動的IPアドレス環境下でのTCPコネクション継続方式の提案

藤田 謙† 村山 公保† 門林 雄基‡ 山口 英†

†奈良先端科学技術大学院大学 情報科学研究科
‡大阪大学 大型計算機センター

概要

本稿では、IPアドレスが動的に変化していくような環境下でもTCPコネクションを維持するTCPコネクション継続方式を提案する。TCPコネクション継続方式では、TCPコネクションを張った2つのホスト間で片方のIPアドレスが変わった場合でも、TCPを使った通信はIPアドレス変更前から変更後にかけて継続的に行うことが可能となる。この方式の実装例について述べるとともに今後の課題についても述べる。

1 はじめに

近年インターネットに接続されるコンピュータの数は飛躍的に増大している。さらに携帯型コンピュータの普及により、ネットワークへの接続形態も固定的なものだけではなく、さまざまな場所のネットワークへ接続を変えていくという動的な形態へと変わりつつある。

ネットワーク媒体も有線のものだけではなく、電波を利用した無線ネットワークや、IrDA(Infrared Data Association)に代表される赤外線通信のネットワークが登場している。ネットワークに接続される機器もコンピュータ以外のものが考えられる。これらの機器やネットワークを組み合わせて使うことにより、いつでも、どこでも、誰とでも通信できる環境が可能となりつつある。

従来のTCP/IPネットワークにおいては、各々のホストに対して静的にIPアドレスを割り当てていた。これを接続時に動的に割り当てる機構として、DHCP(Dynamic Host Configration Protocol)[1][2][3]が提案されており、ホストは割り当てられたIPアドレスを使用してネットワークに接続する。IPv6[4]では、オートコンフィグレーション機能が検討されており、またND(Neighbor Discovery)[5]によってグローバルなIPアドレスの割当が自動的に行われる仕組みが実現されようとしている。これらの方法で割り当てられるIPアドレスには有効期限があり、物理的にネットワークを移動しなくてもIPアドレスが変更されることがある。

TCPはインターネットの主要なプロトコルであるTCP/IPのトランスポート層のプロトコルであり、コネクション指向で信頼性のある通信を上位レイヤに提供している。TCPを使っているアプリケーションとして、具体的にはWWW(World Wide Web)、遠隔端末操作のためのtelnetや、ファイル転送のためのftp等がある。

大規模なLANを持つ事業所、研究所や大学では、ネットワークをサブネットワークに分割して運用している。IPアドレスのネットワーク部はこれらサブネットワーク間で異なっている。よって、他のホストと通信しながら構内を移動するためには、移動の先々のネットワークに対応したIPアドレスを再設定する必要がある。ネットワーク経由で他のホストと通信するアプリケーション、例えばtelnetやftpは、ネットワークを移る毎に一度その通信プロセスを終了し、移動先でIPアドレスを設定した後に改めてアプリケーション実行しなければならない。つまり、携帯型ホストを使ってtelnetで遠隔ホスト上の作業を継続しながらネッ

"A proposal of maintaining TCP connection in dynamic IP address Environments", FUJITA Ken†, MURAYAMA Yukio†, KADOBAYASHI Youki‡ and YAMAGUCHI Suguru†, †Graduate School of Information Science, Nara Institute of Science and Technology, ‡Computation Center, Osaka University

トワークを移動するということができない。

このようにネットワークを移動する等の理由でホストのIPアドレスが変わった場合、そのホストとの間に確立されていたTCPコネクションは切断されるという問題がある。

本稿では、IPアドレスが変わっても2つのホスト間でのTCPコネクションを維持するTCPコネクション継続方式について提案する。この方式では，新たにTCPオプションを定義し，このオプションを使用してIPアドレス変更情報を相手ホストに通知する。この方式に基づいて実装を行い，TCPコネクションを維持することができた。

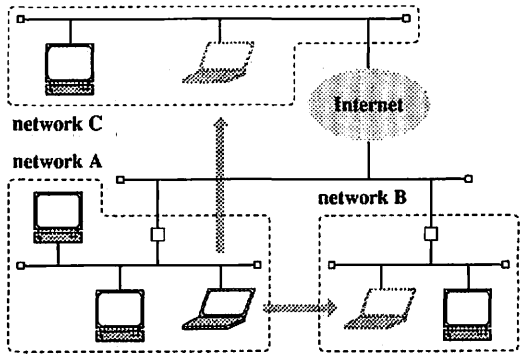

図1: ネットワーク上を移動するホスト

2 動的IPアドレス環境における問題と従来の研究

IPアドレスが他ホストとの通信中に動的に変わっていく環境下でTCPコネクションを維持するためには、各レイヤ毎に解決すべき問題がある。

TCPレイヤでは、変化する自ホストまたは相手ホストのIPアドレスに対応して、TCPコネクションの管理テーブルを更新していかなければならない。

IPレイヤでは、自ホストがどのネットワークと通信可能かを検出し、そのネットワーク上でのIPアドレスを取得しなければならない。さらに使用すべき自ホストのIPアドレスを決定し、それに併せて自ホストのIPアドレス情報や経路情報の更新をしなければならない。

データリンクレイヤでは、自ホストが物理的にどのネットワークと通信可能であるのかを検出する機能が必要である。特に移動ホストが無線ネットワークで接続している場合、この機能によりIPアドレス変更のきっかけがつくられる。

また、これらのレイヤ間インターフェースをどのように定義するかも問題である。

本稿では、特にTCPレイヤでの問題解決について議論する。

2.1 移動ホストからのアプローチ

TCP/IPネットワークであるインターネットでは、ネットワークに接続されたホストの識別にIPアドレスを用いている。同時にIPアドレスの上位ビットはネットワークの識別子になっている。よって、図1のようにホストが移動して別のネットワークに接続した場合にはそのネットワーク上のIPアドレスが必要となり、その結果移動前のホストとは別のホストとして識別されてしまう。この問題を解決するために、いくつかの提案が行われている。また、これらの方式は移動ホストだけでなく物理的にネットワーク上を移動しなくてもIPアドレスを変更するホストにも適用できる。

IETFのMobile-IP WGでは、本来ホストが属するネットワークと移動先のネットワークをトンネリングの技術を用いてつなぐことにより、ホームアドレスと呼ばれる移動ホストのIPアドレスを変更しないで通信するMobile IP[6]を提案している。この方式では、移動先でトンネリングの出口となるIPアドレスが必要である。

WIDEプロジェクトでは、従来のIPアドレスを接続位置の識別子としてとらえ、上位層に対してはホストの識別子であるVIPアドレスを別に定義し、両方のアドレスを対応させることで移動ホスト環境を実現するVIP(Virtual Internet Protocol)[7]を提案している。

Mobile IP方式では、ホームネットワークと移動先ネットワークの間をトンネリングするために、それぞれホームエージェントと訪問先エージェントと呼ばれるホストが必要である。

VIP方式では、ホストを識別するためのIPアドレスと位置を識別するためのIPアドレスの2つを必要とする。つまり、本来1つあればよいIPアドレスを2つ必要とするので、全てのホストが移

動するような環境を考えた場合実質的なアドレス空間は1/2になってしまう。

また、VIPアドレスとIPアドレスとの対応は、ホームルータと呼ばれるホストまたはルータで管理されている。

両方式とも、ネットワーク障害等の理由でこれらのホストやルータと移動ホストとの間で通信できない場合は、TCPコネクションを維持することができない。ホームエージェントやホームルータはホームネットワークにあって移動しないという前提があるので、ホームネットワークを持たないような移動ホストについては対応できない。

2.2 IPv6からのアプローチ

IPv6では、グローバルに使用できるIPアドレスはNDやオートコンフィグレーション機能により自動的に割り当てられる。各々のIPアドレスには使用期限があり、その期限後にIPアドレスが変わるような場合には、TCPコネクションを継続することはできない。この問題を解決するための提案も行われている。

Huitemaは、コネクションの識別をIPアドレスやポート番号で対応させるのではなく、コネクションを張る両ホスト間でPCB(Protocol Control Block)識別子を交換することでIPアドレスとは独立にコネクションを管理するmulti-homed TCP[8]を提案している。

Boundらは、IP層において拡張ヘッダを定義し、動的に変化するIPアドレス情報を交換するためのモデル[9]を提案している。

Huitemaの方法は、相手ポート番号、送信元ポート番号の代わりにPCB識別子を送受する。よって、途中経路に防火壁があった場合にポート番号によるパケット選択ができず、適切なセキュリティ管理ができない。

Boundの方法はIPパケットのヘッダ情報にIPアドレス変更通知を入れるので、制御が複雑になる。

3 TCPコネクション継続方式の提案

TCPコネクションは、相手アドレス、送信元アドレス、相手ポート番号、送信元ポート番号の4つが1組となって識別される。これらいずれかの値が異なっている場合、別のコネクションと識別される。これらの情報はコネクションが確立されている両方のホストのTCPで持っている。

これに着目し、コネクションを持っているホスト間で片方のIPアドレスが変わった場合、そのIPアドレスをTCPにおいても新しいものに更新することでTCPのコネクションを維持する方式、TCPコネクション継続方式を提案する。

3.1 従来の技術との違い

本稿で提案するTCPコネクション継続方式では、TCPコネクションを張っている2つのホスト間で情報を伝達し、ホームエージェント等の第3者を必要としない。よって、TCPコネクションを張っているホスト間の通信が可能であればTCPコネクションは継続できる。

また、本方式ではTCPヘッダ上のTCPオプションを使ってIPアドレス変更通知を実現し、IPプロトコルや他のトランスポート層プロトコルは使用していない。よって、途中の経路上でIPオプション等の制限があるルータを経由しても、そこでパケット破棄される危険性はない。

3.2 TCPコネクションを利用したTCPコネクション継続方式

IPアドレスが変わったホストは、自ホストのIP部からTCP部に対し送信元IPアドレスの変更通知を行う。この通知を受けたTCP部では、全てのコネクションについて送信元IPアドレスの変更処理を行うとともに、相手側ホストに対し送信元IPアドレスの変更を通知する。この送信元IPアドレスの変更通知を受けたホストのTCP部では、以後の通信は変更後の相手IPアドレスを使って行われる。

IPアドレス変更の後に通知を行うのは、IPアドレスを変更するホストは変更後の自分のIPアドレスが変更前には分からない場合があるからである。例えば、ネットワーク間を移動するようなホストでは、移動後のネットワークに接続してからそのネットワーク上のIPアドレスを得るので、移動前の段階で事前にそのIPアドレスを知るこ

とはできない。

IP アドレス更新通知は TCP コネクションを利用して行われる。ここで TCP を使うのは、IP アドレス変更の通知を必要とするホストは TCP コネクションを張っている相手ホストのみでよいからである。ネットワーク上の全ホストに IP アドレス変更通知を送るのは無駄である。なぜなら、IP アドレス変更のあったホストと通信していないホストの方が圧倒的に多いからである。また、IP 部では TCP コネクションが張られている相手ホストが分からないので、TCP コネクションのある相手ホストにだけ IP アドレスの変更通知が届くように TCP 部で通知することにした。

本稿で提案する TCP コネクション継続方式では、IP アドレスが変わった理由は問わない。また、手動によって、またはネットワーク間をホストが移動したことを検出する等によって移動したホストの IP アドレスを付け変えることができることを前提とする。

また、この方式の検討の段階で以下の制限を設けた。これらの制限については、今後の研究課題とする。

- 自ホスト IP 部の IP アドレス変更処理と経路情報変更処理はあるものとする。
- TCP コネクションを張った両側のホストが同時に移動することはない。
- アプリケーション層では、IP アドレスの情報を保持していない。
- UDP はコネクションレス型の通信であるので対象外とした。

3.3 TCP オプション～ADDRESS UPDATE～の追加

2 つのホストの間に張られたコネクション間で片方の IP アドレスが変わった場合、他方へその情報を伝えるために、新たに TCP ヘッダ上の TCP オプション、ADDRESS UPDATE を定義した。

ADDRESS UPDATE のフォーマットを図 2に示す。ここで、OLD ADDRESS フィールドには、IP アドレスを更新したホストの更新前の IP アドレスが入る。一方、新 IP アドレスは IP ヘッダの送信元アドレスに入っているので、このオプションに含める必要はない。

KIND= ADDRESS UPDATE	LEN=6	OLD IP ADDRESS
1byte	1byte	4bytes

図 2: ADDRESS UPDATE のフォーマット

この ADDRESS UPDATE を含むセグメントが TCP コネクション上を流れた場合、IP アドレスの変更がありそのセグメント以降は新しい IP アドレスにコネクションが移動したことを意味する。

3.4 IP アドレス変更の通知

ADDRESS UPDATE は、TCP コネクション毎に IP アドレスの変更のあったホスト側から送信されるセグメントに挿入される (図 3参照)。挿入のタイミングは、IP アドレス変更直後である。ADDRESS UPDATE を含むセグメントを受信した後に、相手ホストからのセグメントを受信したら、IP アドレス更新側のホストでは IP アドレス変更通知が相手ホストに到達したとみなす。相手ホストからのセグメントを一定時間内に受信しない場合は相手ホストに到達していないとみなし、ADDRESS UPDATE を含むセグメントを再送する。それでも一定時間内にセグメントを受信しない場合、TCP コネクションを切断する。

4 TCP コネクション継続方式の実装例

前章で説明した TCP コネクション継続方式を検証するために、NetBSD1.1 をベースとして実装を行った。

4.1 コネクション情報

TCP 部でコネクション情報を管理するテーブルは INPCB(Internet Protocol Control Block) と TCPCB(TCP Control Block) の 2 つあり、それらは互いにリンクしあっている (図 4参照)[10]。

INPCB には、TCP コネクションを識別するのに必要な情報、つまり相手アドレス、送信元アド

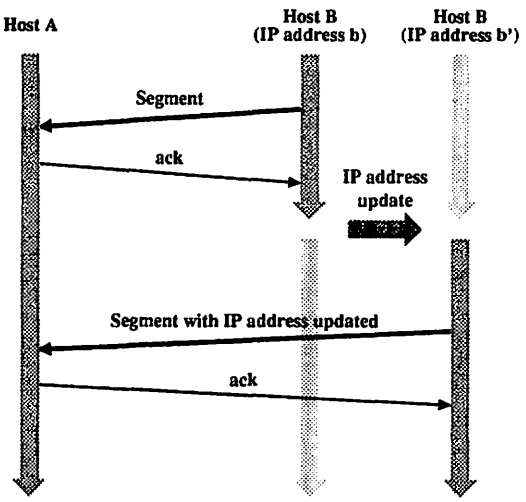

図 3: IP アドレス変更の通知

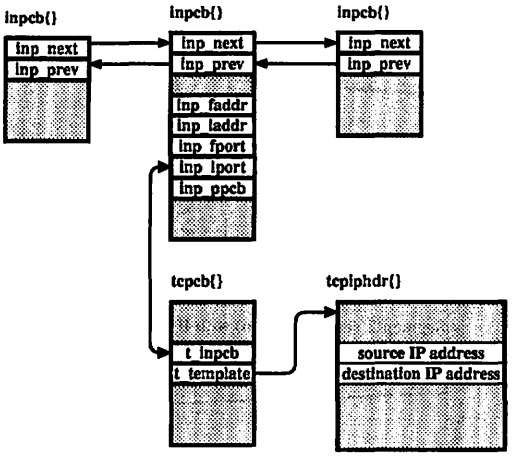

図 4: プロトコル制御ブロック

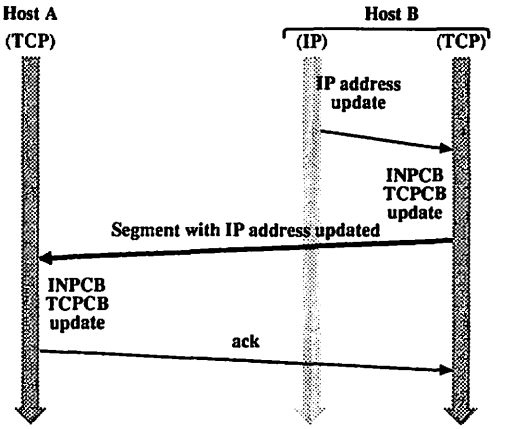

図 5: 処理概要

レス、相手ポート番号、送信元ポート番号の 4 つが含まれている。

TCPCB には、TCP コネクション特有の情報が含まれる。例えば、送信時にコピーされる TCP/IP ヘッダのテンプレートへのポインタがある。コネクション情報を変更する時は、INPCB だけではなく、このテンプレートに含まれる IP アドレス情報を変更している。

4.2 IP アドレス変更処理の概要

以下に IP アドレスを変更する TCP コネクションの両側のホストが行う処理を述べる (図5参照)。この処理により、2 つのホスト間で片方の IP アドレスが変更した後も、IP アドレスが変更する前の TCP コネクションの上で通信し続けることが可能となった。

4.2.1 自ホスト IP アドレス変更処理

自ホストの IP アドレスの変更自体は IP 部で行う。さらに、IP 部は使えなくなった旧 IP アドレスとそれに対応した新 IP アドレスの組を TCP 部に通知するようにする。これを受けた TCP 部では、必要なコネクション情報を更新する。旧 IP アドレスを送信元アドレスに持つ全ての INPCB については、送信元アドレスを新しい IP アドレスに更新する。また TCBCB 上で管理されている TCP/IP ヘッダテンプレート上の送信元アドレスも新 IP ア

ドレスに併せて更新する。これにより、以後のセグメントについては新IP アドレスで送受信できるようになった。

以上の更新の後に、TCP 部では相手ホストに対し送信元アドレスの変更を通知する。このために、新たに定義したTCP オプション、ADDRESS UPDATE を使用した。

4.2.2 相手ホスト IP アドレス変更処理

相手ホストから ADDRESS UPDATE を含むセグメントを受信することで、受信側ホストはこのTCP コネクションに関してはこのセグメント以降相手ホストのIP アドレスが変更したことを認識する。また、送信側の旧IP アドレスはこのADDRESS UPDATE 内のOLD ADDRESS であり、新IP アドレスはIP ヘッダの送信元アドレスに入っている。この旧アドレスに該当するTCP コネクションのTCB の相手IP アドレスを書き換える。また、TCBCB 上で管理されているTCP/IP ヘッダテンプレート上の相手アドレスも併せて新IP アドレスに更新する。これにより、以後のセグメントについては新IP アドレスで送受信できるようになった。

4.3 IP アドレス変更中のセグメント再送処理

旧IP アドレスを相手アドレスとするセグメントが途中のネットワーク上にあり、IP アドレス変更したホストに到達できなかった場合、このセグメントは行き先を無くしてしまう。よって、このセグメントの紛失を防止するために新IP アドレスに向けての再送が必要となる。

TCP には再送制御機構があるので、その仕組みを使うことで相手ホストからセグメント紛失することなく受信できる(図6, 図7参照)。具体的には、IP アドレス変更したホストからコネクションのある相手ホストにデータ送信の必要がない場合でも、TCP オプションのみを含むセグメントを送信することにより、相手ホストでIP アドレスの変更と新IP アドレスを知ることができるようにした。

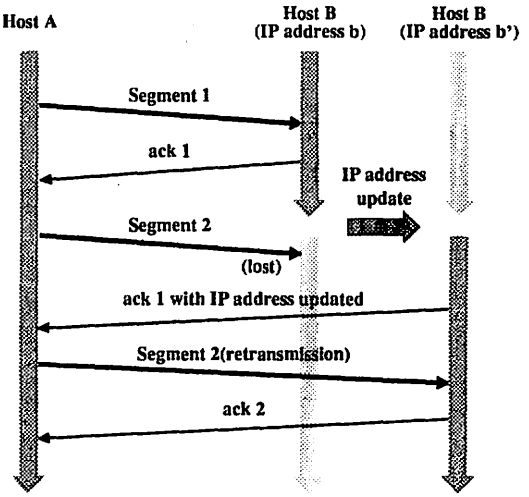

図 6: セグメント再送の例 1

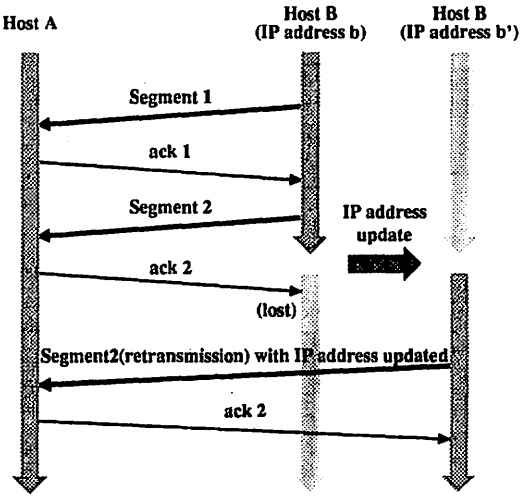

図 7: セグメント再送の例 2

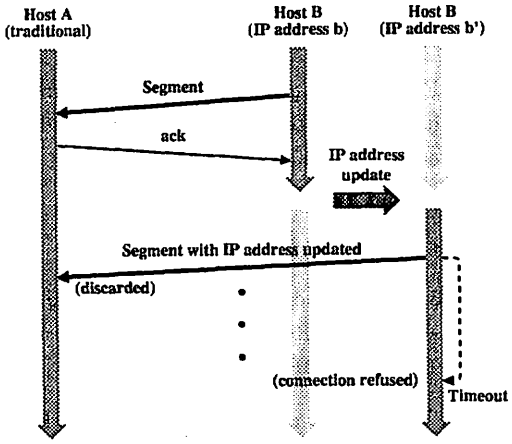

図 8: 従来の TCP との通信例

4.4 既存のホストと通信する場合

本稿で提案する TCP コネクション継続方式を実装していないホストと TCP コネクションがある場合、どちらのホストの IP アドレスが変わっても TCP コネクションを維持することはできずに切断されてしまう。例えば、TCP コネクション継続方式をサポートしている側の IP アドレスが更新され、かつ TCP コネクション上でセグメント送信している場合、セグメント自体は相手ホストに到達する。しかし、相手ホストでは ADDRESS UPDATE を解釈できないので、存在していない TCP コネクションへのセグメントと見なしてしまい破棄されてしまう (図8参照)。

ただし、これによる悪影響はなく、従来と同様 TCP コネクションがタイムアウトにより切断するだけである。

4.5 動作状況

検証のためのネットワーク構成を図9に示す。同一サブネットの Ethernet 上に、TCP コネクション継続方式に基づいて TCP を修正した 2 つのホストを置いた。TCP コネクションは telnet を利用した。また、IP アドレスの変更はコマンドラインからの入力とした。

以上の環境において、これらのホスト間に TCP コネクションを張った状態で一方の IP アドレスを変更し、TCP コネクションが維持できる事を確認した。

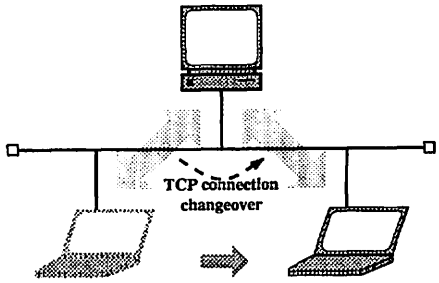

図 9: 検証ネットワーク構成

5 今後の課題

5.1 セキュリティ機構の導入

本稿で提案する TCP コネクション継続方式に基づいた TCP を用いることにより、セキュリティ機構の導入が必要となる。例えば、悪意のあるホストが他のホストが移動したように見せかけてそのホストの TCP コネクションを乗っ取ることができるからである。これを防ぐために、IP アドレスを更新したホストが以前と同じホストであることを TCP コネクションの反対側ホストで識別するための仕組みが必要となる。

この仕組みは、TCP コネクション設定時に暗号化したホストの ID をあらかじめ交換しておき、IP アドレス変更直後に互いにホスト認証を行うことで可能となる。ホストを識別するための ID をどのように定め、それを相手ホストにどのように通知すればよいか、検討しなければならない。

5.2 TCP タイマーの検討

TCP は信頼性のある通信を上位レイヤに提供しているが、それを実現しているのは一定時間内に相手側から応答がないことを検出する再送制御機構である。具体的には、送信側でセグメント送信毎にタイマーをかけ、その時間内に相手ホストより応答が得られなかった場合にセグメント紛失とみなし、該当するセグメントの再送を行う。IP アドレスが変化するような環境では、今までのタイマーの値が短すぎることが予想される。従来コネ

クションが維持できなくなったとみなして切断していたものをIPアドレスの変更中とみなし、さらに一定時間応答が得られない場合をコネクション維持できなくなったとみなすことが必要である。このためのタイマー値をどのくらいにしてサスペンド・リジューム機能を実現するかを検討しなければならない。

6 まとめ

本稿では動的IPアドレス環境下でのTCPコネクション継続方式について提案した。また、この方式を検証するために実装を行った。その結果、この方式に基づいてIPアドレスを変更してもTCPコネクションが維持できることを示した。今後、さらに上記の課題について検討し、実装および評価を行う予定である。

謝辞

本研究を進めるにあたり、議論、助言をしていただいた奈良先端科学技術大学院大学 情報ネットワーク講座の皆様に感謝致します。また、研究の機会を与えて下さった日本電気(株) 交換ソフトウェア技術本部の皆様に感謝致します。

参考文献

[1] R. Droms: "Dynamic Host Configuration Protocol", RFC 1541 (1993).

[2] R. Drams and S. Alexander: "DHCP Options and BOOTP Vendor Extensions", RFC 1533 (1993).

[3] 富永, 寺岡, 村井："動的ホスト設定プロトコル(DHCP)の実装の評価", 情報処理学会マルチメディア通信と分散処理ワークショップ論文集 (1993).

[4] S. Deering and Hinden: "Internet Protocol, Version 6 (IPv6) Specification", RFC 1883 (1995).

[5] T. Narten, E. Nordmark and W. Simpson: "Neighbor Discovery for IP Version 6 (IPv6)", RFC 1970 (1996).

[6] C. Perkins: "Internet Draft — IP Mobility Support" (1996).

[7] F. Teraoka and M. Tokoro: "Host Migration in Virtual Internet Protocol", Proceedings of Inet'92 (1992).

[8] C. Huitema: "Internet Draft — Multi-homed TCP" (1995).

[9] J. Bound and P. Roque: "Internet Draft — Dynamic Reassignment if IP Address for TCP and UDP" (1996).

[10] G. R. Wright and W. R. Stevens: "TCP/IP Illustrated, Volume 2", Addison-Wesley Publishing Company,Inc. (1995).