NTMobile における SIP 通信手法の提案

123430041　吉岡 正裕
渡邊研究室

1. はじめに

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．その中の 1 つとして，IP 電話などのマルチメディア通信が挙げられる．マルチメディア通信では、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、セッションを開始するための情報を端末間で交換するプロトコルであり，SIP サーバを介して情報交換を行い，その情報を元にエンドツーエンドで通信する．しかし，SIP は IP ペイロード部分に IP アドレスが記載されているため，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．この問題をアドレス不整合問題と呼ぶ．　ここで，あらゆるネットワーク環境での通信接続性と移動透過性を可能とする NTMobile（Network Traversal with Mobility）[1][2] を提案している．NTMobile は，仮想 IP アドレスを用いており，アプリケーションには仮想 IP アドレスを認識させる．NTMobile を SIP 通信で利用すると，SIP サーバが仮想 IP アドレスを認識できないため，基本的な仕組みの見直しが必要である．そこで，本論文では SIP サーバにも NTMobile を導入し，NTMobile の機能だけを拡張を行うことにより，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 のプロトコルを使用できる手法について提案する．

2. NTMobile

図 1 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）のほかに，NTM 端末の位置情報を管理する 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構築を支持する装置である．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 IP 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一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．

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 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．

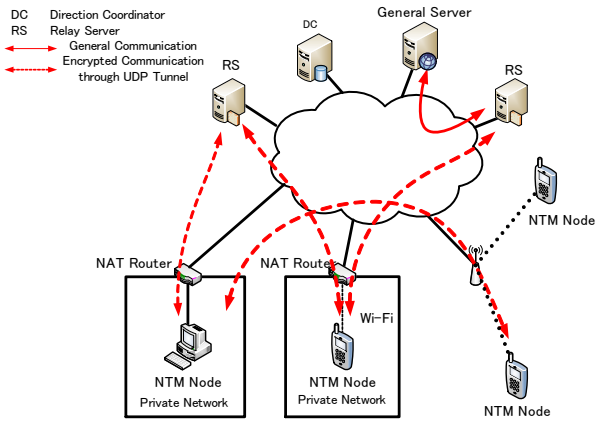


図 1: NTMobile の構成

3. SIP の課題

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が記述されている．送信側は SDP に自分のアドレスを記述した SIP INVITE メッセージを送ることによって相手側に通知する．また，受信側も SDP に自分のアドレスを記述した 200 OK メッセージを送信側に返す．

ここで NAT が通信経路上にあると，NAT では IP ヘッダ部分の処理を行うが，IP ペイロード部分には関与しない．受信側の SIP アプリケーションは SDP に対して返信するが，このアドレスでは NAT テーブルが生成されておらず破棄されてしまう．この課題は NTMobile においても同様で，NTMobile が使用する仮想 IP アドレスを用いて解決することができない．

4. 提案方式

NTMobile において SIP 通信を行う場合，IP アドレスの扱い方により通信経路が大きく変化する．仮想 IP アドレスを RS で RS の実 IP アドレスに変換を行う手法 [2] は，NTM 端末間の通信においても，全ての SIP 通信とメディアセッションを RS 経由でやりとりする必要がある．メディアセッションは，RTP（Real-time Transport Protocol）を用いることが多く，リアルタイム性が求められる．そのため，経由する機器が多いと QoS（Quality of Service）が損なわれる可能性がある．

そこで，仮想 IP アドレスをそのまま使用しながら，メディアセッションをエンドツーエンドで行う手法について提案する．

4.1 概要

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．SIP サーバのアプリケーションに手を加える手法が考えられるが，改造した SIP サーバ以外では使用できない．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．これにより，SIP サーバを NTM 端末とし

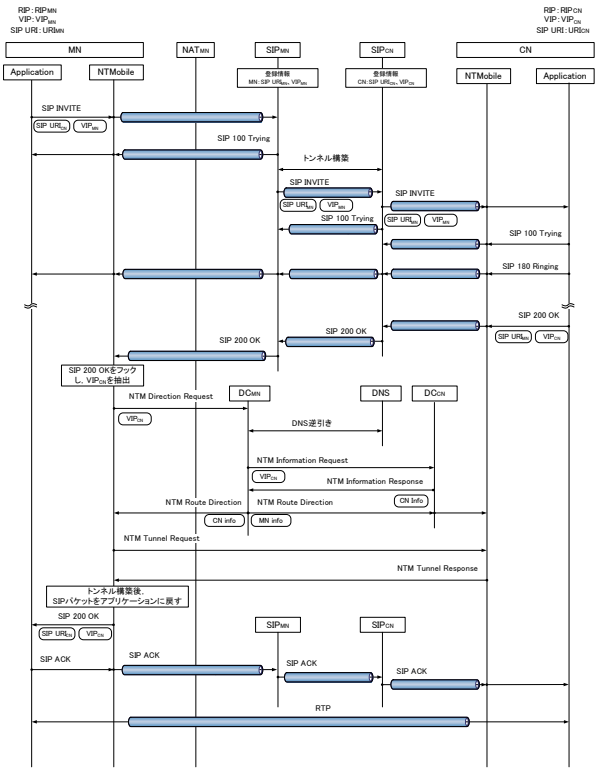


図 2: 提案方式の SIP シーケンス

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．

NTM 端末では，メディアセッションで通信相手の NTM 端末と直接通信するため，NTMobile のネゴシエーション動作を行う必要がある．

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_{CN}）をグローバル上に設置する．MN は NAT 配下に，CN はグローバル上に存在するものとする．SIP サーバにはそれぞれ NTMobile を導入しているものとする．MN と CN は同じ SIP クライアントを使用する．また，MN と CN はそれぞれ NTMobile の登録処理と SIP サーバへのユーザー認証を完了し，SIP 通信に必要な情報を取得しているものとする．

4.3 通信シーケンス

提案方式の SIP 通信シーケンスを図 2 に示す．MN が CN に対して SIP 通信を開始する．MN は，CN の SIP URI（Uniform Resource Identifier）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 CN の SIP URI と自身の仮想 IP アドレス VIP_{MN} を記載した SIP INVITE を SIP_{MN} に送信する．MN と SIP_{MN} は，SIP の登録処理によりトンネルが構築されているため，SIP パケットはトンネルを用いて送受信される．SIP_{MN} は，CN の SIP URI から SIP_{CN} の IP アドレスを取得する．ここで，SIP_{MN} と SIP_{CN} は NTM 端末どうしであるため，トンネルが構築される．SIP_{MN} は，SIP INVITE を SIP_{CN} に送信する．SIP_{CN} は SIP URI から CN の登録情報を取得し，CN に SIP INVITE を送信する．SIP INVITE を受信した CN は，応答として SIP 200 OK を SIP INVITE と同じ経路を通って MN に送信する．

MN は，SIP 200 OK を受信する際，NTMobile でパケットをフックし，MN と CN 間でトンネルが構築されるまで待避する．そして，SIP 200 OK に含まれている VIP_{CN} を取得する．VIP_{CN} を，トンネル構築に必要な情報を取得するキーとして使用する．NTM Direction Request に VIP_{CN} を記載し，DC_{MN} に送信する．DC_{MN} は VIP_{CN} を用いて DNS 逆引きを行う．これにより，VIP_{CN} を CN に割り当てている DC_{CN} の IP アドレスを取得することができる．DC_{MN} は，DC_{CN} に NTM Infomation Request を VIP_{CN} を記載して送信する．DC_{CN} は，VIP_{CN} からトンネル構築に必要な情報を取得し，NTM Infomation Response に取得した情報を記載し返信する．DC_{MN} は，MN と CN に向けてそれぞれの通信相手の情報が記載された NTM Route Direction を送信し，トンネル構築指示を出す．MN と CN 間で，NTM Tunnel Request/Response をやりとりすることでトンネルが構築される．トンネル構築後，MN は待避していた SIP パケットをアプリケーションに渡す．

MN は SIP ACK を SIP INVITE と同様の経路で CN に送信し，MN と CN 間でトンネル介したメディアセッションが行われる．

5. 実装

実装は LinuxOS で行い，仮想マシン上で環境の構築を行った．DC

6. まとめ

本論文では，NTMobile の拡張と SIP サーバに NTMobile の導入することにより，既存の SIP アプリケーションや NAT に一切手を加えることなく SIP の課題の解決した．また，提案方式の実装を行い，既存の SIP アプリケーションをそのまま使用できることを確認した．今後は，実環境においての測定およびハンドオーバ時の動作検証を行う予定である．

参考文献

[1] 鈴木秀和，他：NTMobile における相互接続性の確立手法と実装，pp. .

[2] 吉岡正裕，他：NTMobile における一般 SIP 端末との通信確立手法，p.，.

NTMobileにおける SIP通信方式の提案

名城大学大学院理工学研究科
渡邊研究室
吉岡正裕

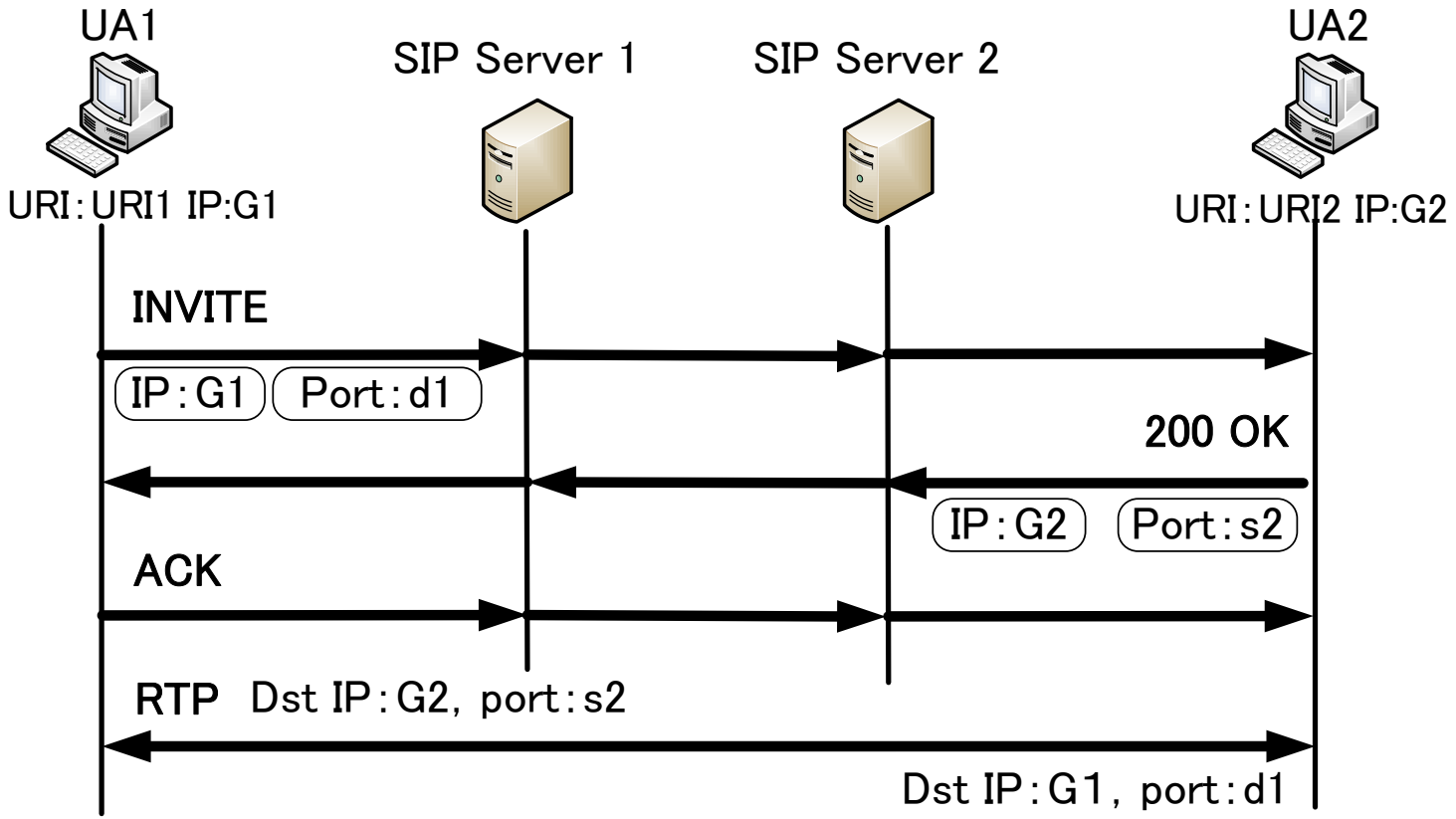
研究背景

- 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

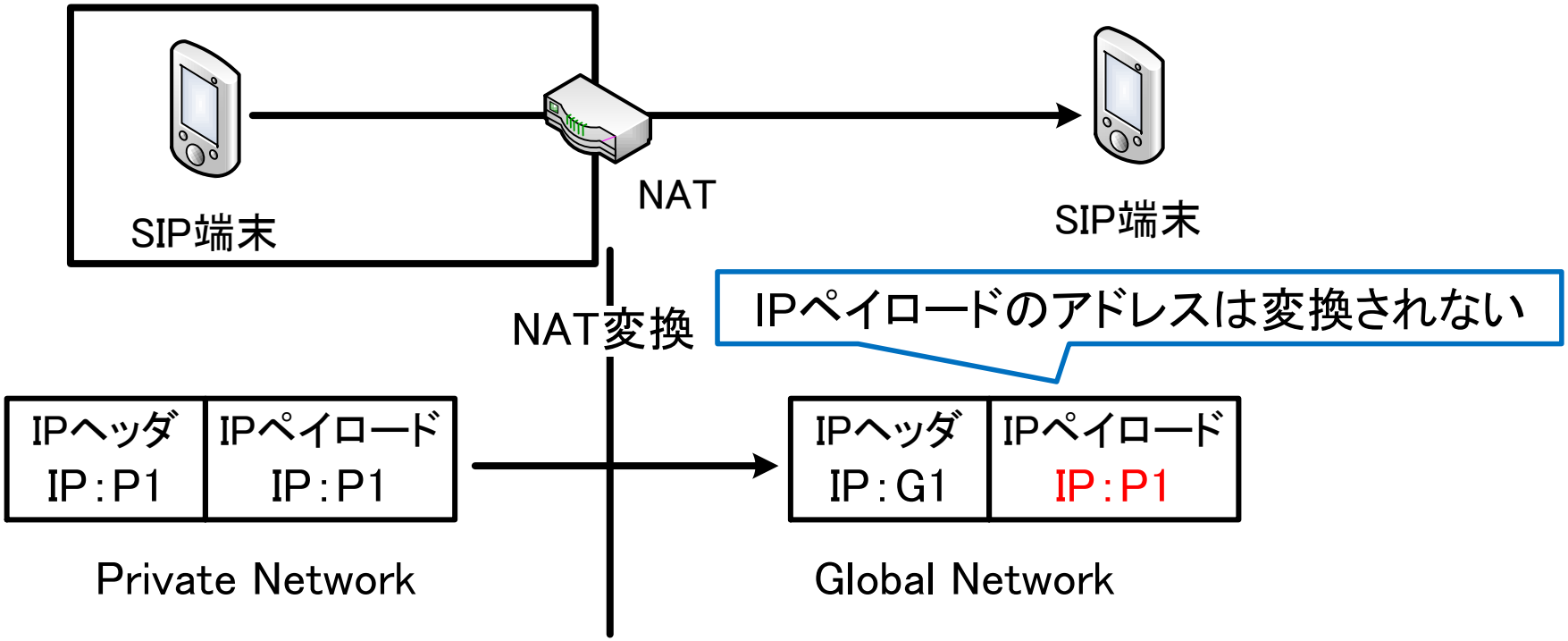
- 通信の開始，通信の切断を行うために使用するプロトコル
- SIPメッセージで，メディアセッションで使用する情報を交換
- メディアセッションは端末間で直接行う



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

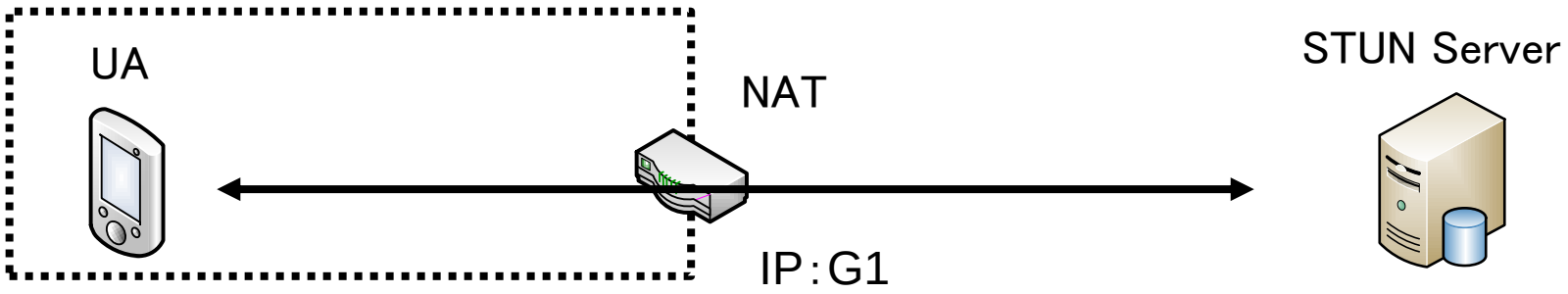


既存技術

- 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

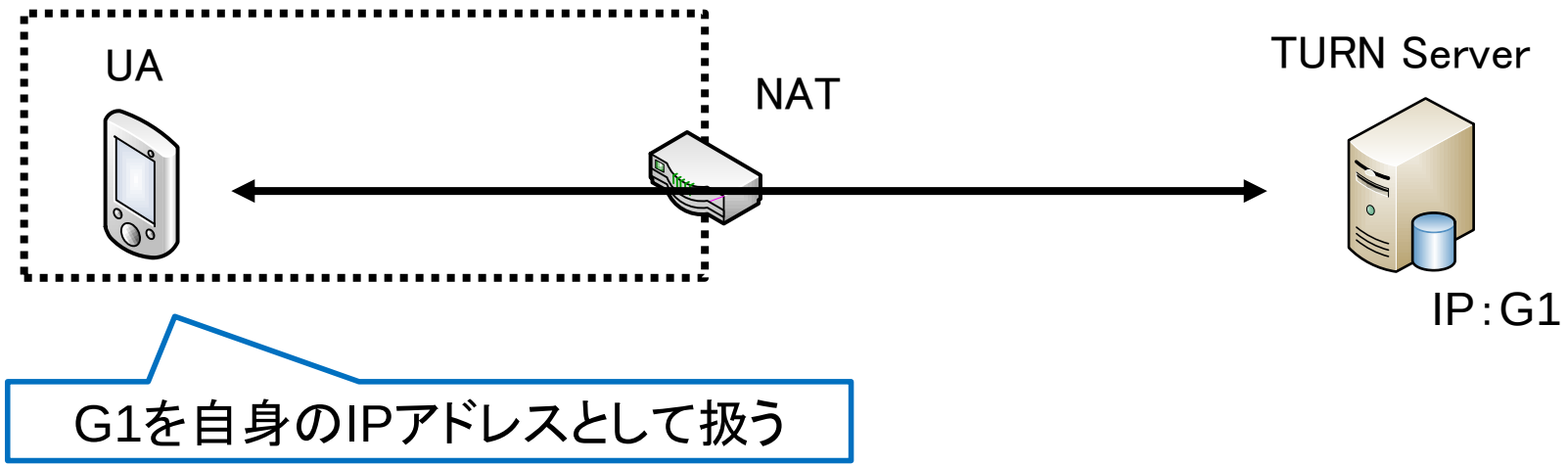
- STUN（Session Traversal Utilities for NAT）
  - SIP通信前にSTUNサーバと通信し，NATの外側IPアドレスを取得する
  - 取得したIPアドレスをSIPメッセージに書き換える
- 利点
  - SIP通信前以外は従来のSIP通信と同様であり，オーバヘッドが少ない
- 欠点
  - NATの種類によっては，使用することができない
  - アプリケーションがSTUNに対応しなければならない



G1を自身のIPアドレスとして扱う

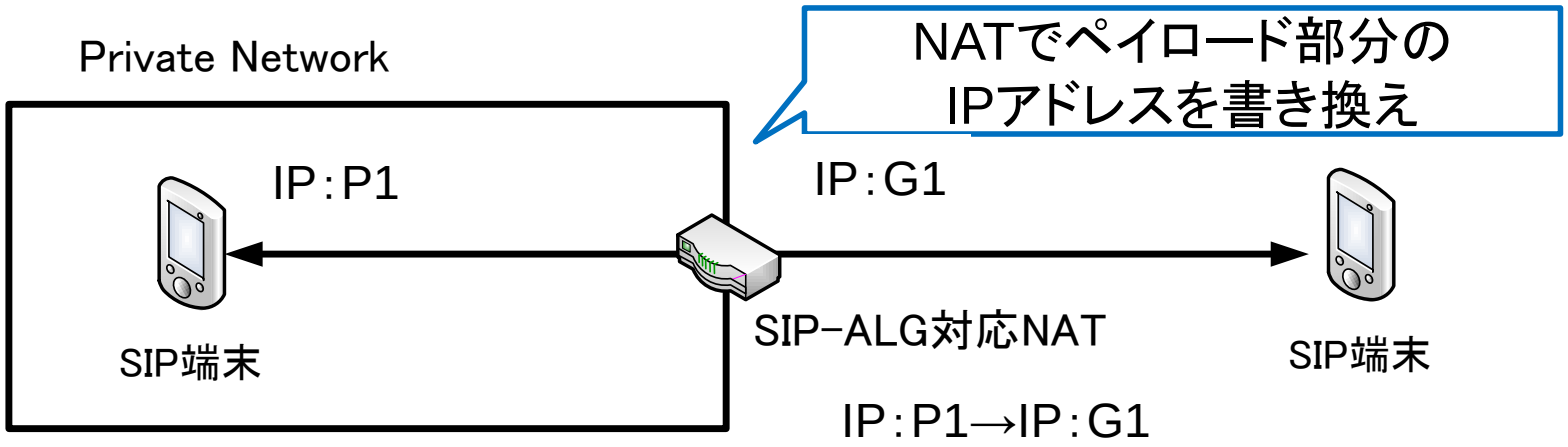
TURN

- 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



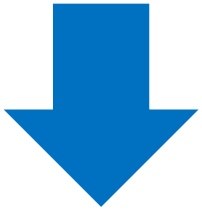
SIP-ALG

- 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

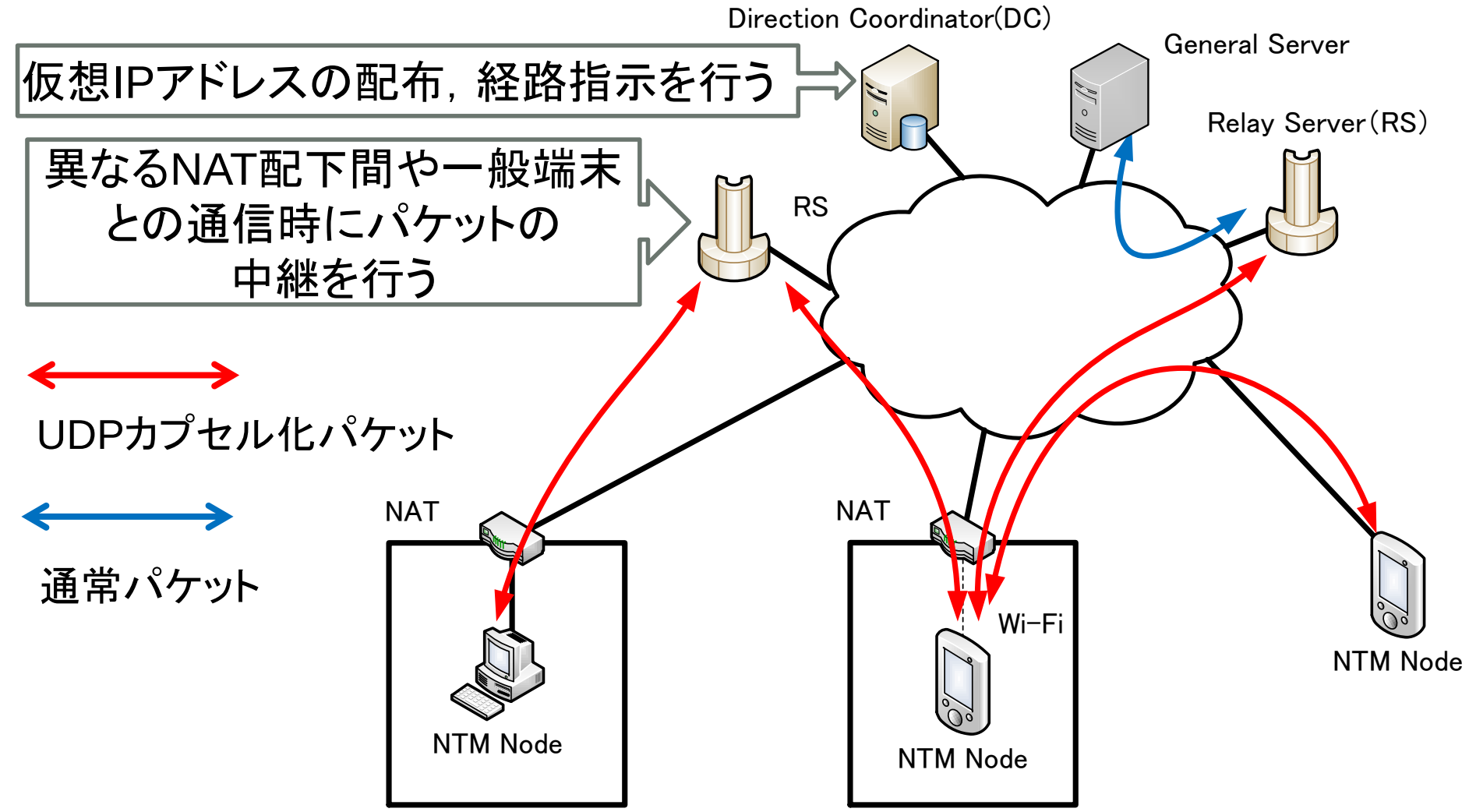
- NTMobile(Network Traversal with Mobility)
  - 端末を一意に識別する仮想IPアドレスを導入
  - 全てのパケットを実IPアドレスでカプセル化
  - 実IPアドレスの変化を隠蔽
  - NATに改造を加えずに実現が可能

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

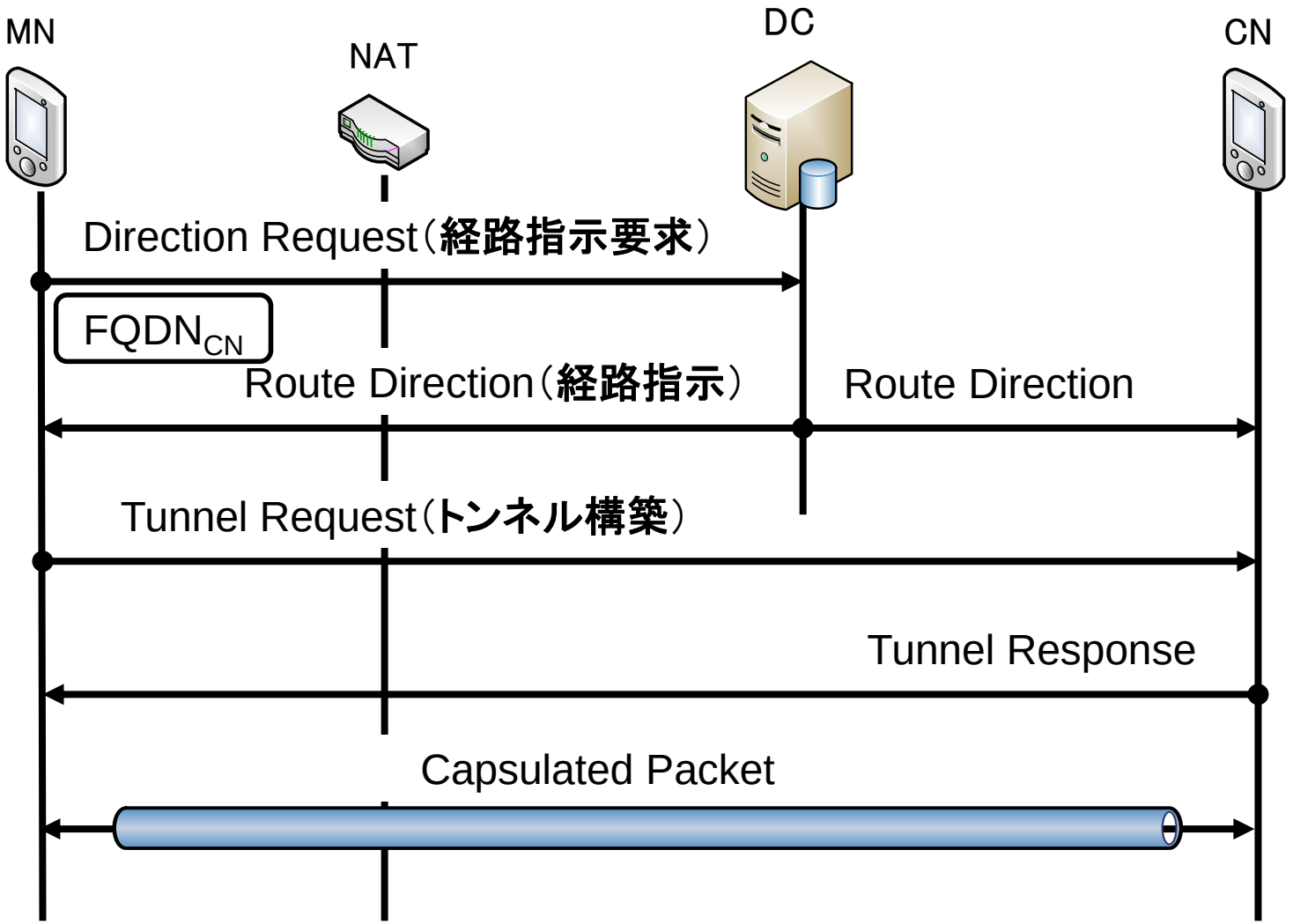
仮想IPアドレスの配布，経路指示を行う

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

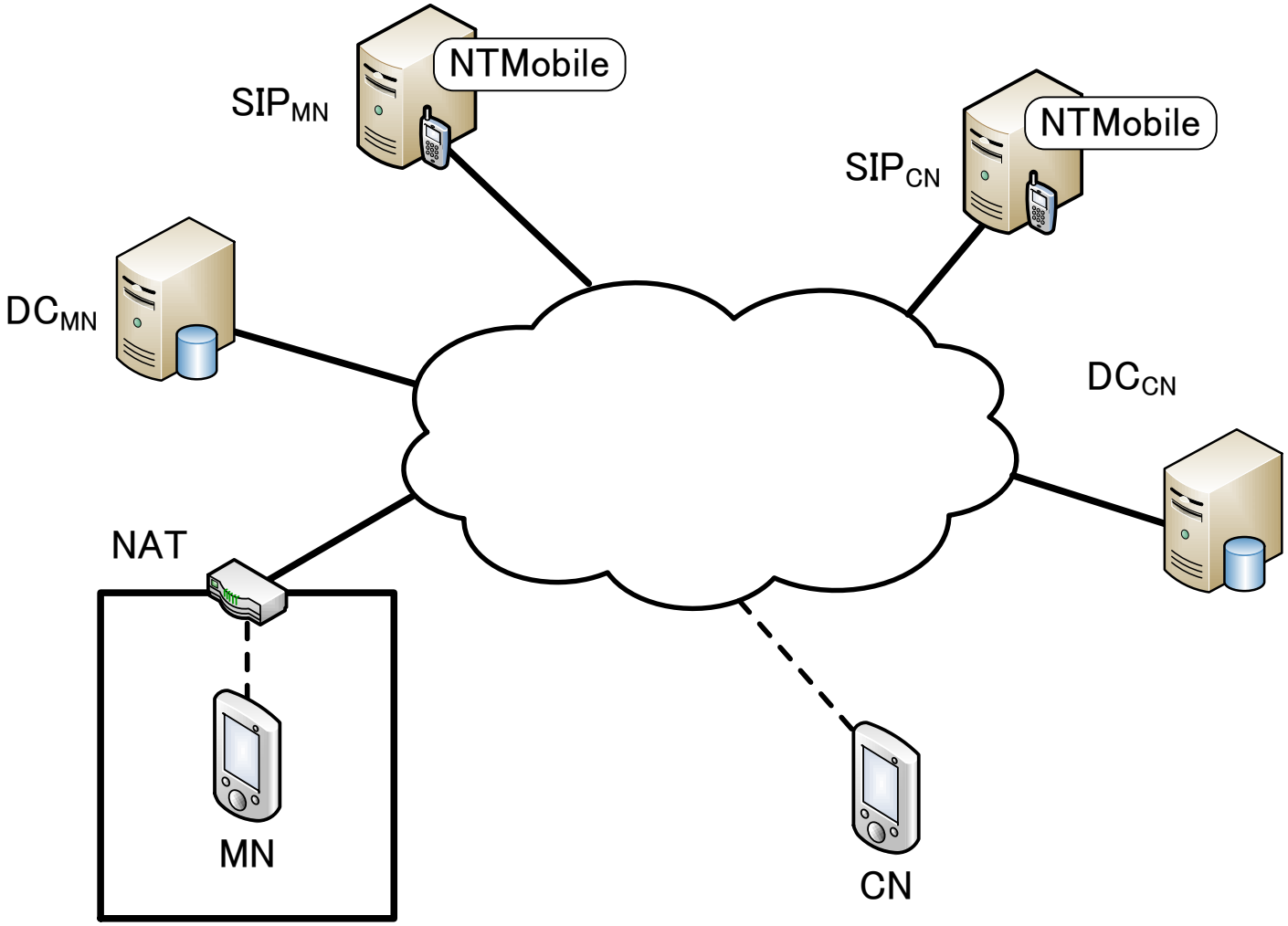
既存のSIPサーバでは仮想IPアドレスを認識できない

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

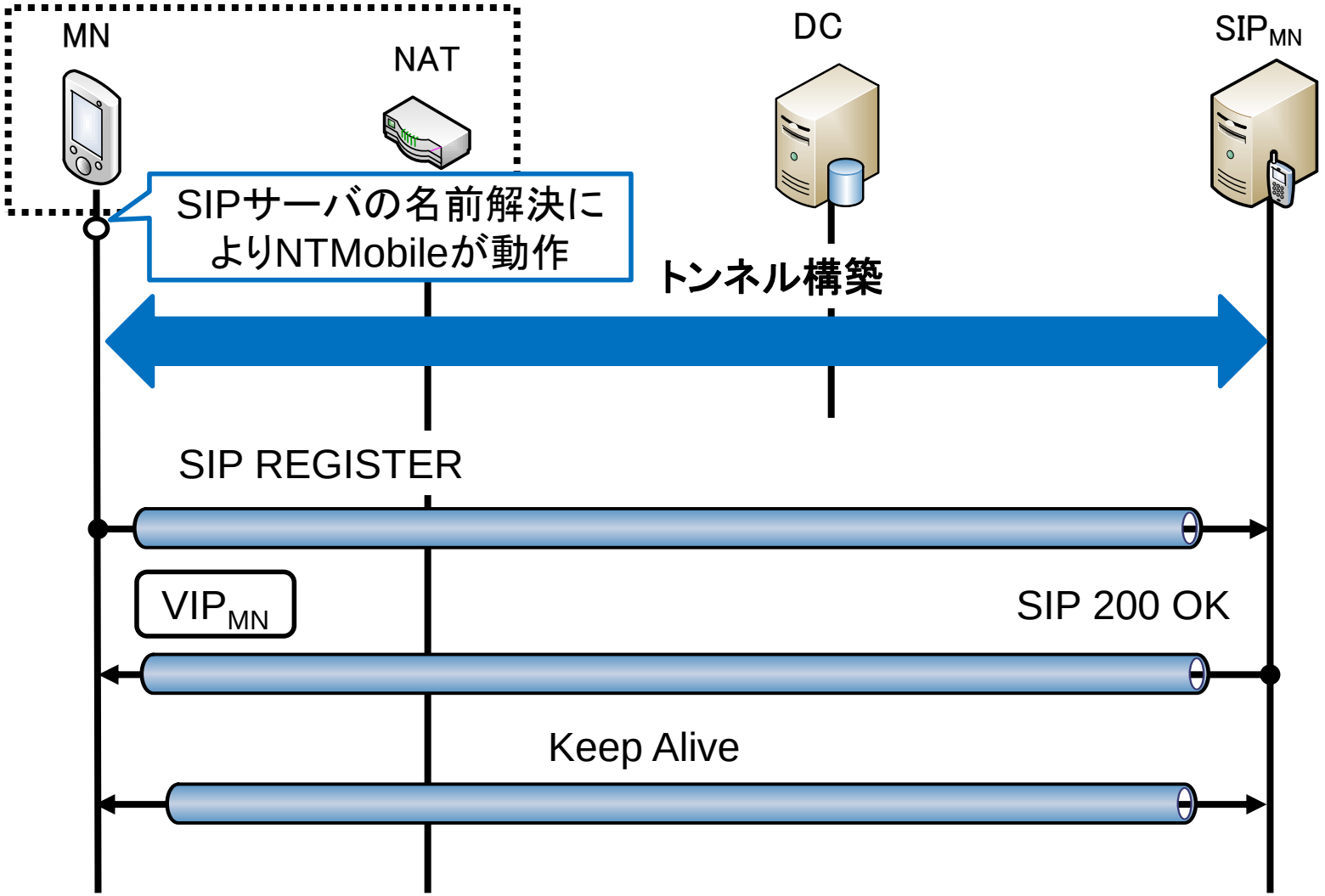
ネットワーク構成

- 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



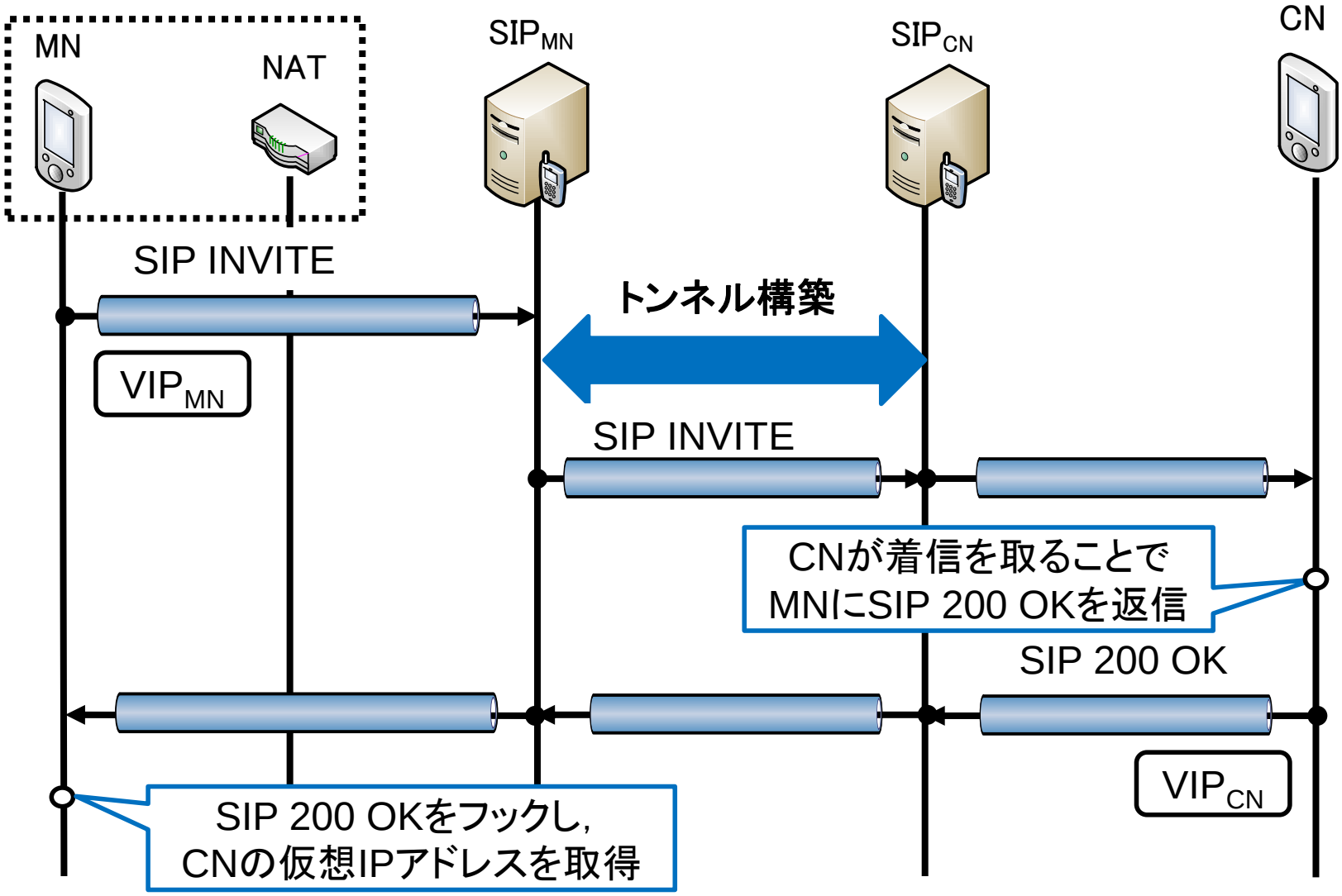
提案方式のSIP登録シーケンス

- 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



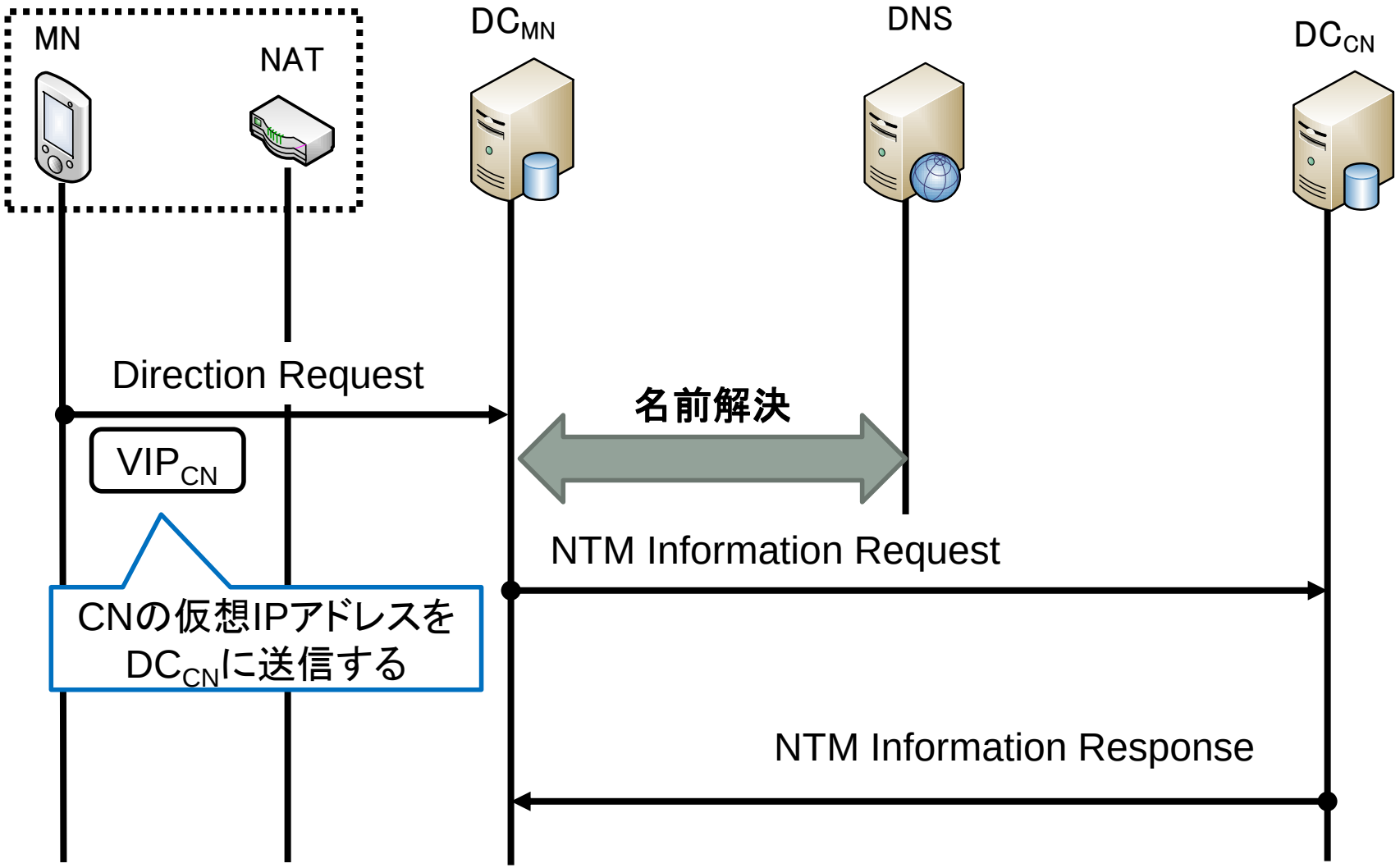
提案方式のSIP通信シーケンス1

- MNがCNにSIP INVITEを送信し，CNが応答する



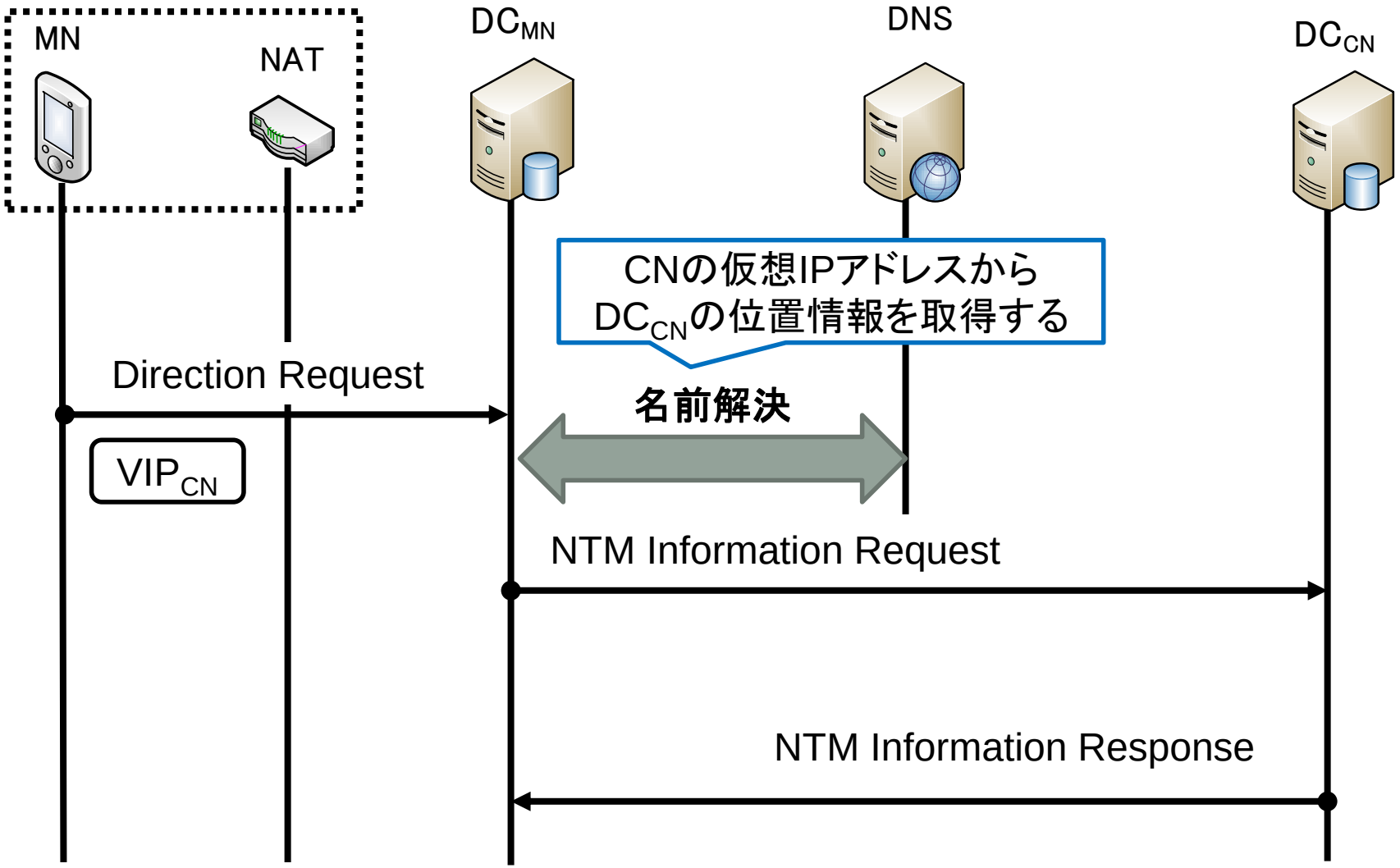
提案方式のSIP通信シーケンス2

- 通信相手の仮想IPアドレスをDCに送信する



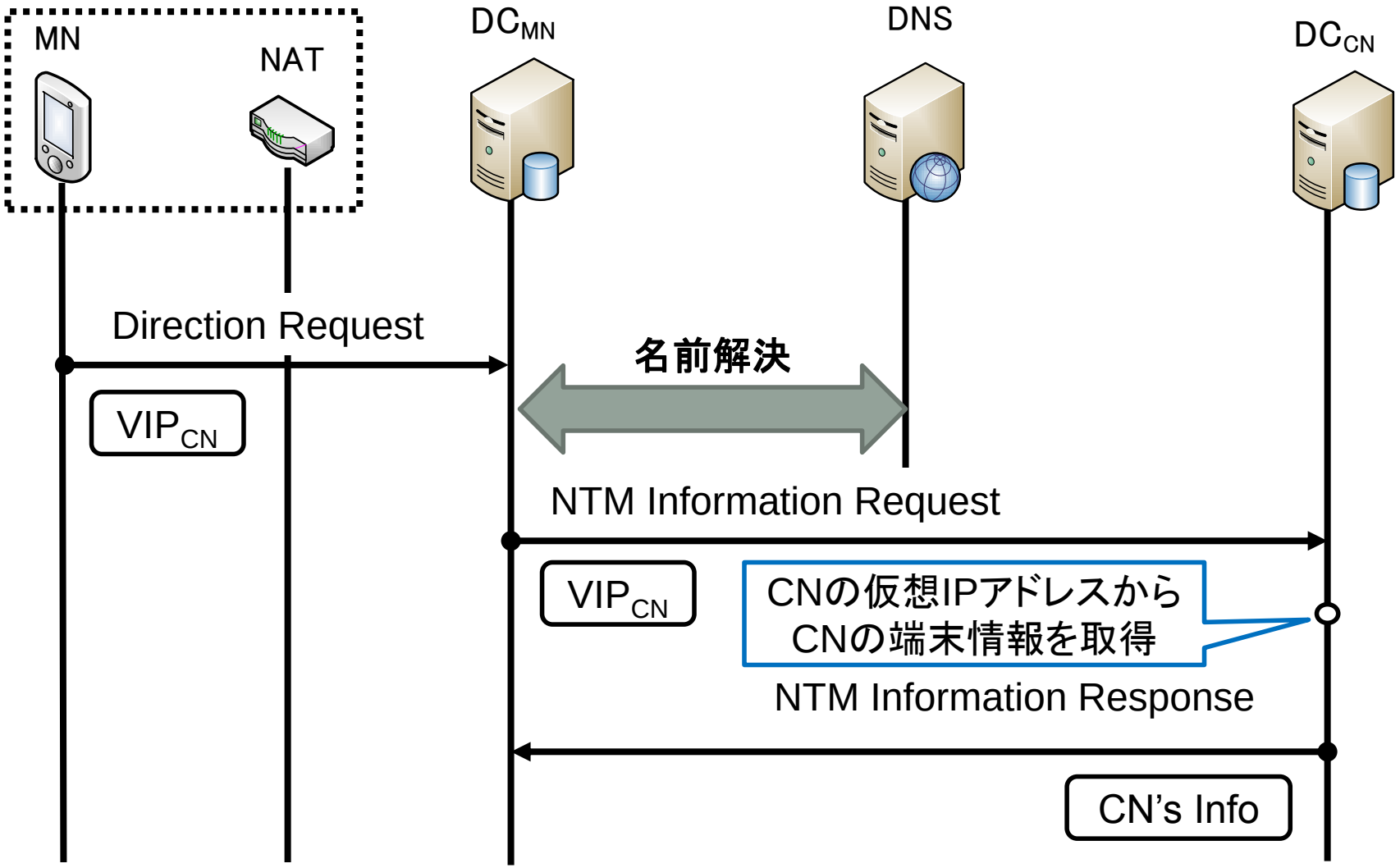
提案方式のSIP通信シーケンス3

- 通信相手の仮想IPアドレスの名前解決を行う



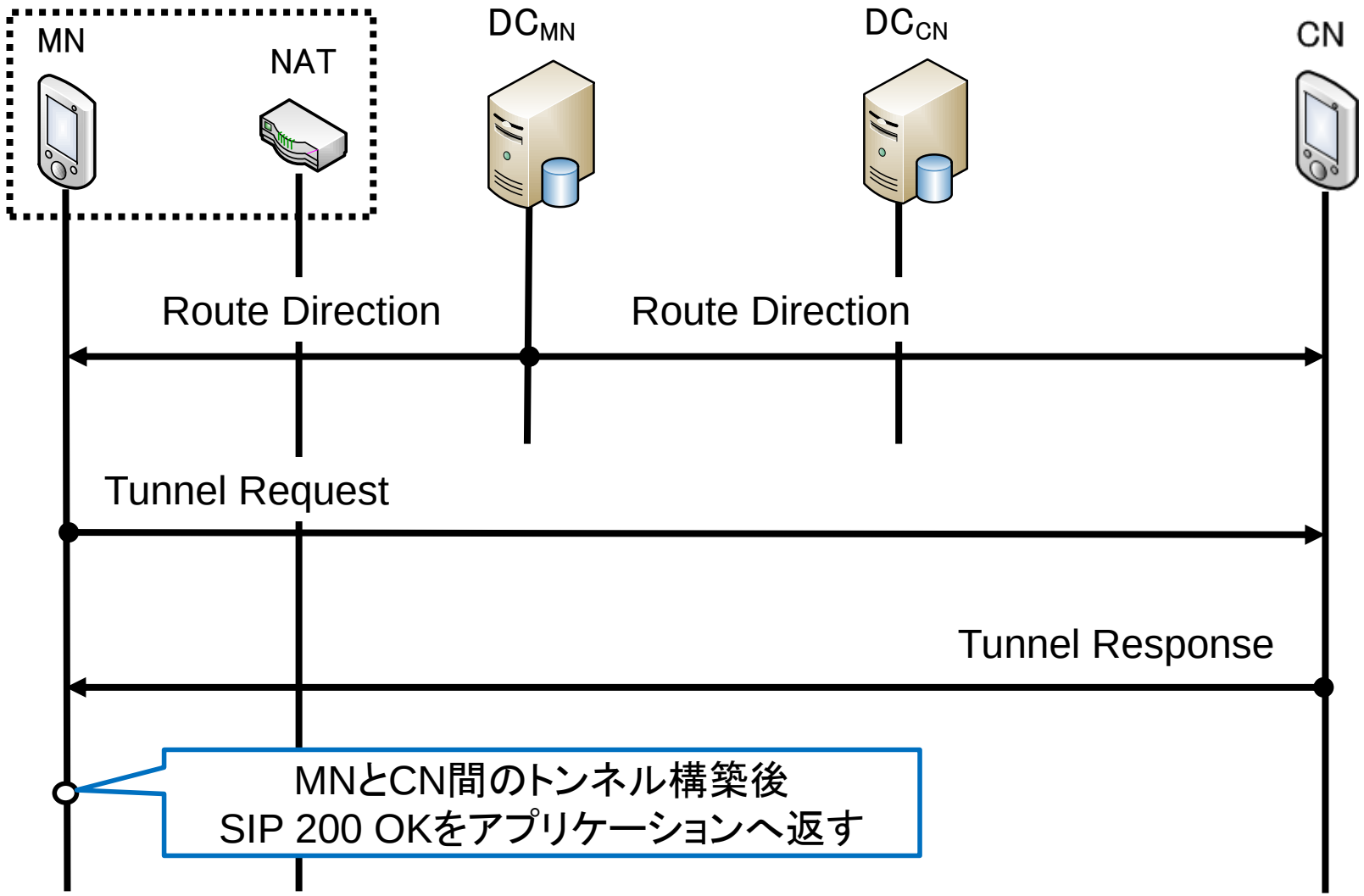
提案方式のSIP通信シーケンス4

- 仮想IPアドレスから端末情報を取得する



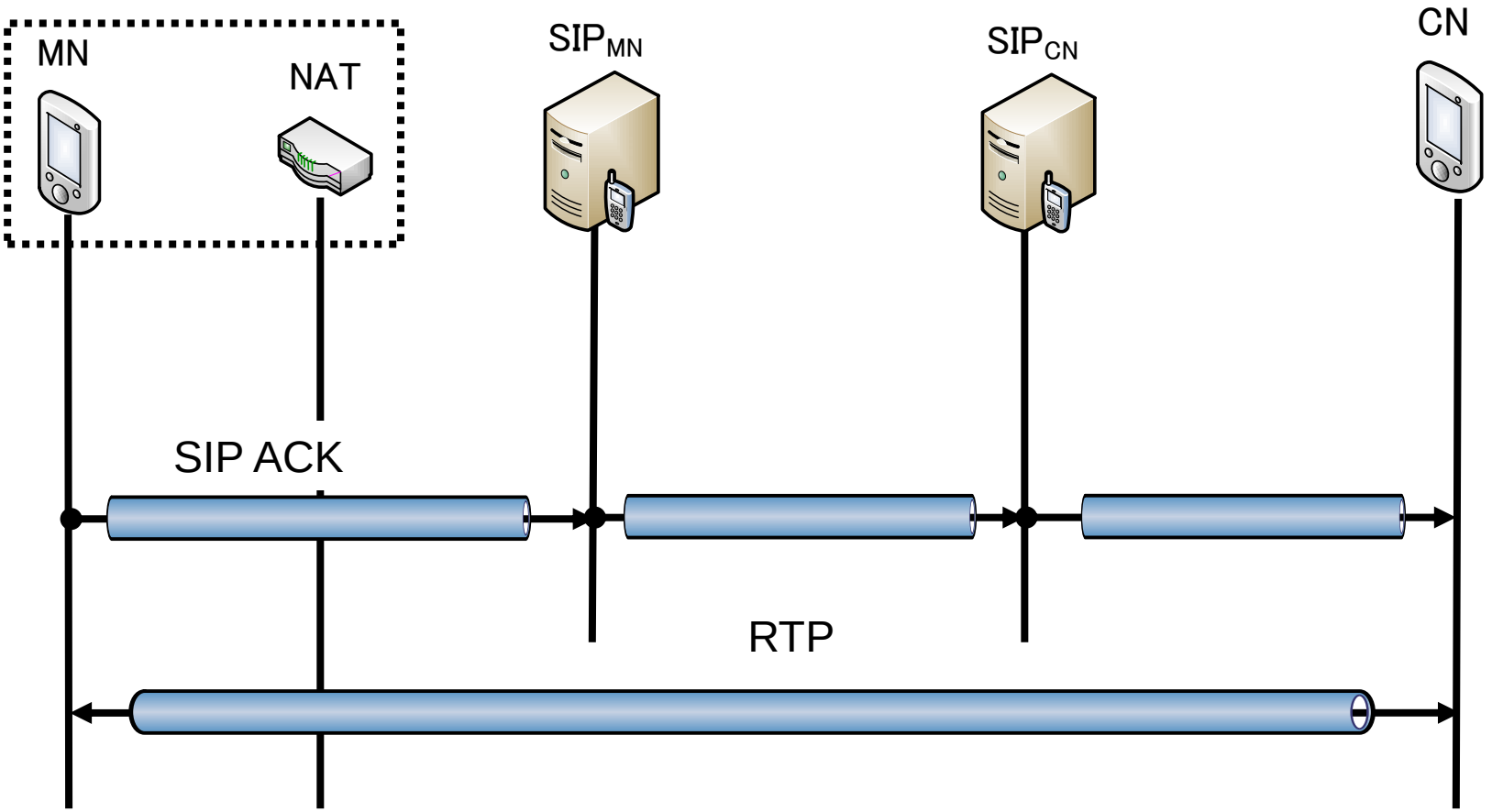
提案方式のSIP通信シーケンス5

- 取得した端末情報を元にトンネルを構築する



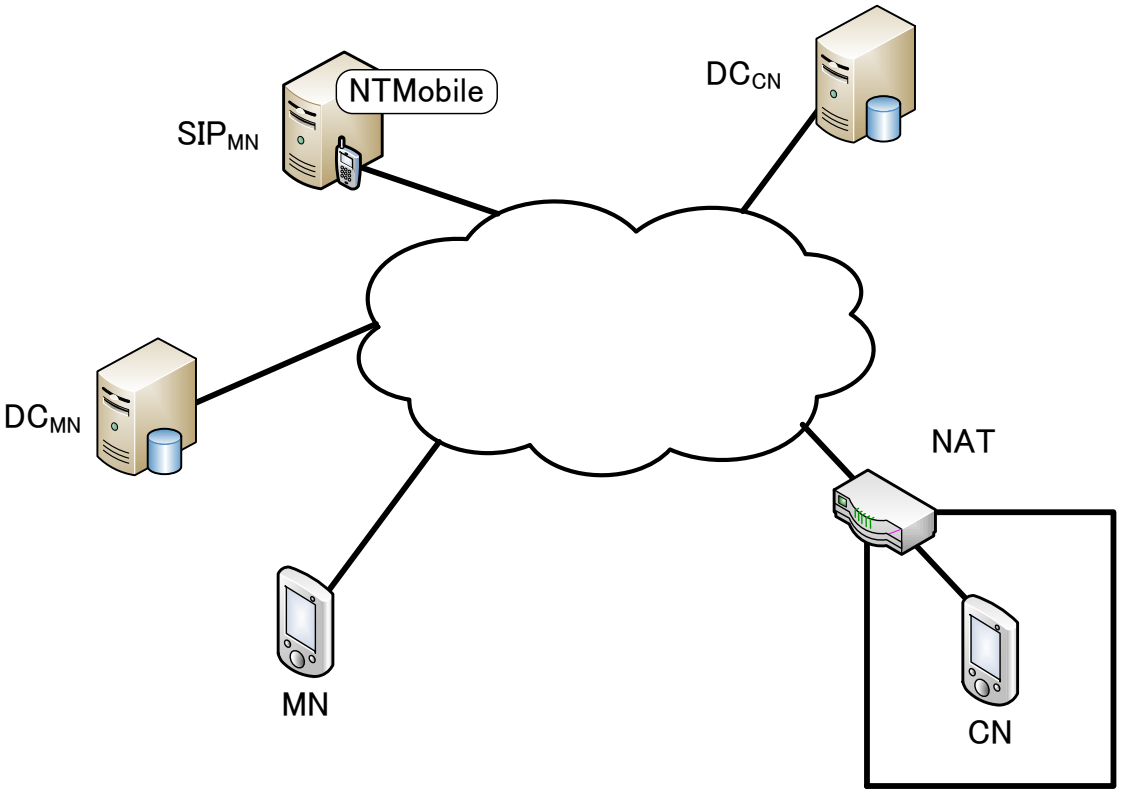
提案方式のSIP通信シーケンス6

- 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



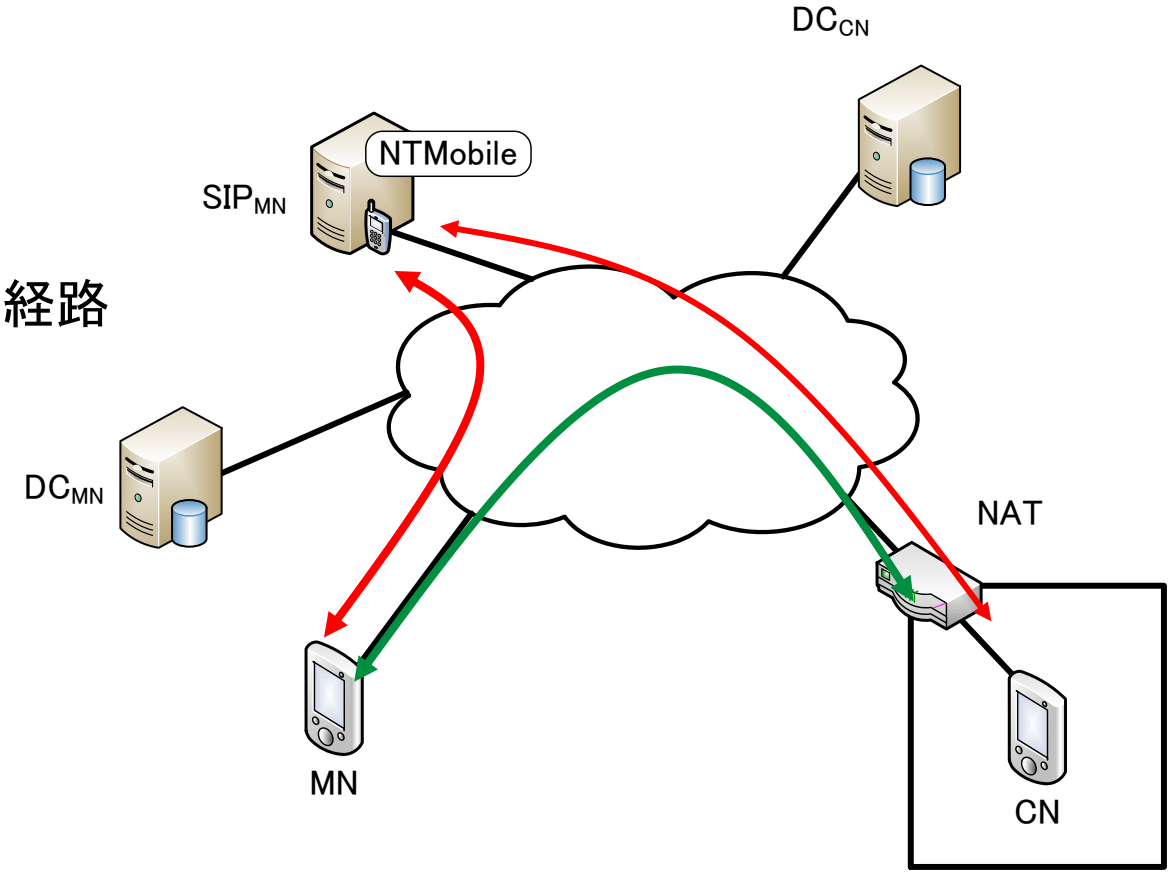
*：Jitsi.http://jitsi.org
**：Asterisk IP PBX,VOIP Gateway,IVR & Open Source Communications. http://www.asterisk.org

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	○	○	△

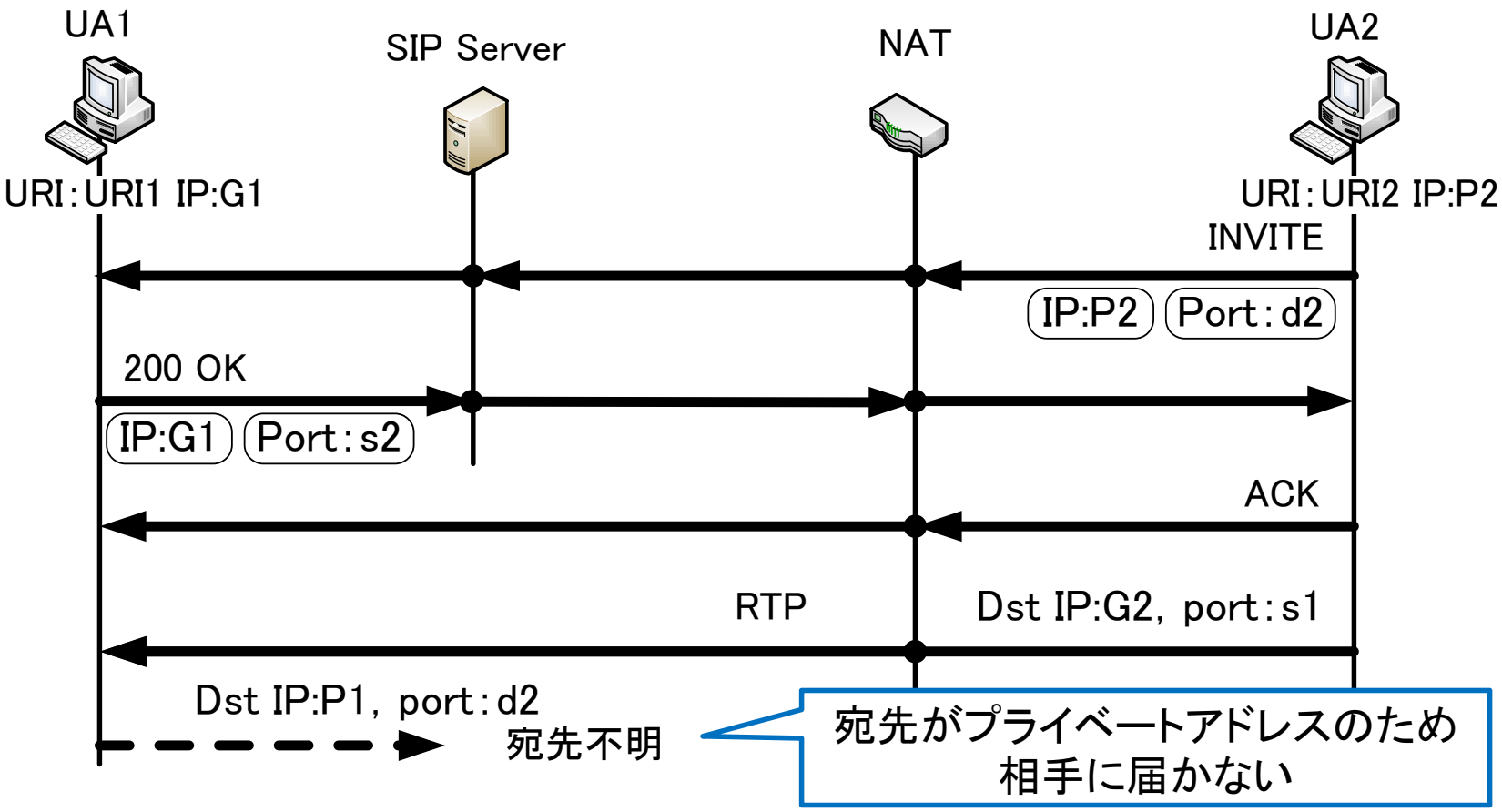
まとめ

- 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

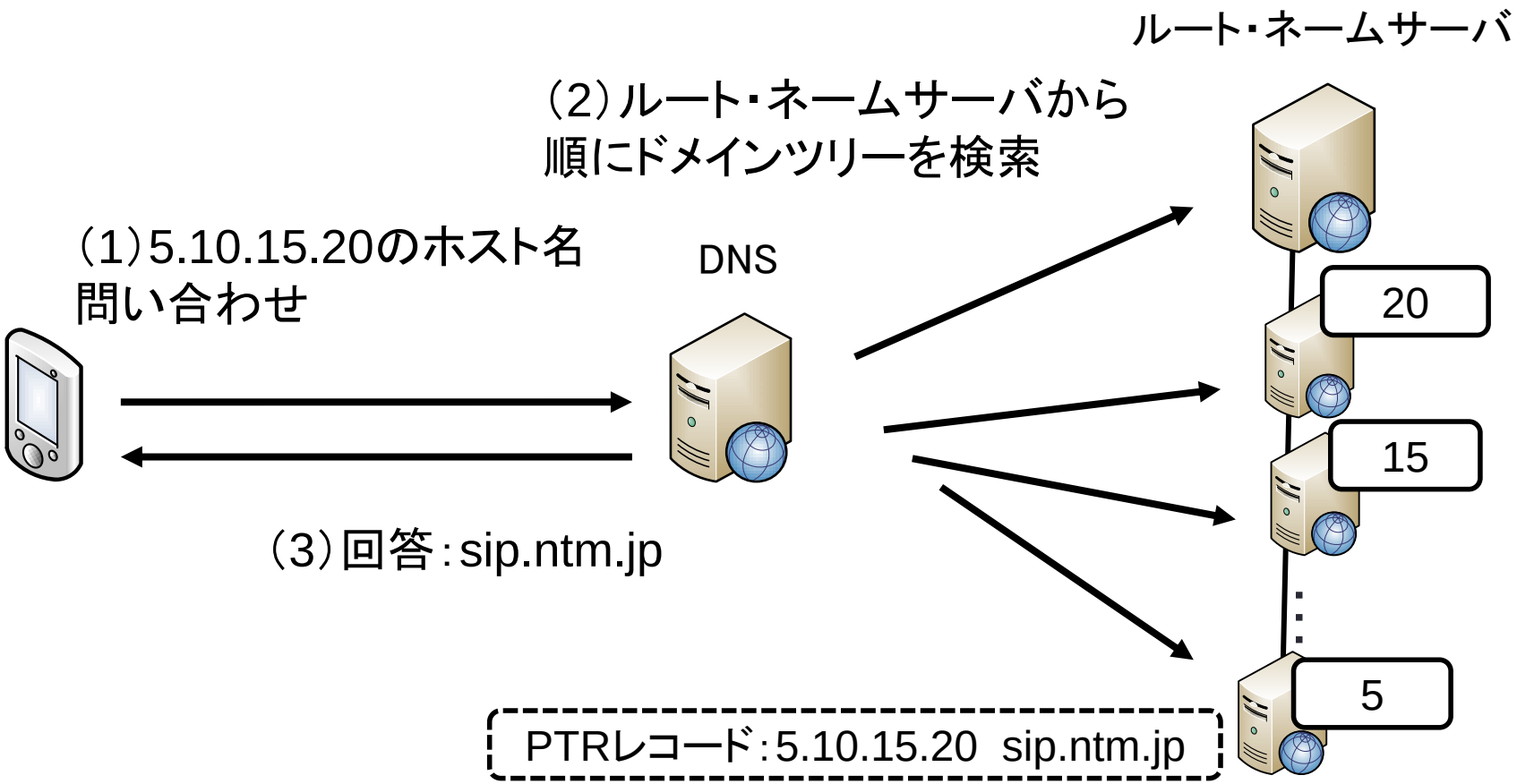
SIPとNAT

- 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