# Evaluation by Implementation of the Policy-based Network Management System Called DACS System

Kazuya Odagiri
Yamaguchi University
Yamaguchi, Japan

Shogo Shimizu
Gakushuin Women's College
Tokyo Japan

Naohiro Ishii
Aichi Institute of Technology
Aichi, Japan

## 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, communications sent from many clients concentrate on a communication control mechanism called PEP (Policy Enforcement Point). 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 studied on the aspect of principle until now. In this research, we implement a DACS system to realize a concept of the DACS Scheme, and show implement method and results of functional experiments.

## Keywords

*Policy-based network management, destination NAT, packet filtering*

## 1. 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 net-work, works on Opengate [6][7] are listed. This is a kind of Policy-based network management (PBNM). Frameworks of PBNM are de-fined 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 show a next generation PBNM, which overcomes these problems and has the function which does not exist in the existing 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]. The past works of the DACS Scheme's mechanism are theoretical researches, and only functional experiments to prove the possibility were performed. In this research, we implement a DACS System to realize a concept of the DACS Scheme, and experiment in the movement of the DACS System [23].

The rest of paper is organized as follows. Section 2 shows past works of the network management including the existing PBNM. In section 3, we describe the mechanisms and effectiveness of the DACS scheme. In section 4, the implement method and movement experiment of the DACS System are shown. Then, conclusions of the work are presented in section 5.

## 2. 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][27] 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.

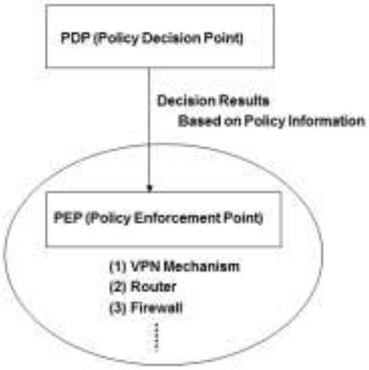

PDP (Policy Decision Point)
Decision Results
Based on Policy Information
PEP (Policy Enforcement Point)
(1) VPN Mechanism
(2) Router
(3) Firewall

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）[16] was opened. The CIM was extended to support the DEN [17], 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.

# 3. Contents of the DACS Scheme

## 3.1 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 pro-gram to the outside of the client, is blocked.

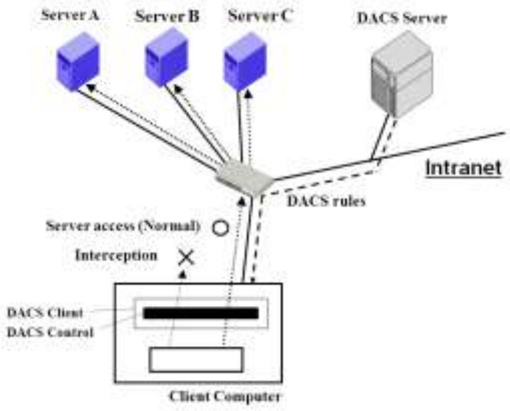


Figure 2 Basic Principle of the DACS Scheme

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.

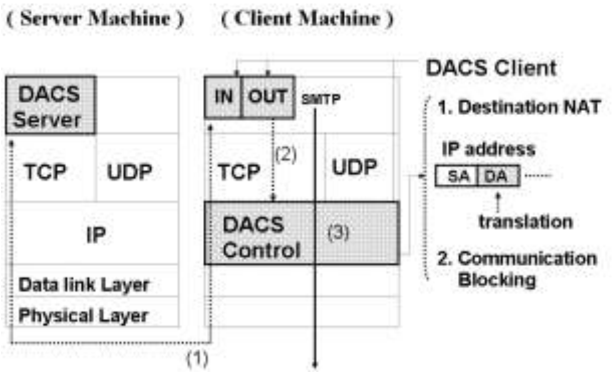


Figure 3 Layer Setting of the DACS Scheme

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.

## 3.2 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.

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

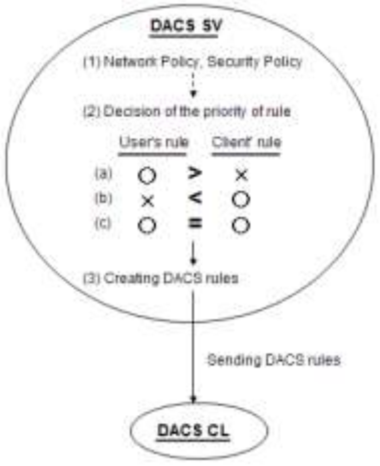


Figure 4 Creating the DACS rules in the DACS Server side

## 3.3 Security Mechanism of the DACS Scheme

In this section, the security function of the DACS Scheme is described. The communication is tunneled and encrypted by use of SSH. By using the function of port forwarding of SSH, it is realized to tunnel and encrypt the communication between the network server and the client which DACS Client is installed in. Normally, to communicate from a client application to a network server by using the function of port forwarding of SSH, local host (127.0.0.1) needs to be indicated on that client application as a communicating server. The transparent use of a client, which is a characteristic of the DACS Scheme, is failed. The transparent use of a client means that a client can be used continuously without changing setups when the network system is updated. The function which doesn't fail the transparent use of a client is needed. The mechanism of that function is shown in Figure 5.

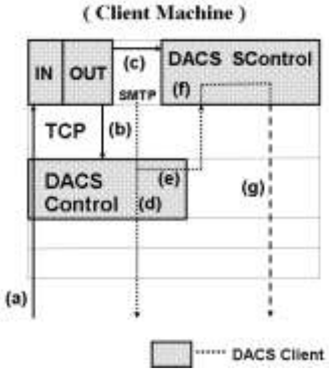


Figure 5 Extend Security Function

The changed point on network server side is shown as follows in comparison with the existing DACS Scheme. SSH Server is located and activated, and communication except SSH is blocked. In Figure 5, the DACS rules are sent from the DACS Server to the DACS Client (a). By the DACS Client which 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. In the DACS rules applied to the DACS SControl, the network server is indicated as the destination of communication. As the functional extension explained in the above, the function of tunneling and encrypting communication is realized in the state of being suitable for the DACS Scheme, that is, with the transparent use of a client. Then, by changing the content of the DACS rules applied to the DACS Control and the DACS SControl, it is realized to distinguish the control in the case of tunneling and encrypting or not tunneling and encrypting by a user unit. By tunneling and encrypting the communication for one network service from all users, and blocking the untunneled and decrypted communication for that network service, the function of preventing the communication for one network service from the client which DACS Client is not installed in is realized. Moreover, even if the communication to the network server from the client which DACS Client is not installed in is permitted, each user can select whether the communication is tunneled and encrypted or not. The function of preventing information interception is realized.

## 3.4 Improvement of User Support Problems

In this section, the improvement results of the user support problem by the DACS Scheme are explained.

### (a) Effective User Support at Changing Setups of Client with the DACS Scheme

When network system is updated, user support by the DACS Scheme is compared with user support by the Non-DACS Scheme, and an ad-vantage of user support by the DACS Scheme is described. User sup-port processes after updating the network system are described in Figure 6.

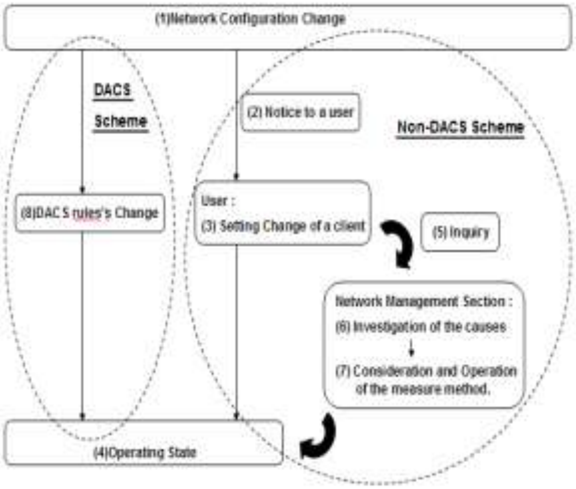

(1)Network Configuration Change
DACS
Scheme
(2) Notice to a user
Non-DACS Scheme
(8)DAC S rules's Change
User :
(3) Setting Change of a client
(5) Inquiry
Network Management Section :
(6) Investigation of the causes
(7) Consideration and Operation of the measure method.
(4)Operating State

Figure 6 Process introducing the DACS Scheme

When the DACS Scheme is not introduced, notification for changing setups is sent to a user in a laboratory (2) after updating the network system (1). It is sent by E-mail and a homepage or a document. The user who accepts that notification updates a client's setups (3). If there is no problem in changing setups of the client, it is enabled to start the operating (4). When it is not possible to update setups by some causes, the user inquires to the network management section (5). In the network section, investigation by hearing comprehension for the user or investigation in the field is done (6). If a cause is specified, the coping way are considered, and carried out (7). It is a burden for a system administrator to support each user for every inquiry. When the DACS Scheme is introduced, a system administrator has only to change the DACS rules (8) at the time of updating the network system. After changing the DACS rules, communication control corresponding to new network system is started at a point in time when the user logs in to a client again (4). Because the system administrator with understanding the policy for using a laboratory network sets the DACS rules, a trouble by a cause except an artificial factor such as missing setups of the DACS rules does not occur. This process of user support is largely simplified in comparison with the process of user support by the Non-DACS Scheme.

### (b) Effective Coping with Annoying Communication by the DACS Scheme

To cope with the communication from a virus infection client and the communication with annoyance to other user such as streaming of moving and sound [28], a system administrator needs to specify which user or client is transmitting the communication to. For example, when there is a direct cause in the client itself such as virus infection, the client must be specified. A user must be specified, when there is a direct cause in user oneself. When the IP address is managed dynamically by DHCP service, much time and effort is spent to specify the client or user. The coping process for annoying communication is described as shown in Figure 7 and explained with an example of the user support for a laboratory.

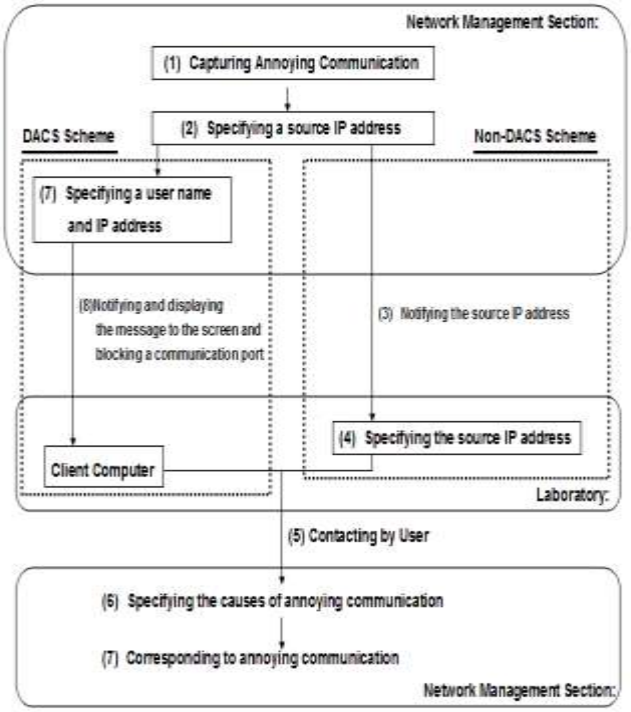

Network Management Section:
(1) Capturing Annoying Communication
(2) Specifying a source IP address
DACS Scheme
Non-DACS Scheme
(7) Specifying a user name and IP address
(8)Notifying and displaying the message to the screen and blocking a communication port
(3) Notifying the source IP address
(4) Specifying the source IP address
Client Computer
Laboratory:
(5) Contacting by User
(6) Specifying the causes of annoying communication
(7) Corresponding to annoying communication
Network Management Section:

Figure 7 Change of User Support

At first, annoying communication for other users is captured by communication detection through the mechanism such as F/W or IDS (1). Next, a source IP address of the annoying communication is acquired (2). To here, it is the same thing when the DACS Scheme is introduced or not introduced. When the DACS Scheme is not introduced, the process of user support is described in the following. Under using DHCP Service, if a whole LAN is divided into multiple subnetworks, and each subnetwork is assigned to each laboratory, a system administrator can manage scope of the IP address used in a laboratory. If not so, the system administrator cannot manage it. In the case of the former, the IP address is notified to the laboratory (3), and the client transmitting the communication is specified (4). In the laboratory, because it is impossible to manage which client uses which IP address, the client is specified after investigating the network setups information of each client. It takes trouble very much. In the case of the latter, it is difficult to specify the client. This is because the system administrator cannot know the laboratory using the IP address. Even if the system administrator can know it, because it is needed to investigate the network setups information of each client, it takes trouble very much. After the client is specified, the user of the laboratory contacts a network management section (5). In the situation that a laboratory cooperates with a network management section, the cause specification of annoying communication and coping with it are done (6). On the other hand, when the DACS Scheme is introduced, source IP address of the annoying communication needs to be acquired (2) to specify the client first. When a user needs to be specified, a user name is specified from the IP address (7). When a user has a direct cause such as streaming of the moving picture and the sound, the message to notify abnormality is transmitted to the IP address of the client which a user logs in. If a client has a direct cause such as infection by virus, the message to notify abnormality is transmitted to the IP address of the client. The message is displayed in the screen of the client. At the same time, the used port by annoying communication is blocked (8). The user sees the message of the screen, and contacts the network management section (5). In the situation that a laboratory cooperates with a network management section, specification of annoying communication and coping with it are done (6). It is shown that the DACS Scheme is effective at the following two points. The first point is that the client which transmits annoying communication is specified simply. The client which has a problem is specified by seeing the message of a screen at a glance. The second point is shown as follows. Because the influence to others is prevented by blocking a communication port of the client, time margin for the cause specification of annoying communication and the coping with it is generated effectively. When the urgent degree such as virus infection is high, the DACS Scheme is particularly effective.

## 4. Implementation Method of the DACS Scheme

### 4.1 Change from the Existing DACS Scheme

As movements of the existing DACS Scheme, there are three phases as follows.

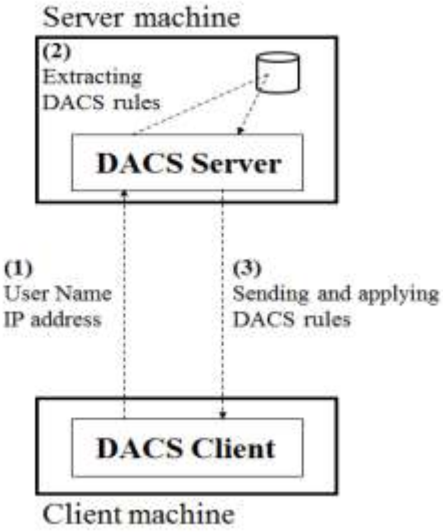


Figure 8 Processes of Phase 1

**(Phase 1) Sending/ Receiving of DACS rules**

In Figure 8, processes of phase 1 are described. When a user logs in to a client, the IP address and user name are sent from the DACS Client to the DACS Server (1) and, the DACS rules corresponding to them are extracting from database (2). Then, they are returned from the DACS Server to the DACS Client and applied to the DACS Control and the DACS SControl on the side of the DACS Client (3).

**(Phase 2-a) Application of DACS rules**

In Figure 9, processes of phase 2 are described. After the DACS rules are changed, the system administrator indicates distribution of the DACS rules (1). Then, the DACS rules are extracting (2) and sent to the DACS Client and are applied to the DACS Control and the DACS SControl (3).

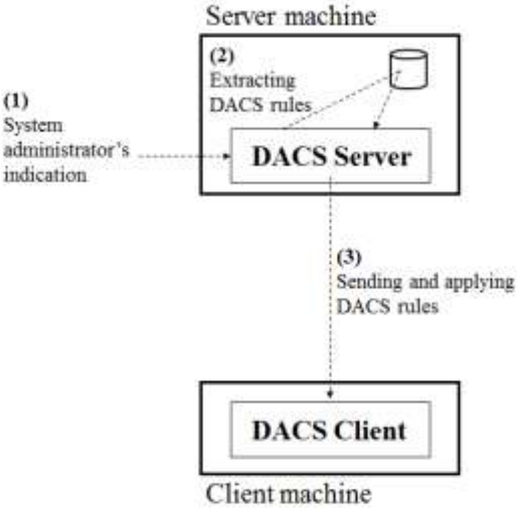


Figure 9 Processes of Phase 2

**(Phase 2-b) Checking of DACS Client's status**
Before process (3) of Phase 2-a in Figure 9, it is checked from the DACS Server side whether the DACS Client on the clients which has been distributed on the network starts.

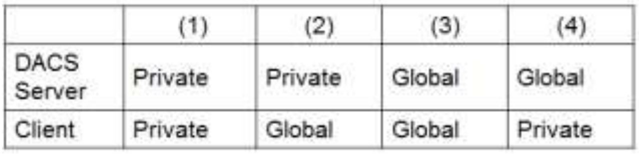
In the existing DACS Scheme described above, there were some problems to introduce it to a real network. Here, the problems and solution for them are drawn as follows.

**(Problem 1) Communication interception by a filtering mechanism at the time of message exchange**
When the DACS rules are changed on the way of the operation, the DACS rules are sent and applied to the DACS Client by the system administrator's indication. However, when there is a packet filtering mechanism such as Firewall on the network to intercept the port that is used at the processing of Phase 2-b, the processing of Phase 2-b does not go well. In addition, when a personal firewall is activate on the client itself, the processing of Phase 2-b does not go well. Therefore, it was changed so that DASC rules were sent form the DACS Server to the DACS Client and were applied to the DACS Client whenever the communication was sent form the client application. That is, after the DACS Client detects the communication sent form the client application, processes in Figure 8 is performed. After it, the communication is sent to the outside of the client. Because the process (1) of phase 1 is freely performed as long as it is not intercepted by a clear intention, the acceptance of the updated DACS rules by process (3) of phase 1 is guaranteed. Therefore, this method is appropriate for the DACS Scheme. Though the communications forward the DACS Server to get the DACS rules concentrate by these changes, it can be prevented by using load balancing technology.

**(Problem 2) Correspondence to the antivirus software on the client**
On the client that is used in the real network, the antivirus software is always installed. However, some kinds of the software are used in the real network. This problem needs to be avoided by the system operation of distributing the setting file that the module name is described in. The module name is changed by the network administrator or the client's user. When the system administrator manages all the software in the network, the system administrator changes the module name in the setting file and distributes it. When the system administrator doesn't manage all the software in the network, the system administrator notifies the setting information to the user, and the user changes module name by oneself.

Besides the above problems, the following points were examined before implementation.

**(Point 1) Correspondence to the mixture of the private IP address and global IP address**
Combinations of IP addresses setting in DACS Server and a client are thought in Figure 10.



|  | (1) | (2) | (3) | (4) |
|---|---|---|---|---|
| DACS Server | Private | Private | Global | Global |
| Client | Private | Global | Global | Private |

Figure 10 Combinations of IP addresses

In this figure, for example, column (1) shows that DACS Server's IP address has a private IP address and each client has a private IP address, too. On the LAN, a pattern of (2) is impossible pairs normally. Usually, when the DACS Server has the private IP address, the client has the private one, too. When IP addresses are assigned in patterns of (1) and (3), (4), it is possible to control a whole LAN by using the DACS system without a problem in particular.

**(Point 2) Correspondence to IP masquerade**
When the processing mechanism of IP masquerade between the DACS Server and the DACS Client is located, problems may occur. Theoretically, directions of the IP masquerade processing are thought as follows.

(a) The direction form the DACS Client to the DACS Server
(b) The direction from the DACS Server to the DACS Client

Because combination patterns of IP addresses were limited to (1) (3) and (4) in (Point 1), it is examined in the range. In case of the pattern (1) and (3), because same kinds of IP addresses are set in the DACS Server and DACS Client, the processing mechanism of IP masquerade do not need to be set. In case of pattern (4), depending on constitution of the LAN, it is necessary. For example, constitution in Figure 11 is listed. This is a case of the direction of the IP masquerade processing in (b), and communications between DACS Sever and DACS Client is performed without a problem in particular.

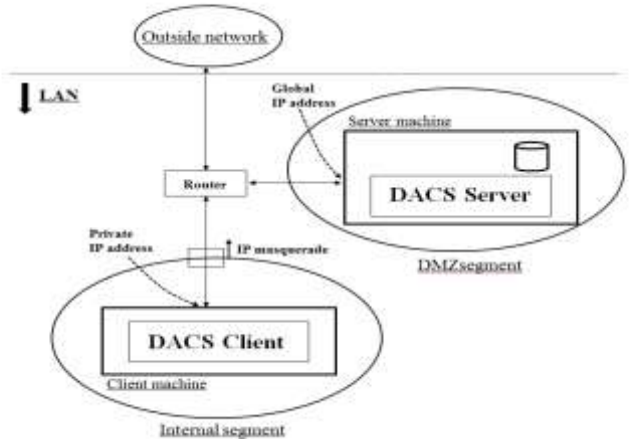


Figure 11 Example of constitution

Then, because the IP masquerade is used to convert private IP address into global IP address, the direction of the IP masquerade processing in (a) does not need to be examined. Therefore, as far as a use range is limited to LAN, IP masquerade does not become the problem in particular.

**(Point 3) Distribution of encryption key**

The DACS system sends the VPN communications. Encryption key is distributed at the same time of distributing the DACS Client to a user. Because the DACS system is used in the LAN of the same organization, this point is no problem in range of this research.

Because point 2 and 3 needs to be solved at the time of applying the DACS system to the Internet, we think that it is a future work.

## 4.2 Specification of the Implementation

The characteristic of the DACS System's implementation is the coping processes at the time of conflicting the relation between communication control every user and communication control every client. At this point, by using algorithm shown in Figure 12, the DACS System is implemented.
First, as Action 1, the judgment table for client control is searched. If the IP address of the client exists in this table, Action 2 is performed. If not, Action 3 is performed. When Action 2 is performed, the control rules every client are searched and extracted from the IP address rule table which has control rules every client (every IP address). When Ac-tion 3 is performed, the judgment table for user control is searched. If the user name logging in the client exists in this table, Action 4 is per-formed. If not, status 1 showing "no applicable rule" is returned. When Action 4 is performed, the control rules every user are searched and extracted from the user rule table or IP user rule table. Because a table name for the search is registered in the judgment table for user control, the search is carried out using the table name. In the user rule table, the DACS rules which are set for each user exist. Then, the IP user rule table has two primary keys (IP address and user name), and the DACS rules are set.

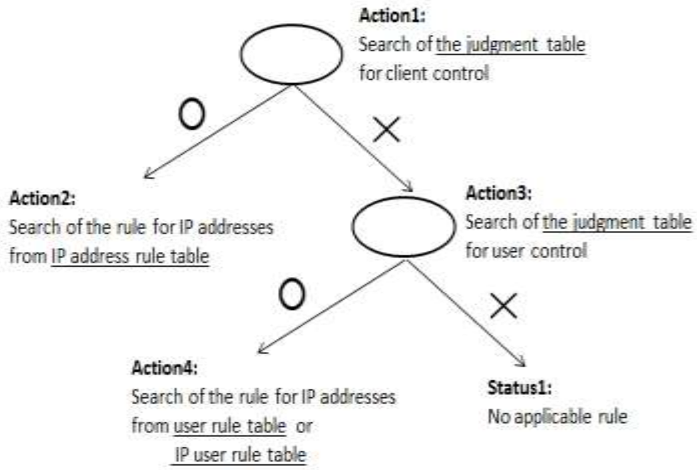

Action1:
Search of the judgment table
for client control
O
×
Action2:
Search of the rule for IP addresses
from IP address rule table
Action3:
Search of the judgment table
for user control
O
×
Action4:
Search of the rule for IP addresses
from user rule table or
IP user rule table
Status1:
No applicable rule

Figure 12 Used Algorism

## 4.3 Technical Points for the Implementation

In this section, technical characteristics of the implementation are explained.

**(a) Environment of the development system**

(a1) DACS Server
OS: Fedora Core 2
Development language: Visual C++ 7.1

(a2) DACS Client
OS: Windows XP Professional Edition
Development language: Visual C++ 7.1,Winsock2 LSP (DACS Control)
Others: Putty (DACS SControl)

**(b) 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.

**(c) 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 13, Winsock2 SPI is a new layer which is created between the existing Winsock API and the layer under it. 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().

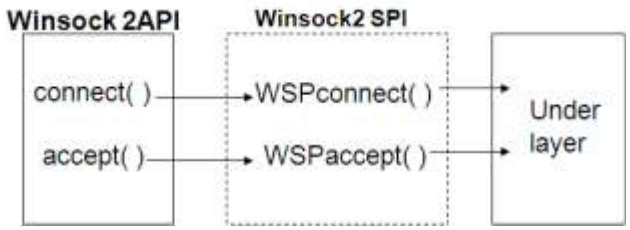


Figure 13 Winsock2 SPI

**(d) 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.

## 4.4 Daemons for the DACS Server

In this section, implementation contents of DACS Server are explained. Figure 14 shows a frame format of the DACS Server. The DACS Server is comprised of a DASC daemon and search processes. The DACS daemon has the functions which receives the request from the DACS Client (1) and can execute the search processes as child process in parallel (2) by the DACS daemon according for each request form the DACS Client. Then, each search process receives the request data such as user name (3), and searches and extracts the DACS rules from the database by using the algorism in Figure 12 (4). After it, the DACS rules are sent back to the DACS Client (5). In these processes, error messages are back to the DACS Client in the processes of Arrow of the dotted line in Figure 14.

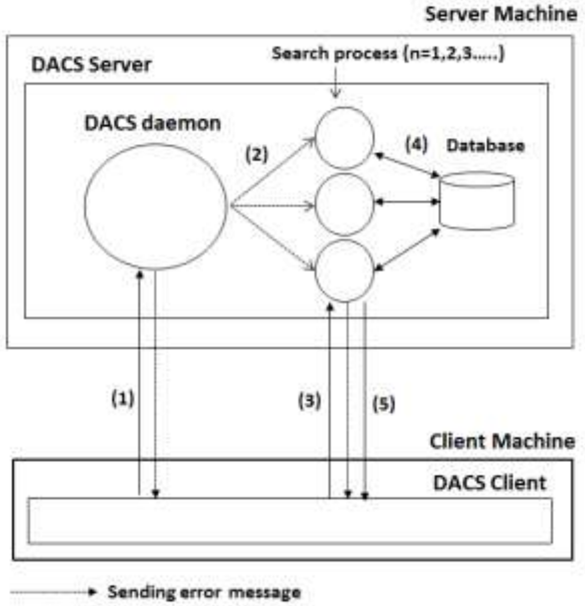


Figure 14 Daemons of the DACS Server

## 4.5 Functional Experiments

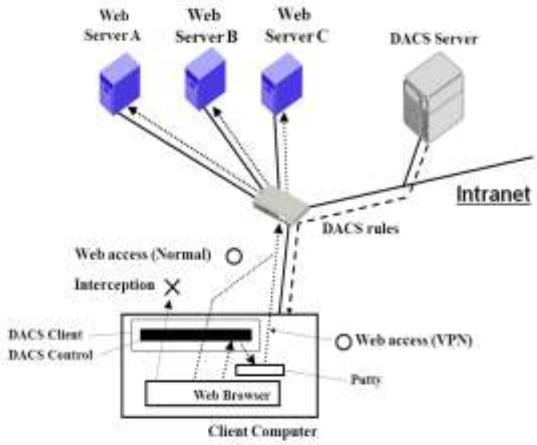
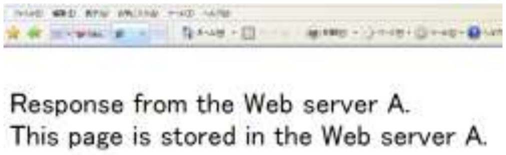


Figure 15 System for the functional experiments

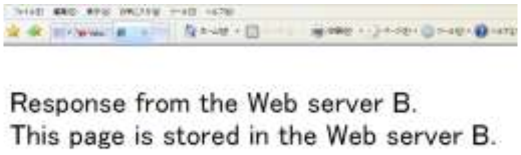
By using this implementation system, functional experiments were performed. First, the function to change the destination of the network servers by using the destination NAT was confirmed. As it was shown in Figure 15, the destination change to some Web servers was confirmed. When user A logged in to the client and inputted the URL X to the Web browser, the Web server A was accessed and the web page shown in Figure 16 was shown on the web browser.



Response from the Web server A.
This page is stored in the Web server A.

Figure 16 Display by the user A

When user B logged in to the client and inputted same URL X to the Web browser, the Web server B was accessed and the web page shown in Figure 17 was shown on the web browser. When user C logged in to the client and inputted same URL X to the Web browser, Web server C was accessed and the web page different from user A and user B was shown on the web browser.



Response from the Web server B.
This page is stored in the Web server B.

Figure 17 Display by the user B

Next, the function to change the destination of the network servers by using VPN communication was confirmed. Before this functional confirmation, the DACS rules were changed as the communication to each Web server was directed to the localhost. This VPN communication was performed by connecting the communication by using the above function to the putty as a VPN client. When user A logged in to the client and inputted the URL X to the Web browser, the Web server A was accessed and the same web page shown in Figure 16 was shown on the web browser. In the case of user B and user C, same web page in the above function was shown. Because the communications besides the VPN communication were blocked in advance, it was sure that these accesses were performed by the VPN communication. Lastly, the function to intercept the communication to the network servers by using the packet filtering mechanism was confirmed. Before this functional confirmation, the DACS rules was changed as the communications to each Web server by user A, user B and user C were intercepted. When each user logged into the client and inputted the URL X to the Web browser, the time out error was displayed on the client and this Web access was intercepted. In these functional experiments, it was confirmed that the DACS system operated correctly in the point of the function.

## 5. Conclusion

In this study, we implemented the DACS system to realize the DACS Scheme as the next generation PBNM. In DACS system, the structural problems of the existing DACS Scheme were improved. To be concrete, communication concentration from many clients to the DACS Server as the PEP was solved, and the problem in sending and accepting the DACS rules between the DACS Server and the DACS Client was solved. We described the results of the functional experiments.

## 6. 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, 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, 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 at el., "A Framework for Policy-based Admission Control", IETF RFC 2753, 2000.

[9] B. Moore at el., "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 at el., " Policy Core Lightweight Directory Access Protocol (LDAP) Schema", IETF RFC 3703, 2004.

[12] D. Durham at el.,"The COPS (Common Open Policy Service) Protocol", IETF RFC 2748, 2000.

[13] S. Herzog at el.,"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 at el.,"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 specifica-tion", April 2006.

[20] K.Odagiri, R.Yaegashi, M.Tadauchi, 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, N.Ishii, “Secure DACS Scheme, ”Journal of Network and Computer Applications,” Elsevier. (in printing)

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

[23] Kazuya Odagiri, Shougo Shimizu, Rihito Taegashi, Makoto Takizawa, Naohiro 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, A.Iwata, “A Remote User Authentication Method Using Fingerprint Matching,” IPSJ Journal, Vol.44, No.2, pp.401-404, 2003.

[25] S.Seno, Y.Koui, T.Sadakane, N.Nakayama, Y.Baba, T.Shikama, “A Network Authentication System by

Multiple Biometrics," IPSJ Journal, Vol.44, No.4, pp.1111-1120, 2000.

[26] http://www.nec.co.jp/univerge/solution/pack/quarantine/

[27] http://www.ntteast.co.jp/business/solution/security/quarantine/index.html

[28] H. Hu, J. Kashio, Y. Honda, H. Suzuki, "Rate Control Method for Real Time Protocol (RTP) Enabling the Coexistence with TCP," IEICE Tran.on Communications,Vol.J84-B,No.11,pp.1994-2004,2001.