Implementation and Evaluation of Authorized Access LAN Sockets Using PPPoE

Hideo Masuda, Michio Nakanishi, Masahide Nakamura, Mio Suzuki
Informedia and Education Division, Cybermedia Center, Osaka University
1-30 Machikaneyama, Toyonaka, Osaka, 560-0043 Japan.
Telephone: +81 6 6850 6076, FAX: +81 6 6850 6084,
E-mail:h-masuda@ime.cmc.osaka-u.ac.jp

Abstract

This paper presents an integrated method to achieve authorized access on LAN sockets in a campus network. The key issues of our method are user authentication and user tracking. We adopt PPPoE (Point-to-Point Protocol over Ethernet) for the user authentication, and integrate IDENT mechanism on the PPPoE server for the user tracking. We conduct performance evaluation with respect to transfer rate and CPU usage. The evaluation shows that the proposed system achieves excellent performance for its deployment cost. As a result, the proposed method could be a good candidate to add network connectivity in campus networks.

1 Introduction

Rich network environment is a key to attract prospective students to universities[1]. Recently, universities tend to provide students with *LAN sockets* in every classroom, for fast and easy access to network resources. From the viewpoint of network administrators, however, it would become an insecure hot bed of network crimes, unless users are properly authenticated.

To cope with the problem, there are some experimental systems, which implement user authentication on LAN sockets (e.g. [2] [3]). In [2], PPTP (Point-to-Point Tunneling Protocol [5]) is used for a secure LAN sockets. In [3], IP over SSL (Secure Socket Layer [6]) is used. Since both approaches are IP over IP fashion, they would suffer from heavy protocol overhead.

In this paper, we have implemented and evaluated a new system to achieve authorized access in an inexpensive manner, specifically, *LAN sockets using PPPoE* (Point-to-Point Protocol over Ethernet [7]). The key features of the proposed system are *user authentication* with the PPPoE and *user tracking* with IDENT[11]. The proposed system can be implemented with inexpensive HUBs and a mid-class PC.

We have conducted an experimental evaluation for the proposed system from viewpoints of transfer rate and CPU usage. The evaluation shows that the proposed system achieves excellent performance for its deployment cost. The system is actually working in the educational computer system in Cybermedia Center, Osaka University, also working in a wireless LAN environment with IEEE802.11b.

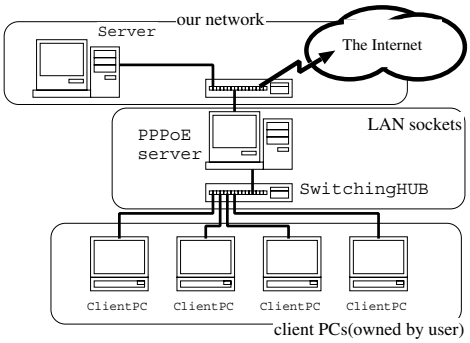

Figure 1. Experimental environment

2 Implementing LAN sockets with PPPoE

Figure 1 shows an experimental environment of our system. The key issues for implementation of the target LAN sockets are (1) how to choose implementation variants of the PPPoE, and (2) how to integrate the IDENT mechanism on the PPPoE.

2.1 Choosing implementation variants of PPPoE

There are two alternatives of the PPPoE server.

1. implementation with userland (called *user mode*)
2. implementation with OS kernel (called *kernel mode*)

The user mode is easy to be deployed. However, the user mode suffers from frequent context switching between kernel space and user space. Although the kernel mode requires kernel reconfiguration, good performance is expected. In this work, we have chosen both implementation variants, and conducted their comparative evaluation.

Proceedings of the 2002 Symposium on Applications and the Internet (SAINT'02)
0-7695-1447-2/02 $17.00 © 2002 IEEE

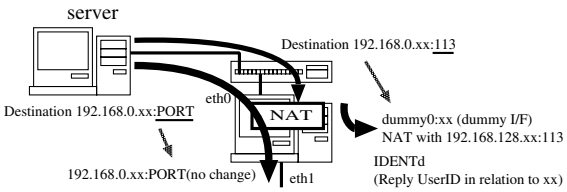

Figure 2. NAT method

2.2 Implementing new IDENT mechanism

The IDENT protocol [11] provides a means to determine the identity of a user of a particular TCP connection. When a client tries to access to a server (e.g., proxy, smtp, etc) with IDENT configuration, the server sends the client IDENT_request with a pair of local/remote port numbers. Then, the client responds user's identity (login name) to the server. However, the original IDENT protocol cannot always guarantee reliable response under the LAN socket environment in campus. Since clients connected to the socket are managed by students themselves, not all clients have the IDENT feature. Moreover, malicious configuration is possible.

Therefore, we try to implement a more reliable IDENT mechanism, by combining the original IDENT protocol with PPPoE authentication. The IDENT protocol utilizes TCP port #113 as well as the TCP network connection. Our key idea is to let the PPPoE server intercept IDENT_requests to the port #113 and respond userID with PPPoE authentication.

To achieve the mechanism, we propose and implement two new methods. The one is a method using NAT (Network Address Translation), called *NAT method*. The other is with IP Masquerade, called *Masq method*.

1. NAT method
   Figure 2 shows the outline of the NAT method. When an incoming connection request arrives at TCP #113 port on a client PC, the client performs NAT (Network Address Translation), and accepts the connection as if it were a connection to a virtual interface (denoted by dummy I/F in the figure) on the PPPoE server prepared for each PC client. In the virtual interface, we bind a program (call it *program A*, denoted by IDENTd in the figure) to respond the IDENT protocol on the TCP #113 port. The program A responds userID with PPPoE authentication for any pair of port numbers.

2. Masq method
   Figure 3 describes the Masq method. By applying IP masquerade technique to the outgoing connection from the client PC, we force the source address of the connection to be the IP address of the PPPoE server. If an incoming IDENT connection arrives at the TCP #113 port on the client PC, a program (call it *program B*, denoted by IDENTd in the figure) on PPPoE server responds the IDENT protocol, since the IP masquerade is used. The program B first identifies which client PC has requested the connection with the pair of port numbers, by looking up the IP masquerade information. Then, the program B responds userID that was used for PPPoE authentication in the identified client PC.

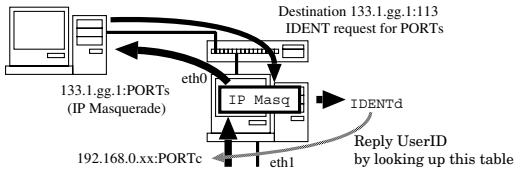

Figure 3. Masq method

3 Experimental Evaluation

We choose the following points as metrics of the performance evaluation.

1. Data transfer rate of the PPPoE server
2. CPU usage of the PPPoE server

As shown in Table 1, we have prepared 3 different PCs for the PPPoE server, 4 different PCs for clients. An ftp server is used for measuring network performance. For the PPPoE server, we have measured the performance of user mode, kernel mode and router mode (without PPPoE). We have also added the proposed IDENT mechanisms to the kernel mode and evaluated their performance.

As for clients, we have measured performance effect when multiple clients are connected, specifically in the following ways: (a) Client A only, (b) Clients A and B, (c) Clients A,B and C, (d) all of Clients A, B, C and D. To simulate network load, we have prepared a large file (size of 10MByte) on the ftp server, and performed file transfer with ftp from the ftp server to the clients.

3.1 Data Transfer Rate

First, we have measured the data transfer rate in the following way.

1. On each client PC, repeat the ftp five times.
2. Under the traffic, obtain the followings values on the PPPoE server at time n, with sleep 1 interleaving: accumulated data size exchanged ($adsx_n$), accumulated CPU time ($acpu_n$).

Proceedings of the 2002 Symposium on Applications and the Internet (SAINT'02)
0-7695-1447-2/02 $17.00 © 2002 IEEE

Table 1. Specification of PCs

	ftp server	ServerA	ServerB	ServerC	ClientA	ClientB	ClientC	ClientD
CPU	PentiumII 450MHz	PentiumIII 1GHz	PentiumIII 550MHz	Pentium 233MHz	Celeron 633MHz	Celeron 633MHz	Celeron 300MHz	Pentium 266MHz
Memory	128MB	256MB	896MB	128MB	256MB	256MB	192MB	128MB
NIC	Intel i8255x	Intel i8255x			SiS 900		Intel i8255x	3CCFE575
OS	Linux$_{2.4.2ac13}$	Linux2.4.2ac22+ kernelized pppoed[9] Linux2.4.2ac22+ rp-pppoe[8]			Linux$_{2.4.2ac22}$ (kernel)[9]	Win2k Pro RASPPPOE 0.95b[10]	Win98	Win98

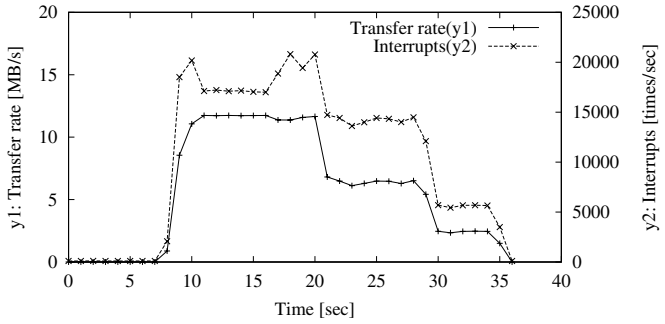

Figure 4. Data transfer rate of Server A

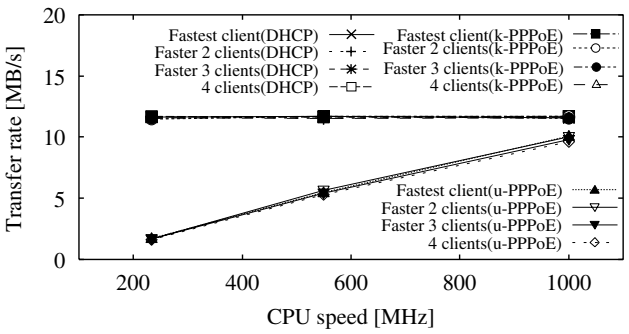

Figure 5. Maximum transfer rate

3. Compute the data transfer rate at time n (DTR_n) as follows: $DTR_n = \frac{adsx_n - adsx_{n-1}}{acpu_n - acpu_{n-1}}$

Figure 4 shows the transfer rate and the number of interruptions w.r.t. server A, without IDENT (4 clients). It can be seen that four client PCs simultaneously started the data transfer around 10 seconds. Then, the fastest PC (Client A) finished the transfer around 15 seconds, followed by other PCs (20, 27, 34 seconds). Although Figure 4 is the result of the server A, similar results are observed for other servers.

From the result, we set a threshold for the maximum transfer rate to be 90% of the measured maximum value. Then, we determine the *maximum transfer rate* of the PPPoE server as an average of values greater than the threshold. Also, we call a time interval in which the transfer rate is greater than the threshold *maximum load interval*.

Figure 5 shows the maximum transfer rates of three servers in Table 1. The maximum transfer rates of servers A, B and C were more than 11,000kByte/Sec, which implies that the servers have used up the bandwidth of 100BaseTX. The performance dropping caused by PPPoE was less than 1% for the kernel mode, which could be ignored. However, the user mode has much worse performance than the kernel mode. Even with 1GHz Pentium III machine, the user mode achieves only 80% of the normal routers.

Figure 6 shows the maximum transfer rates w.r.t. different IDENT mechanisms: without IDENT, NAT method and Masq method. We found that two IDENT methods have no difference w.r.t. the transfer rate.

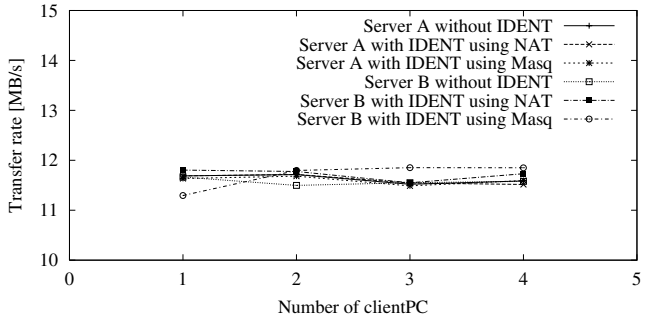

Figure 6. Maximum transfer rate with/without IDENT

3.2 CPU usage

We have calculated the CPU usage as follows:

1. On the PPPoE server, obtain the accumulated CPU time at time n (user:u_n, system:s_n, total:t_n), with sleep 1 interleaving.
2. Obtain the CPU usage at time n (CPU_n) as follows: $CPU_n = \frac{(u_n - u_{n-1}) + (s_n - s_{n-1})}{t_n - t_{n-1}}$
3. Obtain average of CPU_n's, where n is in the maximum load interval.

Figure 7 shows the CPU usage for the three servers w.r.t. the implementation variants. We can see that the CPU us-

Proceedings of the 2002 Symposium on Applications and the Internet (SAINT'02)
0-7695-1447-2/02 $17.00 © 2002 IEEE

age of the kernel mode with CPUs faster than PentiumIII 550MHz is less than 30%. This fact implies that the overhead due to PPPoE can be ignored for the kernel mode. Also, we found that even if we double the performance of CPU (e.g., 1GHz), significant improvement is not achieved. On the other hand, the user mode has exhausted the CPU power, which is almost 100%.

Figure 8 shows the CPU usage of the PPPoE w.r.t. different IDENT mechanisms. The result tells that the CPU usage of the Masq method is slightly higher than that of the NAT method, which can be explained as follows: In the Masq method, the IP masquerade has to rewrite the contents of all data packets exchanged. While, the NAT method has only to check whether the packets are sent to the TCP #113 port or not. That is, the packet rewriting is not needed.

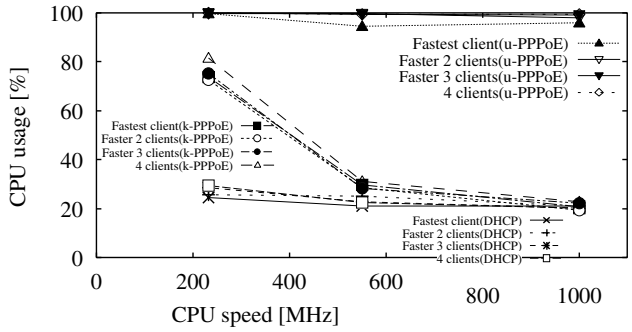

Figure 7. CPU usage

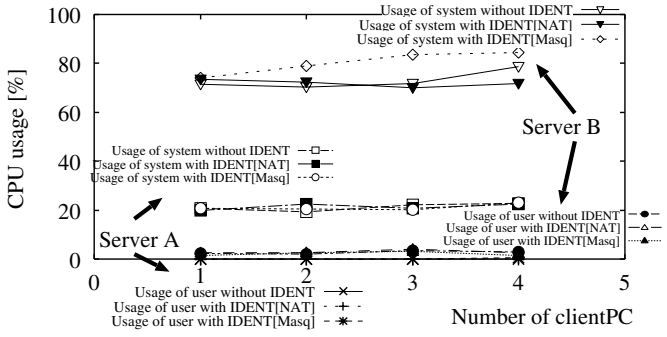

Figure 8. CPU usage with/without IDENT

4 Discussion

It can be seen, in Figures 5 and 7, that even the PPPoE server with Pentium III 550MHz has still enough room in the CPU usage, even though the server uses up the bandwidth of the 100base/TX. Also, even when the number of the client PCs is increased, the CPU usage of the server does not glow dramatically. From this, we consider that the bottleneck of the proposed system is in the network itself. Our performance evaluation imposed heavy load on the network. Therefore, in ordinary circumstances, less expensive servers with around Pentium III 500MHz can sufficiently serve much more client PCs.

Adding the proposed IDENT mechanism did not cause siginificant performance dropping. Each of the NAT and Masq methods has its merits and demerits. In the NAT method, the number of IP addresses is twice as the number of client PCs. Thus, when the number of usable IP addresses is restricted, Masq method would be better than NAT method. In Masq method, applications such as NetMeeting, CU-SeeMe, (active) ftp that directly use the IP address are difficult to work on client PCs, due to the IP Masquerade. This problem does not occur in NAT method.

The following two issues are our future works: The one is to predict the performance of our architecture for much more client PCs using computer simulation. The other is to measure the performance of the system which uses Gigabit Ethernet (1 or 4 Gbps) connection to upper network from PPPoE servers.

References

[1] R. Bernstein: "America's most wired colleges 2000", `http://www.zdnet.con/yil/content/college/`.

[2] S. Shinomiya and Y. Hagiwara: "A construction of wireless access system in campus"(in Japanese), IPSJ Technical Report, 2001-DSM-21, vol.2001, No.50, pp.7-12 (May, 2001).

[3] Y. Ishibashi, N. Yamai, H. Morishita, T. Mori, K. Abe and T. Matsuura: "An authentication system for secure wireless communication"(in Japanese), IPSJ Technical Report, 2001-DSM-21, vol.2001, No.50, pp.13-18 (May, 2001).

[4] H. Masuda, M. Suzuki and M. Nakanishi: "Implementation and evaluation of secure access LAN sockets by PPPoE", (in Japanese), IPSJ Symposium on Multimedia, Distributed Cooperative and Mobile Systems, vol.2001, No.7, pp.379-384 (June, 2001).

[5] K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little, Zorn: Point-to-Point Tunneling Protocol(PPTP), RFC2637 (1999).

[6] OpenSSL Project, `http://www.openssl.org/`.

[7] L. Mamakos, K. Lidl, J. Evarts, D. Carrel, D. Simone and R. Wheeler: A Method for Transmitting PPP Over Ethernet (PPPoE), RFC2516 (1999)

[8] Roaring Penguin's PPPoE Software, `http://www.roaringpenguin.com/pppoe/`.

[9] Michal Ostrowski: PPPoE for Linux 2.3/2.4, `http://www.math.uwaterloo.ca/~mostrows/`.

[10] Robert Schlabbach: RASPPPOE; PPP over Ethernet Protocol for Windows, `http://www.user.cs.tu-berlin.de/~normanb/`.

[11] M. St. Johns: Identification Protocol (IDENT), RFC1413 (1993)

Proceedings of the 2002 Symposium on Applications and the Internet (SAINT'02)
0-7695-1447-2/02 $17.00 © 2002 IEEE