2005－ＤＳＭ－37（８）
2005／5／13

FDBを用いた接続ポート固有のIPアドレスリースが可能なDHCPサーバの設計と実装

桝田 秀夫† 木村 洋介†† 大下 福仁†† 齊藤 明紀††† 増澤 利光††

† 大阪大学サイバーメディアセンター
〒 560-0043 大阪府豊中市待兼山町 1-32
†† 大阪大学大学院情報科学研究科
††† 鳥取環境大学情報システム学科
E-mail: †h-masuda@ime.cmc.osaka-u.ac.jp, ††{y-kimr,f-oosita,masuzawa}@ist.osaka-u.ac.jp,
†††saitoh@kankyo-u.ac.jp

あらまし ネットワーク障害解析のため，あるホストのIPアドレスやMACアドレスからそのホストが存在する場所を探す必要が生じることがある．DHCPを用いた情報コンセントでは，IPアドレスは物理的な端末の位置と無関係に割り当てられるため，この作業は困難である．我々は，個々の情報コンセントに対して固定的にIPアドレスを割り当てるDHCPサーバを開発した．このDHCPサーバはSNMPを用いてスイッチングハブのMACアドレスフォワーディングテーブル(FDB)を取得し，割り当て対象端末の接続したポートを知る．このサーバは通常のサーバより応答時間が0.5秒長い．本システムを利用することで，ネットワーク管理者は容易に特定のDHCPクライアントの設置場所に到達することができる．

キーワード DHCP, スイッチングハブ, FDB, SNMP, ポート固定IPアドレスリース機能

Implementation of a port-aware DHCP server using FDB in the Switching HUB

Hideo MASUDA†, Yousuke KIMURA††, Fukuhito OOSHITA††, Akinori SAITOH†††, and Toshimitsu MASUZAWA††

† Cybermedia Center, OSAKA University.
1-32 Machikaneyama Toyonaka OSAKA, 560-0043, JAPAN.
†† Information Science and Technology, OSAKA University.
††† Department of Information System, Tottori University of Environmental Studies.
E-mail: †h-masuda@ime.cmc.osaka-u.ac.jp, ††{y-kimr,f-oosita,masuzawa}@ist.osaka-u.ac.jp,
†††saitoh@kankyo-u.ac.jp

Abstract For network trouble resolution, we occasionally need to lookup physical location of a host by the IP address or the MAC address. It is difficult in DHCP based information outlet sockets because IP addresses are allocated without sense of physical location. We developped an DHCP server system that allocates fixed IP addresses for each information outlet sockets. Our DHCP server makes SNMP querys to network switches to retrieve MAC-address forwarding table to know on which port the DHCP clients locates. Our server needs 0.5 seconds of longer response time than ordinary one. With our system, network manager can easily reach to physical location of any DHCP client.

Key words DHCP, switching HUB, FDB, SNMP, port-aware

1. はじめに

情報コンセントなどにおいて，ネットワークに接続するホストに対してネットワーク設定情報を提供するプロトコルには，さまざまなものがある．その一つに，LAN上でしばしば用いられるDHCPがある．DHCP(Dynamic Host Configuration Protocol) [5] とは，インターネットに接続しようとするクライアントに対して，ネットワーク設定情報を自動的に割り当てるためのプロトコルである．

ネットワーク管理者が，ユーザに安全な接続を提供するためには，利用情報や通信情報の記録を欠かすことはできない．これまでに，安全な情報コンセントサービスに関する研究は数多くおこなわれてきている [1] ～ [4]．しかし，認証を利用しても，ユーザが誰であったかは分かるが，ユーザの物理的位置を把握することまでは容易ではない．位置を取得するために，監視カメラの設置などをおこなっていては，ログを付き合わせる作業が煩雑になる．

本研究では，情報コンセントのように多数のユーザが入れ替わり立ち替わり接続されるネットワークにおいて，クライアントが接続されている位置にもとづいてIPアドレスを割り当てることを考える．実装したシステムでは，ネットワーク上にアクセスしているクライアントのIPアドレスを参照すれば，接続先のハブのポートを特定することができる．このため，ネットワーク管理者は容易に特定のDHCPクライアントの設置場所に到達することができるようになる．

2. 要求分析

本章では，ネットワークに接続されるクライアントの物理的な位置の情報を得るための仕組みを検討する．

位置情報を得る方法としては，人の手による記録，監視カメラの設置，位置情報をGPSなどから取得する方法，などが考えられる．しかし，これらの方法は手間がかかったり追加のハードウェアが必要になるといった点で問題が多い．

そこで，ソフトウェアの処理で位置の情報を得る方法を考える．位置の情報としては，物理的な接続ポートが考えられる．通常のネットワークの運用では，ハブなどのネットワークへの接続を中継する機器が，物理的な移動を頻繁にすることはない．そこで，それぞれのクライアントがどの物理ポートに接続されているかという情報を管理できれば，クライアントの位置の情報も，当該物理ポートからの配線の範囲内であると限定できる．

これらから，物理ポートを位置の情報とIPアドレスを対応付けることで，クライアントの位置情報を管理できると考える．

このような手法を用いるため，無線LANについては本研究の対象としない．

3. 検　討

3.1 ハブのFDBを利用する方法 (FDB法)

スイッチングハブには，物理的なポートに対して，通信をおこなっている機器のMACアドレスの情報(Forwarding Database, FDB) をもとに，効率的なパケット転送を実現する機能が備わっている．

FDBとは，スイッチのポートとそこに接続された機器のMACアドレス，その機器が所属するVLANのIDなどの組をデータベース化したものである．スイッチがパケットを受信したとき，パケットの宛先がFDB上のエントリにヒットした場合はその接続ポートのみにパケットを転送することで，全体としてのスループットを向上させることができる．

マネージメントスイッチングハブには，多くの場合SNMP(Simple Network Management Protocol) [6] を使って各種情報を取り出すことが可能となっている．RFC1493で定義されているBRIDGE-MIB [7] では，FDBの情報が定義されており，このMIBが実装されていれば，容易に外部に取り出すことができる．

そこで，DHCPを用いてクライアントにIPアドレスをリースする際に，ハブからFDBを取り出してクライアントの接続ポートを割り出し，そのポートに対応したIPアドレスをリースするという方法が考えられる (図1)．

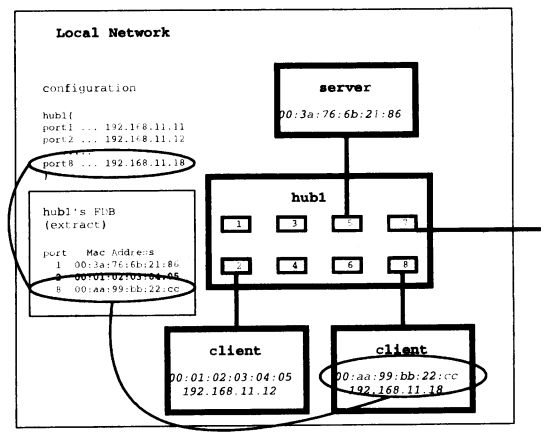

図1　ハブのFDBを利用する方法

3.2 各ポートにVLANを対応付ける方法 (VLAN法)

IEEE802.1qで定義されているVLAN [8] の技術の使えるハブを用いると，ハブのポートをグループ毎に論理的に分割して相異なるネットワークであると見做すことができる．

そこで，クライアントを接続する各物理ポートに相異なるVLANを割り当て，各物理ポートを相異なる別のネットワークとする方法が考えられる．各VLANにそれぞれ別のネットワークを設定しておき，DHCPサーバには，それぞれのネットワーク (サブネット) についてIPアドレスをリースする設定をおこなえばよい．この方法を用いると，どのサブネットのIPアドレスかを見ることでクライアントの物理ポートを知ることができる (図2)．

3.3 FDB法とVLAN法の比較

管理することができるクライアントの最大数　FDB法では，

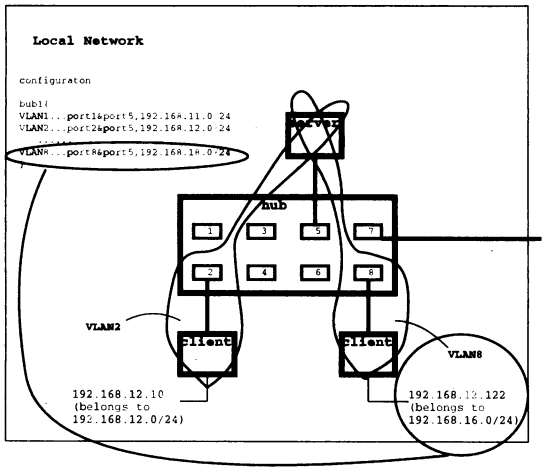

図 2　各ポートに VLAN を対応付ける方法

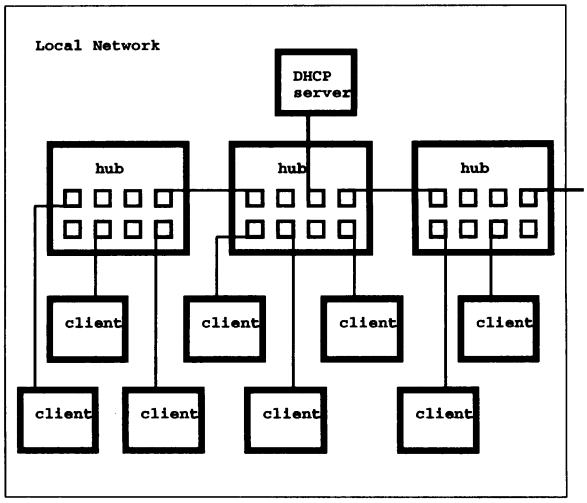

図 3　システムの構成

DHCP サーバが管理するアドレスの個数がリースすることができる IP アドレスの最大数となる．これに対して VLAN 法では，VLANID(それぞれの VLAN を識別するためのもの) が 12 ビットであることから VLAN は 4095(2^{12}-1) 個までしか分割できないので，これが最大数となる．また，VLAN は様々な目的に利用されるので，VLANID を自由に割り当てることは難しい．

IP アドレス空間の有効活用　FDB 法では，DHCP サーバ，ルータ，ハブに割り当てる IP アドレス以外，ネットワーク内全ての IP アドレスをクライアントに割り当てることができる．これに対して VLAN 法では，サブネットを最も細かく分割しても，/30，すなわちクライアントあたり 4 つの IP アドレスが必要(注1) であり，VLAN 法では IP アドレス空間を有効に活用することができない．

ネットワーク機器の制限　FDB 法ではクライアントを直接収容するハブに対して BRIDGE-MIB に対応している必要がある．VLAN 法では IEEE802.1q の VLAN に対応している必要があり，各 VLAN には少なくとも 1 つの DHCP サーバもしくは DHCP エージェントが稼働できる必要がある．ある程度以上のマネージメントハブでは，いずれの機能も標準的に利用可能であるので，適用範囲としては差はほとんどない．

以上のことより，FDB 法での実装を選択する．

4. 設　　計

4.1 システムの前提

本システムでは，研究室規模，もしくは計算機センター規模の，数十台から数百台のクライアントが接続されるネットワークを想定している．システムはサーバマシン，クライアントマシン，ハブから構成される (図 3)．

このうち，サーバマシンについては DHCP サーバとして動作できる程度のスペックがあればよい．クライアントマシンについては，DHCP クライアントとして動作することができればよい．また，ハブについては，その FDB を外部から取り出すことができるマネージメントハブであることが必要である(注2)．

4.2 設 計 方 針

本研究では，既存の DHCP サーバに機能を追加することで要求仕様を満たすシステムを作成する．

既存の DHCP サーバからの変更点は，クライアントにリースする IP アドレスを決定する際，クライアントの位置情報，つまりどのハブのどのポートに接続されているかをもとに IP アドレスを決める点である．

DHCP では，IP アドレスをリースする際に，サーバ・クライアント間でメッセージのやり取りがおこなわれる．作成する DHCP サーバは，既存の DHCP のメッセージ交換に加えて，新たにハブとのメッセージ交換をおこなう．以下では，これらのメッセージのやり取りについて説明する．

クライアントが新規に IP アドレスを要求する場合，以下のような動作となる．

（1） (C) DHCPDISCOVER メッセージをブロードキャストする．

DHCP の規約によりブロードキャストドメイン内に必ず 1 個以上のサーバが配置されているので，このメッセージはサーバに届く．

（2） (S) DHCPDISCOVER が送られてくると，リースする IP アドレスを決めて，DHCPOFFER メッセージを返す．

（3） (C) 使用する IP アドレスを選択し，対応するサーバに DHCPREQUEST メッセージを送り，その IP アドレスを使用したい旨を伝える．

(注1)：ネットワークの大きさが最低 2 ビット (IP アドレス 4 つ分) であることによる．

(注2)：BRIDGE-MIB に対応していなくても，telnet などで取り出すことが可能であるなら，実現可能である．

（4） (S) その IP アドレスが利用可能な状態になっているかを確認した後 DHCPACK メッセージを返し，IP アドレスをリースする．

また，クライアントがリース中の IP アドレスのリース更新を要求する場合，及びクライアントがネットワークからの一時離脱後もう一度 IP アドレスを要求する場合は，DHCPREQUEST メッセージをサーバに送る．このメッセージには使用したい IP アドレス (使用中，もしくは使用していたもの) が含まれている．サーバはその IP アドレスが実際に利用可能かを確認した後 DHCPACK メッセージを返し．IP アドレスを再リースする．

本システムでは，ポート固定 IP アドレスリース機能の利用が設定されている場合，サーバに DHCPDISCOVER メッセージが送られてきてから DHCPOFFER メッセージを返すまでの間と DHCPREQUEST メッセージが送られてきてから DHCPACK メッセージを返すまでの間に，ハブとメッセージを交換する．このとき，サーバはハブから FDB を取り出し，それをもとにクライアントの接続ポートを確認する．そのポートに固定 IP アドレスを割り当てるように設定されていた場合，その IP アドレスをクライアントにリースする IP アドレスとする．

ポート固定 IP アドレスリース機能の利用が設定されているときに，クライアントが IP を新規に要求する場合のサーバ・クライアント・ハブ間のメッセージ交換は，図 4 のようになる．クライアントが IP アドレスの更新を要求する場合，及びネットワークからの一時離脱後にもう一度 IP アドレスを要求する場合のメッセージ交換は図 4 の 5 以降のみである．

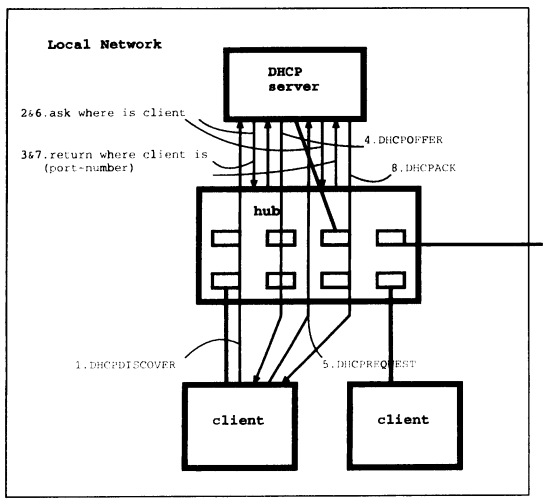

図 4 サーバ，クライアント，ハブのメッセージ交換

4.3 外部仕様

4.3.1 リースする IP アドレスを決定する方法

本システムでは，サーバがクライアントから IP アドレス要求を受け取ったとき，クライアントにリースする IP アドレスを決定するにあたって，以下の三通りの方法を用いることができる．

（1） クライアントが接続されたハブのポートに割り当てられたポート固定 IP アドレスをリースする (ポート固定リース)

（2） クライアントの MAC アドレスに割り当てられたホスト固定 IP アドレスをリースする (ホスト固定リース)

（3） 指定された範囲の IP アドレス群からランダムに選択した IP アドレスをリースする (ランダムリース)

1 は本システムで追加する方法であり，2 と 3 は既存の DHCP でも用いることができる方法である．

4.3.2 設定ファイルの記述

本システムでは，アドレスのリースについての設定情報は，既存の DHCP サーバと同様に，設定ファイル"dhcpd.conf"に記述する．ホスト固定リース，ランダムリースの場合の設定方法は既存の DHCP サーバと同一である．以下では，ポート固定リースの場合の設定方法のみを述べる．

ポート固定リースを利用する場合には，固定 IP アドレスを割り当てるポートそれぞれについて，以下の形式を用いて設定情報を記述する．

```
hub-port portname{
  hub-ipaddress xxx.xxx.xxx.xxx;
  port-number "port";
  port-fixed-address xxx.xxx.xxx.xxx;
}
```

それぞれの項目に記述すべき内容は以下の通りである．

portname ポート固定 IP アドレスを割り当てるポートに対応する名前を記述する．用いることができる文字は英数字と"."であり，名前の先頭の文字は"."でなく，14 文字以内でなければならない．本システムの運用中，エラーメッセージなどはこの名前を用いて表示される．

hub-ipaddress ポート固定 IP アドレスを割り当てるポートが属しているハブの IP アドレスを記述する．

port-number 固定 IP アドレスを割り当てるポート名を記述する．

port-fixed-address 指定したポートに対して割り当てるポート固定 IP アドレスを記述する．

例えば，図 5 に示すように固定 IP アドレスを割り当てたい場合には，以下のように記述する．

```
hub-port hub1port1{
  hub-ipaddress 192.168.254.3;
  port-number "1";
  port-fixed-address 192.168.254.12;
}
hub-port hub2port6{
  hub-ipaddress 192.168.254.4;
  port-number "6";
  port-fixed-address 192.168.254.26;
}
```

5. 実　　装

本システムでは，DHCP のプロトコルを変更していない．ま

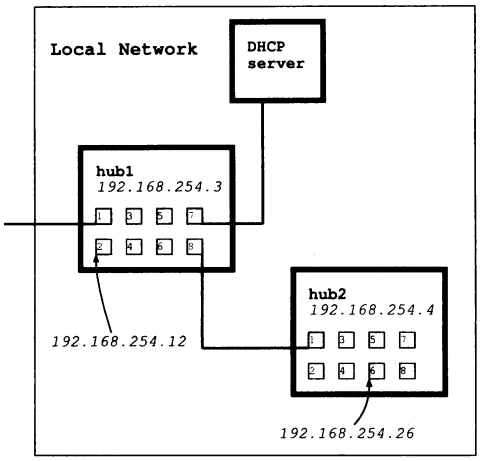

図 5　ポート固定 IP アドレスを割り当てる例

た，既存の DHCP からの変更点は，サーバの IP アドレスリースの方法のみである．そこで，実装にあたっては，既存のコードを改変することによりおこなった．

5.1 概　　要

本システムの実装は，Internet Systems Consortium(ISC) の DHCP3.0.2rc1 [9] のコードを修正することによりおこなった．このコードは広く流布されているものである．

既存のコードは C 言語で記述されているので，コードの修正にあたっては基本的に C 言語を用いた．ただし，ハブと通信して FDB を取得する機能は外部コマンドとして分離し、B シェルのスクリプトとして実装した．これにより、BRIDGE-MIB には非対応だが、telnet などを用いて FDB が取り出せるハブなどへの対応が容易になる。

本システムの内部仕様の設計，及び実際のコードの修正にあたっては，既存のコードの中にある，ホスト固定 IP アドレスをリースするためのコードの構成を参考にし，場合によってはそのまま利用した．まず，設定ファイルを解析する部分では，ホスト固定 IP アドレスの設定に関する字句解析コードを参考にし，利用している．また，設定情報をポートハッシュに保存する部分では，既存のハッシュ構造とその操作のための関数を利用している．さらに，クライアントから IP アドレス要求が送られてきた場合に，割り当てるべきポート固定 IP アドレスが存在するかを検索する部分についても，ホスト固定 IP アドレスを検索するためのコードを参考にし，利用している．

5.1.1 FDB 取得コマンド

本システムでは，ハブとのやり取りは外部コマンドを用いる．この動作を定義したものが，以下で記述するシェルスクリプトである．

シェルスクリプトの役割は，ハブリストに記述されたハブに対して，NetSNMP [10] で実装されている snmpwalk コマンドを用いることにより，ポートとそこに繋がれたクライアントの MAC アドレスの対応を取得し，それを解析することによりクライアントがどのポートに繋がっているかを調べることである．

DHCP サーバからは，外部コマンドとして以下の書式で呼び出される．

```
sh hub.sh chaddr hubipaddr1 hubipaddr2 ...
```

ここで，*chaddr* はクライアントの MAC アドレス，*hubipaddri* はハブリストにあるそれぞれのハブの IP アドレスである．クライアントが接続されているハブがあればそのハブから受け取った"*hubipaddr*．クライアントが接続されているポートの port 番号"を DHCP サーバに返す．また，どのハブにもクライアントが接続されていなかった場合は"nothing"を返す．

DHCP サーバは，このシェルスクリプトの実行結果をもとに固定ポート定義を検索する．

上記のシェルスクリプトはシステム本体 (C 言語で記述された部分) とは完全に独立している．そのため，ハブとの通信方法を変更したい場合はスクリプトの記述を差し替えるだけでよい．

6. 評　　価

本章では，既存の DHCP との比較をおこない，本システムの評価をおこなう．

6.1 機能の追加

本システムでは，既存の DHCP の機能に加えて，新たにポート固定 IP アドレスリース機能を使用できるようになった．これにより，個々のクライアントの物理的な位置を把握できるようになり，ネットワーク管理に役立つことになった．

6.2 実 行 時 間

本システムでは，ポート固定 IP アドレスリース機能を用いる場合，ハブとの通信をおこなうため，既存の DHCP と比べて実行時間が長くなるのを避けることはできない．本節では，本システムがクライアントから IP アドレス要求メッセージを受け取った場合の実行時間を，既存の DHCP の場合の実行時間と比較する．そして，クライアントからみた場合に，IP アドレス要求メッセージを送ってから IP アドレスをリースされるまでの時間が十分に許容範囲内であることを示す．

比較実験は，C 言語の gettimeofday 関数を用いてサーバの処理時間を計測することによりおこなった．ここで，サーバのリース時間とは，クライアントから IP アドレス要求メッセージが送られてきてから，それに対する処理を終えてクライアントにメッセージを返すまでの時間である．

実験に用いた機器は、表 1 である。

サーバ	DELL DIMENSION XPS D333 NetBSD/i386 2.0
ハブ	DELL PowerConnect 5224
クライアント	NEC Lavie Windows2000

表 1　実験に用いた機器

表 2 は，ポート固定 IP アドレスリース機能を用いなかった場合 (既存の DHCP) と，ポート固定 IP アドレスリース機能を用いた場合について，サーバの処理時間を比較したものである．それぞれの場合について，10 回ずつ試行した．

表 2 からわかるように，処理時間はポート固定 IP アドレス

処理時間 (秒)		既存の DHCP	ポート固定リース
IP アドレス新規要求	DHCPDISCOVER	0.002	0.269
	DHCPREQUEST	0.035	0.271
再要求	DHCPREQUEST	0.004	0.265

表 2 サーバの処理時間

リース機能を用いた場合のほうが長くなる．処理時間増加の原因はハブとの通信である．しかし，実際にクライアントが接続する場合を考えると，クライアントからのメッセージに対する処理時間に加えて，サーバ・クライアント間の通信時間，及びクライアントが IP アドレスをリースされてから様々な設定をおこなう時間がある．クライアントが IP アドレスを要求してから IP アドレスをリースされて設定を終えるまでの時間を計ってみたところ，IP アドレスの新規要求で約 4 秒，IP アドレスの再要求で約 1 秒であった．よって，クライアントが待つ時間という観点で考えると，表 2 の処理時間の違いは重要な問題とはならない．

この実験結果はハブを 1 台のみ用いた場合である．2 台以上用いる場合はハブからの情報の取得を並行実行する．よって，ハブが増えることによってリース時間が大幅に増加することは見込まれない．例えば，128 バイトのパケットを 100baseTX の store&forward 型ハブで中継したとすると，その時間は $128 \times 8/100 \times 10^6$(秒) $= 10.24$ (μ秒) 程度であり，図 2 の実験結果と比べた場合，大勢に影響はない．

また，同時に多数のクライアントが IP アドレスを要求した場合，処理は順におこなわれるため，クライアントによっては IP アドレスをリースされるまで待つことになる．クライアントの標準のタイムアウト時間は 60 秒であるので，同時に 100 台程度のクライアントが要求を出すような大規模なネットワークの場合，クライアントがタイムアウトする可能性がある．

6.3 設定ファイルへの記述

本システムでは，ポート固定 IP アドレスリース機能を用いる場合，設定ファイルに専用の記述を追加しなければならない．しかし，設定ファイルへの記述は設定を変更しない限り一度だけであるため，ユーザに大きな負担をかけるものではない．

7. ま と め

本研究では，ネットワーク管理者がクライアントの物理的な位置を特定できるように，DHCP サーバにポート固定 IP アドレスリース機能を追加した．これは，個々の情報コンセントに対して固定的に IP アドレスを割り当て，IP アドレスを要求するクライアントに対してその接続ポートに対応する IP アドレスをリースする機能である．

本システムでは，クライアントから IP アドレス要求メッセージが送られてきた場合に，サーバはハブの MAC アドレスフォーワーディングテーブル (FDB) を BRIDGE-MIB を通じて SNMP を使って入手する．さらに FDB をもとにクライアントの物理的な接続ポート番号を割り出し，ポート番号と設定ファイルの記述をもとに IP アドレスをリースする．

今後の改良点としては，ハブとの通信の時間を短縮することが考えられる．現在のシステムでは，サーバに 100 台程度のクライアントから同時に要求が来るとクライアントがタイムアウトする可能性がある．本システムをより大きなネットワークに適用するためには，ハブとの通信時間の短縮が重要になってくる．このため，FDB の取得情報をキャッシュしたり，複数の DHCP リクエストをまとめて FDB 上の検索を実施する，といった改善が考えられる．

謝 辞

本研究の一部は，科学研究費補助金基盤研究 (B)(2) 15300017 の援助による．

文 献

[1] 桝田 秀夫，中西 通雄：“セキュリティレベルに応じた校内情報コンセントシステムの構成法と運用例”，情報教育シンポジウム，Vol.2002，No.12，pp.31-36 (2002.08.21-23).
[2] 桝田 秀夫，鈴木 未央，中西 通雄：“PPPoE を用いた認証付き情報コンセントの実装と評価”，マルチメディア，分散，協調とモバイルシンポジウム (DICOMO)，Vol.2001，No.7，pp.379-384 (2001.06.28).
[3] 石橋 勇人，阪本 晃，山井 成良，安倍 広多，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 (2001.1).
[4] 丸山 伸，浅野 善夫，辻 斉，藤井 康雄，中村 順一：“既存の DHCP 端末で利用できる利用者にも管理者にも安全な情報コンセントシステムの構築”，情報処理学会研究報告 (99-DSM-14)，Vol.99，No.56，pp.131-136 (1999.7.15-7.16).
[5] Dynamic Host Configration Protocol, RFC2131.
[6] Simple Network Management Protocol, RFC1157/STD0015.
[7] Definitions of Managed Objects for Bridges, RFC1493.
[8] IEEE802.1Q - Virtual LANs, http://grouper.ieee.org/groups/802/1/pages/802.1Q.html.
[9] Internet Systems Consortium, INC., ISC DHCP, http://www.isc.org/sw/dhcp/.
[10] Net-SNMP package, http://www.net-snmp.org/.