NATを跨る移動透過性を実現するMobile PPCの提案

水谷智大[†1]　鈴木秀和[†2]　渡邊晃[†1]

IPv4は今後も使用され続けることが想定される．そのため，IPv4においても移動透過性を実現することは重要である．IPv4ではグローバルアドレス空間とプライベートアドレス空間があり，これらの空間を跨って移動することが想定される．この場合，通信経路上にNATが介在するため，NAT越えを解決しなければならないなど実現は容易ではない．本論文では，通信経路上にNATが介在するあらゆる通信パターンにおいて，Mobile PPC（Mobile Peer To Peer Communication）による移動透過性を実現する方式を提案する．

Proposal of Mobile PPC that realizes the mobility over NATs

Tomohiro MIZUTANI,[†1] Hidekazu SUZUKI[†2] and Akira WATANABE[†1]

IPv4 will continue being used in future. Therefore, realizing mobility is important. there are global address space and private address space in IPv4, and it is possible that a node moves between these space. In this case there is NAT on a communication paths. Therefore, it is not easy to realize this because it must solve NAT Traversal problem. In this paper, we propose the method that can realize mobility with Mobile PPC(Mobile Peer To Peer Communication) in every case NATs exist in communication paths.

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

1. はじめに

公衆無線ネットワークの普及により，屋外でネットワークを使用する機会が増加している．またWi-FiやWiMAXが搭載された小型携帯情報端末も増加しており，移動しながらIP通信を行いたいという需要がある．ところがIPネットワークではノードを識別するIPアドレスが接続する場所によって異なるため，通信中に移動するとIPアドレスが変化し，通信が切断されてしまう．この課題を解決する技術は移動透過性と呼ばれ，これまでにも多くの研究が行われてきた[1)–6)]．しかし移動透過性の研究は将来のIPv6への移行を想定し，IPv6を前提とした方式が主流である．ところがIPv6はIPv4との互換性がなく未だ本格的な普及には至っていない．今後IPv6への移行が進んだとしても，長期に渡ってIPv4はIPv6と混在して使用されると考えられ，IPv4においても移動透過性を実現することは重要である．

IPv4ではグローバルアドレスの不足により，インターネットと組織のネットワークの境界にNAT（Network Address Translation）を設置し，組織のネットワークをプライベートアドレスで構成する形態が一般である．しかしNATがあると外部のネットワークから内部のネットワークが隠蔽され，外部のノードから内部のノードに向けて通信を開始することができない．これはNAT越え問題と呼ばれ，IPv4の汎用性を損なう大きな要因となっている．また近年のNATにはSPI（Stateful Packet Inspection）と呼ばれるフィルタリング機能が搭載されることが多く，TCPのシーケンス番号の順番などに整合性がないパケットは破棄される．そのためSPIの存在を考慮すると，TCPのNAT越えを実現することは極めて難しい状況になっている．

NAT越え問題は移動透過性の実現においても大きな障壁となる．通信中のエンドノードの一方がNAT配下に移動すると，IPアドレスが変化することに加えてNATによりパケットのIPアドレスが変換されてしまい，一般的な移動透過性技術では対応できない．従ってIPv4において移動透過性を実現するためには，NAT越え問題も同時に解決しなければならない．更にTCPにおいては，SPIのフィルタリング機能をくぐり抜ける必要がある．

IPv4における代表的な移動透過性技術にMobile IP[2)]とMobile PPC[6)]がある．Mobile IPではHA（Home Agent）と呼ばれる第三の装置を経由した通信を行うためHAの障害に対して弱く，また経路冗長が発生しスループットが低下するという課題がある．また，パケットの送信元が実際のIPアドレスと異なる経路が存在し，不正パケットとして廃棄される可能性があるという課題がある．Mobile IPではNAT越え問題を解決するために，UDP

によりデータパケットをカプセル化する手法[7] や NAT に独自の機能を追加する手法[8] などが検討されている．しかし前者ではカプセル化に加えて，通信経路上に NAT が介在する場合は常に HA を経由しなければならず，スループットが低下するという課題がある．また後者では NAT に改造を要するなどの課題がある．

Mobile PPC は，エンドノードのみで移動透過性を実現でき，Mobile IP の多くの課題を解決している．ただし，両エンドノードが共に Mobile PPC に対応している必要がある．Mobile PPC では NAT 越え問題を解決するため，Hole Punching を用いる手法[9] や NAT に NAT-f と呼ばれる機能を実装する手法[10] が提案されている．しかし前者では通信相手が外部ネットワーク上にある場合のみを想定しており，移動条件に制約がある．また，後者では NAT に改造を加える必要があり，同様に移動が制限されるという課題がある．

本研究では，エンドエンドの特徴を有する Mobile PPC にあえて第三の機器を導入し，NAT の改造が不要で，かつあらゆる移動パターンに対応できる移動透過性の実現方式を提案する．第三の機器は特定の通信ケースにおいて中継通信を行うため中継サーバ RS（Relay Server）と呼び，また DNS サーバとしての機能も保持する．通信開始前，エンドノードは互いの IP アドレスから通信経路上に NAT が介在するか否かを確認し，通信トポロジに応じて UDP トンネルや RS を利用した通信を行う．ノードが移動すると通信開始時と同様の方法で通信経路を確立し，Mobile PPC による移動透過性を実現する．本機能は Mobile PPC の拡張としてカーネルに実装し，プロトコルや上位アプリケーションが制限されることはない．以上の処理により，あらゆる移動パターンに対して通信を継続することができる．NAT が介在しない場合の通信においては RS を必要とせず，従来のエンドエンドの特徴を維持している．

以降，第 2 章では解決すべき課題，第 3 章で本提案方式について述べ，最後に第 4 章でまとめる．

2. 解決すべき課題

本章では SPI 機能，及び Mobile PPC について説明する．次に移動パターンを整理して解決すべき課題を明らかにする．本章以降で用いる記号を以下に定義する．

- $Gn\ (n = 1, 2, 3 \ldots)$　；グローバルアドレス
- $Pn\ (n = 1, 2, 3 \ldots)$　；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

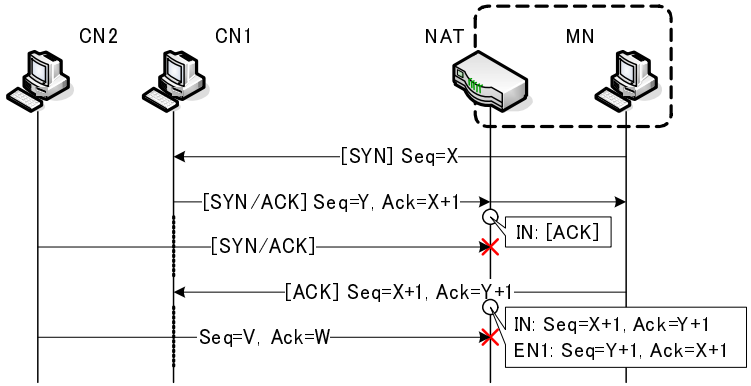


図 1　SPI によるフィルタリング処理
Fig. 1　Filtering process of SPI

- $A : a \leftrightarrow B : b$　；$A : a$ と $B : b$ 間の通信
- $A : a \Leftrightarrow B : b$　；$A : a$ と $B : b$ のアドレス／ポート変換

2.1 SPI

SPI は近年の NAT に実装される TCP フィルタリング機能である．通信パケットを監視して TCP ヘッダ内のフラグやシーケンス番号を解析し，整合性がないパケットを破棄する．

SPI による TCP フィルタリング処理を図 1 に示す．CN1，CN2 は外部ネットワーク，MN は NAT 配下の内部ネットワークに存在するものとする．NAT が存在するため，通信開始は MN 側からのみ可能である．MN は CN1 と TCP セッションを確立するためにシーケンス番号初期値 X の SYN パケットを CN1 に送信する．CN1 はシーケンス番号初期値 Y，確認応答番号 $X + 1$ の SYN/ACK パケットを応答する．NAT はこのセッションに関するログを保持し，このセッションに関する次のパケットは MN からの ACK パケットのみを通過させる．以後に続くデータパケットのやりとりにおいてもシーケンス番号や確認応答番号の整合性を確認し，正しいと判断したパケットのみを通過させる．CN2 から送信元を CN1 と偽装したパケットを MN に送信しても，TCP フラグやシーケンス番号の不整合によりこのパケットは破棄される．ただし，NAT によっては TCP フラグのみをチェックし，シーケンス番号まではチェックしないものなど，SPI の機能が実際にどこまで実装されているかは NAT により異なる．SPI 機能が NAT に搭載されていると，MN と CN1 間の一連の TCP セッションが全て監視対象となり，移動透過性の実現が難しくなる．即ち，MN が

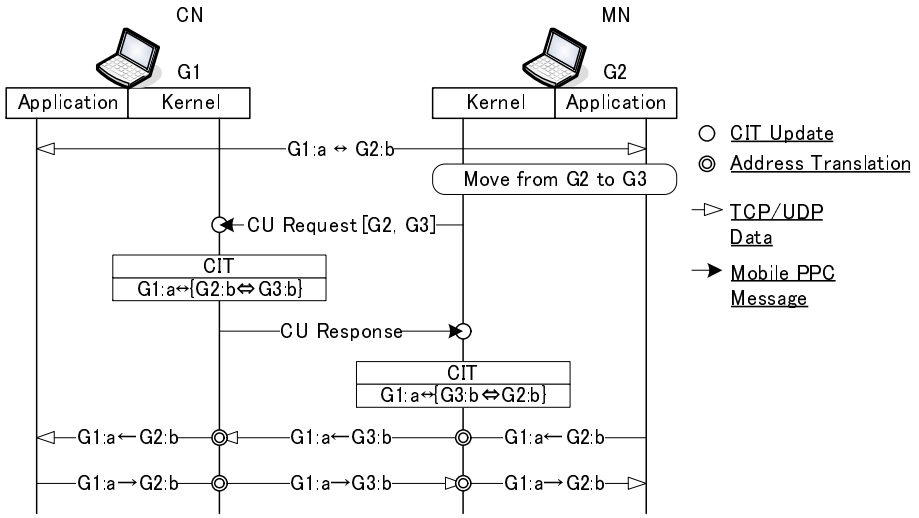


図 2 ノード移動時の Mobile PPC の動作
Fig. 2 Process of Mobile PPC when a node moves

TCP 通信中に NAT 配下に移動すると TCP 通信が途中から NAT を通過することになり，SPI のフィルタリングによりパケットが破棄される．

2.2 Mobile PPC

Mobile PPC は，IPv4 において第三の装置の助けを借りることなくエンドエンドで移動透過性を実現する唯一のプロトコルである．エンドノードが IP 層で全ての通信パケットの IP アドレスを変換することにより，上位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ことができる．Mobile PPC は通信開始時のアドレス解決と通信中の移動に係わるアドレス解決を明確に分離しており，前者を既存技術の DDNS（Dynamic DNS）により実現し，後者を Mobile PPC が実現する．

MN が移動した際の Mobile PPC の動作を図 2 に示す．CN と MN は既に DDNS を用いて，$G1 : a \leftrightarrow G2 : b$ の通信を開始しているものとする．通信中に MN が移動して新しく IP アドレス $G3$ を取得すると，MN は CN との間で CU Request/Response を交換して MN の新旧のアドレス $G2$，$G3$ の対応関係を記録する．CN と MN はカーネルの IP 層に CIT（Connection ID Table）と呼ぶ，以下のような両エンドノード共通のテーブルを生成する．

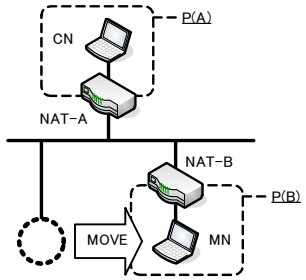


図 3 移動パターン (i)
Fig. 3 Moving pattern (i)

$$G1 : a \leftrightarrow \{G2 : b \Leftrightarrow G3 : b\}$$

このテーブルは $G1 : a \leftrightarrow G2 : b$ の通信を $G1 : a \leftrightarrow G3 : b$ のように変換することを示す．

テーブル生成後，両エンドノードは IP 層にて CIT を参照して，全てのパケットのアドレスを変換する．この処理によりパケットが正しくルーティングされ，かつ両エンドノードの上位アプリケーションは，MN のアドレスが変化したことに気付くことなく通信を継続できる．

ここで，もし MN が NAT 配下のネットワークに移動すると，NAT によるアドレス変換により CU Response 内の情報と IP ヘッダ内のアドレスが一致せず，正しい CIT を生成できない．また，CN が NAT 配下に存在する状況で通信が行われている時に MN が移動すると，NAT 越え問題により CU Request を CN に到達させることができない．仮にこれらの課題が解決されたとしても，NAT の SPI 機能により TCP パケットは破棄される．

2.3 移動パターンの分類と要求仕様

NAT の存在を考慮した場合に MN の移動パターンを整理すると表 1 にようになる．両エンドノードは，それぞれ，グローバルアドレス空間に存在する場合とプライベートアドレス空間に存在する場合がある．また MN は同一アドレス空間だけでなく，NAT を跨っ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間を移動することが考えられる．表 1 において，G はグローバルアドレス空間を，P はプライベートアドレス空間を示す．また P(A)，P(B)，P(C) はそれぞれ異なるプライベートアドレス空間であることを示す．表 1 に示すように移動パターンは 14 通り存在する．

表 1 の内，(i) の移動パターンを図 3 に示す．(i) は，プライベートアドレス空間に存在する CN がグローバルアドレス空間に存在する MN に対して通信を開始した後，MN が CN

表 1　MN の移動パターン一覧
Table 1　Lists of MN's moving patterns

No.	CN	MN (Before Moving)	MN (After Moving)	Reference
(a)	G	G	G	6)
(b)	G	G	P(A)	9)
(c)	G	P(A)	G	9)
(d)	G	P(A)	P(B)	9)
(e)	G	P(A)	P(A)	-
(f)	P(A)	P(A)	P(A)	-
(g)	P(A)	G	G	10)
(h)	P(A)	G	P(A)	-
(i)	P(A)	G	P(B)	10)
(j)	P(A)	P(A)	G	-
(k)	P(A)	P(B)	G	10)
(l)	P(A)	P(A)	P(B)	-
(m)	P(A)	P(B)	P(A)	-
(n)	P(A)	P(B)	P(C)	10)

の存在するプライベートアドレス空間 P(A) とは異なるプライベートアドレス空間 P(B) に移動を行った場合である．この移動パターンは移動透過性を実現する上で最も複雑な処理が必要となるため，3 章以降においては図 3 のケースを説明の対象とする．

Mobile PPC ではこれまでに文献 9) において (b)，(c)，(d) の移動パターンについて検討しているが，NAT が SPI 機能を実装していると実現が困難である．文献 10) では (g)，(i)，(k)，(n) の移動パターンを実現しているが NAT に改造を加える必要がある．また (i)，(k)，(n) では，NAT が SPI 機能を実装していると実現が困難である．

本論文では，表 1 に示す全ての移動パターンを NAT に改造を加えることなく実現することを目的とする．また，全ての NAT には SPI が搭載されていてもよいものとする．Mobile PPC のエンドエンドの特性はできるだけ継承する．更に上位アプリケーションには依存しないものとする．

3. 提 案 方 式

本提案では第三の装置としてリレーサーバ RS（Relay Server）を導入する．RS は DNS サーバとしての役割と特定のケースにおける中継装置としての役割を果たす．MN 側の RS と CN 側の RS は独立していてよい．以後，移動パターンとしては図 3 を用いて説明する．

3.1　立ち上げ時の動作

ノード立ち上げ時の動作を図 4 に示す．CN，MN が依存する RS をそれぞれ $\mathrm{RS_{CN}}$，$\mathrm{RS_{MN}}$ とし，アドレス $G8$，$G9$ を持つ．また CN はアドレス $G3$ の NAT-A 配下に存在し，アドレス $P3$ を持つ．CN は電源投入後，自身の UDP ポート番号 h から $\mathrm{RS_{CN}}$ の UDP ポート番号 r に Registry Request を送信し，FQDN「$CN.exp$」，IP アドレス「$P3$」を報告する．r はメッセージを待ち受ける RS の UDP ポート番号である．この時，NAT-A は $P3:h \rightarrow G8:r$ のパケットにエフェメラルポート h' を割り当て，以下のような NAT テーブルを生成する．

$$\{P3:h \Leftrightarrow G3:h'\} \leftrightarrow G8:r$$

$\mathrm{RS_{CN}}$ はこれを受信するとこれらの情報に加え，NAT-A の外側の IP アドレス「$G3$」と NAT-A に割り当てられたエフェメラルポート「h'」をデータベースに登録する．$\mathrm{RS_{CN}}$ は応答として Registry Response を返す．その後 CN は NAT-A のエフェメラルポート h' の変換テーブルを維持するため，$\mathrm{RS_{CN}}$ に対して定期的に Keep Alive を送信する．

MN も同様の処理により自身の FQDN「$MN.exp$」，IP アドレス「$G1$」を $\mathrm{RS_{MN}}$ のデータベースに登録する．MN はグローバルアドレス空間に存在しているため，NAT の情報は登録されない．

3.2　通信開始時のアドレス解決

CN が MN に通信を開始する場合のアドレス解決処理を図 5 に示す．CN はまず，MN の名前 $MN.exp$ を記載した DNS Query を $\mathrm{RS_{CN}}$ に送信し，MN の IP アドレスを問い合わせる．即ち，$\mathrm{RS_{CN}}$ は CN のプライマリ DNS でもある．$\mathrm{RS_{CN}}$ は DNS の仕組みにより，$\mathrm{RS_{MN}}$ より MN の IP アドレス $G1$ を取得し，CN に返す．この時，CN は自身と MN の IP アドレスがどのような関係であるかを知ることができる，図 3 の場合，CN はプライベートアドレス空間に，MN はグローバルアドレス空間に存在する．

3.3　通信時の動作

通信時の動作を図 6 に示す．CN は取得した情報から，自身の UDP ポート番号 m から MN の UDP ポート番号 r に Tunnel Request を送信し，IP アドレス「$P3$」を報告する．この時 NAT-A は $P3:m \rightarrow G1:r$ のパケットにエフェメラルポート m' を割り当て，以下のような NAT テーブルを生成する．

$$\{P3:m \Leftrightarrow G3:m'\} \leftrightarrow G1:r$$

MN は応答として Tunnel Response を返す．

以上の処理により CN と MN はポート番号 m と r の UDP トンネルを形成し，以後はこ

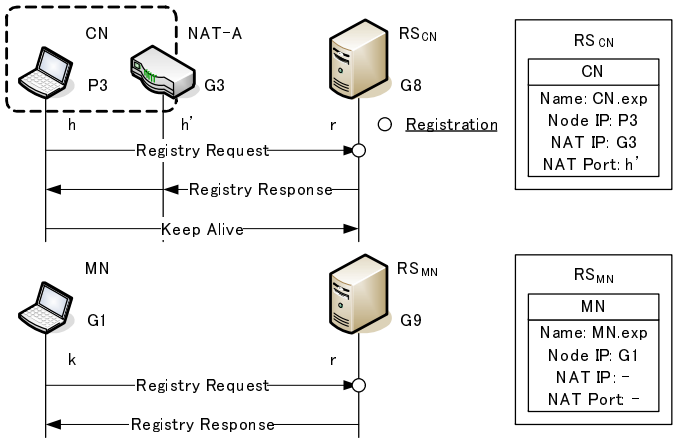


図 4 立ち上げ時の動作
Fig. 4 Setup Process

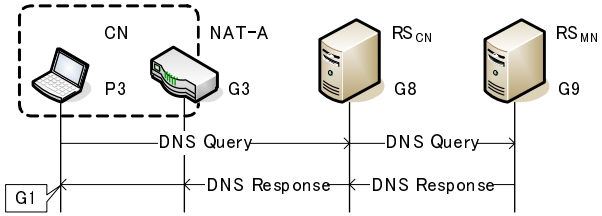


図 5 通信開始時のアドレス解決
Fig. 5 Address Resolution process when communication starts

のトンネルを用いて通信を行う．UDP トンネルを用いることにより，通信パケットが TCP の場合でも SPI に影響されることがなくなる．

3.4 移動時の動作

MN が通信中に NAT-B 配下のプライベートアドレス空間に移動した時の動作を図 7 に示す．MN は $P5$ を取得したものとする．MN は NAT 配下に移動したので，CN が実行した図 4 及び図 6 に示した動作と同様の動作，即ち RS への情報登録とトンネル通信経路の形成を行う．MN は自身の UDP ポート番号 n より Registry Request を $\mathrm{RS_{MN}}$ に送信し，

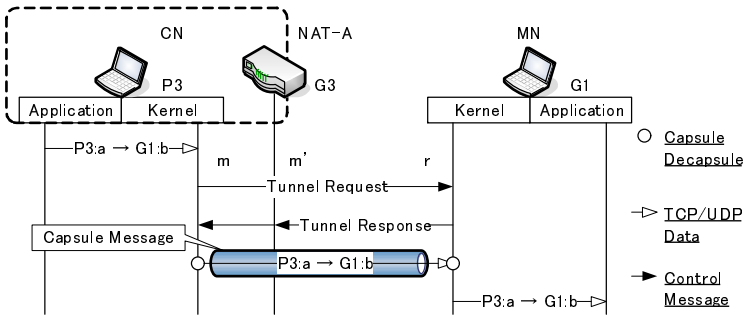


図 6 通信時の動作
Fig. 6 Communication process

MN の IP アドレス「$P5$」，NAT-B の IP アドレス「$G5$」，NAT-B のエフェメラルポート「n'」を登録する．MN は自身の IP アドレスと CN の IP アドレスから，それぞれがどのようなアドレス空間に存在するかを確認する．図 3 の移動パターンの場合，NAT を 2 台経由する必要があることが分かる．この場合は NAT に手を加えないと言う条件の元ではエンドノードで直接通信を行うことができない．そこで RS を経由したトンネル経路を確保し，その経路を用いてエンドエンドの通信を継続する．

MN は $\mathrm{RS_{CN}}$ に対してポート番号 o より Tunnel Request を送信し，MN − $\mathrm{RS_{CN}}$ 間のトンネルを形成する．この時 NAT-B に生成される NAT テーブルは以下のようになる．

$$\{P5 : o \Leftrightarrow G5 : o'\} \leftrightarrow G8 : r$$

CN − $\mathrm{RS_{CN}}$ 間のトンネルは CN が立ち上げ時に既に形成されている．以上の処理により CN-$\mathrm{RS_{CN}}$ 間，MN-$\mathrm{RS_{CN}}$ 間の UDP トンネルが形成され，MN と CN の間の通信経路が確立する．

CN − $\mathrm{RS_{CN}}$ 間及び MN − $\mathrm{RS_{CN}}$ 間の UDP トンネルを用いて中継通信を行うに際し，$\mathrm{RS_{CN}}$ は UDP トンネル同士のバインディングをとる必要がある．そのため，以後のトンネル化されたデータパケットには新たなヘッダを定義し，転送先を示すフィールドを持たせる．このフィールドに宛先のノードが属する NAT の外側の IP アドレスを記載する．図 8 に $\mathrm{RS_{CN}}$ がデータパケットを MN から CN に UDP トンネルを用いて転送する処理を示す．

MN は CN に送信するデータパケットを UDP ヘッダ $G8 : r \leftarrow P5 : o$ でカプセル化し，ヘッダ内に NAT-A のアドレス $G3$ を記述して $\mathrm{RS_{CN}}$ に送信する．このパケットは NAT-B

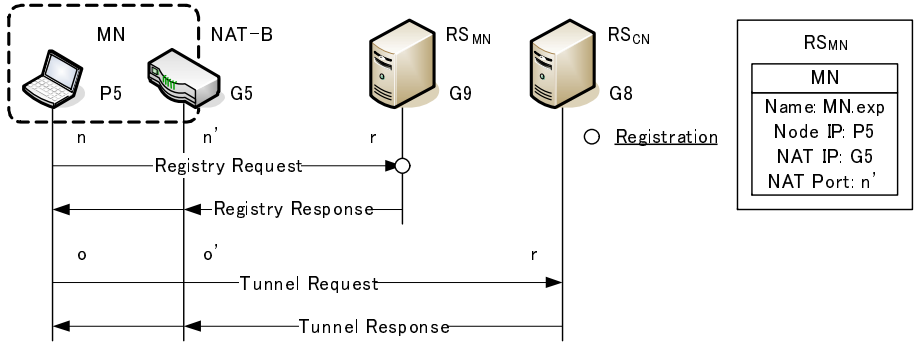


図 7 MN が移動した時の動作
Fig. 7 Mobility process when MN moves

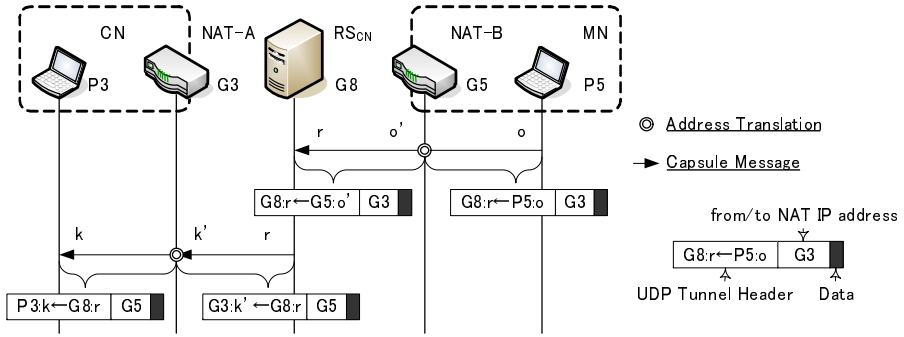


図 8 RS の転送処理
Fig. 8 The transfer processing that RS performs.

にて UDP ヘッダが $G8 : r \leftarrow P5 : o'$ に変換され，$\mathrm{RS_{CN}}$ に到達する．$\mathrm{RS_{CN}}$ はこれを受信すると，NAT-A のアドレス $G3$ から CN $-$ $\mathrm{RS_{CN}}$ 間のトンネルを選択し，一度デカプセル化を行った後に，UDP ヘッダ $G3 : k' \leftarrow G8 : r$ でカプセル化し，NAT-B のアドレス $G5$ を記述して CN に送信する．途中，このパケットは NAT-A で $G3 : k \leftarrow G8 : r$ に変換され，CN に到達する．逆方向の通信においても同様の処理を行うことにより，トンネルによる通信経路が確立する．

図 8 のようにして確保した通信経路を用いて，Mobile PPC によるエンドエンドの移動通

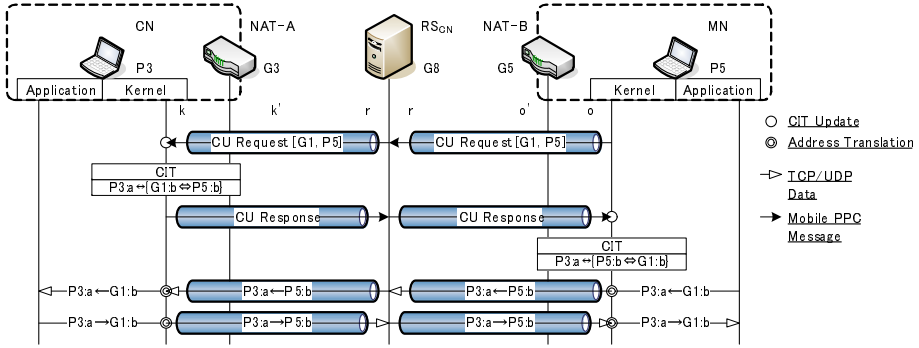


図 9 トンネルを利用した Mobile PPC の動作
Fig. 9 Mobile PPC process with a tunnel technology

知処理を実行する．図 9 に上記 UDP トンネルを用いた Mobile PPC の動作を示す．MN は UDP トンネルを利用して CN との間で通常の Mobile PPC と同様に CU Request/Response を交換する．UDP トンネルを用いるため CU パケットの IP ヘッダの内容は変換されず，CU メッセージ内の情報と不一致となることはない．これにより CN，MN は MN の新旧のアドレス $G1$，$P5$ の対応関係を以下のように CIT に記録することができる．

$$P3 : a \leftrightarrow \{G1 : b \Leftrightarrow P5 : b\}$$

この後の通信では，Mobile PPC の機能により両エンドノードは IP 層にて CIT を参照して，全てのパケットのアドレスを送信時には $G1$ から $P5$ に，受信時には $P5$ から $G1$ に変換する．送受信パケットは全て UDP トンネルを利用して送受信するため，SPI によりパケットが破棄されることはない．この処理により両エンドノードの上位アプリケーションは，MN の IP アドレスの変化に気付くことなく通信を継続できる．

図 3 以外の通信パターンにおいても，両エンドノードのトポロジを調べ，そのトポロジに応じて上記と同様の処理を行うことにより，全てのケースにおいて移動透過性を実現できる．なお，グローバルアドレス空間のみを移動する場合はこれまでの Mobile PPC の動作と全く同じである．

4. ま と め

本論文では，IPv4 において NAT を含むあらゆる通信トポロジや移動パターンで移動透過性を実現する方式を提案した．Mobile PPC と，UDP トンネルを組み合わせ，通信トポ

ロジに応じた通信経路を確立した上でエンドエンドの移動通知を行うことにより SPI が実装された NAT でも NAT 越えを実現しつつ，移動透過性を実現できることを示した．

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， Vol.J87-D1, No.3, pp.308–328 (2004).
2) Perkins, C.: IP Mobility Support for IPv4, RFC 3344, IETF (2002).
3) Johnson, D., Perkins, C. and Arkko, J.: Mobility Support in IPv6, RFC 3775, IETF (2004).
4) Kunishi, M., Ishiyama, M., Uehara, K., Esaki, H. and Teraoka, F.: LIN6: A New Approach to Mobility Support in IPv6, *Proceedings of WPMC2000* (2000).
5) 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性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).
6) 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).
7) Levkowetz, H. and Vaarala, S.: Mobile IP Traversal of Network Address Translation (NAT) Devices, Technical report (2003).
8) 井戸上彰，久保　健，横田英俊：プライベートアドレスを使用するモバイルネットワーク間のローミング手順とその実装，情報処理学会論文誌， Vol.44, No.12, pp.2958–2967 (2003).
9) 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).
10) 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).

NATを跨る移動透過性を実現するMobile PPCの提案

名城大学大学院 理工学研究科
水谷智大，鈴木秀和，渡邊 晃

研究背景

- 移動通信の需要の増加
  - 小型携帯端末や無線LAN環境の普及
- IPv4における移動透過性は重要
  - 移動透過性の研究はIPv6を前提としたものが多い
  - IPv6はIPv4との互換性がほとんどなく，特にエンドユーザにIPv6は普及していない
  - 将来，長期においてIPv4はIPv6と共に混在すると予想される
- IPv4ではNATを介した通信が一般的
  - アドレス枯渇対策NAT → グローバル空間とプライベート空間が存在

NAT: Network Address Translation

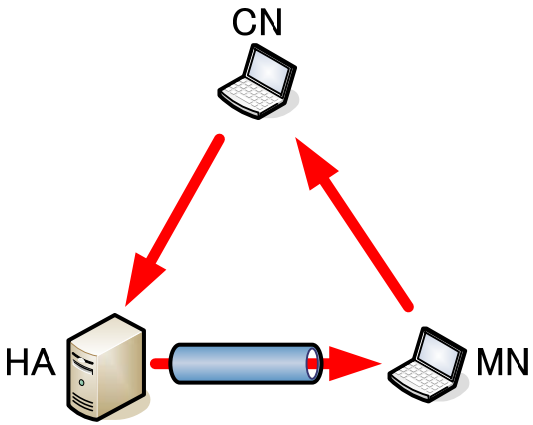
移動透過性

- 移動透過性
  - ノード移動時のIPアドレスの変化をアプリケーションに対して隠蔽
    ⇒ノードが移動しても通信を継続できる

- IPv4における代表的な移動透過性技術 - Mobile IP
  - 常にHAを経由した通信　⇒経路冗長化 ・ 一点障害
  - 常にカプセル化を行う　⇒パケットサイズが冗長
  - MNからCN宛のパケットの送信元IPアドレスの偽装
    ⇒配送途中のルータでの破棄の可能性

- これらの課題を全て解決

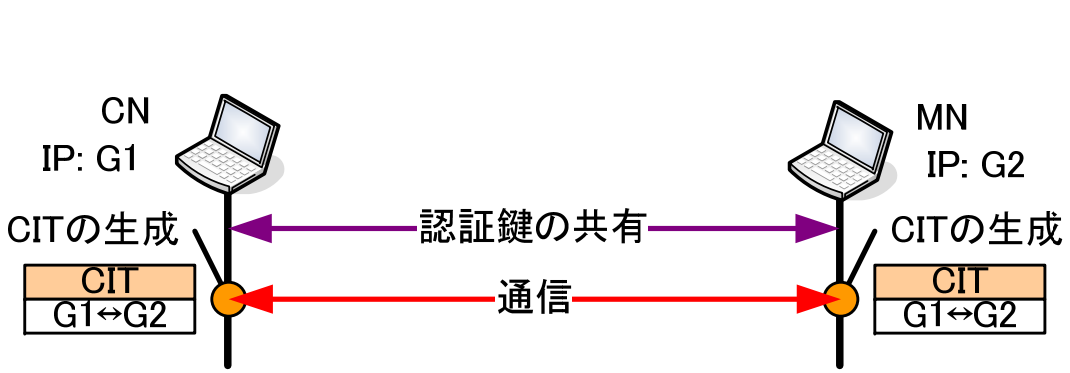
Mobile PPC



HA: Home Agent, MN: Mobile Node, CN: Correspondent Node, Mobile PPC: Mobile Peer to Peer Communication

Mobile PPCの動作概要

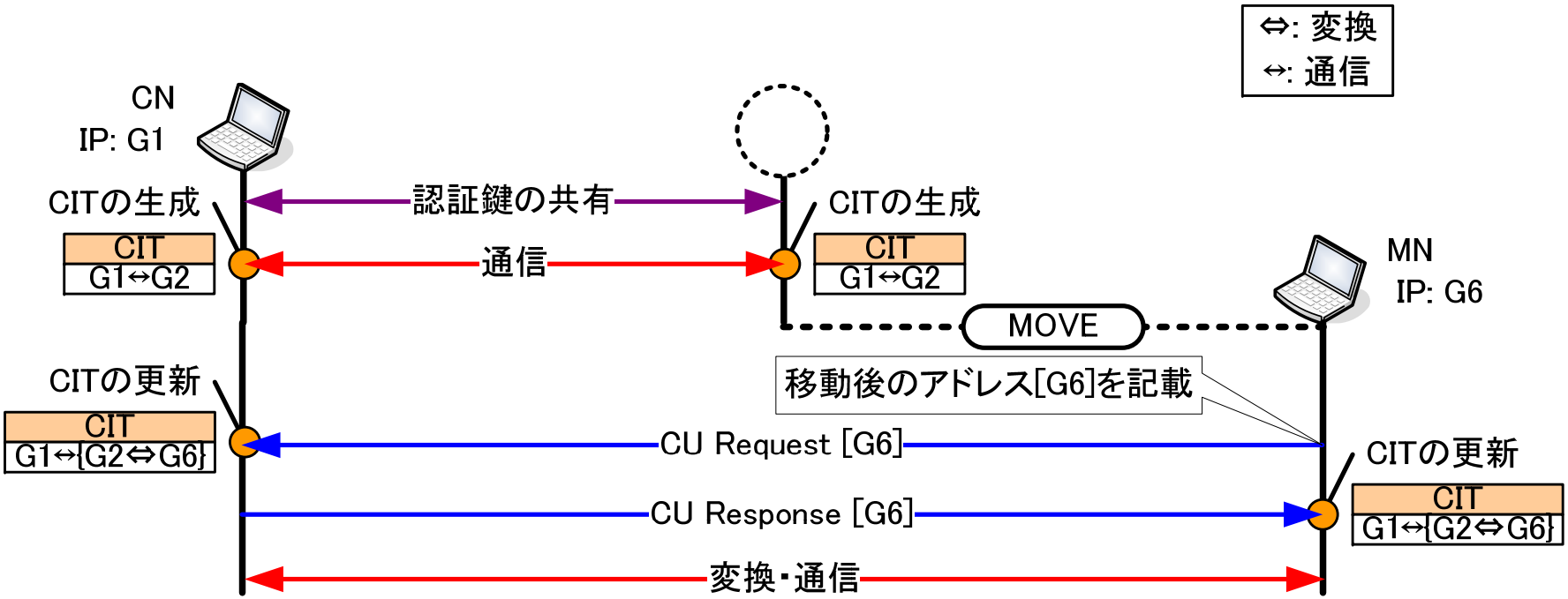
- パケットのIPアドレスを変換してIPアドレスの変化を隠蔽する
  - 両エンドノードはIP層にアドレス変換テーブルCITを持つ
  - MNは移動後，CNと移動情報CUを交換し，両ノードはCITを更新する



CIT: Connection ID Table, CU: CIT Update

Mobile PPCの動作概要

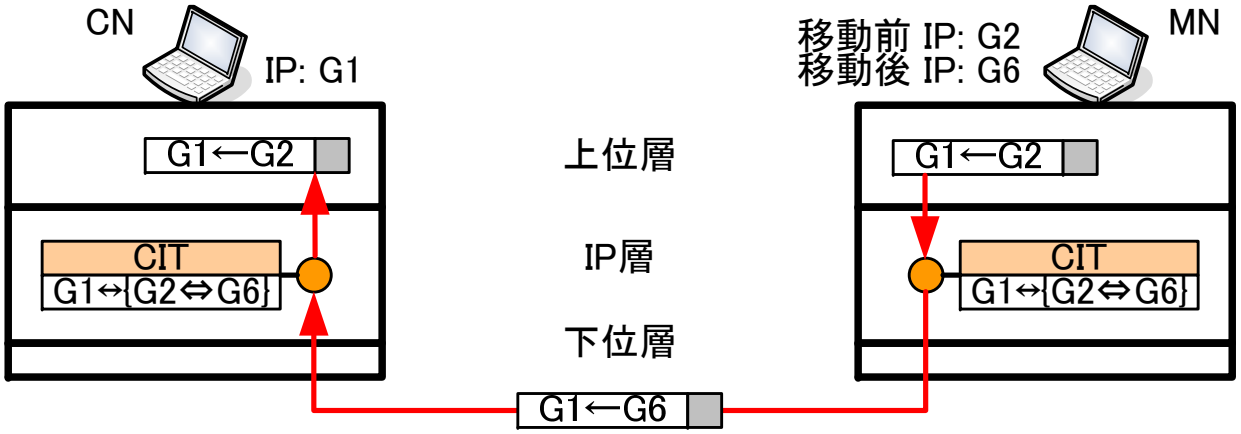
- パケットのIPアドレスを変換してIPアドレスの変化を隠蔽する
  - 両エンドノードはIP層にアドレス変換テーブルCITを持つ
  - MNは移動後，CNと移動情報CUを交換し，両ノードはCITを更新する



CIT: Connection ID Table, CU: CIT Update

移動透過性 - Mobile PPCのアドレス変換処理

- アドレス変換によって通信を継続
  - 上位層: 移動前のアドレスで通信を認識
  - 下位層: 移動後のアドレスでルーティング



- 通信経路にNATが存在する場合

  →NATによる変換により，パケットのIPアドレスがCITに一致しない

NATに対応しなければならない

NAT越え問題とSPI

- NAT越え問題
  - NATは内側からのパケットに対して変換テーブルを生成する（動的）
    ⇒NAT外側から内側に通信を開始できない
  - 近年のNATルータにはSPIが搭載されていることが多い

- SPI
  - 通信が集約されるNATで有効なフィルタリング法
  - TCPにおける3way-handshake，シーケンス番号などの矛盾を検知

強力なフィルタリング ➡ NAT越えをより困難にする

SPI: Stateful Packet Inspection

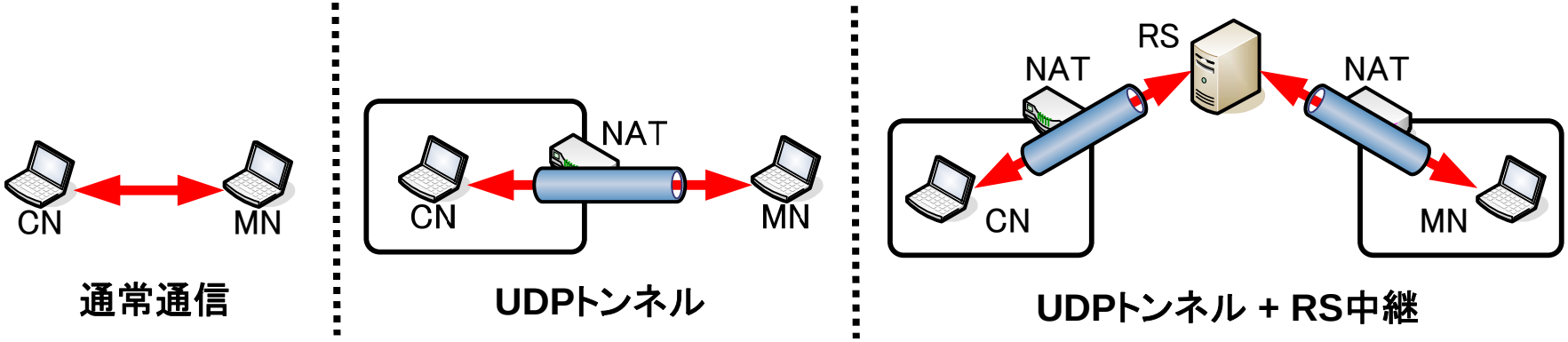
提案方式の目的

NATの存在に関わらず，ノードが自由に移動する

NATへの改造を加えないNAT越え → 中継サーバRSを導入し，中継通信

SPIに対応 → UDPトンネル

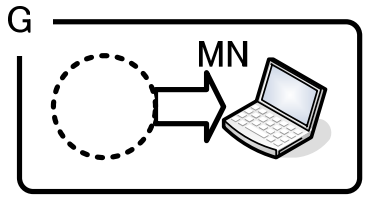
- スループットの低下を避けるため，通信形態を分類



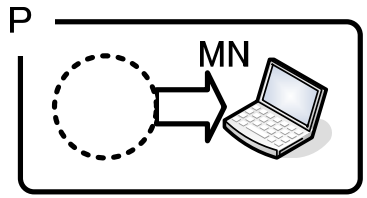
RS: Relay Server

移動パターン

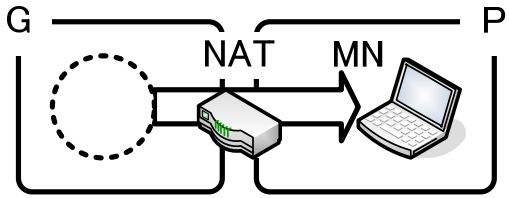
- 考えられるMNの移動



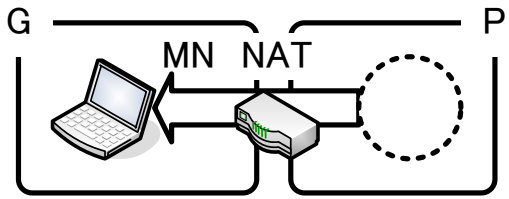
グローバル空間内の移動



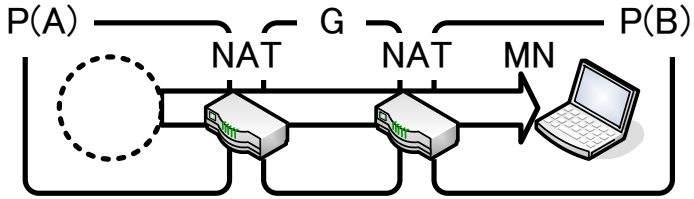
プライベート空間内の移動



グローバル空間から
プライベート空間への移動



プライベート空間から
グローバル空間への移動



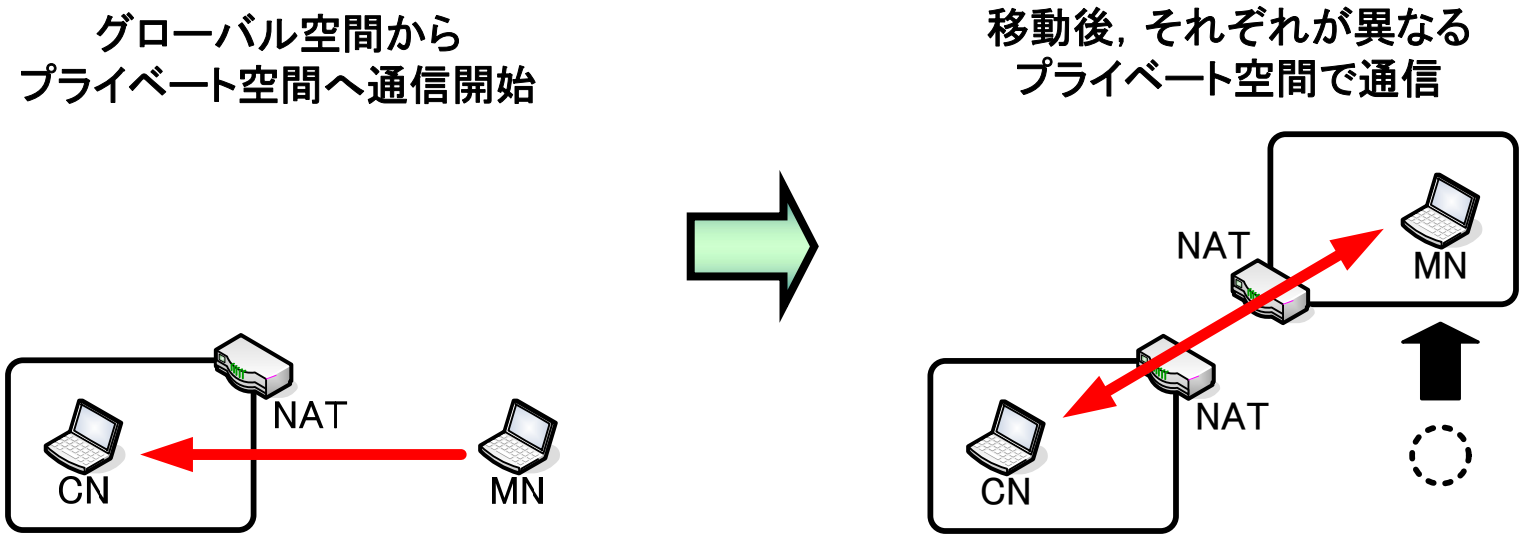
あるプライベート空間から
異なるプライベート空間への移動

- CNが存在するアドレス空間
  - グローバル空間
  - プライベート空間
  - MNと同一のプライベート空間

これら14種を全て実現

本発表で説明する通信

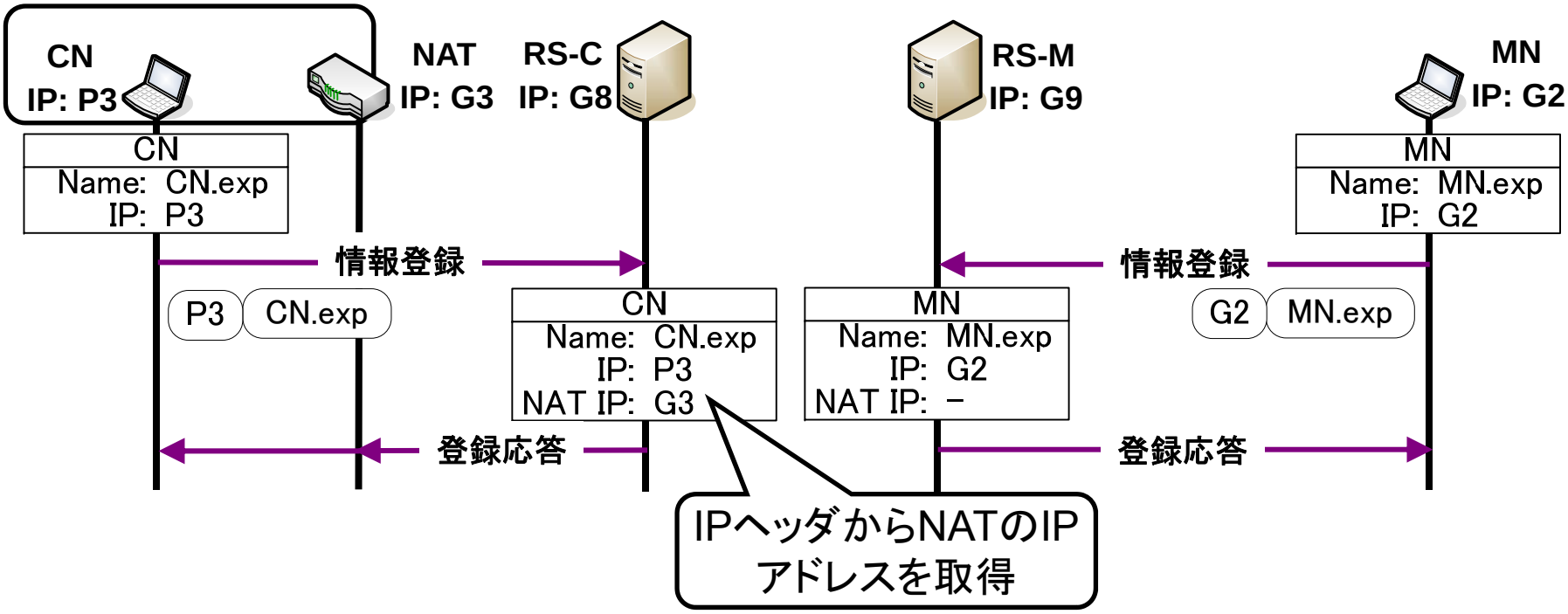
- 14つの移動パターンの内，以下のパターンを例に説明する



- 通信開始時: プライベートアドレス空間への通信開始
  - 片側のNAT越え通信を実現する
- 移動後: 異なるプライベートアドレス空間の通信
  - 両側のNAT越え通信を実現する

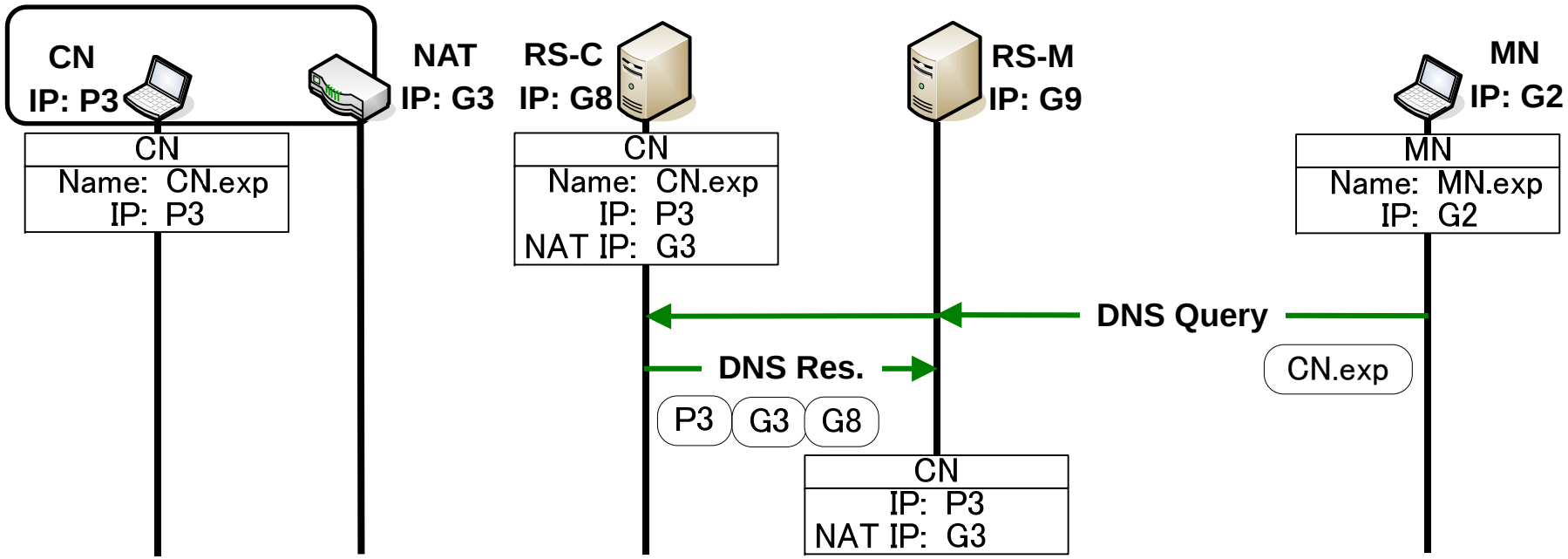
提案方式の詳細動作 - 通信開始 - 登録

- 各エンドノードは立ち上げ時，各々の依存するRSに情報を登録する
  - CNはRS-Cに，MNはRS-Mに情報を登録
  - 本提案で用いるメッセージはUDPベースであり，これにより形成されたNATポートを用いてRSからノードへアクセスする



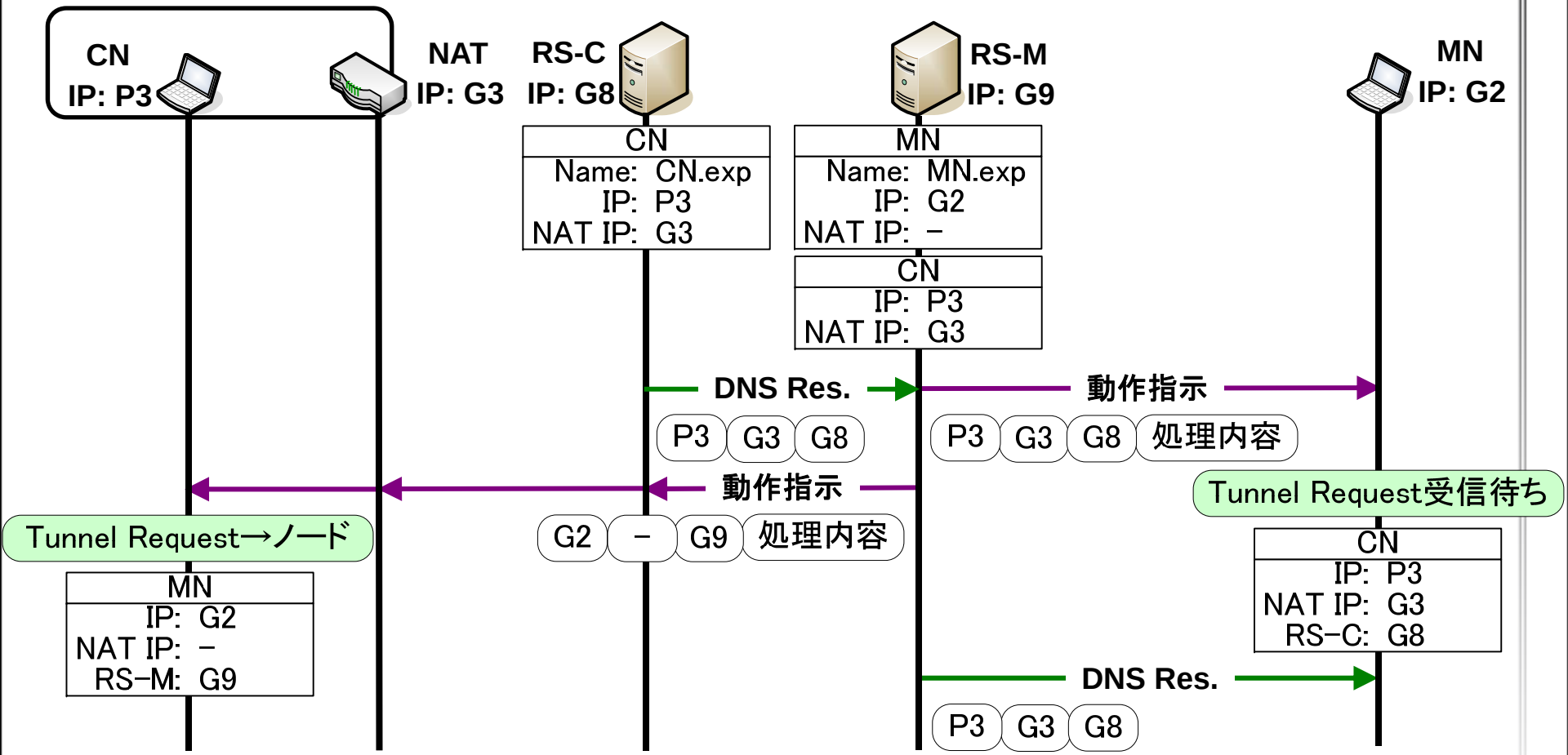
提案方式の詳細動作 - 通信開始 - 問い合わせ (1/2)

- RSはDNSの機能を持つ
- 通信開始ノードはDNSを用い，通信相手ノードの情報を問い合わせる



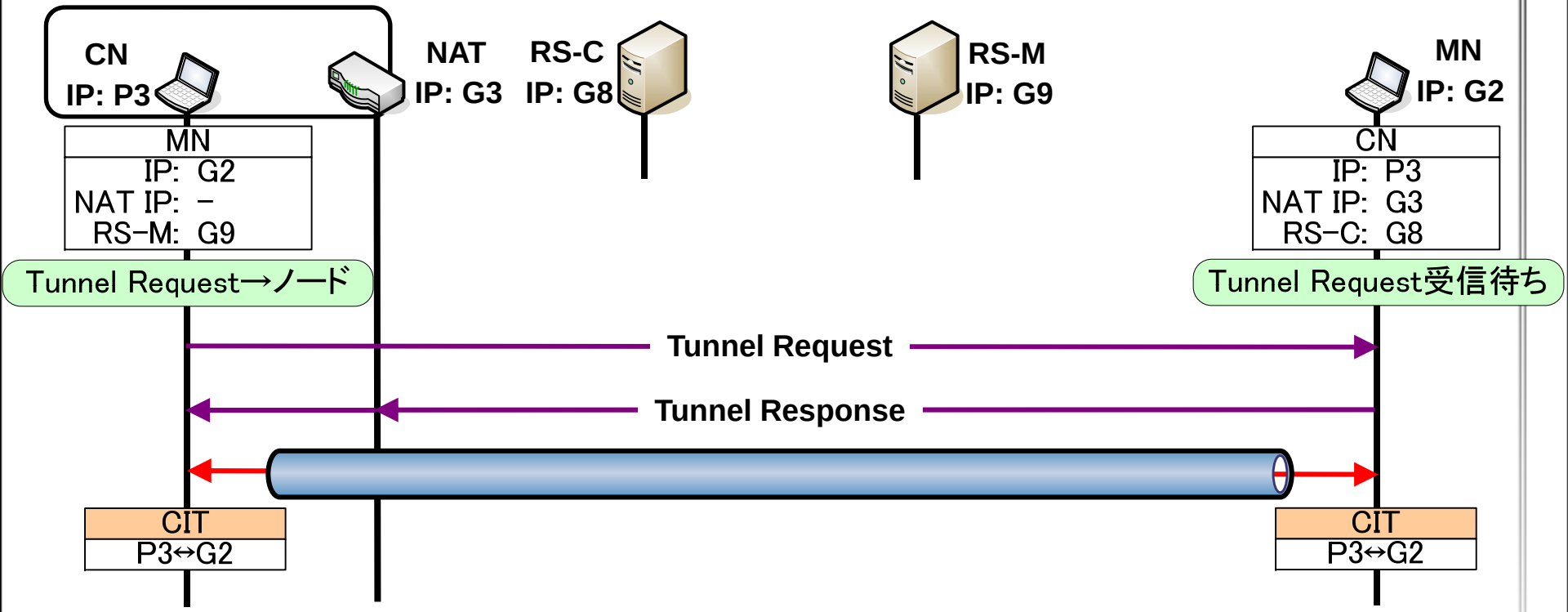
提案方式の詳細動作 - 通信開始 - 問い合わせ (2/2)

- RS-MはCN・MNの情報から，各ノードに適切な動作を指示



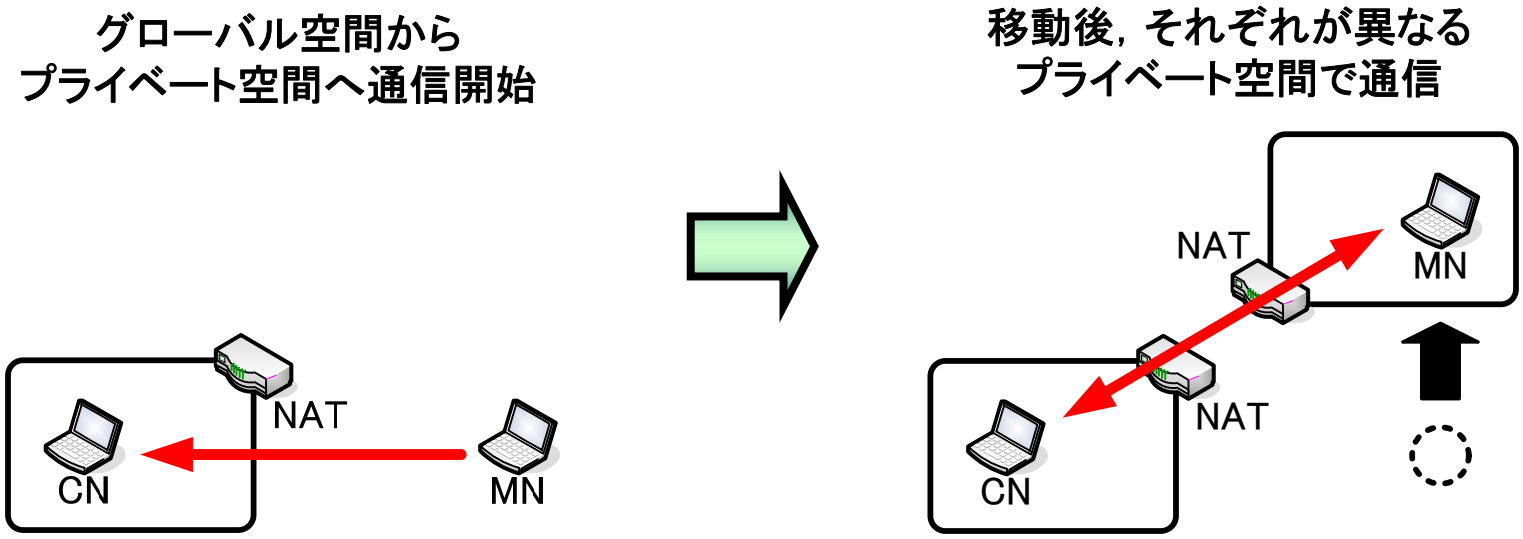
提案方式の詳細動作 - 通信開始 - UDPトンネル生成・通信

- CN・MNは受けた指示に従って処理を行う



本発表で説明する通信

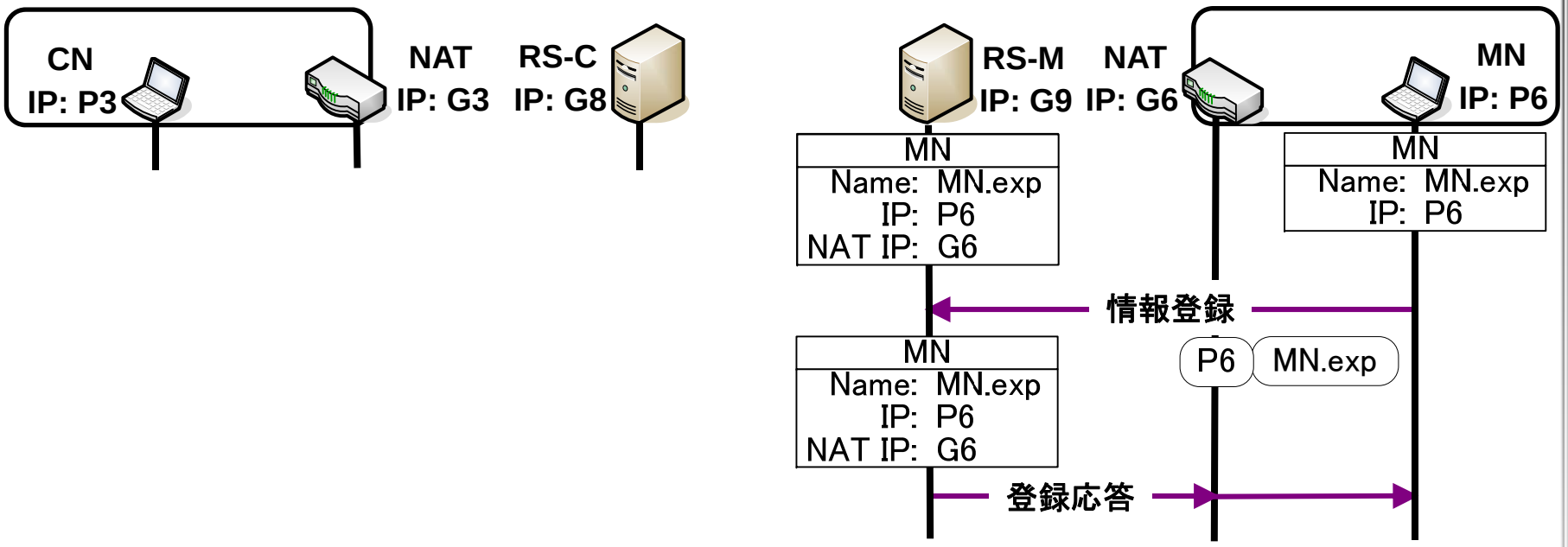
- 14つの移動パターンの内，以下のパターンを例に説明する



- 通信開始時: プライベートアドレス空間への通信開始
  - 片側のNAT越え通信を実現する
- **移動後: 異なるプライベートアドレス空間の通信**
  - **両側のNAT越え通信を実現する**

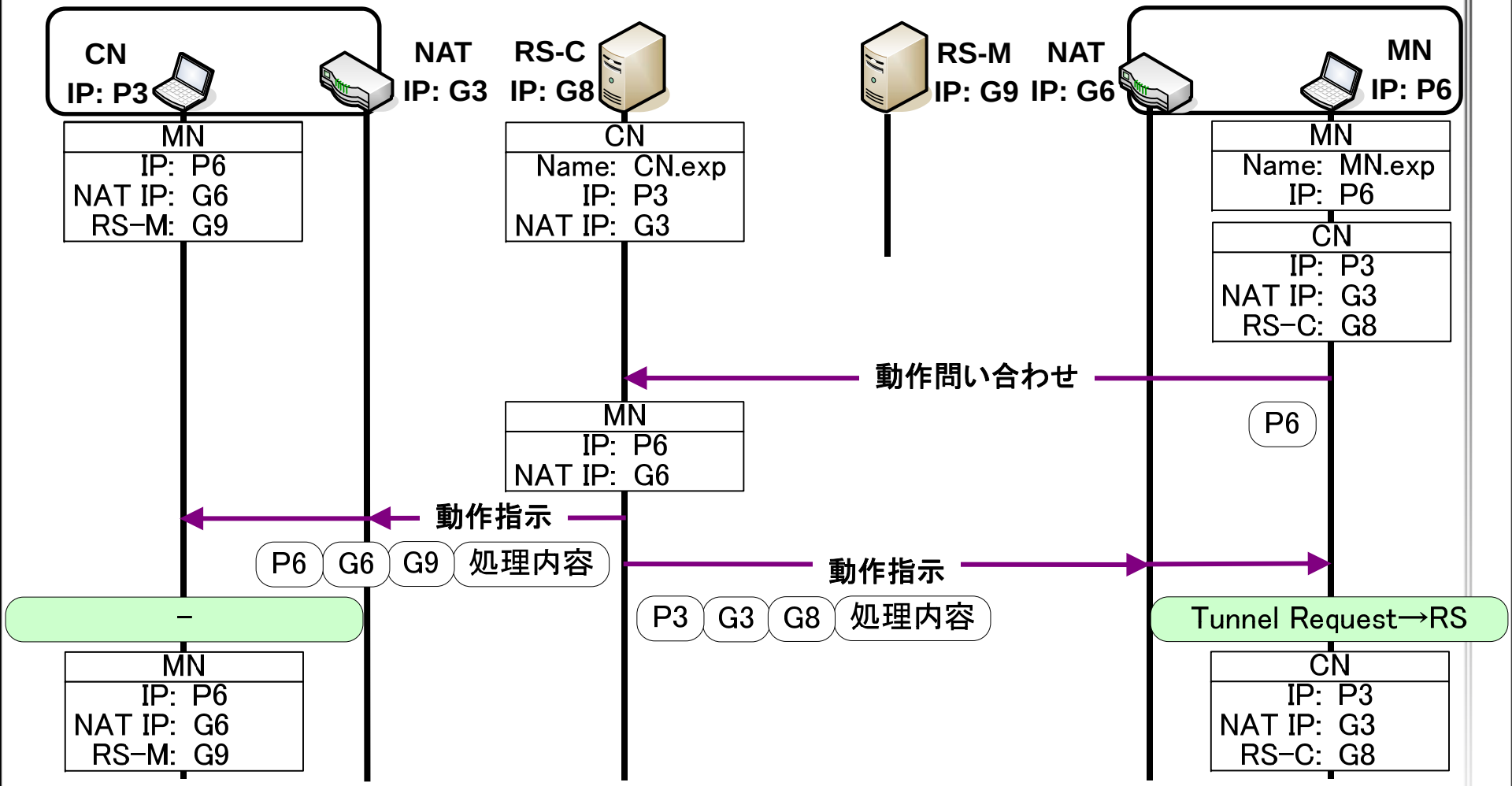
提案方式の詳細動作 - 移動 - 登録

- MNは移動後，自身の新しいIPアドレスをRS-Mに登録する



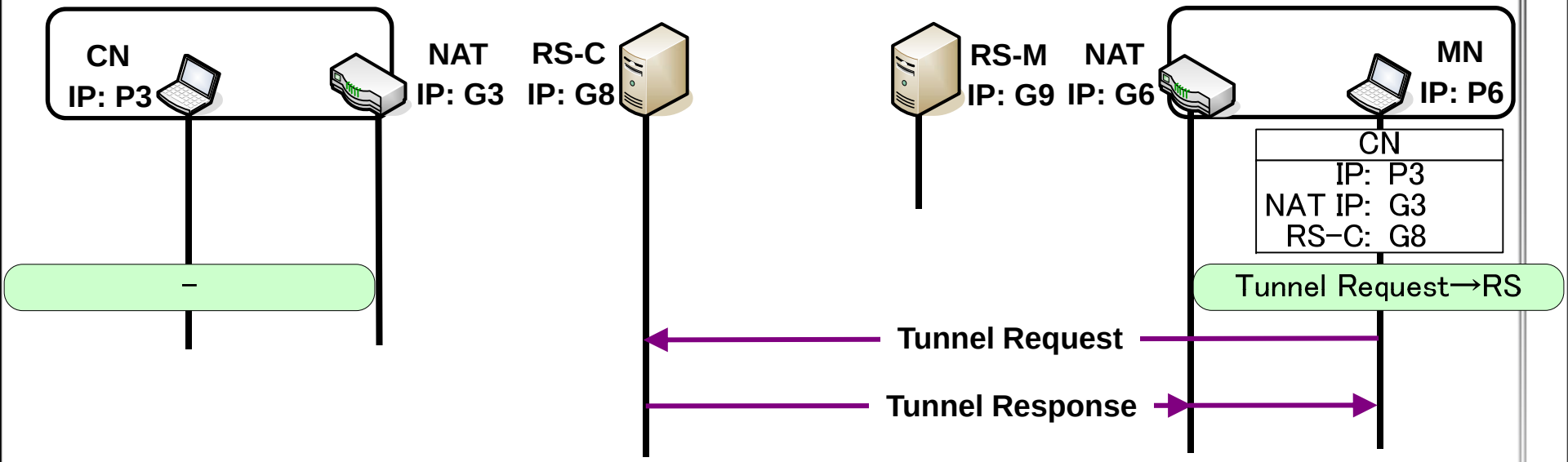
提案方式の詳細動作 - 移動 - 問い合わせ

- MNはRS-Cに対して，動作を問い合わせる



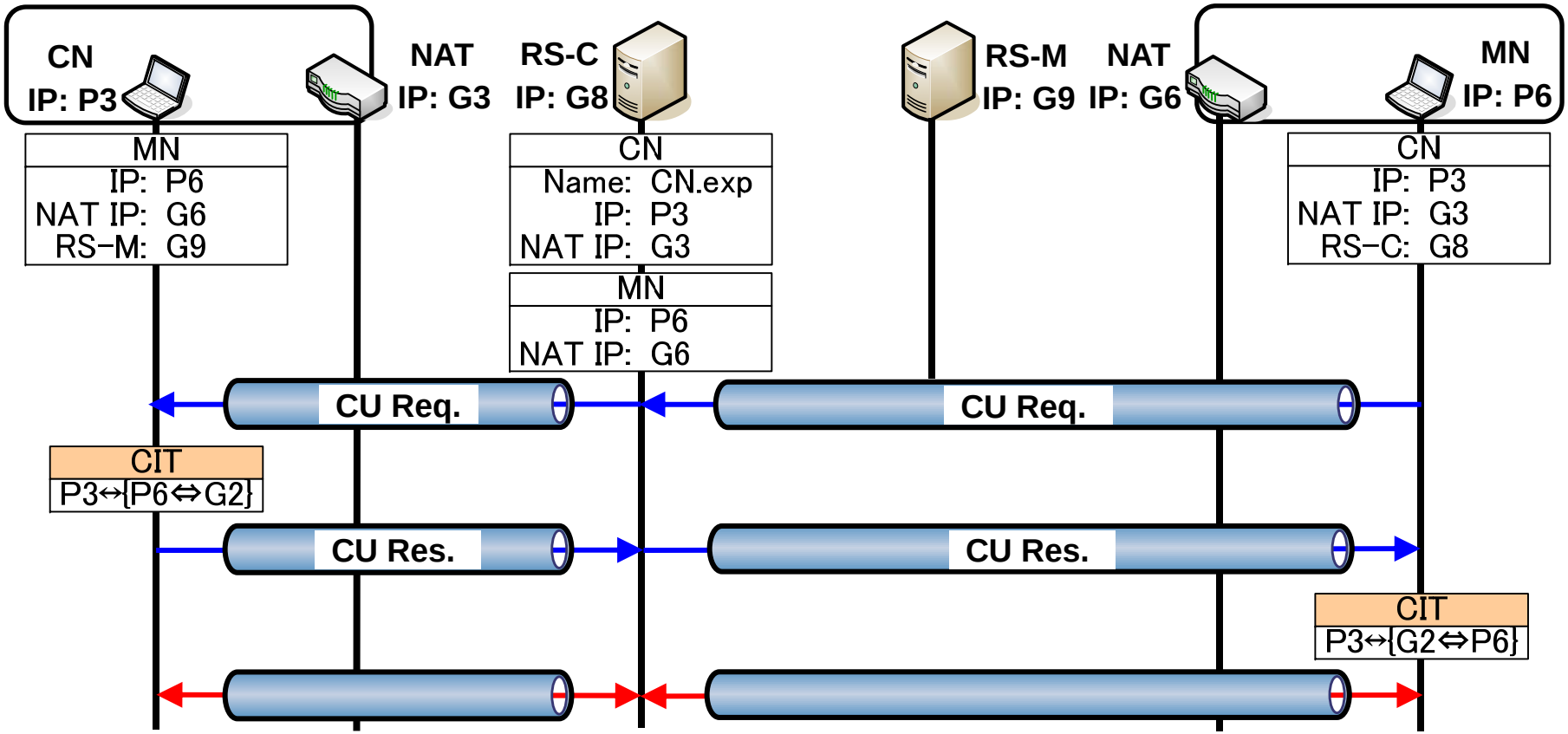
提案方式の詳細動作 - 移動 - UDPトンネル生成

- CN・MNは受けた指示に従って処理を行う



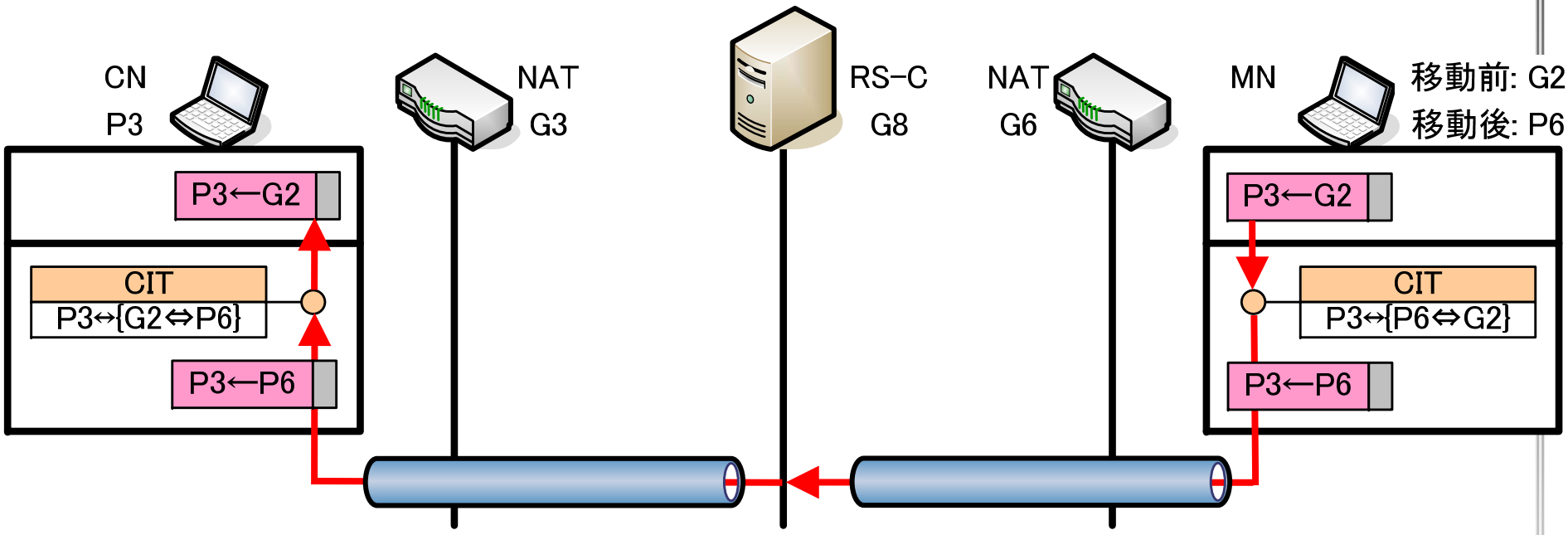
提案方式の詳細動作 - 移動 - CU交換・UDPトンネル中継通信

- 形成されたUDPトンネルを利用し，CU交換を行う
- UDPトンネルと更新されたCITにより，変換と中継通信を行う



提案方式のパケットの遷移

- トンネルを利用する以外は通常のMobile PPCの動作



- 他の移動パターンの場合でも，RSにUDPトンネルの形成の必要の有無や対象を問い合わせ，同様の処理で実現できる

まとめと今後

- IPv4ではNATを利用した通信が考えられ，また近年ではSPIと呼ばれるコネクションの矛盾を検出するフィルタリングが行われていることが多い
- これらSPIを搭載したNATを含む，あらゆる通信形態でNAT越えを実現しつつ移動透過性を実現する方式を提案した
- 今後は提案方式を実装して実機において動作検証を行う予定である