NAT-fを利用したSIPのNAT越え通信方式の提案

三浦 健吉[†1] 鈴木 秀和[†1,†2] 渡邊 晃[†1]

いつでもどこからでもネットワークにアクセスできるユビキタスネットワークの需要が広まっている．ユビキタスネットワークでは，個人同士の通信が重要になるため，IP 電話や情報家電などで利用される SIP が注目されている．ホームネットワークは一般にプライベートアドレスで構築されるため，インターネット側の外部ノードからホームネットワーク内の内部ノードに対して通信を開始できないという NAT 越え問題が存在する．我々は，外部ノードと NAT ルータが連携することにより，NAT 越え問題解決する NAT-f（NAT-free protocol）を提案している．しかし，現在の NAT-f は SIP（Session Initiation Protocol）に対応できないという課題があった．そこで本論では，この NAT-f を利用し，SIP の NAT 越えを実現する手法について検討する．

Researches on NAT traversal for SIP utilizing NAT-f

Kenkichi Miura,[†1] Hidekazu Suzuki[†1,†2]
and Akira Watanabe[†1]

The demand of ubiquitous network that can be accessed from henever and anywhere is spreading. In the ubiquitous network, a communication of the individual becomes important. Therefore, SIP used by the Internet protocol telephone and information appliances is paid to attention. In general, a communication cannot start from a node on the Internet side to a node in the home network because the home network is constructed with private addresses. This problem called the NAT traversal problem. We have proposed NAT-f protocol that modifies the NAT router and the external node to solves the problem. However, NAT-f cannot handle SIP(Session Initiation Protocol). In this paper, We propose the NAT traversal for SIP utilizing NAT-f.

†1 名城大学大学院理工学研究科
Graduate School of Science and Technology, Meijo University
†2 日本学術振興会特別研究員 PD
Research Fellow of the Japan Society for the Promotion of Science

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は NAT（Network Address Translator）[1] 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，外部ノードと NAT ルータが連携することにより，NAT 越え問題を解決する NAT-f（NAT-free protocol）[2] を提案している．しかし，NAT-f は，今後，IP 電話や情報家電で多く使用されると考えられているシグナリングプロトコルである SIP（Session Initiation Protocol）[3] に対応できないという課題があった．

そこで本論文では，SIP Proxy に NAT-f の機能を導入し，外部ノードの代わりに SIP Proxy が NAT ルータと連携し，SIP の NAT 越えを実現する手法について提案する．

以降，2 章で SIP と SIP における NAT 越え問題について説明する．3 章で SIP の NAT 越えを実現する既存技術について簡単に説明する．4 章で NAT-f の動作について説明し，第 5 章で提案方式について説明する．そして第 6 章でまとめる．

2. SIP

2 台の UA（User Agent）が 2 台の SIP Proxy を経由してシグナリングを行う場合について述べる．

2.1 端末情報の登録

図 1 に SIP Proxy に対する端末情報登録時のシーケンスを示す．UA2 は SIP Proxy 2 に対して REGISTER により自身の URI（Uniform Resource Identifier）である URI2 と

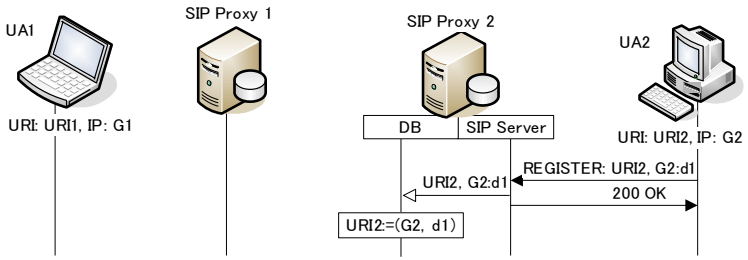


図 1 端末情報の登録シーケンス

SIP メッセージを受信する際に使用するトランスポートアドレス G2:d1 の登録を要求する．SIP Proxy 2 は受信した URI とトランスポートアドレスを DB（Data Base）に登録し，UA2 に対して正常応答を意味する 200 OK を返答する．

2.2 動作概要

2.2.1 SIP の基本シーケンス

図 2 に SIP の基本シーケンスを示す．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，UA2 とのセッションを確立する際に UA1 が使用するトランスポートアドレス G1:s2 が記載されており，SIP Proxy 1 を中継し，SIP Proxy 2 に転送される．SIP Proxy 2 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 が使用するトランスポートアドレス G2:d2 が記載されており，2 台の SIP Proxy を経由して UA1 まで転送される．UA1 は ACK を返答した後，交換したトランスポートアドレスを用いて，UA2 と直接メディアセッションを確立する．

セッション終了時は，セッション切断要求を意味する BYE とそれに対する正常応答 200 OK によってセッションが切断される．

2.3 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 越え問題に係るもので，NAT の外部から内部に向けてシグナリングを開始できないことである．もう 1 つは，SIP は IP ペイロード内に IP アドレス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．

2.3.1 端末情報登録時に生じる問題

UA が NAT 配下にある場合，その UA にはプライベート IP アドレスが割り当てられて

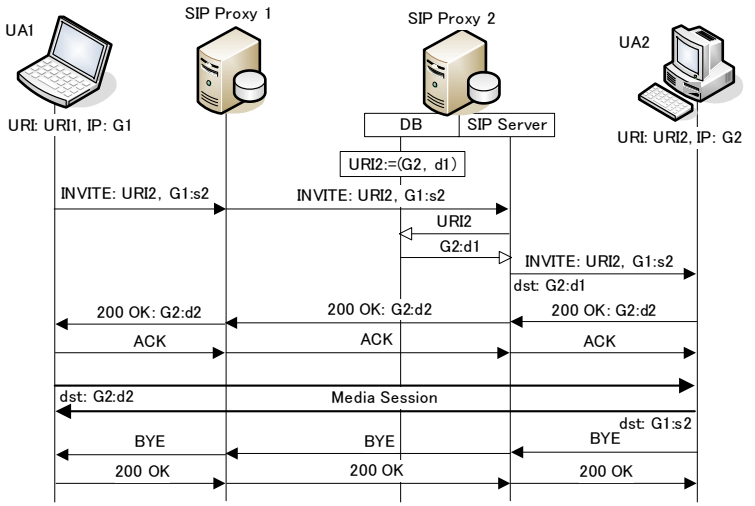


図 2 SIP の基本シーケンス

いる．そのため，UA が REGISTER により SIP Proxy に対して，端末情報の登録を要求すると，SIP Proxy には UA の URI とプライベート IP アドレスが関連付けられて登録される．そして，SIP Proxy は UA に対する 200 OK の返答を試みるが，宛先アドレスがプライベート IP アドレスであるため，宛先不明として処理されてしまう．

これを解決するため，RFC3581[4] では，REGISTER 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．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．

2.3.2 INVITE 時に生じる問題

SIP Proxy は，ある UA から先ほど端末情報を登録した UA に向けた INVITE を受信すると，SIP Proxy は先ほどの UA に対して INVITE の転送を試みる．しかし，先ほどの UA に関連付けられている IP アドレスはプレイベート IP アドレスであるため，宛先不明として処理されてしまう．

2.3.3 セッション確立時に生じる問題

UA は受信した 200 OK に記載されているトランスポートアドレスに基づき，セッション

を確立する．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，セッションを確立することはできない．また，セッション確立時には SIP で使用するポート番号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．

3. 既存技術

ここでは，既存の SIP の NAT 越え技術をアドレス埋め込み型，アドレス書き換え型，サーバ中継型，3 種類に分類し，それぞれについて簡単に説明する．

3.1 アドレス埋め込み型

アドレス埋め込み型は，SIP メッセージを送信する際に，予め NAT 越え問題が解決済みの IP アドレス・ポート番号を埋め込んでおく方式である．ここでは，UPnP と STUN について述べる．

3.1.1 UPnP

UPnP（Universal Plug and Play）[5] では，機能の実装が必要になるのは NAT と NAT 配下の UA である．

SIP メッセージの送信に先立ち，UA と NAT の間で UPnP のネゴシエーションを行い，UA は NAT 外側の IP アドレス・ポート番号を取得する．UA は，この IP アドレス・ポート番号を SIP メッセージに埋め込んで送信する．UPnP のネゴシエーションは，SIP メッセージを受信するためのポートと，メディアセッションを確立する際に使用するポートについてそれぞれ実行する必要がある．

UPnP の機能が実装されている NAT ルータ（ブロードバンドルータ）は数多く存在するが，UA 側のポートと NAT 側のポートが一致していない設定が施せないものや，UPnP の実装が正しく行われていない場合などがあり，上手く動作しない場合がある．

3.1.2 STUN

STUN（Simple Traversal of UDP through Network Address Translators）[6] では，機能の実装が必要になるのは NAT と NAT 配下の UA である．また，第 3 の端末として STUN サーバが必要である．

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 を送信し，NAT 上に NAT テーブルを生成する．STUN サーバは，このとき STUN サーバ側から見た送信元 IP アドレス・ポート番号を Binding Response として返答する．そして，UA は，この IP アドレス・ポート番号を SIP メッセージに埋め込んで送信する．

しかし，この方式には STUN そのものの制約が引き継がれている．即ち，Symmetric NAT には使用できない．また，通信は UDP に限定される．

3.2 アドレス書き換え型

アドレス書き換え型は，NAT が SIP メッセージ中の IP アドレス・ポート番号の書き換える方式である．代表例として，SIP ALG と B2B UA について述べる．

3.2.1 SIP ALG

SIP ALG（Application Level Gateway）[7] では，機能の実装が必要なのは NAT の箇所だけである．NAT の機能を拡張し，プライベートネットワーク側からグローバルネットワーク側に送信された SIP メッセージの中身を参照し NAT 外側の IP アドレスとポート番号へ書き換える．

改造が必要になるのは NAT だけだが，NAT に負荷がかかることや，SIP メッセージが暗号化されていた場合に対応できないなどの課題がある．

3.2.2 B2B UA

B2BUA（Back to Back User Agent）[7] では，機能の実装が必要なのは NAT の箇所だけである．B2B UA はネットワークの境界面である NAT 上で動作し，プライベートアドレス側とグローバルアドレス側にそれぞれ UA が存在するように振舞う．プライベートアドレス側の UA で SIP メッセージを受信すると，グローバルアドレス側の環境に合わせて SIP メッセージ生成し，グローバル側の UA で送信することにより，NAT を超えている．逆方向についても同様である．

3.3 サーバ中継型

サーバ中継型は，グローバルネットワークに設置されたサーバを中継し，通信を行うことで，NAT 越えを実現する方式である．

3.3.1 TURN

TURN（Traversal Using Relay NAT）では，機能の実装が必要になるのは NAT 配下の UA である．また，第 3 端末として TURN サーバが必要である．

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・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 サーバは SIP メッセージを取り出し，送信する．TURN サーバが受信した SIP メッセージについては，カプセル化し，UA

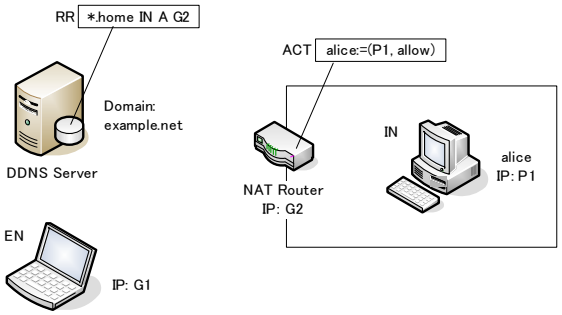


図 3 NAT-f 事前設定

まで転送する．

TURN は NAT の種類に依存せず，NAT 越えが可能であるが，全ての通信が TURN サーバを中継するため，TURN サーバに対する負荷が大きいことと，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．

4. NAT-f

NAT-f は外部ノード EN（External Node）と NAT ルータが連携することにより NAT 越えを実現する技術である．以下に，NAT-f の概要について説明する．

4.1 事前設定

図 3 にシステムの構成と初期設定情報を示す．外部ノード EN（External Node）と NAT ルータには NAT-f 機能が実装されており，内部ノード IN （Internal Node）及び DDNS（Dynamic DNS）[8] サーバは既存のものを利用する．

DDNS サーバには，IN の名前とそれに対応する NAT ルータの IP アドレスを登録しておく．

また，IN の名前，プライベート IP アドレス，及び外部からのアクセス許可情報を NAT ルータの ACT（Access Controll Table）に対して

$$alice := (P1, allow)$$

のように関連付けて登録しておく．

4.2 動作概要

図 4 に NAT-f の通信シーケンスを示す．NAT-f における通信は以下の 3 フェーズから構成される．

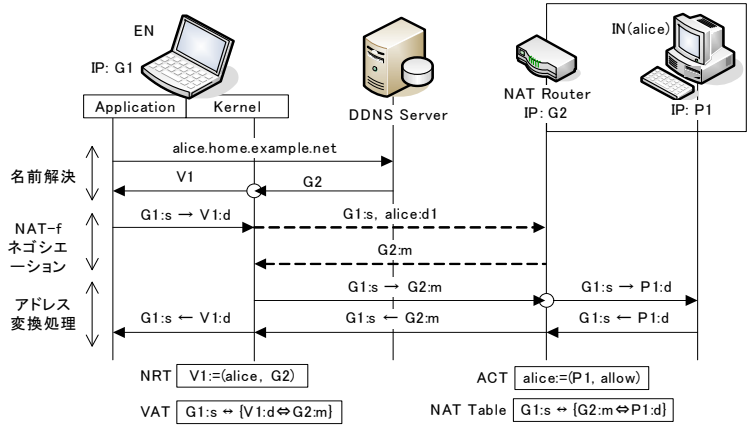


図 4 NAT-f の通信シーケンス

4.2.1 DNS 名前解決

EN は IN へ通信を開始する際，DDNS サーバへ名前解決を依頼する．DDNS サーバは NAT ルータの IP アドレス G2 を返答する．EN は IP 層において取得した NAT ルータの IP アドレスを仮想アドレス V1 へ書き換えてアプリケーションに渡す．このとき，NAT ルータの IP アドレス，仮想 IP アドレス，及び IN の名前の関係を NRT(Name Relation Table) に

$$V1 := (alice, G2)$$

のように関連付けて保存する．以上の処理により，EN は通信相手の IP アドレスを V1 として認識する．

4.2.2 NAT-f ネゴシエーション処理

EN は宛先 IP アドレスが V1 である最初の TCP/UDP パケットを送信する際，一時的にこのパケットをカーネル内に待避させ，NAT ルータとの間で NAT-f ネゴシエーションを実行する．破線部が NAT-f ネゴシエーション処理である．NAT ルータは，ACT を参照し，EN と IN 間の通信に必要な NAT テーブルを

$$G1 : s \leftrightarrow \{G2 : m \Leftrightarrow P1 : d\}$$

のように生成する．これは，IP アドレス・ポート番号が G1:s から G2:m に送信されたパケットの宛先 G2:m を P1:d へ変換することを意味している．そして，NAT ルータは，自身の IP アドレス G2 とマッピングされたポート番号 m を EN に返答する．EN はこの応答

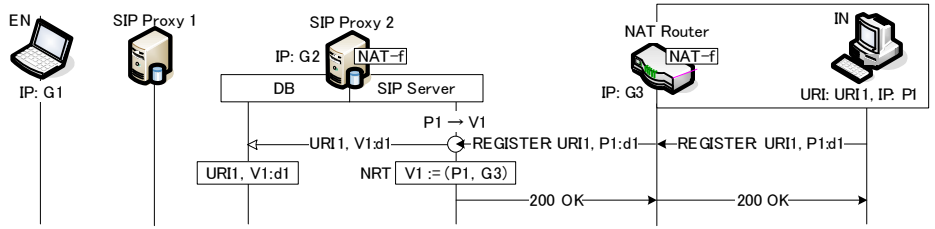


図 5 端末情報登録時のシーケンス

を元に VAT（Virtual Address Translation）テーブルを

$$G1 : s \leftrightarrow \{V1 : d \Leftrightarrow G2 : m\}$$

のように生成する．

4.2.3 通信中の仮想アドレス変換処理

以後，EN は VAT テーブルに従い，送信するパケットの宛先 IP アドレスを V1 から G2 へ，宛先ポート番号をマッピングされたポート番号 m に変換する．NAT に届けられたパケットの宛先 IP アドレス・ポート番号は NAT テーブルに従って変換され，IN に届けられる．逆方向の通信についても同様のアドレス・ポート変換を行う．

以上の処理により，NAT を超えて End-to-End で通信を開始できる．

5. 提 案 技 術

ここでは，提案技術について説明する．本提案を実現するために NAT-f ネゴシエーションを拡張したため，拡張箇所について述べる．そして，提案技術の動作について説明する．

5.1 NAT-f ネゴシエーションの拡張

本提案を実現するために図 4 の NAT-f ネゴシエーションに拡張を加えた．NAT 配下の端末を指定するための情報として，IN のホスト名の代わりに IN の IP アドレスを送信する．これは，NAT 配下の端末を指定するための情報であるため，本質的には変更はない．しかし，通信プロトコルとしては，実際にやり取りする情報に変更が加えられている．

5.2 動 作 概 要

EN 及び IN は SIP 機能を持つ一般端末とする．SIP Proxy 2 及び NAT ルータに拡張 NAT-f 機能を実装する．

5.2.1 端末情報の登録

図 5 に端末情報登録時のシーケンスを示す．EN は SIP Proxy 2 に対して REGISTER に

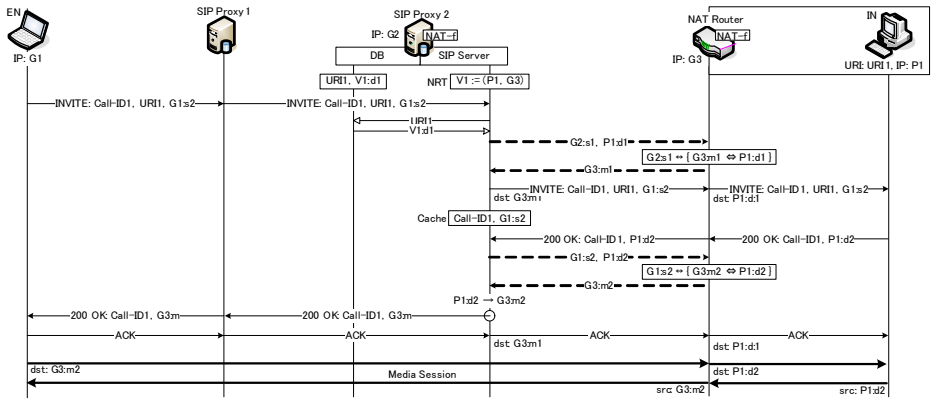


図 6 提案方式のシーケンス

より自身の URI と SIP メッセージを受信する際に使用するトランスポートアドレス P1:d1 の登録を要求する．SIP Proxy 2 は REGISTER 受信時に，記載されている IP アドレスを P1 から仮想アドレス V1 へ書き換えて DB に登録する．この時，SIP Proxy 2 は V1，P1，G3 の関係を NRT に保存し， 200 OK を IN に返答する．

5.2.2 通信開始時の動作

図 6 に通信開始時のシーケンスを示す．EN からの通信開始時，SIP Proxy 2 は EN からの INVITE を受信すると DB の内容により，INVITE の転送先となる V1:d1 を取得する．ここで，宛先 IP アドレス V1 が仮想アドレスであるため，SIP Proxy 2 と NAT ルータ間で NAT-f ネゴシエーションを実行する．SIP Proxy 2 は INVITE の送信元トランスポートアドレス G2:s1，宛先ポート番号 d1，及び NRT に保存した IN のアドレス P1 の情報を NAT ルータに送信する． NAT ルータはこれらの情報を用いて，SIP Proxy 2 と IN の SIP ネゴシエーションに必要な NAT テーブルを生成後，マッピングされた G3:m1 を返答する．SIP Proxy 2 はこのマッピングされたポートに向けて INVITE を送信する．また，SIP Proxy 2 は一連のシーケンスで共通する Call-ID と EN が使用するトランスポートアドレス G1:s2 を対応付けてキャッシュする．

SIP Proxy 2 は，INVITE に対する 200 OK を受信すると，先ほど作成したキャッシュの情報を Call-ID1 で検索し，NAT ルータに対して再度 NAT-f ネゴシエーションを実行する．SIP Proxy 2 は EN のトランスポートアドレス G1:s2 と IN のトランスポートアドレ

ス P1:d2 を通知して EN と IN 間の通信で必要な NAT テーブルを生成する．即ち，SIP Proxy 2 の指示により，NAT ルータ内に EN と IN 間の通信に必要となる NAT テーブルが生成される．SIP Proxy 2 は 200 OK に記載されているトランスポートアドレスを P1:d2 から G3:m2 へ書き換え，転送する．

200 OK を受け取った EN は，ACK 返答した後，交換したトランスポーアドレスに従い，メディアセッションを確立することができる．

6. ま と め

本論文では，NAT-f を利用した SIP の NAT 越えに手法ついて検討した．

SIP Proxy による NAT 外部から内部の IN に対する INVITE に先立ち，SIP Proxy が NAT ルータに対して NAT-f ネゴシエーションを実行し，SIP Proxy と IN 間の通信に必要な NAT テーブルを生成する．また，SIP Proxy が EN と IN 間のセッションの確立に先立ち，NAT ルータに対して NAT-f ネゴシエーションを実行し，EN と IN 間の通信に通信に必要な NAT テーブルを生成する手法を提案した．

今後は，実装と動作確認を行う．

参 考 文 献

1) P.Srisuresh and K.Egevang: Traditional IP Network Address Translator (Traditional NAT), RFC 3022, IETF (2001).
2) 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).
3) J.Rosenberg, H.Schulzrinne, G.Camarillo, A.Johnston, J.Peterson, R.Sparks, M.Handley and E.Schooler: SIP: Session Initiation Protocol, RFC 3261, IETF (2002).
4) J.Rosenberg and H.Schulzrinne: An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing, RFC 3581, IETF (2003).
5) Forum, U.: Internet Gateway Device (IGD) Standardized Device Control Protocol V 1.0 (2001). http://www.upnp.org/.
6) J.Rosenberg, J.Weinberger, C.Huitema and R.Mahy: STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs), RFC 3489, IETF (2003).
7) A.Johnston, S.Donovan, R.Sparks, C.Cunningham and K.Summers: Session Initiation Protocol (SIP) Basic Call Flow Examples, RFC 3665, IETF (2003).
8) P.Vixie, S.Thomson, Y.Rekhter and J.Bound: Dynamic Updates in the Domain Name System (DNS UPDATE), RFC 2136, IETF (1997).

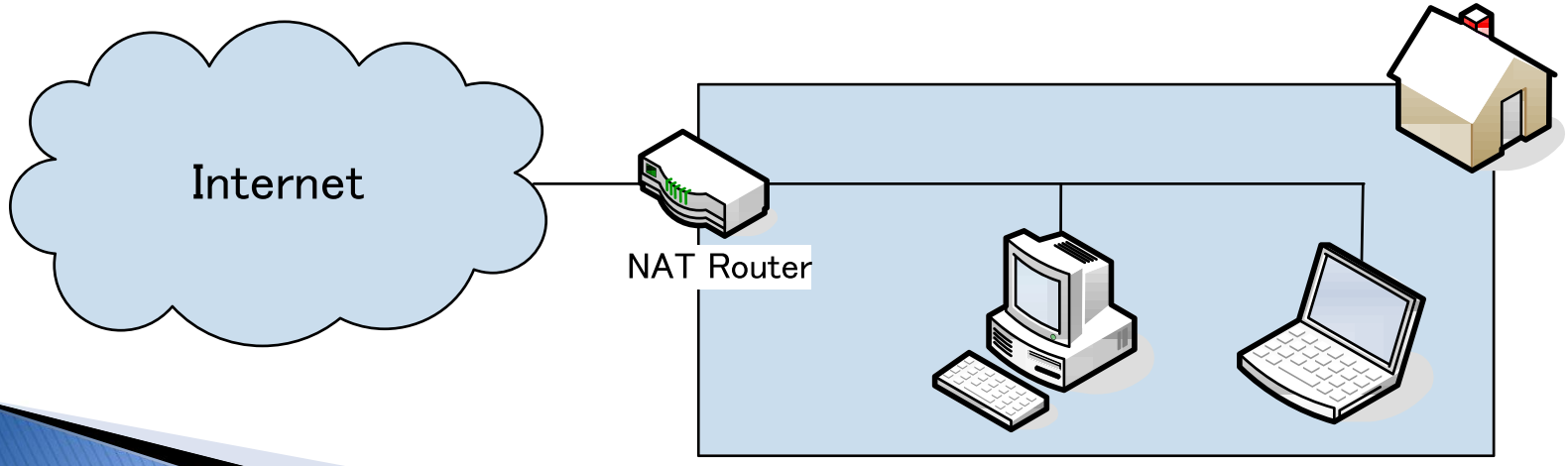
NAT-fを利用したSIPのNAT越え通信方式の提案

名城大学大学院　理工学研究科
三浦 健吉，鈴木秀和，渡邊晃

はじめに

- 一般家庭のネットワークはプライベートIPアドレスで構築
  ⇒ NAT(Network Address Translator)*が使用される

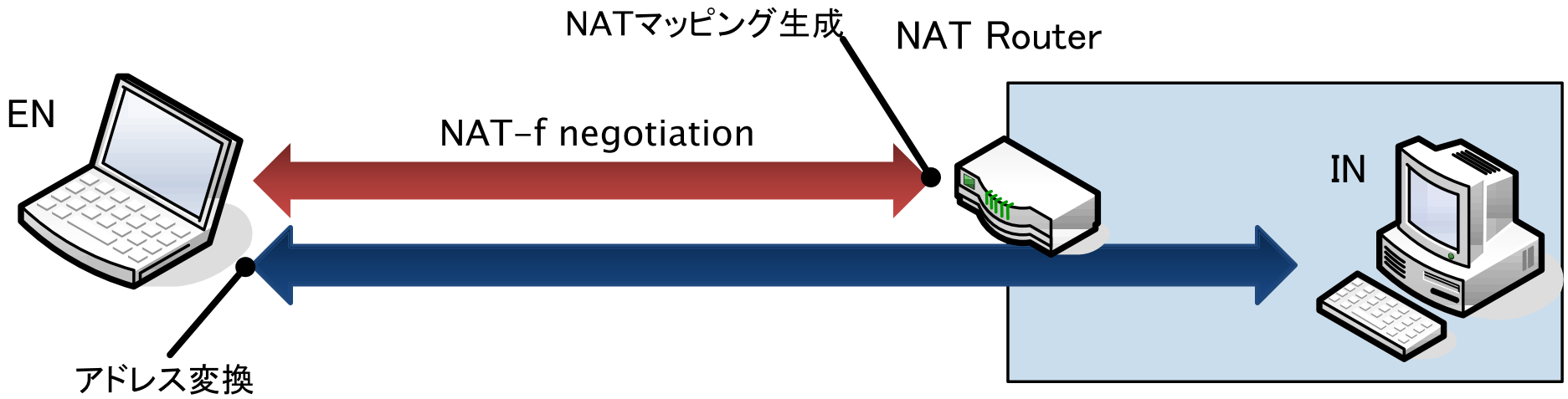
- NAT
  - 1個のグローバルIPアドレスを複数のノードで共有する技術
  - 一般家庭のブロードバンドルータに大抵搭載されている



*本スライドでは，NAPTを含めてNATと呼ぶ

NAT-f

- NAT-f(NAT-free protocol)*
  - 通信に先立ち，ENはNATにマッピングを指示
  - パケットの宛先をマッピングアドレスに変換



*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越えを実現するNAT-fの提案と実装"，情報処理学会論文誌，No.12，pp.3949-3961.

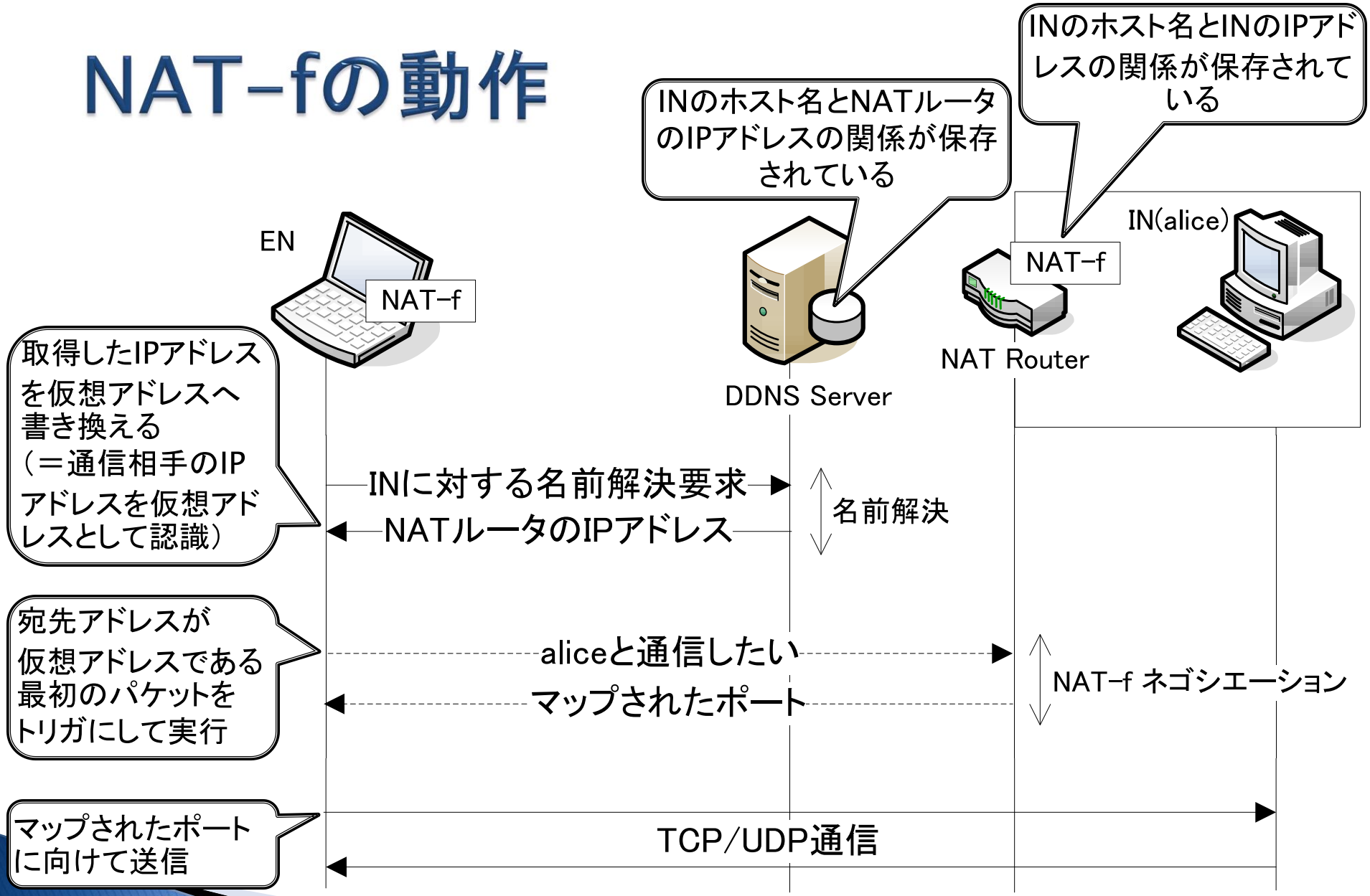
NAT-fの利点と課題

- 利点
  - End-to-Endで通信可能（中継サーバは不必要）
  - アプリケーションに依存しない

- 課題
  - IPペイロード内にIPアドレスが埋め込まれるプロトコルに対応できない
    - プロトコルの例：SIP, ftp

⇒NAT-fにSIP対応機能を付け加える提案

NAT-fの動作



EN: External Node 外部ノード
IN: Internal Node 内部ノード

NAT-fのポイント

- 宛先IPアドレスが仮想アドレスのとき，NAT-fネゴシエーション実行

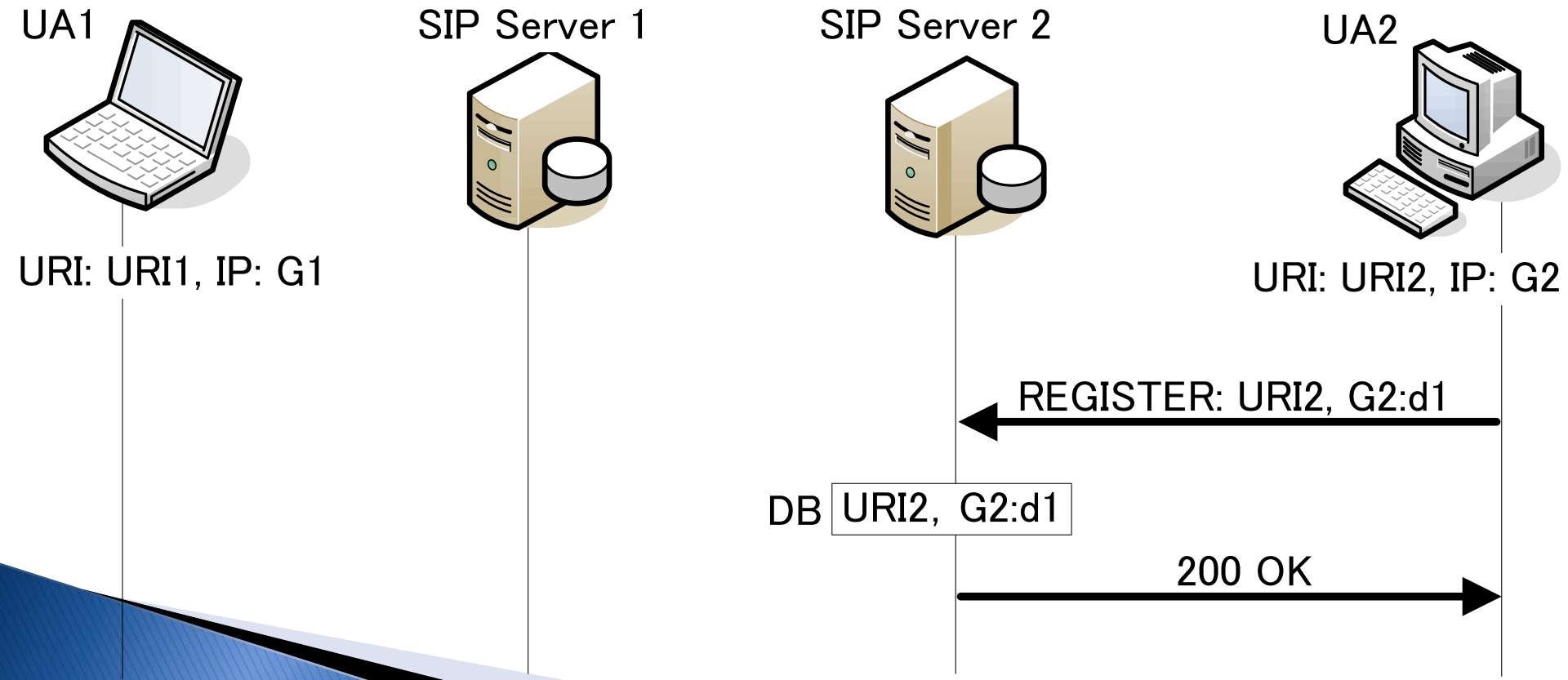
SIP(Session Initiation Protocol)

- IP電話や情報家電などで使用されている

- セッションを確立するためのプロトコル
  - 通信相手の呼び出し
  - 通信方式の交渉
  - セッションを確立すると、通信が開始される

SIPの基本シーケンス(1/2)

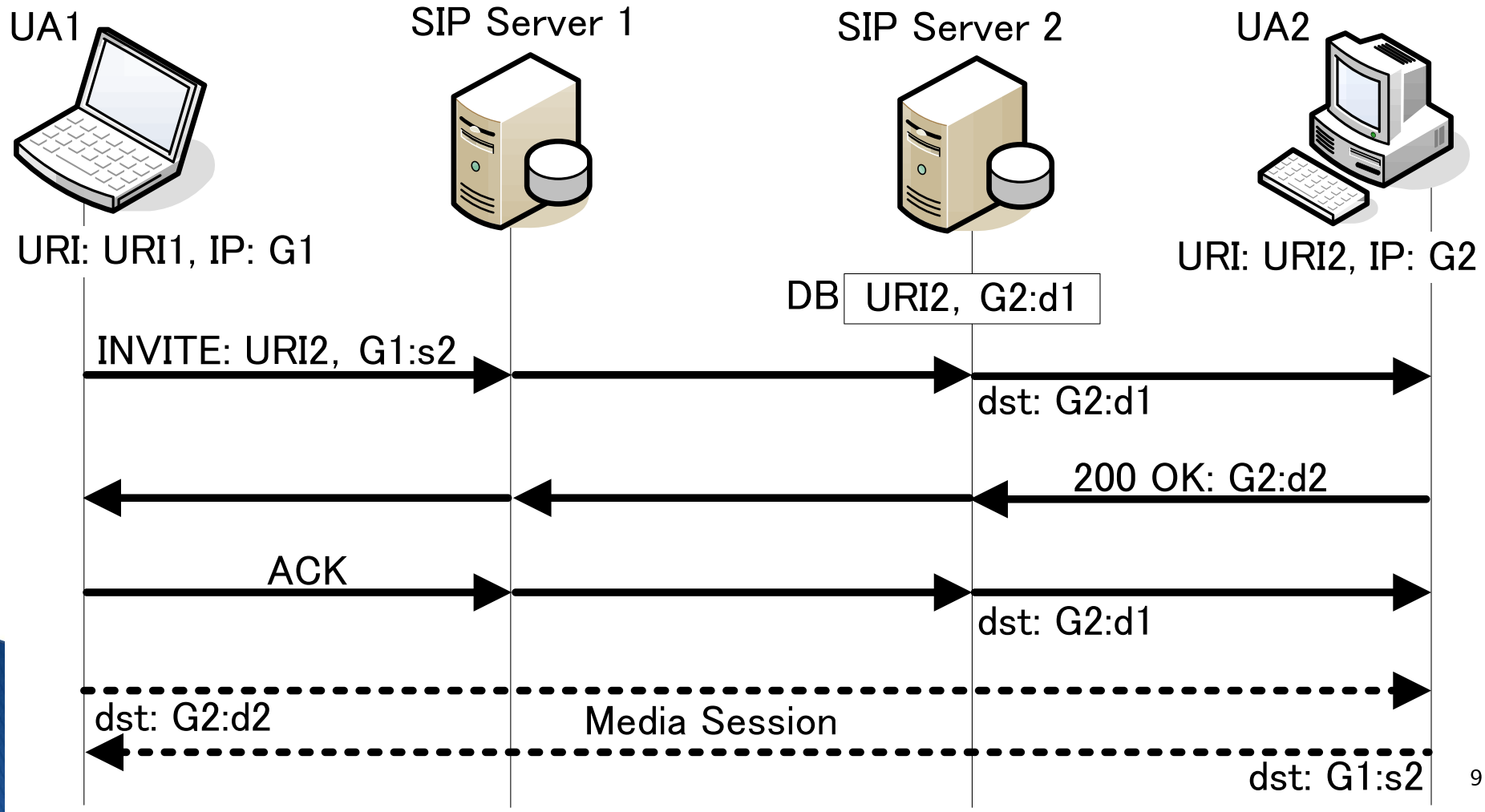
- 端末情報の登録



トランスポートアドレス: IPアドレスとポート番号の組

SIPの基本シーケンス(2/2)

- トランスポートアドレスを交換し，セッションを確立



SIPのポイント

- SIPの動作手順
  1. 端末情報の登録
  2. シグナリングによりトランスポートアドレスを交換
  3. 交換したトランスポートアドレスに基づいてセッション確立

- SIPはポートを2つ使用する
  - s1/d1：シグナリングにおいて使用するポート
  - s2/d2：音声通信において使用するポート

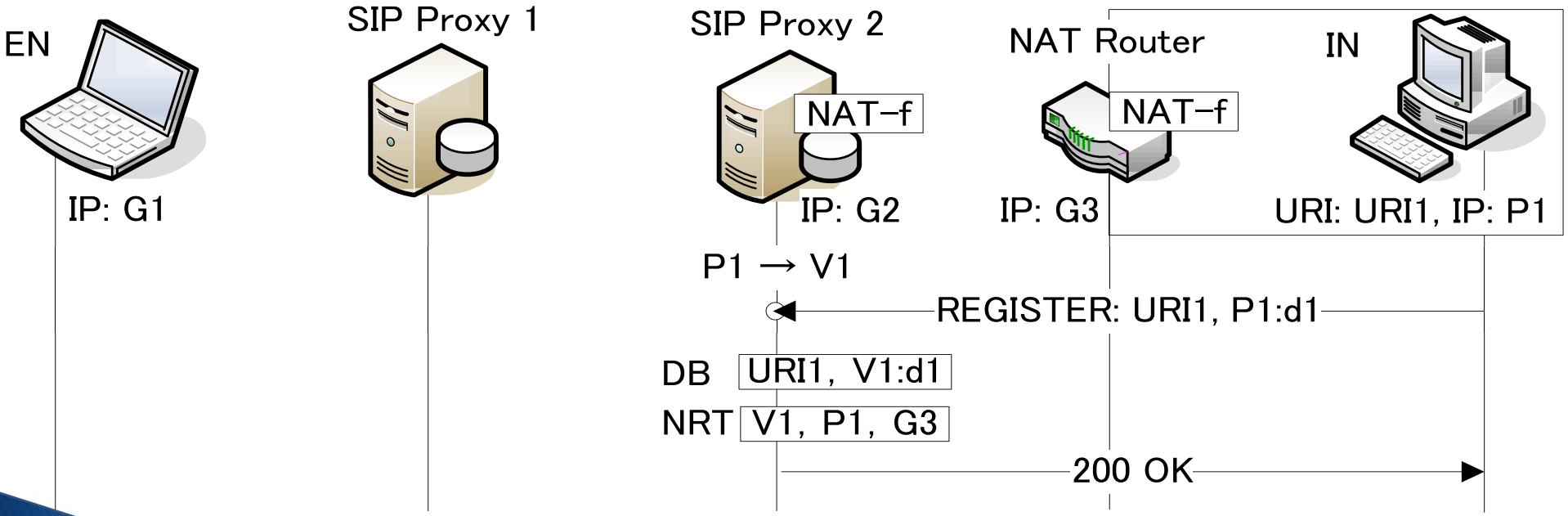
  ⇒ NAT越えには，それぞれのポートについて対応する必要有り

SIPとNAT

- 通常のNAT越え問題
  - NATの外部から内部に向けてシグナリングを開始できない
- IPペイロード内（SIPメッセージ内）にIPアドレスが埋め込まれる
  - 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
    - IPヘッダ内のIPアドレス → NATで変換される
    - IPペイロード内のIPアドレス → NATで変換されない

提案方式(1/3)

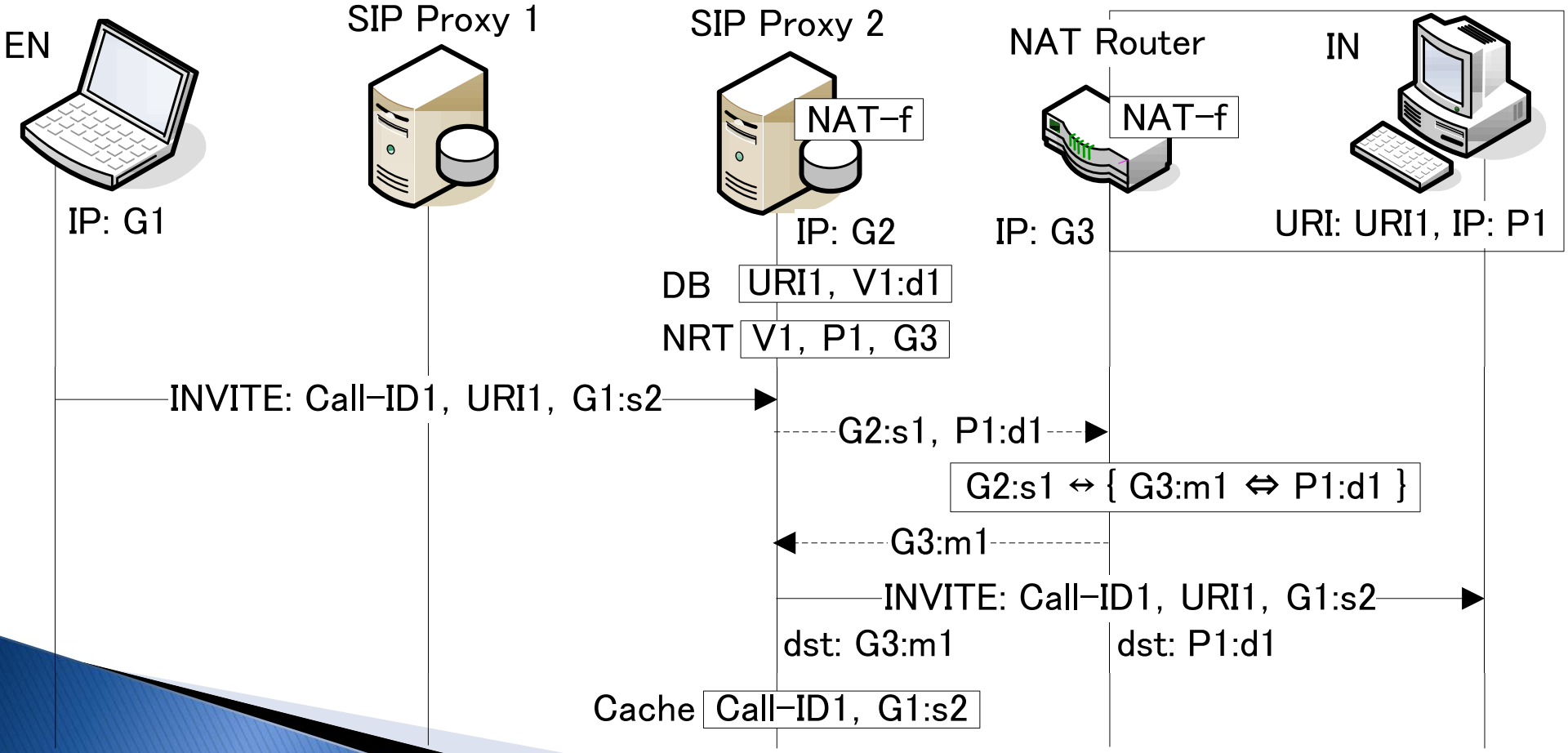
- 端末情報の登録
  - DBには仮想アドレスが登録される
  - アドレス書き換えと同時に，NRT生成



NRT: Name Relation Table 名前関連テーブル

提案方式(2/3)

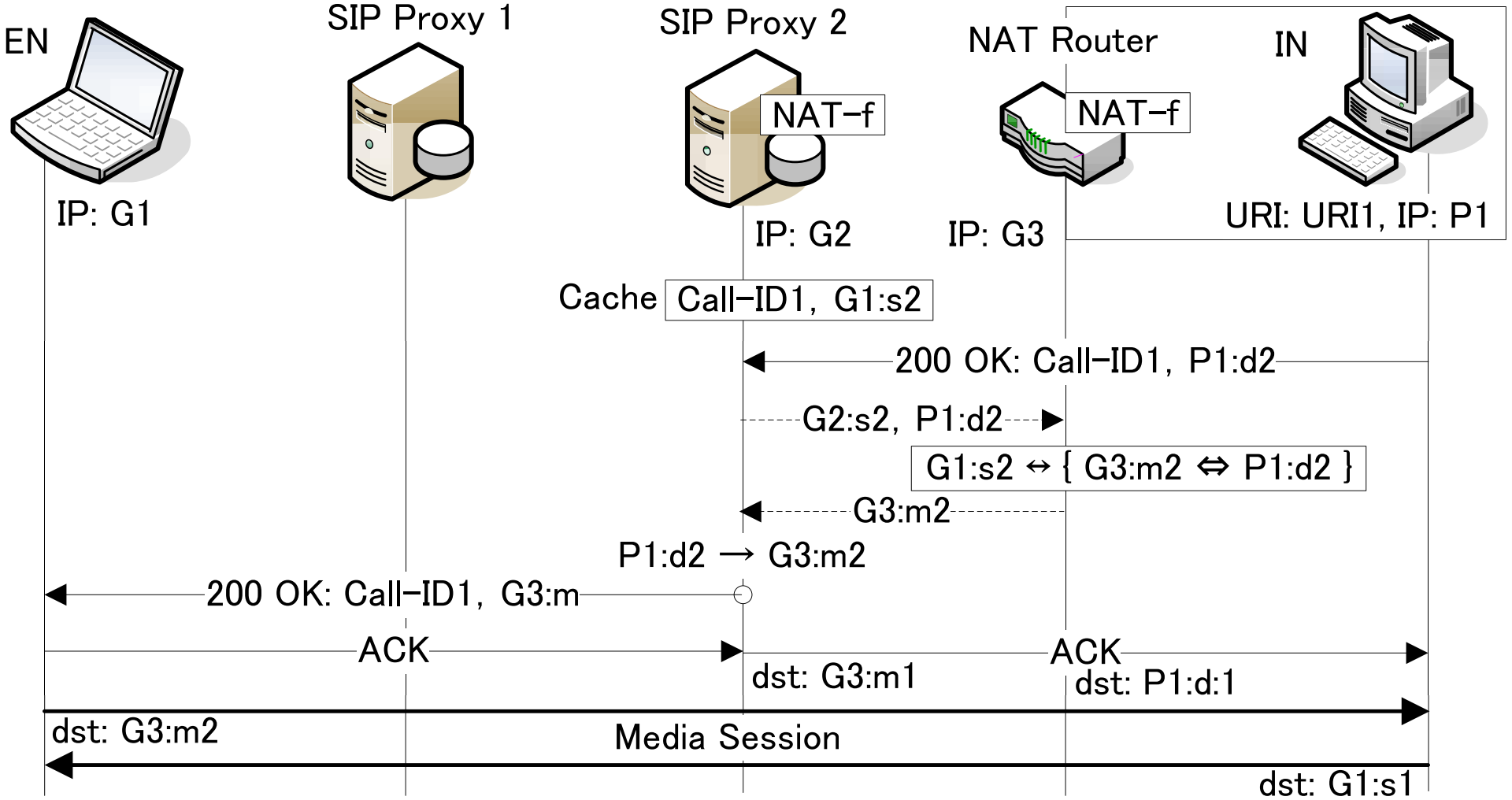
- SIPプロキシ2とIN間のNAT越え



Call-ID: 一連のシグナリングで共通するID

提案方式(3/3)

- ENとIN間のNAT越え



むすび

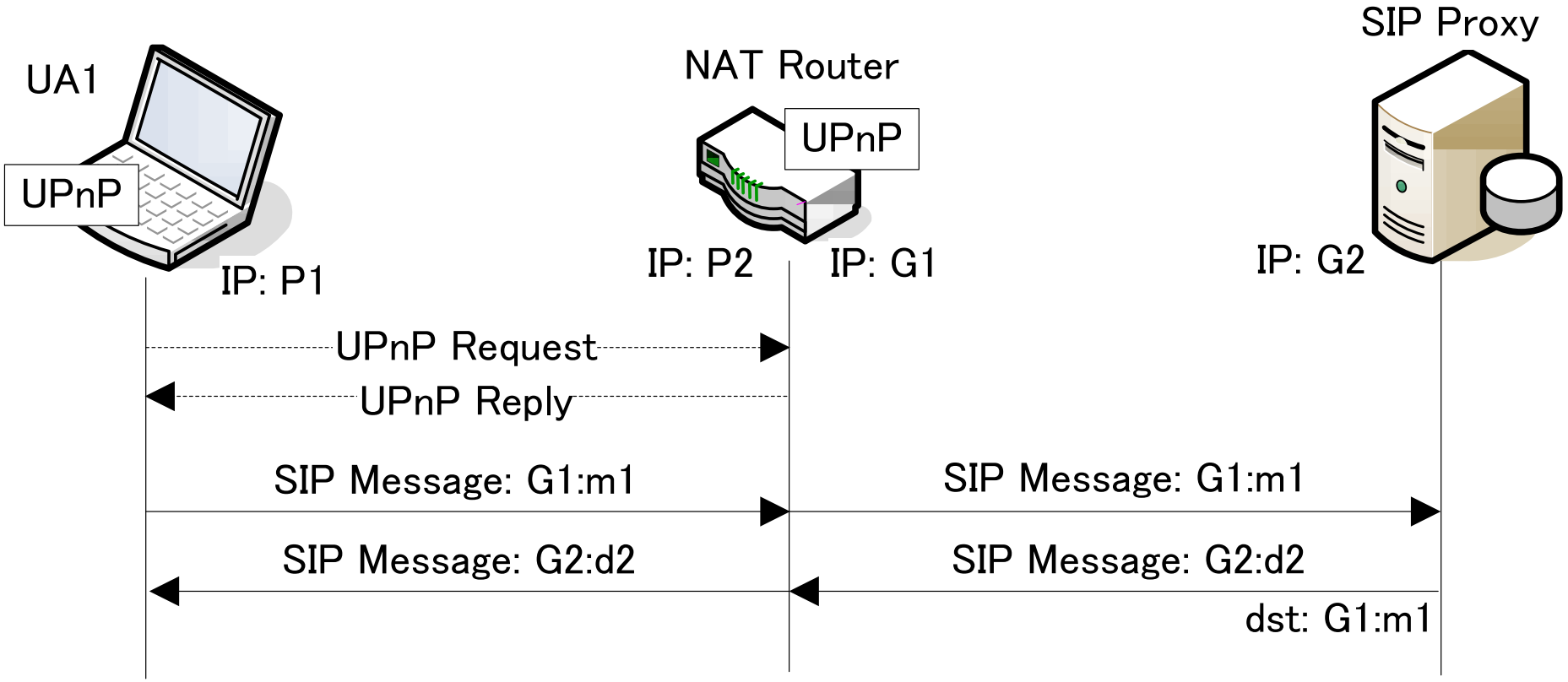
- NAT-fにSIP対応機能を付け加える提案を行った
- SIPサーバがNAT-fネゴシエーションを2回実行
  - シグナリング用のマッピング（SIPサーバとINの間）
  - 音声通信用のマッピング（ENとINの間）
- 今後は，実装と性能評価を行う．

補足資料

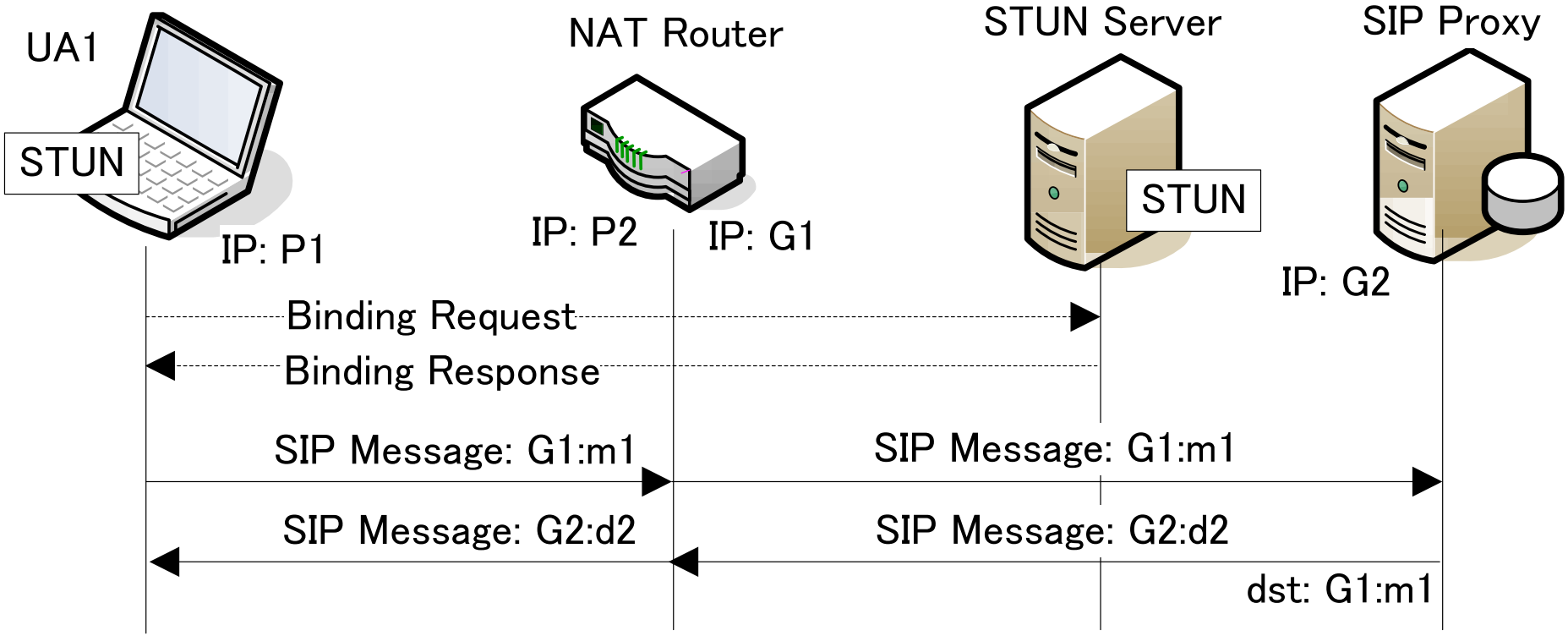
既存技術

- アドレス埋め込み型：UPnP、STUN
  - SIPメッセージを送信する際に，予めNAT越え問題が解決済みのIPアドレス・ポート番号を埋め込んでおく方式
- アドレス書き換え型：ALG
  - アドレス書き換え型は，NATがSIPメッセージ中のIPアドレス・ポート番号の書き換える方式
- サーバ中継型：TURN
  - サーバ中継型は，グローバルネットワークに設置されたサーバを中継し，通信を行うことで，NAT越えを実現する方式

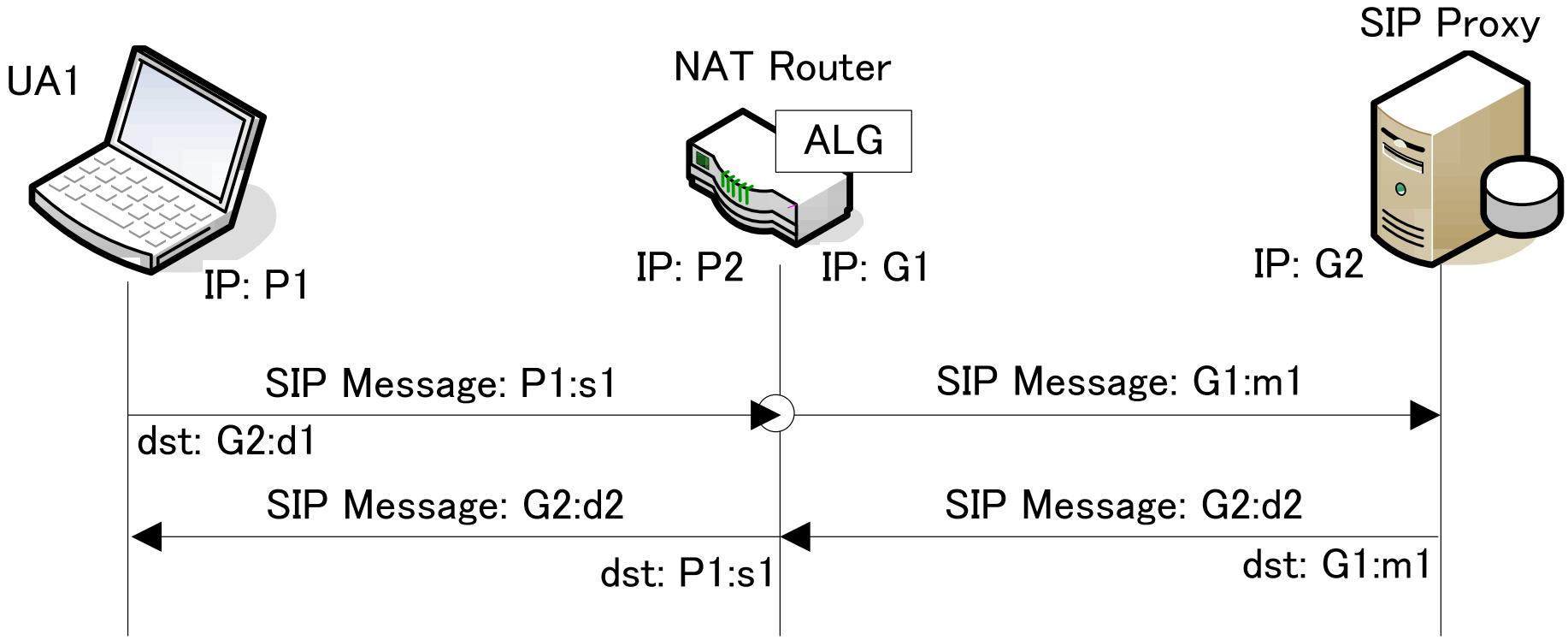
UPnP: Universal Plug and Play



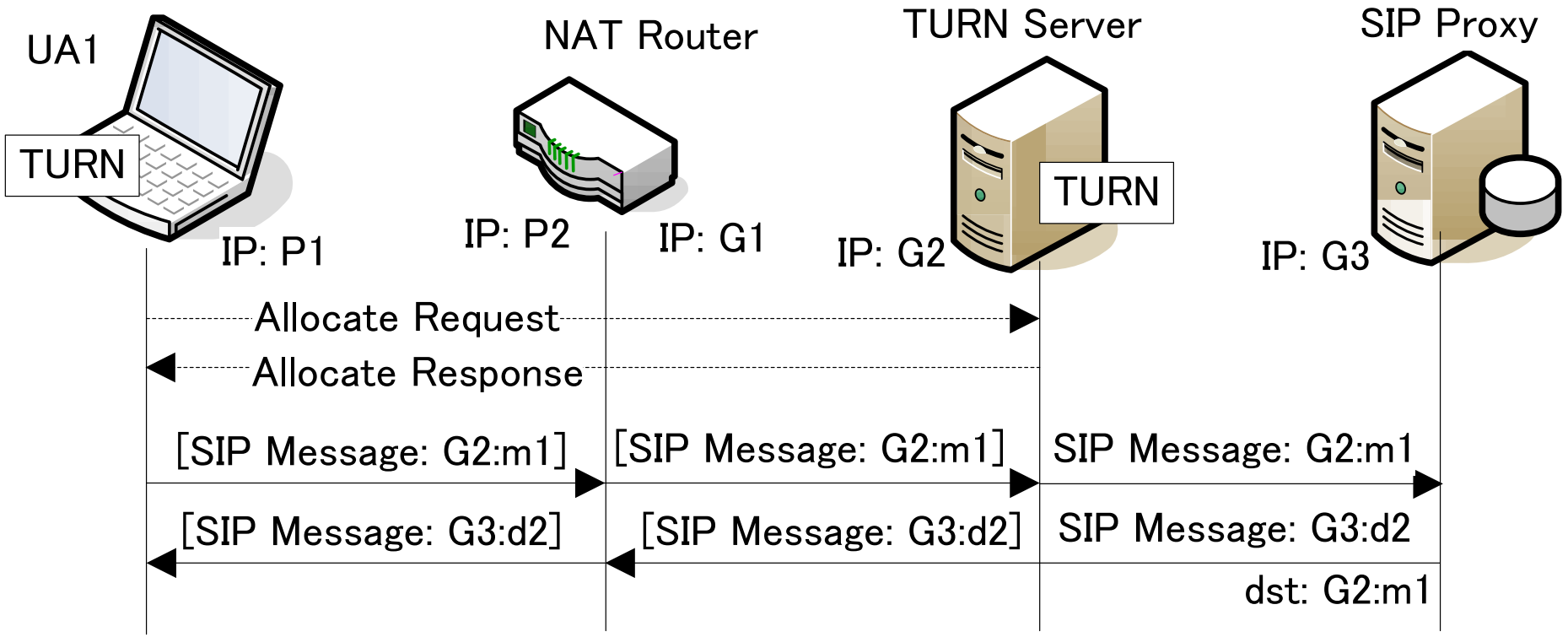
STUN: Simple Traversal of UDP through Network Address Translators



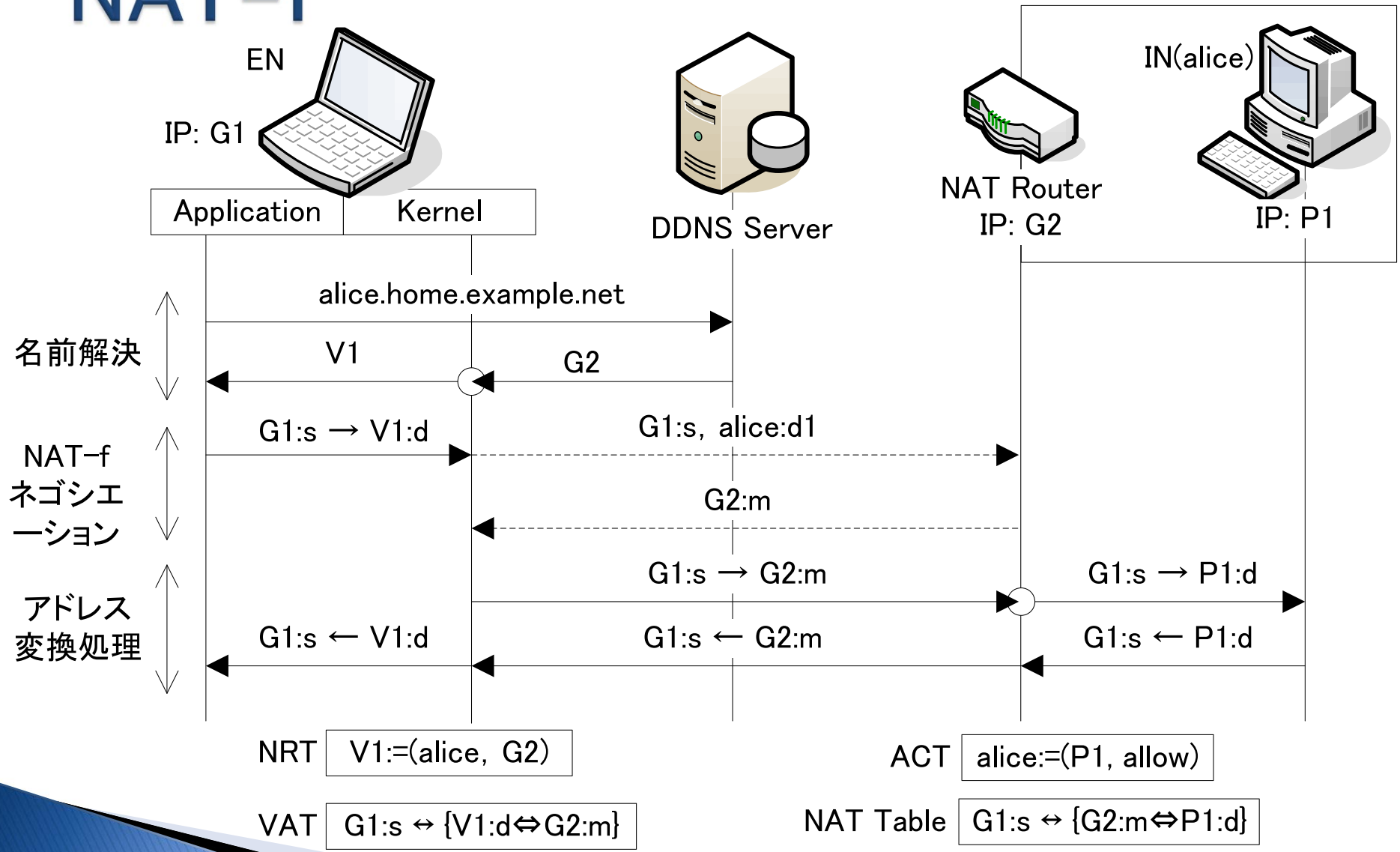
ALG: Application Level Gateway



TURN: Traversal Using Relay NAT



NAT-f


EN
IP: G1
Application
Kernel
DDNS Server
NAT Router
IP: G2
IN(alice)
IP: P1
alice.home.example.net
名前解決
V1
G2
G1:s → V1:d
G1:s, alice:d1
NAT-f
ネゴシエ
ーション
G2:m
G1:s → G2:m
G1:s → P1:d
アドレス
変換処理
G1:s ← V1:d
G1:s ← G2:m
G1:s ← P1:d
NRT
V1:=(alice, G2)
VAT
G1:s ↔ {V1:d⇔G2:m}
ACT
alice:=(P1, allow)
NAT Table
G1:s ↔ {G2:m⇔P1:d}