Report of network hardware used on Finnish campus networks

Report

Produced by CSC/Funet

Author: Janne Oksanen
March 2010

Document No: GN3-NA3-T4-status-hardware
Version / date: 17.03.2010
Original language : English
Original version / date: 1.0 of 17.03.2010
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 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)'.

Background

Funet [1] is involved in TERENA's [2] "Campus Best Practices" project, which is part of GEANT3 (GN3)[3]. Funet has traditionally been a datacommunications operator for Funet member organisations, and the operations have mainly involved the backbone network sector. The GN3 project allows Funet to be more active in the campus network sector and thereby to offer more extensive support for its members.

The objective of the GN3 project is to cooperate with both Funet members and other European NREN organisations (NREN, National Research and Education Network) in finding and documenting best practices benefiting users. Possible forms of cooperation include various seminars, workshops, courses and meetings. The results of the cooperation could be published on the Funet Wiki [4], for example.

A survey on network hardware used to connect to the Funet network was carried out among Funet member organisations. The survey focused on establishing hardware types, brands, age and duplication of hardware or components. Questions were also asked on usage experiences and the factors affecting the purchase decisions for the hardware. This report provides a summary of the results of the survey.

The survey and results

The survey was performed using the Webropol tool [5], which allowed respondents to reply using a web browser. This was done to make responding to the survey straightforward and attractive compared to printed forms, for example. Having the replies in electronic format also sped up the processing of the results.

The survey was advertised in the monthly Funet newsletter, which is distributed to all Funet member organisations, in both November 2009 and January 2010. A link to the survey was also sent by e-mail to technical and administrative Funet contact persons in January 2010. The response rate was 34%. Half of the respondents came from universities and a third from universities of applied sciences.

The preferred brands among the respondents were Cisco, Juniper and HP (Figure 1). Of Cisco hardware, several models were in use. The most popular hardware types were firewalls, followed by routers and switches.

Brand	Model	Hardware type
Cisco	2960	Switch
Cisco	7204	Router
Cisco	7301	Router
Juniper	M7i	Router
Extreme	X450	Switch
Juniper	M120	Router
Sonicwall	NSA2400	Firewall
Cisco	7204	Router
Cisco	7304	Router
Cisco	ASA5520	Firewall
Dell	Dell 2950	Firewall
Nokia	IP 390	Firewall
HP	5412zl	Router
HP	ProCurve 2824	Switch
Checkpoint	Firewall	Firewall
Extreme	X450	Switch
Juniper	M10i	Router
Cisco	ASA5500	Firewall
Cisco	2960	Switch
Juniper	ISG 2000	Firewall

Cisco	2960	Switch
Cisco	Catalyst 3560	Switch
Cisco	Catalyst 3550	Switch
Cisco	WS-C3750G-12S	Router
CheckPoint	Nokia IP 290	Firewall
HP	DL380G5	Firewall

Figure 1. Responders' network hardware

The respondents' network hardware was mainly between 0 and 4 years old. The age distribution can be found in figure 2.

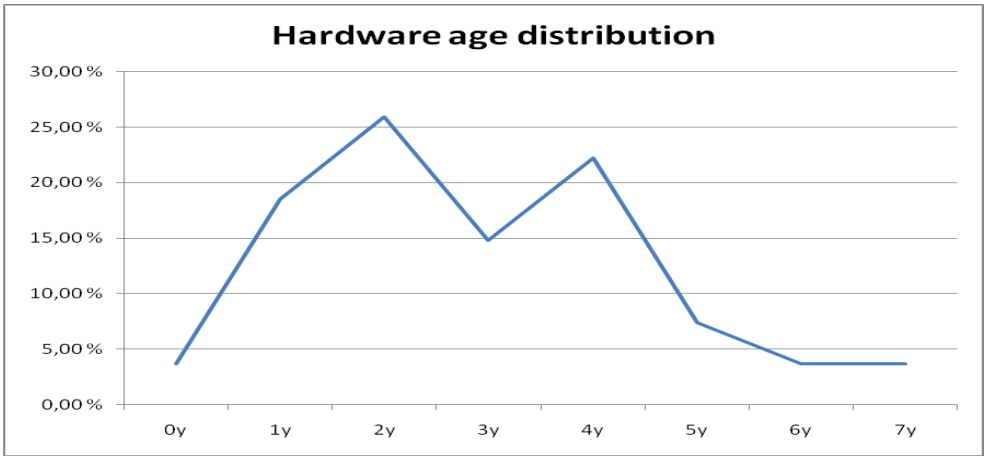

Figure 2. Hardware age distribution

The majority of respondents had taken fault tolerance into consideration. 19.2% had duplicated the entire hardware or had backup hardware that could be quickly taken into use. Those who had not duplicated the entire hardware, had taken fault tolerance into account by duplicating certain components; 41% of respondents had duplicated at least the power supply. Other duplicated components included RE (routing engine) and hard drives

In addition to cost, the following factors affected the decision to purchase the current hardware:

- properties, 46.2%
- compatibility with the rest of the environment, 26.9%
- familiar brand, 19.2%
- number of connections and expandability, 19.2%
- reliability of operation, 15.4%
- performance, 15.4%
- support and maintenance, 15.4%
- reliable and well-known brand,11.5%
- standardised hardware environment, 7.7%

Most respondents ranked properties, such as management and security, as the most important factor. Compatibility with the rest of the environment (proprietary or Funet) was also seen as important. Experiences of the brand also influenced purchase decisions.
Based on the purchase decision for current hardware, the respondents were asked to name factors that should be taken into consideration in future purchases in addition to/instead of the above factors. The responses included the same factors as above: properties, management, compatibility, performance, expandability and reliability. The respondents also found the following factors important:

- duplication/fault tolerance, 20%
- maintenance costs, 6.67%
- 10Gbit/s ports, 6.67%
- IPv6 and multicasting support, 6.67%
- quality, 6.67%

Respondents also commented that the properties of the hardware need to match those promised at the time of purchase. The reason behind this comment was the fact that updates had been necessary to deploy properties that would have been needed at the time of purchase.

As regards positive experiences, network hardware had been found to function faultlessly after initial configuration. Several responses even described the hardware as “working like clockwork”.

Negative experiences include software bugs in Cisco, Sonicwall and Dell hardware and SNMP problems with Juniper. Some respondents had major problems with software updates and performance. In one case the supplier was not performing information security updates despite a service agreement.

All respondents had received help with their problems from the supplier. Cooperation had mainly been smooth and expedient. 76.9% did not have any negative usage experiences.

Of the respondents, 82.6% planned to update network hardware within 2–3 years. The reasons for updating included the need for network hardware duplication and the introduction of 10Gbit/s connections. Moreover, some respondents had the need for updating because of the age of hardware.

Conclusions and remarks

Funet’s network hardware survey was carried out in order to obtain an overall idea of the hardware used by Funet members to connect to the Funet network and to establish any needs that would need to be taken into consideration on the Funet network. The results show that the most popular hardware brands are Cisco, Juniper and HP, while other brands are also in use.

Good care is generally taken of network hardware, and updates are relatively frequent: the majority of respondents update hardware every 4–5 years. This is a sensible approach, since the hardware concerned is among the most important hardware on the campus network. If the hardware is not functioning properly as concerns performance or properties, the entire campus network suffers. Moreover, manufacturers only support hardware for a limited period, after which information security updates and spare parts may not be available.

In addition to age, fault tolerance had also been given some level of attention: hardware components had been duplicated, and in some cases the entire device. If the hardware had not been duplicated, backup hardware with relatively rapid deployment may have been available. However, this requires manual work and may cause lengthy disruptions, even if the operations themselves may be minor. The required maintenance staff may not necessarily be available on site when needed.

Duplicated connections will be available to Funet members as a result of the update of the Funet backbone network. If the campus network has already been duplicated, it would also be sensible to duplicate network hardware. This would improve fault tolerance towards the Funet network. If the components of duplicated hardware have also been duplicated and the hardware is powered by two different UPSs or other secured power supplies, fault tolerance can be said to be at a satisfactory level.

When purchasing hardware, the majority of respondents saw hardware properties, management and information security as the most important factors. Consideration had also been given to the hardware environment by purchasing a compatible device. For some of the respondents the factors affecting the purchase decision included brand recognition, number of connections and expandability. Standardised hardware environment affected the purchase decision of only a small share of respondents. The underlying reasons are likely to include the challenges of tendering and the act on public procurement.

It is positive to note that duplication and fault tolerance were marked as factors to be taken into consideration in future purchases. This leads to the conclusion that in the near future more and more Funet members will have duplicated network hardware with high fault tolerance. This being the case, duplicated Funet connections will be in demand. The mention of 10Gbit/s connections suggests an increase in data transfer speeds.

In addition to duplication, 10Gbit/s was noted as a reason to update current network hardware within a couple of years. Mergers of Funet members have also led to updating needs.

The results do not indicate how IPv6 support has currently been taken into consideration in network hardware. Only a small share of the respondents said that this would need to be taken into account in future purchases. Those lacking IPv6 should seriously consider taking measures towards that end quite soon, since IPv4 addresses will run out within a couple of years. Only 10% of IPv4 addresses are available worldwide. One of the challenges for IPv6 support is that not all hardware manufacturers provide support for it or provide only partial support. This is something that needs to be taken into consideration for firewalls, IDS/IPS hardware and load balancers in particular.

The majority of respondents were satisfied with their network hardware, with most of the problems relating to software. Where problems had occurred, the majority had received support from the supplier, with individual cases leaving room for improvement. Funet members have selected their network hardware and partners well.

Appendices

[1]: Funet: http://www.funet.fi

[2]: TERENA: http://www.terena.org/

[3]: Geant: http://www.geant.net/

[4]: Funet Wiki: https://info.funet.fi/wiki

[5]:Webropol: http://www.webprobol.com