

The Processing Workload Evaluation in two Network Management Models of IP Networks

Kazuya Odagiri^{*1}, Giuseppe De Marco², Rihito Yaegashi^{*3}, Masaharu Tadauchi^{*2}, Naohiro Ishii^{*5}

^{*1} ^{*}Corresponding author *Advanced Institute of Industrial Technology, 1-10-40 Higashi-ooi, Shinagawa-ku, Nagoya-city, Tokyo, Japan*
odagiri@aait.ac.jp

^{*2} *Toyota Technological Institute, 2-12-1 Hisakata, Tenpaku-ku, Nagoya-city, Aichi, Japan*
tadauchi@toyota-ti.ac.jp

^{*3} *Kagawa University, Kagawa, Japan*
rihito@cc.kagawa-u.ac.jp

^{*4} *Aichi Institute of Technology, 1247 Yachigusa, Yakusa-cho, Toyota-city, Aichi, Japan*
ishii@aitech.ac.jp

doi: 10.4156/jcit.vol4.issue3.1

Abstract

As the work for managing a whole network effectively without a limited purpose, there is the work of PBNM (Policy-based network management). PBNM has two structural problems such as communication concentration from many clients to a communication control mechanism called PEP (Policy Enhancement Point) and the necessity of the network system updating at the time of introducing PBNM into LAN. Moreover, user support problems in campus-like computer networks such as trouble user support at updating a client's setups and coping with annoying communication cannot be improved by PBNM. To improve these problems, we show a next generation PBNM called it DACS (Destination Addressing Control System) Scheme which overcomes these problems and has the function which does not exist in existing PBNM. However, when DACS Scheme is used in real networks, the processing load of communication control can be heavy with respect to standard mechanisms of other schemes. About this point, we show and evaluate two network management models: 1) Infrastructure-based Management (INM) model for PBNM, and 2) Client Management (CM) model for DACS Scheme. Finally, we show the fact that that CM model as DACS Scheme is an advantageous with respect to INM model at the point of processing load.

1. Introduction

In computer networks where the usage policies are well defined, the network management is relatively

easy. This is the case of enterprise computer networks, where security policies and access control lists are well defined. On the other hand, in campus-like computer networks, the management is quite complicated. Because the computer management section manages only a small portion of the wide needs of the campus network, there are some user support problems as follows. For example, when the mail boxes on one server are relocated to different server machines, an update of user machine's setups is necessary. Usual operation for a system administrator is to make them aware of the settings update. This administrative operation is executed by means of e-mail, web pages and/or posters. Since students do not check frequently them, the system administrator must support each student for their inquiries. For the system administration, individual technical support is a stiff part of the network management.

As the work of network management, there are various kinds of works such as the server load distribution technology [1] [2], VPN (Virtual Private Network) [4] [5]. However, these works are performed forward the specified different goal, and don't have the purpose of effective whole network management. As the work for managing a whole network effectively without the limited purpose, there is the works of PBNM (Policy-based network management) [6] [7] [8] [9] in IETF (Internet Engineering Task Force). However, PBNM has two structural problems such as communication concentration from many clients to a communication control mechanism called PEP (Policy Enhancement Point) and the necessity of the network updating at the time of introducing PBNM into LAN. Moreover, it is often difficult for PBNM to improve the

user support problems in campus-like computer networks explained above.

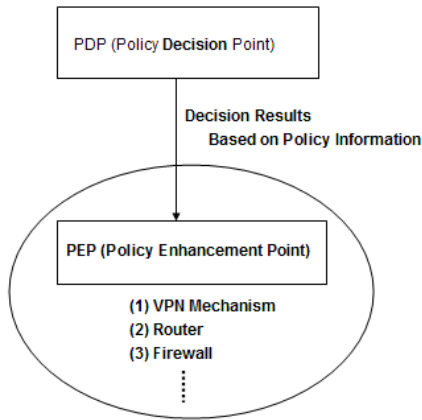


Figure 1 PBNM in IETF

To improve these problems of PBNM, we show a next generation PBNM called it DACS (Destination Addressing Control System) Scheme, which overcomes these problems and has the function which does not exist in existing PBNM. As the works of DACS Scheme, we showed the basic principle of DACS Scheme [10], the function to make communication control every user coexist with communication control every client [11] and security function [12] [13]. In addition, we showed new user support realized by use of DACS Scheme [14] [15]. The past work of DACS Scheme's mechanism was executed as a network management scheme for campus-like computer networks.

When DACS Scheme is used in real networks, the processing load of communication control can be heavy with respect to the standard mechanism of existing scheme. About this point, we show and evaluate two network management models: 1) Infrastructure-based Management (INM) model such as PBNM, where the control of the network is performed by means of mechanisms deployed along the path from clients to servers and 2) Client Management (CM) model such as DACS Scheme, where the management is performed by means of special services located into the client machines. Finally, we show the fact that DACS as CM model is advantageous with respect to INM model [16].

2. Motivation and Related Works

As the works on existing network management, there are various works such as authentication [17] [18] the server load distribution technology [1] [2] [3], VPN [4] [5] and quarantine network [19] [20]. However, these works are performed forward the specified different goal. Realization of effective management for a whole network is not a purpose. These works are performed for the specific purpose, and don't have the purpose of managing a whole network. As the work for managing a whole network effectively without the limited purpose, there is the work of PBNM [6] [7] [8] [9] in IETF. The content of PBNM is described in Figure 1.

Specifically, 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 PEP which is the mechanism such as VPN mechanism, router and firewall located on the network path among hosts such as servers and clients. Based on that judgment, the control is added to the communication that is going to pass by. As problems of this method, three points are presented as follows.

(1) Communications sent from many clients are controlled by the PEP located on the network path. Processing load for that controlling 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) There are some user support problems in network management which is not solved by PBNM.

(Problem 1) Trouble user support at the time of updating a client's setups

When some mail boxes on one server machine are expected to be relocated into separate server machines, some users has to updating a client's setups. In this case, the notice of updating the client's setups will be sent by e-mails, web pages and posters from the network administrator. The user who accepted the notice usually updates the client's setups by oneself. When it is impossible to update it, the user inquires to the network management section. The network administrator replies the inquiry through telephone, or goes to the place which the client exists and updates the client's setups. For the network administrator, such user supports are very heavy workload.

(Problem 2) Coping with annoying communication

Under the management by DHCP service, much time and effort are spent to specify which client or user is transmitting annoying communication. As an example of annoying communication, the communication which is sent from the client infected by computer virus is considered. In this case, the source IP address of annoying communication is specified first. Next, the client having that IP address is found out by a user or a network administrator as the client infected by computer viruses, and the user who used that client is specified. The main point is shown as follows. When an IP address is dynamically managed by using DHCP service, the IP address of the client may be updated according to the lease period of an IP address and the usage situation of the client (the period to next usage). Therefore, the IP address of the client is not necessarily grasped. As the result, after the source IP address of annoying communication is specified by the network management section, the client having that IP address must be specified among many clients by the user or network administrator. As another example, the communication problem by using UDP (User Datagram Protocol) such as streaming of the moving picture and the sound which will cause the congestion of the network [21] is described. The congestion of the network becomes the cause of holding down the TCP (Transmission Control Protocol) communication. To cope with this problem, it is necessary to specify the user who is using the client at that time. About this point, it cannot be specified easily in the conventional network scheme. There is no guarantee that the user can certainly be specified.

To improve these problems of PBNM, we show a next generation PBNM called it DACS (Destination Addressing Control System) Scheme, which overcomes these problems and has the function which does not exist in existing PBNM. As the works of DACS Scheme, we showed the basic principle of DACS Scheme [10], the function to make communication control every user coexist with communication control every client [11] and security function [12] [13]. In addition, we showed new user support realized by use of DACS Scheme [14] [15]. However, because these are theoretical works, the work needed to apply DACS Scheme to a practical network is not performed. When DACS Scheme is used in real networks, the processing load of communication control can be heavy with respect to the standard mechanism of PBNM as an existing scheme. About this point, we need to show the fact that DACS Scheme is advantageous with respect to an existing scheme at the point of processing load.

The rest of paper is organized as follows. In section 3 and section 4, we describe the basic mechanism of the DACS Scheme and the security function as

extended function of DACS Scheme. In section 5, we show the concrete effectiveness of DACS Scheme. In section 6, we propose two simple network models: 1) Infrastructure-based Management model (INM) for PBNM of existing scheme, where the control of the network is performed by means of mechanisms deployed along the path from clients to servers and 2) Client Management model (CM) for DACS Scheme, where the management is performed by means of special services located into the client machines. Then, we show the fact that CM model as DACS Scheme is advantageous with respect to INM model [16].

3. Basic Mechanism of DACS Scheme

3.1. Basic Principle of DACS Scheme

Figure 2 shows the basic principle of the network services by DACS Scheme. At the time 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.
- (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 authorized user.

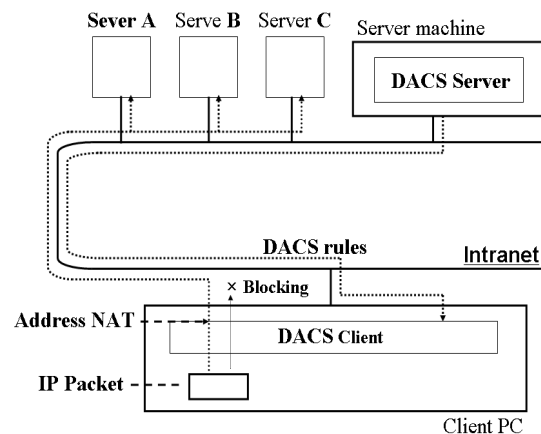


Figure 2 Basic Principle of DACS Scheme

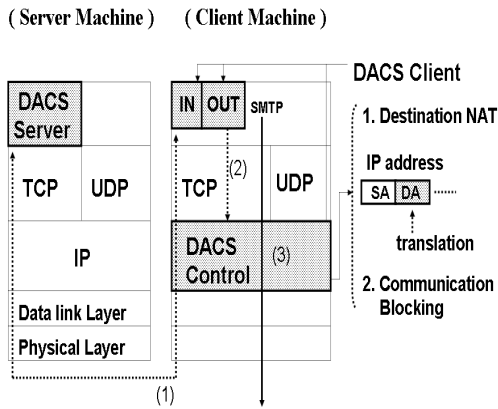


Figure 3 Layer Set of DACS Scheme

(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. The system administrator can distribute a communication of authorized user to the specified server among servers A, B or C. For example, when the system administrator wants to forbid a 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 Figure 3. As shown by (1) in Figure 3, the distribution of DACS rules are 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 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.

To change destination information on IP Packet and block IP Packet by destination information, the system administrator needs to know the IP address of a network server. For that reason, the intranet under management of the system administrator becomes the scope of DACS Scheme mainly.

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 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, 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 DACS rules are created (3). DACS rules are transmitted to DACS Client. In the

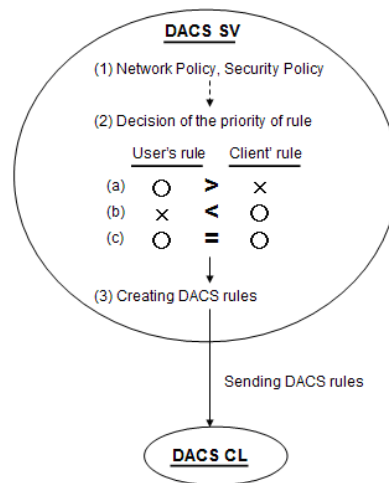


Figure 4 Creating DACS rules in the DACS Server side

DACS Client side, DACS rules are applied to DACS Control. The difference between the user's rule and the client's rule is not distinguished.

3.3. Network Service Corresponding to DACS Scheme

In this section, network service's corresponding to DACS Scheme is explained. In existing DACS Scheme, information for communication control by a user unit and by a client unit has been maintained as DACS rules on the DACS Server. By applying that information for communication control to DACS Client (DACS Control) located on a client, communication from the client is controlled. As the result, the specific mechanism is not needed on the network server. However, on the network introducing DACS Scheme, if a correspondence list of a client's IP address and user name logging in that client is passed to the network server, it becomes possible to identify which user is sending the communication from a client. As the result, it becomes possible for a program on the network server to perform different processing for every each user. Concrete example is the Web Service's correspondence to DACS Scheme.

4. Effectiveness of DACS Scheme

4.1. Improvement of Structural Problems in PBNM

Here, the improvement results of the two structural problems shown as (1) and (2) in section 2 are explained. In the DACS Scheme, PEP as communication control mechanism is located on the client. Because communication control is performed on the client, the communications sent from many clients don't concentrate on the PEP. The problem in (1) of section 2 is improved. Then, when DACS Scheme is applied to LAN, only two points are necessary as follows.

(Point 1) DACS Server is built and connected to LAN.

(Point 2) DACS Client as PEP is installed to each client.

Therefore, existing network system is not updated except these. The problem in (2) of section 2 is improved.

4.2. Improvement of Structural Problems in PBNM

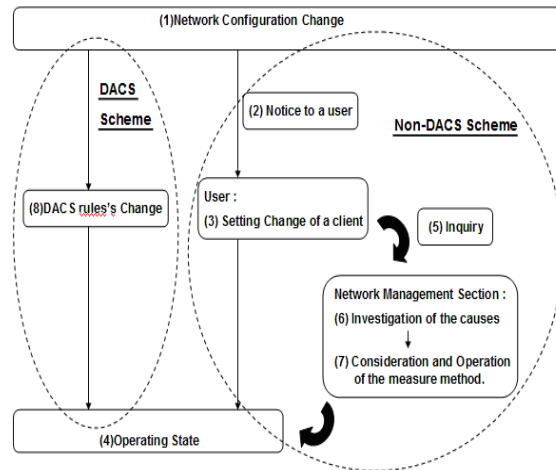


Figure 5 Process introducing DACS Scheme

In this section, the improvement results of the user support problem as shown as (3) in section 2 are explained.

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

When a network system is updated, user support by DACS Scheme is compared with user support by Non-DACS Scheme, and an advantage of user support by DACS Scheme is described. User support processes after updating the network system are described in Figure 5.

When 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 DACS Scheme is introduced, a system administrator has only to change DACS rules (8) at the time of updating the network system. After changing 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 DACS rules, a trouble by a cause except an artificial factor such as missing setups of DACS rules does not occur. This process of user support is largely simplified in comparison with the process of user support by Non-DACS Scheme.

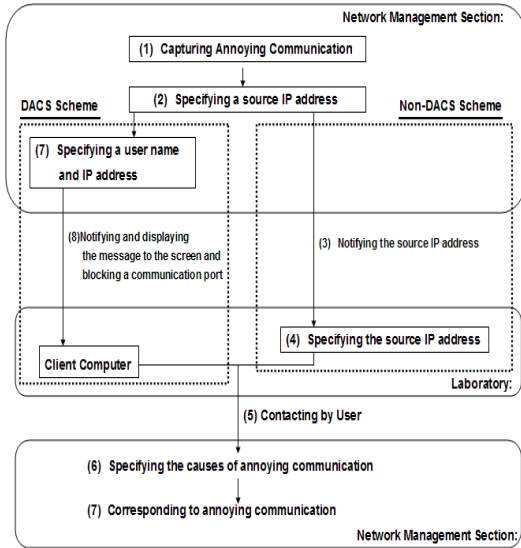


Figure 6 Change of User Support

(b) Effective Coping with Annoying Communication by 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, 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 6 and explained with an example of the user support for a laboratory. A characteristic of this mechanism is the next two processing on Web Server.

(x) User authentication is performed by user information.

(y) Information related to user is searched and extracted from data which is accumulated beforehand.

Processing of (x) is performed after processing of (5) in Figure 6. This processing is necessary to perform processing of (y) and becomes essential so that Web

Service premises anonymous user. Web page as Personal Portal is generated by the program such as CGI on the Web Server. Because the program is introduced by system administrator and can't usually be changed by a user, the Personal Portal can't always be easy to use for each user or customize for personal use. In this paper, to overcome this problem, two kinds of functions of Web Service based on DACS Scheme, which make each user creates Personal Portal freely and easily, were developed. By using these functions, when each different user inputs same URL on Web Browser, the different information for each user is searched and extracted from database or document medium, and displayed on Web Browser. However, in these functions, it is possible only to send and accept information by a user unit. Because it is necessary to send and accept information by a group unit and by all users unit, these functions are insufficient. In addition, these two kinds of functions are independent with each other. So, to use in actual network, these two kinds of functions need to be integrated as one service, and integrated interface needs to be brought to each user. Therefore, after extending these two kinds of functions of Web Service to send and accept information not only by a user unit, but also by a group unit and by all users unit, DACS Web Service, is proposed, which is realized as the result of having integrated these extended two kinds of functions of Web Service.

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 DACS Scheme is

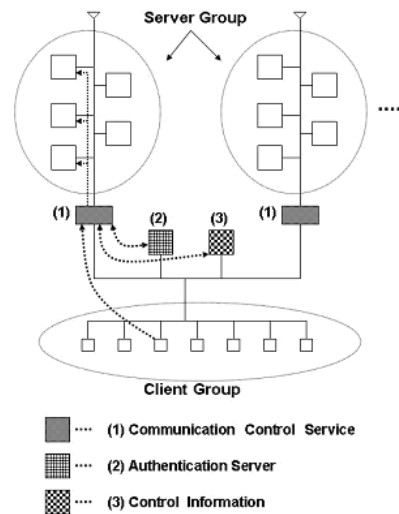


Figure 7 Infrastructure Management type model

introduced or not introduced. When DACS Scheme is not introduced, the process of user support is described in the following. Under using DHCP Service, if a whole network 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 can not 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 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 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, DACS Scheme is particularly effective.

5. Comparison of CM and INM models

5.1. Two models for Communication Control

The INM as PBNM model is shown in Figure 7. Servers group and clients group are in separate networks, interconnected through the Communication Control Service (CCS) which is the part of the network infrastructure. In this model, the communications sent from clients are controlled by the CCS. Usually, there is a Control Information Management Server (CIMS), where the management of information and access control rules is stored in the so called Control Information (CI) database. From the point of view of the processing workload, the bottleneck is the CCS, which increases with the number of clients/users. This is not an unrealistic assumption, because, generally, the communication rate among clients and servers is high.

The alternate model is the CM model as DACS Scheme. This model is shown in Figure 8. The CCS and the CI are now distributed within the client machines. After a user logging into a particular client machine, the CI set for that user and that client is extracted from the CIM. The extracted CI is applied to the CCS located onto the client machine, and the control of the communication is performed by the CCS. Compared to the INM model, the CM model differs because a small amount of the CI is distributed into the client machines. In both models, the CI is centrally managed by the CIMS. We see that this little share of

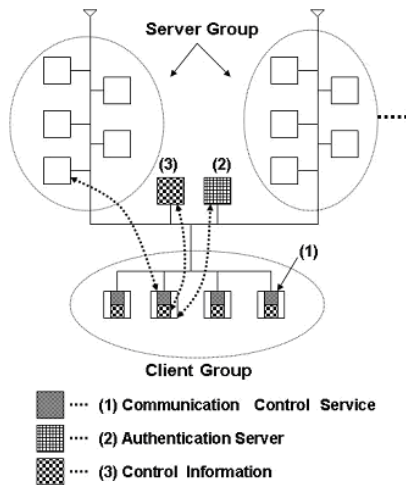
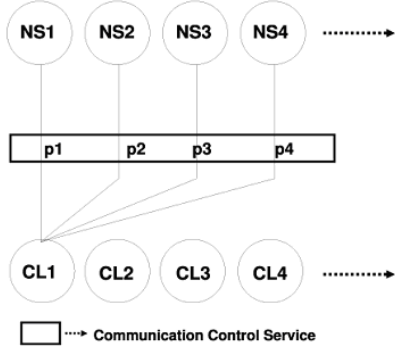


Figure 8 Client Management type model

information among client machines helps reducing the total workload sustained by the CCS.



5.2. Analysis of INM and CM Models

In this section, processing workload with respect to the communication control model is analyzed. When the communication between the client software and the network service in these two models takes place, the processing workload can be divided as follows.

- (1) Processing by the network service of the requests from client machines.
- (2) Processing by the client machine of communication controls.
- (3) Other processing on the client machines.

The processing in (1) and (3) are the same for both models. Therefore, we should only compare the processing in (2) in the INM model and the CM model, respectively. For instance, the processing workload of the communication control at 1) the CCS and at 2) the client machine.

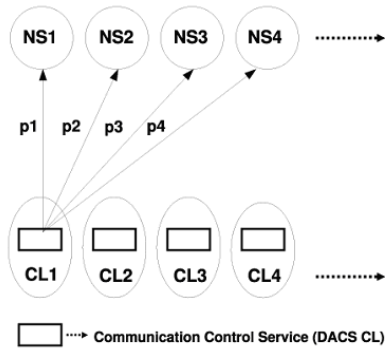


Figure 10 Processing load in CM model

For the analysis, the INM and the CM model are drawn as shown in Figure 9 and Figure 10, respectively. In both figures, network configuration is the same, except the place of the CCS. Moreover, each network service is referred to as NS1, NS2, ..., NS N , where N is the total number of network services. Similarly, CL1, CL2, ..., CL M represent the clients, where M is the total number of clients. The processing workloads due to communication between the network services and the clients are represented by p_1, p_2, \dots, p_N . Other processing workload are kept unchanged, e.g. those of the clients and those of the network services. Then, processing performance of each server where each network service is located on, is the same, and processing performance of each client is also the same. Hereinafter, we assume that the processing capabilities are the same for every client. Thus, the analysis will focus on a generic client, only. Under these assumptions, it is straightforward to show that the processing load of the INM model is:

$$WINM = M \sum_{k=1}^N Pk \quad (x)$$

where WINM is the workload.

For the CM model, the processing load occurring in the CCS is now:

$$WCM = \sum_{k=1}^N Pk \quad (y)$$

The equation in (y) means that the workload is independent of the number of client machines, which is in accord with the CM model. It is clear that the workloads are upper bounded by physical constraints of the hardware of client and server machines. We refer to these upper bounds as UINM and UCM, respectively. Usually, since server machines are more powerful than client machines, $UINM = kUCM$; $k > 1$. Then, the processing rates can be defined as:

$$PINM = \frac{WINM}{100UINM} \% = \frac{MWCM}{100kUCM} \% ; \text{ INM model, } (z)$$

$$PCM = \frac{WCM}{100UCM} \% ; \text{ CM model.}$$

Equation in (x) is a linear function of the number of clients. That is, given N , i.e. the number of network services requested by clients, WINM increases with M . This is shown also by the line (A) in Figure 11. Obviously, the processing rate of the CM model is

independent of M , as shown also in the line (B) of Figure 11.

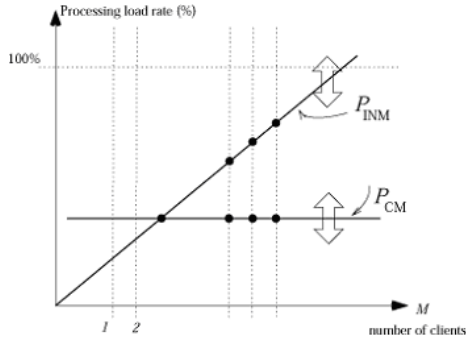


Figure 11 Comparison in both models

As final test, we also analyzed the impact of processing load due to the DACS software. In fact, actually we have

$$WCM = \sum_{k=1}^N Pk + \gamma$$

where γ is due to the processing workload of point 3. That is, the client machine must sustain the additional workload of the DACS software. It is clear that if the client machine is used without DACS, the declined line does not move and we conclude that CM model is always better than INM model. However, γ could be as high as to shift up the declined line. In our experiments, carried out on a campus LAN, we verified that always $P_{INM} > P_{CM}$, for some M , MC , where MC is the cross point of two lines in Figure 11. From these preliminary experiments, we are confident that DACS can assure a lower processing workload with respect to other INM-like model.

6. Conclusion

In this paper, we illustrated a new proposal for network management, where the control is distributed within the client machine pool. So far, the work of DACS Scheme was mainly about its functionalities, and the evaluation of applying DACS to real networks was not investigated. A legitimate doubt against CM model like DACS Scheme was that when they are deployed, the processing workload could augment. In that direction, we presented a simple comparison of

two types of communication control that we called INM model as PBNM and CM model as DACS Scheme, respectively. The analytical evaluations of the processing workload are supported by real experiment in our computer network, and they confirm the fact that the increase of the processing workload is marginal. In particular, it is independent of the number of client machines managed. Future investigations concern the implementation of a more complete system and its evaluation in more real use cases.

7. 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] S.Jha, M.Hassan, "Java implementation of policy-based bandwidth management," Int. J. Network management, John Wiley&Sons, Vol.13, issue.4, pp.249-258, July, 2003.
- [7] G.M.Prerez, F.G.Skarmeta, S.Zeber, T.Symchych, "Dynamic Policy-Based Network Management for a Secure Coalition Environment," IEEE Communications Magazine, Vol.44, issue.11, pp.58-64, November, 2006.
- [8] D.C.Verma, "Simplifying Network Administration Using Policy-Based Management," IEEE Network, Vol.16, issue.2, pp.20-26, March-April, 2002.
- [9] M.Sugano, S.Tanaka, Y.Sakata, K.Oguma, N.Shiratori, "Application and Implementation of Policy Control Method "PolicyComputing" in Computer Networks," IPSJ Journal, Vol.42, No.2, 2001.
- [10] 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, 2006a.
- [11] K.Odagiri , R.Yaegashi , M.Tadauchi , N.Ishii, " Efficient Network Management System with DACS Scheme" , Proc. of Int. Conf. on Networking and Services, Silicon Valley, USA, IEEE Computer Society, July, 2006b.
- [12] K.Odagiri , R.Yaegashi , M.Tadauchi , N.Ishii, " Secure DACS Scheme," Journal of Network and Computer Applications, Elsevier. Vol.31, Issue 4, pp.851-861, November, 2008a (in printing)

The Processing Workload Evaluation in two Network Management Models of IP Networks
Kazuya Odagiri, Giuseppe De Marc, Rihito Yaegashi, Masaharu Tadauchi, Naohiro Ishii

- [13] K.Odagiri , R.Yaegashi , M.Tadauchi , N.Ishii, "Extended DACS Scheme implementing Security Function," Proc. of Int. Conf. on Networking and Services, Athens, Greece, IEEE Computer Society, June, 2007a.
- [14] 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, Vol.4, Issue 3, pp.138-146, August, 2007b.
- [15] K.Odagiri , R.Yaegashi , M.Tadauchi , N.Ishii, "Simplified Network Management with DACS Scheme," Proc. of Int. Conf. on Networking and Services, Athens, Greece, IEEE Computer Society, June, 2007c.
- [16] K. Odagiri, G. D. Marco, N. Tanoue, R. Yaegashi, M. Tadauchi, N. Ishii, "Evaluation of the Processing Workload for two Models of Communication Control in IP Networks," The IEEE 22nd Int. Conf. on Advanced Information Networking and Applications, Okinawa, Japan, IEEE Computer Society, pp.348-354, March, 2008b.
- [17] 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.
- [18] 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.
- [19] <http://www.nec.co.jp/univerge/solution/pack/quarantine/>
- [20] <http://www.ntteast.co.jp/business/solution/security/quarantine/index.html>
- [21] 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.

Authors' bio.

Kazuya Odagiri

received the degree of B.S in 1998 from Waseda University. He is assistant professor in Advanced Institute of Industrial Technology in Japan. He got his Ph.D. in engineering from Aichi Institute of Technology of Technology in March 2008. He engages in a study of network management.

Rihito Yaegashi

received the degree of B.S in 1999 and The degree of M.S in 2001 from Shibaura Institute of Technology, Tokyo. He is assistant professor in Kagawa University. He is a member of Information Processing Society of Japan (IPSJ), The Institute of Electronics Information and Communication Engineering (IEICE), and The Society of Project

Management. He got his Ph.D. in engineering from Shibaura Institute of Technology in March 2005.

Masaharu Tadauchi

received the B.E., M.E. and Dr.-eng degree from Waseda University, Japan in 1968, 1970 and 1990, respectively. He joined Hitachi Research Laboratory of Hitachi, Ltd. in 1970. He was a professor in Information Science Laboratory of Toyota Technological Institute since 2003.

Naohiro Ishii

received the B.E., M.E. and Dr. of Engineering degree from Tohoku University, Japan in 1963, 1965 and 1968, respectively. He was a professor in Department of Intelligence and Computer Science at Nagoya Institute of Technology. From 2003, he is a professor in Department of Information Science at Aichi Institute of Technology. His research interest includes computer engineering, artificial intelligence, and human interface.