

# FP7 Research Infrastructures

## BSI

### Black Sea Interconnection



---

## Deliverable D4.2

### Operational Procedures and Management Framework

---

**Author(s):** Beyhan Çalışkan

**Status –Version:** Final

**Date:** September 24, 2009

**Distribution - Type:** Public

**Code:** BSI-D4.2-a-2009-09-24

**Abstract:** This document describes the created BSI network topology, equipment specifications and configuration, routing and addressing plans, also established links characteristics. The information provided in this document will be used by technical personnel involved in the management of the BSI network (BSI NOC).

© Copyright by the BSI Consortium

The BSI Consortium consists of:

TUBITAK  
GRNET  
CEENET  
DANTE  
GRENA  
AzRENA

Coordinating Contractor  
Contractor  
Contractor  
Contractor  
Contractor  
Contractor

Turkey  
Greece  
Austria  
United Kingdom  
Georgia  
Azerbaijan



This document contains material, which is the copyright of certain BSI contractors and the EC, may not be reproduced or copied without permission.

The commercial use of any information contained in this document may require a license from the proprietor of that information.

The contractors do not warrant that the information contained in the report is capable of use, or that use of the information is free from risk, and accept no liability for loss or damage suffered by any person using this information.

## Document Revision History

<b>Date</b>	<b>Issue</b>	<b>Author/Editor/Contributor</b>	<b>Summary of main changes</b>
July 14 <sup>th</sup> , 2009	a	Beyhan Çalışkan	First draft version
September 24 <sup>th</sup> , 2009	b	Beyhan Çalışkan	Final Version

## Preface

The Black Sea Interconnection (BSI) project aims to achieve a high-speed network backbone among the NRENs of the South Caucasus countries (Armenia, Azerbaijan and Georgia) and enable connectivity to the pan-European GÉANT network. The BSI project intends to introduce new technologies and services to the Information Society in those countries and be an important leap towards the integration of those countries' scientific potential with the European Research Area. The project involves the development of strategies for interconnecting the existing infrastructures in the region, realization of the connections and supplying operational support for the established network. The project beneficiaries are TUBITAK, GRNET, CEENET, DANTE, GRENA, AzRENA and NAS RA.

The main objectives of the BSI project are:

1. Building a proper regional research and education network among South Caucasus countries and connecting it to GÉANT.
2. Integration of South Caucasus scientific potential to Europe by successfully disseminating the infrastructure and promoting the ICT projects in South Caucasus countries.
3. Fostering collaboration between homogenous scientific communities by identifying the involved communities in the region and establishing mechanisms for knowledge transfer.

The BSI project has started its activities on March 2008 and is planned to be completed by the end of February 2010. BSI is coordinated by TUBITAK. The total budget of the project is 1 861 908 € and it is co-funded by the European Commission's Seventh Framework Programme for Research Infrastructures and National budgets of South Caucasian Countries.

The BSI consortium will achieve the following milestones:

Milestone number	Milestone name	Date	Status
M1	Kick-off meeting	M1	√
M2	Project management information system established	M1	√
M3	Promotional package available	M4	√
M4	NRENs requirements collected and analysed	M2	√
M5	Technical and operational requirements analysed	M3	√
M6	Tenders prepared	M3	√

M7	Suppliers selected	M4	√
M8	Connectivity and equipment contracts signed	M5	√
M9	Final BSI topology determined	M5	√
M10	Operation of the regional networking infrastructure offering access to BSI NRENs GÉANT2 access	M6	√
M11	Management framework in place and stable network operation	M8	√
M12	Services/tools selected	M10	√
M13	Successful completion of first period project review	M12	√
M14	Workshop/Conference Track in region organized	M20	
M15	Services/tools deployed	M20	
M16	Successful completion of project - final project review	M24	

The project will issue the following deliverables:

<b>Del. no.</b>	<b>Deliverable name</b>	<b>Nature</b>	<b>Dissemination Level</b>	<b>Date</b>	<b>Status</b>
D1.1	Project Management Information system	R	CO	M1	√
D1.2	Network Acceptable Use Policy	R	PU	M4	√
D2.1	Requirements capture and an analysis	R	PU	M1	√
D2.2	Networking topology options and implementation approaches	R	PU	M2	√
D3.1	Tender progress report	R	CO	M4/M5/M6	√
D3.2	Network topology	R	PU	M6	√
D4.1	Network implementation and equipments configuration	R	PU	M9	√
D4.2	Operational procedures and management framework	R	PU	M10	
D4.3	Networking services and tools specifications	R	PU	M12	
D4.4	Deployment of essential network services and management tools	R	PU	M21	
D5.1	Web site, docs repository and mailing lists	R	PU	M1	√

D5.2	BSI Promotional material	O	PU	M8	√
D5.3	Stakeholders meetings in beneficiary countries	R	PU	M15	
D5.4	Report on awareness and liaison activities	R	PU	M23	

*R = Report , O = Other , PU = Public, CO = Confidential (only for members of the consortium incl. EC).*

## Table of Contents

<b>1. Introduction .....</b>	<b>12</b>
<b>2. BSI Standardized Operational Procedures.....</b>	<b>13</b>
2.1. FAULT MANAGEMENT.....	13
2.2. CONFIGURATION MANAGEMENT.....	14
2.3. ACCOUNTING MANAGEMENT.....	14
2.4. PERFORMANCE MANAGEMENT.....	14
2.5. SECURITY MANAGEMENT .....	14
2.6. SERVICE MANAGEMENT.....	15
2.6.1. MONITORING .....	15
2.6.2. CONTROL .....	15
2.6.3. REPORTING .....	15
<b>3. BSI Virtual NOC Framework .....</b>	<b>15</b>
<b>4. Network Management and Monitoring Instruments.....</b>	<b>17</b>
4.1. NAGIOS .....	17
4.1.1. INTRODUCTION .....	17
4.1.2. MONITORING WITH NAGIOS.....	19
4.2. TROUBLE TICKET SYSTEM .....	20
4.3. SLA MANAGEMENT.....	20
4.4. NETWORK TRAFFIC CLASSIFICATION AND USAGE .....	21
4.4.1. NFSEN & NFDUMP .....	21
4.4.2. NETWORK USAGE MONITORING .....	23



## References

- [1] BSI Consortium, “Black Sea Interconnection (BSI), Annex-I Description of Work”, March, 2008
- [2] BSI Consortium, “D2.1 BSI Requirements Capture and an Analysis”, April, 2008.
- [3] BSI Consortium, DoW9 Description of Work
- [4] Deliverable D4.1 Network Implementation Equipments Configuration
- [5] INTERNATIONAL TELECOMMUNICATION UNION M.3400
- [6] <http://www.nagios.org>
- [7] <http://oss.oetiker.ch/mrtg/><http://oss.oetiker.ch/mrtg/>
- [8] <http://nfsen.sourceforge.net/>
- [9] <http://www.cacti.net>

## List of Figures

Figure 1 Nagios monitoring example.....	19
Figure 2 Nfsen tool at NASRA.....	22
Figure 3 Classifying traffic characteristic with NFSEN .....	23

## Executive Summary

### What is the focus of this deliverable?

The focus of this deliverable is to present standardized operational procedures, problem solving tasks and maintenance tasks in the day-to-day use of the BSI network. This deliverable reports on the management framework of the network and describes the concept and implementation of BSI VNOC daily operations. Selected and installed tools used to manage the network connections and services presented in this document.

### What is next in the process?

1. Develop close relation with GEANT and work for the full integration of established infrastructure in GEANT.
2. Work for integration of South Caucasus countries scientific potential to Europe.
3. Disseminate the knowledge gained among research and educational institutions in the region.
4. Work with international donor organizations and local governments for the continuation of this project.

### What are the deliverable contents?

The deliverable consists of an introductory chapter followed by the management framework of the network, concept and implementation of the BSI daily operations and main software tools used to manage the network connections and services.

### Conclusions

In Deliverable 4.2, BSI management framework and operational procedures reported in detail. This report could be use as a handbook for beneficiary NRENs for day-to-day operations and management.

## 1. Introduction

The BSI (Black Sea Interconnection) project intends on bridging the digital divide that exists between the South Caucasus countries and Europe by establishing a regional research and education network in the South Caucasus and connecting it to GÉANT. The project involves the development of strategies for interconnecting the existing infrastructures in the region, realization of the connections and supplying operational support for the established network. The existence of interconnections between the South Caucasus countries and connection to GÉANT with reasonable capacities will enable introduction of new services to the region and will be an important step towards the integration of the scientific potential in the region with Europe.

In this document BSI VNOC activities, management, monitoring and operating procedures reported in detail. Selected BSI service tools and their options described for NRENs technical staffs. Therefore this text could be a handbook for operational actions.

## 2. BSI Standardized Operational Procedures

The comprehensive management of an NREN's information technology (IT) infrastructure is a fundamental requirement. Researchers and high level applications like GRID rely on IT services where availability and performance are mandated, and problems can be quickly identified and resolved. Mean time to repair (MTTR) must be as short as possible to avoid system downtimes where a loss of revenue or lives is possible. For this reason FCAPS defined in Open System Interconnection Systems Management Overview (SMO) standard. FCAPS is an acronym for Fault, Configuration, Accounting, Performance, Security which are the management categories into which the ISO model defines network management tasks.

The following components are used for BSI network management;

- Fault management
- Configuration management
- Accounting management
- Performance management
- Security management

Additionally following components are used for BSI service management;

- Monitoring
- Controlling
- Reporting

To comprise all components mentioned, Open Source tools employed in the BSI network operations. Management and service tools described below in detail.

### 2.1. Fault Management

The main scope of fault management is to recognize, isolate, correct and log faults that occur in the network. Furthermore, it uses trend analysis to predict errors so that the network is always available. This can be established by monitoring different things for abnormal behavior. Fault management at the BSI network to be ensured by **Nagios**. The correction of discovered problems follows a procedure between BSI VNOC, GEANT NOC and the OTEGLOBE helpdesk.

## **2.2. Configuration Management**

The goals of configuration management cover;

- to gather and store configurations from network devices
- to simplify the configuration of the device
- to track changes which are made to the configuration
- to configure ('provision') circuits or paths through non-switched networks

BSI network configuration management will be implemented with **CVS/RANCID** and **Looking Glass**. RANCID can automatically archive backup copies of configuration (config) files to a Concurrent Versions System (CVS) repository, detect updates and backup config file versions to CVS, and notify operators of individual command changes via email. With this tool BSI has a disaster recovery solution.

## **2.3. Accounting Management**

Accounting is often referred to as billing management. The goal is to gather usage statistics for users. Using the statistics the users can be billed and usage quota can be enforced. However billing not take place in BSI.

## **2.4. Performance Management**

Performance management enables the manager to prepare the network for the future, as well as to determine the efficiency of the current network. By collecting and analyzing performance data, the network health can be monitored. Trends can indicate capacity or reliability issues before they become service affecting. This type of management will be implemented with Nagios and NFSEN.

## **2.5. Security Management**

Security management is the process of controlling access to assets in the network. Data security can be achieved mainly with authentication and encryption. Authorization to it configured with OS and DBMS access control settings. Security management will be implemented with the deployment of **ACLs**, the help of **CVS/RANCID** and **NFSEN** anomaly detection plugins.

## **2.6. Service Management**

### **2.6.1. Monitoring**

Monitoring of services purpose to get information from network devices. It will be done with Nagios, Cacti and MRTG. The following services are intend for monitoring;

- BSI border router interfaces
- BSI border router cpu utilization
- Status of BGP sessions
- Status of monitoring servers
- Status of NTP servers

### **2.6.2. Control**

Manipulation of devices requires human interaction. No automatic action will take place.

### **2.6.3. Reporting**

Reporting refers to documentation of abnormal events and circulating the documents. This will be implemented by Request Tracker and BSI NOC mail list.

## **3. BSI Virtual NOC Framework**

BSI NOC using a virtual NOC scheme. The basic concept of the VNOC scheme is that BSI operations and services management will be provided by different NREN NOCs following a fully distributed paradigm. Main responsibilities of VNOC described below;

- Regularly arrange meetings between NOC members to guarantee efficient problem solving and defining new services.
- Perform high level design of services and implement to the network.
- Monitor the services provided by the BSI Network.
- Implement advanced services.
- Interact with GEANT NOC and service provider (OteglobE) helpdesk for fault management.
- Provide a study for proposed services related to BSI Network.
- Provide configuration and installation files to implement proposed services.
- Testing the new services before implement to the network.

- Responsible for appropriately configuring the NREN access router.
- Monitor network operation in their area of authority.

Following table shows BSI VNOG members.

<b>Country</b>	<b>BSI – NREN</b>	<b>NOC member(s)</b>
Turkey	ULAKBIM	Beyhan Caliskan Tel.:+903122989376 Fax:+903122989393 E-mail: beyhan@ulakbim.gov.tr
Armenia	NAS RA	Arthur Petrosyan Tel.: +37493656507 E-mail: arthur@sci.am  Armen Khachatryan Tel.: +37494672706 E-mail: armen@hf.a  Eugene Prokhorenko Tel: +374 10 526742 E-mail: eugene@sci.am
Azerbaijan	AzRENA	Irshad Guliyev Tel.: +994(12) 510 11 00 Mob: +994 70 244 61 95 E-mail: admin@azrena.org
Georgia	GRENA	Nick Elbakidze Tel.: +995 32 250591 Mob: +995 93 355 755 E-mail: nelbakidze@grena.ge David Kvatadze Tel.: +995 32 251440 E-mail: datok@grena.g



## 4. Network Management and Monitoring Instruments

BSI management and monitoring instruments selected from popular Open Source softwares. Furthermore this softwares running on Open Source operating systems. Therefore BSI management and monitoring tools implemented in the manner of cost effective / high performance frame.

Each NREN installed and configured their own monitoring server and ULAKBIM monitors all of them continuously.

### 4.1. Nagios

#### 4.1.1. Introduction

Nagios is a powerful monitoring system that enables organizations to identify and resolve IT infrastructure problems before they affect critical business processes. Because of below Nagios features BSI NOC choose it to install.

##### 1. Comprehensive Monitoring

- Capabilities to monitor applications, services, operating systems, network protocols, system metrics and infrastructure components with a single tool
- Powerful script APIs allow easy monitoring of in-house and custom applications, services, and systems

##### 2. Visibility

- Centralized view of entire monitored IT infrastructure
- Detailed status information available through web interface

##### 3. Awareness

- Fast detection of infrastructure outages
- Alerts can be delivered to technical staff via email or SMS
- Escalation capabilities ensure alert notifications reach the right people

##### 4. Problem Remediation

- Alert acknowledgments provide communication on known issues and problem response
- Event handlers allow automatic restart of failed applications, services, and services

##### 5. Proactive Planning

- Trending and capacity planning addons ensure you're aware of aging infrastructure

- Scheduled downtime allows for alert suppression during infrastructure upgrades

## **6. Reporting**

- Availability reports ensure SLAs are being met
- Historical reports provide record of alerts, notifications, outages, and alert response
- Third-party addons extend reporting capabilities

## **7. Multi-Tenant Capabilities**

- Multi-user access to web interface allows stake holders to view infrastructure status
- User-specific views ensures clients see only their infrastructure components

## **8. Extendable Architecture**

- Integration with in-house and third-party applications is easy with multiple APIs
- Hundreds of community-developed addons extend core Nagios functionality

## **9. Stable, Reliable, and Respected Platform**

- Over 10 years of active development
- Scales to monitor 100,000+ nodes
- Failover capabilities ensure non-stop monitoring of critical IT infrastructure components
- Multiple awards, media coverage and recognition prove Nagios' value

## **10. Vibrant Community**

- An estimated 250,000 users worldwide
- Active community mailing lists provide free support
- Hundreds of community-developed addson extension Nagios' core functionality

## **11. Customizable Code**

- Open Source Software
- Full access to source code
- Released under the GPL license

### 4.1.2. Monitoring with Nagios

Monitoring targets are mainly BSI border routers and service servers. Each NREN configured Nagios for monitoring;

- BSI border router interface status
- BSI border router cpu utilization
- BSI border router memory utilization
- BSI border router interface statistics
- BSI border router traffic usage
- BSI border router BGP status
- BSI service server NTP service
- BSI service server health status
- BSI service server cpu utilization
- BSI service server disk usage

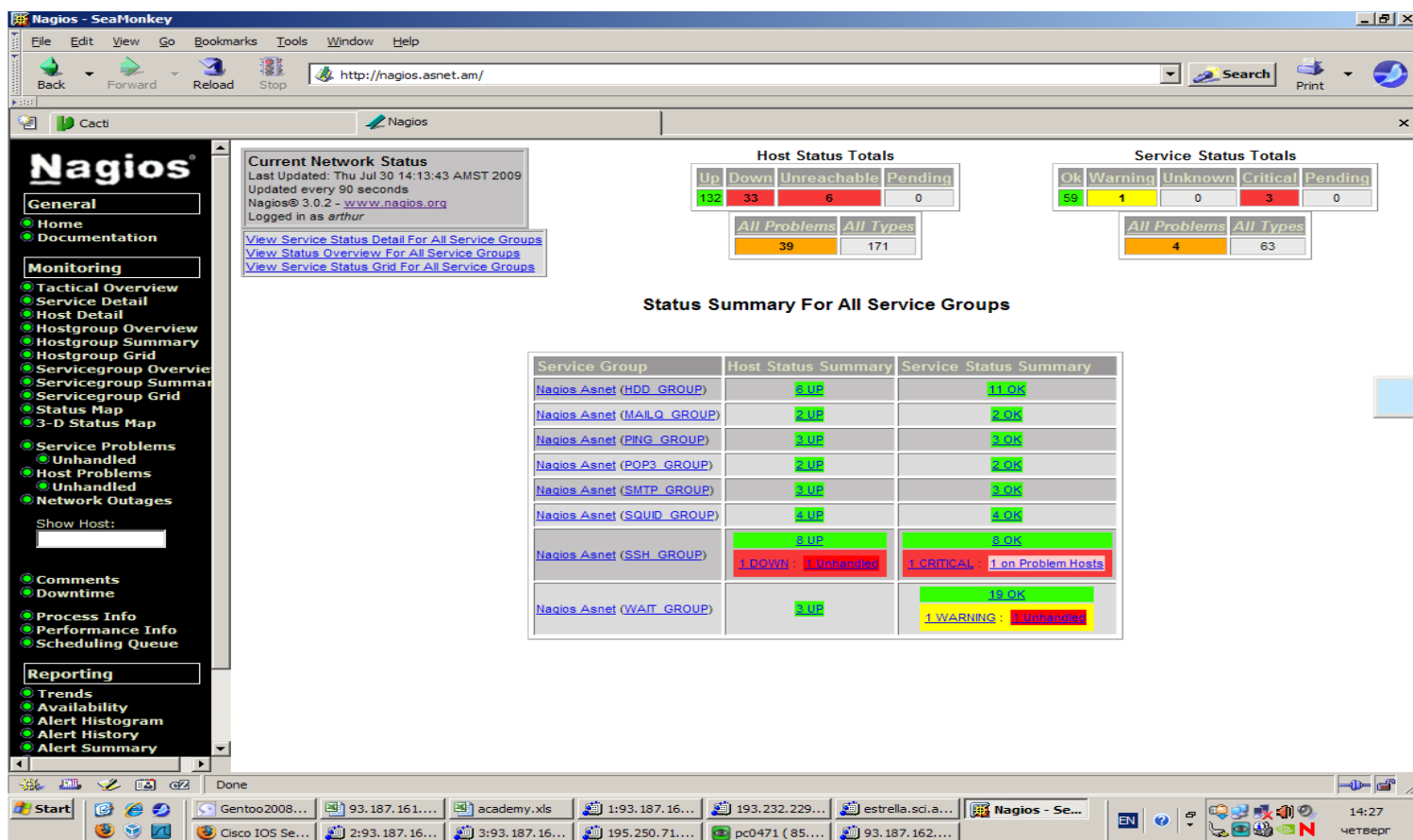


Figure 1 Nagios monitoring example

## 4.2. Trouble Ticket System

RT is an enterprise-grade ticketing system which enables a group of people to intelligently and efficiently manage tasks, issues, and requests submitted by a community of users. The RT platform has been under development since 1996, and is used by systems administrators, customer support staffs, IT managers, developers and marketing departments at thousands of sites around the world. Written in object-oriented Perl, RT is a high-level, portable, platform independent system that eases collaboration within organizations and makes it easy for them to take care of their customers.

RT manages key tasks such as the identification, prioritization, assignment, resolution and notification required by enterprise-critical applications including project management, help desk, NOC ticketing, CRM and software development. RT is used by Fortune 100 companies, government agencies, educational institutions, and development organizations worldwide.

BSI NOC is using GEANT NOC's request tracker system instead of installing own RT. This approach resolves complex workflow between BSI VNOC and GEANT. BSI NREN NOC members, are registered to GEANT's request tracker database to directly connect and quickly resolve possible problems.

## 4.3. SLA Management

According to contract with the connectivity provider, SLA affects failures caused by the provider only. Therefore, BSI NOC informs the provider immediately on the basis of individual event logs which are generated by Nagios.

For SLA monitoring each three of NREN set up their own Nagios application and ULAKBIM monitors all of them continuously. Some of the error and warning notifications generated by Nagios below;

```
***** Nagios 2.6 *****  
  
Notification Type: PROBLEM  
  
Service: PING  
Host: nasra router  
Address: 62.40.125.178  
State: WARNING  
  
Date/Time: Wed Jul 15 10:29:46 UTC 2009  
  
Additional Info:  
  
PING WARNING - Packet loss = 20%, RTA = 113.03 ms
```

### Packet Loss Warning

```
***** Nagios 2.6 *****  
  
Notification Type: PROBLEM  
Host: nasra  
State: DOWN  
Address: 62.40.125.178  
Info: CRITICAL - Plugin timed out after 10 seconds  
  
Date/Time: Tue Jul 21 14:54:06 UTC 2009
```

#### Host Down Warning

```
***** Nagios *****  
  
Notification Type: RECOVERY  
Host: nasra  
State: UP  
Address: 62.40.125.178  
Info: PING OK - Packet loss = 0%, RTA = 59.81 ms  
  
Date/Time: Thu Jul 23 07:10:40 EEST 2009
```

#### Host Up Notification

## 4.4. Network Traffic Classification and Usage

Identifying network characteristic at BSI Network is very important task. Therefore, since the beginning of NOC activities, BSI NOC members informed about this subject at every turn. Regarding to this subject Beyhan ÇALIŞKAN prepared a special training at 9 - 11 February 2009, Tbilisi. Monitoring traffic characteristics and identifying network anomalies with **NFSEN** trained and practiced exhaustively. For ease of installation automatic NFSEN installation script developed for FreeBSD operating system.

BSI link usage is being monitored via various Open Source tools and also from different locations. All of the three NREN links monitoring from centralized server which was located at ULAKBIM and each NREN is monitoring their own link usage individually. BSI NOC is using **MRTG**, **CACTI** and **Network Weather Map** for monitoring links.

### 4.4.1. Nfsen & Nfdump

The nfdump tools collect and process netflow data with optimized speed and efficient filtering on the command line. To visualize nfdump operations, Nfsen provides the web interface. These tools have below usable features for BSI network classification approaches;

- Display netflow data: Flows, Packets and Bytes using RRD (Round Robin Database).

- Easily navigate through the netflow data.
- Process the netflow data within the specified time span.
- Create history as well as continuous profiles.
- Set alerts, based on various conditions.
- Easy to write plugins to process netflow data on a regular interval.

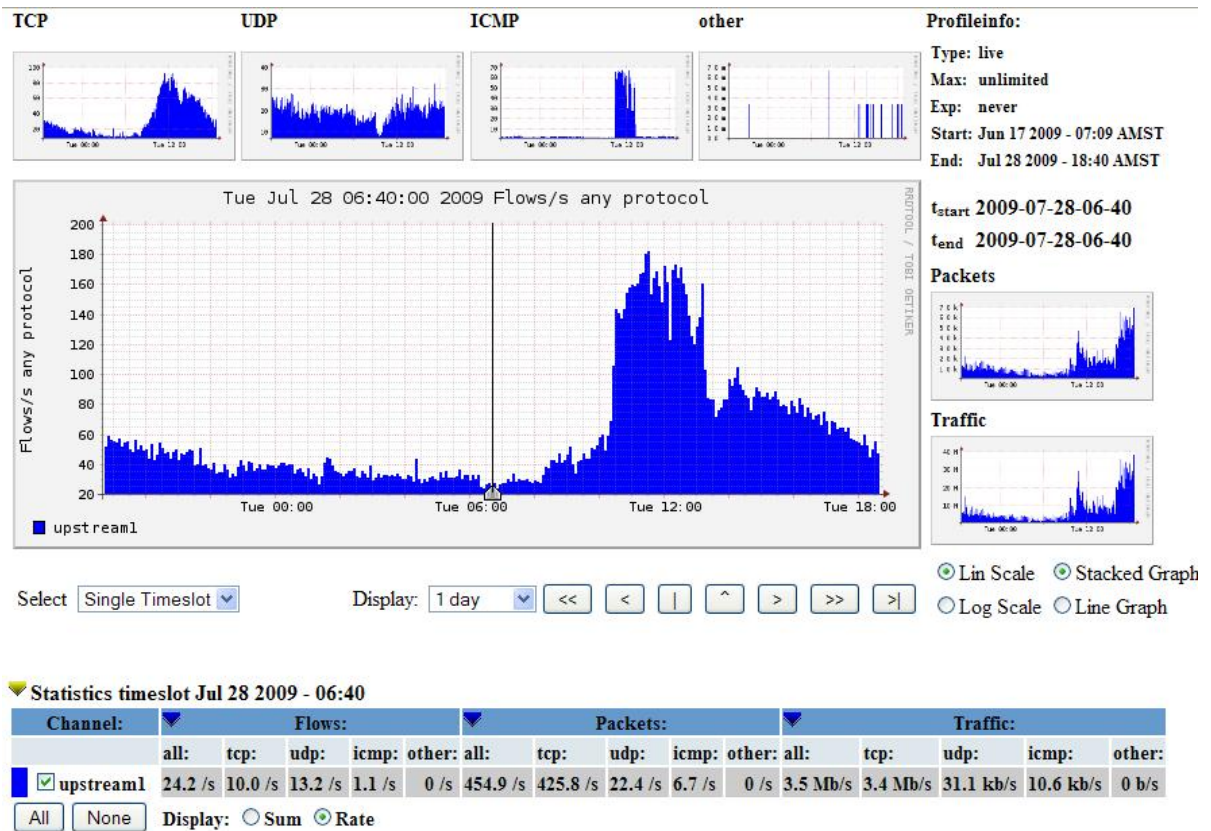


Figure 2 Nfsen tool at NASRA



Figure 3 Classifying traffic characteristic with NfSen

### 4.4.2. Network Usage Monitoring

BSI NOC deployed three different tool to monitor link usage. This well known tools are MRTG, CACTI and Network Weathermap. This tools are selected because of the ease of installation, efficiency and free of charge.

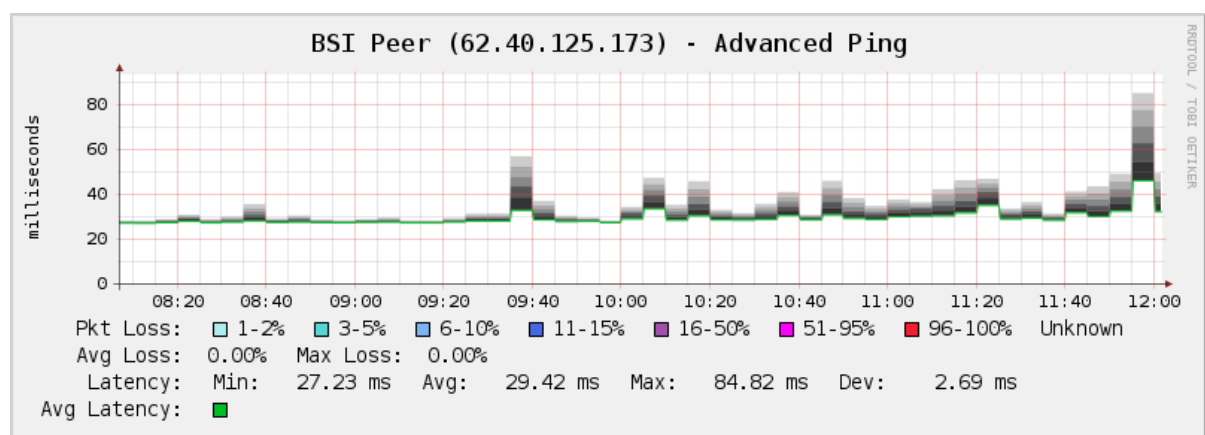


Figure 4 Cacti, Advanced ping between GEANT and GRENA



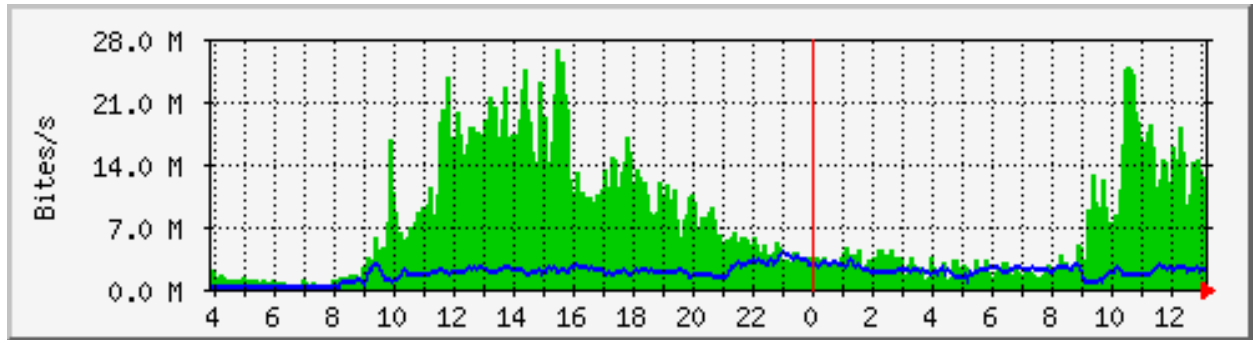


Figure 5 NASRA, Uplink Usage

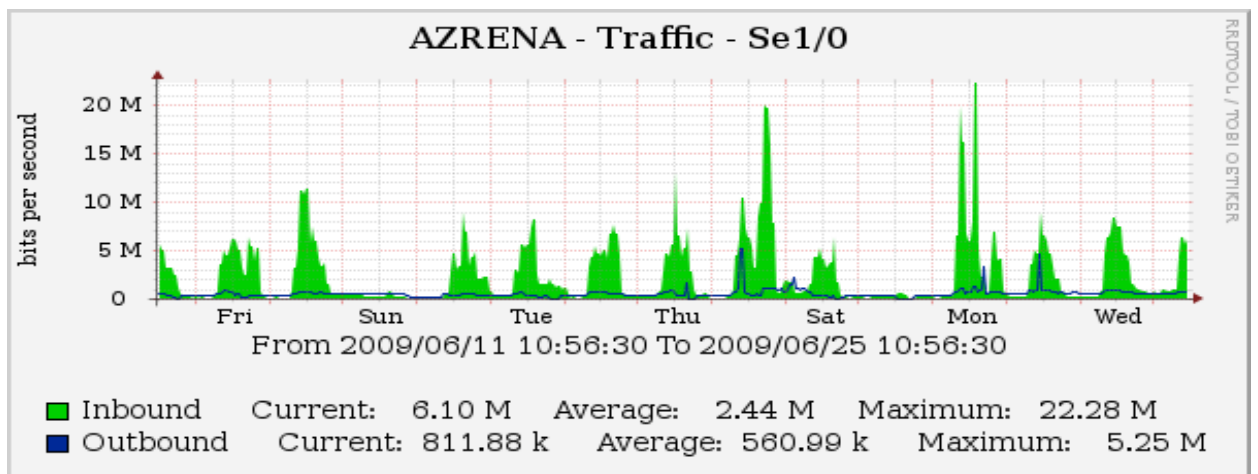


Figure 6 AZRENA, Uplink Usage



Figure 7 Network Weathermap, Link Usage Graph



## **5. Conclusion**

This deliverable, describes management procedures and main software tools to monitor BSI Network. Currently many of these tools deployed to the BSI Network and they will retail in the Deliverable D4.3 Networking Services and Tools Specifications.