NAT-fの移動透過通信への拡張

鈴木秀和[†] 金本綾子[†] 渡邊晃[†]

IPv4 ネットワークにおいて，グローバルアドレス空間とプライベートアドレス空間の違いを意識せずに，移動透過通信を実現できると有益である．従来の NAT を介した移動透過技術は，移動ノードが異なるアドレス空間に移動する前に，ノード間の通信が既に確立していることを前提にしている．しかし，ノード間に NAT が介在すると，NAT 外部のノードから内部のノードへ通信を開始することができないため，適用範囲が限定されていた．本稿ではこの問題を解決するために，通信開始時に NAT 越えを実現する NAT-f（NAT-free protocol）と，移動透過技術である Mobile PPC（Mobile Peer-to-Peer Communication）を融合した拡張 NAT-f を提案する．移動ノードと NAT は拡張 NAT-f により，移動ノードの移動前後の IP アドレスの関係，および NAT のマッピング関係を共有し，NAT-f と Mobile PPC におけるアドレス変換を同時に行う．インターネット上の移動ノードは，ホームネットワーク内のノードに対して通信を開始することができ，かつ通信中に移動しても通信継続性が保証される．

NAT-f Extension for Mobile Communications

Hidekazu Suzuki,[†] Ayako Kanemoto[†] and Akira Watanabe[†]

It is quite useful if mobile transparency can be realized without considering the difference between global address space and private address space in IPv4 network. Existing technologies for mobile transparency over NAT are based on the assumption that a communication between nodes has already been established before the mobile node moves to another address space. However, these technologies can be applied only to a certain situation because a node located in the outside of NAT cannot initiate communications to a node behind NAT. This paper presents Extended NAT-free protocol (ENAT-f) in order to solve the problem. ENAT-f is composed of NAT-f that realizes NAT traversal communications, and Mobile Peer-to-Peer Comunication (Mobile PPC) that realize mobile transparency. An external mobile node and NAT share the information of relationship between IP addresses before and after movement and a NAT mapping using ENAT-f, and execute the address translation of NAT-f and Mobile PPC at the same time. The mobile node on the Internet can initiate a communication to the node located in a home network, and its communication is guaranteed even if the mobile node moves.

1. はじめに

無線ネットワーク環境の普及に伴い，ノードはどこからでもネットワークに接続できるようになってきている．しかし，通信中に移動すると IP アドレスが変化するため，通信が切断されてしまう．この課題を解決するために，通信中に IP アドレスが変化しても通信に影響を与えない移動透過性が要求されている．移動透過性を実現する技術は，Mobile IP[1)~2)] をはじめ，様々な方式が提案されている[3)~7)]．

近年では計算機の高性能化，小型化やブロードバンドの普及に伴い，IP 電話やマルティメディア通信など個人間の通信が増加している．このような利用形態においては，グローバルネットワークに接続したノードから，ホームネットワーク内のノードに向けて通信を開始することが十分に想定される．IPv4 ネットワークでは IP アドレスの枯渇を避けるために，ホームネットワークにはプライベート IP アドレスを適用するのが一般である．ホームネットワークとインターネットの接点には NAT☆ を設置する必要がある．しかし，NAT によりエンドツーエンド接続性が失われ，NAT の外部から内部のノードへ通信を開始することができない，いわゆる NAT 越え問題が表面化してきた．IPv6 は IPv4 との上位互換性を保持しておらず，IPv4 環境は

† 名城大学大学院理工学研究科
Graduate School of Science and Technology, Meijo University

☆ 本稿における NAT には，ポート番号の変換も行う NAPT（Network Address Port Translation）を含むものとする．

IPv6 ネットワークと混在する形で当分続くことが想定される．そのため，NAT 越え技術の必要性が高まっており，様々な手法が提案されている[8)~12)]．

IPv4 において NAT 越え通信と移動透過通信を同時に実現することは，現状の IPv4 ネットワークにおいてユビキタスネットワークで想定される柔軟な通信スタイルを実現できることを意味しており，有益な試みである．しかし，多くの移動透過技術は同一アドレス空間内を移動する場合を想定しており，NAT を越えた通信や移動は想定されていない．そこで，従来の移動透過技術を応用することにより，NAT を越えた移動透過通信を実現する方法が提案されている[13)~16)]．これらの方法は，通信相手ノード（以後 CN）はサーバとしてグローバルアドレス空間に存在し，移動ノード（以後 MN）がグローバルアドレス空間とプライベートアドレス空間の間を移動することを可能としている．すなわち，MN 側から CN へ通信を開始することを前提としており，本稿で想定する MN がグローバルアドレス空間に，CN がサーバとしてプライベートアドレス空間に存在する状況における移動透過通信を実現することはできない．

筆者らは独自の NAT 越え技術として，NAT-f（NAT-free protocol）[17)] を提案している．NAT-f は NAT 外部のノードが NAT 内部のノードへ通信を開始する際，NAT とネゴシエーションを実行することにより，NAT にマッピング情報を生成し，相互にマッピングアドレス☆ を共有する．その後，外部ノードは送信パケットの宛先をマッピングアドレスに変換することにより，NAT 越え通信を実現する．また筆者らはエンド端末同士で移動透過性を実現する Mobile PPC（Mobile Peer-to-Peer Communication）[7)] を提案している．Mobile PPC は通信中のノードの IP アドレスが変化した際，両エンドノードにおいて移動前後の IP アドレスを共有し，IP 層でアドレス変換処理を行うことにより，上位層から IP アドレスの変化を隠蔽する．

本稿では両技術の共通機能となるアドレス変換に着目し，NAT-f と Mobile PPC を融合することにより，異なるアドレス空間において移動透過性を実現する拡張 NAT-f を提案する．MN は移動時に，拡張 NAT-f を用いて NAT とネゴシエーションすることにより，MN の移動前後の IP アドレスの関係，および NAT 配下の CN に対応する NAT マッピングの関係を共有し，NAT-f および Mobile PPC におけるアドレス変換を同時に行う．

以下，2 章では異なるアドレス空間において移動透過性を実現する従来技術を挙げる．3 章において移動透過通信に対応した拡張 NAT-f を提案する．4 章において拡張 NAT-f の実装について述べ，最後に 5 章でまとめる．

2. NAT が介在した移動透過通信

以下に，NAT が介在した移動透過通信に関わる従来技術を紹介する．

2.1 Mobile IP に関する技術

Mobile IPv4 を実環境で運用するために必要となる機能のひとつとして，プライベート IP アドレスを考慮した技術がある[13)~14)]．

Reverse Tunneling for Mobile IP[13)] は，ネットワークトポロジの整合性を図り，Ingress Filtering 問題[18)] を解決するための手法である．この技術を応用することにより，MN にプライベート IP アドレスを割り当てることができる．**図 1** に Reverse Tunneling for Mobile IP の通信を示す．ホームエージェント（以後 HA）は NAT 機能を有しており，ホームネットワークはプライベートアドレス空間である．そのため，MN のホームアドレス（以後 HoA）はプライベート IP アドレスとなる．MN がグローバルアドレス空間へ移動すると，外部エージェント（以後 FA）より気付けアドレス（以後 CoA）が割り当てられ，FA を経由して HA へ Binding Update（以後 BU）を送信する．FA はこの BU を転送する際，Visitor List を生成する．Visitor List には MN のプライベート IP アドレス HoA と，HA のグローバル IP アドレス，および MN の MAC アドレスが保存される．HA は BU 受信時に，Mobility Binding List を生成する．Mobility Binding List には MN の HoA と，CoA が保存される．以後，MN から CN への通信パケットは，FA か

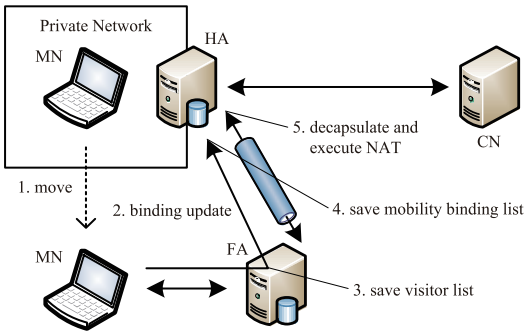


図 1 Reverse Tunneling for Mobile IP
Fig. 1 Reverse Tunneling for Mobile IP.

☆ NAT でマッピングされた IP アドレスとポート番号の組．

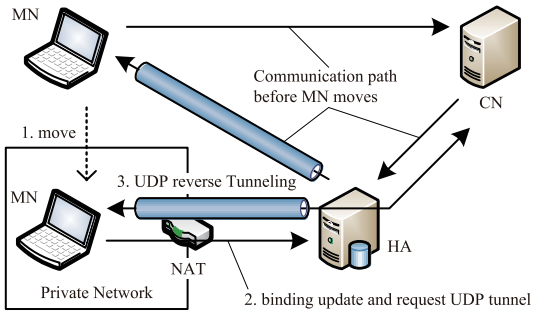


図 2 Mobile IP traversal of NAT
Fig. 2 Mobile IP traversal of NAT.

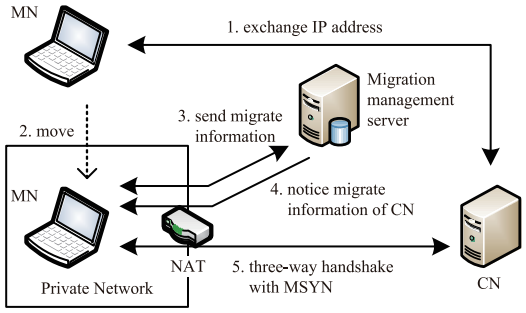


図 3 TCP コネクション維持プロトコルによる通信
Fig. 3 Communication based on TCP connection sustaining protocol.

ら HA へ逆方向トンネリングにより送信される．HA はデカプセル化した後，NAT により送信元 IP アドレスを HoA から HA のグローバル IP アドレスに変換してから，CN へ転送する．CN から MN への通信は上記と逆の手順により，HA を経由して FA まで送信される．FA はデカプセル化した後，Visitor List に保存した MN の MAC アドレスを用いて，MN へ転送する．

Mobile IP Traversal of NAT[14] により，グローバルアドレス空間に存在する MN が NAT 配下のネットワークに移動することが可能になった．**図 2** に Mobile IP Traversal of NAT の通信を示す．MN は Mobile IP による通信時に，NAT 配下のネットワークに移動し，そのネットワークには FA が存在しないことを想定している．MN は移動後に，DHCP などによりプライベート IP アドレスが割り当てられ，これを共存気付けアドレス（以後 CCoA）とする．その後，HA に対して BU を送信する際，オプションとして UDP トンネルを要求する．HA は BU により通知された CCoA と BU の送信元 IP アドレス，すなわち NAT のグローバル IP アドレスを比較することにより，MN が NAT 配下に移動したことを知る．MN は HA からの応答を受信した後，CN 宛のパケットを UDP-in-IP による逆方向トンネルを形成して，HA へ送信する．

いずれの方法においても，MN と HA の間において双方向トンネルを用いた通信が行われ，冗長な経路を通るため，スループットが低下するという課題がある．また後者の技術において，MN は HA との間に確立した UDP トンネルを維持するために，KeepAlive を行う必要があり，MN 数が増加するにつれて，HA に発生する負荷が増大する．

2.2 TCP コネクション維持プロトコル

トランスポート層での実現方法として，TCP コネクション維持プロトコル[15] がある．このプロトコルは，移動先情報交換プロトコルと，An End-to-End Approach to Host Mobility[6] を拡張した拡張 TCP から構成される．**図 3** に TCP コネクション維持プロトコルによる通信を示す．

MN と CN は移動前に移動先情報交換プロトコルを用いて，自端末の IP アドレスと，自端末に見えている相手端末の IP アドレスを相手端末との間で交換する．MN が通信中に移動すると，移動情報管理サーバに対して，MN の移動前後の IP アドレス／ポート番号を通知する．このとき，移動情報管理サーバは通知された IP アドレスの変換を検出して，MN が NAT 配下のネットワークに移動したかどうかを判断する．その後，NAT による接続の片方向性を考慮して，MN と CN のうち，通信開始が可能な端末へ相手端末の移動先情報を通知する．上記通知を受けた端末は，MSYN パケット☆ に移動前に交換していた情報を Migrate-Permit オプションとして付与し，相手端末と MSYN の 3 ウェイハンドシェイクを行うことにより，TCP コネクションを再開する．

本手法は TCP に特化した技術であるため，IP 電話やマルティメディア通信において利用される RTP（Real-time Transport Protocol）など，UDP 上で動作するアプリケーションに適用することができない．

2.3 Mobile PPC に関する技術

ネットワーク層におけるエンドツーエンド方式として Mobile PPC がある．Mobile PPC は移動ノード到達生の実現には既存の Dynamic DNS（以後 DDNS）を利用し，通信継続性の実現には Mobile PPC によるアドレス変換処理を行う．本稿では以後，Mobile PPC におけるアドレス変換を移動アドレス変換と呼ぶことにする．筆者らは文献 16) において，DPRP

☆ 移動前後の IP アドレスを通知するための TCP オプションである Migrate オプションが付与された SYN パケットを示す．

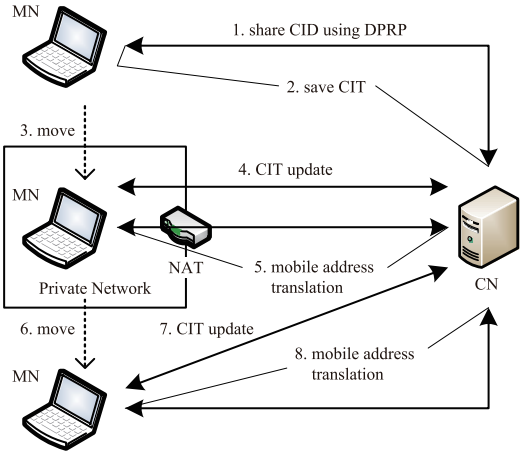


図 4 Mobile PPC による NAT 越え移動透過通信
Fig. 4 Mobile communication traversal of NAT based on Mobile PPC.

(Dynamic Process Resolution Protocol) [19)~20)] を用いて移動アドレス変換に必要な情報を交換することにより，MN がグローバルアドレス空間とプライベートアドレス空間を自由に移動することを可能にする方式の検討を行っている．**図 4** に Mobile PPC による NAT 越え移動透過通信を示す．

MN と CN，および NAT は DPRP の機能を有している．MN と CN が通信を開始する場合，DPRP によりその通信の CID（Connection ID）☆ を交換し，CIT（CID Table）を生成しておく．MN が通信中に NAT 配下のネットワークに移動すると，DHCP によりプライベート IP アドレスが割り当てられる．MN は CN に対して DPRP を用いて，移動通知である CIT Update（以後 CU）を行う．このとき，NAT では MN と CN 間の通信に対するマッピングを行う．CU には MN の移動前後の CID に加えて，NAT でマッピングされたグローバル IP アドレスとポート番号が含まれる．CN は CU により CIT を更新した後，MN へ CU Reply を応答する．その後，MN は更新した CIT に基づいて，送信パケットの送信元を移動後の IP アドレスに変換して CN へ送信する．CN は NAT を介して送信された MN のパケットに対して，移動アドレス変換により移動前の IP アドレスに変換することにより，通信の継続を実現する．MN はプライベートアドレス空間からグローバルアドレス空間へ移動する場合も，上記と同様の手順により CIT を更新し，移動アドレス変換処理を行う．

☆ TCP コネクションや UDP ストリームを識別するための送信元／宛先 IP アドレス，ポート番号，およびプロトコル番号の組．

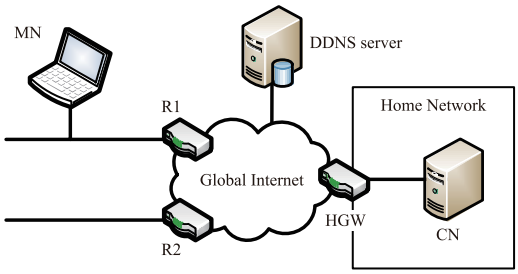


図 5 システム構成
Fig. 5 System Configuration.

なお，MN が DPRP に対応していない一般の NAT 配下に移動した場合は，文献 14) と同様に，MN と CN 間で UDP トンネルを形成することにより解決できる．この場合，MN と CN 間の通信は，移動後の IP アドレスに変換した後のパケットに UDP カプセル化することになる．

Mobile PPC による手法は MN の位置を管理する装置（HA や移動情報管理サーバ）を必要とせず，最適経路で通信できることから，低遅延，高スループットを実現することができる．しかし，他の技術と同様に，NAT 越え問題によりグローバルアドレス空間側ノードから NAT 内部に存在するノードへ通信を開始することができない．

3. 拡張 NAT-f

本稿では既存技術の共通の課題であった NAT 越えを解決するために，拡張 NAT-f を提案する．拡張 NAT-f は，従来の NAT-f および NAT 機能の一部を拡張することにより，Mobile PPC の移動通知機能および移動アドレス変換機能を包括する方式である．

以下に，本稿で用いる記号を定義する．

- $X : x$; IP アドレス X，ポート番号 x
- $X \rightarrow Y$，$Y \leftarrow X$; X から Y への通信
- $X \leftrightarrow Y$; X と Y 間の通信
- $X \overset{Z}{\Leftrightarrow} Y$; 機能 Z により X から Y，または Y から X に変換

なお，機能 Z は以下のいずれかが対応する．

- NAT ; 通常の NAT によるアドレス変換
- VAT ; NAT-f における仮想アドレス変換（VAT; Virtual Address Translation）
- MAT ; Mobile PPC における移動アドレス変換（MAT; Mobile Address Translation）

図 5 に示すシステム構成において，MN がホームネットワーク内部に存在する CN へ通信を開始し，通信中にルータ R1 配下のネットワーク（以後，NET_{R1} と表記）から NET_{R2} に移動する状況を想定する．MN

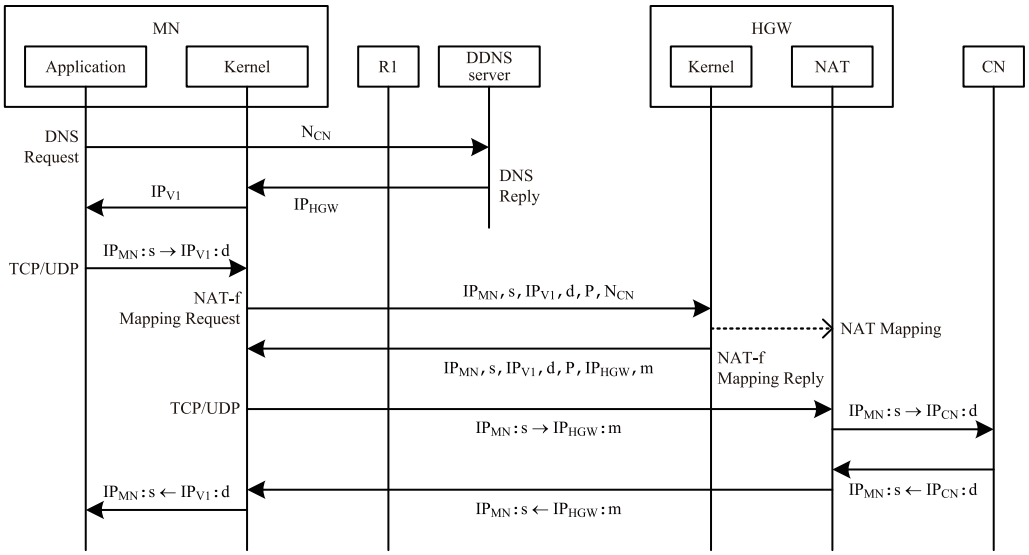


図 6 NAT-f による NAT 越え通信シーケンス
Fig. 6 Sequences of NAT traversal communication with NAT-f.

とホームゲートウェイ（以後 HGW）は拡張 NAT-f を実装しており，CN は移動透過性及び NAT 越えを実現する機能を一切有さない一般ノードでよい．また，DDNS サーバには CN のホスト名 N_{CN} と HGW の IP アドレス IP_{HGW} の対応関係が，HGW には CN のホスト名とプライベート IP アドレス IP_{CN} の対応関係が既に登録されているものとする．

3.1 NAT 越え通信

図 6 に通信開始時におけるシーケンスを示す．通信開始時は，既存の NAT-f をそのまま適用する．以下に，MN と CN が通信を確立するまでの手順について述べる．

(1) **DNS 名前解決**

MN は DDNS サーバに対して CN の名前解決を依頼し，CN のアドレスとして IP_{HGW} を取得する．ここで，MN のカーネルにおいて，取得した上記アドレスを仮想 IP アドレス IP_{V1} に書き換える．これら 3 つの関係（IP_{V1}，IP_{HGW}，N_{CN}）を NRT（Name Relation Table）に保存した後，アプリケーションには CN の IP アドレスを IP_{V1} として通知する．

(2) **NAT-f ネゴシエーション**

MN は宛先 IP アドレスが仮想 IP アドレスとなっている TCP/UDP パケットを送信する際，カーネルにおいてパケットの CID より VAT テーブルを参照する．VAT テーブルとは，仮想 IP アドレスと HGW で割り当てられたマッピングアドレスとの変換関係を示すテーブルで，NAT-f ネゴシエーション完了時に生成される．MN が CN に初めて通信する場合は VAT テーブルに該当するエントリがないため，NAT-f ネゴシエーションを開始することになる．

MN は送信しようとしていた TCP/UDP パケットをカーネル内に一時待避し，NAT-f マッピング要求を HGW へ送信する．NAT-f マッピング要求には待避したパケットの CID（IP_{MN}，s，IP_{V1}，d，P☆）と，NRT に保存されている CN の名前 N_{CN} が記載される．HGW は NAT-f マッピング要求を受信すると，通知された CID と N_{CN} に対応する IP アドレスから

$$IP_{MN} : s \leftrightarrow \{IP_{HGW} : m \overset{NAT}{\Longleftrightarrow} IP_{CN} : d\}$$

のように NAT マッピング情報を生成する．これは MN と CN 間においてポート番号 s，d を用いた通信に対して，HGW は NAT により IP アドレス／ポート番号を IP_{HGW} ／ m に変換することを意味する．HGW はこのマッピングアドレス $IP_{HGW} : m$ を NAT-f マッピング応答に記載して MN へ応答する．

MN は NAT-f マッピング応答を受信すると，仮想 IP アドレスとマッピングアドレスの変換関係を示すエントリ

$$IP_{MN} : s \leftrightarrow \{IP_{V1} : d \overset{VAT}{\Longleftrightarrow} IP_{HGW} : m\}$$

を生成し，VAT テーブルに格納する．その後，NAT-f ネゴシエーション開始時に待避した TCP/UDP パケットを復帰させる．

(3) **仮想アドレス変換**

復帰した TCP/UDP パケットは VAT テーブルに基

☆ 待避したパケットのプロトコルタイプ．TCP，または UDP が指定される．

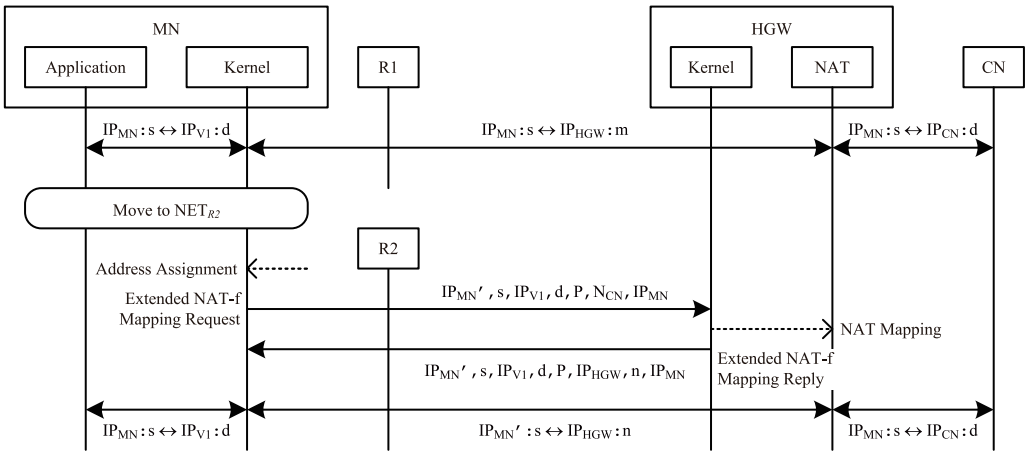


図 7 移動透過通信シーケンス
Fig. 7 Sequences of mobile trancparent communication.

づいて，宛先 IP アドレス／ポート番号が $IP_{V1} : d$ から $IP_{HGW} : m$ に変換され，HGW に送信される．HGW は先ほど生成した NAT マッピング情報に基づいて，当該パケットの宛先 IP アドレス／ポート番号を $IP_{HGW} : m$ から $IP_{CN} : d$ に変換し，MN の通信相手である CN へ転送する．

以上の処理により，MN から CN への通信開始が完了する．CN から MN への応答パケットは，上記と逆の変換処理を行う．以後の通信は MN 内の VAT，HGW 内の NAT によるアドレス変換だけが実行される．

3.2 移 動 通 知

MN は通信中に移動した際，拡張 NAT-f により移動通知を行い，VAT テーブルの更新および NAT マッピング情報の再生成を行う．また MN の VAT 処理と HGW の NAT 処理において，Mobile PPC の移動アドレス変換を同時に行うことにより，MN の上位アプリケーションおよび HGW 配下の CN に対して，MN の移動を隠蔽する．**図 7** に MN が NET_{R2} に移動した後のシーケンスを示す．なお，MN は移動後の IP アドレスとして $IP_{MN}{}'$ が割り当てられたものとする．

(1) 移動通知と NAT マッピングの更新

MN は新しい IP アドレスを取得した後，移動前に生成した VAT エントリの情報（IP_{MN}，s，IP_{V1}，d，P），仮想 IP アドレスに対応する CN の名前 N_{CN}，および移動後の IP アドレス IP'_{MN} を拡張 NAT-f マッピング要求に記載して，HGW へ送信する．HGW はこの拡張 NAT-f マッピング要求を受信すると，通知された情報から

$$\{IP_{MN}{}' : s \overset{MAT}{\Longleftrightarrow} IP_{MN} : s\} \leftrightarrow \{IP_{HGW} : n \overset{VAT}{\Longleftrightarrow} IP_{CN} : d\}$$

のように，HGW の通信相手側，すなわち MN 側のアドレスも変換するように NAT マッピング情報を生成する．HGW は新たに割り当てられたマッピングアドレス $IP_{HGW} : n$ を拡張 NAT-f マッピング応答に記載して MN へ応答する．

MN は拡張 NAT-f マッピング応答を受信すると，仮想 IP アドレスとマッピングアドレスの変換関係に加えて，MN の移動前後の IP アドレスの変換関係を示すエントリ

$$\{IP_{MN} : s \overset{MAT}{\Longleftrightarrow} IP_{MN}{}' : s\} \leftrightarrow \{IP_{V1} : d \overset{NAT}{\Longleftrightarrow} IP_{HGW} : n\}$$

を生成し，VAT テーブルを更新する．

(2) 仮想アドレス変換と移動アドレス変換の統合

EN は VAT テーブルに基づいて，TCP/UDP パケットの送信元を移動前の $IP_{MN} : s$ から移動後の $IP'_{MN} : s$ に移動アドレス変換する．さらに宛先を仮想アドレス変換により，仮想 IP アドレス $IP_{V1} : d$ からマッピングアドレス $IP_{HGW} : n$ に変換し，送信する．HGW は先ほど生成した NAT マッピング情報に基づいて，移動アドレス変換により送信元を MN の移動前の IP アドレス $IP_{MN} : s$ に変換する．さらに通常の NAT 処理により宛先をマッピングされた $IP_{CN} : d$ に変換し，MN の通信相手である CN へ転送する．

MN の VAT 処理および HGW の NAT 処理により，MN の上位アプリケーションおよび CN は，移動が発生して IP アドレスが変化したことに気づくことなく，通信を継続することができる．なお，CN から MN への通信は上記と逆の手順でアドレス変換を行う．

4. 実　　装

FreeBSD 6.1-RELEASE を用いて，プロトタイプ

システムを実装した．**図 8** に MN おける実装の概要を示す．

4.1 カーネル内の処理

拡張 NAT-f モジュールは IP 層に実装され，IP 入出力関数 `ip_input()`，`ip_output()` から呼び出される．拡張 NAT-f モジュールは，従来の NAT-f に備えていた DNS 書き換え機能，仮想 IP アドレス変換機能，および NAT-f ネゴシエーション機能に，Mobile PPC における移動アドレス変換機能と移動管理機能を統合させることにより実現した．

NRT および VAT テーブルはハッシュテーブルとして作成した．MN が NAT-f マッピング要求を送信する際，VAT エントリを一時的に生成し，VAT テーブルに格納する．この VAT エントリの状態はネゴシエーション実行中であることを示す “`WAIT`” 状態となり，ネゴシエーションのトリガとなった TCP/UDP パケットはカーネルメモリ内に待避しておく．VAT エントリがこの状態時に，トリガパケットに続くパケットが上位アプリケーションから IP 層に渡された場合，そのパケットは破棄される．MN が NAT-f マッピング応答を受信すると，VAT エントリの状態はアドレス変換を指示する “`TRANSLATE`” となり，有効なエントリとなる．NAT-f ネゴシエーションは短時間で完了するため，TCP における再送処理が発生することはない．VAT エントリは無通信状態が一定時間以上続いた場合，または TCP コネクションが切断された場合にカーネルタイマにより削除する．

仮想 IP アドレスは CN の FQDN に対応して生成する．仮想 IP アドレスを “A.B.C.D” と表記した場合，各バイトには以下の値が設定される．A はユーザが設定することができ，実ネットワーク上に一致するアドレスが存在しなければ任意の値でよい．プロトタイプシステムでは，実験的目的のために予約されているクラス E にあたる 240 を設定した．NAT-f モジュールはこの値により，仮想 IP アドレスか否かを判断する．B は初期値として 0 が設定される．C は CN のドメイン名のハッシュ値が，D は CN のホスト名のハッシュ値が設定される．ハッシュ関数の出力値の範囲は 1〜254 とした．このように仮想 IP アドレスを割り当てることにより，異なるホームネットワークに同じホスト名のノードが存在しても，重複を避けることができ，MN は仮想 IP アドレスより対応するホスト名を NRT から取得することができる．ハッシュが衝突した場合は，B を異なる値に変化させることにより，仮想 IP アドレスと CN のホスト名を一意に対応づけることができる．

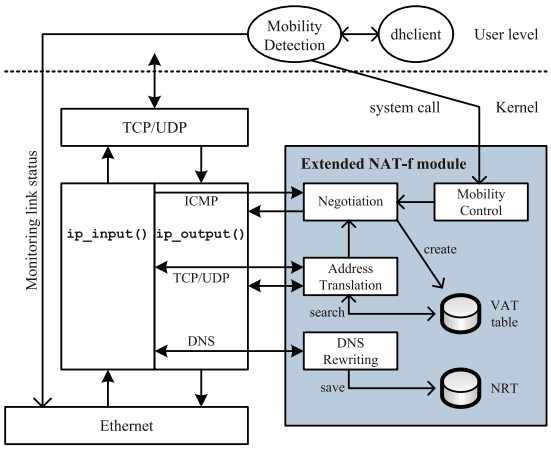


図 8 MN における拡張 NAT-f の実装
Fig. 8 Implementation of Extended NAT-f in MN.

MN は DHCP などにより新たな IP アドレスが割り当てられた場合，HGW に対して拡張 NAT-f マッピング要求を送信する必要がある．IP アドレスがインタフェースに割り当てられるとき，IP アドレスの変化を検知したら，VAT テーブル内の古い IP アドレスで生成されたエントリの状態を “`TRANSLATE`” から，移動通知を指示する “`IP_NOTICE`” に変更する．その後，移動検知アプリケーションから移動通知システムコールが発行されると，カーネルでは状態が “`IP_NOTICE`” となっている VAT エントリに対して，拡張 NAT-f マッピング要求を生成し，送信する．

4.2 移動検知処理

IPv4 ネットワークでは，IPv6 ルータが定期的に送信する RA（Router Advertisement）のような仕組みがないため，MN は移動を検知する手段がない．Mobile IPv4 では FA からのエージェント広告により移動の検知は可能であるが，本提案方式では FA のような装置がないため，MN が自律的に解決する手段が必要となる．今回はインタフェースのリンク状態を監視するアプリケーションを作成し，移動検知を実現した．

図 9 に移動検知処理の仕組みを示す．移動検知処理は定期的に `ioctl` システムコールを実行することにより，インタフェースのリンク状態を取得する．取得したリンク状態が “no carrier” から “active” に変化したら，ネットワークに接続したと判断する．次にルーティングソケットを利用して，ルーティングテーブルからゲートウェイの IP アドレスを取得し，それを宛先として ICMP Echo を送信する．応答を受信した場合，同一ネットワークに再接続したと判断し，再びリンク状態の監視を続ける．一定時間内に応答を受信できなかった場合，ゲートウェイが変わったと見な

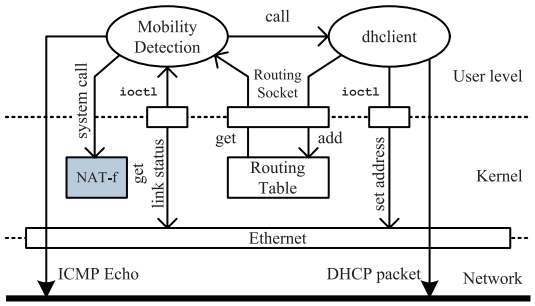


図 9 移動検知処理の仕組み
Fig. 9 Mechanism of mobility detection process.

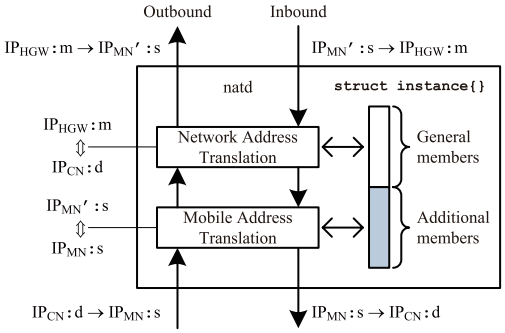


図 10 Mobile PPC 対応 natd の仕組み
Fig. 10 Mechanism of natd improved for Mobile PPC.

せるため，異なるネットワークに接続したと判断し，dhclient☆ を実行する．dhclient は DHCP サーバより DHCP ACK を受信すると，`ioctl` システムコールを通じて IP アドレスの設定を行う．その後，Gratuitous ARP による二重アドレスチェック，およびルーティングテーブルにゲートウェイ情報の設定を行う．以上の処理が完了したら，カーネルに対して移動通知システムコールを発行する．

4.3 natd の拡張

図 10 に Mobile PPC に対応した natd☆☆ の仕組みを示す．natd は構造体 `instance` に NAT マッピング情報を格納する．この構造体のメンバを拡張することにより，受信した拡張 NAT-f マッピング要求に含まれる MN の移動前後の IP アドレスを保持する．このデータは natd が疑似パケットをフックすることにより設定する．疑似パケットとは CN から MN への通信パケットに見せかけたパケットであり，NAT マッピング情報を生成するために用いられる．疑似パケットは既存の NAT-f と同じ手法で生成され[17]，疑似パケットの TCP/UDP ペイロード部には拡張 NAT-f マッピング要求に含まれていたデータを転記する．

natd には通常のアドレス変換機能に加えて，Mobile PPC のカーネルで実行していた移動アドレス変換を実装した．NAT 内部への通信に対しては，通常の NAT 処理により宛先をマッピングされた CN の情報へ変換した後，移動アドレス変換処理により，MN の移動後 IP アドレスから移動前 IP アドレスに変換する．NAT 外部への通信に対しては，上記と逆の順序で処理することにより，CN へのマッピングと MN の移動前後のマッピングを同時に実現する．

なお，プロトタイプシステムでは HGW のカーネル部に，ネゴシエーション応答処理など，従来の NAT-f と同一の機能を実装したが，natd にネゴシエーション処理機能を実装することも可能である．この方法では HGW のカーネルには機能を実装する必要がなくなるため，容易に提案手法に対応した HGW を実現することが可能になる．

☆ FreeBSD に搭載されている DHCP クライアントアプリケーション．
☆☆ FreeBSD に搭載されている NAT アプリケーション．

5. ま と め

本稿では NAT 越え技術の NAT-f と，移動透過技術の Mobile PPC を融合した拡張 NAT-f を提案した．拡張 NAT-f により，MN と NAT は MN の移動前後の IP アドレスの関係，および CN と NAT のマッピング関係を共有し，NAT-f における仮想アドレス変換と Mobile PPC による移動アドレス変換を同時に行う．これにより，NAT 外部の MN は NAT 配下の CN に通信を開始し，かつ通信中に移動しても通信継続性が保証される．

今後は実装したプロトタイプシステムにより，通信開始時や移動時の処理遅延，およびアドレス変換処理がスループットに与える影響などの評価を行う．

参 考 文 献

1) Perkins, C.: IP Mobility Support for IPv4, RFC3220, IETF (2002).
2) Johnson, D., Perkins, C. and Arkko, J.: Mobility Support in IPv6, RFC3775, IETF (2004).
3) Ishiyama, M., Kunishi, K., Uehara, K., Esaki, H. and Teraoka, F.: LINA: A New Approach to Mobility Support in Wide Area Networks, *IEICE Trans. Comm.*, Vol. E84-B, No. 8, pp. 2076–2086 (2001).
4) 相原玲二，藤田貴大，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).
5) Bhagwat, P., Maltz, D. and Segall, A.: MSOCKS+: an architecture for transport layer

mobility, *Computer Networks*, Vol.39, No.4, pp. 385–403 (2002).
6) Snoeren, A. and Balakrishnan, H.: An End-to-End Approach to Host Mobility, *Proc. ACM/IEEE MobiCom2000*, pp.155–166 (2000).
7) 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).
8) Rosenberg, J.: Interactive Connectivity Establishment (ICE): A Methodology for Network Address Translator (NAT) Traversal for Offer/Answer Protocols, Internet-draft, IETF (2007). draft-ietf-mmusic-ice-15.txt.
9) UPnP Forum: *Internet Gateway Device (IGD) Standardized Device Control Protocol V 1.0* (2001). http://www.upnp.org/standardizeddcps/igd.asp.
10) Huitema, C.: Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs), RFC4380, IETF (2006).
11) 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).
12) Guha, S. and Francis, P.: Characterization and Measurement of TCP Traversal through NATs and Firewalls, *Proc. ACM International Measurement Conference (IMC)*, pp. 199–211 (2005).
13) Montenegro, G.: Reverse Tunneling for Mobile IP, revised, RFC3024, IETF (2001).
14) Levkowetz, H. and Vaarala, S.: Mobile IP Traversal of Network Address Translation (NAT) Devices, RFC3519, IETF (2003).
15) 清水智行，中村素典，美濃導彦：NAPT を越えた端末の移動時の TCP コネクション維持による移動透過性保証プロトコル，情報処理学会研究報告，2001-DPS-107, Vol.2002, pp.25–30 (2002).
16) 榎本万人，鈴木秀和，坂本順一，渡邊　晃：プライベートアドレス空間とグローバルアドレス空間を跨る移動透過性の検討，*DICOMO2006*, Vol.2006, pp.813–816 (2006).
17) 鈴木秀和，渡邊　晃：アドレス空間透過性を実現する NAT-f の実装と評価，*DICOMO2006*, Vol.2006, pp.453–456 (2006).
18) Ferguson, P. and Senie, D.: Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, RFC2827, IETF (2000).
19) 鈴木秀和，渡邊　晃：フレキシブルプライベートネットワークにおける動的処理解決プロトコル DPRP の実装と評価，情報処理学会論文誌, Vol.47, No.11, pp.2976–2991 (2006).
20) 後藤裕司，鈴木秀和，渡邊　晃：グローバルアドレスとプライベートアドレス空間を跨る DPRP の検討，情報処理学会第 68 回全国大会講演論文集 (2006). 講演番号 3R-3.

Multimedia, Distributed, Cooperative, and Mobile (DICOMO) Symposium
July 4th–6th, 2007
Program No. 5A-1

NAT-fの移動透過通信への拡張

名城大学大学院理工学研究科
鈴木 秀和　　金本 綾子　　渡邊 晃

Agenda

異種アドレス空間における移動透過性の実現

1. IPv4における移動透過技術
2. 異種アドレス空間に対応した従来技術と課題
3. NAT越え技術
4. 提案手法
   - 通信開始時
   - ノード移動時

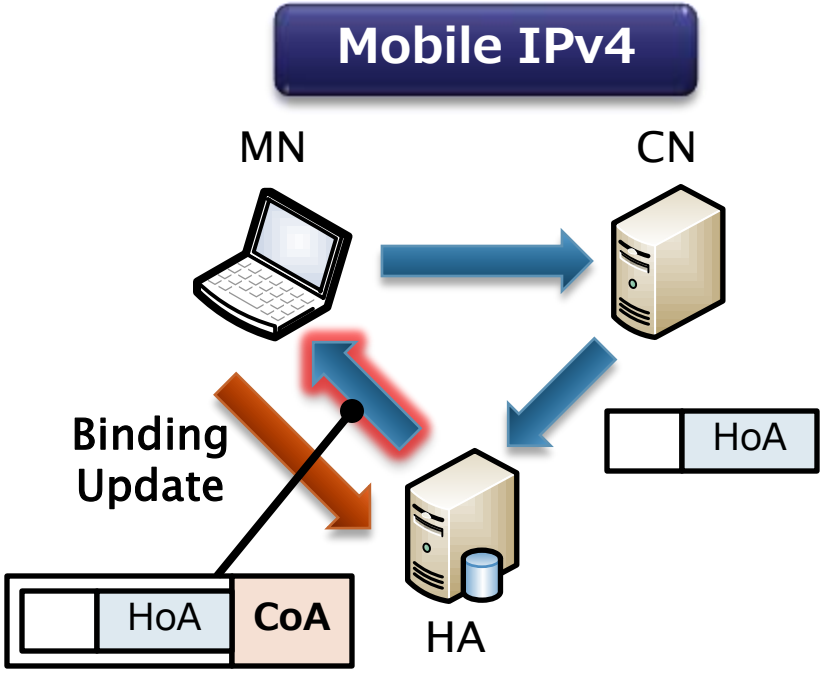
移動透過性
ノード到達性と通信継続性を満たす
（通信開始時）（移動時）

移動透過技術

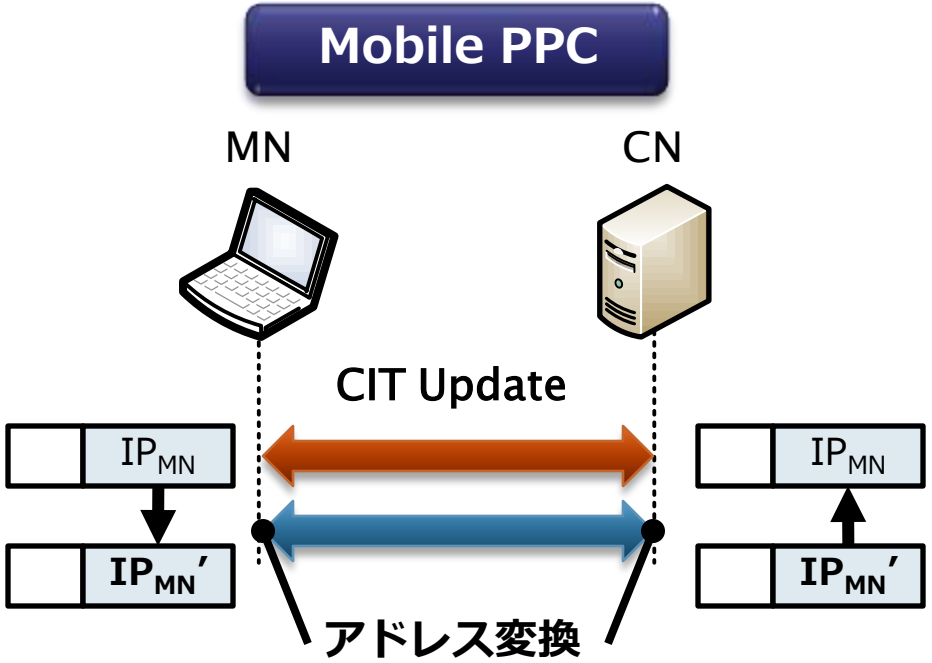
移動通知
通信
トンネリング通信

MN：移動ノード
CN：通信相手ノード

MN移動時の動作



移動前IP（HoA）を
移動後IP（CoA）で
カプセル化



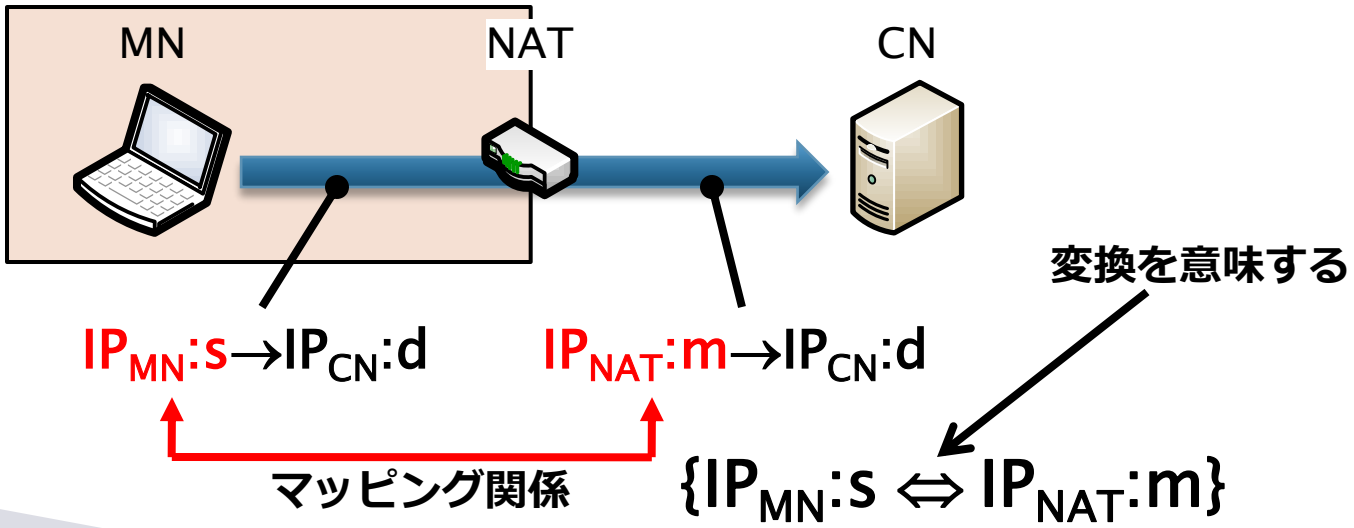
移動前IP（IP_{MN}）を
移動後IP（IP_{MN}'）へ
アドレス変換

IPv4における問題点

- 従来のIPv4における移動透過技術
  - 同一アドレス空間を前提（Global⇔Global ）

- ホームネットワークはプライベートアドレス空間
  - NATはグローバル／プライベートIPアドレスを変換

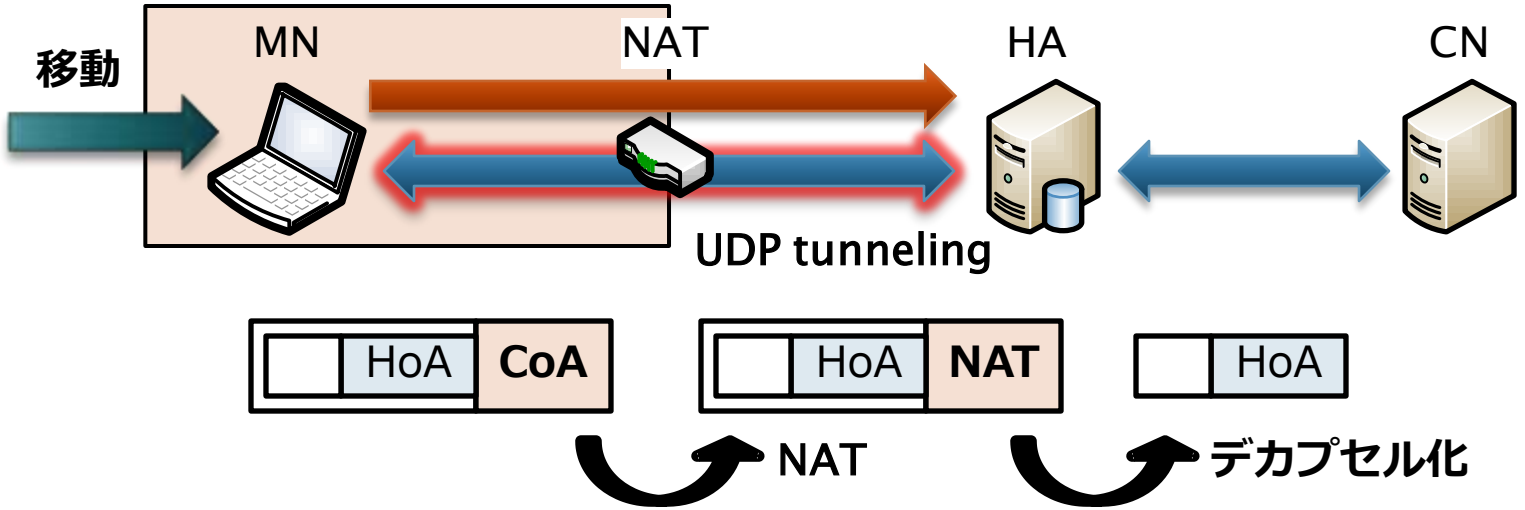
  ➔**外部からNAT背後のノードが見えない**



異種アドレス空間対応技術

MN移動時の動作

- Mobile IPベース
  - RFC3024　Reverse Tunneling for Mobile IP
  - RFC3519　Mobile IP Traversal of NAT Devices

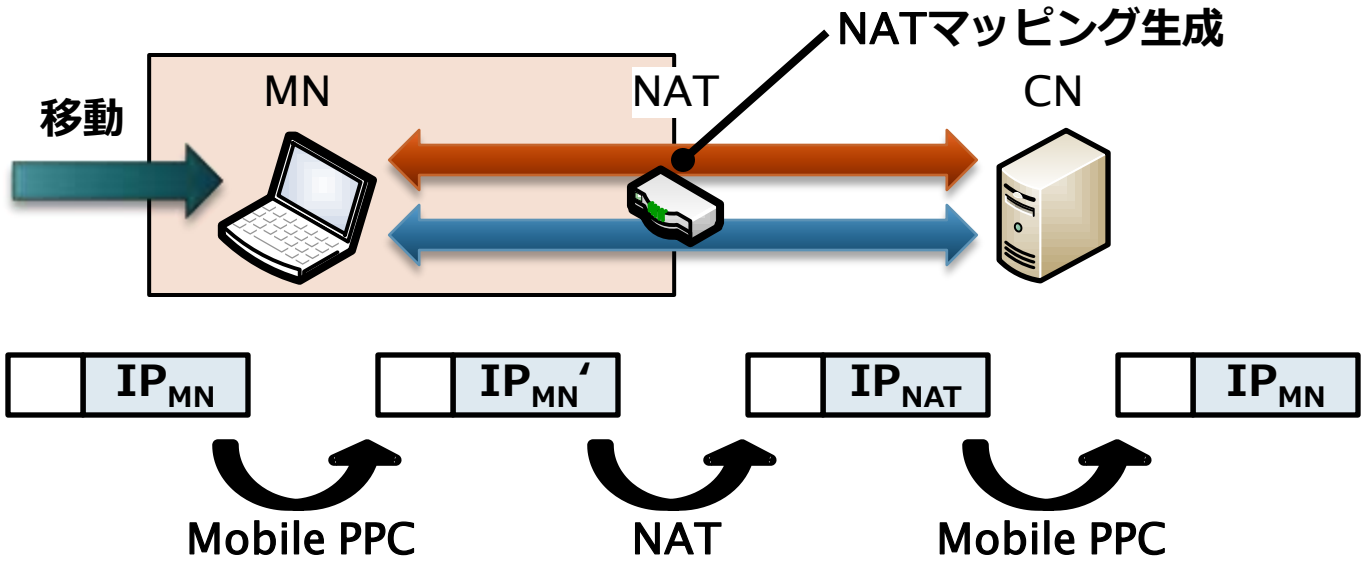


MNとCN間は双方向トンネリング
➔NATのアドレス変換による影響を防止

異種アドレス空間対応技術

MN移動時の動作

- Mobile PPCベース
  - 拡張Mobile PPC（DICOMO2006，pp.813-816）



移動通知時にNATはマッピング処理を実行

➔NATを考慮したMobile PPCアドレス変換を実行

従来技術の課題

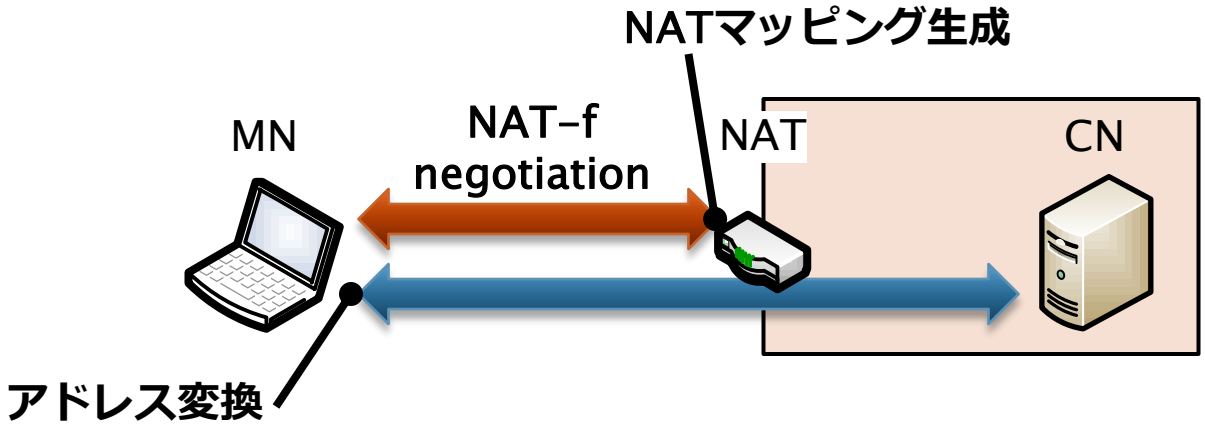
- 従来技術の共通点
  - MNはNATの内外を自由に移動可能（**通信継続性を実現**）
  - MNは移動前にCNと通信していることを前提
    ➔**ノード到達性を満たしていると想定**

- Mobile PPCは両ノードが共に移動可能
  ➔**通信相手がNAT配下にいる可能性は高い**
  ➔**従来技術ではノード到達性を満足できない**

NAT越え技術を利用することにより
ノード到達性の問題を解決する

NAT越え技術

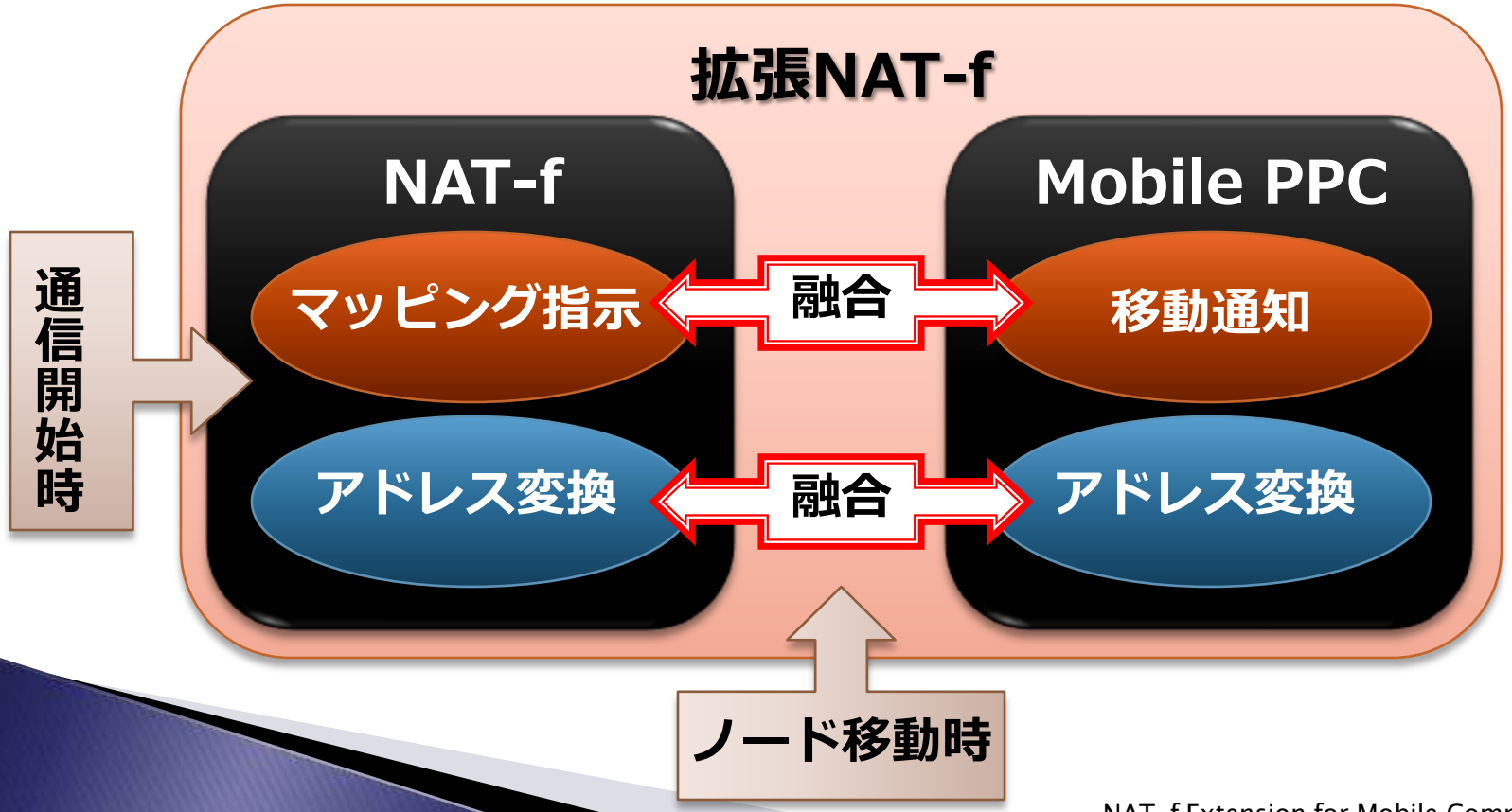
- NAT配下のノードに対して通信を開始する技術
  - UPnP（Universal Plug and Play）
  - ICE（Interactive Connectivity Establishment）
  - **NAT-f（NAT-free protocol）** ← 提案技術



- NATにマッピング生成を指示
- パケットの宛先をマッピングアドレスに変換

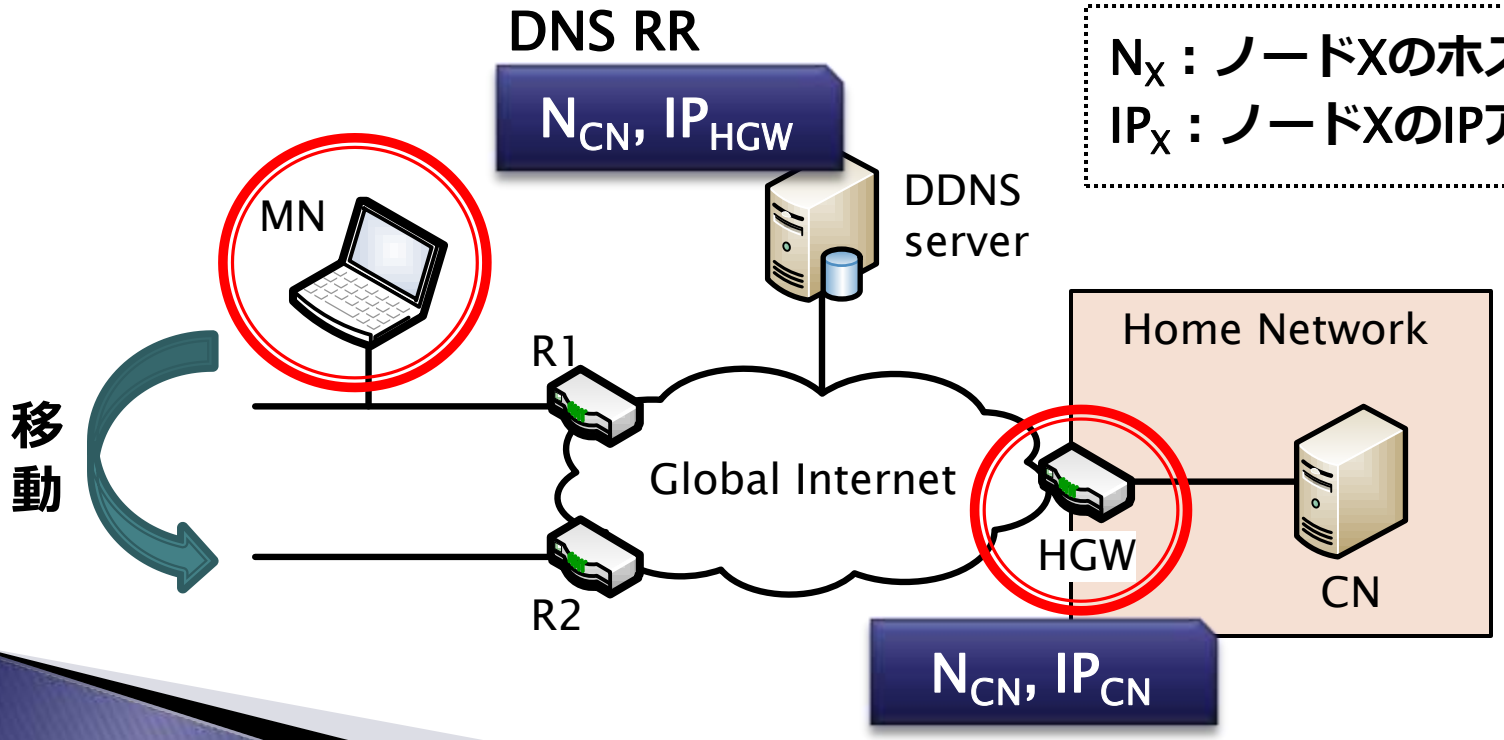
拡張NAT-fの提案

- NAT-fとMobile PPCの共通機能を融合
  - ネゴシエーション（マッピング指示，移動通知）
  - アドレス変換処理



提案方式の構成と初期登録

- MNとHGW（ホームゲートウェイ）に実装
- 初期情報と登録先
  - MNから見たCNの情報（N_{CN}，IP_{HGW}）→ DDNSサーバ
  - 実際のCNの情報（N_{CN}，IP_{CN}）→ HGW

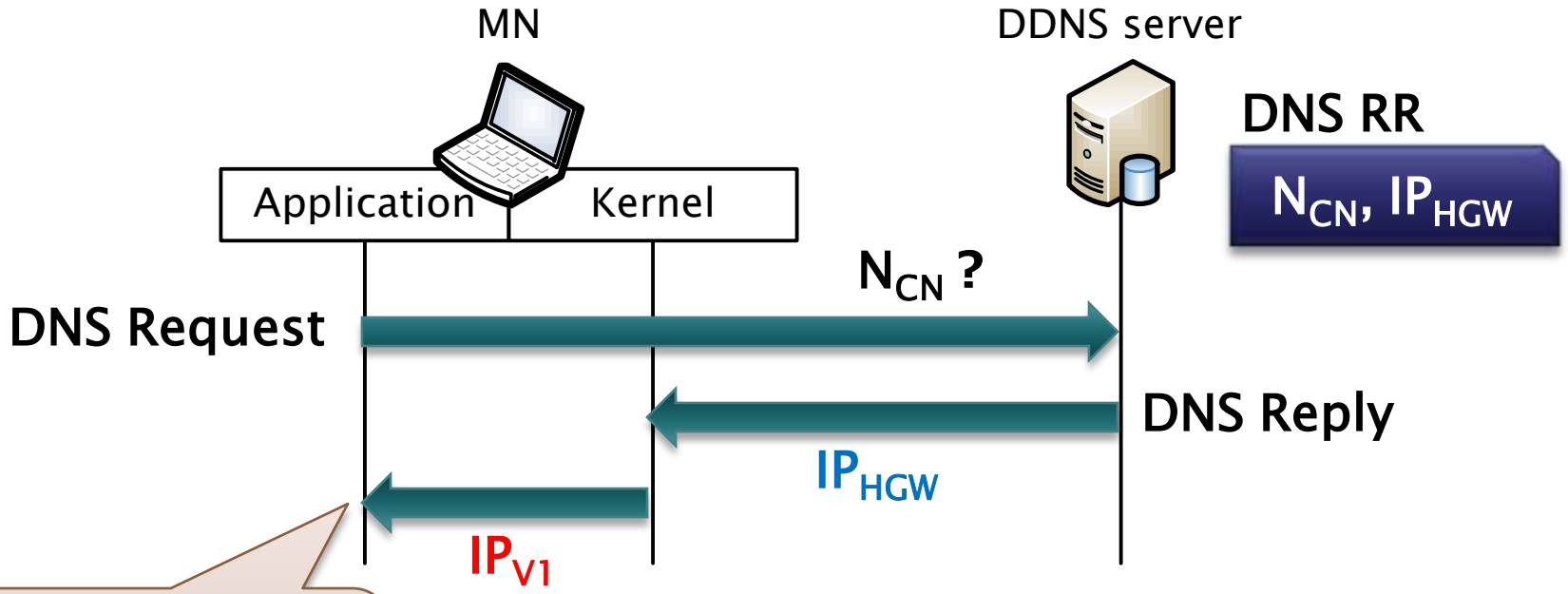


通信開始時　～DNS名前解決～

Watanabe Lab.
Department of Information Engineering, Meijo University
Information Networks Laboratory

NAT-f

- DNS応答の書き換え
  - 通知されたIP_{HGW} → 仮想IPアドレスIP_{V1}



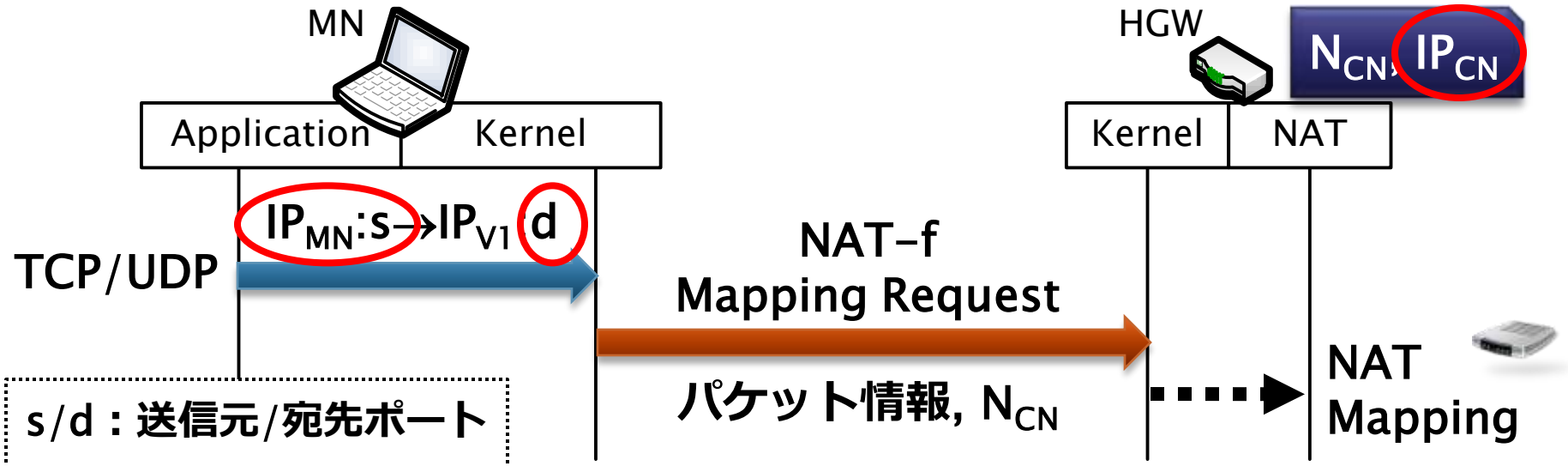
アプリケーションは
CNのアドレスを
IP_{V1}と認識

VIP

通信開始時　～マッピング要求～

NAT-f

- NAT-fネゴシエーションにより情報通知
- HGWはNATマッピングを生成
  - マッピングアドレス＝IP_{HGW}:m



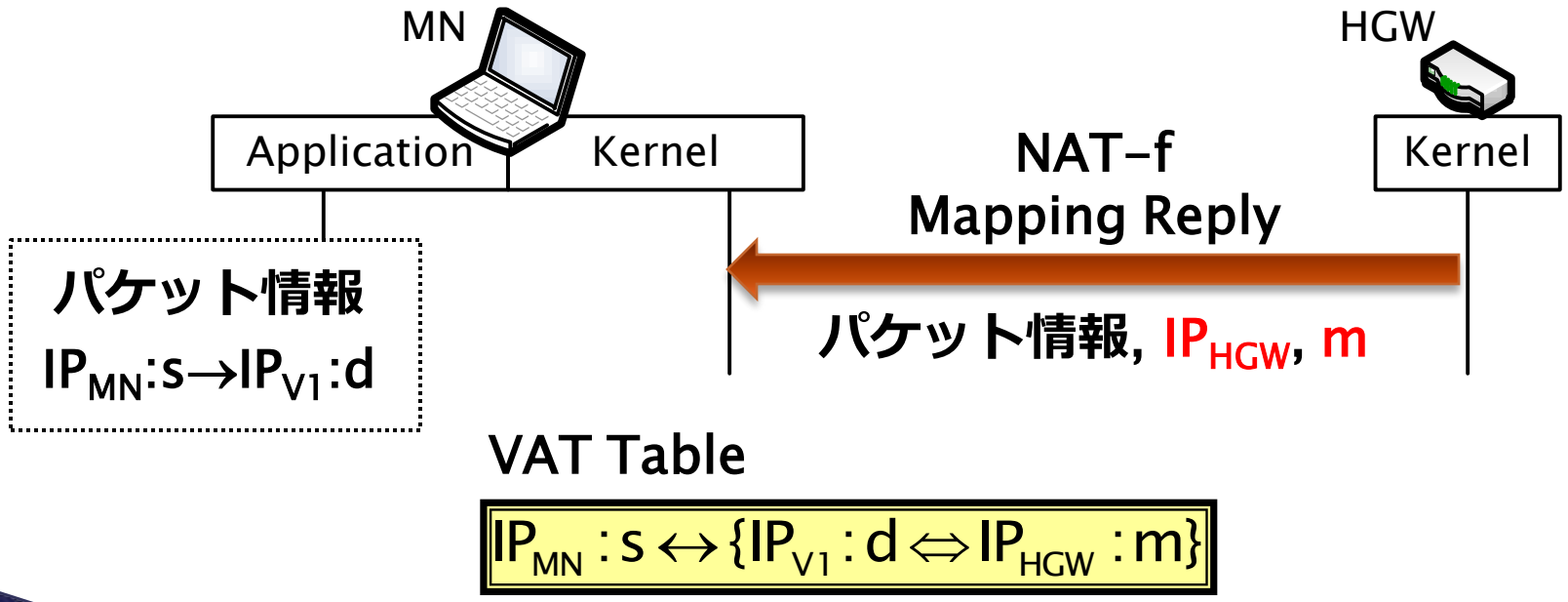
NAT Mapping

$IP_{MN}:s \leftrightarrow \{IP_{HGW}:m \Leftrightarrow IP_{CN}:d\}$

↔ … 送受信関係
⇔ … 変換関係

通信開始時　～マッピング応答～

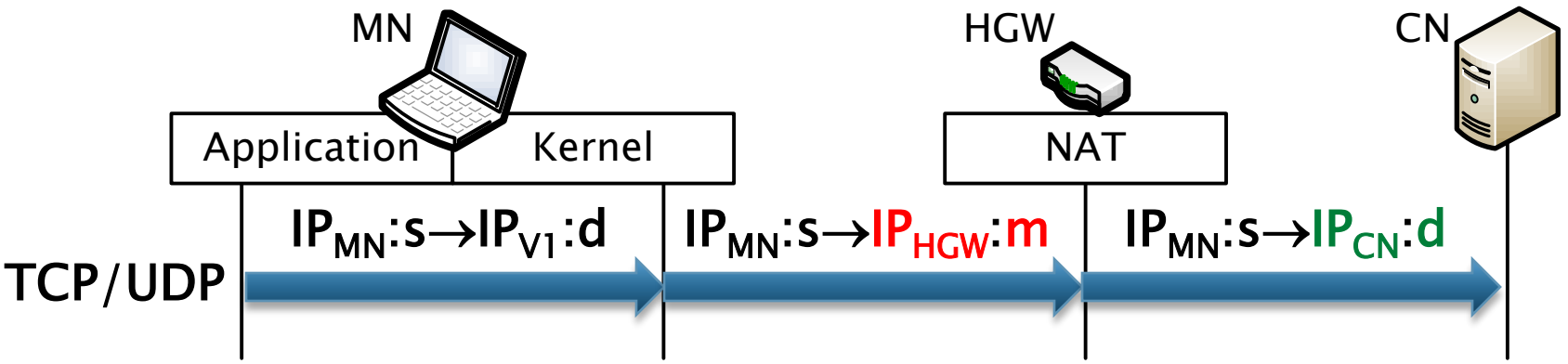
- HGWはマッピングアドレスを応答
- MNはVATテーブルを生成
  - 仮想IPアドレスとマッピングアドレスの変換関係を示す



通信開始時　～仮想アドレス変換～

NAT-f

赤字：NAT-f　緑字：NAT



VAT Table

$IP_{MN} : s \leftrightarrow \{IP_{V1} : d \Leftrightarrow IP_{HGW} : m\}$

NAT Mapping

$IP_{MN} : s \leftrightarrow \{IP_{HGW} : m \Leftrightarrow IP_{CN} : d\}$

MNからNAT配下のCNに対して通信開始を実現

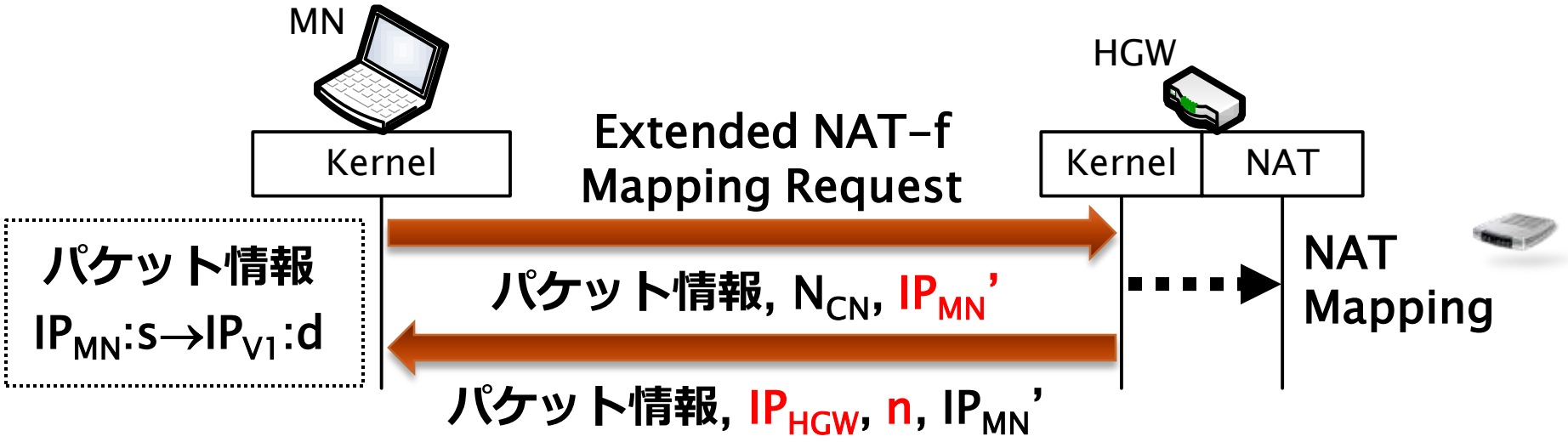
ノード到達性の実現

ノード移動時

Watanabe Lab.

拡張NAT-f

- MNが移動　IPアドレス：IP_{MN}→IP_{MN}'
- 拡張NAT-fネゴシエーション
  - 通常のマッピング要求情報+**移動後のIPアドレス**



VAT Table

$$\{IP_{MN}:s \Leftrightarrow IP_{MN}':s\} \leftrightarrow \{IP_{V1}:d \Leftrightarrow IP_{HGW}:n\}$$

NAT Mapping

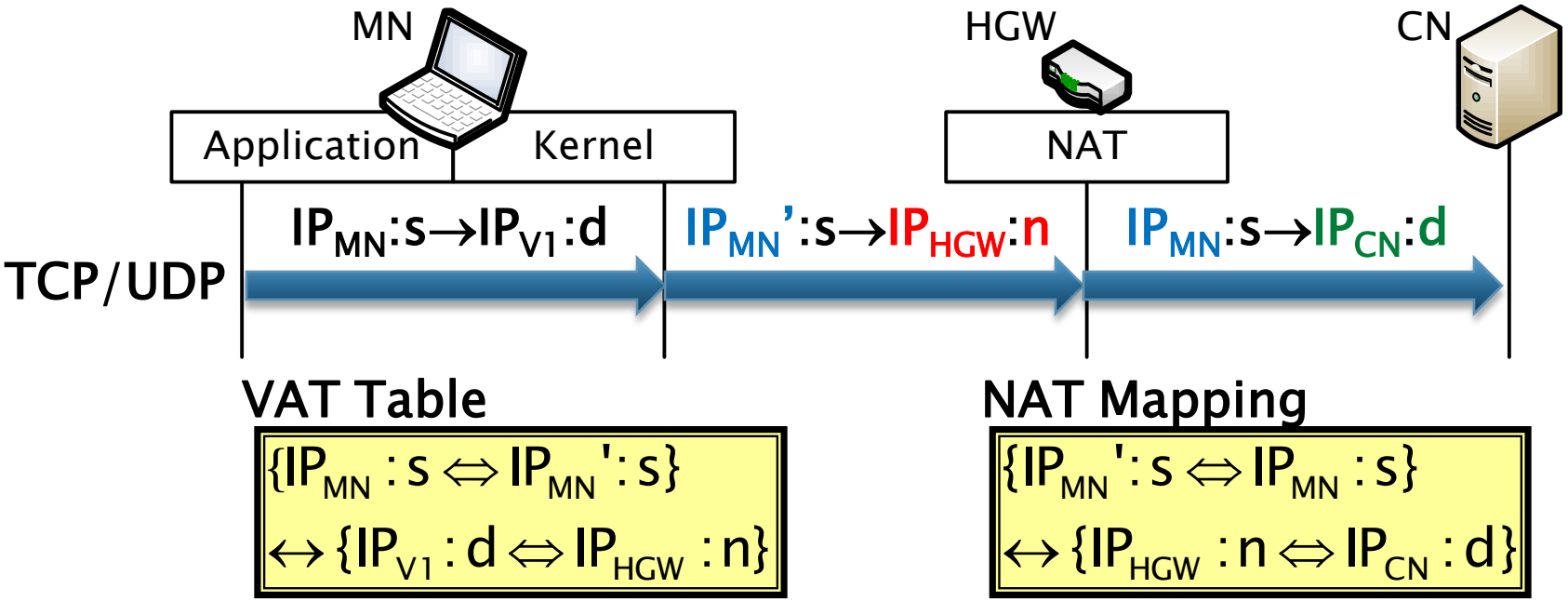
$$\{IP_{MN}':s \Leftrightarrow IP_{MN}:s\} \leftrightarrow \{IP_{HGW}:n \Leftrightarrow IP_{CN}:d\}$$

ノード移動時

青字：Mobile PPC
赤字：NAT-f
緑字：NAT

Watanabe Lab.
Department of Information Engineering, Meijo University
Information Networks Laboratory

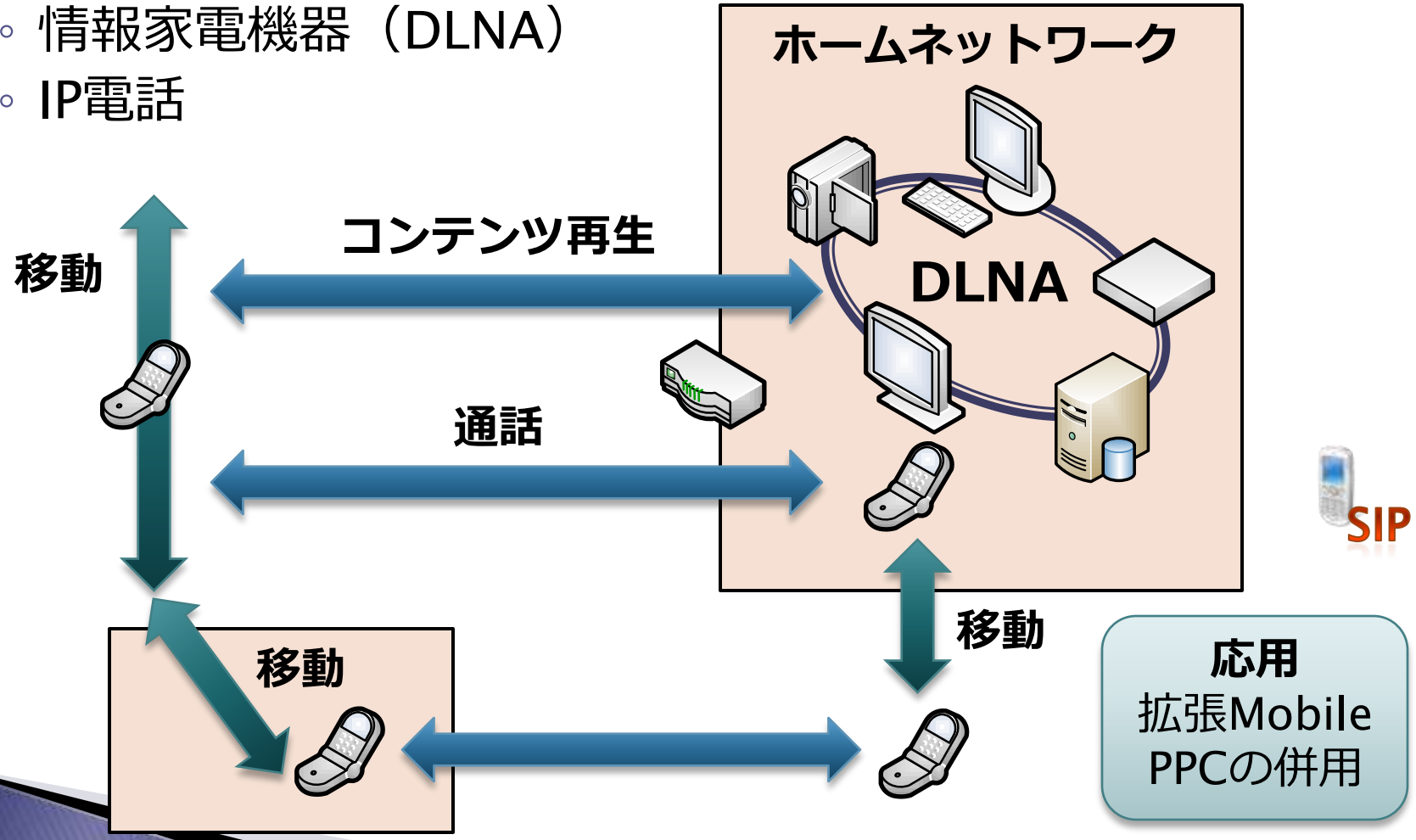
拡張NAT-f



HGWにおいてMNの移動をCNに対して隠蔽することにより，MNとCN間の通信を継続

提案方式の利用シーン

- ホームネットワークのノードと通信中に移動
  - 情報家電機器（DLNA）
  - IP電話



まとめ

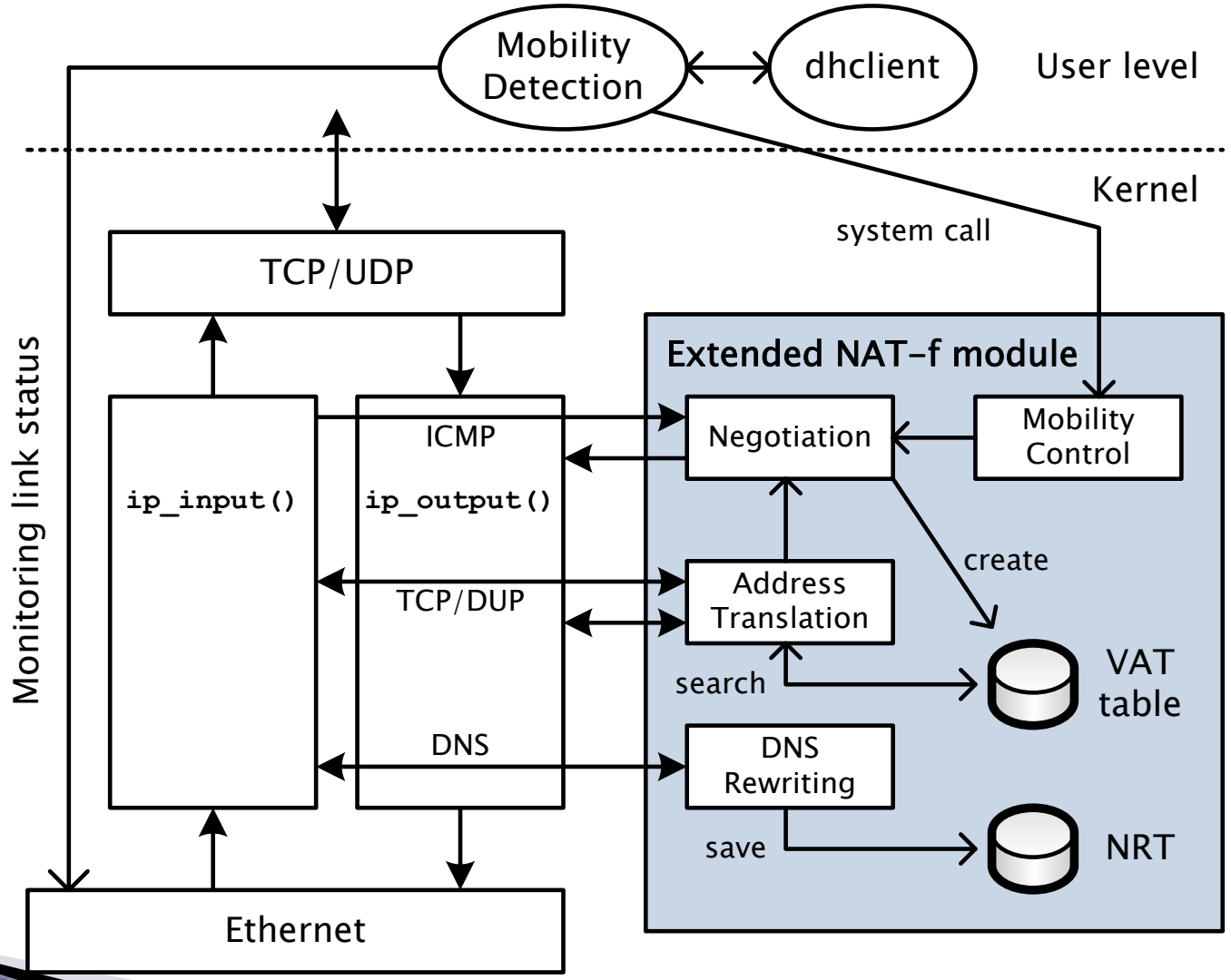
- 拡張NAT-fを提案
  - 通信開始時：NAT-f
  - ノード移動時：拡張NAT-f ＝ NAT-f ＋ Mobile PPC

  ➔異種アドレス空間における移動透過性を実現

- プロトタイプシステムの実装
  - 動作確認までは完了（通信の継続を確認）

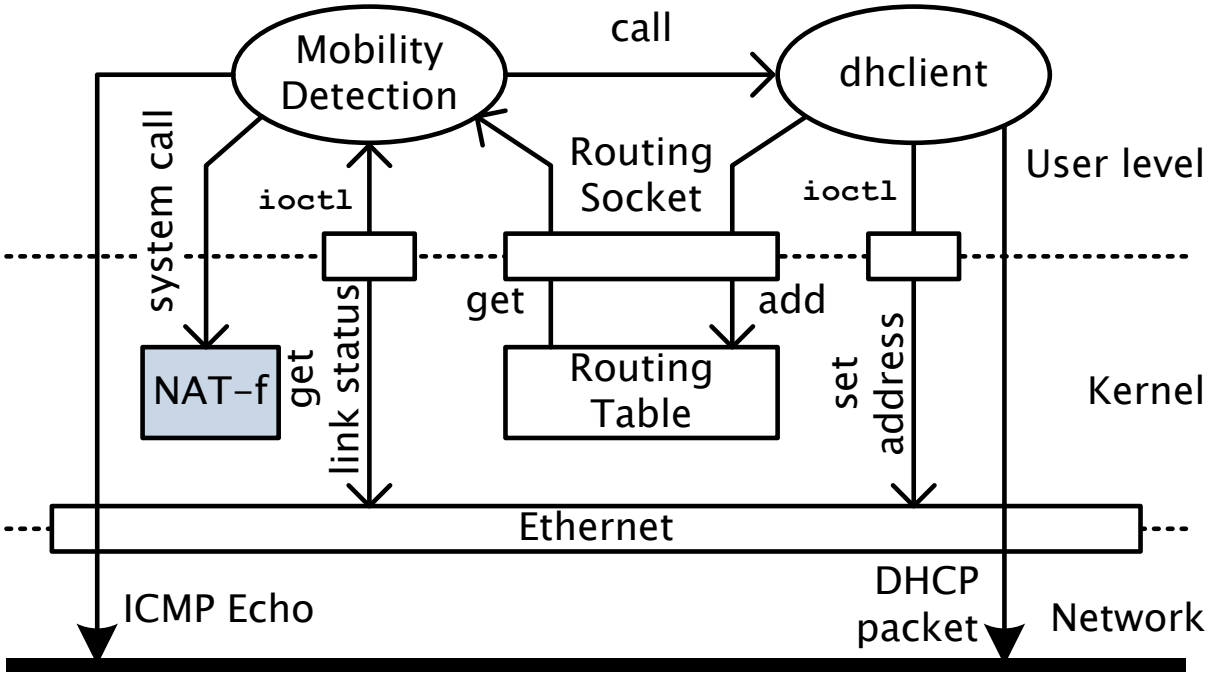
- 今後の課題
  - 性能評価（通信開始時，移動時の処理遅延）
  - IPv4とIPv6混在環境への対応

実装　～移動ノード側～

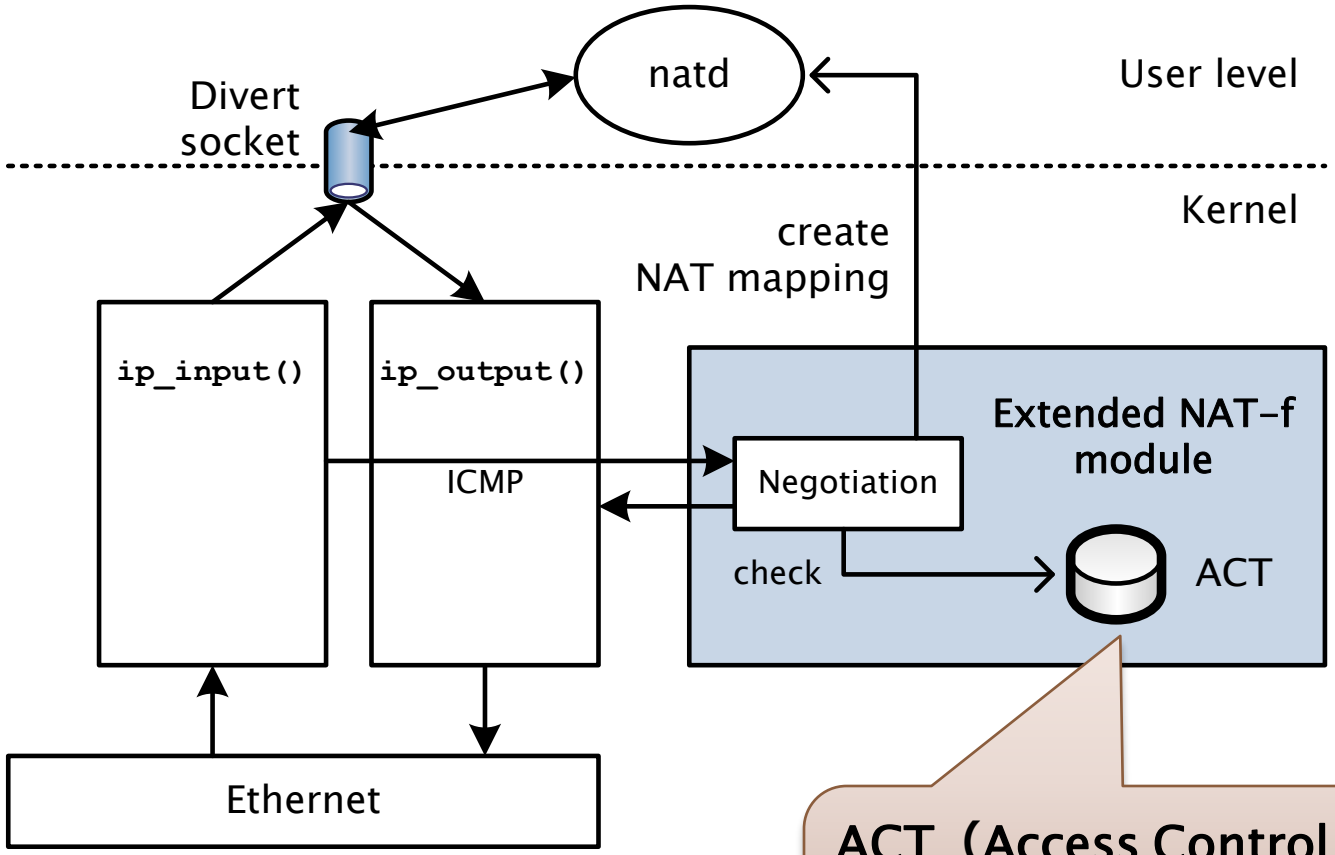

Mobility Detection
dhclient
User level
Kernel
system call
TCP/UDP
Extended NAT-f module
Monitoring link status
ip_input()
ip_output()
ICMP
TCP/DUP
DNS
Negotiation
Mobility Control
Address Translation
create
search
VAT table
DNS Rewriting
save
NRT
Ethernet

実装　～移動検知～

- インタフェースのリンク状態を監視
  - ステータス：”no carrier”→”active” ➔ 移動したと判断
  - GWにping：応答なし ➔ DHCP実行



実装　～HGW側～

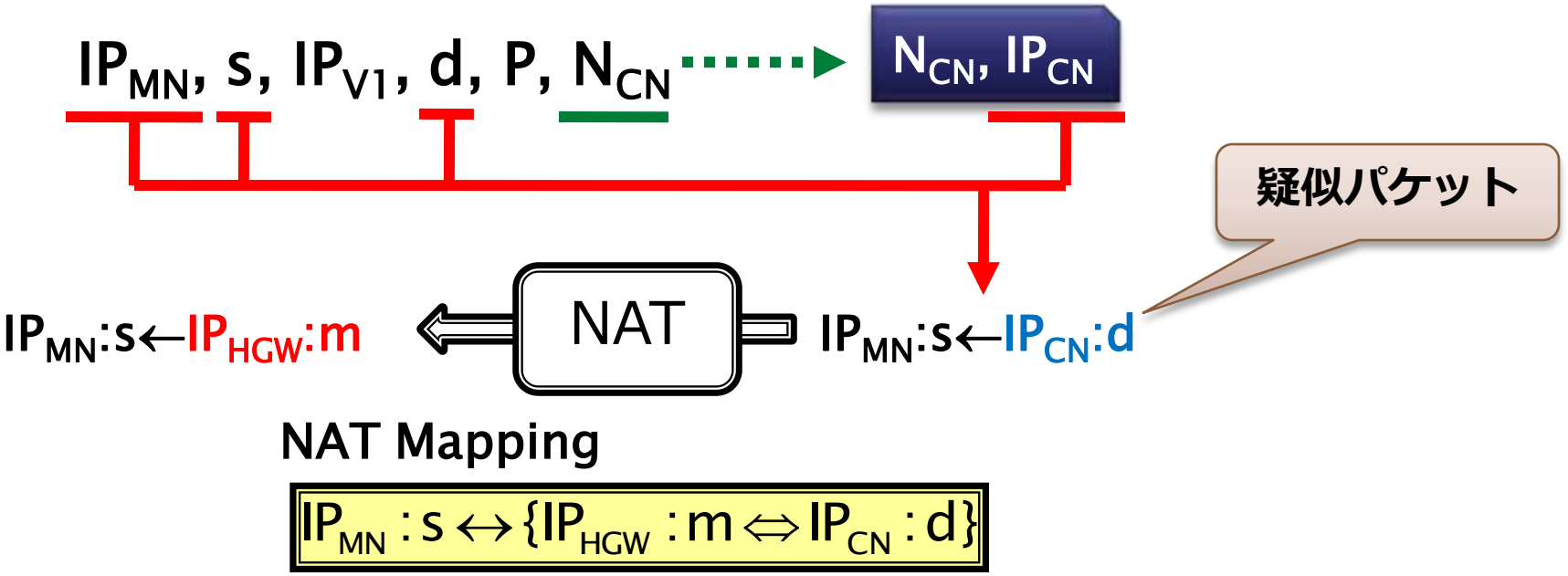


ACT（Access Control Table）

CNのホスト名とプライベートIPアドレスを格納

NATのマッピング方法

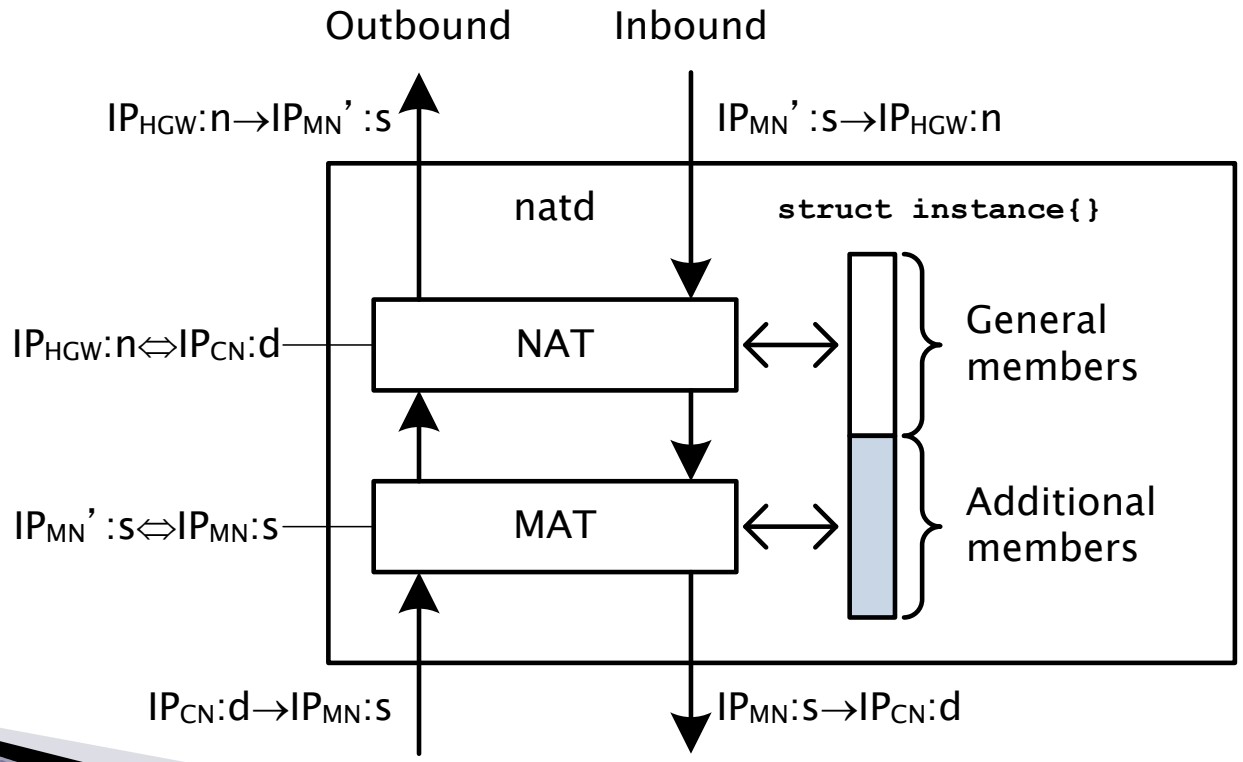
- MNからの通知情報とIP_{CN}から疑似パケットを生成
  - CNからMNへの送信パケットに見せかけたデータ



現在はカーネルで作成しているが，NATデーモンで直接マッピングを生成することは可能

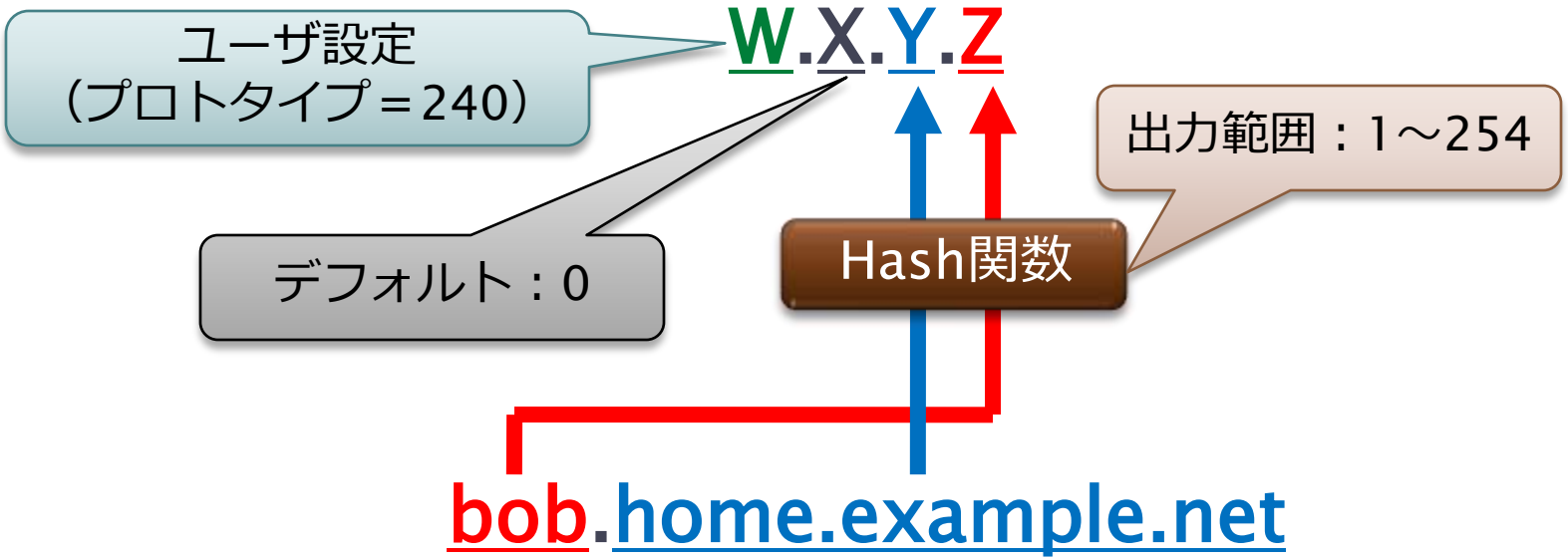
実装　～NATの改良～

- 移動アドレス変換（MAT）機能を追加
  - MNとHGW間→MN移動後のIPアドレス
  - CNとHGW間→MN移動前のIPアドレス



仮想IPアドレス

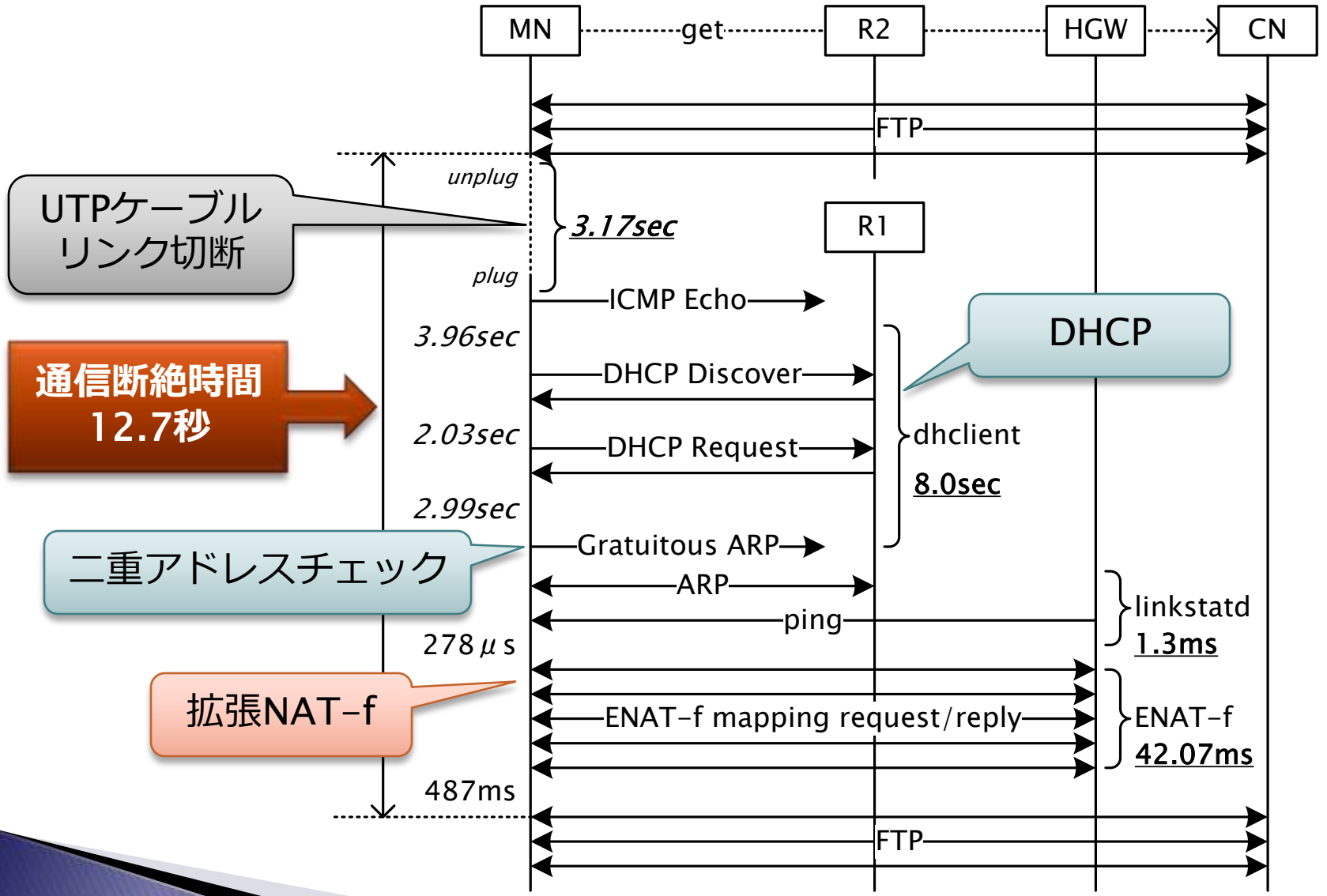
- MNのL3より上位層でのみ有効なアドレス
- CNのFQDNに対応して割り当てる



- ハッシュが衝突した場合
  - Xを異なる値に変化➔**仮想IPアドレスとCNが一意に対応**

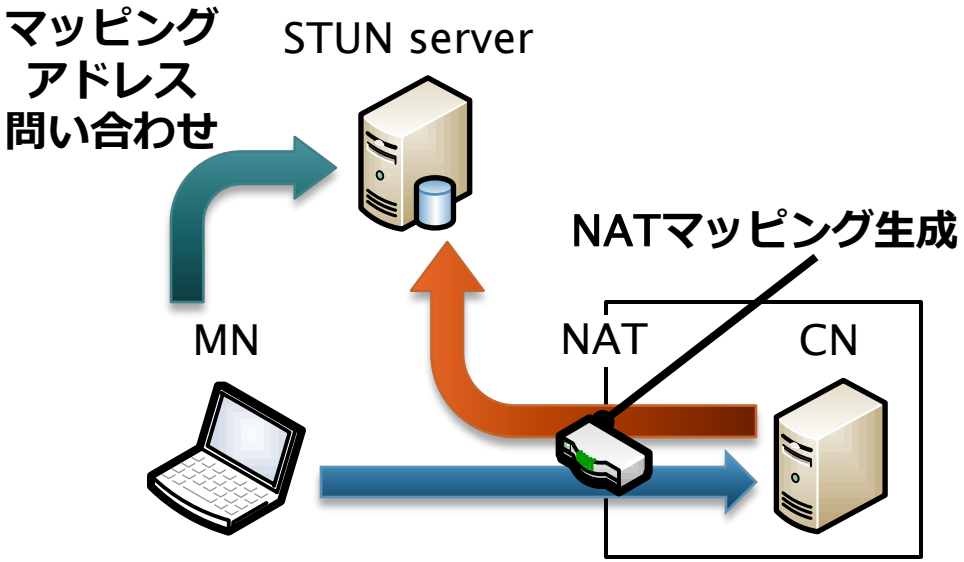
通信断絶時間

R1,R2：WZR-G144NH
Buffalo社製無線BBR



ICE (Interactive Connectivity Establishment)

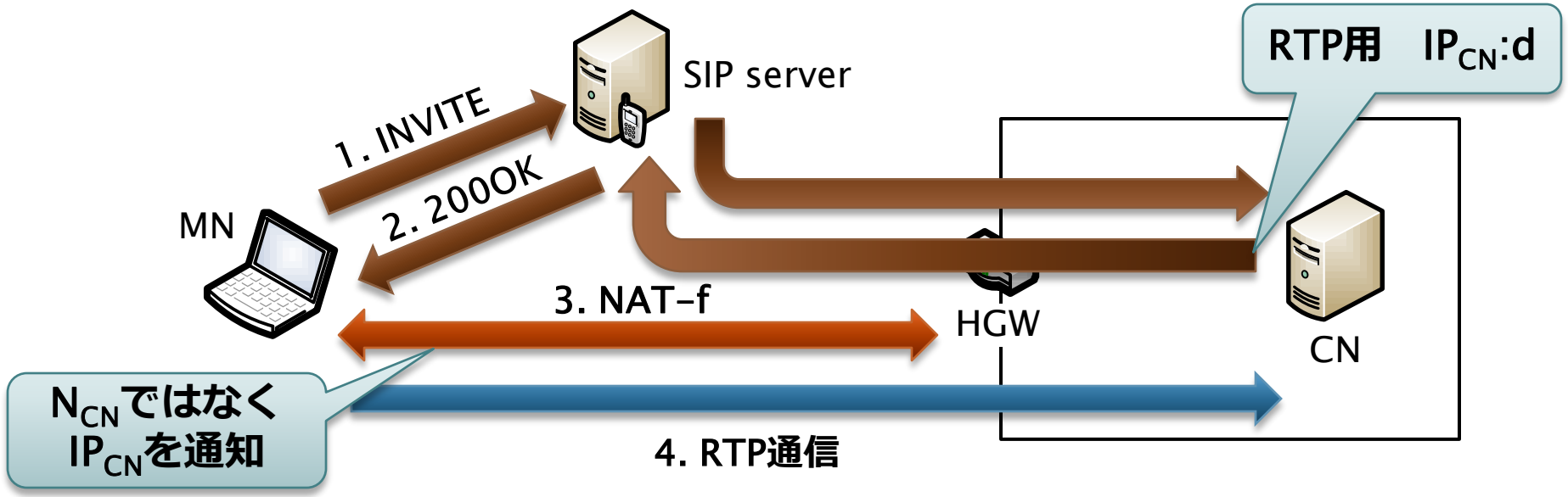
- IETF-Draft（draft-ietf-mmusic-ice-14）
  - STUN，TURNを用いるフレームワーク
  - SIPアプリケーションのNAT越え



1. Binding Requestを送信
2. NATマッピングを生成
3. マッピングアドレスを保存
4. マッピングアドレスを取得
5. パケットの宛先をマッピングアドレスに設定して送信

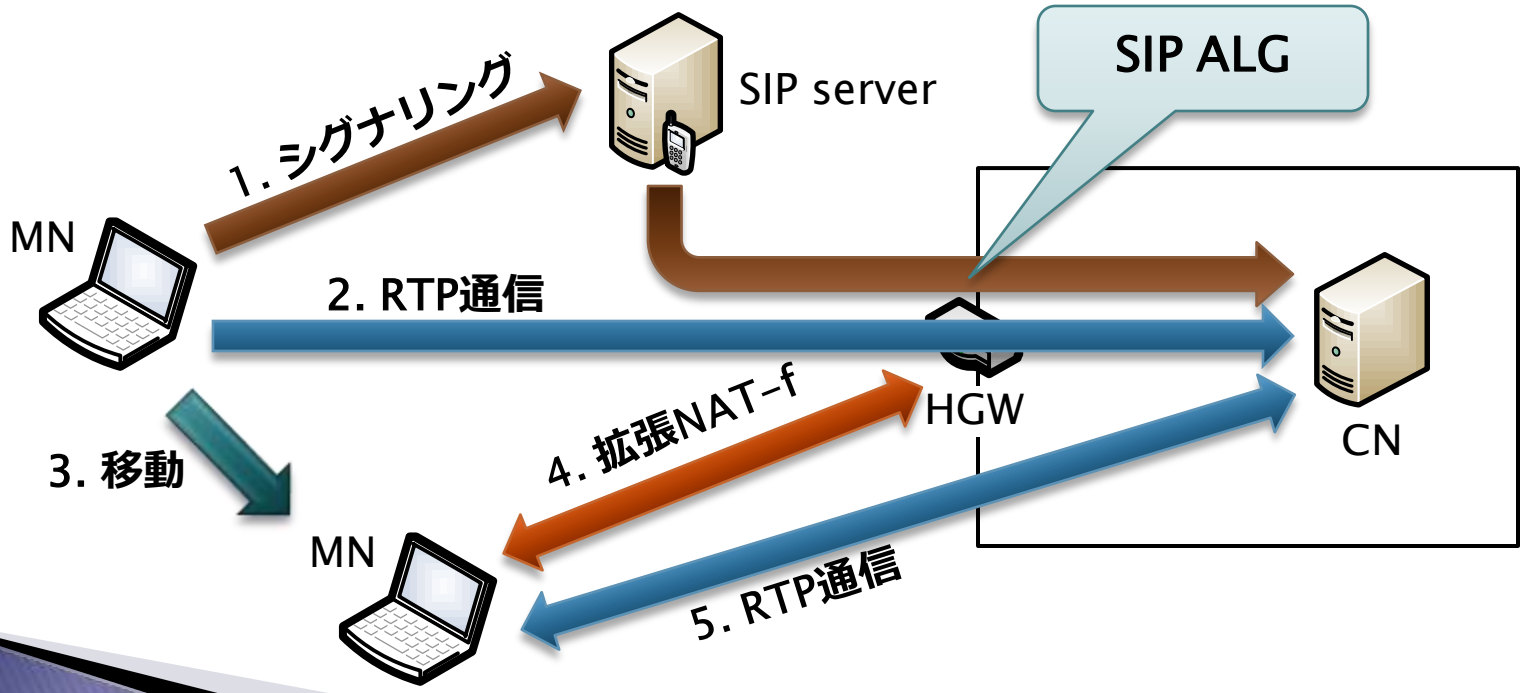
SIPへの対応（1）

- SIPのNAT越えはRFC3581で対応
- NAT-fはその後のRTP通信のNAT越えに利用
  - 200 OKに含まれる情報でNATマッピング生成

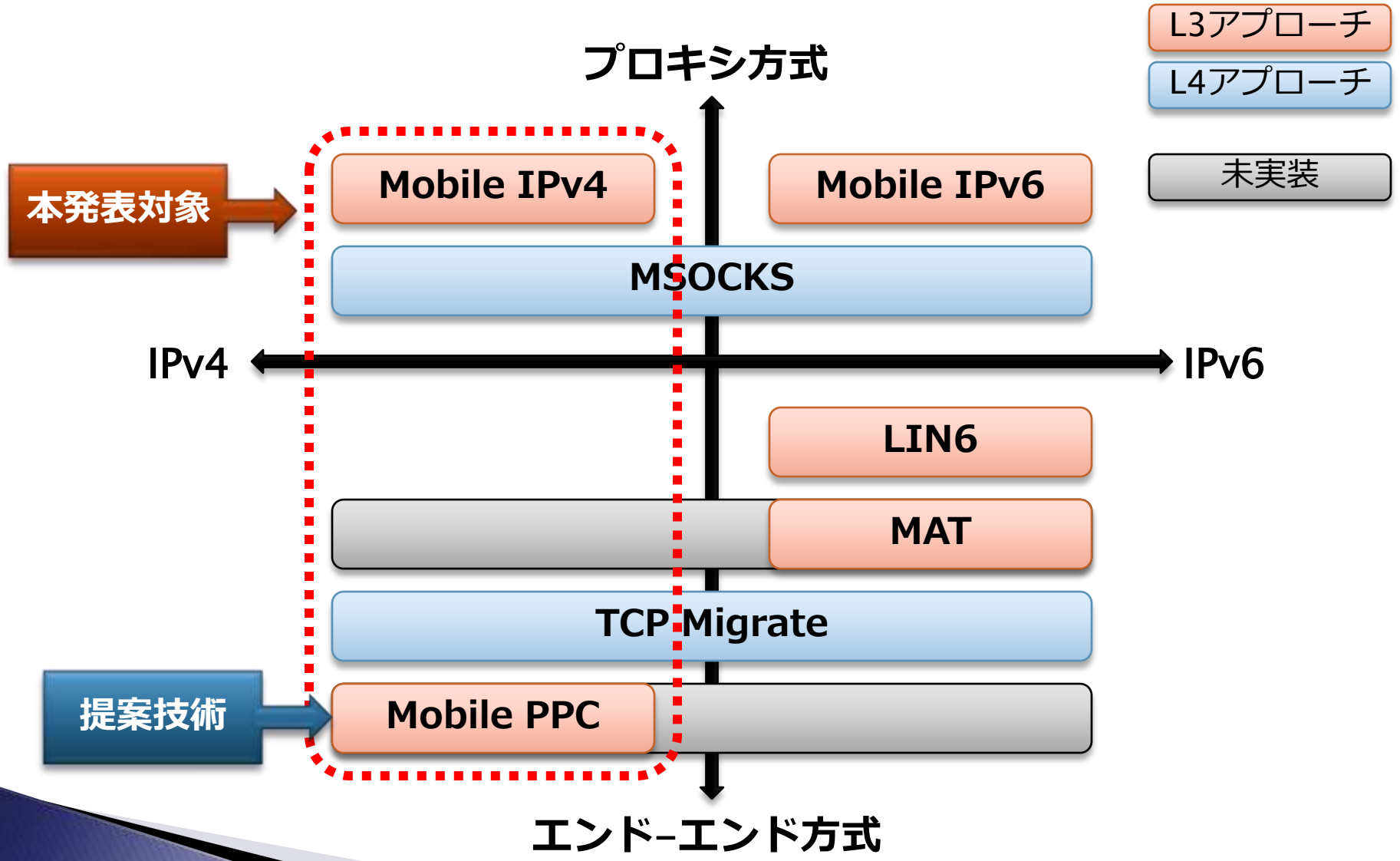


SIPへの対応（2）

- SIP ALGを実装するだけでもよい（簡単）
- ただし移動後もRTP通信を継続するためには…
  - 拡張NAT-f（or Mobile PPC）を実行する必要あり

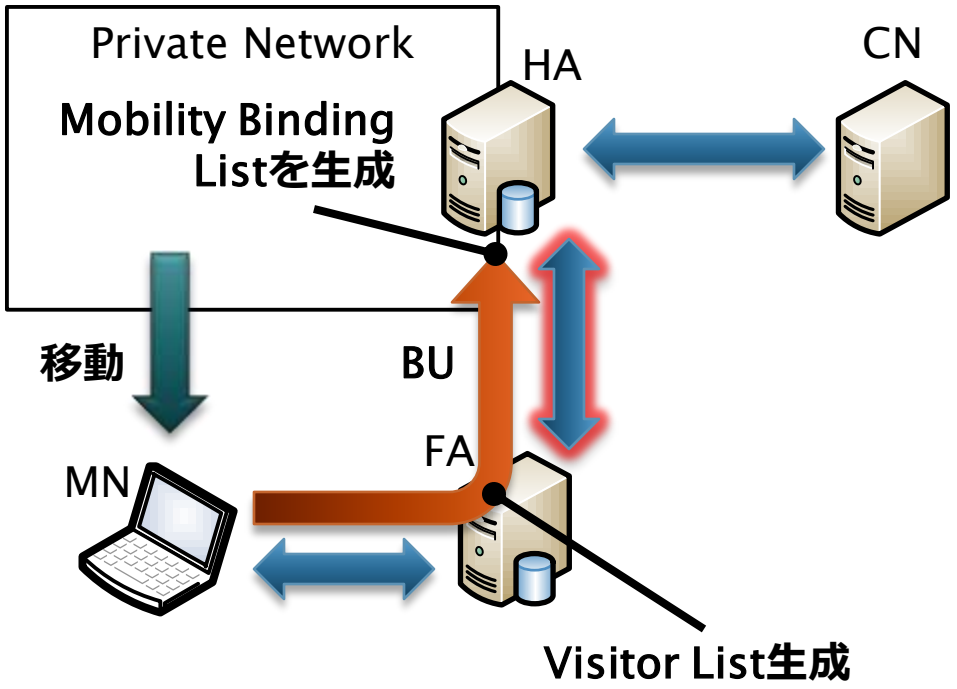


移動透過技術


L3アプローチ
L4アプローチ
未実装
プロキシ方式
本発表対象
Mobile IPv4
Mobile IPv6
MSOCKS
IPv4
IPv6
LIN6
MAT
TCP-Migrate
提案技術
Mobile PPC
エンド-エンド方式

Reverse Tunneling for Mobile IP

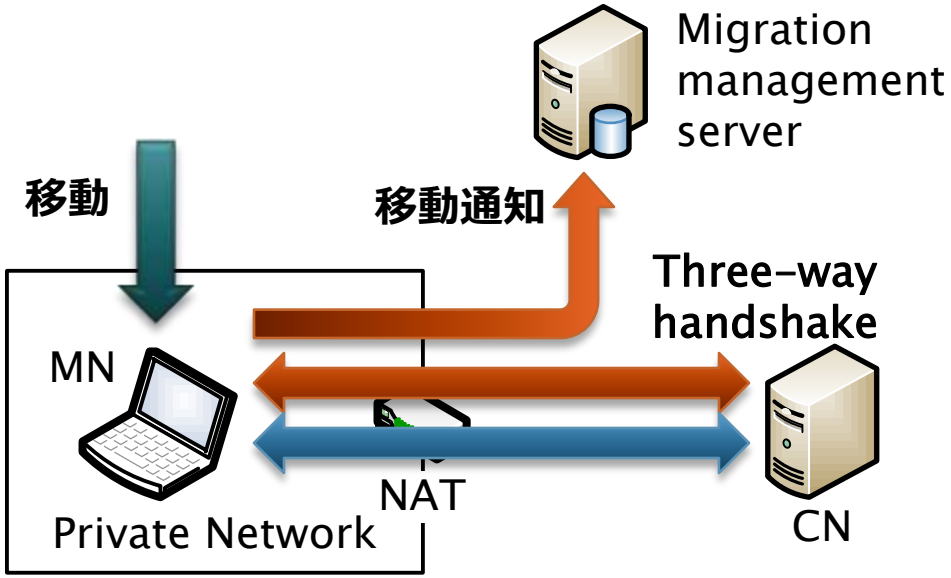
- RFC3024
  - Ingress Filtering問題に対する手法（逆方向トンネル）



1. Binding Updateを送信
   - Visitor List生成（FA）
   - Mobility Binding List生成（HA）
2. FA→HA：逆方向トンネル
3. HAはデカプセル化後，送信元をHoAからIP_{HA}へ変換

TCPコネクション維持プロトコル

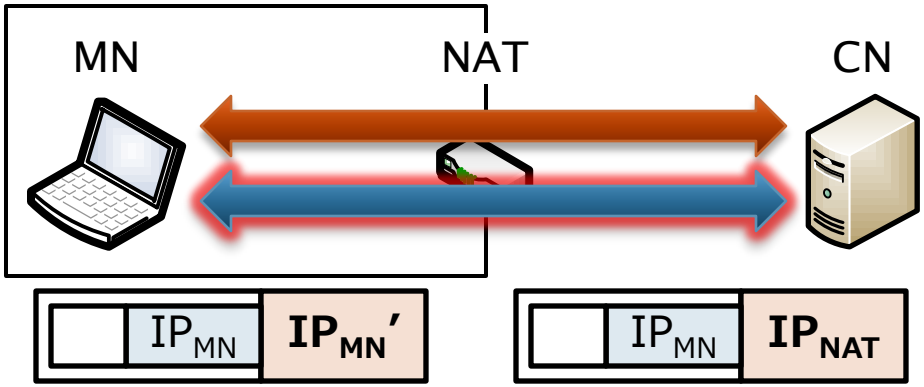
- L4におけるアプローチ
  - 移動先情報交換プロトコル
  - An End-to-End Approach to Host Mobility

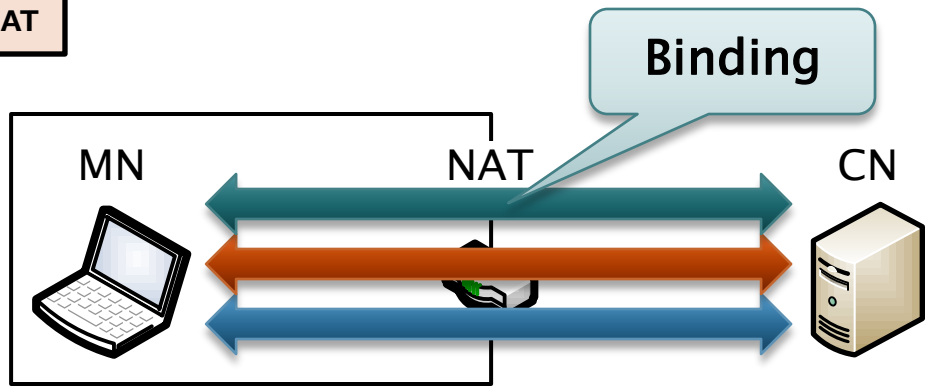


1. 移動情報管理サーバに移動通知
2. サーバはMNとCNのうち，通信開始が可能なノード側に相手側情報を返答
3. MNはCNとMSYNによりTCPコネクションを張り直す

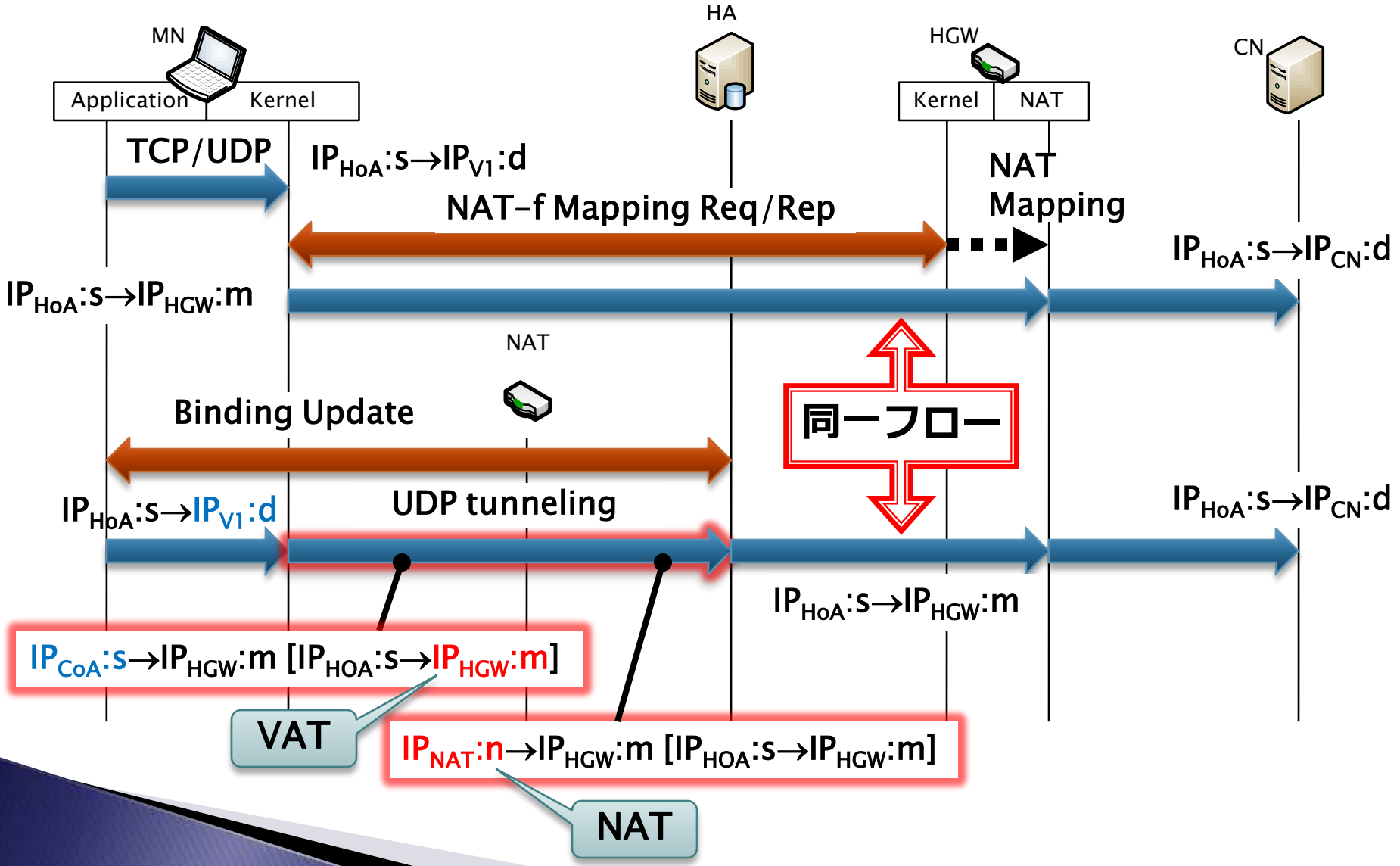
拡張Mobile PPC

- NATマッピングの作成方法
  - DPRP（Dynamic Process Resolution Protocol）
  - MN，CN間をUDPトンネリング
  - STUNのようなbinding





Mobile IPとNAT-fの併用



IPv4/v6混在環境への対応

- IPv4⇔IPv6における移動透過性の実現
  - NAT-PT（Protocol Translation）の利用
  - エンドノードにおいてPT対応VAT処理