18.05.10

Deliverable DN3.4.1,1: Annual Report on Campus Best Practices

Deliverable DN3.4.1,1

Contractual Date:	31-03-2010
Actual Date:	18-05-2010
Grant Agreement No.:	238875
Activity:	NA3
Task Item:	T4
Nature of Deliverable:	R (Report)
Dissemination Level:	PU (Public)
Lead Partner:	UNINETT
Document Code:	GN3-10-120v2
Authors:	Vidar Faltinsen (UNINETT), Wenche Backman (Funet), Mara Bukvic (AMRES), Jiri Navratil (CESNET)

Abstract

'Campus Best Practice' is the title of one of the Tasks (Task 4) in the Networking Activity 'Status and Trends' (NA3) of the GN3 project. The overall objective of the Task is to address 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 first year of the GN3 project (April 2009 – March 2010) and the results of that work.

Table of Contents

Executive Summary

‘Campus Best Practice’ is the title of one of the Tasks (Task 4) in the Networking Activity ‘Status and Trends’ (NA3) of the GN3 project. The overall objective of the Task is to address 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 first year of the GN3 project (April 2009 – March 2010) 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, for example, physical infrastructure, network architecture, mobility, security and operations/measurements. Participants from the relevant technical units at the universities were invited to participate in the working groups, which work to propose recommendations in best-practice documents.

Four pilot NRENs are participating in the current Task of the GN3 project, namely UNINETT from Norway, CSC/Funet from Finland, CESNET from the Czech Republic and AMRES from Serbia. During the first year, each of these NRENs organised national working groups and a start was made with the international collaboration on best practices.

At the start of the project, an initial set of technical focus areas was identified. Together with the management and dissemination work they form the subtasks of the ‘Campus Best Practice’ Task. The technical focus areas are: procurement, basic infrastructure, audio visuals, ligthpath service, LAN infrastructure and IPv6, wireless, network monitoring, SIP and IP telephony, and security. Not every pilot NREN is involved with every focus area, but there is a good overlap.

Chapter 3 of the current report describes the main results achieved in the first year of the project. It begins with a description of the starting position of each of the four pilot NRENs, and the working groups created by them. The chapter then describes the focus areas one by one, and lists the results achieved. In total, 24 reports and best-practice documents were produced during the year. These are listed in section 3.3, and abstracts of all these documents are reproduced in Appendix C.

The main conclusion is that the Task work is in its early stages, but that the results obtained during the first year are quite satisfactory.

The Task team has emphasised the focus on national working groups. The reason for this is that community building is far easier to achieve within a country, where there is a joint culture and language. Therefore the Task team focuses in the first two years of the GN3 project on results within the countries of the four pilot NRENs. When working groups within those countries are maturing and best-practice documents are evolving, it will naturally attract interaction and collaboration across borders.

In the second year of the GN3 project the Task team will devote more effort to dissemination. Mature best-practice documents will be published in English. Workshops will complement the messages written in the best-practice documents. The Task team will make presentations at national and European conferences.

1 Introduction

'Campus Best Practice' is the title of one of the Tasks (Task 4) in the Networking Activity 'Status and Trends' (NA3) of the GN3 project. The overall objective of the Task is to address 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 Task aims to challenge individual National Research and Education Networking organisations (NRENs) to reinforce their national efforts in promoting best practices in campus networking. Better synchronisation of efforts at the national level of research networking and on campus 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, for example, physical infrastructure, network architecture, mobility, security and operations/measurements. Participants from the relevant technical units at the universities were invited to participate in the working groups, which work to propose recommendations in best-practice documents.

Four pilot NRENs are participating in the current Task of the GN3 project, namely UNINETT from Norway, CSC/Funet (hereafter Funet) from Finland, CESNET from the Czech Republic and AMRES from Serbia. During the first year (April 2009 – March 2010), each of these NRENs organised national working groups and a start was made with the international collaboration on best practices. At the moment, the work of the Task team is carried out according to an internal two-year plan. That plan foresees the production of a number of best-practice documents. In addition, workshops are organised, in each of the four countries, and also aiming at the European level.

In the early phases of the Task work, participation is predominantly by working groups set up by the four pilot NRENs. In the last two years of the GN3 project, there will be a stronger emphasis on a wider dissemination of the results of the work and promoting the implementation of best practices across Europe.

Vidar Faltinsen from UNINETT is the Task Leader. He reports to the NA3 Activity Leader, Karel Vietsch from TERENA. The leading coordinators from the other pilot NRENs are Mara Bukvic (AMRES), Jiri Navratil (CESNET) and Wenche Backman (Funet). At the end of the first year, the Task team had sixteen 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 management commitment of 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 Subtasks and two-year plan

The Task team held its kick-off meeting in Trondheim, Norway on 27-28 May 2009. Here there was a wide-ranging discussion of current challenges at the campus level. Each of the pilot NRENs presented its own experiences and thoughts for the future. One of the authors of the EARNEST report on Campus Issues [1], Michael Nowlan, gave a presentation of the EARNEST findings and participated in the follow-up discussion.

On the second day of the meeting, the team elaborated on how to organise and set up the activities in the Task at national level. UNINETT presented their experiences from the GigaCampus project. Prior to the meeting, a document, UFS101 [2], had been made available that describes how the Norwegian working groups were organised and best-practice documents were produced.

An initial set of technical focus areas was identified. Together with the management and dissemination work they form the subtasks of the 'Campus Best Practice' Task. Not every pilot NREN is involved with every focus area, but there is a good overlap. The subtasks are described in more detail in section 3.2 of the current report.

	Subtask	UNINETT	AMRES	CESNET	Funet
0	Task management and dissemination	X	X	X	
1	Procurement	X			
2	Basic infrastructure	X	X		
3	Audio Visual (AV)	X			
4	Lightpath service				X
5	LAN infrastructure and IPv6	X		X	X
6	Wireless	X		X	X
7	Network monitoring	X	X	X	X

	Subtask	UNINETT	AMRES	CESNET	Funet
8	SIP and IP telephony	X		X	
9	Security	X	X		
	Number of subtasks	**9**	**4**	**5**	**4**

Table 2.1: Current subtasks

The kick-off meeting also started the planning process that led to the Task team's internal two-year plan. By July 2009, each pilot NREN had made its own planning with milestones and commitment of resources. These plans were discussed further in the team and then put together into an overall two-year planning for the Task. This planning has turned out to be a very effective tool for the team. All pilot NRENs remained committed to deliver results according to the milestones that were agreed in July 2009. Looking back on the first year, it turns out that almost all milestones have been reached and most of them on time. Appendix A gives an overview of milestones achieved, and more details can be found in section 3.2.

2.2 Task management and support

The Task team mainly uses email for its internal communication. In addition, the team had a meeting by videoconference every month, and the minutes of those meetings were made available to the team. Before each meeting, every pilot NREN reported on the activities in the previous month and in particular on the status of milestones. These monthly reports were used as the basis for quarterly reports to the NA3 Activity Leader, who in turn used those for his contribution to the quarterly progress reports of the GN3 project as a whole that were submitted to the European Commission.

Some of the reports that the Task will deliver are written in other languages than English – namely in Norwegian, Czech, Finnish or Serbian – and therefore need to be translated. The budget for hiring professional translators is part of TERENA's share in the overall budget of the GN3 project. Translators are therefore sought by way of open calls for proposals published by TERENA.

The tender process for Norwegian-to-English translators was run in the autumn of 2009. It resulted in contracts with two companies, which were signed in December. Both companies were given assignments to translate specific Norwegian documents in the January-March 2010 period. A similar tendering for Czech-to-English translators was carried out early in 2010. It resulted in a contract with a single company, which was signed in March. A call for proposals for Finnish-to-English translators is to be published early in the second year of the GN3 project's lifetime.

3 Results

3.1 Working groups in each country

An important component of the plan for the first year of the Task's work was to establish working groups at the national level corresponding to the agreed subtask commitments (see Table 2.1). In this chapter we give an overview of the working groups that were operational at the end of the first year. We also provide some background information on the situation of each pilot NREN.

3.1.1 Norway

Prior to the start of the GN3 project, UNINETT had established its working groups as part of the GigaCampus project. Currently there are eight working groups in total. The table below lists the current working group leaders; in some cases there have been changes of working group leadership in the past years. In three cases, which are marked with an asterisk in the table below, the current working group leader is not a member of the Task team. This means that the costs of his work are not charged to the GN3 project budget but are borne entirely by UNINETT.

Subtask	Group	Current leader	Founded
1	Procurement	Lars Skogan *	Jan 2006
2	Basic infrastructure	Roald Torbergsen *	Jan 2006
3	AV	Magnus Strømdal *	Mar 2008
5	Network architecture	Gunnar Bøe	Jan 2006
6	Mobility	Tore Kristiansen	Dec 2006
7	Network monitoring	Vidar Faltinsen	Jun 2005
8	Person-to-person communication (SIP)	Jardar Leira	Jan 2006

Subtask	Group	Current leader	Founded
9	Security	Gunnar Bøe	Jun 2008

Table 3.1: Norwegian working groups

UNINETT has very positive experiences with the working group concept. It requires an active working group leader who sets the agenda and invites practitioners to workshops with interesting topics. For the production of best-practice documents the key author needs to prepare an outline with some content before a fruitful discussion can take place. Typically the prominent experts are very busy and do not have much time to devote to the working groups, but they will happily share their experience and knowledge in meetings and take part in discussions with colleagues from other universities.

3.1.2 Serbia

Before the start of the GN3 project, there was no experience in Serbia with the concept of national working groups for specific technical areas of campus networking, nor with the production of best-practice documents. It was therefore a first priority for the AMRES members of the Task team to explain the benefits of organising working groups and writing national best-practice documents to the higher-education community in Serbia. AMRES promoted these objectives both in direct contacts with colleagues and in regular meetings of IT staff. At a national meeting in July 2009, the Serbian members of the Task team explained the concepts of best-practice documents and working groups, the UNINETT experience (including the model described in UFS101 [2]) and the reasons for AMRES' choice of areas of interest. AMRES installed a wiki and used it as a new way to exchange information within the higher-education sector in Serbia.

Later in 2009, AMRES created three working groups, as shown in the table below. In one case, marked with an asterisk in the table below, the current group leader is not a member of the Task team. This means that the costs of his work are not charged to the GN3 project budget but are borne entirely by AMRES.

Subtask	Group	Current leader	Founded
2	Basic infrastructure	Esad Saitovic	Nov 2009
7	Network monitoring	Slavko Gajin *	Sep 2009
9	Security	Mara Bukvic	Sep 2009

Table 3.2: Serbian working groups

Besides AMRES staff members, technicians from four universities and several research institutes are participating in the working groups. Each working group has 6-10 members.

AMRES organised a workshop on network monitoring with participants from Serbian universities and from five other countries; details can be found in Appendix B of the current report. The university staff expressed

enthusiasm and hoped for similar workshops in other areas. Workshops are seen as a good way to trigger participation in working groups.

Best-practice documents are initially produced in the Serbian language, because requiring technicians in the country to write in English would have been an obstacle to creativity and productivity. Because the Serbian language is similar to other languages in southeast Europe, these reports can be understood and used in other countries in the region. Nevertheless these documents will be translated into English later, in order to benefit the whole of Europe.

3.1.3 Czech Republic

The goals of the current Task of the GN3 project are not new to CESNET. In the past years, CESNET activity teams have carried out similar work as part of CESNET's national mission, not in exactly the same form as the GigaCampus working groups, but producing similar results. Because of the success of that set-up and CESNET's limited resources for the Task work, CESNET will use its existing structure and national goals rather than follow the Norwegian GigaCampus model in its entirety.

During the first year of the GN3 project, CESNET has sought pragmatic ways to use the existing CESNET infrastructure and style of working to achieve the Task goals. It is encouraging staff members from relevant technical units at universities to volunteer to participate in the preparation of best-practice documents. It will be a challenge to include a broader group of people in the iterative process of gradually improving the documents. National and international workshops are seen as a useful forum for discussions before best-practice documents are issued. A workshop on a single theme organised as part of the Task work is a good way to achieve this goal.

In the first year of the GN3 project CESNET created three working groups; see the table below. The working groups on network monitoring and on IP telephony each have participants from five universities, while fourteen universities are actively participating in the IPv6 working group. In two cases, which are marked with an asterisk in the table below, the current working group leader is not a member of the Task team. This means that the costs of their work are not charged to the GN3 project budget but are borne entirely by their employers: the Technical University of Brno in the case of Petr Lampa and CESNET in the case of Jan Ruzicka.

Subtask	Group	Current leader	Founded
5	IPv6	Petr Lampa *	Jan 2010
7	Network monitoring	Tomas Podermanski	Nov 2009
8	IP Telephony	Jan Ruzicka *	Nov 2009

Table 3.3: Czech working groups

3.1.4 Finland

In the last couple of years Funet has recognised the need to get more involved in activities at the campus level. Close cooperation between Funet and the staff of IT departments at universities is expected to improve the quality of services provided to end-users. Furthermore, large synergy effects can be achieved through collaboration between IT departments of different universities.

During the first year of the GN3 project, Funet established two working groups and put effort into making them well-known in the community and thereby raising the interest for the production of best-practice documents in Finland. The first working group in the table below covers a wide area and will in practice carry out its work in subgroups. As indicated by the asterisk in the table, its leader is currently not a member of the Task team. This means that the costs of his work are not charged to the GN3 project budget but are borne entirely by Funet.

Subtask	Group	Current leader	Founded
4, 5, 7	AccessFunet	Janne Niemi *	Feb 2010
6	MobileFunet	Wenche Backman	May 2009

Table 3.4: Finnish working groups

In order to get a clear picture of the status and needs of Finnish campuses, Funet initially focused on carrying out surveys and analysing the results. The challenges and immediate needs that were identified will be used as focus areas for the first best-practice documents. In this way Funet hopes to achieve that the best-practice documents will be disseminated widely and used well.

Prior to the start of the GN3 project, Funet had established a wiki for collaboration and sharing of experience in Finland. During the first year of the project, the wiki pages served as a working environment for the production of best-practice documents, with reading and writing privileges for the staff of IT departments of universities and research institutes. However, most of the input was received orally during meetings.

3.2 Results of each subtask

In this section we summarise the results obtained in each technical focus area. The NRENs contributing to each subtask are listed in parenthesis. In the text we refer to documents that have been produced; a complete list of these can be found in section 3.3. The abstracts mentioned are available in Appendix C of the current report.

It should be noted that although it is reported below that in some cases the work on a document was completed, actually at the end of the first year of the GN3 project none of these documents had been published in its final layout with the proper references and in a common format. It will be a priority in the first months of the second year to put these completed texts in the final format and make them publicly available.

3.2.1 Procurement (UNINETT)

UNINETT has good experiences with organising common procurement processes for the benefit of the entire higher-education community in Norway. During the GigaCampus project (2006-2009), in total 30 contracts were concluded in ten distinct areas. The work was done by working groups consisting of staff members from UNINETT and universities. It is expected that other countries can benefit from these experiences. In the subtask UNINETT focuses on making its procurement best practices available. A document on this is planned for May 2010. The abstract was completed in January 2010.

3.2.2 Basic Infrastructure (UNINETT, AMRES)

This subtask deals with producing, developing and maintaining best-practice documents in the area of basic infrastructure (generic cabling, power supply, cooling etc in ICT rooms). Prior to the start of the GN3 project, UNINETT had developed five best-practice documents in this area. The documents were updated (to version 3) as part of the GN3 project. This work was finished in December 2009 and the English translation was completed in February 2010.

AMRES is also active in this subtask. It established a working group in November 2009 and scheduled milestones for producing best-practice documents in the area. It is planned that by March 2011, four documents will be completed. The work on the first document, which is about generic cabling systems, has started and a draft is planned to be available in April 2010. The Serbian working group will use the Norwegian documents for their work, but will need to adopt the material to the local environment and regulations.

3.2.3 Audio Visual (UNINETT)

Audio visual (AV) infrastructure will be increasingly important for universities in the future. We foresee a development where network-based services such as streaming, multipart conferencing etc. will be used for lectures to a much greater extent.

AV infrastructure is a complex area and the pitfalls are numerous. There is a demand for formulating common requirements. Since 2008 UNINETT has an operational working group and two comprehensive best-practice documents were completed in May 2009, while a third document is scheduled for December 2010. In March 2010 the document titled 'Technical and Functional System Requirements for AV Equipment' was completed in English. The English version of the second document, 'Functional description of AV equipment in lecture halls and meeting rooms', is scheduled for April 2010.

3.2.4 Lightpath service (Funet)

Providing end-to-end optical connections is a fairly new service for NRENs; it introduces a new set of interesting possibilities. In order to reach the end-user environment, hybrid networking will typically pose new requirements for the campus infrastructure. The subtask will base its work on the ongoing DWDM campus experiences in Finland; it will produce a best-practice document on how to use lightpaths on campus.

In the first year of the GN3 project, a national survey was conducted in Finland. A summary report on that survey was completed in February 2010 (in Finnish, the abstract was translated in English). The best-practice document mentioned above is scheduled for November 2010.

3.2.5 LAN infrastructure and IPv6 (UNINETT, CESNET, Funet)

This subtask deals with the campus network itself. It will formulate requirements for equipment with functionality for layer 3, layer 2, multicast, IPv6, security etc. Also network design is important, with an emphasis on resilience. A series of cookbooks on configuration will be produced. Lessons learnt from end-to-end performance surveys will be included in the work.

In March 2010, an English translation was produced of UNINETT's best-practice document 'Recommended configuration for switches in campus networks'. In December 2009, CESNET produced an English draft of the

best-practice document 'Recommended Resilient Campus Network Design'. The document describes a test set-up and its results. CESNET also produced a cookbook for configuring HP switches in campus networks; this document is currently in Czech, the English translation is scheduled for April 2010. UNINETT has a similar cookbook and it will be investigated if the two documents can be merged during the second year of the GN3 project. Moreover, prior to the start of the GN3 project UNINETT published equivalent cookbooks for Cisco and Alcatel equipment; English translations of these cookbooks are scheduled to be produced in the second year of the project.

Funet carried out two interesting surveys: one on end-to-end performance and the other on network hardware used in Finnish campus networks. The survey reports were completed in March 2010 in the Finnish language, with abstracts in English. Based on the survey findings, Funet will make a recommendation to its campus community as to which equipment to use on campus and the best ways to set it up.

This subtask will also have a particular focus on IPv6 deployment on campus. The current situation is that IPv6 is implemented at the NREN level, but few universities have implemented IPv6 on campus. Formulating best practices in IPv6 transition on campus is thus an important objective of the subtask. CESNET created a working group on IPv6 in November 2009. It is also participating in a pilot programme with HP to test IPv6 functionality.

3.2.6 Wireless (UNINETT, CESNET, Funet)

The subtask deals with the wireless infrastructure on campus. Best practices on WLAN network planning, WLAN security, access point set-up, eduroam implementation etc. will be included in the subtask. The best practices will be based on the vast amount of experience gained from campus wireless build-outs. Implementing good wireless networks is not easy, the pitfalls are many and lessons learnt should be disseminated.

In October-November 2009 Funet conducted a survey of the current status of wireless networks in Finland. The summary report, written in English, was completed in December. Wenche Backman presented the results in a meeting of TERENA's task force TF-Mobility and Network Middleware in Vienna in February 2010.

In November, Funet arranged a national course on server configuration for eduroam. The course was fully subscribed with twelve participants. During the course, the participants learned to configure a FreeRADIUS server and connect it to the eduroam infrastructure. In addition, they learned to configure access points and supplicants.

The MobileFunet working group had several meetings and produced a draft version of its first best-practice document 'Best practice on WLAN security' in March 2010. This document is scheduled to be published as a national best-practice document in May 2010 and will subsequently be translated to English. A best-practice document from UNINETT on a similar topic (recommended security systems for wireless networks), which was originally written in December 2007, was translated into English. A joint workshop will be organised in the second year of the GN3 project, at which the recommendations from the two countries can be compared.

Two other best-practice documents, on network planning and equipment configuration, are scheduled to be produced by Funet in the second year of the GN3 project. UNINETT is working on a new recommendation titled 'A roadmap to installation and set-up of a Cisco controller in an 802.1X and eduroam environment'. The document is due for translation in June 2010. CESNET contributed with a cookbook for configuration of HP wireless equipment (in Czech, due for translation in April 2010).

3.2.7 Network monitoring (UNINETT, AMRES, CESNET, Funet)

A comprehensive set of tools is necessary for professionally operating a campus network. The tools may be commercial, open source or tailor-made, and they should (at some level) be integrated. The subtask will survey the field of network monitoring and share experiences and recommended best practices.

All four pilot NRENs are engaged in this subtask and they all have a lot of experience in the field. The Task team decided that an early kick-off workshop would be helpful. The workshop was hosted by AMRES in Belgrade in 20-21 October 2009. Besides participants from the four countries represented in the Task team, AMRES invited participants from two neighbouring countries, FYR Macedonia and Montenegro, and from a number of Serbian universities. There were altogether 31 participants at the workshop; the programme of the event included 21 presentations and numerous fruitful discussions.

Since the workshop, the Serbian working group on network monitoring produced a best-practice document on recommended network management architecture (in Serbian, with an English abstract). AMRES is planning a follow-up document on NMS tool configuration in the second year of the GN3 project.

As part of the GigaCampus project, UNINETT deployed a number of self-developed and open-source management tools on campus networks around Norway. For the second year of the Task work, cooperation with Funet is planned on deployment and beta testing of the NAV (Network Administration Visualised) tool in Finland.

CESNET plans to produce a report on the Czech experiences with methods and tools for network monitoring in June 2010 and to organise a follow-up workshop in September. Funet is planning to produce a national report in June and to complete a best-practice document on the subject in December 2010.

3.2.8 SIP and IP Telephony (UNINETT, CESNET)

This subtask deals with the challenges on campus related to step-by-step migration from traditional PBXs to VoIP and SIP. A SIP infrastructure will not only reduce traffic cost, but also include the possibility to offer new and integrated services like video, presence, messaging and other applications.

UNINETT gained experience with SIP throughout the GigaCampus project and has a strategy in place to offer SIP services to the universities and university colleges in Norway. A report that proposes an architecture and a suitable migration scheme was completed in February 2010 and translated to English in March 2010.

CESNET created its working group on IP telephony in November 2009. The group produced a report on current IP telephony solutions in Czech universities (March 2010). CESNET will also organise an international open workshop on VoIP on 29-30 April 2010 in Prague, with contributions from all four pilot NRENs.

3.2.9 Security (UNINETT, AMRES)

This subtask involves work at several levels. A sound security architecture with best practices on zone implementation and packet filtering is of key importance for campus networks. At the policy level, every university should have an approved security policy (i.e., approved by the university management). The subtask will produce best practices to guide the security work on campus in the right direction.

Since January 2008 UNINETT put an emphasis on helping the Norwegian higher-education sector to get a security policy in place. A generic security policy template has gradually evolved during this process. Based on

the GigaCampus experience UNINETT is working on a best-practice document that is scheduled to be completed in May 2010. The abstract was finalised in March. The UNINETT working group on security is also planning to produce a best-practice document on security architecture in the second year of the GN3 project.

AMRES created its working group in September 2009. The group's first draft document, 'Best practice for packet filtering', was completed in March 2010 (in Serbian, abstract in English). The document is scheduled to be published as a national best-practice document in May 2010.

3.3 Reports and best-practice documents produced

As described in section 3.2, a number of reports and best-practice documents have been produced and/or translated during the first year of the GN3 project. The table below gives an overview (see also the legend).

	Document	NREN	Area	Status	GN3	Language
1	Definition of U engineering task force and the UFS documents	U	0	BPD	Tr	English
2	Procurement process best-practice document	U	1	Abst	Part	English
3	Requirements for generic cabling systems	U	2	BPD	UpTr	English
4	Requirements for the design of ICT rooms	U	2	BPD	UpTr	English
5	Power supply requirements for ICT rooms	U	2	BPD	UpTr	English
6	Ventilation and cooling requirements for ICT rooms	U	2	BPD	UpTr	English
7	Fire protection requirements for ICT rooms	U	2	BPD	UpTr	English
8	Description of AV equipment in lecture halls and meeting rooms	U	3	BPD	Tr	English
9	System requirements for AV equipment	U	3	BPD	Tr	English
10	Report on current status of lightpaths in campuses	F	4	Rep	All	Finnish
11	Recommended configuration for switches in campus networks	U	5	BPD	Tr	English
12	Recommended resilient campus network design	C	5	Draft	All	English

	Document	NREN	Area	Status	GN3	Language
13	Cookbook for configuration of HP switches in campus networks	C	5	Draft	All	Czech
14	Finnish national end-to-end performance survey	F	5	Rep	All	Finnish
15	Report on network hardware used in Finnish campus networks	F	5	Rep	All	Finnish
16	Report on status of WLAN networks in Finnish campuses in 2010	F	6	Rep	All	English
17	Recommended security system for wireless networks	U	6	BPD	Tr	English
18	Best practice in WLAN security	F	6	Draft	All	English
19	Cookbook for configuration of HP wireless equipment	C	6	Draft	All	Czech
20	Recommended network management architecture	A	7	BPD	All	Serbian
21	UNINETT SIP infrastructure	U	8	Rep	All	English
22	Review of solutions of IPT in Czech universities	C	8	Draft	Part	English
23	Best practice for packet filtering	A	9	Draft	Part	Serbian
24	Security policy template best-practice document	U	9	Abst	All	English

Table 3.5: Reports and documents produced

NREN: A = AMRES, C = CESNET, F = Funet, U = UNINETT

Status: status of the document at the end of the first year

BPD = nationally approved best-practice document
Draft = national draft of a best-practice document
Rep = national report
Abst = only abstract completed so far

GN3: what is paid from the GN3 project budget

Tr	=	translation only
UpTr	=	update of national best-practice document and translation
All	=	all the work
Part	=	partly paid from GN3 budget, partly by the NREN

English abstracts are available for all 24 documents. They are reproduced in Appendix C.

As mentioned in the introduction of section 3.2, the documents do not yet have a common cover page, acknowledgements and copyright statement. This final editing will be completed by June 2010 and all mature documents (not the drafts) will then be published.

4 Conclusions

The Task work is in its early stages, but the results obtained during the first year are quite satisfactory. Organising working groups at the national level and getting real commitment from the community takes time. It requires active dissemination of information at the national level. The universities must clearly see the benefits of engaging in working groups: there has to be something in it for them. It is important to produce descriptions of best practices that are to the point and that address current unresolved challenges. It must be stated clearly that the recommendations are just recommendations, i.e., advisories that the universities may adopt as they see fit. It should also be clear that working group meetings are not just about producing documents. They are also an arena for exchanging ideas. Workshops should complement regular meetings on best-practice documents to stimulate discussions and spread knowledge. After all, different campuses are faced with more or less the same challenges. Solving a problem once in a real good way is far better than working separately, in solitude, on a potentially more suboptimal solution.

The Task team has emphasised the focus on *national* working groups. The reason for this is that community building is far easier to achieve within a country, where there is a joint culture and language. It is a fact that many IT staff will be shy to participate in a debate at the European scene, and therefore it is better to start close to home. This is why in the first two years of the GN3 project the Task team focuses on results within the countries of the four pilot NRENs.

When working groups within those countries are maturing and best-practice documents are evolving, it will naturally attract interaction and collaboration across borders. This has in fact already started in the field of network monitoring at the Belgrade workshop. It will continue in April 2010 with the IP Telephony workshop in Prague. That workshop will include presenters and participants from across Europe.

In the second year of the GN3 project the Task team will devote more effort to dissemination. Mature best-practice documents will be published in English. Workshops will complement the messages written in the best-practice documents. The Task team will make presentations at national and European conferences.

Of course one cannot expect the current small Task to have a direct real impact on all the hundreds of universities across Europe. That would require a lot more resources and much more time. Being realistic, the Task team sees itself as demonstrators of what can be done. The EARNEST report concludes that it is vital for the NRENs to reinforce their national efforts and get engaged in campus challenges. After all, services are end-to-end, and the ends are inevitably on campus. If and when more NRENs would like to strengthen their campus focus, the Task's pilot NRENs can contribute their experiences.

5 Appendices

5.1 Appendix A: First-year milestones

	2009			2010
	A M J	J A S	O N D	J F M
Subtask 0: Task management and support				
U0.1: Translate UFS101	U			
U0.2: Procure translator service			U	
A0.1: Promote BP & WG idea for IT staff in AMRES		A		
A0.2: Establish AMRES Wiki		A		
A0.3: Promote the first national BPDs for IT staff in AMRES			A	
A0.4: Disseminate @YUInfo (national IT conference)				A
C0.1: Promote BP & WG idea on meeting of CESNET RP		C		
C0.2: Establish WG for documents preparation			C	
C0.3: Promote the first two national BPDs and translate			C	
Subtask 1: Procurement				
U1.1: Abstract for the Procurement Process BPDs				U
Subtask 2: Basic infrastructure				
U2.1: Abstract available for the 5 BPDs			U	
U2.2: The 5 BPDs translated to English				U
A2.1: Working group in subtask #A2 established with leader			A	
Subtask 3: AV				
U3.1: Abstract available for the UFS116 and UFS119				U
U3.3: UFS116 translated to English				U
Subtask 4: Lightpath service				
F4.1: Report on current status of lightpaths in campuses				F
Subtask 5: LAN infrastructure and IPv6				
U5.1: Translated UFS105 and relevant cookbooks				U
C5.1: Working group for IPv6 established			C	
C5.3: Resilient network design (IPv6)			C	
F5.1: National report of hardware used in campuses				F
F5.2: National E2E performance survey				F
F5.5: GN3 report for E2E performance survey results				F

	2009			2010
	A M J	J A S	O N D	J F M
F5.9: National workshop on campus networks			F	
Subtask 6: Wireless				
U6.1: Translate UFS112 to English				U
C6.2: Cookbook for HP wireless - in Czech			C	
F6.1: WLAN information gathered from universities			F	
F6.2: Report on status of WLAN networks in Finland			F	
F6.3: First version of WLAN security BPD				F
F6.9-12: MobileFunet –meeting			F	F
F6.14: National course on server configuration for eduroam			F	
Subtask 7: Network monitoring				
T7.1: Network management workshop in Belgrade			T	
U7.1: Virtual image of NAV and tool box available		U		
U7.2: Doc on essential campus network monitoring features			U	
A7.1: Working group in subtask #A7 established with leader		A		
A7.2: Draft avail: 'Rec. network management architecture'			A	
A7.3: National BPD: 'Rec. network management architecture'				A
C7.1: Working group 'LAN monitoring' established			C	
Subtask 8: SIP and IP telephony				
U8.1: SIP requirement specification in English				U
C8.1: Working group for IPT established with leader			C	
C8.2: Draft: 'Review of solutions of IPT in Czech Universities'				C
C8.3: BPD: 'Review of solutions of IPT in Czech Universities'				C
Subtask 9: Security				
U10.1: Abstract of Security Policy template BPD				U
A10.1: Working group in subtask #A90 established with leader		A		
A10.2: Draft avail: 'Best practice for packet filtering'				A

Table 5.1: Internal milestones achieved

Legend: A = AMRES, C = CESNET, F = Funet, U = UNINETT, T = Task team

5.2 Appendix B: Network monitoring workshop for NA3/T4

The Task team organised a two-day workshop on 20-21 October 2009 in Belgrade. There were 31 participants from six countries (Serbia, Norway, Czech Republic, Finland, FYR Macedonia and Montenegro).
The slides of the presentations are available at https://ow.feide.no/geantcampus:netw_monitoring_oct_2009

The agenda of the workshop was as follows.

20 October 2009		
09:00	Welcome to Belgrade	Slavko Gajin, AMRES
09:20	About GN3/NA3/T4 and about GigaCampus	Vidar Faltinsen, UNINETT
09:30	Overview of network monitoring activity in Norway	Vidar Faltinsen, UNINETT
10:00	Overview of network monitoring development at AMRES	Slavko Gajin, AMRES
11:00	University Campus Network Monitoring in Everyday Life	Tomas Podermanski, Brno Univ
11:30	Network monitoring in Funet	Jani Myyry, Funet
12:00	Report from FYR Macedonia and Montenegro	Ljiljana Adzic/Goran Muratovski
14:00	ICMyNet.IS	Slavko Gajin, AMRES
14:45	The Campus NMS tool NAV	Morten Brekkevold, UNINETT
16:00	Draft on network management architecture	Ivan Ivanovic/Esad Saitovic, AMRES
16:30	Network management requirements / recommendations	Vidar Faltinsen, UNINETT
17:00	Round the table discussions: tools people use / would like	All
21 October 2009		
09:00	ICMyNet.Flow	Dusan Pajin, AMRES
10:00	Flows at Masaryk University Brno	Jan Vykopal, Masaryk University
11:00	Stager: Presenting and aggregating network statistics	Arne Øslebø, UNINETT
11:30	Passive monitoring service	Ales Friedl, CESNET
12:00	Deploying a large-scale monitoring infrastructure	Arne Øslebø, UNINETT
14:00	Advanced traceroute	Ales Friedl, CESNET
14:30	A perfSONAR implementation using NetConf	Arne Øslebø, UNINETT
14:50	Discussions on passive monitoring and E2E measurements	All
15:20	ICmyNet.MIB tool - SNMP/MIB browser	Ivan Ivanovic
16:00	Campus network situation in Belgrade	Mara Bukvic, AMRES
16:30	Visit AMRES/RCUB equipment room	All

Table 5.2: Programme of Belgrade workshop

5.3 Appendix C: Abstracts of documents produced/translated

In the first year of the GN3 project, the Task team produced 24 abstracts in English. Fifteen of the corresponding full-text documents have been written or translated in English.

Five of the documents are classified as reports. The rest (19) are classified as best-practice documents, and are either nationally approved (11), drafts (6) or not yet completed (2).

Some of these documents were written before the start of the GN3 project, but were updated and/or translated in the first year of GN3.

Below, the abstracts are sorted according to subtask (area of focus).

5.3.1 Subtask 0: Task management and support

5.3.1.1 *Definition of UNINETT engineering task force and the UFS documents (UFS101)*

Country	Norway
Original	Written in Norwegian
Status	National BPD. Current version approved December 2007
Translation	Document translated to English May 2009
Paid by GN3	Translation only
Main author	Vidar Faltinsen, UNINETT

This document defines what the UNINETT engineering task force is and how the working groups within should operate.

The document further defines the working group's main product: the UFS documents (UNINETT white papers). The process towards final approval of an UFS document is explained and requirements for content and style are given.

5.3.2 Subtask 1: Procurement

5.3.2.1 *Procurement process best practice document (UFS125)*

Country	Norway
Original	Written in Norwegian
Status	Abstract completed January 2010. National BPD scheduled for September 2010
Translation	Abstract translated to English January 2010
Paid by GN3	Partly, the rest by UNINETT
Main author	Lars Skogan, UNINETT

This best-practice document describes experiences and best practices in procurement from the Norwegian University College and University (UC) cooperation.

The document describes the background and reasoning behind the initiative for this cooperation. Combining purchasing power has many benefits and has produced huge savings for customers. An external report compiled by the consultancy firm CapGemini has documented this. The savings are related both to the procurement process itself and to better terms in the contracts.

There are many legal regulations relating to public tenders in Norway. Most, if not all, are adopted or influenced by EU law and precedents. The focus in this paper will mainly be on EU regulations, but it will relate this to local implications.

The procurement process will be explained, given the legal framework and the challenges of coordinating independent educational institutions. This process includes: collecting requirements/needs, an analysis of the requirements/needs, recruiting UC and organising a working group, contacts with the suppliers, writing tender documents, tendering, evaluation of offers, contracts and follow-up. The focus will be on management, achieving customer satisfaction and cooperation in these processes. Finally, other experiences and pitfalls will be described.

5.3.3 Subtask 2: Basic Infrastructure

5.3.3.1 *Requirements for generic cabling systems (UFS102)*

Country	Norway
Original	Written in Norwegian
Status	National BPD. Current version (v3) approved December 2009.
Translation	Full document translated to English February 2010
Paid by GN3	Update from v2 to v3, proof reading and translation
Main author	Stein Nygaard, UNINETT and COWI

This document provides specifications of the Norwegian higher-education sector's recommended standards for generic cabling systems.

When setting up a generic cabling system, it is recommended that the latest version of any currently applicable norms or standards be used at all times. If one wishes to install cable of higher quality than is called for by the applicable norms or standards, one must be aware of possible disadvantages.

Currently, the recommendation is to use:

- at least 1 Gb/s capacity in the horizontal cabling system, in other words, Class E / Category 6
- building backbone cabling and campus backbone cabling subsystems consisting of single-mode (SM) fibre-optic cables.

In connection with new buildings and renovation, it is important to ensure the allocation of necessary space and pathways to enable the establishment of a fully functional IT environment.

The standard of workmanship is considered extremely important, as regards both interior and exterior installation work. The characteristics of the selected products should be appropriate to the area of use, installation location and environment. Installation firms should have the necessary authorisations for the work to be carried out as well as certification for the products used.

Installation personnel should always be required to provide documentation for the installation, and Documents of Conformity as required by the authorities. In the case of complex installations or installations of a quality exceeding the applicable norms or standards, a system and application guarantee from the manufacturer should also be required.

5.3.3.2 *Requirements for the design of ICT rooms (UFS103)*

Country	Norway
Original	Written in Norwegian
Status	National BPD. Current version (v3) approved December 2009.
Translation	Full document translated to English February 2010
Paid by GN3	Update from v2 to v3, proof reading and translation
Main author	Stein Nygaard, UNINETT and COWI

This document provides specifications of the Norwegian higher-education sector's recommended requirements for the design of ICT rooms

An important condition for the efficient functioning of ICT systems is that ICT rooms are of satisfactory quality. Inadequate quality can lead to reduced productivity on the part of the institution's personnel.

The type and number of ICT rooms must be suited to the needs of the institution, whether they be large, advanced server rooms or storerooms for ICT equipment. In building projects, the allocation of space will often generate conflict between different interests. It is therefore important to analyse the institution's current and future space requirements so that these can be clarified and justified. Space that is allocated will often be fixed for the entire lifetime of the building and it may be difficult to get additional space allocated at a later date.

ICT rooms need to be optimally located in the building complex. In addition to the size of the rooms, one must consider factors related to security, fire resistance, noise, heating, electrical fields, conduit paths, equipment transport, floor loads and any extrinsic general building structures.

When fitting out ICT rooms it is important to be actively involved in the design of the rooms in terms of width/depth/height, raised floors, location of equipment racks and cooling units (including spare capacity), internal conduits (generic cabling systems and power), control of air currents, lighting, surface treatment of walls, ceilings and floors, access control and fire prevention.

5.3.3.3 *Power Supply Requirements for ICT Rooms (UFS 107)*

Country	Norway
Original	Written in Norwegian
Status	National BPD. Current version (v3) approved December 2009.
Translation	Full document translated to English February 2010
Paid by GN3	Update from v2 to v3, proof reading and translation
Main author	Stein Nygaard, UNINETT and COWI

A centralised on-line UPS should be installed to supply ICT rooms. The necessary UPS battery life should be assessed as part of a risk analysis if no standby power generator is to be installed. The UPS should be electrically isolated both during normal inverter operation and in static bypass operation mode.

The minimum requirement for main electrical panels for normal power supply, emergency supply and uninterruptible power supply is that they should be located in separate cabinets. Main electrical panels supplying essential ICT rooms should be constructed according to Form 4-b in the EU Low-voltage switchgear and control gear assemblies norm NEK EN 60439-1.

The need for overvoltage protection of the distribution grids must be assessed. If overvoltage protection is present in the main distribution grid, at least equivalent overvoltage protection should be installed in the secondary distribution system for ICT rooms.
The creation of a single earth potential in ICT rooms is considered to be very important for maintaining the necessary accessibility and uptime. All conductive structural elements and equipment surfaces should be at the same earth potential.

5.3.3.4 *Ventilation and Cooling Requirements for ICT Rooms (UFS108)*

Country	Norway
Original	Written in Norwegian
Status	National BPD. Current version (v3) approved December 2009.
Translation	Full document translated to English February 2010
Paid by GN3	Update from v2 to v3, proof reading and translation
Main author	Stein Nygaard, UNINETT and COWI

This document provides specifications of the Norwegian higher-education sector's recommended ventilation and cooling requirements for ICT rooms.

In general terms, the document recommends the installation of satisfactory ventilation and cooling systems. Inadequate cooling may have consequences for computer systems' uptime and accessibility, which in turn will affect an institution's productive capacity.

When installing a ventilation system, it is important to ensure that it is isolated as much as possible from other ventilation systems, and that in the event of fire it is able to prevent the spread of flue gases to ICT rooms. ICT rooms must be pressurised and incoming air must be filtered. Air humidity must be regulated in compliance with requirements pertaining to the equipment being used in the room. The ventilation of battery rooms must be carried out in compliance with prevailing standards.

The design and installation of cooling systems must focus on energy conservation, i.e., the application of systems that require little energy in order to produce cooling and, if possible, that recycle surplus heat. The most preferred systems are based on the 'free cooling' principle (involving either the intake of external air or the production of cooling water by means of outdoor heat exchangers), combined with supplementary compressor-based cooling systems which operate when the external air temperature does not permit adequate cooling. The construction of 'green' ICT rooms may entitle the institution to an investment subsidy from a public-sector body such as Enova.

The ideal room temperature is determined based on what is currently defined as 'best practice'. Work is currently being carried out in the international arena to reduce the energy consumption of ICT rooms. This may result in an increase in ideal room temperature threshold values. In essential ICT rooms, the emphasis should be on resilience to ensure that any faults that arise do not result in a shutdown of operations. For installations that have large per-rack cooling capacity requirements, water-cooled racks should be evaluated. The document illustrates various examples of air flow regulation. It recommends systems that maximise air flow regulation, thus providing optimal exploitation of the supplied cooling output.

A BMS (Building Management System) must be established to regulate operation of the ventilation and cooling systems, and to monitor room temperature and humidity. The BMS must have an interface to the ICT operations management system.

5.3.3.5 *Fire Protection Requirements for ICT Rooms (UFS104)*

Country	Norway
Original	Written in Norwegian
Status	National BPD. Current version (v3) approved December 2009.
Translation	Full document translated to English February 2010
Paid by GN3	Update from v2 to v3, proof reading and translation
Main author	Stein Nygaard, UNINETT and COWI

This document provides specifications of the Norwegian higher-education sector's recommended fire protection requirements for ICT rooms.

In general, all requirements stipulated by the authorities in relation to fire detection and extinguishing must be met.

Each institution must prepare written response procedures/instructions for its own ICT personnel in the event of fire. These will focus on loss reduction measures. Such procedures/instructions should also include fire hygiene requirements.

All ICT rooms must be equipped with smoke detectors. Essential ICT rooms (e.g., those used for data processing/storage, core switch/routers and resilience functions) must be equipped with an early-detection facility based on laser aspiration detectors. Less essential ICT rooms (e.g., telecommunications rooms) must be equipped with high-sensitivity point smoke detectors. Other ICT rooms must be equipped with point smoke detectors similar to those employed in the remainder of the building.

In general, a fire alarm system based on early detection, employed in combination with procedures/instructions, will greatly reduce the risk of fire. If an overall assessment of the importance of an ICT room, together with the procedures/instructions, indicates that a fire extinguishing system ought to be installed, this document recommends the use of hypoxic air venting.

5.3.4 Subtask 3: Audio Visuals

5.3.4.1 *Functional description of AV equipment in lecture halls and meeting rooms*

Country	Norway
Original	Written in Norwegian
Status	National BPD. Current version (v1) approved May 2009.
Translation	Abstract available March 2010, full document will be translated April 2010
Paid by GN3	Proof reading and translation
Main author	Bård Støfringsdal, UNINETT and COWI

This document is the first of three documents that gives recommendations for AV equipment in the Norwegian higher-education sector. UFS116 gives a functional description for recommended AV equipment solutions in lecture halls, seminar rooms, class rooms, meeting rooms and group rooms.

Areas that are covered are: requirements for building construction and technical installations, sound, picture, control system, requirements for remote lecturing, videoconferences, and burglar-proofing of the equipment. A system description is given for large lecture halls (over 80 seats), smaller lecture halls (less than 80 seats),

seminar/class rooms, meeting rooms and rooms for videoconferencing. Finally, relevant integration and interfacing towards other contractors is covered.

5.3.4.2 *Technical and Functional System Requirements for AV Equipment (UFS119)*

Country	Norway
Original	Written in Norwegian
Status	National BPD. Current version (v1) approved May 2009.
Translation	Full document translated to English March 2010
Paid by GN3	Proof reading and translation
Main author	Bård Støfringsdal, UNINETT and COWI

This document is a shared supporting document for UFS 116 and 120. These documents specify functional descriptions for recommended AV equipment solutions at universities and colleges in Norway. In UFS 119, there are technical and functional system requirements for the various components included in the functional descriptions.

5.3.5 Subtask 4: Lightpath service

5.3.5.1 *Report on current status of lightpaths in campuses*

Country	Finland
Original	Written in Finnish
Status	National report. Completed February 2010
Translation	Abstract translated March 2010
Paid by GN3	All the work
Main author	Janne Oksanen, Funet

A survey was carried out amongst Funet members about lightpath technology and its familiarity. The objective was to map how widely information about this technology is circulated within member organisations. This report outlines the survey results.

The survey asked if lightpath technology was familiar, whether the campus employs its own infrastructure, and how, for example, a research group would get a lightpath for use in their workstation, and what kind of support is needed for lightpath technology.

80.8% of all respondents said that they were familiar with lightpath technology at some level. Although most respondents had some knowledge of the technology, less than 10% of respondents had lightpath infrastructure of their own in use. In these organisations they had the ability to make use of this technology within their own network infrastructure in various applications, such as campus backbone connections, computer laboratory networks and in remote connections. Both DWDM and CWDM technologies had been used to create 1 Gb/s and 10 Gb/s connections.

The responses showed that the technology was not very well known and further information was desired in various formats. For example, some application examples were requested, together with training programmes and information about tried and tested equipment, and general information about how one can obtain and use a lightpath (in Funet and with own equipment).

Based on the survey, Funet can plan future operations in a way that allows it to provide the support that is wanted and needed for lightpath technology. Two practical test cases will be disseminated, of which one is already in use and the other will be available within a year.

5.3.6 Subtask 5: LAN infrastructure and IPv6

5.3.6.1 *Recommended configuration for switches in campus networks (UFS105)*

Country	Norway
Original	Written in Norwegian
Status	National BPD. Current version approved December 2007
Translation	Document translated to English in March 2010
Paid by GN3	Translation only
Main author	Vidar Faltinsen, UNINETT

This document presents a recommendation regarding the configuration of switches in campus networks. Layer 2 and Layer 2+ functions are covered, but not Layer 3 (routing). The recommendation is generic. A number of configurations intended for supplier-specific layouts will support the recommendation (currently only in Norwegian and for Cisco, HP and Alcatel).

The document does not deal with the design of campus networks, but focuses on the individual components and their configuration. Topics covered are: physical requirements, software, naming standards, configuration for management set-up, VLAN, spanning tree, multicast snooping and security functionality.

5.3.6.2 *Recommended resilient campus network design (CBPD 111)*

Country	Czech Republic
Original	Written in English
Status	Draft of national BPD. Current version completed December 2009.
Translation	English proof reading done January 2010
Paid by GN3	All the work
Main author	Tomas Podermanski, CESNET and Brno University of Technology

This document describes how to set up a fully resilient network design on a campus. The recommendations for standards and proper technologies are discussed. Descriptions of all the parts - core network, distribution switches and resilient server connections - are described.

The main idea of resilient topology is to eliminate downtime during crashes and device upgrades. This document describes how all critical devices are deployed in duplicate to avoid having a single point of failure. Therefore, any single device can be turned off without significant disruption for the connected applications and users.

The use of standardised protocols is encouraged throughout the document. This allows devices offered by different suppliers to interoperate. A further requirement was to keep the configuration as simple as possible.

5.3.6.3 *Cookbook for configuration of HP switches in campus networks*

Country	Czech Republic
Original	Written in Czech
Status	Draft of national BPD. Current version completed December 2009.
Translation	Abstract translated to English February 2010, the rest is scheduled for April 2010
Paid by GN3	All the work
Main author	Tomas Podermanski, CESNET and Brno University of Technology

The document describes how to configure HP devices in a campus environment. The document is divided into two main parts. The first describes the basic and common layer 2 configuration. All options necessary and useful for a local network environment like DHCP snooping, IGMP, GVRP and 802.1X port authentication are described. The second part is oriented towards layer 3 features such as OSPF routing, PIM SM/DM configuration, access lists etc.

All steps are shown in small configuration examples, which could be used by administrators in a cut-and-paste way. The basic switch configuration is also included, which describes how to configure SSH, RADIUS authentication and how to correctly protect the device.

5.3.6.4 *Finnish national E2E performance survey*

Country	Finland
Original	Written in Finnish
Status	Report. Completed January 2010
Translation	Abstract translated March 2010
Paid by GN3	All the work
Main author	Janne Oksanen, Funet

It has been said that the weakest link between the user and the service is often the campus network. The campus network is thus the bottleneck that hinders users from getting high-speed connections at their desktop and hinders their ability to effectively use the services available in the network.

Encouraged by the EARNEST Report on Campus Issues (January 2008), a Funet customer survey of campus networks was carried out. The report outlines the survey results.

The survey asked what size campus networks were at present, in terms of users and port numbers, among the Funet customer base. Furthermore, it was asked what data transfer speeds have been obtained on the campus networks' backbone connection and if there is any interest in a spare Funet connection. The survey also mapped which technologies were in use to connect to the campus networks' branch offices. The report also considered how the current changes to the Funet network would affect campus networks.

The survey results show that responses came from both large and small organisations. It appears that the current primary port speeds offered to end-users are either 100 Mb/s or 1 Gb/s. The backbone has been kept at a faster speed, i.e., either 1 Gb/s or 10 Gb/s. The number of 10 Gb/s ports was still low. There may be many reasons for this, such as real need or cost.

In due course, some of the changes in the Funet network will reflect on campus networks. When enough capacity to the Internet can be offered and the price of 10 Gb/s ports comes down, campus networks will be able to offer larger capacities to end users. DWDM technology

makes it possible to use lightpaths in campus networks if there is sufficient fibre network infrastructure available. It is therefore possible to get up to 10 Gb/s speed all the way to the workstations.

5.3.6.5 *Report of network hardware used on Finnish campus networks*

Country	Finland
Original	Written in Finnish
Status	Report. Completed January 2010.
Translation	Abstract translated March 2010
Paid by GN3	All the work
Main author	Janne Oksanen, Funet

A survey was carried out amongst Funet member organisations about edge devices that they have used to connect to the Funet network. The survey uncovered which types, brands and ages of devices were in use, and also if the device or its components had been doubled. The survey also asked about user experiences and what aspects had affected their decision to purchase that specific device.

The most popular brands amongst the respondents were Cisco, Juniper and HP. There were many different Cisco device models in use. The most popular device type was a firewall. The next most popular devices were routers and switches. The typical age of the devices was 0-4 years.

High availability was a consideration for most respondents. 19.2% had doubled the entire device or had a spare device as a backup that could be brought into use at short notice. Those who had not doubled the entire device had taken high availability into consideration by doubling components.

In addition to cost, the following considerations played a part when purchasing the current device:

- features: 46.2%
- performance: 15.4%
- compatibility with the rest of the environment: 26.9%
- support and maintenance: 15.4%
- familiar brand: 19.2%
- trusted and known brand: 11.5%
- number of connections and expandability: 19.2%
- reliability: 15.4%

Based on current purchasing decisions, the survey asked what additional or alternative considerations should be taken into account during future purchases. Answers revealed the same considerations as before, such as features, management, compatibility, performance, expandability and reliability. In addition to these, the respondents considered the following to be important:

- high availability: 20%
- IPv6 and multicast support: 6.67%
- maintenance costs: 6.67%
- quality: 6.67%
- 10 Gb/s connections: 6.67%

It was positive to note that high-availability aspects had been considered in relation to future purchases. We can conclude from this that an increasing number of Funet members will be running edge devices with doubling and high availability in the near future. Therefore there will be an increased demand for spare Funet connections. That 10 Gb/s connections are mentioned also indicates that data transfer speeds are on an upward trend.

The survey does not give sufficient indication of how IPv6 support has currently been taken into consideration with edge devices. Only a few respondents mentioned that this aspect should be taken into consideration in future purchases. However, it is sensible to prepare seriously for IPv6 support, if this has not been done already, because the IPv4 addresses will run out within a couple of years. Globally, only 10% of IPv4 addresses are still available. The challenge facing IPv6 support is that not all equipment manufacturers provide this feature or, if they do, they do so only in part. Particularly in terms of firewalls, IDS/IPS equipment and load balancers, one has to pay close attention to this matter.

The respondents were mostly happy with their edge devices and the biggest problem areas were related to the equipment software. When problems were encountered, most received support and help from the device manufacturer, although in some instances there was room for improvement.

5.3.7 Subtask 6: Wireless

5.3.7.1 *Report on current status of WLAN networks in Finnish campuses in 2010*

Country	Finland
Original	Written in English
Status	Report. Completed January 2010.
Translation	Not necessary
Paid by GN3	All the work
Main author	Wenche Backman, Funet

In order to achieve an up-to-date picture about the current status of WLAN networks at Finnish university and research institute campuses, a survey was carried out in the autumn of 2009. The survey consisted of 31 questions about WLAN equipment in use, authentication and security, maintenance, services as well as experiences and practices. A total of 36 answers were obtained from representatives of 34 different campuses. From the answers it can be seen that a key issue on campuses today is cost-effective WLAN network planning including AP site selection and signal-strength measurements. Synergy effects could also be achieved with centralised guidelines for WLAN-related equipment configuration, e.g., supplicants and RADIUS servers.

Furthermore, the paradigm shift from stand-alone access points to controller-based networks was clearly seen and has to be supported. As for services in wireless networks, roaming is the most used one while VoIP and positioning have not attracted large attention yet.

5.3.7.2 *Recommended security system for wireless networks (UFS112)*

Country	Norway
Original	Written in Norwegian
Status	National BPD. Current version approved December 2007
Translation	Document translated to English in March 2010

Paid by GN3	Translation only
Main author	Jardar Leira, UNINETT

This document gives an overview of the various security mechanisms available for wireless networks. Disadvantages of using MAC address based security filters, WEP or web portals are discussed. IEEE 802.1X with mutual authentication complemented by using EAP and either TLS, PEAP or TTLS for authentication is argued to be the best solution. The IEEE 802.11i standard, better known as WPA and WPA2 supporting TKIP and AES encryption respectively, is covered. AES is the best solution and is recommended, but not supported by all clients, thus TKIP should also be an option.

Certificate management is quite complex. The document goes into detail and contains scripts that can simplify this process. Finally, eduroam is recommended. eduroam is the international RADIUS hierarchy solution for academic institutions that gives users of one institution access to the wireless network of another institution and vice versa.

5.3.7.3 *Best practice on wireless security*

Country	Finland
Original	Written in Finnish
Status	Draft completed March 2010. National BPD scheduled for May 2010.
Translation	Scheduled for July 2010
Paid by GN3	Most of the work
Main author	Wenche Backman, Funet

WLAN security includes user authentication, encryption as well as rules for handling the user's traffic during the session. Detailed authentication server configuration, WLAN controller and supplicant configuration will be addressed in a later best-practice document, namely the best-practice document on WLAN-related equipment configuration. In this document 802.1X is recommended due to the high-quality security that it provides but web-based authentication is not recommended to be abolished, because of its simplicity. However, security issues related to web-based authentication, including fake login pages, are highlighted. As for encryption, WPA2-AES is recommended both for its security and for the fact that using the same encryption on several campuses eases supplicant configuration for roaming. Furthermore, it is recommended that SMTP connections from Internet to WLAN clients should be denied and SMTP connections from WLAN clients should be allowed only to a few specific SMTP servers. In addition, WLAN clients should not be allowed to communicate directly, without the traffic going through an access point. Unprotected protocols should, if possible, be prohibited if web-based authentication is used. Finally, it is recommended that a separate user password is used for authentication in WLAN.

5.3.7.4 *Cookbook for configuration of HP wireless equipment*

Country	Czech Republic
Original	Written in Czech
Status	Draft of national BPD. Current version completed December 2009.
Translation	Abstract translated to English February 2010, the rest is scheduled for April 2010
Paid by GN3	All the work
Main author	Tomas Podermanski, CESNET and Brno University of Technology

'Cookbook for configuration of HP wireless equipment' describes how to correctly configure HP wireless devices. Both single access points and central management solutions are described. An example configuration shows how to properly set up both single web authenticated and eduroam connections. The last section shows examples of the proper RADIUS configuration.

5.3.8 Subtask 7: Network monitoring

5.3.8.1 *Recommended network management architecture (AMRES BPD 101)*

Country	Serbia
Original	Written in Serbian
Status	Current version approved as national BPD February 2010.
Translation	Abstract translated February 2010
Paid by GN3	All the work
Main author	Esad Saitovic and Ivan Ivanovic, AMRES

The aim of this document is to be an introduction to NMS along with recommendations for IT staff (who are not familiar with NMS tasks but) who are planning to implement NMS tools inside their campuses.

The document begins with network topology considerations. Small changes in topology are proposed according to the notion that NMS activity should be mainly run through a management segment of the network. Two alternatives are discussed. A management network and a production network can be physically separated networks (out-of–band management segment), or they can share the same physical network (VLAN management segment).

The document identifies a minimum of three components that should be covered by the campus management system. Those are configuration management and log management in addition to a well recognised network monitoring component provided by various NMS Packages.

The document briefly describes most of the common management protocols and their use in different environments and different types of devices in networks (i.e., network devices, servers, UPSs, A/Cs) in order not to compromise network security.

5.3.9 Subtask 8: SIP and IP Telephony

5.3.9.1 *UNINETT SIP Infrastructure*

Country	Norway
Original	Written in Norwegian
Status	Report. Current version completed February 2010
Translation	Document translated to English in March 2010
Paid by GN3	All the work
Main author	Jardar Leira, UNINETT

This document describes UNINETT's proposed SIP infrastructure. It is the result of work carried out as part of the GigaCampus project (2006-2009) and forms the basis of UNINETT's continued work in this field. From 2010, the campus coordination activity will be a permanent area of emphasis for UNINETT, and SIP infrastructure is incorporated as a key focus area.

The document outlines the component issues and recommendations regarding the practical implementation of the establishment of, and transition to, SIP. Moreover, it describes a range of possible services that can be

introduced. The document is written for higher-education institutions that wish to find out more about the background concepts, technology and the procedure required to participate in the SIP infrastructure.

5.3.9.2 *Review of solutions of IPT in Czech Universities*

Country	Czech Republic
Original	Written in English
Status	Draft of national BPD. Current version completed March 2010.
Translation	Not necessary
Paid by GN3	Partly, the rest by CESNET
Main author	Miroslav Voznak, CESNET

The document will describe the most important VoIP implementations at Czech universities. IP telephony appears in the Czech education sector with following features:

- only in combination with legacy PBX – no pure IP telephony solution is in use
- Czech universities are involved in CESNET's IP telephony project and can call each other free-of-charge (more than 40 VoIP gateways are registered in the CESNET project which started in 1999)
- IP telephony can be easily implemented as an option of existing PBXs and with proprietary protocols (e.g. Siemens, Avaya, Alcatel, …)
- the legacy PBX without the possibility of IP telephony is mostly combined with Cisco Call Manager
- only four universities offer IP telephony based on open-source solutions (based on Asterisk and OpenSER).

The document first gives an overall overview of the scenarios used. The motivation for deploying each scenario comes from the user needs, but the document discusses the reasons behind VoIP implementation. There are two basic reasons: the first one is an economic effect and the later is easier integration of information resources into communications. Three operation modes can be found at Czech universities:

- IP trunking - in this mode the existing PBXs of an institution are interconnected through IP (simple replacement of transmission path with very high level of security)
- IP telephony extensions - the created accounts can be used in SW or HW IP phones (if an open-source solution is implemented then the IP telephony is strictly based on SIP)
- SIP trunking - many telecommunications companies are able to provide telephony through SIP (e.g., Telefónica O2, T-Mobile, Vodafone).

5.3.10 Subtask 9: Security

5.3.10.1 *Best practice for packet filtering (AMRES BPD 102)*

Country	Serbia
Original	Written in Serbian
Status	Current draft March 2010, scheduled as national BPD in May 2010.
Translation	Abstract translated March 2010
Paid by GN3	Partly, the rest by University of Kragujevac
Main authors	Zoran Mihajlovic, University of Kragujevac; Bojan Jakovljevic and Mara Bukvic, AMRES

For reducing the security threats to their network, institutions (AMRES members) use different devices and techniques for packet filtering. The aim of this document is to help certain institutions/organisations apply the three basic recommendations: to define and/or modify their packet filtering rules, to choose the most suitable technology for implementing those rules, to configure and maintain all of the solution's components.

In the first part of the document, the available packet filtering technologies are briefly described and recommendations are formulated for their use and application, within the hierarchical structure of the AMRES network.

Thereafter, the most commonly used local network services are analysed, as well as the recommendations for their filtering. This is followed by recommendations for different packet filtering strategies, along with the good and bad characteristics of certain strategies.

At the end of the document, examples are given to illustrate the recommended application and parts of configuration files with packet filtering commands.

5.3.10.2 *Security policy template BPD (UFS126)*

Country	Norway
Original	Written in English
Status	Abstract completed March 2010, complete national BPD scheduled for June 2010
Translation	Not necessary
Paid by GN3	All the work
Main author	Gunnar Bøe, UNINETT

Information management is an essential part of good IT governance. An integral part of this is information security, in particular pertaining to personal information. However, many organisations do not have a clear policy for information security management.

This document combines legal requirements and current best practice for an information security management policy for Norwegian universities and university colleges. It provides a policy with information security strategy and objectives, and defines roles and responsibilities.

Core principles for information security management, as defined in ISO/IEC 27002, are adapted to the local situation for the following areas:

- risk assessment
- organising information security
- asset management
- human resources security
- physical security
- communications and operations management
- access control
- system development and maintenance
- information security incident management
- business continuity management
- compliance.

Governing documents for Information Security Management are also defined.

The foundation for this best practice are ISO/IEC 27001 and ISO/IEC 27002, which have been condensed to a manageable and applicable level (25-30 pages as opposed to the 108 pages of ISO/IEC 27002). Norwegian legal requirements have also been fulfilled. The EU equivalents can be found in

- Directive 95/46/EC (the Data Protection Directive)
- Directive 2002/58/EC (the E-Privacy Directive)
- Directive 2006/24/EC Article 5 (the Data Retention Directive)

References

[1] EARNEST Report on Campus Issues
Jean-Paul Le Guigner, Martin Price, Rogelio Montañana and Michael Nowlan
http://www.terena.org/publications/files/EARNEST-Campus-Report.pdf

[2] UFS101: Definition of UNINETT engineering task force and the UFS documents
Vidar Faltinsen, UNINETT
https://ow.feide.no/geantcampus:ufs101

Glossary

AES	Advanced Encryption Standard
AV	Audio Visual
BMS	Building Management System
BP	Best Practice
BPD	Best Practice Document
CWDM	Coarse Wavelength Division Multiplexing
DHCP	Dynamic Host Configuration Protocol
DWDM	Dense Wavelength Division Multiplexing
E2E	End to End
EAP	Extensible Authentication Protocol
EARNEST	Education And Research Networking Evolution Study
EU	European Union
Gb/s	Gigabits per second
GN3	Multi-Gigabit European Research and Education Network and Associated Services
GVRP	GARP VLAN Registration Protocol
HP	Hewlett-Packard Company
ICT	Information and Communication Technologies
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPS	Intrusion Prevention System
IPT	IP Telephony
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IT	Information Technology
LAN	Local Area Network
Mb/s	Megabits per second
MIB	Management Information Base
NA	Networking Activity
NAV	Network Administration Visualised
NMS	Network Management Station
NREN	National Research and Education Networking organisation

OSPF	Open Shortest Path First
PEAP	Protected Extensible Authentication Protocol
PBX	Private Branch Exchange
PIM DM	Protocol-Independent Multicast Dense Mode
PIM SM	Protocol-Independent Multicast Sparse Mode
RADIUS	Remote Authentication Dial In User Service
SIP	Session Initiation Protocol
SM	Single Mode
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTLS	Tunneled Transport Layer Security
UC	University College and University
UPS	Uninterruptible Power Supply
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
WDM	Wavelength Division Multiplexing
WEP	Wired Equivalent Privacy
WG	Working Group
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access