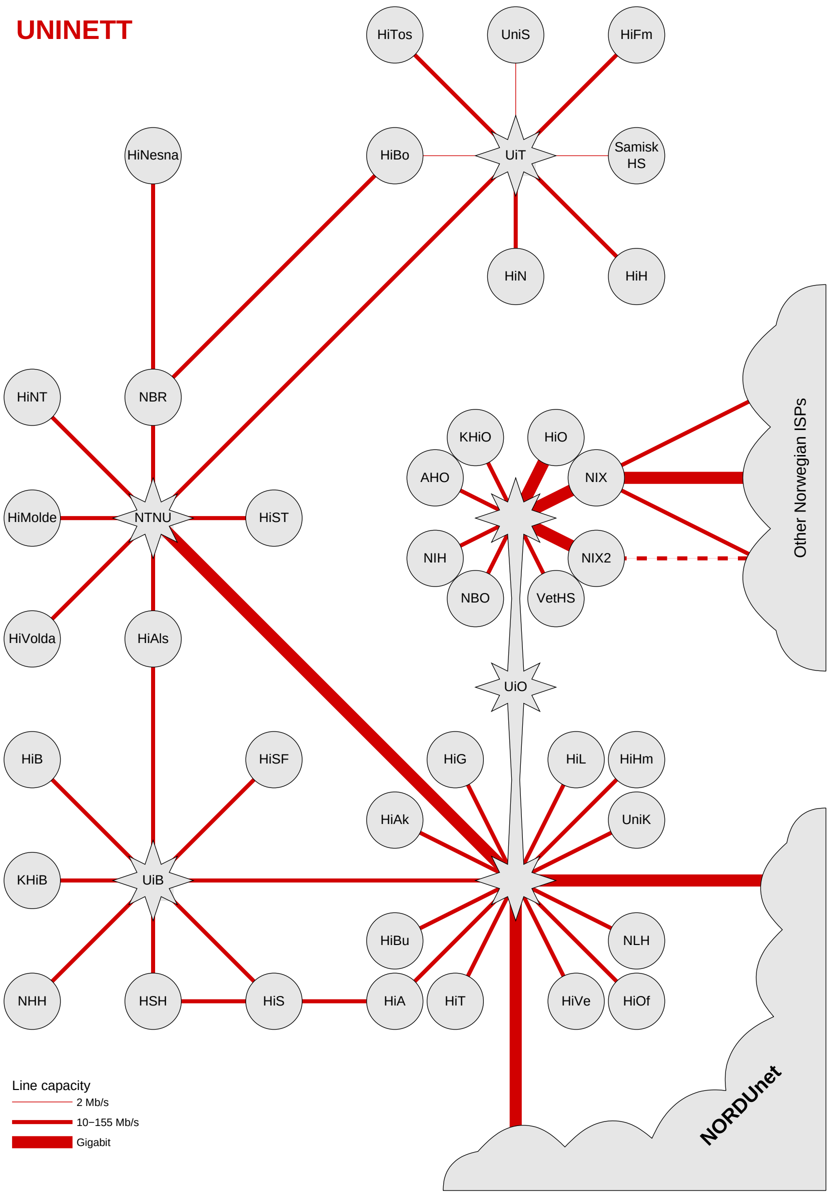

Figure 4.2: UNINETT Operational Network

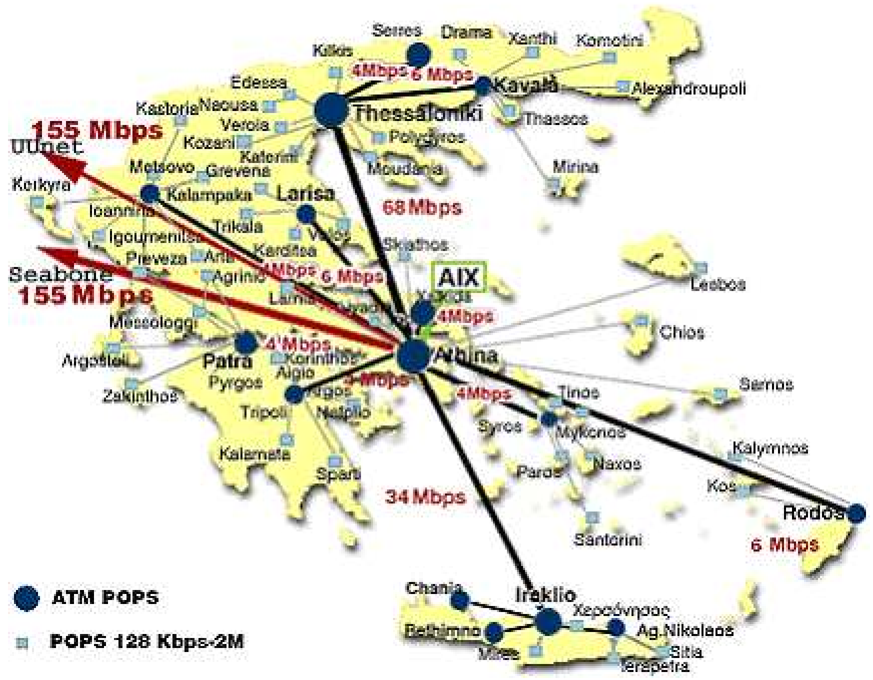

Figure 4.3: FORTHNET Operational Network

4.1.3 FORTHNET

FORTHnet (fig. 4.3) as a Greek Internet Service Provider and an alternative Telephony (VoIP) Provider operates a commercial network as shown in the respective figure. It's backbone links speed range from NxE1 to OC3. Network connections continuously upgraded as the demand increases. Services supported by this network are described briefly below:

- **Internet Access Services:** PSTN dialup, ISDN, Dedicated lines
- **Telecommunication Services:** Frame Relay, DATA VPN services, FORTHnet Telephony, LMDS
- **Content, Value Added Services** such as Real time Stock Market info, Web hosting, Directory services
- By using the appropriate equipment, the user may also have wireless connection of high speed local networks (LAN-Lan) (up to 34Mbit/s), wireless connection of telephone centres (PBX), permanent wireless high speed Internet connections

The following equipment is available:

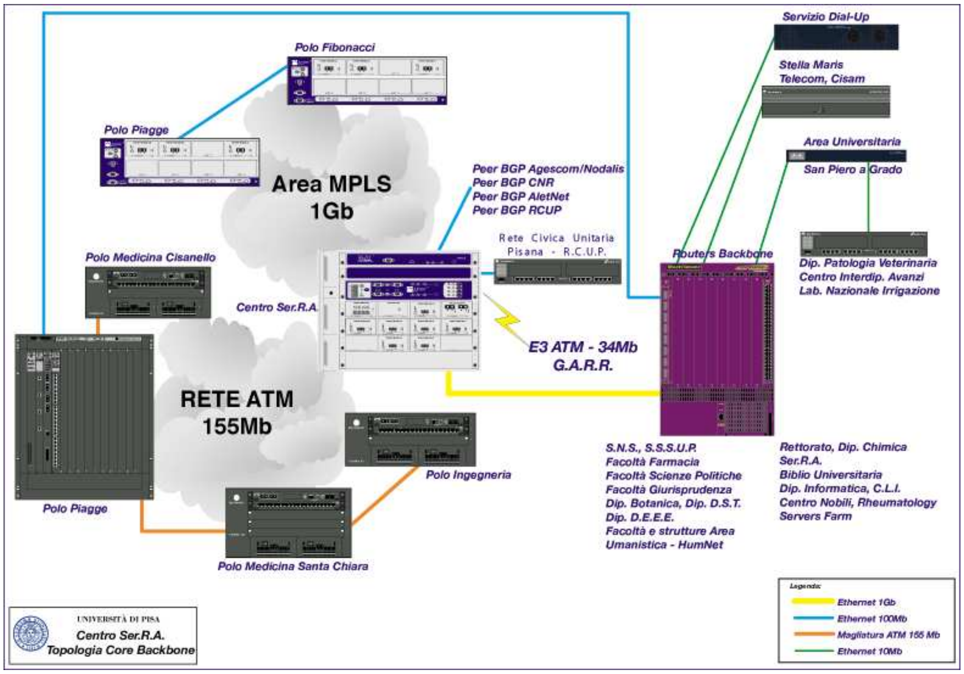

Figure 4.4: University of Pisa Operational Network

- Cisco 7500, 7200 routers with Gigabit Ethernet adapters and FastEthernet ports.
- Cisco 6500 - 5500 catalysts switches
- 25 Cisco ATM switches (IGX 8410-8420, BPX 8620, MGX 8230)
- 4 Gigabit Ethernet and over 20 FastEthernets
- Intel-based PCs running Linux operating system and Sun servers with Solaris operating system All the above equipment and networks are currently in operational use.

The network can be used for SCAMPI evaluation provided that its production operation will not be disrupted in any way. Privacy of users must also be guaranteed through proper technical and administrative measures.

4.1.4 University of Pisa

Optional tests might be conducted ont the backbone network of the University of Pisa (fig 4.4). This will soon move from 1 to 2.5 Gb for the Internet Backbone.

4.1.5 TERENA

Terena can cooperate with nationwide providers in order to provide access to high-speed network links, provided that the production operation will not be disrupted and that the privacy of users are guaranteed through proper technical and administrative measures.

Chapter 5

Requirements Summary

This section describes current infrastructure extensions that need to be provisioned.

Optional equipment for generation of 10 Gb/s testing streams with required patterns. Following options are availabe for this:

- 10GBASE-LR adapter + PC
- A set of 1000BASE-SX adapters and PCs + switch
- Commercial 10 Gb/s generator

Bibliography

[1] SCAMPI Consortium, “Deliverable D1.1: High Level SCAMPI Architecture and Components”

[2] SCAMPI Consortium, “Deliverable D0.1: ”Description and Analysis of State-of-the-art”

[3] *IST SCAMPI Project*, http://www.ist-scampi.org