NTMobileを用いたSIP通信方式の提案と実装

吉岡正裕[1]　鈴木秀和[1]　内藤克浩[2]　渡邊晃[1]

概要：マルチメディア通信用プロトコルのSIP（Session Initiation Protocol）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，NATとの相性が極めて悪い．我々は，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．しかし，NTMobileにおいてもSIPのような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しては工夫が必要である．そこで本論文では，SIPサーバにNTMobileを導入することにより，SIPサーバをNTM端末として扱いNATを介したSIP通信を可能にする手法を提案する．また，提案手法の実装を行い，動作検証を行った．

キーワード：NAT越え，SIP，移動透過性

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 Translation）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のアドレス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，CGN（Career Grade NAT）[1], [2]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越え問題を解決することは有益である．

[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

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手法 [3]，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手法 [4], [5], [6]，端末の改造を不要とすることを目的とした手法 [7], [8] がある．

一方，マルチメディア通信用プロトコルのSIP（Session Initiation Protocol）[9] がセッション制御技術として注目され始めている．SIPをNATが存在する環境で使用する場合，以下の2つの課題がある．1つは，通常の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点である．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．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．

我々は，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 [10], [11], [12]．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SIPのような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しては工夫が必要である．

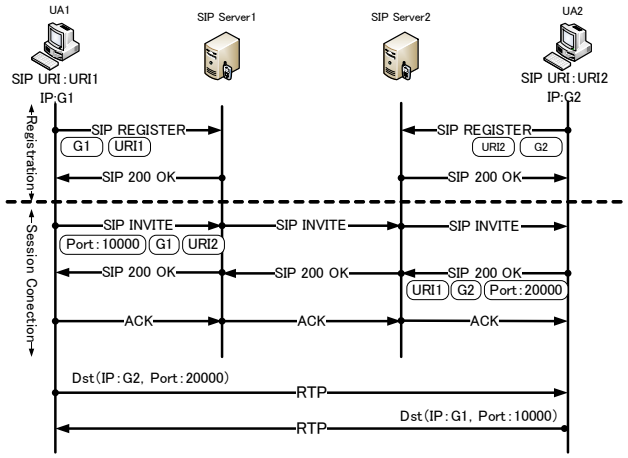


図 1 SIP のセッション確立

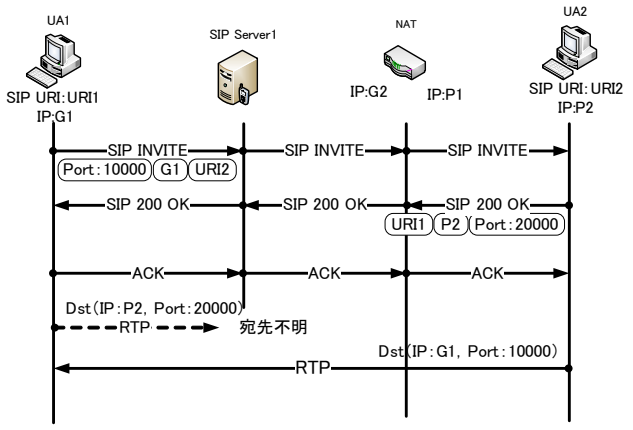


図 2 SIP 通信で発生するアドレス不整合問題

そこで，本論文では SIP サーバに機能拡張した NTMobile を導入し，既存の SIP アプリケーションおよび既存の NAT に一切の手を加えることなく SIP プロトコルを使用することができる手法を提案する．この手法により，NTMobile による移動通信の恩恵を受けることができる．提案方式の実装を行い，既存の SIP アプリケーションを用いて動作検証を行った．

2. 既存技術

本章では，SIP の概要および SIP の課題を述べ，これを解決する既存技術として既存の NAT をそのまま利用できる STUN（Session Traversal Utilities for NAT）と TURN（Traversal Using Relays around NAT）について示す．ただし，これらの技術はアプリケーションに改造を加える必要がある．ここでは，SIP クライアントを使用するエンド端末を UA（User Agent）と呼称する．

2.1 SIP

2.1.1 概要

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．

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，REGISTER 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．

2.1.2 SIP のアドレス不整合問題

図 2 にアドレス不整合問題の例を示す．図 2 では，UA2 が NAT 配下にあり，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 に通信を開始したものとする．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．

2.2 STUN

図 3 に STUN の動作概要を示す．UA に機能の実装が必要であるとともに，第 3 の端末として STUN サーバが必要となる．

SIP メッセージの送信に先立ち，UA は SIP メッセージを送信する際に使用するのと同じポート番号を使用し，STUN サーバに対して Binding Request を送信する．これにより，NAT 上に NAT テーブルを生成する．STUN サーバは，STUN サーバ側から見た送信元の IP アドレスとポート番号を Binding Response として UA に返答する．UA は，Binding Response に記載されている IP アドレスおよびポート番号を SIP メッセージに埋め込み SIP サーバへ送信する．

STUN による方式には，制約がある．それは，Symmetric NAT には使用できないことである．Symmetric NAT は通信相手毎にポート番号が変わる．そのため，宛先が SIP

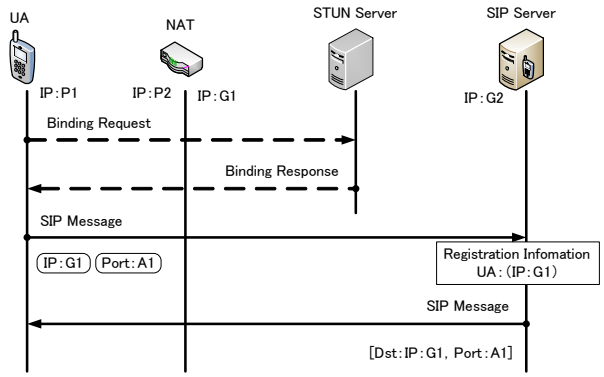


図 3 STUN の動作概要

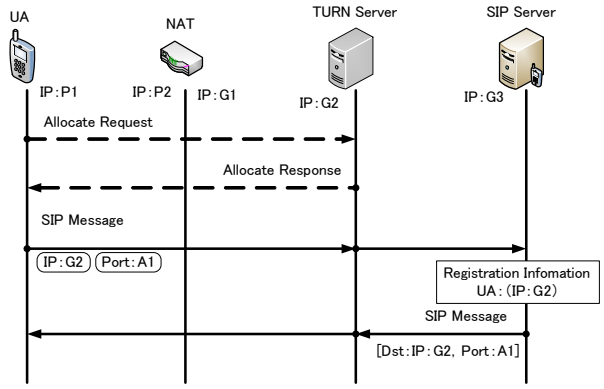


図 4 TURN の動作概要

サーバから UA に切り替わる際，NAT でポート番号の不一致が発生する．

2.3 TURN

図 4 に TURN の動作概要を示す．この方式においても UA に機能の実装が必要であり，かつ第 3 の端末として TURN サーバが必要になる．

UA は通信開始に先立ち，TURN サーバに対して Allocate Request を行う．これに対して，TURN サーバは，自身のポートを割り当て，Allocate Response により UA に通知する．この後，UA は TURN サーバとの間でセッションを維持し続ける．UA は，TURN サーバ上に割り当てられた IP アドレスとポート番号を SIP メッセージに埋め込み，パケットをカプセル化して TURN サーバに送信する．TURN サーバが受信した SIP メッセージについては，カプセル化を行い，UA まで転送する．

TURN は NAT の種類に依存せず，アドレス不整合問題が解決可能である．しかし，TURN サーバは全ての通信を中継するため，TURN サーバに対する負荷が大きいことと，メディアセッションのスループットが低下するという課題がある．

3. NTMobile

本章では，提案方式のベースとなる NTMobile について説明する．

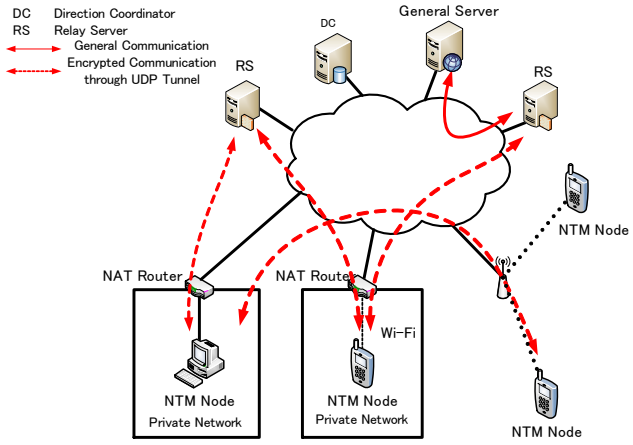


図 5 NTMobile の構成

3.1 概要

図 5 に NTMobile の構成について示す．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，NTM 端末の情報をデータベースで管理している．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．

3.2 通信シーケンス

以後の説明では，通信開始側の NTM 端末を MN（Mobile Node），受信側の NTM 端末を CN（Correspondent Node）として説明する，また，端末 N の FQDN を $FQDN_N$，仮想 IP アドレスを VIP_N，アドレス情報を管理している DC を DC_N，その実 IP アドレスを RIP_{DC_N} とする．

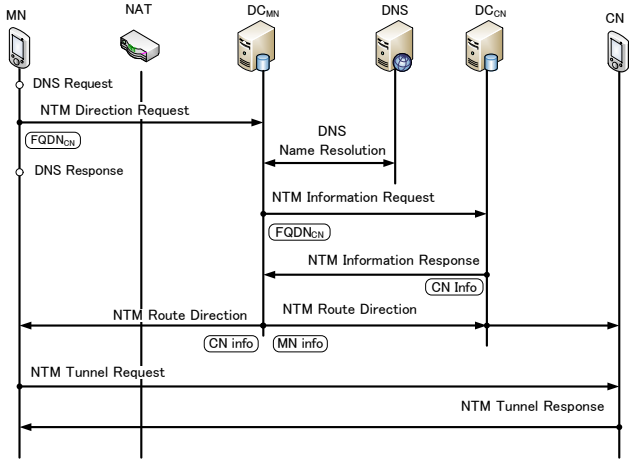


図 6 NTMobile の通信シーケンス

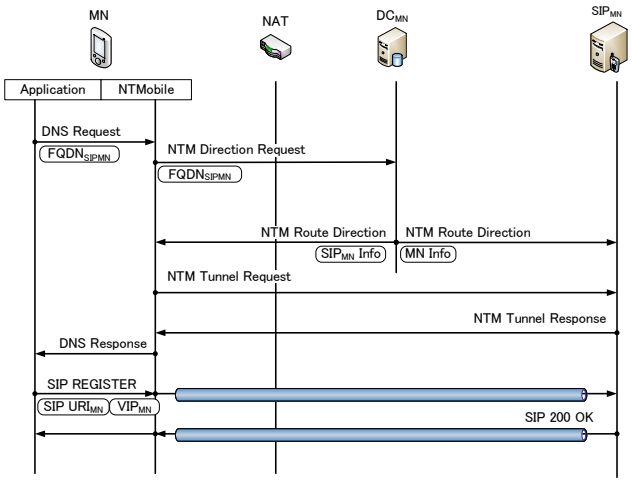


図 7 提案方式の SIP 登録シーケンス

3.2.1 名前解決処理

図 6 に NTMobile の通信シーケンスを示す．MN は，アプリケーションからの DNS 問い合わせを検出すると，そのパケットから $FQDN_{CN}$ を抽出して独自のネゴシエーションを開始する．

MN は，NTM Direction Request に $FQDN_{MN}$ と $FQDN_{CN}$ を記載して DC$_{MN}$ へ送り，名前解決およびトンネル構築指示を依頼する．DC$_{MN}$ は NTM Direction Request に記載している $FQDN_{CN}$ を利用し，DNS の仕組みにより DC$_{CN}$ を発見する．DC$_{MN}$ は NTM Infomation Request/Response により CN の端末情報を取得する．

3.2.2 トンネル構築処理

DC$_{MN}$ は，3.2.1 項で述べた処理によって得た MN と CN の情報から最適なトンネル経路を判断する．DC$_{MN}$ は，経路判断を元にトンネル構築に必要な情報を載せた NTM Route Direction を MN と CN に送信する．NTM 端末が NAT 配下にいる場合，NTM Tunnel Request を NAT 配下の NTM 端末から送信させることによってトンネル通信の経路を確保する．

MN のアプリケーションは仮想 IP アドレスのみを認識しているため，アプリケーションは仮想 IP アドレスによるパケットを生成する．MN はこれを実 IP アドレスによりカプセル化し，CN へ転送する．CN は受信したパケットをデカプセル化し，抽出したアプリケーションパケットを上位アプリケーションへ渡す．逆方向の通信も同様である．

この方式により，実 IP アドレスの変化をアプリケーションに対して隠蔽し，NAT 越え問題の解決と移動透過性を同時に実現できる．

4. 提案方式

4.1 提案方式の方針

仮想 IP アドレスを使用するためには，SIP サーバが仮想 IP アドレスを認識できなければならない．NTMobile で用いる仮想 IP アドレスは，NTMobile に関連する機器以外では認識することができない．また，SIP 通信ではグローバル上に存在する SIP サーバを必ず経由する必要があり，この課題を解決しなければならない．SIP サーバのアプリケーションに手を加える手法も考えられるが，SIP アプリケーションが限定されるため望ましくない．次に，仮想 IP アドレスを実 IP アドレスに変換し，SIP サーバに登録を行う手法も考えられるが，変換を行う装置をグローバルネットワーク上に設置する必要があり，経路が冗長化する．そこで，SIP サーバのアプリケーションに手を加えず，NTMobile を SIP サーバに導入する方式を採用する．この方法により，SIP サーバを NTM 端末として扱うことができるため，仮想 IP アドレスの認識が可能になる．

4.2 構成

本提案のネットワーク構成として，DC（DC$_{MN}$，DC$_{CN}$）と SIP サーバ（SIP$_{MN}$，SIP$_{MN}$）をグローバル上に設置する．NTM 端末の MN は NAT 配下に，CN はグローバル上に存在する．SIP サーバには，NTMobile を導入する．SIP サーバのアプリケーションと SIP クライアント，NAT には一切の変更を加えない．MN と CN は，それぞれ SIP$_{MN}$ と SIP$_{CN}$ へユーザ認証が完了し，SIP URI と認証パスワードが発行されているもとのする．MN と CN は互いの SIP URI を保持しているものとする．

提案方式では，NTM 端末が異なる NAT 配下に存在したネットワーク構成においても，NTMobile の仕組みにより RS を介して SIP 通信は実現できるが，本論文では簡単のため MN のみが NAT 配下に存在するものとする．

4.3 SIP 登録処理

図 7 に SIP 登録処理シーケンスを示す．MN は SIP サーバに自身の位置情報である VIP_{MN} を登録するため，$SIPURI_{MN}$ の名前解決を行う．名前解決により，NTMo-

bile のネゴシエーションが開始される．今回は，NTMobile が導入された SIP サーバが通信相手であるため，MN と SIP_{MN} の間でトンネルが構築される．トンネル構築後，MN は SIP_{MN} に SIP 登録メッセージである SIP REGISTER を送信する．SIP REGISTER には仮想 IP アドレスが含まれており，図 7 では VIP_{MN} となる．正常に登録処理が完了すると，SIP_{MN} は MN に SIP 200 OK 返しリクエストが成功したことを通知する．SIP クライアントは起動中，SIP サーバに対して定期的にパケットを送信し経路確保を行う．このため，SIP クライアントが起動している間は MN と SIP_{MN} で構築されたトンネルは維持される．

4.4 SIP 通信処理

提案方式の SIP 通信シーケンスを**図 8** に示す．MN が CN に対して SIP 通信を開始する．MN は，CN の SIP URI を用いて通信を始める．SIP URI は，SIP のみで使われる識別子であり，メールアドレスのように扱われる．MN は宛先の情報である $SIPURI_{CN}$ と自身の仮想 IP アドレス VIP_{MN} を記載した SIP INVITE を，すでに生成済みのトンネルを介して SIP_{MN} に送信する．SIP_{MN} と SIP_{CN} は NTM 端末として動作しているため，両者の間にトンネルが構築される．その後，SIP INVITE は SIP_{CN} を経由し CN に送信される．SIP INVITE を受信した CN は，SIP INVITE と同様の経路で自身の仮想 IP アドレス VIP_{CN} と $SIPURI_{CN}$ を SIP 200 OK に記載し，MN に送信する．ここまではトンネル通信であることを除き，通常の SIP 通信と同様である．

NTM 端末間にてメディアセッションの直接通信を行うためには，MN と CN 間にトンネルの構築を行う必要がある．SIP 通信前にトンネル構築を行う方法も考えられるが，通信相手が応答しないという場合も考えられる．そのため，通信相手が応答したことが確定した後にトンネル構築を行う．SIP 通信において，メディアセッションに応じることが確認できるタイミングは，通信相手の SIP 200 OK の送信である．そこで，通信開始側の NTM 端末は SIP 200 OK の受信をトリガとして，NTMobile ネゴシエーションを開始し，MN と CN 間でトンネル構築を行う．MN はトンネル構築が完了するまでは，SIP 200 OK を保持しておく．

図中の A から D は提案方式固有の動作である．A において，MN は SIP 200 OK を受信すると，NTMobile の機能によりパケットをフックする．このパケットは，D までの間保持する．NTMobile は SIP 200 OK に含まれている VIP_{CN} を取得する．取得した VIP_{CN} を NTM Direction Request に記載し，DC_{MN} に送信する．

NTMobile では通常，通信相手の FQDN から端末を管理している DC の IP アドレスを取得を行う．しかし，SIP メッセージには FQDN が含まれていないため，仮想 IP アドレスから DC の位置情報を取得するよう DC の拡張

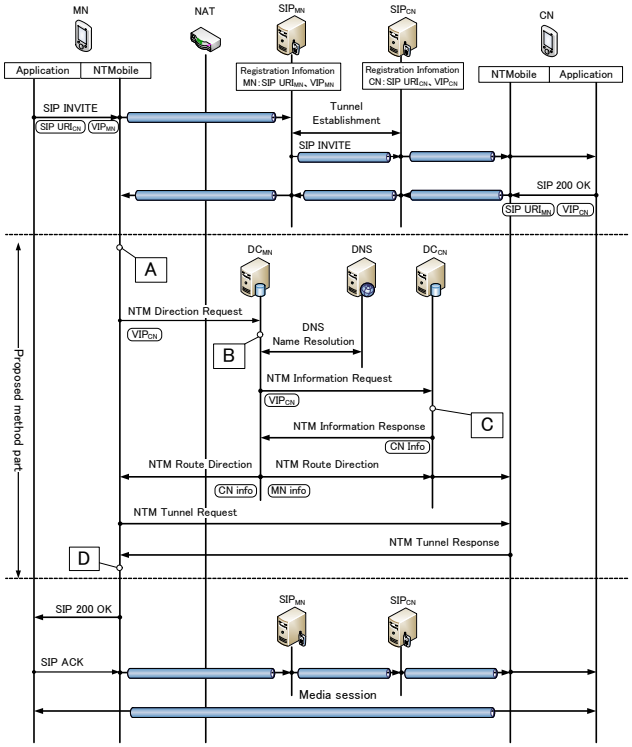


図 8 提案方式の SIP 通信シーケンス

を行う．図中 B において DNS 逆引きの仕組みを利用し，VIP_{CN} から DC_{CN} の FQDN を取得する．続けて DNS 正引きを行い，DC_{CN} の IP アドレスを取得する．

NTM Infomation Request を受信した DC_{CN} は，C においてメッセージに記載されている情報をキーとしてデータベースを検索する．ここでも，仮想 IP アドレスから端末情報を取得できるよう DC の拡張を行う．すなわち，VIP_{CN} をキーとして CN の端末情報を取得する．その後，NTM Infomation Response に取得した情報を記載し DC_{MN} へ応答する．

C から D までの処理は通常の NTMobile の動作と同様である．トンネルに必要な情報を交換し，トンネルを構築する．

D において，トンネル構築が正常に構築できると，MN が保持していた SIP 200 OK をアプリケーションに通知する．MN は SIP ACK を SIP INVITE と同様の経路で CN に送信する．以後は，NTMobile のトンネルによりエンドエンドのメディアセッションが可能になる．

5. 実装

提案方式を Linux に実装を行った．ディストリビュージョンは Ubuntu10.04，カーネルバージョン 2.6.32-24-generic を使用した．実装は NTM 端末と DC について行った．

図 9 に NTM 端末のモジュール構成を示す．提案方式を実現するため，NTMobile 独自のデーモンに SIP 通信のみで使用するモジュールの追加を行った．SIP 通信は UDP

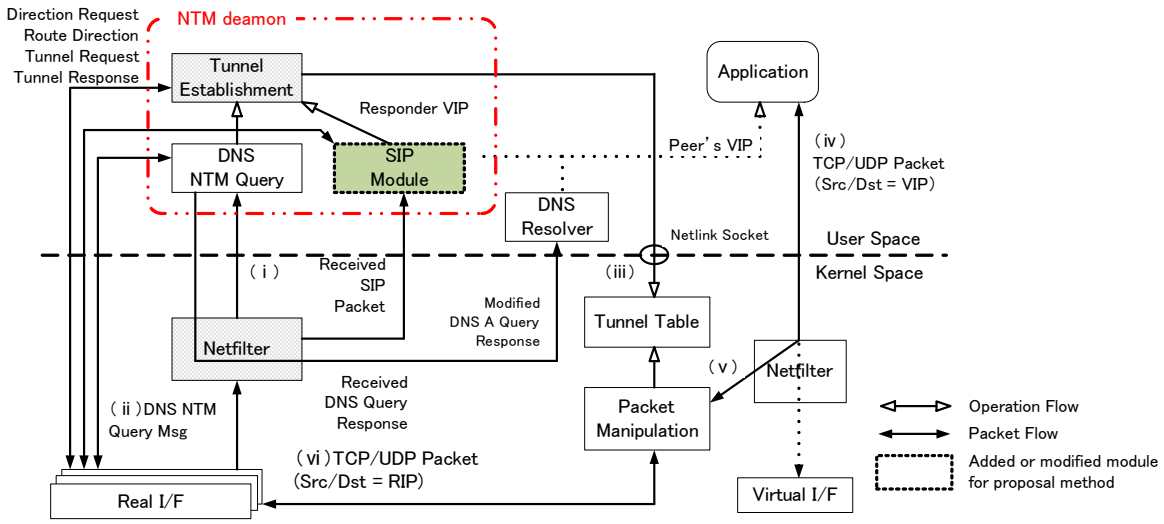


図 9 NTM 端末のモジュール構成

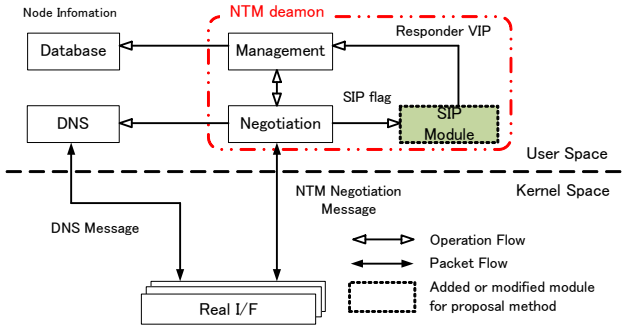


図 10 DC のモジュール構成

上で動作し，デフォルトポートは 5060 番となっている．そこで，カーネルモジュールに受信したパケットの UDP ポートが 5060 番の時にフックする処理を追加した．カーネルモジュールでフックした SIP パケットを新規に作成した SIP 通信専用のモジュールに渡す．ここで，解析を行いパケットが SIP 200 OK かつメディアセッションの情報が含まれていた場合，メッセージに含まれている仮想 IP アドレスを抽出する．抽出した通信相手の仮想 IP アドレスを NTM Direction Request の拡張ヘッダに記載する．NTM Direction Request には通信開始側と受信側の FQDN が記載されているが，これに仮想 IP アドレスの情報を付加できるように NTMobile 独自のヘッダに追加した．

図 10 に DC のモジュール構成を示す．これまでの DC では，NTM Direction Request に含まれている通信相手の FQDN から，トンネルに必要な情報の取得に使用していた．提案方式では，FQDN を取り扱わないため，DC の NTMobile デーモンに SIP 通信のみで使用するモジュールを新規に作成し追加した．NTM Direction Request に SIP 専用のフラグを立てることで処理を分岐し，仮想 IP アドレスを FQDN の代わりに用いることでトンネル構築に必要な情報を取得する．また，NTM Infomation Request の宛て先を見つけるため，仮想 IP アドレスを DNS 逆引きおよび正引きする処理を追加した．これにより，仮想 IP アドレスを管理している DC の IP アドレスを取得できる．

6. 評価

6.1 動作検証

提案方式がアドレス不整合問題を解決できていることを確認するため，既存の SIP アプリケーションを用いて NAT を含めたネットワークを構築し動作検証を行った．**図 11** に試験ネットワークの構成を示す．1 台の実機 PC 上にインストールした VMware6.0 を利用して，NTM 端末 3 台および DC2 台，NAT を仮想マシンとして構築した．NTM 端末 1 台に SIP サーバアプリケーションをインストールし，SIP サーバとして扱う．NTM 端末 1 台と DC2 台，SIP サーバと NAT を同一ネットワークに接続し，NTM 端末 1 台を NAT 配下へ接続した．MN と CN は同じ SIP サーバを使用する．NTM 端末の MN から NAT 配下に存在する NTM 端末 CN へ通信を開始する．

SIP クライアントは Linux で動作するフリーソフト Jitsi[15] を使用した．SIP サーバアプリケーションには一般に使用されているフリーソフトの Asterisk[16] を選択した．上記の環境にて，SIP で開始する IP 電話を実行した．Wireshark[17] を用いてパケットをキャプチャし，IP 電話が NAT を越えて通信できたことを確認した．また，マイクおよびヘッドホンを用いて正常に音声通話が開始できることを確認した．

6.2 既存技術との比較

STUN と TURN を既存技術の代表としてとりあげ，提案方式との比較を行った結果を表 1 に示す．

- アドレス不整合問題の解決

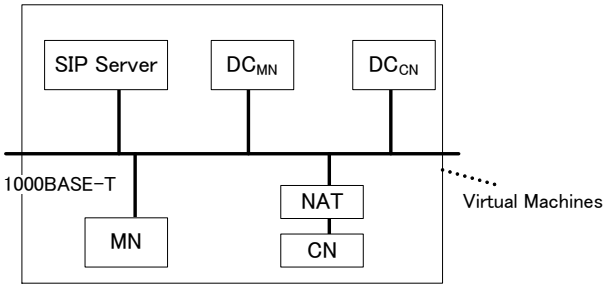


図 11 試験ネットワークの構成

表 1 既存技術と提案方式の比較

	STUN	TURN	提案方式
アドレス不整合問題の解決	△	○	○
SIP アプリケーションの改造	×	×	○
移動通信への対応	×	×	○
SIP サーバの改造	○	○	△

STUN は，NAT が Symmetric NAT の場合は使用することができない．TURN は中継装置を用い，提案方式は仮想 IP アドレスを使用することで，それぞれ NAT の種類に依存せず通信を行うことができる．

- SIP アプリケーションの改造
  STUN および TURN は，SIP クライアントを改造する必要がある．また，ユーザは使用する STUN や TURN のサーバを各々設定する必要があり，ユーザがこれらの技術を意識しなければならない．提案方式では，SIP クライアントは NTMobile を意識する必要がなく，既存のものをそのまま流用することができる．
- 移動通信への対応
  STUN および TURN は，端末の移動を想定していないため，端末の IP アドレスが変化すると再度 IP アドレスを取得しなければならず，メディアセッションを継続することができない．提案方式では，NTMobile の移動透過性をそのまま活かすことができ，端末の IP アドレスが変化した場合は再度トンネル構築処理を行い，通信を継続させることができる．
- SIP サーバの改造
  STUN および TURN は，既存の SIP サーバをそのまま使用できる．提案方式では，NTMobile を導入する必要がある．しかし，SIP サーバのアプリケーションは手を加える必要がないため，NTMobile の導入のみで実現できる．

7. まとめ

本論文では，NTMobile の拡張を行うことにより，既存の SIP アプリケーションや NAT に一切の手を加えずに SIP 通信を行う方式について提案を行った．SIP サーバに NTMobile を導入し，仮想 IP アドレスを識別可能とした．また，メディアセッションを NTM 端末間で行うために NTMobile に機能追加を行い，SIP 通信中に NTMobile のネゴシエーションを行うよう拡張した．さらに，提案方式を実装し，動作確認を行った．

今後は，実ネットワーク上環境において実装したシステムの詳細な性能評価を行う．NTM 端末が異なる NAT 配下に存在する場合および，ハンドオーバ時の動作検証も進めていく．また，測定を行い性能評価を進める．

謝辞 本研究は，SCOPE/PREDICT の委託研究に基づく結果である．

参考文献

[1] J.Livingood : Considerations for Transitioning Content to IPv6，RFC6589，IETF（2012）.
[2] I.Yamagata, S.Miyakawa, A.Nakagawa, H.Ashida : Common Requirements for Carrier-Grade NATs（CGNs）, RFC6888，IETF（2013）.
[3] Forum，U. : Internet Gateway Device (IGD) Standardized Device Control Protocol V 1.0（2001）.
[4] 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）.
[5] 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）.
[6] Levkowetz，H.，and Vaarala，S. : Mobile IP Traversal of Network Address Translation（NAT）Devices，RFC 3519，IETF（2003）.
[7] 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）.
[8] 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）.
[9] 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）.
[10] 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，情報処理学会論文誌，Vol.54，No.1，pp.367-379（2013）.
[11] 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，情報処理学会論文誌，Vol.54，No.1，pp.380-393（2013）.
[12] 上酔尾一真，鈴木秀和，内藤克浩，渡辺　晃 : IPv4/IPv6 混在環境で移動透過性を実現する NTMobile の実装と評価，マルチメディア，分散，協調とモバイル（DICOMO2012）シンポジウム論文，Vol.2012，No.1，pp.1169-1179，Jul.2012.
[13] Rosenberg，J.，Mahy，R.，Matthews，P.，and Wing，D. : Session Traversal Utilities for NAT（STUN），RFC 5389，IETF （2008）.
[14] Mahy，R.，Matthews，P.，and Rosenberg，J. : Traversal Using Relays around NAT（TURN），RFC 5766，IETF (2010).
[15] http://www.jitsi.org
[16] Asterisk IP PBX,VOIP Gateway,IVR & Open Source Communications．http://www.asterisk.org
[17] Wireshark. http://www.wireshark.org.

NTMobileにおける SIP通信方式の提案と実装

†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‡，渡邊晃†

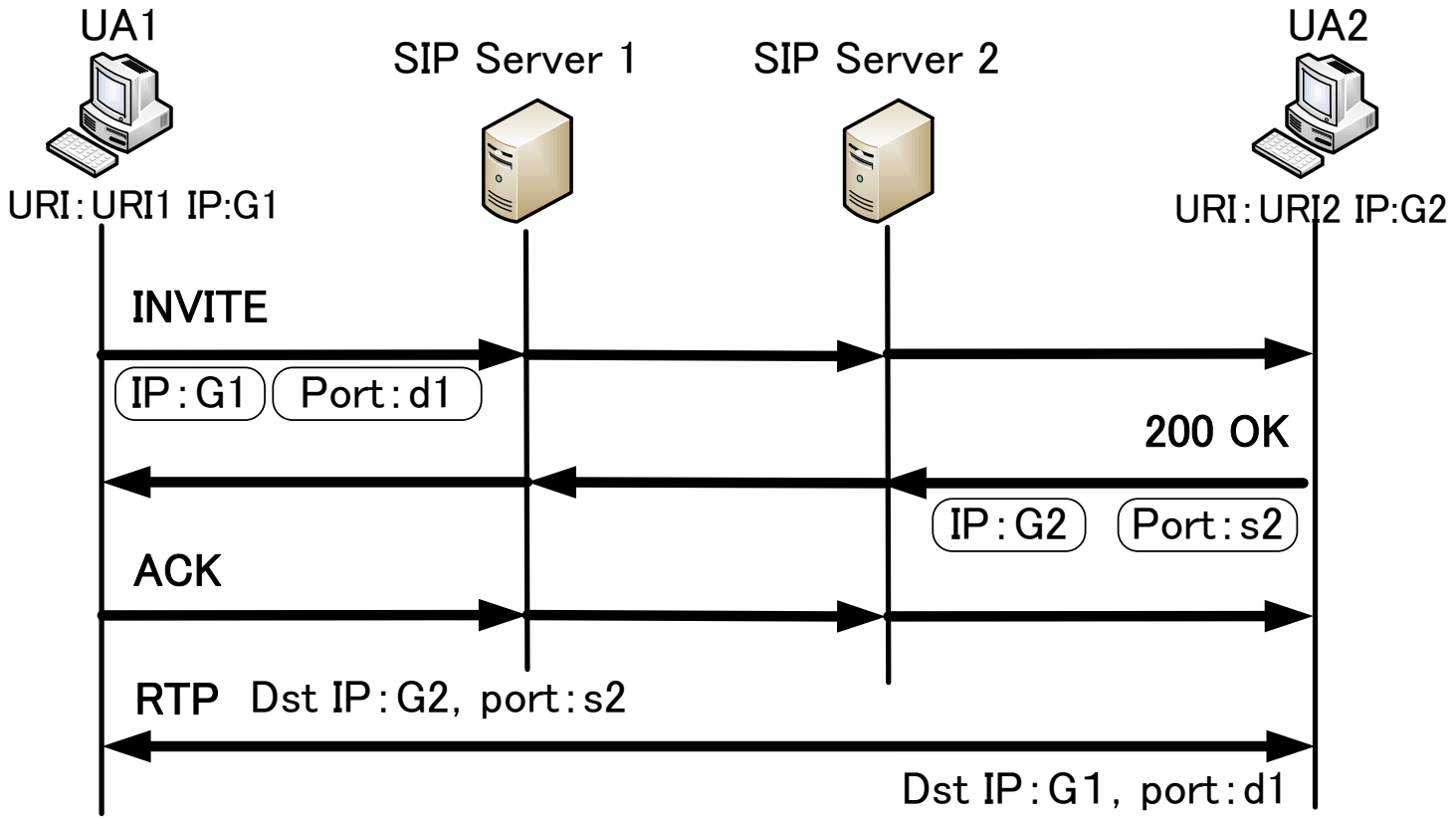
研究背景

- 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
  - 端末間のメディアセッションは直接行われる
  - 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

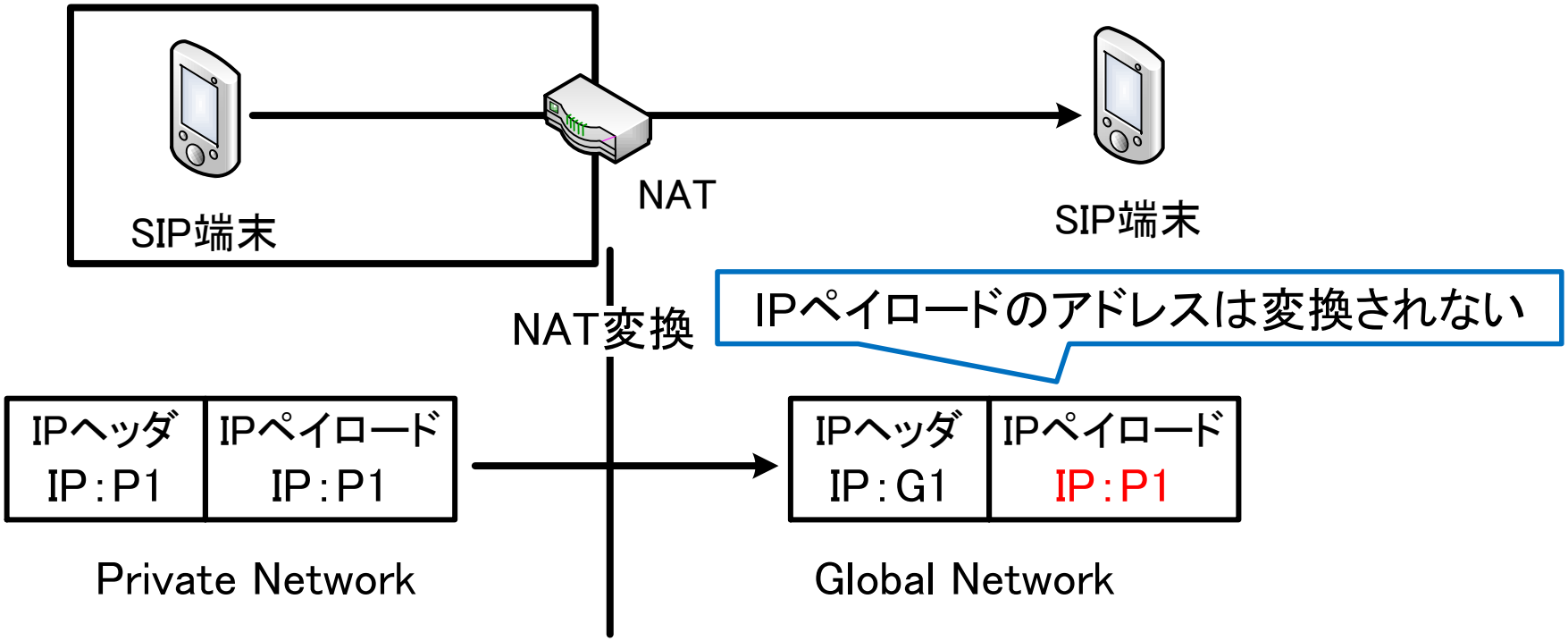
- 通信の開始，通信の切断を行うために使用するプロトコル
- SIPメッセージで，メディアセッションで使用する情報を交換
- メディアセッションは端末間で直接行う



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

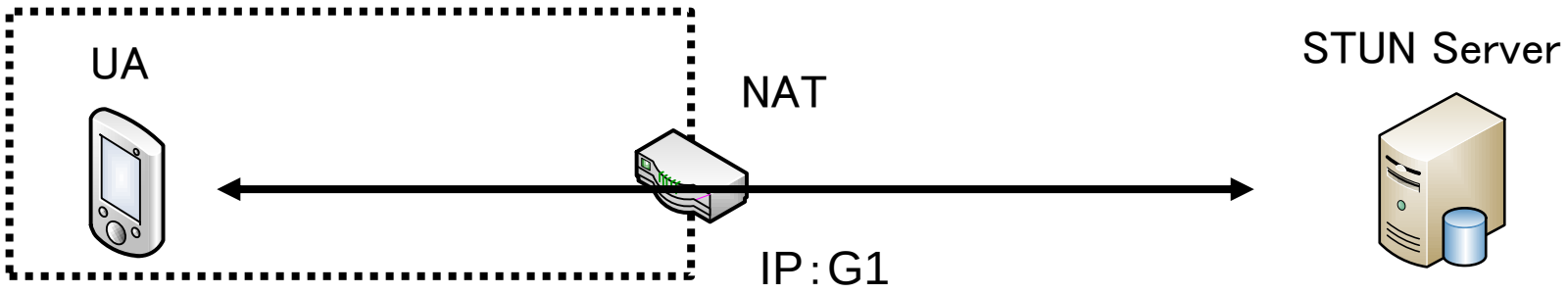


既存技術

- アプリケーション改造手法
  - アプリケーション改造および第3の装置を必要とする
  - NATの外側IPアドレスもしくは中継サーバのIPアドレスを取得し，SIPメッセージに書き込む
  - STUN，TURN
- NAT改造手法
  - NATの改造を行う
  - NATにおいて、SIPメッセージに含まれるIPアドレスをNATの外側IPアドレスに書き換える
  - SIP-ALG

STUN

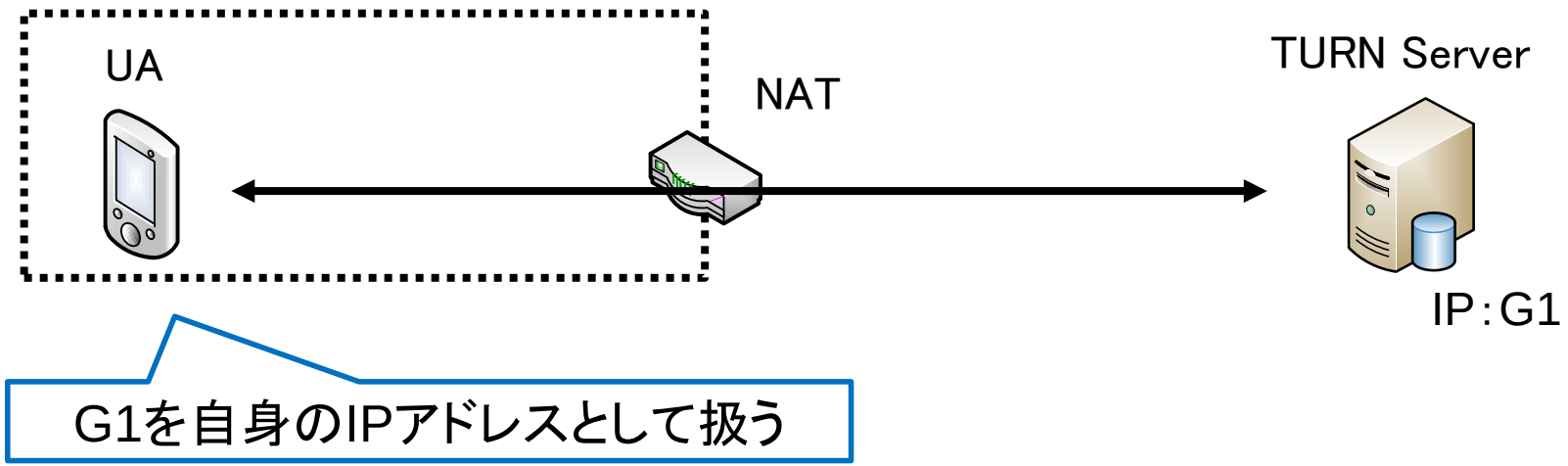
- STUN（Session Traversal Utilities for NAT）
  - SIP通信前にSTUNサーバと通信し，NATの外側IPアドレスを取得する
  - 取得したIPアドレスをSIPメッセージに書き換える
- 利点
  - SIP通信前以外は従来のSIP通信と同様であり，オーバヘッドが少ない
- 欠点
  - NATの種類によっては，使用することができない
  - アプリケーションがSTUNに対応しなければならない



G1を自身のIPアドレスとして扱う

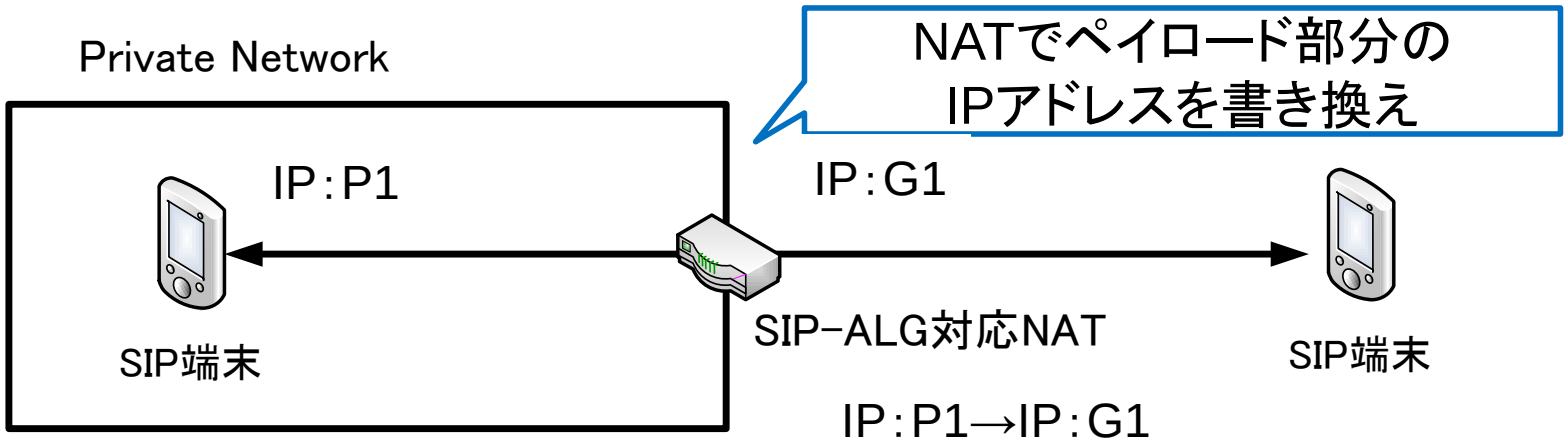
TURN

- TURN（Traversal Using Relays around NAT）
  - SIP通信前にTURNサーバと通信し，TURNサーバのIPアドレスを取得する
  - 取得したIPアドレスをSIPメッセージに書き換える
- 利点
  - NAT種類関係なく，SIP通信を行うことができる
- 欠点
  - SIP通信およびメディアセッションは全てTURNサーバを経由するため，スループットが低下する



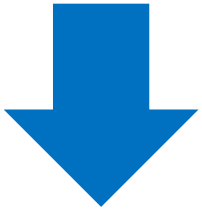
SIP-ALG

- 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



既存技術の課題

- アプリケーション改造手法
  - SIP端末が別ネットワークに移動すると再度IPアドレスを取得する必要がある
  - メディアセッション中の移動によるIPアドレスの変化に対応できない
- NAT改造手法
  - SIP端末が非対応のNAT配下に移動すると使用できない
  - 既存のNATに手を加えることは難しい



NATに依存せずかつIPアドレスの変化に対応した技術が必要

NTMobile

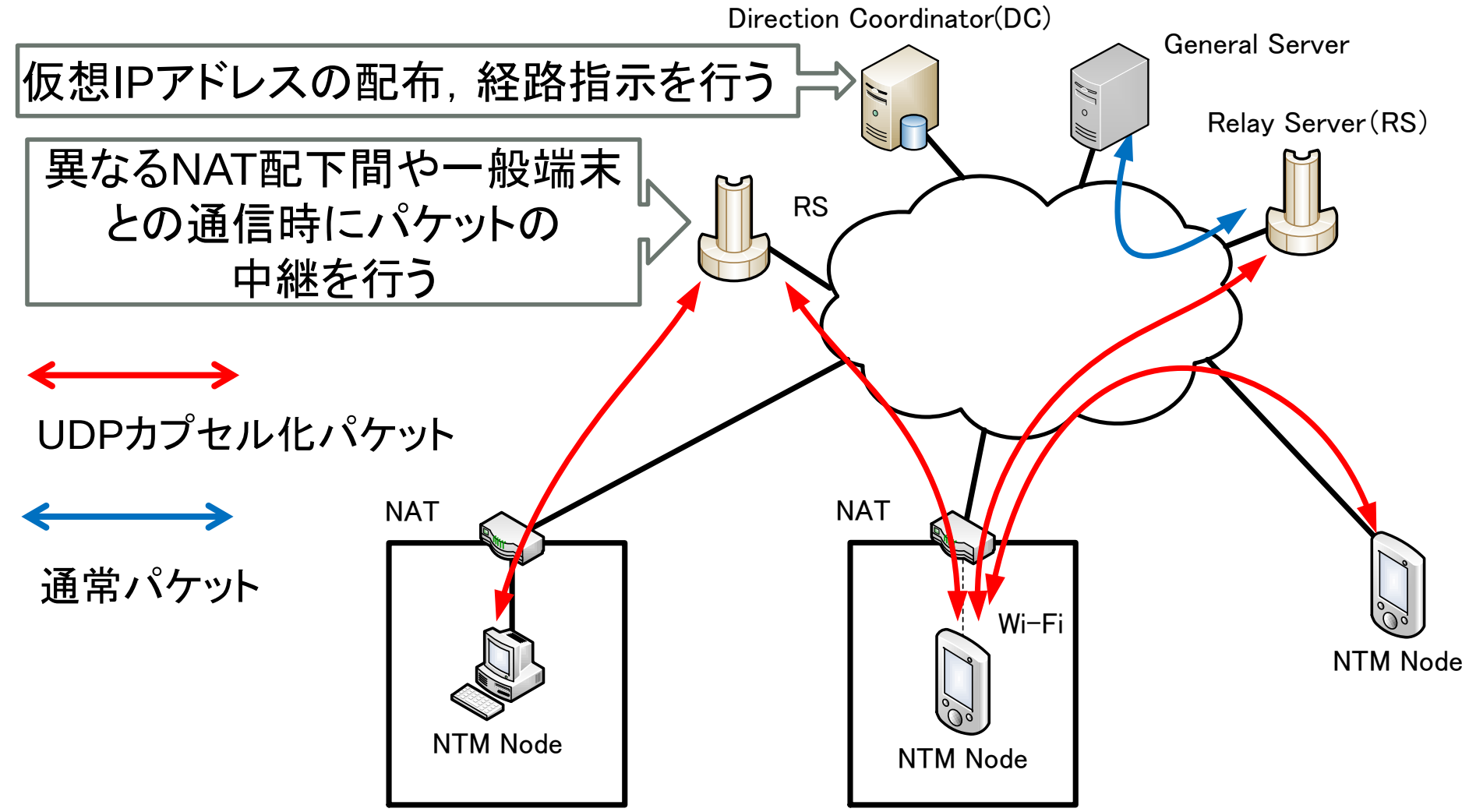
- NTMobile(Network Traversal with Mobility)
  - 端末を一意に識別する仮想IPアドレスを導入
  - 全てのパケットを実IPアドレスでカプセル化
  - 実IPアドレスの変化を隠蔽
  - NATに改造を加えずに実現が可能

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

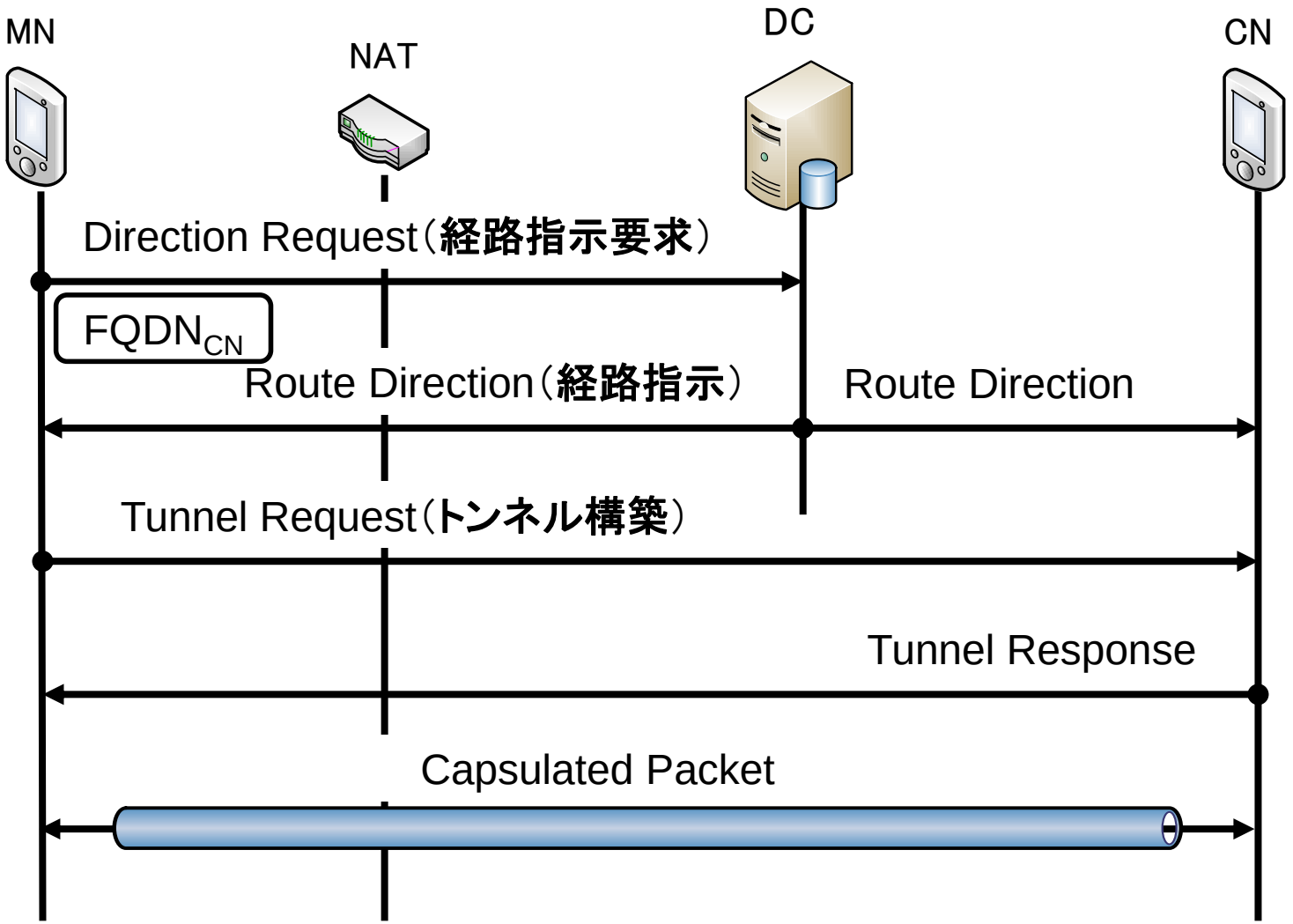
仮想IPアドレスの配布，経路指示を行う

異なるNAT配下間や一般端末との通信時にパケットの中継を行う



NTMobileの通信シーケンス

- 通信相手の名前解決をトリガとして動作を開始する



NTMobileにおけるSIP通信の課題

- NTM端末のアプリケーションは仮想IPアドレスを自端末のIPアドレスとして認識する
- SIPパケットには仮想IPアドレスが含まれる

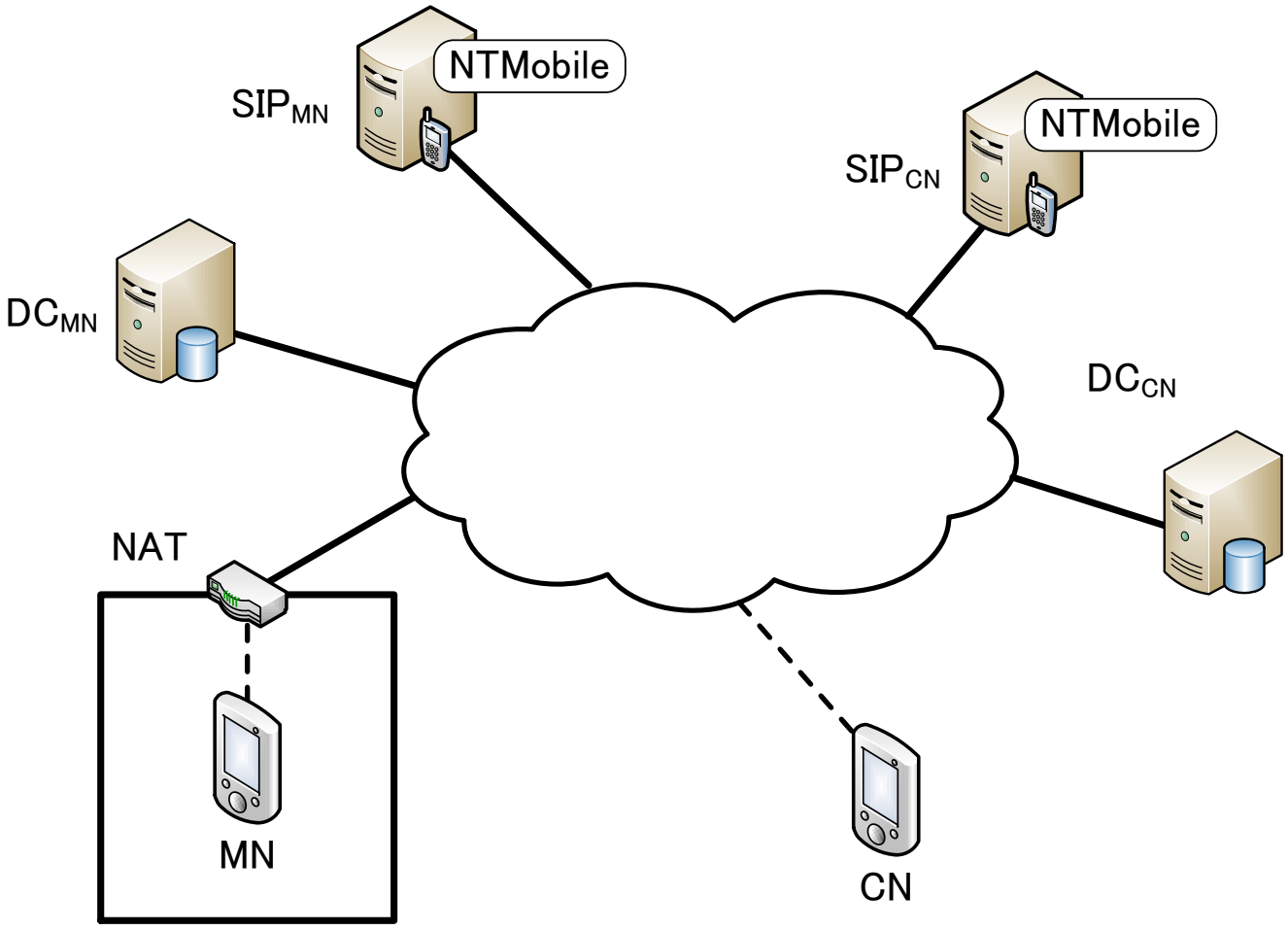
既存のSIPサーバでは仮想IPアドレスを認識できない

提案方式

- SIPサーバにNTMobileを導入し，NTM端末として扱う
  - SIPサーバに仮想IPアドレスを認識させる
- NTMobileのみ拡張を行う
  - メディアセッション前にNTM端末間のトンネル構築を行う必要がある
- 既存のSIPアプリケーションおよびNATには手を加えずSIP通信を実現する

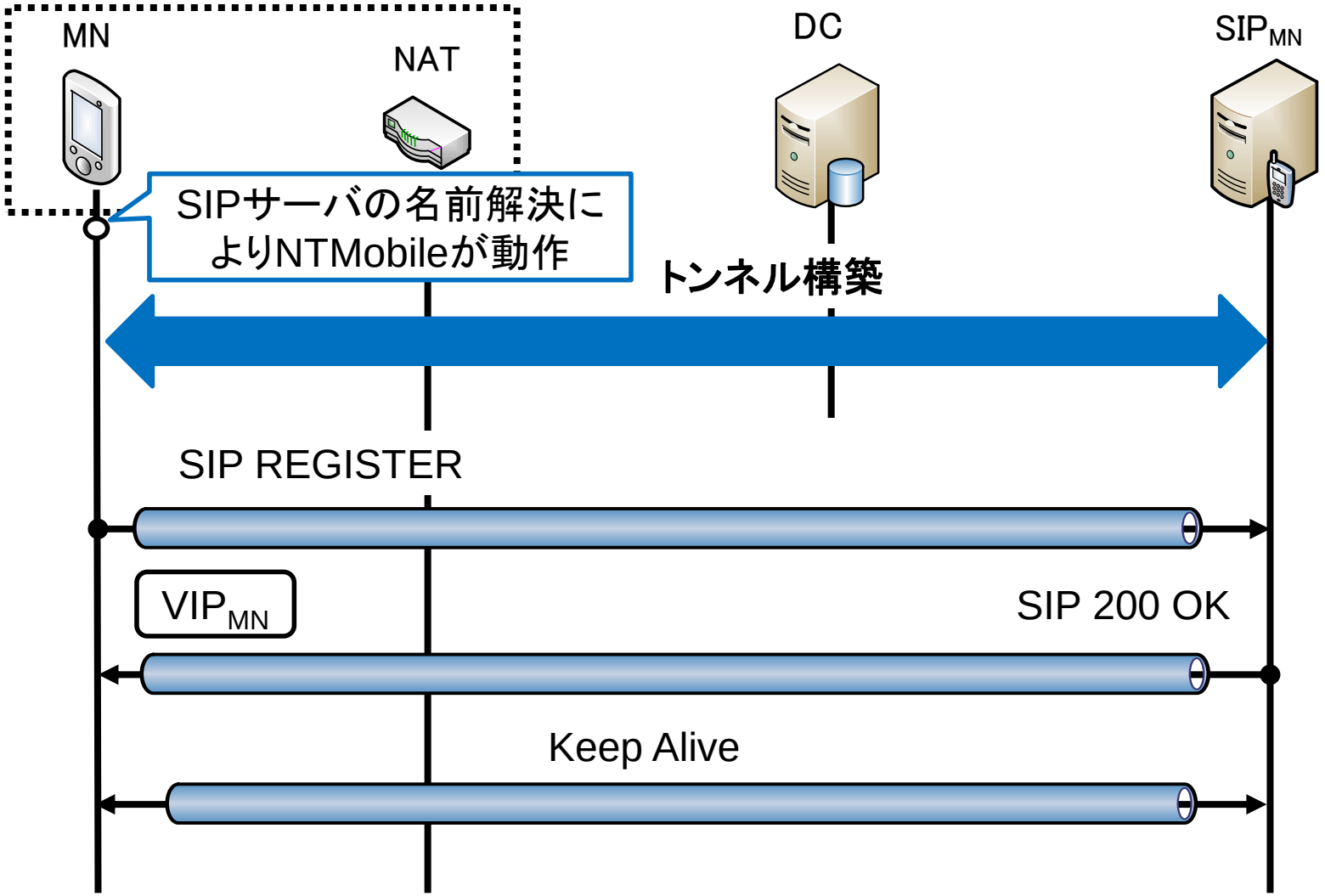
ネットワーク構成

- MNを除いた全ての機器はグローバル上に存在するものとする



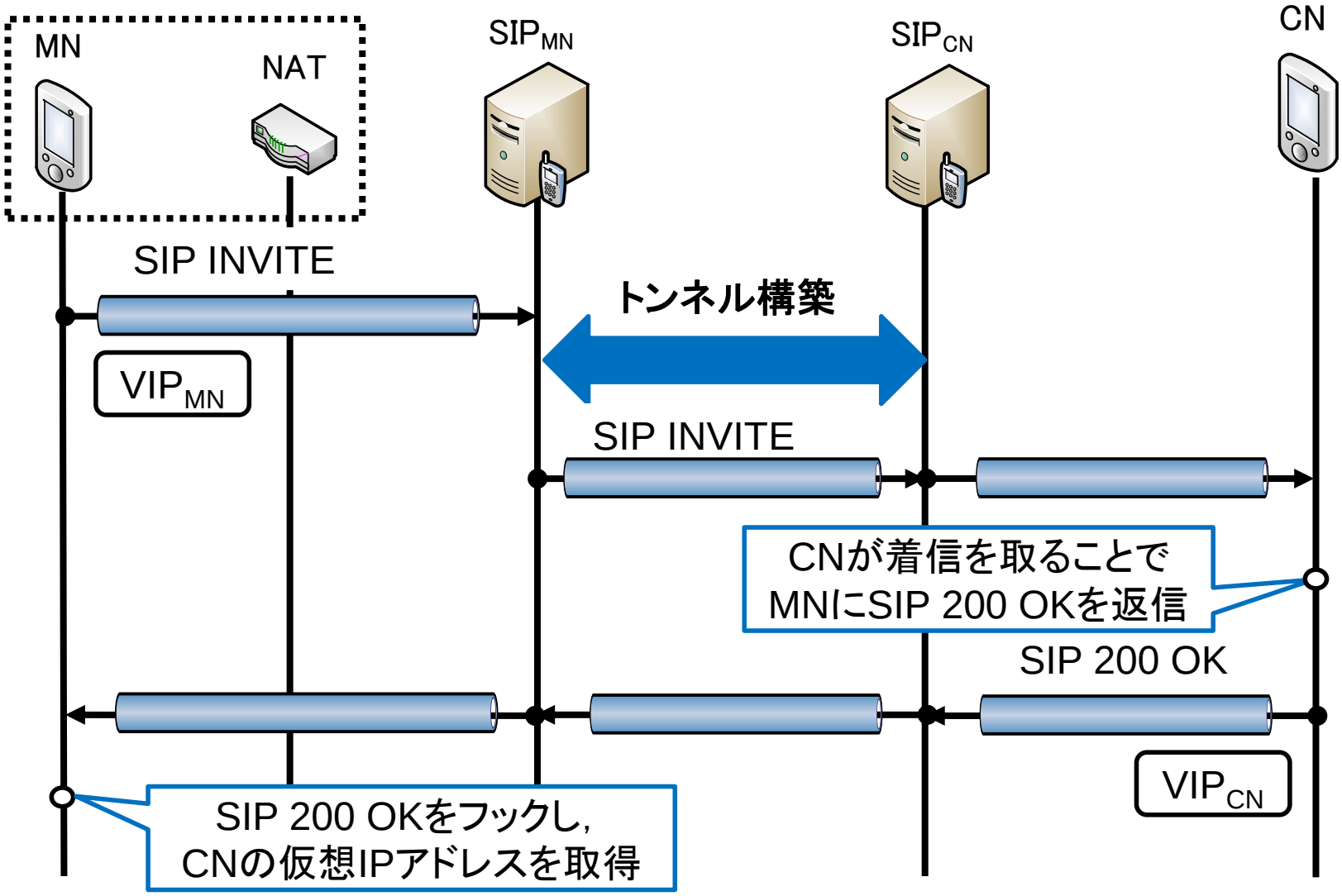
提案方式のSIP登録シーケンス

- SIPサーバとトンネルを構築し，仮想IPアドレスを登録する



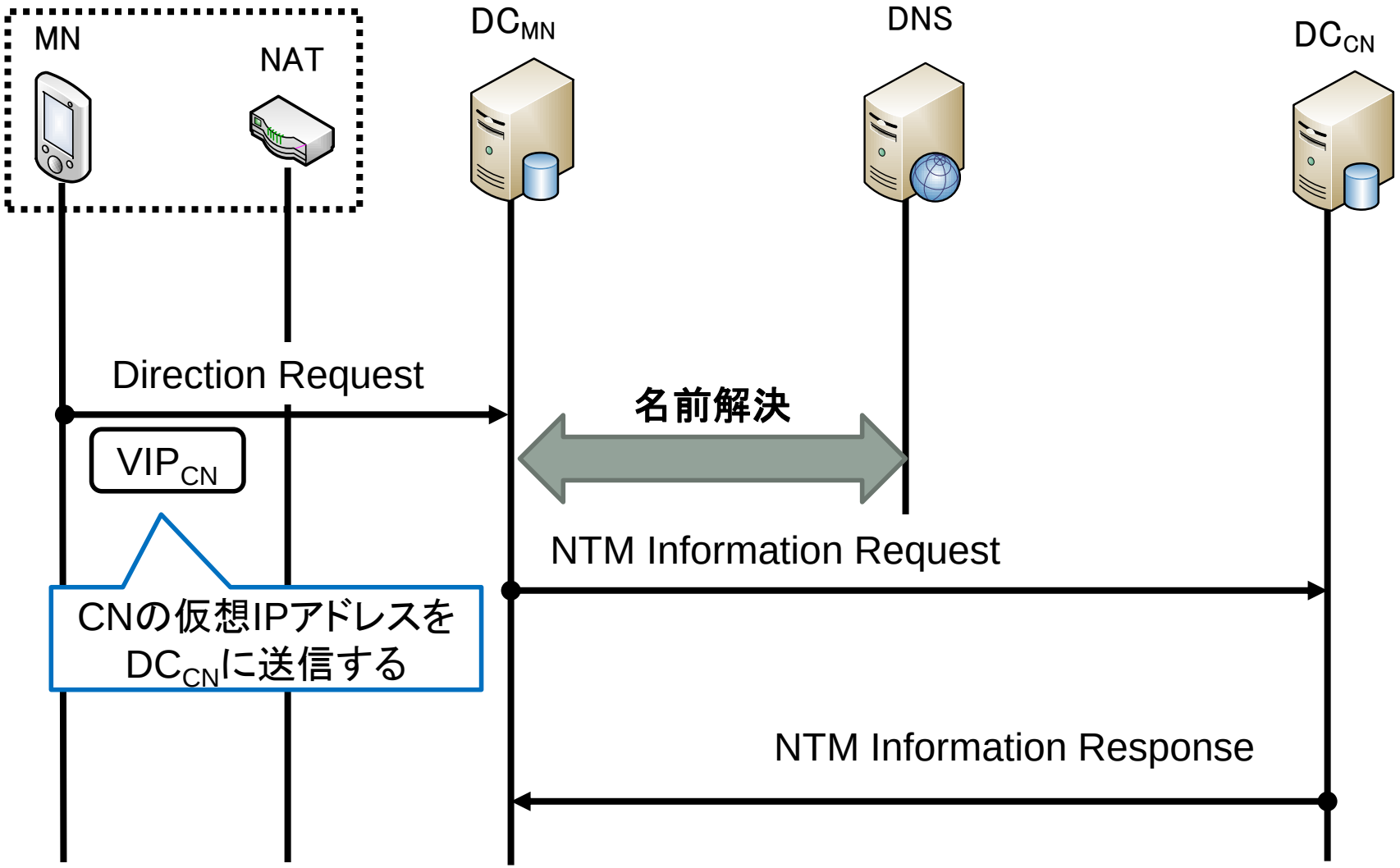
提案方式のSIP通信シーケンス1

- MNがCNにSIP INVITEを送信し，CNが応答する



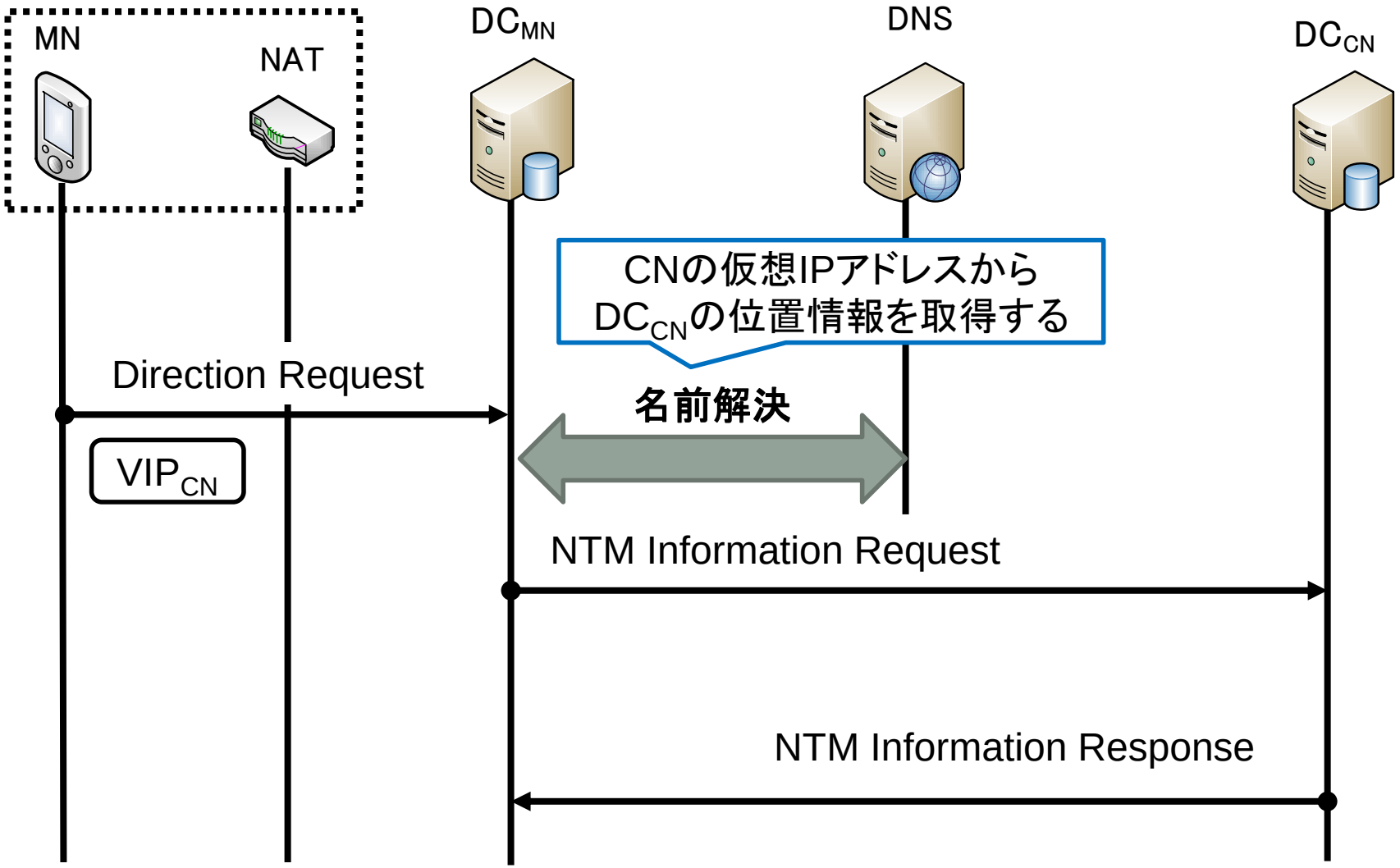
提案方式のSIP通信シーケンス2

- 通信相手の仮想IPアドレスをDCに送信する



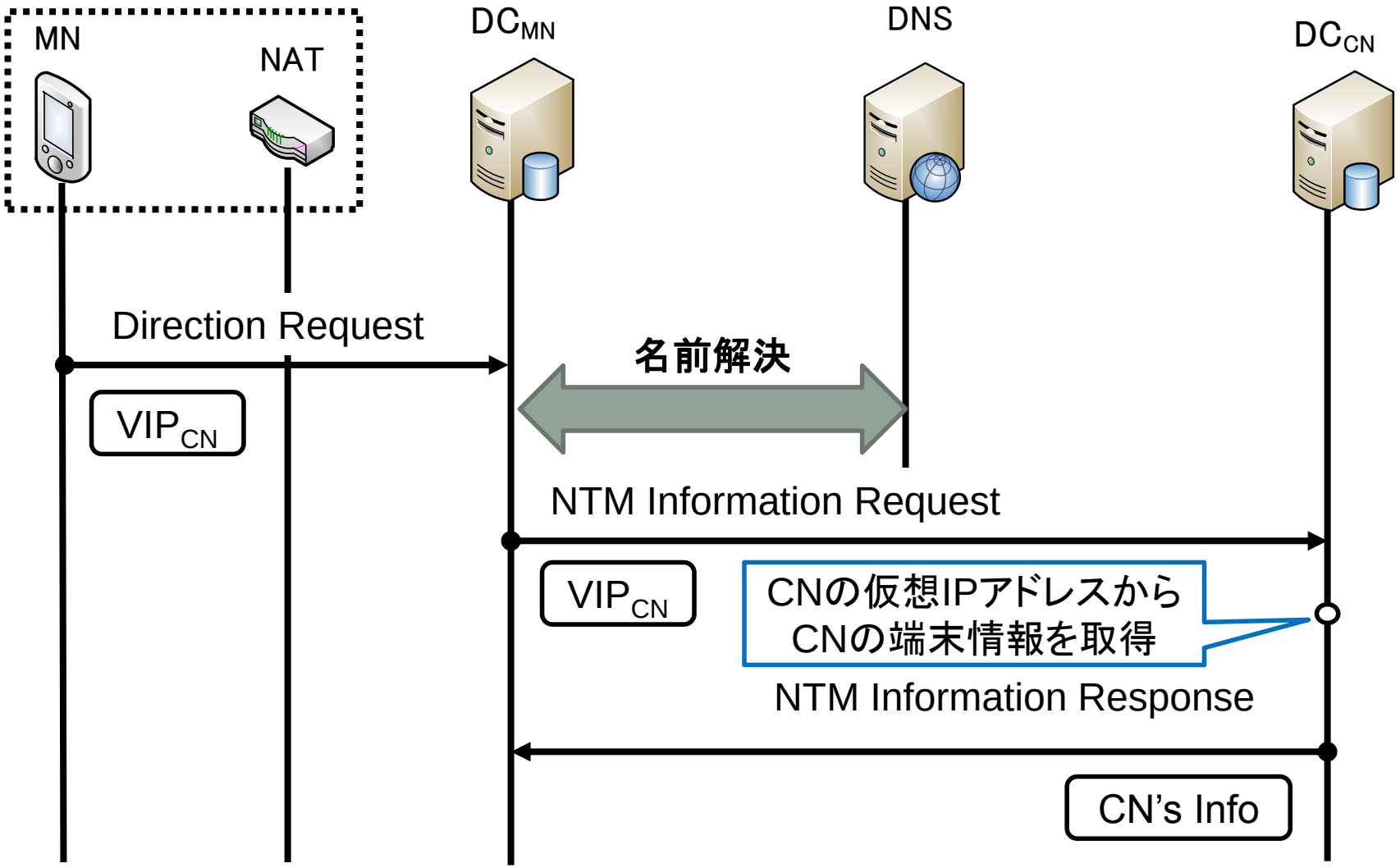
提案方式のSIP通信シーケンス3

- 通信相手の仮想IPアドレスの名前解決を行う



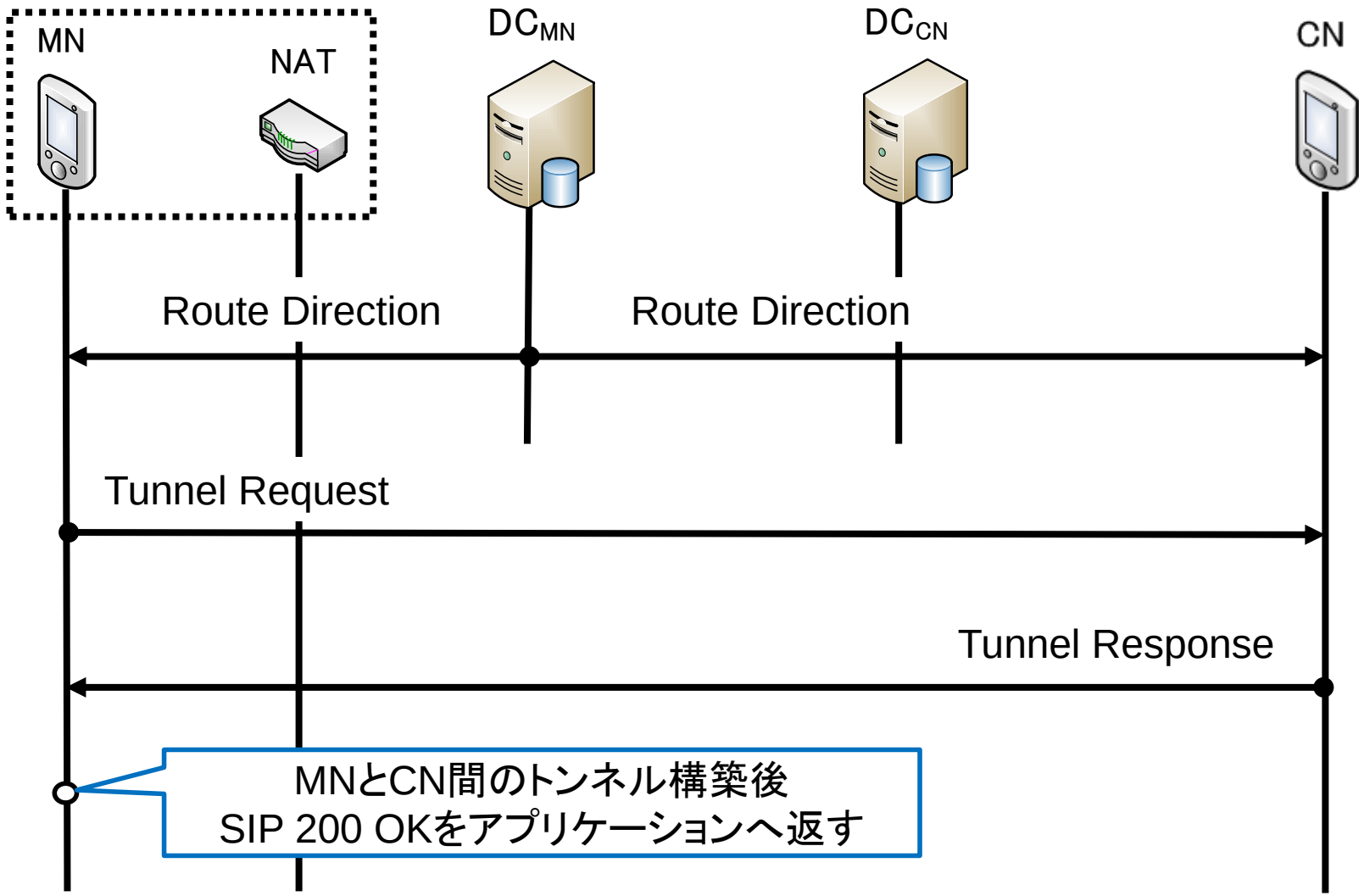
提案方式のSIP通信シーケンス4

- 仮想IPアドレスから端末情報を取得する



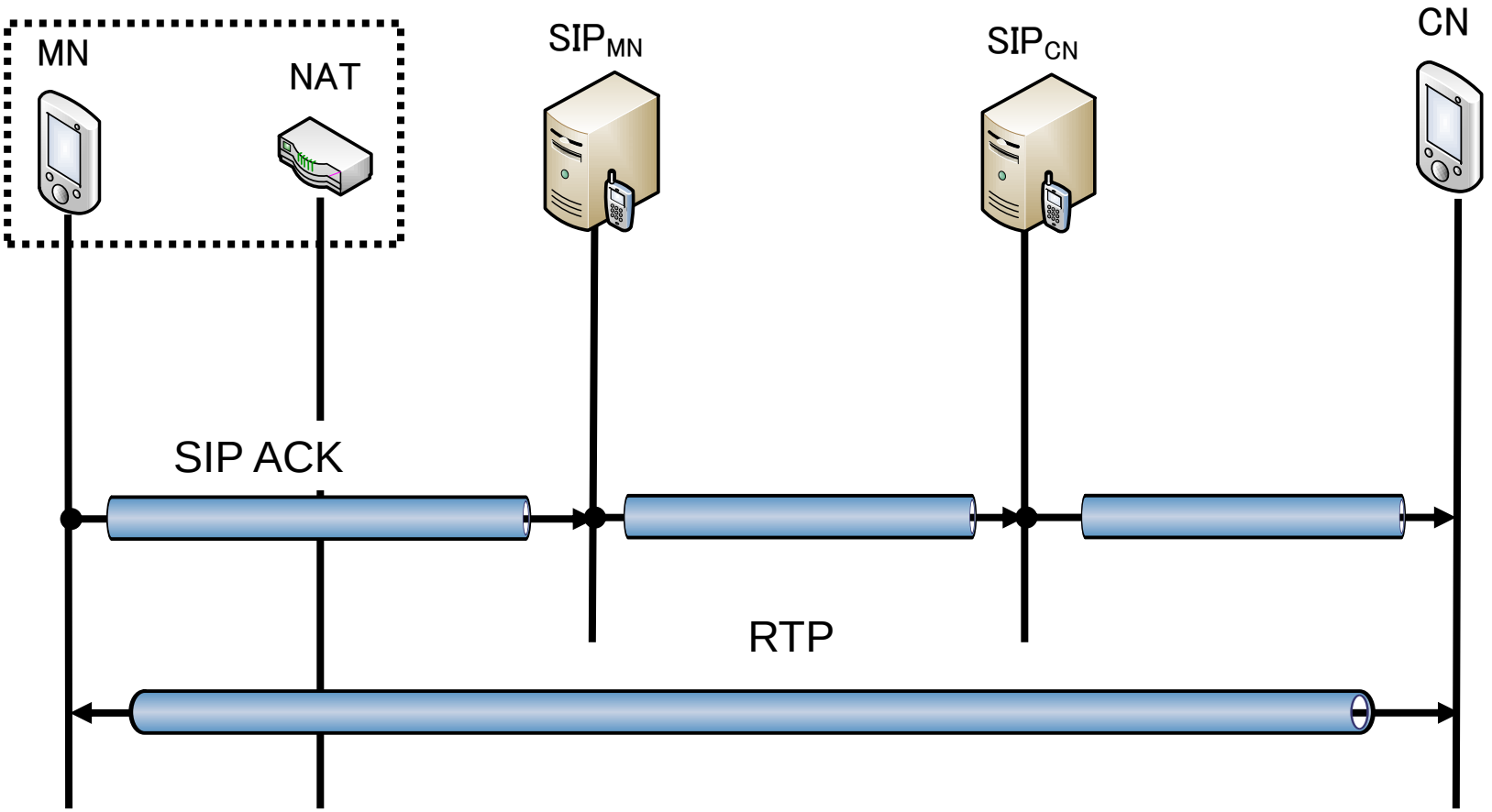
提案方式のSIP通信シーケンス5

- 取得した端末情報を元にトンネルを構築する



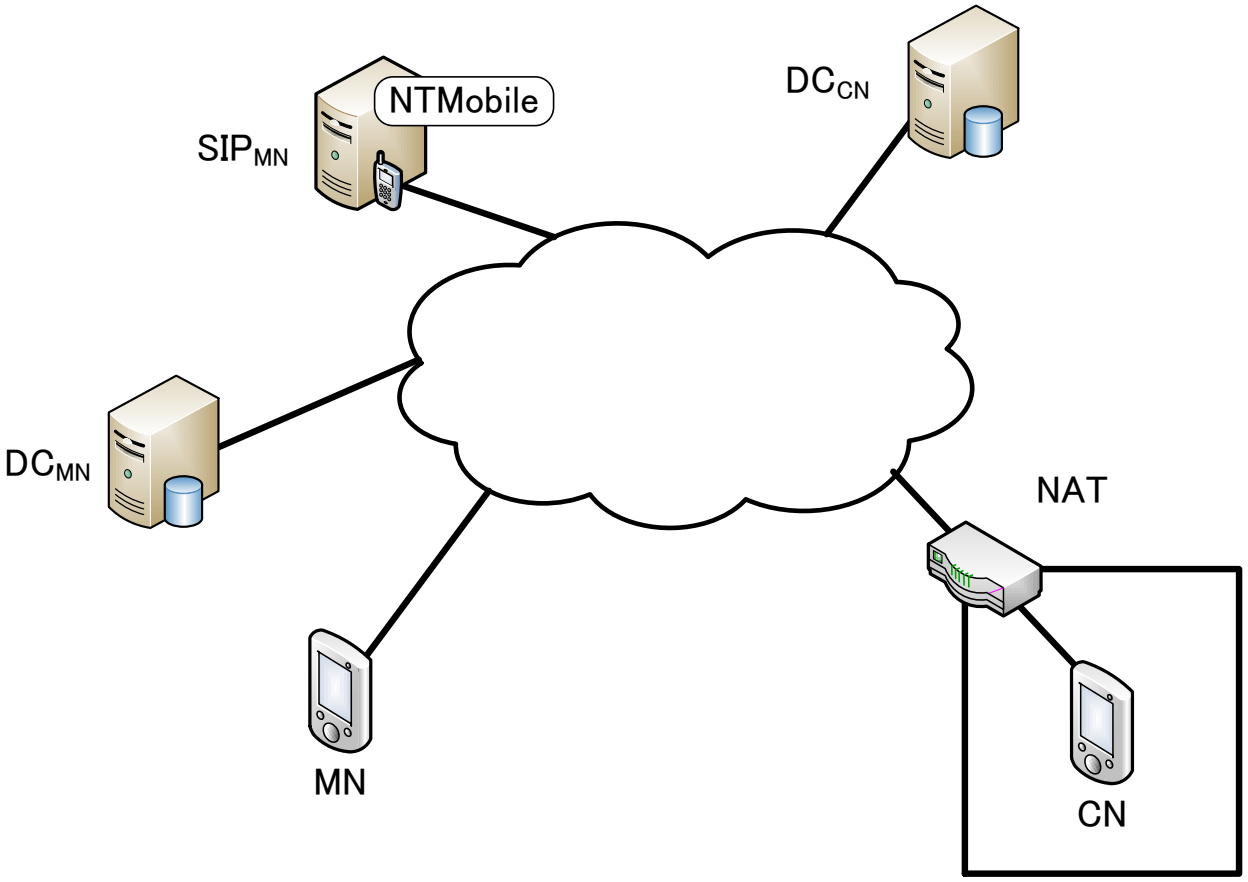
提案方式のSIP通信シーケンス6

- SIP ACKを送信し，メディアセッションをトンネル経路で開始



実装

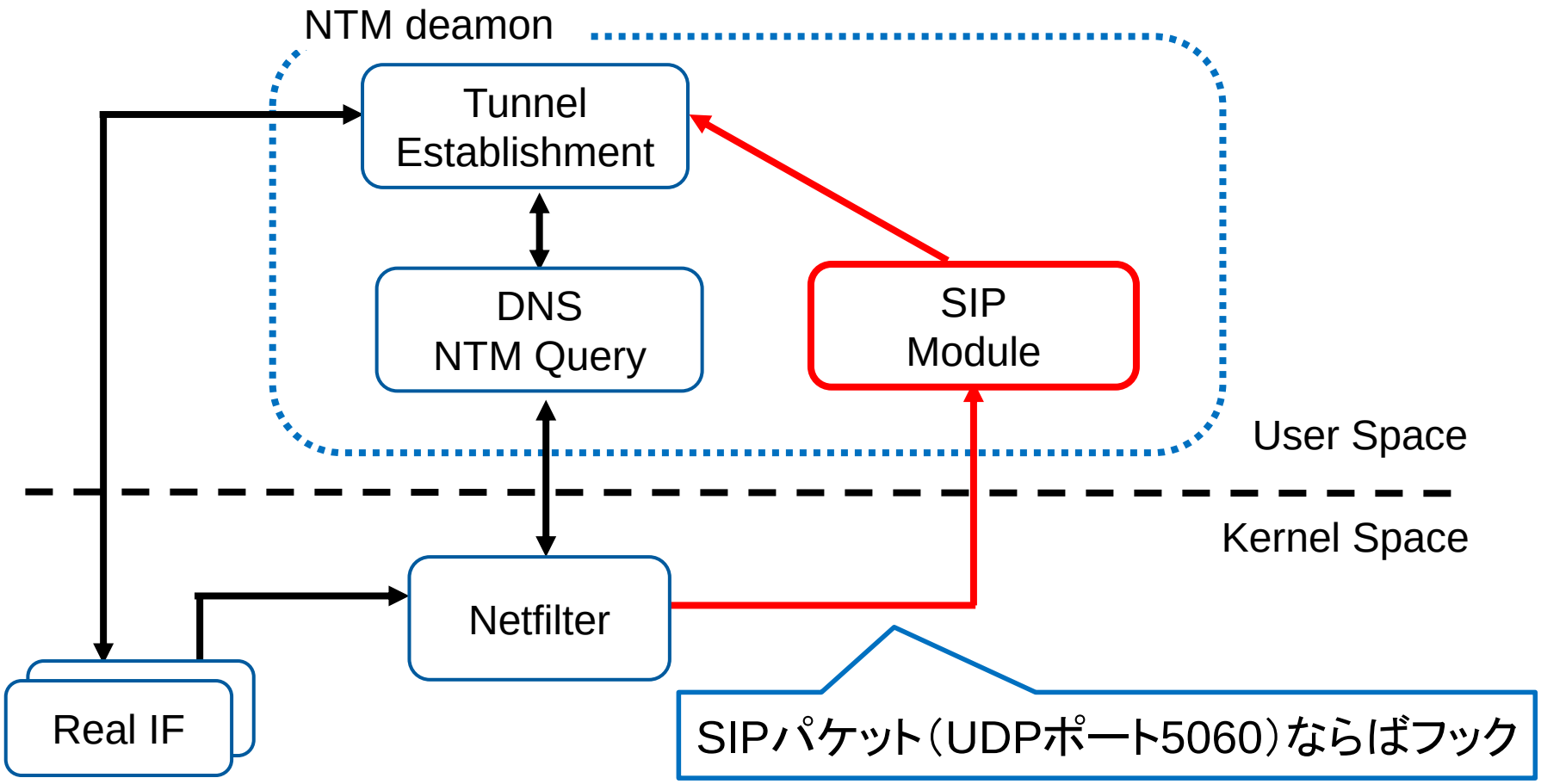
- 仮想マシンを6台構築し，NTM端末とDCに提案方式を実装
- 一般に使用されているSIPクライアント*とSIPサーバ**を使用



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

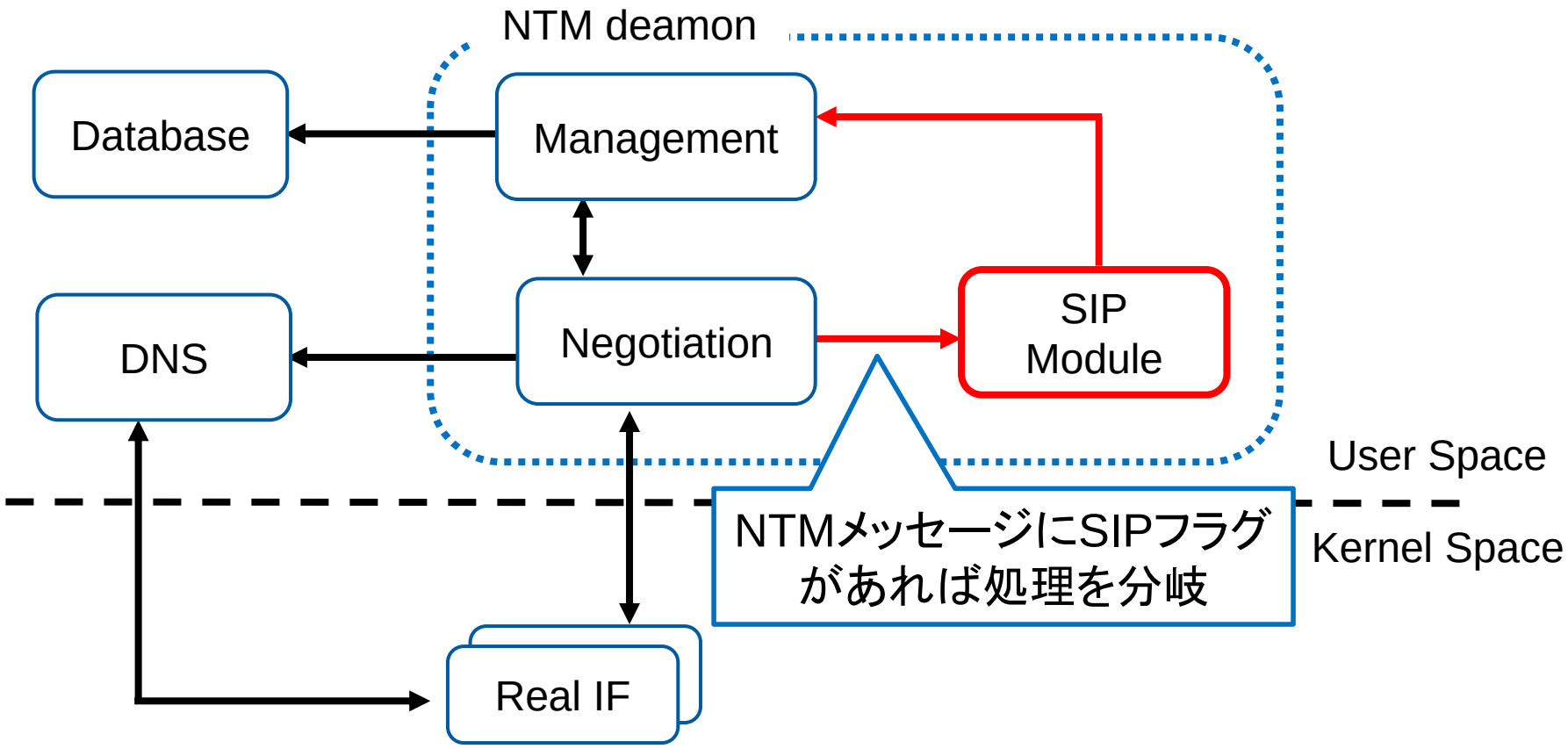
NTM端末のモジュール構成図

- NTMデーモンにSIP専用のモジュールを追加
- カーネルモジュールにSIPパケットフック処理を追加



DCのモジュール構成図

- NTMデーモンにSIP専用のモジュールを追加
- NTMメッセージにSIPフラグを追加

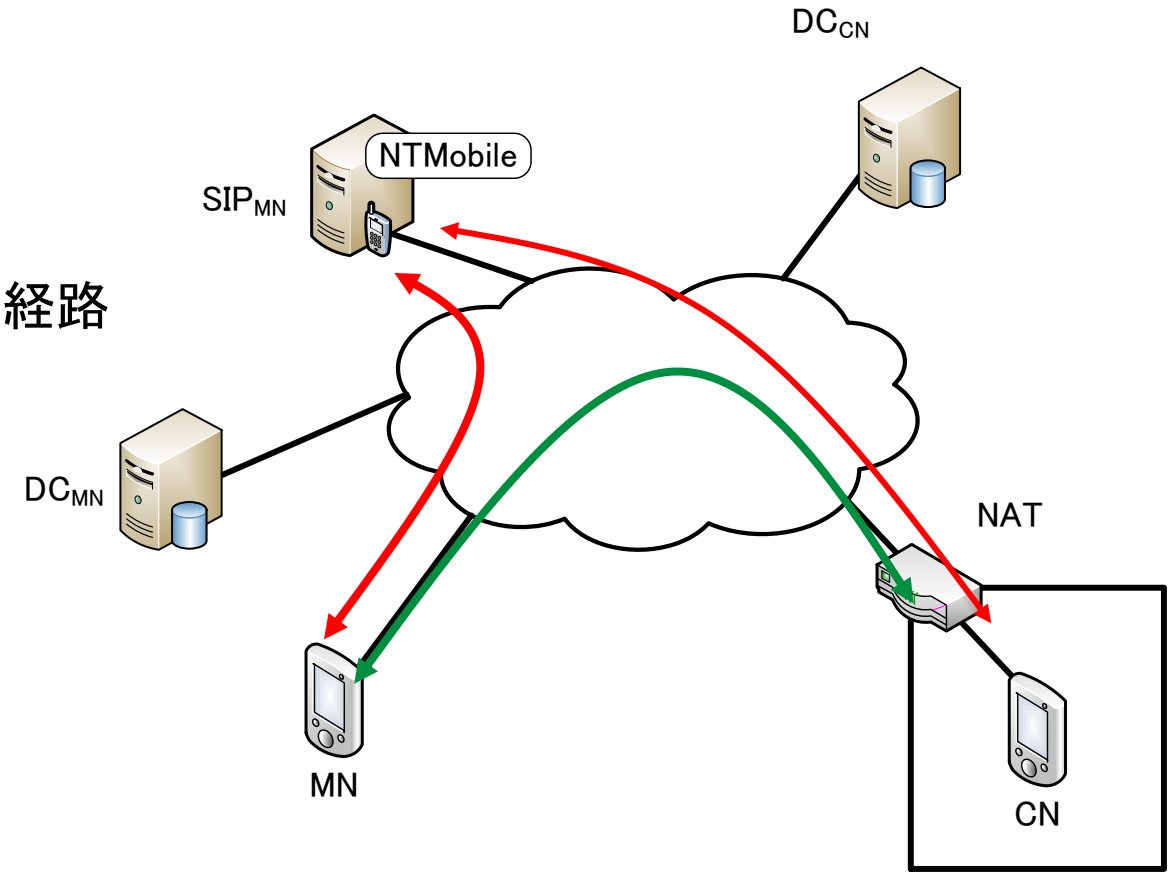


動作検証

- 提案方式および既存のSIPアプリケーションの動作確認
- MNからCNへIP電話を実行
- パケットキャプチャーし，提案方式が動作したことを確認

SIP通信経路

メディアセッション経路



定性評価

	アプリケーション改造手法	NAT改造手法	提案方式
NAT越えの解決	○	○	○
移動通信の対応	×	×	○
SIPアプリケーションの改造の必要性	×	○	○
SIPサーバの改造の必要性	○	○	△

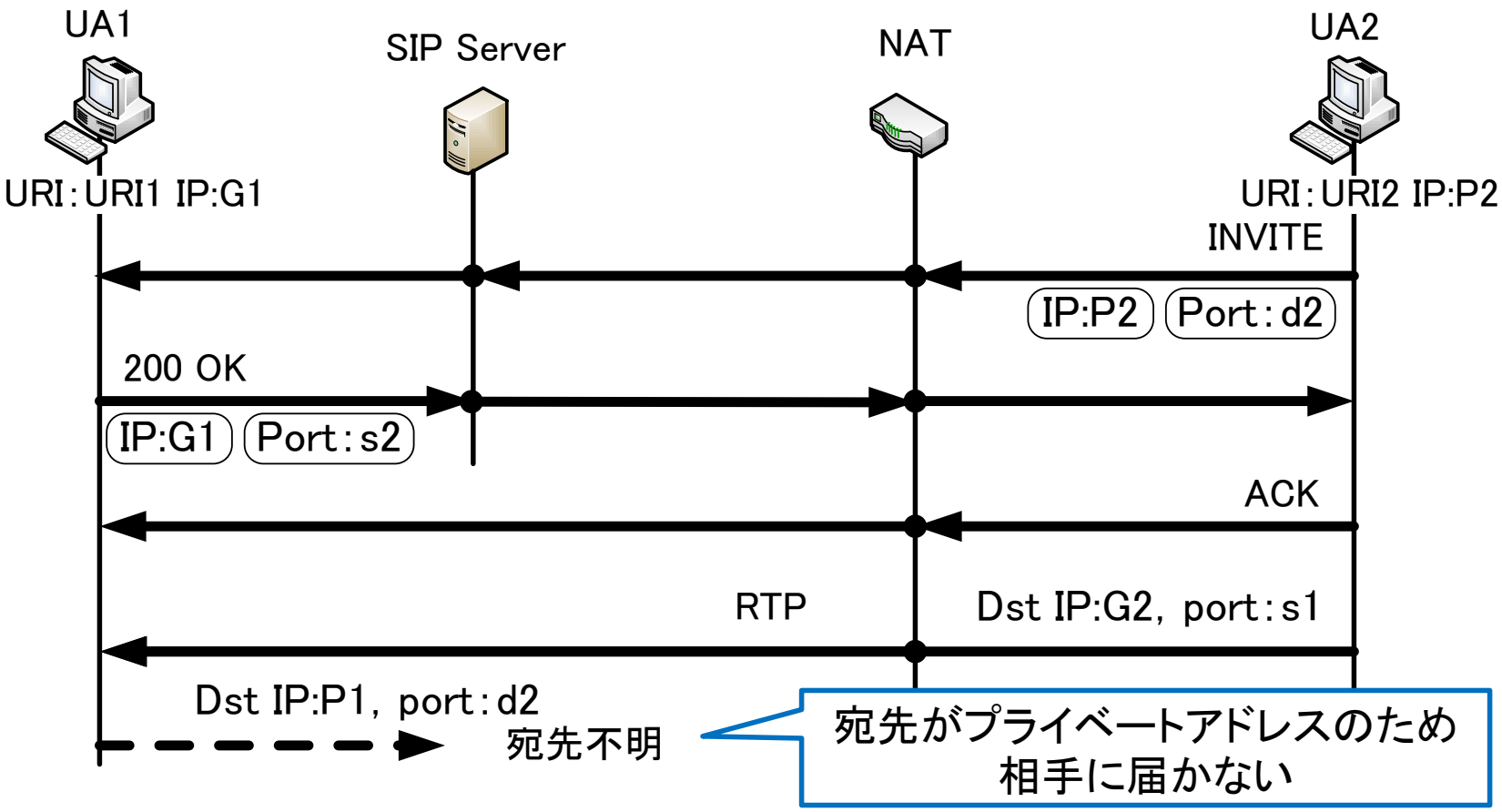
まとめ

- NTMobileにおいてSIP通信を行う手法について提案した
- 提案方式を実装し，動作検証を行い既存のSIPアプリケーションを使用できたことを確認した
- 今後は，ネットワーク環境を変え動作検証及び，測定し評価を行う

補足資料

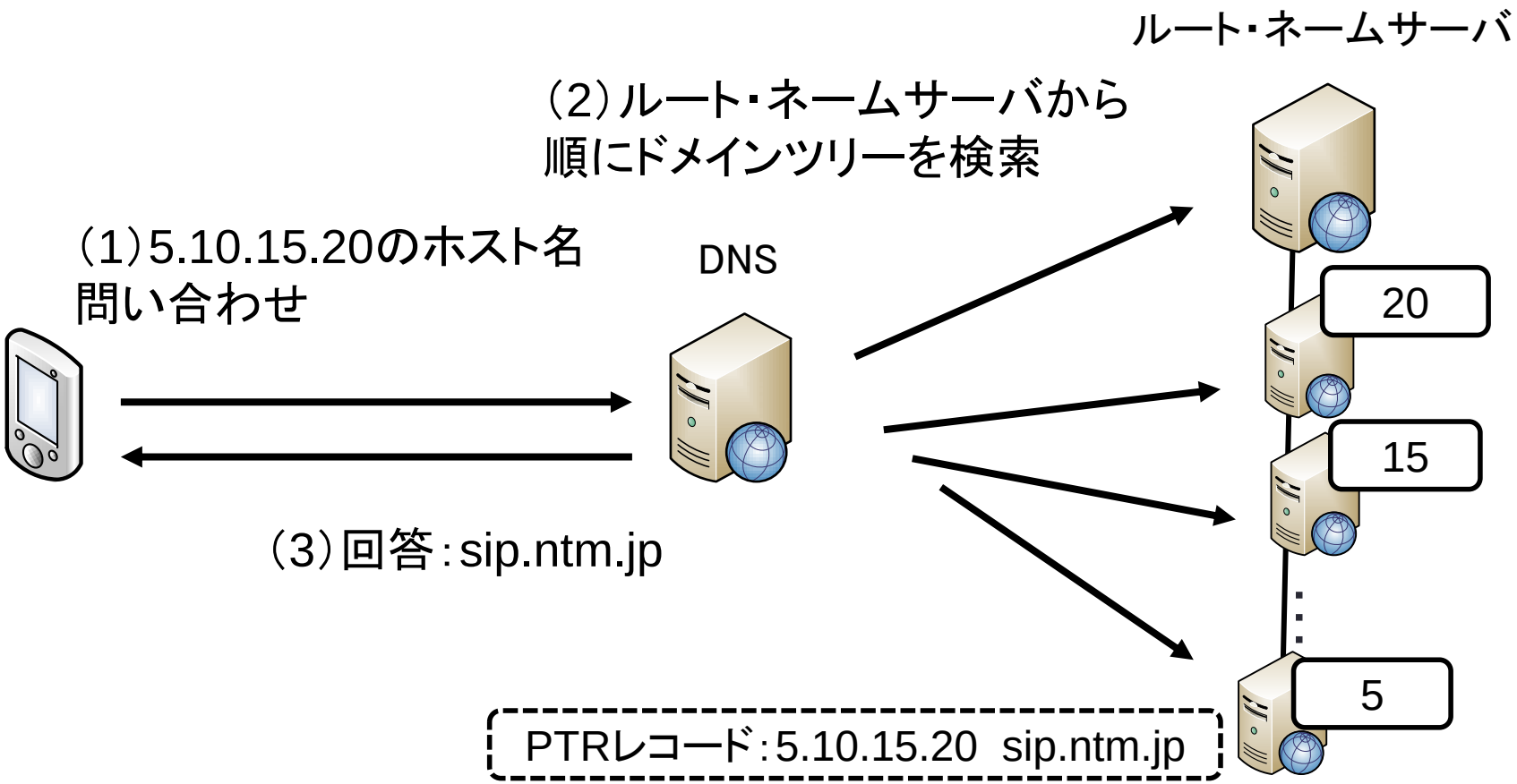
SIPとNAT

- 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



DNS逆引き

- DNSを用いて，IPアドレスからドメイン名に変換する処理
  - ドメイン名からIPアドレスに変換する処理は正引き



H.323

- ITUによるIP網で音声・動画通信を行うための通信プロトコル
- 以下のプロトコルやコーデックを使用
  - H.225：登録，許可，状態，呼シグナリング
  - H.245：制御シグナリング
  - RTP
  - G.711，G.729，G.723.1：オーディオコーデック
  - H.261，H.263：ビデオ・コーデック
- 構成機器
  - ゲートキーパー（H.323端末制御，管理）
  - ゲートウェイ（H.323-H.320）
  - MCU（多地点接続装置）

ITU（International Telecommnication Union）：国際電気通信連合

NATの種類

- NATの種類は大きく4つに分けられる
  - Full Core NAT
  - Restricted Cone NAT
  - Port Restricted Cone NAT
  - Symmetric NAT

- STUNを使用する場合，Symmetric NATの場合は使用できない
  - 内部の端末からパケットを受け取った外部端末のみパケットを送信できる
  - STUNサーバとの通信はできるが，メディアセッションを行う端末と通信ができない