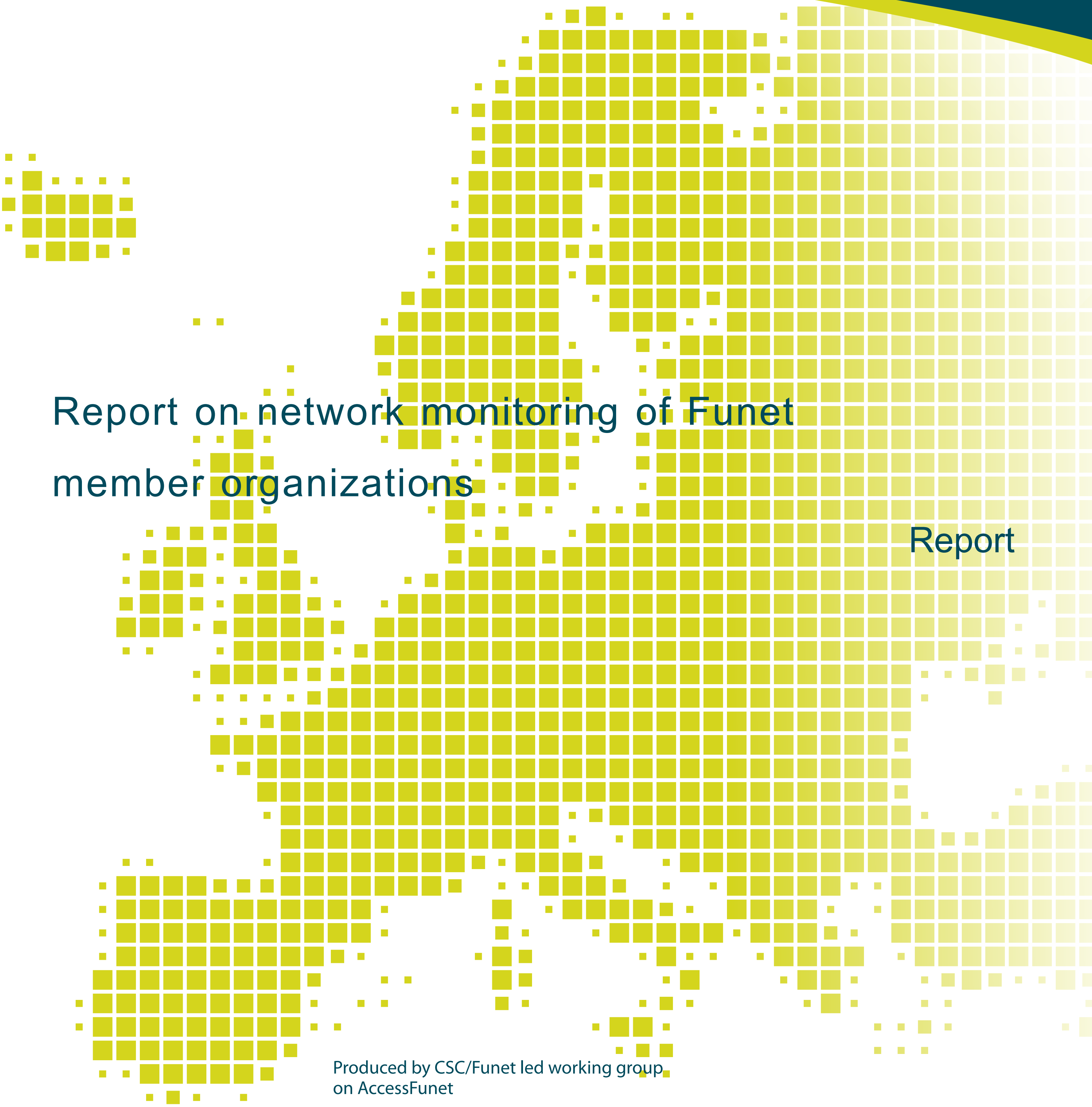

Report on network monitoring of Funet member organizations

Report

Produced by CSC/Funet led working group
on AccessFunet

Author: Janne Oksanen

January 2011

Document No:	GN3-NA3-T4-netmon-2010
Version / date:	12.01.2011
Original language :	English
Original version / date:	1.0 of 12.01.2011
Contact:	janne.oksanen (at) csc.fi

CSC/Funet bears responsibility for the content of this document. The work has been carried out by a CSC/Funet led working group on AccessFunet as part of a joint-venture project within the HE sector in <country>.

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)'.

Background

Towards the end of 2010 Funet carried out a survey charting the methods and tools used by Funet members for network monitoring. This report contains a summary of the survey results.

The survey and results

The survey was performed using the Webropol tool [1], which allowed respondents to reply using a web browser. This was done to make responding to the survey straightforward and attractive.

The survey was advertised in November and December 2010 in the monthly Funet newsletter, distributed to all Funet member organisations. The survey was also advertised at Funet conference in December 2010. The response rate was 16.8%. Of the respondents, 61.5% came from universities and 23.1% from universities of applied sciences.

The first questions charted the methods used in network monitoring. 84.6% of the respondents had a centralised help desk for data communications issues. A NOC address was used by 61.5% of respondents, with the most popular format being noc@organisation.fi. The service hours were the same as office hours for 76.9%, while the remaining respondents had longer service hours or did not have any regular service hours.

Various methods were employed in the detection of data communications problems. Figure 1 illustrates the distribution of the responses. None of the respondents had outsourced network monitoring. Other methods employed included tools provided by Funet, such as the internet monitoring service (IM) [2], or the detection of network service failure through use of the service.

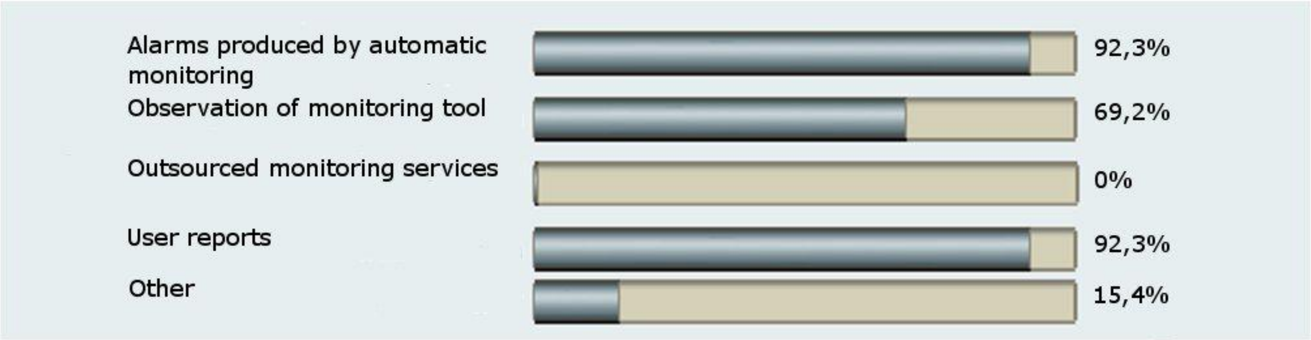

Figure 1. Methods for detection problems

The survey also contained questions on the network monitoring tools used by the respondents. Half the respondents reported that they use self-made tools and scripts; these could not be listed, however, because of the lack of more detailed information. The other tools mentioned by the respondents are listed below with a short description of the purpose of use and selected user experiences, if given. The tools are listed in order of popularity:

Nagios: Monitoring of devices, services and connections [3]. Easy implementation, but can be somewhat laborious. Nagios is versatile, with a wide range of plugins available. Scripts can be used to run automated functions.

Cacti: Graphs on devices and servers, recording of traffic volumes, and monitoring of UPS and machine room temperatures [4]. The tool produces beneficial graphs on traffic volumes, for example.

Smokeping: Measuring of service and device availability and response times [5]. A handy tool with efficient visualisation of network lag and the ability to send e-mail alarms.

Cricket: Collection of traffic data [6]. Easy to take into use, a number of improvements over MRTG. As a downside, Cricket has no alarm functions, only monitoring.

KiwiSyslog: Collection of log data [7]. An efficient tool for collecting log data that can be analysed from the UNIX command line, for example. The server version is commercial.

Splunk: Data collection from devices [8]. Commercial software. A good log server that you can modify according to your needs. The software is able to send alarms.

The following tools, listed below in alphabetical order, were also mentioned by individual respondents:

Airwave: Monitoring of wireless network access points and controllers, and user statistics [9]. Commercial software. Works better with standalone access points than with WLAN controllers. Occasionally displays erroneous data or no data at all when used with controllers.

Funet tools, including Funet scanner, IM and Zino:

- **Funet scanner**: A service for detecting information security gaps from outside campus systems and networks [10].
- **IM**, Internet Monitor: Tool for monitoring devices and connections [2].
- **Zino**: Tool for monitoring traffic volumes and connections [11].

ManageEngine OpManager: Monitoring of network, servers and services [12]. Commercial software.

ManageEngine DeviceExpert: Configuration management and monitoring of active devices [13]. Commercial software.

MetaNav: Monitoring of devices and connections [14]. Laborious to take into use.

MRTG: Graphs on traffic volumes [15].

Netdisco: Locating of devices on the network [16]. Able to create a map of the network topology, for example.

Nfsen/Nfdump: Netflow tools [17, 18].

RRDtool: Graphs on traffic volumes [19].

Snort: IDS/IPS tool [20]. Easy to introduce but troublesome to maintain.

What's UP: Monitoring of network connections [21]. Commercial software. Cost-efficient and easy-to-use. Able to create a map of the network topology and gather various types of log data. Plugins are available and can be created by the user.

Zappix: Monitoring of servers and software [22].

In addition to the above tools, several respondents exploited the built-in logs and software found on devices, including:

Extreme Epicenter: A handy tool for configuration and updates.

HP Procurve Manager: A handy tool for configuration and updates. Able to collect device and configuration data from HP devices and discover the network topology. The tool also allows the monitoring of traffic volumes and the timing of updates. The price of the software licence is determined on the basis of the number of devices.

HP Intelligent Management Center. More comprehensive and cost-efficient than its predecessor, Procurve Manager.

In addition to the tools employed, the questions also charted the respondents' opinions on the current status of network monitoring: 23.1% of the respondents said that the level of network monitoring was sufficient with regard to needs, but 53.8% felt that development would be required at some point. The remaining 23.1% said that network monitoring would need development in the immediate future.

Regarding development plans, the respondents commented that monitoring will expand automatically as the network expands. Some of the respondents called for more graphs that would allow improved observation and anticipation of potential problems. Ready-made tools were also in demand, but ones suitable for all needs of the network might not necessarily be available. The use of several network monitoring tools has led to a situation in which monitoring is dispersed and the tools laborious to maintain. In some cases this is the result of the organisation having been merged with another organisation that uses different tools.

Regarding the updating process, development plans include the introduction of a centralised ticket system that could receive automatic messages and alarms and user reports.

Some of the respondents feel that the current tools or existing devices are unable to produce the desired or required information. The tools produce differing information, which makes it difficult to maintain control over the general situation. For example, the detection of network loops may be time-consuming in the absence of suitable tools and methods for locating or preventing them.

Conclusions and remarks

Most respondents have arranged a centralised help desk for data communications issues. This is a recommendable approach, as it makes it easy to instruct users on whom to contact in case of any problems.

The use of a NOC address (e.g. noc@organisation.fi) is recommendable, as it allows several people to participate in the service instead of the service only being available through a limited number of individuals. This eliminates the need to inform the parties of new contact details resulting from personnel changes and during holidays.

Most respondents had office hours as their service hours, which is likely to be sufficient for most Funet members. Depending on the network environment and services, it might also be beneficial to publish information on whom to contact outside office hours. Funet monitors network operations 24/7; if the Funet subscription of a Funet member suffers a failure, the organisation in question is contacted and an attempt is made to reach the known contact persons.

Nearly all respondents were using tools that produce automatic alarms, but an equal number of respondents received information on network problems on the basis of user reports. This leads to the conclusion that the tools used for network monitoring fail to provide information on all service-related problems quickly enough or to allow the anticipation of potential problems. While the tools employed may be able to produce information on future problems, it is also possible that the information is not noticed in time to allow rapid response. There are also situations that cannot be anticipated with the use of monitoring tools. For example, disk space alarm limits can be set to allow actions to be taken before the server crashes, but monitoring tools are unable to foresee breakdowns in fibre optic cables. In preparation for such events, operators are requested to notify all fibre optic cable maintenance work in advance. This allows for some leeway if something goes wrong. Maintenance notifications for all Funet subscriptions are sent to Funet NOC, where duty officer then forwards the information and ensures that those affected by the maintenance operations are aware of the situation.

The respondents used a range of tools for various purposes. Since network environments are varied, there might not be a tool available on the market to suit all of these. As a result, several respondents had created monitoring tools themselves to produce the desired information. Problems frequently associated with self-made tools include the lack of resources for their development. The person who created the tools may also no longer be available and the tools may be difficult to use or suitable for one purpose only. If faulty, self-made scripts may also cause major problems.

The tools used by the respondents are listed here to allow the readers of this report to familiarise themselves with them and to determine their suitability for their own network environment; a more versatile and easy-to-use tool might be available for replacing another tool or reducing the number of tools employed.

Network monitoring is one of the topics of AccessFunet; meetings of the working group are a forum for meeting others interested in the subject, who may be able to provide help with using a certain tool.

Appendices

[1]: http://www.webrobol.com
[2]: http://im.funet.fi
[3]: http://www.nagios.org/
[4]: http://www.cacti.net/
[5]: http://oss.oetiker.ch/smokeping/
[6]: http://cricket.sourceforge.net/
[7]: http://www.kiwisyslog.com/
[8]: http://www.splunk.com/
[9]: http://www.arubanetworks.com/products/airwave_management.php
[10]: https://info.funet.fi/palvelut/cert/ (available to Funet members only)
[11]: http://www.csc.fi/funet/status/tools/wm
[12]: http://www.manageengine.com/network-monitoring/
[13]: http://www.manageengine.com/products/device-expert/index.html
[14]: http://metanav.uninett.no/
[15]: http://oss.oetiker.ch/mrtg/
[16]: http://www.netdisco.org/
[17]: http://sourceforge.net/projects/nfsen/
[18]: http://sourceforge.net/projects/nfdump/
[19]: http://oss.oetiker.ch/rrdtool/
[20]: http://www.snort.org/
[21]: http://www.whatsupgold.com/
[22]: http://www.zabbix.com/