Implementation of IPv6 Functions for a Network User Authentication System Opengate

Makoto Otani
Saga University
1 Honjo-cho, Saga-city,
Saga, Japan
+81-952-28-8593
otani@cc.saga-u.ac.jp

Katsuhiko Eguchi
Saga University
1 Honjo-cho, Saga-city,
Saga, Japan
+81-952-28-8563
eguchi@ai.is.saga-u.ac.jp

Hirofumi Eto
Saga University
1 Honjo-cho, Saga-city,
Saga, Japan
+81-952-28-8594
etoh@cc.saga-u.ac.jp

Kenzi Watanabe
Saga University
1 Honjo-cho, Saga-city,
Saga, Japan
+81-952-28-8828
watanabe@is.saga-u.ac.jp

Shin-ichi Tadaki
Saga University
1 Honjo-cho, Saga-city,
Saga, Japan
+81-952-28-8505
tadaki@cc.saga-u.ac.jp

Yoshiaki Watanabe
Saga University
1 Honjo-cho, Saga-city,
Saga, Japan
+81-952-28-8564
watanaby@is.saga-u.ac.jp

ABSTRACT
In Japan, many research networks are implemented with Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6) dual stacks, and some ISPs are beginning to provide IPv6 services. Popular operating systems such as Windows XP, Mac OS X and Linux also support IPv6. Therefore, the user will use IPv6 transparently in the near future. From this background, it is important to implement a network user authentication system that can control both communications of IPv4 and IPv6, simultaneously.

At Saga University we have been developing and using a network user authentication system called "Opengate" This system has functions for user authentication and access control according to the authentication and logging of their usage. The Opengate has a simple user interface via a Web browser. The system authenticates users by authentication mechanism such as POP3, POP3S, FTP, RADIUS, and PAM. After authentication, the system allows the user access to the network and places a Java Applet into the user's Web browser. The applet establishes a TCP connection to the Opengate server. When the connection closes, the server detects the end of network usage and closes the network.

We implement functions for IPv6 into the Opengate without changing characteristic features of the system. This paper describes the implementation of the Opengate and its IPv6 extension.

Categories and Subject Descriptors
C.2.3 [**Network Operations**]: Network management

General Terms: Network management

SIGUCCS'05, November 6–9, 2005, Monterey, California, USA.

Keywords
Opengate, IPv6, Internet, Network user authentication system

1. INTRODUCTION
Dual stacks of IPv4 and IPv6 have been serviced in many Japanese research networks. Some ISPs are beginning to provide IPv6 services. IPv6 functions are supported in various types of popular operating systems such as Windows XP, Mac OS X and Linux. With those operating systems and network environments, users will use IPv6 transparently.

To use the network effectively, wireless access points, network sockets and terminals for public use are implemented in organizations. However, there is a possibility that this publicly used network suffers network incidents such as computer cracking and copyright infringement. To identify the user at these incidents, some authentication and logging systems are required.

We have been developing a network user authentication system using Opengate. The system has been used on the campus network of Saga University for more than 4 years [2]. It has functions for user authentication, access control according to the authentication and logging of their usage. Via Web browsers, the Opengate system authenticates users by such authentication mechanism as POP3, POP3S, FTP, RADIUS, and PAM. After authentication, the system opens its firewall to allow user's terminal passing through the firewall.

We implement functions for IPv6 into the Opengate without changing characteristic features of the system [1]. This paper describes the implementation of the Opengate and its IPv6 extension.

2. OPENGATE

2.1 Outline
The Opengate is a user authentication and logging system applied to the network environment where many and unspecified users connect various terminals. It has been developed in Saga University and been widely used since 2001 on campus.

The system allows user terminals to connect to the Internet, without a special application forms or software setups.

The operation flow of the Opengate is shown in Figure 1. The flow is explained in the following subsections.

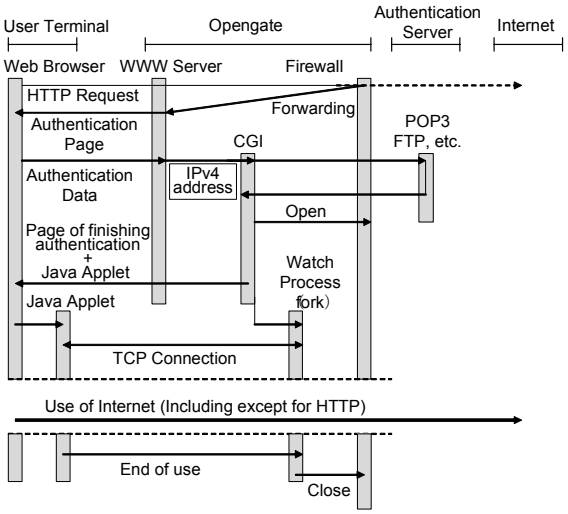

Figure 1. Operation Flow of the Opengate

2.2 System Requirements

The Opengate is developed on FreeBSD. Its firewall function ipfw was used for controlling communications and Apache was used as a Web server. A CGI program is coded with C language. The Opengate servers can use DHCP and NAT as well depending on network composition. Java Applet is desirable to operate on the Web browser of a user terminal.

2.3 Authentication

To connect to the Internet through the Opengate service, a user needs to communicate to a Web servers using HTTP first. At this time, the gateway forwards the request of HTTP to the Web server of the Opengate server using the forwarding function of the firewall. An authentication page will be displayed on the user terminal by this forwarding.

The user inputs his/her user ID and the password through this authentication page. The Opengate, started as CGI, gets the user ID and the password which is authenticated by an external authentication server. The Opengate supports authentication mechanism such as POP3, POP3S, FTP, RADIUS, and PAM.

2.4 Getting the IP Address of User Terminal

The Opengate gets the (IPv4) IP address of the user terminal from the Web server through the environment variable (REMOTE_ADDR), and opens and closes the communication path using the terminal's IP address.

2.5 Watching A User Terminal

The completion page of authentication is displayed on the user terminal after authentication, and a Java Applet is downloaded to the user terminal. This Java Applet establishes a TCP connection to the watch process forked from the CGIs. When the TCP connection is lost or when the Java Applet does not answer a response message from the watch process, the system judges the termination of use and the communication path is closed. If the Java Applet does not connect to the watch process, the communication path is closed after the predefined time is passed. The communication path is also closed if the MAC address is changed, or no communication packets are found.

2.6 Watching Communication State

After opening the gateway, the user terminal will continue to communicate to the Internet. The Opengate system observed the packets to/from the terminal passing the gateway. If no packet is observed for a long time, the system judges the termination of usage.

2.7 Logging User Information

The Opengate records the user's information using a SYSLOG function. The stored Information is the ID, terminal IP address, MAC address, start time and end time of the user.

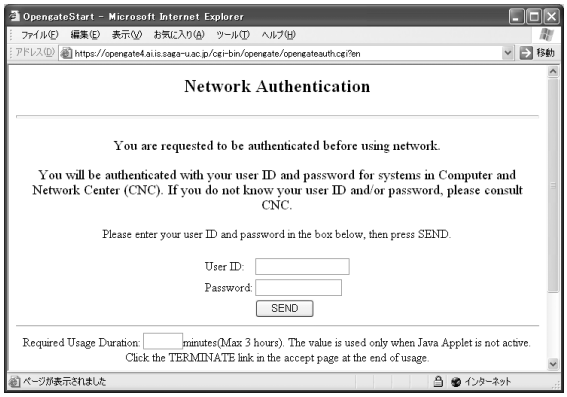

Figure 2. Authentication interface

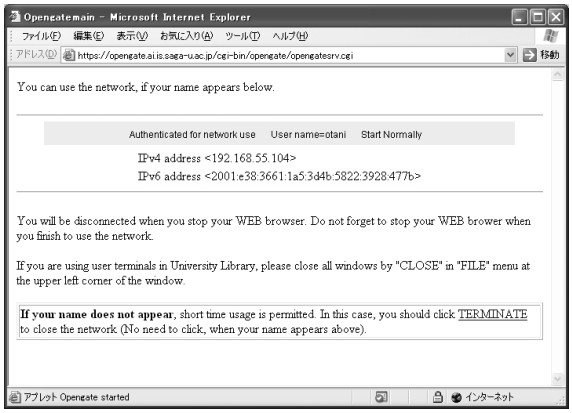

Figure 3. The page after authentication

3. IMPLEMENTATION OF IPv6 OPENGATE

3.1 System Requirements

The Opengate system supporting IPv6 (*IPv6 Opengate* in short) is also developed on FreeBSD as the (IPv4) Opengate. The IPv6 Opengate needs to control the communication paths of both IPv4 and IPv6. Therefore, it is designed to use ipfw for IPv4 communication as in the IPv4 Opengate, and ip6fw for IPv6 communication. The system uses DHCP for assignment of IPv4

addresses. A router advertisement daemon (rtadvd) is used for assignment of the IPv6 addresses.

In addition, as needed to get the IPv6 address of a user terminal from the Web server on the IPv6 Opengate, the system uses Apache having IPv6 support.

The authentication interface of the IPv6 Opengate is shown in Figure 2. The page after authentication is shown in Figure 3.

3.2 Getting the IP Address of User Terminal

A user terminal supports IPv4 and IPv6 has two types of addresses. In order to get the IPv4 and IPv6 addresses of the user terminal by an environment variable (REMOTE _ADDR) in HTTP protocol, it is necessary for the terminal to communicate with the Web server through both IPv4 and IPv6 addresses, respectively. Many Web browsers (Internet explorer 6, Firefox, Opera, etc.) use IPv6 initially, and if IPv6 communication fails, those Web browsers will use IPv4 communication instead. The IPv6 Opengate gets two types of addresses based on those behaviors of Web browsers.

The IPv6 Opengate also needs two FQDNs (FQDN_4 and FQDN_64) for connecting the gateway by terminals. For example, FQDN_4 is opengate4.saga-u.ac.jp (IPv4 address: 192.168.55.1). And FQDN_64 is opengate_64.saga-u.ac.jp (IPv6 address: 2001:e38:3661:1a5::1, IPv4 address: 192.168.55.1).

3.2.1 Case of the IPv4 and IPv6 dual stacks Web server.

Here we describe the process of getting addresses of user terminals in case of Web servers with IPv4 and IPv6 addresses.

The case of the Web servers only with IPv4 will be described in 3.2.2.

(1) The Web browser transmits an IPv6 HTTP request to a Web server (IPv4 and IPv6 dual stacks Web server). Because the communication path is closed, however, the IPv6 HTTP request is timeout.

(2) Next, the Web browser transmits an IPv4 HTTP request to the same Web server. Here, this IPv4 HTTP request is forwarded to the Web server on the IPv6 Opengate (http://opengate4.saga-u.ac.jp) by a firewall forward function.

(3) By the HTML refreshing function, the Web browser requests the CGI to display the authentication page. At this time, the URL of the destination is specified by FQDN_4 (http://opengate4.saga-u.ac.jp). The IPv4 address of the user terminal can be obtained through the environment variable.

(4) The user inputs his/her user ID and the password into the authentication page. In this page, the IPv4 address of the user terminal is embedded by the CGI using the hidden tag. The embedded IPv4 address is transmitted (POST) to the IPv6 Opengate CGI together with authentication data. At this time, the URL of the IPv6 Opengate CGI is specified by FQDN_64 (http://opengate64.saga-u.ac.jp).

(5) Because the URL of the IPv6 Opengate CGI is specified by FQDN_64 (http://opengate64.saga-u.ac.jp), the Web browser communicates to the IPv6 address (2001:e38:3661:1a5::1). So, the IPv6 Opengate gets the IPv6 address of the user terminal by the environment variable (REMOTE_ADDR). As, the IPv4 address is transmitted (POST) together with authentication data, IPv4 address is obtained from this POST method by the IPv6 Opengate.

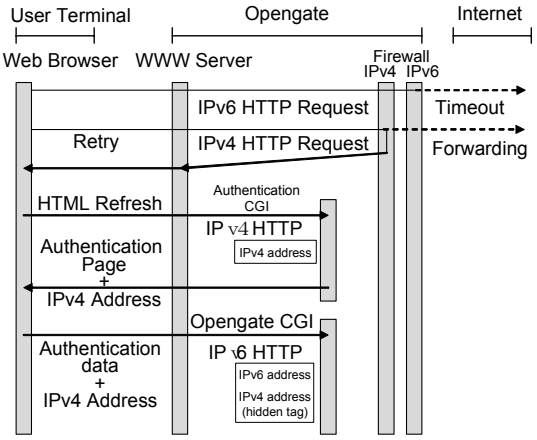

Figure 4. Getting terminal information in the IPv6 Opengate

The flow of getting the user terminal information on the IPv6 Opengate is shown in Figure 4.

By using HTML Refresh mechanism, we implement the way of getting two types of addresses, without changing the interface provided in the (IPv4) Opengate.

As described in (1), the first IPv6 HTTP request to a IPv6 Web server cannot be forwarded to the Web server of IPv6 Opengate. This is because the forwarding function is not implemented to the IPv6 firewall (ip6fw) on FreeBSD. For this reason, a user has to wait for the timeout of IPv6 HTTP request. Though the waiting time for timeout varies with Web browsers, the waiting time is only about 5 - 15 seconds.

3.2.2 Case of the IPv4 Web server

If the Web server, the terminal tries to connect first, is a IPv4 server, the IPv6 Opengate behaves as follows.

(1) The Web browser transmits an IPv4 HTTP request to a Web server. Here, this IPv4 HTTP request is forwarded to the Web server on the IPv6 Opengate (http://opengate4.saga-u.ac.jp) by the firewall.

The remaining process is the same as process of Section 3.2.1 (3)-(5). Because the first HTTP request is IPv4, The IPv6 HTTP request of Section 3.2.1 (1) is not performed.

The above descriptions are based on the assumption that, the IPv4 address must be assigned at least to FQDN of the Web server that a user terminal tries accesses first and may have the IPv6 address.

When only the IPv6 address is assigned to the Web server, the IPv6 Opengate cannot forward communication. However, because there are still few such Web servers, I think that it is not an issue.

3.3 Opening a Communication Path

After finishing authentication, the communication path for the user terminal is opened by adding rules to two firewalls (ipfw and ip6fw).

3.4 Watching a User Terminal

In order to watch the use status of the user terminal, a TCP connection is established between the watch process and the Java Applet downloaded to the user terminal. When the TCP

connections is lost, or when the Java Applet does not answer a response message from the watch process, the system judges the termination of use and the communication path is closed. This TCP communications is established only using IPv4, because some Java VM on the Web browser might not support IPv6.

3.5 Watching a Communication State

The IPv6 Opengate also observes the communication state of the terminal. The number of the packets (IPv4 and IPv6) passing the IPv6 Opengate is watched. If no packet (IPv4 or IPv6) transmitted from the user terminal is found for a long time, the system judges the termination of use and IPv4 and IPv6 communication paths are closed.

3.6 Watching Multiple IPv6 Addresses

In IPv6, a user terminal may have multiple global IPv6, such as in multi-homed environment, the case where the anonymous address is used.

In the IPv6 Opengate, communication paths are opened only for the IP addresses used for HTTP requests at the authentication. And, for the addresses which was not used at the authentication are closed.

Therefore, the NDP (Neighbor Discovery Protocol) entries are also watched for adding multiple IPv6 addresses. If a new IPv6 address of the user terminal is added into the NDP entries, the IPv6 Opengate opens the communication path for the new IPv6 address. When a IPv6 address is deleted from the NDP entries, the IPv6 Opengate closes the communication path for this IPv6 address. So, the IPv6 address that was not used at the authentication can also be used later.

3.7 Logging a User Information

The IPv6 Opengate records user information using a SYSLOG function as in the (IPv4) Opengate. If a user terminal uses IPv4 and IPv6, the IPv6 Opengate records user ID and both IPv4 and IPv6 addresses, a MAC Address, usage start time, and usage finish time. In addition, the IPv6 Opengate records IPv6 address that is not used for authentication. If the user terminal supports only IPv4, it records only IPv4 address.

3.8 About the Web Browser Using IPv4 Before IPv6

Many Web browsers use IPv6 before IPv4. The IPv6 Opengate uses this sequence for getting IPv4 and IPv6 addresses.

However, some Web browsers (safari on Mac OS X 10.3, for example) use IPv4 before IPv6. Therefore, the NDP entry is also watched for adding IPv6 addresses used after authentication.

3.9 About the Web Browser Only Using IPv4

The user terminal that uses only IPv4 may be connected to the network. In such a case, only the IPv4 address is obtained by the IPv6 Opengate. Therefore, the IPv6 Opengate controls only the communication path of IPv4.

4. DISCUSSION

4.1 Scalability

The IPv6 Opengate starts one CGI process to one user terminal as in (IPv4) Opengate. Currently, many Opengate servers have been operating in Saga University so that at most each the Opengate server can manage the 256 IPv4 addresses.

When operating the IPv6 Opengate, the dividing the network under control to a proper size might be desirable. Optimal address assignment to the user terminals with IPv4 and IPv6 dual stacks are a future task, and needs to verify the IPv6 Opengate on a larger experiment network.

4.2 Restrictions

Since the IPv6 Opengate opens first only the communication path of the address used for authentication, the communication paths of other IPv6 addresses are closed. So, The NDP entry is watched for adding other IPv6 addressed later. Delivery of NDP is restricted only in the same sub network. Therefore, in order to use the NDP protocol in the IPv6 Opengate, you must be composed such that other routers are not installed between the IPv6 Opengate and user terminals.

User terminal only using IPv6 also exists. The IPv6 Opengate always uses IPv4 for getting the address and watching the connection state. This is not the serious restriction, because almost all terminals use IPv4 protocols currently.

4.3 Application of the Proposed Technique

Various types of authentication systems for network usage have bee studies. The IPv6 Opengate controls the communication in the network layer. In many other systems for network authentication, communication paths are controlled in the date link layer or in the network layer. The system that controls communication in the data link layer does not use the IP address for control. So, such a system does not need to take IPv6 into consideration.

Those systems that controls communication in the network layer needs to consider IPv6. When supporting IPv6 in such systems, the following techniques used in our research might be effective.

- Getting the IPv4 and IPv6 addresses of user terminal
- Control of communication path
- Watching the communication state
- Support of multiple IPv6 global addresses

5. CONCLUSION

We have been developing a network user authentication system Opengate, and been using it in campus network of Saga University. This system has functions for user authentication, access control according to the authentication and logging of their usage. After the authentication, the system allows the user to use the network for communication to the Internet.

We extend the Opengate system to the IPv6 Opengate. By the IPv6 Opengate, user terminals are able to use of both IPv4 and IPv6 for connection. Moreover, user terminal can use multiple global IPv6 addresses.

Because IPv6 will be popular in the near future, this research might be useful for IPv6 support in other network authentication systems.

6. REFERENCES

[1] Katsuhiko Eguchi, Kenzi Watanabe, Implementation of IPv6 Functions for Opengate, IPSJ's SIG DSM Meeting, No.2004-DSM-36, pp.7 - 12, 2005

[2] Shin-ichi Tadaki, Hirofumi Eto, Kenzi Watanabe, Yoshiaki Watanabe, Implementation and Operation of Large Scale Network for Users' Mobile Computers by Opengate, IPSJ's SIG DSM journal, Vol.46, No.4, pp. 922-929, 2005.