NATを跨る移動透過性を実現するNTMobileの提案

093430031 水谷 智大
渡邊研究室

1. はじめに

TCP/IP はインターネットにおける通信インフラとして普及したが，IPv4 グローバルアドレスの枯渇が問題になっている．この問題への長期的解決策である IPv6 は IPv4 と互換性がなく，本格的な普及に至っていない．したがって IPv4 は今後も主流を占めると予想される．

IPv4 ではアドレスの枯渇への短期的対策として NAT が導入されたが，NAT 外部から内部に通信を開始できない，NAT 越え問題が新たに発生している．NAT 越え技術には様々あるが，接続できるプライベートネットワークの制限やスループットの低下など，それぞれ課題がある．

また近年では小型端末や公衆無線網の普及により，移動しながら通信したいという需要がある．しかし TCP/IP では通信識別子である IP アドレスが接続場所により異なるため，ノードが移動すると通信が切断される．IPv4 において，これを解決する移動透過性技術には Mobile IP や Mobile PPC（Mobile Peer to Peer Communication）がある．

Mobile PPC は Mobile IP の課題を解決しており，プロトコルの制限やスループットの低下，第三の機器の必要性はないが，NAT の存在は考慮されていなかった．

本研究では，NAT の存在に関わらず通信開始や移動が可能で，またプロトコルや移動範囲が制限されない手法，NTMobile（NAT Traversal with Mobile）を提案する．

2. Mobile PPC の概要とその課題

Mobile PPC では両エンドノードが IP 層に，ノードの移動前後のアドレス情報を保持する CIT（Connection ID Table）と呼ぶテーブルを持つ．移動ノード（MN; Mobile Node）は移動すると，通信相手ノード（CN; Correspondent Node）と CU（CIT Update）を交換し，CIT を更新する．その後 CIT を参照して全てのパケットのアドレスを変換することにより，アプリケーションに対してアドレスの変化を隠蔽し，かつパケットを正しくルーティングして通信を継続する．

しかし MN が NAT を跨いで移動したり，CN が NAT 配下に存在したりすると CIT によるアドレス変換が上手くいかず，通信が切断される．そこで Mobile PPC では，以下に述べる Hole Punching を組み合わせる方式 [1] と，NAT-f を組み合わせる方式 [2] が提案されている．

2.1 Hole Punching を組み合わせた方式

CN は MN が NAT 配下に移動したと判断すると，MN に Hole Punching に当たる Binding の交換を行うように要求する．MN は CN と Binding を交換して NAT にマッピングを生成し，そのマッピングアドレスを CU に記載して再度 CN と CU を交換する．これにより CIT は NAT マッピングに対応した更新がなされる．

しかしこの手法では CN が NAT 配下に存在する場合に対応できない．また，近年の NAT に搭載される SPI と呼ばれるフィルタリング機能により，TCP ではパケットが破棄される可能性がある．

2.2 NAT-f を組み合わせた方式

MN は通信開始時，NAT-f ルータと NAT-f ネゴシエーションを行い，NAT-f ルータにマッピングを生成する．MN はこのマッピングに対して通信を開始すると，NAT-f ルータはマッピングにしたがってパケットのアドレスを変換し，NAT 内部の CN にパケットを転送する．その後 MN が通信中に移動すると，MN は NAT-f ルータと CU を交換する．これにより MN と NAT-f ルータに CIT が生成される．

しかしこの手法では CN の移動を想定しておらず，CN が接続する場所も NAT-f ルータ配下に限られる．また MN は NAT 配下へ移動できない．

3. 提案方式

IPv4 で自由な移動を実現するためには，NAT に改造を加えない NAT 越えと移動透過性を同時に実現しなければならない．このとき，プライベートアドレスは別々の管理者が管理している可能性があるため，プライベートアドレスが重複することも考慮する必要がある．

そこで本提案では，両エンドノード間で生成した UDP トンネルを用いて通信を行うことにより，NAT への改造を回避する．両エンドノードがそれぞれ異なる NAT 配下に存在する場合は，両エンドノードが第三の機器と UDP トンネルを生成し，中継通信を行う．

またエンドノードを常に一意に識別する仮想アドレスを導入する．アプリケーションは通信を仮想アドレスで認識し，送受信時にパケットのアドレスを物理アドレスと変換する．これによりアプリケーションに対して移動によるアドレスの変化を隠蔽でき，かつプライベートアドレスの重複にも対応できる．

以下にグローバルネットワーク側の MN がプライベートネットワーク内の CN に通信を開始し，更に通信中に移動する場合を説明する．以降の説明で使用する記号は以下の通りである．

- $G*$ ；グローバルアドレス
- $P*$ ；プライベートアドレス
- $A:a$ ；IP アドレス A，ポート番号 a
- $A:a \rightarrow B:b$ ；送信元 $A:a$ から宛先 $B:b$ のパケット
- $A:a \leftrightarrow B:b$ ；$A:a$ と $B:b$ との通信
- $A:a \Leftrightarrow B:b$ ；$A:a$ と $B:b$ のアドレス変換
- $VO*$ ；自分自身を示す仮想アドレス
- $VC*$ ；通信相手を示す仮想アドレス

3.1 登録処理

図 1 に通信開始時の登録処理を示す．本方式を実現するため，UDP トンネル生成を指示する機能を DDNS に追加し，これを DS（Direction Server）と呼ぶ．DS_{CN}，DS_{MN} はそれぞれ CN，MN が所属する DS であり，G_{CN}，G_{MN} を持つ．DS は各エンドノードの情報を管理する Node Table を持ち，DNS 機能には新たに NTM レコードを定義する．NTM レコードは各エンドノードを識別する Node ID とノードの物理アドレス，属する NAT の IP アドレスで構成される．また各エンドノードは仮想アドレスと物理アドレスの関係を保持した VPT（Virtual Physical Translation）Table と，通信相手の情報を管理する Tunnel Table を持つ．

CN はネットワーク接続時，DS_{CN} に Registry Request を送信して，自身の Node ID "NID_{CN}"，FQDN "*cn.exp.com*"，物理アドレス "P_{CN}" を DS_{CN} に登録する．

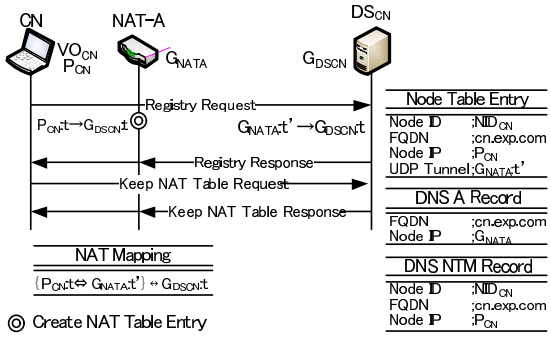


図 1: 通信開始時の登録処理

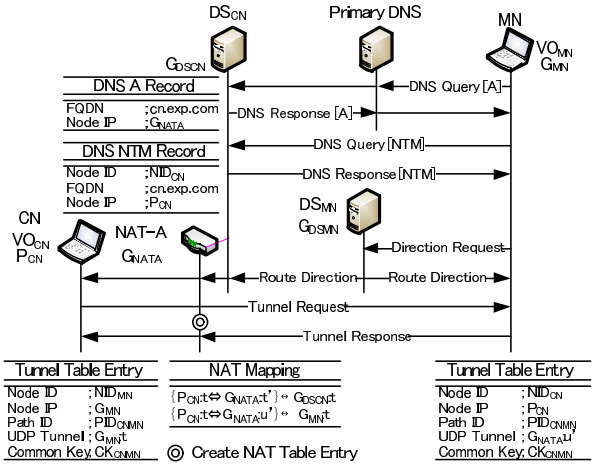


図 2: UDP トンネル生成ネゴシエーション処理

この時 NAT-A には NAT マッピングが生成される．DS_{CN} は Registry Request に記載された情報に加え，マッピングアドレスと NAT のアドレスを Node Table に登録する．

その後 CN は NAT-A のマッピングを維持するため，定期的に DS_{CN} と Keep NAT Table を交換する．MN 側も同様に DS_{MN} に自身の情報を登録する．

3.2 UDP トンネル生成ネゴシエーション

MN が CN に通信開始する場合の UDP トンネル生成ネゴシエーション処理を図 2 に示す．MN のアプリケーションは”*cn.exp.com*”により A レコードの DNS 問い合わせを自プライマリ DNS に行うと，DS_{CN} は G_{NATA} を応答する．MN はこれをカーネルモジュールにて一時的に退避し，以後の処理に必要な CN の情報を取得するため，”*cn.exp.com*”を記載して DNS の NTM レコードを DS_{CN} に問い合わせる．DS_{CN} はこれに対し，NTM レコードを返す．

その後 MN は CN と自身の Node ID や物理アドレスを記載した Direction Request を DS_{MN} に送信する．DS_{MN} は Direction Request の送信元 IP アドレスと MN の物理アドレスが同一であることから MN がグローバルネットワークに存在すると判断する．同様に CN の物理アドレス G_{CN} と NAT の IP アドレス G_{NATA} が異なることから CN がプライベートネットワークに存在すると判断する．

DS_{MN} はこの判断結果から，Route Direction を DS_{CN} 経由で CN に送信し，MN に Tunnel Request を送信するように指示する．同様に Route Direction を MN に送信し，CN からの Tunnel Request を待つように指示する．CN は Route Direction を受信すると，MN に関する情報を

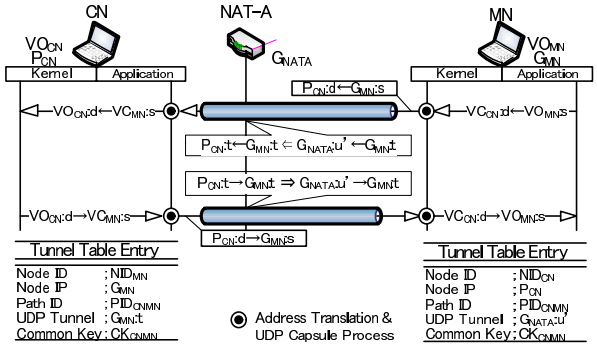


図 3: 送受信パケットのアドレス変換とカプセル処理

Tunnel Table に登録し，また VPT Table に $\{VO_{CN} \Leftrightarrow P_{CN}\} \leftrightarrow \{VC_{MN} \Leftrightarrow G_{MN}\}$ を登録する．その後，指示にしたがって G_{MN} に Tunnel Request を送信する．MN も同様，Tunnel Table に CN に関する情報を，VPT Table に $\{P_{CN} \Leftrightarrow VC_{CN}\} \leftrightarrow \{G_{MN} \Leftrightarrow VO_{MN}\}$ を登録した後，指示にしたがい Tunnel Request を待つ．

MN は Tunnel Request を受信すると CN に関する Tunnel Table に UDP トンネル情報 ”$G_{NAT} : t'$”を追加登録し，CN に応答を返す．また一時退避していた A レコードの DNS レスポンスの内容を仮想アドレス VC_{CN} に書き換えて上位ソフトウェアに通知する．

3.3 アプリケーションデータの通信

MN が CN との間で送受信するパケットのアドレス変換とカプセル処理を図 3 に示す．MN のアプリケーションは DNS の A レコード ”VC_{CN}”から，$VO_{MN} : s \rightarrow VC_{CN} : d$ を生成する．MN は VPT Table を参照してアドレスを $G_{MN} : s \rightarrow P_{CN} : d$ に変換し，物理アドレスでカプセル化して送信する．

送信されたパケットは NAT-A で外側のアドレスが変換されて CN に転送される．CN はカーネルモジュールにて UDP カプセルを除去し，Tunnel Table を参照して $G_{MN} : s \rightarrow P_{CN} : d$ を $VC_{MN} : s \rightarrow VO_{CN} : d$ に変換してアプリケーションに渡す．逆方向も同じ処理により，CN と MN は NAT-A に影響されずにパケットを送受信できる．

MN の移動後も通信開始時と同様のシーケンスにより，DS_{MN} から指示を受ける．CN，MN は指示にしたがい両エンドノード間の UDP トンネル生成と互いの Tunnel Table や VPT Table の更新を行い，アドレス変換・カプセル処理を行なうことにより，移動後も通信を継続できる．

4. まとめ

本論文では IPv4 において，移動透過性と NAT 越えを同時に実現し，エンドノードがあらゆる移動を可能とする方式を提案した．本提案では UDP トンネルを使用することで SPI フィルタリングを持つ NAT でも NAT に改造を加えることなく NAT 越えを実現する．また仮想アドレスを導入し，プライベートアドレスの重複にも対応した．今後は実装を完成させ，検証や性能測定を行う．

参考文献

[1] 鈴木秀和, 渡邊　晃: Hole Punching を用いた NAT 越え Mobile PPC の設計, 情報処理学会研究報告, Vol.2008, No.44, pp.69-74 (2008).

[2] 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, 電子情報処理学会論文誌 (B), Vol.J92-B, No.1, pp.109-121 (2009).

NATを跨る移動透過性を実現するNTMobileの提案

名城大学大学院
理工学研究科 情報工学専攻
093430031
渡邊研究室

水谷智大

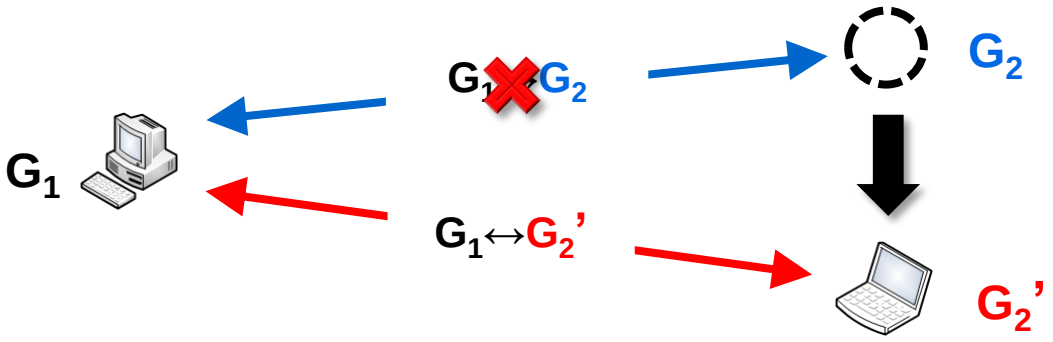
研究背景

- 移動しながら通信をしたい，という需要
  - 小型携帯端末や，公衆無線網の普及
- TCP/IPでは通信中に移動すると通信は切断される
- “移動透過性”技術はほとんどがIPv6ベース
  - IPv4グローバルアドレスの枯渇によるIPv6への移行
- IPv4は今後も使用される
  - IPv6はIPv4と互換性がない >> IPv6への移行の停滞

IPv4における移動透過性技術

移動透過性

- TCP/IPでは通信中に移動すると移動前に行っていた通信は切断される
  - アプリケーションは通信の識別をIPアドレスで行う
  - IPアドレスは接続する場所によって異なる



- IPv4における移動透過性技術

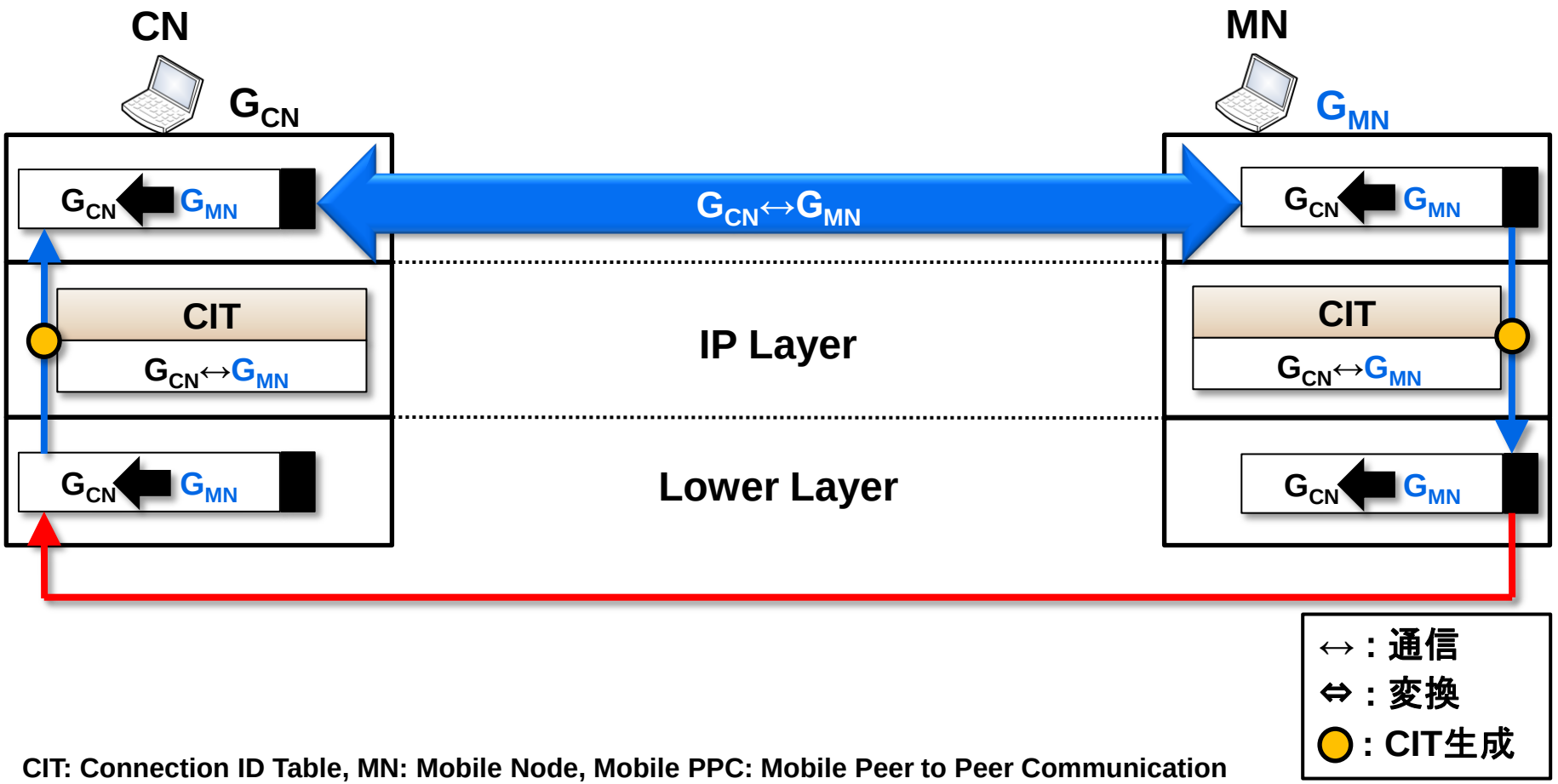
Mobile IP

Mobile PPC

Mobile PPC: Mobile Peer to Peer Communication

移動透過性技術 - Mobile PPC（移動前の通信）

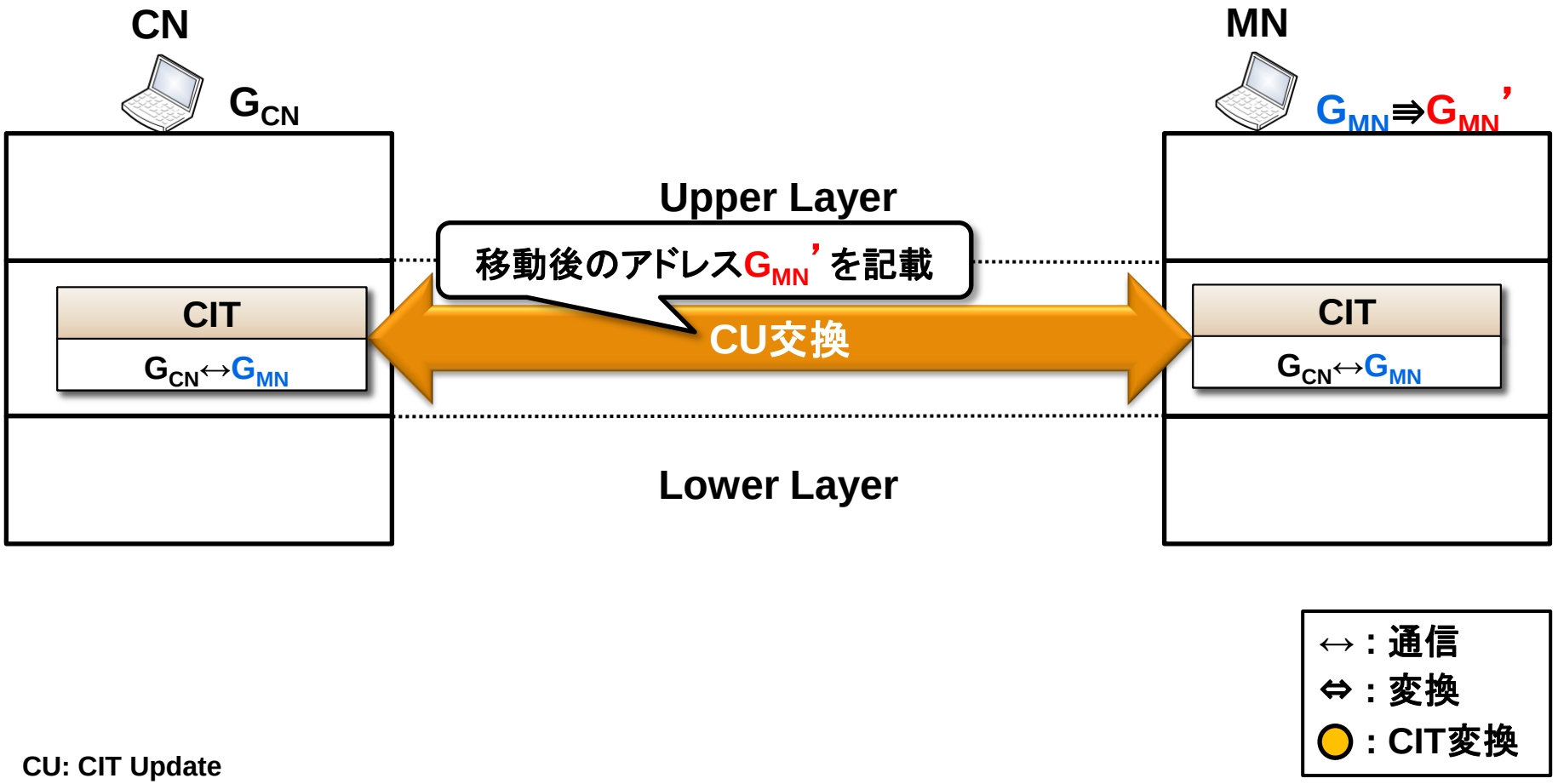
- エンドノードのみで移動透過性を実現
  - 通信相手に変化したIPアドレスを通知して“CIT”を更新
  - エンドノードがIP層に持つ“CIT”を使ってパケットのアドレスを変換



CIT: Connection ID Table, MN: Mobile Node, Mobile PPC: Mobile Peer to Peer Communication

移動透過性技術 - Mobile PPC（移動後のCIT更新）

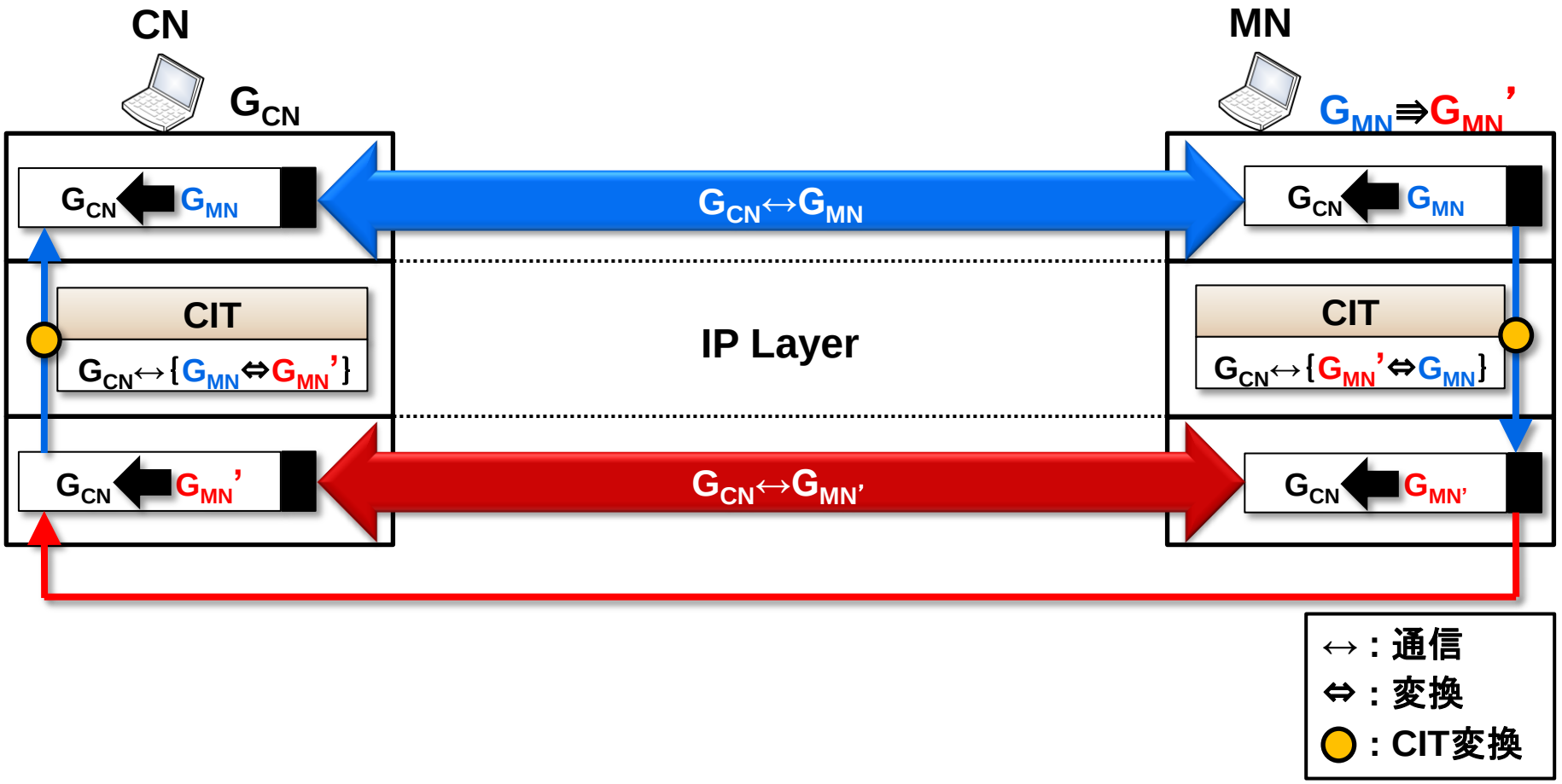
- エンドノードのみで移動透過性を実現
  - 通信相手に変化したIPアドレスを通知して“CIT”を更新
  - エンドノードがIP層に持つ“CIT”を使ってパケットのアドレスを変換



CU: CIT Update

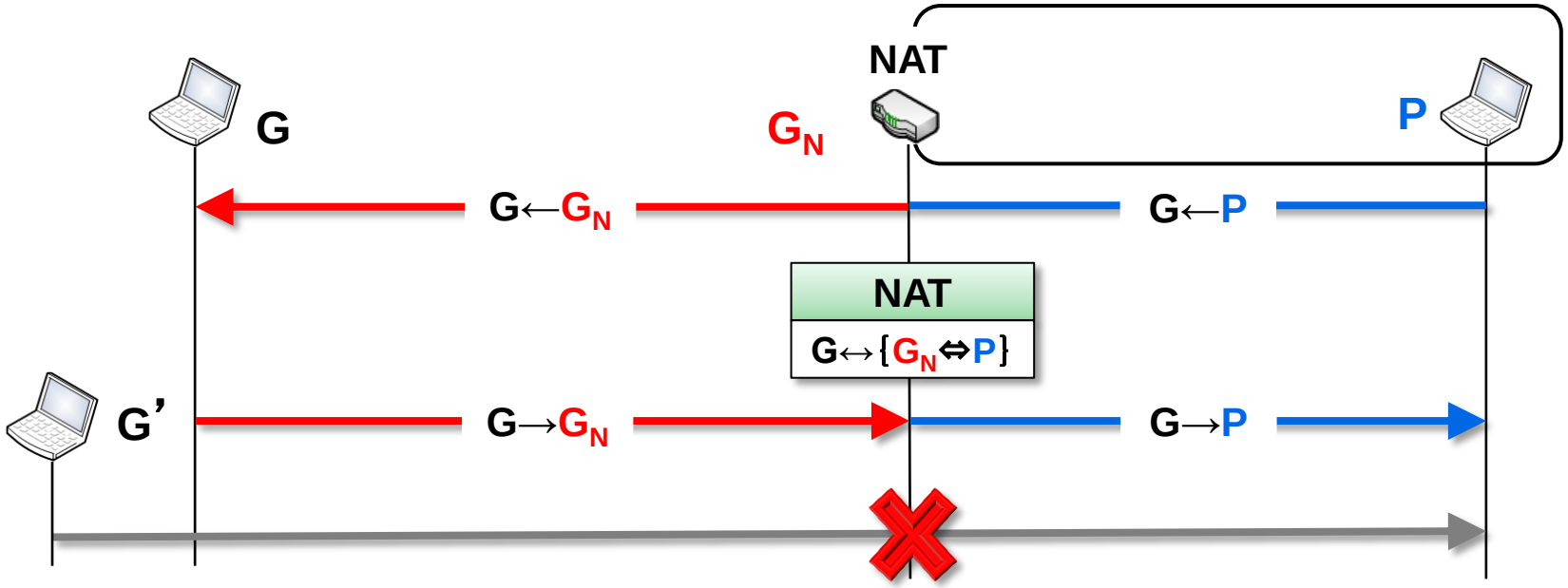
移動透過性技術 - Mobile PPC（移動後の通信）

- エンドノードのみで移動透過性を実現
  - 通信相手に変化したIPアドレスを通知して“CIT”を更新
  - エンドノードがIP層に持つ“CIT”を使ってパケットのアドレスを変換



IPv4における課題 - NAT越え問題

- NAT越え問題
  - IPv4グローバルアドレスの枯渇によるプライベートアドレスの導入
  - IPv4ではNATが存在する場合がほとんど



  - NAT内部にパケットを到達するためにはNATマッピングが必要

移動透過性技術にもNAT越えは影響する

NAT: Network Address Translation

移動透過性技術 - NATに対応したMobile PPC

手法1

Hole Punchingを用いたNAT越えMobile PPCの実装
情報処理学会研究報告，2009-MBL-49，Vol.2009，No.17，pp.1-7，Apr.2009.

- NAT内部から一度パケットを送信し，NATマッピングエントリを生成
- CUによりNATマッピングとCITエントリを対応させる

MNはNATを跨って移動可能

セッション情報不一致によるTCP切断

**CNの移動範囲が
グローバルネットワーク内に限定**

手法2

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.13，Jan.2009.

- 特殊NATにMobile PPC機能を実装

CNがNAT配下でも通信開始可能

CNの動作は特殊なNAT配下のみ

CNは移動できない（想定外）

**MNの移動範囲が
グローバルネットワーク内に限定**

移動範囲の制限

上位プロトコルの制限

IPv4における移動透過性技術に対する要求

NATの有無に関わらず，自由に通信開始，移動できる

① 移動によるIPアドレスの変化

② 上位プロトコルの制限

移動範囲の制限

③ NATへ改造を加えないNAT越え問題

④ プライベートアドレスの重複

異なるプライベートネットワーク同士の通信

実現手法

① 移動によるIPアドレスの変化

移動範囲の制限
④ プライベートアドレスの重複

→ 移動しても変化しない，通信相手を一意に識別する **仮想アドレス** を導入

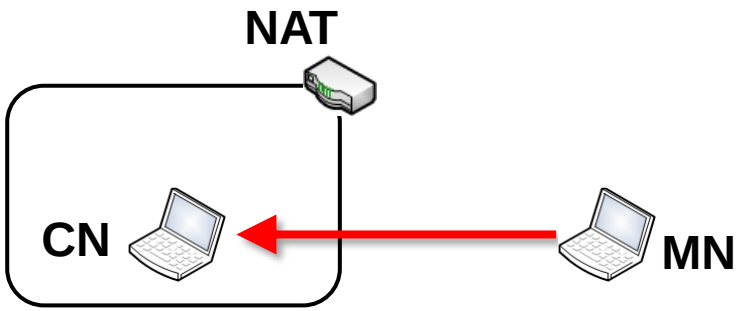
② 上位プロトコルの制限

移動範囲の制限
③ NATへ改造を加えない NAT越え問題

→ **UDPトンネル** による通信

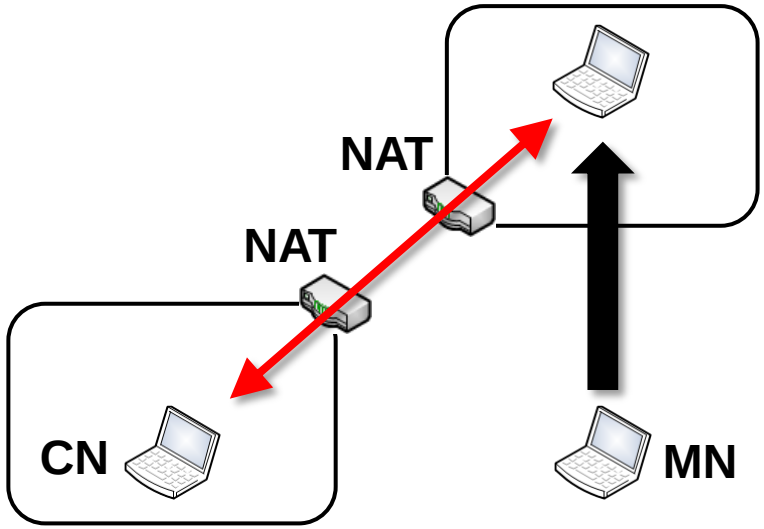
本発表で想定する通信と移動

グローバルネットワークから
プライベートネットワークに通信開始



通信開始時のNAT越え

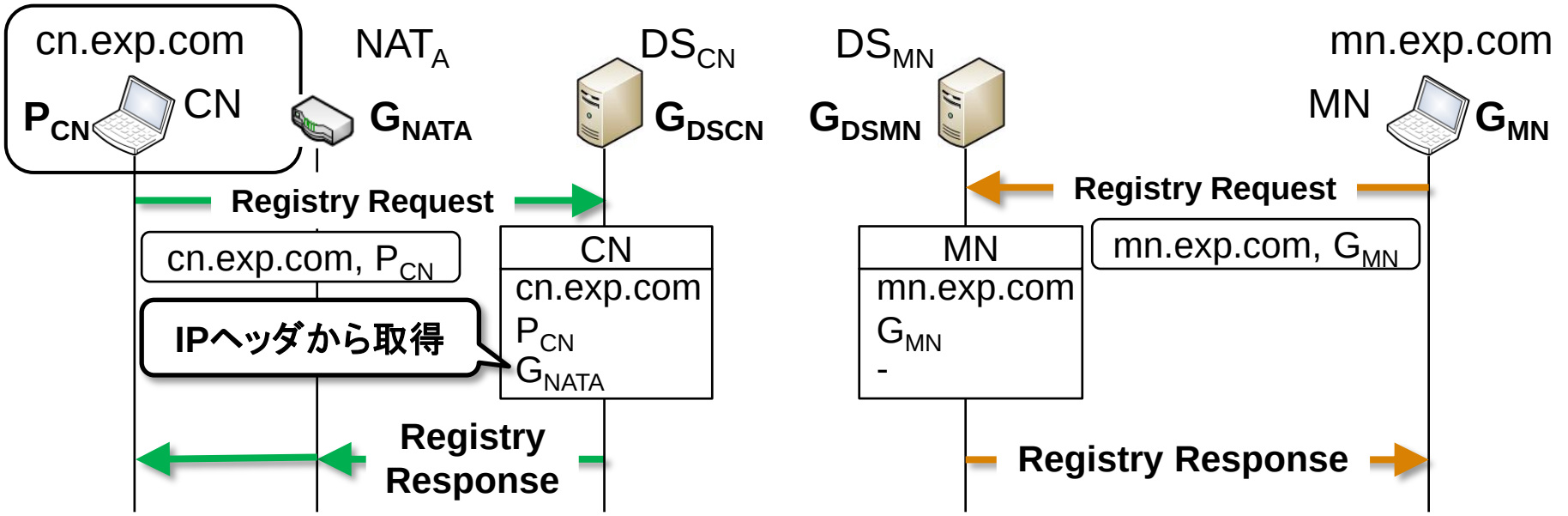
異なるプライベートネットワーク
同士で通信



NATを跨った移動

提案手法 - 登録処理

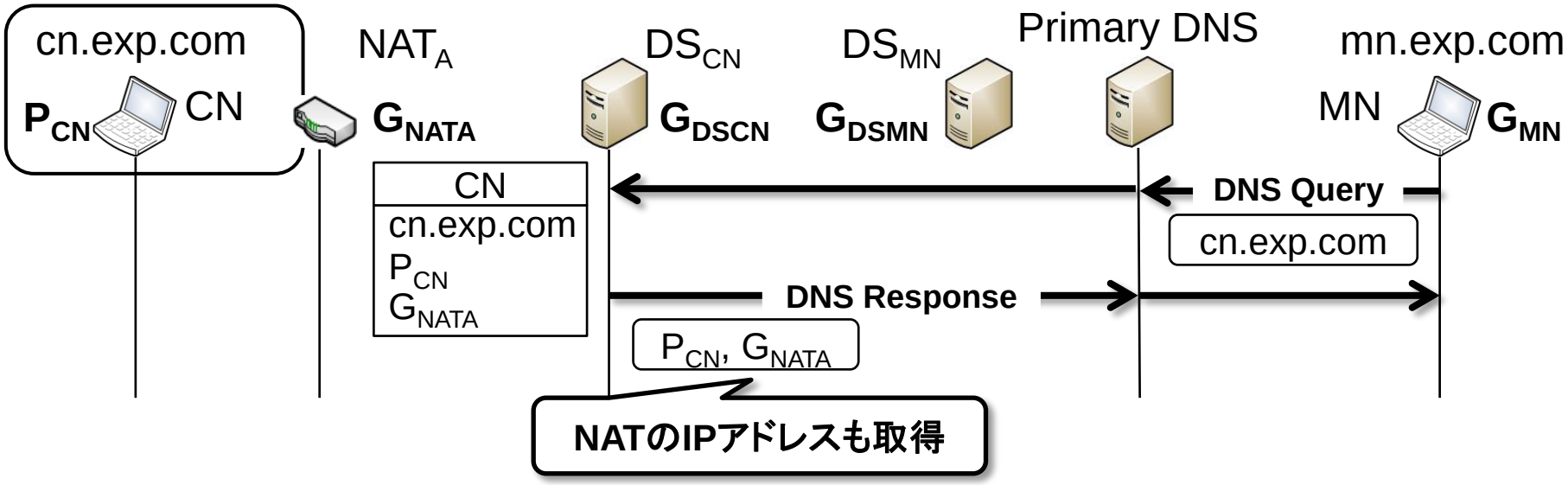
- 各エンドノードはネットワーク接続時，DSに情報を登録する
  - DSはDDNSに改造を加えて構成する
  ① CNはDS_{CN}に，MNはDS_{MN}に登録
  ② DSは受け取った情報を本手法で使うテーブルと，DNSに登録する
  - 制御メッセージはUDPベースで，このメッセージで作られたNATマッピングを用いてDSからエンドノードへアクセスする



DDNS: Dynamic DNS, DS: Direction Server

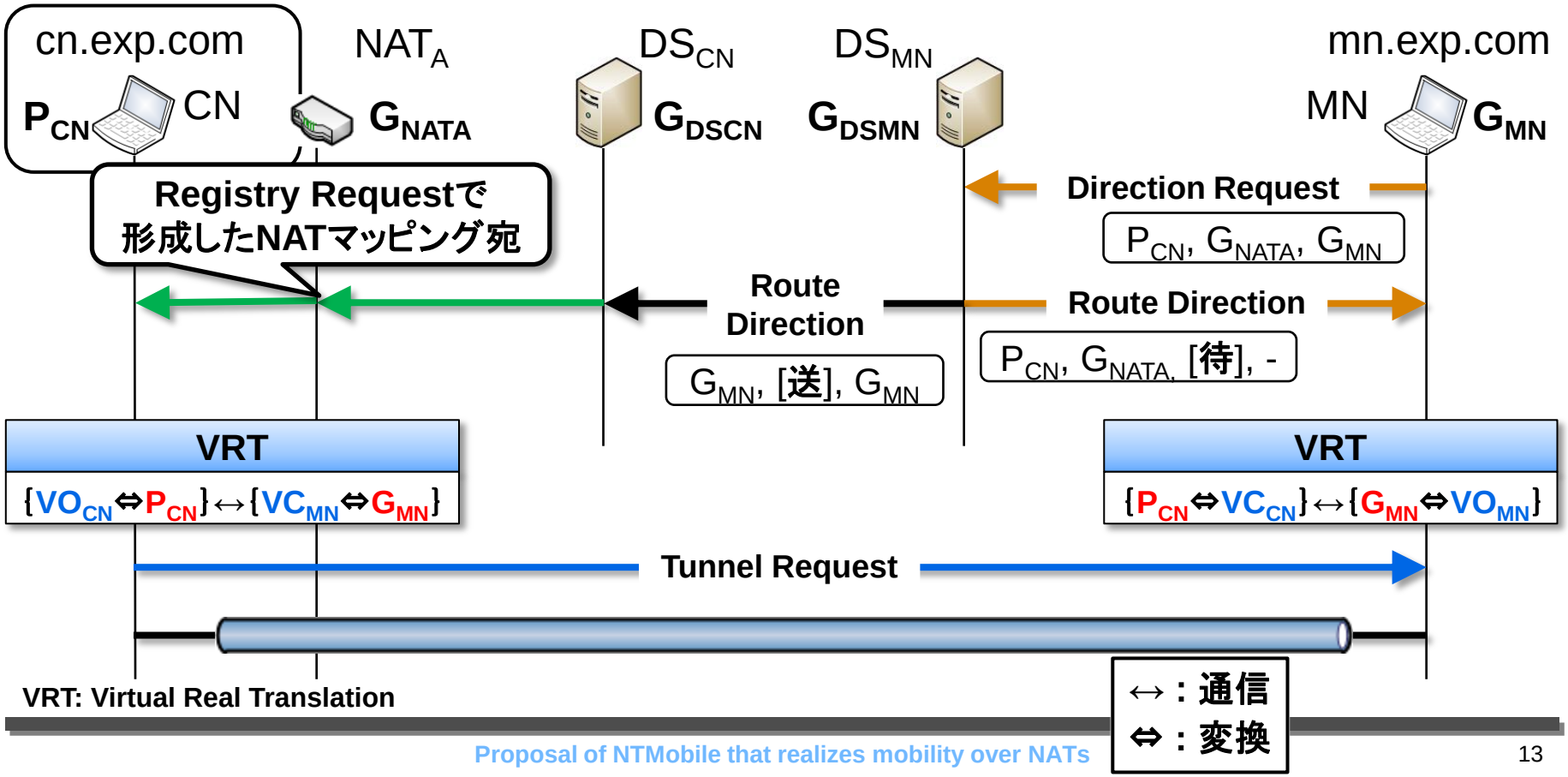
提案手法 - UDPトンネル生成処理（1/2）

- UDPトンネル生成に必要な情報の問い合わせを行う
  - ① CNのIPアドレス，NATのIPアドレスを問い合わせ
  - ② CNとMNの情報をDS_{MN}に通知し，UDPトンネル生成方法を問い合わせ



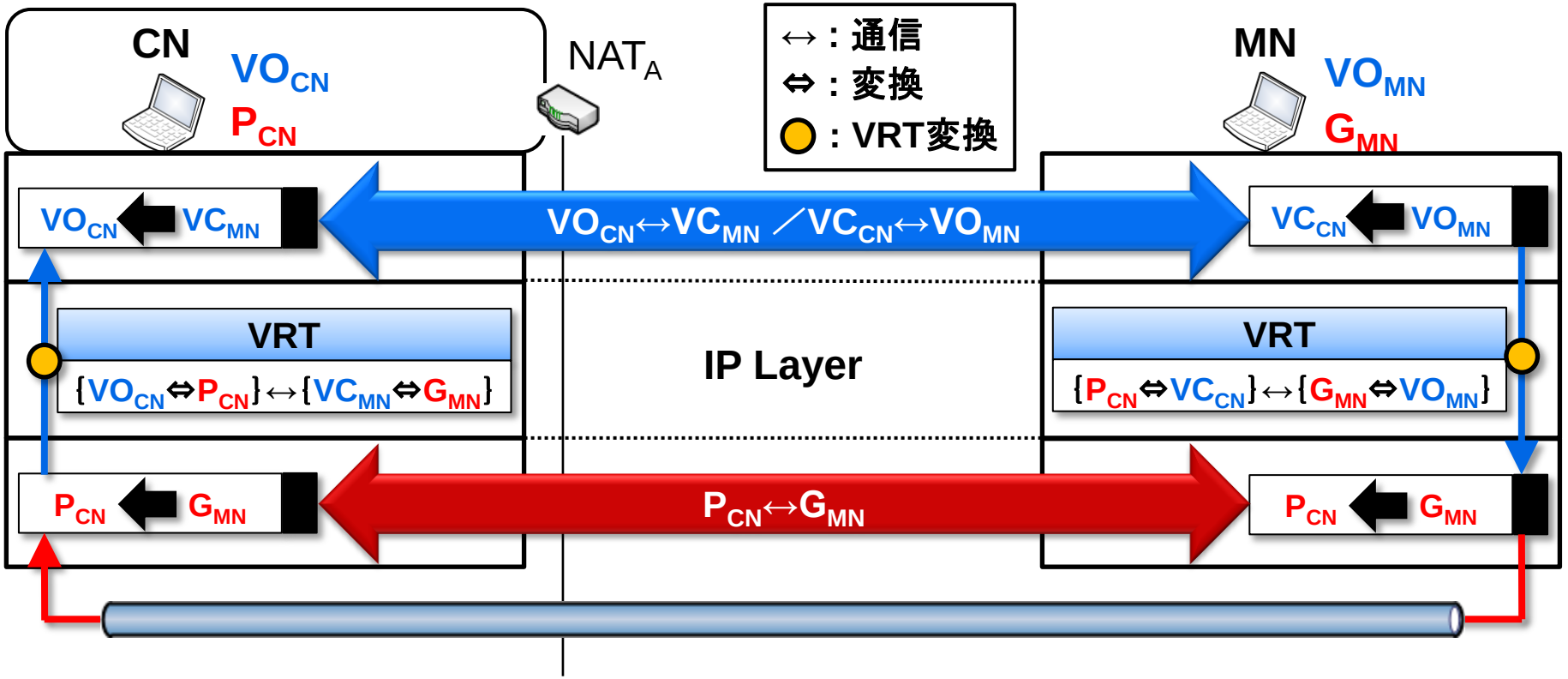
提案手法 - UDPトンネル生成処理（2/2）

- UDPトンネル生成に必要な情報の問い合わせを行う
  - ④ CNとMNの情報をDS_{MN}に通知，UDPトンネル生成方法を問い合わせ
  - ⑤ 受け取った情報からCN，MNがNAT配下か否か調べる
  - ⑥ 結果からCN，MNそれぞれにUDPトンネル生成に必要な動作を指示



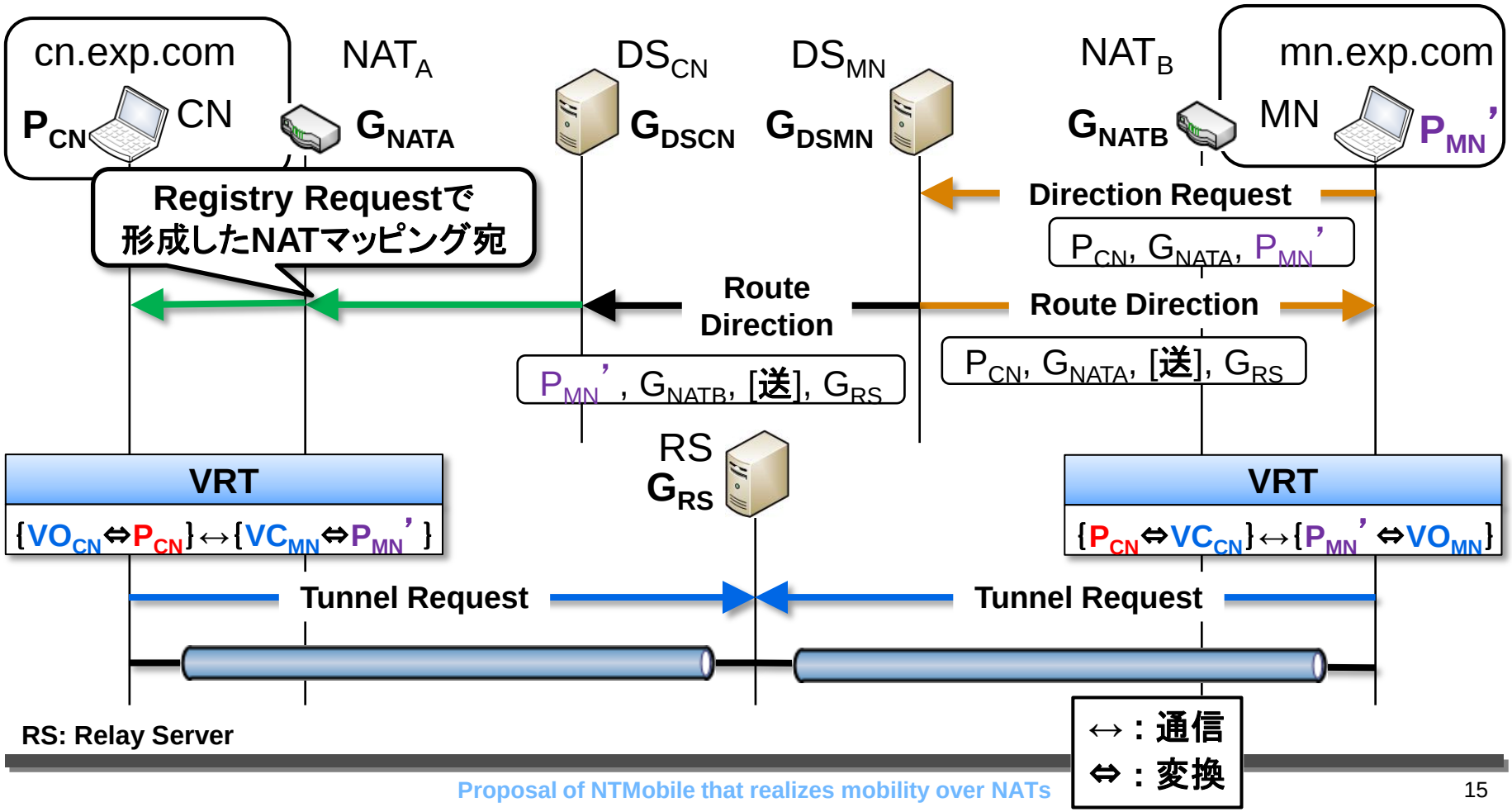
提案手法 - アドレス変換とカプセル通信

- 生成したVPNテーブルによる変換とUDPトンネルを使用
  - ① 仮想アドレスのパケットを，VRTテーブルで実アドレスに変換
  - ② UDPトンネル（カプセル化）を使用して通信相手ノードに送信
  - ③ カプセルを解除し，VRTテーブルで実アドレスから仮想アドレスに変換



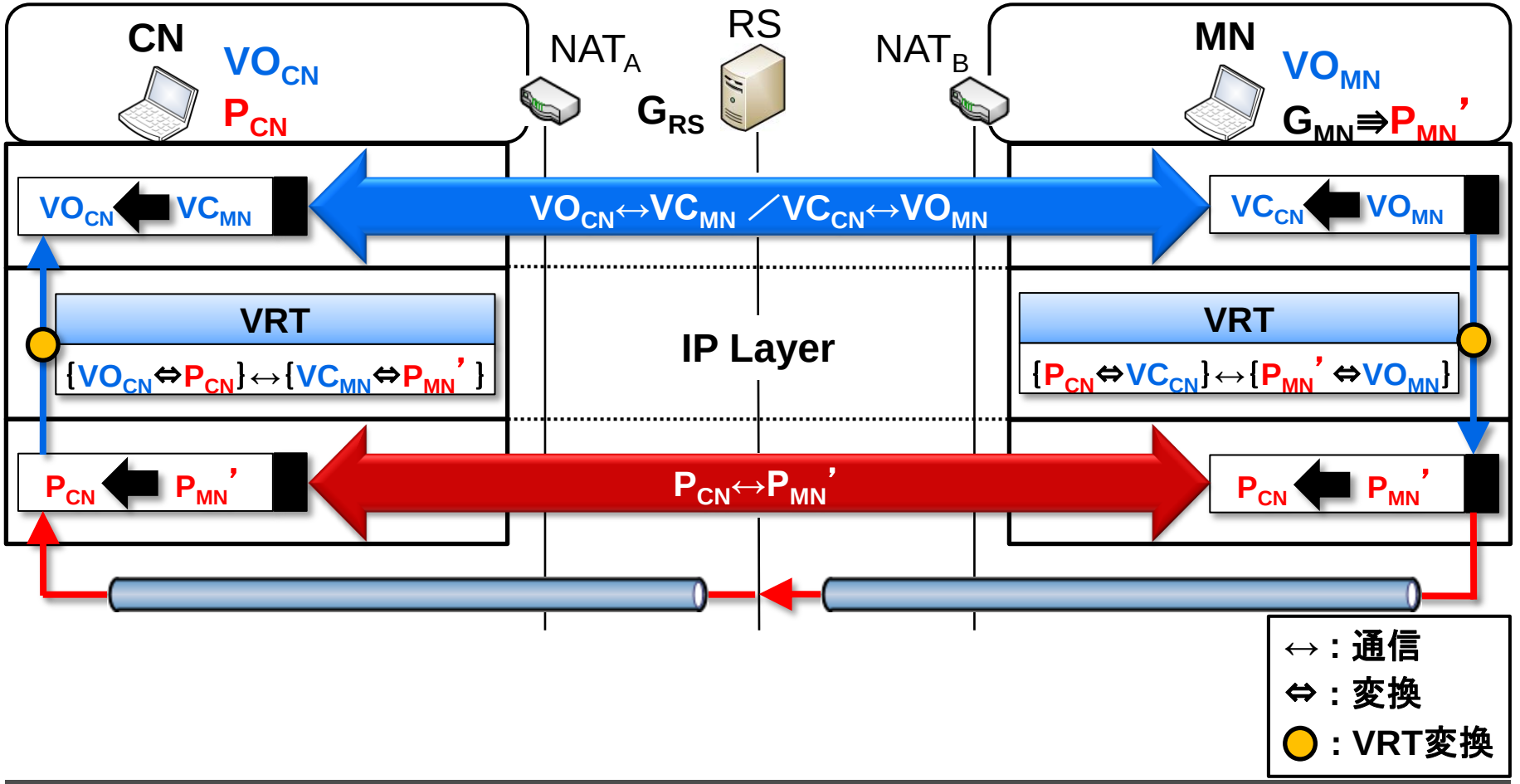
提案手法 - 移動後のUDPトンネル生成処理

- 通信開始時と同様の手法で，UDPトンネルを生成する
  - 両エンドノードがプライベートネットワークに存在 >> 共にNAT越え問題が発生
  - 中継機器**RS**を経由した通信となる



提案手法 - 移動後のアドレス変換とカプセル通信

- 通信開始時と同様，アドレス変換とUDPトンネルで通信を行う
  - 両エンドノードがプライベートネットワークに存在 >> 共にNAT越え問題が発生
  - 中継機器**RS**を経由した通信となる



考察

（NAT対応）Mobile IP

Levkowetz, H. and Vaarala, S.:
Mobile IP Traversal of Network Address Translation (NAT) Devices,
RFC 3519 (2003).

両エンドノードがプライベートネットワークに存在する場合のみ中継通信を行う ← 常に中継通信を行うことによるスループットの低減

パケットへの処理をIP層で行う ← 上位アプリケーションの制限

RSは自由に選択可能 ← RSの負荷集中

改造するネットワーク機器はDDNSのみ ← 既存ネットワーク環境への影響

まとめ

- IPv4における移動透過性の実現に必要な要素を整理した
  - 移動によるIPアドレスの変化への対応
  - NATを改造せずNAT越え問題を解決
  - 上位プロトコルの非制限
  - 上位アプリケーションの非制限

- UDPトンネル通信と仮想アドレスにより対応
  - その他，機器への負荷を回避
  - 既存のネットワーク機器への影響を回避

- 今後は実装を完成し，動作テストと測定を行なう予定