

平成23年度 卒業論文

邦文題目

NTMobileにおけるSIP通信の実現手法

英文題目

**Proposal of SIP-based Communications based
on NTMobile**

情報工学科

(学籍番号: 080430109)

吉岡 正裕

提出日: 平成24年2月3日

名城大学理工学部

内容要旨

いつでもどこからでもネットワークにアクセスすることができるユビキタスネットワークの需要が広まっている。しかし、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、各端末に対して仮想アドレスを割り当て、実際の通信を実アドレスによる UDP トンネルで実現することによりあらゆる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。本稿では NTMobile を利用することにより、NAT を経由するネットワークにおいても SIP を利用できる手法を提案する。

Abstract

The demand of ubiquitous network that can be accessed from henever and anywhere is spreading. However, SIP (Session Initiation Protocol) is frequently used in recent years in multimedia communication, in order to contain the IP address in the message, not available as there is a NAT (Network Address Translation) address translation devices on the communication path. We assigned a virtual address for each terminal, has proposed NTMobile (Network Traversal with Mobility) that enables connectivity in any environment by implementing a UDP tunnel communication with the actual real address. In this paper, by using NTMobile, we propose a method can be used in a SIP network through the NAT.

目次

第1章	はじめに	2
第2章	SIPにおけるNAT越え問題	4
2.1	端末情報登録時に生じる問題	4
2.2	INVITEメッセージ時に生じる問題	5
2.3	セッション確立時に生じる問題	5
第3章	NTMobile	6
3.1	NTMobileの概要	6
3.2	NTMobileの通信確立手順	7
第4章	提案方式	10
4.1	アドレス無変換型リレーサーバRST	10
4.2	起動時の経路確立	10
4.3	SIPサーバへの登録	10
4.4	SIP通信の実現	12
4.5	SIP通信時に起きる問題と解決策	13
第5章	まとめ	15
	参考文献	17

第1章 はじめに

スマートフォンやタブレットなど高性能な携帯端末が急激に普及しつつある。これらの移動端末は無線 LAN だけでなく、3G や WiMAX など複数の手段によりインターネットに接続することが可能である。そのため、利用者の位置や無線ネットワークの状況に応じて最適な通信品質を選択するために、通信メディアを切り替えて通信を行う場面が一般的になりつつある。しかし、無線システムを切り替えると同時に移動端末が接続するネットワークも変化するため、移動端末の IP アドレスが変化してしまう。インターネットで使用されている TCP/IP は IP アドレスを用いて通信端末間の接続を管理しているため、ネットワークの移動が発生すると接続が切断されてしまう。この問題を解決する技術を移動透過性と呼ぶ。

一方で、IPv4 ネットワークでは IP アドレスの枯渇を回避するため、家庭内や企業内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 NAT (Network Address Translator) が必要である。しかし、このような環境ではインターネット側の端末からプライベートアドレス空間の内部が見えなくなるため、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、今後は家庭にもネットワークが導入されるようになり、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十分に考えられる。このため IPv4 ネットワークにおいて NAT 越え問題を解決することは有益である。

我々は、あらゆるネットワーク環境で 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) を提案している。NTMobile は、各端末に対して仮想 IP アドレスを割り当て、端末間の通信を実 IP アドレスによる UDP トンネルで実現している。しかし、近年頻繁に使用されるマルチメディア通信の一つである SIP (Session Initiation Protocol) は、IP ペイロード部分に IP アドレスが記載されているアプリケーションであるため、NTMobile では解決することはできない。そこで本論文では、NTMobile にアドレス無変換型リレーサーバ RST (Relay Server Transparent type) を導入し、かつ端末側のルーティングテーブルを適切に操作することにより、NAT を経由するネットワークにおいて SIP を利用できる手法を提案する。

以降，第 2 章で SIP における NAT 越え問題について説明する．第 3 章で NTMobile の概要と動作について説明し，第 4 章で提案方式について説明する．第 5 章でまとめる．

第2章 SIPにおけるNAT越え問題

NATが存在する環境でSIPを使用する場合、以下の2つの問題がある。1つは、通常のNAT越え問題にも関わるもので、NAT外部から内側に向けてシグナリングを開始できないことである。また、SIPはIPペイロード内のSDP(Session Description Protocol)部分にIPアドレスやポート番号を記載しているため、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。

2.1 端末情報登録時に生じる問題

図1にUAがNAT配下にある場合に発生する問題を示す。なお、破線で示されているのは失敗時の動作である。UA2はNAT配下にあり、プライベートIPアドレスが割り当てられる。UA2はSIP Serverに対して、REGISTERによりSIPメッセージを受け取る際に使用するアドレスP2の登録を要求する。SIP Serverは受信したURIを登録し、200 OKメッセージをP2宛てに返信する。しかし、P2はプライベートIPアドレスのため、200 OKメッセージは宛先不明として処理されてしまい、UA2には到達しない。

これを解決するためにRFC3581では、REGISTERメッセージの送信元IPアドレス・ポート番号に向けて、応答を返す方法が規定されている。図4では、NATにより変換されたREGISTERの送信元G2に向けて200 OKメッセージを返答し、UA2まで到達させることができる。これにより、SIP Serverに端末情報を登録することが可能になる。RFC3581はNAT配下にいるUAから開始されるシグナリングの場合、全てのSIPメッセージについてNAT越え可能である。しかし、以下に示すケースには対応できない。

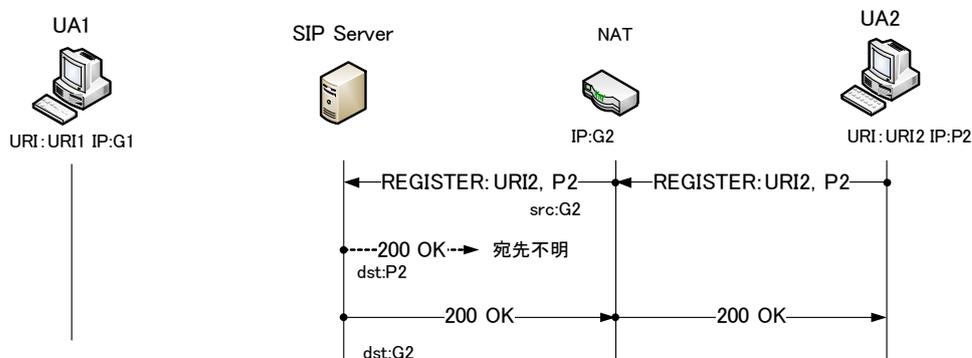


図 2.1 端末情報登録時に生じる問題

2.2 INVITE メッセージ時に生じる問題

図 2 に INVITE メッセージに生じる問題を示す。SIP Server は、UA1 から UA2 に向けた INVITE メッセージを受信すると、登録情報の中から UA2 の情報を取得する。しかし、P2 はプライベート IP アドレスであるため、SIP Server が INVITE メッセージを P2 宛てに送信しても宛先不明として処理されてしまい、UA2 には到達しない。

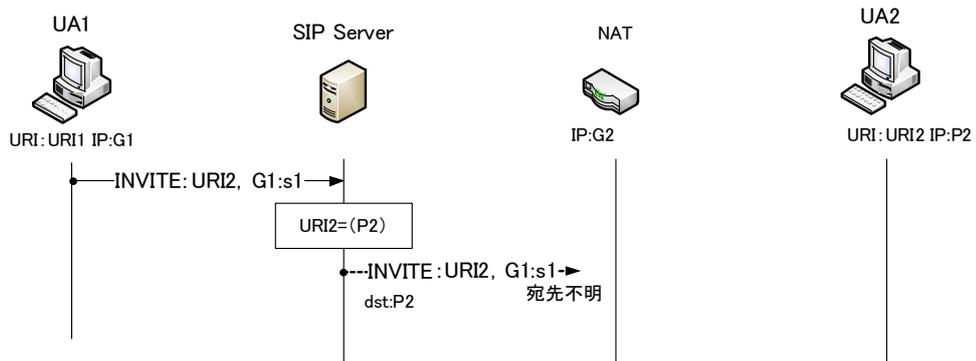


図 2.2 INVITE メッセージに生じる問題

2.3 セッション確立時に生じる問題

図 3 にセッション確立時に生じる問題を示す。UA1 は受信した 200 OK に記載されている UA2 の登録情報に基づき、セッションを確立する。しかし、P2 はプライベート IP アドレスであるため、UA1 からセッションを確立することはできない。また、セッションには SIP とは別のポート番号が使われるので、そのための NAT 越え対策が必要である。

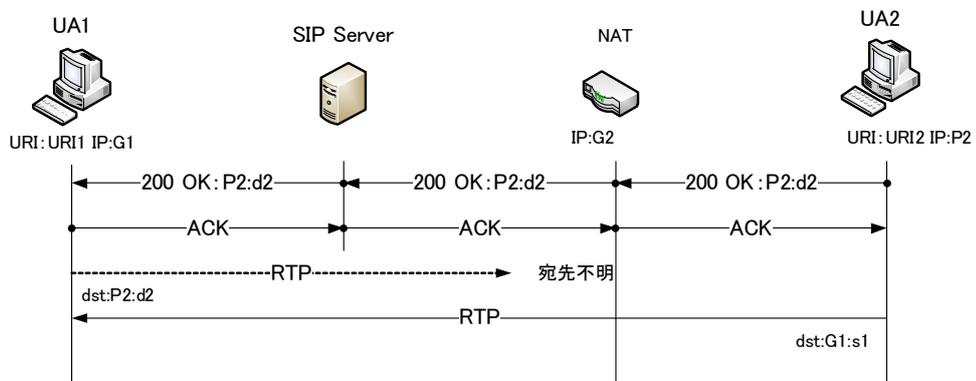


図 2.3 セッション確立時に生じる問題

第3章 NTMobile

3.1 NTMobileの概要

図1にNTMobileの概要を示す。システムの構成要素としてNTM端末の他に、NTM端末のネットワーク位置情報を管理するDC (Direction Coordinator)、必要に応じて通信パケットを中継するRS (Relay Server)がある。NTM端末は、無線LANや3G、WiMAXなど複数の無線通信技術を実装している。NATは、SPI (Stateful Packet Inspection)などのフィルタリング機能を実装した一般的なNATルータを想定し、NTMobileに関わる特別な機能は一切持たないものとする。

すべてのNTM端末はネットワーク接続時にDCに対して位置登録処理を行う。位置登録処理では、DCに対してNTM端末の実IPアドレス、ノードID、FQDNに加えて、NTM端末がプライベートネットワークに存在する場合はNATのグローバルIPアドレスが登録される。この時、NTM端末はDCから仮想IPアドレスを割り当てられる。NTM端末のアプリケーションは、仮想IPアドレスを用いてコネクションを確立する。実際の通信は実アドレスによるUDPトンネルを用いることにより、通信経路上にNATが存在しても確実にコネクションの確立を実現することができる。仮想IPアドレスを用いているため、移動に伴う実IPアドレスの変化を隠蔽して移動透過性を実現できる。NTM端末間の通信はエンドエンドで暗号化され、盗聴の防止や改ざんの検出が可能である。

NTMobileでは、できる限りエンドツーエンド通信が行えるように、DCが通信ペアとなるNTM端末のネットワーク位置情報に応じて、NTM端末に最適なトンネル構築を指示する。この指示は通信開始時だけでなく、NTMノードが様々なネットワークへ移動した場合にも行われる。どちらか一方のNTM端末がグローバルネットワークに存在すれば、他方はNAT配下のプライベートネットワークにいても、RSを経由しない最適経路による通信を実現できる。RSによる中継通信が行われるのは、2台のNTMノードが異なるプライベートネットワークに存在する場合と、通信相手がNTMobileに対応しない一般端末の場合などである。

DCはDynamic DNS機能を有しており、NTM端末のアドレス管理や暗号鍵の生成、配布を行う。この他に、NTM端末に割り当てる仮想IPアドレスプールの保持や、NTM端末に対してトンネル構築指示を行う役割を担っている。DCとRSはグローバルネットワーク上に設置し、ネットワークの規模に応じて分散設置が可能である。

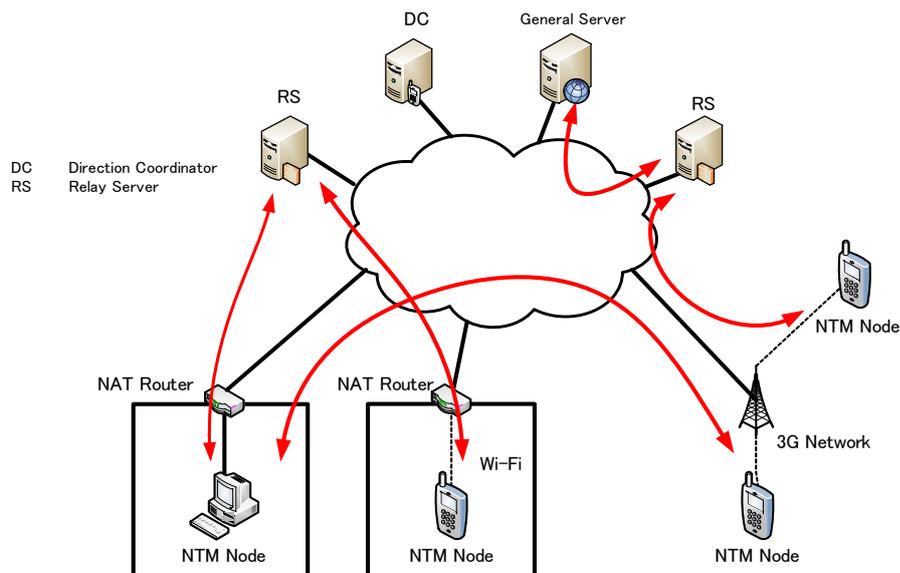


図 3.1 NTMobile のシステム構成

3.2 NTMobile の通信確立手順

NTMobile における NTM ノード間のコネクション確立手順について詳述する。NTMobile では通信を行うペアが本方式に対応していれば、双方とも移動が可能であるが、以後の説明では通信開始側 NTM 端末を MN、通信相手側端末を CN として説明する。

3.2.1 前提条件

エンド端末はネットワーク接続時の位置登録処理を完了しており、 DC_N にはエンド端末 N のネットワーク位置情報が登録されているものとする。エンドノードが使用する仮想 IP アドレスは DC により割り当てが行われ、重複がないものとする。なお、 DS_N とエンド端末 N 間、各 DC と RS 間には信頼関係があるものとする。

3.2.2 通信シーケンス

NTMobile ではエンド端末が存在しているネットワークのアドレス空間の違いに応じて、最適な通信経路が確立できるようにトンネル確立フェーズのシーケンスが変化する。基本的な考え方として、通信ペアとなる NTM 端末のうち、どちらか一方がグローバルネットワークに接続している場合は、エンドエンドでトンネルを構築する。両端末ともプライベートネットワークに存在したり、通信相手が一般端末の場合は RS を中継したトンネルを構築する。

ここで、NTMobile 対応の MN・CN の一方が NAT 配下のプライベートネットワークに存在しているパターンを取り上げて、通信シーケンスを図 2 に示す。

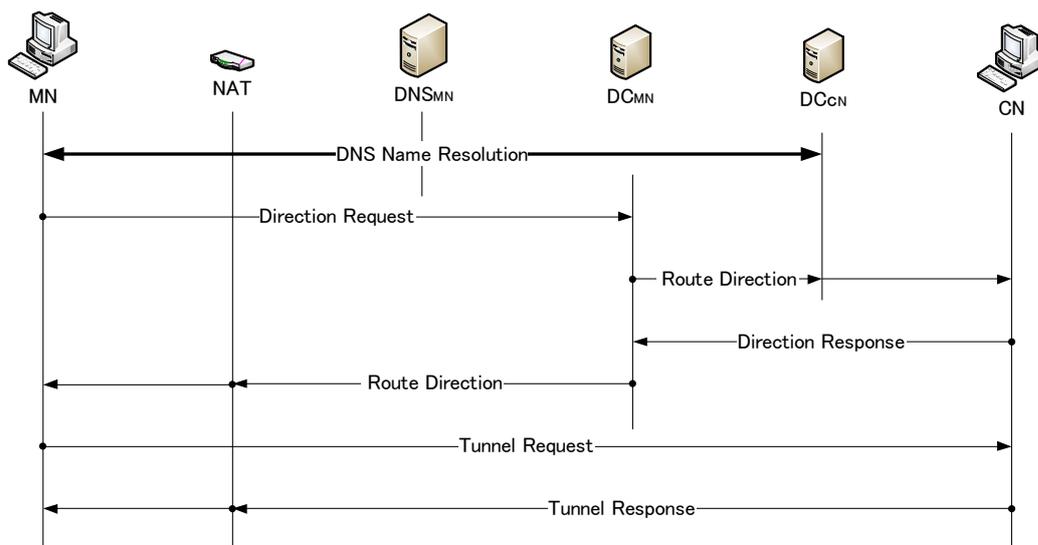


図 3.2 NTMobile の基本シーケンス

MN は DNS により CN の名前解決を行い、 DC_{MN} に登録されている CN の実 IP アドレスが記載された DNS クエリの応答を受信する。ここで、MN はカーネルで DNS クエリ応答を一時退避させ、 DC_{MN} へ NTMobile 専用レコードの問い合わせを行う。CN が NTM ノードであれば、MN は DC_{CN} から NTMobile 専用レコードを入手でき、CN に関する追加情報 (NID_{CN} , RIP_{CN} , VIP_{CN} , RIP_{DCCN}) を取得し記録する。完了後に退避していた DNS クエリ応答メッセージに記載されている RIP_{CN} を VIP_{CN} に書き換えてから、DNS リゾルバに渡す。これにより、MN の上位アプリケーションは CN のアドレスを VIP_{CN} と認識することになる。

MN は DC_{CN} へ Direction Request メッセージを送信する。このメッセージには MN 自身の情報 (NID_{MN} , RIP_{MN} , VIP_{CN}) と NTMobile 専用レコードにより入手した CN の情報、および CN との間に構築するトンネルの識別子が記載されている。

DC_{MN} は受信した MN と CN のノード ID および各種 IP アドレス情報からトンネル構築手順を決定する。構築手順が決定した後、Route Direction メッセージにより各ノードにその後のトンネル構築動作を指示する。なお、Route Direction メッセージには DC_{MN} が生成した共通鍵 K_{MN-CN} を配布する役割を担う。

MN と CN 間のエンドエンドでトンネルを構築する。このとき、MN はプライベートネットワークに存在するため、以後のシーケンスは MN 側から開始する必要がある。そのため、 DC_{MN} は Route Direction メッセージにより、MN には CN へ Tunnel Request メッセージを送信するよう指示する。一方、CN には DC_{CN} を経由して、MN からの Tunnel Request メッセージを受信するよう指示する。Route Direction メッセージは先に CN に対して送信する。CN の Direction Response メッセージが返信された後、MN に Route Direction メッ

セージを送信する。

以上の処理により、片方の NTM 端末が NAT 配下のプライベートネットワークに存在していても、エンドエンドで通信することができる。

第4章 提案方式

4.1 アドレス無変換型リレーサーバ RST

NTMobile ではアドレス変換型リレーサーバ RSN (Relay Server NAT type) を使用することにより、通常相手が一般端末であっても NTM 端末の移動透過性を実現できる。しかし、RSN ではアドレス変換をするため SIP の課題を解決できない。そこで本稿ではアドレス無変換型リレーサーバ RST を利用する。RST は、あらかじめ DC より複数の実 IP アドレスを配布してもらい所持する。NTM 端末は通常の NTMobile で使用する仮想アドレスを割り当てる仮想インターフェイスの他に、RST で使用する仮想インターフェイスを持ち、割り当てられた実 IP アドレスを新たな仮想インターフェイスに割り当てる。NTM 端末は、RST から割り当てられた実 IP アドレスを自身の仮想 IP アドレスとして認識する。

RST は、端末間の通信パケットをカプセル化とデカプセル化するのみで、アドレス変換を行わない。NTM 端末は起動時に RST とトンネルを構築することによって、一般端末からの通信開始するケースに対応することが可能になる。

4.2 起動時の経路確立

MN 起動時の経路確立シーケンスを図 1 に示す。MN はプライベートアドレス空間に存在する NTM 端末とする。

MN は、起動時に DC_{MN} に対して自身の実 IP アドレスを登録する。この時、 DC_{MN} は MN に対して仮想 IP アドレスと共に RST の実 IP アドレスのうちの 1 つを通知する。MN はこれを受けて RST との間にトンネルの構築を行う。そこで、 DC_{MN} に指示要求を行い、 DC_{MN} の指示に従って RST との間にトンネルを構築する。このトンネルは以後も確立したままとしておく。

4.3 SIP サーバへの登録

SIP サーバへの登録シーケンスを図 2 に示す。最初に、SIP サーバの DNS 問い合わせを行う。NTMobile は DNS 問い合わせをトリガーとして動作するが、SIP サーバは一般に NTMobile 非対応であるため NTMobile 専用レコードを取得できない。よって、MN は NTMobile を動作させずに起動時に構築したトンネルを用いる。

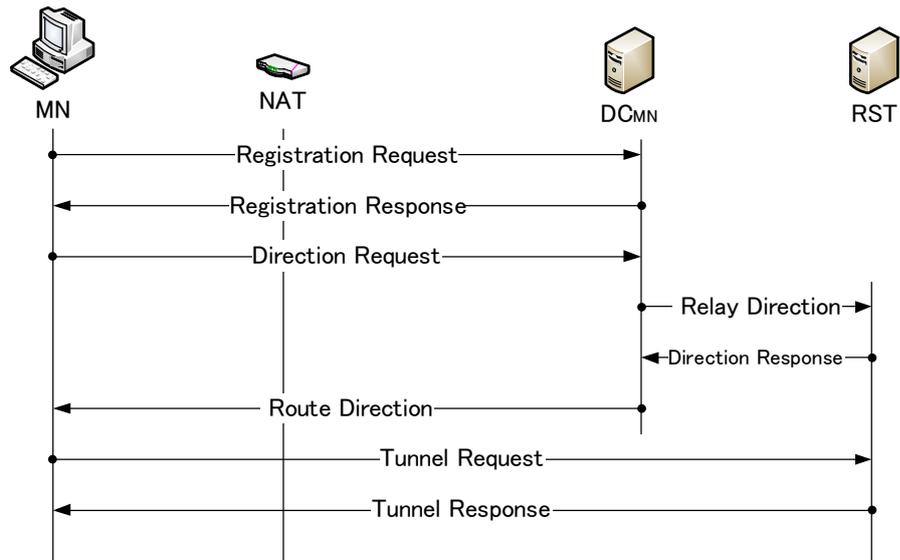


図 4.1 MN 起動時の経路確立シーケンス

MN は SIP Server A に REGISTER メッセージを送信する。この時、登録する IP アドレスは端末起動時に RST から割り当てられたグローバル IP アドレスとする。REGISTER メッセージを受信した SIP Server A は登録処理を行い、完了したことを 200 OK として MN に返す。これにより、一般端末は MN をあたかもグローバル空間上に存在する SIP 端末として認識することができる。

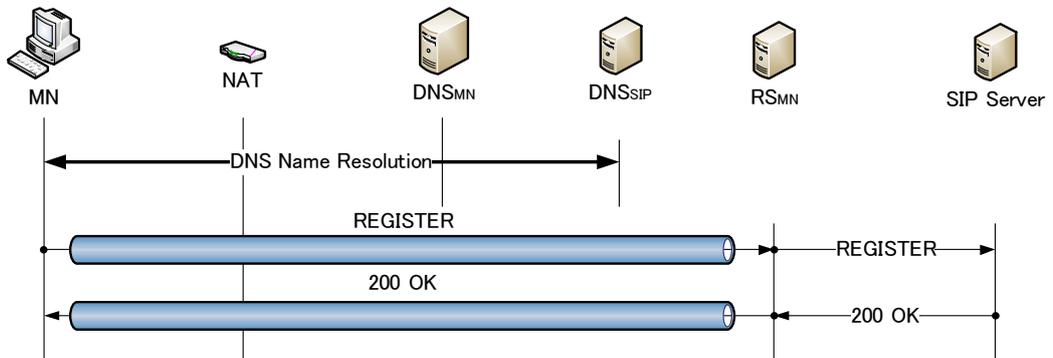


図 4.2 SIP 登録シーケンス

4.4 SIP 通信の実現

4.4.1 NTM 端末間における SIP 通信

RST を用いた NTM 端末間における SIP 通信シーケンスを図 3 に示す。MN と CN はそれぞれ NTM 端末であり、異なるプライベート空間に存在する。MN は RST_{MN} とトンネルを構築しており、割り当てられた IP アドレスを使用する SIP サーバ SIP_{MN} に登録してあるものとする。同様に、CN は RST_{CN} とトンネルを構築しており、割り当てられた IP アドレスを使用する SIP サーバ SIP_{CN} に登録してあるものとする。MN から CN に対して通信を開始するケースについて示す。

DNS クエリにて SIP サーバの名前解決が終了した後、MN は構築しておいたトンネルを通して SIP 通信を開始する。MN と RST_{MN} 間、CN と RST_{CN} 間はそれぞれトンネル通信となる。MN から見ると RST_{CN} の位置に CN が存在しているように見え、CN から見ると RST_{MN} の位置に MN が存在しているようにみえることになる。

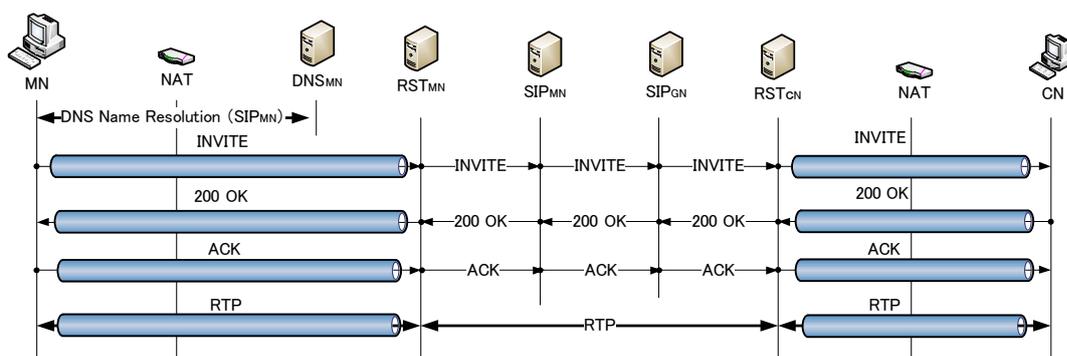


図 4.3 NTM 端末間における SIP 通信シーケンス

4.4.2 NTM 端末と一般端末間における SIP 通信

RST を用いた NTM 端末と一般端末間における SIP 通信シーケンスを図 4 に示す。MN は NTM 端末でプライベート空間に、GN は一般端末でグローバル空間に存在するものとする。また、SIP サーバ SIP_{MN} と SIP_{GN} には必要な情報が既に登録してあるものとする。図 4 は MN から GN に対して通信を開始した場合である。

DNS クエリにて SIP サーバの名前解決が終了した後、MN は構築してあったトンネルを通して SIP メッセージのやり取りを開始する。MN と RST 間はトンネル通信となるが、GN から見ると、RST の位置に MN が存在しているようにみえる。

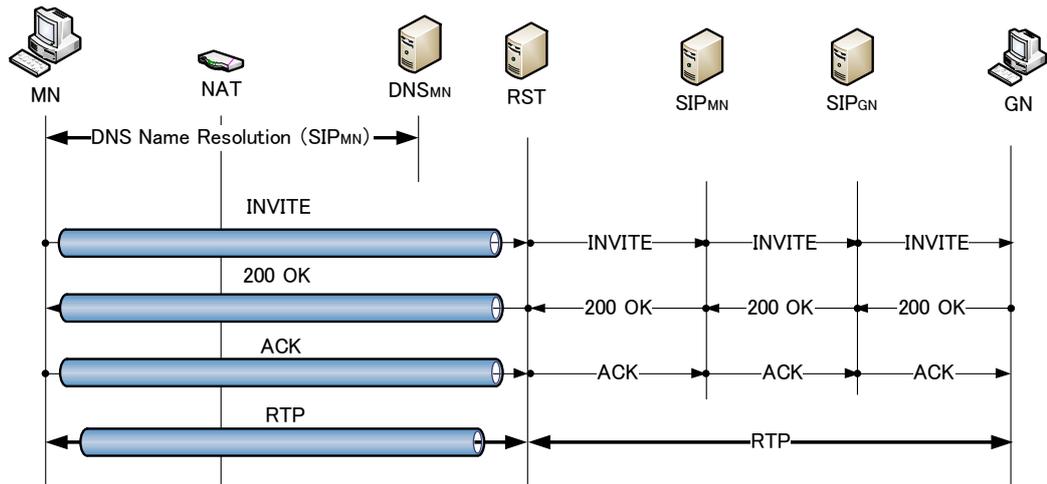


図 4.4 NTM 端末と一般端末間における SIP 通信シーケンス

4.5 SIP 通信時に起きる問題と解決策

前述の SIP 通信において、SIP の最後のメッセージ ACK が終了し、RTP (Real-time Transport Protocol) によるエンドエンドの通信に切り替わる時、以下の考慮が必要である。すなわち、MN は GN 宛てのルーティングテーブルが生成されていないため、パケットが MN のデフォルトルートに送信されてしまい RST に届かないという問題が発生する。現在の RST では、デフォルトルートのゲートウェイが設定されていないため、デフォルトルートを参照したパケットは外部に出ていかない。ここでルーティングテーブルとは、端末が保持しているパケットの配送先に関する経路情報のことである。ある端末から他の端末へとパケットを送信する場合に、目的の端末が自ネットワーク内に存在しない時、ルーティングテーブルを参照することによってパケットを中継させる端末を決定する。

この問題を解決するために、デフォルトルートを参照するパケットを RST に転送するという設定を加えた。これにより、ルーティングテーブルが生成されていない場合においても SIP のエンドエンド通信を開始することができる。ここで、図 4 における MN のルーティングテーブルの内容を表 1 に示す。

表 1 のルーティングテーブルは、NTMobile により RST とのトンネル構築時に動的に作成される。VIP は仮想 IP アドレスであり、VIP_{RST} は MN の仮想 IP アドレスとして RST から割り当てられた IP アドレスである。DGW はデフォルトゲートウェイ、interface の tun とは該当するパケットをトンネル処理を行うことを示している。表 1 の 2 行目は NTMobile 特有の部分で、宛先アドレスの "10.0.0.0" は NTMobile で使用される仮想 IP アドレスであり、NTM 端末宛にパケット送信する場合に参照される。NTM 端末宛のパケットはカプセル化され、仮想インターフェイスへパケットを流す。3 行目から 5 行目は DNS_{MN}、DC_{MN}、RST にパケットを送信する場合に参照される。これらのパケットはカプセル化されずに

表 4.1 MN のルーティングテーブル

adress	netmask	gateway	interface
0.0.0.0	0.0.0.0	VIP _{RST}	tun0
10.0.0.0	255.0.0.0	VIP _{MN}	tun1
DNS _{MN}	255.255.255.255	DGW	eth0
DC _{MN}	255.255.255.255	DGW	eth0
RST	255.255.255.255	DGW	eth0

物理インターフェイスを通して出ていく。1行目はデフォルトルートと呼ばれ、本論文特有の部分である。送信するパケットの宛先がルーティングテーブルにない場合に参照される。デフォルトルートを参照したパケットはカプセル化され、通常の NTMobile で使用される仮想インターフェイスとは別の仮想インターフェイスを通してゲートウェイである RST に送信される。

以上の処理により、通信経路上に NAT が介在しても RST を用いることによって SIP 通信が可能となる。

表 1 はトンネルを構築し、SIP サーバに登録処理を行った後で動的に作成される。ルーティングテーブルが生成されている場合は物理インターフェイスを通してゲートウェイへパケットが流れる。また、デフォルトルートの優先度低く設定されておりルーティングテーブルに相手端末の情報がない場合のみ使用する。

第5章 まとめ

本論文では，NTMobile を利用した SIP 通信の実現手法について検討した．

SIP によるコネクション確立前に，あらかじめアドレス無変換型リレーサーバ RST とトンネルを構築し，ルーティングテーブルを適切に操作することにより通信経路上に NAT が介在しても SIP 通信が可能になる手法を提案した．

今後は，実装と動作確認を行う．

参考文献

- [1] 鈴木秀和 ,水谷智大 ,西尾拓也 ,内藤克浩 ,渡邊 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)DICOMO2011 シンポジウム論文集 , pp. 1339–1348(2011)
- [2] 内藤克浩 ,西尾拓也 ,水谷智大 ,鈴木秀和 ,渡邊 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 ,マルチメディア,分散,協調とモバイル(DICOMO2011) DICOMO2011 シンポジウム論文集 , pp. 1349–1359(2011)
- [3] 西尾拓也 ,内藤克浩 ,水谷智大 ,鈴木秀和 ,渡邊 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 , pp. 1139–1145(2011)
- [4] J.Rosenberg, H.Schulzrinne, G.Camarillo, A.Johnston, J.Peterson, R.Sparks, M.Handley and E.Schooler: SIP: Session Initiation Protocol, RFC3261(2002).
- [5] J.Rosenberg, and H.Schulzrinne: An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing, RFC3581(2003).

