

NTMobileにおける一般SIP端末との通信確立手法

吉岡 正裕¹ 鈴木 秀和¹ 内藤 克浩² 旭 健作¹ 渡邊 晃¹

概要: マルチメディア通信で近年頻繁に利用される SIP (Session Initiation Protocol) は, メッセージ内に IP アドレスを記述するため, 通信経路上に NAT (Network Address Translation) のようなアドレス変換装置があると利用できない. 我々は, あらゆるネットワーク環境での接続性を可能とする NTMobile (Network Traversal with Mobility) を提案している. NTMobile では, あらゆるケースにおける接続性を実現するため, 通信パケットの中継を行う RS (Relay Server) と呼ぶ機器が存在する. 本稿では, RS が端末の利用するポート番号を割り当てを行うことにより, NTMobile において一般 SIP 端末との通信が可能になる手法について提案する.

キーワード: 移動透過性, NAT 越え, SIP

Method for establish communication with SIP Terminal in NTMobile

YOSHIOKA MASAHIRO¹ SUZUKI HIDEKAZU¹ NAITO KATSUHIRO² ASAHI KENSAKU¹ WATANABE AKIRA¹

Abstract: SIP is widely used as the signaling protocol for multimedia communication. However, SIP cannot traverse NAT because it contains IP addresses in message body of IP packets. We have been proposing NTMobile (Network Traversal with Mobility) that can prove connectivity in every network environments. NTMobile has the convenient device called RS (Relay Server) that relays packets when end to end communication is difficult. In this paper, we propose the SIP communication method that can traverse NAT between an NTMobile node and a general SIP node. The proposed method uses modified RS that has the allocation function of port numbers of the NTM node.

Keywords: Mobility, NAT Traversal, SIP

1. はじめに

IPv4 ネットワークでは IP アドレスの枯渇を回避するため, 家庭内や企業のネットワークはプライベートアドレスで構築するのが一般的である. それらのネットワークとインターネットの間には NAT (Network Address Translator) が導入されている. このような環境ではインターネット側からは NAT しか見えなくなるため, NAT 外側の端末から内側の端末へ通信を開始することができないという制約が

ある. これは NAT 越え問題と呼ばれている. これまでのインターネットの利用形態は WWW の閲覧やメールの利用など, 一般にグローバルアドレス空間に設置されたサーバに対してプライベートアドレス空間に存在する端末側から通信を開始していた. ファイアウォールでもこのような通信形態のみを許可するのが一般的であったため, NAT の制約が表面化することはなかった. しかし, 家庭にもネットワークが導入され始めており, 外出先から家庭内の端末に自由にアクセスしたいというニーズが増加していくものと考えられる. また, LSN (Large Scale NAT) のようにインターネットプロバイダ自身のネットワークをプライベートアドレスで実現するような状況も想定される. このため IPv4 ネットワークにおいて NAT 越え問題を解決す

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

² 三重大学大学院工学研究科
Graduate School of Engineering, Mie University

ることは有益である。NAT 越え問題を解決する技術としては、現存する NAT をそのまま使えることを目的としたアプリケーションレベル改造方式 (STUN[2], TURN[3], UPnP[4]), 既存のアプリケーションをそのまま使用することを目的としたネットワークレイヤ改造方式 (4+4[5], NAT-f[6], MIPNAT[7]), 端末の改造を不要とすることを目的とした端末非依存方式 (AVES[8], NTSS[9]) がある。

一方、近年頻繁に使用されるマルチメディア通信の SIP (Session Initiation Protocol) [1] がセッション制御技術として注目され始めている。SIP は IP ペイロード部分に IP アドレスが記載されているプロトコルであり、単なる NAT 越え技術のみでは対応できない。SIP が NAT を通過できる手段としては、NAT において SIP メッセージ中の IP アドレス/ポート番号を書き換える SIP-ALG (Application Level Gateway) [10] が挙げられる。これにより、SIP が NAT を通過することは可能であるが、NAT に改造が必要であるため、端末が一般の NAT 配下に移動できないという課題がある。

著者らは、NAT に改造を加えることなく NAT 越え問題の解決と移動透過性を同時に実現する NTMobile (Network Traversal with Mobility) と呼ぶ技術を提案している [11][12][13][14]。NTMobile は、端末に対して仮想 IP アドレスを割り当て、実際の通信を実 IP アドレスによる UDP トンネルを用いることで実現する。しかし、NTMobile においても IP ペイロード部分に IP アドレスが含まれているアプリケーションに対応する工夫が必要である。その方法の 1 つとして、NTMobile のアドレス無変換型 RS (Relay Server) という装置があり、これを利用することにより SIP 通信を実現する方法がある [15]。この方法では、端末の数だけグローバルアドレスが必要である。しかし、IP アドレスが枯渇する中で十分な数のグローバルアドレスを確保することは困難と考えられる。

そこで、本論文では、アドレス無変換型 RS からポート番号の割り当てを行うことにより RS のアドレスを 1 個で実現する手法を提案する。この方法によると、相手が一般の SIP 端末である場合においても SIP による接続性を実現することができる。

2. SIP

SIP はセッション制御プロトコルとして開発されており、セッションの開始・変更・終了のみを行う。主な用途として IP 電話やインターネット上の web 会議などの制御で使用されている。本章では、SIP のセッション確立方法と、SIP と NAT の関係について述べる。

2.1 セッション確立方法

図 1 に SIP の基本シーケンスを示す。UA (User Agent) 1 と UA2 は、それぞれ SIP Server A と B に対して、REG-

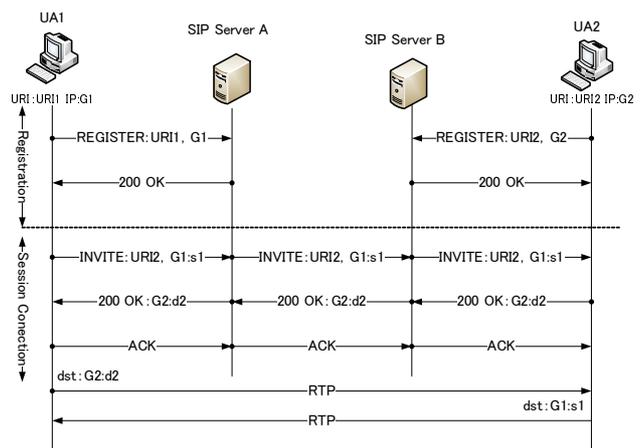


図 1 SIP の基本シーケンス

Fig. 1 Basic sequence of SIP.

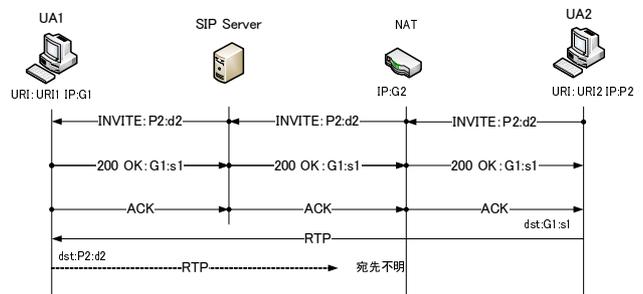


図 2 アドレス不整合問題

Fig. 2 Address mismatch problem.

ISTER により自身の URI (Uniform Resource Identifier) と自身の IP アドレス G1 および G2 を登録しておく。

通信開始時、UA1 は INVITE により UA2 とのセッションの確立を要求する。INVITE には、UA1 が使用する IP アドレス G1 とポート番号 s1 が記載されている。SIP Server A は URI2 に対応する SIP サーバの名前解決を行い、SIP Server B に転送する。SIP Server B は、URI2 の名前解決を行い、INVITE を UA2 へ転送する。INVITE を受信した UA2 は、200 OK を返答する。200 OK には、UA2 が使用する IP アドレス G2 とポート番号 d2 が記載されており、INVITE と同様の経路を通り UA1 まで転送される。UA1 は ACK を返答した後、交換した IP アドレスとポート番号を用いて、UA2 と直接メディアセッションを確立する。以後の通信は、RTP (Real-time Transport Protocol) などにより、UA1 と UA2 間で直接実行される。

2.2 SIP と NAT の関係

NAT が存在する環境で SIP を使用する場合、以下の 2 つの課題がある。1 つは、通常 NAT 越え問題に関わるもので、NAT の外側から内側方向に向けてシグナリングを開始することができない問題がある。もう 1 つは、SIP の IP ペイロード内に IP アドレス/ポート番号が埋め込ま

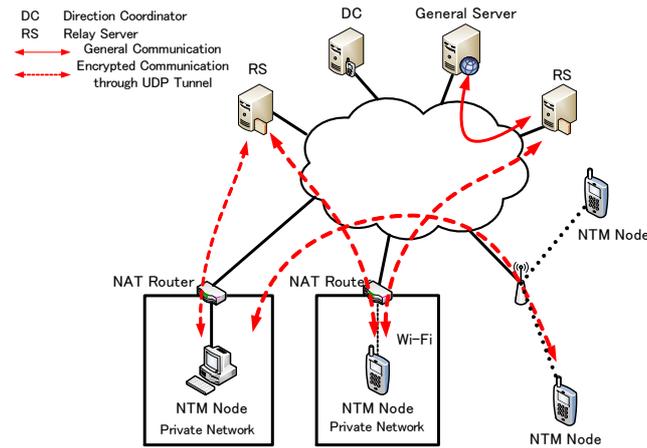


図 3 NTMobile の概要

Fig. 3 Overview of NTMobile.

れるため、NAT を通過すると IP ヘッダ内の IP アドレスとの間で IP アドレスの不整合が生じる問題である。本論文では、この問題をアドレス不整合問題と呼ぶ。

図 2 にアドレス不整合問題の例を示す。図 2 では、UA2 が NAT 配下であり、プライベートアドレスを持っている。プライベートネットワークにある UA2 からグローバルネットワークにある UA1 に通信を開始したとする。SIP メッセージに基づき、UA1 は受信した INVITE に記載されている IP アドレスとポート番号に基づき、セッションを確立しようとする。しかし、記載されている IP アドレスがプライベート IP アドレスであるため、宛先不明でパケットが UA2 に届かず、セッションを確立することはできない。

3. NTMobile

3.1 構成

図 3 に、NTMobile の構成を示す。NTMobile の構成要素として、NTMobile の機能を実装した端末（以下 NTM 端末）の他に、NTM 端末のアドレス情報を管理する DC (Direction Coordinator)、エンドエンドの通信が行えない場合にパケットを中継する RS (Relay Server) が存在する。DC は、NTM 端末に仮想 IP アドレスを配布する他、NTM 端末に対してトンネル経路を指示する装置であり、Dynamic DNS の機能を包含している。NTM 端末は、DC から端末を一意に識別できる仮想 IP アドレスを与えられ、NTM 端末同士の通信の識別に使用する。アプリケーションは、割り当てられた仮想 IP アドレスを自分のアドレスとして認識する。

実際の通信は、仮想 IP アドレスのパケットを実 IP アドレスによる UDP でカプセル化をすることにより実現する。DC はエンド端末が存在するネットワーク上の位置から適切な通信経路を決定し、NTM 端末にトンネル経路を指示する。NAT が存在する場合は、NAT の内側からトンネルを構築するように指示するため、NAT 越え問題を回避す

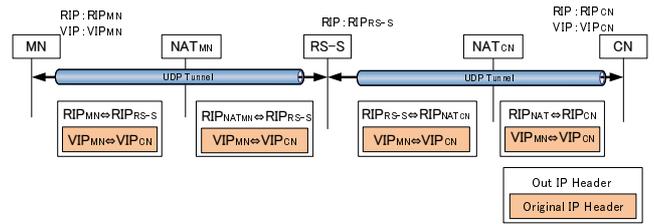


図 4 RS-S を用いた通信の packets 遷移の様子

Fig. 4 Translation state of the packet communication using the RS-S.

ることができる。両エンド端末が異なる NAT 配下に存在するなど、エンドエンド通信が行えない場合には RS を経由したトンネル経路を構築する。この手法によって、アプリケーションに対して、NAT の存在や移動に伴う実 IP アドレスの変化を隠蔽することができる。

DC どうし、DC と RS、DC と NTM 端末間には信頼関係があることを前提としており、NTMobile で使用される制御メッセージは、全て暗号化される。また、NTM 端末間や NTM 端末と RS の間で行われるトンネル通信は、トンネル構築時に DC より配布される共通鍵と NTM 端末が一時的に構築する共通鍵を合成した鍵を用いて暗号化される。

3.2 Relay Server

NTMobile ではエンドエンドの通信ができないと判断された場合に RS を経由したトンネルを構築する。RS は、使用用途によって以下の 3 種類に分類できる。ここでは、場所を移動する NTM 端末を MN (Mobile Node)、通信相手の NTM 端末を CN (Correspondent Node)、一般端末を GN (General Node) と呼ぶ。

3.2.1 RS-S (RS type-S : Switch)

RS-S は、トンネル切換え型の RS である。図 4 に、RS-S を用いた通信における通信パケットの遷移の様子を示す。

MN と CN が異なる NAT 配下に存在する場合、NAT 越え問題によって直接通信を行うことができない。このような場合、DC はエンド端末に対して RS-S との間に UDP トンネルを構築するよう指示する。MN から送信されたパケットは、実 IP アドレスでカプセル化されて RS へ転送される。RS は受信パケットの外側 IP ヘッダのアドレス変換を行って NAT_CN へと転送し、CN はパケットを受信するとデカプセル化を行う。このように、NAT や RS-S により実アドレスが変換されても、上位アプリケーションは仮想 IP アドレスを利用した通信を行うことができる。

また、NTMobile ではエンド端末が RS との間にトンネルを構築した後、MN と CN が互いに制御パケットを投げ合うことにより、エンドエンド通信が可能であればトンネル経路を再構築する自律的経路最適化機能を有している [16]。

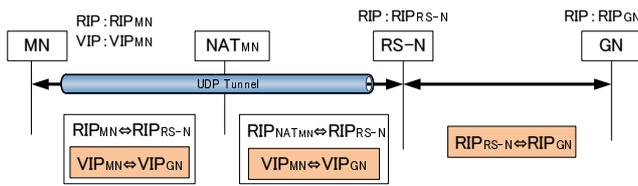


図 5 RS-N を用いた通信の packets 遷移の様子

Fig. 5 Translation state of the packet communication using the RS-N.

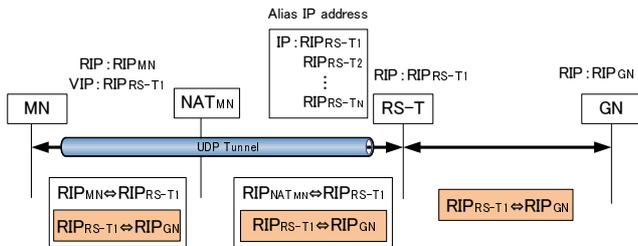


図 6 RS-T を用いた通信の packets 遷移の様子

Fig. 6 Translation state of the packet communication using the RS-T.

3.2.2 RS-N (RS type-N : NAT)

RS-N は、アドレス変換型の RS である。図 5 に RS-N を用いた通信における通信パケットの遷移の様子を示す。RS-N の用途として、インターネット上の一般サーバとの通信などが挙げられる。サーバへの改造をさけるため、RS-N においてカプセル/デカプセル化処理と仮想アドレスのアドレス変換処理を行う。

DC は、MN に対して RS-N との間に UDP トンネルを構築するよう指示する。RS-N が MN からパケットを受信すると、パケットのデカプセル化を行い、仮想 IP アドレスを RS-N と GN の実 IP アドレスへアドレス変換して GN へと転送する。GN は応答する時、通信相手が RS-N であると認識し、RS-N に対して応答を送信する。RS-N はこの応答に対して、仮想 IP アドレスの変換とカプセル化を行い MN に送信する。このように RS-N を中継した通信を行うことにより、NTM 端末が移動しても RS-N が軸となって一般端末への中継を行うため、NTM 端末の移動透過性を実現することができる。

3.2.3 RS-T (RS type-T : Transparent)

RS-T は、アドレス無変換型の RS である [15]。図 6 に、RS-T を用いた通信における通信パケットの遷移の様子を示す。RS-T を利用することにより、SIP のようなメッセージ内に IP アドレスを含むアプリケーションを利用することができる。

RS-T には、予め複数の実 IP アドレスが DC より配布されている。MN には通常の仮想 IP アドレスの他に、RS-T が保持している実 IP アドレスの内の一つが第 2 の仮想 IP アドレスとして割り当てられる。MN の SIP アプリケーションは、自身のアドレスとして上記の第 2 の仮想 IP ア

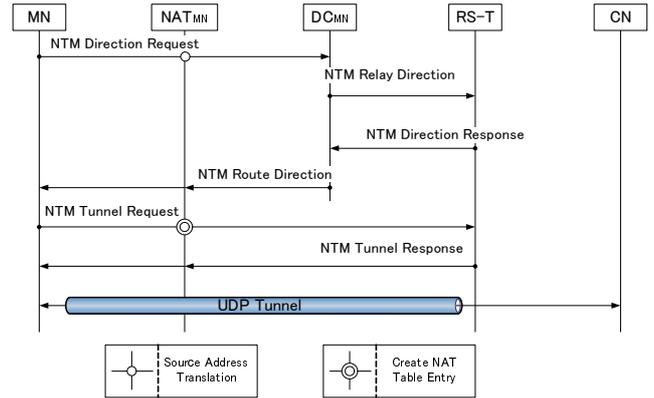


図 7 RS-T を介した通信シーケンス

Fig. 7 Connection procedure via RS-T.

ドレスを使用する。RS-T は MN からパケットを受信すると、パケットのデカプセル化を行い、アドレス変換を行わないまま GN に向けて送信する。GN は通信相手を RS-T と認識し、RS-T に向けてパケットを返す。RS-T は単にカプセル化を行い MN に送信する。このように RS-T を利用することにより、MN のアプリケーションと GN がエンドエンドでセッションを構築するため、メッセージ内にアドレス情報が含まれていても通信が可能である。

3.3 RS-T を利用した動作シーケンス

本節では、RS-T を介した通信の例を示す。

3.3.1 ネットワーク接続時

全ての NTM 端末は、ネットワーク接続時に DC に対してアドレス情報の登録処理を行う。この時、NTM 端末は DC から重複しないことが保証された仮想 IP アドレスを与えられる。RS-T を利用するときは、仮想 IP アドレスとして利用する IP アドレスは、RS-T から割り当てられた実 IP アドレスとなる。

3.3.2 名前解決

通信開始時、MN は DNS によって相手端末の名前解決を行う。MN では DNS への問い合わせパケットをフックし、自身のプライマリ DNS へ NTM Mobile 専用のレコード (以下 NTM レコード) の問い合わせを行う。相手端末が NTM 端末であれば、相手側の DC から NTM レコードを入手できる。NTM レコードが取得できない場合は、相手端末が一般端末であることがわかる。

3.3.3 コネクション確立

図 7 に RS-T を介した経路確立手順を示す。MN は NAT 配下にあるものとする。MN は DC_MN に対して NTM Direction Request を送信し、経路指示を要求する。DC_MN は、NTM Direction Request に記載されている MN と GN のアドレス情報より、MN がプライベートネットワークに存在する NTM 端末、GN が一般端末であると判断し、RS-T を介したトンネル経路を決定する。DC_MN は RS-T

に対して NTM Relay Direction/NTM Direction Response を交換し、中継装置となることを指示する。NTM Relay Direction には、MN の NTM レコードの情報が記載されている。次に、DC_{MN} は MN に NTM Route Direction を送信し、RS-T との間にトンネル経路を構築するように指示する。MN は RS-T との間に NTM Tunnel Request/NTM Tunnel Response を交換してトンネル経路を構築する。

3.3.4 トンネル通信

MN は宛先が仮想 IP アドレスの packets を送信する際、UDP でカプセル化し、RS-T に向けて送信する。通信経路上に NAT が存在しても、外側 IP ヘッダの IP アドレスが変化するのみであり、内側の packets は変更されない。このようにして MN と GN 間のアプリケーションの間でエンドエンドのセッションを確立するため、SIP 通信を実現できる。

3.3.5 RS-T を介した通信の課題

RS-T では、MN1 台に対して 1 個のグローバルアドレスを割り当てる必要がある。これは、RS-T が GN から受信した packets をどの MN に送信するのかを識別する必要があるためである。また、IPv4 アドレス枯渇の中で、RS-T に複数のグローバルアドレスを割り当てることは望ましくない。

4. 提案方式

本章では、RS-T から NTM 端末に対し重複しないポート番号の割り当てを行うよう拡張することにより、RS-T のグローバルアドレスを 1 個だけで管理できる手法を提案する。

4.1 提案方式の構成

本提案のネットワーク構成として、DC と拡張した RS-T をそれぞれグローバルネットワークに設置する。RS-T は 1 個のグローバル IP アドレスを所持する。NTM 端末はプライベートネットワークに存在し、一般の SIP 端末はグローバルネットワークに存在するものとする。グローバルネットワーク上には SIP 端末を管理する一般の SIP サーバが設置されている。一般の SIP サーバと SIP 端末には一切の改良を加えない。

4.2 通信シーケンス

4.2.1 端末情報の登録処理

図 8 に端末起動時の登録処理シーケンスを示す。DC_{MN} には、MN の NTM レコードがすでに登録され、MN には仮想アドレスが配布されているものとする。

SIP の登録処理メッセージである REGISTER をトリガーとして、MN と RS-T の間にトンネルを構築する。トンネル構築手順については、通常の NTM Mobile における一般端末との通信確立手順と同様であるが、トンネル構築

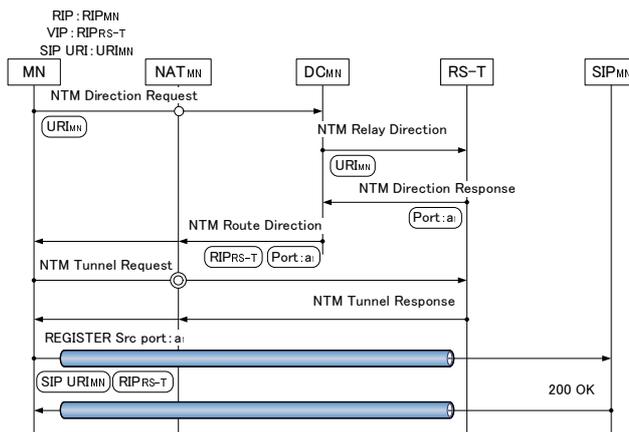


図 8 NTM 端末の SIP 登録処理シーケンス

Fig. 8 Sequence of SIP registration process of NTM node

のためにやりとりするメッセージに情報を新しく記載する。MN が DC_{MN} に送信する NTM Direction Request には、自身の SIP URI を記載する。DC_{MN} は RS-T に対する NTM Relay Direction の中に、MN の SIP URI の情報を記載する。RS-T は受信したメッセージに含まれている SIP URI を自身のテーブルに登録し、SIP 通信に必要なポート番号を 1 つ記載した NTM Direction Response を DC_{MN} に返信する。RS-T に届く SIP メッセージの中に含まれている SIP URI から、登録されている SIP URI を検索し送信端末を判断する。RS-T から割り当てられたポート番号は、以後の SIP 通信のポート番号として使用される。DC_{MN} は MN に対し、RS-T の実 IP アドレスと上記ポート番号が記載された NTM Route Direction を送信する。MN は受信したメッセージに含まれている RS-T の実 IP アドレスを自身の仮想 IP アドレスとして使用する。この処理の後、MN は RS-T とトンネル構築を行う。

RS-T とのトンネル構築が完了した後は、一般の SIP サーバ SIP_{MN} に通常の SIP 登録処理が行われる。この時、SIP_{MN} に登録される MN の IP アドレスは、RS-T の実 IP アドレスである。

登録処理が完了した後、MN は DC_{MN} と RS-T の両者に対して定期的に Keep Alive を実行することにより、制御メッセージ用の通信経路を確保する。

4.2.2 NTM 端末からのセッション確立

図 9 に MN から一般の SIP 端末 GN に対して通信を開始するシーケンスを示す。MN は SIP_{MN} への登録処理を完了しており、GN も SIP_{GN} に対して登録処理が完了しているものとする。

MN は、SIP アプリケーションからセッション確立のために最初に送信される INVITE をトリガーとして、RS-T に NTM SIP Port Request を送信し、ポート番号の割り当て要求を行う。RS-T は NTM SIP Port Request を受信すると、RS-T 内で使用していないポート番号の一つを決定し、

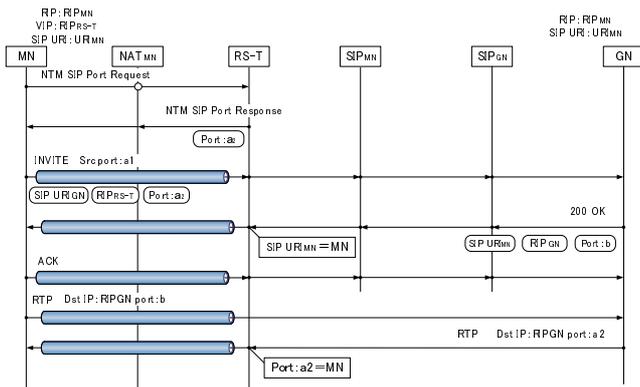


図 9 MN から通信を開始した場合の動作シーケンス

Fig. 9 Operation sequence in the case where communication started from MN

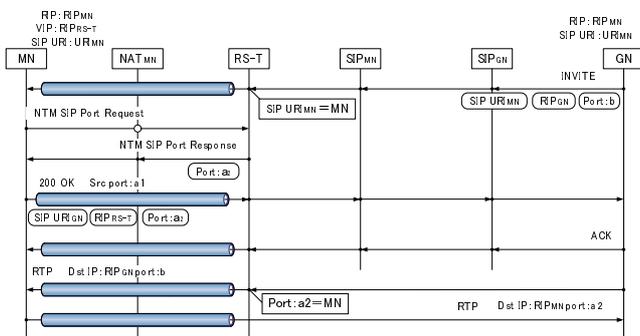


図 10 GN から通信を開始した場合の通信シーケンス

Fig. 10 Operation sequence in the case where communication started from GN

NTM SIP Port Response に記載して返信する。RS-T は、このポート番号と NTM 端末の対応付けを記憶しておく。RS-T から割り当てられるポート番号の範囲は、MN では使用しないよう、カーネルの使用範囲を限定しておく。MN は、INVITE の SDP (Session Description Protocol) に含まれているメディアセッションで使用するポート番号情報を RS-T から割り当てられたポート番号 a_2 に書き換える。書き換えを終えると、RS-T を経由して SIP_{MN} に INVITE を送信する。以降は、通常の SIP におけるセッション確立と同様で、 SIP_{MN} は SIP_{GN} を経由し GN に INVITE を転送する。GN は INVITE に対する応答として 200 OK を逆経路で MN に返す。MN は ACK を GN に送信することでセッションを確立する。以降に続く MN と GN 間のメディアセッションでは、必ず RS-T を経由した通信経路となる。

4.2.3 一般 SIP 端末からのセッション確立

図 10 に GN から NTM 端末である MN に対して通信を開始するシーケンスを示す。MN と GN はそれぞれ自身が使用する SIP サーバに対して登録処理が完了しているものとする。

GN は MN とのセッションを確立するため、自身を管理する SIP_{GN} に MN 宛ての INVITE を送信する。 SIP_{GN} は

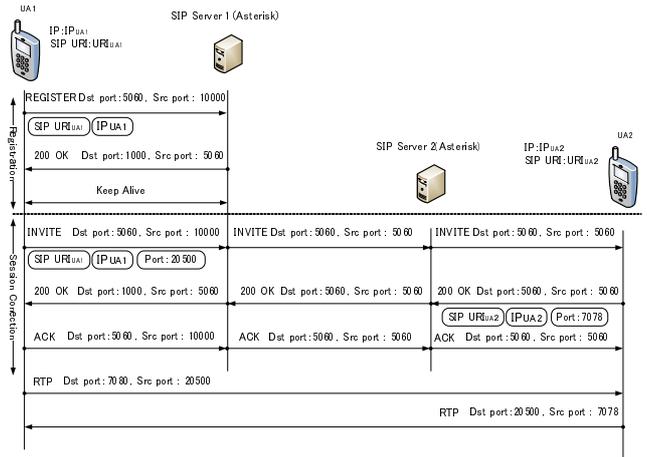


図 11 動作検証の通信シーケンス

Fig. 11 Communication sequence operation verification

INVITE に含まれている SIP URI を元に MN を管理する SIP_{MN} を発見し転送を行う。 SIP_{MN} に登録されている MN の IP アドレスは RS-T の実 IP アドレスであるため、GN からの INVITE は RS-T に転送される。INVITE を受信した RS-T は、SIP URI からどの NTM 端末宛てなのかを自身に登録されている SIP URI より検索し、MN に INVITE を送信する。

MN は受信した INVITE をトリガーとして RS-T との間で NTM SIP Port Request/Response のやり取りを行い、RS-T から使われていないポート番号の割り当てを受ける。MN は 200 OK の SDP に含まれるポート番号を上記で割り当てられたポート番号に書き換えて送信する。次に通常の SIP によるセッション確立と同様に ACK を受信後、メディアセッションを開始する。

5. 動作検証

提案方式では、SIP プロトコルのメッセージ内容を変更するだけであるため、プロトコル自体の修正は必要としない。しかし、実アプリケーションの実装が提案方式の処理に対応可能なか確認する必要がある。そこで、一般に利用されている SIP クライアントアプリケーションと、SIP サーバアプリケーションを用いて、提案方式の動作の検証を行った。

5.1 動作環境

動作検証のためのネットワーク構成として、SIP クライアント UA1 と UA2 は Linux で動作する Linphone[17] を用いた。SIP Server 1 と SIP Server 2 は、一般に使用されているフリーソフトの Asterisk[18] を選択した。UA1 と UA2, SIP Server 1 と SIP Server 2 はすべて同じネットワーク上に存在しているものとする。

5.2 動作検証

図 11 に動作検証の通信シーケンスを示す。SIP 通信では、メッセージ交換のポート番号は標準で 5060 を使用することになっている。提案方式では、SIP 登録処理時に RS-T からポート番号の割り当てを行う点が異なる。ここでは、RS-T から SIP 通信用に適切なポート番号が割り当てられたものと仮定し、UA1 が SIP 通信で使用するポート番号を 10000 とした。UA1 は、割り当てられたポート番号を送信元ポート番号として、SIP Server 1 に REGISTER を送信する。SIP Server 1 は UA1 からのパケットを受信したあと、登録処理が完了した事を 200 OK にて応答する。検証の結果、200 OK の宛先ポート番号は 10000 が使用されていたため、正しく登録処理が完了したと判断できる。登録処理後は、UA1 と SIP Server 1 の間で Keep Alive を行っていることを確認した。これにより、SIP で使用するポート番号を任意のポート番号に変更しても通信が可能であることを確認した。

次に、UA1 が UA2 に対してセッションを確立する。提案方式において、INVITE を送信する前に RS-T からメディアセッションで使用するポート番号の割り当てを行う。ここで、RS-T から SIP 通信用に適切なポート番号が割り当てられたものと仮定し、UA1 がメディアセッションで使用するポート番号を 20500 とした。このポート番号を INVITE に含み、UA1 から SIP Server 1 に INVITE を送信した。検証の結果、UA1 と SIP Server 1 の SIP 通信で用いるポート番号は、SIP 登録処理で使用したポート番号と同じになった。UA1 と UA2 は、通常の SIP シグナリングと同様にメディアセッションに必要な情報を交換することで、メディアセッションを開始する。UA1 と UA2 の間のメディアセッションにおいて、UA2 が UA1 に送信するパケットの宛先ポート番号が、RS-T から割り当てられたポート番号の 20500 であることを確認した。これにより、メディアセッションで用いるポート番号においても任意のポート番号で通信が行われることが確認できた。

これらの検証から、任意のポート番号をそれぞれ SIP 通信とメディアセッションのポート番号として割り当てを行う提案方式が、実際の環境において適用が可能であることが確認できた。

6. まとめ

本論文では、NTMobile の NAT 越え機能とポート番号の割り当てを行うよう拡張した RS-T を用いることによって、一般 SIP 端末との間で NAT を跨る SIP 通信を実現する手法を提案した。動作検証により、ポート番号の割り当てが可能であることを確認した。今後は、実装と動作検証を進める予定である。

参考文献

- [1] Rosenberg, J., Schulzrinne, G., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and Schooler, E.: SIP: Session Initiation Protocol, RFC 3261, IETF (2002).
- [2] Rosenberg, J., Mahy, R., Matthews, P., and Wing, D.: Session Traversal Utilities for NAT (STUN), RFC 5389, IETF (2008).
- [3] Mahy, R., Matthews, P., and Rosenberg, J.: Traversal Using Relays around NAT (TURN), RFC 5766, IETF (2010).
- [4] Forum, U.: Internet Gateway Device (IGD) Standardized Device Control Protocol V 1.0 (2001).
- [5] Turanyi, Z., Valko, A. and Campbell, A.: 4+4: An Architecture for Evolving the Internet Address Space Back Toward Transparency, *ACM SIGCOMM Computer Communication Review*, Vol.33, No.5, pp.43-54 (2003).
- [6] 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).
- [7] Levkowitz, H., and Vaarala, S.: Mobile IP Traversal of Network Address Translation (NAT) Devices, RFC 3519, IETF (2003).
- [8] 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).
- [9] 宮崎 悠, 鈴木秀和, 渡邊 晃: 端末の改造が不要な NAT 越え通信システム NTSS の提案と評価, *情報処理学会論文誌*, Vol.51, pp.1234-1241 (2010).
- [10] Johnston, A., Donovan, S., Sparks, R., Cunningham, C., and Summers, K.: Session Initiation Protocol (SIP) Basic Call Flow Examples, RFC 3665, IETF (2003).
- [11] 鈴木秀和, 水谷智大, 西尾拓也, 内藤克浩, 渡辺 晃: NTMobile における相互接続性の確立手法と実装, マルチメディア, 分散, 協調とモバイル (DICOMO2011) シンポジウム論文集, Vol.2011, No.1, pp.1339-1348 (2011).
- [12] 内藤克浩, 西尾拓也, 水谷智大, 鈴木秀和, 渡辺 晃, 森香津夫, 小林英雄: NTMobile における移動透過性の実現と実装, DICOMO2011 論文集, Vol.2011, No.1, pp.1349-1359 (2011).
- [13] 西尾拓也, 内藤克浩, 水谷智大, 鈴木秀和, 渡辺 晃, 森香津夫, 小林英雄: NTMobile における端末アドレスの移動管理と実装, マルチメディア, 分散, 協調とモバイル (DICOMO2011) シンポジウム論文集, Vol.2011, No.1, pp.1139-1145 (2011).
- [14] 上野尾一真, 鈴木秀和, 内藤克浩, 渡辺 晃: IPv6 ネットワークにおける NTMobile の検討, *情報処理学会研究報告*, Vol.2011-MBL-59, No.9, pp.1-7 (2011).
- [15] 土井敏樹, 鈴木秀和, 内藤克浩, 渡辺 晃: NTMobile におけるアドレス無変換型 RS の検討, *情報処理学会第 74 回全国大会論文集* pp.3-225-3-226 (2011).
- [16] 納堂博史, 鈴木秀和, 内藤克浩, 渡辺 晃: NTMobile の経路最適化の検討, *情報処理学会研究報告*, Vol.2011-MBL-61, No.33, pp.1-8 (2011).
- [17] linphone, open-source voip software — Linphone, an open-source video sip phone. <http://www.linphone.org/>.
- [18] Asterisk IP PBX, VOIP Gateway, IVR & Open Source Communications. <http://www.asterisk.org>

NTMobileにおける 一般SIP端末との通信実現手法

[†]名城大学大学院理工学研究科 [‡]三重大学大学院工学研究科
吉岡正裕[†], 鈴木秀和[†], 内藤克浩[‡], 旭健作[†], 渡邊晃[†]

研究背景

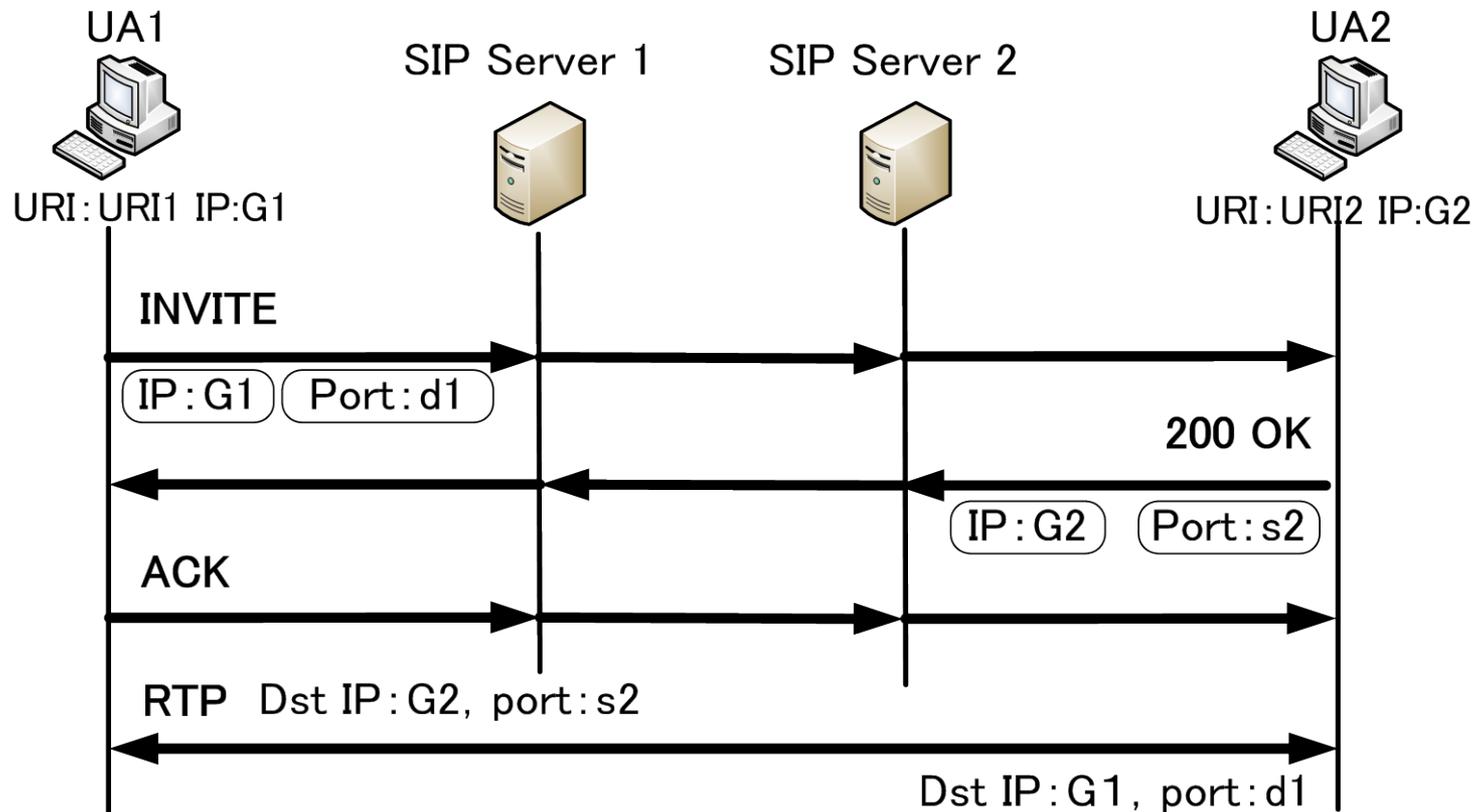
- IPv4のアドレス枯渇
 - インターネットの発展に伴い、IPv4グローバルアドレスが不足
 - 組織や家庭のネットワークはプライベートアドレスが一般的
 - NATを介した通信が必須
- SIP (Session Initiation Protocol) の普及
 - IP電話のシグナリング処理として使用されている
 - SIP単体ではNATを通過することができない

NAT: Network Address Transration

*: 本稿ではNAPTまたはIPマスカレードを含めてNATと呼ぶ

SIPの概要

- SIP (Session Initiation Protocol)
 - 通信の開始, 通信の切断を行うために使用するプロトコル
 - SIPメッセージで, メディアセッションで使用する情報を交換

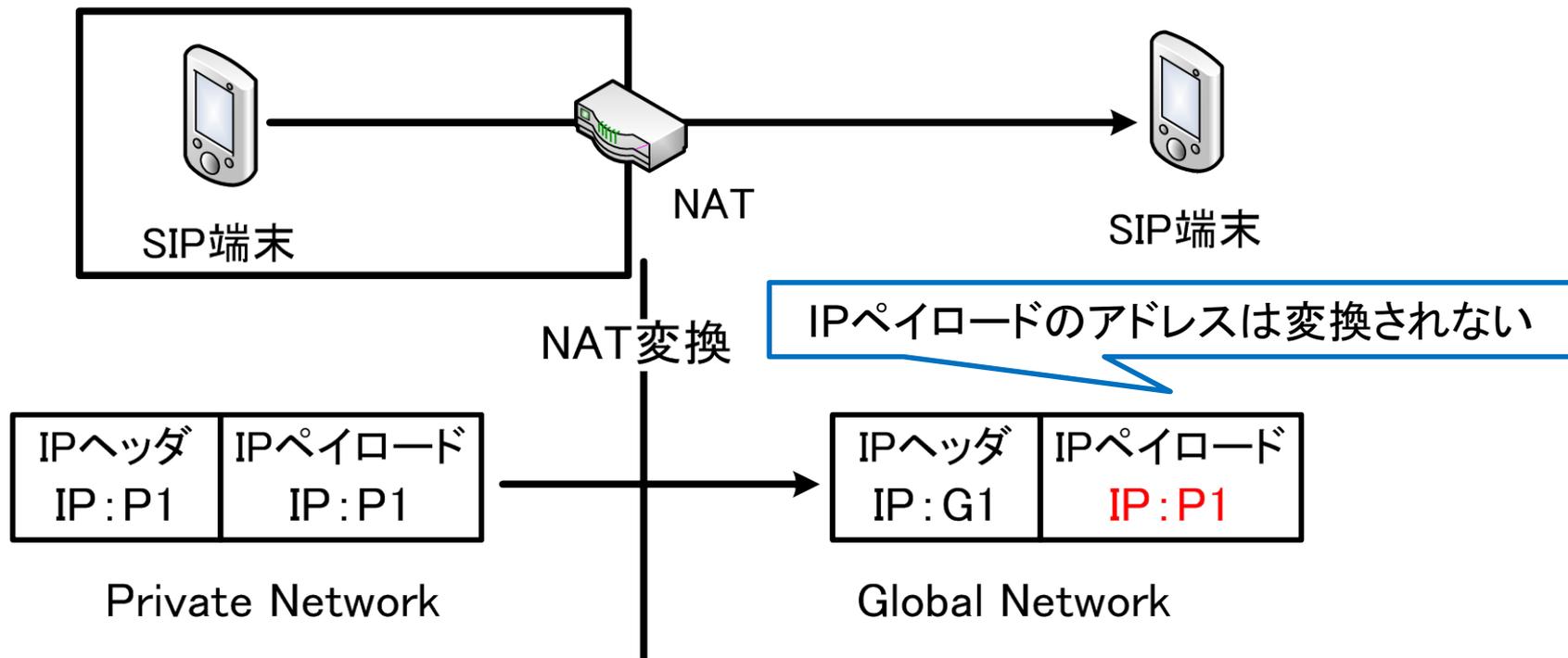


UA: User Agent

RTP: Real-time Transport Protocol リアルタイム・データ転送プロトコル

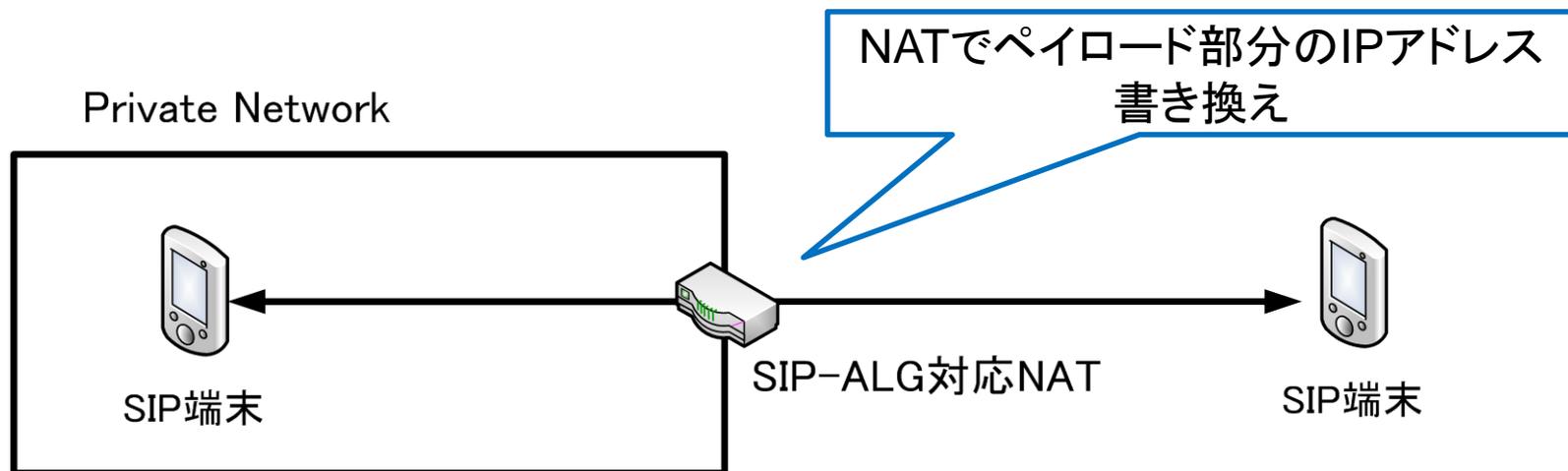
SIPとNAT

- NAT越え問題
 - NAT外部から内側に向けて通信を開始できない
- アドレス不整合問題
 - NATでは, IPペイロード部分のアドレス変換を行わない
 - SIPメッセージがNATを通過するとアドレスの不整合が生じる



SIP-ALG

- SIP-ALG (SIP-Application level Gateway)
 - NAT機能を拡張し、ペイロード内のIPアドレスをNAT外側のIPアドレスに書き換える
- 利点
 - SIP端末に改造を加える必要がない
- 欠点
 - パケットの中身まで検査するため、NATに負荷がかかる
 - SIPメッセージが暗号化されている場合には対応できない

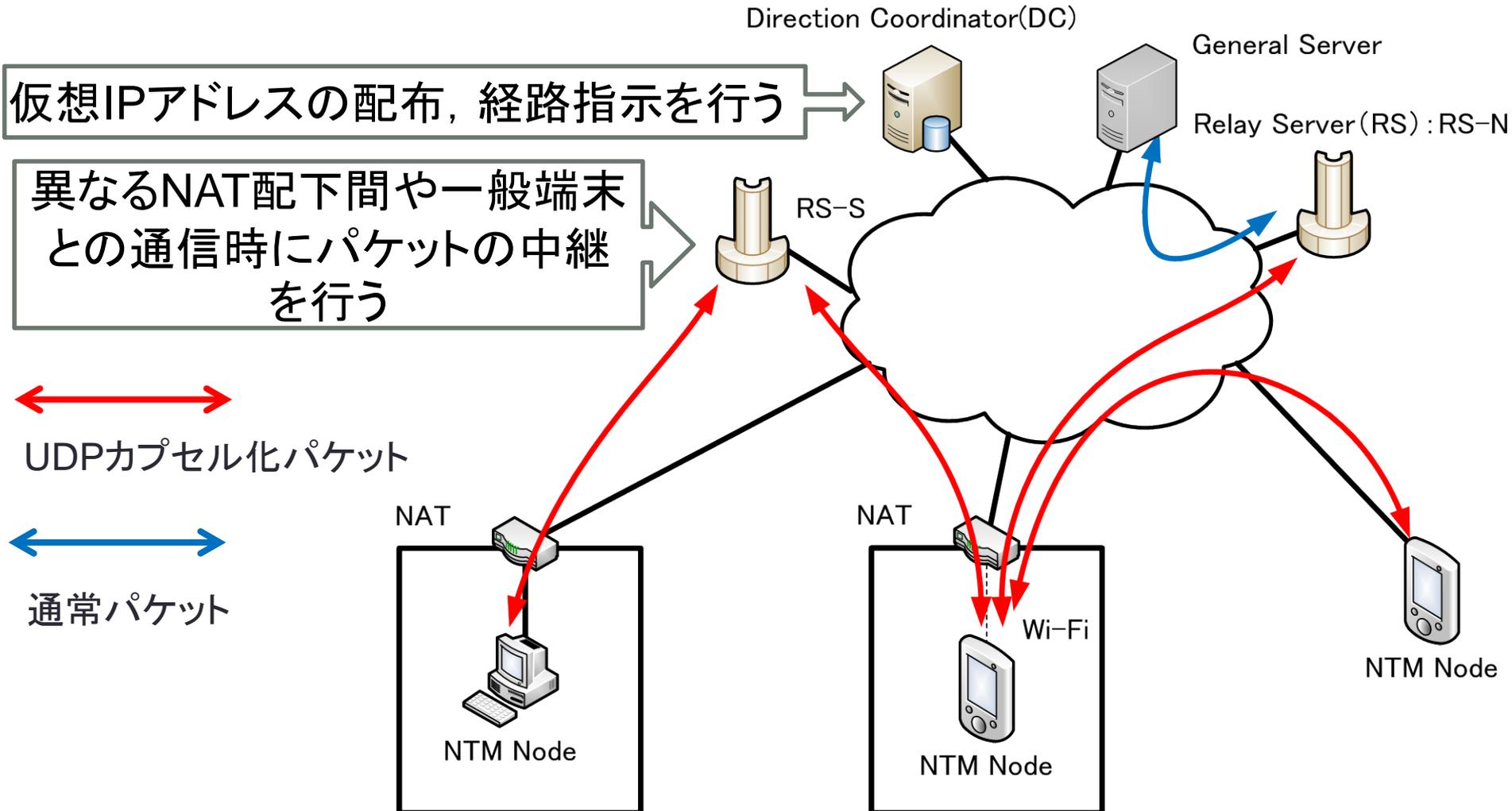


NTMobile

- NTMobile(Network Traversal with Mobility)
 - 端末を一意に識別する仮想アドレスを導入
 - 全てのパケットを実IPアドレスでカプセル化
 - 実IPアドレスの変化を隠蔽
 - NATに改造を加えずに実現が可能

NAT越えと移動透過性を同時に実現することができる

NTMobileの概要

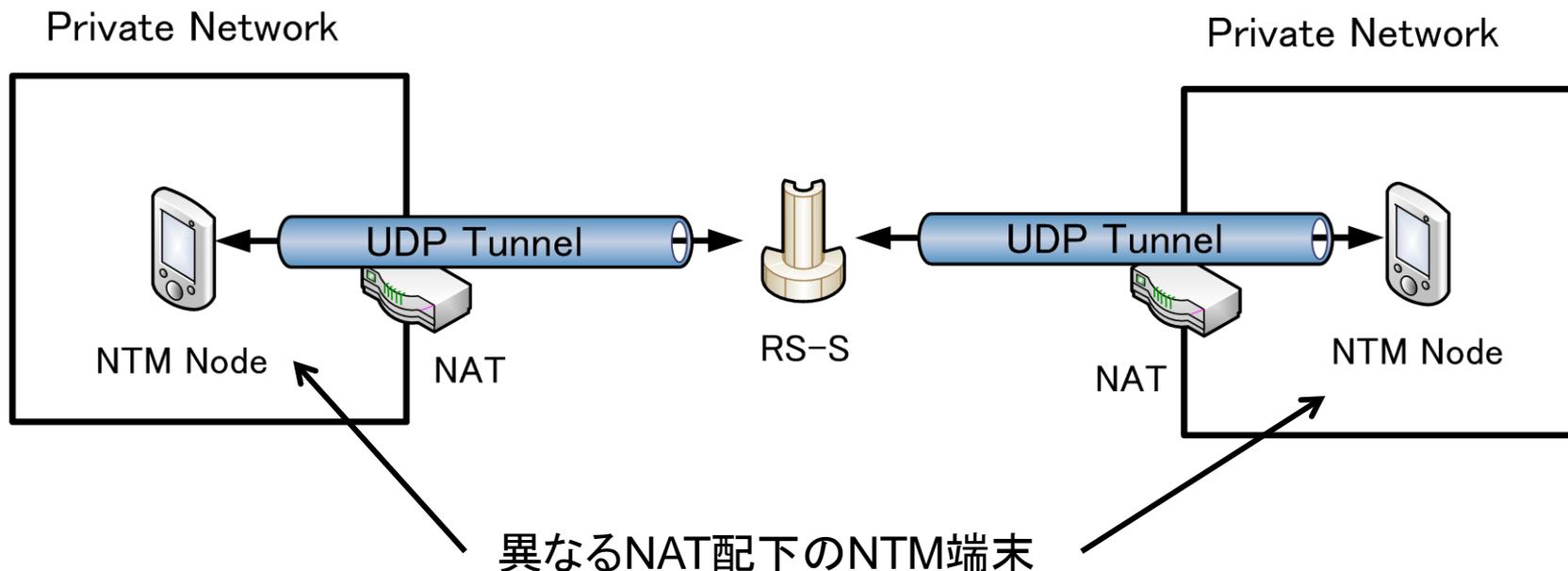


Relay Server

- 特定の条件においてパケットの中継を行うサーバ
- RS-S: Relay Server type Switch
 - トンネル切り替え型
 - 異なるNAT配下のNTM端末間のパケットの中継
- RS-N: Relay Server type NAT
 - アドレス変換型
 - 一般サーバとNTM端末間のパケットの中継
- RS-T: Relay Server type Transparent
 - アドレス無変換型
 - IPアドレスを含むアプリケーションを使用する場合にパケットの中継

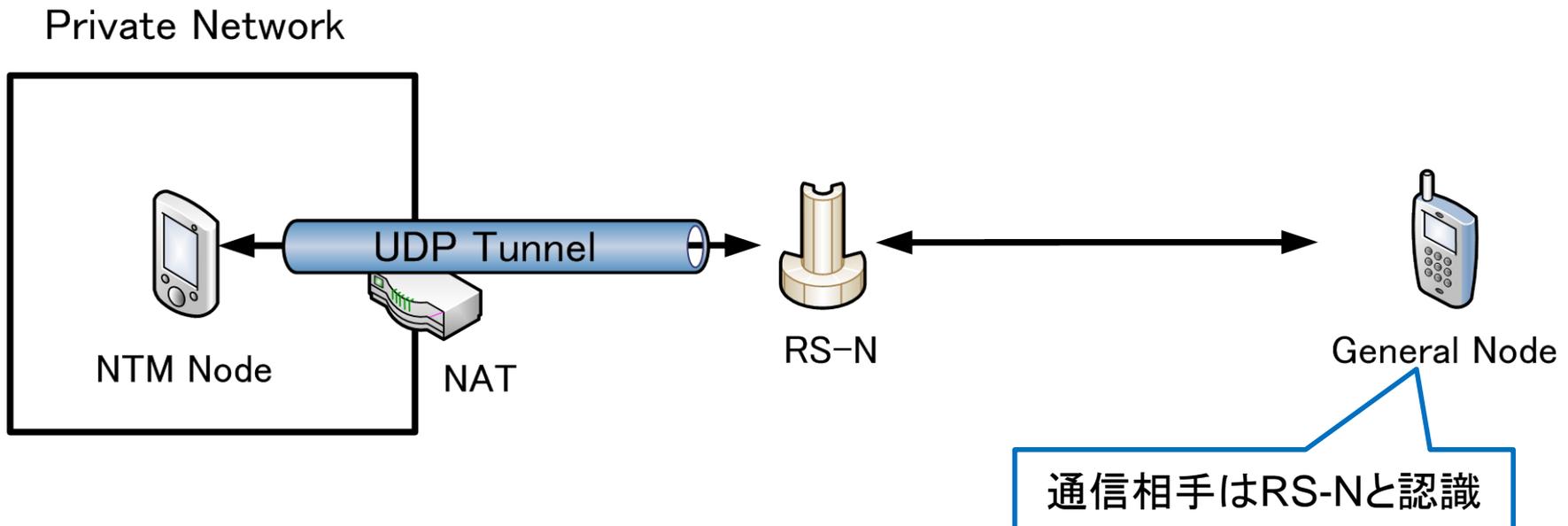
RSの種類(1/3)

- RS-S (RS type Switch)
 - トンネル切り替え型RS
 - NTM端末が異なるNAT配下に存在する場合に使用
 - 双方のNTM端末との間にUDPトンネルを構築
 - 直接通信が出来る場合は, NTM端末の判断で自律的に経路切り替え



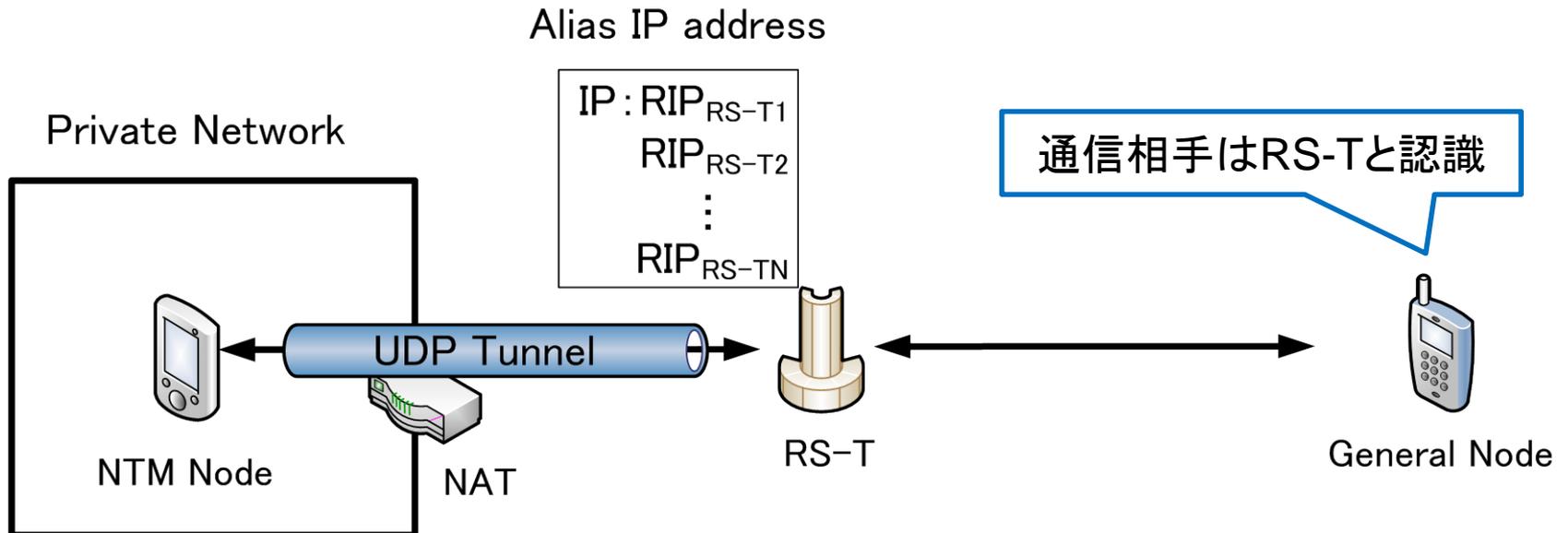
RSの種類(2/3)

- RS-N(RS type NAT)
 - アドレス変換(NAT)型RS
 - 通信相手端末がインターネット上の一般サーバの場合に使用
 - NTM端末との間にUDPトンネルを構築
 - RS-Nは仮想IPアドレスと実アドレスの変換
 - 一般端末はRS-Nを通信相手と認識

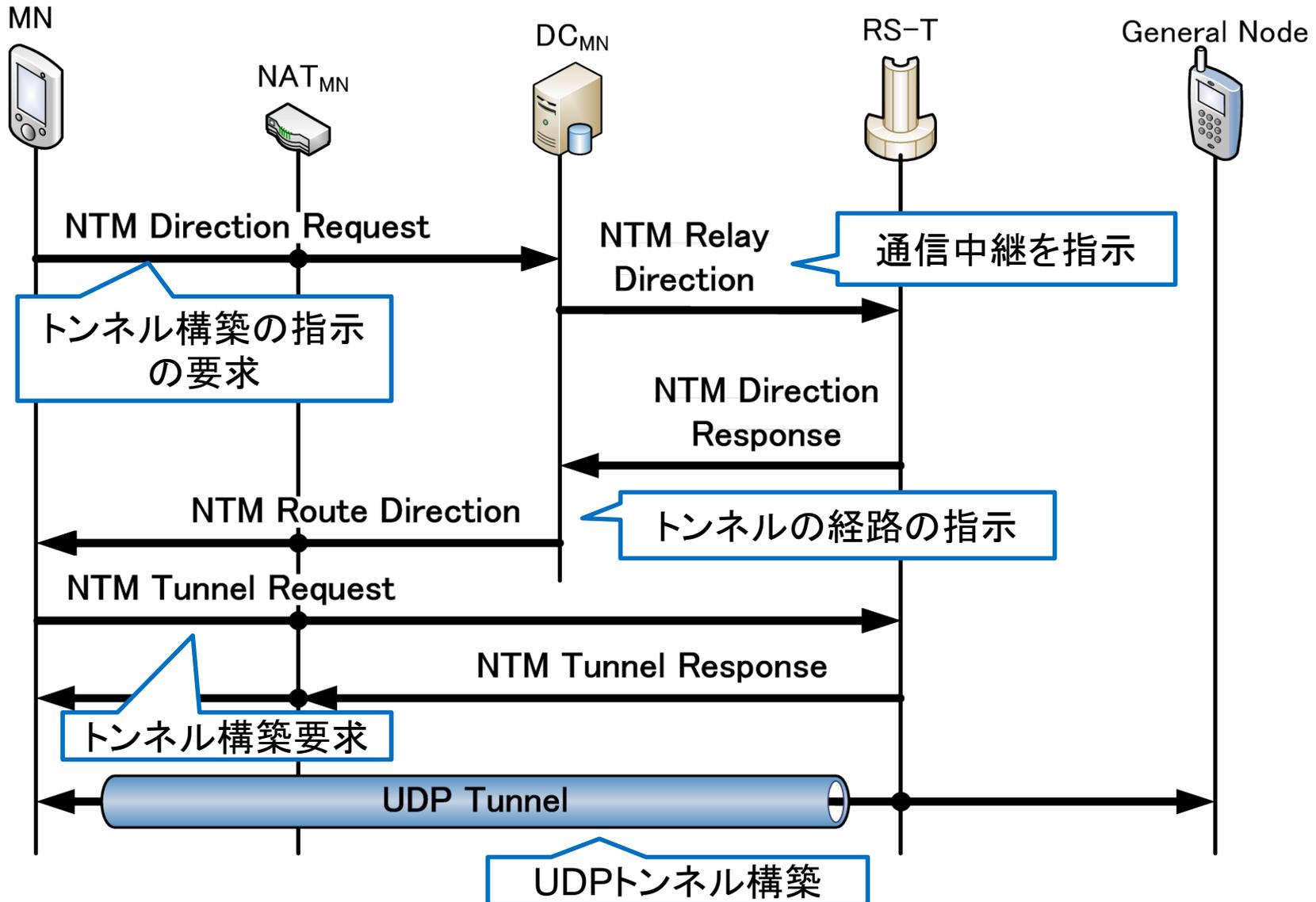


RSの種類(3/3)

- RS-T (RS type Transparent)
 - アドレス無変換型RS
 - ペイロードにIPアドレスを含むアプリケーションを用いる場合に使用
 - RS-Tが持つ実IPアドレス群の1個をNTM端末に割り当てる
 - NTM端末はこれを仮想アドレスとして使用

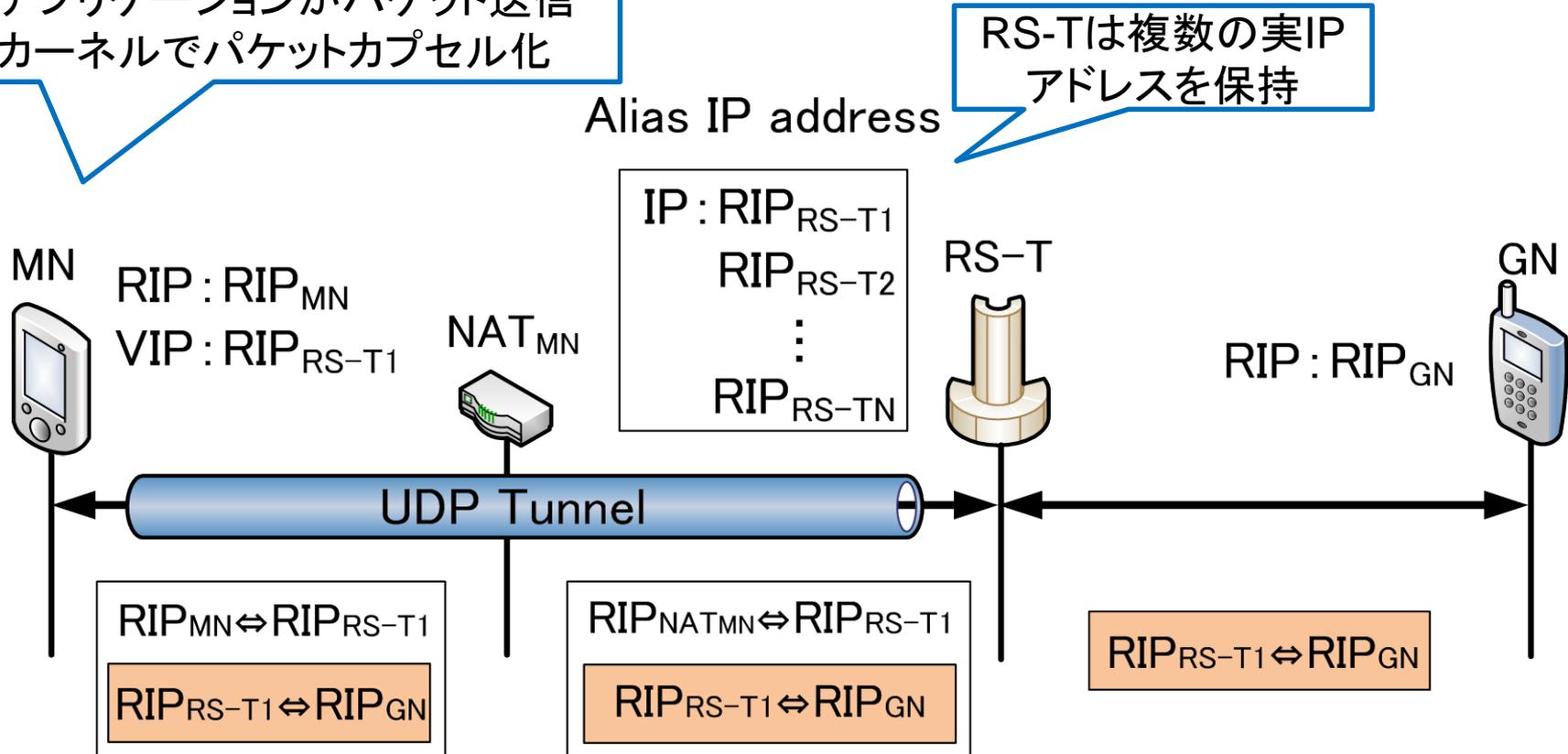


RS-Tを用いた通信シーケンス



RS-Tを用いたトンネル構築シーケンス(1/4)

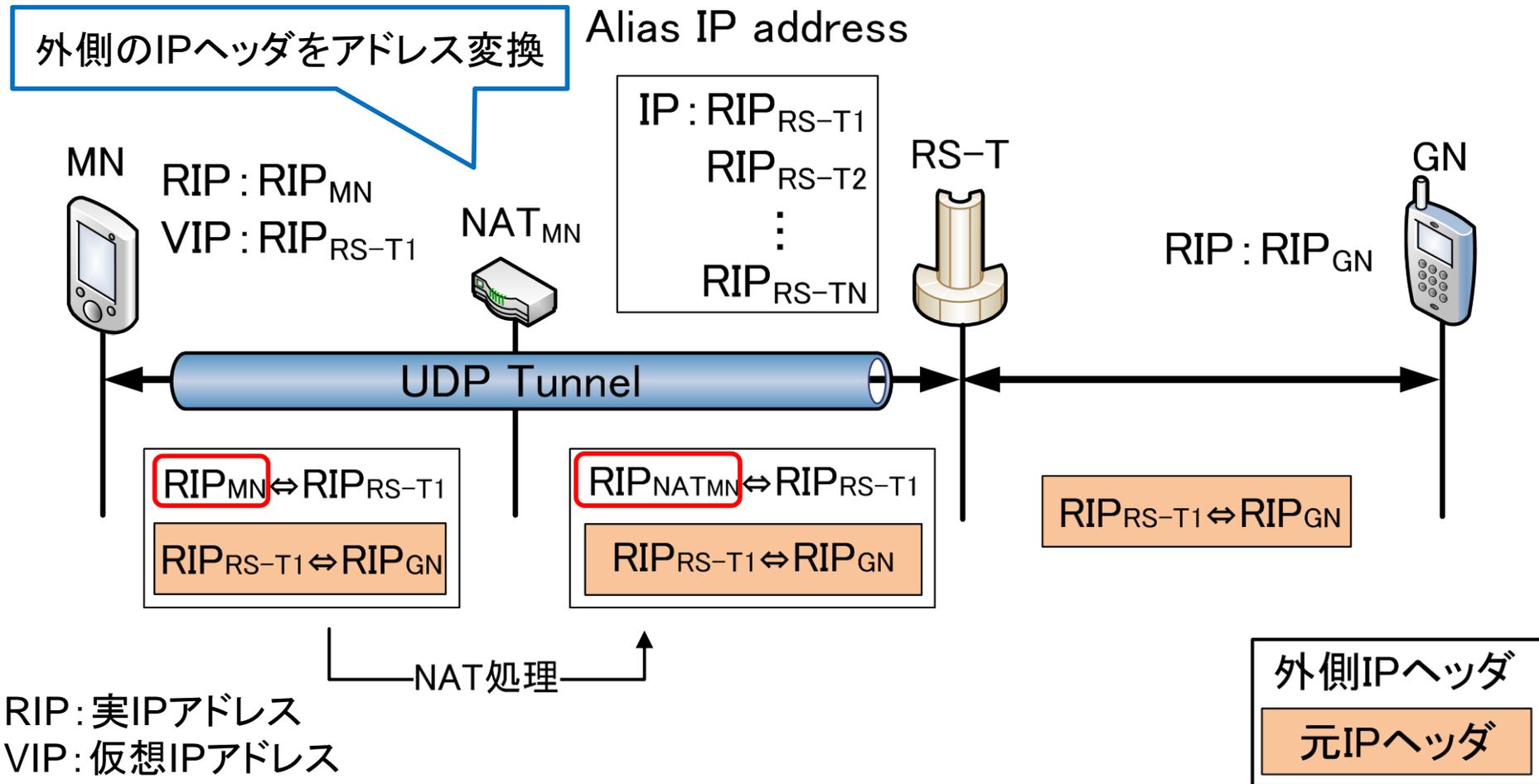
- アプリケーションがパケット送信
- カーネルでパケットカプセル化



RIP: 実IPアドレス
VIP: 仮想IPアドレス

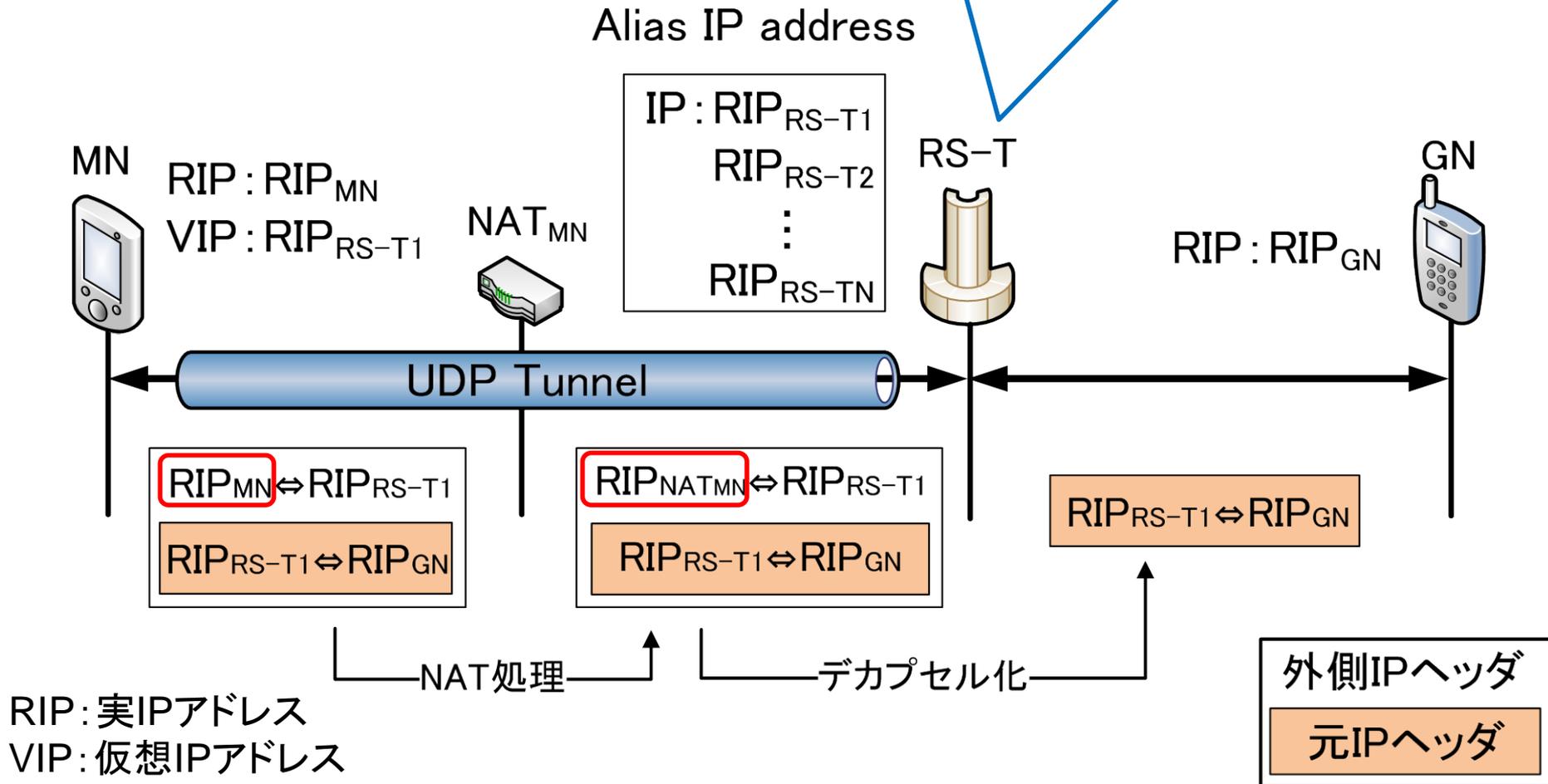
外側IPヘッダ
元IPヘッダ

RS-Tを用いたトンネル構築シーケンス(2/4)



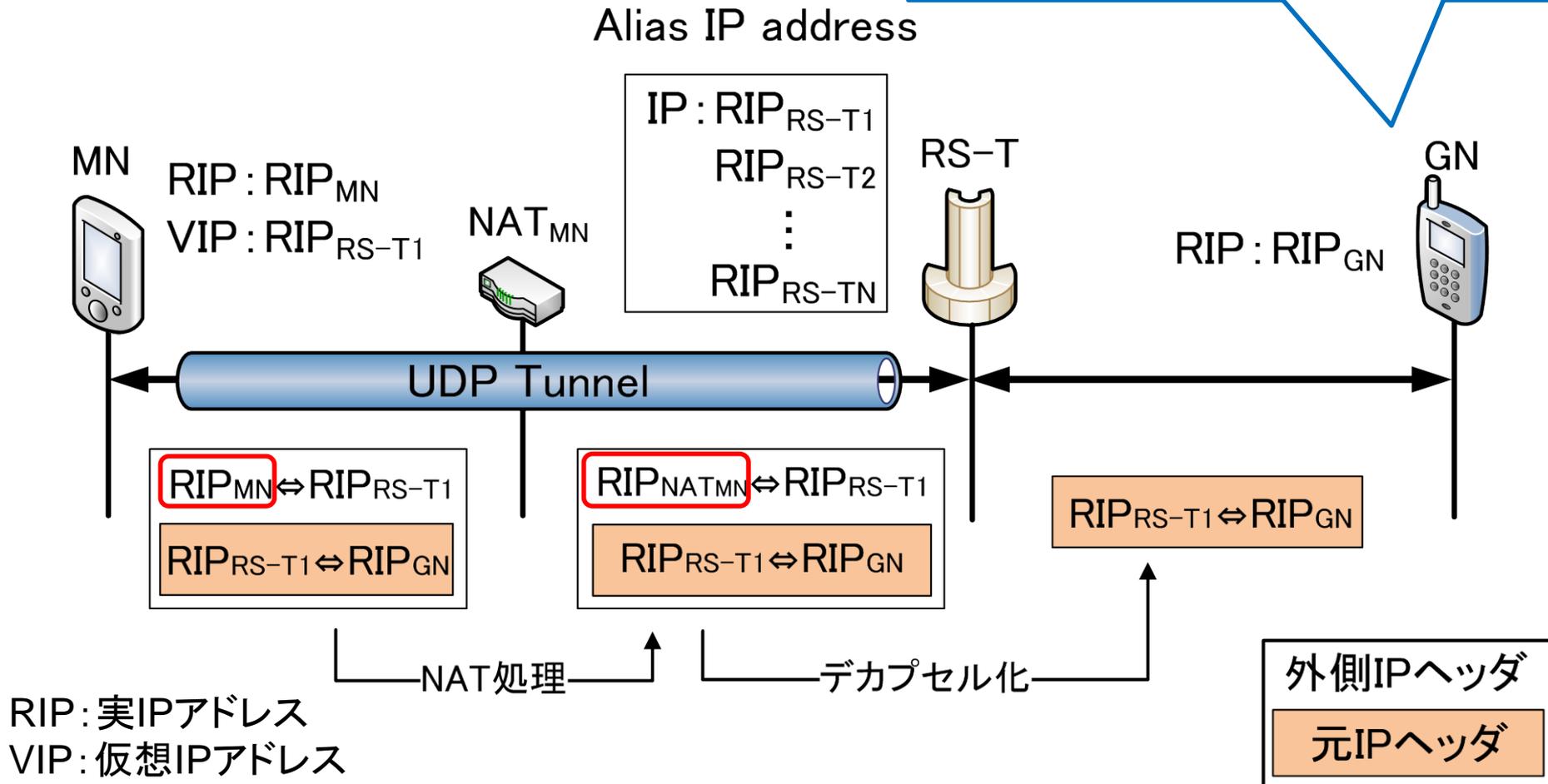
RS-Tを用いたトンネル構築シーケンス(3/4)

- 受信したパケットをデカプセル化
- アドレス変換は行わない



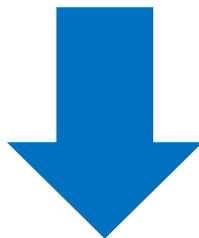
RS-Tを用いたトンネル構築シーケンス(4/4)

- RS-Tからパケットを受信
- 通信相手はRS-Tと認識する



RS-Tを介したSIP通信の課題

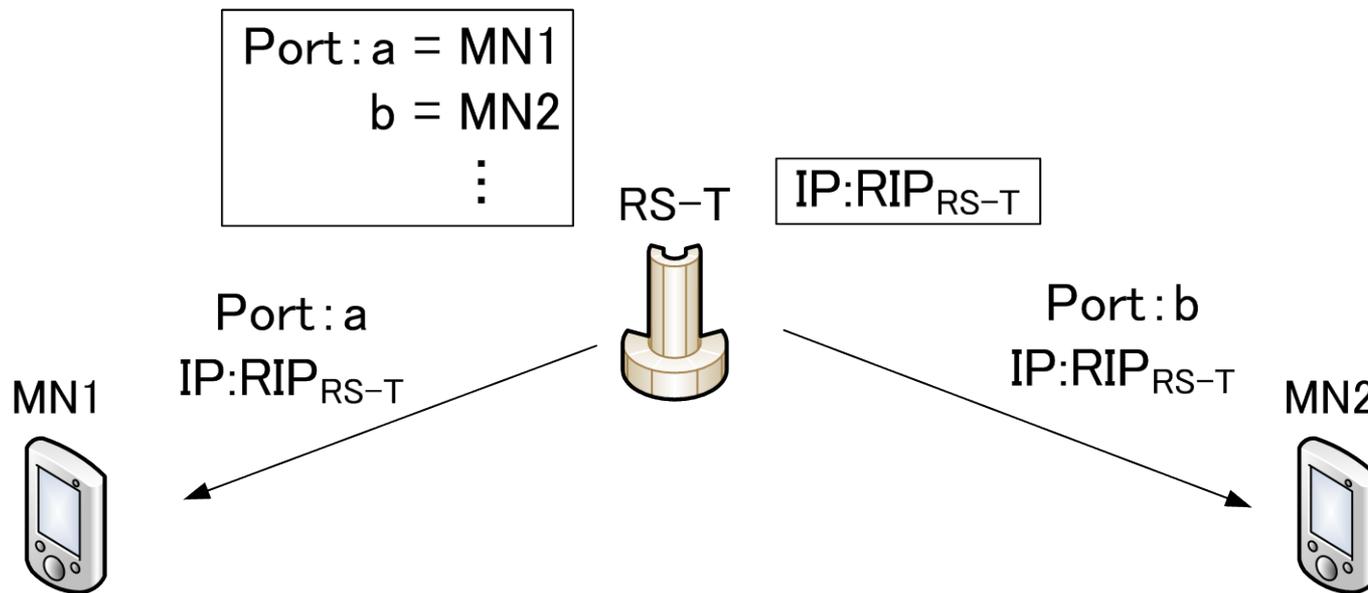
- NTM端末1台に対して、1個のグローバルIPアドレスを割り当てを行う
- IPアドレスによりNAT配下のNTM端末を識別



グローバルIPアドレスの枯渇問題に逆行する

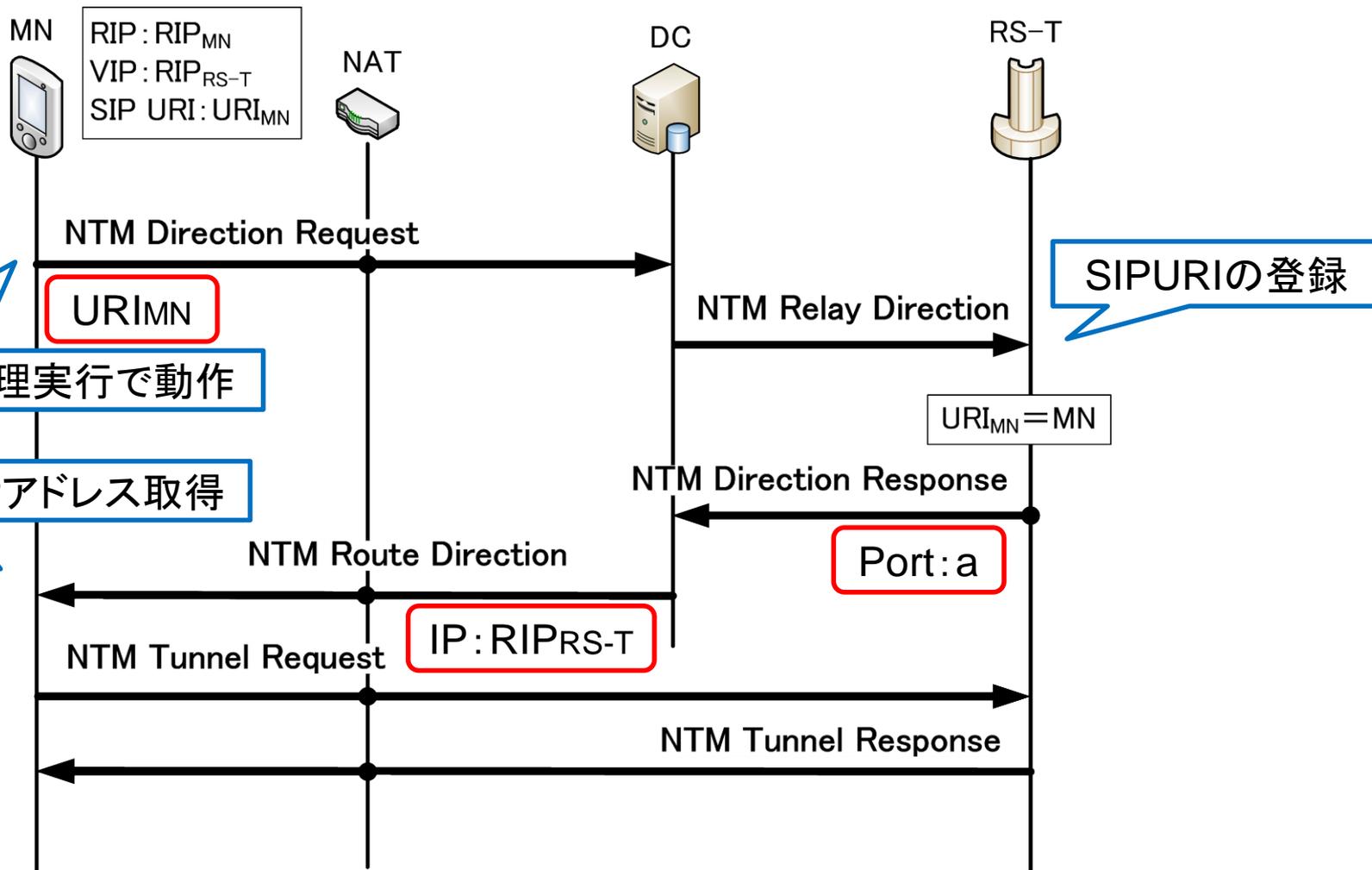
提案方式

- ポート番号を利用し, NAT配下のNTM端末を識別
- RS-TからSIP通信開始時に, NTM端末に重複しないポート番号の割り当てる
- グローバルアドレスを1個だけでNTM端末を管理



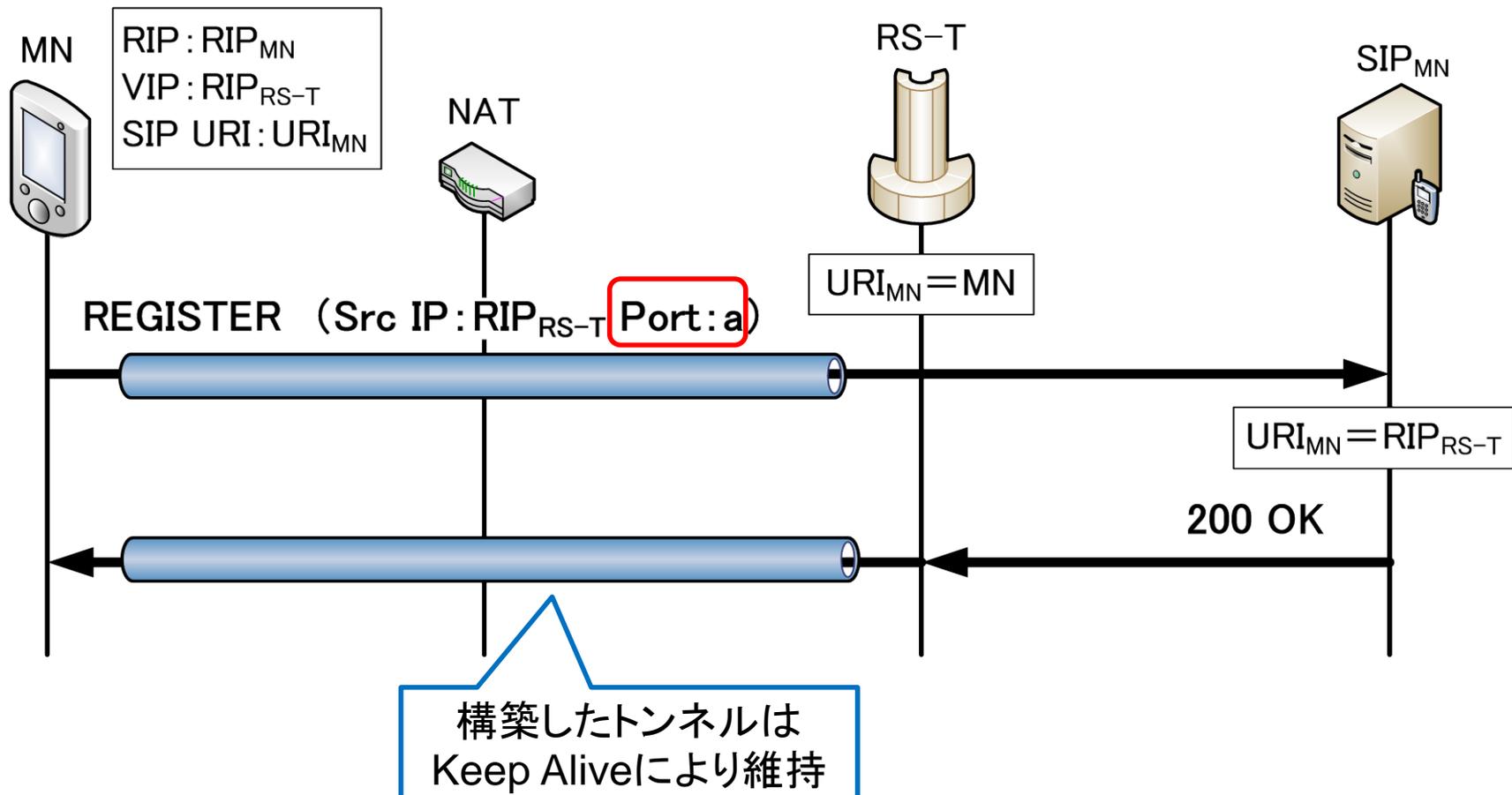
事前処理

- RS-Tとトンネルを構築し, RS-Tから必要な情報を取得



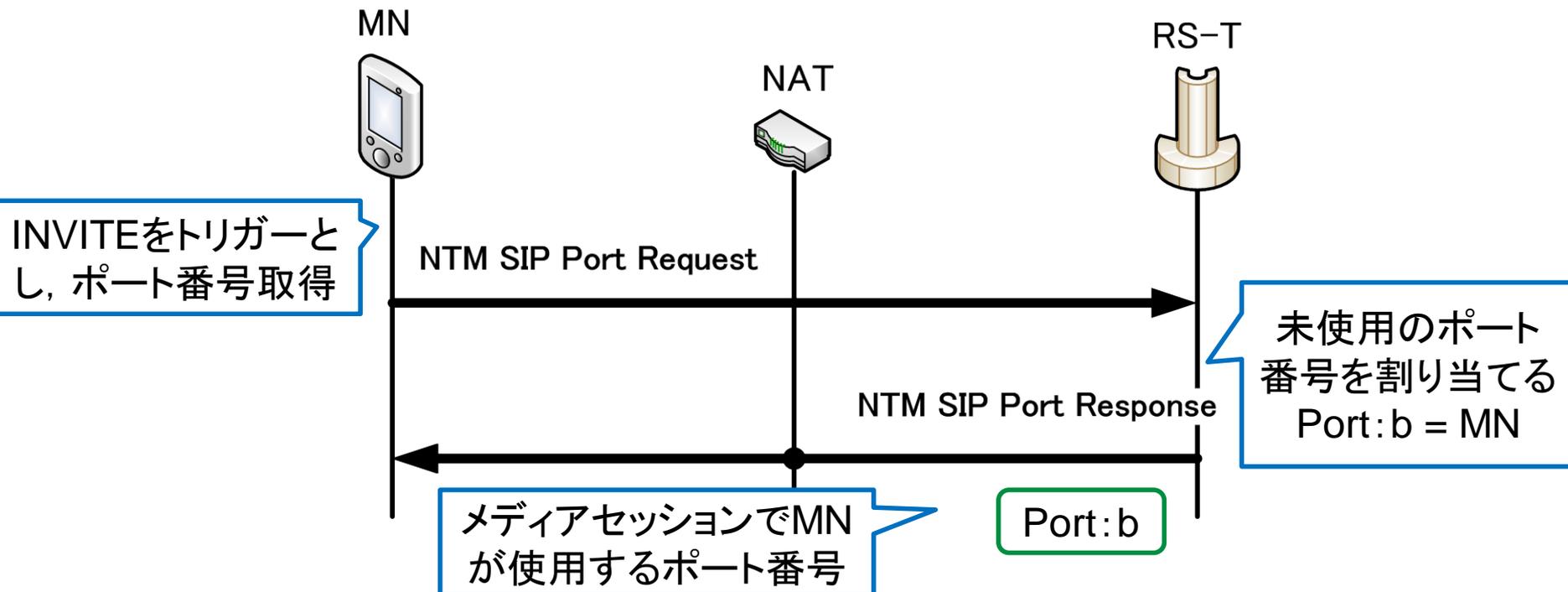
SIPサーバへの登録

- 割り当てられたポート番号を用いて, SIPサーバへ登録



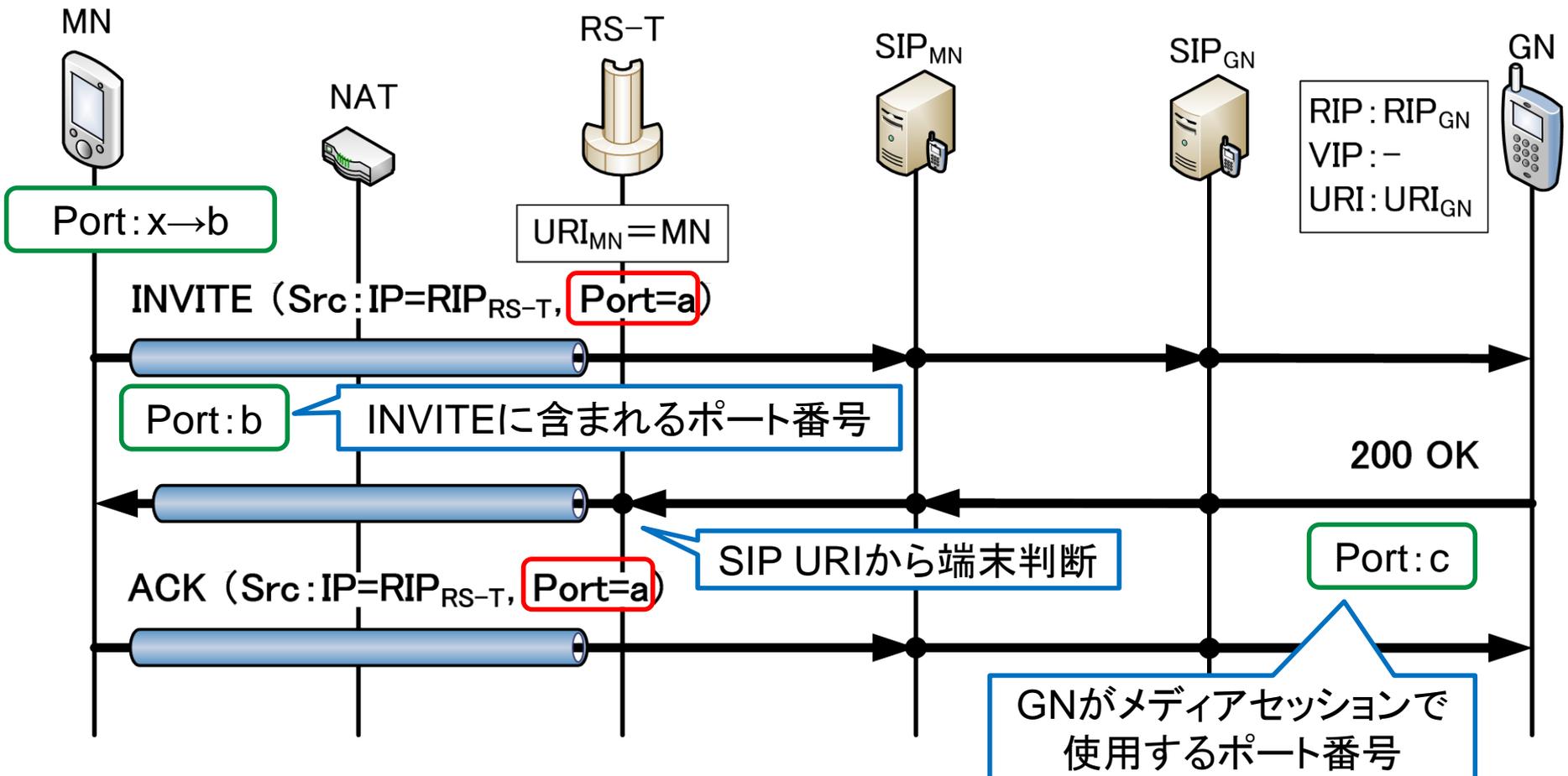
MNから通信開始時

- INVITE送信前にメディアセッションで用いるポート番号の割り当てを受ける
- 割り当てられるポート番号の範囲は、カーネルが使用しないように事前設定する



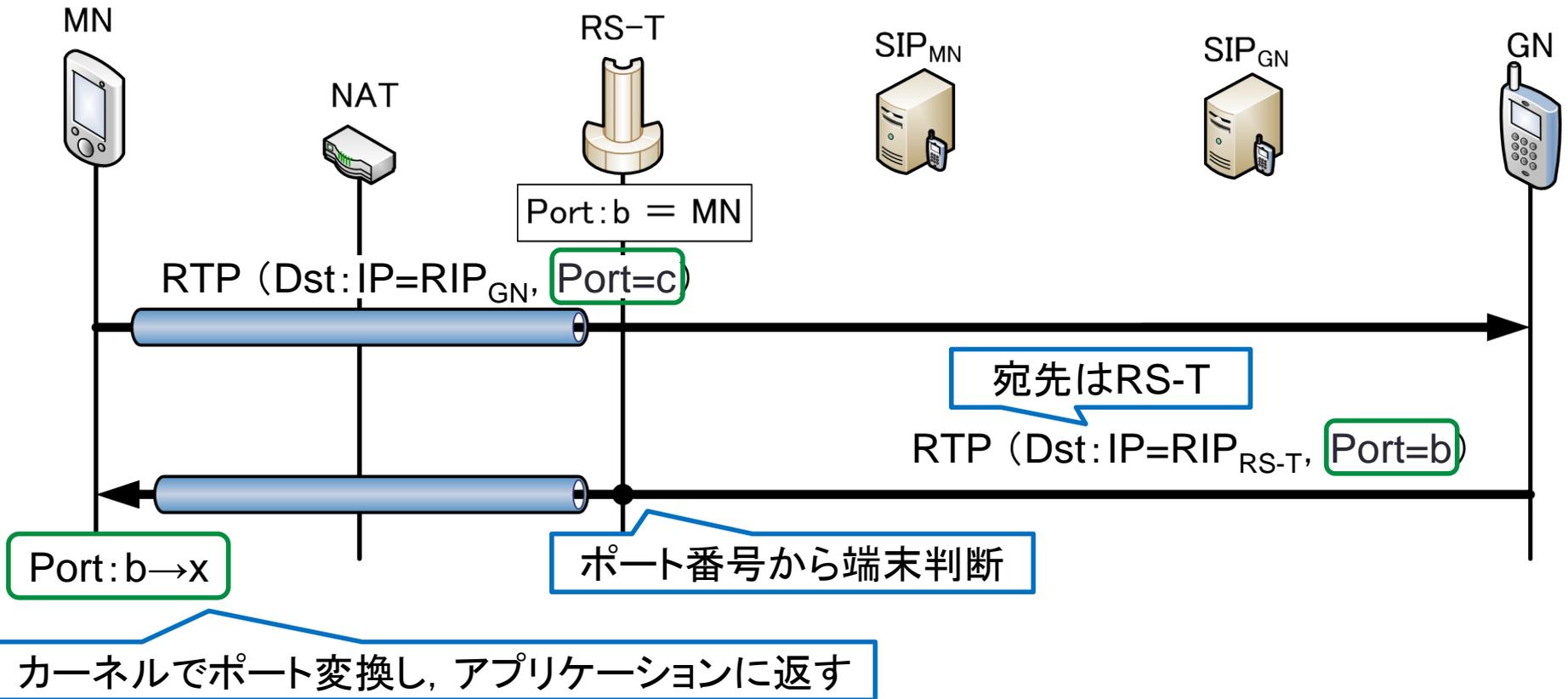
発信処理

- INVITEに含まれるポート番号を、登録時に取得したポート番号に書き換える



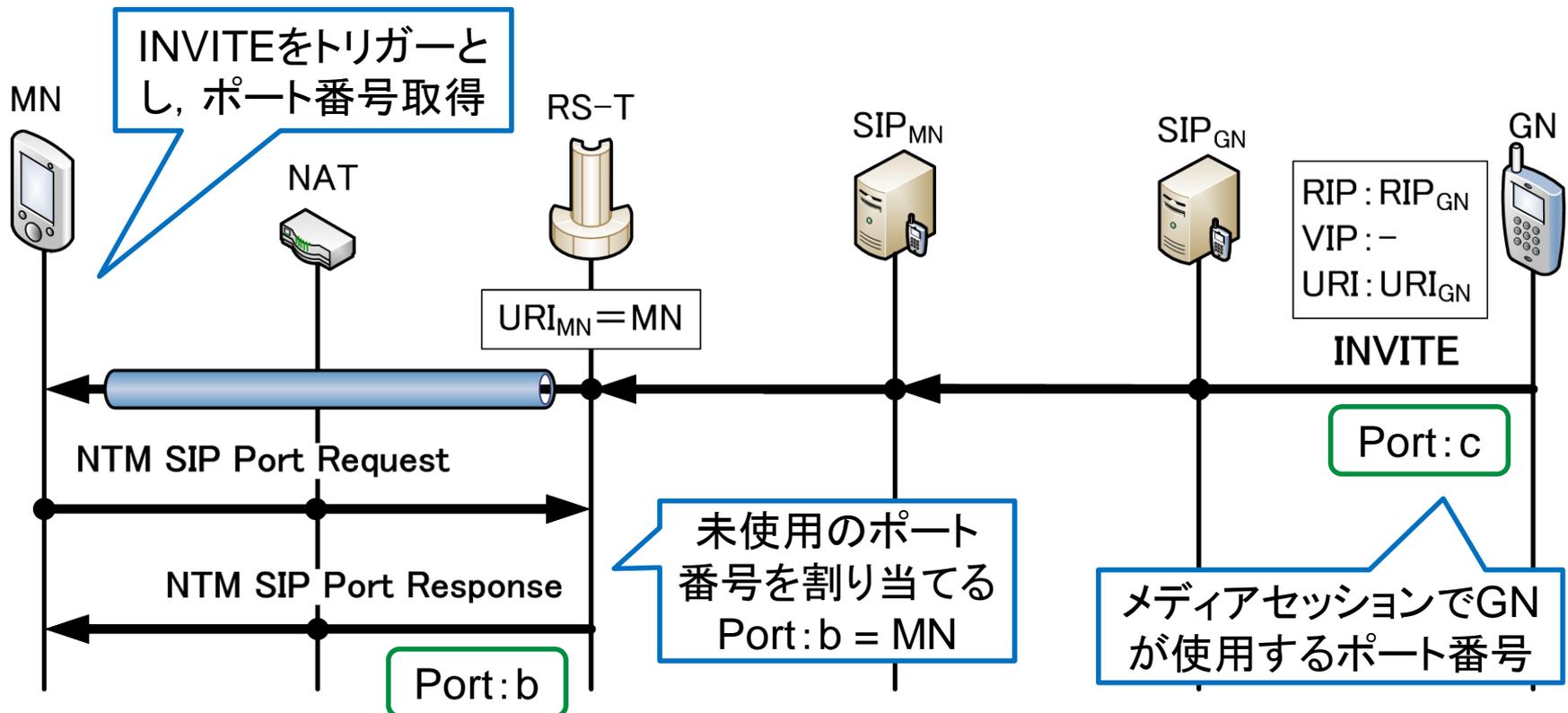
メディアセッション

- MNがポート変換を行うことにより, NATに改造が不要
- RS-Tのアドレスは1個で可能



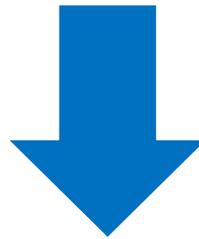
GNから通信開始時

- INVITE受信により, RS-Tからポート番号の割り当てを受ける



確認事項

- 提案方式では, SIPのメッセージ内容を動的に変更するのみ
- SIP自体の修正は必要としない



実アプリケーションの実装が提案方式の処理に対応可能なのか確認する必要がある

- 一般に使用されているSIPクライアント*とSIPサーバ**を用いて, 提案方式の実現可能性を調査

*: Linphone open-source voip software | Linphone, an open-source video sip phone. <http://www.linphone.org/>.

** : Asterisk IP PBX, VOIP Gateway, IVR & Open Source Communications. <http://www.asterisk.org>

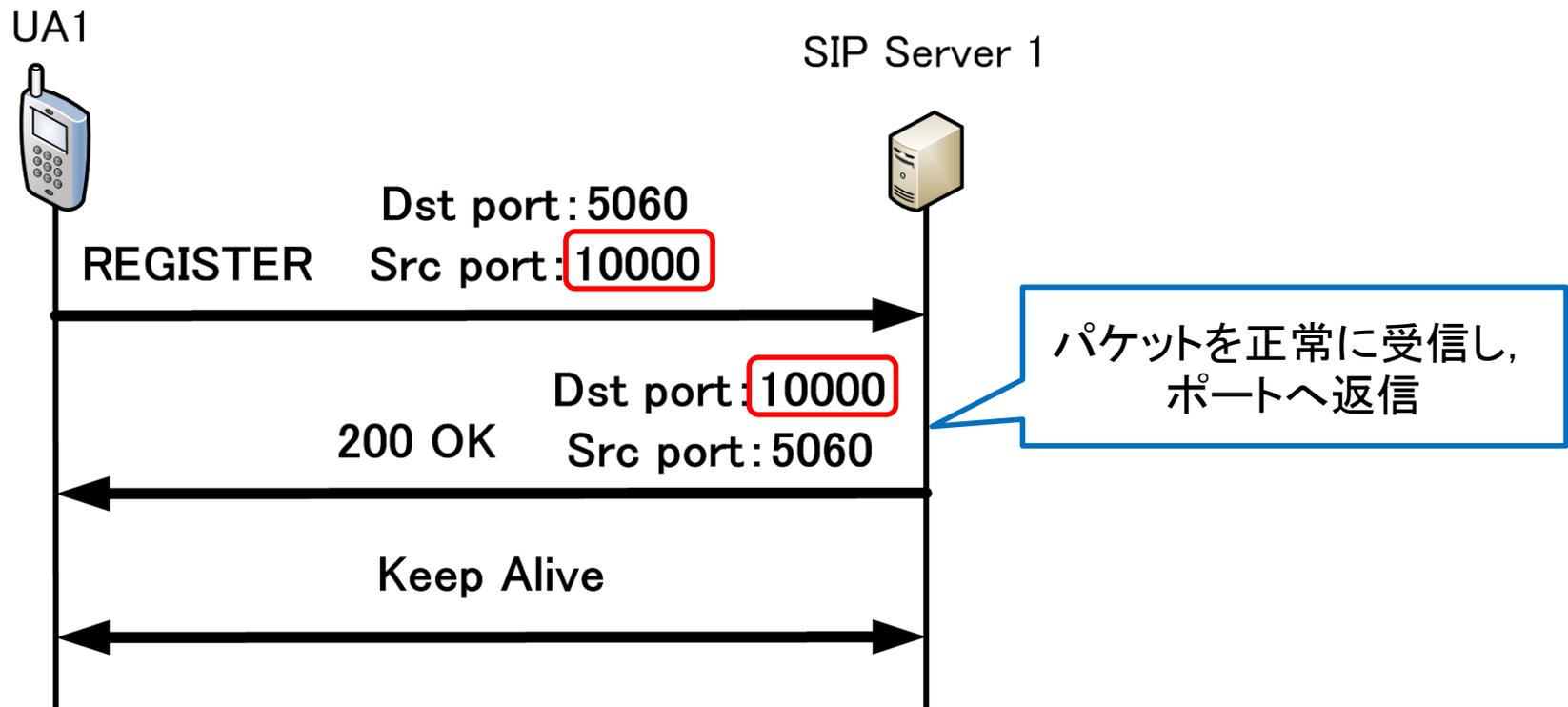
動作確認の目的

- ① SIP通信のポート番号は5060が標準(RFC3261)
 - 独自で指定したポート番号でSIP通信が行えるか

- ② RTPなどメディアセッションで使用するポート番号は、アプリケーションに依存
 - アプリケーションが使用するポート番号と異なるポート番号で通信が行えるか

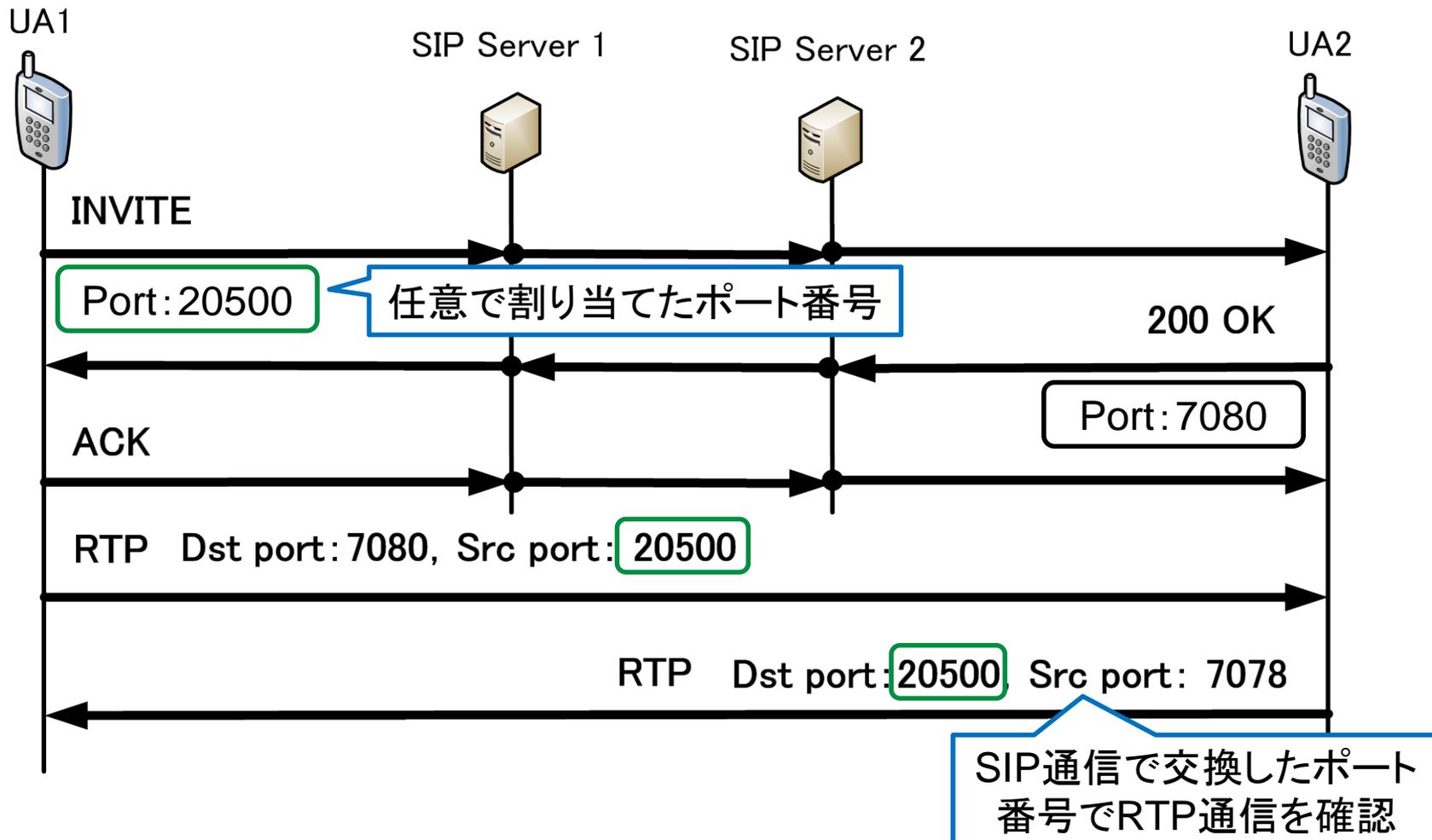
動作確認①: SIP登録処理

- SIP通信のポート番号を5060から10000に変更し, SIP登録処理を実行



動作確認②: SIP通信処理

- メディアセッションで使用するポート番号を, アプリケーションが決めるものから任意のポート番号に変更する



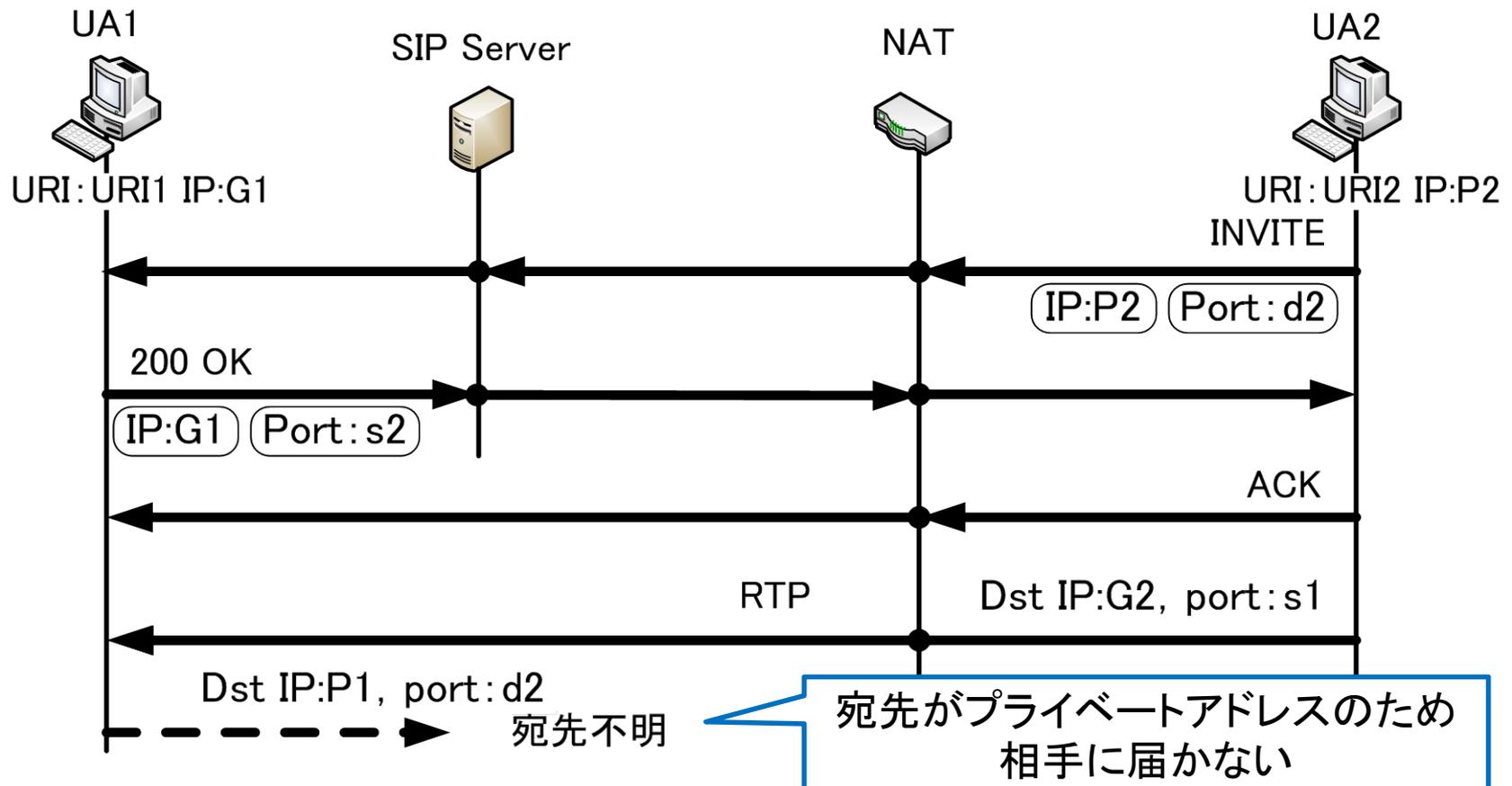
まとめ

- NTMobileにおける一般SIP端末との通信実現手法の提案
 - RS-Tを拡張し、重複しないポート番号によりNTM端末を識別
- 動作確認により、提案方式が実現可能であることを確認した
- 今後は、実装と評価を行う

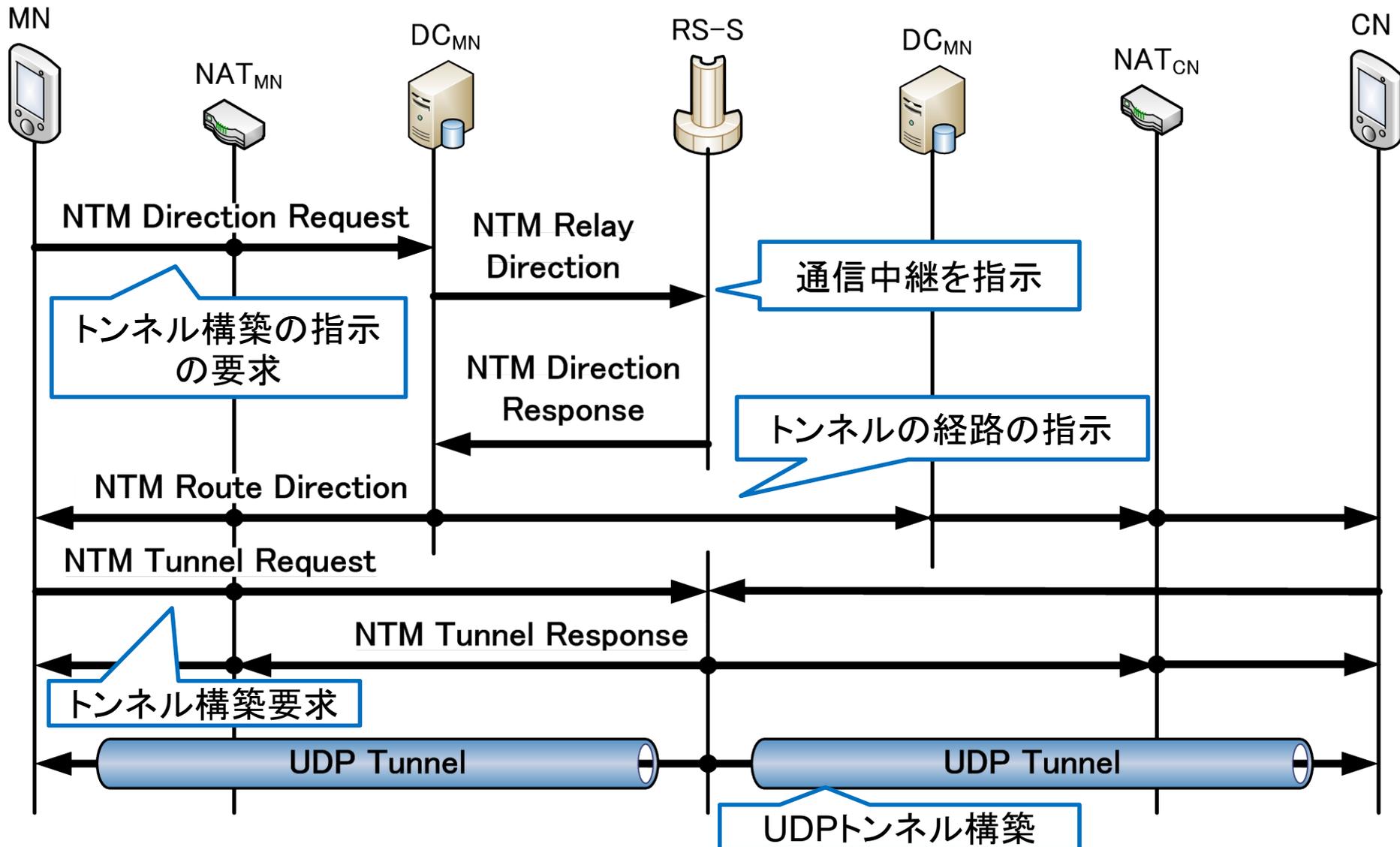
補足資料

SIPとNAT

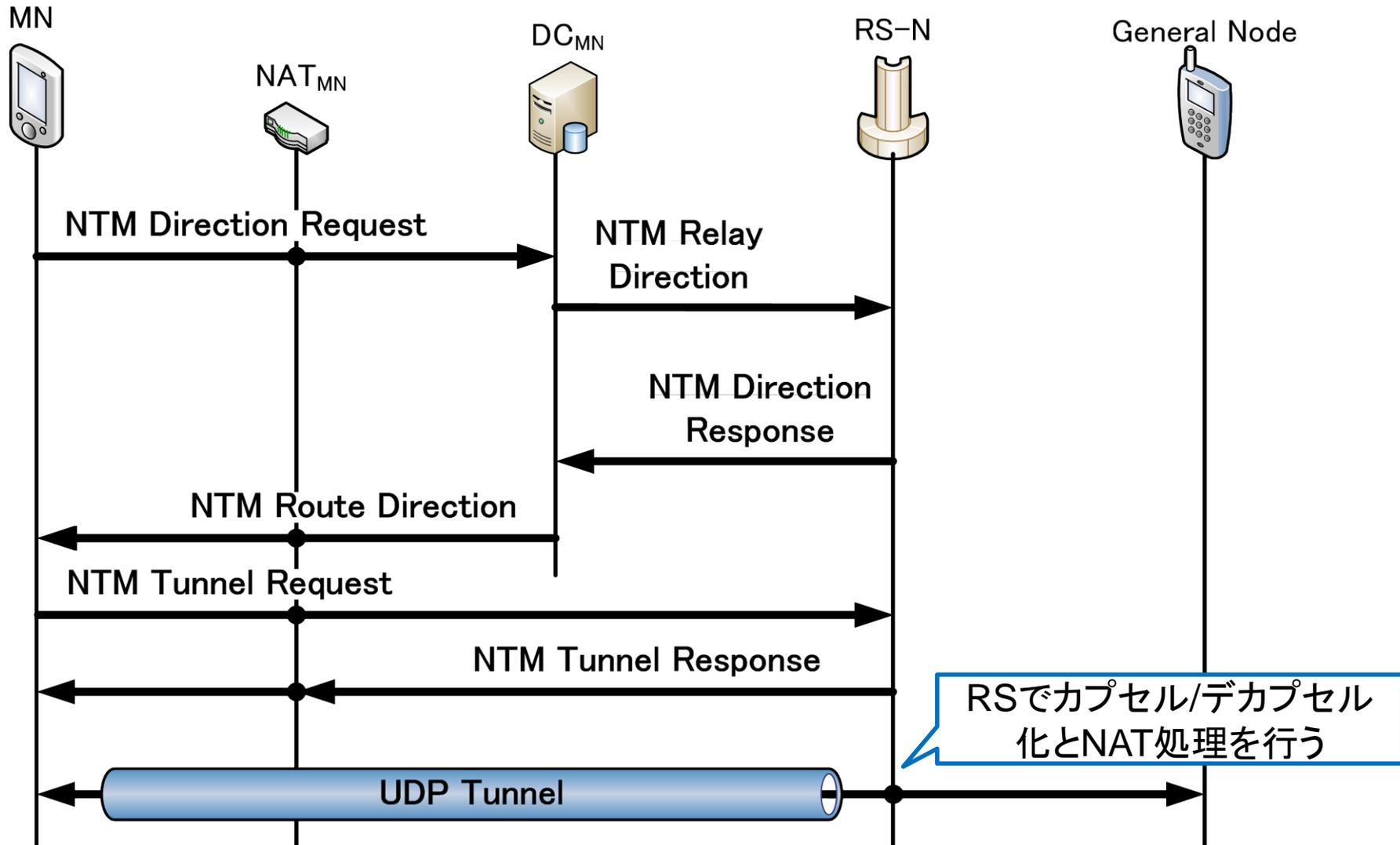
- SIP通信で交換するIPアドレスがプライベートアドレスだった場合、メディアセッションを開始できない



RS-Sを用いたトンネル構築シーケンス

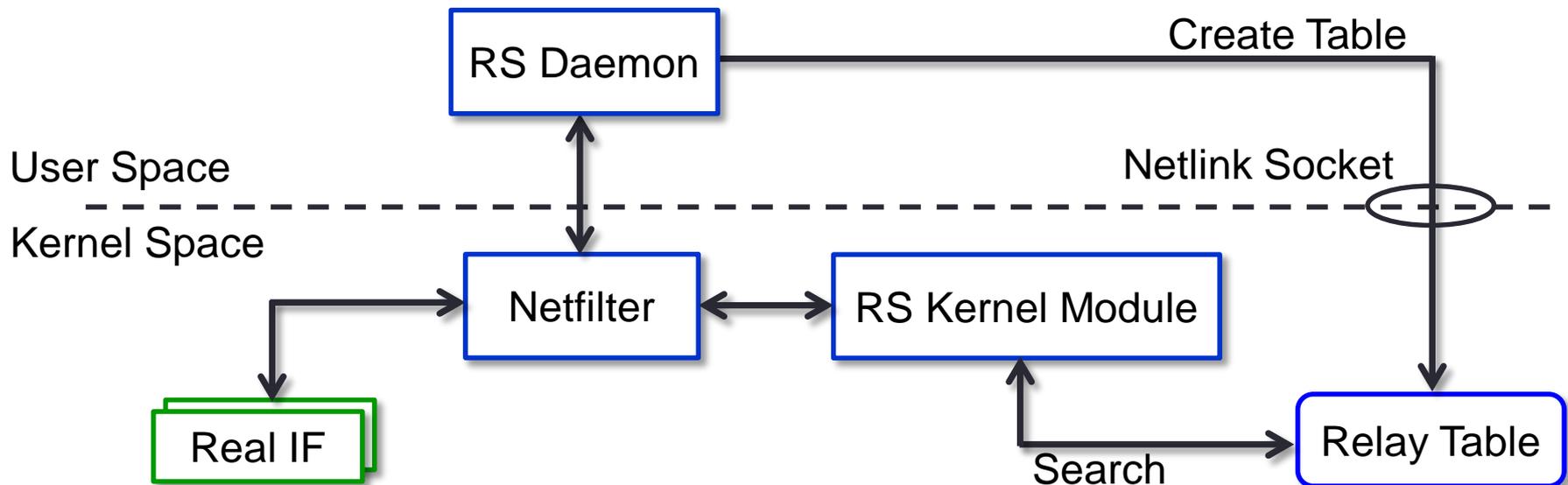


RS-Nを用いたトンネル構築シーケンス



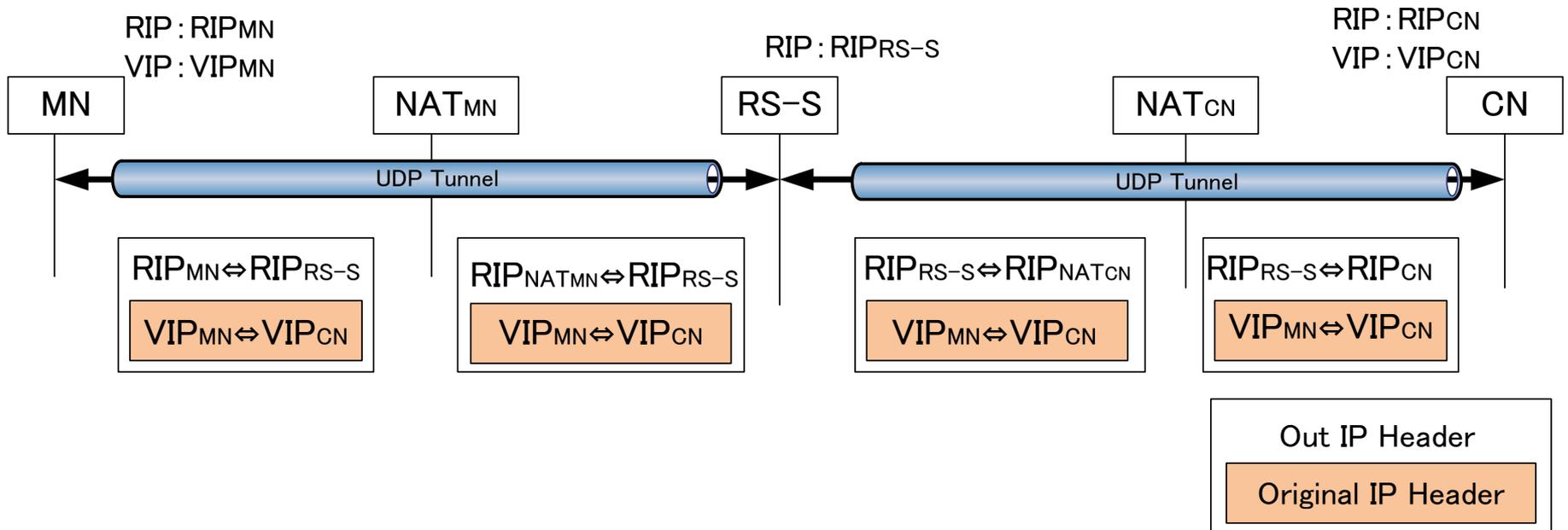
RSの実装

- RSの実装
 - ユーザー空間のRS Daemon
 - カーネル空間のRS kernel Module
- Relay Table
 - RSが保持しているテーブル
 - 転送に必要な情報(トンネル経路の情報など)が記録されている



RS-Sのパケット遷移

- RS-Sはトンネル経路の切替を行う
- 外側IPヘッダのみアドレスが変化



RS-Nのパケット遷移

- パケットのカプセル/デカプセル化を行う
- 元パケットのアドレス変換を行う

