情報処理学会論文誌 Vol. 50 No. 10 2543–2555 (Oct. 2009)

プライベートアドレスによるネットワークモビリティを実現するMobile NPCの提案

坂本順一[†1,*1] 鈴木秀和[†1,†2] 伊藤将志[†1,*1]
宇佐見庄五[†1] 渡邊晃[†1]

ネットワーク自体が移動しても，ネットワーク内のノードと外部ノードの通信を継続できるネットワークモビリティの要求が高まっている．移動透過性の研究はこれまでIPv6を中心に行われてきており，ネットワークモビリティも同様である．しかし，IPv4は今後も使われ続けてゆくものと考えられ，IPv4においてそれを実現することも重要な課題である．IPv4対応のネットワークモビリティの代表技術として，IPv4 Network Mobility Extensions for Mobile IPv4（RFC5177）があるが，ネットワーク内のアドレスがプライベートアドレスであると利用できず，IPv4のグローバルアドレス枯渇問題に対応できない．本論文では上記の課題を解決するための技術としてMobile NPC（Mobile Network to Peer Communication）を提案する．Mobile NPCは，IPv4においてエンドノードだけで移動透過性を実現することができるMobile PPC（Mobile Peer to Peer Communication）と，エンドノードとルータに機能追加することによりNAT越えを実現することができるNAT-f（NAT-free protocol）を組み合わせた技術である．Mobile NPCは，移動するネットワークの中がプライベートアドレスでよく，エンドエンドの通信を維持したまま移動透過性を実現することができる．Mobile NPCをFreeBSDに実装して評価した結果，想定した動作を実行でき，中継によるオーバヘッドもほとんどないことを示すことができた．

A Proposal of Mobile NPC Realizing Network Mobility with Private Addresses

Junichi Sakamoto,[†1,*1] Hidekazu Suzuki,[†1,†2]
Masashi Ito,[†1,*1] Shogo Usami[†1]
and Akira Watanabe[†1]

The demand for network mobility, whereby communications are maintained even when the network moves, is increasing these days. While researches on the mobility have been thus far conducted mainly with IPv6, IPv4 will also continue to be used in future, and the realization of mobility with IPv4 remains an important issue. IPv4 Network Mobility Extensions for Mobile IPv4 (RFC5177) is a technology that realizes network mobility with IPv4. However, as the addresses in their network need to be global ones, it does not solve the problem of exhausting IPv4 global addresses. In order to solve the above problem, we propose, in this paper, "Mobile Network to Peer Communication (Mobile NPC)" which is the combination of technologies for Mobile PPC and NAT-f. Mobile NPC can realize network mobility by using private IP addresses. We have implemented Mobile NPC on FreeBSD and have demonstrated its good performance.

1. はじめに

無線LANやインターネットの急速な普及により，ノードが移動しながら通信できる環境が要求されている．しかしIPネットワークでは，通信中のノードが移動するとIPアドレスが変化するため，通信を継続することができない．そこで，移動によってIPアドレスが変わっても通信を継続できる移動透過性の研究が行われている[1]．また，電車内や自動車内にIPネットワークを構築し，そのネットワーク自体が移動するというケースも考えられる．この場合は，ネットワークの境界に位置するルータが複数のノードに代わって移動透過機能を実行し，ネットワーク内のアドレスはそのまま維持する方法が検討されている．これはネットワークモビリティと呼ばれ，移動にかかわる制御情報を減らし，かつ通信の中断時間を最小限にできる効果がある．

IP層で移動透過性を実現するプロトコルとして，IPv4対応にはMobile IP[2]，Mobile PPC（Mobile Peer to Peer Communication）[3]，IPv6対応にはMobile IPv6[4]，LIN6（Location Independent Networking for IPv6）[5]，MAT（Mobile IP with Address Translation）[6]などが提案されている．また，これらの技術を利用してネットワークモビリティを実現させた技術として，IPv4対応にはNetwork Mobility Extensions for Mobile IPv4（以下NEMOv4）[7]，IPv6対応にはNetwork Mobility Basic Support Protocol（以下NEMOv6）[8]，χLIN6-NEMO[9]，MAT-MONET[10]などが提案されている．ネットワークモビリティを含む移動

†1 名城大学大学院理工学研究科
Graduate School of Science and Technology, Meijo University
†2 日本学術振興会特別研究員PD
Research Fellow of the Japan Society for the Promotion of Science
*1 現在，株式会社東芝
Presently with Toshiba Corporation

透過性の研究は，これまで将来 IPv6 の時代がくることを見越して IPv6 を前提としたものが多かった．しかし，IPv6 は予想していたような普及をしておらず，仮に IPv6 が普及を始めたとしても当分の間は IPv4 と IPv6 の共存環境になると考えられる．したがって IPv4 においても移動透過性を実現できることは意義がある．

IPv4 に対応した既存のネットワークモビリティ技術として，前述のように NEMOv4 があるが，移動ネットワーク内はグローバルアドレスでなければならないという前提がある．IPv4 ではアドレス枯渇の問題が深刻であり，移動ネットワーク内はプライベートアドレスを使用できることが望ましい．プライベートアドレスはアドレスの取得が不要で，アドレス管理が容易であるという利点もある．ところが，ネットワーク内がプライベートアドレス空間であると，外部ネットワークから内部ネットワークのアドレスが隠蔽された形となり，外部ネットワークのノードから内部ネットワークのノードへの通信開始ができない．これは NAT 越え問題と呼ばれており，IPv4 の汎用性を損なう大きな要因となっている．

NAT 越え問題を解決する技術は様々な方式が検討されている．たとえば，外部のグローバルネットワーク上に STUN サーバを設置し，内部ノードと STUN サーバが連携して NAT テーブルを生成する STUN（Simple Traversal of User Datagram Protocol Through Network Address Translators）[11]，内部ノードと NAT が連携して NAT テーブルを生成する UPnP [12]，waypoint と呼ばれるサーバと NAT が連携する AVES（A Waypoint Service Approach to Connect Heterogeneous Internet Address Spaces）[13]，外部ノードと NAT が連携する NAT-f（NAT-free protocol）[14] などがある．いずれも連携する装置を改造することが前提である．NAT 越え技術と移動透過性を融合した技術としては文献 15)，16) などがあるが，ノード側が移動することを想定したものであり，プライベートアドレスのネットワークが移動する研究例は筆者らの知るところまだない．NAT 越えと融合したネットワークモビリティを実現できれば，プライベートアドレス空間のネットワークの移動が可能となり，きわめて有用であると考えられる．

そこで，本論文では上記要求を満たす通信プロトコルとして Mobile NPC（Mobile Network to Peer Communication）を提案する．Mobile NPC は Mobile PPC と NAT-f を融合させた技術である．一般に移動透過性を実現するには，通信中に一方のノードが移動しても通信を継続できる通信継続性と，相手ノードがどこにいても通信の開始ができる移動ノード到達性の両者の機能を満たす必要がある．Mobile PPC は，特殊なサーバを利用することなくノード単位の通信継続性をエンドエンドで実現する技術であり，この技術をベースに通信継続性を実現する．NAT-f は特殊なサーバを利用することなく NAT 越えを実現できる技術であり，この技術をベースに移動ノード到達性を実現する．

Mobile NPC を FreeBSD 上に実装し，プライベートアドレスを用いたネットワークモビリティを実現できることを確認した．評価の結果，スループットの低下はほとんど見られず，移動時のパケットロスも十分小さくできることが分かった．

以下，2 章で Mobile PPC と NAT-f について記述し，3 章で Mobile NPC の要求条件と動作の詳細を記述する．4 章で Mobile NPC の実装，5 章で評価の結果を述べる．最後に 6 章でまとめる．

2. Mobile PPC と NAT-f

以下に，Mobile NPC のベースとなる Mobile PPC と NAT-f の概要を述べる．本論文で用いる記号を以下に定義する．

- Gn：グローバルアドレス（$n = 1, 2, 3, \cdots$）
- Pn：プライベートアドレス（$n = 1, 2, 3, \cdots$）
- Vn：仮想アドレス（$n = 1, 2, 3, \cdots$）
- s, d：送信元ポート番号，宛先ポート番号
- m：NAT の外部ポート番号
- $A \leftrightarrow B$：A と B 間の通信
- $A \rightarrow B$：A から B への通信
- $A \Leftrightarrow B$：A と B のアドレス変換

2.1 Mobile PPC

Mobile PPC は，エンドエンドで移動透過性を実現する方式であり，移動ノード到達性と通信継続性を明確に分離した点に特徴がある．移動ノード到達性には DDNS（Dynamic DNS）[17] サーバを利用し，通信継続性に関わる機能を Mobile PPC で実現する．

図 1 に Mobile PPC の処理を示す．MN と CN は DDNS サーバを利用して通信相手の名前解決後，IP アドレス $G1$ と $G3$ で通信を開始するものとする（$G1 \leftrightarrow G3$）．MN と CN は IP 層内にアドレス変換テーブル CIT（Connection ID Table）を保持している．CIT はパケットの IP アドレスの移動前と移動後の対応関係を記録したテーブルである．通信開始時点では，CIT の内容は以下のようになっている．

$$\{G1 \Leftrightarrow G1\} \leftrightarrow \{G3 \Leftrightarrow G3\}$$

ここで，“⇔” の両側は移動前と移動後の IP アドレスの関係を示す．MN が移動する前は，両側の値は同じであり，アドレス変換は行われないことを意味する．

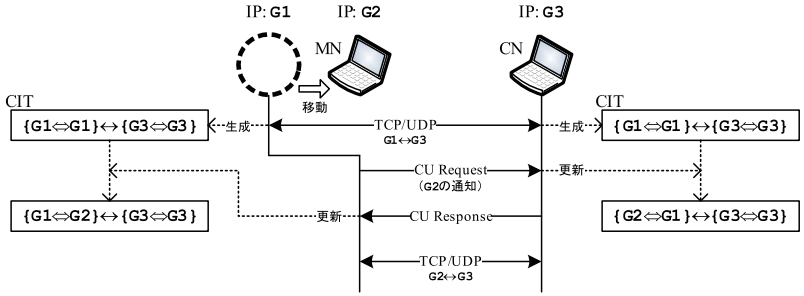

図 1　Mobile PPC の基本処理
Fig. 1　Basic operation of Mobile PPC.

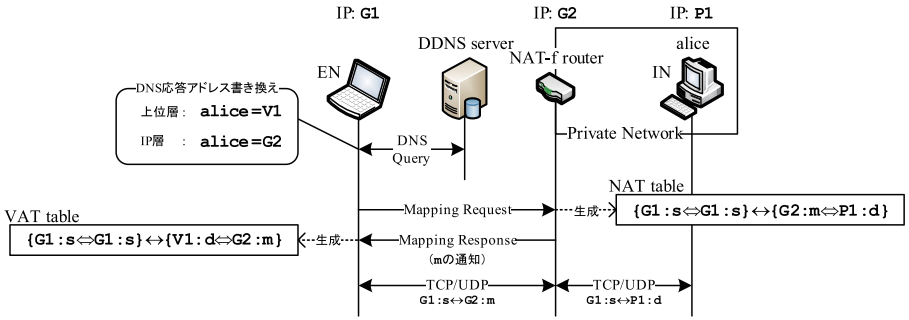

図 2　NAT-f の基本処理
Fig. 2　Basic operation of NAT-f.

MN が通信中に移動して，IP アドレスが $G1$ から $G2$ に変わると，MN と CN は CU（CIT Update）Request と CU Response による移動通知ネゴシエーションを行い，CIT を以下のように更新する．

$\{G1 \Leftrightarrow G2\} \leftrightarrow \{G3 \Leftrightarrow G3\}$

CIT 更新後は全パケットに対し，MN と CN はそれぞれ IP 層において，CIT に基づきアドレス変換を行う．たとえば，CN 側で上位層から送信元 $G3$，宛先 $G1$ として送信指示されたパケットは，IP 層において，送信元 $G3$，宛先 $G2$ に書き換えられてネットワーク上に送信される．CN の上位層は MN の IP アドレスが変化していないように見えるため，コネクション ID が維持され，IP 層以下においては実際の IP アドレスによる通信となり，移動透過性を実現できる．

なお，CIT の内容は，TCP の場合は 24 時間，UDP の場合は 300 秒間通信がない場合に消去する．タイマの設定方法は一般の NAT 装置における NAT テーブルの消去方法に準じている．

2.2　NAT-f

NAT-f はインターネット上の外部ノードと NAT に機能を追加して，NAT 越え通信を実現するプロトコルである．NAT-f を実装することにより，通信ノードはグローバルアドレスとプライベートアドレスの違いを意識することなく，相互に通信を開始することができる．そのため，両アドレス空間が混在した環境下において，移動ノード到達性を実現できる技術として位置づけることができる．ここで，本論文における NAT とは，ポート番号の変換も行う NAPT（Network Address Port Translator）[18] を含むものとする．

図 2 に NAT-f の処理を示す．NAT-f 機能を実装したルータを NAT-f ルータと呼び，NAT-f ルータの外部および内部ネットワークに存在するノードをそれぞれ EN（External Node），IN（Internal Node）と表記する．DDNS サーバには IN の FQDN（Fully Qualified Domain Name）と NAT-f ルータのグローバルアドレス $G2$ を関連付けて登録しておく．また，NAT-f ルータは配下の IN のホスト名 *alice* とプライベートアドレス $P1$ の対応関係をあらかじめ保持している．

EN は DDNS サーバに IN の名前解決を依頼すると，DDNS サーバは NAT-f ルータのグローバルアドレス $G2$ を応答する．応答を受信した EN はカーネル内の IP 層においてこのパケットをフックし，NAT-f ルータのグローバルアドレス $G2$ を仮想アドレス $V1$ に書き換えて上位層に渡す．仮想アドレスの内容は，実ネットワーク上に存在せず，かつ EN の内部で重複しないような任意のアドレスを選ぶ．仮想アドレスとは NAT-f ルータ配下のどの IN と通信するのかを区別するために用いる仮想的なアドレスである．

次に，EN は仮想アドレス宛の通信 “$G1 : s \rightarrow V1 : d$” を開始する．このとき EN は最初の送信パケットをカーネル内に待避し，NAT-f ルータに対して Mapping Request/Mapping Response によるネゴシエーション処理を実行する．Mapping Request には，EN が送信しようとしていた通信パケットのコネクション ID（送信元/宛先 IP アドレスとポート番号，およびプロトコルタイプの組）と，$V1$ に対応するホスト名 *alice* が記載されている．NAT-f ルータは受信したこれらの情報と *alice* のプライベートアドレス $P1$ を用いて，強制的に以下のような NAT テーブルを生成する．

$\{G1 : s \Leftrightarrow G1 : s\} \leftrightarrow \{G2 : m \Leftrightarrow P1 : d\}$

ここで，m は NAT-f ルータが動的に割り当てた外側ポート番号である．この NAT テーブルによると，NAT-f ルータ宛パケットの宛先 IP アドレスとポート番号は，$G2:m$ から $P1:d$ に変換されて中継される．外部ポート番号 m の値は Mapping Response により，EN に通知される．EN がこの通知を受信すると，仮想アドレスと上記ポート番号の対応関係を記録した仮想アドレス変換（VAT; Virtual Address Translation）テーブル

$$\{G1:s \Leftrightarrow G1:s\} \leftrightarrow \{V1:d \Leftrightarrow G2:m\}$$

を IP 層内に生成する．

EN から IN への通信パケットは，EN の VAT テーブルおよび NAT-f ルータの NAT テーブルに基づいて，宛先 IP アドレス・ポート番号が変換される．すなわち，EN は NAT-f ルータで生成された NAT テーブルに合わせて，パケットのアドレスとポート番号を変換することにより，通信の開始が可能となる．以降のすべての通信パケットに対して，VAT テーブルと NAT によるアドレス・ポート変換が行われる．

IN 側から EN へ通信が開始される場合については，既存の NAT 経由の通信とまったく同様の動作が行われる．すなわち，NAT によるアドレス・ポート変換のみが実行される．

NAT-f ネゴシエーションは ICMP Echo Request 上で定義されている．EN が送信した Mapping Request は，NAT 側が NAT-f に対応していない場合，ICMP Echo Reply として NAT から返送される．この応答を判断することにより，EN は相手が NAT-f に対応しているかどうかを判断できる．NAT が NAT-f 機能を持たない場合は EN から IN に向けての通信開始はできない．

なお，VAT テーブルの内容を消去するタイミングは，2.1 節で説明した CIT と同様の考えに基づいている．

3. Mobile NPC

3.1 要求条件

ここでは，IPv4 におけるネットワークモビリティを実現するために必要となる要求条件を整理する．利用場面としては，ユビキタスネットワークの代表的アプリケーションとして，IP 電話を想定する．ユーザはバス，電車のような移動ネットワーク内におり，外部のグローバルアドレス空間の端末と IP 電話で通話を行う．移動ネットワーク内はプライベートアドレス空間であるものとする．そのため，ネットワーク管理者は移動ネットワーク内のグローバルアドレスを取得する必要がない．ネットワーク境界部分の NAT 装置のみがグローバルアドレスを保持することによりグローバルアドレスの枯渇を防止する．

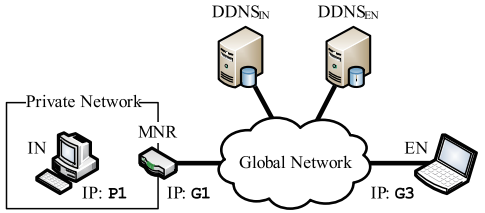

図 3　Mobile NPC のネットワーク構成
Fig. 3　Network configuration of Mobile NPC.

上記システム構成において，以下のような要求条件を設定する．

(1)　外部端末 EN と内部端末 IN は，互いに通信の開始が可能である．

(2)　通話中にネットワークが移動しても通信中のセッションが継続できる．

(3)　通信は移動前後にかかわらずエンドエンドでかつ高速な通信が可能である．

(1) を実現するには，EN からの通信開始において NAT 越え問題を解決する必要がある．本提案では NAT-f の原理を適用することによりこれを解決する．(2) を実現するにはネットワークモビリティ技術が必要となるが，本提案では Mobile PPC の原理を適用することによりこれを解決する．なお，同様のシステム構成のもとで，通信中に EN 側が移動する場合については，実現方法がすでに明確になっており[15),16)]，本論文の記述範囲から除外する．(3) を実現するには，NAT 越えと移動透過性をいずれもエンドノードだけで実現できる必要がある．STUN などの既存の NAT 越え技術や，NEMOv4 などの既存のネットワークモビリティ技術では，通信経路が第 3 の装置を経由するため最適化されていない場合が多く，経路の冗長が発生する．このようなオーバヘッドは IP 電話などのエンドエンド間のリアルタイム通信には適さない．本提案では NAT-f と Mobile PPC がともにエンド端末だけで実現する方式であるため，移動の前後においてエンドエンドの通信を維持することができる．

3.2 動作概要

図 3 に Mobile NPC のネットワーク構成を示す．ネットワークモビリティを実現するルータを MNR（Mobile NPC Router）と呼ぶ．移動ネットワーク内は IPv4 のプライベートアドレス空間とし，複数の IN が存在できる．DDNS サーバは既存のシステムをそのまま利用する．EN，IN はそれぞれの DDNS サーバ DDNS$_{EN}$，DDNS$_{IN}$ に通信開始時に必要となる IP アドレスを登録しておく必要がある．DDNS サーバへの登録とその更新方法については，3.3 節で述べる．MNR，IN および EN には Mobile NPC の機能を実装する．

MNR と EN はそれぞれ移動可能で，MNR 配下の IN と EN が通信することを想定する．

ここで，IN が移動し MNR 配下と外部ネットワークとの間を移動することも考えられるが，これには別の仕組みが必要であり，本論文では検討の対象としない．この方法の実現については，たとえば文献 15)，16) で検討されている．

Mobile NPC では Mobile PPC の CIT と，NAT-f の VAT テーブルを統合し，ECIT（Extended CIT）を定義する．ECIT は通信開始時のコネクション ID と，アドレス・ポート番号の変換関係を示す情報からなっており，3.4 節以降でその内容を記述する．

Mobile PPC は通信継続性と移動ノード到達性の実現を明確に分離し，移動ノード到達性については既存の DDNS の仕組みをそのまま利用した点が大きな特徴である．Mobile PPC そのものは通信継続性を実現するプロトコルである．NAT-f は移動ノード到達性にかかわる機能であり，両者の機能分担は比較的容易に実現できる．多くの移動透過性技術では通信継続性と移動ノード到達性の機能が一体となっており，NAT 越え技術と機能を融合するには多くの検討が必要になる．しかし，Mobile PPC と NAT-f は機能分担が明確であり，本論文に述べるように最小限の変更で組合せが可能である．

Mobile NPC は通信を開始する方向により，生成される ECIT の内容と，以後の通信手順が異なるという特徴がある．これは EN から通信を開始する場合は，EN において NAT テーブルに合わせてアドレス・ポート番号を変換する必要があるためである．逆方向についてはこのような変換は不要である．以下に DDNS サーバへの登録・更新方法，通信開始の方向に対応したアドレス変換の様子について述べる．

3.3　DDNS への登録と更新

EN，IN は自身の FQDN と現在の IP アドレスの対応関係を，各々の DDNS サーバに登録する必要がある．ここで，EN，IN とそれぞれの登録先 DDNS サーバとの間には信頼関係があり，DDNS 登録や更新に TSIG（Transaction Signature）[19]，または SIG(0) [20] の認証の仕組みを利用できるものとする．EN は移動してアドレスが変わると，$\mathrm{DDNS_{EN}}$ に新 IP アドレスを報告し，内容を更新する．登録に利用する DDNS Update パケットには，あらかじめ DDNS サーバと共有している共通鍵を用いた署名がなされ，安全に登録処理を行うことができる．以上の処理は一般の DDNS Update と同様である．

IN の DDNS 登録処理を以下に示す．IN の IP アドレスは，MNR が内蔵する DHCP サーバから取得する．この IP アドレス $P1$ はプライベートアドレスのため，IN は DDNS サーバに登録するために，MNR のグローバルアドレス $G1$ を取得する必要がある．MNR のアドレスは移動により変化する可能性があるため，定期的にまたはアドレスが変化した時点で内部ネットワークにブロードキャストしてその旨を IN に伝える．IN はこれを受けて，

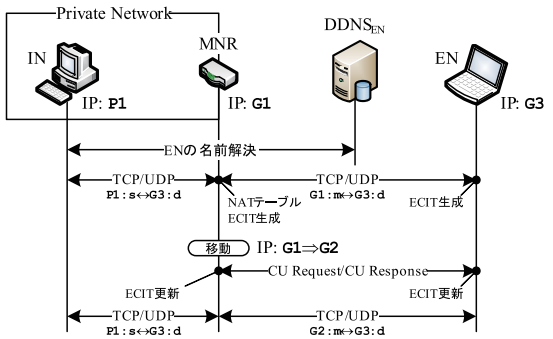

図 4　IN から EN へ通信を開始する場合のシーケンス
Fig. 4　A sequence in case the communication starts from IN to EN.

MNR のアドレスが変化したときに，$\mathrm{DDNS_{IN}}$ に対して DDNS Update パケットを送信し，MNR のグローバルアドレスを自身の IP アドレスとして登録する．

3.4　IN から EN に通信を開始する場合

3.4.1　通信開始時の処理

図 4 に IN から EN に通信を開始し，通信中に MNR が移動した場合のシーケンスを示す．通信開始時の処理は，一般の NAT を介した通信と変わらない．すなわち，IN は EN の FQDN を用いて DNS 名前解決を行い，EN の IP アドレス $G3$ を取得する．

次に，IN は EN に通信パケット “$P1 : s \rightarrow G3 : d$” を送信する．このパケットを受信した MNR は，送信元アドレスを IN のプライベートアドレス $P1$ から MNR のグローバルアドレス $G1$ に変換する NAT テーブル

$$\{P1 : s \Leftrightarrow G1 : s\} \leftrightarrow \{G3 : d \Leftrightarrow G3 : d\}$$

を生成する．パケットは NAT テーブルに従ってアドレス変換され，EN に送信される．さらに，MNR と EN の IP 層内に以下のような ECIT

$$\{G1 : m \Leftrightarrow G1 : m\} \leftrightarrow \{G3 : d \Leftrightarrow G3 : d\}$$

を生成し，通信を開始する．この時点ではアドレス変換前と後の値が同じであり，結果的にアドレスは変換しないということを意味する．

図 5 に IN から EN への通信開始後の ECIT および NAT テーブルの内容と，パケットのアドレスとポート番号が変化していく様子を示す．この時点では NAT によるアドレス・ポート変換だけが実行される．

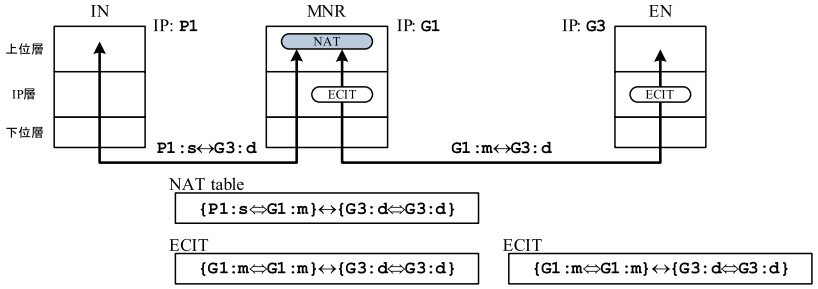

図 5　IN から通信開始後の IP アドレスとポート番号
Fig. 5　IP addresses and port numbers in case the communication starts from IN.

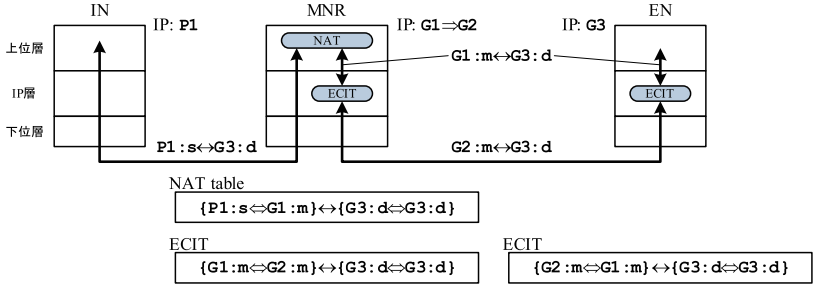

図 6　MNR が移動したときの IP アドレスとポート番号（IN から EN への通信開始後）
Fig. 6　IP addresses and port numbers after moving MNR (In the case communication starts from IN).

3.4.2　MNR 移動時の処理

通信中に移動ネットワークが移動して，MNR のグローバルアドレスが $G1$ から $G2$ に変わると，図 4 示すように MNR と EN の間で移動通知処理が行われる．MNR と EN の ECIT は CU Request/CU Response のシーケンスにより，

$$\{G1 : m \Leftrightarrow G2 : m\} \leftrightarrow \{G3 : d \Leftrightarrow G3 : d\}$$

のように更新される．このとき，NAT テーブルにはいっさい影響がない．

図 6 に MNR 移動後の ECIT および NAT テーブルの内容と，パケットのアドレスとポート番号が変化していく様子を示す．IN から EN へパケットが送信されると，MNR は NAT テーブルを参照して，送信元アドレスとポート番号を $P1 : s$ から，MNR の移動前のグローバルアドレスと割り当てたポート番号 $G1 : m$ に変換し，IP 層へ渡す．MNR の IP 層では

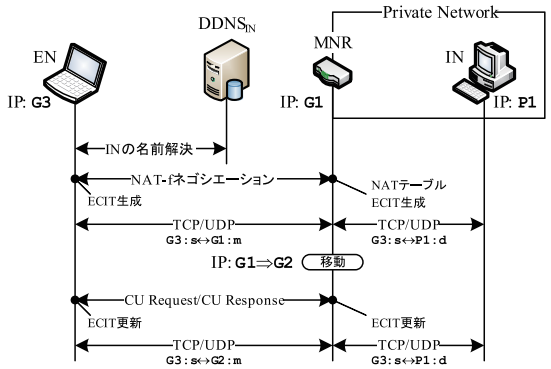

図 7　EN から IN へ通信を開始する場合のシーケンス
Fig. 7　A sequence in case the communication starts from EN to IN.

ECIT に基づくアドレス変換処理が行われ，送信元アドレスが移動後のアドレスに変換される．最終的に，IN から送信されたパケットは，“$G2 : m \rightarrow G3 : d$” となって EN へ送信される．EN は ECIT を参照して，パケットの送信元アドレスを $G2$ から $G1$ へ変換してから上位層へ渡す．

このようにして，パケットは正しくルーティングされ，かつ EN および MNR の上位層には，MNR のアドレスの変化が隠蔽される．逆方向のパケットは上記と逆の変換が行われる．

3.5　EN から IN に通信を開始する場合

3.5.1　通信開始時の処理

図 7 に EN から IN に通信を開始し，通信中に MNR が移動した場合のシーケンスを示す．EN は IN の FQDN を用いて DNS 名前解決を行い，MNR のグローバルアドレス $G1$ を取得する．ここで，EN は IP 層において取得した MNR のグローバルアドレスを仮想アドレス $V1$ に書き換えて，上位層に渡す．すなわち，EN の上位層は，IN のアドレスを仮想アドレス $V1$ と認識する．本処理の内容は NAT-f におけるそれと同様である．

次に，EN は仮想アドレス宛の通信 “$G3 : s \rightarrow V1 : d$” を開始する際，IP 層においてこの通信開始パケットをカーネル内に一時的に待避した後，MNR に対して NAT-f ネゴシエーションを実行する．Mapping Request には，待避した通信パケットのコネクション ID と通信相手 IN の FQDN の各情報が記載され，MNR に送信される．MNR は受信した情報

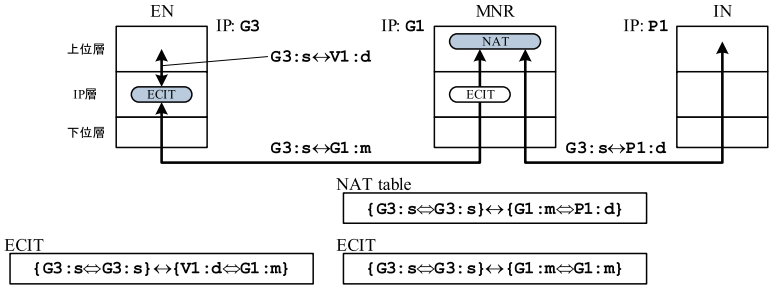

図 8　EN から通信開始後の IP アドレスとポート番号
Fig. 8　IP addresses and port numbers in case the communication starts from EN.

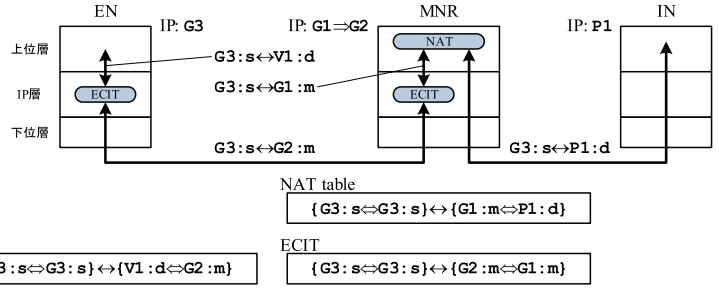

図 9　MNR が移動したときの IP アドレスとポート番号（EN から IN への通信開始後）
Fig. 9　IP addresses and port numbers after moving MNR (In the case communication starts from EN).

と，保持していた IN の FQDN と IP アドレスの対応情報から，強制的に NAT テーブル

$$\{G3 : s \Leftrightarrow G3 : s\} \leftrightarrow \{G1 : m \Leftrightarrow P1 : d\}$$

を生成する．MNR は NAT テーブル生成後，動的に割り当てた外側ポート番号 m を EN に通知する．この通知を受信した EN は，仮想アドレスと通知されたポート番号の変換関係を示す ECIT

$$\{G3 : s \Leftrightarrow G3 : s\} \leftrightarrow \{V1 : d \Leftrightarrow G1 : m\}$$

を生成する．その後，EN は待避していたパケットを ECIT に従い，アドレス・ポート変換して MNR に送信する．

図 8 に EN から IN への通信開始後の ECIT および NAT テーブルの内容と，パケットのアドレスとポート番号が変化していく様子を示す．EN は IP 層で ECIT を参照し，宛先仮想アドレスとポート番号 $V1 : d$ から，MNR のグローバルアドレスと割り当てられたポート番号 $G1 : m$ に変換して MNR に送信する．MNR では ECIT による変換処理は行われず，そのまま NAT モジュールに処理を渡し，宛先アドレスとポート番号を $G1 : m$ から $P1 : d$ に変換して IN に送信する．IN から EN への通信は上記と逆の変換が行われる．

このようにして，EN 側から MNR 配下の IN に対して通信を開始することができる．通信開始の原理は 2.2 節で示した NAT-f と同様であるが，MNR の移動に備えてテーブルの内容が拡張されている．

3.5.2　MNR 移動時の処理

通信中に MNR のグローバルアドレスが $G1$ から $G2$ に変わると，MNR と EN の間で図 7 に示すように移動通知処理が行われる．CU Request/CU Response のシーケンスにより，MNR の ECIT は

$$\{G3 : s \Leftrightarrow G3 : s\} \leftrightarrow \{G2 : m \Leftrightarrow G1 : m\}$$

のように，また EN の ECIT は

$$\{G3 : s \Leftrightarrow G3 : s\} \leftrightarrow \{V1 : d \Leftrightarrow G2 : m\}$$

のように更新される．このとき，NAT テーブルにはいっさい影響がない．

図 9 に MNR 移動後の ECIT および NAT テーブルの内容と，パケットのアドレスとポート番号が変化していく様子を示す．EN の上位層から IP 層にパケットが渡されると，ECIT が参照され宛先アドレスとポート番号が “$G3 : s \rightarrow G2 : m$” となって MNR に送信される．MNR は IP 層で ECIT を参照して，宛先アドレスを MNR 移動後のアドレス $G2$ から移動前のアドレス $G1$ に変換して，NAT モジュールに処理を渡す．NAT モジュールは NAT テーブルを参照して，宛先アドレスとポート番号を $G1 : m$ から $P1 : d$ に変換して IN に送信する．

このようにして，パケットは正しくルーティングされ，かつ EN および MNR の上位層，すなわち NAT モジュールには MNR のアドレスの変化が隠蔽される．IN から EN への通信は上記と逆の変換が行われる．

3.6　ECIT の役割

NAT-f における VAT テーブルは，上位ソフトウェアが意識する IP アドレス・ポート番号と，実際に使われる IP アドレス・ポート番号の変換を行うものであった．また，Mobile PPC で作られる CIT は，移動前の実アドレスと移動後の実アドレスを変換するものであった．Mobile NPC において定義した ECIT は，上位ソフトウェアが意識する IP アドレス・

表 1　通信の制約
Table 1　Restrictions of communications.

Case	Mobile NPC 機能の有無			移動ノード到達性（通信開始の方向）		通信継続性
	MNR	EN	IN	IN→EN	EN→IN	
1	✓	✓	✓	○	○	○
2	✓	✓	—	○	△	○
3	✓	—	✓	○	×	×
4	✓	—	—	○	×	×
5	—	✓	✓	○	×	×
6	—	✓	—	○	×	×
7	—	—	✓	○	×	×
8	—	—	—	○	×	×

✓：Mobile NPC 機能あり　—：Mobile NPC 機能なし

ポート番号と，実際に使われる IP アドレス・ポート番号の変換を行い，かつ実 IP アドレスの部分が移動にともない書き換えられるものとなる．

一方，MNR 側では NAT テーブルと ECIT という 2 つのテーブルが必要となる．ここで両テーブルを統合するという方法もあるが，NAT 処理はすでに枯れた技術であり，この機能はそのまま残すべきと考えた．そこで，ECIT から見ると NAT 処理があたかも上位アプリケーションであるかのように位置づけ，NAT 処理に与える影響を最小限になるようにした．このため，MNR 側では ECIT と NAT による 2 回のアドレス変換が実行されることになる．ただし，このような構造にすることにより，カーネル内の TCP チェックサムの演算など，NAT 処理の一部を改造する必要が出てきた．これについては 4.2 節に示す．

なお，ECIT の消去方法は，CIT および VAT テーブルと同様の考えに基づいている．MNR が保持する NAT テーブル，MNR と EN が保持する ECIT はセッションごとにその内容が存在し，一定の時間だけ通信がないとそれぞれ独立したタイマにより内容が消去される．テーブル消去後に新たなパケットが発生した場合は，それを検出したノードが送信元に対しそのことを通知する．送信元ノードは新たに Mapping Request から始まるシーケンスによりテーブルを生成する．テーブルの内容が重複する場合は上書きされる．使われなくなったテーブルの内容はタイマによりいずれ消去される．このようにテーブルが複数存在することにより問題が新たに発生することはないよう考慮されている．

3.7　既存ノードとの共存

本提案は，EN，IN および MNR が Mobile NPC の機能を保持することにより実現できる．いずれかの装置がこの機能を保持しない場合，通信の制約が発生する．ただし，従来可能であったことができなくなることはない．この関係を**表 1** に示す．

移動ノード到達性に関しては，通信開始の方向が IN→EN であればすべて可能である．逆方向の通信開始には NAT 越えが必要であり，MNR と EN の双方が機能を有している必要がある（Case 1，2）．Case 2 では，IN が一般の DDNS サービスに加入していれば，移動ネットワーク内で立ち上げ時に MNR のアドレス登録ができるので，EN 側からの通信開始が可能である．しかし，ネットワークが移動して MNR のアドレスが変わると，MNR のアドレス変化を IN が認識できないため，DDNS への登録を更新できない．そのため Case 2 は △ とした．通信継続性に関しては，MNR と EN の両者が機能を有する場合のみ可能で，それ以外の場合はネットワークの移動にともない通信が途中で途切れることになる．

4.　Mobile NPC の実装

Mobile NPC の通信にかかる部分を FreeBSD 5.3-RELEASE 上に実装し，動作検証を行った．今回の実装では DDNS の登録に関する部分については未実装であるが，提案方式の要求条件を確認するには十分である．NAT 機能の実現には FreeBSD で標準的に使用されているアプリケーション `natd` を改造して流用した．本章では Mobile NPC のモジュール構成と，`natd` の改造について記述する．なお，仮想アドレスの実現方法などについては，文献 14) に詳細が記述されているのでそちらを参照されたい．

4.1　モジュール構成

図 10 に MNR における Mobile NPC のモジュール構成を示す．すでに開発済みの Mobile PPC および NAT-f のモジュールを流用し，両者の連携処理を追加実装した．また，ECIT 関連サブモジュールに NAT-f の VAT テーブル関連サブモジュールを統合した．MNR はグローバルアドレスが設定されたインタフェースからパケットを受信したとき，またはパケットを送信するとき，IP 層の入出力関数 `ip_input()`，`ip_output()` より Mobile NPC モジュールを呼び出す．Mobile NPC モジュールはパケット判定を行った後，アドレス変換サブモジュール，移動管理サブモジュール，またはマッピング処理サブモジュールを呼び出す．各サブモジュールは処理を終えたら，`ip_input()` または `ip_output()` に操作を差し戻すため，既存の IP 層の処理に影響を与えることはない．

Mobile PPC モジュール内の移動管理サブモジュールは，移動して IP アドレスが変化したことをトリガとして呼び出される．IP アドレスの変化を判断するために，IP アドレス取得後，ARP モジュールにより実行される Gratuitous ARP による重複アドレスチェックを用いる．ECIT 操作サブモジュールを利用して，通信中のすべての EN に対して CU Request/CU Response を実行する．

NAT-f モジュール内のマッピング処理サブモジュールは，通信開始時に EN との間でネゴシエーション処理を行い，ECIT と natd 内の NAT テーブルを生成する．アドレス変換サブモジュールは IP アドレスやポート番号の変換処理を行い，ECIT 操作サブモジュールは ECIT の作成・更新・削除・検索を行う．ECIT の削除方法は，CIT，VAT テーブルで実施していた方法を継承する．natd は Divert ソケットを介して，アドレス変換を行う．EN にも MNR と同じ Mobile NPC モジュールが実装される．ただし，natd にかかわる処理は不要である．

4.2　natd の改造

本実装では natd をできる限り流用したが，以下の処理については変更が必要になった．natd はグローバル側のインタフェースに割り当てられているアドレスをつねに監視しており，そのアドレスが新しいアドレスに変わると，保持している NAT テーブルをすべて削除してしまう．そのため，MNR が移動しても NAT テーブルを削除せず，保持したままにするように改造した．

また，natd はパケットのプライベートアドレスをグローバルアドレスに変換した後，現在インタフェースに設定されているグローバルアドレスでチェックサムの差分計算を行う．しかし Mobile NPC では，MNR 移動後に変換されたパケットのアドレスは移動前のグローバルアドレスであるため，チェックサムの値が異なり破棄されてしまう．そのため，移動前のグローバルアドレスにより，チェックサムの再計算を行うように改造した．

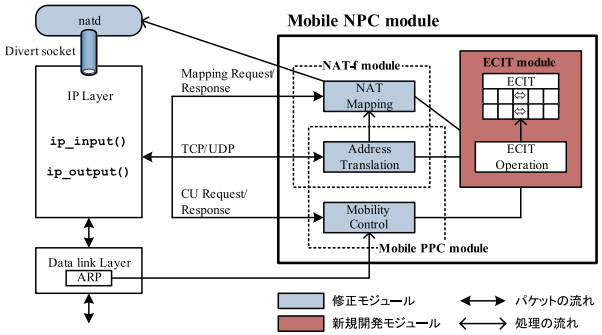

図 10　Mobile NPC のモジュール構成
Fig. 10　Module structure of Mobile NPC.

5. 評　　価

5.1　動 作 検 証

Mobile NPC を EN と MNR に実装した結果，3.1 節に示す要求条件を満たすことを確認した．グローバルアドレス空間上の EN とプライベートアドレス空間に属する IN が，双方向から互いに通信を開始できる．EN と IN はエンドエンドで直接通信を行う．次に，EN と IN が通信中にネットワーク側が移動してもエンドエンドの経路を維持したまま通信を継続できる．また，EN と IN の通信ペアを複数存在させても問題なく通信できることを確認した．ただし，通信開始に必要となる DDNS への登録はあらかじめマニュアルにより設定した．本提案方式を実装することによるスループットの測定結果，および移動時のシーケンスとそれにかかわる通信中断時間の測定結果については 5.2 節以降で示す．

5.2　性能測定環境

提案方式の性能を測定するための評価システムの構成を**図 11** に，機器仕様を**表 2** に示す．MNR および EN1〜3 に Mobile NPC を実装し，ネットワークはすべて 100 BASE-TX とした．IN1〜3 は一般端末とし，通信開始は IP アドレスの直接指定で実行した．MNR の

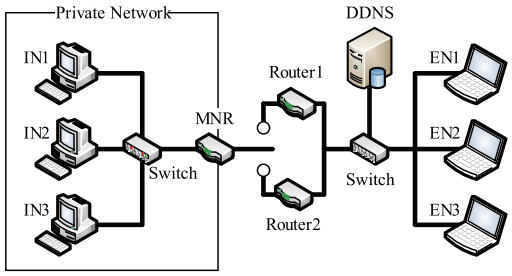

図 11　評価システムの構成
Fig. 11　The organization of evaluation system.

表 2　評価システムの機器仕様
Table 2　Machine specification in evaluation system.

	CPU	Memory	OS
MNR	Pentium4 3.0 GHz	1 GB	FreeBSD 5.3-RELEASE
EN1〜3	Pentium4 3.0 GHz	1 GB	FreeBSD 5.3-RELEASE
IN1〜3	Pentium4 3.4 GHz	1 GB	Windowd XP Professional

表 3　IN から EN のスループット
Table 3　Throughput from IN to EN.

IN と EN のペア数	実装なし	実装あり
1	94.9	94.7
2	47.5	47.5
3	31.7	31.7

単位：Mbps

表 4　EN から IN のスループット
Table 4　Throughput from EN to IN.

IN の台数	実装なし	実装あり
1	94.1	94.1
2	47.1	47.1
3	31.3	31.4

単位：Mbps

移動は，手動で LAN ケーブルをルータ 1 とルータ 2 の間で繋ぎ換えた後に，各ルータで動作する DHCP サーバよりアドレスを取得させた．アドレスの取得には `dhclient` コマンドを手動で実行した．

5.3　スループットの測定

EN と MNR に Mobile NPC を実装した場合と実装しない場合のスループットの違いを比較するための測定を行った．Mobile NPC では，IN から通信を開始した場合と EN から通信を開始した場合でテーブルの内容が異なるため，両者のケースにおけるスループットを測定した．通信ペアとして IN1-EN1，IN2-EN2，IN3-EN3 の 3 ペアを準備し，同時通信ペアの数を 1 から 3 まで変化させた．このときの IN1 におけるスループットを Iperf[21] により測定し，30 秒間の通信を 10 回試行して平均をとった．

表 3 は IN 側から通信を開始し，通信ノードのペア数を 1 から 3 まで増加させた場合，**表 4** は EN 側から通信を開始し，通信ノード数を 1 から 3 まで増加させた場合の測定結果である．ここで，EN から通信を開始する場合，Mobile NPC の実装なしの場合の測定方法については，MNR に NAT テーブルを手動で静的に設定する IP フォワード機能により実現した．表 3，表 4 から分かるように，通信ペア数が増加すると，帯域を分けあうためその分スループットが低下している．しかし，MNR と EN が Mobile NPC を実装した場合と実装していない場合を比べると，スループットの違いはほとんどないことが分かる．パケットの中継における Mobile NPC としての処理増加は EN と MNR における ECIT によるアドレス変換のみである．これらのアドレス変換処理は FreeBSD のカーネル内で実行されており，ほとんどオーバヘッドにはならないためと考えられる．

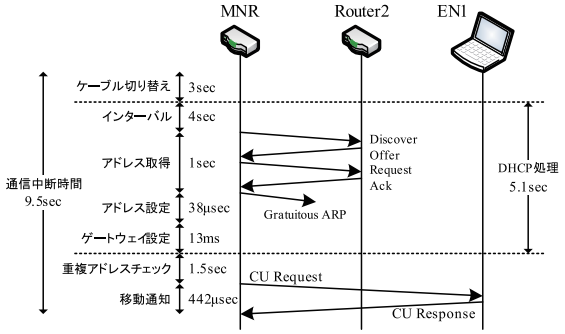

図 12　MNR 移動時の通信中断時間
Fig. 12　Suspended time when MNR moves.

5.4　通信中断時間の測定

MNR が通信中に移動すると，移動にかかわる処理が完了するまで通信が中断する．そこで，通信が再開されるまでの通信中断時間の測定を行い，その内訳を調査した．パケットの送受信時間の測定にはネットワークアナライザ Wireshark を，Mobile NPC モジュールおよびカーネルの処理時間の測定には RDTSC（Read Time Stamp Counter）[22] を用いた．測定結果は，MNR の移動を 10 回行ったときの平均である．

測定結果は**図 12** のとおりである．LAN ケーブルの手動切替え（L2 ハンドオーバ）に約 3 秒，DHCP によるアドレス取得に 5.1 秒，Gratuitous ARP による重複アドレスチェックに 1.5 秒，Mobile NPC による移動通知処理（CU Request/CU Response）に 442 マイクロ秒かかった．この結果より，Mobile NPC による移動通知処理にかかわる時間は，切替え時間全体から見ると十分小さく，DHCP 処理などに大部分の時間がかかっていることが分かる．

DHCP によるアドレス取得動作の内訳を見ると，DHCP Discover を送信するまでのインターバル時間が約 4 秒，DHCP Discover を送信してからアドレス取得するまでの動作が 1.0 秒，DHCP 動作後に取得したアドレスをインタフェースに設定するまでが 38 マイクロ秒，取得したデフォルトゲートウエイのアドレスがルーティングテーブルに追加されるまでが 13 ミリ秒であった．ここでインターバル時間とは，DHCP Discover が複数のノードか

ら 1 度に送信されるのを防ぐために設けられたランダムな時間で，単一のネットワークが移動するような今回のシステムでは不要な時間である．

通信中断時間の 9.5 秒のうち，LAN ケーブルの切替えにかかる 3 秒と，上記インターバル時間 4 秒の計 7 秒が，無駄な時間として多くの時間を占めている．また，図中の Gratuitous ARP は重複アドレスチェックのために実行されるが，タイムアウトするまで待つ必要があり，ここでも多くの時間を要する．LAN ケーブルの切替え部分は，無線 LAN においては L2 ハンドオーバの時間に相当するため，実際は 50〜400 ミリ秒となると考えられる[23]．インターバル時間は不要な機能であることから，MNR の `dhclient` を改造することによりゼロにできる．これらのことから，通信中断時間は容易に 2.6〜3 秒以下にすることができる．

通信中断時間をさらに減少させるには，別の対策が必要である．たとえば，文献 24) では無線 LAN カードを 2 枚搭載することにより，Mobile PPC のアドレス切替え時のパケットロスを完全に回避できることが示されている．この方式を MNR に適用すれば，通信中断に係るパケットロスは 0 にできる．この方式は，グローバルアドレス側にインタフェースが 2 枚必要になるが，このような対策を MNR に施せば，ネットワーク内の個々の端末が対策をとらなくても移動時のパケットロスを完全に回避できる可能性があり，今後検討の価値がある．

5.5　移動通知時間の測定

5.4 節の測定結果に示したとおり，Mobile NPC の処理として必須の移動通知処理（CU Request/CU Response の交換）にかかる時間は他の処理時間に比べてきわめて小さい．しかし，移動通知処理の交換は通信中のすべてのペアに対して必要となる．この処理は MNR が複数の IN に代行して実行する必要があるため，通信中ペア数が増加すると MNR に負荷がかかる可能性がある．MNR は通信ペア数が複数ある場合は，CU Request を各 EN に対して連続的に送信し，それぞれの CU Response をまとめて待ちうける方式をとっている（**図 13** 参照）．

MNR は各 EN へ一連の CU Request を送信し終えると，CU Response が戻るまでのラウンドトリップ時間（RTT）の間ウエイト状態に入る．その後 CU Response を連続的に受信し ECIT を順次更新してゆく．図 13 に今回の測定環境において，EN が 1 台の場合と 3 台の場合について移動通知時間を測定した結果を示す．測定値は 10 回行ったときの平均である．EN が 1 台のときは 442 マイクロ秒，3 台のときは 551 マイクロ秒となった．これらの処理時間はカーネルで処理していることもあり，EN 台数が増加しても，DHCP 処理など他の処理に比べ相対的にきわめて小さいことが分かる．実環境においては，RTT が状

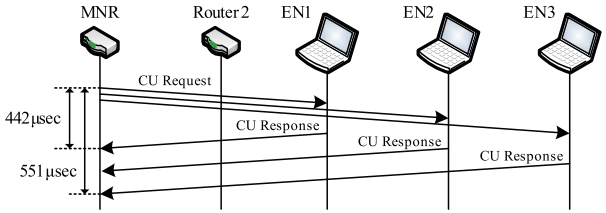

図 13　Mobile NPC のアドレス通知時間
Fig. 13　Address report time in Mobile NPC.

況により異なり，一連の CU Request 送信中に CU Response が個別に戻ることも想定され，処理が複雑になる．このように EN 台数が増えた場合の正確な処理時間予測は難しい．しかし移動通知にかかわる処理自体は EN が複数あってもきわめて高速に実行されており，全体の処理に大きな影響を与えることはほとんどないものと考えられる．

移動通知処理がこのように短時間で実現可能なのは，Mobile NPC の原理がシンプルであることと，処理をカーネル内で実行していることによるものである．MNR に文献 24) の方式を用いる場合は，移動通知にかかわる処理を通信していない側のインタフェースを用いて実行するため，EN がいくつであっても移動通知にかかわるパケットロスは原理的に 0 にできる可能性があり，今後検討の価値があるものと考えられる．

6. ま と め

本論文では IPv4 プライベートアドレスが利用可能なネットワークモビリティを実現する Mobile NPC を提案した．Mobile NPC ではノード単位で移動透過性を実現する Mobile PPC と，NAT 越え通信を実現する NAT-f の機能を統合することにより，上記の目的を実現した．Mobile NPC によると，複数のセッションを同時に実現できる．また，特殊なサーバが不要で，かつ移動の有無にかかわらずエンドエンドの通信を継続することができる．

Mobile NPC を試作し，想定した動作が可能であることを確認した．通信性能を測定した結果，スループットの低下はほとんどなかった．移動にともなう通信中断時間の内訳を解析し，MNR に適切な処置を施すことによりパケットロスを低減させることができることを示した．今後は DDNS 登録にかかわる実装を完了し，フィールドでの評価を実施する．また，セキュリティにかかわる考察を行ってゆく予定である．

参 考 文 献

1) 寺岡文男：インターネットにおけるノード移動透過性プロトコル，電子情報通信学会論文誌（D-I），Vol.J87-D1, No.3, pp.308–328 (2004).
2) Perkins, C.: IP Mobility Support for IPv4, RFC 3344, IETF (2002).
3) 竹内元規，鈴木秀和，渡邊　晃：エンドエンドで移動透過性を実現する Mobile PPC の提案と実装，情報処理学会論文誌，Vol.47, No.12, pp.3244–3257 (2006).
4) Johnson, D., Perkins, C. and Arkko, J.: Mobility Support in IPv6, RFC 3775, IETF (2004).
5) Ishiyama, M., Kunishi, M., Uehara, K., Esaki, H. and Teraoka, F.: LINA: A New Approach to Mobility Support in Wide Area Networks, *IEICE Trans. Communications*, Vol.E84-B, No.8, pp.2076–2086 (2001).
6) 相原玲二，藤田貫大，前田香織，野村嘉洋：アドレス変換方式による移動透過インターネットアーキテクチャ，情報処理学会論文誌，Vol.43, No.12, pp.3889–3897 (2002).
7) Leung, K., Dommety, G., Narayanan, V. and Petrescu, A.: Network Mobility (NEMO) Extensions for Mobile IPv4, RFC 5177, IETF (2008).
8) Devarapalli, V., Wakikawa, R., Petrescu, A. and Thubert, A.: Network Mobility (NEMO) Basic Support Protocol, RFC 3963, IETF (2005).
9) Banno, A., Oiwa, T. and Teraoka, F.: χLIN6-NEMO: A Network Mobility Protocol Based on LIN6, *IEICE Trans. Communications*, Vol.E89-B, No.4, pp.1070–1079 (2006).
10) 藤田貴大，野村嘉洋，西村浩二，前田香織，相原玲二：MAT によるモバイルネットワークの実現，マルチメディア，分散，協調とモバイル（DICOMO2003）シンポジウム 2003 論文集，pp.105–108 (2003).
11) Rosenberg, J., Weinberger, J., Huitema, C. and Mahy, R.: STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs), RFC 3489, IETF (2003).
12) UPnP Forum: Internet Gateway Device (IGD) Standardized Device Control Protocol V 1.0 (2001). http://www.upnp.org/standardizeddcps/igd.asp
13) Ng, T., Stoica, I. and Zhang, H.: A Waypoint Service Approach to Connect Heterogeneous Internet Address Spaces, *Proc. USENIX Annual Technical Conference*, pp.319–332 (2001).
14) 鈴木秀和，宇佐見庄五，渡邊　晃：外部動的マッピングにより NAT 越え通信を実現する NAT-f の提案と実装，情報処理学会論文誌，Vol.48, No.12, pp.3949–3961 (2007).
15) 鈴木秀和，渡邊　晃：プライベートネットワーク内のノードを通信相手とした移動透過性の実現方式，電子情報通信学会論文誌（B），Vol.J92-B, No.1, pp.109–121 (2009).
16) 鈴木秀和，寺澤圭史，渡邊　晃：Hole Punching を用いた NAT 越え Mobile PPC の実装，情報処理学会研究報告，Vol.2009-MBL-49, No.17, pp.1–7 (2009).
17) Vixie, P., Thomson, S., Rekhter, Y. and Bound, J.: Dynamic Updates in the Domain Name System (DNS UPDATE), RFC 2136, IETF (1997).
18) Srisuresh, P. and Egevang, K.: Traditional IP Network Address Translator (Traditional NAT), RFC 3022, IETF (2001).
19) Vixie, P., Gudmundsson, O., Eastlake, D. and Wellington, B.: Secret Key Transaction Authentication for DNS (TSIG), RFC 2845, IETF (2000).
20) Eastlake, D.: DNS Request and Transaction Signatures (SIG(0)s), RFC 2931, IETF (2000).
21) Tirumala, A., Qin, F., Dugan, J., Ferguson, J. and Gibbs, K.: Iperf: The TCP/UDP Bandwidth Measurement Tool. http://dast.nlanr.net/Projects/Iperf/
22) Intel Corp.: Using the RDTSC Instruction for Performance Monitoring (1998). http://developer.intel.com/drg/pentiumII/appnotes/RDTSCPM1.htm
23) Mishra, A., Shin, M. and Srbaugh, W.: An Empirical Analysis of the IEEE802.11 MAC Layer Handoff Process, *ACM SIGCOM Computer Communication Review*, Vol.33, No.2, pp.93–102 (2003).
24) 金本綾子，鈴木秀和，伊藤将志，渡邊　晃：IPv4 移動体通信システムにおけるパケットロスレスハンドオーバの提案，情報処理学会論文誌，Vol.50, No.1, pp.133–143 (2009).

(平成 21 年 3 月 2 日受付)
(平成 21 年 7 月 2 日採録)

坂本　順一

2005 年名城大学理工学部情報科学科卒業．2007 年同大学大学院理工学研究科情報科学専攻修了．在学時代，モビリティプロトコルに興味を持ち，ネットワークモビリティに関する研究にたずさわる．現在，株式会社東芝勤務．修士（工学）．

鈴木　秀和（正会員）

2004 年名城大学理工学部情報科学科卒業．2006 年同大学大学院理工学研究科情報科学専攻修了．2009 年同大学院理工学研究科電気電子・情報・材料工学専攻博士後期課程修了．2008 年より日本学術振興会特別研究員．ネットワークセキュリティ，モバイルネットワーク，ホームネットワーク等の研究に従事．博士（工学）．電子情報通信学会，IEEE 各会員．

伊藤　将志（正会員）

2004 年名城大学理工学部情報科学科卒業．2006 年同大学大学院理工学研究科情報科学専攻修了．2009 年同大学院理工学研究科電気電子・情報・材料工学専攻博士後期課程修了．同年株式会社東芝入社．VoIP，無線ネットワーク等の研究に従事．博士（工学）．電子情報通信学会会員．

宇佐見庄五（正会員）

1997 年名古屋工業大学知能情報システム学科卒業．2002 年同大学大学院博士後期課程修了．同年同大学院ベンチャービジネスラボラトリ研究員．2004 年より名城大学理工学部情報工学科講師．現在，同大学准教授．量子情報理論，符号理論の研究に従事．博士（工学）．電子情報通信学会，情報理論とその応用学会各会員．

渡邊　　晃（正会員）

1974 年慶應義塾大学工学部電気工学科卒業．1976 年同大学大学院工学研究科修士課程修了．同年三菱電機株式会社入社後，LAN システムの開発・設計に従事．1991 年同社情報技術総合研究所に移籍し，ルータ，ネットワークセキュリティ等の研究に従事．2002 年名城大学理工学部教授，現在に至る．博士（工学）．電子情報通信学会，IEEE 各会員．