03-04-2013

Deliverable DN3.4.1,4: Annual Report on Campus Best Practices

Deliverable DN3.4.1,4

Contractual Date:	31-03-2013
Actual Date:	03-04-2013
Grant Agreement No.:	238875
Activity:	NA3
Task Item:	Task 4
Nature of Deliverable:	R (Report)
Dissemination Level:	PU (Public)
Lead Partner:	UNINETT
Document Code:	GN3-13-086
Authors:	Vidar Faltinsen (UNINETT), Jari Miettinen (Funet), Ivan Ivanovic (AMRES), Jiri Navratil (CESNET)

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7 2007–2013) under Grant Agreement No. 238875 (GÉANT).

Abstract

Campus Best Practice is the name of one of the Tasks (Task 4) in Networking Activity 3, Status and Trends (NA3), of the GN3 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. The current GN3 deliverable reports on the work carried out in the Task during the fourth and final year of the GN3 project (April 2012 – March 2013) and the results of that work.

Table of Contents

Table of Figures

Table of Tables

Executive Summary

Campus Best Practice is the name of one of the Tasks (Task 4) in Networking Activity 3, Status and Trends (NA3), of the GN3 project. The overall objective of the Task is to address the key challenges for campus networks in Europe, organise working groups and provide an evolving and to-the-point set of best-practice documents for the community. The current GN3 deliverable reports on the work carried out in the Task during the fourth year of the GN3 project (April 2012 – March 2013) and the results of that work.

The working methods in the Task build on the experiences from UNINETT's GigaCampus project (2006–2009). As part of that project, UNINETT organised a number of working groups in Norway dealing with campus issues in different technical areas. Participants from the relevant technical units at the universities were invited to participate in the working groups that proposed recommendations in best-practice documents.

Four pilot National Research and Education Network organisations (NRENs) have participated in the Task since the start of the GN3 project, namely UNINETT from Norway, CSC/Funet from Finland, CESNET from the Czech Republic and AMRES from Serbia. In addition, RENATER from France joined the Task in Year 4. Each NREN has organised working groups in its country. Initially, work was done in nine technical areas. To allow a stronger concentration of results, from the start of Year 3 the number of working areas was narrowed down to six. Work within these six areas continued in Year 4. Icons identifying each area are shown in Figure ES.1

Figure ES.1: Campus Best Practice work areas and icons

As new best-practice documents are approved at the national level, they are translated into English and published on both the GÉANT and TERENA websites [GÉANT-BP, TERENA-BP]. In Year 4, 16 new best-practice documents were published, generating a total of 58 documents.

With this comprehensive toolkit of best practice documents available, it is still a major challenge 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 about results and working methods. In Year 4, the Task team has done this

in various ways: talks at conferences, direct dialogue with NRENs, workshops in new countries, and European-level workshops.

In Year 4, the team gave a total of 16 presentations at networking conferences. These included the AfREN conference in Gambia, the TERENA Networking Conference (TNC), the EUNIS conference, the NORDUnet conference, the CARNet user conference, the ARNES twentieth-anniversary conference and the RoEduNet conference in Romania. The Task team also organised three European-level workshops in three different technical areas: network monitoring, IPv6 and wireless. Finally, the team set up kick-off workshops in four new countries: Lithuania, Bosnia and Herzegovina, France, and Montenegro. The latter two countries have decided to join Campus Best Practice for GN3plus. (France had already joined in GN3 Year 4.)

In this fourth and final annual report, each of the four original NRENs reflects upon the lessons they have learned during the four-year project. The following are the highlights from each national report:

- AMRES emphasises the difference between isolated/random activities aimed at improving the situation on campuses as opposed to a more structured approach through the Campus Best Practice model. The latter leads towards the establishment of a long-term and planned process of support that campuses can rely on in the future. A small financial investment is needed to begin a CBP activity; this, however, brings large benefits to the community.
- In Finland the MobileFunet and AccessFunet working groups have evolved into an accepted and recognised activity. The joint best-practice development is well-placed to support the community during the future turbulent years of structural changes and ever-increasing and diverse use of the network and its services.
- CESNET sees the key benefit of NA3 T4 as being the creation of a new forum for international dissemination of important, current challenges that concern many campuses. CESNET considers the workshops that were organised in NA3 T4 as the highest level of knowledge dissemination.
- For UNINETT, NA3 T4 has given new dimensions to the established national-level work. Campus Best Practice has created an international community where best practices have been published in English and where campus experts on the European level have met to present and discuss results and current challenges.

In conclusion, it is satisfactory to see such positive results from the joint Task team work. This would not have been possible had not *all* the members of the Campus Best Practice Task been so dedicated, positive and hard-working. In this picture one must not forget the many national working groups, where the real work is done, where important ideas are exchanged, discussed, elaborated and, in the end, written down as best practices.

The experiences of GN3 will be useful when Campus Best Practice continues its work in GN3plus. Then four new NRENs will join the Task team: FCCN, BREN, MREN and MARnet. In addition, all the Year 4 NRENs, Funet, UNINETT, CESNET, AMRES and RENATER, look forward to continuing the Task's work.

1 Introduction

Campus Best Practice is the name of one of the Tasks (Task 4) in Networking Activity 3, Status and Trends (NA3), of the GN3 project. The overall objective of the Task is to address the key challenges for campus networks in Europe, organise working groups and provide an evolving, and to-the-point set of best-practice documents for the community.

The Task challenges individual National Research and Education Network organisations (NRENs) to reinforce their national efforts in promoting best practices in campus networking. Better synchronisation of campus-directed efforts at the national level of research networking and on campus itself is essential for viable end-to-end services. Another target is to find the means to develop and maintain national best-practice recommendations.

The working methods in the Task build on the experiences from UNINETT's GigaCampus project (2006–2009). As part of that project, UNINETT organised a number of working groups in Norway dealing with campus issues in different technical areas. Participants from the relevant technical units at the universities were invited to participate in the working groups, which worked to propose recommendations in best-practice documents.

Four pilot NRENs have participated in the Task since the start of the GN3 project, namely UNINETT from Norway, CSC/Funet (hereafter Funet) from Finland, CESNET from the Czech Republic and AMRES from Serbia. In Year 4, RENATER from France joined the team.

This deliverable reports on the fourth year of the GN3 project. See deliverables [DN3.4.1,1, DN3.4.1,2 and DN3.4.1,3] for reports on the first, second and third years.

Vidar Faltinsen from UNINETT is the Task Leader. He reports to the NA3 Activity Leader, John Dyer of TERENA. The leading coordinators from the other pilot NRENs are Ivan Ivanovic (AMRES), Jiri Navratil (CESNET), Jari Miettinen (Funet) and Vanessa Pierne (RENATER). In Year 4 the Task team had twenty members. They have a key role in organising and leading working groups and producing best-practice documents. To achieve good results it is crucially important to attract a wide set of participants in the working groups organised at national level. These include participants from the NREN itself and from universities and colleges.

A high level of management commitment from the NRENs involved is considered essential. In order to succeed with this work, the NREN must be willing and dedicated to get involved with addressing the issues and problems at the campuses of its prime customers.

2 Approach

2.1 Technical focus areas

The Task team has continued its work in the six working areas on which it started to focus at the start of Year 3. Table 2.1 gives an overview of the areas and the NRENs that are contributing. The "(√)" notation in the table means that this is not a main contribution area for the NREN in question, but that work is, to some extent, conducted.

Area		UNINETT	AMRES	CESNET	Funet	RENATER
Ref	Name					
0	Task management and dissemination	√	√	√	√	√
1	Physical infrastructure	√	√			
2	Campus Networking, including IPv6	√	(√)	√	√	√
3	Wireless	√	(√)	(√)	√	
4	Network monitoring	√	√	√	(√)	
5	Real-time communications	√		√		
6	Security	√	√			√
	Number of technical focus areas:[1]	**6**	**3 (5)**	**3 (4)**	**2 (3)**	**2**

Table 2.1: List of focus areas applicable in Year 4

A brief description of the focus areas follows, along with the icons identifying each area.

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

Physical infrastructure. This area addresses the requirements for generic cabling systems on campus, both fibre and twisted pair. 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.

Campus networking. This area deals with the campus network itself, with the routers and switches as its basic building blocks. Requirements to 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 are given, many of which have been developed within the GÉANT community.

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 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 (DNS) is also dealt with.

2.2 Development process for best-practice documents

The NREN-led working groups within each country have continued to develop best-practice documents (BPDs) in Year 4. Appendix A gives an overview of the active working groups within each area in the contributing countries. The development process is unchanged. Figure 2.1 captures this process.

Figure 2.1: The development process for best-practice documents (BPDs)

2.3 Translation into English and web publishing

The Task team's approach to translation and web publishing has continued in Year 4. After a document is approved at the national level, it is translated into English and published on both the GÉANT and TERENA websites [GÉANT-BP, TERENA-BP].

An open-announcement mailing list, campus-bp-announcements@terena.org, is used for announcing new documents when they become available.

2.4 Task management

In Year 2, the Task team made an overall plan for the final two years of the project. In May 2012, a more detailed, internal Year 4 plan was agreed upon. Work in Year 4 has followed this plan. Each NREN has reported monthly on its progress and milestone status. These written reports have been complemented by monthly videoconference meetings. In addition, an internal face-to-face meeting was organised in Vienna, Austria on October 17 2012 (in conjunction with the GN3 symposium).

The monthly reports have been used as the basis for quarterly reports to the NA3 Activity Leader, who in turn used these to prepare his contribution to the quarterly progress reports of the GN3 project as a whole. These were submitted to the European Commission.

3 Results

The main product of the Task team's work is the growing toolkit of best-practice documents. The dissemination efforts are of complementary importance. The Task needs to get the message out to the campus network managers across Europe. In this process, it is important to establish contact with more NRENs and inform them about results and working methods. The Task team does this in various ways: talks at conferences, direct dialogue with NRENs, workshops in new countries, and European-level experts' workshops.

3.1 Best-practice documents

As mentioned in Section 2.3, the best-practice documents are published in English on both the GÉANT and TERENA websites [GÉANT-BP, TERENA-BP]. By the end of Year 3, 42 documents had been published. In Year 4, another 16 documents were published, making a total of 58 documents. Table 3.1 shows how these documents are distributed in the six working areas.

Area		Documents published
Ref	Name	
1	Physical infrastructure and AV	9
2	Campus networking, including IPv6	17
3	Wireless	8
4	Network monitoring	11
5	Real-time communications	5
6	Security	8
	Total	**58**

Table 3.1: Overview of documents published in English within each area at the end of GN3

The best-practice documents that were published in Year 4 are listed in Table 3.2 below. The abstracts for these new documents are provided in Appendix B. In addition to the new documents, five of UNINETT's best practice documents on physical infrastructure have been updated. Further, a paper on AMRES's experiences

with implementing the Campus Best Practice model was published (more information is provided in Section 4.2).

It should be noted that the best-practice documents are very popular. The Information Security best-practice document [UFS126] was the most downloaded document on the entire GN3 public website [GN3Website] in Year 4 with over 8,000 downloads.

Documents marked with an asterisk (*) will be publicly available after April 5 2013.

No.	Document	NREN	Area	Completed
1	Anonymity in Campus Networks	CESNET	Network monitoring	May 2012
2	Experiences with IDS and Honeypots	CESNET	Network monitoring	May 2012
3	Support for the Operation of IPv6 Multicast and Anycast	CESNET	Campus networking	Nov 2012
4	Virtualisation of Critical Network Services	CESNET	Campus networking	Nov 2012
5	The Technical Infrastructure of Data Centres*	CESNET	Campus networking	Nov 2012
6	FreeRADIUS Database Connection	Funet	Wireless	Jan 2013
7	Organising a Network Operations Centre on Campus	Funet	Network monitoring	Jan 2013
8	Lightpath Deployment: Guide for IT Support	Funet	Campus networking	Feb 2013
9	IPv6 Migration Guide	Funet	Campus networking	Feb 2013
10	Monitoring of RADIUS Infrastructure	AMRES	Network monitoring	Feb 2013
11	Centralised Web Traffic Filtering System*	AMRES	Security	Mar 2013
12	The Implementation of the AMRES VPN Service*	AMRES	Security	Mar 2013
13	Implementation of 802.1X in the Wired Network*	UNINETT	Security	Mar 2013
14	Guidelines for Information Classification*	UNINETT	Security	Mar 2013
15	IPv4 Multicast Setup in Campus Networks*	UNINETT	Campus networking	Mar 2013
16	Recommendations for IPv6 Addressing Plan for the HE Sector*	UNINETT	Campus networking	Mar 2013

Table 3.2: Best-practice documents published in Year 4

3.2 Dissemination

3.2.1 New poster and leaflet

In preparation for TNC 2012 in Reykjavik, Iceland in May 2012, a new poster and a new leaflet were prepared. The poster was accepted for the conference. Both poster and leaflet have been used at all the workshops and conferences in which the Team has participated in Year 4.

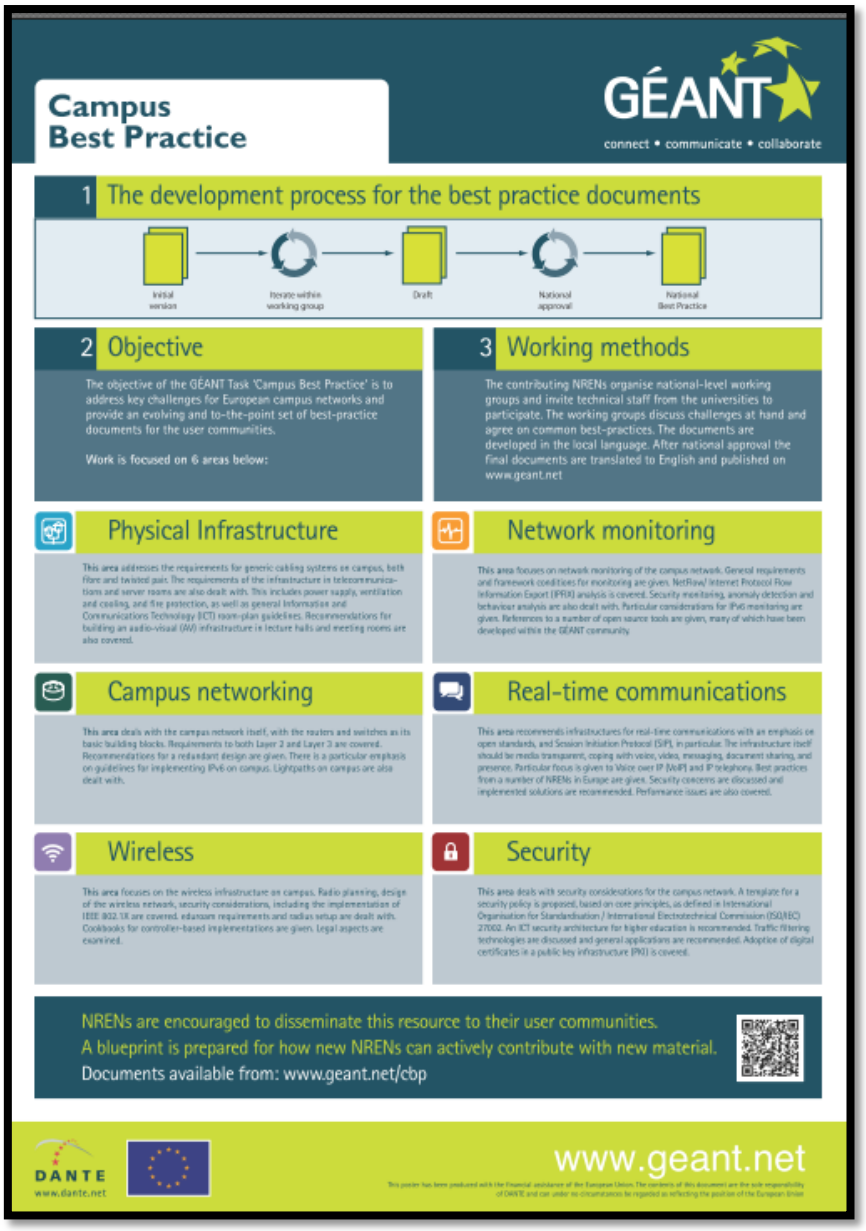

Figure 3.1: New Campus Best Practice poster

3.2.2 Presentations at conferences

The Task team has been active in Year 4, and has presented results at a number of conferences. A total of 16 presentations were given, as shown in Table 3.3. In some cases, the results of individual best practices were presented; in other cases, an overview of the Task team's results and working methods was given.

No.	Date	Event	Presentation	Presenter
1	May 14 2012	AfREN conference, Serekunda, Gambia	Campus Best Practices	Gunnar Bøe, UNINETT
2	May 21 2012	TNC 2012, Reykjavik, Iceland	Deploying IPv6 – practical problems from the campus perspective	Tomas Podermanski, CESNET
3	May 31 2012	CNRS Webinar (for French universities)	Recommendations for a redundant campus network	Vidar Faltinsen, UNINETT
4	June 20 2012	EUNIS 2012, Vila Real, Portugal	Cloud computing security considerations	Per Arne Enstad, UNINETT
5	June 20 2012	EUNIS 2012, Vila Real, Portugal	Impact of undesirable traffic on electrical power consumption in ICT rooms	Ivan Ivanovic, AMRES
6	Sept 19 2012	NORDUnet 2012, Oslo, Norway	A scalable SIP infrastructure for universities and colleges in Norway	Jardar Leira, UNINETT
7	Sept 19 2012	NORDUnet 2012, Oslo, Norway	Presenting and visualising network monitoring data using perfSONAR NC	Arne Øslebø, UNINETT
8	Sept 19 2012	NORDUnet 2012, Oslo, Norway	Flow analysis at 10+ Gbps	Olav Kvittem, UNINETT
9	Sept 19 2012	NORDUnet 2012, Oslo, Norway	Campus Network Weather Map	Morten Brekkevold, UNINETT
10	Sept 20 2012	NORDUnet 2012, Oslo, Norway	Security challenges in IPv6 from the campus perspective	Tomas Podermanski, CESNET
11	Nov 14 2012	CARNet user conf., Rijeka, Croatia	The AMRES campus best practice experiences	Ivan Ivanovic, AMRES
12	Nov 21 2012	TELFOR 2012, Belgrade, Serbia	Monitoring of radius infrastructure	Jovana Palibrk, AMRES
13	Nov 29, 2012	ARNES 20th anniversary, Ljubljana, Slovenia	Monitoring your campus network with the open source tool NAV	Morten Brekkevold, UNINETT
14	Dec 6, 2012	CNRS Webinar (for French universities)	Deploying IPv6 on campus	Tomas Podermanski, CESNET
15	Jan 18, 2013	RoEduNet Conference, Sinaia, Romania	AMRES experience with implementing the Campus Best Practice model	Mara Bukvic, AMRES

No.	Date	Event	Presentation	Presenter
16	March 5 2013	Yu Info Conference, Kopaonik, Serbia	Centralised system for web traffic filtering	Ivan Ivanovic, AMRES

Table 3.3: Presentations at conferences in Year 4

The team has also carried out dissemination activities in Africa. The African NREN community has shown significant interest in the Task's best-practice documents and team members were invited to give a presentation of the Task's work at the annual AfREN forum in Gambia in May 2012. There is a lot of focus on building capacity in AfREN and there is great potential for saving resources by using the Campus Best Practice documents.

Figure 3.2: Campus Best Practice discussed at AfREN forum in Gambia

3.2.3 Workshops in new countries

3.2.3.1 *Overview*

To capture the interest of new NRENs, the presentations that the Task team gives at conferences are vital. In a number of cases, this has led to a follow-up interest. The natural next step is further dialogue with these NRENs, through email, videoconferences, and/or face-to-face meetings. The Team then seeks to provide a

more in-depth explanation of what Campus Best Practice is about and how the NRENs and the campuses can benefit from this work.

Table 3.4 below presents a summary of the Campus Best Practice workshops held in new countries in Year 4. Further details are provided in Appendix D.

Workshop site	Hosted by	Date	Participants
Giraičiai, Lithuania	LITNET	August 28, 2012	70
Paris, France	RENATER	October 25, 2012	16
Banja Luka, Bosnia and Herzegovina	Elektrotechnicki fakultet Banjaluka	November 1, 2012	16
Zabljak, Montenegro	MREN	February 27, 2013	25

Table 3.4: Campus Best Practice workshops in new countries in Year 4

3.2.3.2 *Baltic countries*

In Year 3, the Task worked in the manner outlined in Section 3.2.3.1 with all three Baltic countries. In Year 4, this was followed up in Lithuania, where the Task team was present at the 17th annual LITNET conference held in Giraičiai on August 28 2012 and attracting 70 participants. A half day was dedicated to Campus Best Practice, with an emphasis on wireless (see Appendix D.1 for the agenda). The LITNET member universities are considering enlarging and upgrading their current WLAN networks, so the Task's presentations were timely and pertinent. The universities also got new ideas on how to improve their eduroam service.

3.2.3.3 *France*

The team's dissemination work in France in Year 3 triggered interest from RENATER and as of Year 4 RENATER is a participant in the Campus Best Practice Task; it will continue to be so in the GN3plus project. A kick-off workshop for the French campus community was held in Paris on October 25. The NA3 Activity Leader and the NA3 T4 Task Leader were both present and gave talks. 16 people participated in the workshop and the group decided to establish four working groups, three of them working in the campus networking area (metropolitan area network, IPv6 services, virtual switching) and the last in the security area (secure DNS). Each group aims to publish its first best-practice document in the summer of 2013.

3.2.3.4 *Bosnia and Herzegovina*

Thanks to AMRES the Task team has managed to establish interest in its work in Bosnia and Herzegovina. Bosnia and Herzegovina has significant challenges in terms of network infrastructure; in fact it is one of the last countries in Europe without an NREN. To get a clearer picture of the situation at the campus level, a survey questionnaire was developed during summer 2012 and sent to eight different universities in the country. The results showed that only 58% monitored their campus network, no one had implemented IPv6 and 8% had no wireless network at all, while only 33% had heard about the eduroam service. The Task team tailored a

workshop to address the most pressing challenges in Bosnia and Herzegovina. The workshop was held in Banja Luka on November 1 (see Appendix D.3 for the agenda). A survey conducted after the workshop proves that the event was very well received. The openLDAP lab and the network monitoring presentations received the highest score.

Figure 3.3: Campus Best Practice workshop in Banja Luka, Bosnia and Herzegovina

3.2.3.5 *Montenegro*

The Task's work in Montenegro is also giving positive results. The introductory presentation given by the team in the country in Year 3 was followed up in Year 4 with a full-day workshop held during the 18th information technology conference organised by MREN in collaboration with the University of Montenegro in the Zabljak Mountains. This time a survey was conducted prior to the workshop, to map fields of interest. Network monitoring turned out to be the hottest topic. Respondents reported that they need better tools to analyse traffic, on both the wired and wireless networks. The workshop included several talks on NetFlow-based network monitoring. Other topics were wireless (including eduroam), security (including the TERENA Certificate Service (TCS)), and an openLDAP lab (see Appendix D.4 for the full agenda). MREN is one of the new NRENs joining Campus Best Practice for GN3plus, so the workshop served as an excellent kick-off for the activity in Montenegro.

Figure 3.4: Campus Best Practice workshop in the Zabljak Mountains, Montenegro

3.2.4 European-level workshops

3.2.4.1 *Overview*

Another way of disseminating results is to organise European-level workshops where experts from a number of countries meet to present and exchange experiences. In Year 4 the Task team organised three such workshops, as shown in Table 3.5.

Topic	Workshop site	Hosted by	Date	Participants
Campus network monitoring	Brno, the Czech Republic	CESNET	April 25-26, 2012	70
IPv6	Helsinki, Finland	Funet	October 4-5, 2012	16
Wireless	Stockholm, Sweden	KTH Royal Institute of Technology and SUNET	March 13-14, 2013	43

Table 3.5: Campus Best Practice European-level workshops in Year 4

3.2.4.2 *Campus network monitoring*

The first workshop was in Brno in April 2012 and the topic was campus network monitoring. Participants discussed common practices in monitoring and shared their experiences with using different tools and processes. The workshop consisted of several sessions dedicated to general aspects of campus/LAN monitoring, detection of problematic traffic, monitoring of IPv6, monitoring of multi-media traffic, and experience in real-world network monitoring. The workshop had a total of 22 talks and there were 70 participants from 13 different countries. See Appendix E.1 for the agenda.

Figure 3.5: Campus network monitoring workshop in Brno, April 2012

3.2.4.3 *IPv6*

The second workshop focused on IPv6. It was organised by Funet in October 2012 and took place on an island close to Helsinki. The title was “The last IPv6 workshop?”, building on the fact that the main content providers now are supplying their services over IPv6 natively. Helped by successful events such as the Internet Society’s World IPv6 Launch Day on June 6th 2012 [IPv6Day], IPv6 has become mainstream. However, has everything been done on campus? Will this be the last IPv6 workshop? These were the key questions discussed by the 38 participants present.

The agenda for the two days is listed in Appendix E.2. There were 19 speakers in total, and, in addition, five live demos showing IPv4 to IPv6 multicast translator, IPv6 man-in-the-middle attack prevention and more. The workshop was streamed and 131 attendees followed day one, while 79 joined in on day two.

The workshop concluded that IPv6 is in a good state at the NREN backbone level and gradually improving at the campus level. The areas that need further attention were identified to be: firewalls and IP security solutions in general, home networks, mobile networks and the skills of the end users.

3.2.4.4 *Wireless*

The third experts' workshop took place in Stockholm in March 2013 and was titled "GN3 wireless workshop – the next wave". With Long-Term Evolution (LTE) networks and the new IEEE 802.11ac standard imminent, and eduroam spreading widely and becoming increasingly mature, the workshop aimed to answer such questions as: is everything in order in the wireless campus networks? Where should we focus our attention next? The workshop had 14 speakers and included a panel discussion on future trends based on Passpoint Hotspot 2.0, the IEEE 802.11u standard, Bring Your Own Device (BYOD) and more. The workshop was streamed and will be archived. In addition to the 43 attendees present, remote participants joined in; the number peaked at 37. See Appendix E.3 for the complete agenda.

4 Lessons Learned

Year 4 concludes four years of Campus Best Practice work within the GN3 project. As mentioned in the Introduction, the Task's working methods have been built on the model implemented in Norway during the GigaCampus project (2006–2009). Each country has set up national-level working groups that have worked to produce best-practice documents. Every country is different, and the experiences will vary accordingly. This chapter summarises the most significant lessons learned.

4.1 General experiences related to working groups' activity

The following observations and recommendations are based on the general experience of the working groups and are not country specific.

- Community building takes time.
- The working group leader should be motivated and able to motivate.
- Use the phrase "participant" rather than "member" in working groups. "Participant" is a more active term than "member".
- Since participants typically contribute as volunteers in their own institution's time it can be challenging for the working group leader to enforce progress.
- The key experts are usually very busy and have no time to write. If they are willing to write, then that is the best solution. Anyway, it is important to have them in the group, contributing to discussions.
- Establish an inner core of participants/contributors, but also allow a less formal outer community (open membership).
- Initially the NREN should pick best-practice topics. As the working group matures, the group should discuss and decide on new best-practice topics themselves.
- Draft best-practice documents should be prepared in advance of meetings to ensure the best discussion.
- Do not write text books. Write to the point about lessons learned. Documents that are too long are hard to maintain and fewer people will read them.
- The working-group meetings are highly valuable for informal talks and discussions on related topics.

4.2 Experiences of AMRES, Serbia

AMRES prepared a paper [AMRES-CBP] prior to the RoEduNet conference in Romania in January 2013. The paper gives a good overview of AMRES's experience with implementing the Campus Best Practice model (see Figure 4.1 and [GÉANT-CPB]). AMRES realises that it is the only NREN in the NA3 T4 team faced with solving the problem of poor technological development, the so-called digital divide problem. NRENs faced with this problem typically give undivided attention and significant budget to improving the backbone infrastructure and services, or external NREN connections. Insufficient attention has been focused on understanding and mitigating the problems of discontinuity in the quality of infrastructure, services and expertise of staff, which generally exist between the NREN backbone and campus network. The GÉANT Campus Best Practice Task examines a working model as one possible solution of the problem. The work is aimed at increasing cooperation between the NREN's member institutions in order to arrive at common technical solutions and recommendations for campuses.

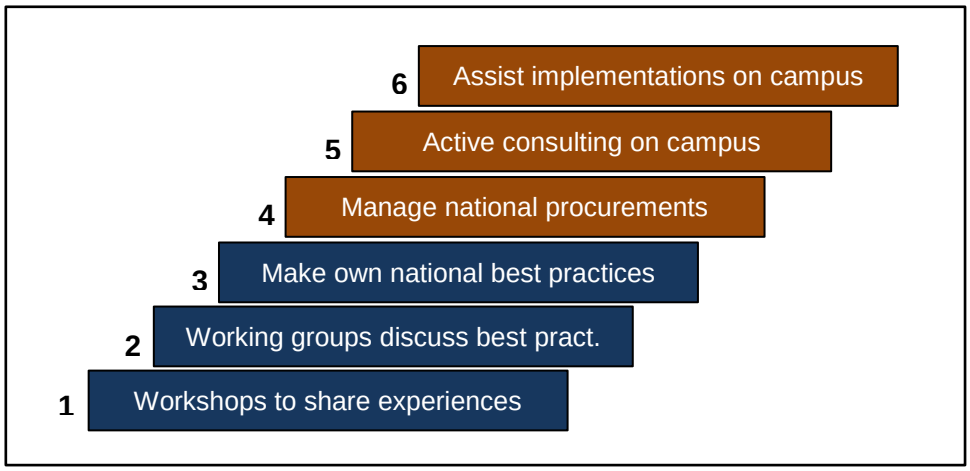

Figure 4.1: Campus Best Practice model

Prior to GN3, AMRES already had an established practice of inviting its campus communities to regular meetings (step 1 in the model). The next two steps from the proposed model were completely new to AMRES: organising the community into working groups for individual technical areas (step 2), and developing/using their own best-practice documents (step 3).

AMRES's criteria for selecting technical areas for working groups have been: a prominent need for recommendations in a particular area, experience gained in the area and/or campuses interested in the area. Based on these criteria, three groups were formed in AMRES: physical infrastructure, network monitoring and security. During the four years of GN3 the Serbian working groups have successfully produced 13 best-practice documents, of which 7 have been translated into English.

AMRES finds it important to emphasise the difference between isolated/random activities aimed at improving the situation on campuses as opposed to a more structured approach through the Campus Best Practice model. The latter leads towards the establishment of a long-term and planned process of support that campuses can rely on in the future. A small financial investment is needed to begin a CBP activity; this, however, brings large

benefits to the community. In order for the CBP concept to be sustainable in the NREN, it is necessary to ensure the support of technical staff on campuses, as well as that of strategic management and the bodies that fund NREN activities. Today, a solid base for the next steps has been created in Serbia. Further implementation of the steps of the model in AMRES will depend on the NREN's capability to implement them.

4.3 Experiences of CSC/Funet, Finland

Prior to GN3, during the period 2005–2009, the Funet community had several loosely connected special-interest groups. The groups typically had meetings during the annual "Funet technical days" conference. The two most active groups, the security community and video technology special interest group (VideoFunet) had regular meetings throughout the year. Just before the start of the GN3 project, three cooperation groups were established: SecureFunet, AccessFunet and MobileFunet. The purpose was to discuss and exchange experiences between the Funet member organisations and the NREN. The two latter groups had a particular focus on campus and naturally joined the GN3 Campus Best Practice Task when GN3 started.

The Campus Best Practice working method intensified the communication and interaction between CSC/Funet and the campuses. There was a remarkable flow of information and practices between the national and international community, where CBP work was the enabler. During the four years of GN3 the two working groups have delivered 11 best-practice documents, all relevant to current, hot topics at Finnish campuses. In other words, the groups reached step 3 in Figure 4.1.

CSC/Funet also organised two European-level workshops on IPv6. With the support of the NA3 T4 team in particular, and the GÉANT community in general, the workshops were able to cover a wide range of topics and raise awareness of current IPv6 challenges seen from the campus perspective. The jointly planned and organised events attracted excellent speakers and provided high-quality presentations. The workshops triggered the AccessFunet working group to compile the national campus IPv6 transition guidelines.

CSC/Funet has actively disseminated the Campus Best Practice working methods in its sister NRENs to the south, the Baltic NRENs EENET, SigmaNet and LITNET. CSC/Funet feels the work has been mutually beneficial and contributed naturally to the organisations' normal interaction.

The MobileFunet and AccessFunet working groups have evolved into an accepted and recognised activity in Finland. The joint best-practice development is well-placed to support the community during the future turbulent years of structural changes and ever-increasing and diverse use of the network and its services.

The higher steps in the Campus Best Practice model (see Figure 4.1) have also been addressed, but by other CSC/Funet departments. Traditionally there has been a rather strict division of work and responsibilities between CSC/Funet and the universities, where the campus border has been the demarcation line. The advent of cloud services will change this landscape; in fact the situation is already being transformed as new Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) services are being introduced.

4.4 Experiences of CESNET, Czech Republic

CESNET's path to participation in NA3 T4 was probably a bit different from that of the other partners. Since the beginning of its existence as an NREN, CESNET has had close contacts with the universities. CESNET has always been responsible for the national backbone, but, in the Points of Presence (PoPs), the engineering staff has worked 50% for the university and 50% for CESNET. In this way, the organisations have shared many networking engineers and CESNET has had no problems with distributing news and implementations and pushing solutions through to the universities. This is valid in particular for the activities that relate to the basic levels of networking. Staff were in daily contact, they were invited on regular networking meetings and they also attended similar education courses. This has also resulted in similar equipment being purchased by the different universities for their respective campus networks.

The second aspect that has formed CESNET's knowledge base stems from the fact that, for the past 10 years, CESNET has worked as a research institute, sponsored by the Ministry of Education, in the field of advanced networking. Within the framework of this programme, CESNET has organised many research teams in various fields, and always included specialists from the universities. In this way, CESNET built strong teams for developing optical networking, monitoring devices, multimedia, etc. These teams have studied the newest trends in their respective fields, found ways of implementing their new solutions, technologies and methods in the existing networks and, in turn, have offered this to the users. CESNET has regularly organised seminars and workshops where it has informed a diverse, professional community about what it is working on and how that community could use its new tools and solutions.

When the GN3 project was set up, CESNET noted and welcomed the Campus Best Practice Task initiated by UNINETT. The Task fully matched CESNET's previous activities and the NREN knew it would immediately be able to offer its experiences to the GÉANT international community. The questions were in what fields and how the participants could work most effectively. Some of CESNET's groups preferred to continue their work in their established research teams, presenting results in papers at scientific conferences or participating as specialists in the TERENA Task Forces. In four fields, however, CESNET found specialists who were ready to work within the framework of the GN3 Task. The fields were: reliability in campus networks, advanced monitoring, VoIP and IPv6. What was particularly positive was that practically everyone CESNET recruited for Campus Best Practice already worked at the university campus level.

Seen from the outside one might think that producing best-practice documents has been the main task for the CESNET Campus Best Practice team. The reality has been different. The main task has been to disseminate knowledge to the campus engineers. It has done this by establishing two new Campus Best Practice working groups: "WG Monitoring" and "WG IPv6". The groups have had regular meetings with well-prepared programmes. They have also had web pages and mailing lists where the participants have exchanged opinions about the latest news and events. The mailing lists have at times created engaging and long discussions.

CESNET sees the key benefit of NA3 T4 as being the creation of a new forum for international dissemination of important, current challenges that concern many campuses. CESNET considers the workshops that were organised in NA3 T4 as the highest level of knowledge dissemination, and is happy that it could actively participate in all of them.

4.5 Experiences of UNINETT, Norway

GN3 has given UNINETT an opportunity to add new dimensions to the work it started in the GigaCampus project (2006–2009)[2]. The Norwegian best-practice documents can now be translated into English and reach a much larger audience. NA3 T4 has created an international community where campus experts have met in workshops to present results (best practices) and current challenges. This has been of great value both to UNINETT and to Norwegian universities and colleges. In fact UNINETT believes that this has been of mutual benefit for all the NA3 T4 participating countries, and others that have signed up for its workshops or listened in on its talks at conferences, etc.

Leading the work of NA3 T4 has been an amazing journey, where the UNINETT participants have learned a lot about the challenges faced by other campus networks in other countries. There are many similarities, but also many differences, all equally interesting. Being a part of a dissemination effort in which UNINETT, together with the rest of the NA3 T4 team, has been given the opportunity to spread its lessons learned to a number of countries and campus networks across Europe, even Africa, has been thrilling.

It is of course satisfactory in itself that the Task has seen such positive results from its joint work. This would not have been possible had not *all* the members of the Campus Best Practice Task been so dedicated, positive and hard-working. It has been a pleasure for UNINETT to work with all the participants. In this picture one must not forget the many national working groups, where the real work is done, where important ideas are exchanged, discussed, elaborated and, in the end, written down as best practices.

UNINETT is glad that RENATER joined the team in Year 4. With a large country like France as a player, Campus Best Practice is likely to have an even stronger impact in Europe. UNINETT looks forward to the continued collaboration with *all* the current GN3 NRENs and, of course, to meeting the four new NRENs joining the Task for GN3plus.

[2] Read more about GigaCampus in chapter 3 of [GÉANT-CPB].

5 Plans for GN3plus

As previously mentioned, four new countries (FCCN, BREN, MREN and MARnet) have signed up for Campus Best Practice in GN3plus, bringing the total number of participating countries to nine. A kick-off workshop for the new Task team is already scheduled for April 2013 in Paris. The objective is to identify areas of interest among the new and existing NRENs and to agree upon new areas for inclusion; a work plan for the two-year project period will also be defined.

New working groups will then be organised at the national level. They will work according to established routines and contribute to the production of new best-practice documents. The Task team will also monitor the existing working areas and possibly withdraw exhausted areas (if any).

Methods for improving the quality of the best-practice documents will be investigated and applied as good practices are found. The activity is highly dependent on the quality of work done in the national working groups. The motto will be quality rather than quantity. The Task team estimates that another twenty documents will be translated and published during the two years of GN3plus, making nearly 80 documents in total. In addition, the oldest documents will be revised and updated.

The team will continue to focus on dissemination, both within the new countries and to other parts of Europe. The Task team intends to harness the GN3plus project support for dissemination and outreach. The goal is to reach even wider campus audiences and to report the encouraging results obtained. Talks and poster presentations at conferences will continue. Webinars will be considered. The team will organise more international workshops within the different areas of focus (five workshops are estimated). The workshops will, whenever possible, be streamed and archived.

The Task expects many new network engineers to join the existing and new working groups, and hopes that more campus personnel will benefit from the working results and that new NRENs will consider the Campus Best Practise model for their own country in the future.

Appendix A Working Groups

A list of active working groups in each country is given below. In some cases, there have been changes in the leadership of the working groups. 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 4 team. This means that the costs of their work are not charged to the GN3 project budget, but are borne entirely by the NREN.

A.1 UNINETT

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

Table A.1: Norwegian working groups

A.2 AMRES

Area	Group	Current leader	Founded
1	Physical infrastructure	Ivan Ivanovic	Nov 2009
4	Network monitoring	Ivan Ivanovic	Sep 2009
6	Security	Mara Bukvic	Sep 2009

Table A.2: Serbian working groups

A.3 CESNET

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

Table A.3: Czech working groups

A.4 Funet

The AccessFunet working group covers two areas: campus networking (2) and network monitoring (4).

Area	Group	Current leader	Founded
2,4	AccessFunet	Janne Oksanen and Juha Hopia	Feb 2010
3	MobileFunet	Wenche Backman-Kamila	May 2009

Table A.4: Finnish working groups

A.5 RENATER

Area	Group	Current leader	Founded
2	Metropolitan Area Network	Aurélien Méré	Oct 2012
2	IPv6 services	Jean Benoit	Oct 2012
2	Virtual switching	Jean-Pierre Feuillerat	Oct 2012
6	Secure DNS	Olivier Prins	Oct 2012

Table A.5: French working groups

Appendix B Abstracts of the Year 4 Best-Practice Documents

B.1 Anonymity in Campus Networks (CESNET)

This document focuses on the anonymity of campus networks. The negative aspects of anonymity for a university's reputation are discussed, and the challenges of solving security incidents are addressed. The main problem with anonymity occurs when an offender leaves footprints on the Internet that lead back to the university. This document provides recommendations on how to set up anonymity in the campus network from both a technical and legislative point of view.

B.2 Experiences with IDS and Honeypots (CESNET)

There are a number of ways to secure networks and network devices. A defence-in-depth approach is recommended, which will set up a defence perimeter at many levels. This can be complemented by deploying intrusion detection systems (IDSs). The document summarises CESNET's experiences in the field of intrusion detection and prevention.

B.3 Support for the Operation of IPv6 Multicast and Anycast (CESNET)

Multicast support under the IPv6 protocol is, in many ways, similar to multicast under IPv4. However, the additional address length has enabled the integration of some improvements. This document examines IPv6 multicasting in detail.

B.4 Virtualisation of Critical Network Services (CESNET)

This document describes a way to virtualise network servers that are required for the operation of a large campus network. This includes Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS),

Virtual Private Network (VPN), email, network monitoring, and RADIUS. The document is focused on the requirements to be considered when choosing the appropriate hardware for the job, with emphasis on the price/performance ratio, while maintaining all the benefits of the Vmware vSphere virtualisation platform. Configuration of network devices, Internet Small Computer System Interface (iSCSI) storage, and VMware vSphere hypervisors is covered. Practical experience and pitfalls are discussed. The benefits of virtualisation are emphasised.

B.5 The Technical Infrastructure of Data Centres (CESNET)

The purpose of a data centre is to provide operational, network, server, computing, and storage infrastructure for IT services, with sufficient, scalable capacity to operate these services using converged network technology, virtualisation of servers, and shared physical infrastructures. Data centre technology is currently developing at a rapid pace and many old rules no longer apply. The document describes various options that should be considered when designing and operating a data centre, in order to provide an optimal environment for upgrades and expansion of capacity.

B.6 FreeRADIUS Database Connection (Funet)

This document describes how to connect a FreeRADIUS server to external user databases and directories. For all practical purposes this is mandatory in order to minimise administrative work. The instructions follow the configuration of a FreeRADIUS server set up according to MobileFunet's FreeRADIUS Configuration best-practice document.

B.7 Organising a Network Operations Centre on Campus (Funet)

This document discusses Network Operations Centres (NOCs) from the perspective of Funet member organisations relative to the Funet NOC. The document includes a brief description of what a Network Operations Centre is and presents models for organising a NOC. The document also discusses commonly used tools that are essential to NOC operations and how to use them. Network monitoring tools are not included in the scope of this document.

B.8 Lightpath Deployment: Guide for IT Support (Funet)

The purpose of this document is to support IT personnel who are implementing a lightpath connection in the Funet network. This document contains a step-by-step description of what should be taken into consideration in the deployment of a lightpath. A lightpath is a dedicated data-transfer channel between two end points. Lightpaths are separately priced additional services provided by Funet.

B.9 IPv6 Migration Guide (Funet)

This document contains a high-level description of procedures that enable a controlled migration to IPv6 in an organisation currently using IPv4. The working order suggested in this document can be used, for example, as a framework for an IPv6 project plan, or otherwise as support in the planning of IPv6 migration. The starting point of this document was that the IPv4 protocol will be eventually phased out completely.

B.10 Monitoring of RADIUS Infrastructure (AMRES)

This document describes the implementation of the system used for monitoring a complex server authentication hierarchy based on the RADIUS protocol. The solution presented herein has been developed within the *eduroam*®[3] service of the Academic Network of Republic of Serbia (AMRES). The *eduroam*® authentication infrastructure requires a suitable monitoring system, which enables testing of the functionalities of all the RADIUS servers this service comprises. The monitoring system has been designed to provide a sufficiently detailed insight into the state of the RADIUS infrastructure, while not infringing upon user privacy as required under the *eduroam*® policy.

B.11 Centralised Web Traffic Filtering System (AMRES)

This document describes an IronPort firewall technical solution for web traffic filtering suitable for a campus environment. General ideas and techniques can be applied to equipment from other vendors. Design, configuration and positioning of the centralised firewall system are discussed. Important recommendations regarding mechanisms ensuring redirection and distribution of web traffic towards the firewall devices are dealt with. The advantages and shortcomings of a centralised system are discussed. Collection and analysis of traffic passing through the firewall are covered.

B.12 The Implementation of the AMRES VPN Service (AMRES)

This document describes the deployment of the AMRES VPN service. This solution involves the implementation of the Secure Sockets Layer / Transport Layer Security (SSL/TLS) protocol using OpenVPN technology. The main advantages of an OpenVPN solution are the implementation of advanced data encryption algorithms, the simplicity of installation and maintenance, and the fact that it is supported by almost all of the client and server platforms that are popular today. For user authentication, the AMRES VPN service relies on the RADIUS infrastructure, which was developed for AMRES' eduroam® service. The document also provides a detailed configuration of the relevant RADIUS servers on the FreeRADIUS platform.

[3] eduroam is a registered trademark of TERENA, the Trans-European Research and Education Networking Association.

B.13 Implementation of 802.1X in the Wired Network (UNINETT)

Ensuring the security of wired networks where physical access to outlets is unrestricted is resource-demanding. IEEE 802.1X is considered the most elegant solution. IEEE 802.1X is a Layer 2 protocol that enforces user or machine authentication. Typically, most types of traffic are blocked until the connected user or machine has been authenticated. The switch will forward Extensible Authentication Protocol over LAN (EAPoL) traffic between the supplicant (machine) and the RADIUS server, similar to a wireless deployment. The recommendations are generic, but include instructions for vendor-specific configuration of some switches. Client configurations for Windows, Apple and Linux are included.

B.14 Guidelines for Information Classification (UNINETT)

This document specifies the recommended guidelines for information classification in the higher education institutions in Norway. Means of identifying and in turn classifying the institution's information objects are given. Classification is done based on sensitivity and criticality. Adequate retention periods and disposal regulations are suggested. Careful measures should be taken before approving storage of information objects on mobile devices and cloud-based services. The guidelines will serve as an important tool set for information owners to secure mission-critical content.

B.15 IPv4 Multicast Setup in Campus Networks (UNINETT)

This document gives a recommendation for multicast setup at the campus level for higher education institutions in Norway. A general introduction to multicast is given. Both Any Source Multicast (ASM) and Source Specific Multicast (SSM) with typical deployment scenarios are covered. Layer 3 and Layer 2 challenges are discussed. Security issues are taken into consideration. Configuration examples for Cisco, Juniper and HP are provided. An overview of web-based and command line troubleshooting tools is included.

B.16 Recommendations for IPv6 Addressing Plan for the HE Sector (UNINETT)

Based on best practice in the higher education community in Norway, this document gives a very specific recommendation on how you should allocate your IPv6 address space in your campus environment. Emphasis is on simplicity and readability. The plan considers the recommended campus network security architecture. Prefix allocations within the same security zones crossing multiple campuses should facilitate summarised expressions in respective filtering rules. The document recommends static addresses for routers, switches and servers according to a proposed numbering scheme. Clients should rely on DHCPv6. An example of an IPv6 addressing plan is included.

Appendix C Workshops Organised at the National Level

The following workshops were organised at the national level in Year 4.

No.	Date	Area	Topic	Country	#days	Participants
1	April 2012	2	IPv6	The Czech Republic	1	21
2	April 2012	3	Wireless	Finland	½	8
3	April 2012	2	Campus networking	Finland	½	20
4	May 2012	5	SIP/VoIP workshop	Norway	2	12
5	September 2012	2	IPv6 workshop	Norway	1	14
6	November 2012	3	Wireless	Finland	½	13
7	November 2012	2	Campus networking	Finland	½	13
8	December 2012	2	Campus network workshop	Norway	2	62
9	March 2013	2	IPv6	Norway	1	16
10	March 2013	3	Wireless workshop	Norway	1	19
11	March 2013	3,4	IPv6 and network monitoring	CESNET	1	40

Table C.1: Workshops organised at the national level

Appendix D Workshops in new countries

D.1 Giraičiai, Lithuania – August 28 2012

Time	Presentation	Presenter
0900	Campus best practices in a nutshell	Gunnar Bøe (UNINETT)
0930	WLAN network planning	Anders Nilsson (SUNET)
1030	eduroam Configuration Assistant Tool (CAT) and eduroam companion demos	All
1100	WLAN network planning (cont.)	Anders Nilsson (SUNET)
1120	eduroam debugging	Tom Myren (UNINETT)
1150	Experiences with wireless deployment	Ricardas Sabaliauskas (Vilnius University)
1220	Q&A, discussion	All

Table D.1: Campus Best Practice workshop in Lithuania with focus on wireless

D.2 Paris, France – October 25 2012

Time	Presentation	Presenter
1200	Lunch	All
1300	Welcome to the workshop	Sabine Jaume (RENATER)
1315	Introduction to GN3	John Dyer (TERENA)
1330	Overview of CBP and UNINETT's experiences	Vidar Faltinsen (UNINETT
1400	Introduction to the discussion on French CBP working groups	Vanessa Pierne (RENATER)
1415	Discussions – all parties contributing	All

Time	Presentation	Presenter
1645	Wrap up – conclusions so far	Vanessa Pierne (RENATER)
1700	End of workshop	

Table D.2: Campus Best Practice workshop in France

D.3 Banja Luka, Bosnia and Herzegovina – November 1 2012

Time	Presentation	Presenter
0900	Campus Best Practice introduction	Ivan Ivanovic, AMRES
0920	CBP – the AMRES experience	Ivan Ivanovic, AMRES
1000	Filtering web traffic	Jovana Palibrk, AMRES
1045	Break	
1100	AMRES eduroam experience	Marko Stojakovic, AMRES
1200	eduroam demonstration	Marko Stojakovic, AMRES
1230	Lunch	
1330	Identity management	Marina Vermezovic, AMRES
1400	openLDAP exercise	Ivan Ivanovic, AMRES
1530	Break	
1545	Management and monitoring of network infrastructure	Ivan Ivanovic, AMRES
1615	NetFlow Monitoring	Ivan Ivanovic, AMRES
1700	End of workshop	

Table D.3: Campus Best Practice workshop in Bosnia and Herzegovina

D.4 Zabljak Mountains, Montenegro – February 27 2013

Time	Presentation	Presenter
0900	Campus Best Practice introduction	Ivan Ivanovic, AMRES
0920	CBP – the AMRES experience	Ivan Ivanovic, AMRES
0940	AMRES eduroam experience	Marina Vermezovic, AMRES
1020	Break	

Time	Presentation	Presenter
1040	AMRES TERENA Certificate Service (TCS)	Jovana Palibrk, AMRES
1120	ID management	Marina Vermezovic, AMRES
1200	Break until afternoon	
1600	OpenLDAP hands-on lab	All
1830	Threat analysis based on NetFlow	Milan Cabak, MREN
1900	Practical use of the NetFlow protocol	Ivan Ivanovic, AMRES
1930	End of workshop	

Table D.4: Campus Best Practice workshop in Montenegro

Appendix E European-Level Workshops

NA3 T4 organised three European-level experts' workshops in Year 4. This appendix presents the agenda of each workshop and a reference to presentations and further details.

E.1 Campus Network Monitoring Workshop – Brno, April 25–26 2012

Time	Presentation	Presenter
Day 1		
0900	Welcome	Vidar Faltinsen, UNINETT
0915	Anonymity in university campus networks	Aleš Padrta, ZCU Plzen
0945	CESNET offers IP monitoring service for universities	Tomáš Košnar, CESNET
1015	nfdump/nfsen	Peter Haag, SWITCH
1045	Break	
1100	Monitoring with flowmon probes	Jiri Tobola, INVEA-tech
1130	Flow-Based Monitoring of IPv6	Tomáš Podermanski, Matej Grégr— CESNET/VUT Brno
1200	Network security monitoring and behaviour analysis	Pavel Celeda, MU Brno
1230	renetcol – RENATER NetFlow collector	François-Xavier Andreu, RENATER
1300	Lunch	
1400	Analysis of tunnelled traffic	Matej Grégr, VUT Brno
1430	Ironport proxy servers	Ivan Ivanovic, RCUB/BUCC Beograd
1500	Share and visualise your data using the perfSONAR NC framework	Arne Øslebø, UNINETT
1530	Break	

Time	Presentation	Presenter
1600	Automatic topology detection and IPv6 machine tracking in campus networks	Morten Brekkevold, UNINETT
1630	Managing your network with Netmagis	Jean Benoit, University of Strasbourg
1700	Using Zabbix to monitor and manage lab PCs	Lukas Macura, SLU Opava
1730	End of first day	
Day 2		
0900	Experiences with IDS-based on honeypots	Radoslav Bodó, Michal Kostenec—ZCU Plzen/CESNET
0930	Application detection using Appflow and passive monitoring	Arne Øslebø, UNINETT
1000	NfQuery: A Privacy-Friendly Framework for Multi-Domain Threat Analysis	Serdar Yigit, Murat Soysal, Emre Yüce, ULAKBIM
1030	Break	
1100	Exploiting NetFlow: Detection of sophisticated threats	Karel Šimek, CognitiveSecurity
1130	Monitoring and analysing audio, video, and multi-media traffic on the network	Slavko Gajin, RCUB/BUCC Beograd
1200	Security Issues in IP Telephony and their Solutions	Miroslav Voznák, TU Ostrava
1230	Quality measurements in streaming media	Olav Kvittem, UNINETT
1300	Lunch	
1400	eduroam Monitoring	Jovana Palibrk, AMRES
1430	Simplify monitoring of a campus network with Nagios: Our experiences	Pierre Wallemacq, BELNET
1500	Nagios-Surfer—a quality reporting tool for Nagios	Teemu Kiviniemi, Funet
1530	What we have learned from the workshop	Jirí Navrátil, CESNET
1600	End of first day	

For presentations and other details, see [MonitoringWorkshop].

E.2 The Last IPv6 Workshop? – Helsinki, 4–5 October 2012

Time	Presentation	Presenter
Day 1		
0900	Welcome	Juha Oinonen, Funet

Time	Presentation	Presenter
0915	Supporting IPv6 in Data Centres and Hosting Platforms	Sami J. Mäkinen, Cybercom
0950	NORDUnet IPv6 Background, Status & Perspective	Frank Blankman, NORDUnet
1025	IPv6 deployment and adoption in HE in Norway	Gunnar Bøe, UNINETT
1100	Lunch	
1200	IPv6 on 3GPP mobile handsets	Teemu Savolainen, Nokia
1230	Email services over IPv6	Ondrej Caletka, CESNET
1300	IPv6 network filtering and firewalls	Pavel Turbin, F-Secure
1330	Extreme IPv6 Networking at Home	Jari Arkko, Ericsson
1400	Break	
1430	Requirements for IPv6 in ICT equipment	Jan Zorz, Go6 institute
1515	IPv6 security threads and mitigations	Eric Vyncke, Belgian IPv6 Council and Cisco
1600	End of first day	
Day 2		
0900	Intro to day 2	Juha Oinonen, Funet
0915	Lightning talk: Testing implementation of NAT66	Matej Gregr, CESNET
0922	Lightning talk: IPv6 status in BUC/AMRES	Ivan Ivanovic, AMRES
0929	Lightning talk: Promoting IPv6 and eduroam with mobile access points	Karri Huhtanen, Arch Red
0936	Lightning talk: Evading security appliances using IPv6	Olli-Pekka Niemi, Stonesoft
0943	Lightning talk: Today's IPv6 penetration amongst content providers and at the edge of the CESNET network	Tomas Podermanski, CESNET
0950	Break	
1000	Lightning demos	
	Promoting IPv6 and eduroam with mobile access points	Karri Huhtanen , Arch Red
	Evading security appliances using IPv6	Olli-Pekka Niemi, Stonesoft
	IPv6 man-in-the-middle Attack and Prevention Against It	Tomas Podermanski, CESN
	IPv4 to IPv6 Multicast Translator (Mcast46), DNS64, NAT64	Teemu Kiviniemi, Funet
	Dual-stack monitoring	Ville Mattila, Funet
1100	Lunch	

Time	Presentation	Presenter
1200	IPv6 deployment at Oslo and Akershus University College of Applied Sciences	Harald Terkelsen, Oslo University, College of Applied Sciences
1225	Extending the miserable life of IPv4	Jan Zorz, Go6 Institute
1245	“Open mic” discussion	Aleksi Suhonen, TUT
1330	Workshop result summary	Jani Myyry, Funet
1400	End of workshop	

For presentations and details, see [IPv6Workshop].

E.3 Wireless Workshop – Stockholm, 13–14 March 2012

Time	Presentation	Presenter
Day 1		
1200	Welcome to the workshop!	Anders Nilsson (SUNET)
1230	Campus best practices – what’s that?	Vidar Faltinsen (UNINETT)
1300	Developing wireless networks in Sweden	Fredrik Pettai (SUNET)
1330	Break	
1400	eduroam status overview	Miroslav Milinovic (Univ. of Zagreb)
1430	Advances in the GN3 project	Stefan Winter (RESTENA)
1500	Man-in-the-middle attack demo	Anders Nilsson (SUNET)
1530	Break	
1600	Panel discussion about eduroam future steps, Passpoint Hotspot 2.0, 802.11u standard, BYOT	
1700	End of day 1	
Day 2		
0900	Introduction to LTE technologies	Pete Vickers (Com4)
0950	Experiences of 4G networks	Maurice van den Akker (Surfnet)
1030	Break	
1100	eduroam monitoring	Jovana Palibrk (AMRES)
1130	eduroam authentication in NTLR, IdPs and SPs	Karri Huhtanen (Arch Red)
1200	Debugging eduroam at campus	Matti Saarinen (University of Helsinki)

Time	Presentation	Presenter
1230	Lunch	
1400	Do we need WLAN networks anymore?,	Peter Jerhamre (Cisco)
1430	Planning networks with 802.11ac standard in sight	Anders Nilsson (SUNET)
1500	Workshop summary, farewell,	Anders Nilsson (SUNET)
1530	End of workshop	

For presentations and details, see [WirelessWorkshop].

References

[AMRES-CBP]	"AMRES Experience with Implementing the 'Campus Best Practices' Model" http://www.terena.org/activities/campus-bp/pdf/amres_experience_with_cbp.pdf
[DN3.4.1,1]	Vidar Faltinsen, Wenche Backman, Mara Bukvic, Jiri Navratil, "Deliverable DN3.4.1,1: Annual Report on Campus Best Practices" http://www.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://www.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://www.geant.net/Media_Centre/Media_Library/Media%20Library/GN3-12-143_DN3-4-1-3_Campus-Best-Practice_v1.0.pdf
[GÉANT-BP]	www.geant.net/About_GEANT/Campus_Best_Practice/
[GÉANT-CPB]	GÉANT Campus Best Practices http://www.geant.net/Media_Centre/Media_Library/Media%20Library/geant-campus-best-practices.pdf
[GIGACAMPUS]	www.terena.org/activities/campus-bp/pdf/gigacampus_final_report.pdf
[GN3Website]	www.geant.net
[IPv6Day]	http://www.internetsociety.org/deploy360/blog/2012/01/world-ipv6-launch-on-june-6-2012-to-bring-permanent-ipv6-deployment/
[IPv6Workshop]	http://openwiki.uninett.no/geantcampus:ipv6_oct_2012
[MonitoringWorkshop]	http://www.ces.net/events/2012/campus-monitoring/
[TERENA-BP]	www.terena.org/campus-bp
[UFS126]	http://www.terena.org/activities/campus-bp/pdf/gn3-na3-t4-ufs126.pdf
[WirelessWorkshop]	http://www.eduroam.se/meetings/gn3wirelessworkshop.4.431755a013cdecf6abc10.html

Glossary

AfREN	African Research and Education Network
ASM	Any Source Multicast
AV	Audio Visual
BPD	Best-Practice Document
BYOD	Bring Your Own Device
CAT	Configuration Assistant Tool
CNRS	French National Centre for Scientific Research
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EAPoL	Extensible Authentication Protocol over LAN
EUNIS	European University Information Systems Organisation
HE	Higher Education
IaaS	Infrastructure as a Service
ICT	Information and Communications Technology
IdP	Identity Provider
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPFIX	Internet Protocol Flow Information Export
iSCSI	Internet Small Computer System Interface
ISO	International Organisation for Standardisation
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LTE	Long-Term Evolution
NA3	GN3 Networking Activity 3, Status and Trends
NA3 T 4	NA3 Task 4, Campus Best Practice
NOC	Network Operations Centre
NREN	National Research and Education Network organisation
NTLR	National Top-Level RADIUS
PaaS	Platform as a Service
PKI	Public Key Infrastructure
PoP	Point of Presence
RADIUS	Remote Authentication Dial-In User Service

SIP	Session Initiation Protocol
SP	Service Provider
SSL/TLS	Secure Sockets Layer / Transport Layer Security
SSM	Source Specific Multicast
TCS	TERENA Certificate Service
TELFOR	Telecommunications Forum
TERENA	Trans-European Research and Education Networking Association
TNC	TERENA Networking Conference
VoIP	Voice over IP
VPN	Virtual Private Network
WLAN	Wireless Local Area Network