PPPoEを利用した認証付き情報コンセントの実装と評価

桝田 秀夫[1]，鈴木 未央[2]，中西 通雄[1]
h-masuda@cmc.osaka-u.ac.jp, mio@ecs.cmc.osaka-u.ac.jp, naka@cmc.osaka-u.ac.jp
[1] 大阪大学サイバーメディアセンター
[2] 大阪大学基礎工学部電子物理科学科

概要 本論文では、情報コンセントや無線LANのように、特定多数のノートパソコンを容易に接続可能なネットワークにおいて、利用者認証を行う際に、公開された通信プロトコルであるPPPoE(PPP over Ethernet)を用いる方法を提案する。PPPoE自体は特殊なハードウェアは必要とせず、WindowsやUNIXを問わず無償のクライアントプログラムも存在している。今回実現した方式では、VLAN機能のないスイッチングHUBでも、接続されたノートパソコンに対して利用者認証をおこなうことができ、さらに、IEEE802.11bなどの無線LAN環境でも用いることができる。また、利用者の登録に関しても、計算機の利用者情報(ログイン名とパスワード)のみでよく、IP addressやMAC addressの事前登録は不要であり、ノートパソコンが変わるたびに登録し直したりする必要がない。

キーワード 情報コンセント，利用者認証，PPPoE，無線LAN

Implimentation and evaluation of secure access LAN sockets using PPPoE

Hideo Masuda[1] , Mio Suzuki[2] , Michio Nakanishi[1]
h-masuda@cmc.osaka-u.ac.jp, mio@ecs.cmc.osaka-u.ac.jp, naka@cmc.osaka-u.ac.jp
[1] Cybermedia Center, Osaka University
[2] School of Engineering Science, Osaka University

Abstract In this paper, we propose a new method to achieve secure access on LAN sockets using PPPoE(Point-to-Point Protocol over Ethernet). PPPoE is a public protocol, and there are some free software for Windows and UNIX. This method requires no VLAN function in the network device, and works in wireless environment(e.g. IEEE802.11b), too. In order to authenticate users, it needs userID and password, but does not need MAC address or IP address registration. We evaluate this method by measuring the PPPoE server load and throughput.

keywords LAN sockets, user based authentication, PPPoE, wireless LAN

1. はじめに

近年、大学や図書館などにおいて、利用者自身が持ち込んだノートパソコンを直接ネットワークに接続できるように、情報コンセントや無線LANを配置することが多くなってきた。これは、利用者が自分の環境をそのまま利用することができること、また運用者側からみれば利用者用計算機端末群を維持していく必要がないという利点を持つが、逆に利用者のネットワークの使用について詳細な情報を取得することが難しくなり、不正アクセスなどの温床になりやすいという問題を持っている。情報コンセントを使用する際に、利用者認証をする為の機構がいくつか提案[1, 2]されており、いくつかは実際に運用されているが、VLANの設定が可能なスイッチン

グ HUB やノートパソコン用の専用ハードウェアが必要となる。また、MAC address をあらかじめ登録しておく方式では、登録作業に手間がかかるという問題がある。

本論文では、情報コンセントや無線 LAN のように、特定多数のノートパソコンを容易に接続可能なネットワークにおいて、利用者認証を行う際に、公開された通信プロトコルである PPPoE(PPP over Ethernet)[3] を用いる方法について、実装と評価をおこなう。PPPoE 自体は特殊なハードウェアは必要ではなく、また本方式では VLAN を必要とするような高価なスイッチング HUB を用意せずに、ノートパソコンごとに利用者認証をおこなうことができる。さらに、利用者の登録作業に関しては、システムに対する利用者アカウント (ログイン名とパスワードの組) を持っていればよく、IP address や MAC address の登録のようにノートパソコンが変わるたびに登録し直したりする必要がない。また、利用者認証には RADIUS サーバ [6, 7] を使用し、通信媒体としては、スイッチング HUB のような有線 LAN だけではなく、IEEE802.11b のような無線 LAN を用いた環境でも動作を確認した。

2. PPPoE を用いた情報コンセントの実装方式

情報コンセントにおいて、利用者が持ち込むノートパソコン (以下、クライアント PC と呼ぶ) 毎に利用者認証をおこなう場合、要求される事項は、以下のものが挙げられる。

1. 認証前には外部と通信することができない。
2. 認証後に別のクライアント PC に入れ換えた場合、通信することができない (再度認証が必要)。

PPPoE は、Ethernet のようなブロードキャスト型媒体上に、仮想的な一対一通信路を生成し、その通信路上で、PPP 接続をおこなう。PPP 接続に際してはログイン名とパスワードによる利用者認証が可能であり、ユーザ認証が完了した後に IP address などの設定がなされる。従って、認証前には通信することができず、(1) の要求事項を満たすことができる。また、仮想的な一対一通信路は、PPPoE サーバ上で、クライアント PC の MAC address と通信路 ID の組で識別されている。従って、異なる MAC address を持つ別のクライアント PC は、この通信路を横取りすることはできず、(2) の要求事項も満たすことができる。

また本手法では、PPP 接続時の利用者認証には RADIUS サーバを使用し、認証時にはより安全な CHAP 方式を用いることとした。さらに、通信媒体として、スイッチング HUB のような有線 LAN だけではなく、IEEE802.11b のような無線 LAN を用いた環境でも動作を確認した。

3. 本方式の評価

3.1 測定環境

本方式の有効性を評価する為に実験環境を構築し、PPPoE サーバの性能評価を行った。ここでは、性能評価の指標として、以下の項目を選択した。

1. 転送レート (スループット)
2. PPPoE サーバの CPU 使用量
3. PPPoE サーバのメモリ使用量

測定に用いた環境は図 1 の通りである。

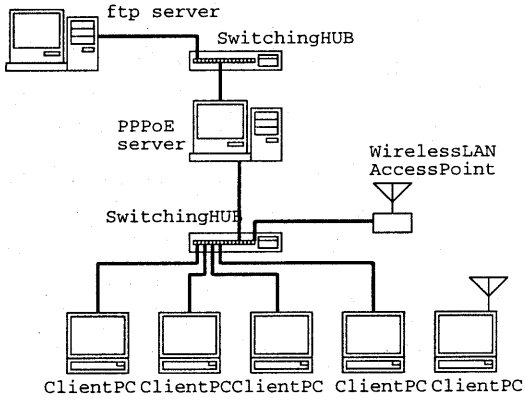

図 1: 測定環境

3.2 PPPoE の実装の選択

PPPoE サーバの実装には、大きく分けて

1. userland で実現したもの (user モード)
2. kernel で実現したもの (kernel モード)

の 2 種類が存在している。user モードの実装は、kernel に手を加えることなく通常のアプリケーションと

ftp サーバ	PentiumII 450MHz, 128MB, Intel EtherExpress Pro/100, Linux 2.4.2-ac13
HUB	IBM 8275-416 (10/100base-TX 自動切替 16port)
無線 LAN	MELCO AIR-CONNECT (IEEE802.11b 準拠)

表 1: 使用した機材

	ServerA	ServerB	ServerC	ServerD
CPU	PentiumIII 1GHz	MMX Pentium 233MHz	Pentium 100MHz	PentiumIII 550MHz
Memory	256MB	128MB	64MB	896MB
NIC	Intel EtherExpress Pro/100 x 2			
OS	Linux2.4.2ac22(PPPoE オプション有り) + kernel level pppoed[4] Linux2.4.2ac22(PPPoE オプション無し) + rp-pppoe[4] (注) Linux2.2.18pre21 + rp-pppoe(Server C のみ)			

表 2: サーバ計算機のスペック

	ClientA	ClientB	ClientC	ClientD
OS	Windows2000 Pro	Windows98	Windows98	Linux2.4.2ac22 + kernel level pppoed[4]
	RASPPPOE version 0.95b[5]			
CPU	Celeron 633MHz	Celeron 300MHz	Pentium 266MHz	Celeron 633MHz
Memory	256MB	192MB	128MB	256MB
NIC	SiS 900	Intel EtherExpressPro/100	3CCFE575BT (PCCARD)	SiS 900

表 3: クライアント PC のスペック

して実装されたもので、導入は容易だがパケットの送受信を大量に行うことになる PPPoE サーバの性質上、kernel 内処理と user 空間処理の切り替えが頻発すると考えられ、パフォーマンスがあまり出ないことが予想される。これに対し kernel モードの実装は、kernel 自体に組み込む形で実装されたもので、kernel の再構築など導入が若干困難であるが、パケット送受信の処理が kernel 内処理のみで済むため、パフォーマンスが良いことが期待される。

本稿では、両方の実装に対して測定をおこない、実際にどれだけの差があるのかを調査する。

3.3 測定結果

本測定環境の元で、CPU スペックの異なる 4 種類のサーバ (表 2) のそれぞれで性能がどのように変化するかを測定した。また、OS に関しては Linux を用い、PPPoE の実装が user モードの場合、kernel モードの場合、さらに比較のため単純にルータとして動作させた場合の 3 種類 の場合について測定した。

また、クライアント PC に関しては 4 台用意 (表 3) し、それぞれの構成毎の性能の違いや、複数台接続した場合のサーバ計算機の性能を測定した。

性能測定の為のネットワーク負荷として、10MByte のファイルを ftp サーバ上に用意し、各クライアント PC から ftp を使ってデータの転送をおこなった。また、クライアント PC の接続パターンとしては、それぞれ 1 台ずつの場合 (合計 4 通り) を測定したのち、ftp の結果が速いものから 2 台を選んで動かした場合、3 台を選んで動かした場合、4 台すべてを動かした場合、の合計 7 通りについて測定をおこなった。

3.3.1 転送レート

Linux サーバの転送レートの算出方法は以下の通りである。

1. 各クライアント PC において 5 回のファイル転送を連続しておこなう。
2. そのうちの中間値 3 回分の平均値をそのクライアント PC の転送レートとみなす。
3. 接続していたクライアント PC の転送レートの総和を PPPoE サーバの転送レートとする。

OS 毎に、4 種類のスペックを持つ Linux サーバのそれぞれについて算出した転送レートは図 2, 図 3, 図 4 のようになった。

あらかじめ、ftp サーバと Linux サーバの間で ftp によるファイル転送をおこなったところ、最低スペックの Server C は 4400kByte/s、他の Linux サーバは 11000kByte/s 以上であり、100baseTX の帯域をほぼ限界まで使っている値が得られた。

図 2 と図 3 より、PPPoE を利用することによる転送レートの低下は約 9%であった。図 4 より、user モードの PPPoE を利用すると、1GHz の PentiumIII を用いても通常のルータとして利用した場合の半分程度の転送レートになってしまうことが分かった。

これらの図で、転送レートが理論値である 12500kByte/s を越えている理由は、クライアント PC を複数接続した場合の測定において、ftp の開始と終了に時間差が生じ、速いクライアント PC が転送を終了していくにつれ遅いクライアント PC が回線を占有できるようになり、転送速度が上がったように見えるため、と推測される。

クライアント PC 毎の ftp の結果は、ServerD を使った user モードの場合を除いて、速いもの順に ClientD, ClientA, ClientB, ClientC の順であり、ほぼ CPU 速度の順となった。ServerD を使った user モードの場合に関しては、ClientD と ClientA の差がほとんどないことと、OS の違いによる ftp クライアントの挙動の差が user モードの場合には比較的顕著に処理順序の差として現れているのではないか、と推測される。

3.3.2 CPU 利用率

PPPoE サーバの CPU 利用率の算出方法は以下の通りである。

1. PPPoE サーバ上で vmstat コマンドを用い、毎秒の CPU 利用率などを記録する。
2. 割り込み数がある閾値 tn を越えた時刻からその閾値を下回った時刻までの間を、実際のクライアント稼働時間とする。
3. 稼働時間内の CPU 利用率の平均を取る。

このようにして測定した PPPoE サーバの CPU 利用率は、図 5, 図 6, 図 7 のようになった。また、最速の Server A に対して、4 つのクライアント PC を稼働させた場合のついて、測定時間に対する CPU 利用割合とコンテキストスイッチと割り込み数をグラフにしたものが図 8, 図 9 である。図 8,9 より、閾値 tn を測定時間内の最大値の 10%と設定することにした。

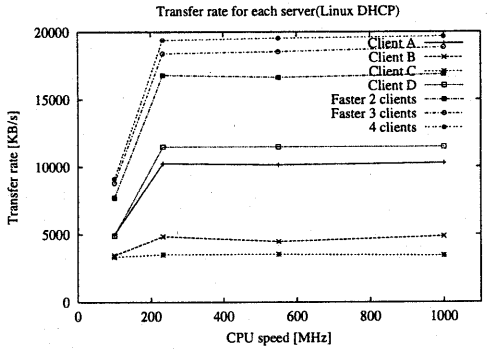

図 2: 転送レート: Linux サーバを DHCP サーバ+ルータにした場合

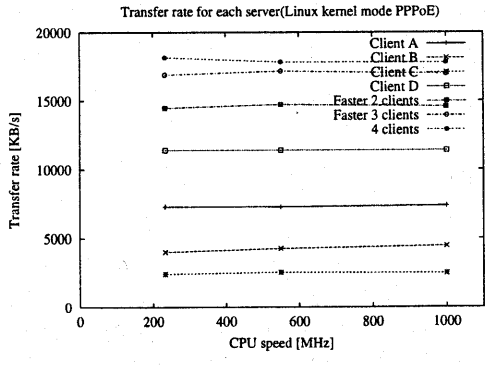

図 3: 転送レート: Linux サーバで kernel モードの PPPoE を動かした場合

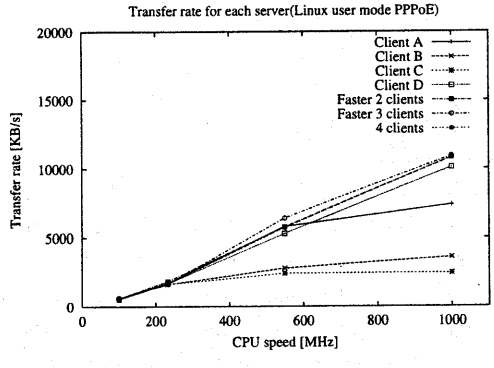

図 4: 転送レート: Linux サーバで user モードの PPPoE を動かした場合

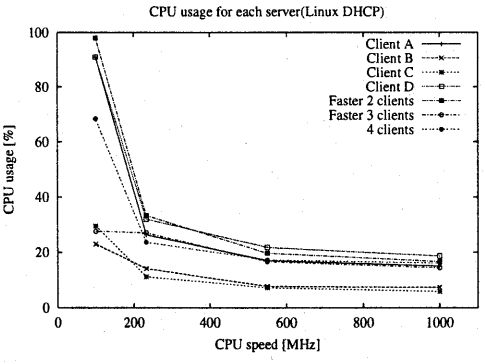

図 5: CPU 利用率: Linux サーバを DHCP サーバ+ルータにした場合

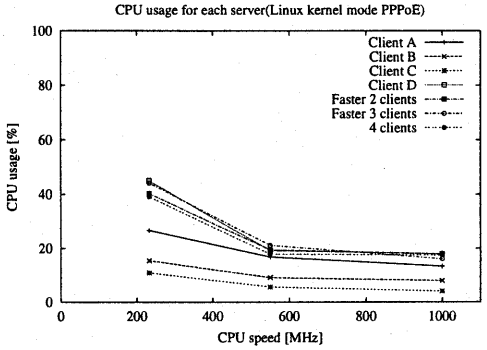

図 6: CPU 利用率: Linux サーバで kernel モードの PPPoE を動かした場合

図 5 と図 6 から CPU 利用率に関しては、CPU が PentiumIII 550MHz 以上ではおおむね 20%以下であり、kernel モードの PPPoE を使用したことによるオーバヘッドの増加はほぼ無視できることが分かった。また、PentiumIII 1GHz と CPU 性能を倍近くに上げてもそれほど大きな効果は得られないことも分かった。さらに、図 7 から user モードの PPPoE を使用すると CPU をほぼ 100%使い切ってしまうことも分かった。図 8 と図 9 から、user モードの場合は kernel モードとほぼ同数の割り込みを処理しており、CPU も user モードで user が使っている量と、kernel モードで system が使っている量とがほぼ同じになっている傾向がある。しかし、user モードの場合はコンテキストスイッチが大量に発生するために残りの CPU を消費してしまっていることが分かる。

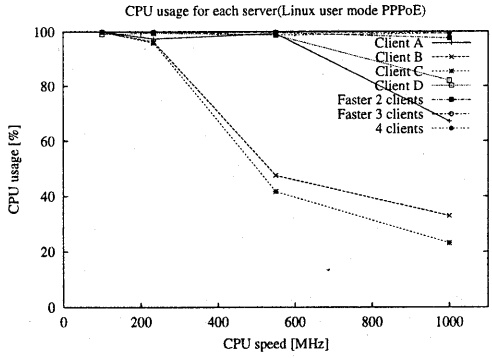

図 7: CPU 利用率: Linux サーバで user モードの PPPoE を動かした場合

3.3.3 メモリ使用量

PPPoE サーバのメモリ使用量の算出方法は以下の通りである。

1. PPPoE サーバ上で top コマンドを用い、毎秒の稼働プロセスとプロセスサイズを記録する。

kernel モードの PPPoE サーバの場合、pppoed が 1 つ稼働しており、クライアント PC が接続するたびに pppd が 1 つ起動される。計測中、pppoed は 536kByte 以下、pppd は 1 つあたり 940kByte 以下であった。

user モードの PPPoE サーバの場合、pppoe-server が 1 つ稼働しており、クライアント PC が接続するたびに pppoe と pppd が 1 つずつ起動される。計測中、pppoe-server は 552kByte 以下、pppoe は 1 つあたり 436kByte、pppd は 1 つあたり 940kByte 以下であった。

従って、メモリ使用量だけみれば、128MByte のメモリを搭載したサーバであれば、kernel モードで数十台のクライアント PC の接続に、user モードではその $\frac{2}{3}$ 程度のクライアント PC の接続に耐えられると考えられる。しかし、CPU 利用率からも分かるように、user モードではクライアント PC が増えるとコンテキストスイッチが増大するので、メモリ使用量だけで単純には議論できない。

4. まとめ

本稿では、PPPoE を用い、認証つき情報コンセントの実装を行い、実験環境を構築し実際に性能を評価

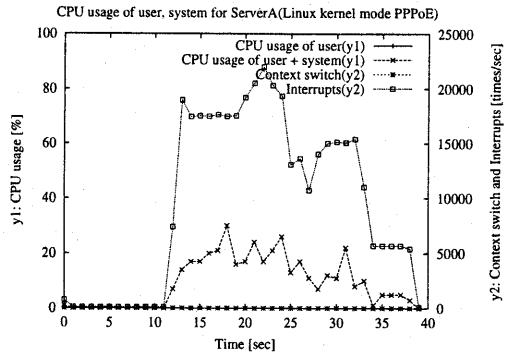

図 8: CPU 利用割合とコンテキストスイッチおよび割り込み数: Linux サーバで kernel モードの PPPoE を動かした場合 (Server A)

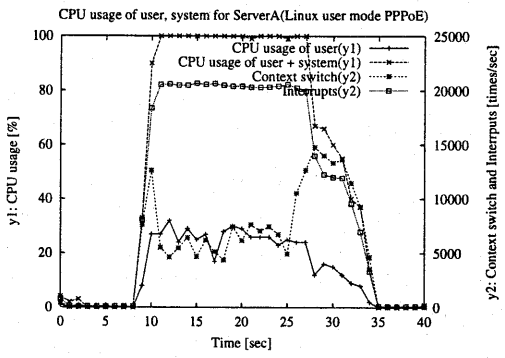

図 9: CPU 利用割合とコンテキストスイッチおよび割り込み数: Linux サーバで user モードの PPPoE を動かした場合 (Server A)

した。転送レートの図 3 から、PentiumIII 550MHz の Linux サーバでも 100baseTX の帯域の限界まで使い切っているが、CPU 利用率にはまだ余裕があり、また、クライアント PC 数を 1 から 4 まで増やしても、特に CPU 利用率の大きな増大は見られないので、ボトルネックは、ネットワーク側であると推測できる。従って、Linux 上の kernel モードの PPPoE を使用すれば、PentiumIII 500MHz 程度の安価な PC で PPPoE サーバを構築しても、十分な性能が得られそうである、といえる。

今後の課題としては、

1. もっと多くのクライアント PC が接続される環境でのサーバの性能を、シミュレーションなどを行うことで予測すること。
2. PPPoE サーバのネットワークインターフェイスを Gigabit Ethernet などのより大容量な媒体にして測定すること。
3. 実運用を行い運用ノウハウを蓄積していくこと。

などが挙げられる。

謝辞

有益な意見や実験の協力を戴いた大阪大学サイバーメディアセンター情報メディア教育研究部門の教職員および学生ボランティアスタッフの皆様に感謝します。

参考文献

[1] 石橋勇人, 山井成良, 安倍広多, 阪本 晃, 松浦 敏雄: 利用者ごとのアクセス制御を実現する情報コンセント不正利用防止方式, 情報処理学会論文誌, Vol.42, No.1, pp.79–88 (2001)

[2] Cisco Systems Inc.: Cisco Aironet350 series; EAP (Extesible Authentication Protocol), http://www.cisco.com/japanese/warp/public/3/jp/solution/smbiz/aironet/.

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

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

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

[6] C. Rigney, S. Willens, A. Rubens, and W. Simpson: Remote Authentication Dial In User Service (RADIUS), RFC2865 (2000)

[7] Livingston RADUIS server, http://www.dit.co.jp/support/products/livingston/radius/