Technical Points in the Implementation of the Support System for Operation and Management of DACS System

Kazuya Odagiri
Yamaguchi University
Yamaguchi, Japan
odagiri@yamaguchi-u.ac.jp
kazuodagiri@yahoo.co.jp

Shogo Shimizu
Gakushuin Women's College
Tokyo, Japan
shogo.shimizu@gakushuin.ac.jp

Naohiro Ishii
Aichi Institute of Technology
Aichi, Japan
nishii@acm.org

***Abstract*—As the work for managing a whole LAN effectively without limited purposes, there are works of Policy-based network management (PBNM). The existing PBNM is defined in some organizations including the Internet Engineering Task Force (IETF). However, it has structural problems. For example, it is necessary to add and exchange the mechanism called the PEP located between network servers and clients. That is, it is needed to exchange the network system configuration. To improve the problems, we have been studying next generation PBNM called Destination Addressing Control system (DACS) Scheme. The DACS Scheme controls the whole LAN through communication control by the client software as PEP which locates on a client computer. We have been directly studied the essential part to realize the DACS Scheme. That is, we have not been examined the support system for operation and management of DACS system. In this paper, technical points in the implementation of the support system are examined.**

Keywords-policy-based network manageme; support system.

I. INTRODUCTION

In enterprise computer networks, because network policies and security policies are well defined and are observed forcibly, network management is relatively easy. On the other hand, in campus-like computer networks, network management is quite complicated. Because a computer management section manages only a part of the campus network, there are some user support problems. For example, when mail boxes on one server are divided and relocated to some different servers by a system change, it is necessary for some users to update client's setups. Most of users in campus computer networks are students. Because students do not check frequently their e-mail, it is hard work to make all students aware of necessity of settings update. As the result, because some users inquire for the cause that they cannot connect to a mail server, a system administrator must cope with it. For the system administrator, individual user support is a stiff part of the network management.

As the works on network management, various kind of works such as the server load distribution technology [1][2][3], VPN (Virtual Private Network) [4][5] are listed. However, these works are performed forward the different goal, and don't have the purpose of effective management for a whole LAN. As the work for managing the whole network, works on Opengate [6][7] are listed. This is a kind of Policy-based network management (PBNM). Frameworks of PBNM are defined in various organizations such as Internet Engineering Task Force (IETF) and Distributed Management Task Force (DMTF). However, the PBNM has some structural problems. First problem is communication concentration on a communication control mechanism called PEP (Policy Enforcement Point). Second problem is the necessity of the network updating at the time of introducing the PBNM into LAN. Moreover, third problem is that it is often difficult for the PBNM to improve the user support problems in campus-like computer networks explained above.

To improve these problems of the PBNM, we showed a next generation PBNM. We call it Destination Addressing Control system (DACS) Scheme. As the works of DACS Scheme, we showed the basic principle of the DACS Scheme 20], and security function [21]. In addition, we showed new user support realized by use of the DACS Scheme [22]. Then, the DACS system to realize the DACS Scheme was implemented [23]. We have been directly studied the essential part to realize the DACS Scheme, and have not been examined the support system for operation and management of DACS system. In this paper, technical points in the implementation of the support system are examined.

The rest of paper is organized as follows. Section II shows past works of the network management including the existing PBNM. In Section III, we describe the mechanisms and effectiveness of the DACS scheme. In Section IV, technical points in the implementation of the support system for operation and management of DACS system are shown.

II. Motivation and Related Works

As the works on existing network management, various works such as authentication [24][25], the server load distribution technology [1][2][3], VPN [4][5] and quarantine network [26] are listed. However, these works are performed forward the different goal. Realization of effective management for a whole LAN is not a purpose. These works are performed for the specific purpose, and don't have the purpose of managing a whole LAN. As the work for managing a whole LAN, there is the work of Opengate [6][7], which controls Web accesses from LAN to internet. This work is a kind of PBNM. In PBNM, the whole LAN is managed through various kinds of communication controls such as access control and Quality of Service (QOS) control, communication encryption. The principle of PBNM is described in Figure 1. To be concrete, in the point called PDP (Policy Decision Point), judgment such as permission and non-permission for communication pass is performed based on policy information. The judgment is notified and transmitted to the point called the PEP which is the mechanism such as VPN mechanism, router and firewall located on the network path between servers and clients. Based on that judgment, the control is added for the communication that is going to pass by.

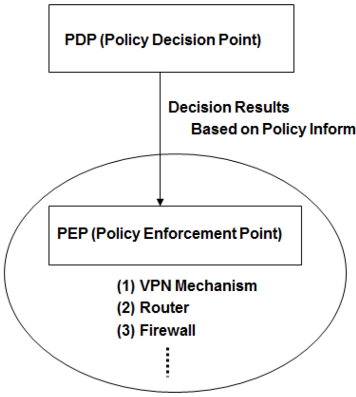
PDP (Policy Decision Point)
Decision Results
Based on Policy Information
PEP (Policy Enforcement Point)
(1) VPN Mechanism
(2) Router
(3) Firewall

Figure 1. PBNM in IETF

The PBNM's standardization is performed in various organizations. In IETF, a framework of PBNM [8] was established. Standards about each element constituting this framework are as follows. As a model of control information stored in the server storing control information called Policy Repository, Policy Core Information model (PCIM) [9] was established. After it, PCMIe [10] was established by extending the PCIM. To describing them in the form of Lightweight Directory Access Protocol (LDAP), Policy Core LDAP Schema (PCLS) [11] was established. As a protocol to distribute the control information stored in Policy Repository or decision result from the PDP to the PEP, Common Open Policy Service (COPS) [12] was established. Based on the difference in distribution method, COPS usage for RSVP (COPS-RSVP) [13] and COPS usage for Provisioning (COPS-PR) [14] were established. RSVP is an abbreviation for Resource Reservation Protocol. The COPS-RSVP is the method as follows. After the PEP having detected the communication from a user or a client application, the PDP makes a judgmental decision for it. The decision is sent and applied to the PEP, and the PEP adds the control to it. The COPS-PR is the method of distributing the control information or decision result to the PEP before accepting the communication.

Next, in DMTF, a framework of PBNM called Directory-enabled Network (DEN) was established. Like the IETF framework, control information is stored in the server storing control information called Policy Server which is built by using the directory service such as LDAP [15], and is distributed to network servers and networking equipment such as switch and router. As the result, the whole LAN is managed. The model of control information used in DEN is called Common Information Model (CIM), the schema of the CIM（CIM Schema Version 2.30.0）[17] was opened. The CIM was extended to support the DEN [16], and was incorporated in the framework of DEN.

In addition, Resource and Admission Control Subsystem (RACS) [18] was established in Telecoms and Internet converged Services and protocols for Advanced Network (TISPAN) of European Telecommunications Standards Institute (ETSI), and Resource and Admission Control Functions (RACF) [19] was established in International Telecommunication Union Telecommunication Standardization Sector (ITU-T).

However, all the frameworks explained above are based on the principle shown in Figure 1. As problems of these frameworks, two points are presented as follows.

(1) Communications sent from many clients are controlled by the PEP located on the network path. Processing load on the PEP becomes very heavy.

(2) The PEP needs to be located between network servers and clients. Depending on the network system configuration, updating for adding the PEP is needed.

To improve these problems of the PBNM, we have been proposed a next generation PBNM called the DACS Scheme. However, the DACS Scheme has some troublesome points in doing operation and management practically. The points are described as follows.

(Point 1)

Because the tool which easily performs registration and deletion of DACS rules does not exist, it is necessary for the network administrator to register it with a database using an SQL language directly.

(Point 2)

When the network administrator grasps the IP address of the client which the user who logged in uses, it is necessary to refer to the table with the information in the direct database.

(Point3)

The tool to easily send a message to the client-side does not exist. Though the possibility of sending the message was confirmed by the functional experiment [22], the tool which each network administrator can use was not implemented.

III. EXISTING DACS SCHEME

A. Basic Principle of the DACS Scheme

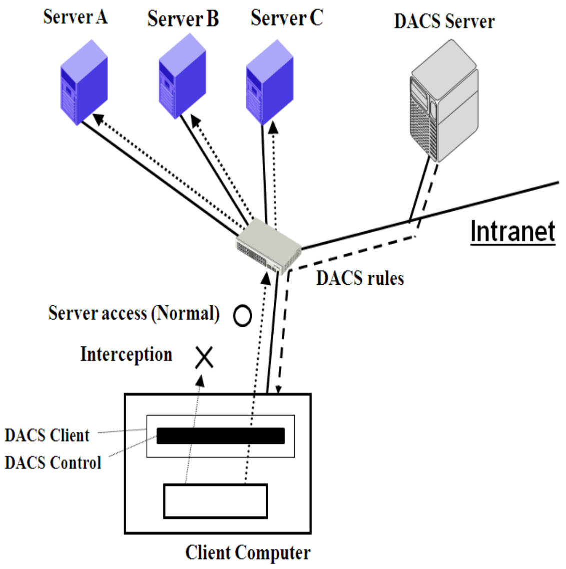

Figure 2. Basic Principle of the DACS Scheme

Figure 2 shows the basic principle of the network services by the DACS Scheme. At the timing of the (a) or (b) as shown in the following, the DACS rules (rules defined by the user unit) are distributed from the DACS Server to the DACS Client.

(a) At the time of a user logging in the client.

(b) At the time of a delivery indication from the system administrator.

According to the distributed DACS rules, the DACS Client performs (1) or (2) operation as shown in the following. Then, communication control of the client is performed for every login user.

(1) Destination information on IP Packet, which is sent from application program, is changed.

(2) IP Packet from the client, which is sent from the application program to the outside of the client, is blocked.

An example of the case (1) is shown in Figure 2. In Figure 2, the system administrator can distribute a communication of the login user to the specified server among servers A, B or C. Moreover, the case (2) is described. For example, when the system administrator wants to forbid an user to use MUA (Mail User Agent), it will be performed by blocking IP Packet with the specific destination information.

In order to realize the DACS Scheme, the operation is done by a DACS Protocol as shown in Figure 3. As shown by (1) in Figure 3, the distribution of the DACS rules is performed on communication between the DACS Server and the DACS Client, which is arranged at the application layer. The application of the DACS rules to the DACS Control is shown by (2) in Figure 3. The steady communication control, such as a modification of the destination information or the communication blocking is performed at the network layer as shown by (3) in Figure 3.

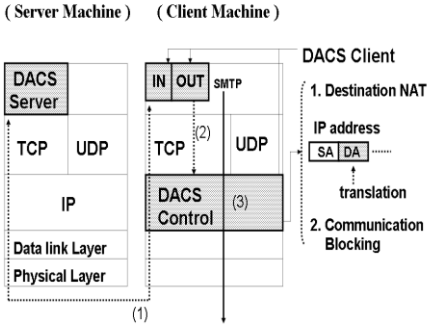

Figure 3. Layer Setting of the DACS Scheme

B. Communication Control on Client

The communication control on every user was given. However, it may be better to perform communication control on every client instead of every user. For example, it is the case where many and unspecified users use a computer room, which is controlled. In this section, the method of communication control on every client is described, and the coexistence method with the communication control on every user is considered.

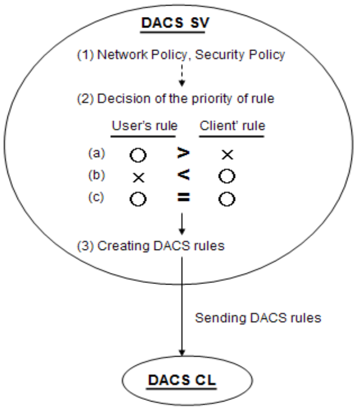

Figure 4. Creating the DACS rules on the DACS Server

When a user logs in to a client, the IP address of the client is transmitted to the DACS Server from the DACS Client. Then, if the DACS rules corresponding to IP address,

ISBN: 978-1-61208-256-1

is registered into the DACS Server side, it is transmitted to the DACS Client. Then, communication control for every client can be realized by applying to the DACS Control. In this case, it is a premise that a client uses a fixed IP address. However, when using DHCP service, it is possible to carry out the same control to all the clients linked to the whole network or its subnetwork for example.

When using communication control on every user and every client, communication control may conflict. In that case, a priority needs to be given. The judgment is performed in the DACS Server side as shown in Figure 4. Although not necessarily stipulated, the network policy or security policy exists in the organization such as a university (1). The priority is decided according to the policy (2). In (a), priority is given for the user's rule to control communication by the user unit. In (b), priority is given for the client's rule to control communication by the client unit. In (c), the user's rule is the same as the client's rule. As the result of comparing the conflict rules, one rule is determined respectively. Those rules and other rules not overlapping are gathered, and the DACS rules are created (3). The DACS rules are transmitted to the DACS Client. In the DACS Client side, the DACS rules are applied to the DACS Control. The difference between the user's rule and the client's rule is not distinguished.

C. *Security Mechanism of the DACS Scheme*

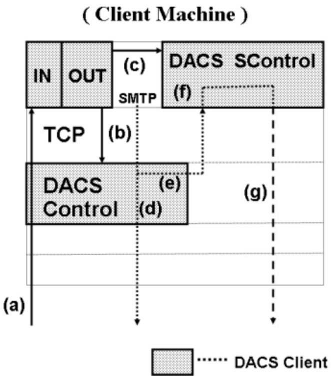

Figure 5. Extend Security Function

In Figure 5, the DACS rules are sent from the DACS Server to the DACS Client (a). By the DACS Client that accepts the DACS rules, the DACS rules are applied to the DACS Control in the DACS Client (b). The movement to here is same as the existing DACS Scheme. After functional extension, as shown in (c) of Figure 5 the DACS rules are applied to the DACS SControl. Communication control is performed in the DACS SControl with the function of SSH. By adding the extended function, selecting the tunneled and encrypted or not tunneled and encrypted communication is done for each network service. When communication is not tunneled and encrypted, communication control is performed by the DACS Control as shown in (d) of Figure 5. When communication is tunneled and encrypted, destination of the communication is changed by the DACS Control to localhost as shown in (e) of Figure 5. After that, by the DACS STCL, the communicating server is changed to the network server and tunneled and encrypted communication is sent as shown in (g) of Figure 5, which are realized by the function of port forwarding of SSH. In the DACS rules applied to the DACS Control, localhost is indicated as the destination of communication.

D. *Specifications of DACS System*

Technical points for implementation of the DACS Scheme are described form (a) to (c).

(a) Communications between the DACS Server and the DACS Client

The Communications between the DACS Server and the DACS Client such as sending and accepting the DACS rules were realized by the communications through a socket in TCP/IP.

(b) Communication control on the client computer

In this study, the DACS Client working on windows XP was implemented. The functions of the destination NAT and packet filtering required as a part of the DACS Control were implemented by using Winsock2 SPI of Microsoft. As it is described in Figure 6 Winsock2 SPI is a new layer which is created between the existing Winsock API and the layer under it.

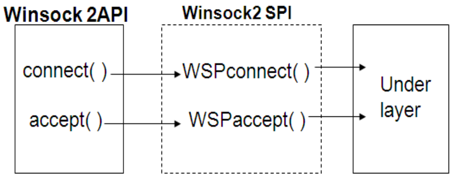

Figure 6. Winsock2 SPI

To be concrete, though connect() is performed when the client application accesses the server, the processes of destination NAT for the communication from the client application are built in WSP connect() which is called in connect(). In addition, though accept() is performed on the client when the communication to the client is accepted, the function of packet filtering is implemented in WSPaccept() which is called in accept().

(c) VPN communication

The client software for the VPN communication, that is, the DACS SControl was realized by using the port forward function of the Putty. When the communication from the client is supported by the VPN communication, first, the destination of this communication is changed to the localhost. After that, the putty accepts the communication, and sends the VPN communication by using the port forward function.

IV. TECHNICAL POINTS IN THE IMPLEMENTATION OF SUPPORT SYSTEM FOR OPERATION AND MANAGEMENT

In this section, to overcome three troublesome points, the support system for operation and management in DACS system is shown. The functions the support system must have are as follows.

(1) Function the network administrator register, change and delete the DACS rules to DACS Server.

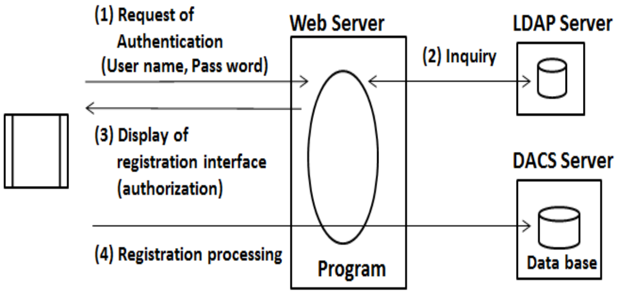
(1) Request of Authentication (User name, Pass word)
Web Server
LDAP Server
(2) Inquiry
(3) Display of registration interface (authorization)
DACS Server
(4) Registration processing
Program
Data base

Figure 7. Function of DACS rule's registration

Figure 7 shows the function of registering the DACS rules. Process (1) is the request process of User Authentication. After the network administrator inputs a user name and pass word into the demand interface of them, they are sent to the program on the Web Server which is implemented in this research. After it, the inquiry processing for user authentication is performed between the program and a LDAP Server which has the information of user account (2). After the authentication is authenticated, registration interface is displayed on the Web Browser on the client (3). When the system administrator inputs the registration information for DACS rules, it is sent to the data base of the DACS Server through the program on the Web Server. In other functions of changing and deleting the DACS rules, the processes from (a) to (c) in Figure 7 are same processes. Only the process (4) replaces changing processing or deleting processing.

The reason of implementation based on http (or https) protocol is why the DASC system will be extended to the direction of Internet management. Therefore, the Web system is more convenient than C/S system.

(2) Function to grasp the correspondence relationship of the user name that logged in the client and the IP address of it

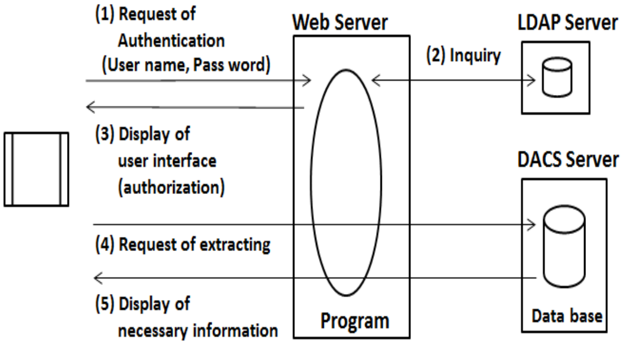
(1) Request of Authentication (User name, Pass word)
Web Server
LDAP Server
(2) Inquiry
(3) Display of user interface (authorization)
DACS Server
(4) Request of extracting
(5) Display of necessary information
Program
Data base

Figure 8. Function of extracting the correspondence relationship of user name and IP address

Figure 8 shows the function of extracting the correspondence relationship of the user name that logged in the client and the IP address of it. Process (1) and process (2) are same as those in Figure 7. After the authentication is authenticated, user interface for inputting extraction conditions are displayed on the Web Browser on the client (3). When the system administrator inputs the extraction conditions, it is sent to the program on the Web Server. The program performs an inquiry on the table which stores the user name and IP address. The correspondence relationship records of user name and IP address are extracted and displayed on the Web Browser through the program on the Web Server.

(3) Function that a system administrator transmits a message to a client-side

Figure 9 sows the function of sending a message to the client side. Process (1) and process (2) are same as those in Figure 7. After the authentication is authenticated, the lists of the user name that logged in the client and the IP address are acquired (3). Based on the lists, the user interface for sending a message to the client side is displayed on the Web Browser on the client. The user interface has the function of selecting destination users or clients, and the function of inputting the message sentences. After the network administrator selects and inputs them, a request of sending the message is sent to the program on the Web Server. The message is sent through the program, and displayed on the Web Browser at the client side.

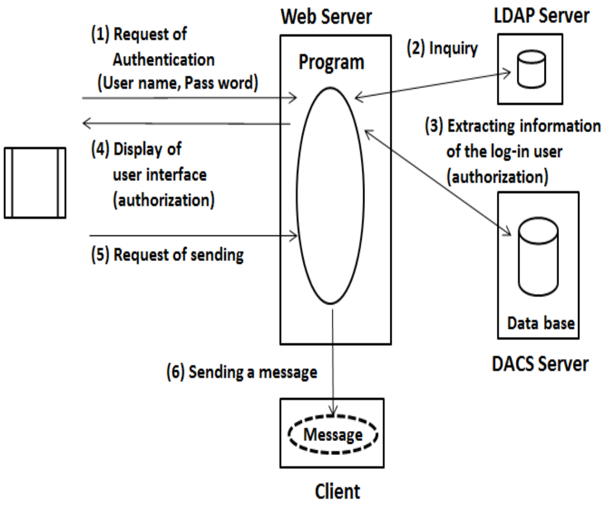
Web Server
LDAP Server
(1) Request of Authentication (User name, Pass word)
Program
(2) Inquiry
(3) Extracting information of the log-in user (authorization)
(4) Display of user interface (authorization)
(5) Request of sending
Data base
DACS Server
(6) Sending a message
Message
Client

Figure 9. Function of sending a message to the client side

As a first point, authentication processes are needed to be implemented by use of encrypted communication based on https protocol and public key infrastructure (PKI). To be concrete, processes of (1)(3)(4) in Figure 7 and those of (1)(3)(4)(5) in Figure 8, those of (1)(4)(5) in Figure 9 need to be encrypted. Next, as means of the security measures of Web Server, access control by client authentication needs to be adapted. Client authentication is a method of access control on the Web Server that is realized by using the private key which a system administrator holds. Therefore, security level becomes higher than simple authentication method using user name and password.

This is because it is necessary for future extensibility of the DACS system to be considered. The DACS system is going to be expanded to operate on the Internet. Therefore, implementation using that is used https and PKI on the Internet normally, is necessary. In addition, LDAP server is adapted as an authentication server. Because it is used on the Windows Server and Unix/Linux Server normally, it is adopted in many organizations. To be concrete, Active Directory is used on a Windows server, OpenLDAP is used on UNIX/Linux servers.

Then, when a Web Server and the LDAP server are located on the different server machine, process (2) in Figure 7,8 and 9 need to be also encrypted. Similarly, when a Web Server and the LDAP server are located on the different server machine, communication processes between the Web Server and a DACS Server need to be also encrypted. Then, as a Certificate Authority (CA) which is used for secure and certain key management, the CA in the high-integrity organization needs to be selected.

VI. CONCLUSION

The DACS system is for the realization of the effective network management based on the DACS Scheme which is one of the policy-based network management schemes. In this paper, we showed technical points in the implementation of the support system for operation and management of the DACS system. To be concrete, we showed three problem of the DACS Scheme on operation and management, and technical points in the implementation of the functions. Because the DASC scheme will be extended into the Internet management system, these functions are realized a web-based application based on http (or https) protocol to meet it. As a near future work, implementation of the support system proposed in this paper will be performed.

REFERENCES

[1] S.K. Das, D.J. Harvey, and R. Biswas,”Parallel processing of adaptive meshes with load balancing,” IEEE Tran.on Parallel and Distributed Systems, vol. 12, No. 12, pp. 1269-1280, Dec 2002.

[2] M.E. Soklic,“Simulation of load balancing algorithms: a comparative study,” ACM SIGCSE Bulletin, vol. 34, No. 4, pp. 138-141, Dec 2002.

[3] J. Aweya, M. Ouellette, D.Y. Montuno, B. Doray, and K. Felske,”An adaptive load balancing scheme for web servers,” Int.,J.of Network Management., vol. 12, No. 1, pp. 3-39, Jan/Feb 2002.

[4] C. Metz, "The latest in virtual private networks: part I," IEEE Internet Computing, Vol. 7, No. 1, pp. 87–91, 2003.

[5] C. Metz, "The latest in VPNs: part II," IEEE Internet Computing, Vol. 8, No. 3, pp. 60–65, 2004.

[6] Y. Watanabe, K. Watanabe, E. Hirofumi, and S. Tadaki,"A User Authentication Gateway System with Simple User Interface, Low Administration Cost and Wide Applicability," IPSJ Journal, Vol. 42, No. 12, pp. 2802-2809, 2001.

[7] S. Tadaki, E. Hirofumi, K. Watanabe, and Y. Watanabe,"Implementation and Operation of Large Scale Network for User' Mobile Computer by Opengate," IPSJ Journal ,Vol. 46, No. 4 pp. 922-929, 2005.

[8] R.Yavatkar, D. Pendarakis, and R. Guerin, "A Framework for Policy-based Admission Control", IETF RFC 2753, 2000.

[9] B. Moore, E. Ellesson, J. Strassner, and A. Westerinen, "Policy Core Information Model -- Version 1 Specification", IETF RFC 3060, 2001.

[10] B. Moore.,"Policy Core Information Model (PCIM) Extensions", IETF 3460, 2003.

[11] J. Strassner, B. Moore, R. Moats, and E. Ellesson, " Policy Core Lightweight Directory Access Protocol (LDAP) Schema", IETF RFC 3703, 2004.

[12] D. Durham, Ed., J. Boyle, R. Cohen, S. Herzog, R. Rajan, and A. Sastry,"The COPS (Common Open Policy Service) Protocol", IETF RFC 2748, 2000.

[13] S . Herzog, Ed., J. Boyle, R. Cohen, D. Durham, R. Rajan, and A. Sastry,"COPS usage for RSVP", IETF RFC 2749, 2000.

[14] K. Chan et al.,"COPS Usage for Policy Provisioning (COPS-PR)", IETF RFC 3084, 2001.

[15] CIM Core Model V2.5 LDAP Mapping Specification, 2002.

[16] M. Wahl, T. Howes, and S. Kille,"Lightweight Directory Access Protocol (v3)", IETF RFC 2251, 1997.

[17] CIM Schema: Version 2.30.0, 2011.

[18] ETSI ES 282 003: Telecoms and Internet converged Services and protocols for Advanced Network (TISPAN); Resource and Admission Control Subsystem (RACS); Functional Architecture, June 2006.

[19] ETSI ETSI ES 283 026: Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control; Protocol for QoS reservation information exchange between the Service Policy Decision Function (SPDF) and the Access-Resource and Admission Control Function (A-RACF) in the Resource and Protocol specification", April 2006.

[20] K. Odagiri, R. Yaegashi, M. Tadauchi, and N. Ishii, ”Efficient Network Management System with DACS Scheme : Management with communication control,” Int. J. of Computer Science and Network Security, Vol. 6, No. 1, pp. 30-36, January 2006.

[21] K. Odagiri, R. Yaegashi, M. Tadauchi, and N. Ishii, “Secure DACS Scheme, ”Journal of Network and Computer Applications, Elsevier, Vol. 31, Issue 4, pp. 851-861, Nov 2008.

[22] K. Odagiri, R. Yaegashi, M. Tadauchi, and N. Ishii, “New User Support in the University Network with DACS Scheme,” Int. J. of Interactive Technology and Smart Education.

[23] K. Odagiri, S. Shimizu, R. Yaegashi, M. Takizawa, and N. Ishii, "DACS System Implementation Method to Realize the Next Generation Policy-based Network Management Scheme," Proc. of Int. Conf. on Advanced Information Networking and Applications (AINA20010), Perth, Australia, Japan, IEEE Computer Society, pp. 348-354, May 2010.

[24] K. Wakayama, Y. Decchi, J. Leng, and A. Iwata, “A Remote User Authentication Method Using Fingerprint Matching,” IPSJ Journal, Vol. 44, No. 2, pp. 401-404, 2003.

[25] Seno, Y. Koui, T. Sadakane, N. Nakayama, Y. Baba, and T. Shikama, “A Network Authentication System by Multiple Biometrics,” IPSJ Journal, Vol. 44, No. 4, pp. 1111-1120, 2000.

[26] Trusted Computing Group, TNC Architecture for Interoperability Version 1.4, Revision 4, 2009.