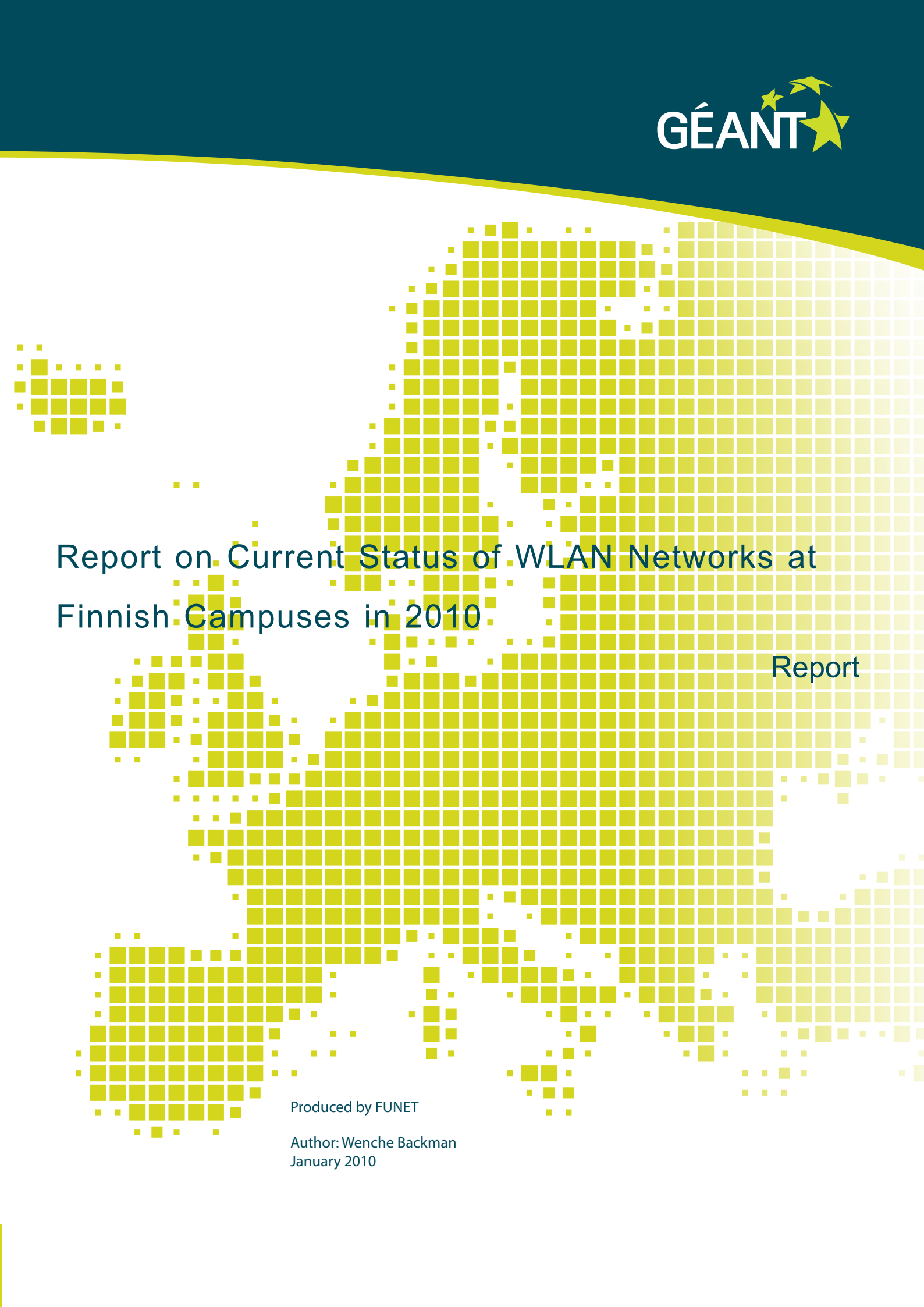

Report on Current Status of WLAN Networks at Finnish Campuses in 2010

Report

Produced by FUNET

Author: Wenche Backman
January 2010

Document No: GN3-NA3-T4-status-WLAN-networks
Version / date: 01.03.2010
Original language: English
Original version / date: 1.0 of 29.01.2010
Contact: wenche.backman (at) csc.fi

Funet bears responsibility for the content of this document. The work has been carried out by Funet as part of a joint-venture project within the HE sector in Finland.

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 238875, relating to the project 'Multi-Gigabit European Research and Education Network and Associated Services (GN3)'.

Table of Contents

Executive Summary

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 centralized 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.

1 Introduction

This work has been carried out as part of the third generation GÉANT project (GN3) [1], which is funded by the European Commission (EC) under the EU's 7th Framework Programme. The project includes 34 partners, of which 32 are European National Research and Education Network (NREN) operators responsible for the networks connecting national universities and research institutes to each other and to Internet. More precisely, this work is part of the task related to best practices on campuses, which objective is to address key challenges for the European campus networks and provide an evolving and to the point set of best practice documents (BPDs) for the community.

At Funet, the making of best practice documents has been started in two ways. In May 2009, a task force, MobileFunet, related to wireless systems and mobility, was established. The objectives of the MobileFunet task force is to bring together IT specialists from Funet organisations to share experience and identify best practices related to wireless systems and services. Secondly, in order to collect experience and practices from as many campuses as possible, a wireless LAN survey was carried out and answers were collected through a web site. The results of the survey are presented in this report. The questionnaire that was used for the survey focused both on technical aspects of the networks, such as equipment and security configurations as well as on services and practices. This way, a good picture of the current status of the WLAN networks is obtained and, furthermore, current good practices can be spread and areas, in which best practice documents are needed, can be identified.

2 Survey outline

The questionnaire was categorized as follows:

1. Access points and controllers (9 questions).
2. Authentication and security (5 questions)
3. Maintenance and control (5 questions)
4. Services in the wireless network (5 questions)
5. Experiences and practices (7 questions)

In addition, the name and details of the organizations were collected. The only mandatory question was the one in which the name of the answerer and the organization he/she represented was asked. The web questionnaire in Finnish can be obtained from the author.

The web questionnaire was first presented in Funet's monthly newsletter sent at the end of October 2009. A three-week answering period was given. The newsletter is sent to about 350 IT and security specialist and managers at the Funet customer organizations. A week later a personal reminder was sent to the members of MobileFunet and to IT specialists that had earlier showed interest in wireless network technology. When the three-week answering period had passed a reminder with a one-week answering period was sent to the IT specialists and IT managers that had earlier also received the newsletter. Lastly, the questionnaire was marketed at the national campus meeting on December 1st, 2009, during a workshop related to WLAN networks and roaming.

3 Survey results and analysis

3.1 WLAN equipment in use

The total number of access points (APs) for each of the 36 campuses can be seen in Figure 1. The campuses have been sorted according to the total number of access points present on campus. Three of the campuses do not have any WLAN access points while the largest campuses have several hundreds of APs. In the graph stand-alone access points and access points attached to a controller have been distinguished.

The ongoing paradigm shift from stand-alone access points to controller-based access points can clearly be seen from Figure 1. 17 campuses out of 36, i.e. 47 %, have reported that they possess access points attached to a controller. Still, as can be seen from the figure, there are large numbers of stand-alone access points left, foremost on large campuses.

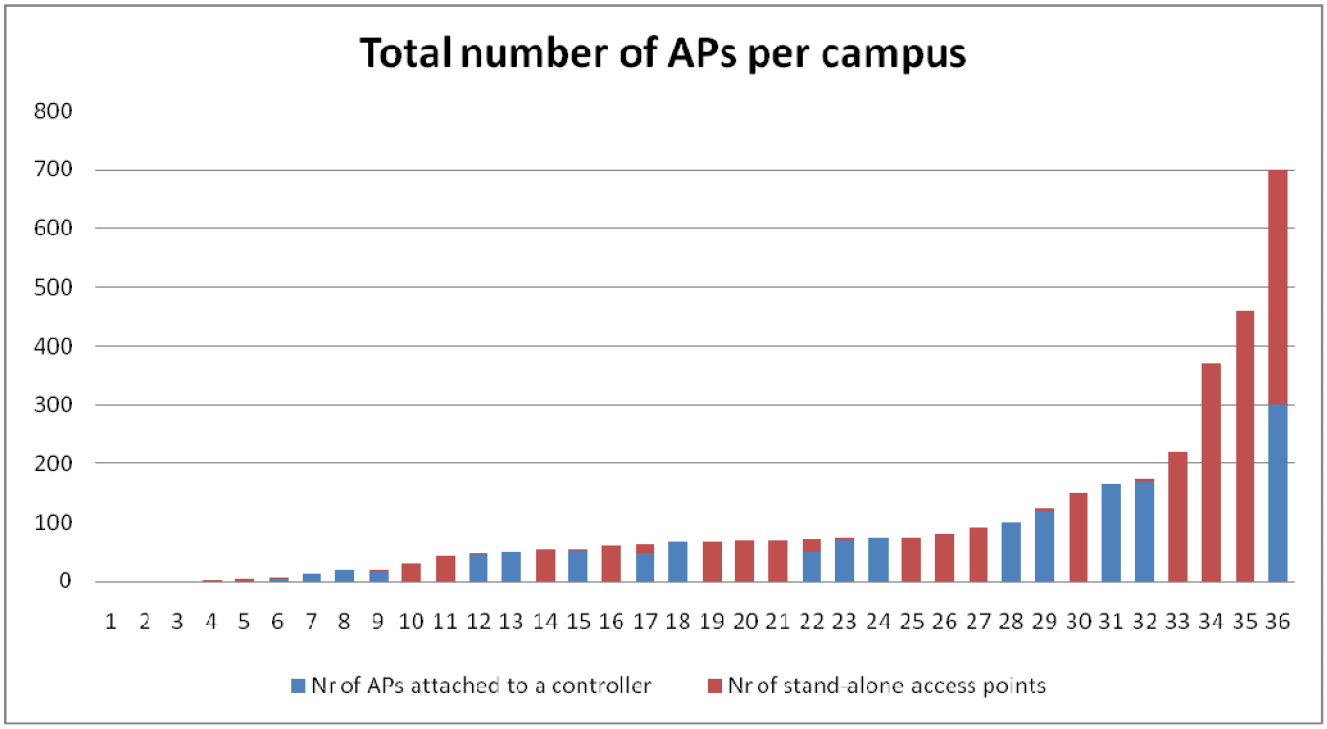

Figure 1. The total number of access points (APs) per campus.

The standards supported by the access points are presented in Figure 2. The campus number is equal to the campus number in Figure 1. The support for each standard is presented as the percentage of APs on each campus that supports the particular standard. From the figure it can be seen that the support for standard 802.11g is close to 100% on most campuses, regardless of whether the campuses are big or small. Please recall that the campuses were sorted according to size leaving the smaller campuses with a small number and the larger campuses with a high number. The support for 802.11b is still widespread but it can be seen that a few large campuses do not possess APs supporting 802.11b. The support for 802.11a is spread evenly between small and large campuses. As for 802.11n, it seems that it will be introduced on smaller campuses first.

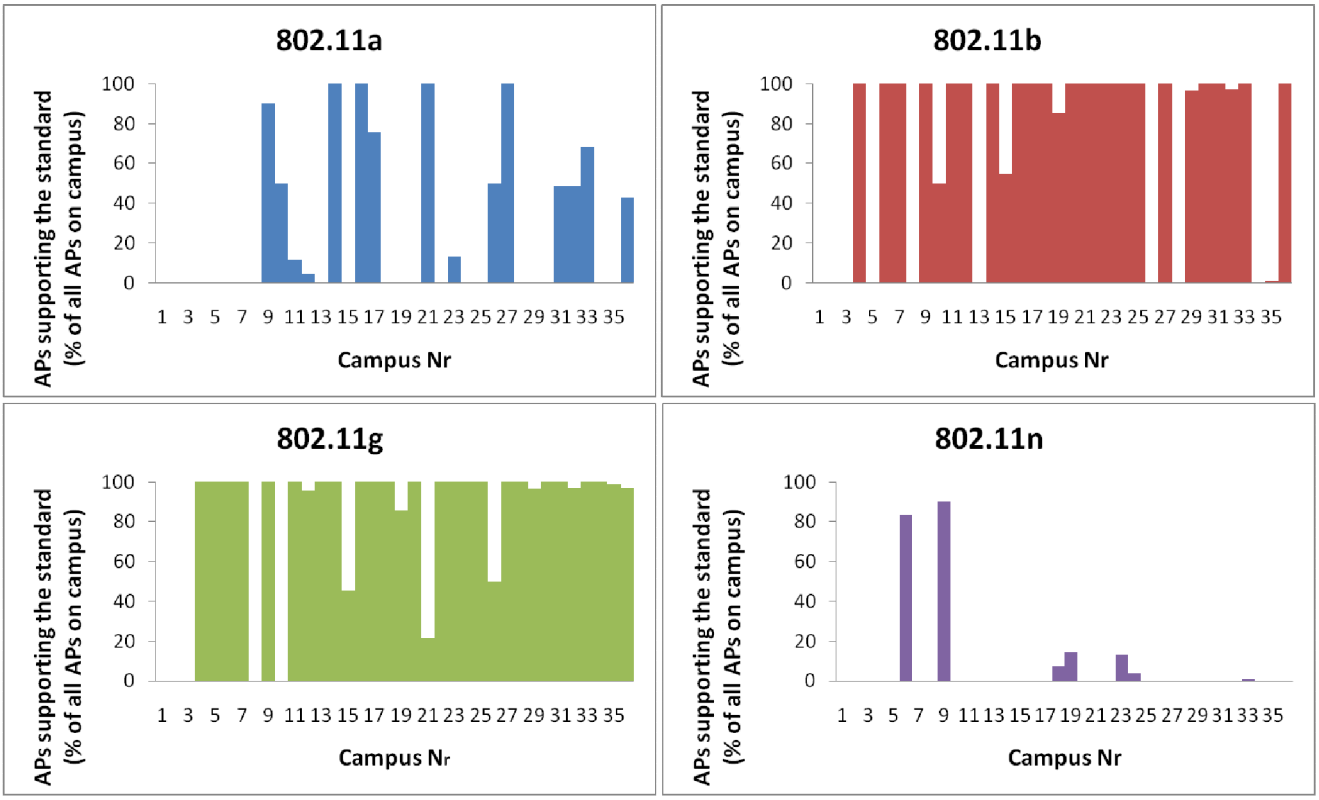

Figure 2. The percentage of APs that support a specific standard on each campus.

Among the campuses provided with WLAN controllers, Cisco and Hewlett-Packard (HP) are the most popular manufacturers. Eight of the campuses reported using Cisco while six uses HP. Other labels, used at one campus each, are Extreme and Sonicwall. Two of the campuses even use more or less self-developed software solutions for centralized AP management.

Also the most popular access point vendor is Cisco. 34 campuses reported the labels of their access points and 18 of them use Cisco. About one third of the campuses use access points from more than one vendor. All vendors are presented in Table 1. Although Cisco is by far the most popular access point label the wide range of labels used has to be taken into account when providing services for all university and research institute campuses in Finland.

Table 1. Access point vendors on Finnish campuses.

Vendor	Nr of campuses on which APs from the vendor is used
Cisco	18
HP	6
Buffalo	6
DLink	3
Proxim	3
Linksys	3
Extreme	2
Apple	2
ZyXEL	2
3com	1
Sonicwall	1

Cisco and HP also get good recommendations from several participants in the survey. However, some compatibility problems between HP and Intel wireless network cards as well as between Cisco and Macs have been observed. Moreover, frequent reboots have occurred for Proxim access points. Among the cheaper AP manufacturers ZyXEL gets recommended.

3.2 Authentication and Security

Eight of the 34 campuses have open wireless networks and seven use a pre shared key for authentication for at least part of their network. The rest have a user database with unique passwords for each user. More details about authentication handling are shown in Figure 3.

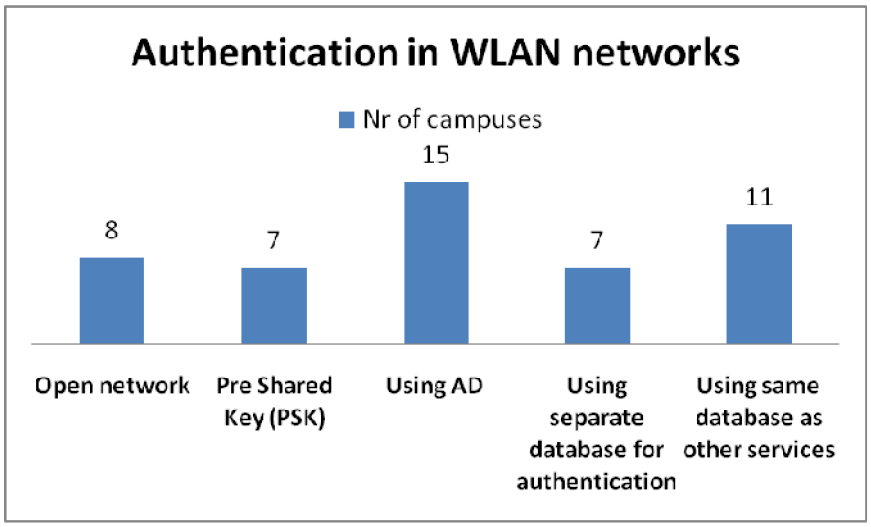

Figure 3. Authentication methods in campus WLAN networks.

16 campuses or 43% report that they use 802.1x authentication for at least part of their network. Of these almost everyone, 15, support PEAP-MsCHAPv2 as EAP method. This is probably because PEAP-MsCHAPv2 is the only EAP method provided natively with the Microsoft supplicant. The distribution of the other methods used is shown on the left side of Figure 4. On the right side of Figure 4 the supplicants with which users are advised to join the network are shown. It can be seen that the most popular way is for the IT support to urge the users to use the supplicant already provided with their operating system. This way, no installation is needed but the downside is the need for configuration instructions for a lot of different supplicants. However, at present there is no supplicant that would suite several operating systems and this way, lower the need for supporting various kinds of different supplicants. The number of supplicants can only be narrowed to one supplicant per operating system, e.g. use only SecureW2 for Windows.

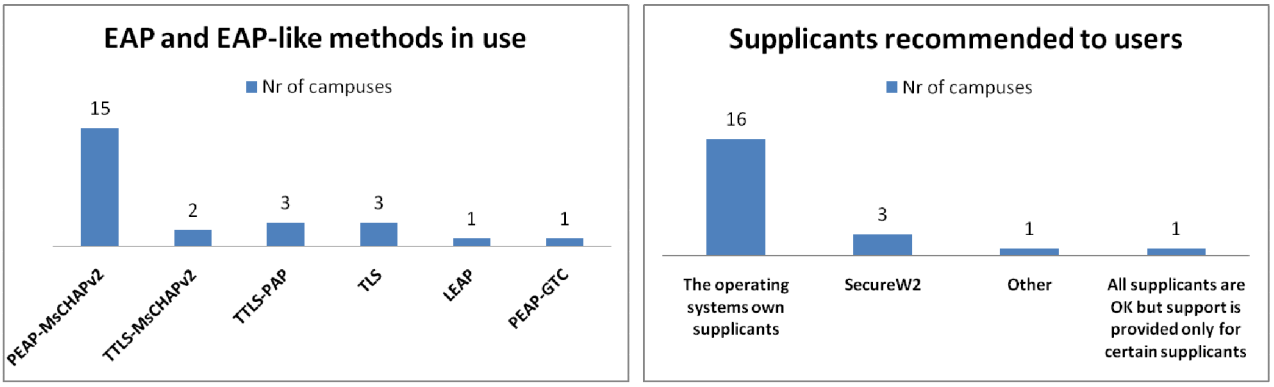

Figure 4. EAP methods in use on campuses (left) and supplicants recommended to users by the IT support (right).

The encryption used in the secured campus wireless networks for the SSID *eduroam* is shown in Figure 5. Apparently, the more exotic encryption methods WPA/AES and WPA2/TKIP are used to a significant extent. Still, the ordinary methods WPA2/AES and WPA/TKIP are the most popular ones. Although the securest method, the WPA2/AES method, is the most popular one, other methods are still largely used.

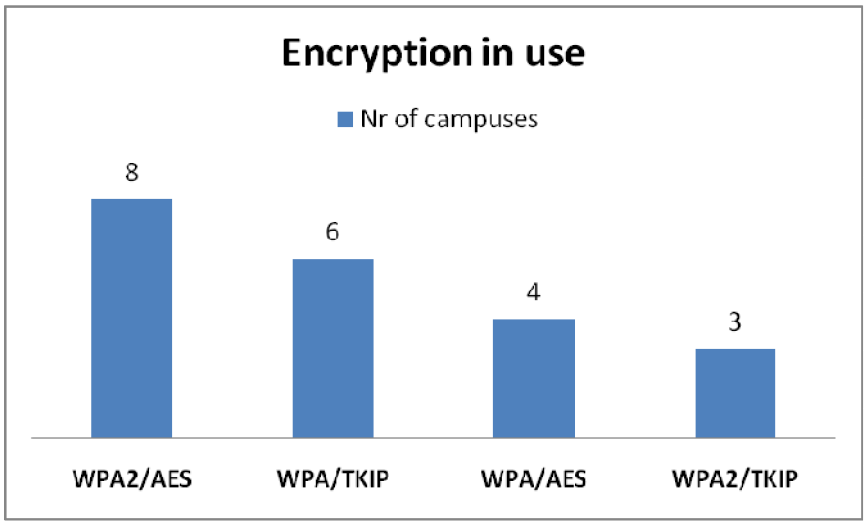

Figure 5. Encryption in WLAN campus networks.

The RADIUS server in use at campuses was also asked in the questionnaire. FreeRADIUS and Microsoft's RADIUS solutions (IAS/NPS) proved to be the most popular ones, used on 13 campuses each. However, from the answers it cannot be determined that these RADIUS servers are used for network authentication and encryption. Anyway, Radiator was used on seven campuses and Cisco's ACS on three.

3.3 Maintenance and control

Nine out of 33 campuses, or 27%, report that they do not monitor their whole WLAN network or a part of it regularly. Consequently, problems are noticed only through customer feedback. An equal amount, nine campuses, report that they check the controller's maintenance window or Cisco WCS regularly to observe problems before the users do. Cisco's monitoring solutions for autonomous access points, i.e. WLSE, is still used on three campuses. WLAN network monitoring using Nagios is used on five campuses. In short, many campuses monitor their WLAN network and several have more sophisticated monitoring methods than simply checking if the access points respond to ping commands. However, some problems, especially problems related to the air interface, may still go unnoticed. The most evolved method for WLAN network monitoring include surveillance eyes mounted among the APs in order to monitor the network seen from the user's point of view. More information about this and WLAN monitoring in general can be found from [2].

Among the problems observed in campus WLAN networks, coverage holes and AP capacity limit being reached are the only problems to occur daily, as can be seen from Figure 6. Both of these can be related to too few APs being present on campus and this, in turn, relate to the fact that the WLAN networks do not yet cover the whole campus satisfactory. Besides, it was also reported that flooding attacks by Windows Vista may have caused part of the network outages. Improvements in usability are needed, since many campuses report problems related to configuration every week or every month. Certainly many of these problems arise from supplicant misconfiguration in 802.1x networks.

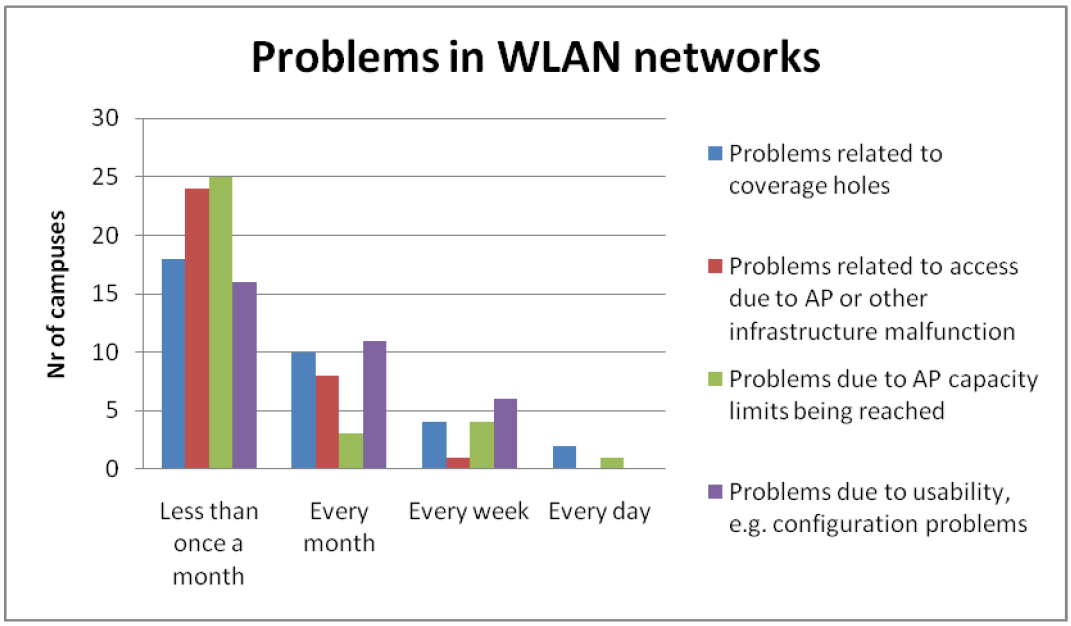

Figure 6. Problems observed in campus WLAN networks.

Other reported problems include WLAN driver malfunction in terminals and compatibility problems between APs and terminals. In addition, users accidentally or on purpose removing the power or network cable have also caused network outages.

Methods to solve problems include checking configurations, connections and logs. The controller's monitoring interface has also proven to be valuable for fault isolation. Also tcpdump checks are used in fault isolation. Evidently, booting the AP solves many problems. Naturally, the magnitude of the problem is checked in the first step. If it involves only one AP, that AP is checked thoroughly including checks over the air interface and/or the configuration of the user's terminal is checked. If the problem involves many APs the fault is usually sought at the controller. As for user's terminal, upgrading the WLAN driver or inserting a USB-WLAN adapter and show the network is working were suggested.

Next, the most time-consuming processes related to WLAN network maintenance and control was surveyed. The following processes were mentioned:

- WLAN network planning and expansion, including signal strength measurements, AP site selection and AP mounting (6 times)
- Supporting terminal configuration (4 times)
- Fault isolation (4 times)

Undoubtedly, focus needs to be put on providing consultation, courses and best practice documents related to WLAN network planning. Furthermore, large synergy effects can be achieved by preparing terminal configuration instructions in a centralized manner.

3.4 Services in the wireless network

The services included in the questionnaire were VoIP, positioning and roaming. Nine out of 35 campuses had at some point tried out VoIP in their WLAN networks. The experience was in general good although the need for extensive configuration was noted. Furthermore, handover caused problems; at least before controller-based networks were introduced. Many campuses reported that they could not see a need for VoIP in WLAN at present, especially since the introduction of fixed priced GSM subscriber connections.

Only three out of 35 campuses had experience of positioning services in their WLAN network, but seven campuses were interested in trying out such a service. The other campuses saw no need for positioning at this time. Anyway, many campuses could try using positioning since a position estimate can be obtained from WLAN controllers by checking to which AP the user's terminal is connected. The coordinates of the AP, provided that they are known, gives the position estimate. This may be sufficient for many needs but a more accurate position estimate can only be obtained using signal strength measurements or predictions from campus.

Ten out of 33 campuses were using eduroam at the time of the survey. Of these three reported supplicant configuration and lack of appropriate user database to have caused problems. Providing students access to their own resources also caused problems and this needs to be focused on in future plans of actions. A centralized solution to this problem could ease the work of the IT support and push the rollout of eduroam forward, provided that the solution is secure enough. Moreover, eight campuses reported intentions to introduce eduroam on their campus within a year and an additional two to introduce eduroam within two years. The main reason for having no current plans to introduce eduroam was no known need for the service.

The national roaming service called Funet-roaming (Funet-verkkovierailu in Finnish) is used on 13 of 32 campuses. Four campuses reported intentions to take the service into use within two years. Reasons for not introducing the service yet included shortage of resources and no known need for the service.

3.5 Experiences and practices

3.5.1 Problematic or time-consuming processes in WLAN network

The questionnaire included a question regarding which processes were the most problematic and/or time-consuming in the planning and installation phases. The result is shown in Table 2. It can be seen that advice regarding radius configuration as well as network planning could help organizations that are planning their first WLAN network or renewing their existing network. Of the other mentioned processes, equipment evaluation could be performed centrally to achieve synergy effects.

Table 2. Nr. of campuses that have experienced a specific process time-consuming or problematic.

	Nr. of campuses
Network planning (choosing AP sites)	5
Radius configuration and 802.1x	4
Controller configuration	3
Access point configuration (including remote monitoring)	3
Selection of equipment	3
The physical work included	2

3.5.2 Current best solutions

When asked what kind of solution that would be most favorable a majority suggested controller-based WLAN networks, which was expected. However, voices were also raised in favor of simpler solutions, stand-alone APs with centralized maintenance and monitoring using e.g. a web browser. Furthermore, the advantage of multiple SSIDs and eduroam for both own users and guest users were realized. Outsourcing the network roll-out as well as using Power over Ethernet –capable switches for AP power supply was also suggested.

3.5.3 Best practices

Among current best practices, smooth roaming was mentioned. The need for WLAN access within the whole city was also seen as important, not just roaming between campuses. Moreover, the importance of clear illustrated instructions for supplicant configuration was emphasized. Also here controller-based solutions and Power over Ethernet was mentioned.

Focusing on signal strength measurements for AP site selection in order to achieve maximum coverage areas and minimum interference was mentioned among the most usable practices. The Ekahau software was recommended for network planning. Also limiting the maximum number of clients that can be attached to a certain AP was mentioned. Having equipment from only one vendor in the WLAN network was advised.

3.5.4 Future projects and challenges

The campuses' future projects and challenges related to wireless networks are presented in **Error! Reference source not found.**. Among the challenges related to authentication, introducing eduroam was mentioned twice. Furthermore, 802.1x authentication was seen as laborious and instead of authentication, abuse monitoring was suggested. Expanding the network and dealing with an increasing number of users was mentioned by several participants. Also introducing controller-based WLAN networks as well as renewing the whole wireless network, which may include introducing controllers, was mentioned.

Table 3. Future projects and challenges on campuses.

	Nr. of campuses
Challenges related to authentication	6
Expanding network and dealing with increased nr of users	5
Renewal of the whole WLAN network	3
Introducing a controller-based network	2
Harmonize networks due to fusion of universities	2
Challenges related to firewalls	1

The last question in the questionnaire related to the draft versions of the BPDs available in the Best Current Practices (BCP) part of Funet-wiki [3]. It turned out that 46% was familiar with the content of the web pages. The comments showed that the users had drawn benefit from each other's experience and been able to obtain practical advice from the wiki.

4 Survey results and analysis

Currently, within the GN3 project, three BPDs are planned with the topics WLAN security, WLAN-related equipment configuration and WLAN network planning. Of these, there seems to be a great need for the WLAN network planning BPD. Also courses, consultation and examples on web pages related to network planning seems relevant.

Another area in which synergy effects could be obtained is by preparing centralized documentation for supplicant configuration. These could be included in the WLAN-related equipment configuration BPD.
Also help with introducing eduroam and enhancing the RADIUS configuration guidelines seem relevant. This work can also be included in the WLAN-related equipment BPDs. There is also a need to provide more than just network access with eduroam, access to the student's or staff member's own resources should be provided as well.

The paradigm shift from stand-alone access points to controller-based networks was clearly seen in the survey and a need for advice on controller configuration could be seen. At least Cisco and HP controller configurations could be included in the first step since these are the most popular vendors and they received good recommendations.

Other conclusions from the survey include a need for objective equipment evaluation. Furthermore, easily configurable and cost-efficient solutions for network monitoring and fault isolation must also be focused on.
As for services in wireless networks, VoIP and positioning have not yet gained a lot of attraction but in they should not be forgotten since services within networks are expected to grow, in WLAN networks as in other networks and other segments of IT.

Undoubtedly, a proactive approach is essential in BPD documentation and WLAN network support, since in the best case documentation should be available when the problems occur on campuses within Finland.

References

[1] http://www.geant.net

[2] W. Backman, MobileFunet, “Monitoring and ensuring WLAN performance” Report, CSC – IT Centre for Science, 2009, GN3-NA3-T4-WLAN-monitoring.

[3] BPDs on Funet-wiki: https://info.funet.fi/wiki/BCP (password-protected)

Glossary

AES	Advanced Encryption Standard
AP	Access Point
BCP	Best Current Practice
BPD	Best Practice Document
Funet	Finnish University and Research Network
GSM	Global System for Mobile Communications
LAN	Local Area Network
MobileFunet	a working group on wireless systems and mobility led by Funet
NREN	National Research and Education Network
RADIUS	Remote Authenticated Dail-In User Service
SSID	Service Set Identification
TKIP	Temporal Key Integrity Protocol
VoIP	Voice over IP
WCS	Wireless Control System
WLAN	Wireless Local Area Networks
WPA and WPA2	Wi-Fi Protected Access