公共スペースにおけるIP接続性の確保と認証を両立したネットワーク運用方式と実証実験

小林　孝史

要　旨

IPネットワークの普及，利用希望の高まりに伴って，様々な場所においてIPネットワークとそのサービスを利用できるようになってきた．しかし，その利用は情報機器が常設され，利用者登録の完了している範囲内だけであり，真の「どこでも（anywhere)」ではない．大学において「anywhere」から最も遠いのは，ゼミ室や講義室である．ゼミ室，講義室だけでなく，学生サービスの一環で設けられている場所は，不特定多数の利用者が入退出を繰り返す空間であり，このような場所にIPネットワークを敷設し，その空間の利用者に自由に利用できるようにすることはセキュリティ上好ましいことではない．本論文では，いわゆる公共スペースにおける一般的なIP接続性の問題点を述べ，現有資源を有効に利用した利用者を特定できるIP接続性の運用方法，実証実験，性能評価について述べる．

Management Policy and Techniques to Achieve Safe and Authorized IP Connectivity

Takashi KOBAYASHI

Abstract

In the public space, such as seminar and lecture rooms and community spaces at universities, it is difficult to provide the IP network and its connectivity as freely as in private spaces. We can access the Internet from these places using DHCP automatically, but there is no authentication method in this method. Moreover there are too many users and anonymity allow s　malicious users to hide from management systems, which is not desirable thing from the point of view of computer network security. Therefore, authentication methods were developed to distinguish normal users from malicious ones. To achieve "Real IP anywhere", that is safe and able to specify users, I describe the general problems of IP connectivity, management methods, experimental work and evaluation of performance.

1．はじめに

Web 利用に始まったインターネット利用の形態の変化はコンピュータを利用した実習科目だけではなく，専門的な教育を行う演習科目や一般の講義科目の実施方法にも影響を与えてきているのはもはや周知の事実である．このような利用形態の変化に伴って，要求されるネットワーク需要の増大をカバーすべく，本学でも1998年にATMネットワーク，2001年度にGigabitネットワーク，とキャンパス内IPネットワークが順次整備され，どこでも高速大容量のTCP/IPアプリケーションが利用できる環境が整ってきている．しかし，重点的に整備されているのは，研究用ネットワーク，および情報機器が常設され必ず利用者登録を行っている実習用ネットワークのみにすぎない．これはネットワークの利用者を特定することに問題があるからである．

このような講義室，ゼミ室等の不特定多数の利用者が存在する空間のネットワークを経由して学内外のあらゆる情報資源を自由に利用できる運用を行うことは，セキュリティ上好ましいことではない．しかし，管理・運用ルールを定めたセキュリティポリシーの策定次第によっては管理・運用を円滑に行うことができる．そのための技術的な手法がいくつか存在しており，特別な投資の必要もなく，現有設備を用いることによって，事後に利用者を特定でき，安全に高速大容量のTCP/IPアプリケーションを利用できる環境を準備することができるようになる．

本論文では，利用者としては比較的安全にネットワークに接続する手段を利用でき，管理者側としては管理・運用方針に基づいた利用者の特定が可能なアクセス手段の提供が可能となる機構についての考察を行い，実験ネットワークにおけるアクセス機構の設定，配備，接続実験の結果について報告する．

2．一般的な技術によるIP接続性提供の問題点

公共スペースでのIP接続性提供のための一般的な技術としては，有線LANと無線LANにおけるDHCP（Dynamic Host Configuration Protocol，動的ホスト構成プロトコル）[1]がある．

TCP/IP接続を行うためには最低でもIPアドレス，ネットマスク，ゲートウェイアドレス等の設定を行う必要がある．これらの情報は利用するネットワークごとに異なるものであるために，利用者による設定の変更を強いることに繋がる．これらの情報を自動的に設定するDHCPがもっとも多く利用されている．DHCPは管理者の手を煩わすことなくTCP/IP接続を希望するホストの設定（具体的にはIPアドレス，ネットマスク，ゲートウェイアドレスなど）を自動的に動的割り当てを行う機能を持ったプロトコルである．

DHCPによる割り当ては非常に便利である反面，セキュリティに配慮された設計ではないため，今日ではさまざまな問題点が挙げられている．それらの問題点についてまとめてみる．

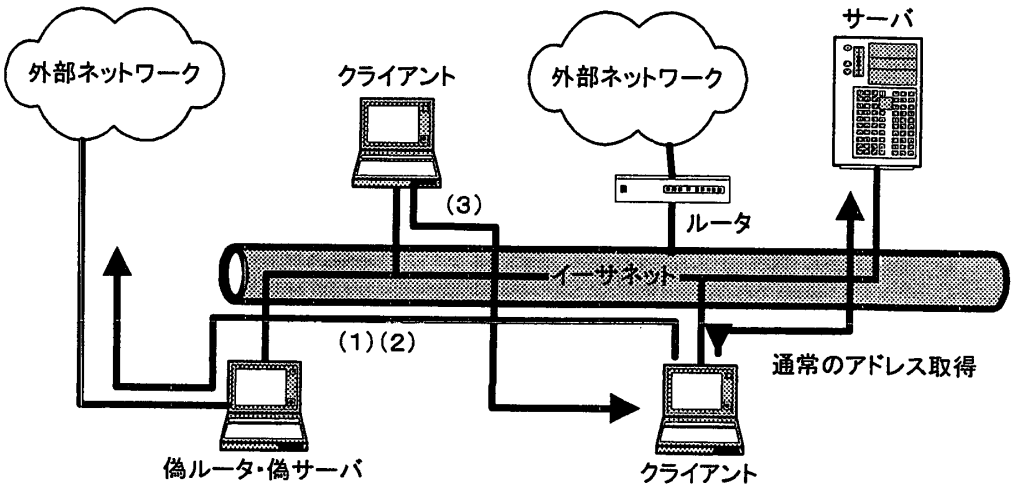

図1　DHCPを利用した場合の問題点

2.1 DHCPの場合の問題点

DHCPはアドレスの割り当てを設計目標にしているため，セキュリティに対する考慮はなされていない．セキュリティ問題については図1に示すような(1)偽のDHCPサーバの起動問題，(2)それに伴う不正なアドレスの取得やルーティング設定の問題，(3)悪意あるクライアントからの不正な情報収集などが挙げられている．もっとも問題とされるのはDHCPによるアドレス割り当ての機構に「ユーザー認証」が含まれていないことである．この問題により，冒頭でも述べたようなオープンな環境においてDHCPをサービスすると，IPアドレスと利用者（正確には利用者の情報機器のハードウェアアドレス）の対応付けが不可能になるのである．ハードウェアアドレスによるDHCPアクセスの制限を行うことも可能であるが，毎年最大数百名の登録更新（削除および新規登録）が必要であるため非現実的な運用を強いることにつながる．

DHCPによるIPアドレス割り当て等のネットワーク設定は，DHCPによる設定を回避して手動での設定が可能であることが分かっている．DHCPを使用して設定を行う際にユーザー認証を行う製品もすでに発表されているが，サーバで持っているユーザー情報を利用することができず，RADIUSなどの外部の認証用データベースを必要とする．パケットフィルタリングツールとして利用することも可能な製品も存在し，これはその機器を通過するネットワークパケットを監視し，認証の完了していないパケット交換に対して強制的に認証を要求する仕組みを持っている．これに対しても外部の認証用データベースが必要となる．しかし，アプリケーション層でのフィルタリングのために，あるアプリケーションに対してのみ認証を強制し，(1)他のアプリケーション・プロトコルは通過させない，(2)シームレスな認証を受けることができない，(3)「抜け穴」となる可能性がある，という運用上の問題もある．

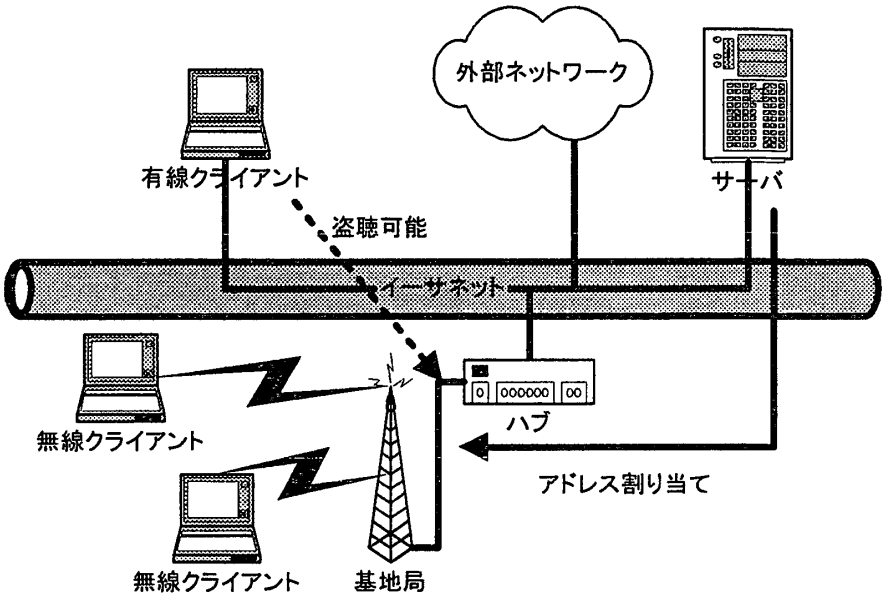

図2　無線LANを利用した場合の問題点

2.2　無線LAN（802.11x）の場合の問題点

有線 LAN と比較して，ケーブルの取りまわしが不要，無線の届く範囲内ならば場所を選ばないなどの理由により，無線 LAN を導入する例も多々ある．無線 LAN 専用の broadcast domain を設定した場合には，無線クライアントの認証問題，DHCP と同様のアドレス割り当ての問題が考えられる．既存の有線による broadcast domain の内に無線 LAN の環境を設定すると，アドレス割り当てに利用している DHCP の問題の他に，有線部分から無線部分の盗聴が可能になることを考慮に入れる必要がある（図2）．

最近では，フリースポットと呼ばれる，街角で無線 LAN による IP 接続性のサービスを利用できるようになってきている．このフリースポットを設置するための製品パッケージには認証機構も付属しており，業界内においても利用者の特定には配慮する姿勢を見ることができる．

さらに，無線 LAN にクライアントに対するユーザー認証によって制限を設けることができても，ネットワーク帯域の問題がある．現在一般的に使われている IEEE 802.11b 規格の無線 LAN では公称 11Mbps であるものの，実際には数 Mbps の能力しかない．これは 10base-T で構築した LAN の約6割程度の性能である．しかも同じアクセスポイントを複数の無線クライアントで共有するとその数に反比例して利用可能な帯域が減少する．また次の実用規格である IEEE 802.11a では帯域の問題は解決しそうである（54Mbps）が，アクセスポイント当たりの利用可能なチャンネル数が減少するため，配置するアクセスポイントを増やす必要がある．

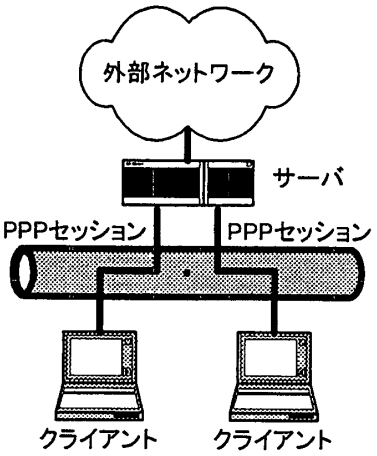

図3　PPPoEによるIP接続性の提供

3．PPPoEによるIP接続性の提供

これまで述べたような「不特定多数の利用が見込まれる空間」に対して「不正利用を防ぐための技術的な限界」を持ったDHCPの代替手段として，PPPoE（PPP over Ethernet）[2]によるIP接続性を提供することができる．PPPoEはEthernet上でPPPセッションを確立する技術で，ADSL（Asynchronous Digital Subscriber Line）やFTTH（Fiber To The Home）を利用するための認証手段およびIP接続性の提供手段として用いられている．PPPoEサーバ側ではネットワークインターフェイスの設定を行う必要がなく，PPPoEによるセッションの確立を行うまではネットワーク設定を知ることができない．手動による設定を行っても対向するサーバの設定ができていないので，PPPセッション以外のネットワーク設定は不可能である．このようにPPPoEでは，アドレスの割り当ては認証が完了した段階で行われるため，クライアントによる不正なアドレスの取得，アドレスの重複，不正なサーバの起動，他人のPPPセッションの覗き見などを防ぐことが可能で，より安全なIP接続性を提供することができる．

現在，主要なサーバOS上でPPPoEのサーバ機能を利用することができ，比較的安価にPPPoE環境を用意することができる．このことは，すでに利用している認証用データ，つまりPPPoEサーバで認識できる認証用データを引き続き利用することができるため，登録データを新たに準備する必要もないことを意味する．ただし，サーバ側でパスワードを有効期限つきで運用を行っている場合には，サーバの利用だけでなくPPPoEの利用も影響を受けることに注意する必要がある．DHCPに対する認証のためにサーバで運用しているRADIUS[3]サーバを利用する際にも同様の注意が必要である．

クライアントでも同様に主要なクライアントOS上で利用することができるため，導入に対して不公平を生じるケースは非常に少ないと考えられる．

PPPoEサーバをどのオペレーティングシステムで実装したとしても，認証用のデータベースへのアクセスを避けて通ることはできない．ここでは認証用データベースへのアクセス方法，プロ

トコルについて考察してみる.

PPPoEで使用する認証は次の4種類である.

- パスワード認証
- PAP（Password Authentication Protocol）
- CHAP（Challenge Handshake Authentication Protocol）
- ホストパスワード認証
- 外部データベース利用

通常のPPPにおいてもPAPやホストパスワード認証の認証方式を利用している.PPPoEの場合もユーザー情報，パスワードはPPPoEパケットにカプセル化されているが暗号化されていないものであるため，利用については注意を要する.CHAPについては毎回異なるChallengeが示され，それに対するハッシュ値をResponseとして返すのでパスワード自身がPPPパケットとして流れることはない．どの認証の場合にも共通することであるが，サーバが自分自身でパスワードデータベースを持っている場合にはネットワークをパスワード文字列またはDESによる暗号化された文字列が通過することはないが，他のサーバで提供しているパスワードデータベースを利用する場合は，データベースを利用するための通信の安全性と内容の正当性を考慮に入れる必要がある．運用と利便性のトレードオフがあるが，できるだけ安全な認証方法を採用することを考えて運用ポリシーを策定する必要はある.

4．サーバ機種を変更した場合の比較

PPPoEのプロトコル仕様はRFCに定義されているが，サーバとなるOSの種類によって実装している機能が異なる．その実装上の違いについて解説する.

4.1 Solarisの場合

Solarisでは，Solaris8 Maintenance Update6（7/01）よりPPPoEサーバ／クライアントを構成することができるようになっている．このPPPoEスタックはANU（Australia National University）で開発されたPPPスタックをベースにしており，いくつかの拡張がなされたものである．その拡張の一つとして，IPv6対応が挙げられる．IPv6の売りの一つに「Plug & Play」機能があるが，IPv6のアドレス割り当て機構に対するユーザー認証の仕組みは組み込まれていない．つまり，「繋げばすぐに使える」状態であり，多人数の利用者が利用する状況下ではIPv6対応とすることはセキュリティの観点からも非常に難しい．そういった場面で，SolarisのPPPoEスタックを利用する価値が生まれる．ただし現時点ではSolaris同士での接続時に限定される.

SolarisによってPPPoEサーバを実装する場合は，そのサーバに依存するネットワークを細かく分割することができる．具体的には表1に示すようなアドレス分割を行うことができ，基本的にはサブアロケーションによるCクラス以下のネットワークアドレスの割り当てとほぼ同じ（先

表1：n bitマスクの場合の割り当て可能アドレス数

n	blocks	addresses	total
25	1	126	126
26	3	62	186
27	7	30	210
28	15	14	210
29	31	6	186
30	63	2	126

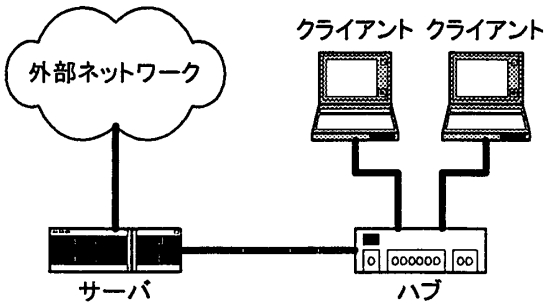

図4　実験用ネットワーク

頭ブロックのみ使用不可）である．表1より，割り当て可能なアドレス数を最大にできるマスクビット値は28もしくは29ビットになるが，用意できるネットワークインターフェイス数に上限のある現実的なネットワーク構成における最適なマスクビット値は26もしくは27であると考えられる．

4.2　FreeBSDの場合

Usermode PPPによる実装であり，サーバ／クライアントの構成が可能である．サーバの場合はpppoedによる直接モードのPPPとして実装されている．SolarisによるPPPoEサーバの実装と異なるのは，PPPの枠組みの中で管理するネットワークを分割するのではなく，物理的なネットワークインターフェイスで管理するネットワークを分割することである．PPPoE用の回線に対して24ビットのネットワークアドレスを利用する際にはより多くのクライアントにサービスを提供することができる．

5．性能測定用ネットワーク構成と測定プログラム

実験で使用したネットワーク構成は図4の通りである．
サーバを経由して外部ネットワークへ到達するネットワーク構成とし，性能測定はサーバとクライアントの間で行った．

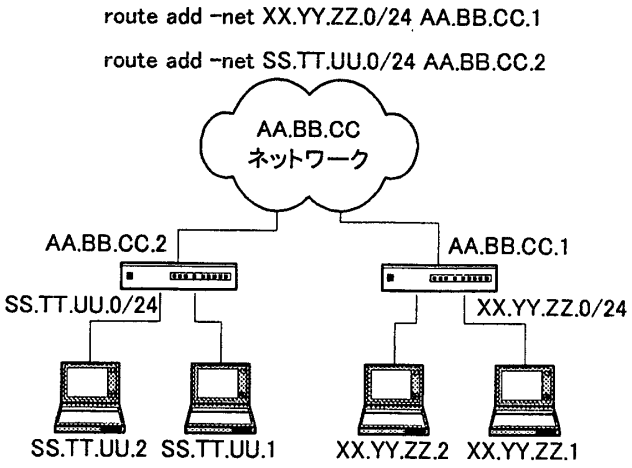

図5　静的な経路設定

実験用ネットワークでは，サーバとクライアントは PPPoE によって通信が可能であるが，PPPoE サーバを越えた通信を行う場合には PPPoE サーバの上位でのルーティング制御を行う必要がある．PPPoE で構成するネットワークは通常のネットワークとは異なって経路情報を広報できないため，PPPoE サーバの上位のルータ（またはスイッチ）において，静的な経路情報の登録が必要になる．図5のようなネットワークの場合，通常のネットワークであればルーティング機能（RIP など）によって XX.YY.ZZ.0/24 や SS.TT.UU.0/24 のネットワークまでの経路情報を広報できるが，XX.YY.ZZ.0/24 や SS.TT.UU.0/24 のネットワークは PPPoE によってはじめて構成されるため，route コマンドなどによってルーティング情報を設定することで静的に経路情報を構成する必要がある．

5.1　使用した機器のスペック

実験ネットワークで使用したハードウェアは次のとおりである．

・サーバ

SunFire v100，Solaris9，UltraSPARC IIe 500MHz，メモリー128MB

・クライアント1

Apple iBook，MacOS X v10.1.5，PowerPC G3 700MHz，メモリー256MB

・クライアント2

Dell Inspiron2000，FreeBSD 4.4-STABLE，Celeron 400MHz，メモリー256MB

・クライアント3

Toshiba Libretto100，FreeBSD 4-STABLE，MMX Pentium 166MHz，メモリー64MB

5.2　測定用プログラム

TCP 性能を測定するために dbs-1.1.5 を使用した．DBS（Distributed Benchmark System）は，TCP 転送性能，損失率，ウィンドウサイズなど TCP についてのすべてを計測することができる．計測用コマンド（スクリプト）のコントローラ，計測用パケットを発行するデーモン，計

測結果の可視化ツールからなり，一般ユーザーの権限で動作可能である．

Solaris，FreeBSDについてはそのまま利用できるが，MacOS Xについてはベースとなっている FreeBSD とは使用している TCP/IP スタックが微妙に異なるためにそのままではコンパイルできない．そこで，いずれの OS 環境でも使用できるように修正を施してコンパイル作業を行った．具体的には/usr/include/netinet 内のヘッダファイル tcp_debug.h の構造体の差異を吸収するマクロを定義し，それらのマクロをソースコードに埋め込んで実行環境に適合したコンパイル結果を得られるようにしている．これらのマクロは TCP Debug 機能（シーケンス番号，TCP フラグなど）に関する部分であり，今回の測定のターゲットである TCP 転送性能には直接関係しないため，DBS パッケージがコンパイル可能になることを目指した．

```
#if !defined(__APPLE__)
#define DBS_TCP_SEQ td_ti.ti_t.th_seq
#define DBS_TCP_ACK td_ti.ti_t.th_ack
#define DBS_TCP_FLAGS td_ti.ti_t.th_flags
#define DBS_IP_HEADER_LEN td_ti.ti_i.ih_len
#define DBS_TCP_HEADER_OFFSET td_ti.ti_t.th_off
#else
#define DBS_TCP_SEQ td_th.th_seq
#define DBS_TCP_ACK td_th.th_ack
#define DBS_TCP_FLAGS td_th.th_flags
#define DBS_IP_HEADER_LEN td_ip.ip_len
#define DBS_TCP_HEADER_OFFSET td_th.th_off
#endif
```

6．実験ネットワークにおける TCP 転送性能の測定

本実験ネットワークにおける PPPoE 接続の TCP 転送性能を測定した．測定に使用した DBS では，測定のための模擬パケットのシナリオを自由に設定できるので，本論文の結果に用いたすべての測定実験では，初期パケット長 8192 バイト，終期パケット長 8192 バイト，遅延時間 0 ミリ秒，処理オーバーヘッド 0 ミリ秒という理想的なパケット発生源を想定して実験を行った．

測定実験は，(1)クライアント・ハードウェア性能による違いを調べる，(2)ネットワーク・ハードウェアの性能による違いを調べる，ために行った．また同時に IEEE 802.11b 規格の無線 LAN 環境における転送性能を同様の組み合わせでの測定も行った．

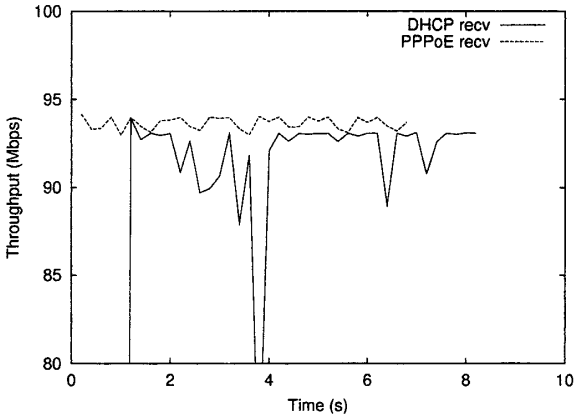

図6 iBookにおける性能比較（受信）

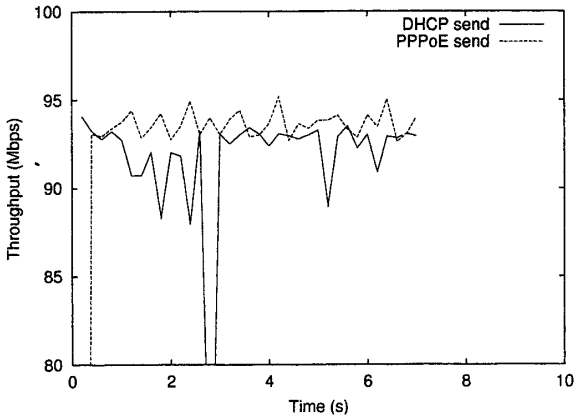

図7 iBookにおける性能比較（送信）

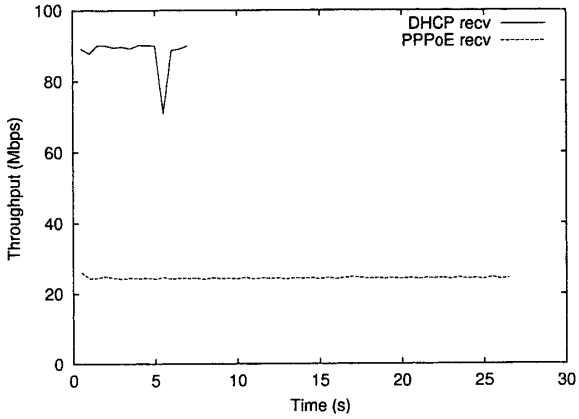

図8 Inspironにおける性能比較（受信）

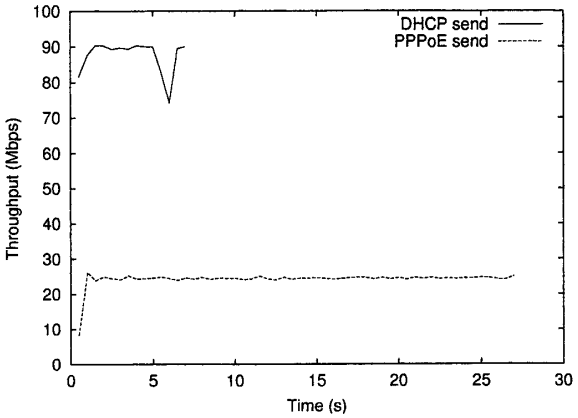

図9 Inspironにおける性能比較（送信）

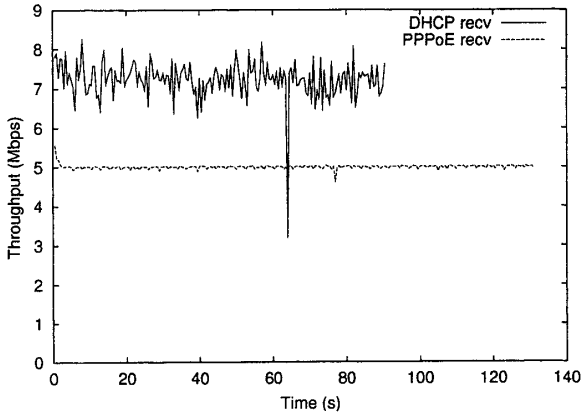

図10 Librettoにおける性能比較（受信）

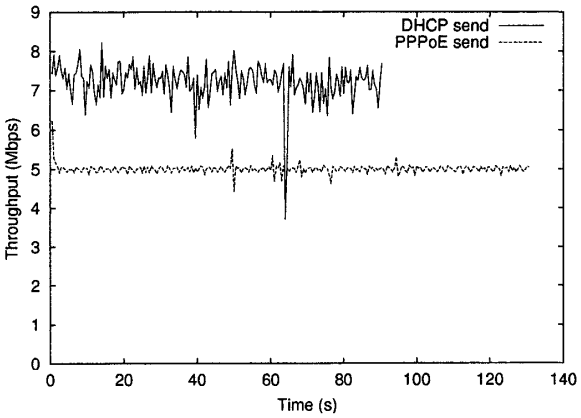

図11 Librettoにおける性能比較（送信）

6.1 クライアントの違いによる性能の評価

100Base-TXでのネットワーク設定を行ったものと，PPPoEでのアドレス割り当てを行ったものとでの比較を行う．どちらの場合も同じネットワーク・ハードウェアを使用している．

図6および7は，PowerPC G3 700MHzプロセッサを搭載したiBookである．DHCPによるアドレス割り当て，PPPoEによるアドレス割り当てのどちらの場合もすべての時刻において

90Mbpsを超えており，非常に高い性能を示していることがわかる．DHCPの場合の転送性能の時間依存のゆらぎはPPPoEの場合には見られない．これはPPPoEでのパケットのカプセル化により，個々のパケットの処理時間が加わることで転送性能が平滑化し，全体の転送性能を押し上げていることが推測できる．

図8および9はIntel Celeron 400MHzプロセッサの搭載されたパーソナルコンピュータである．DHCPによるアドレス割り当てを行った場合と比較して，PPPoEの場合のTCP転送性能はかなりの劣化が見られる．DHCPの場合もPPPoEの場合も同じ数（10000個）のパケットを転送して測定を行っているが，DHCPの方が約4分の1の時間で終了している．先の図6と7と比較して分かることは，PPPセッションを確立した場合にはそのセッションの維持にプロセッサやハードウェアの処理時間を消費するのであろうということである．DBSによる測定の場合はネットワークに副奏が発生するほどのパケットを発生させて測定を行うため，このパーソナルコンピュータのOS上で稼動しているPPPoEデーモンが到着するパケット，送信すべきパケットを処理できていない可能性もある．

図9および10は，MMX Pentium 166MHzプロセッサを搭載したノート型パーソナルコンピュータでの結果である．このパーソナルコンピュータでは物理的なネットワークインターフェイスが10Base-Tに限定されているため，転送性能の物理的な上限は10Mbpsとなる．DHCPの場合と比較してPPPoEでは約6割の性能を示している．これはプロセッサ自体が非力なため，PPPoEパケットの処理に時間を費やしてしまい，TCP転送性能を低下させていると推測できる．

これらの結果より，DHCPではプロセッサやハードウェアの影響は少ないと見てよいが，PPPoEを利用するためにはある程度性能の高いプロセッサやハードウェアを利用する必要があると考えられる．

6.2　802.11bによるネットワーク構築と性能測定

無線LAN環境においてPPPoEを利用した例は見当たらない．その理由としては利用可能な帯域が狭いことが挙げられる．どのくらいの帯域を実際に利用できるのかを調べるために，無線LAN環境についても同様の測定を行った．

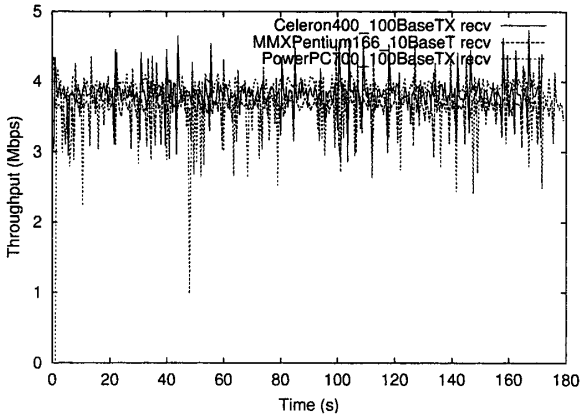

図 12　802.11b における性能比較（受信）

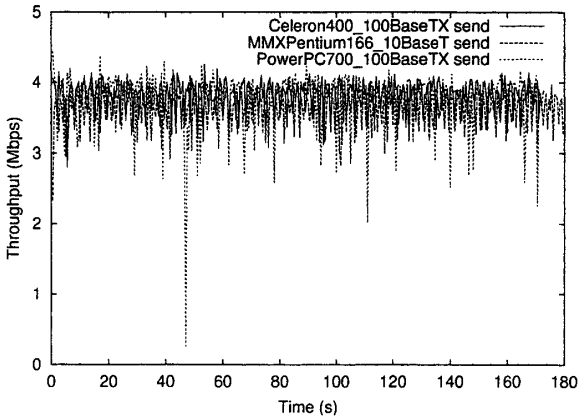

図 13　802.11b における性能比較（送信）

図 12 および 13 は無線 LAN クライアントにおけるスループットの測定結果である．図に示すように無線 LAN の場合では，どの機種においても最高 4 Mbps 程度の性能であった．基地局，クライアントともに市販の普及価格帯のものである．この結果はそれぞれを単独で測定した結果であり，同時利用を想定した同時測定では利用台数に反比例してスループット性能は減少している．ケーブル等の取り回しが不要である分の利便性は高まるが，このような利用可能帯域の狭さにより無線 LAN 環境においては大容量コンテンツの利用は現実的ではなく，利用する情報資源を考慮する必要がある．

7．今後の検討課題

公共スペースにおいて，従来から広く利用されている DHCP によるアドレス割り当てを利用する上での問題点を明らかにし，DHCP と組み合わせて利用が普及している無線 LAN の運用の問題，利用可能帯域の問題を明らかにした．その上で，現在最も有望な PPPoE についてその設定，接続実験，スループット性能の測定を行った．

DHCP によるアドレス割り当て，PPPoE によるアドレス割り当てのどちらもアドレスを自動で割り当てるという設計目標は達成している．特に PPPoE によるアドレス割り当てでは利用者認証が加わることにより，割り当てたアドレスと利用者の組み合わせを特定することが可能になり，公共的な空間における IP 接続性の提供にも使用できる．

スループット性能の点から考察すると DHCP によるアドレス割り当てではほぼ最高性能を引き出すことができるが，PPPoE によるアドレス割り当てでは PPPoE パケットのオーバーヘッドが加わるために若干の性能低下が見られる．利用しているプロセッサの性能にもよるが，最新のプロセッサを利用したクライアントにおいては重大な性能低下とはならないことが実証できた．

本論文で対象としたのは Solaris サーバ上の PPPoE サーバ機能であるが，FreeBSD 上の PPP ではパッチを適用することにより，IPV6CP を利用できるようになる．これにより利用者認証を行った上で IPv6 アドレスを割り当てることが可能になる．この点の検証も行う必要がある．

謝辞

本研究の一部は平成 14 年度関西大学重点領域研究助成による助成を受けて行われたものである.

参考文献

[1] Dynamic Host Configuration Protocol, http://www.ietf.org/rfc/rfc2131.txt?number=2131, (1997).
[2] A Method for Transmitting PPP Over Ethernet (PPPoE), http://www.ietf.org/rfc/rfc2516.txt?number=2516, (1999).
[3] Remote Authentication Dial In User Service (RADIUS), http://www.ietf.org/rfc/rfc2058.txt?number=2058, (1997).

付録A PPPoEサーバの設定

A.1 Solaris8 7/01以降（SPARC/Intel共通）

Solarisによる実装では，設定ファイルは複数にまたがる．ある一つのファイルの設定が別のファイルに依存することもある．

○/etc/netmasks：

```
192.168.xxx.0  255.255.255.0
```

○/etc/ppp/pppoe：

```
log "/var/adm/pppoe.log"

service プロバイダ識別名
    device インターフェイス名
    pppd "proxyarp 192.168.xxx.1:"
```

○/etc/ppp/pppoe.if：

```
インターフェイス名
```

○/etc/ppp/pap-secrets：

```
"*"     *     ""     192.168.xxx.64/26+
```

第1フィールドはユーザー名，第2フィールドはパスワード，第3フィールドはサーバ名，第4フィールドは割り当てるネットワークIDで，最後の+記号の指定によって，トンネル番号が自動で付加される．

○/etc/ppp/options：

```
login
pam
novj
novjccomp
refuse-chap
require-pap
mru 1454
mtu 1454
logfile /var/adm/pppd.log
idle 600
```

pamオプション識別子を用いることと，pap-secretsのユーザー名，パスワードを*とすることにより，Solarisで利用できるアカウントデータベース（PAM：Pluggable Authentication Module）経由によってユーザー・パスワード認証を行うことができるようになる．login識別子により，wtmpxファイルに認証時の時刻情報とセッション情報が記録される．これにより利用者の利用状況を把握することが可能になる．

A.2 FreeBSD

FreeBSDによる実装では，設定ファイルは一つである．実際にあるインターフェイス上でPPPoEサーバ機能を実現するためには，pppoedデーモンを起動する必要がある．

○/etc/ppp/ppp.conf：

```
定義名:
  set mru 1454
  set mtu 1454
  allow mode direct
  enable lqr proxy
  enable passwdauth
  set ifaddr 192.168.xxx.1 192.168.xxx.2-192.168.xxx.254
  accept dns
```

付録B PPPoEクライアントの設定

B.1 FreeBSD

○/etc/ppp/ppp.conf :

```
義名:
  set device PPPoE:インターフェイス名:プロバイダ識別子
  set timeout 0
  set mru 1454
  set mtu 1454
  set cd 5
  set dial
  set login
  enable passwdauth
  disable vjcomp
  disable pred1
  set authname ユーザー名
  set authkey パスワード
  set redial 0 0
  add default HISADDR
```