Efficient Network Management System with DACS Scheme

Kazuya Odagiri
Aichi Institute of Technology
1-38-1 Higashiyamadouri Chikusa-ku Nagoya-city Aichi Japan
Email: odagiri@toyota-ti.ac.jp

Rihito Yaegashi and Masaharu Tadauchi
Toyota Technological Institute
2-12-1 Hisakata Tenpaku-ku Nagoya-city Aichi Japan
Email: rihito@toyota-ti.ac.jp   tadauchi@toyota-ti.ac.jp

Naohiro Ishii
Aichi Institute of Technology
Email: ishii@aitech.ac.jp

Abstract

Where customers with different membership and position, use computers as in the university network systems, it often takes much time and efforts for them to cope with the change of the system management. This is because the requirements for the respective computer usage are different in the network and security policies. In this paper, a new destination addressing control system (DACS) scheme for the university network services is proposed. The DACS Scheme performs the network services efficiently through the communication management of a client. As the characteristic of DACS Scheme, only the setup modification is required by a system administrator, when the configuration change is needed in the network server. Then, the setup modification is unnecessary by a customer, which shows a merit for both a system administrator and a customer. This paper describes the instruction and the prototype for DACS Protocol as the implementation of DACS Scheme. Then, the simplicity of the system management in DACS Scheme, is examined from the customer and the system administrator viewpoints.

1. Introduction

The characteristic of the operation and management in the university network systems, is that people with different membership and position as students, faculties, external persons, et al., use the network services comparatively freely. In the business corporations, it is comparatively easy to spread the information of the network usage based on a network policy or a security policy. However, in the university, it is often difficult to spread the information of the network usage, since the computer management section does not perform all operation and management for the respective needs. Although the system administrator of the computer section, carries out management and operation of the most network infrastructure and servers, the customer mainly performs the management of their clients[1]. Operation and management of the network system, are conventionally focused on the control in the infrastructure or server side [2][3]. For example, DNS round robin[4], the control using the load balancer and the load distribution of the server [5][6][7], are performed at the infrastructure or server side. When the configuration change of a server is carried out, it is necessary to make a setup change at the client side. For example, the environment where student uses a notebook-sized personal computer, is assumed. When comfortable internet environment is needed for exclusive use of a classroom, it is necessary to reconnect to the PROXY Server by setting change of the Web browser. In such a case, if the system administrator is able to control the communication freely between the server and client, it is not necessary to make setup change at the client side.

In this paper, a new DACS (destination addressing control system) scheme for the university network services, is proposed. The DACS Scheme performs the network services efficiently through the communication management. As the characteristic of DACS Scheme, only the setup modification is required by the system administrator, when the configuration change is needed in the network server. Then, the setup modification is unnecessary for the customer, which shows a merit for both a system administrator and a customer. This paper proposes the design of the DACS Scheme and DACS protocol which is needed to realize DACS Scheme. The experimental evaluation is performed in the DACS Protocol for confirming the possibility of realization.
2. Synopsis of DACS Scheme

2.1. Basic Principle of DACS Scheme

Fig. 1 shows the basic principle of the network services by DACS Scheme. At the timing of the (a) or (b) as shown in the following, DACS rules (rules defined by the user unit) are distributed from DACS Server to 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 distributed DACS rules, 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 Fig. 1. In Fig. 1, 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 DACS Scheme, the operation is done by DACS Protocol as shown in Fig. 2. As shown by (1) in Fig. 2, the distribution of DACS rules is performed on communication between DACS Server and DACS Client, which is arranged at the application layer. The application of DACS rules to DACS Control is shown by (2) in Fig. 2. 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 Fig. 2.

2.2 Comparison with Existing Technology

Here, the difference between DACS Scheme and the existing technology is explained. Specifically, the difference from the technology of name resolution service (ex, WINS, DNS) and server load balancing is discussed.

First, the difference from the name resolution service is explained. Although the mapping of a host name and an IP address is performed in the existing name resolution service, the mapping of the group of a host name, a user name and an IP address can be performed altogether by DACS Scheme. As the result, the IP address to be different for every user can be determined for the same host name. Next, the difference from server load balancing technology is explained. To realize server load balancing, there are methods by DNS round robin, and by the load balancer. Then, the difference from how to use the load balancer using Destination NAT is explained. The large difference from DACS Scheme is the place which arranges Destination NAT. Although the load balancer arranges Destination NAT on the network course, it is arranged on the client in DACS Scheme. When Destination NAT is arranged on the network course, it cannot be specified whether IP Packet was sent by which user. For the reason, it is difficult to control communication per user. However, it can be guaranteed in DACS Scheme by arranging on the client that all IP Packet at the time of Destination Nat conversion is sent by the login user. But, when the client is multi-user system, the mechanism in the no login from remoteness is required. It is confirmed that the communication is sent by the user who sits down before a client and logs in directly, by the method of intercepting the unnecessary communication from the client outside.

3. DACS Protocol Phases

DACS Protocol is a communication protocol required by DACS Scheme, and can be realized by Phase1 and Phase2 which is separated in the state of DACS Client.

Phase1 Initializing process of DACS Client
Phase2 Steady state process of DACS Client

a. When DACS rules is applied to DACS Control.
When DACS Server checks whether DACS Client has started.
The possibility of realization was checked by experiment as shown in chapter 4.

3.1. DACS Protocol

3.1.1 Phase 1

The protocol of Phase1 is shown in Fig.3. (S1-S4 indicate the processing sequence by the server side, and C1-C9 indicate the processing sequence of the client side.) First, when OS starts (C1), DACS Client starts (C2). Then, DACS client is in the status of waiting for user login (C3). When user login is completed (C4), DACS Client acquires the IP address and login user name of the client (C5). Then, DACS Client transmits them to DACS Server (C6). Usually, how to set the IP address to the client has either to set up automatically using DHCP service, or other way in which the customer and the system administrator do manual setting. When a network interface starts, the IP address is set up by a method of either. Therefore, if DACS Client acquires the IP address of the client at the time of user login, there are no problems to acquire the IP address. Although it is how to acquire the IP address and login user name, in the experiment explained later, the IP address is extracted from the practice result message of a command to display network setting information. Moreover, since the user name is set to the environment variable when logged in OS, the user name is acquired through the environment variable. By DACS Scheme, since it is premised on the scheme which performs the user authentication of the client, the checks to the user name is not performed in DACS Server. Incidentally, the LDAP Server (OpenLDAP) is adopted as an authentication server in this experiment. After transmitting the user name and the IP address to DACS Server, processing is performed in DACS Server. The DACS Server registers newly or updates the IP address and DACS Client presence of the client into the status table, in which a user name is the main key (S2).

Status=0 : DACS Client stops.
Status=1 : DACS Client starts.

In the next processing, DACS rules of the login user registered into the rule table is extracted (S3), and it transmits to DACS Client (S4). Although DACS Client applies DACS rules to DACS Control (C9) after the reception (C8), it performs actually controlling the communication in DACS Control. In addition, at the time of the end of DACS Client, status is updated to 0.

3.1.2 Protocol in Phase 2-a

Next, the protocol in Phase2-a is shown in Fig.4. (S1-S5 shows the processing sequence performed in the server side, and C1-C3 shows the processing sequence in the client side.) The system administrator gives DACS Server the indication of distributing DACS rules (S1). The DACS rules are applicable to DACS Client of the client to which the specific user logs in. As the sequence, the system administrator registers new DACS rules into a rule table first. Then, the user name used as the candidate for application is given to DACS Server. DACS Server checks the IP address of the client and the startup presence or absence of the client in the status table (S2). When the status is 1, the seizing acknowledgment of DACS Client is performed. When the data in the status table shows an outage (i.e., when status is 0), the startup check of DACS Client is done (S3). When the client is in the status of seizing the presence of DACS Client, DACS rules are transmitted to DACS Client (S5). Then, DACS rules are applied to DACS Control (C3). DACS Client is in the status of awaiting after the application of DACS rules (C1).

3.1.3 Protocol in Phase 2-b

Protocol in Phase2-b is shown in Fig.5. DACS Server checks whether DACS Client has started. The timing which
Figure 5. Protocol in Phase 2-b

seizes the presence of DACS Client is as follows.
• When carrying out with the fixed interval periodically.
• When carrying out in Phase2-a before a transmission of
DACS rules.(When Status is 0 in the status table.)
DACS Client is in the status that the receiving process from
DACS Server is awaited. Therefore, when DACS Server
asks, there is a response if DACS Client has started and
an error occurs if it has stopped. When the error occurs,
status is updated from 1 to 0 in the status table. The rea-
son for checking whether DACS Client has started peri-
odically is to improve the system efficiently by the mini-
ummum startup check of DACS Client in the sequence (S3)
of Phase2-a. Here, the status description of DACS Server
and DACS Client is shown in Fig.6. The directional ar-
row of the dotted line shows the flow of the state transition
of DACS Server and DACS Client. The state changes in
order as follows; to Active (steady state) from Initializing
(initializing status), Off (idle state), and Initializing. Non-
Active (transient status) in DACS Client shows all the sta-
tuses that it is not Active, when it does not reach to a steady
state after the Off, or Initializing. When DACS Client is in
the status of Initializing, status is changed into 1 from 0.
Under a steady state (Active), status is not changed from 1
in response to the notice from DACS Client for the startup
check. However, when judged with Non-Active as a result
of the startup check of DACS Client, status is changed into
0 by DACS Server from 1. Moreover, explanation about
the directional arrow (solid line) of DACS Server (Active)
and DACS Client (Active, Off, Non-Active) is given. First,
there is a directional arrow between DACS Server (Active)
and DACS Client (Active) as follows.
• The inquiry to DACS Client from DACS Server
• The response from DACS Client to the above-mentioned
inquiry
• The transmission of DACS rules from DACS Server to
DACS Client
In the opposite arrow of a dashed line for the directional
arrows of solid line from DACS Server (Active) to DACS
Client (Off, Non-Active), it is shown that there is no re-
response from DACS Client to the inquiry from DACS Server
to DACS Client.

4. Experimental Results

In order to prove the possibility of realization of the net-
work services by DACS Scheme, the prototype was built.
Then, the functional test was actually carried out under the
operation. The prototype developed here, is shown in Fig.7.
Server Machine and Client Machine use FedoraCore3 as
the OS.DACS Server and DACS Client is implemented by
JAVA language.DACS Control uses the function of Netfil-
ter,which is equipped in Unix or Linux. As the result of
prototype construction, the function of changing a commun-
icating PROXY server by a system administrator is real-
ized as shown in Fig.7. When a PROXY Server A is set
as reference PROXY server of the Web browser on a client,
communication is done via PROXY Server B by the control
of DACS Control. The confirmation by the way of PROXY
Server B is identified in the access log of squid. The con-
firmation of no communication via PROXY Server A was
also identified in the access log of squid.
4.1. Displayed Results of Status Table

Here, the window results of the status table are shown in Fig.8. In Phase1, the user name and the IP address of the login client are first transmitted from DACS Client. The IP address and the status flag are changed into the record of each user unit beforehand registered by the system administrator (status 0 → 1). Moreover, in phase 2-a, before transmitting DACS rules to DACS Client, the startup check is carried out to DACS Client.

4.2. Displayed Results of Displayed Results of Rule Table

Next, the result of a rule table used by Phase1 and Phase2 of DACS Protocol is shown in Fig.9. In every phase, DACS rules which are registered to the user name transmitted from DACS Client are extracted. Then, they are transmitted to DACS client.

4.3. Displayed Results after Application of DACS Rules

The result after the application of DACS rules from DACS Server to DACS Client (DACS Control) by Phase1 and Phase2 is shown in Fig.10. In this prototype, the functionality of Netfilter is used for DACS Control, and the iptables command is used for the application of DACS rules. The list of the rules is presented.

5. Discussion of Effectiveness

In this chapter, a discussion is performed from the viewpoint of a customer and a system administrator about the effectiveness by DACS Scheme.
become to be an important problem, it becomes more important to protect their policies. The management by DACS Scheme developed here, can perform the system processing faithful to the policy.

6. Coexistence of Communication Control

From chapter 1 to chapter 5, 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 chapter, 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 transmitted to DACS Server from DACS Client. Then, if DACS rules corresponding to IP address, is registered into the DACS Server side, it is transmitted to DACS Client. Then, communication control for every client can be realized by applying to 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, it is necessary to give priority. It is decided according to the network policy or the security policy. The judgment is performed in the DACS Server side, and only DACS rules with the priority is transmitted to DACS Client. In the DACS Client side, DACS rules are applied to DACS Control.

7. Conclusion

As a way for making the efficiency of an operation and management for network services better, DACS Scheme is proposed here. The characteristic of the operation and management by DACS Scheme is that the centralized management by the system administrator is possible after once the customer performs the initial setups. For the reason, it is not necessary to change the setups on client. Moreover, communication server is determined, and available services can be set for every user by performing the management of a user and DACS rules. DACS Protocol required to realize DACS Scheme was described, and the prototype was actually built. Then, experimental result was shown. The study was discussed from the viewpoint of the customer and the system administrator about the effectiveness of the operation and the management of the network services. For the customer, the load intensity of a management is reduced, such as changing the setups of the client, which shows as an advantage of the proposed DACS Scheme. On the other hand, since affinity with the existing system is high, for a system administrator, utility value is high at the following points.

- The initial introduction of DACS is very easy.
- The operation and management after an initial introduction of DACS Scheme are very easy.
- After starting the operation and management by DACS Scheme, a change of servers can be made freely and safely.
- There is an effect which reduces customer supports.

A construction of the whole system for the real operation, and implementation, will be done as a future project.

References