FP6 - Research Infrastructures

SEEREN2

South-Eastern European Research & Education Network

Deliverable D13a

SEEREN2 Services and Tools Specification

Author(s): András Kovács (editor), Yannis Mitsos, Constantinos Kotsokalis, Aleksandar Dimeski, Amir Hadžimehmedović, Mihajlo Savic, Neki Frasheri, Pavle Vuletic, Samra Mujačić, Sasa Mrdovic, Slavko Gajin, Vedrin Jeliazkov

Status –Version: Final – h

Date: September 8th, 2006

Distribution - Type: Public – Report

Code: SEEREN2-WP1-HU-001-D13aServicesToolsSpecs-h-2006-09-08.doc

Abstract: Main goal of this document is to support several other WP5 activities by providing state of the art technology reviews on technologies in scope of the project and by giving a detailed report on feasibility studies prepared in the other WP5 activity 5A2. In addition, the document contains evaluation and summary of the results of WP5 services and tools survey completed by all SEEREN2 project partners in March-April of year 2006 in the framework of activity 5A1. The survey intends to help SEEREN2 project to identify deployment status of most important basic and advanced services at each partner's network in order to help further development of the project and support service deployment at partners where they are needed.

The SEEREN2 Consortium consists of:

GRNET	Coordinator	Greece
DANTE	Contractor	United Kingdom
TERENA	Contractor	The Netherlands
NIIF	Contractor	Hungary
RoEduNet	Contractor	Romania
ISTF	Contractor	Bulgaria
UoB/AMREJ	Contractor	Serbia-Montenegro
UKIM/MARnet	Contractor	FYR of Macedonia
ASA/INIMA	Contractor	Albania
UPT	Third Party	Albania
UT	Third Party	Albania
BIHARNET	Contractor	Bosnia-Herzegovina
UoTu	Third Party	Bosnia-Herzegovina
UoBL	Third Party	Bosnia-Herzegovina
UoS	Third Party	Bosnia-Herzegovina
UOM/MREN	Contractor	Serbia-Montenegro

The SEEREN2 initiative is funded by the European Commission under the Framework Programme 6 – Research Infrastructures (Contract #026748).

Document Revision History

Date	Issue	Author/Editor/Contributor	Summary of main changes
April 28, 2006	a	András Kovács	Draft ToC for approval, survey diagrams
May 10, 2006	b	András Kovács	Final ToC, some state of the art descriptions added from feasibility studies
June 1, 2006	c	Vedrin Jeliazkov	Eduroam and perfSONAR updates
June 19, 2006	d	Mihajlo Savic, Amir Hadžimehmedović, András Kovács	Streaming and video on demand update, Voice over IP update
July 14, 2006	e	Neki Frasheri, Pavle Vuletic, András Kovács, Slavko Gajin, Yannis Mitsos, Sasa Mrdovic, Mihajlo Savic	Multicast update, QoS update, NetIIS, IPv6, update on BoD, update on basic user-level services, IPv6 monitoring parameters, introduction
September 1, 2006	f	Aleksandar Dimeski	Security services part added *First version for review by partners*
September 8, 2006	g	Vedrin Jeliazkov, András Kovács	Final version to the Coordinator
September 11, 2006	h	Yannis Mitsos	**Final version to the EC**

Preface

SEEREN2 aims at creating the next generation of the SE European segment of GÉANT, that intends to make leading-edge technologies and services available to the entire Research and Education communities and all scientific sectors without discrimination between users and sites in SE Europe in an attempt to further ease the 'digital divide' that still separates most of the SE European countries from the rest of the continent. The central element of this infrastructure is the SE European R&E backbone network that extends, through the participating National Research and Education Networks (NRENs), to the end-users in all participating countries. With respect to its predecessor, the infrastructure will be substantially enhanced in its performance but more significantly will add a new key item to its fundamental characteristic, the consolidation of the networking and Grid infrastructures, into an eInfrastructure for SE Europe, fully integrated with the pan-European efforts (GÉANT2, EGEE, SEE-GRID, etc). The project involves the NRENs of Albania, Bosnia-Herzegovina, Bulgaria, FYR of Macedonia, Greece, Hungary, Romania, Serbia-Montenegro, as well as TERENA and DANTE.

The main objectives of the SEEREN2 project are to:

1. To continue to assist the incubating and existing NRENs in SE Europe to fully establish themselves and to integrate with related European-wide organisations and initiatives (TERENA, CEENet, e-IRG, EUGridPMA, etc);
2. Create the next generation of the SE European segment of GÉANT, that intends to make leading-edge technologies and services available to the entire SE European R&E community;
3. Provide a significant increase in the network capacity available for communication and experimentation among end users of the research and education community in SE European countries and of the rest of the world;
4. Guarantee the stable operation of the networking infrastructure and interoperability with GÉANT;
5. Ensure that the investment in this resource is effectively exploited with a promotional and training activity involving the distribution of publicity material, presentations at scientific conferences, and other relevant activities that will be undertaken, with an objective to strengthen the human network in the area of eInfrastructures in SE Europe;
6. Increase awareness of IST in SE European non-EU countries and serve as a paradigm for bridging the digital divide in other areas. Provide a platform for cooperation of scientific and educational communities of EU Member States with Associated States and 3rd Countries;
7. Investigate additional sources of funding from the EC, from National funds and international organizations that are actively involved in the SEE region, such as UNESCO, NATO, CEENet, UNDP, WorldBank, USAID.

The expected key results of the project are:

- NRENs requirements collected and analysed;
- Promotional package available;
- Technical and operational requirements analysed;
- Tenders prepared, suppliers selected, connectivity and equipment contracts signed;
- Final SEEREN2 topology determined;
- Operation of the regional networking infrastructure offering GÉANT2 access;
- Management framework in place and stable network operation;
- Services/tools selected;
- SEEREN2 track in YUINFO and sessions at TNC2006/2007 organized;
- training workshops completed;
- Services/tools deployed.

The SEEREN2 project has started its activities on October 2005 and is planned to be completed by the end of March 2008. It is led by Dr. Jorge-A. Sanchez-P. of GRNET. Eleven contractors (GRNET, DANTE, TERENA, NIIFI, RoEduNet, ISTF, UoB/AMREJ, UKIM/MARNET, ASA/INIMA, BIHARNET, UoM/MREN) and five third parties (UPT, UT, UoTuzla, UoBanja Luka, UoSarajevo) participate in the project. The total budget is 3.083.856€. The project is co-funded by the European Commission's Sixth Framework Programme for Research & Technological Development and National budgets of SE European Countries.

The Project issued the following deliverables:

Del. no.	Deliverable name	WP no.	Type	Security	Planned delivery
D01a	SEEREN2 project handbook	WP1	R	CO	1/11/2005
D02a	SEEREN2 portal	WP6	R	PU	1/11/2005
D03a	SEEREN2 promotional package	WP6	R	PU	1/12/2005
D04a	Market analysis and requirements for SEEREN2	WP2	R	PU	1/11/2005
D05a	Networking topology options and implementation approaches	WP2	R	CO	1/11/2005
D06a	Tender evaluation results (connectivity and equipment tender)	WP3	R	PU	1/12/2005
D06b	Tender evaluation results (connect. and equip. tender responses)	WP3	R	PU	1/1/2006
D08	SEEREN2 acceptable use policy	WP1	R	PU	1/1/2006
D09a	Acceptance tests specification and network implementation	WP4	O	CO	1/2/2006
D07a	SEEREN2 topology	WP3	R	PU	1/4/2006
D10a	SEEREN2 sessions in TNC2006	WP6	R, O	PU	1/11/2006
D13a	SEEREN2 services/tools specification	WP5	R	PU	1/11/2006

The Project plans to issue the following deliverables:

Del. no.	Deliverable name	WP no.	Type	Security	Planned delivery
D05b	Networking topology options and implementation approaches	WP2	R	CO	1/10/2006
D09b	Acceptance tests specification and network implementation	WP4	O	CO	1/10/2006
D07b	SEEREN2 topology	WP3	R	PU	1/10/2006
D11a	Periodic reports (1st period progress report)	WP1	R	CO	1/11/2006
D12a	SEEREN2 management framework and VNOC operations	WP4	R	PU	1/11/2006
D04b	Market analysis and requirements for SEEREN2	WP2	R	PU	1/2/2007
D14a	SEEREN2 training workshops	WP6	R, O	PU	1/2/2007
D15a	SEEREN2 services/tools assessment	WP5	R	PU	1/5/2007
D16	SEEREN2 conference track in 2007 in the region	WP6	R, O	PU	1/6/2007
D01b	SEEREN2 project handbook	WP1	R	CO	1/10/2007
D10b	SEEREN2 sessions in TNC2007	WP6	R, O	PU	1/11/2007
D11b	Periodic reports (2st period progress report)	WP1	R	CO	1/11/2007
D12b	SEEREN2 management framework and VNOC operations	WP4	R	PU	1/11/2007
D13b	SEEREN2 services/tools specification	WP5	R	PU	1/11/2007
D14b	SEEREN2 training workshops	WP6	R, O	PU	1/12/2007
D02b	SEEREN2 portal	WP6	R	PU	15/3/2008
D03b	SEEREN2 promotional package	WP6	R	PU	15/3/2008
D15b	SEEREN2 services/tools assessment	WP5	R	PU	15/3/2008
D17	SEEREN2 liaison activities and future plans	WP6	R	PU	15/3/2008
D18	Final report	WP1	R	CO	15/3/2008

Table of contents

List of figures

References

[1] SEEREN2 Consortium, "South-Eastern European Research and Education Network, Annex I-Description of Work", Contract Number I2004-026748, September 2005.

[2] *Eduroam* project website, http://www.eduroam.org

[3] SEEREN2 Consortium, "Service IP Telephony: Feasibility and Deployment Study", February 2006.

[4] SEEREN2 Consortium, "Service Videoconferencing System: Feasibility and Deployment Study", February 2006.

[5] SEEREN2 Consortium, "Service Video Streaming: Feasibility and Deployment Study", February 2006.

[6] SEEREN2 Consortium, "Service Directory Services: Feasibility and Deployment Study", October 2005.

[7] SEEREN2 Consortium, "Service Bandwidth on Demand: Feasibility and Deployment Study", April 2006.

[8] SEEREN2 Consortium, "Service SLA Management: Feasibility and Deployment Study", February 2006.

[9] SEEREN2 Consortium, "Service Trouble Ticket System: Feasibility and Deployment Study", January 2006.

[10] SEEREN Consortium, "South-Eastern European Research and Education Networking, Annex I-Description of Work", Contract Number IST-2001-38830, November 2002.

Executive summary

What is the focus of this deliverable?

The focus of this deliverable is to give a review of the current state of established and emerging technologies, and software tools applicable to network services and management and will evaluate – in addition to the feasibility studies being prepared in activity A5.2 – their usefulness for the SEEREN2 partners. The consortium has already identified a number of key services and tools of special interest for the SEEREN2 community. These include: directory services, multicast support, IP telephony, videoconferencing, video streaming, IPv6, IP multicast, network management, bandwidth on demand, QoS provisioning, network security, etc.

In addition, the document contains evaluation and summary of the results of WP5 services and tools survey completed by all SEEREN2 project partners in March-April of year 2006 in the framework of activity A5.1. The survey intends to help SEEREN2 project to identify deployment status of most important basic and advanced services at each partner's network in order to help further development of the project and support service deployment at partners where they are needed.

This document also gives a review of feasibility studies prepared in WP5 activity A5.2 on the deployment and development of identified tools and services in support of the SEEREN2 community.

What is next in the process to deliver the SEEREN2 results?

1. Deployment of networking services and tools (e.g., Helpdesk, monitoring tools, statistics, etc).
2. Promote the use of SEEREN by informing the appropriate user groups through special events such as organizing workshops, distributing publicity material, delivering presentations at scientific conferences, setting demonstrations in academic events, all aiming at presenting the new opportunities provided by SEEREN. Individual NRENs will carry out complementary promotional activities in their national user communities as well as participate in activities at the European level.
3. Monitoring the operation. Ensure stable operation.
4. Provision of technical support during stable operation.
5. Evaluate the usefulness of emerging technologies in the context of the SEEREN2 project.
6. Execute an evaluation study on the results of the aforementioned task.
7. Definition of the architecture and the interaction between tools and services. Evaluation of the deployed services/tools.
8. Establish relations with organizations that are actively involved in the SEE region, such as UNESCO and NATO, in order to work out common visions towards reducing the "digital divide" in the Region under question, i.e. the information and technological gaps within the region, as well as between the region and European Member States.
9. Look for other possible sources of funding including funds from the EC, EU States national funds dedicated for assisting development in the region and international organizations that are actively involved in the southeast European region, such as UNESCO, NATO, European Investment Bank, WorldBank. Extra funding will be used so as to ensure network's viability beyond the project's lifetime.
10. Disseminate the knowledge gained. Participation in public events. Organise sessions in TNC-2007.
11. Assessment of project results.

What is the deliverable's content?

Chapter 1 introduces the document. Chapter 2 contains a review of the feasibility studies prepared in the framework of WP5 activity A5.2. Chapter 3 presents the state of the art technology reviews on technologies selected by the Consortium and evaluation of services and tools survey completed by SEEREN2 project partners.

1. Introduction

In the course of the SEEREN1 project a number of services and tools have been deployed. The following picture depicts services deployed in the SEEREN1 infrastructure [10]. Those services will need up to a point re-engineering and re-configuration. SEEREN2 will further invest into the deployment of additional services and tools while maintaining in operation the previous ones.

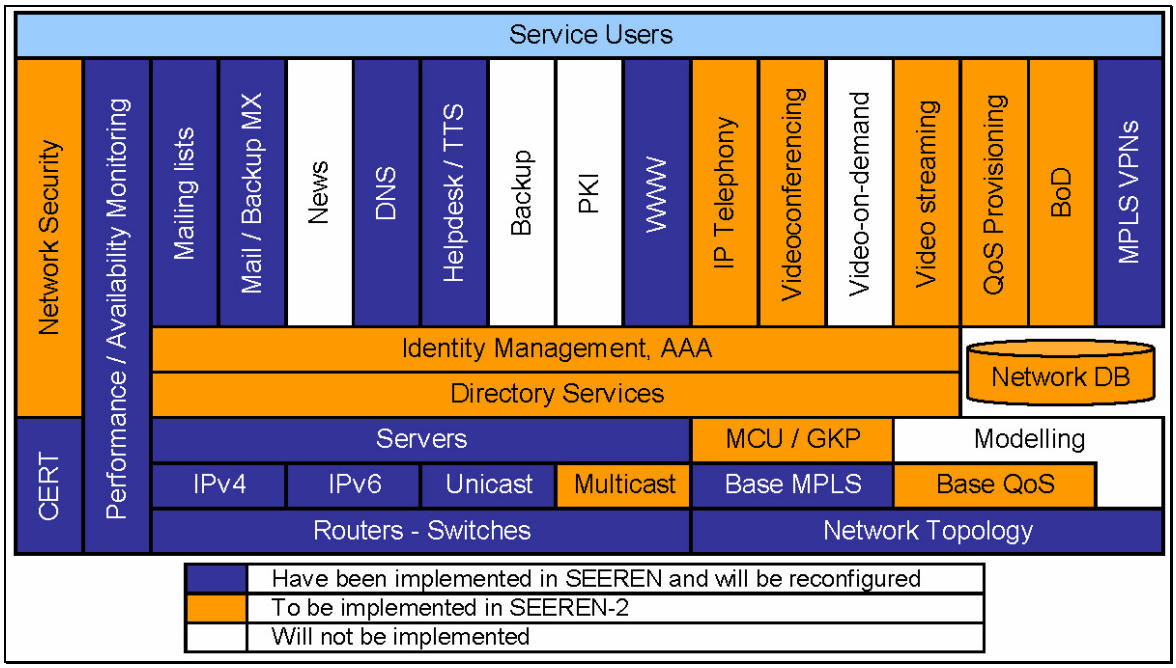

Figure 1: Services and tools structure [1]

Orange coloured set of technologies are the subject of SEEREN2 project and were selected with awareness of other research and education project such as GÉANT2, SEE-GRID and SEEFIRE for example and in order to assure seamless continuation of the first SEEREN project respectively.

This document intends to give a detailed state of the art description of each relevant technology in order to support decision making when selecting appropriate services and tools serving SEEREN2 community in the most optimal way. The state of the art descriptions – together with separate feasibility studies – will help brighten and emphasize all the important aspects of a specific technology field in support of this activity. The main goal of services and tools survey results included in this deliverable is to summarize SEEREN2 partners' general opinions on each element of this service/tool portfolio to provide direct input to service selection discussions taking place in the next few months. A short review of these feasibility studies is also included in the document.

In detail, the following main areas of services are preliminary selected by the SEEREN2 project [1] and will be covered by this deliverable accordingly:

Administrative information: a short survey section was devoted to gather some administrative information on SEEREN2 partner membership and their activity in RIPE NCC.

IPv6 protocol: IPv6 connectivity will be ensured all over the core network. Partner IPv6 connectivity to SEEREN2 backbone will also be provided in order to support partners' users and advanced network services. Several aspects of IPv6 technology and current deployment were surveyed and results will be analyzed in this document.

IP multicast: capabilities will be available over the core network, both for IPv4 and IPv6. This section of the document will introduce multicast technology and present survey results on multicast deployments at partners' networks, most popular multicast applications and interdomain level of traffic exchange.

Quality of Service (QoS): QoS provisioning is an important service for the whole community. Information from current QoS deployments and applications were collected and will be presented.

Bandwidth on Demand (BoD): end-to-end bandwidth on demand refers to the ability of a network user to setup, semi or fully automatically, a path to a destination host with guaranteed maximum bandwidth. Survey on overall need for SEEREN2 BoD services and possible applications will be introduced.

Network management: in network management section several monitoring tools, technologies are described and affected, namely: active/passive monitoring, SLA monitoring, NetIIS and its proposed improvements, IPv6 monitoring applications and most important parameters to be monitored, perfSONAR monitoring tool, unified graphical representation of monitored data, Trouble Ticketing Systems and their usage in partners' management infrastructure.

Security services: Computer Security Incident Response Team (CSIRT), a team of people inspecting and monitoring security incidents will be formed as part of a SEEREN2 activity. Such activities will include handling of DoS/DDoS attacks, unauthorized access to equipment used by SEEREN2 (routers, monitoring servers, other). To support work of SEEREN2 CSIRT group, partners were asked on their local CSIRT groups, and about their preferences in using certain DoS/DDoS protective/preventive tools.

Voice over IP (VoIP) and videoconferencing: beyond the state of the art technology reviews on both technology, survey on partners' needs for VoIP and videoconference services and their opinions about service components to be deployed to support SEEREN2 community will be detailed and analyzed.

Video streaming: it is envisaged that video streaming will be a key technology for the SEEREN2 community in hosting online lectures, seminars and other events, whenever possible. Survey results will cover partner deployments.

Basic user-level services: this section will give a short overview on the availability status of basic user-level services in partners' network such as: web hosting, FTP, mail/mailing list and Network Time Protocol (NTP) services.

Directory services: finally, a technology scope on directory services will be given. Associated survey will give information on current local deployments, on partners' commitment to different directory service architectures and on overall status of *Eduroam* infrastructure deployment in SEEREN2 countries.

2. Report on feasibility studies

The Feasibility Study is a detailed analysis of a preferred facility development strategy as determined in the Technical Annex. It should enable a network to fully determine the outcome which will provide the most cost efficient and effective delivery of its services. The preferred options for developing functions to accommodate service delivery can then be determined.

The Feasibility Study will identify the viable range of options available for the deployment of a specific service if decided to be undertaken. These options should then be evaluated against a set of agreed criteria. The Feasibility Study generally recommends a course of action and a realistic estimate of the total project end cost.

A Feasibility Study comprises the following activities:

- Review of technical annex;
- Functional analysis of determination of functional requirements and relationships;
- Identify viable development options;
- Evaluation of options;
- Cost estimation (if necessary);
- Implementation schedule.

In this context SEEREN2 partners have conducted a number of feasibility studies based on a preliminary decomposition that is available in the respective Description of Work. The available or on-going feasibility studies are listed below:

- End-to-End Bandwidth on demand;
- Trouble Ticketing System;
- Knowledge Base;
- QoS provision;
- IPv6 connectivity;
- IPv4 & IPv6 Multicast;
- IPv6 management;
- Monitoring tools integration:
    - Correlation of active & passive monitoring;
    - Unified graphical representation of monitored data;
- SLA management;
- Computer Security Incident Response Team/DDoS attack prevention and detection;
- IP telephony;
- Video-conferencing;
- Video streaming;
- Directory services;
- Identity management;
- Eduroam;
- perfSONAR.

The outcome if this process has already bore significant results. Some of the aforementioned services have already been deployed. Furthermore, some services that were not included in the original plan have enriched the network's service basket. To mention a few, the consortium has already established synergy with the

perfSONAR development team and currently the measurement archives of the network statistics are available under the umbrella of GN2-JRA1.

Concluding, the following sections provide a seamless integration on some of the outcomes of the feasibility studies along with the results of a questionnaire that was compiled and answered by the consortium.

3. State of the art technology reviews

This chapter is primarily focusing to the state of the art technology reviews. These reviews include a short description of relevant networking technologies, preferred deployment scenarios and promising future solutions which are not yet in production, but will be possibly very important from the aspect of research networking and to be more specific for the whole SEEREN community. Reviews cover elemental administrative services, basic and advanced network services and network management facilities that are crucial from points of research networking service portfolio and network operation and maintenance.

In order to support service selection and deployment planned in the framework of SEEREN2 project a comprehensive survey was prepared and completed by all the project partners inquiring about current deployment status of networking services and technologies at each participating NREN's network and as well as about future plans and needs of each partner.

The web based survey was prepared, hosted and evaluated by NIIF/HUNGARNET with support from other project partners. Topics – also detailed in state of the art reviews - were covered by nearly 70 survey questions on current service deployments, future plans, network management and related software tool usage. This survey was completed by the following project partners:

- AMREJ;
- GRNET;
- INIMA;
- ISTF;
- NIIF/HUNGARNET;
- RoEduNet;
- UKIM/MARNET;
- UnTz;
- UoBL;
- UoM/MREN;
- UoS.

In detail, the survey covered the following major topics:

- Administrative information: elemental administrative services and organizational membership (RIPE membership, LIR service and country level domain delegations);
- IPv6 protocol: IPv6 routing, IPv6 deployment, IPv6 capable equipments, problems of introducing IPv6, etc.;
- IP multicast: IPv4 and IPv6 multicast deployment, related applications and interdomain traffic exchange;
- Quality of Service: QoS deployment, applications and SEEREN2 network requirements;
- Bandwidth on Demand: survey on future services, applications to be used with dynamically allocated bandwidth provisioning technologies and overall partner need for BoD deployment in SEEREN network;
- Network management: active/passive monitoring, data representation, SLA management and related tools, trouble ticketing, NetIIS and perfSONAR software tools, IPv6 monitoring tools;
- Security services: questions related to national and SEEREN level CSIRT services;
- Voice over IP: VoIP deployments, future plans and needs;
- IP based videoconference: videoconference service deployment;
- Streaming and video on demand: streaming and video on demand deployment;

- Basic user-level services: web hosting, FTP, mail and network time services;
- Directory services: directory service deployment and *Eduroam* usage.

3.1. Administrative information

The very first section of the survey was dealing with gathering some administrative information on SEEREN2 partner membership and their activity in RIPE NCC.

3.1.1. RIPE membership

According to this survey question, more than half (58%) of SEEREN2 partners are members of RIPE NCC organization and 42% of them are not yet members.

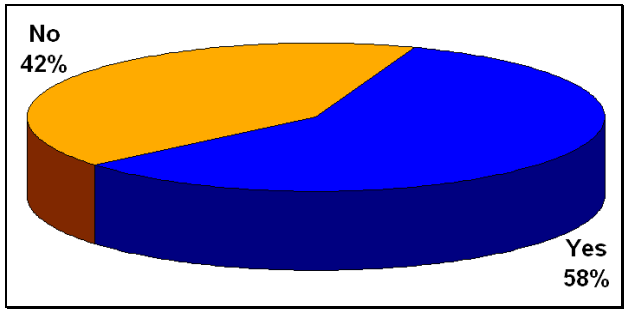

Figure 2: Is your organization a member of RIPE NCC?

3.1.2. Local Internet Registry

Most SEEREN2 partners (50% of all partners), who are members of RIPE NCC operate – 6 out of 7 – as a Local Internet Registry for their constituency. The diagram features the rate of partners that are members of RIPE but do not operate a LIR service.

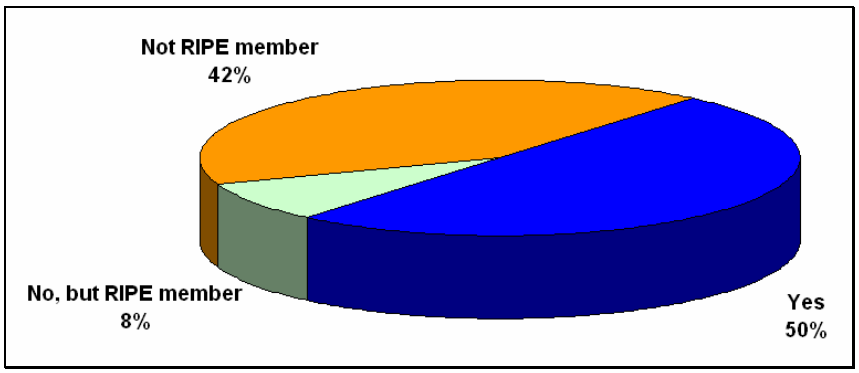

Figure 3: Does your NREN operate a Local Internet Registry (LIR)?

3.1.3. Country level domain delegations

Exactly one third (33%) of all SEEREN2 partners are responsible for country level domain delegation in their countries. The diagram below shows the rate of partners that are RIPE members but do not operate a *country code Top-Level Domain* since being a ccTLD requires RIPE membership.

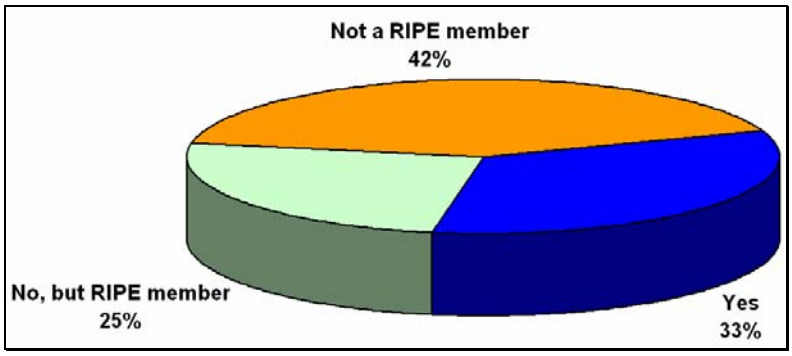

Figure 4: Is your NREN responsible for country level domain delegations?

3.2. The IPv6 protocol

IPv6 was invented to succeed IPv4 as the network layer standard used to address equipment connected to the Internet, allowing for a much larger address space than its predecessor. Even though IPv4 was originally introduced in 1981 (RFC 791), it has not been substantially changed since then. Among the characteristics that made IPv4 being predominately deployed are its robustness, its easy implementation and its interoperability. Nevertheless, the most important reason was that it stood the test of scaling to the size of internet today. However, while IPv4 supports 4.3×10^9 unique addresses, IPv6 can support up to 3.4×10^{38} of them, solving the problem of address exhaust that would normally occur following the trend of new networked devices such as cell phones and PDAs. Techniques such as Network Address Translation (NAT) and Classless Inter-domain Routing (CIDR) were deployed in the past to extend IPv4 lifetime. Those techniques appeared to increase the available address space but failed to meet the requirements of the emerging peer-to-peer applications.

IPv6 was adopted by IETF in 1994 (back then as "Internet Protocol next generation" – IPng), and although its market share is still minimal (mainly slowed down by the introduction of Network Address Translation/NAT, which however breaks the end-to-end nature of the Internet) it is expected that at some point it will be broadly adopted. It is quite certain, however, that it will co-exist with IPv4 for the foreseeable future.

IPv6 technologies for transition from IPv4 but also for allowing IPv6-only hosts and networks to reach other (either IPv6 or IPv4) similar entities over IPv4 networks, have stabilized for quite some time now. We expect that it will be straightforward to implement IPv6 over the SEEREN2 backbone, since all routers with a decently recent operating system support it. It is true, however, that research is still ongoing to develop new services that take advantage of the IPv6 features and resolve problems with currently existing such services. Another challenge for the project will be to deploy IPv6 on a wide basis, within the participating NRENs and the universities.

RFC2460 describes the latest IPv6 specification.

3.2.1. Most important IPv6 features

IPv6 includes a number of improvements over IPv4, the most significant of which are the following:

- Larger address space: This was the initial motivation for the specification of IPv6, as explained earlier in this document. This extension from 32-bit addresses to 128-bit addresses has some interesting repercussions: Large address blocks can be allocated, due to the vast number of available addresses, which leads to smaller routing tables and easier management of the address space; Also, scanning the IPv6 address space for vulnerabilities is much harder than with IPv4, which makes IPv6 more resilient to attacks;
- Stateless autoconfiguration of hosts: When an IPv6-enabled host is connected to a respective network, it issues a broadcast message requesting configuration information. The gateway can then provide a router advertisement with such information included, so that the host is automatically configured. This feature makes renumbering easier and as a result the migration from one ISP to another reduces significantly the network management overheads;
- Multicast is a part of the protocol itself – although IPv6 multicast support at the moment is very limited within most routers. IPv6 does not use broadcast at all. The functions previously supported by

IPv4 (e.g.: router discovery) are directly handled by the protocol itself. IPv6 uses specific multicast group addresses for its various functions. Thus, IPv6 multicast prevents the problems caused by broadcast storms in IPv4 enabled networks;

- Jumbograms: IPv6 includes support for packets larger than 64 Kb, when the link layer supports this option. Such packets are called jumbograms and can improve performance significantly over high-throughput links;
- IPsec: Although not widely deployed at the moment as a feature, IPsec is natively supported by IPv6 and it is part of the protocol suite. IPv6 provides security extension headers, making easier the implementation of encryption and authentication. On top of this, end-to-end security services can be provided omitting the need of additional hardware machines that typically introduce additional administrative overheads and performance bottlenecks;
- Last but not least even though QoS in IPv6 is handled the same way as it is currently handled in IPv4 a new field in its header enables QoS devices in the path to take appropriate actions based on this label.

3.2.2. IPv6 transition mechanisms

There are three main mechanisms for the transition from IPv4 to IPv6. This does not necessarily require a host to support IPv6 only. As a matter of fact, all IPv6-enabled hosts currently support both versions of the protocol, either with a single IPv4+IPv6 stack, or (experimentally) with two distinct stacks.

- **Dual stack:** This approach is fully described in RFC4213. Hosts can interoperate natively with either IPv4 or IPv6 peers, using respective packets. The latter case does depend on IPv6 being deployed on the capabilities of the network in between, especially when the hosts are in different LANs. In the case of dual stack hosts, and as long as both versions of the protocol are enabled, the host is assigned one address for each protocol on each connected NIC. Assignment of addresses can take place either statically or dynamically/automatically with DHCP (for IPv4) and stateless autoconfiguration or DHCPv6 (for IPv6);
- **Tunnelling:** There are two different methods defined for tunnelling, *automatic* and *configured*. Essentially, tunnelling is about encapsulating IPv6 packets in IPv4 packets, thus using IPv4 as a link layer for IPv6. Generic encapsulation schemes such as GRE may be used, while there is also the option of encapsulation within IPv4 with a protocol number equal to 41, or even encapsulation within UDP packets;
    - **Automatic tunnelling:** In this case, the tunnel endpoints are automatically decided by routing infrastructure. The recommended technique for this approach known by the name "*6to4"* and is defined in RFC3056. In this case, encapsulation using protocol number 41 is taking place. In practice, it is method for assigning an interim unique IPv6 address prefix to any site that currently has at least one globally unique IPv4 address, and a specification of the encapsulation for transmitting IPv6 packets using such a prefix over the global IPv4 network;
    - **Configured tunnelling:** Configured tunnelling is specified in RFC4213. In this case, tunnels are specified explicitly, either by a human operator or by a *tunnel broker* service. Due to the more deterministic nature of this approach, debugging is quite easier when problems come up, especially in larger networks;

  RFC3904 states:

  > *Configured tunnels have many advantages over automatic tunnels. The client is explicitly identified and can obtain a stable IPv6 address. The service provider is also well identified and can be held responsible for the quality of the service. It is possible to route multicast packets over the established tunnel. There is a clear address delegation path, which enables easy support for reverse DNS lookups.*
  >
  > *Automatic tunnels generally cannot provide the same level of service. The IPv6 address is only as stable as the underlying IPv4 address, the quality of service depends on relays operated by third parties, there is typically no support for multicast, and there is often no easy way to support reverse DNS lookups (although some workarounds are probably possible). However, automatic tunnels have other advantages. They are obviously easier to configure, since there is no need for an explicit relation with a tunnel service. They may also be more efficient in some cases, as they allow for "path optimization".*

- **Proxying and translation:** This approach refers to the need to access an IPv4-only service from an IPv6-only host. In this case, a translation mechanism is needed. Low-level (application-agnostic) methods have been proposed but have been found to be unreliable due to the wide range of functionality required by common application-layer protocols. Thus, the recommended approach is to use application-layer proxies, which perform this translation between the two ends;

3.2.3. IPv6 deployment

IPv6 deployment in the first phase of SEEREN was important and is reflected in the following chart. Although a completely different technology was used back then in order to support the Carrier-over-Carrier technique, the know-how achieved provided significant help for the immediate support of IPv6 in a part of the currently existing backbone of SEEREN2. Later deployment refers mostly to sites that remain to be connected as well as the internal part of participating NRENs.

According to experts studies, IPv6 should be initially deployed at the edges first and then move towards the network core to reduce the cost and operational impacts of the integration. The key strategy used in deploying IPv6 at the edge of a network involve carrying IPv6 traffic over IPv4, allowing isolated domains to communicate between them before the full transition to a native IPv6 enabled backbone. In this context, SEEREN2 will explore the potential to propagate IPv6 usage in each beneficiary NREN edge that is capable of supporting it in their access nodes.

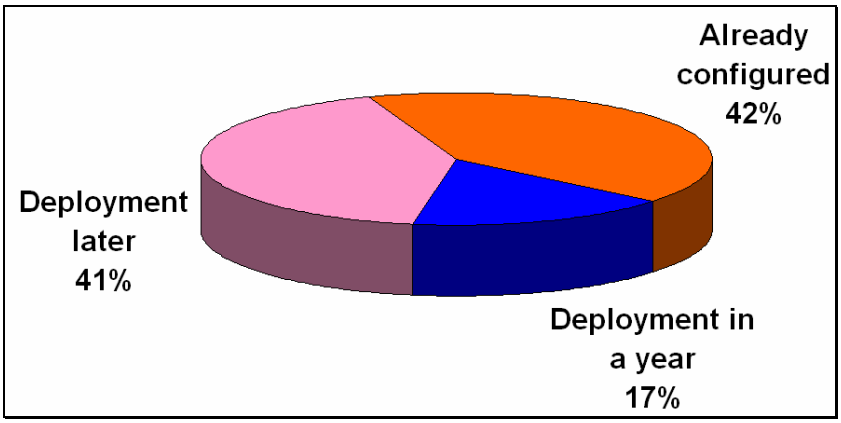

Figure 5: IPv6 deployment and plans to deploy

3.2.4. IPv6 IGP protocol usage

For the sites that have deployed IPv6 internally, IS-IS (*Intermediate System to Intermediate System*) is the protocol of choice, followed by RIPng and then OSPFv3. The popularity of IS-IS for IPv6 has to do with its protocol neutrality, whereas RIP and OSPF (largely popular with IPv4) were built exactly with IPv4 in mind. Because of that, IS-IS fits the IPv6 purpose much better.

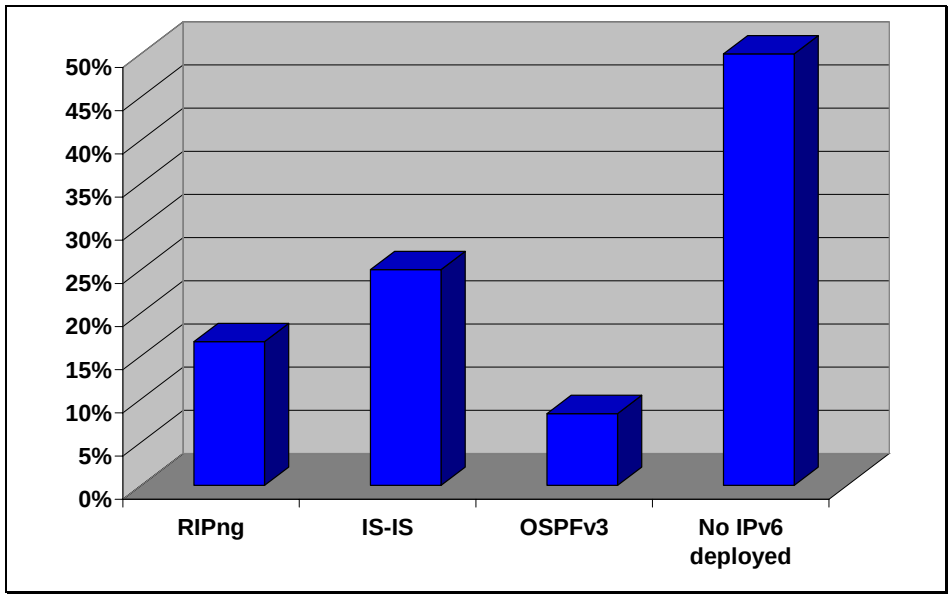

Figure 6: What IPv4 IGP protocols are used in your network?

3.2.5. Fraction of network equipment supporting IPv6

This chart indicates that a large percentage of the networking equipment used within the SEEREN2 partner networks is older and does not support IPv6, which may be a problem in the phase of wide deployment within the NRENs and the universities. The SEEREN2 consortium is making a constant effort to keep an active link to the industry and explore any donation opportunities.

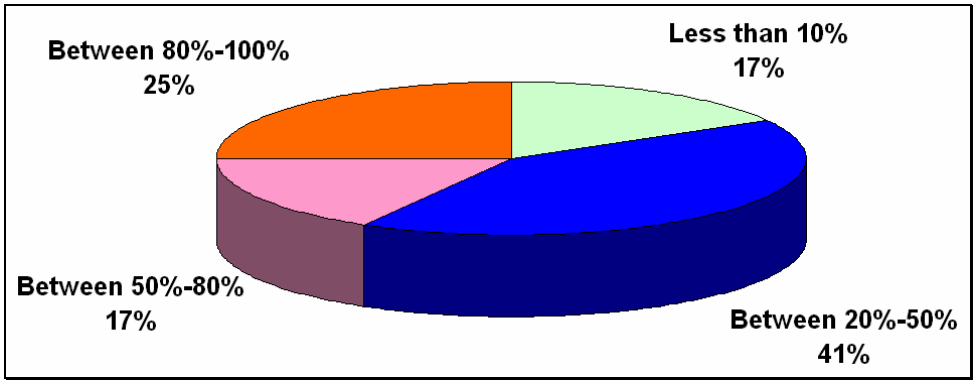

Figure 7: Fraction of network equipment supporting IPv6 protocol

3.2.6. Challenging problems of introducing IPv6 protocol

This chart provides very interesting insight to the reasons why IPv6 might have problems being widely deployed. One can easily realize that three of the four more important reasons are not technical. Rather, they have to do with the lack of IPv6-enabled applications and the poor content reachable over IPv6, which results to lack of interest from the customers. SEEREN partners should advertise the IPv6 benefits and capitalize on a view to future trends, with more and more portable and/or non-computing devices joining the Internet for various reasons. The lack of IPv6 know-how is something to be addressed by the SEEREN2 consortium, through the production of material and the organization of seminars.

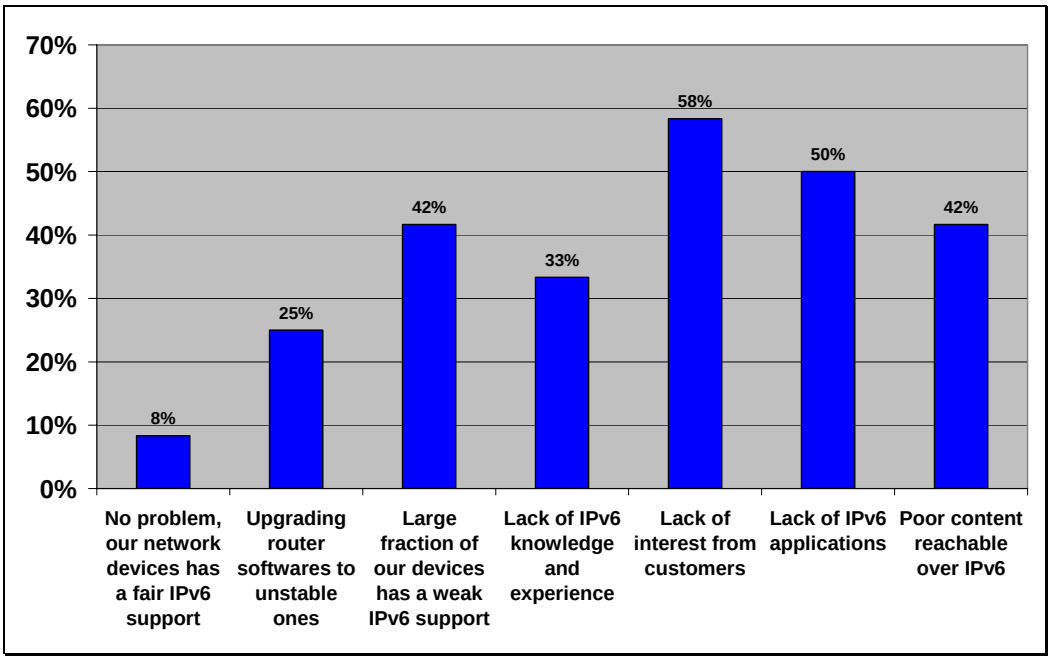

Figure 8: What do you think which are the most challenging problems of introducing the IPv6 protocol?

3.2.7. Need for international IPv6 peering through SEEREN2 network

The chart indicates that although the wide majority of the partners want to have IPv6 connectivity, the largest part still does not have IPv6 enabled internally in order to use international IPv6 facilities. As mentioned earlier, IPv6 is already deployed on the backbone network to a large extent, and it is the intention of the SEEREN2 consortium to deploy it on each backbone link.

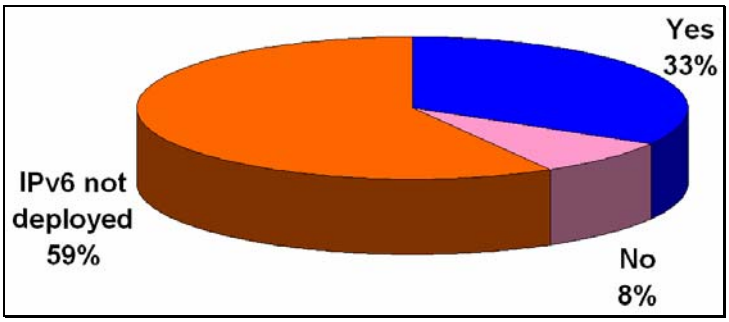

Figure 9: Does your network need international IPv6 peering through the SEEREN2 network?

3.3. IP multicast

IP based multicast traffic transportation have always been considered as a key technology for preserving network bandwidth when audio and video based real time services are provisioned. Unfortunately, multicast technology have never become a breakthrough mainly because of the lack of so called “killer application” suitable for commercial service deployment. In addition, IP based multicast needs efficient and stable support from network equipment: IGMP (IPv4) and MLD (IPv6) protocols for group management, multicast routing protocols (PIM-SM, MSDP and MBGP mainly); special knowledge from network administrators and special applications for management and monitoring of a multicast capable network.

Most popular applications of IP multicast:

- Videoconferencing: multicast technology is not used in standard H.323 or SIP based videoconferencing. However, there are proprietary computer applications providing good videoconference capabilities (e.g. vic, rat, etc.);
- Streaming broadcast: main area of multicast service usage. Most streaming servers support multicast technology;
- IP television.

IP multicast technology is based on the idea of so called groups wherein receivers and sources are located. Any data packet sent by any group members is delivered to all the other group members regardless of their location where they are connected to the Internet. An Internet multicast group is identified by a multicast address assigned at the time of group creation. Below table summarizes both IPv4 and IPv6 multicast address spaces and some of the most important functional sub domains:

Multicast address space	Sub address space	Description
224.0.0.0/4		IPv4 multicast address space
	224.0.0.0/24	Local scope, reserved for well-known multicast addresses (e.g. "All-OSPF-routers).
	224.0.1.0-238.255.255.255	Global scope addresses, can be used between organizations across the Internet
	239.0.0.0-239.255.255.255	Local scope addresses to be used inside an organization (e.g. inside an AS, campus network, etc.)
FFxy::/16		IPv6 multicast address space
		x (flags, 4 bit) = permanent/temporal group address y (scope, 4 bit) = local, organizational or global scope group address The remaining 112 bits represent an IPv6 multicast group.

When forming a multicast group, allocation strategies should be followed in order to avoid collision of group addresses both in case of local scope and global scope addresses. However, colliding with a global multicast group is considered as more harmful than with a local scope group as the latter one remains a local scope problem. These collision avoidance techniques include for example the SAP protocol to receive announced multicast sessions worldwide, autonomous system (AS) based group address allocation and Source Specific Multicast (SSM).

In case of IPv4 the IGMP (Internet Group Management Protocol) is used for group management and MLD (Multicast Listener Discovery) for IPv6. Group management protocols work between endpoints located on a LAN network and their local multicast capable router in order to join, leave and maintain group membership.

After a source/receiver connected to a specific multicast group a new branch of distribution tree must be built along the network path to the closest router distributing the traffic of this particular group. This task is done by multicast routing protocols inside a single authority (intradomain). There are many such intradomain routing protocols that can accomplish this, but most of them are deprecated (e.g. DVMRP, MOSPF, etc.) or very rarely used (e.g. PIM-DM). The single multicast protocol that lived through and still is widely deployed is the Protocol Independent Multicast – Sparse Mode (PIM-SM) multicast routing protocol, which uses exclusively the content of the unicast forwarding table regardless of the underlying unicast routing protocol that constructed it. PIM-SM uses Reverse Path Forwarding (RPF) checks against the unicast routing table in order to verify whether a multicast packet is arriving on the correct interface from the direction of multicast source or RP (see below).

PIM-SM protocol is designed on the assumption that the multicast group members are sparsely distributed throughout the network. By default, PIM-SM uses shared distribution trees (only a single tree per group is built, and all the traffic is forwarded down along this tree from the source to the receivers) routed at a selected multicast router, called Rendezvous Point (RP). When a new branch of the distribution tree is being built, the particular multicast router (i.e. managing endpoint by IGMP or MLD protocols, see above) sends multicast traffic to the RP encapsulated in unicast packets. While the RP is receiving this traffic and forwarding it down to the shared tree, it starts creating a shared tree branch towards the multicast router intending to join. After the new tree segment is ready, traffic is carried along from/to the new member. However, PIM-SM protocol is also

able to use source based trees (one tree per source of a group) and moreover switch dynamically between shared and source based trees.

PIM-SM protocol version 1 was designed in 1995, but was never standardized by IETF. Version 2 was specified in 1997, in RFC 2117 and updated in 1998 (RFC 2362). PIM-SM is widely deployed and used in provider and organizational networks; it's proved to be efficient and scalable.

PIM-SM protocol works on the intradomain level, so additional building blocks are needed when exchanging multicast traffic on the interdomain level. There are two major problems with extending PIM-SM to the interdomain level:

- RP sharing: a router of a specific provider acting as an RP cannot be used as an RP of a different authority (e.g. a different AS), as aspects of resource sharing is complicated in terms of maintenance, accounting and policy;
- RP only knows about sources/receivers in its domain and it does not have any information from other domains.

In order to let RPs located in different domains to communicate an additional protocol was specified, called MSDP (Multicast Source Discovery Protocol). MSDP protocol is able to support extending of distribution trees between PIM-SM RPs located in different domains by exchanging multicast group and source information between domains.

IPv6 multicast technology is also available and ready to use. However, it's much less mature than its IPv4 brother. For IPv6 intradomain routing PIM-SM multicast routing protocol is used as well as for IPv4. In case of IPv6 MSDP hasn't been yet specified due to the fact that MDSP is considered as an unscalable protocol. At this moment, only source specific multicast or embedded RP address in IPv6 address can be used for interdomain communication. It's also very important to note, that most network equipment implementations are still lacking IPv6 multicast feature as a whole or just support it in a rather limited (e.g. MPLS VPNs, MLD snooping, etc.) or an inefficient way (i.e. software forwarding).

3.3.1. Type of multicast service deployed in partners' network

Exactly half of SEEREN2 partners have already deployed IPv4 based multicast services, a quarter of them is planning to introduce. On the IPv6 side, only 17% of partner networks are provisioning IPv6 to their users, none of the others are planning to introduce such a service. 25% of partners are not interested in deploying any kind of multicast service.

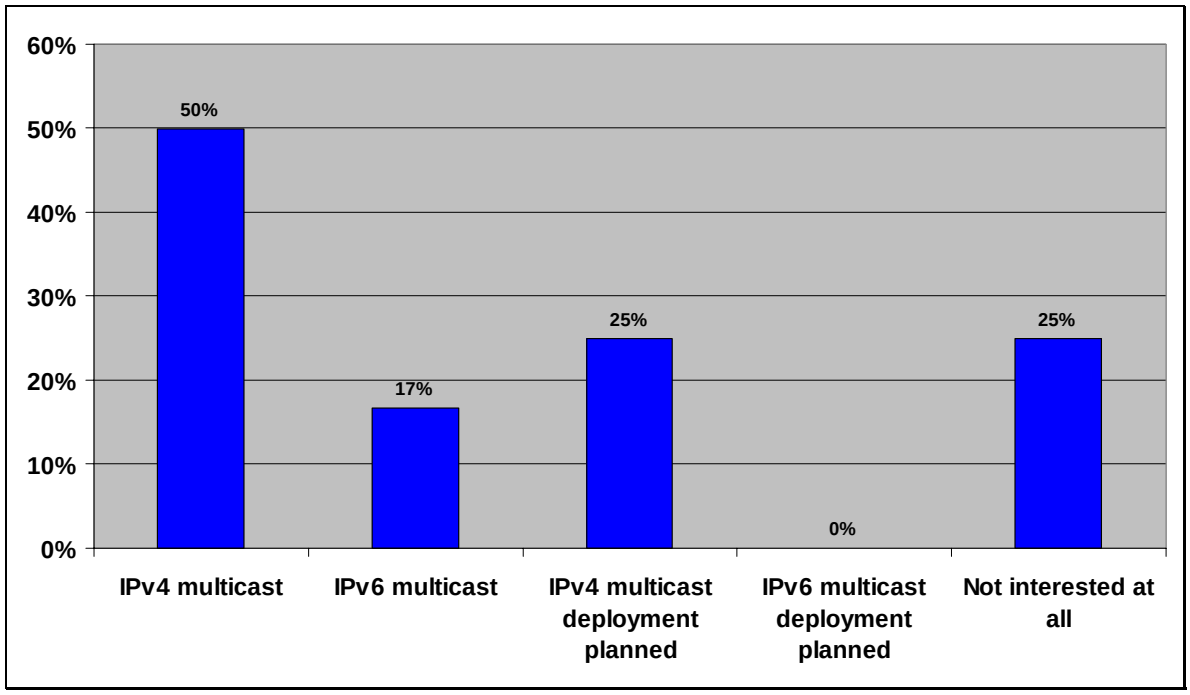

Figure 10: Multicast service deployment and plans

3.3.2. IP multicast application usage

As it was mentioned in the introduction, IP based multicast technology misses a real "killer application" that would offer value added services to the end users. According to current practices in research and education networks, most popular multicast applications are the well known MBONE tools for conferencing and collaboration and multicast streaming for watching multicast enabled internet broadcasts.

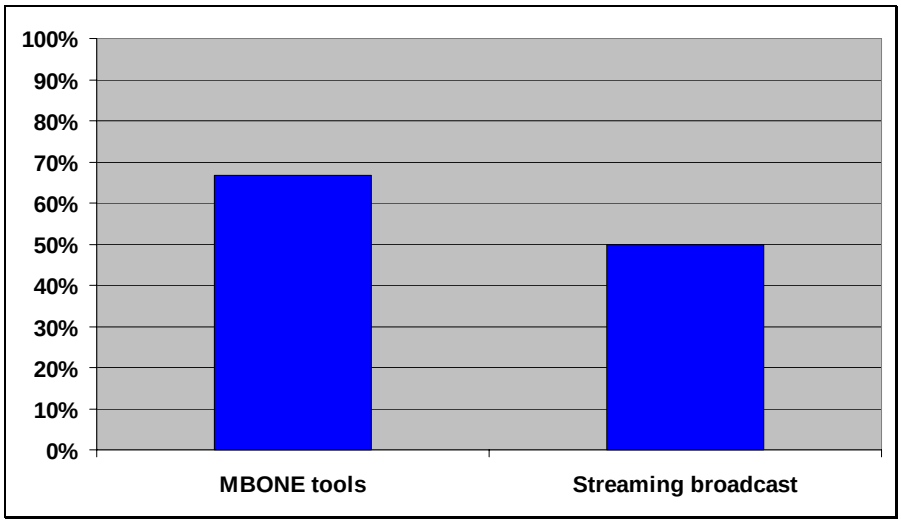

Figure 11: What are the main applications of IP based multicast in your network?

66% of partners are using the MBONE tools intensively (vic, rat, wb, sd, etc.), obviously including VRVS and Access Grid video and audio conferencing. The same number of partners also indicated that multicast streaming is a very important service among their users. Although it was possible to name other applications, none of the partners provided different applications from MBONE tools and streaming.

3.3.3. IP multicast interdomain traffic exchange

In the IP multicast world it is very common that a single administrative domain has a multicast enabled network, and it is particularly true for research and education networks. However, exchanging multicast traffic between two separate providers on the interdomain level is somewhat rare. Intention of this question is to have a general idea on the proportion of SEEREN2 partners having interdomain multicast peerings with other providers.

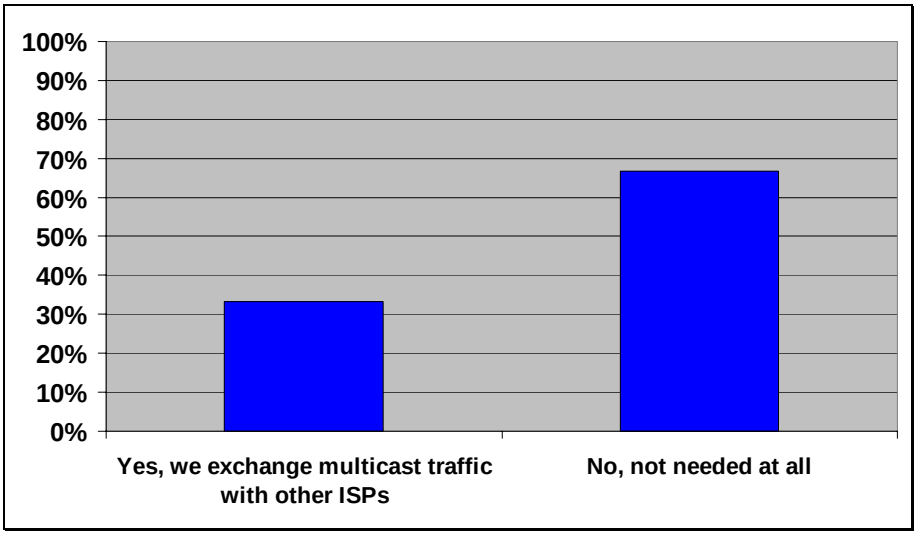

Figure 12: Portion of partners exchanging interdomain multicast traffic

Only 33% (in this case, only two partners) of multicast enabled partner networks are exchanging multicast based interdomain traffic with other providers, both with its NREN peers and ISPs. The rest of partners (66%) doesn't even interested in establishing such peerings.

3.4. Quality of Service

Quality of service (QoS) is a set of techniques which aim to support traffic types with very different service requirements (data traffic with different priorities, voice, video) in a single network, through traffic differentiation and network resource usage control. QoS is usually used on congested links on which high priority or real-time traffic (voice, video) might suffer from other competing traffic flows. However, even on high capacity uncongested links QoS techniques might be useful either as a way to ensure that some traffic parameters (delay, jitter) are kept within limits that are defined by standards for the type of traffic (for example, ITU-T G.114 recommendation for voice traffic), or as a tool to suppress different kinds of Denial of Service (DoS) attacks.

QoS mechanisms and features are present in different types of equipment from different vendors and can be used in all parts of the network, either as a technique to improve network responsiveness on some links, or as an end-to-end solution. With the emerging convergence of different traffic types over single network infrastructure end-to-end QoS architecture based on Differentiated services architecture becomes the architecture which can ensure satisfying QoS for all types of traffic.

This section presents a brief description of various QoS techniques and architectures, a survey of some practices from European networks and recommendations for its use in SEE countries. The wide range of different circuit capacities makes reasonable QoS deployment in SEEREN2 and associated NRENs quite a challenge.

Packet classifying and marking

The first phase in any QoS deployment is defining and classifying different types of traffic in a network. Main engineering task is to recognize traffic types which require different services from the network, and to define those services in terms of main performance measures (delay, jitter, packet loss, and required bandwidth).

Packet classifying and marking usually happens at network's access in end-to-end QoS solution, and in that case it is done in access switches or routers, though it is possible to have packet marking in only one part of the network, not necessarily in network access. Mechanisms that are used for packet marking are setting 802.1p fields in 802.1q tag, at OSI layer 2 on trunk links, or IP precedence or DSCP fields in IP header at OSI Layer 3. The use of different marking techniques depends on the type of traffic and the available networking equipment. It is possible to switch from one marking scheme to another (for example at one point in network to have translation from 802.1p to DSCP or vice versa). It is of the utmost importance to plan well the marking scheme and to keep it consistent throughout the network.

Traffic rate measurement

Traffic rate measurement techniques are used in routers or Layer 3 switches for the measurement of the compliance of the traffic to the QoS parameters that are defined for that type of traffic defined in the previous phase. Leaky bucket or Token bucket algorithms are used for traffic measurement. Traffic that is compliant with the QoS parameters is usually untouched, while noncompliant traffic is either dropped, delayed or marked in a way which shows the non-compliance (for example, changed, or marked down DSCP value).

Resource allocation

Resource allocation is done through different queuing mechanisms which are described in this section.

FIFO Queuing: default behaviour of routers; effective when there is sufficient transmission capacity and queue depth remains short, when queues became fully populated all subsequent packets are discarded and all services degenerate.

Priority Queuing: certain types of traffic can be identified and pushed to the front of the queue and transmitted ahead of other traffic, having adverse impact on processor load, leading to buffer starvation and dropping of normal traffic when high priority traffic is unusually high; not well scalable.

Class Based Queuing (CBS): several output queues are defined together with their preference and the amount of queued traffic to be drained from the queue on each pass of servicing rotation; with computational overhead of intensive queue management, not well scalable.

Weighted Fair Queuing (WFQ): gives low-volume traffic flows preferential treatment and allowing higher volume traffic flows to obtain equity in the remaining amount of queuing capacity, preventing the latter from consuming the bandwidth; with computational overhead, not well scalable.

Congestion avoidance and Packet Drop Policy

Congestion avoidance and packet drop policy techniques are used to avoid the problem of global synchronization in TCP streams in case of FIFO tail drops on congested links. Techniques which are used are RED and WRED.

Random Early Detection (RED) monitors the queue depth and when it begins to fill it randomly select individual TCP flows from which to drop packets, signalling flow senders to slow down. More queue fills, more flows are selected for packet drops and signalled to slow down avoiding the congestion. The threshold is configurable. RED may be combined with precedence mechanisms, lower the precedence higher the probability of dropping the packet (Weighted RED).

QoS and Routing

Mechanisms within both interior (intra-domain) and exterior (inter-domain) routing protocols can provide the capability to prefer one particular path over another, being an important tool in implementing policy, end the latter is a critical tool to implement a QoS strategy.

RIP - the administrator may artificially increase the hop count in any node of the network to control path-selection processes.

OSPF - a cost is assigned to each link and OSPF selects the least-cost path. The administrator may alternatively cost each path differently to control path-selection processes.

BGP - the de facto method for inter-domain routing in the Internet. There are several methods for influencing the BGP path selection process via manipulation of BGP protocol attributes, each of which has topological significance:

- Filtering based on the AS path attributes: filtering of routes for certain prefixes (accepting or not and propagating or not a specific route);
- AS path prepend: when comparing two advertisements of the same prefix but with differing AS paths, by default BGP prefers the shortest path (with smallest number of transit AS hops), and it is possible to influence it by inserting additional instances of the originating AS into the beginning of the AS path prior to announce the route to an exterior neighbour, used commonly as a mechanism of defining candidate backup paths;
- BGP communities: an AS may classify its downstream peers into different BGP communities and apply differentiated policies for different communities; it is very flexible tool that extends beyond manipulation of the default forwarding behaviour into an extended set of actions that can modify any of actions undertaken by the router;
- Local preference (IBGP): designation within an AS of preferences for its gateways; it is local and not propagated to neighbouring ASs; border routers propagate within the AS local preferences towards their internal peers, so internal routers may select a particular path to reach the exit gateway in the border of the AS;
- Multi-exit discriminator (MED): similar with local preference, but MED attribute is used to tell neighbouring AS how to return traffic across a preferred inbound link; it is propagated only to neighbours, used when multiple links are between the two ASs with the same length prefix.

QoS Architectures

This section introduces IntServ and DiffServ quality of service architectures that are currently being used for QoS provisioning.

Integrated services architecture

In Integrated Services architecture (IntServ) the application requests a specific kind of service from the network before it sends data. The request is made by explicit signalling. The application informs the network of its traffic profile and requests a particular kind of service that can encompass its bandwidth and delay requirements. The application is expected to send data only after it gets a confirmation from the network. It is also expected to send data that lies within its described traffic profile.

The network performs admission control, based on information from the application and available network resources. It also commits to meet the QoS requirements of the application as long as the traffic remains within the profile specifications. The network fulfils its commitment by maintaining a per-flow state and then performing packet classification, policing, and intelligent queuing based on that state.

The IntServ model allows applications to make use of the IETF Resource Reservation Protocol (RSVP)**,** which can be used by applications to signal their QoS requirements to the router. RSVP protocol is a signalling service with QoS control information as the signal content. RSVP requires the receiver responsible for requesting specific QoS service instead of sender. RSVP sender sends path messages to RSVP receiver, path messages store path information in each node for specified flow as indicated in sender's Traffic Specification (TSpec), RSVP receiver sends back reservation request (Resq) to the sender along the same path, Resq message specifies desired QoS and set up reservation state in each path's node. RSVP requests only unidirectional resources, for applications acting as sender and receiver sending and receiving are treated as logically distinct functions.

Routers, in conjunction with RSVP, are able to use intelligent queuing mechanisms to provide two types of services:

- **Guaranteed Rate Service** – provides guaranteed bandwidth and delay bound. The guaranteed service framework asserts that queuing delay is a function of token-bucket depth and data rate application requires, and controls the maximum queuing delay; the application controls these values and has a-priori knowledge of queuing delay. The application invokes the guarantee service by specifying TSpec

and Receiver by requesting desired service level RSpec. RSpec consists of data rate and slack term, with data rate greater or equal to token-bucket rate. Every node calculates two error terms: cumulative delay and per-element delay, end-to-end total errors represent flow's deviation from the 'fluid model' ('fluid model' supposes that flows within available total service model can operate independently);

- **Controlled Load Service** – attempts to provide end-to-end traffic within the same bounds as unloaded network in the same situation. Application provides the network with an estimation of the traffic it will generate - TSpec. If requested resources fall outside of what is available, application may experience negligible delayed or dropped packets.

Main problem with IntServ architecture is its scalability. Keeping per flow state in each router inside the network is a problem with many applications and different flows requesting different QoS mechanisms. Furthermore, IntServ architecture requires QoS aware applications. All these lead to relatively low implementation of RSVP as architecture of choice for QoS deployment.

Differentiated services

The Differentiated Services or DiffServ architecture is standard from the IETF. This architecture specifies that each packet is classified upon entry into the network. The classification is carried in the IP packet header, using either the IP precedence or the preferred Differential Services Code Point (DSCP). These are represented using the first three or six bits of the Type of Service (ToS) field. Classification can also be carried in the Layer 2 frame in the form of the 802.1p field embodied in 802.1Q frames.

Once packets are classified at the edge by access layer switches or by border routers, the network uses the classification to determine how the traffic should be queued, shaped, and policed. Unlike the IntServ model, DiffServ does not require network applications be QoS aware. Also, routers inside the network do not have to maintain per-flow state for each flow requesting QoS as in IntServ model. These are crucial arguments for the deployment of the DiffServ architecture in the network.

3.4.1. Quality of Service deployment

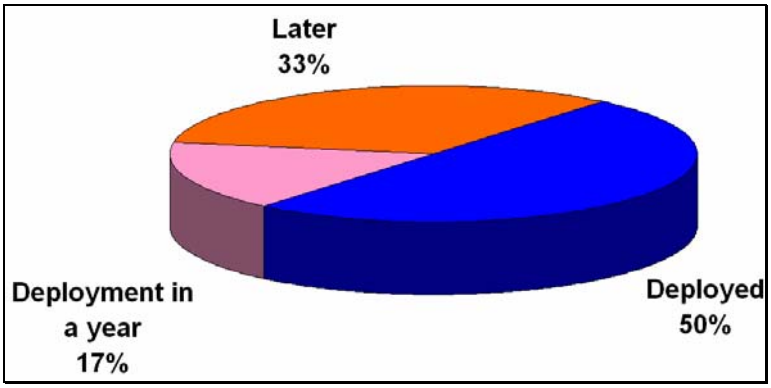

Figure 13: Quality of Service deployment in partners' networks

Some NRENs have implemented an experimental DSCP marking scheme for certain categories of traffic in their backbone in order to allow their clients to apply whatever policies they would like to. For example, some Universities are using these DSCP markers to match some categories of traffic and assign to them different local priorities. This is useful for avoiding access links congestion in some cases.

3.4.2. Applications of Quality of Service

Survey on applications of Quality of Service technology is obviously following service trends of research and education networks. One quarter (25%) of partners consider videoconferencing as a dominant application of QoS and an another quarter plus 15% have the same views on premium IP and less than best effort traffic classification, which are very well known from GÉANT network service portfolio having been a stable and useful services of the last three years. 15% of partners think of VoIP as a realtime application that needs QoS. 7% also mentioned streaming and video on demand among the important services that needs prioritization.

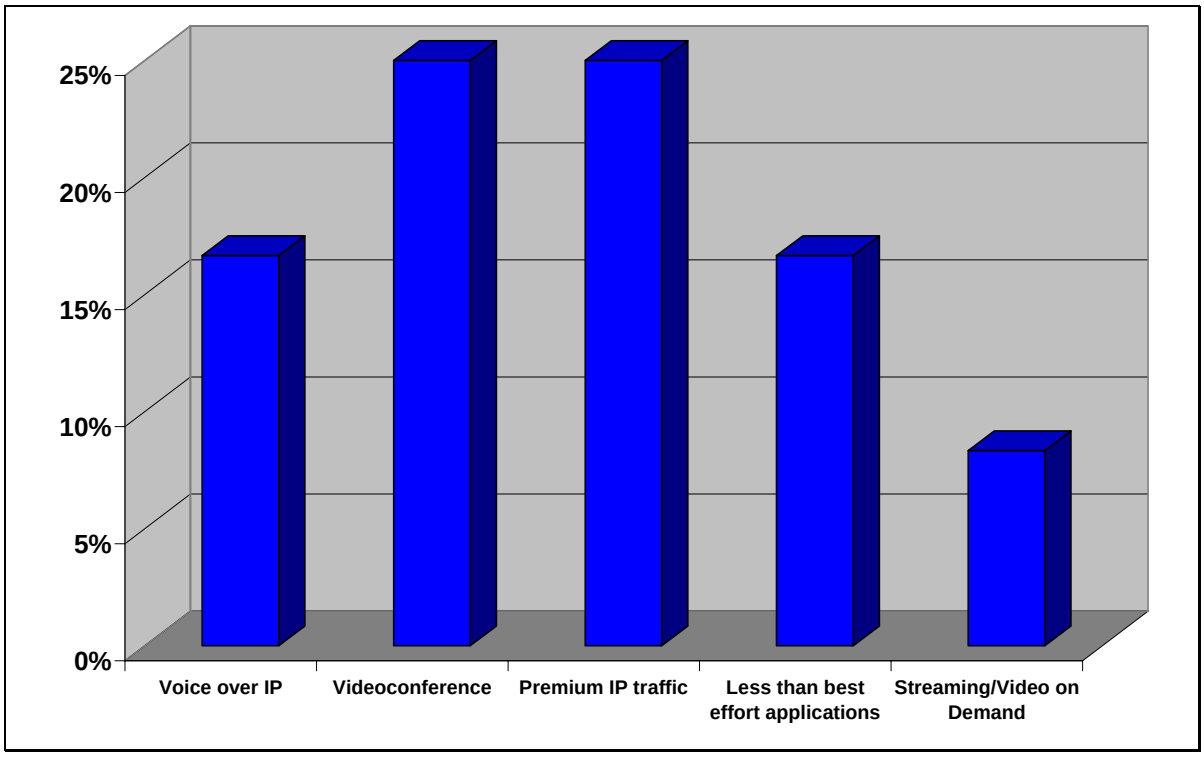

Figure 14: Applications of Quality of Service

3.4.3. Need for Quality of Service on SEEREN2 backbone

When considering available QoS options, care should be taken to avoid stressing router CPUs too much. In many cases SEEREN routers run already at the edge of their performance capabilities.

Some NRENs consider that the best approach to QoS is to never ever have a need for it. That is, to have over provisioning in the underlying infrastructure. Unfortunately over provisioning is not always financially viable, especially in our region. As a rule of thumb, QoS should be deployed only if (and where) there would be some real benefits of using it.

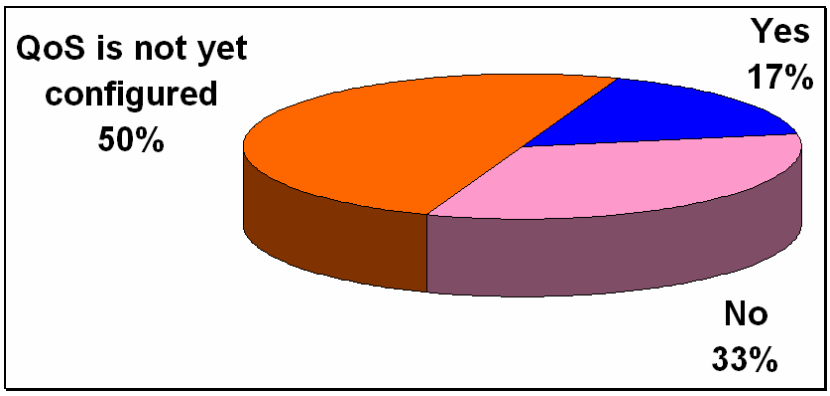

Figure 15: Does your network need QoS configured on SEEREN2 backbone?

3.5. Bandwidth on Demand

Bandwidth on demand is a data communication technique for providing additional capacity on a link as necessary to accommodate bursts in data traffic, a video conference, or other special requirements. The technique is commonly used on dial-up lines and wide area networks (WANs) to temporarily boost the capacity

of a link. Some call it "rubber bandwidth" because the capacity can be increased or decreased as needed. It is also called dynamic bandwidth allocation or load balancing. A similar technique is bandwidth on time of day, which refers to providing additional capacity at specific times of the day.

A network administrator who cannot be sure of traffic patterns between two sites can install routers that provide bandwidth-on-demand features. Such routers can automatically establish links on demand (dial-up, ISDN, or other switched services) to provide more capacity, and then bring the line down when traffic demands diminish. Home users with ISDN connections can aggregate two 64-Kbit/sec lines into a single 128-Kbit/sec line on demand.

Bandwidth on demand is both economical and practical. It makes sense to use a switched line and only pay for services as they are needed, rather than lease an expensive dedicated line that may go underused part of the time. Networks such as frame relay can automatically provide more capacity without the need to add additional lines, but the capacity is limited by the size of the trunk that connects a customer to the frame relay network.

Inverse multiplexing is a technique that combines individually dialled lines into a single, higher-speed channel. Data is divided over the lines at one end and recombined at the other end. Both ends of the connection must use the same inverse multiplexing and demultiplexing techniques. A typical dial-on-demand connection happens like this: A router on one end makes a normal connection, and then queries the router at the other end for additional connection information. When traffic loads are heavy, the additional connections are made to accommodate the traffic requirements.

Although a large number of transport technologies exist the reality is that most of the European NRENs still only have IP networks and often are supporting services using MPLS (e.g. L2VPNs). The reality is that only a few networks are deploying SDH networks. In addition, there are a few NRENs that have deployed a native Ethernet network. It is recommended to gather the future plans of the NRENs regarding the introduction of lightpath services, a good starting point is the Terena compendium.

In terms of signalling, the only signalling protocol that the IETF is currently working on for GMPLS implementation is the Resource Reservation Protocol (RSVP). The parallel work on CR-LDP has been postponed.

The following BoD frameworks have been proposed by the Internet Engineering Task Force (IETF), the International Telecommunication Union (ITU) and the Optical Internetworking Forum (OIF).

- **Generalized Multi Protocol Label Switching (GMPLS)**

  According to the Generalized MPLS (GMPLS) framework (RFC3945), the MPLS Traffic Engineering (TE) control plane is extended to include network elements such as Add-Drop Multiplexers (ADMs) and Optical Cross-Connects. Whereas the MPLS framework (RFC3031) was proposed for network elements that were assumed to be able to recognize packet or cell boundaries, the GMPLS framework was proposed for network elements that in addition can recognize time-slots, lambdas or ranges of lambdas and fibres;

- **Automated Switched Optical Network (ASON)**

  To overcome the limitations of centralised manual provisioning, ITU-T Study Group 15 started, following a top down approach, the development of complete definition of the operation of an Automatically Switched Transport Network (ASTN). An Automated Switched Optical Network (ASON) is an optical transport network that has a dynamic connection capability. This capability is accomplished by using a control plane that performs the call and connection control functions;

- **User Network Interface (UNI)**

  The definition of the physical interfaces between clients and the network, the connectivity services offered by the transport network, the signalling protocols used to invoke the services, the mechanisms used to transport signalling messages and the auto-discovery procedures that aid signalling constitute the User to Network Interface (UNI), the service control interface between the user devices and the transport network. The UNI interface does not allow exchange of routing information, while this happens over I-NNI and E-NNI interfaces. Many different specification of UNI have been produced by various bodies: the ATM Forum, the ITU-T, MPLS Forum, Frame Relay Forum, Metro Ethernet Forum, IETF, Optical Internetworking Forum.

3.5.1. Overall need for Bandwidth on Demand service

According to survey results only one quarter (25%) of respondents expressed no interest at all from their user base for Bandwidth on Demand services. Half (50%) of the partners answered positively but were not sure of possible users. The remaining quarter (25%) not only confirmed need for BoD services but also knew exactly what it can be useful for.

It could be concluded that there is general awareness of the need for BoD services, but certain obscurity about their possible applications. This implies that information on BoD applications should be made available and actively presented to all partners.

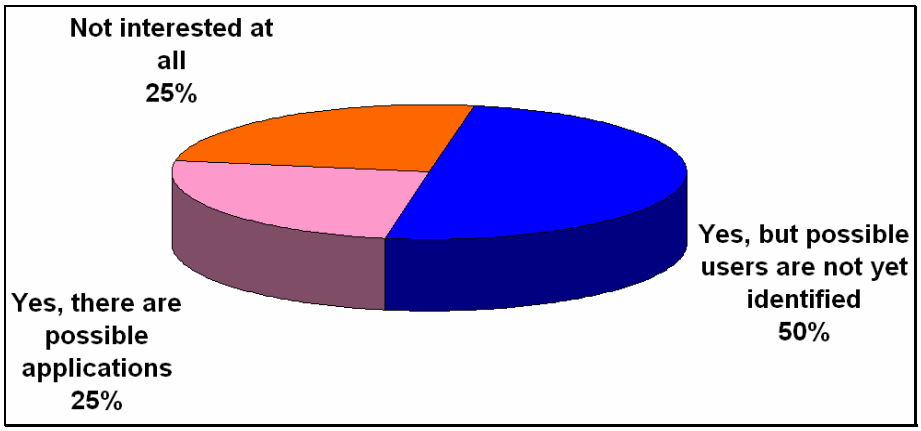

Figure 16: Does your user base need Bandwidth on Demand services?

3.5.2. Possible Bandwidth on Demand applications

Although previous survey result showed lack of information on possible BoD applications, some applications were selected as the most needed among those partners who were aware of them. The biggest percentage (almost 60%) saw supercomputing and GRID applications as the ones most suited and with the most need for Bandwidth on Demand. Almost half of them (little over 30%) consider high bandwidth real time traffic transportation as a BoD application. Approximately, one fifth (just over 20%) finds International project cooperation as a possible BoD application. Only small percentage (some 12%) of respondents answered that possible BoD applications are not yet identified, and that percentage is somewhat different from what could have been expected from previous point.

Survey results might be little biased towards GRID and supercomputing applications since there are a number of SEEREN partners in SEE-GRID project who are familiar with GRID applications. Also general international project cooperation seems to be a term that might include different applications that might need BoD services. Again, the conclusion might be that dissemination of knowledge about applications of BoD is really needed.

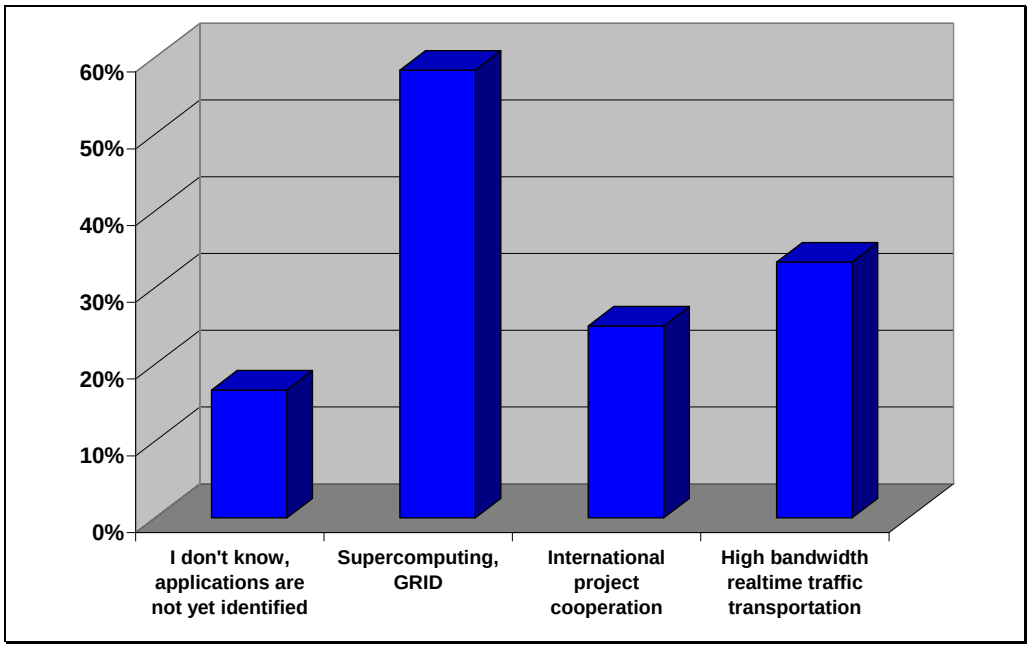

Figure 17: Applications of Bandwidth on Demand

3.5.3. Need for Bandwidth on Demand service on SEEREN2 backbone

In the spirit of answers to the previous survey question, only 17% of respondents believe that their organization needs BoD services implemented on the SEEREN2 backbone network. Obviously partners do not consider BoD services to be of high priority service on SEEREN2 backbone network. Since only small percentage know about possible applications of BoD, it's not strange that it's not considered as an important service.

With increase of number of BoD applications and wider awareness of them it might be reasonably expected that need for implementation of BoD service on SEEREN2 backbone network will rise.

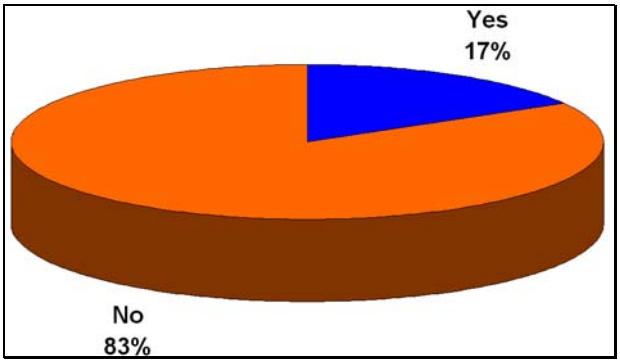

Figure 18: Does your organization need BoD services implemented on the SEEREN2 backbone network?

3.6. Network management

Improvement of network management facilities of SEEREN2 project partners is one of the most important goals of the project.

3.6.1. Type of monitoring used

Rapid network development and technology changes forced the new approach in network management and monitoring. The two common approaches are the *passive* and *active* monitoring. Both have their advantages and should be used complementary in conjunction with one another.

With the passive monitoring approach, information about network performance and status is collected by periodically polling the networking devices. Commonly used monitoring protocol is Simple Network Monitoring Protocol (SNMP) which is generally supported by modern routers, switches and end hosts. SNMP capable devices measure and collect information about performance and status, defined in Management Information Bases (MIB). SNMP allows users to access devices and remotely read the collected data. Besides this polling, the passive monitoring does not additionally increase the traffic on the network for the measurements.

The active approach relies on the capability to inject test packets into the network or send packets to servers and applications, following them and measuring the results obtained from the network. Therefore, the active approach provides explicit control on the generation of packets for measurement scenarios. The simplest and widely applied example of active monitoring assumes sending icmp ping packets and measuring round trip time and packet loss. More advanced techniques can emulate various services, applications and functions chosen to be monitored.

Given the complementarily of the two mechanisms, we need to explore ways to get the best of both. By comparing and contrasting the active and passive measurements, the co-validity of the different measurements can be verified and much more detailed information is made available.

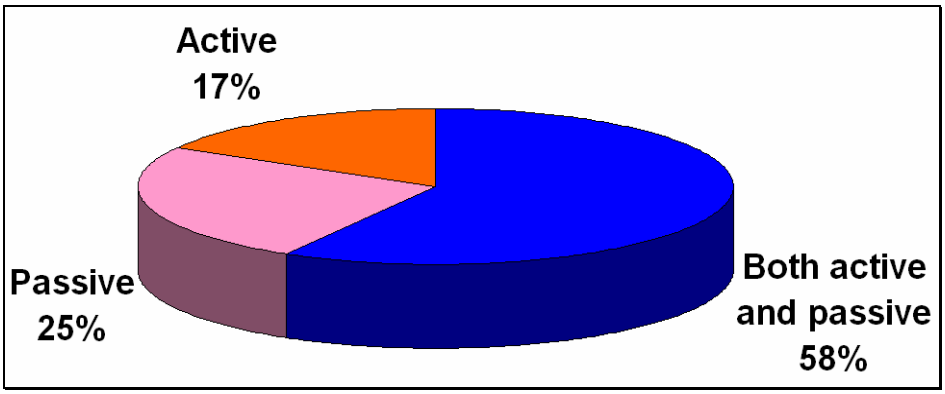

Figure 19: What type of monitoring is used in your network?

As the above graph shows active monitoring is used by 17% of project partners, passive monitoring by 25%, and both type of monitoring is used by 58% of them.

3.6.2. Passive monitoring tool usage

This question surveyed different type of active monitoring tool used by partners. Passive monitoring tools include traffic measurement applications, routing monitoring, equipment configuration monitoring and versioning, looking glass, weathermap application, etc.

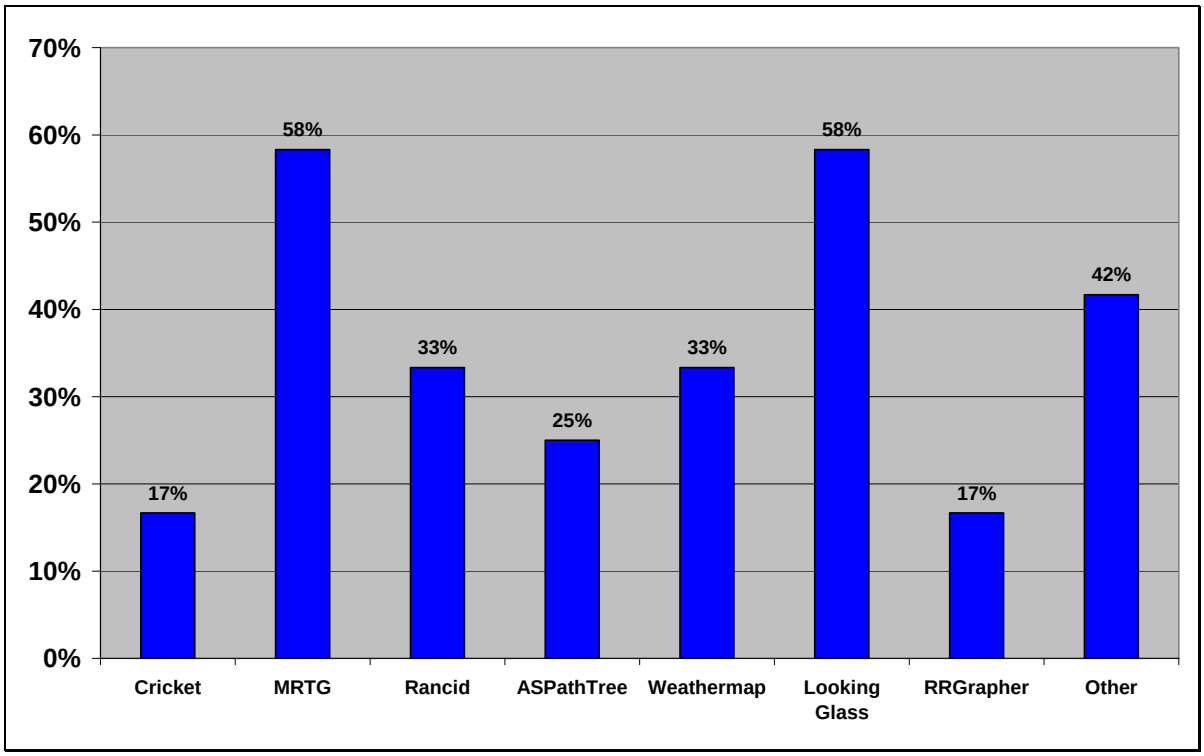

Figure 20: What passive monitoring tools are used in your network?

Traffic measurement software tools are used by nearly all the partners. 17% are using Cricket, 58% are using MRTG and another 17% are using RRGrapher for a long term observation of traffic at router and switch interfaces. One third (33%) of partners also runs a weathermap application as well. For routing monitoring using of ASPathTree (25%), for configuration management Rancid (33%) were reported. 59% of partners are also using a looking glass application in order to support easy and quick debugging of network problems.

Nearly half of partners (42%) indicated using of other passive network management tools including Cacti, ntop, perfSONAR, OpenNMS and other, self-made custom scripts and tiny software tools.

3.6.3. Active monitoring tool usage

For active network monitoring Nagios (25%), SmokePing (25%) and NetIIS were reported. In section "other" (33%) perfSONAR, OpenNMS, Sitescope, and self-made tools were indicated.

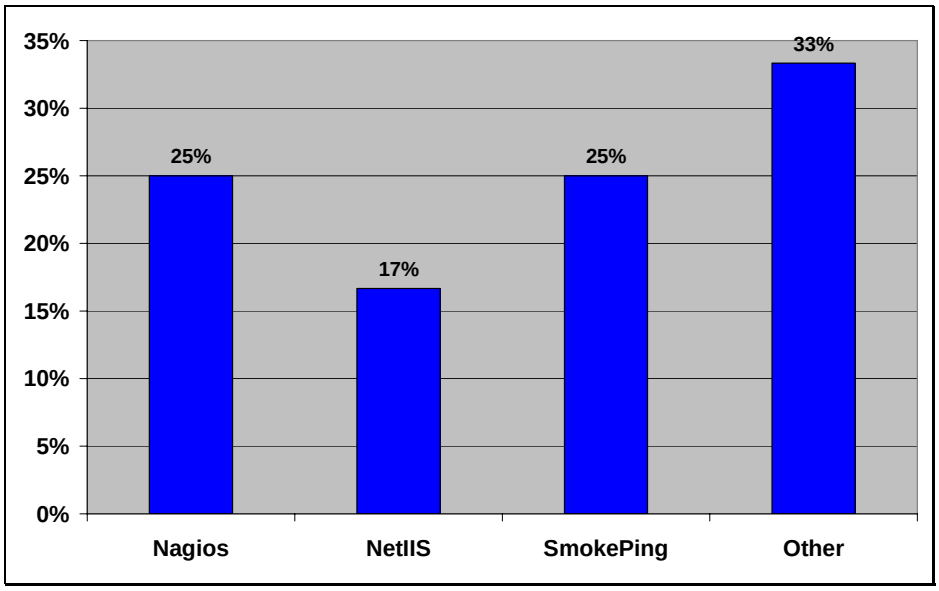

Figure 21: What active monitoring tools are used in your network?

3.6.4. SLA management tool usage

A Service Level Agreement (SLA) is a part of the contractual documentation that is included in the agreement concluded between the customer leasing telecommunication capacities and the telecommunication provider. The main purpose of a SLA is to define the services that the communications service provider is obliged to deliver to the beneficiaries, to stipulate the parameters according to which the quality of the service shall be evaluated and to define the mutual rights and obligations of the contracting parties with respect to certain value ranges that these parameters may take [8].

In general, basic SLA parameters could be the following:

- Time To Deliver (TTD) – the time by which the communications service provider commits to implement the service;
- Fault Handling period – weekly timeframe when provider's help desk is available and ready to deal with error report by customer;
- Mean Time Between Failures (MTBF) – maximum of average time between two service failures;
- Mean Time To Restore – the average of the "times to restore" in a reporting period being defined as one calendar month. The "time to restore" is the timeframe between the moment a trouble ticket is opened by the service provider upon request from the purchaser until the moment the trouble ticket is closed after a mutual consent between the purchaser and the service provider;
- Service Availability Rate – the percentage of time during the reporting period where the communications service is available. The availability of the service is again evaluated according to the potential trouble tickets;
- Service Bit Error Rate – average bit error ratio observed in the reporting period.

Although, these are the most important and most common SLA parameters, there could be plenty of others derived from the nature of the service implemented by the customer on the top of the telecommunication service leased from the service provider. SLA parameters must be measured by customer for its own interest in order to audit real quality of service specified by the agreement. When the provisioned telecommunication service parameters are not within the agreed SLA thresholds the customer is entitled to receive compensation from the service provider based on contractual clauses. However, accurate measurement of SLA parameters can be rather complicated and needs a SLA management software environment and statistics from trouble ticketing systems as a minimum.

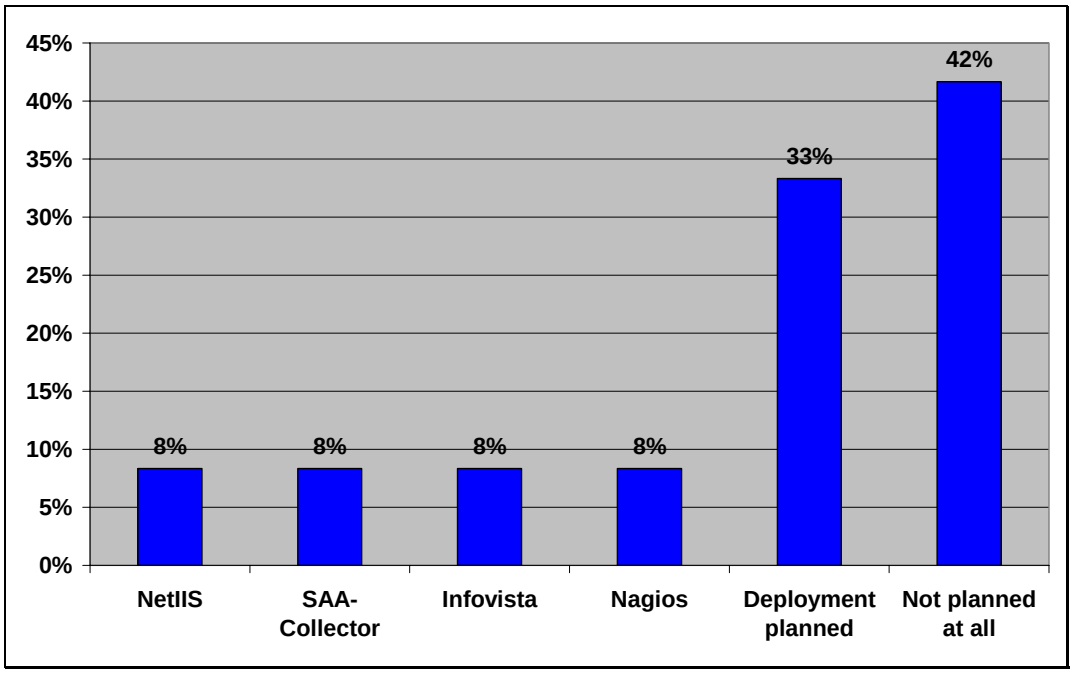

Figure 22: What tools are used for SLA management in your network?

This question intends to survey SLA management software usage in SEEREN2 partner networks and intention to use such software in the near future. The above diagram shows that NetIIS, SAA-Collector, InfoVista and Nagios are all used each by a single (8%) project participant, 33% of them are planning to introduce it, and 42% are not interested at all.

3.6.5. NetIIS management tool deployment and usage intention

NetIIS is an advanced, efficient, multi-user, easy to use, web based networking information and monitoring system. NetIIS has been developed in Belgrade University Computer Centre (RCUB) with the idea to discover, collect and offer all relevant networking information and help the network administrators in their everyday technical activities.

NetIIS performs both passive and active monitoring, giving reliable and up-to-date status about running the network infrastructure, services and attached devices. Furthermore, a flexible software framework can also be used as a technical knowledge database with the ability for users to store various texts and information about the target network and networking problems.

The software is developed on java platform, running on the Linux web application server with a MySQL database.

Monitoring elements of interests in the networking environment are:

- **Traffic monitor** – measuring traffic throughput on the link;
- **Port monitor** – link status;
- **SNMP monitor** – getting arbitrary SNMP variables, such as BGP session status, router CPU load, router memory usage, MPLS status, system uptime, etc.;
- **Ping monitor** – active monitor which performs native icmp ping from NetIIS server to the assigned device, and retrieves ping results: min/max/average round trip time, sent and received packets and packet loss;
- **NMAP monitor** - active monitor which performs native NMAP action from NetIIS server and check if specified UDP/TCP port is open on the assigned device;
- **External monitor** – executes a separate program on NetIIS server, named agent, and retrieves the results from it.

The software is problem solving oriented, specially adopted to fit users needs and to link database and monitoring information following the logical troubleshooting methods. Typical user access is performed though standard web interface. It allows browsing the database, finding information, having a various views on network status and other details. Since the living network requires active interaction with the technical staff, web access also supports simple set-up and data changing.

NetIIS is aimed to help the users who manage NREN or any large scale network as well as SEEREN2 backbone network. Therefore, intelligent auto-discovery functions have been developed. This capability enables complex network topologies to be easily translated into equivalent logical forms, with all relevant technical information (IP/MAC address, host and port names, descriptions, SNMP IDs etc.). Auto-discovery also automatically keeps the information up-to-date. Network items and links from the database can be presented graphically, allowing efficient topology overview, information access and performance monitoring.

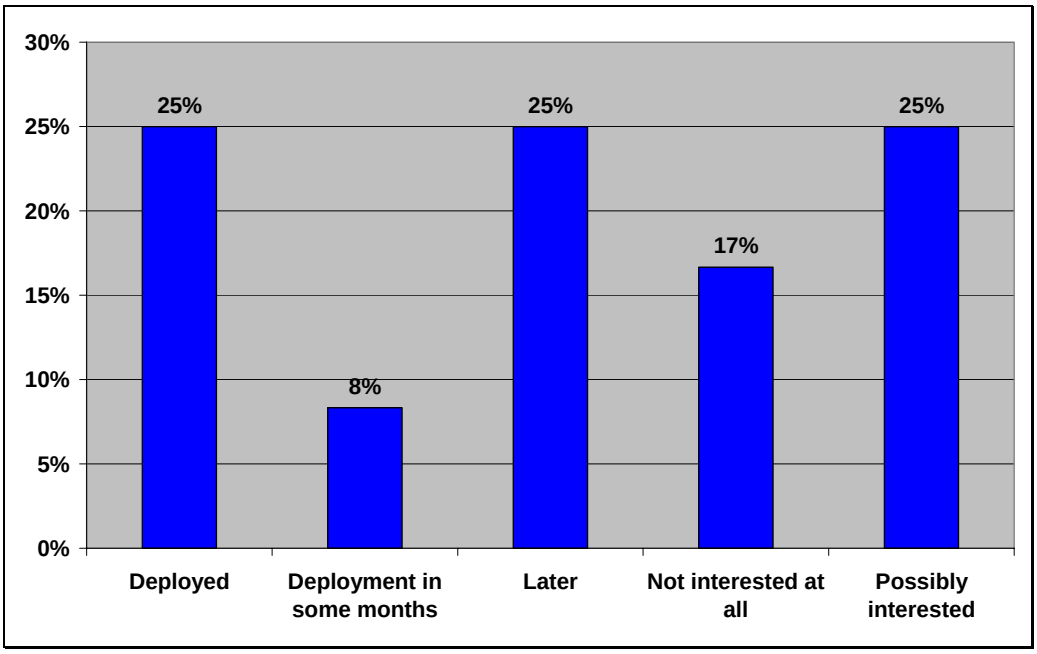

Figure 23: NetIIS monitoring tool deployment and plans to deploy

As the graphs shows, 25% of SEEREN2 partners have already deployed NetIIS monitoring tool and an additional 8% of them are planning to use it soon and another 25% are willing to use it later. 17% are not interested at all, the remaining 25% haven't decided yet on NetIIS usage.

3.6.6. Partner suggestions to improve NetIIS management tool

A single question was devoted to ask project partners on required improvements to NetIIS network management tool according to their user experiences with the software and needs in their network management environment. The following suggestions were received:

- Traffic Weathermap;
- SLA management;
- Looking Glass facility;
- Full address management support, including IPv6;
- Sharing data with other application via an XML/SOAP interface. Make possible for external applications to point user directly (after authentication) to specific position within NetIIS entity tree;
- Seamless integration with TTS and SLA management/calculations;
- Unified graphical representation of all monitored data, as well as introduction of new probes and modules.

Based on partners' suggestions and requirements, the following new features have been already developed and included in running NetIIS version:

- Traffic Weathermap;
- Looking Glass.

Integration with TTS is also possible - email format and other data should be defined with TTS administrators. Current development is taking other requirements into account.

3.6.7. Most important IPv6 network parameters to be monitored

Two survey questions were asking partners about their opinions on the most important IPv6 parameters to be monitored and which monitoring tools should be deployed (see next section).

Slightly less that half of the partners (42%) think that monitoring of IPv6 traffic volume has the greatest importance of all the other parameters. One third of partners voted for router and host reachability monitoring, another one third for IPv6 routing table monitoring (i.e. BGP routing table entries, etc.) and 17% percent thinks that latency measurements (i.e. round trip time, one way delay) can be useful in world of IPv6.

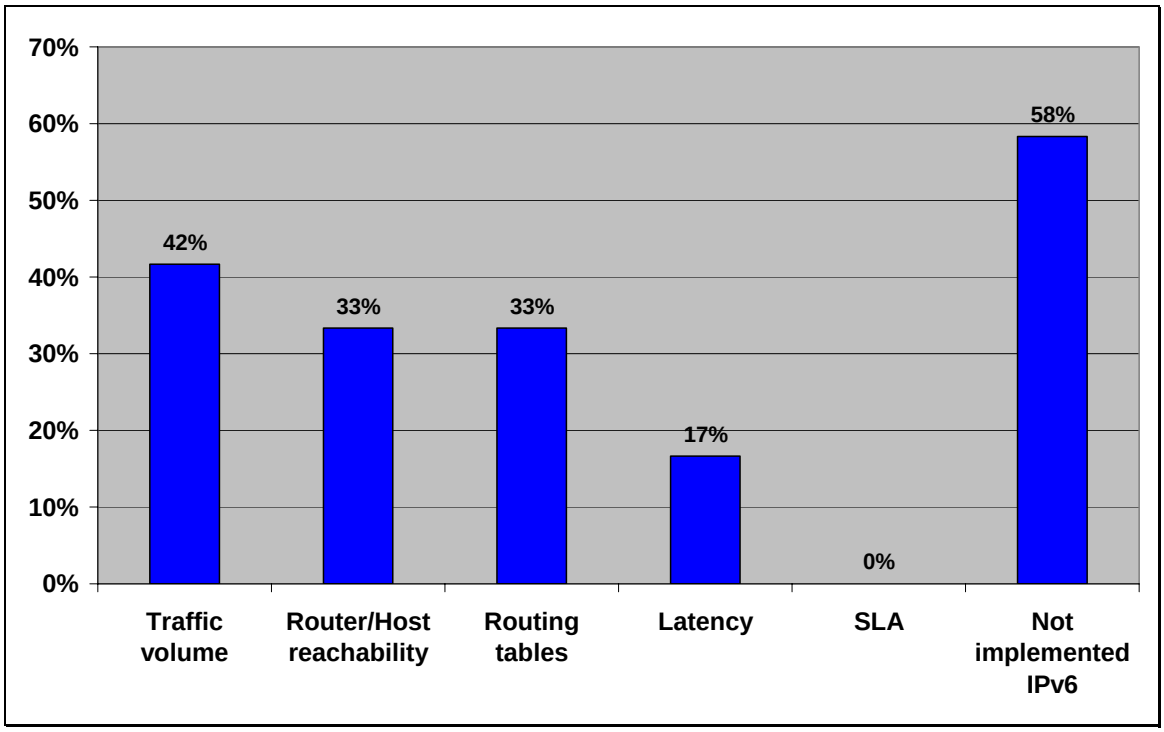

Figure 24: What do you think which are the most important IPv6 network parameters to be monitored?

Surprising, but none of the partners are convinced about the need for IPv6 SLA monitoring at this stage. When protocol deployment progresses, SLA monitoring and cross checking will obviously gain much more attention from partners. Survey graph also shows that 58% of partners haven't yet introduced IPv6 protocol.

3.6.8. IPv6 monitoring tools used in IPv6 enabled partner networks

Monitoring tools are essential to achieve observation of the most important IPv6 parameters detailed by the previous section. 60% of SEEREN2 project partners have already deployed looking glass and reachability monitoring facilities. 40% use IPv6 traffic monitoring separately from IPv4 traffic measurements. 20% use routing monitoring tools like ASPathTree for example to have certain statistics and visualization of IPv6 routing tables. Finally, a 20% of partners are using SLA monitoring for IPv6.

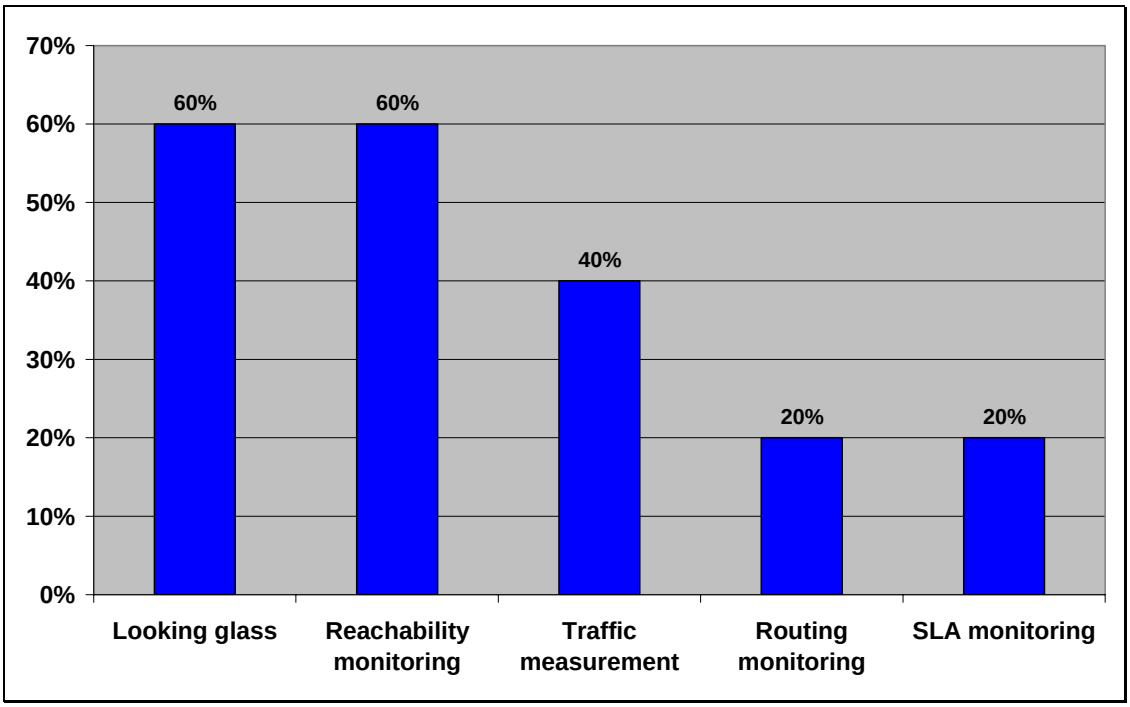

Figure 25: IPv6 monitoring tools used in IPv6 enabled partner networks

3.6.9. Performance focused Service Oriented Network monitoring ARchitecture (perfSONAR)

The need for a flexible, secure, scalable, fault tolerant, transparent, and open source multi-domain active and/or passive network performance monitoring framework has inspired the Performance focused Service Oriented Network monitoring ARchitecture (perfSONAR) project, jointly developed by 16 European NRENs, Dante, GÉANT2, ESnet, Internet2, RNP, and the University of Delaware. The project name reflects the choice of a Service Oriented Architecture for system's implementation. Within the framework of this activity, ISTF has developed an open source, publicly accessible, easy to use, and yet powerful standalone graphical user interface client, capable of querying all available perfSONAR services and displaying the returned data in a concise manner.

The performance focused service oriented network monitoring architecture (perfSONAR) provides efficient means for performance monitoring of data exchange between networks, making it easier to solve performance problems occurring between hosts, interconnected by several networks. It contains a set of services, delivering performance measurements in a multi-domain environment through well defined protocols, introducing intermediate layers between the performance measurement tools and the visualization applications.

The Measurement Points are the lowest layer in the system, performing active or passive measurements and storing network characteristics. The Measurement Point Layer of a domain consists of different monitoring components or agents, deployed within its boundaries. A monitoring agent provides information on a specific metric (e.g., one-way delay, jitter, loss, available bandwidth) by accessing the corresponding Measurement Points. Each network domain can, in principle, deploy Measurement Points of its choice.

The Service Layer is the middle layer of the system and consists of separate administrative domains. It allows for the exchange of measurement data and management information between those domains. In each domain, a

set of entities (services) is responsible for the domain control. Each of them is in charge of a specific functionality, like authentication and authorisation, discovery of the other entities providing specific functionalities, resource management, or measurement of network traffic parameters. In particular, the Measurement Archive (MA) Service is designed as a repository for measurement results. The interaction of the entities inside a domain as well as the access to the Measurement Point Layer or other domains may not be visible to the end user. Some of the entities contain an interface which can be accessed by the User Interface Layer.

The User Interface Layer consists of visualization tools (user interfaces), which adapt the presentation of performance data to be appropriate for the needs of specific user groups. In addition, they may allow users to perform tests, using the lower layers of the framework.

The aim of perfSONAR's design is to provide the main functionalities at the Service Layer as independent entities, allowing increased flexibility for the system. Existing elements may be replaced easily or new ones can be inserted. Even if the number of entities is large, they can be identified and invoked using discovery functionalities.

The development of PerfsonarUI began in Q4 of 2005, triggered by the explicit need to provide an open source, publicly accessible, easy to use, and yet powerful stand alone graphical user interface client, capable of querying all available perfSONAR services and displaying the returned data in a concise manner. At the time of this writing, PerfsonarUI supports all deployed Round Robin Database (RRD) and IP Performance Measurement (HADES) MA services.

A Java runtime environment on the client system is required for PerfsonarUI, which makes it platform independent. It uses the Apache Axis SOAP implementation to query perfSONAR services. The visualization is based on JFreeChart – an open source Java library for generating charts.

PerfsonarUI is distributed with a fully automated offline installer (PerfsonarUI-vX.YZ-setup.exe), compatible with recent versions of the Microsoft Windows (NT, 2000, XP, 2003) operating system, as well as a ZIP archive. Both distributions include the source code of the application, released under the GNU LGPLv2.1. Windows users should prefer the automatic installer, while the ZIP archive is suitable for any other platform.

PerfsonarUI provides seamless access to network performance data across different domains through a flexible and universal user interface, integrating an easily extensible set of different performance metrics. The multi-domain scenario is natively supported, thanks to the fully distributed design and implementation of the interactions between the User Interface Layer and the Service Layer.

At present, PerfsonarUI is able to query one or several RRDs and/or HADES MAs simultaneously (in parallel threads) and visualize the returned data. Users can apply filters (a list of IPv4/IPv6 interface addresses or arbitrary traceroute output) in order to search for a particular subset of interface utilization data. The visualization is done both in tabular and graphical form. A condensed summary of interface utilization is provided in a radar chart. Users can select different criteria for sorting the data. The tool provides a quick overview of the interface utilization vs. capacity in several user-selected domains simultaneously, as well as detailed views for any particular interface. Time intervals for summary and detailed views are selectable through radio buttons and sliders. Another important feature of PerfsonarUI is the ability to visualize one-way delay (OWD), IP Delay Variation (IPDV), and packet loss between HADES Measurement Points. Graph zooming capabilities are built-in. Users can select source, destination, probe packet size, and date. Support for more options, as well as better error handling and reporting are planned for future releases.

The primary target user groups for PerfsonarUI include Network Operations Centres' (NOCs) and Performance Enhancement and Response Teams' (PERTs) staff, as well as projects with demanding network performance requirements. End-users with some basic technical background are supposed to master the tool quite easily too.

Three SEEREN2 partners have already deployed perfSONAR services (GRNET, ISTF and UOM/MREN). Others are expected to follow, as soon as the expected first official and supported packaged set of perfSONAR services for multi-domain monitoring is publicly released.

3.6.10. Tools used for unified representation of monitored data

Unified representation of monitored data coming out of network equipments, management software components and tools is an important and effective way of representing different measurement results in the same or similar form. This ensures comparability and lower cost of management.

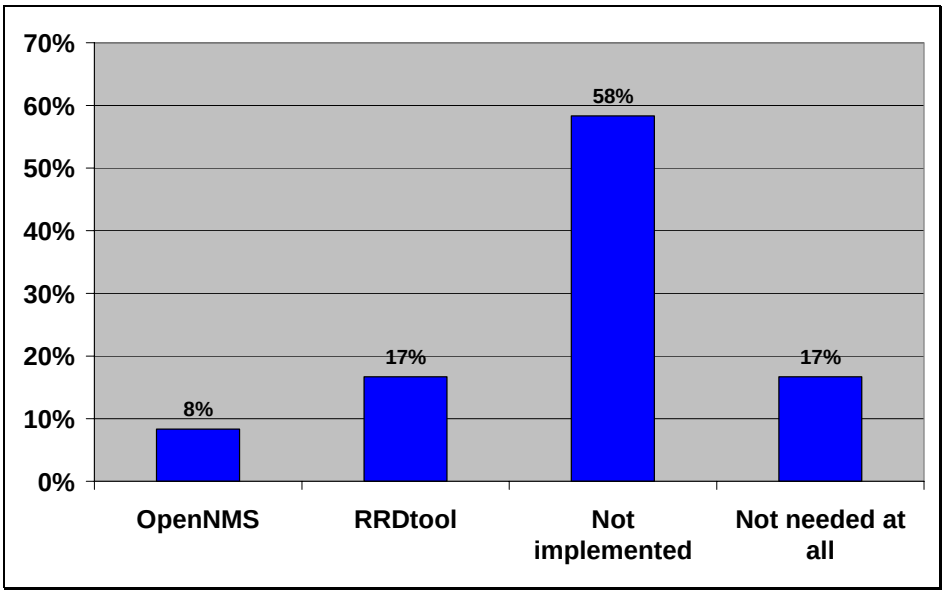

Figure 26: What tools are used for unified representation of monitored data in your network?

A major part of SEEREN2 project partners (58%) is not yet using unified representation of measured data, and another 17% think that it's not needed at all. 8% and 17% of the partners have already deployed OpenNMS or RRDtool.

3.6.11. Trouble Ticketing System usage at partners

Fault tracking and resolution is a time-consuming activity and one of the most useful tools available to network and service managers is that of a trouble ticket system. Trouble tickets are essentially fault reports that are administered as documents. These documents are active from the time a fault is reported, during its diagnosis, and until its eventual correction. They are then generally archived to provide statistical information. [9]

A trouble ticket contains not only information about the related fault but also represents the on-going activity related to the correction of the fault. Hence, a trouble ticket contains not only information about the fault (such as a description of the problem, probable cause, and time of reporting) but also status of any corrective action initiated and the current owner of the problem.

The Trouble Ticket API should meet the following functional requirements:

- allowing clients to create, remove, or cancel trouble tickets;
- allowing clients to change the values of trouble ticket parameters;
- allowing clients to be informed of changes to trouble tickets via a notification mechanism.

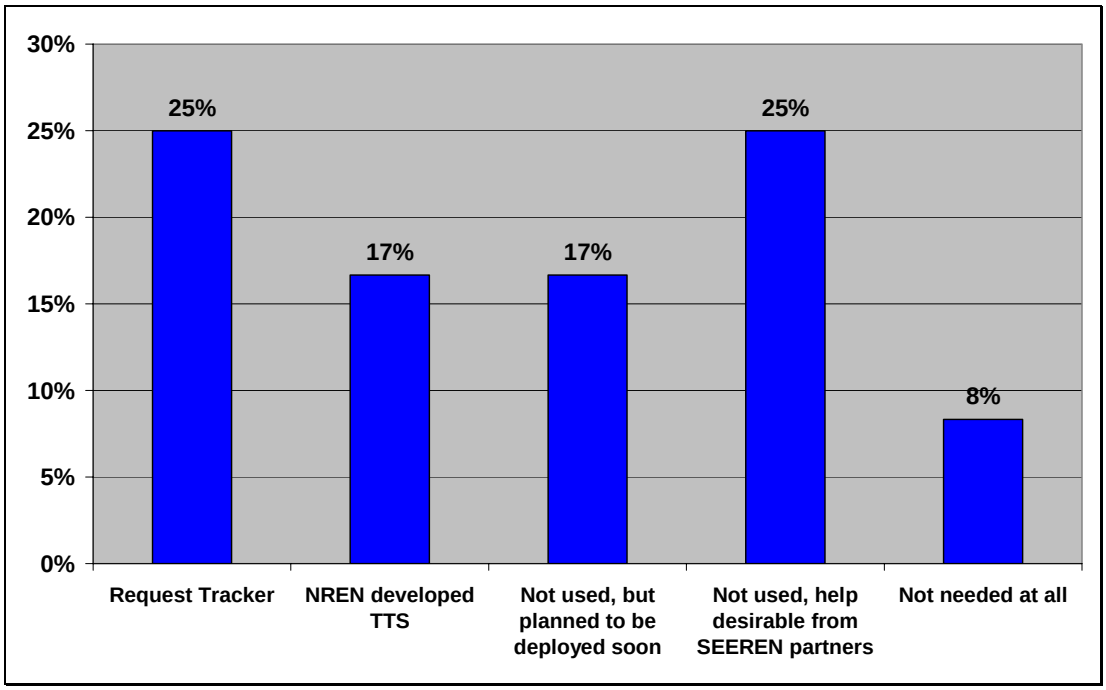

Figure 27: What TTS system is used in your network?

3.7. Security services

A Computer Security Incident Response Team (CSIRT) is a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity. Their services are usually performed for a defined constituency that could be a parent entity such as a corporation, governmental, or educational organization; a region or country; a research network; or a paid client.

A CSIRT can be a formalized team or an ad hoc team. A formalized team performs incident response work as its major job function. An ad hoc team is called together during an ongoing computer security incident or to respond to an incident when the need arises.

Even the best information security infrastructure cannot guarantee that intrusions or other malicious acts will not happen. When computer security incidents occur, it will be critical for an organization to have an effective way to respond.

The speed with which an organization can recognize, analyze, and respond to an incident will limit the damage and lower the cost of recovery. A CSIRT can be on-site and able to conduct a rapid response to contain computer security incident and recover from it. CSIRTs may also have familiarity with the compromised systems and therefore be more readily able to coordinate the recovery and propose mitigation and response strategies.

Their relationships with other CSIRTs and security organizations can facilitate the sharing of response strategies and early alerts to potential problems. Proactively, CSIRTs can work with other areas of the organization to ensure new systems are developed and deployed with "security in mind" and in conformance with any site security policies. They can help identify vulnerable areas of the organization and in some cases perform vulnerability assessments and incident detection.

They can focus attention on security, and provide awareness training to the constituency. CSIRTs can also provide expertise to do preventive and predictive analysis to help mitigate against future threats.

A CSIRT may perform both reactive and proactive functions to help protect and secure the critical assets of an organization. There is not one standard set of functions or services that a CSIRT provides. Each team chooses their services based on the needs of their constituency.

Determining the size of a CSIRT can be a challenge, and unfortunately there is little empirical data that can be used to answer this question. Different CSIRTs have different staffing levels based on their resources, needs and workload. A model that works for one organization may not work for another.

3.7.1. CSIRT service

The tasks and functions of a CSIRT service can be grouped according to the followings.

Information Filtering

The number of security Advisories and Warnings is growing at an enormous rate. The CSIRT will filter information from multiple sources on relevance and urgency before passing on the information to participants, thereby facilitating the decision making process and at lower cost than working on their own. This information can be disseminated via a website, email lists, conferences and mail shots.

Access to Expert advice

Many of the Advisories and Warnings require specialist knowledge to fully understand the significance and required action to reduce the risk of a successful attack. The CSIRT will facilitate information sharing between experts both within the SEEREN community and other CSIRT s. It will liaise with other experts from trusted organisations such as CERT, thereby producing higher quality solutions.

Early Warning

The CSIRT will provide a validated and trusted reporting environment, which will enable participants to benefit from the experience of others when attacks are taking place. The CSIRT will advise an organisation on initiating emergency preventative measures.

Strategic Decision Support

The CSIRT will over time analyze incidents and the most effective countermeasures, and together with threat forecasts, produce strategic reports (with additional information provided from other CSIRTs), which can be used to support the business decision process for security investment, thereby optimizing the value of the investment.

Education and Awareness

Information Security is a topic that is continually evolving as new technologies are introduced, new threats identified and new solutions developed. The CSIRT will provide a channel to disseminate advice on new security topics, based on the relevance to the members of the SEEREN community, from sources such as the CERT Coordination Center (CERT/CC) and CSIRTs. Regular training sessions for CSIRT personnel will be employed. Sharing of experiences and knowledge with other SEEREN members at events such as the SEEREN conference will also be promoted.

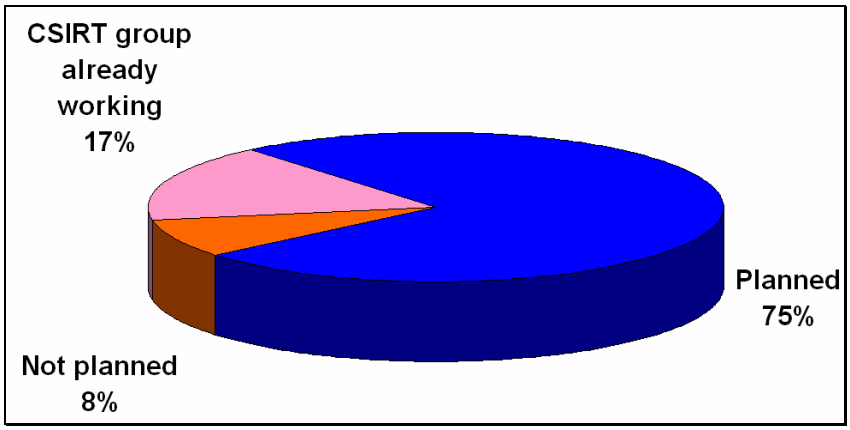

Figure 28: CSIRT groups working at partners' networks

According to the diagram above, 75% of SEEREN2 project partners are planning to establish CSIRT security groups for their customers. In 17% of them a CSIRT group is already working. 8% of partners do not plan introducing such a service.

3.7.2. Need for a common SEEREN2 CSIRT service

The SEEREN CSIRT will provide a trusted community of interest between SEEREN members where they can report incidents and seek advice without the fear that the information will be used to harm them. Trust and confidence are crucial characteristics of any on-line services. Maintaining Confidentiality, Integrity or Availability of the information related to these services is paramount in ensuring continued confidence in these services.

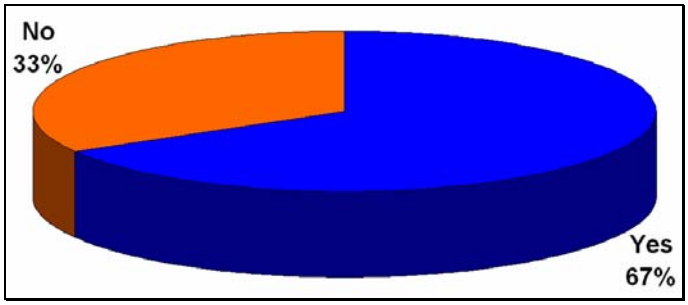

Figure 29: Does your organization need a SEEREN2 level CSIRT service?

The result of the survey question shows that 67% of SEEREN2 partners are convinced that they need a SEEREN2 level CSIRT group. One third of them think that they do not need a SEEREN2 CSIRT.

3.7.3. Need for DoS or Distributed DoS attack prevention and detection tools

In computer security a denial-of-service attack (DoS attack) is an attempt to make a computer resource unavailable to its intended users. Typically the targets are high-profile web servers, the attack aiming to cause the hosted web pages to be unavailable on the Internet. It is a computer crime that violates the Internet proper use policy as indicated by the Internet Architecture Board (IAB).

DoS attacks have two general forms:

- Force the victim computer(s) to reset or consume its resources such that it can no longer provide its intended service;

- Obstruct the communication media between the intended users and the victim in such that they can no longer communicate adequately.

Attacks can be directed at any network device, including attacks on routing devices and Web, electronic mail, or Domain Name System servers.

A DoS attack can be perpetrated in a number of ways. There are three basic types of attack:

1. consumption of computational resources, such as bandwidth, disk space, or CPU time;
2. disruption of configuration information, such as routing information;
3. disruption of physical network components.

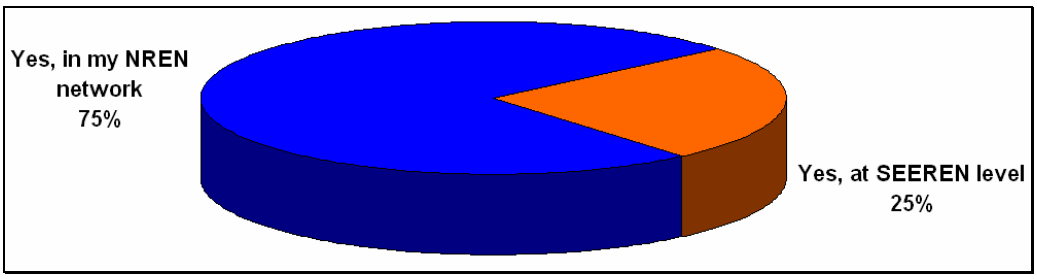

Figure 30: Does you need DoS and DDoS attack prevention and detection tools?

The diagram reflects that three quarter of project partners would like to have some kind of support from SEEREN2 project in establishing DoS and DDoS attack prevention tools or services in their own networks. The rest of the partners think that it should be implemented on SEEREN2 level.

3.8. Voice over IP

Voice-over-Internet Protocol (VoIP) is one of the most important audio transmission technology of nowadays. VoIP represents a fundamental shift away from the circuit-based telephony architecture that has been the backbone of the telecommunications infrastructure for more than 100 years and carries with it a number of important implications for the management of data networks, security and telecommunications systems. Because VoIP sends information as packets like other Internet traffic, and because VoIP is not nearly as regulated as conventional telephony, it offers several potential advantages to organizations of all sizes, especially educational and research institutions. Due to its capability to use existing network infrastructure, such as the SEEREN2 backbone, without any additional cost for infrastructure it makes it very cost-effective way of communicating among network users and potentially with the rest of the classic public available phone systems via VoIP providers or other PBX systems. [3]

There are numerous advantages in adding VoIP services to existing IP infrastructure such as:

- Lower costs per call (especially for long-distance calls through a contracted VoIP provider, or totally free calls e.g. to another VoIP enabled research network);
- Lower infrastructure costs: when VoIP infrastructure is installed, no or little additional telephony infrastructure is needed;
- While lowering infrastructure costs better coverage is achieved in parts where phone installations were not traditionally established (i.e. student's labs);
- Higher speech quality (but usually higher bandwidth consumption);
- Benefits of additional services integrated with VoIP (video communications, whiteboard, data exchange, instant messaging etc.);
- Reduction of maintenance expenses of a telephone network being parallel to existing data networks;

- Mobility of users across different geographical areas at the cost of local access to public networks such as Internet.

In process of creating voice traffic over existing IP networks, two steps are needed: digitizing voice and turning it into IP packets. Using the IETF RTP protocol (Real-time Transport Protocol), which is a connectionless end-to-end protocol designed to transport delay-sensitive information, digitized voice is transported across the IP network. RTP identifies the encapsulated payload type and includes sequence numbers and time stamps that are used to synchronize real-time information flows. RTP uses the unreliable UDP (User Datagram Protocol) protocol as a transport protocol that prevents from retransmission of lost or corrupted packets by not providing an acknowledgment mechanism, which would cause unreasonably high delay and jitter to the time sensitive audio stream. Delivering VoIP services on IP networks is much more challenging task than carrying voice on a traditional PSTN (Public Switched Telephone Network) network, as IP's best-effort delivery service is unable to guarantee basic transmission parameters such as bandwidth, delay and jitter that are indispensable for packet based voice conversations. To overcome these IP performance limitations it is necessary to deploy bandwidth management techniques such as prioritization (QoS) to ensure that critical applications get the performance they need.

Increasing the amount of total bandwidth of the network usually does not give the demanded performance, since it will be used by more aggressive applications that run on the network. Also increasing existing bandwidth usually creates additional costs for organizations. In order for VoIP to function network stability and prioritized packet delivery is strongly recommended. Introduction of QoS for handling VoIP packets for end-to-end connectivity between users is strongly recommended. Advantage of VoIP in terms of predicting needed bandwidth is relatively easy since it consumes predictable amounts of bandwidth per call in progress.

VoIP protocols

In order to carry voice signal over IP infrastructure and initiate connections VoIP protocols must be used. Some of most widely used are H.323 set of protocols and SIP (Session Initiation Protocol). VoIP uses the Internet Protocol (IP) to send/receive voice as data packets over an IP network. By using a VoIP protocol, voice communications can be achieved on any IP network infrastructure regardless of the fact that it is Internet, intranets or Local Area Networks (LAN) or combination of them. A VoIP signalling protocol is needed to set up, maintain and disconnect calls, locate users and negotiate parameters of communication or to exchange additional information. There are a few important VoIP protocol stacks which have derived from various standard bodies and vendors, namely H.323, SIP, and MGCP.

H.323

H.323 is an ITU-T recommendation or to be more precise a reference for many ITU-T recommendations covering packet based voice, video and data communications both for point-to-point calls and multipoint conferences. H.323 is often referred as a protocol umbrella as ITU-T recommendation H.323 references many related protocols such as H.225.0 (call signalling), H.245 (multimedia control protocol), H.235 (security), H.450 (supplementary services) and many, many others.

Originally, H.323 was designed for multimedia conferencing in Local Area Networks but according to its rapid acceptance among organizations it was expanded to cover VoIP communications and later videoconference. VoIP expansion covers not only point to point communications, but conferencing among users. Basically, it is defined by four logical components: terminals, gateways, gatekeepers and Multipoint Control Units (MCUs). Terminals, gateways and MCUs are commonly known as endpoints. These components are designed to cover the following tasks:

- **Terminals:** telephone devices, softphone applications, voice mail devices, etc.;
- **Gateway:** a gateway device is capable of protocol translation in order to ensure connectivity between two voice networks separated by different signalling protocols (e.g. a H.320-H.323 gateway connects ISDN networks to H.323 based VoIP networks);
- **Gatekeepers:** gatekeepers are optional elements of a H.323 network but they provide many essential network services such as address resolution (i.e. phone number to IP address), call routing, call admission control, endpoint authorization and call accounting, etc.;
- **MCU:** a Multipoint Control Unit is primarily designed to provide multipoint conference facilities by connecting numerous terminals into one large conference. MCU is responsible for multipoint

call management by terminating several point to point calls, media mixing, switching and conversion in order to overcome on different terminal capabilities. An MCU must be able to run several parallel conferences at a time according to its capacity. Read more about MCUs in section 3.9.

Session Initiation Protocol (SIP)

Session Initiation Protocol (SIP) is an IETF protocol defined by RFC 3261. SIP is an application layer control protocol that was designed for initiating, modifying and terminating interactive sessions carrying multimedia communications data including voice, video, instant messaging, online gaming, etc. It uses client – server communication model to exchange necessary information needed for establishment of connections.

The world is obviously moving from the H.323 protocol towards SIP, as H.323 protocol is too complicated so it makes difficult to improve products and ensure sufficient interoperability.

VoIP service providers and PSTN connectivity

To utilize full advantages of VoIP, VoIP service provider can be contracted so that connectivity with the classical telephony (PSTN) can be established with reduced prices. VoIP providers can be selected and configured independently at every NREN or it can be done at SEEREN level in which case a billing solution would be necessary at SEEREN level.

Legal issues

It must be brought to attention that in some countries VoIP services are not clearly handled by local laws or even considered illegal. Detailed inquiry is necessary in these cases as a precaution since it might violate service agreements with local Telecom providers.

3.8.1. Voice over IP services in SEEREN2 partner networks

Surprisingly, none of the project partners have a Voice over IP service entirely based on the H.323 protocol. Only one partner use the SIP protocol exclusively and another two partners use both H.323 and SIP protocols in a mixed manner in order to implement their services. 75% of project participants have not yet deployed a VoIP service.

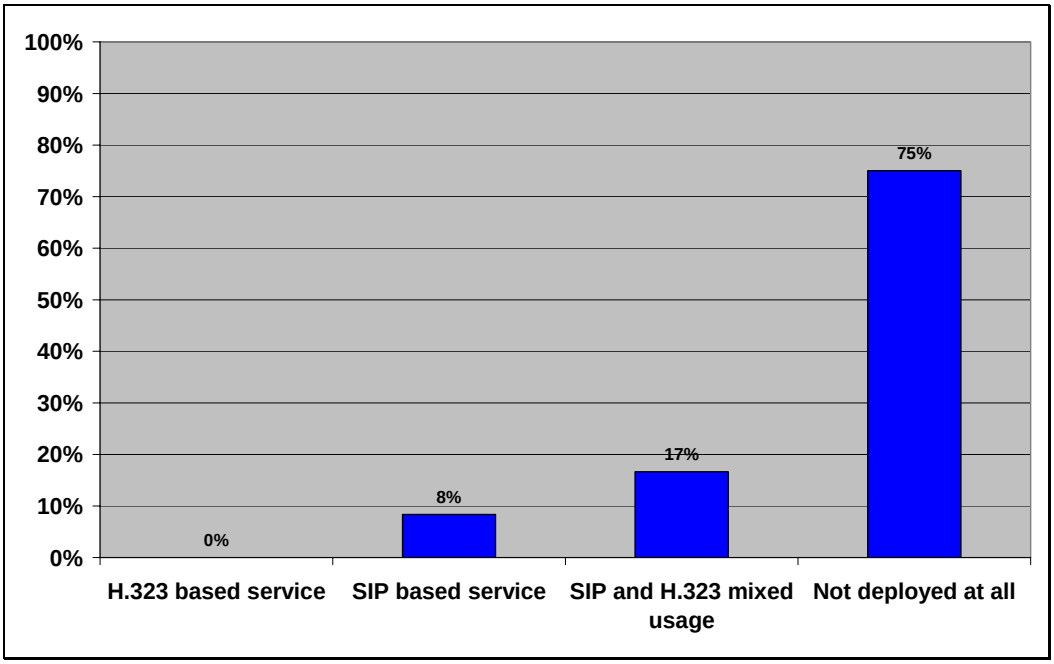

Figure 31: VoIP deployments in partners' network and used protocols

According to survey results current deployment of VoIP services is not significant but this can be an advantage if service is deployed at SEEREN level so that support for users of VoIP PBX systems can be managed with unified approach. Additionally, it is easier to create a network policies concerning QoS, NAT, traffic filtering, security, etc. in case of a single software solution distributed in every partners location as well as creating a dialling schema which can ensure scalability, if particular NREN decides to expand the number of users without creating requirements for additional hardware for other SEEREN partners.

3.8.2. Need for SEEREN level Voice over IP service support

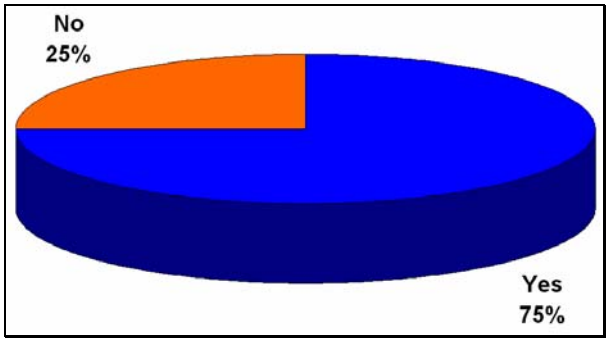

Figure 32: Would you like to have SEEREN2 level VoIP support?

Survey clearly shows that demand for VoIP support is high. Choice of stable open source solution with constantly updated documentation is crucial. Asterisk PBX can deliver stable service to the network since it has been already tested as part of SEEREN2 project and a choice of single open source software solution can ease support issues. In order to deploy service easily, preconfigured distributions with GUI included, can be found.

3.9. IP based videoconference

Videoconference makes it possible for groups of people and individuals on separate locations to meet interactively. At the most basic level, the videoconference is limited to transmission of video and audio from one location to another. Videoconference is a bi-directional communication between two or more geographically separated persons using tools for transmission of video and audio signal. It consists of video, audio and data as well as transmission media, which can be analogue telephone network or POTS, ISDN network, LAN network or Internet network. [4]

A simple videoconference can be implemented in many ways both based on international standards or proprietary solutions. Providers must always prefer standard based solutions in order to allow using of diverse network and terminal equipment ensuring independence from certain manufacturers. However, there are many quality computer based solutions that use proprietary protocols and methods to connect two or more participants of a videoconference. Apart from the fact these applications provide many smart collaboration features from audio/video transmission to data and desktop sharing, it is very difficult to bring them to a national scale.

Standard based IP videoconference can use two different protocols:

- H.323: ITU-T protocol suite designed for Voice over IP and IP based videoconference;
- SIP: IETF open standard for IP based audio and video transmission.

A short introduction of these two protocols can be found in section 3.8, where Voice over IP is discussed.

Almost all professional quality videoconference equipment is H.323 compatible, but SIP is also supported in most products. A transition from the world of H.323 to the world SIP is being undertaken in these years. SIP based videoconference implementations are a bit of immature, so today's production videoconferencing services are still based on H.323 mainly.

A scalable, modern videoconference service can be implemented using gatekeepers, Multipoint Control Units and videoconference terminals (professional hardware based terminals, software based conferencing systems, softphones, etc.).

Hardware based videoconference systems use a special purpose built processors (audio/video DSPs) for encoding and proper transmission of audio and video between two or more terminals connected to the Internet. In this case, the quality of audio and video is significantly higher as with software based videoconferencing systems, since the number of transmitted frames per second is significantly higher together with an improved picture quality (i.e. sharpness, colours, etc.). In addition, hardware based terminals have special peripherals providing a higher level of videoconference control and participation: special echo cancelled microphones, remote control, OSD menu and controllable quality camera, many video and audio inputs/outputs. Advantages and disadvantages of hardware based systems are:

- Better video and audio quality than software-based systems;
- Higher level of conference control and participation;
- Can serve up 10-15 people in the same room (automatic camera, zoom, etc.);
- Data sharing;
- Usually very expensive.

There is a high number of hardware-based videoconferencing system products and vendors available (e.g. Polycom, Radvision, Tandberg, VCON, etc.). [4]

Software-based videoconferencing systems are equipped with a simple video camera, which is attached to an USB or an IEEE-1394 port, or has its own desktop video capture card for capturing video from the camera. It uses the computer's main CPU for encoding and transmission of video and audio data to other terminals connected to the Internet, which requires very high CPU load. Advantages and disadvantages of software based videoconference systems are:

- Inexpensive, a personal computer is needed with a high performance CPU;
- Often the only extra equipment needed is a camera, and a software based videoconference client;
- Software clients may have shared whiteboard, chat, and file transfer;
- Offers low-quality video of participants, especially on low-end computers;
- Limits the audience size to 1-2 persons as a maximum (due to manual camera focus and unmovable camera unit);
- Less control over the peripherals (e.g. camera is not controllable);
- According to experiences software clients often implement standards in a wrong way, thus not being compatible with manufacturers' equipment.

A Multipoint Control Unit (MCU) is considered as a very high importance network infrastructure unit in the world of videoconferencing. An MCU is capable of establishing multipoint videoconferences allowing 3 or more participants to share the same conference and interact with each other. An MCU device is responsible for handling many point-to-point video calls and distributing video data among the participants connected to the same conference. This requires audio and video switching and mixing capabilities supported by purpose built processors (DSPs). The basic functions of an MCU are:

- Hardware based in order to provide a reasonable capacity;
- Can include gatekeeper and gateway (e.g. ISDN) services;
- Voice Switched conferences: the participant speaking can be seen on the screen;
- Continuous Presence: participants see a split layout allowing more participants on one screen;
- Handling high number of parallel conferences;
- Chair Control: conference chair person can control the conference;
- Transcoding: an MCU can fully transcode video and audio streams if an endpoint is not capable of receiving the streams that other endpoints are sending;

- IVR: interactive voice response based control using DTMF signals;
- Hardware based MCU can be extremely expensive.

There is a range of hardware (Codian, Polycom, Radvision and Tandberg MCU systems) and software-based MCUs.

In order to help H.323 videoconference users to dial and find each other, research and education community has formed a so called Global Dialling Scheme (GDS), providing the same international dialling facilities that PSTN networks can provide. GDS consists of a number of redundant gatekeepers spread all over the world for handling and controlling world zone 00. Countries connecting to this GDS gatekeeper network are allowed to use and maintain their national number space for IP based H.323 devices. For more information, see: http://www.wvn.ac.uk/support/h323address.htm.

Apart from the solutions detailed above, we must have a note on other systems being used in the academic and research community. A rather popular computer based application suite is the so called MBONE tools package, which uses IP multicast for audio and video transmission over the internet. MBONE tools include audio and video conferencing applications (rat and vic), session manager (sdr), whiteboard tool (wb) and many else. Although these tools use a proprietary way of multimedia transmission, they are free, open source and available for most operating system platforms (e.g. Windows, Linux, FreeBSD, Solaris, etc.).

Another videoconference system being very popular among researchers and academic users is VRVS (Virtual Room Videoconferencing System, http://www.vrvs.org). VRVS provides a web based mechanism for virtual meeting room reservation, realtime conference management and user authentication. The VRVS infrastructure consists of so called reflector nodes located all over the world allowing a distributed, load balanced functioning. VRVS makes possible to connect both using MBONE tools and H.323 based videoconference terminals by relaying at reflector nodes thus providing a bridge between two separated worlds of videoconferencing.

The Access Grid (AG, http://www.accessgird.org) videoconference system is very similar to the VRVS system, created by the high performance computing research community. AG is also based on the MBONE tools suite but it doesn't allow H.323 compatible terminals/clients by default. However, it's possible to make connection between VRVS and AG systems rather easily.

3.9.1. Videoconference service deployment

The diagram below presents the current IP based videoconference service deployments, related plans to start such a service in the near future and the proportion of partners not being interested in videoconferencing..

33% of partners have already deployed videoconference in their networks, 17% plan to introduce the service in a one year timeframe and another 33% of them plan to establish it later. One partner (8%) thinks that there is not chance to introduce videoconference service into its portfolio in the foreseeable future due to low network capacity. Only one partner (8%) showed no interest in videoconferencing at all.

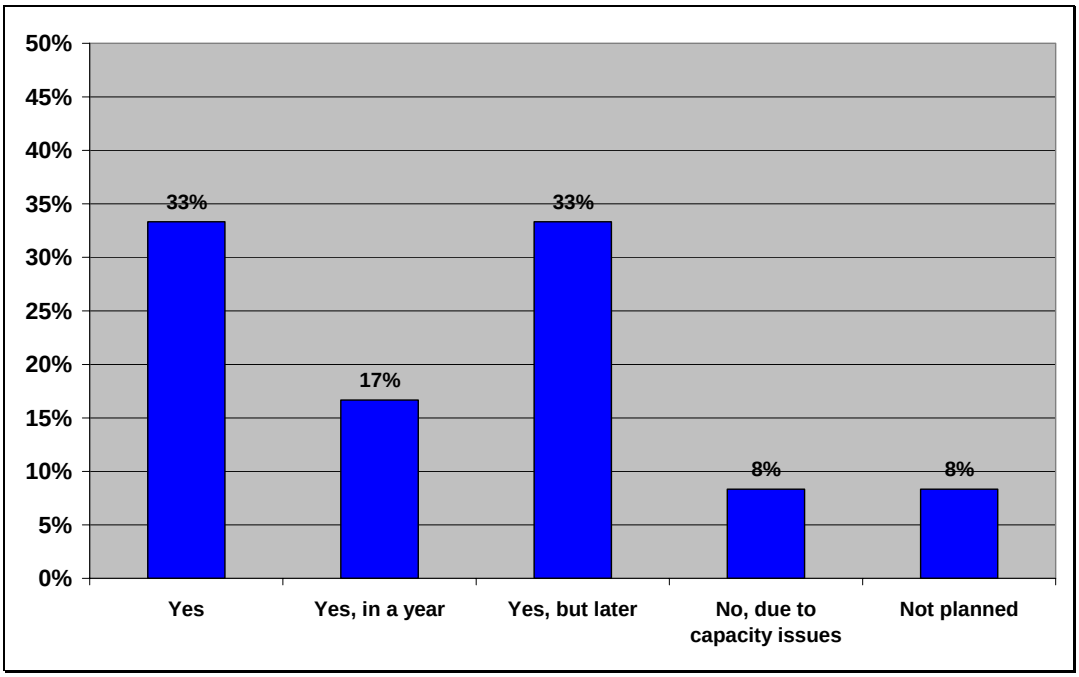

Figure 33: Videoconference service deployments in partners' networks

3.9.2. Videoconference protocols usage

As videoconference industry is in the phase of transition from the H.323 protocol to the less complicated and more promising SIP protocol, it's very interesting to see what directions are taken in the SEEREN2 community. Only 17% of the project partners are using exclusively the H.323 protocol, another 17% are using both H.323 and SIP protocols in a mixed manner. Although SIP based videoconference implementations are rather immature, these partners have already started experimenting in order to get well prepared when SIP implementations turn to be production quality. 8% of partners also indicated MBONE tools based videoconferencing usage, which surely incorporates VRVS and Access Grid usage.

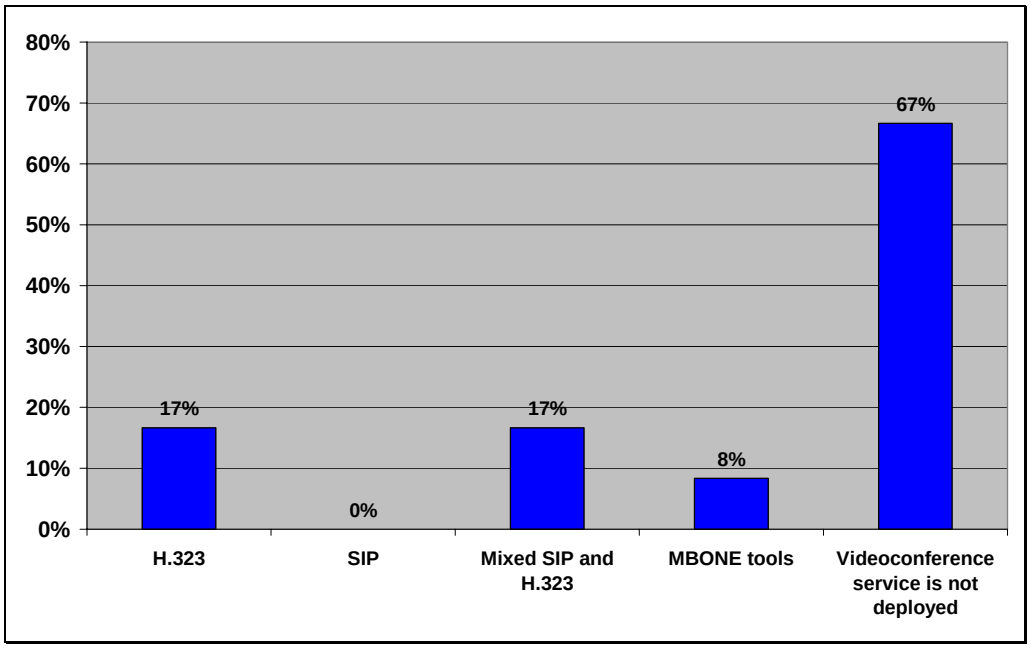

Figure 34: Videoconference protocols usage

3.9.3. Need for SEEREN level videoconference support

The aim of this survey question was to form an overall view on partners' expectations from SEEREN2 project in the field of videoconference. Nearly 60% would require a SEEREN2 level multipoint videoconference unit, slightly more than 40% think that a SEEREN2 gatekeeper would be a good idea. One third of the responses indicated a need for GDS connectivity through the SEEREN2 network. At last, none of the partners thought that there is no need for support from the project.

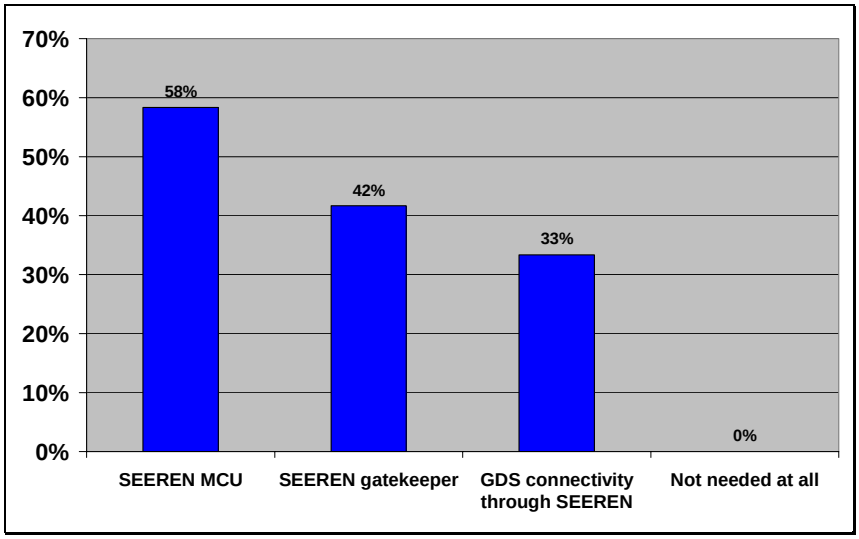

Figure 35: What kind of videoconference support would you require from SEEREN2?

Other individual comments given by partners:

- SIP server/registrar would be needed;
- Asterix PBX deployment would be desirable;
- Asterix PBX to all partner sites.

3.10. Streaming and Video on Demand

Video streaming or multimedia streaming is one of the technologies that are a foundation for many advanced internet services and applications being in use today or planned for the near future. Streaming technology is about one way transmission of audio, video and possibly other content (so called "rich media") to an end user having a personal computer and an internet connection. The very basic ideas of streaming are:

- Extend the number of participants of an event with passive participants through the internet (e.g. conference, seminar broadcast);
- Web radio and television broadcast;
- Make archive video files available on an on demand basis (Video on Demand);
- Enable participants to consume content in a new way (several simultaneous streams giving user choice of which camera to watch or to have user-initiated instant replay).

The direction of streaming of audio and video data is exclusively from the server to the user, and never the other way. It is very important to mention, that streaming has nothing to do with videoconferencing, somewhat these two very different technologies are often mixed verbally.

General elements of a streaming system are:

- Video signal(s) (i.e. camera, or any video source) and audio signal(s);
- Encoder: computer capturing/digitalizing (depends on the source) video signal and encodes it into desired digital format using various audio and video codecs;

- Media server(s): the encoder computer transmits digitally encoded signal to one or more media servers. Media servers are responsible for distributing audio and video streams to a large number of streaming clients (i.e. media players) connecting usually by using unicast or multicast transportation;
- Client(s): media players running on personal computers, PDAs, mobile phones, etc.

One could also include the transport network and its quality of service as an element of the streaming system. Most of the related issues are covered by ITU-T recommendations G.1000 (Communications Quality of Service: A Framework and Definitions) and G.1010 (End-user multimedia QoS categories). The most important QoS parameters for streaming are:

- Delay – including the time to establish the service;
- Delay variation – eliminated by buffering (at the expense of adding additional fixed delay);
- Information loss – includes loss due to bit errors, out-of-order delivery or packet loss, as well as the loss due to any other reason (e.g. use of low bit rate or low quality codecs).

When transmitting audio and video codec data over the Internet RTP (Real Time Protocol) and RTCP (Real Time Control Protocol) IETF protocols are used together with UDP protocol as an obvious framework for realtime data transmission. However, HTTP protocol is also very often used for TCP based streaming.

Most widely used codecs for streaming applications:

- H.261 / H.263 / H.264 (ITU-T video codecs);
- MP3;
- MPEG-2, MPEG-4;
- OGG Vorbis (audio codec designed for OGG container format, patent free, based on open standards);
- QuickTime (Apple proprietary);
- RealMedia (RealNetworks proprietary);
- Windows Media Video (Microsoft proprietary).

Most frequently used containers for streaming media are:

- MPEG-TS (MPEG Transport Stream);
- RealMedia (RealNetworks - proprietary);
- ASF (Microsoft - proprietary);
- QuickTime (Apple proprietary);
- OGG (Patent free container format based on open standards).

Control protocols also play a key role in accessing the content stored at media servers using streaming capable media players. Control protocols are used mainly for requesting appropriate media stream(s) from the server (i.e. by providing an URL to the server), for negotiating basic network transmission parameters (e.g. such as transport protocols (TCP/UDP), port intervals, etc.) and for providing description of each stream or substream (i.e. several audio and video channels) encoding in order to identify codecs to be used by the media player. The most often used streaming control protocols are:

- HTTP: often used for TCP based streaming when firewall traversal or proxy usage is important. Media player connects to a HTTP URL and can access the stream through the web server, which is basically a simple file download due to the nature of HTTP protocol;
- MMS (Microsoft Multimedia Streaming / System): Microsoft's proprietary streaming protocol used with Windows Media Player and Windows Media Services;
- RTSP (RealTime Streaming Protocol): IETF's open protocol, described by RFC 2326. RTSP is a client-server multimedia control protocol, designed to address the needs for efficient delivery of streamed multimedia over IP networks.

When giving an overview on streaming control protocols, it is also very important to mention SDP (Session Description Protocol) IETF protocol, which is a general purpose text based protocol to describe multimedia streams for session announcement. This information includes session name and purpose, media codec information (audio and video), session addresses and ports, etc. SDP is used mostly by RTSP, SIP (Session Initiation Protocol) and SAP (Session Announcement Protocol) protocols.

3.10.1.Streaming and Video on Demand services deployment

One quarter of responding partners have already deployed streaming or Video on Demand services in their networks. 17% are planning to introduce it in a one year timeframe, another 33% have the intention to do it later. 17% of them lack network capacity for such a demanding service, 8% are not interested at all.

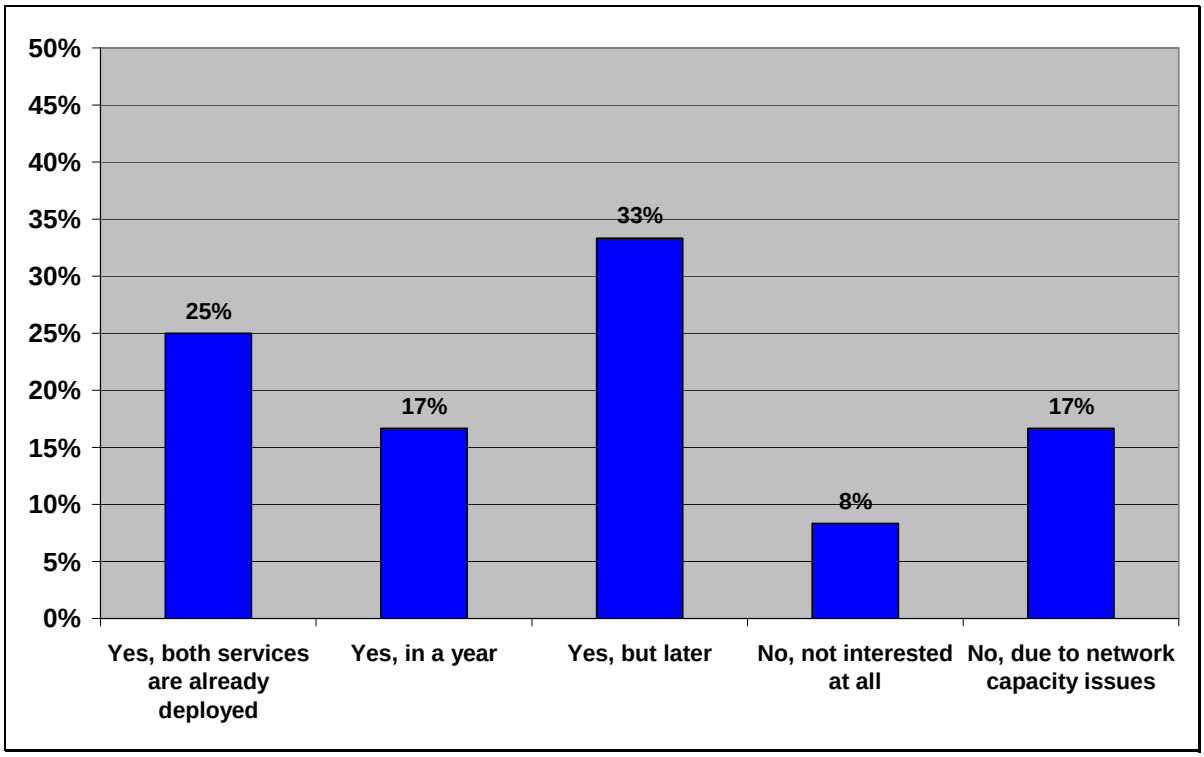

Figure 36: Streaming and Video on Demand service deployment status

As one can see, all but one partner (8%) is interested in streaming and VoD. There are two partners (17%) that indicated network capacity issues as the main deterrent from implementing these services. As the aim of the SEEREN2 is, in part, to solve such network problems for partners, we can conclude that 92% of partners are willing to use streaming and VoD on national and international (SEEREN2) level. Moreover, one quarter of partners are already using these services which provides stable base for technology know-how transfer to less experienced partners in the region.

3.11.Basic user-level services

This topic covers basic user-level services and their adoption among SEEREN partners.

3.11.1.Web hosting services

World Wide Web is probably the most used Internet service at the present and is considered as one of the most important means of electronic information dissemination. In the last couple of years there is a notable trend of transition from text-based to multimedia representation of information as well as using the web as two-way communication tool. Rough overview of present web hosting infrastructure among SEEREN partners reveals that practically all of the partners use Apache web server and most of the installations are on Linux based systems. This setup enables the partners to offer royalty-free web hosting and virtual hosting to their member institutions or end-users.

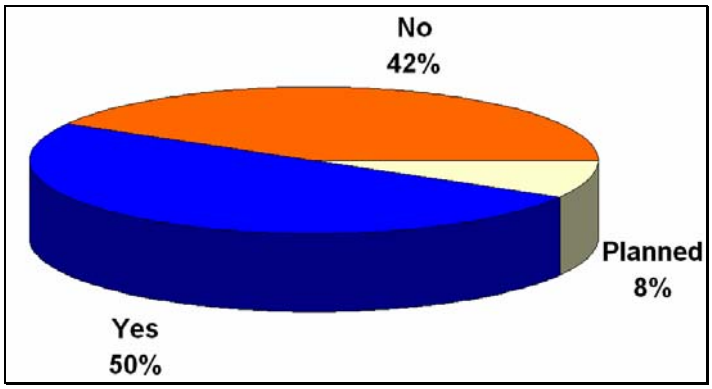

Figure 37: Does your organization provide web hosting services to its members/users?

Exactly half of the partners already offer web hosting services to their members or users, with another 8% planning to do so in future. There are 42% of the partners are not offering and are not planning to offer such services to potential users.

3.11.2.FTP services

File Transfer Protocol (FTP) is one of the oldest network services and is mainly used for large file transfer as well as setting up file repositories. FTP servers can be anonymous (allowing unauthenticated users with restricted rights) or they can demand valid user credentials to be provided. There are also public FTP severs that are accessible by general public as well as restricted servers intended for internal use within, for example, one institution.

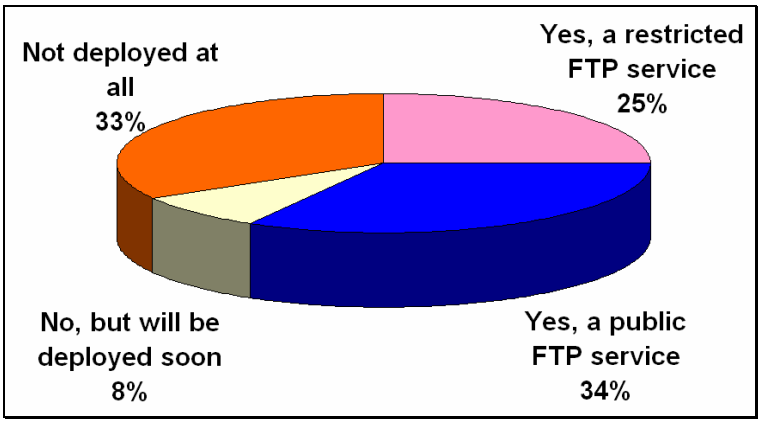

Figure 38: Does your organization provide FTP services to its members/users?

One third (33%) of the partners have no FTP service and no plans to introduce it, 8% are planning to introduce it in foreseeable future, while 59% offer some kind of FTP service. Out of those that do offer FTP, 34% offer it as a public service and 24% offer FTP in a restricted form.

3.11.3.Mail services

E-mail as a service predates Internet and is considered as one of the cornerstones of modern communication. In a typical setup, mail services can be offered in bulk or individual manner. Bulk mail services cover transferring of the mail for the needs of whole institutions, while individual offer services on a per-user basis most often through virtual mail servers. Another very important aspect of mail service are mailing lists that represent one of the most often used means of information exchange between a group of people. Rough look at SEEREN partners email servers reveal that almost all of them are based on some sort of Unix (Linux, *BSD, Solaris) with Sendmail being the most frequently used one with others including QMail, Postfix, Exim, etc.

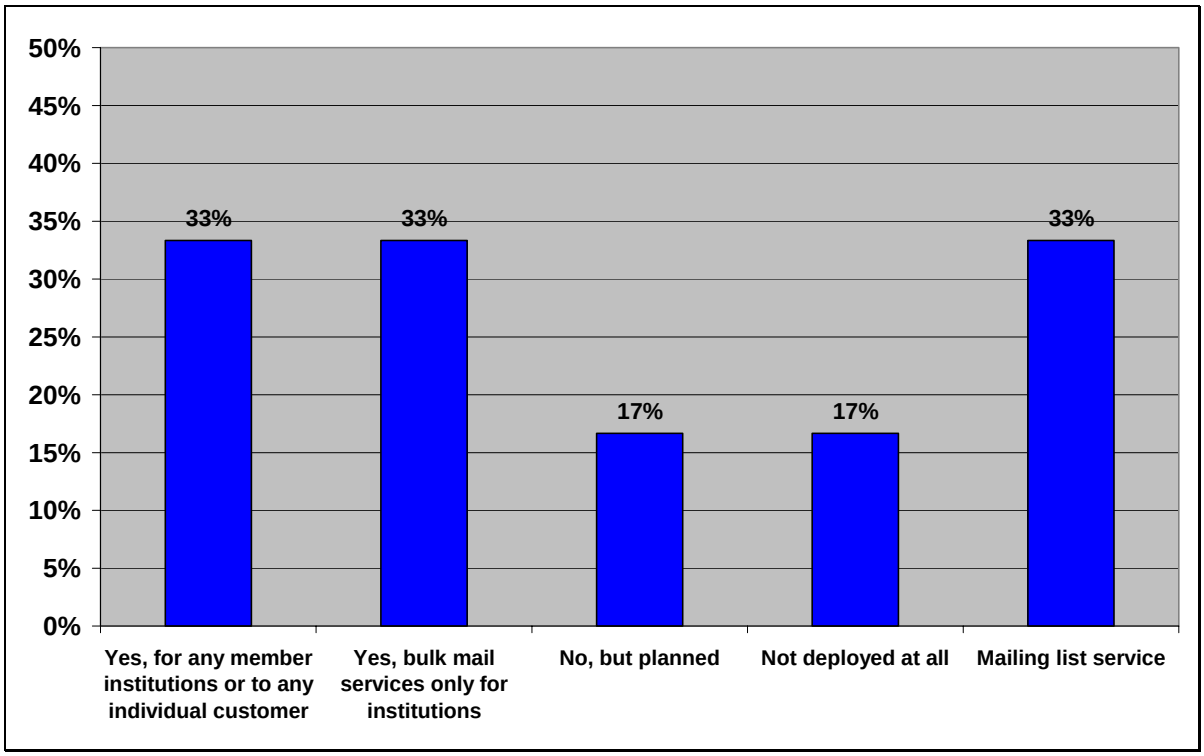

Figure 39: Does your organization provide mail services to its members/users?

Only 17% of the partners do not offer and have no plans of offering the mail service to their users. Another 17% have no present mail services but are planning to offer them. Two thirds of partners do offer mail services with one third offering it for individual members or end-users and one third for bulk email services only. One third of all partners offer mailing list services to their users.

3.11.4.Network Time Protocol (NTP) service

Network time protocol is often overlooked, but its importance should not be underestimated. This service enables huge number of hosts to have synchronized time which is very important in various fields (GRID computing, security, etc). Depending on the accuracy of the reference clock, NTP servers are classified as Stratum 1, Stratum 2 and Stratum 3, counting from more to less precise. It is common practice for networks to have common either Stratum 1 or Stratum 2 server that synchronizes all hosts on the network.

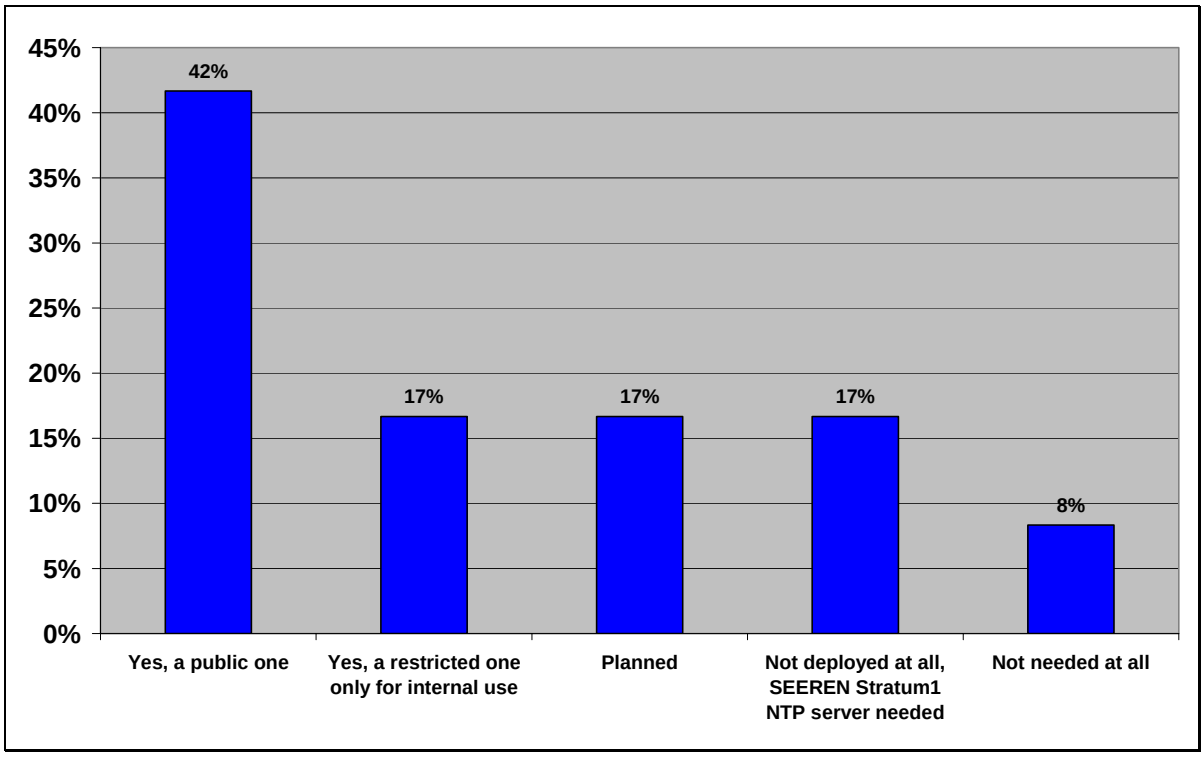

Figure 40: Does your organization provide NTP services?

Only one partner has no need for NTP service while more than a half of the partners (59%) already offer either public (42%) or internal (17%) services. Another 17% are planning to introduce this service with another 17% feel that SEEREN should introduce Stratum 1 NTP server for partners' needs.

3.11.5.Type of Network Time Protocol (NTP) servers

Stratum 1 and Stratum 2 types of NTP servers are present with 40% each among partners with Stratum 3 being used in 20% of the cases.

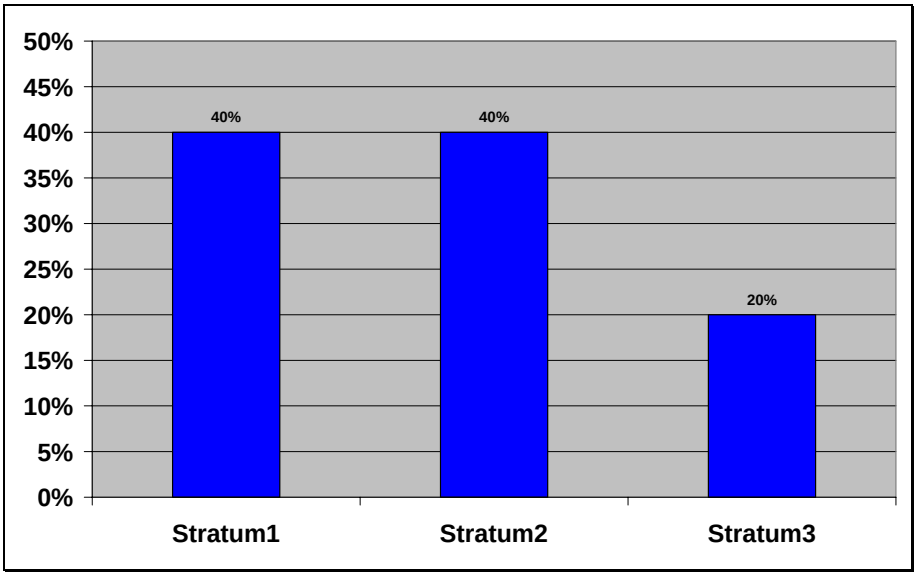

Figure 41: Type of Network Time Protocol servers used in partners' network

3.12. Directory services

With the advent and wider disposition of various internet based applications that need to acquire information on the availability of different services, resources, users, and other objects both in the nearer and wider networking environment, means of clear, structured and consistent data representation about them is needed. That is what directories are used for. So directories represent information management and retrieval systems where different objects are represented by a collection of data as one or more values of a defined set of object attributes. Directories provide the capability of data insertion, data modification and most importantly they provide a highly optimized method for data retrieval. The access to the directory is controlled by some authentication mechanism meaning that different entities that interact with the directory are granted different access rights.
It is important to point out how directories differ from relational database management systems (RDBMS):

- directories provide for very fast read operation, while RDBMS additionally provide for very fast write operations most often transactionaly executed;
- directories comprise of fairly static data, while in contrast RDBMS of dynamic data with frequent and high volume changes;
- directories are hierarchical or tree-like in structure while the data in RDBMS is organized within tables with relations between them;
- directories support a simple search mechanism optimized for speed and efficiency. RDBMSes use SQL which is very powerful access method;
- with directories clients use standard access protocol while with RDBMS systems the vendor shall provide for a suitable driver;
- loosely coupled replication v.s. highly coupled replication with RDBMS with commit operations.

The first general purpose directory standard was X.500 which was developed jointly by CCITT and OSI and defines the DAP – directory access protocol, the information and functional model, the namespace and the authentication framework. This is what is referred as the heavyweight directory access protocol since DAP is a full OSI protocol that contains extensive functionality much of which is rarely used. The implementation of X.500 requires a full-blown OSI stack which has not gained wider acceptance.

On the other part the Lightweight Directory Access Protocol (LDAP) was designed to alleviate some of the burden of X.500. Most importantly it runs on a TCP/IP stack as a transport layer making it available to a wide variety of machines and applications. It has evolved over several versions the last being v3 (RFC3494).

3.12.1. Directory services deployment in partners' networks

One third of partners have already deployed some kind of directory service, 17% are planning to deploy in one year and an additional 25% are also aware of the importance of a directory service and intend to implement the service later. One quarter of partners are not interested at all.

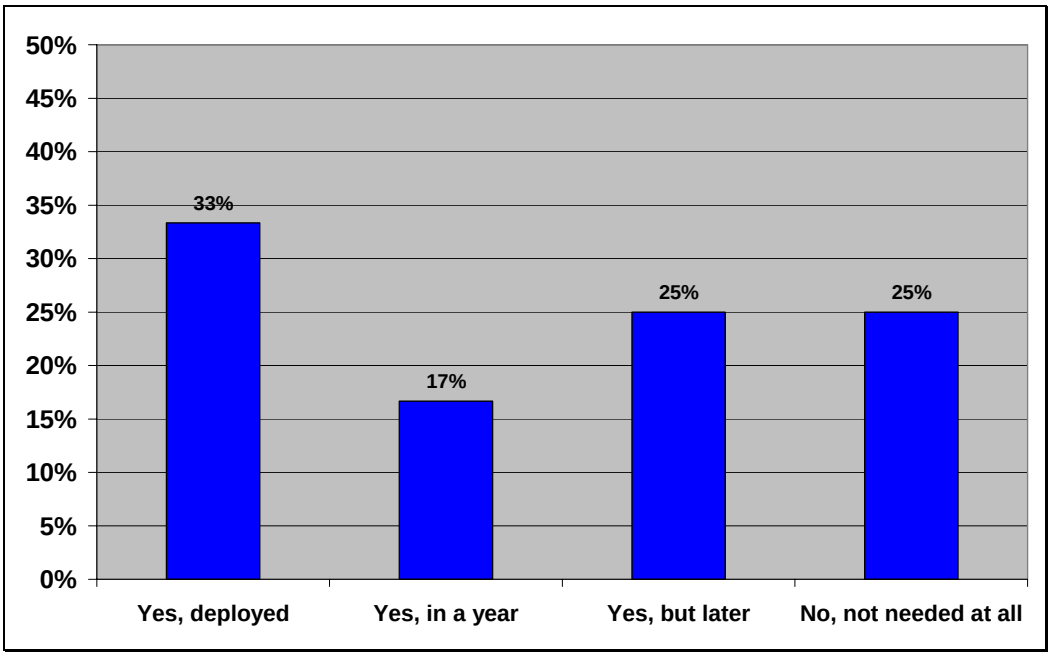

Figure 42: Directory service deployment status

3.12.2.Directory services architecture

Directory services that are being used in SEEREN2 partner networks are based on two different architectures, namely LDAP and Microsoft Active Directory. The latter one is used by 25% of partners that are running a directory service, and LDAP is used by 75% of them.

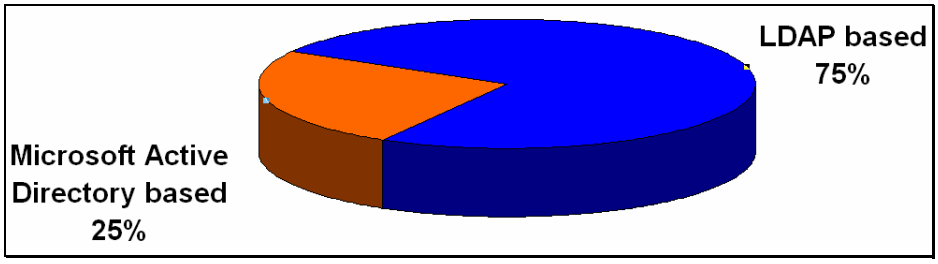

Figure 43: What is the architecture of your directory service?

3.12.3.Eduroam deployment and intention of use

The *Eduroam* service, which stands for Education Roaming, is a RADIUS-based infrastructure that uses 802.1X security technology to allow for inter-institutional roaming.

Being part of *Eduroam* allows users visiting another institution connected to *Eduroam* to log on to the WLAN using the same credentials (username and password) the user would use if he was at his home institution. Depending on local policies at the visited institutions, *Eduroam* participants may also have additional resources at their disposal.

The European countries currently connected to *Eduroam* are Austria, Belgium, Bulgaria, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Ireland, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovenia, Spain, Switzerland and UK. Iceland and Sweden are in the process of joining *Eduroam*. The map on Figure 44 depicts the NRENs that participate in the European *Eduroam* RADIUS hierarchy.

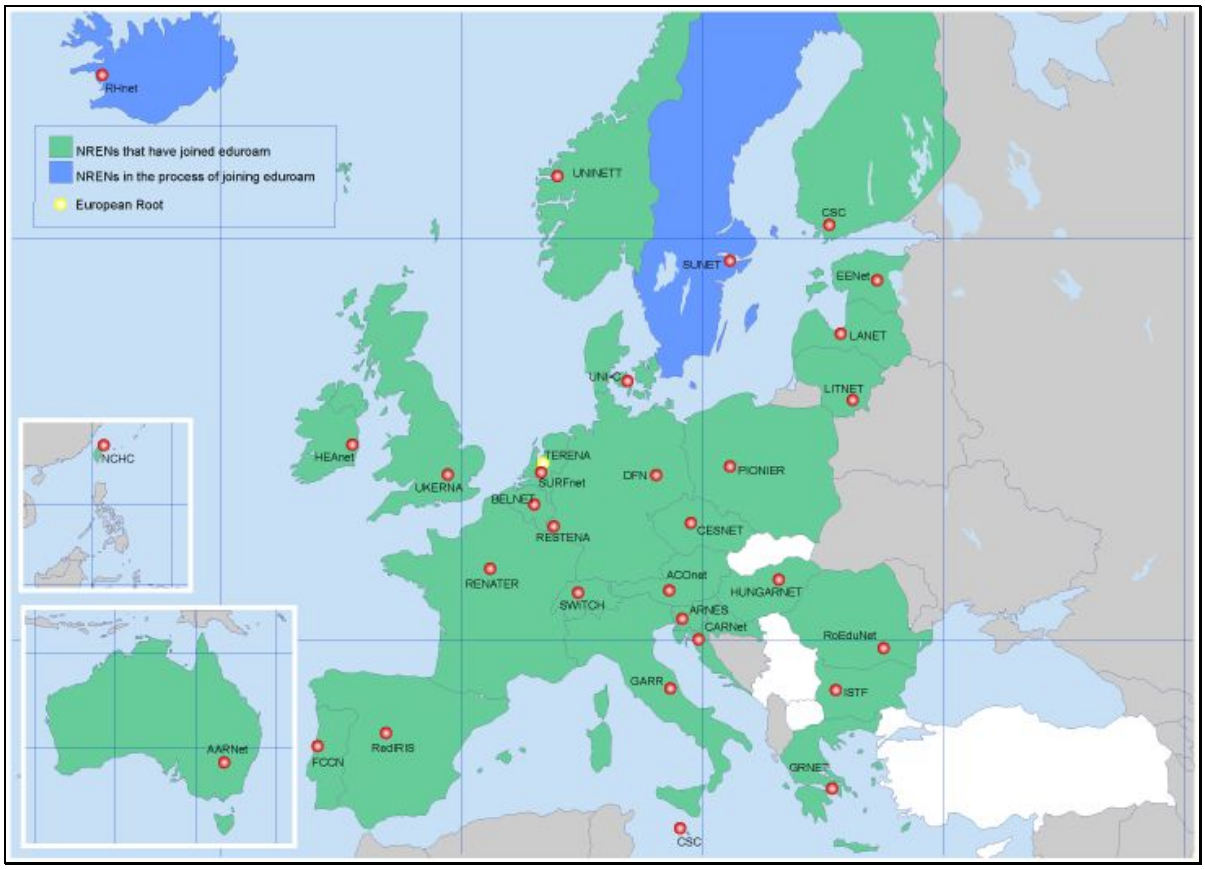

Figure 44: NRENs participating in Eduroam

TERENA provides the European root (yellow bullet). The two servers that provide this service are operated by SURFnet (the Netherlands) and Forskningsnettet (Denmark). In green are NRENs that have already joined. In blue are NRENs that are in the process of joining. The countries in white represent TERENA's members that have not joined *Eduroam* yet.

The non-European countries that are members of *Eduroam* are Australia, China and Taiwan. In the USA, interest in the *Eduroam* has taken hold and as result of this a development approach similar to that in Europe is ongoing.

Some more details about *Eduroam* are available at http://www.eduroam.org/. [2]

At present the *Eduroam* relies on a hierarchy of radius servers, deployed all over Europe. The two most popular types of radius servers in use are:

- FreeRADIUS, available at http://www.freeradius.org/
- Radiator, available at http://www.open.com.au/radiator/

Radiator implements some interesting functionalities, but is a commercial product. FreeRADIUS is a very popular open source RADIUS server, released under the GNU General Public License.

In order to become a member of *Eduroam* each country (NREN) should configure at least 2 national level radius servers and 1 institution level radius server. Furthermore, wireless access points, preferably supporting the 802.1x technology should be deployed at each participating site. A national web site with instructions for end-users on how to make use of *Eduroam* and where it is available is highly recommended.

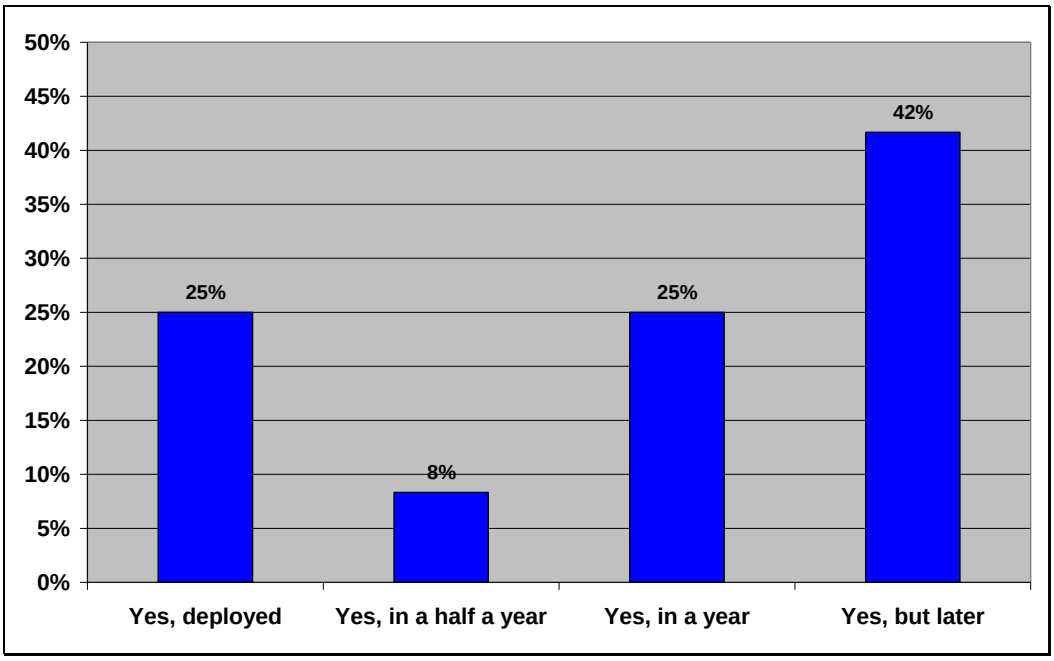

Figure 45: Eduroam deployment status and intention to join the initiative later

The *Eduroam* infrastructure has already been deployed by quarter of project partners', only 8% (one partner) plan to start off the service in the next half year, a quarter in a one year timeframe. A major part (42%) indicated their intention to use the services provided by the *Eduroam* infrastructure, but plan to join later than a year. Negative answer was not registered, which shows a very strong support of *Eduroam* and great recognition of the project.

4. Conclusion

Deliverable D13a “SEEREN2 Services and tools specifications” consolidates the results of the activities A5.1, A5.2 and A5.3. In the context of the aforementioned activities, the consortium setup a longwinded questionnaire targeting in collecting precise data on the implementation status of networking services of the SEEREN2 participating NRENs. The results were gathered and further processed in order to accent the current status of the implementation of the chosen services within the participating NRENs.

In-line with the results of the questionnaire, the outcomes of the feasibility studies were seamlessly integrated. The objective was to evaluate the importance of the services correlating them with the current status of their implementation. Thereby, the consortium is able to shape a concrete overview of the services needed to be further elaborated.

This input is deemed critical for the following technical activities of WP5 that will focus on the implementation of the aforementioned services.

