Detecting Active Devices in Intranets Using Existing Network Management Information *

Hiroshi TSUNODA†, Masahiro MATSUDA†, Yuusuke SYOUJI†,
Kohei OHTA‡, and Glenn Mansfield KEENI‡
† *Tohoku Institute of Technology, Japan* ‡*Cyber Solutions Inc., Japan*
E-mail: tsuno@m.ieice.org

Abstract

Global warming is now a major social concern. Stemming the growth of CO2 in the atmosphere is imperative. Fossil fuel is a major source of CO2. The Great East Japan Earthquake has shown that over-dependence on nuclear energy carries a heavy risk. Thus, power consumption must be reduced. Considering the fact that the ICT industry is a major power consumer, the wasteful activities of ICT devices must be detected and eliminated. In this paper we examine the use of existing network management information to make transparent the power-on/off state of ICT devices in intranets. This will expose the waste, if any, due to ICT devices that are not in use but powered on and will bolster social awareness of power wastage. Subsequently we look at the relationship between individual ICT devices and network topology and discuss how a Greener Network Architecture can be achieved.

Keywords: *Green IT, network management, connection management*

1: Introduction

Global warming is now a major social concern. Stemming the growth of CO2 in the atmosphere is imperative. A major source of CO2 in the atmosphere is the fossil fuel which must be burnt to generate power. The Great East Japan Earthquake has driven home the point that electrical power is not unlimited and is certainly not cheap when the true risks and costs are taken into consideration. Thus, power consumption must be reduced.

ICT industry is a major power consumer. It has already overtaken the automobile industry [1] and is slated to overtake the aerospace industry in the year 2020 [2]. In 2007, the total carbon footprint of ICT devices including personal computers (PCs) and peripherals, tele-communication devices and data centers was about 2% of the estimated total emissions from human activity [3]. This figure is expected to grow at the rate of 6% annually until 2020. It should be noted that the carbon generated from materials and the manufacturing of ICT related objects is about one-fourth of the total footprint and the remainder of the carbon is generated from the use of ICT technology [3].

A *green* network system is one that does not use more energy than is absolutely necessary. The purpose of this research is greening network systems by fully utilizing existing network

* This paper is a revised and expanded version of a paper entitled "Estimating Device Activities Using Network-based Information in the Intranet" presented at the 1st International Workshop on Smart Technologies for Energy, Information and Communication (IW-STEIC2012) on October 18-19, 2012 held at Tohoku University Sendai, Japan.

management systems, technologies, and knowledge. For saving power consumption in ICT area, various ICT devices, such as PCs, network interfaces, routers, and switches, should be put in sleep mode or, even better, powered off when not in use [4]. To enforce savings and eliminate waste, the power-on/off state of ICT devices should be monitored and managed. The networking of ICT devices and availability of standard technologies for monitoring and management of these devices, provides some means of detecting and monitoring the powered-on/off state of ICT devices.

In this paper, we discuss the utilization of existing information for detecting and monitoring the active ICT devices. Since a variety of information is available in current intranets, we categorize this information based on the information source and show that it can be fruitfully used to detect and monitor active devices in an organization.

The remainder of the paper is organized as follows. We describe related works in Sec. 2. In Sec. 3, we discuss the types of information that can be used for detecting and monitoring active devices. In Sec. 4, we present experimental results and analyze the detected wasteful activities of devices in an intranet. In Sec. 5, we discuss a Green Network Architecture and related problems, followed by conclusions in Sec. 6.

2: Related works

Various power saving mechanisms have been considered and implemented in ICT devices themselves. For example, operating systems dim the display after a time-out period of user inactivity. In the Microsoft Windows 8 operating system, a new power-friendly application model is developed and improvements to lengthen the duration of the idle state are introduced [5].

Basic strategies for improving energy efficiency are sleeping and rate-adaptation [6]. These approaches are used in Ethernet technology and standardized as Energy Efficient Ethernet (EEE) in IEEE P802.3az task force [7]. Sleeping and rate-adaptation are known as low-power-idle (LPI) and rapid PHY selection (RPS) in EEE, respectively.

It must be noted that even in the idle/sleep mode, there is a non-zero power consumption [8]. Considering the large number of sleeping devices, and the corresponding large sleeping times, the resultant power consumption still emerges as a significant figure and cannot be ignored. So we have to focus on detecting unused devices which are not powered off.

For greening the Internet, the methods for measuring and estimating the consumed power in the Internet are studied. Adelin et al. [9] measure the power consumed by routers and show that it depends on the volume of computed traffic and does not depend on the queue management policies. In [10], the authors present an estimation of the power consumption based on the network-based model covering the core, metro/edge, and access networks. They show that access equipment dominates the power consumption in the current Internet. They also indicate that as access rates increase, the power consumption of core networks increases and eventually overtakes that of access networks. On the other hand, the power consumption of user networks (i.e., intranets) has not been well-examined due to the wide variety of network environment, equipment and usage patterns.

A direct approach for measuring the power consumption of intranets is to use intelligent power outlets. In [11], the author develops an electric power usage monitoring system in a university campus network by deploying intelligent power outlet boxes. The system

visualizes the measurement result and thereby raises the awareness of students in power consumption. However, intelligent power outlets are a prerequisite for such approaches. Recently, network equipment has been developed with embedded power meters and proprietary implementation of power saving schemes and techniques. Cisco EnergyWise [12] monitors the power consumption of network equipment and controls the supply of power to equipment based on an organization policy. However, due to the heterogeneous nature of intranets and presence of legacy systems, open standard-based systems are desirable.

In this paper, we discuss how we can utilize the existing information in intranets, such as logs, network management information, traffic data, etc. for greening networks. In recent studies, this information was used for implicit sensing of building occupancy [13, 14], but our approach is to use this information in order to make transparent the power-on/off state of ICT devices in intranets, covering the leaf nodes.

3: Available Information for Detecting Active Devices

ICT devices are literally omnipresent. The examples are servers, PCs, LCD displays, TVs, network equipment (switches, routers, etc.), and peripherals. These days, not only PCs and servers, but also various other devices have been connected to an intranet and are able to communicate with each other. This trend enables sharing of functions of networked devices among multiple users through the intranet. Moreover, considering the rapid developments in IoT (Internet of Things) and M2M (Machine-to-Machine) communication, networked devices will continue to proliferate and dominate the future intranet. Thus, in this research, we focus on networked devices among ICT devices.

In the usual case, an intranet has a management system which collects data on the networked devices. The data source spans device logs, agents on devices, packets exchanged among devices etc. Analysis of the collected data enables us to discover useful information about the operations of the network and connected devices. We would like to argue that this collected information is also useful for detecting networked devices in the intranet and for monitoring their power-on/off state. A device is *active* when it is powered-on. Although the information on active devices does not give the power consumption directly, one can estimate the number of *device-hours* in an intranet which serves as an indirect measure of the power consumption of the intranet.

The available information can be categorized as device-based, infrastructure-based, or packet-based depending on the source of information. Device-based information is the information generated by the device itself. Typical examples are the various logs generated by applications and operating systems running on a device. It provides detailed information about events happening on the device. Activities on the device are directly reflected in this information. The infrastructure-based information is the information managed on infrastructure equipment, such as intelligent switches, DHCP servers etc. Packet-based information is obtained from packets exchanged in intranets. Infrastructure-based and packet-based information provide indirect indication of active devices. The basic premise of these is that an active device is connected to an intranet and communicates with other devices in or beyond the intranet. Table 1 summarize the pros and cons of each category of information.

Also, detailed information in each category is enumerated in Table 2. This information can be used stand alone or in conjunction with information from other sources.

Table 1. Categories of Available Information

Source	Pros	Cons
Device	Detailed information on device behavior can be obtained	Overhead for information collection is high
Infrastructure equipment	Overhead for information collection is low	Scope and availability of the information depends on the equipment
Packet	Relatively easy to deploy	Scope of information is limited. Unavailable if there is no network activity

Table 2. Detailed Information Components Available for Detecting and Monitoring Active Devices

Source	Information	Information Content
Device	Microsoft Windows Event log	Times of Logon/Logoff, Username, Device name, Service name, Application usage
Device	UNIX Syslog	Times of Login/Logout, Username, Application usage, Device name or IP address
Device	Existing SNMP MIBs	Process name, Resource usage, sysUpTime
Infra.	DHCP lease log	Lessee device's IP address, MAC address, Lease time
Infra.	Logs of authentication servers	Logged-on device's IP address, MAC address, Username, Authentication time
Infra.	Logs of authentication switches	Logged-on device's IP address, MAC address, Username, Authentication time
Infra.	Existing SNMP MIBs on managed switches	Connected device's IP address, MAC address, Connection time
Packet	All packets	Source device's IP address, MAC address, Payload information
Packet	Unicast response packets of active probing	Source device's IP address, MAC address
Packet	Multicast IGMP packets	Source device's IP address, MAC address, Connection time
Packet	Broadcast ARP/NDP packets	Source device's IP address, MAC address, Connection Time
Packet	Broadcast DHCP packets	Source device's IP address, MAC address, Lease time
Packet	Broadcast NetBIOS packets	Source device's IP address, MAC address, NetBIOS name

In the remainder of this section, we discuss the characteristics of each information category in detail.

3.1: Information Obtained from Devices

The advantage of using this type information is that detailed information of device behavior can be obtained. For example, event logs on Microsoft Windows systems and syslog information on UNIX systems are likely to contain information on when the device was booted up and when it was shutdown. We can also find details of application usage and authentication events from some types of logs. Such logs as these give an indication of whether the device is actually utilized by users or not. In addition, network management data available from the device provides valuable information pertaining to the activity of the device. For example, Host Resources MIB [15] provides information about processing load, names of running processes, and so on.

The disadvantage of using this information is the cost of information collection. For consolidated management, some sort of a process or agent must be present on each device to collect and transmit the logs to a manager. Deployment of agents and transmission of the logs incurs management overhead. If a device does not generate a log, or if the log is not accessible to the manager, the activity of the device cannot be monitored. This means that the availability of this type of information entirely depends on the environment of the target network. Moreover log information often includes privacy information like user name. Therefore, careful handling of information is required.

3.2: Information Obtained from Infrastructure Equipment

Infrastructure-based information comprising of log and/or management information infrastructure equipment such as servers, routers, and intelligent switches provide indications of device activities.

For example, from the address lease log of a DHCP server, we can discover which device got connected, what IP address was allocated and when. Intelligent switches with authentication functions (e.g., IEEE802.1X, Mac address, or Web) know which devices tried to authenticate for connecting to an intranet. Moreover, management information defined in some MIB modules such as RFC1213-MIB, BRIDGE-MIB and IF-MIB can be used to detect connected devices and compute the port at which the device is connected.

The advantage of using this information is the relatively low cost of information collection. The number of collection targets is smaller than that in the case of device-based information and information of multiple devices can be obtained from one equipment. Therefore, the collection cost is relatively low.

The disadvantage is that it depends on the availability of intelligent devices in the intranet infrastructure.

3.3: Information Obtained from Packets

Packets exchanged among networked devices provide important clues regarding the device activity. If a packet is seen, one infers that the sender of the packet is active. It is necessary to deploy a probe or packet sensor in the intranet, in order to use packet-based information. Since the replacement of existing elements is not required, ease of deployment

is a significant advantage in using this information. A drawback in using this information is that it does not work if there is no network activity.

Packet-based information collection uses connection management techniques which are often used in intranet security management. As shown in Table 3, the packet-based information can be obtained with passive monitoring, active probing, and the hybrid method of passive monitoring and active probing.

Table 3. Methods to Obtain Packet-based Information

Method	Accuracy	Traffic overhead
Passive monitoring	Moderate	Low
Active probing	High	High
Hybrid (Active & Passive)	High	Moderate

In the passive method, a probe passively monitors packets and generally looks for IPv4 address resolution protocol (ARP) request packets and IPv6 neighbor discovery protocol (NDP) packets. These packets are broadcast by a device when the device tries to ascertain the MAC address of another device in the intranet. As shown in Table 4, they are also broadcast for the purposes of IPv4 address conflict detection [16] and IPv6 duplicate address detection [17] at the startup phase of server and client devices. Thus, ARP and NDP packets which indicate that a device is active are useful for detecting newly booted devices. Moreover, other broadcast or multicast protocol packets, such as DHCP discover/request packets and IGMP membership query, will be monitored in this method. Also, if switches in the target intranet support port mirroring function, all packet exchanges in the intranet can be passively monitored. In that case, detailed behavior of connected devices can be known, but careful treatment of information is required. The probe by itself does not generate any packets, and this method introduces no traffic overhead. However, a device which has little occasion to send packets spontaneously is likely to remain undetected. A good example of such a device is a network printer. Furthermore, the power-off of the device must be inferred from a time-out period of inactivity. Thus, lack of accuracy is a disadvantage of this method.

In the active method, probe packets are periodically sent out to elicit response packets from some or all networked ICT devices in the intranet. The absence of response within a pre-defined timeout period would indicate that the corresponding device is not active. ICMP ping sweep is a typical method of active probing. In this method, generally, a probe packet is sent to every address in the address space of the target intranet and devices which will be missed by the passive method can be detected. However, this could potentially generate a large volume of traffic and requires careful design and deployment. In some designs, the target address could be limited to a specific part of the address space. If the target address space is very large e.g. a class-A or class-B address space, the usability of this method is doubtful. The latency in the detection of newly booted device will depend on the frequency of the probe packets. For early detection, probe packets will need to be sent more frequently.

In the hybrid method, the passive method and the active method complement each other. The passive method detects newly booted devices and monitors activities of continuously communicating devices. The active method is used to monitor the activities of devices that communicate infrequently. Since newly booted devices can be detected by the passive

Table 4. Start-up Behavior of Various Operating Systems

Operating systems	Start-up behavior
Microsoft Windows XP	Sends gratuitous ARP and performs address resolution of Default gateway
Microsoft Windows Vista	Sends ARP and performs address resolution of Default gateway
Microsoft Windows 7	Sends ARP and performs address resolution of Default gateway
Microsoft Windows Server 2003	Sends gratuitous ARP and performs address resolution of Default gateway
Microsoft Windows Server 2008	Sends ARP and performs address resolution of Default gateway
Linux Kernel 2.6	Performs address resolution of Default gateway
Linux Kernel 3	Performs address resolution of Default gateway
FreeBSD 8.2	Sends gratuitous ARP and performs address resolution of Default gateway
NetBSD 5.1	Sends gratuitous ARP
OpenBSD 4.9	Sends gratuitous ARP
Solaris 11	Sends gratuitous ARP and ARP, performs address resolution of Default gateway
MacOS X 10.5.8	Sends ARP and gratuitous ARP, performs address resolution of Default gateway
iOS5	Sends gratuitous ARP and performs address resolution of Default gateway
iOS6	Sends gratuitous ARP and performs address resolution of Default gateway
Android 3.2	Performs address resolution of Default gateway
Android 4.2	Performs address resolution of Default gateway

method, the volume of probe packets in the active method can be lowered by removing the detected devices from the target list of active probing. Hence, the hybrid method can achieve a high accuracy with moderate traffic overhead.

4: Detection and Monitoring of Active Devices in Real Environments

We carried out an experiment of detecting and monitoring active devices in our university computer room. Through this experiment, we show the effectiveness of the packet-based information in detecting active devices. We also show that collating information from multiple sources is useful in finding wasteful activities of devices.

4.1: Experimental Environment

The following devices are connected to the network segment in the university computer room. Each device has an IP address of the form 192.168.0.X (X: 2 $\sim$ 253). The device type can be identified by the value of X as follows.

- 116 user terminals (Microsoft Windows 7) : X=10 $\sim$ 124, and 241
- five network printers : X=2 $\sim$ 6
- seven network switches : X= 247 $\sim$ 253

The computer room is available during business hours (from 8:30 to 20:00) on weekdays. Students and staff can freely use terminals and printers during these hours.

Figure 1 shows the network topology of the target network.

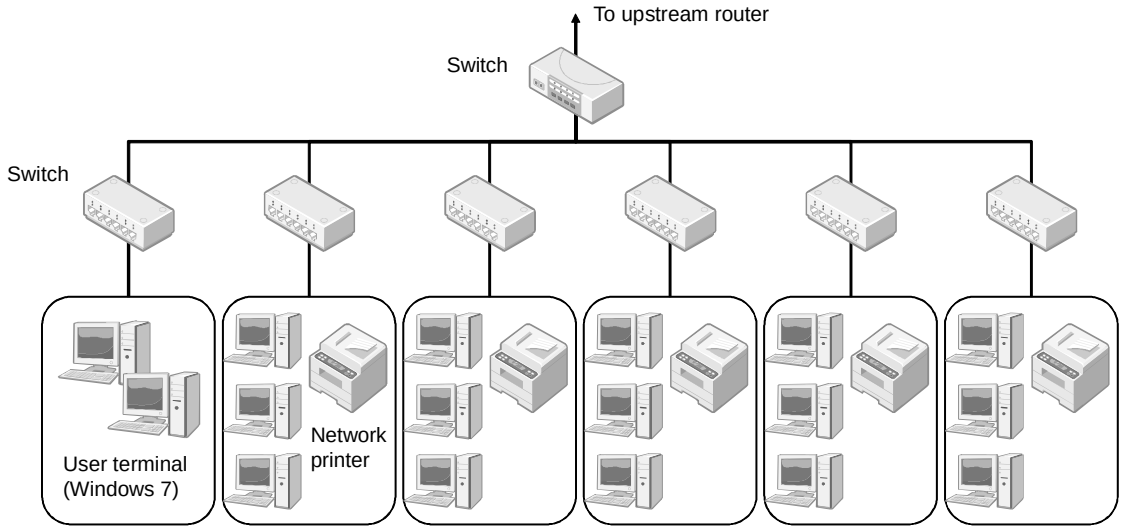

Figure 1. Network Topology

Utilizing both packet-based and device-based information, we detect and monitor the active devices in this environment. We deployed a packet probe for obtaining packet-based information. The probe passively monitors ARP packets and sends probe packets

once every ten minutes for actively monitoring activities of printers and switches. The duration of the period of inactivity for inferring the power-off of a device is set to one hour in order to estimate device activities conservatively, to avoid underestimating the power consumption by a device. For the purpose of network management in the target experimental environment, Logon and Logoff events on every user terminal are reported to a central server. Therefore, the device-based authentication information is also available.

4.2: Experimental Results

The experiment was conducted from Dec. 16th, 2011 to May 27th, 2012. In this subsection, we discuss the wasteful activities of various devices based on the results of monitoring of active devices.

4.2.1: Wasteful Activities of Printers and Switches

To begin with, results of monitoring with packet-based information are discussed. Figure 2 shows the variation in the number of active devices on a certain day during the experiment. From this figure, we can see that a constant number of devices are always active in this network.

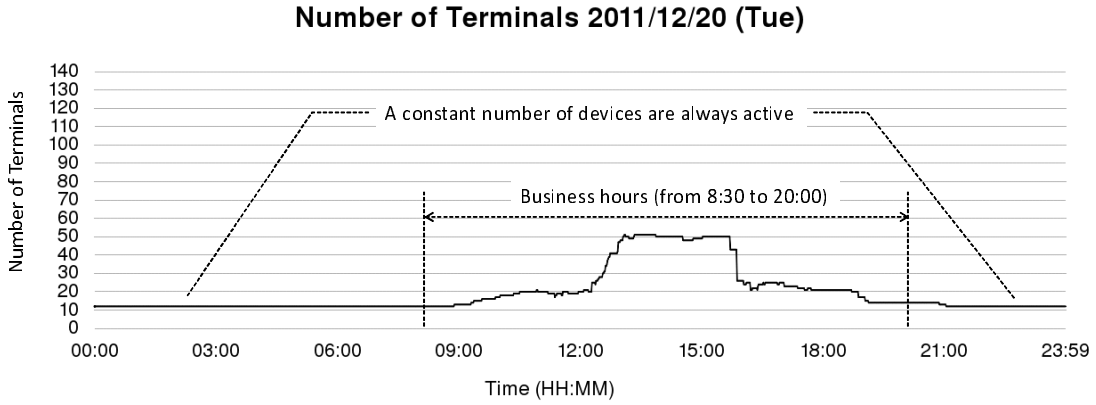

Figure 2. The Number of Active Devices

Figure 3 illustrates the power-on/off state of individual devices on the same day. Figure 4 explains how to understand Fig. 3. As shown in Fig. 3, beyond business hours all user terminals are powered off. However, printers and switches are powered on round the clock. This exercise helped in identifying wasteful power consumption. These printers and switches must be powered off after business hours.

For detecting and eliminating this type of wasteful power consumption, the inter-dependence among devices should be clear. In this environment, printers and switches depend on user terminals because printers and switches should not be powered on if there is no active user terminal in the network. Our future work will focus on analyzing and visualizing such dependencies.

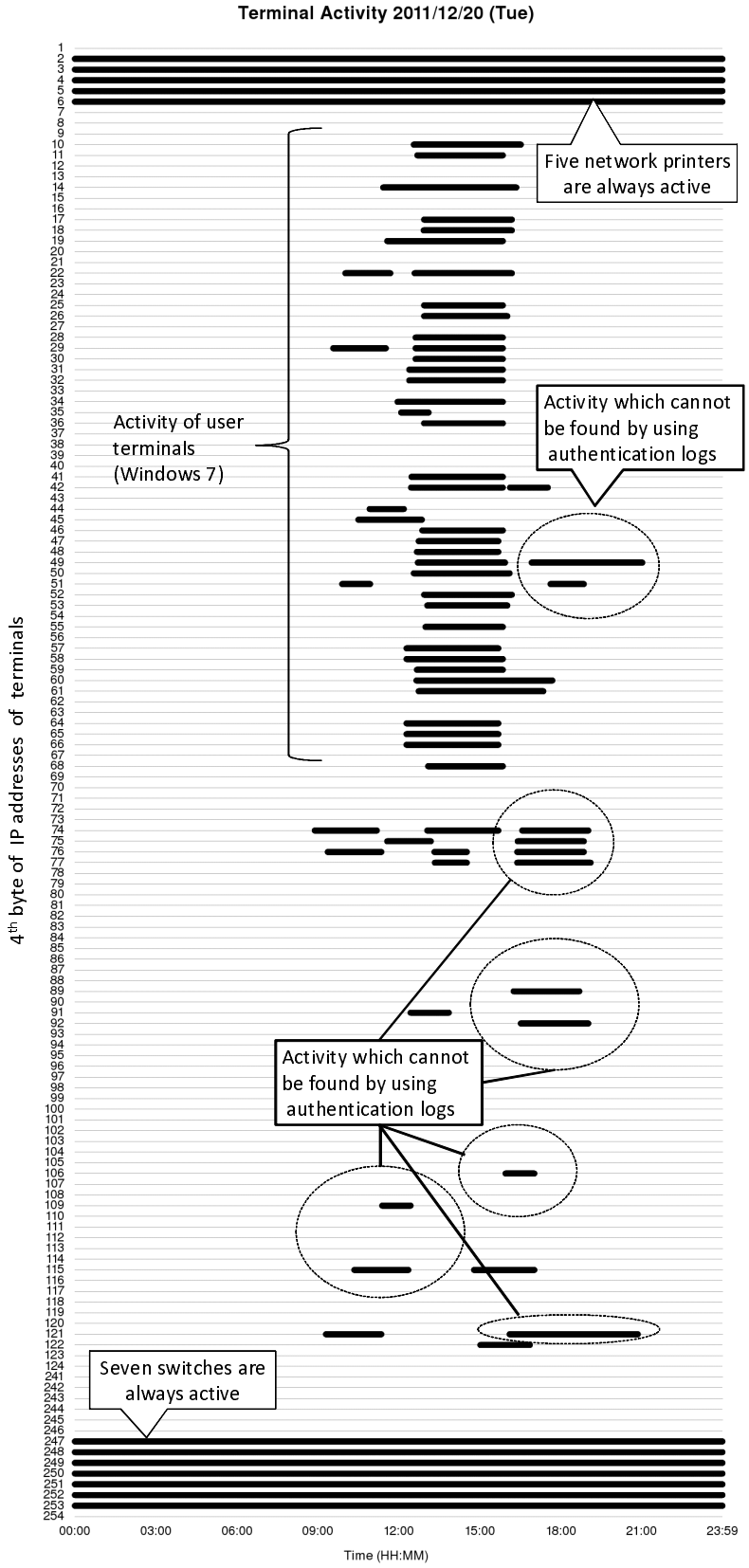

Figure 3. Activities of Devices (Generated with Packet-based Information)

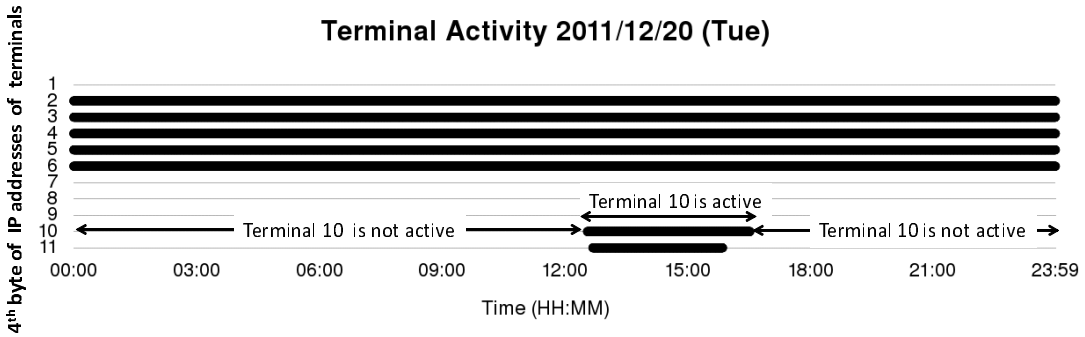

Figure 4. Example of Activity Chart

4.2.2: Wasteful Activities of User Terminals

A device is considered to be *actually used* from the time of Logon to the time of Logoff. As discussed in Sec. 3.1, certain logs contain authentication event information and we can know not only whether a device is active but also whether the device is actually used by a user. If the device was not actually used by a user, the device activity was wasteful. In this section, we show the power-on/off state detected with a device-based authentication information, and try to clarify the wasteful activities of user terminals by comparing the monitoring results with packet-based information.

Figure 5 shows the power-on/off state of devices detected based on times of Logon and Logoff.

By comparing Figs. 3 and 5, we observe the following points.

- As shown in Fig. 5, with the device-based information the power-on state of printers and switches cannot be detected. This is because authentication information or related logs did not exist or, could not be collected, from these devices. This is a limitation of device-based information.
- The active period estimated by using packet-based information is always longer than the period estimated by using device-based information. This is due to the conservative setting of the time-out period. The appropriate setting of the time-out period is an outstanding issue.

Some of the active periods detected using packet-based information do not appear in Fig. 5. This is because some terminals were powered on and connected to the network, but no one logged on. Subsequently they were powered off. In other words, they were not actually used. The terminals consumed power wastefully while they were active. This result suggests the usefulness of the combination of device-based and packet-based information for detecting wasteful device activity.

Figure 6 shows the results of long-term monitoring from May 7th to 27th, 2012. This figure shows a number of active periods where the corresponding device was not actually used, for each day. There are a total of 79 wasteful active periods. As shown in this figure, the number of the periods depends on the day of the week. It appears to indicate a dependence on the class; 49 out of 79 wasteful active periods were monitored in the classes. In Fig. 7, we summarize the number of wasteful active periods per class. It is clear that

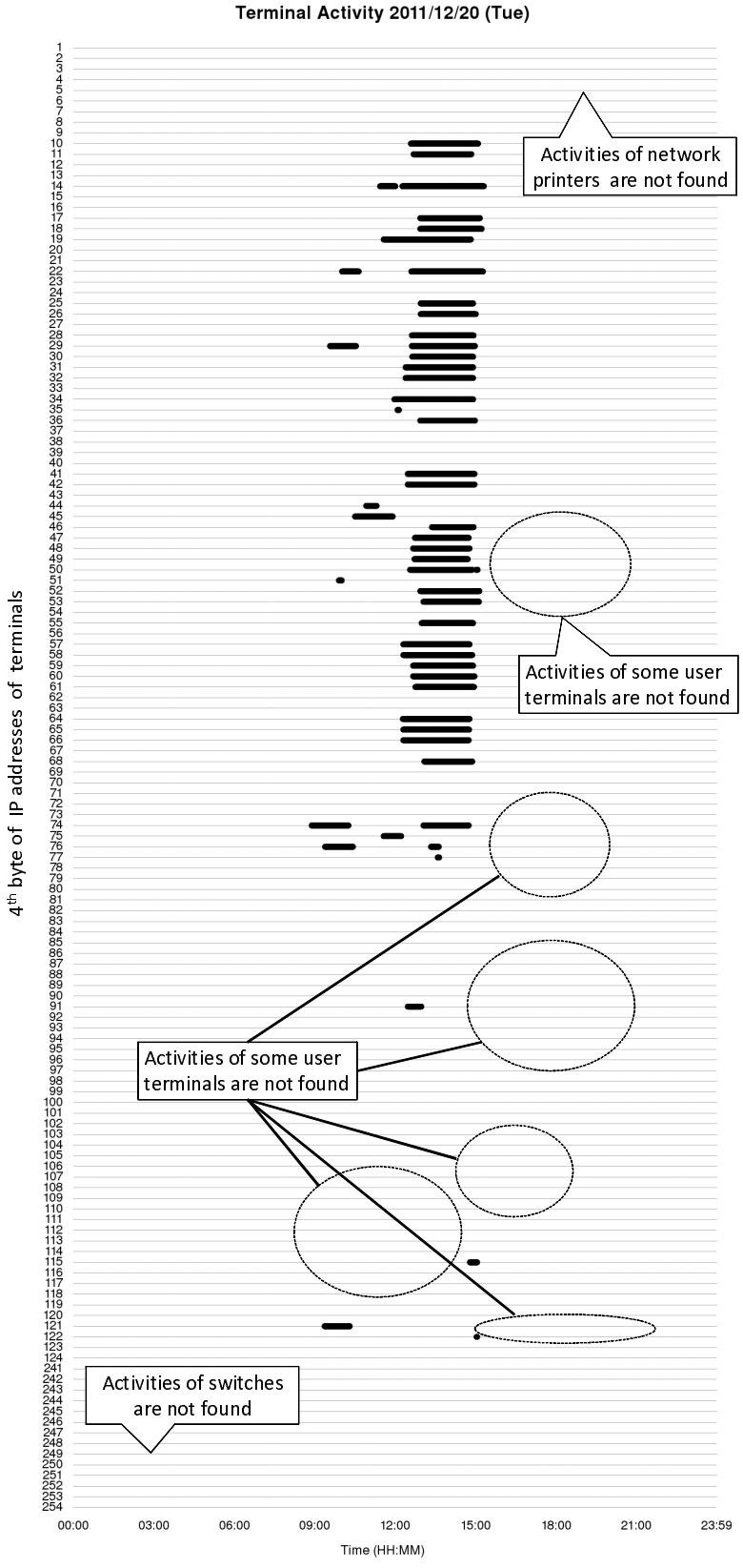

Figure 5. Activities of Devices (Generated with Device-based Authentication Information)

there is a relationship between a class and the corresponding number of wasteful active periods. In order to deepen users' awareness, it is important to report the existence of these wasteful active periods to users.

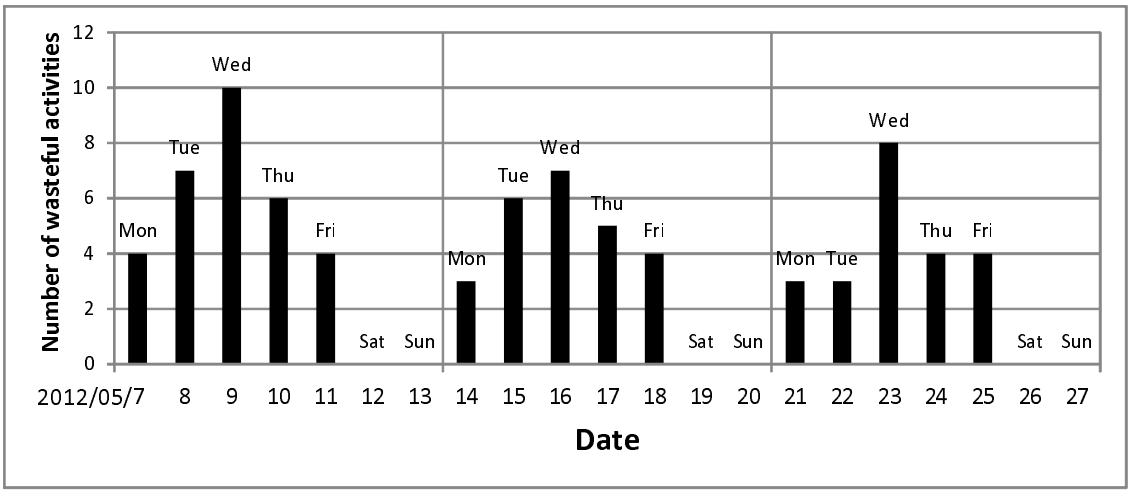

Figure 6. Number of Wasteful Activities per Day

[18] estimates that the power consumption due to wasteful activities of user terminals in the same environment as that in the current work. According to the estimation, the wasteful power consumed from April to October 2012 is about 71kWh. The authors have also reported that users complete the Logon procedure within 15 minutes in 95% of active periods of user terminals. Assuming that the remaining 5% of active periods are not usual but wasteful activity, they estimate that 61kWh out of 71kWh can be reduced by shutting down a terminal if the terminal is not logged into within 15 minutes of power-on.

In addition, it will be useful to force a terminal into sleep mode in case it is difficult to power off the terminal. Since most switches, printers, servers, and user terminals have the standby/sleep mode wherein the power consumption is minimal, putting the terminals in sleep mode is the second-best way for reducing wasteful power consumption.

5: Green Network Architecture

Devices in networks can be categorized into clients, servers, and infrastructure equipment, according to their roles. Clients are user terminals such as desktop PCs or laptop PCs. Servers are further categorized based on the target of services. Intranet servers provide services to clients in an intranet. DHCP, Proxy, and Internal Web servers are examples of intranet servers. Network printers too are intranet servers. Internet servers provide services to clients outside of the intranet. Web, Mail, DNS servers are categorized as Internet servers. Although we mainly focus on edge devices and their power consumption in this research, in a network it is not enough to just power on a server and a client to realize a service. All the network devices, including the infrastructure equipment that connect the client to the server must be powered on.

In order to minimize power consumption in a network, it is important to design the

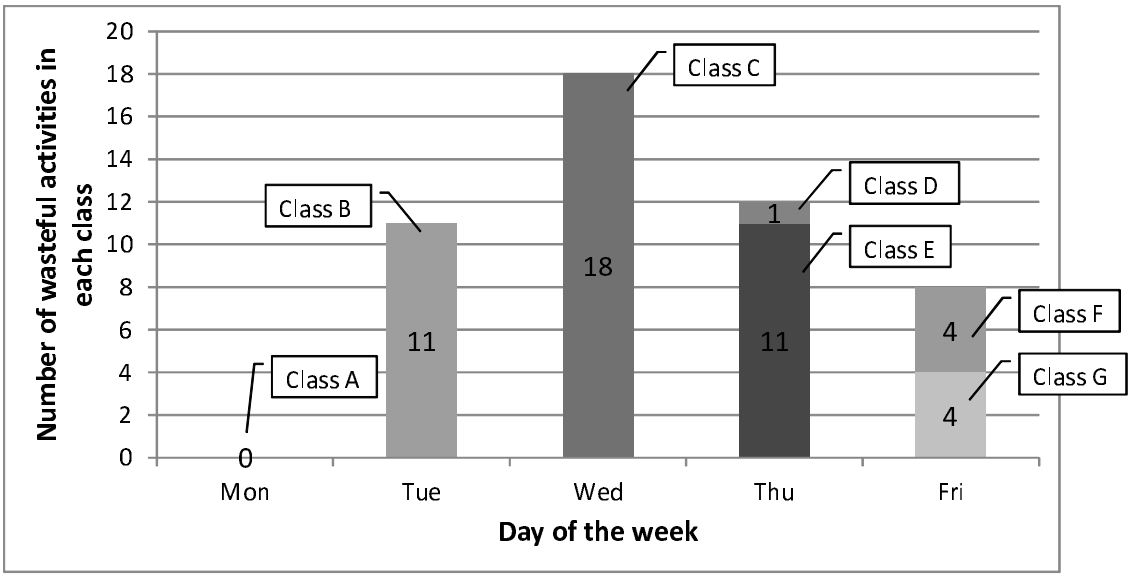

Figure 7. Number of Wasteful Activities in Each Class

network so that a minimum number of devices are required to be powered on to provide a service. However, such network design needs careful consideration of the category of the devices. A Green Network Architecture is one that takes into consideration the roles of the constituent devices to minimize the overall network power consumption. In the following, we discuss how we can implement a Green Network Architecture.

An *activity pattern* is the activity state of a device seen over a period of time. The activity pattern of a device depends on the category of the device. Generally speaking, clients become active intermittently during business hours according to the usage patterns of users. Since intranet servers provide services to clients, they should be active continuously during business hours. In other words, these servers must be active during business hours and are not required to be active beyond business hours. Internet servers should be active and running round the clock. Due to the difference of the activity pattern, if devices that have different patterns of activities are connected to the same network segment, it results in wasteful activity of infrastructure equipment. Figure 8 illustrates an example of such a network architecture. In Fig. 8, every network segment includes Internet servers, intranet servers and clients. Thus, even if all clients are powered off after business hours, the infrastructure equipment, e.g. the switches need to be powered on to provide connectivity for the Internet servers.

It is important to segregate parts of a network based on activity patterns as shown in Fig. 9. In other words, Internet servers will not be placed in a network segment which contains clients and intranet servers. If a segment contains only clients and intranet servers, the entire segment including the infrastructure equipment in that segment can be powered off if no device activity needs to be supported. In this manner, a Green Network Architecture makes it possible to aggressively power off more infrastructure equipment and reduce power consumption.

For realizing such a Green Network Architecture, automatic/semi-automatic network map [19,20] generation technologies that discover the layer-3, layer-2 network topology will

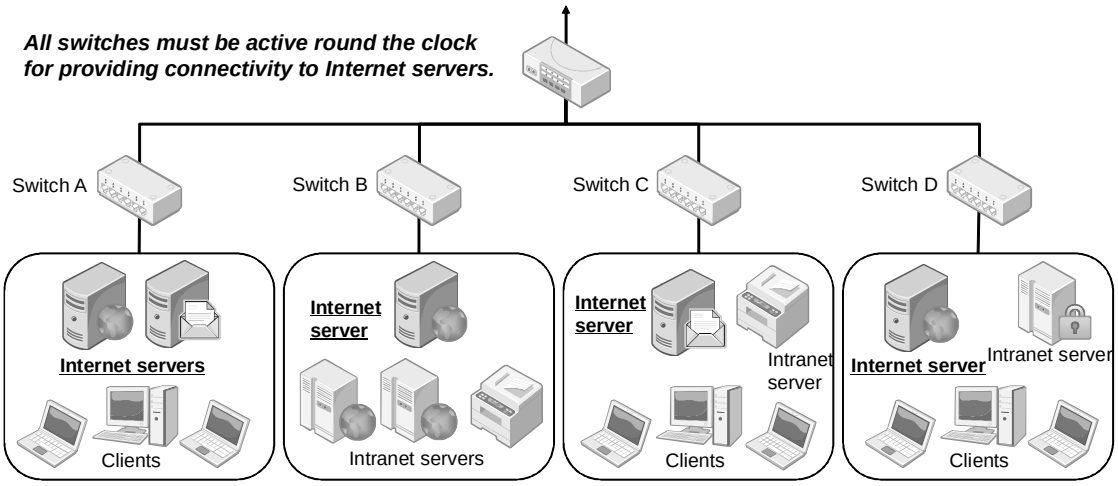

Figure 8. Network Architecture Including Wasteful Activities

play a significant role in visualizing the layer-3 and layer-2 infrastructure equipment that are consuming power in the network.

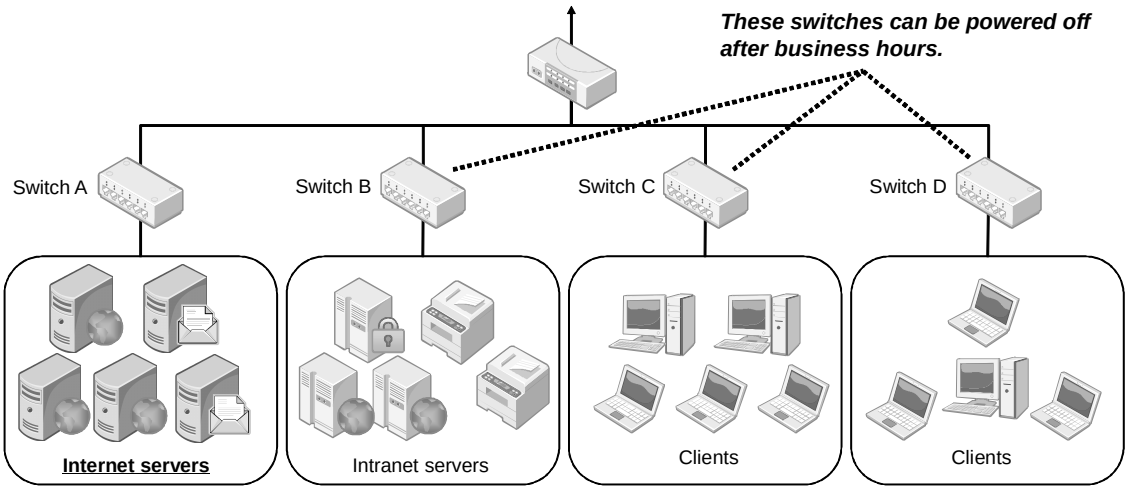

Figure 9. Greener Network Architecture

6: Conclusion

In this paper, we have addressed the issue of detecting and monitoring active devices in an intranet using network management technology. We have shown that existing mechanisms and information available in the network using standard protocols can be used to monitor the power-on/off state of ICT devices. Through experiments in a real network, we have shown that the power wastage due to network printers, switches, and user terminals can

be detected. We could see that printers and switches were active beyond defined business hours and some user terminals were powered on but not used.

This information can be used not only to prevent immediate waste but also to redesign and/or reorganize the network topology for energy efficiency.

Apart from the engineering aspect of detecting and preventing waste, we believe that the result helps in developing a clearer and deeper social awareness of the power wastage and will lead to prevention of wastage. We also believe that, with the spread of IPv6, more and more devices will be networked and effectively widen the scope of this work.

ACKNOWLEDGMENTS

The authors would like to thank the Promotion program for Reducing global Environmental loaD through ICT innovation (PREDICT-115102001), Ministry of Internal Affairs and Communications, Japan, for supporting this work.

References

[1] The Internet: One big power suck. `http://money.cnn.com/2011/05/03/technology/internet_electricity/index.htm`.

[2] The Green Data Center Opportunity. `http://www.datacenterjournal.com/facilities/the-green-data-center-opportunity/`.

[3] Smart 2020: Enabling the low carbon economy in the information age, 2008. `http://www.smart2020.org/_assets/files/02_Smart2020Report.pdf`.

[4] M. Gupta and S. Singh. Greening of the Internet. In *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*, SIGCOMM '03, pages 19–26, New York, NY, USA, 2003. ACM.

[5] S. Sinofsky. Building a power-smart general-purpose Windows, November 2011. `http://blogs.msdn.com/b/b8/archive/2011/11/08/building-a-power-smart-general-purpose-windows.aspx`.

[6] S. Nedevschi, L. Popa, G. Iannaccone, S. Ratnasamy, and D. Wetherall. Reducing network energy consumption via sleeping and rate-adaptation. In *Proceedings of the 5th USENIX Symposium on Networked Systems Design and Implementation*, NSDI'08, pages 323–336, Berkeley, CA, USA, 2008. USENIX Association.

[7] IEEE P802.3az Energy Efficient Ethernet Task Force. `http://www.ieee802.org/3/az/index.html`.

[8] Standby Power. `http://standby.lbl.gov/`.

[9] A. Adelin, P. Owezarski, and T. Gayraud. On the impact of monitoring router energy consumption for greening the Internet. In *Grid Computing (GRID), 2010 11th IEEE/ACM International Conference on*, pages 298 –304, October 2010.

[10] K. Hinton, J. Baliga, M.Z. Feng, R.W.A. Ayre, and R.S. Tucker. Power consumption and energy efficiency in the internet. *Network, IEEE*, 25(2):6 –12, March-April 2011.

[11] T. Nagata. An electric power energy monitoring system in campus using an internet. In *Proceedings of IEEE Power Engineering Society General Meeting*, 2006.

[12] Cisco EnergyWise Technology. `http://www.cisco.com/en/US/products/ps10195/index.html`.

[13] R. Melfi1, B. Rosenblum, B. Nordman, and K. Christensen1. Measuring Building Occupancy Using Existing Network Infrastructure. In *Proceedings of the 2011 International Green Computing Conference and Workshops*, pages 1–8, July 2011.

[14] G. Bellala, M. Marwah, M. Arlitt, G. Lyon, and C. E. Bash. Towards an Understanding of Campus-scale Power Consumption. In *Proceedings of ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Buildings (BuildSys 2011)*, November 2011.

[15] S. Waldbusser and P. Grillo. Host Resources MIB. RFC2790, 2000.

[16] S. Cheshire. IPv4 Address Conflict Detection. RFC5227, 2008.

[17] S. Thomson, T. Narten, and T. Jinmei. IPv6 Stateless Address Autoconfiguration. RFC4862, 2007.

[18] Y. SYOUJI, H. TSUNODA, and M. MATSUDA. Estimation of Power Consumption Due to Wasteful Activities of User Terminals in Intranet. In *Proceedings of the 75th National Convention of IPSJ 1E-1*, March 2013. (In Japanese.).

[19] G. Mansfield, K. Jayanthi, T. Ika, K. Ohta, and Y. Nemoto. Network cartographer. In *Proceedings of the fourth ACM international conference on Multimedia*, MULTIMEDIA '96, pages 439–440, New York, NY, USA, 1996. ACM.

[20] G. Mansfield, M. Ouchi, K. Jayanthi, Y. Kimura, K. Ohta, and Y. Nemoto. Techniques for automated network map generation using SNMP. In *INFOCOM '96. Fifteenth Annual Joint Conference of the IEEE Computer Societies. Networking the Next Generation. Proceedings IEEE*, volume 2, pages 473–480, March 1996.

Authors

Hiroshi TSUNODA received his B.E. degree from the Department of Information Engineering at Tohoku University in 2000, the M.S. and Ph.D. degrees from the Graduate School of Information Sciences at Tohoku University in 2002 and 2005, respectively. From April 2005 to March 2008 he was an assistant professor in the Graduate School of Information Sciences, Tohoku University. He is now a Senior Assistant Professor in the Department of Information and Communication Engineering, Tohoku Institute of Technology. His research interests include wireless networking, network management, and network security. He is a member of the IEICE, IPSJ, and IEEE.

Masahiro MATSUDA received his B.S., M.S., and Ph.D. degrees in engineering from Utsunomiya University in 1995, 1997, and 2000, respectively. He is currently an Associate Professor at the Faculty of Engineering, Tohoku Institute of Technology, Miyagi, Japan. His current research interests include embedded system, network management, and network security. He is a member of the ASJ, IEICE, JSKE and IPSJ.

Yuusuke SYOUJI received his B.E. degree from the Department of Information and Communication Engineering at Tohoku Institute of Technology in 2012. He is currently working for his M.S. degree at the Graduate School of Engineering, Tohoku Institute of Technology. His research interests include Green IT and network management. He is a member of the IEICE.

Kohei OHTA received his M.S. and Ph.D. degrees from the Graduate School of Information Sciences, Tohoku University, Sendai, Japan, in 1995 and 1998, respectively. He is currently R&D manager of Cyber Solutions Inc. Sendai, Japan. He has been engaged in research on network and security management.

Glenn Mansfield KEENI received his Ph.D. degree in Information Engineering from Tohoku University, Japan. He is currently President/CEO of Cyber Solutions Inc. Sendai, Japan. His research interests include expert systems, computer networks, network management and network security. He is a member of the ACM, IEEE Computer Society and is an active member of the IETF.