1. Introduction
SEEREN is the South Eastern European segment of the multi-gigabit pan-European Research and Education network, GÉANT. SEEREN interconnects the Research and Education Networks of Albania, Bosnia-Herzegovina, Bulgaria, Greece, FYRoM, Hungary, Romania and Serbia-Montenegro. This accomplishment not only interconnects the research communities in the South-Eastern European countries amongst themselves, but also connects them to the existing European backbone network for research and education. The extension makes it much easier for SE European research communities to participate effectively in joint research and educational activities with the rest of Europe.

The SEEREN infrastructure was launched and entered its stable operation on January 2004. This paper briefly presents the Virtual NOC scheme and the Network Management Framework used for managing the SEEREN network.

2. Virtual NOC Framework
The SEEREN Network Operations Center (NOC) is organized in a Virtual NOC (VNOC) scheme. The VNOC scheme implemented in SEEREN, including interactions between NOC entities, is presented in Figure 1.

In the VNOC concept the SEEREN operations and services management are provided by different entities in a distributed paradigm:

- **Network Management Entity (NME):** This is a small group formed by all the SEEREN Access Port Managers (APMs) –one per NREN– that have the administrative control of the overall SEEREN VNOC, guaranteeing proper functioning.
- **HelpDesk:** This entity monitors for connectivity problems and handles the Trouble Tickets System.
- **Services Implementer Entities (SIEs):** These are the entities which design, specify and orchestrate the deployment of advanced services on the SEEREN infrastructure.

- **SEEREN NREN NOCs:** Each NREN has the responsibility of appropriately configuring its access router so as to guarantee proper connection to the SEEREN network.
- **PSC (Project Steering Committee):** It is not considered part of the Virtual NOC, however it interacts with the APMs and it makes decisions on strategic aspects of the project and the deployed services.

The advantage of this framework is that all critical information flows through the NME (centralized aspect to network operations). At the same time distribution is achieved through the SIEs and the SEEREN NOCs. The latter provide network management and user support within their area of authority, while the SIEs are responsible for services implementation on the entire network.

More importantly, knowledge and experience is generated in a distributed way, in the NRENs and in the universities/research centers which demonstrably possess international experience and competence.

![Figure 1: SEEREN Virtual NOC interactions](image-url)
3. Network Management Framework

According to the FCAPS model there are five components (Fault, Configuration, Accounting, Performance and Security management) involved in network management and three components used for service management (Monitoring, Control, Reporting). The SEEREN Network Management Framework covers all components with a combination of open source tools or instruments that are presented in detail in the following section.

Fault management has to do with network problems discovery and correction. Potential problems are identified, and steps are taken to prevent them from occurring or recurring. This way, the network is kept operational and downtime is minimized. Fault management, with regard to detection, is implemented with Nagios and NetIS. The correction of discovered problems is not automatic, but rather follows a path of procedures and communication between NME, SIEs, Helpdesk and the Operator.

Configuration management is responsible for network operation control. Hardware and programming changes, including the addition of new equipment and programs, modification of existing systems and removal of obsolete systems and programs, are coordinated. An inventory of equipment and programs is kept and updated regularly. Configuration management is implemented with CVS/RANCID and Looking Glass. With these tools, it is possible to monitor permanent changes in configuration or its current (temporary) state.

Accounting management is devoted to distributing resources optimally and fairly among network subscribers. This makes the most effective use of the systems available, minimizing the cost of operation. This level is also responsible for ensuring that users are billed appropriately. Resource allocation and billing are not planned in SEEREN.

Performance management is involved with managing the overall performance of the network. Throughput is maximized, bottlenecks and other potential problems are identified. A major part of the effort is to identify which improvements will yield the greatest overall performance enhancement. This type of management will be implemented with a Nagios and NetIS combination. Monitoring will be accomplished not only by the Helpdesk but also by the APMs. The latter will utilize this information to plan future upgrades.

At the Security Management level, the network is protected against offenders, unauthorized users, and physical or electronic sabotage. Confidentiality of users’ information is maintained where necessary or warranted. The security systems also allow network administrators to control what each individual authorized user can (and cannot) do with the network equipment. Security management will be implemented with the deployment of ACLs, the help of CVS (to monitor for changes), and the realization of the SEEREN CERT.

Monitoring of services involves gathering data about the network services. It will be done using Nagios, NetIS and custom software. The following services are monitored: status of interfaces on border routers, status of BGP sessions and the size of the routing table, CPU utilization on routers, MPLS status, status of SEEREN web server, status of SEEREN FTP server, status of SEEREN DNS server, status of NRENs DNS servers, status of web servers at NRENs that provide information about the network (Looking glass pages, NetIS pages, etc).

Control refers to manipulation of devices. No automatic manipulation is planned for the first year of operations; rather, all such intervention will be accomplished by human interaction.

Reporting refers to documenting abnormal events and circulation of these documents. It will be materialized by the Helpdesk and the TTS (Trouble Tickets System). The CERT will also be a part of this component, since it will report about known security issues that have been exploited within the SEEREN network boundaries.

4. Network management instruments

NetIS: The Network Information System (NetIS) is developed by AMREJ and hosted in Belgrade University Computing Center. It is a network information system with integrated monitoring modules and tools. Software is running on a Linux web application server, with a separate SQL data server.

The following tasks can be performed by NetIS: monitor the status of the network nodes, lines and services, traffic accounting and reporting, read-only access to network routers, traffic monitoring for network threats and attacks response.

Software configuration and management is allowed through a special application. User access is Web based. Protected data and login with username and password is also supported, with arbitrary
user/group read/write permissions (e.g., contact information of SEEREN members is publicly accessible, while sensitive technical information is protected and only shared by SEEREN staff).

The software periodically polls network elements, reads the “current status”, and stores the data in a database. Alarms can be assigned to monitors, which alerts (by email) network administrators about events based on the collected data (link status down, not established eBGP session, etc). Monitoring elements of interest in the SEEREN networking environment are:

- Traffic throughput statistics (traditional MRTG graphs)
- Router/switch interface status (up/down)
- SNMP OIDs (variables), such as BGP session status, router CPU load, router memory usage, MPLS status, etc.
- Ping results of arbitrary IP nodes (ping loss, minimum/maximum round trip time).
- Service status by NMAP tool (availability of DNS service, etc).
- Arbitrary looking glass output (“show interface” parameters, etc).

The monitored results are organized in groups and presented as web based table reports. Moreover, network nodes from the database are linked following physical network topology, and can be organized in topology graphs. Combined with the monitors in groups, these graphs work as “weather-map” graphs with web sensitive MRTG statistics.

**RANCID**: It is used for the CVS repository of router configuration. RANCID is installed on the management server and maintained by ISTF. All information provided by RANCID is analyzed and if problems are detected, a trouble ticket is issued.

**Nagios**: Provides the following important features:

- Contact notifications - email, pager, phone
- Ability to define event handlers for service and host events
- Capability to define scheduled downtimes for suppressing host and service alarms
- Web interface for viewing current network status, notification and problem history, log files
- Support for user defined plug-ins to perform service checks
- Hierarchical user authorization for access to the web interface

Special plugins will be developed for MPLS specific actions. Nagios will contact, depending on the nature of the fault, all entities within the VNOC. For example, NRENs border routers availability will be reported to the involved APMs and the Helpdesk, special services failures (like IPv6) will be reported to specific SIEs, MPLS malfunction will be reported to the Helpdesk, etc. The structure of this process will evolve and will be modified to meet the day-to-day needs.
day operation of the network.

Centralized installation of Nagios provides access for NME, APMs and SIEs. Each entity will gain access to monitor, modify and set the status of resources in their area of responsibility such as Downtime, Acknowledge, etc.

Looking Glass: Tools for fast web based (read-only) access to the routers are fundamental for the efficiency of the APMs and SIEs operations. Looking Glass has the following features:

- user level access authorization;
- configuration file viewer;
- interfaces status and parameter viewer;
- IP routing table and/or single IP route viewer;
- routing protocols status viewer;
- simple debugging tools (ping and traceroute);
- router command line interface.

Looking Glass:

Helpdesk and Trouble Ticket System: A distributed HelpDesk based on a web collaboration tool is the most acceptable solution for SEEREN operations. The main task of the Helpdesk will be the operation of Trouble Ticket System that is implemented on open source software.

The SEEREN Helpdesk provides services only to the SEEREN NREN NOCs. Each NOC operates its own HelpDesk for their connected institutions.

RoEduNet has a good experience with Request Tracker, a Trouble Ticket System with the following features:

- Web-based interface with user level authentication;
- Multiple queues support (administrative, technical, etc.);
- Interface for ticket submitting and operation via e-mail;
- Granular user access control (requestor, watcher, admin, owner, etc.);
- SQL database storage system;
- Hierarchical tickets linking system (parent-child relationships);
- Customizable templates for system messages.

CERT: the SEEREN-CERT (Computer Emergency Response Team) responds to incidents within the SEEREN core network. The latter is defined as the border routers and the network monitoring nodes. Incidents within the NREN parties’ boundaries are not addressed by SEEREN-CERT, however cooperation and coordination of activity between SEEREN-CERT and attacked NRENs is envisioned. A DoS/DDoS attack which traverses the SEEREN network to attack a host within the boundaries of a beneficiary NREN is considered as an incident within the joint authority of SEEREN-CERT and the NREN’s management team.

5. Conclusions

SEEREN is expected to upgrade and integrate the Internet services and infrastructure of the National Research and Education Networks of SE Europe, in an attempt to ease the "digital divide" that still separates most of the SEE countries from the rest of the continent. This paper presents the framework used to manage the SEEREN network.

Acknowledgment

The SEEREN initiative is funded by the European Commission under the Information Society Technologies (IST) Programme (IST-2001-38830). The SEEREN project outcome is a mosaic of commitment and tremendous effort by many people. The SEEREN consortium includes: GRNET, (Greece), HUNGARNET/NIIF (Hungary), RoEduNet (Romania), INIMA (Albania), BIHARNET (Bosnia-Herzegovina), ICTDA (Bulgaria), MARNET (FYRoM), AMREJ (Serbia & Montenegro), DANTE, TERENA.

References


Author Biographies:

Dr. Jorge A. Sanchez-Papazipeli received the Dipl.-Ing. and the Dr.-Ing. degrees in Electrical and Computer Engineering from NTUA in 1992 an 1996 respectively and the Master's Certification in Program/Project Management from the Stevens Institute of Technology in 2000. From 1992 to 1995, he was with the Telecoms Laboratory of NTUA and, from 1994 to 1996, with the Institute of Communications Systems and Computers (ICS). From 1996 to 1998 he was a Scientific Consultant to Bell Laboratories, Advanced Communication Technology Center of Excellence in New Jersey and from 1998 to 2000 he was a System Architect in the Forward Looking Work EMEA Dept. of Lucent Technologies in the Netherlands. From January 2001 to July 2002 he supervised the Communications Systems and Technology Group of Bell Labs Advanced Technologies EMEA. He joined GRNET on July 2002 with major responsibility for the development of regional innovation infrastructures. Jorge has served as an expert/consultant for the EC, EICTA, various telecoms companies, and venture capital groups. He is a member of IEEE, FITCE, PMI, TEE. He has received several national and international awards for academic achievement while studying and working in the industry. He has more than 30 articles in worldwide recognized journals and conferences.

Dipl.-Ing. Constantinos Kotsokalis received the Dipl.-Ing. Degree from the Department of Electrical and Computer Engineering, National Technical University of Athens (NTUA), Greece. He has worked for the Network Management Centers of the NTUA and the Athens University of Economics and Business, as well as the Greek Research and Education Network. His areas of expertise include software engineering, computer security, data networking and grid computing.

Dr. Octavian Rusu: Ph.D in Physics, AL.Cuza University Iasi, Romania, March 1999, Specialization: Electronic Physics Manager of RoEduNet Iasi Network Operation Center, 1998 - present. Development and management of Iasi Metropolitan Area Network (MAN); project founded by NATO (co-director of the project NIG 976328 entitled “Consolidation of Romanian Education Network in N-E of Romania. Coauthor for Romanian Education Network project (Wide Area Network with six Network Operation Center and up to 34 Points of Presence) and main author of Iasi Metropolitan Area Network; Main Contact an Instructor for Regional Cisco Networking Academy OAO RoEduNet Iasi: coordination of 11 Local Cisco Networking Academy; Head of Digital Communications Department, AL.Cuza University Iasi, Romania, 1996 - present. Established the development strategy of the digital communications for “AL.Cuza” University. Involved at each layer of designing, building and operation of Universities Campus Network for data and voice communications: 2000 nodes and up to 1000 phones and Internet connectivity; Implementing, management and support of major servers of “AL.Cuza” University. Involved at number of projects including the stable and efficient operation of the University Computer Network and especially in its daily maintenance.

Dr. Hristo Turlakov received his M.Sc. in 1970, Ph.D. in 1981, Associate Professor in 1986. He is the Deputy Head of the Department for Distributed Systems and Networks at the Central Laboratory of Parallel Processing of the Bulgarian Academy of Sciences. He has 35 Publications. He is author and co-author of 10 Books and Manuals. He has 15 Bulgarian patents, 2 USA patents and 1 UK patent.


Goran Muratovski: Education: Bachelor of Science in Electrical Engineering - Computer Science and Control Systems, Graduated at the Faculty of Electrical Engineering in Skopje, 1989. During the last 9 years at the University Computer Center, has been actively participating in all stages of the foundation of the University Computer Network and especially in its daily maintenance including the stable and efficient operation of the University Computer Network by means of implementing proper principles of network design and network equipment configuration and maintenance. With the foundation of the Macedonian Academic and Research Network (MARNet) and the advent of the Internet paradigm in the academic environment he was the chief technical officer responsible for the foundation of the MARNet NOC and implementation of the new technology. This meant doing new network topology design by utilizing contemporary CISCO equipment, planning and implementing routing and switching configurations and migrating the existing DECnet based network to a TCP/IP based one. Day to day tasks also include organizing and implementing network monitoring, security, and implementation of various Internet information services.