04-06-2015

Deliverable D3.5 (DN3.2.2)
Annual Report on Campus Best Practice

Deliverable D3.5 (DN3.2.2)

Contractual Date:	31-03-2015
Actual Date:	04-06-2015
Grant Agreement No.:	605243
Activity:	NA3
Task Item:	Task 2
Nature of Deliverable:	R (Report)
Dissemination Level:	PU (Public)
Lead Partner:	CSC
Document Code:	GN3PLUS14-1254-16
Authors:	Jari Miettinen (CSC/Funet), Tom Myren (UNINETT), Tomi Salmi (CSC/Funet), Janne Oksanen (CSC/Funet), Jiri Navratil (CESNET), Miloš Kukoleča (AMRES), Vanessa Pierne (RENATER), Vangel Ajanovski (MARnet), Radoslav Yoshinov (BREN), Carlos Friacas (FCT-FCCN), Vladimir Gazivoda (MREN), Milan Cabak (MREN), Michal Przybylski (CEENET)

© GEANT Limited on behalf of the GN3plus project.
The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7 2007–2013) under Grant Agreement No. 605243 (GN3plus).

Abstract

Campus Best Practice is the name of one of the Tasks (Task 2) in Networking Activity 3, Status and Trends (NA3), of the GN3plus project. The overall objective of the Task is to address the key challenges for European campus networks, organise working groups and provide an evolving and to-the-point set of best practice documents for the community. This deliverable reports on the work carried out in the Task during the second year of the GN3plus project (April 2014 – April 2015) and the results of that work.

Table of Contents

Table of Figures

Table of Tables

Executive Summary

Campus Best Practice (CBP) is Task 2 of Networking Activity 3, Status and Trends (NA3) of the GN3plus project. During GN3plus, nine NRENs took part in this activity: UNINETT (Norway), CESNET (Czech Republic), AMRES (Serbia), CSC/Funet (Finland), RENATER (France), BREN (Bulgaria), FCT-FCCN (Portugal), MARnet (F.Y.R of Macedonia) and MREN (Montenegro). CEENET (Central and East European Networking Association) and GÉANT Association (formerly TERENA, Trans-European Research and Networking Association) also contributed to the task in a supporting role.

The CBP Task's objectives for the second and final year of the GN3plus project were to continue work on Best Practice Documents (BPDs) and to disseminate the results, to encourage NRENs and institutions to work together on developing expertise in best practices and implementing them on campuses across Europe. Work on updating existing BPDs was also planned, to support the deployment of GÉANT services and existing investments.

The CBP groups formed by the task member NRENs continued their activities during the second project year, resulting in the production of 27 BPDs. Several national workshops were held in the member countries. Dissemination continued at national and international events. The workgroup also organised two international workshops and three international training events, which also included workshop sessions. A lighting talk session on CBP was also held at the GN3plus Symposium 2015 in Athens.

The number of BPDs produced during GN3plus exceeded expectations by roughly 100%. This result was due to a slightly higher number of contributions than expected from the NRENs that had originally been part of the CBP task during the GN3 project, as well as a surprisingly large number of contributions coming from the NRENs that joined the task at the beginning of GN3plus. These starter NRENs not only established campus working groups in their own countries, but were also able to contribute to the Task's knowledge base. Some of the BPDs were produced in collaboration by various NRENs. The review process also began on the BPD documents written during the GN3 project, resulting so far in one BPD being updated, while several others were confirmed to be still current.

All planned dissemination activities took place successfully and met expectations both in terms of number of participants and quality. The feedback from each session was used to plan successive events. The task liaised with the other GN3plus tasks and partners in arranging co-located and back-to-back events, and the resulting knowledge dissemination and cooperation contributed towards supporting the deployment of eduroam and identity federations, as well as raising awareness of the new GÉANT connectivity services and best practices in IT security.

1 Introduction

Campus Best Practice is Task 2 of Networking Activity 3, Status and Trends (NA3), of the GN3plus project. The task is based on the previous work carried out for the GN3 project by NA3 T4, led by UNINETT [DN3.4.1,1, DN3.4.1,2, DN3.4.1,3, DN3.4.1,4]. The origins of the Campus Best Practices lie in the UNINETT GigaCampus project [GIGACAMPUS]. The importance of the development of campus networks and services was also raised in the EARNEST report [CampusIssues]. The experiences of the GigaCampus project and the EARNEST report recommendations greatly influenced the establishment of the Campus Best Practices task as part of the GÉANT project. Further reasoning for applying the CBP method within NRENs can be found in AMRES's document on the subject [AMRES-CBP].

This deliverable reports on NA3 T2 for the second year of the GN3plus project.

The objectives of NA3 T2 are to address the current challenges for campus networks through:

- A series of best practice documents written in collaboration groups.
- Workshops and training events.
- Dissemination of best practices and best practice documents.

The work of the task aims to promote cooperation between peer groups, encourage the development of expertise within the NRENs and the community in general, and support the deployment of best practices in the campuses.

The following NRENs are involved in the task: AMRES (Serbia), BREN (Bulgaria), CESNET (Czech Republic), CSC/Funet (Finland), FCT-FCCN (Portugal), MARnet (F.Y.R. of Macedonia, hereafter Macedonia), MREN (Montenegro), RENATER (France) and UNINETT (Norway). In addition, GÉANT Association and CEENET participate in a supporting role.

NA3 T2's approach and working methods are described in Section 2 of this report. Section 3 summarizes its key results, while Section 4 includes national summaries of CBP activities in the member countries. Section 5 summarises and draws conclusions on the work carried out. The Appendices include a list of the national campus working groups (Appendix A), abstracts of the best practice documents written during GN3plus Y2 (Appendix B), a list of workshops organised at the national level (Appendix C) and short programs of the international workshops and training events held by the task (Appendix D).

2 Approach

2.1 Technical Focus Areas

The Task team inherited six work areas from the GN3 mother task. The focus areas were discussed and negotiated in the task establishment phase. After lengthy debate, the workgroup settled on six areas of focus, essentially identical to those for GN3. However, although the only visible change may be the internal reference numbering, there have been important shifts in the areas of interest within the focus areas themselves. Table 2.1 gives an overview of the focus areas and the NRENs that are contributing to them.

Area		AMRES	BREN	CESNET	CSC/ Funet	FCT-FCCN	MARnet	MREN	RENATER	UNINETT
Ref	Name									
0	Task management and dissemination	√	√	√	√	√	√	√	√	√
1	Physical infrastructure: Virtualisation and datacentre	√	√		√		√			
2	Real-time communications and AV	√		√		√			√	
3	Campus networking: LAN and IPv6	√		√	√	√			√	√
4	Wireless		√		√		√			√
5	Network monitoring	√		√			√	√		√
6	Security	√		√	√			√	√	√
	Number of technical focus areas:[1]	**5**	**2**	**4**	**4**	**2**	**3**	**2**	**3**	**4**

Table 2.1: List of focus areas applicable in GN3plus Y2

[1] Not counting area 0 (task management and dissemination).

A brief description of the focus areas follows alongside the icons identifying each area.

Physical infrastructure. This area addresses the requirements for generic cabling systems on campus, both fibre and twisted pairs. The requirements of the infrastructure in telecommunications and server rooms are also dealt with. This includes power supply, ventilation and cooling, and fire protection, as well as general Information and Communications Technology (ICT) room-plan guidelines. Recommendations for building an audio-visual (AV) infrastructure in lecture halls and meeting rooms are also covered virtualisation technologies to this area.

Campus networking. This area deals with the campus network itself, and with the routers and switches as its basic building blocks. Requirements for both Layer 2 and Layer 3 are covered. Recommendations for a redundant design are given. Metropolitan area networking and virtual switching is covered. There is a particular emphasis on guidelines for implementing IPv6 on campus. Lightpaths on campus are also dealt with.

Wireless. This area focuses on the wireless infrastructure on campus. Radio planning, design of the wireless network, security considerations, including the implementation of IEEE 802.1X are covered. eduroam requirements and Remote Authentication Dial-In User Service (RADIUS) setup are dealt with. Cookbooks for controller-based implementations are given. Legal aspects are examined.

Network monitoring. This area focuses on network monitoring of the campus network. General requirements and framework conditions for monitoring are given. NetFlow/Internet Protocol Flow Information Export (IPFIX) analysis is covered. Security monitoring, anomaly detection and behaviour analysis are also dealt with. Particular considerations for IPv6 monitoring are given. References to a number of open source tools, many of which have been developed within the GÉANT community, are given.

Real-time communications. This area recommends infrastructures for real-time communications with an emphasis on open standards and Session Initiation Protocol (SIP) in particular. The infrastructure itself should be media transparent, coping with voice, video, messaging, document sharing, and shared presence. Particular focus is given to Voice over IP (VoIP) and IP telephony. Best practices from a number of NRENs in Europe are given. Security concerns are discussed and implemented solutions are recommended. Performance issues are also covered.

Security. This area deals with security considerations for the campus network. A template for a security policy is proposed, based on core principles, as defined in International Organisation for Standardisation / International Electrotechnical Commission (ISO/IEC) 27002. An ICT security architecture for higher education is recommended. Traffic filtering technologies are discussed and general applications are recommended. Adoption of digital certificates in a public key infrastructure (PKI) is covered. Secure Domain Name System (DNSSEC) is also dealt with.

2.2 Writing Process for Best Practice Documents

The basic writing process for the best practice documents has continued unchanged from the GN3 project. The working groups are coordinated by the NRENs in their respective countries. The same working method has been adopted by the new NRENs that joined the work at the beginning of GN3plus. Appendix A gives an overview of the active working groups within each area in the contributing countries. Figure 2.1 shows the BPD workflow.

Figure 2.1: Writing process workflow for best practice documents (BPDs)

Some of the NRENs which joined later have preferred to write their initial versions of the best practice documents in English and not in their native language. As a related new development, task members have peer-reviewed the BPDs of other NRENs. These peer reviews have been aimed at finding some additional viewpoints and use cases, as the original documents are already quite accurate in the details. Peer reviews are undertaken once the English language documents are available, whether in the original or in translation where needed.

In addition, some NRENs that share work areas already liaised during the very early writing phase of the BPDs. It is expected that in this way all partners involved will be able to benefit, as their fields of expertise complement each other. For example, RENATER and CSC/Funet collaborated on DNS security during GN3plus year Y1 and both delivered a BPD.

Recently, work on a preliminary joint initial version of a BPD was started in cooperation between UNINETT and SURFnet, even though the latter is not part of NA3 T2 as such, in order to evaluate the writing process, which again takes place in English.

2.3 Translation into English and Publication

An internal process and a bookkeeping system for the translation service was used in order to clarify procedures for all partners and enable those involved to manage the translation process, so that the translation of individual documents can now be easily carried out.

The GN3 approach to translation and web publishing was maintained by the NA3 T2 team for GN3plus; once a document is approved at the national level, it is translated into English and published on the GÉANT website [GÉANT-BPDs].

Several short articles on the CBP workshops and training events have also been published in the GÉANT CONNECT magazine. The task poster and fliers were displayed and distributed at all events, together with supplementary material from the GÉANT project. New documents are announced when they become available through a mailing list [BP-Announcements]. A new website was designed and set up under the GÉANT services web portal (see Figure 2.2). The new website contains the published BPDs and white papers. In addition, it provides services to visitors who are seeking information about the task activities. Upcoming events and new BPDs are highlighted.

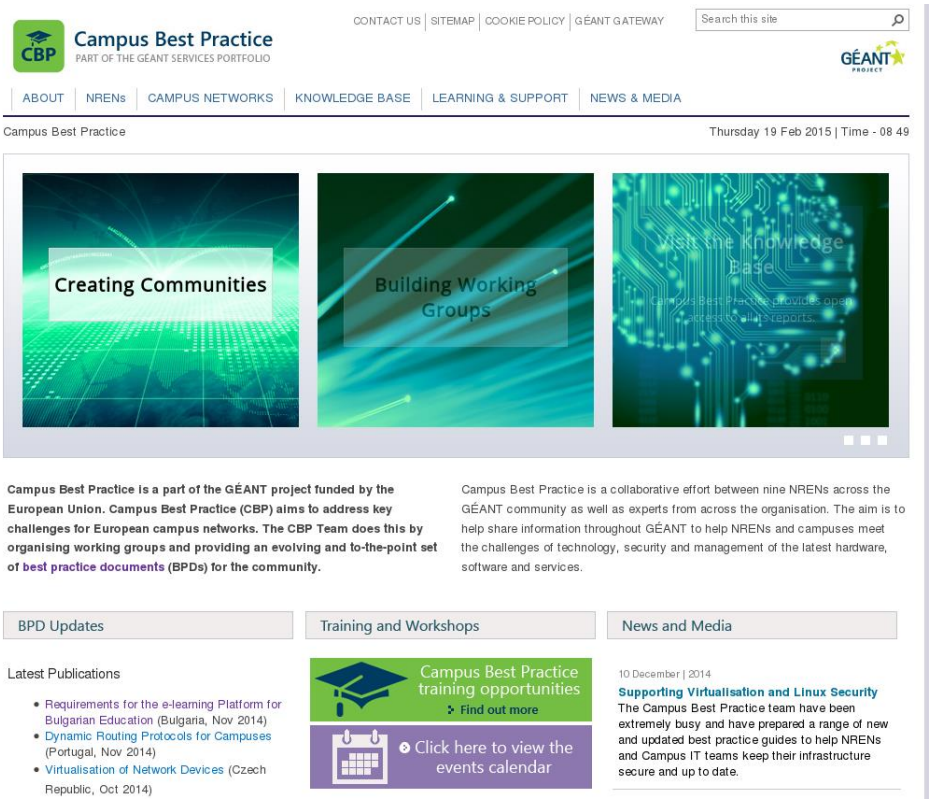

Figure 2.2: New campus best practices website at services.geant.net.

2.4 Task Management

The workgroup continued to use the procedures established during year 1 of the project, such as the technical focus area model (Section 2.1), and followed the two-year plan of action summarised in the official NA3 T2 GN3plus Project Initiation Document (PID).

Monthly videoconference meetings, where work is reported and topical items discussed, ensure cooperation within the workgroup. Monthly progress and milestones achieved are documented in monthly reports made available on the workgroup intranet. This reporting mechanism provides an information base which is utilised for the project's administrative monthly and yearly reporting. The task has a mailing list for official announcements, information exchange and discussion. IMS tools and videoconferencing are used quite frequently as needed.

NA3 searched for liaisons and cooperation partners both inside the GN3plus project and among the community. The aim was to join efforts and resources in completing major tasks, such as, for example, for organisation of the training events. Cooperation also makes it possible to reach wider audiences, for example by making new contacts in co-located events.

3 Results

NA3 T2 is producing a growing toolkit of best practice documents (BPDs). Dissemination efforts are also of complementary importance as the Task needs to get the message out to campus network managers across Europe. In this process, it is important to establish contact with more NRENs and inform them of the Task's results and working methods. This is achieved through various methods: talks at conferences, direct dialogue with NRENs, workshops in new countries, and European-level expert workshops and training events.

These activities are summarised in the sections below, followed by a short progress report from each of the member NRENs.

3.1 Best Practice Documents

During the second project year, 27 best practice documents (BPDs) were completed, 10 of which have already been published, having gone through the translation and editing process. Table 3.1 shows the BPD distribution between the focus areas. Table 3.2 provides a more detailed list of all documents. The abstracts of the BPDs can be found in Appendix B.

Area		Documents completed
Ref	Name	
1	Physical infrastructure: Virtualisation and datacentre	4
2	Real-time communications and AV	4
3	LAN and IPv6	10
4	Network monitoring	2
5	Wireless	3
6	Security	4
	Total	**27**

Table 3.1: Overview of documents completed in English in each area in GN3plus Y2

No.	Document	NREN	Area	Completed
1	Using Windows NPS as RADIUS in eduroam	UNINETT	Wireless	Feb 2015
2	NAT44 Address Translation	UNINETT	Wireless	Apr 2015
3	Infrastructure for active and passive measurements at 10 Gbps and beyond	UNINETT	Network Monitoring	Apr 2015
4	Physical infrastructure for digital exams	UNINETT	Physical Infrastructure	Mar 2015
5	Traffic Analysis and Device Management based on NetFlow data in MREN	MREN	Network monitoring	Mar 2015
6	Building an identity repository	RENATER	Security	Mar 2015
7	Efficiently run a mailing list server	RENATER	LAN and IPv6	Mar 2015
8	ToIP interconnection	RENATER	LAN and IPv6	Mar 2015
9	Creating a university CERT	RENATER	Security	Mar 2015
10	Best practices for the infrastructure of a sustainable datacentre	RENATER	Physical Infrastructure	Mar 2015
11	Enabling Quality of Service in a campus network	RENATER	Real-time communications and AV	Mar 2015
12	Dynamic Routing Protocols for Campuses	FCT-FCCN	LAN and IPv6	Oct 2014
13	IPv6 deployments within RCTS	FCT-FCCN	LAN and IPv6	Mar 2015
14	Portuguese R&E VoIP network status	FCT-FCCN	Real-time communications and AV	Mar 2015
15	Securing Linux Servers	AMRES	Security	Apr 2014
16	H.323 gatekeeper installation and configuration	AMRES	Real-time communications and AV	Feb 2015
17	Deployment of open source PBX solution (Asterisk)	AMRES	Real-time communications and AV	Mar 2015
18	Securing service access with digital certificates (update)	AMRES	Security	Mar 2015
19	Integration of Office365 with existing faculty SSO	MARnet	Physical Infrastructure	Nov 2014

No.	Document	NREN	Area	Completed
20	DNSSEC deployment guide	CSC/Funet	LAN and IPv6	Aug 2014
21	Campus network: IPv6 and firewalling	CSC/Funet	LAN and IPv6	Mar 2015
22	Service prioritisation as part of the data centre continuity plan	CSC/Funet	LAN and IPv6	Mar 2015
23	Server certificate practices in eduroam	CSC/Funet	Wireless	Mar 2015
24	Intelligent Resilient Framework at University Campus	CESNET	LAN and IPv6	Mar 2015
25	Specification of Main Components for Designing a Data Centre for Educational Purposes	BREN	Physical Infrastructure	Mar 2015
26	Requirements for the e-learning platform for Bulgarian education	BREN	LAN and IPv6	Nov 2014
27	Design and Construction of a Metropolitan Network	RENATER	LAN and IPv6	Sep 2014

Table 3.2: Best practice documents completed in GN3plus Y2

The abstracts for the BPDs can be found in Appendix B.

3.2 Dissemination

3.2.1 Presentations at Conferences

A total of 12 presentations were given at international and national conferences during project year 2. The presentations are listed in Table 3.3.

No.	Date	Event	Presentation	Speaker
1	23 September 2014	NORDUnet Conference 2014, Uppsala, Sweden	UNINETT Campus Best Practice activities	Tom Myren, UNINETT
2	23-25 September 2014	NORDUnet Conference 2014, Uppsala, Sweden	Campus best practices poster presentation at the GÉANT booth	Tom Myren, UNINETT; Jari Miettinen CSC/Funet
3	11 February 2015	Jornadas FCCN 2015	IPL Metro Network in 2015	Pedro Ribeiro, IPLISBOA
4	11 February 2015	Jornadas FCCN 2015	IPv6@RCTS Update	Carlos Friaças, FCT-FCCN

5	2-6 April 2014	43th Spring Conference of Mathematicians, Borovets (Bulgaria)	Best Practice – definition, classification. Quality assurance, validation and verification.	Radoslav Yoshinov, BREN
6	2 April 2014	Seminar: Contest – "Mathematics with Computer"	What are the goals of CBP task in GÉANT	Radoslav Yoshinov, BREN
7	3 April 2014	Workshop, the Scientific Approach in the Education in Mathematics and Applied Sciences, Borovets (Bulgaria)	The five steps model of storing and sharing know-how - BPDs	Radoslav Yoshinov, BREN
8	24-26 April 2014	National Conference on Innovative Solutions and Good Practices in Education, Velingrad (Bulgaria)	From Best Practice to onsite realization	Radoslav Yoshinov, BREN
9	30 October 2014	QED UNESCO International Workshop, Sofia (Bulgaria)	Implementing the "Campus Best Practice" model in education	Radoslav Yoshinov, BREN
10	31 October 2014	National Seminar "Mathematics with Computer", Sofia (Bulgaria)	The pillars in e-learning. Implementing the CBP model.	Radoslav Yoshinov, BREN
11	5 November 2014	Finnish National University IT Days 2014	Campus Best Practices	Janne Oksanen, CSC/Funet
12	8 December 2014	ISE and MASCIL Joint Seminar, Sofia (Bulgaria)	Reflection of BEST PRACTICES in BP Documents. Sharing the know-how.	Radoslav Yoshinov, BREN

Table 3.3: Presentations at conferences in GN3plus Y2

3.2.2 Workshops and Training Events

This section describes the five international events, two workshops and three combined training-workshop events (GÉANT Summer Workshops) that were organised by the Task during Y2 of GN3plus. The two workshops were organised in Prague in April 2014 and in Helsinki in September 2014 respectively, whereas the three combined training-workshop events were held in Sofia in June 2014, in Chișinău in September 2014, and in Belgrade in March 2015.

A more detailed program of the international workshops can be found in Appendix D, and each of the events is discussed in detail in the following chapters. Additionally, a list of workshops organised at a national level can be found at Appendix C, while European-level workshops and training events are listed in Table 3.5.

Event	Location	Hosted by	Date	Participants
Campus Monitoring and Security workshop	Prague, Czech Republic	CESNET, Czech Republic	24 – 25 April, 2014	50
E-infrastructure Summer Workshops (security, GEANT services – wireless, federations)	Sofia, Bulgaria	BREN, Bulgaria	16 - 20 June, 2014	37 participants + 16 speakers + 5 organisers
E-infrastructure Autumn Workshops (optical networks, monitoring and analysis, federated services)	Chișinău, Moldova	RENAM, Moldova	8 - 11 September, 2014	49 participants, + 11 speakers + 5 organisers
Datacentre IaaS Workshop	Helsinki, Finland	CSC/Funet, Finland	11-12 September, 2014	39
Security Workshop	Belgrade, Serbia	AMRES, Serbia	18-20 March 2015	40 participants + 10 speakers + 5 organisers

Table 3.4: Campus Best Practice European-level workshops and training events in GN3plus Y2

3.2.2.1 International workshops

International workshops are a core activity of the Campus Best Practices task. They are intended to provide a space in which participants can exchange ideas and experiences and have an opportunity to present their recent results and initiatives to the community. The various presentations and discussions also give guidelines for future areas of co-operation and best practice documents.

The workshops were organised according to the two-year plan which was agreed by the partners during GN3plus project year 1. The workshop themes were chosen to support the work on BDPs in the NRENs. The workshops were organised in collaboration with several NRENs, with the hosting NREN covering the steering role for practical reasons.

3.2.2.2 International training events combined with a workshop

The purpose of the training events was to support the development of NRENs from Eastern Europe by providing training in key network technology areas, identified during previous workshops of the same type organised by the FP7 CEENGINE project from the Central and Eastern European Networking Association (CEENET). The participants were recruited mainly from countries identified by the EC's European Neighbourhood and Partnership Instrument (ENPI) programme.

Two events, the E-infrastructure Summer and Autumn Workshops, which took place in Sofia and Chișinău in June and September 2014 respectively, were concluded successfully during project Y2, with over 90 participants trained in various networking technologies. The main training topics included: IT security, backbone technologies and federated services. With each event organised (taking into account previous workshops of the same type organised by CEENET in the CEENGINE project), there has been increasingly active participation on the part of NREN personnel, more interest in the uptake of GÉANT services and more specific training demands for the future.

The organisation of the training events has been strengthened by the EC's Development and Cooperation (DEVCO) – EuropeAid's Eastern Partnership Programme, which gave a substantial financial contribution which helped to improve the quality of the events and provided logistic and subsistence support.

The third combined training and workshop event, the Belgrade Security Workshop, took place in March 2015 (3.2.2.8).

3.2.2.3 Campus Monitoring and Security Workshop (Prague)

The workshop was organised by CESNET in Prague on 24 and 25 April 2014 [CESNETWS2014]. The program covered two days with two sessions each, with discussions on common practices in monitoring, tools used, and processes deployed to improve the management of campus networks.

Funding

The event was funded by GÉANT and CESNET.

Participants

50 participants from eleven countries took part in the workshop. Participants were members of universities and NRENs in the GÉANT community, and from the USA and Japan.

Speakers

The programme included speakers from European universities, from NRENs and from Japan, as well as one speaker from INVEA technologies.

Structure and programme

The first workshop day focused on available tools and products which might be suitable for use in modern high-speed networks. The discussion progressed to applications and solutions currently used in the community.

The second day started with an analysis and reporting part. Various network security aspects were raised by the speakers. The workshop ended with discussions of future developments. The speakers introduced recent results and discussed the relevancy and applicability of standards to their daily practical work.

Event summary

- The seminar offered lectures focused on topics related to improving security levels using advanced monitoring tools and tools for deep analysing of flow data.
- Participants recommended repeating this type of workshop every year in consideration of the dramatic growth in various kinds of attacks and security threats.

- It was considered that the workshop should be open to the wider community, not just to NRENs and participants in the GÉANT project, but also university network specialists and members of academic institutions.

3.2.2.4 *E-infrastructure Summer Workshops (Sofia)*

This was a five-day event including a mix of lectures and hands-on practice, conducted by leading specialists and experts both from within and outside the community, around three core topics: Security, Services, and Federated Identity [Sofia2014]. The workshop was held at the Institute of Mathematics and Informatics and the Laboratory of Telematics at the Bulgarian Academy of Sciences in Sofia, Bulgaria, on 16 - 20 June 2014. It was hosted by the Bulgarian NREN, BREN, which provided the location and technical lab. Mobile eduroam was set up by the NA3 T2 team to facilitate WiFi access in the rooms.

Funding

The event was jointly funded by GÉANT and the Eastern Partnership Platform 4.

The three selected participants from six target EAP countries received full financial support for their travel and subsistence from Platform 4, as part of its dedicated Eastern Partnership Program, which aims to improve e-Infrastructures in the partner countries of Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine. 18 members of the audience received financial support from Platform 4, while another 19 received funding through the GN3plus budgets for NA4 T4 and NA3 T2.

Participants

The audience included a total of 37 participants from across Eastern European NRENs, universities and libraries. In addition, the workshops were attended by several IT professionals from the Bulgarian NREN (BREN) and the two largest universities in Bulgaria. The total number of attendees was around 50.

Speakers

Speakers for the different technical and strategic sessions came from the CEENET and GÉANT communities and expert groups from countries including Poland, Sweden, Serbia, the UK, Switzerland, Norway, France, Bulgaria and The Netherlands.

Structure and programme

The first three days were aimed at staff from NOCs (Network Operation Centres) and featured training on network security.

On the first day and the morning of the second day, participants learned how to implement security policies, how to select and operate the security tools needed in daily network management and how to operate CSIRTs (Computer Security Incident Response Teams) in the GÉANT environment.

The afternoon of the second day and the third day were devoted to hands-on experience in the form of “CERT games”. The objectives of participating mixed-nationality teams were to secure the existing infrastructure of IT enterprise and to fight ongoing external attacks.

The following days included a half-day GÉANT Services Workshop on campus best practices in wireless networks. This was a ‘crash course’ covering the most important aspects of Wi-Fi wireless network deployment and

included live demonstrations and the sharing of practical experiences, with a particular focus on the eduroam service.

The final part of the summer workshops in Sofia included a federated identity technology workshop aimed at managers and IT leaders. The objective was to educate the managers and decision-making attendees from NRENs, libraries and campuses on policy issues and business case and deployment options related to the development and support of pan-European and global identity e-infrastructures. The first part focused more on theoretical aspects and involved a number of presentations, while the second half had a more practical approach, with several "hands-on" activities.

Event summary and recommendations

In summary, the event was given a high score assessment by the participants, with several factors seen as contributing to its success:

- The combined funding from GN3plus and DEVCO enabled wider participation and better logistics, relieving the team of many organisational needs and costs not directly related to the programme (e.g. travel, accommodation, catering)

- A good mix of hands-on practice and lectures, including open competitions, encouraged teamwork and a lively interest from the audience. Four teams competed in separate, identical virtual environments to score the highest services security and availability rank. This was the most enthusiastically received and most exciting part of the workshop, and produced excellent teamwork from the ad-hoc teams.

- The duration of the workshop (four days) also contributed to the team-building process, the exchange of information between participating NRENs and the creation of a safe discussion space.

As quoted in the July 2014 issue of CONNECT magazine [CONNECT], Jari Miettinen of CSC-Funet, who leads the Campus Best Practices task, said regarding the success of the workshop: *"As the Technical University of Sofia had just joined eduroam and the Sofia University was in the process of enabling eduroam, it really was a good time to get together and discuss best practices … The workshops provided a great opportunity for international multi-directional information exchange and community building. All the partners, their expertise and contributors are needed in the European co-operation."*

The participants of the workshop recommended that more hands-on security and backbone technologies training should be provided in the future, and expressed a wish for in-depth training to be provided on selected technology areas.

3.2.2.5 E-infrastructure Autumn Workshops (Chișinău)

The workshops took place in late summer (8–11 September 2014) in Chișinău (Moldova), and focused on NRENs' technology and identity provisioning services [Chisinau2014].

The training workshops took place at the Faculty of Engineering and Management in Electronics and Telecommunications at the Technical University of Moldova. Mobile eduroam was set up by the NA3 T2 team to facilitate WiFi access in the rooms.

The four days in Moldova comprised a mix of lectures and hands-on practice, conducted by leading specialists and experts both from within and outside the GÉANT community, covering the themes of optical/broadband networking technologies, network monitoring and services, and Identity Federation.

Funding

The event was jointly funded by GÉANT and Eastern Partnership Platform 4. Three selected participants from six target EAP countries received full financial support for their travel and subsistence from Platform 4, as part of its dedicated Eastern Partnership Program, which aims to improve e-Infrastructures in the partner countries of Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine.

Participants

The audience included 49 participants from across Eastern European NRENs, universities and libraries. In addition, several IT professionals from the local NREN (RENAM) and the three largest universities in Moldova attended the workshops.

Speakers

Speakers from the CEENET and GÉANT communities and expert groups from countries including Poland, Germany, Romania, Italy, Serbia, Croatia, Bulgaria, Armenia, Denmark, France, and the Netherlands took part in the various technical and strategic sessions.

Structure and programme

The workshop started on 8 September 2014 with a working lunch/registration, followed by a session devoted to optical networking, which is relevant to future network developments in the area, which included overviews, characteristics, good practices, recommendations and practical experiences on different Optical Transmission Systems with a focus on ENPI NRENs' interconnections. Other planned topics for the remainder of the workshop included: dark fibre networks - lighting the fibre; (C/D) WDM systems; MPLS services; and GÉANT lightpath services.

The morning training session on 9 September 2014 focused on network measurement and monitoring, focusing on NetFlow and the AMRES Network Management System tool NetIIS [NetIIS], providing the audience with an understanding of what a NetFlow is, how and why to use it, how it works and its benefits. The subject of the afternoon session was the deployment of network services, including basic communication services such as VoIP and eduroam. The Bulgarian representative spoke in detail about eduroam, since it is the one federated service that is widely adopted across the globe and is experiencing continual growth. The session also highlighted the opportunities provided by GÉANT testbeds.

Training for federated identity building was held during the last two days of the workshop (10–11 September 2014). This technical hands-on training focused on the tools and skills necessary to deploy identity infrastructure for the library, campus or country, and provided the attendees with information on:

- How to safely and securely expose the identities of your user community within their organisation and beyond.
- How to offer (as well as access) services and resources in a federated community.

- How the development of a hub and spoke federated identity infrastructure is scalable from the campus to the country level.

The afternoon session on 11 September 2014, provided an opportunity to address the local audience from Moldova and Romania, as the organisers of the joint RENAM/RoEduNet conference invited GÉANT and EC representatives to provide a plenary speech at the opening session of the conference: Dorte Olesen, gave a presentation on behalf of GÉANT, entitled "GEANT4: opportunities, challenges, a place for Eastern Europe".

Event summary

The Chișinău event was very well received, as was the earlier Sofia workshop, with similar factors accounting for its success:

- Combined funding from GN3plus and DEVCO.
- Interesting content in line with expectations.

The duration of the workshop (four days) also contributed to the team-building process, the exchange of information between participating NRENs and the creation of a safe discussion space. The participants of the workshop recommended that future training should focus on lab activities, with fewer topics covered in greater depth.

The most demanding areas identified for training were advanced backbone routing and MPLS technologies. Support for the deployment of federated services remains in scope and requires continued attention.

3.2.2.6 Datacentre IaaS Workshop 2014 (Helsinki)

This was a two-day event that took place in Helsinki on 11-12 September 2014, and was hosted by CSC/Funet [CSCWS2014]. The programme consisted of six sessions spread over two days. It included presentations by 21 speakers who covered the Datacentre IaaS topic from a variety of angles, as well as a visit to a live datacentre.

Funding

The event was funded by GÉANT.

Participants

The event included 39 participants from eight countries, and was webcast using Adobe Connect. The broadcast was attended remotely by up to 17 participants simultaneously on the first day and up to 14 on the second day. The recordings are available online [CSCWSDay1] [CSCWSDay2].

Speakers

Speakers were mainly from the universities and NRENs belonging to the GÉANT community, as well as speakers from three commercial companies: elfCloud, Invea and Powerfolder.

Structure and programme

The intended target audience were the network engineers and NREN staff involved in working on the deployment of IT services and datacentres on campuses.

The first day focused on green datacentre technologies and cloud service provisioning. The last session focused on joint procurements, costs and agreements related to IaaS.

On the second day, the speakers discussed the various security aspects of existing services and lessons learned. Networking and interconnection possibilities were covered. Lastly, various production services and major service initiatives were introduced.

Event summary

The workshop highlighted the fact that the existing datacentres, management systems and identity federations are strengths in the current phase of development of datacentre technologies and practices in the higher education community. The risk of vendor lock, security and procurement were considered the areas to be most in need of further action.

The following items were considered fruitful areas for further work:

- Best practice in datacentre management.
- Best practice in datacentre hosting.
- Strategy work for joining forces in NRENs.
- Cloud storage service implementation.
- Monitoring of high-speed networks and new high-density devices.
- Standardisation.

3.2.2.7 Campus Best Practice at the GN3plus Symposium 2015 (Athens)

NA3 T2 organised a lightning talk session during the GN3plus Symposium 2015, which was held in Athens on 23-26 February 2015 [Symposium2015]. The session provided a 10-minute window in which to present recent BPDs and future initiatives. A total of eight presentations were given. Also the GÈANT Green Team (NA3T3) gave a presentation on the environmental policy template.

The CBP work was highlighted in the Symposium Plenary session. The NA3T2 activity leader gave a lightning talk on the campus best practice documents, and the campus best practices method was introduced during the NA3 joint meeting.

3.2.2.8 Security Workshop 2015 (Belgrade)

AMRES organised a 3-day security workshop as part of the GN3plus NA3 T2 Campus Best Practice activities. The workshop was held in Belgrade, Serbia, on 18-20 March 2015, and included a security training session and a security seminar [AMRESWS2015]. The workshop aimed to address the security aspects of network services and promote the BPDs produced by the CBP community. Training took place during the first two days of the workshop, and participants were given the opportunity to improve their skills and experiences through practical work on IT infrastructure and network services. The Polish CERT team, COMCERT, which already had experience of organising similar events, led the training. The third day of the workshop was reserved for a seminar devoted to promoting security-related best practice documents on various network services: DNS, IPv6, log processing, NAT, etc. Over 35 people from eight European countries took part.

The Security Training part of the workshop was addressed at system administrators of academic institutions who are involved in maintaining and protecting basic network services. The goal of the training was to review the security mechanisms that system administrators use in their day-to-day operations, discover frequent errors and gain knowledge about effective protection mechanisms. Additionally, training participants had a chance to test their organisational and communication skills.

Training participants were divided up into teams of two or three members, each with a laptop with wireless networking access for hands-on exercises. Each team was given a different IT infrastructure to be protected from potential network attacks. Teams had the goal of securing their network infrastructure and then defending it from ongoing DDoS attacks. Each team was tasked to maintain service availability and data security despite the ongoing network attacks. After the attack simulations were over, the training instructors advised training participants on the most common errors in securing network services and gave recommendations on how they could better protect their IT infrastructure in the future.

The training was structured in two stages:

1. CERT GAMES (much appreciated at past events) interleaved with lectures on CERT threats experienced and related prevention methods.

2. A Security Seminar, where presentations were given by members of the CBP community on other security issues affecting Campus Networks and NRENs.

3.2.3 Summaries of selected national events

3.2.3.1 FCT-FCCN CBP meeting during Jornadas 2015 (Lisbon)

A CBP session took place at Jornadas FCCN 2015 (the annual FCCN member meeting), held in Lisbon on 10-12 February 2015 at ISCTE-IUL [Jornadas2015]. 30 people participated in the session which included two presentations (one on IPv6 and another on a Metro Network connecting several sites in Lisbon) as well as a lively discussion on future work/BPDs.

3.2.3.2 CIIT 2014 - MARnet National Level Campus Best Practice Workshop (Bitola)

The CIIT 2014 National Level Campus Best Practice Workshop was prepared and organised towards the end of Y1 but took place at the very beginning of Y2 of the project. The workshop was held as part of the International Conference on Informatics and Information Technology [CIIT], which took place in Bitola, Macedonia (FYROM), on 11-13 April 2014. Members of the networking staff from the largest higher education campuses in Macedonia were invited in order to agree on future collaborations in the production of national best practice documents and to expand the existing groups through the addition of new members.

3.2.3.3 CIIT 2015 - MARnet National Level Campus Best Practice Workshop (Bitola)

The CIIT 2015 National Level Campus Best Practice Workshop, organised as part of the International Conference on Informatics and Information Technology [CIIT], was held on April 23-26, 2015, in Bitola, Macedonia (FYROM). The main goal of this dissemination event was to present the GN3plus CBP project and task, and to discuss in more detail the goals accomplished and the completed best practice documents, in order to understand possible future CBP priorities and activities to be organised by the MARnet-led working groups, as well as to

increase participation from campuses of other universities in the country. The workshop itself took place on 23 April. From 24 to 26 April, a GÉANT dissemination desk was made available to other conference participants.

4 CBP activities in the NRENs

4.1 AMRES

AMRES was one of the original four NRENs that started the Campus Best Practice task, and has been active from the start in two of its six technical focus areas – Security and Network Monitoring – to which it added a third – Real-time Communications and AV – in Y2 of GN3plus. In Y2, AMRES produced a new BPD, "Securing Linux servers", in the Security technical area, as well as two new documents based on its previous best practice experiences, "H.323 Gatekeeper Installation and Configuration" and "Deployment of open source PBX solution (Asterisk)", bringing their total number of BPDs written since February 2011 to ten.

AMRES was very active in promoting CBP activities at various events organised under the GN3plus activities during Y2 of the project. It presented its best practice experiences on device discovery using the SNMP protocol at the Campus Network Monitoring and Security Workshop organised by CESNET in Prague in April 2014, and also took part in the Summer Workshops in Sofia, organised by BREN in June 2014, where it gave one presentation and held a hands-on lab exercise on FreeRADIUS configuration and infrastructure monitoring. At the Datacentre IaaS workshop in Helsinki in September 2014, organised by CSC/Funet, AMRES presented its experiences on virtualising datacentre infrastructure. It also took part in the GN3plus project symposium in Athens, giving two presentations during the "Thunder in the Campus" lightning talk session, when it introduced its latest BPDs.

As part of its efforts to popularise the use of BPDs and introduce best practices to academic IT staff, AMRES organised the Belgrade Security Workshop 2015 (3.2.2.8) under the GN3plus CBP activity. The workshop was held on 18-20 March 2015 in Belgrade, Serbia, and included a security training session to provide all participants with hands-on experience on securing major network services, as well as a security seminar in which the BPDs were promoted.

4.2 BREN

In Y2 of GN3plus, BREN finalised and published one BPD, "Requirements for the e-learning platform for Bulgarian education", in the area of LAN and IPv6,, and prepared another, "Specification of Main Components for Designing a Data Centre for Educational Purposes", in the Physical Infrastructure area.

BREN gave a presentation on Best Practice and Quality Assurance at the 43th Spring Conference of Mathematicians in Borovets in April 2014. It also presented GN3plus and the future of the network

development in Bulgaria at its annual national meeting-workshop with Bulgarian universities, in April 2014. It introduced GÉANT and the CBP task to various external bodies, including at ISE and ODS meetings in Belgrade in September 2014 and at a bilateral meeting of the Bulgarian Academy of Sciences and VERINT in February 2015.

BREN hosted the E-infrastructure Summer Workshops in Sofia in June 2014 (3.2.2.4), for which it prepared the technical support and organised the logistics. It also took part in the E-infrastructure Autumn Workshops in Chișinău, in September 2014, where it gave a lecture on CBP for the implementation of eduroam in Bulgaria.

4.3 CEENET

During the second year of the GN3Plus project, CEENET contributed to the organisation of three workshops, including by coordinating the various technical and strategic sessions and presentations at the E-infrastructure Summer and Autumn Workshops, held in Sofia in June 2014 and in Chișinău in September 2014 respectively, and assisting in the organisation of the Belgrade Security Workshop which took place in March 2015.

4.4 CESNET

CESNET is a founding member of the NA3 Campus Best Practice activity, and although it acts mainly in a support capacity for research, the GN3plus project remains important for it as it connects the experiences of national and international communities. However, due to the limited resources allocated for participation in the task, its activities in this area were reduced in GN3plus with respect to previous projects. In Y2, CESNET prepared two BPDs, “Virtualisation of Network Elements”, which was originally planned in Y1, and “Configuring IRF technology”. CESNET runs two working groups as part of NA3 T2: an IPv6 working group (WG) and a Monitoring WG. It also organises various workshops in different CBP-related fields, under a common framework called “CESNET days”. In the last year, workshops focused on services and on security were organised at various universities in different cities. The IPv6 CBP WG is very active in organising meetings of network managers, and maintains special mailing lists for hot topics as well as its own website. The members of the IPv6 WG also actively contribute with news items from the IPv6 world to the electronic journal “root.cz”, which is regularly read by hundreds of IT specialists from the Czech and Slovak Republics. CESNET also has own its web page dedicated to Ipv6 [CESNET-Ipv6].

CESNET organises a wide spectrum of events in different fields under a common frame called “CESNET days”. In Y2 of GN3plus, it ran a number of workshops focused on services and security at universities in various cities.. CESNET’s Monitoring WG organised the international Campus Monitoring and Security Workshop, which was held in Prague in April 2014 (3.2.2.3), and which included 20 talks in four different sections and nearly 50 participants from 11 countries (NO, FI, DE, LI, FR, USA, JP, SB, SL, CH, and CZ).

CESNET representatives also participated in several workshops organised in other countries, and gave a presentation at the Datacentre IaaS Workshop which took place in Helsinki in September 2014, as well as two talks, “First hop security in IPv6” and “ Identifying users behind NAT devices” at the Security Workshop in Belgrade, in March 2015.

Figure 4.1: Opening session of the Monitoring and Security workshop in Prague.

4.5 CSC/Funet

During the second year of the project, CSC attended several video conferences and led two national working groups, AccessFunet and MobileFunet, on the focus areas of MPLS, datacentres, mobile roaming and SIM authentication techniques. It produced four BPDs, “Guidelines for Deploying DNSSEC”, “Campus Network: IPv6 and firewalling”, “Service prioritisation as part of the data centre continuity plan”, and “Server certificate practices in eduroam”, although due to changes in personnel resources some of these had to be reduced in scope with respect to what had been planned.

CSC was the organiser of the International Datacentre IaaS (Infrastructure as a Service) workshop, held in Helsinki in September 2014 (3.2.2.6), which included 21 presentations and a visit to the local modern datacentre. 39 participants from eight different countries took part in the workshop and video streaming was available throughout the event.

During Y2, CSC attended a number of other CBP dissemination events, including the Campus Network Monitoring and Security workshop in Prague in April 2014, the E-Infrastructure Autumn Workshops in Chișinău in September 2014, the NORDUnet2014 conference in Uppsala in September 2014, the Finnish National University IT days in November 2014 and the GN3plus Symposium in Athens in February 2015. CSC representatives also gave presentations on their Campus Best Practice activities at the E-infrastructure Summer Workshops in Sofia in June 2014, on DNSSEC deployment at the Belgrade Security Workshop in March 2015,

and on collaboration and CBP work in Finland at the CIIT 2015 MARnet campus best practices workshop in April 2015.

4.6 FCT-FCCN

In Y2 of GN3plus, FCT-FCCN led a working group in two CBP areas, LAN/IPv6 and Real Time Communications, which produced five BPDs: "Dynamic Routing Protocols for Campuses", "IPv6 deployments within RCTS", "Portuguese R&E VoIP network status", "Open Source Routers", and "AV infrastructures and services within RCTS".

During Y2 of GN3plus, a CBP session was held at FCCN's annual member meeting, Jornadas FCCN 2015, which took place in Lisbon in February 2015 (3.2.3.1). During the session, two short presentations were given, the first on IPv6 deployment, as a corollary to one of the BPDs produced, and the second focused on the IPLISBOA campus interconnecting experience using MPLS technology, a topic which may be addressed in a new BPD during the next CBP lifecycle.

During the session on the Portuguese NREN's backbone (RCTS) which preceded the CBP session at the same event, a presentation about open source routers was also delivered by members of TECNICO, who contributed to the BPD produced by FCT-FCCN on the subject.

Figure 4.2: Portuguese campus best practices meeting during Jornadas 2015 in Lisbon.

4.7 MARnet

MARnet's efforts in the second year of the project were mainly focused on finalising the publication of the two BPDs produced during Y1 of the project and organising the activities to set up environments and hold discussions with the area working groups for the production of the two documents planned for Y2: "Integration of Office365 with existing faculty SSO" and "Cloud implementation using OpenNebula".

The MARnet CBP team also worked on organising two National Level Best Practice Workshops, CIIT 2014 and CIIT 2015, which were held in Bitola in April 2014 (3.2.3.2) and April 2015 (3.2.3.3) respectively.

4.8 MREN

In Y2 of GN3plus, MREN produced and published two BPDs: "Traffic Analysis and Device Management based on NetFlow data in MREN", which describes monitoring and management methods for computer networks and how their performance affects the quality and availability of computer network services, and "Security recommendation for Ubuntu server based systems", which focuses on the planning and implementation of security measures for any Ubuntu-based system that can be accessed publicly from the Internet.

4.9 RENATER

RENATER is in charge of managing and coordinating the French working group of NA3 T2.The working group is composed of participants from universities, research centres and metropolitan or regional networks. Most of the institutions involved are connected to the RENATER backbone through a metropolitan network. This working group is in turn split into smaller groups, each dedicated to a specific topic.

During Y2 of GN3plus, the French team delivered six best practice documents, which are all available in French and English: "Building an identity repository", "Efficiently run a mailing list server", "ToIP interconnection", "Creating a university CERT", "Best practices for the infrastructure of a sustainable datacentre", and "Enabling Quality of Service in a campus network".

Following the publication of the Y2 plan, RENATER was asked to give presentations at the workshops organised by CEENET and FUNET. Two RENATER speakers took part in the E-infrastructure Summer Workshops in Sofia, in June 2014, and two other speakers took part in the Datacentre IaaS Workshop in Helsinki, in September 2014. A RENATER speaker also contributed to a lightning talk, "Innovation on Campus, Getting Engaged with Campus Best Practices", during the GN3plus Project Symposium in February 2015. RENATER presented its two BPDs on CERT and secured DNS at the Security Workshop in Belgrade, in March 2015.

4.10 UNINETT

In Y2 of GN3plus, UNINETT has continued the work from Y1 mainly in four technical focus areas: LAN and IPv6, Wireless, Network Monitoring and Security.

UNINETT has written a recommendation, "NAT44 address translation", in response to increasing challenges related to IPv4 exhaustion (manly due to wireless clients) and wireless networks being re-defined as primary networks. In addition, several other BPDs were sent for review and publication in Y2, including: "Using Windows

NPS as RADIUS in eduroam", "Infrastructure for active and passive measurements for 10Gbps and beyond", "Management of information security", "Physical infrastructure for digital exams", and "Guide to configuring eduroam using Aruba equipment".

During Y2 of GN3plus, UNINETT attended a series of videoconferences and several international events as part of the CBP activity. UNINETT representatives gave four presentations at the Campus Network and Monitoring Workshop in Prague in April 2014, and UNINETT speakers also took part in the E-infrastructure Summer Workshops in Sofia in June 2014, as well as in the Datacentre IaaS Workshop in Helsinki and NORDUnet Conference in Uppsala, which were both held in September 2014.

5 Conclusions

During the second year of GN3plus, NA3 T2 Campus Best Practices delivered 27 new BPDs. The task was very active in all its work areas. The groundwork and preparations carried out during Y1 gave results beyond what was expected for the second year of the project.

Three more training events were organised in Y2 as a follow up to the first training event held during Y1. New audiences were reached thanks to active co-operation between the partners. Feedback from the training sessions was used to identify the topics for subsequent events and audience responses in general were very positive.

A great number of Best Practice Documents were produced, providing ample subject material for the organisation of a number of high-standard international workshops. These workshops provided a meeting place for experts, in which new ideas could emerge and be exchanged, giving rise to a positive feedback cycle.

CBP work is set to continue in future projects. In addition to pursuing the activities carried out during the GN3plus project, the task is intensifying its efforts to co-operate in the field of training. A revision of the published BPD documents is also being carried out, starting from the early documents from the GN3 project.

Appendix A Working Groups

A list of active working groups in each country is given below. The leaders listed are those that are active at the time of writing. Working group leaders that are marked with an asterisk in the tables below are not members of the NA3 Task 2 team. This means that the costs of their work are not charged to the GN3plus project budget, but are borne entirely by the NREN. The local NREN coordinators are highlighted in bold.

A.1 AMRES

Area	Group	Current leader	Founded
1	Physical infrastructure	Nemanja Ninkovic	Nov 2009
4	Network monitoring	**Miloš Kukoleča**	Sep 2009
6	Security	**Miloš Kukoleča**	Sep 2009
2	Multimedia – VoiP	Ognjen Milosavljevic	Jun 2013

Table A.1: Serbian working groups. The NREN coordinator is **Miloš Kukoleča** (AMRES).

A.2 BREN

Area	Group	Current leader	Founded
1	Network architecture	Krasimir Simonski	Mar 2009
1	Physical infrastructure	Vassil Vassilev	Mar 2009
6	Security	Roumen Trifonov	May 2012
5	Network Monitoring	Deyan Stoykov	Apr 2011

Table A.2: Bulgarian working groups. The NREN coordinator is **Radoslav Yoshinov** (BREN)

A.3 CESNET

Area	Group	Current leader	Founded
2	IP telephony	Jan Ruzicka*	Nov 2009
3	IPv6	Martin Pustka	Jan 2010
4	Network monitoring	Tomas Podermanski	Nov 2009

Table A.3: Czech working groups. The NREN coordinator is **Jiri Navratil** (CESNET).

A.4 CSC/Funet

The AccessFunet working group covers three areas: Virtualisation and Datacentre (1), LAN Infrastructure and IPv6 (3) and Security (6).

Area	Group	Current leader	Founded
1,3,6	AccessFunet	Janne Oksanen and Kaisa Haapala	Feb 2010
5	MobileFunet	Juha Hopia and Tomi Salmi	May 2009

Table A.4: Finnish working groups. The NREN coordinator is **Manne Miettinen** (CSC).

A.5 FCT – FCCN

Area	Group	Current leader	Founded
3	Networking	**Carlos Friaças**	Jul 2013

Table A.5: Portuguese working groups. The NREN coordinator is **Carlos Friaças** (FCT-FCCN).

A.6 MARnet

The groups were organised in an interdisciplinary manner as task groups directly related to the main areas of the proposed CBP documents.

Area	Group	Current leader	Founded
5,6	Access control and monitoring for campus computer labs	**Vangel Ajanovski**	May 2013
4,6	Campus wireless infrastructure and security	Anastas Mishev	May 2013
1	Virtualization and cloud campus services infrastructure	Boro Jakimovski	May 2013

Table A.6: Macedonian working groups. The NREN coordinator is **Vangel Ajanovski** (MARnet).

A.7 MREN

Area	Group	Current leader	Founded
4	Network monitoring	Milan Cabak	May 2013
5	Security	**Vladimir Gazivoda**	June 2013

Table A.7: Montenegrin working groups. The NREN coordinator is **Vladimir Gazivoda** (MREN).

A.8 RENATER

Area	Group	Current leader	Founded
6	Building an identity repository	Olivier Salaün	Jan 2014
6	Creating a university CERT	Jean Benoit	Jan 2014
3	ToIP interconnection	Sami Honein	Jan 2014
3	Efficiently run a mailing list server	David Verdin	Jan 2014
2	Enabling Quality of Service in a campus network	Sébastien Boggia	Jan 2014
1	Best practices for the infrastructure of a sustainable datacentre	Romaric David	March 2014

Table A.8: French working groups. The NREN coordinator is **Vanessa Pierne** (RENATER)

A.9 UNINETT

Area	Group	Current leader	Founded
1	Physical infrastructure	Helge Stranden	Jan 2006
2	Real-time communications (SIP)	Jardar Leira	Jan 2006
3	Network architecture	Vidar Faltinsen	Jan 2006
4	Network monitoring	Arne Øslebø	Jun 2005
5	Mobility	**Tom Myren**	Dec 2006
6	Security	Rolf Sture Normann*	Jun 2008

Table A.9: Norwegian working groups. The NREN coordinator is **Tom Myren** (UNINETT).

Appendix B Abstracts of GN3plus Year 2 Best Practice Documents

The abstracts below provide a summary of the contents of the Best Practice Documents produced during Y2 of GN3plus. Completed Best Practice Documents are available on the project web page [GÉANT-CBP]

B.1 Using Windows NPS as RADIUS server in eduroam (UNINETT)

Many eduroam IdP's use Windows Network Policy Server (NPS) as their RADIUS server. This document provides a detailed description of how NPS can best be configured for operating as part of the eduroam AAA structure. It contains a short overview for more experienced users as well as a detailed (cut and paste) configuration guide for administrators that are new to NPS.

B.2 NAT44 Address Translation (UNINETT)

Until recently the HE sector has had good access to IPv4 addresses. Today, however, these addresses are running out. In this document a recommendation is made on how Network Address Translation (NAT) can be used in a simple but effective way using a Linux server for NAT44. It has been shown that a virtual server is easily capable of acting as the NAT44 GW for a /20 network (~4000 clients). One important security aspect is the continued traceability of online clients. Logging via Netflow/IPFIX is used for this purpose.

B.3 Infrastructure for active and passive measurements at 10 Gbps and beyond (UNINETT)

This document describes how to set up an infrastructure for active and passive measurements to be used as a very useful tool for both performance and security network monitoring as well as for debugging network problems. The monitoring probe is usually a commodity hardware server, and for passive monitoring either a specialized monitoring card or a commodity NIC is used, where active monitoring actively generates network traffic and measures the results while passive monitoring passively captures and monitors the existing network traffic.

B.4 Physical infrastructure for digital exams (UNINETT)

Under the auspices of the eCampus programme, UNINETT has set up a project on digital exams. The project consists of several working groups and a steering group. The present document was produced by the Physical Infrastructure working group to describe recommended solutions for digital exams in universities and colleges, and is aimed at technical staff and advisors responsible for the planning and holding of the digital exams to ensure that chosen solutions are based on and satisfy the real needs of the users, that is, of the students and lecturers

The document does not take a position on all the existing software solutions for digital exams, but rather focuses on infrastructure requirements, as the type of software, servers, virtualisation solutions, firewalls, and surveillance systems used will depend on software solution that is chosen.

B.5 Traffic Analysis and Device Management based on NetFlow data in MREN (MREN)

This document describes monitoring and management methods for computer networks, in consideration of the fact that the quality and availability of computer network services depend on the performance of the monitoring system, as well as on the control system.

The document describes a flow collector for assembling and analysing data on generated network traffic data obtained from network device exporters. A solution for network traffic analysis is presented for implementing a network devices management system based on the qualitative analysis of network traffic.

Some of the basic techniques for computer network management are also analysed. The proposed solution sends warnings and automatic actions for changing the configuration of network devices, based on data obtained from qualitative network traffic analysis.

B.6 Building an identity repository (RENATER)

This document suggests an approach for setting up the identity repository for a research and teaching institution.

The identity repository is located between the applications producing the identities upstream and the applications consuming the identities downstream. A functional split of the identity repository into two layers is recommended.

Setting up the identity repository requires analysis of the existing system. For this purpose, a method for inventorying the populations, cataloguing the applications managing each population and evaluating the population overlaps is suggested. The next stage consists of defining a data model, including information describing the people and the associated meta-information (expiration date, status, data source). An LDAP directory is considered as an appropriate choice for implementing the account repository.

Handling identities involves the use of identifiers allowing reference to be made to the user. Different formats of identifiers that can be used (name-based, opaque and mixed) are presented, listing the advantages and disadvantages of each. The connection identifier is presented as a solution for reconciling user ergonomics and the use of opaque identifiers.

B.7 Efficiently run a mailing list server (RENATER)

As an organisation grows, a system becomes necessary for the routing of information to its members. This is why mailing lists are ubiquitous in research and teaching institutions.

This document describes the best practice that must be respected in order to effectively deploy a list service, taking into account the typical characteristics of such servers including: the large quantity of information that passes through them, the critical nature of the information contained, proximity to the Information System and the required openness of the system to the world outside the institution.

It should be noted that although there are many mailing list software applications, all examples and illustrations in this document are based on the Sympa software package, which is particularly well-suited to research and teaching institutions.

B.8 ToIP interconnection (RENATER)

This document describes the connection specifications for the telephony over IP (ToIP) service installed at RENATER.

The aim of this service, based on an SIP call router, is to link up the RENATER sites that have deployed a ToIP solution within their institutions. This router only sends SIP signalling and not RTP traffic, which is transmitted point-to-point between the two users.

B.9 Creating a university CERT (RENATER)

The purpose of this document is to describe the creation and the role of an operational structure, a CERT, to deal with security incidents in an academic context. The document focuses on detailing the services offered by this structure as well as on the organisational and practical aspects of the creative process involved.

B.10 Best practices for the infrastructure of a sustainable datacentre (RENATER)

Datacentres, whether they are being newly constructed or renovated, are strategic for institutions in the research/teaching community. They account for very large investment and operating costs in relation to a

university's budget, in the area of several million euros and hundreds of thousands of euros in annual electricity bills.

For these projects of great structural significance to succeed, a large number of skills and specialties need to be assembled, including, besides computer specialists, electricians, heating engineers, urban planners and safety specialists. Therefore, this document is addressing each of these specialties, with the aim of providing a common foundation of best practices, specific to datacentres. It aims to help lay the foundations of good cooperation between these features. It deals with the crucial aspects related to cooling and electricity, and finally also covers the topics of servers and monitoring.

B.11 Enabling quality of Service in a campus network (RENATER)

The aim of this document is to explain the principles and reasons underlying the implementation of a Quality of Service (QoS) policy within a campus network.

The first section therefore introduces the basic concepts of QoS. These are then illustrated using a concrete example of deployment of a QoS policy on equipment of a Juniper brand campus network.

The document does not deal with QoS applied to IPv6, multicast and MPLS traffic, for which, nevertheless, the processes are similar.

B.12 Dynamic routing protocols for campuses (FCT-FCCN)

Numerous documents about dynamic routing protocols from several different sources are already easily available nowadays. This document aims to provide a different, campus-oriented, perspective on the subject, based on the experience of several campus network managers.

The main audience for this work are other campus network managers looking to build new IP network infrastructures or enhance their existing setup.

IPv6 aspects are covered throughout this document, given that higher education institutes often pursue innovation, and the new Internet Protocol is a technology ready to be used.

The content of the document is designed to be light enough for use as a quick reference in terms of dynamic routing protocols usage, by any (even inexperienced) network administrator. Sample configurations for Cisco IOS and Open Source software Quagga – which can run over simple servers – are the main focus of this work.

B.13 IPv6 deployments within RCTS (FCT-FCCN)

This document provides a view of IPv6 deployment at RCTS, the Science Technology & Society Network, which comprises the Portuguese NREN, managed by FCCN as a unit of FCT,I.P.

Efforts to deploy IPv6 in the Portuguese R&E began some time ago, but there is clearly still a lot of work to be done in order to achieve full deployment.

As IPv6 has long been implanted in the RCTS backbone, its increased usage depends solely on campus deployments, and IPv6-enabled external applications/content used by campus users. It is hoped that this document can encourage by example organisations that haven't yet started IPv6 deployment.

B.14 Portuguese R&E VoIP network status (FCT-FCCN)

The VoIP@RCTS project started around 2007 following the network infrastructure upgrade of Rede Ciência, Tecnologia e Sociedade (RCTS) – the Portuguese NREN – that connected around 85% of the Portuguese research and higher education community over a dedicated optical fiber network. The remaining 15% of this community is also enabled, but over leased connections. VoIP over RCTS was the next logical step in order to exploit all the bandwidth that became available.

In late 2012, the Portuguese government decided to integrate FCCN, the organization managing the NREN into Fundação para a Ciência e a Tecnologia, I.P. (FCT,I.P.). That integration process was completed in October 2013. FCT, I.P. is the public institute responsible for funding science in Portugal, and FCCN became one of its units, still with the main responsibility of managing RCTS.

This document is essentially an update on the Portuguese chapter of CBPD146, published during the GN3 project.

B.15 Securing Linux servers (AMRES)

This document covers guidelines and recommended practices that system administrators should follow during initial Linux installation for a server environment. The purpose of the document is to help administrators protect the server and its services before going into production, using the readily available protection mechanisms that Linux distributions offer. It describes widely used practices that have stood the test of time and that offer general security in the Linux working environment.

B.16 H.323 gatekeeper installation and configuration (AMRES)

This document describes the theoretical basis of the H.323 protocol with the aim of presenting a solution for the implementation and integration of the H.323 Gatekeeper into the existing infrastructure of the Academic Network of Serbia (AMRES). Specifically, it outlines the software implementation of the Gatekeeper solution.

B.17 Deployment of open source PBX solution (AMRES)

This document describes the implementation of an IP telephone exchange at the central location (the headquarters - HQ) of the Academic Network of Serbia (AMRES) using the free Asterisk software package. The paper contains all the instructions necessary for installing and configuring the Asterisk software package, as well as basic information on the accompanying services. The communication of the Asterisk IP Telephone Exchange outside the IP domain is carried out via a SIP trunk provider, and the procedure for its configuration

is described in detail. The process of configuring the configuration files necessary for the proper operation of the Asterisk Server is also explained.

B.18 Securing service access with digital certificates (AMRES)

This document promotes the adoption of digital certificates in the member institutions of the Academic Network of Serbia (AMRES) as a means of establishing secure communication channels.

In order to establish secure communication when sending or receiving data to/from a server, users must be sure that they are indeed accessing the resources they intended to access and that no one can read and/or alter the data that is being sent or received. Such security is provided by the use of digital certificates in conjunction with SSL technology.

The document outlines the components of a PKI infrastructure, and also the implementation of PKI functions should AMRES be included in the TCS service (TERENA Certificate Service). It also specifies the various needs for PKI of NRENs, which require various types of digital certificates, and special attention has been given to the use of the PKI infrastructure and digital certificates in combination with SSL technology for the purpose of the mutual authentication of services and their users.

The procedure for obtaining a server certificate, key generation, the creation of certificates and the preparation and submission of the request for signing a server certificate are explained. The final part of the document contains instructions for installing digital certificates on Linux servers.

B.19 Integration of Office365 with existing faculty SSO (MARnet)

This document describes the steps needed to integrate Office365 with a local SSO. First the best practice architecture to use in faculty and/or university environments is discussed, followed by a description of the SSO implementation process, with all needed details and attributes. Federating an existing Office365 domain in order to enable it to accept authentication messages from a local SSO is also explained. Lastly, the final step of user synchronisation that must be completed in order to link local users with Microsoft Office 365 accounts is discussed.

B.20 DNSSEC deployment guide (CSC/Funet)

This document contains guidelines and best practices for the deployment, administration and monitoring of DNSSEC. The guidelines and recommendations were written based on publicly available documentation (such as RFC documents) and CSC/Funet's own experiences and observations. However, it should be noted that not all of these recommendations are necessarily suitable for every environment. Each environment's particular technical limitations must always be taken into consideration, as should practices relating to individual operating models. The document does not aim to give a detailed description of domain name service or DNSSEC operation principles, to which only a brief introduction is provided.

B.21 Campus network: IPv6 and firewalling (CSC/Funet)

The translation was not available when this report was written.

B.22 Service prioritisation as part of the datacentre continuity plan (CSC/Funet)

The translation was not available when this report was written.

B.23 Server certificate practices in eduroam (CSC/Funet)

The translation was not available when this report was written.

B.24 Intelligent Resilient Framework at University Campus (CESNET)

This document focuses on Intelligent Resilient Framework (IRF), a network virtualization technology developed by HP (originally by 3Com) available on most current models of HP Ethernet switches and routers based on comware software.

IRF can simplify the network topology of datacentre and campus networks, eliminating the need for a dedicated aggregation layer and providing more direct, higher capacity connections between users and network resources.

The document describes a rather unconventional setup (in most installations the virtual chassis is typically formed of two physical devices) to migrate a traditional STP based campus network to one IRF virtual chassis using long-range fibre between 4 distant locations.

The first part of the document describes the original state of the computer network along with the main disadvantages of this solution. In the next sections, the ways in which the topology changes after deploying the virtual chassis are explained. The third part is devoted to a specific configuration of network devices and to the preparation that needs to be done before connecting individual parts of the virtual chassis. Finally, a summary is provided of the benefits and pitfalls of the technologies used and the operating statistics before and after deployment.

B.25 Specification of main components for designing a datacentre for educational purposes (BREN)

This document focuses on the components required to design a centralised datacentre to support the integrated network infrastructure for Research and Education in Bulgaria, which is a fundamental element to three of the four pillars of the country's national IT strategy for education. These are:

- Network infrastructure – (National backbone with “Last mile” to the institution (regional inspectorate of education, university, research institute, research laboratory, college, school etc.), extended with the local network of the institution.
- Storage infrastructure
- E-learning platform
- Digital educational content

A centralised datacentre is an essential element of the proposed integrated network’s storage infrastructure and E-learning platform, and to enable the relevant digital content.

This document accordingly attempts to define appropriate strategies to support e-learning in educational & research institutions in Bulgaria, including through identifying suitable storage and devices for the centralised datacentre that are compatible with educational and research technologies, technological enhancements for an education environment for e-learning, STEM or blended learning, updates to reflect contemporary tendencies in ICT technologies, in terms of modern educational applications, and the most suitable equipment for creating, operating and managing storage for a centralized datacentre for the Bulgarian education.

B.26 Requirements for the e-learning Platform for Bulgarian Education (BREN)

This document contains specifications for the key requirements for building an e-learning platform for the Bulgarian education system.

The specifications address requirements in terms of system administration, course management, content management, management of school societies and organisations, collaboration and videoconferencing, electronic register, and anti-plagiarism.

The services that an e-learning platform should offer are covered, including localised, online training with user guides, and video tutorials covering basic operations such as log-in, navigation, system settings, creating, editing, or deleting a course, and other key functions.

The document also outlines the need for training administrators and teachers in the use of the system and to provide relevant documentation (system, technical and user documentation).

B.27 Design and Construction of a Metropolitan Network (RENATER)

The aim of this document is to present best practices for the construction and implementation of a metropolitan or regional backhaul network. These backhaul MANs (Metropolitan Area Networks) connect the local and campus networks of partners of the French Research and Education (R&E) community to RENATER (the French NREN). This document therefore deals neither with Local Area Networks (LANs) nor Campus Area Networks (CANs), subjects already covered extensively.

Among the several combinations that exist for MAN design, the authors have selected those they have the greatest knowledge of. In order to define the boundary of the MAN, the willingness of the French R&E community to manage its local and campus networks is also considered, based on the physical infrastructure of the backhaul network.

This document does not include operating instructions for a MAN or WAN. This is dealt with in the 'Best Practice Network Operation' document, but the problem of exporting the operations of a network of this type is briefly mentioned.

Appendix C Workshops Organised at the National Level

The following workshops were organised at the national level in Year 2 of the GN3plus CBP task.

No.	Date	Area	Topic	Country	#days	Participants
1	14-15 May 2014	2	Realtime communication, SIP / Lync	Norway	2	30+
2	3-4 June 2014	5	Network monitoring	Norway	2	30+
3	7-8 September 2014	6	Security workshop	Norway	2	50+
4	28-29 October 2014	3,4	Wireless workshop	Norway	2	40+
5	2-4 December 2014	2	Realtime communication and eCampus (1 day for realtime)	Norway	1	30
6	11-12 March 2015	1-6	@Campus workshop	Norway	2	50+
7	11 February 2015	3	CBP session at Jornadas FCCN 2015, ISCTE-IUL, http://jornadas.fccn.pt/geant-campus-best-practices/	Portugal	1/2	30
8	11-13 April, 2014	1,4,5, 6	CIIT 2014 – MARnet National Level Campus Best Practice Workshop	Macedonia	1	10
9	23 April, 2015	1,4,5, 6	CIIT 2015 - MARnet National Level Campus Best Practice Workshop	Macedonia	1/2	17
10	15 May, 2014	1,3	AccessFunet meeting	Finland	1/2	26
11	15 May, 2014	5	MobileFunet meeting	Finland	1/2	26
12	5 December 2014	1,3,5	AccessFunet and MobileFunet joined meeting	Finland	1/2	16

Table C.1: Workshops organised at the national level

Participants in the events with several sessions or multiple days are marked with a plus notation (+).

Appendix D European-Level Workshops and Training Events

NA3 T2 organised N European-level expert events in year 2. This appendix shows the agenda of each workshop and gives references for presentations and further details.

D.1 Monitoring and security workshop – April 24-25 2014, Prague

Time	Presentation	Presenter
Day 1		
	Theme: Tools and products	
9:30-10:00	FPGA accelerated application monitoring in 40 and 100G networks	Petr Kaštovský / INVEA
10:00-10:30	Coffee break	
10:30-11:00	Monitoring of Application protocos in 40/100Gb Networks	Viktor Puš / CESNET
11:00-11:30	pncweblib: A library for rapid development of web interfaces for use with the perfSONAR NC Framework	Arne Oslebo / UNINETT
11:30-12:00	Extended netflow processing with LibNf	Tomáš Podermanski / Brno University of Technology
12:00-13:00	Lunch	
	Theme: Applications and solutions	
13:00-13:30	Configuratble device discovery based on SNMP	Slavko Gajin / University fo Belgrade

13:30-14:00	From traditional to alternative approach to storage and analysis of flow data	Martin Žádnik/Brno University of Technology
14:00-14:30	Large scale passive monitoring at 10Gbps on commodity hardware	Arne Oslebo / UNINETT
14:30-15:00	Coffee break	
15:00-15:30	Monitoring IPv4 address utilization/depletion in UNINETT	Morten Brekkevold / UNINETT
15:30-16:00	The perfSONA Project at 10 Years: Status and Trajectory	Jason Zurawski (ESNET)
16:00-16:30	New Approach to Recognition of VoIP Attacks from Honeypots	Miroslav Vozňák, Jakub Šafařik / CESNET
16:30-17:00	NeMo/DDoS-Detection	Jochen Schoenfelder (DFN-CERT)

Time	Presentation	Presenter
Day 2		
	Theme: Analysis and Reporting	
9:30-10:00	Computer Incident Response Team as Integral Part of Campus Security	Jan Soukal, Pavel Čeleda, Jan Vykopal / Masaryk University Brno
10:00-10:30	Measuring Quality of Penetration of IPv6 services	Matěj Grégr / Brno University of Technology
10:30-10:45	Coffee break	
10:45-11:15	Harvesting Logs and Events Using MetaCentrum Virtualization Services	Radoslav Bodó, Daniel Kouřil, Jiři Sitera, Miloš Mulač, Pavel Vondruška / University of West Bohemia
11:15-11:45	Wifi service in university campuses, performance status and statistics	Koji Okamura / Kyushu University
11:45-12:15	Log Analysis using Open Source Scalable Systems	Gurvinder Singh (UNINETT)
12:!5-13:00	Lunch	
	Theme: The future	

13:00-13.30	NIX.CZ platform and SECURE VLAN	Petr Jiran /CZ.NIC
13:30-14:00	Network traffic monitoring & security – from academic project to commercial product	Petr Špringl / INVEA
14:00-14:30	Customized anomaly detection and analysis tools as a service	Tomáš Košňar /CESNET
14:30-15:00	Teaming network operation complexity with change detection, inventory and automated deployment	Jean Benoit (University of Strasbourg)

Table D.1: The event agenda.

D.2 E-Infrastructure Summer Workshops, June 16-17 2014, Sofia.

Time	Presentation	Presenter
Day 1		
8:30-9:00	Registration and coffee	
9:00-9:10	Welcome and logistics	Michal Przybylski / CEENET
9:10-10:40	Introduction to network security	Spyridon Dossis, Irvin Homem/ DSV, Stockholm University
10:40-10:50	Coffee Break	
10:50-12:20	Basic Network Security toolbox #1	Spyridon Dossis, Irvin Homem/ DSV, Stockholm University
12:20-13:20	Lunch Break	
12:20-13:20	Basic Network Security toolbox #2	Spyridon Dossis, Irvin Homem/ DSV, Stockholm University
14:50-15:00	Coffee Break	
15:00-17:00	DNS Security	Spyridon Dossis, Irvin Homem/ DSV, Stockholm University

Time	Presentation	Presenter
Day 2		
9:00-10:30	CSERT/CSIRT operations	Michelle Danho / RENATER, Guilhem Borghesi / University of Strasbourg
10:30-10:40	Coffee Break	
10:40-12:40	Intrusion Detction Systems	Spyridon Dossis, Irvin Homem/ DSV, Stockholm University
12:40-13:40	Lunch break	
13:40-14:40	Step by step development of Security policy for Edu	Øivind Høiem / UNINETT
14:40-14:50	Coffee break	
14.50-15:10	Introduction to CERT games	Dawid Osojca, Krystian Kochanowski / COMCERT SA, Cybersecurity Foundation
15:10-18:10	CERT games part 1	Dawid Osojca, Krystian Kochanowski / COMCERT SA, Cybersecurity Foundation

Time	**Presentation**	**Presenter**
Day 3		
9:00-13:00	Morning CERT games	Dawid Osojca, Krystian Kochanowski / COMCERT SA, Cybersecurity Foundation
12:40-13:40	Lunch Break	
13:40-18:00	Afternoon CERT games	Dawid Osojca, Krystian Kochanowski / COMCERT SA, Cybersecurity Foundation

Time	**Presentation**	**Presenter**
Day 4		
	Campus best practices in Wireless Networks	

8:30-9:00	Campus Best Practices in Wireless Networks – Welcome	Jari Miettinen/ CSC, FUNET
8:40-9:00	Campus Best Practice in Practice	Jari Miettinen / CSC, FUNET
9:00-10:10	Network Planning	Anders Nilsson / Umeå University
10:10-10:20	Coffee Break	
10:20-11:20	FreeRADIUS Configuration	Jovana Palibrk / AMRES
11:20-12:20	RADIUS and WLAN Infrastructure Monitoring	Jovana Palibrk / AMRES
12:20-13:20	Lunch Break	
13:20-14:00	CBP Experiences from Bulgaria	Slavcho Manolov / BREN, Deyan Stoykov / University of Ruse
	Event continued with "Federated identity Technology Workshop"	

Table D.2: The event agenda.

D.3 E-Infrastructure Autumn Workshops, 8-11 September 2014 Chișinău

Time	Presentation	Presenter
Day 1		
	Theme: Backbone – Optical transmission systems important for ENPI NRENs interconnections	
12:00-13:00	Lunch	
13:00-13:30	Q&M of dark fibre networks – good practices, procedures	Octavian Rusu / RoEduNet
13:30-14:30	Best practices in effective lighting of fiber (1)	Volkert Lempert / ADVA Optical Networking

14:30-14:45	Coffee break	
14:45-15:15	Best practices in effective lighting of fiber (2)	Volkert Lempert / ADVA Optical Networking
15:15-16:15	NREN's choice of (C/D)WDM systems – overview, characteristics, recommendations, practical experiences (1)	Matheusz Firuta, Ralf Labeda /CIENA
16:15-16.30	Coffee break	
16:30-17:00	NREN's choice of (C/D)WDM systems – overview, characteristics, recommendations, practical experiences (1)	Matheusz Firuta, Ralf Labeda /CIENA
17:00-17:30	Building lightpaths & Dynamic lightpaths in GÉANT (AutoBAHN)	Tangui Coulouarn / DeIC (videoconference)
17:30-18:30	MPLS services (multi-domain VPN)	Xavier Jeannin / RENATER (videoconference)

Time	Presentation	Presenter
Day 2		
	Theme: Network routing, monitoring, services	
9:00-9:30	GÉANT support to cloud services	Branko Radojevic / CARNET
9:30-10:00	Monitoring backbone networks – tools, what to monitor, operations, Netflow, NetIIS	Manuel Subredu, Valeriu Vraciu /RoEduNet
10:00-10:15	Coffee break	
10:15-12:15	Netflow – NetVisura	Milos Zekovic / Soneco, Serbia
12:15-13:15	Lunch	
13:15-14:00	Network performance monitoring	Szymon Trocha / PSNC
14:00-14:40	Deploying VoIP in the network	Branko Radojevic / CARNET
14:40-14:55	Coffee break	

14:55-15:55	Deploying eduraom	Deyan Stoyko / University of Ruse
15:55-16:25	GÉANT testbeds – status, opportunities, availability, rules of use (cancelled)	Jerry Sobieski / NORDUnet

Table D.3: The event agenda.

D.4 Datacentre IaaS Workshop - September 11-12 2014, Helsinki

Time	Presentation	Presenter
Day 1		
9:00	Reception opens	
10:00-10:15	Opening	Jari Miettinen/FUNET
	Session I – Theme: Green datacentre technologies	Chair: Juha Hopia/FUNET
10:15-10:35	Modular DC solutions: CSC Kajaani datacentre	Jukka-Pekka Partanen/CSC
10:35-11:05	Do-it-yourself traditional DC	Romaric David/University of Strasbourg
11:05-11:25	Do-it-yourself datacentre – case Tampere University of Technology	Tuure Vartiainen/Tampere University of Technology
11:25-12:35	Lunch break	
	Session II – Theme: Cloud service provisioning	Chair: Jovana Palibrk/AMRES
12:35-13:05	Strategic approach to cloud computing deployment	Slavko Gajin/University of Belgrade
13:05-13:35	Providing IaaS to Greek Academic Users	George Kargiotakis/GRNET
13:35-14:05	Provisioning Cloud Services to Academic Users in the Czech Republic	Filip Hubik/Masaryk university in Brno
14:05-14:40	Coffee break	
	Session III – Theme: Joint procurement, costs and agreements	Chair: Jari Miettinen/FUNET

14:40-15:00	Cost of outsourced datacentre services	Kimmo Penttinen/Laurea University of Applied Sciences
15:00-15:20	How to calculate cost efficiency of energy	Robert Ferret/RENATER
15:20-15:40	Finnish “energy efficiency tool” (presentation cancelled)	Petri Hyyppä/Proceed Consulting Ltd
15:40-16:00	Legislation and agreements – Funet Boksi use case	Pekka Palin/CSC
16:00-16:15	Ending of the first day	Janne Oksanen/FUNET
Time	Presentation	Presenter
Day 2		
9:30	Reception opens	
9:45	Opening	Janne Oksanen/FUNET
	Session IV – Theme: Security	Chair: Janne Oksanen/FUNET
9:45-10:15	Safe file storage and databases	Josef Spillner/Technical University of Dresden
10:15-10:45	SURFdrive: an Owncloud sync & share service	Rogier Spoor/SURFNET
10:45-11:05	elfCLOUD – Credibly secure cloud storage	Tuomas Tonteri/efCLOUD
11:05-11:25	Sync&share / Cloud service in education and research	Christian Sprajc/Powerfolder
11:25-12:30	Lunch break	
	Session V – Theme: Network	Chair: Miloš Kukoleča/AMRES
12:30-13:00	Services and DC Infrastructure of VSB-Technical university	Martin Pustka/VSB-TU Ostrava
13:00-13:30	Hardware accleration for high-density datacentre monitoring	Denis Matousek/Invea
13:30-13:45	Multi-domain connectivity services	Jani Myyry/FUNET
13:30-14:15	Coffee break	

	Session VI – Theme: Lightning talks	Chair: Tomi Salmi/FUNET
14:15-14:30	AMRES virtualization solution	Miloš Kukoleča/AMRES
14:30-14:45	Self service for Virtual Machines	Sigmund Augdal/UNINETT
14:45-15:00	Pouta Cloud Service	Kalle Happonen/CSC
15:00-15:15	Case IDA – storage service for Finnish HE institutions and Academy of Finland projects	Jorma Paananen/CSC
15:15-15:45	EUDAT – Standardized storage services for European research communities	Ari Lukkarinen/CSC
15:30-15:45	Feedback	Kaisa Haapala/FUNET
15:45-16:00	Ending of the workshop	Jari Miettinen/FUNET

Table D.4: The event agenda.

D.5 Campus best practices in the GN3plus Symposium 2015, 24 February 2015

Time	Presentation	Presenter
Day 1		
	Pleanry, lightning talks	
	Getting engaged with campus best practices	Jari Miettinen /CSC, Funet
	Thunder in the campus – lightning talks on campus activities	
14:00-14:05	Introduction to the thunder	Jari Miettinen / CSC, Funet
14:05-14:15	Securing Linux servers	Miloš Kukoleča / AMRES
14:15-14:25	h. 323 gatekeeper installation and configuration	Ognjen Milosavljević / AMRES
14:25-14:35	UNINETT eduroam pages	Tom Myren / UNINETT

14:35-14:45	User experience with connection to China	Jiri Navratil / CESNET
14:45-14:55	IPv6 deployments within RCTS	Carlos Friaças / FCT-FCCN
14:55-15:05	Building an identity repository	Olivier Salaün / RENATER
15:05-15:15	Active knowledge transfer	Michal Przybylski / CEENET
15:15-15:25	Green Initiatives	Albert Hankel /SURFnet

D.6 Belgrade Security Workshop 2015 – 18-20 March 2015, Belgrade

Time	Presentation	Presenter
Day 1		
1000	Security Training Introduction	Miroslaw Maj, Dawid Osojca, Krystian Kochanowski / COMCERT SA Cybersecurity Foundation
1100	Coffee break	
1130	Preventive protection of network services	Miroslaw Maj, Dawid Osojca, Krystian Kochanowski / COMCERT SA Cybersecurity Foundation
1300	Lunch break	
1400	Simulation Attacks – phase 1	Miroslaw Maj, Dawid Osojca, Krystian Kochanowski / COMCERT SA Cybersecurity Foundation
1530	Coffee break	
1600	Attack explanation and proper protection	Miroslaw Maj, Dawid Osojca, Krystian Kochanowski / COMCERT SA Cybersecurity Foundation
Day 2		

1000	Simulation Attacks – phase 2	Miroslaw Maj, Dawid Osojca, Krystian Kochanowski / COMCERT SA Cybersecurity Foundation
1100	Coffee break	
1130	Attack explanation and proper protection	Miroslaw Maj, Dawid Osojca, Krystian Kochanowski / COMCERT SA Cybersecurity Foundation
1300	Lunch break	
1400	Simulation Attacks – phase 3	Miroslaw Maj, Dawid Osojca, Krystian Kochanowski / COMCERT SA Cybersecurity Foundation
1530	Break	
1600	Conclusions	Miroslaw Maj, Dawid Osojca, Krystian Kochanowski / COMCERT SA Cybersecurity Foundation
Day 3		
1000	Welcome Note	
1015	Recommended ICT Security Architecture in the HE Sector	Øivind Høiem / UNINETT
1100	DNSSEC operational experiences and recommendations	Antti Ristimäki/ CSC/FUNET
1130	Improving DNS Reliability and Security	Jean Benoit/ RENATER
1200	Coffee break	
1230	First hop security in IPv6 – CESNET	Tomas Podermanski / CESNET
1300	Log Analysis as a Service using open source scalable systems	Gurvinder Singh / UNINETT
1330	Identifying users behind NAT devices	Matej Gregr / CESNET
1400	Lunch break	
1500	Guidelines for Information Classification	Øivind Høiem / UNINETT
1530	Creating a university CERT	Jean Benoit / RENATER
1600	Forensic Analysis	Aleš Padrta / CESNET
1650	Closure	

Table D.2: Belgrade Security Workshop agenda – 18-20 March 2015, Belgrade.

References

[AMRES]	http://cbp.rcub.bg.ac.rs/
[AMRES-CBP]	Mara Bukvić , "AMRES Experience with Implementing the 'Campus Best Practices' Model"
[AMRESWS2015]	http://cbp.rcub.bg.ac.rs/?page_id=614
[BP-Announcements]	https://www.terena.org/mail-archives/campus-bp-announcements/ http://www.terena.org/activities/campus-bp/pdf/amres_experience_with_cbp.pdf
[CampusIssues]	Jean-Paul La Guigner, Martin Price, Rogelio Montañana and Michael Nowlan, **"**EARNEST Report on Campus Issues", ISBN 978-77559-15-4 (January 2008) http://www.terena.org/publications/files/EARNEST-Campus-Report.pdf
[CESNET-Ipv6]	http://www.cesnet.cz/services/ip-connectivity-ip/ipv6/?lang=en
[CESNETWS2014]	http://www.cesnet.cz/cesnet/events/campus-network-ws/?lang=en
[Chisinau2014]	https://www.terena.org/activities/development-support/Moldova2014/
[CIIT]	http://ciit.finki.ukim.mk
[CONNECT]	GÉANT CONNECT Magazine http://www.geant.net/MediaCentreEvents/CONNECT/Pages/default.aspx
[CSCWS2014]	https://info.funet.fi/wiki/display/avoin/Datacentre+IaaS+workshop+2014
[CSCWSDay1]	https://connect.funet.fi/p7laomhwapt/
[CSCWSDay2]	https://connect.funet.fi/p4x8gxzdhzj/
[DN3.4.1,1]	Vidar Faltinsen, Wenche Backman, Mara Bukvic, Jiri Navratil, "Deliverable DN3.4.1,1: Annual Report on Campus Best Practices" http://geant3.archive.geant.net/Media_Centre/Media_Library/Media%20Library/GN3-10-120v2-DN3-4-1-1_Annual_report_on_Campus_Best_Practices.pdf
[DN3.4.1,2]	Vidar Faltinsen, Wenche Backman, Mara Bukvic, Jiri Navratil, "Deliverable DN3.4.1,2: Annual Report on Campus Best Practices" http://geant3.archive.geant.net/Media_Centre/Media_Library/Media%20Library/GN3-11-132-DN3412-v04-FinalReviewed.pdf
[DN3.4.1,3]	Vidar Faltinsen, Wenche Backman, Mara Bukvic, Jiri Navratil, "Deliverable DN3.4.1,3: Annual Report on Campus Best Practices" http://geant3.archive.geant.net/Media_Centre/Media_Library/Media%20Library/GN3-12-143_DN3-4-1-3_Campus-Best-Practice_v1.0.pdf
[DN3.4.1,4]	Vidar Faltinsen, Jari Miettinen, Ivan Ivanovic, Jiri Navratil, "Deliverable DN3.4.1,3: Annual Report on Campus Best Practices" http://geant3.archive.geant.net/Media_Centre/Media_Library/Media%20Library/GN3-13-086_DN3-4-1-4_Campus-Best-Practice.pdf

[GÉANT-BPDs] GÉANT Campus Best Practice Document Repository
http://services.geant.net/cbp/Knowledge_Base/Pages/Home.aspx

[GÉANT-CBP] GÉANT Campus Best Practice
http://services.geant.net/cbp/Pages/Home.aspx

[GIGACAMPUS] www.terena.org/activities/campus-bp/pdf/gigacampus_final_report.pdf
[GN3plusWebsite] www.geant.net
[Jornadas2015] http://jornadas.fccn.pt/
[NetIIS] http://netiis.rcub.bg.ac.rs/netiis/NetIIS
[Sofia2014] https://www.terena.org/activities/development-support/sofia2014/index.html
[Symposium2015] http://www.geant.net/MediaCentreEvents/Events/Symposium_2015/Pages/Home.aspx

Glossary

API	Application Program Interface
ASM	Any Source Multicast
AV	Audio Visual
BGP	Border Gateway Protocol, RFC4271
BPD	Best Practice Document
CBP	Campus Best Practice
CEENET	Central and East European Networking Association
CEPIS	Council of European Professional Informatics Societies
CERT	Computer Emergency Response Team
CNRS	French National Centre for Scientific Research
DANE	DNS based Authentication of Named Entities
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol for IPv6
DNS	Domain Name System
DNSSEC	Domain Name System Security Protocol
EAPoL	Extensible Authentication Protocol over LAN
EUNIS	European University Information Systems Organisation
GRENA	Georgian Research and Education Networking Association, the Georgian NREN
HE	Higher Education
IaaS	Infrastructure as a Service
ICT	Information and Communications Technology
IMS	Instant Messaging Service
IdP	Identity Provider
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPv6	Internet Protocol version 6
IPFIX	Internet Protocol Flow Information Export
ISO	International Organisation for Standardisation
LAN	Local Area Network
NA3	GN3plus Networking Activity 3, Status and Trends
NA3 T2	NA3 Task 2, Campus Best Practice
NAT	Network Address Translation
NOC	Network Operations Centre

NREN	National Research and Education Network organisation
NTLR	National Top-Level RADIUS
PID	Project Initiation Document
PKI	Public Key Infrastructure
PoP	Point of Presence
RADIUS	Remote Authentication Dial-In User Service
RCTS	Rede Ciencia Tecnologia e Sociedade (Portuguese Science, Technology and Society Network)
RFC	Request For Comments, IETF internet standard
SLAAC	Stateless Address Auto-Configuration
SIP	Session Initiation Protocol
SP	Service Provider
SSL/TLS	Secure Sockets Layer / Transport Layer Security
TELFOR	Telecommunications Forum
TERENA	Trans-European Research and Education Networking Association
TNC	TERENA Networking Conference
VoIP	Voice over IP
VPN	Virtual Private Network
WACREN	West and Central African Research and Education Network
WLAN	Wireless Local Area Network