端末に依存しないNAT越え通信に関する研究

073432029 宮崎 悠
渡邊研究室

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形態が一般的である．それらのネットワークとインターネットの間にはアドレス変換装置 (以下 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 の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，サーバ/クライアントモデルに基づいたシステムであり，一般にインターネット上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，近年の急速なインターネットの普及に伴い，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必要性は高まっている．

NAT 越え問題を解決する為にこれまで様々な解決手法が提案されている．既存技術の代表として，STUN (Simple Traversal of User Datagram Protocol Through Network Address Translators)[1]，AVES(Address Virtualization Enabling Service)[2] および NAT-f (NAT-free protocol)[3] などがある．STUN はインターネット上の専用サーバを利用することにより NAT 越えを実現するが，第三の装置が必要で，かつアプリケーションが限定されるという課題がある．AVES は waypoint と呼ばれる特殊なサーバと改造したルータが協調し，waypoint がパケットを中継することにより NAT 越えを実現する．しかし，STUN と同様に専用のサーバが必要であり，通信経路が冗長になるという課題がある．NAT-f はインターネット上の端末と NAT ルータが連携することによりエンドエンドで NAT 越えを実現できる．しかし，端末の通信機能を改造する必要があることから，一般ユーザが導入するのは難しいという課題がある．

今後は携帯端末など，機能追加が難しい端末を用いた通信も要求されることが予想される．そこで本論文では改造した DNS サーバと NAT ルータが協調して NAT 越え通信を実現することにより，エンドのユーザ端末に機能を追加することなく，エンドエンドの通信を実現できる方式を提案する．

提案方式を FreeBSD 上に実装し, 動作検証を行った．

2 既存技術（AVES）

既存の NAT 越え通信の中で，AVES は端末に改造を加える必要がなく，目的が本研究と一致している．そこで，AVES について詳細に説明する．

AVES ではインターネット上に waypoint と呼ばれる機器を配置し，それを経由して通信を行う．EN が DNS サーバに IN の名前解決を行うと，DNS サーバは waypoint と IN についてのルート確認情報を交換する．ルート確認情報には IN のプライベート IP アドレスとその NAT ルータのグローバル IP アドレスが含まれる．その後 DNS サーバは waypoint の IP アドレスを EN に応答する．EN は waypoint を IN と見なして通信を開始する．waypoint は EN からのパケットを NAT ルータ宛のアドレスでカプセル化して NAT ルータへ送信する．NAT は上記パケットのカプセル化を解除し IN へ送信する．IN からの応答は直接 EN へ送信される．以後，同様にして三角経路での通信を行う．

AVES はユーザ端末に機能を実装をせずに NAT 越えを実現できるという利点があるが，第三の特殊な装置が必要で，かつ DNS を改造する必要がある．また経路が冗長になることや，IP in IP カプセリングによるパケット冗長が発生するなどの課題がある．

3 提案方式

本提案方式を NTS(NAT-Traversal Support) システムと呼び，本方式で使用する改造した DNS サーバを NTS サーバ，改造した NAT ルータを NTS ルータ，実行するプロトコルを NTS プロトコルと呼ぶ．EN と IN は一般の端末で構わない．提案方式で必要となる装置は次の通りである．インターネット上にはプライベートネットワークと接続するための NTS ルータ，DNS サーバを改造した NTS サーバ，IN の名前解決に使用する DDNS サーバが存在する．ここで EN，NTS ルータのグローバル IP アドレスをそれぞれ GA1，GA2，IN(alice) のプライベート IP アドレスを PA1 とする．alice はプライベート端末のホスト名である．以下の動作説明では EN から IN(alice) へ通信を開始する場合の例を，事前設定，名前解決，通信開始にわけ，それぞれ説明する．

3.1 事前設定

提案方式を適用するに当たり，EN はプライマリ DNS として NTS サーバを登録しておく．外部からの通信を許可するにあたり，IN は予め FQDN(Fully Qualified Domain Name) と NTS ルータのアドレスを DDNS に登録しておく．また NTS ルータに，IN プライベート IP アドレスと FQDN の関係を PHL(Private Host List) と呼ぶテーブルに登録しておく．

3.2 DNS 名前解決

図 1 に EN から IN(alice) へ通信を開始する場合の名前解決シーケンスを示す．EN は IN(alice) と通信を開始す

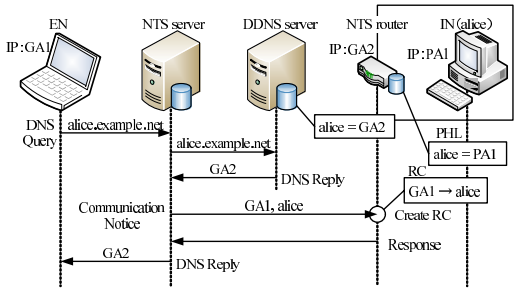


図 1: 名前解決シーケンス

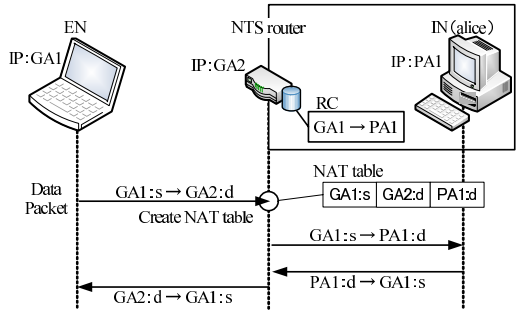


図 2: 通信開始シーケンス

るに当たり，alice.example.net の名前解決を NTS サーバへ依頼する．依頼を受けた NTS サーバは通常の DNS 名前解決処理により，NTS ルータの IP アドレス GA2 を取得する[1]．次に NTS サーバは EN から alice への接続依頼があることを NTS ルータに通知する．NTS ルータこの通知を受け取ると PHL を参照し，“GA1 から PA1 へ通信がある” ということを RC(Request Cache) へ記憶しておく．NTS サーバは NTS ルータの応答を受信した後，EN に対して NTS ルータのアドレス GA2 を応答する．

3.3 通信開始

図 2 に通信開始シーケンスを示す．EN は取得した IP アドレス GA2 へ向けて通信を開始する．NTS ルータは上記パケットを受け取ると RC の内容を確認する．該当する RC があれば，受け取ったパケットと RC の情報から宛先・送信元 IP アドレスとポート番号，プロトコルタイプから NAT テーブルを動的に生成する．NTS ルータはこの生成した NAT テーブルに従いパケットを IN(alice) に転送する．これに対する alice からの応答パケットもこの NAT 処理に従い内側から外側へ転送される．

4 実装

プロトタイプシステムとして，NTS サーバモジュールを FreeBSD のアプリケーションとして，NTS ルータモジュールを FreeBSD のルータに実装した．

4.1 NTS サーバ

図 3 に NTS サーバの実装概要を示す．NTS サーバには DNS アプリケーションの BIND をインストールし，これを 10053 番ポートでリッスンするように設定する．また，NTS サーバ処理モジュールは通常の DNS アプリケーションと同様に TCP/UDP の 53 番ポートでリッスンし，各ユーザ端末からの DNS パケットを受信し，通常の DNS 処理は BIND へ受け渡す．DNS リクエストパケットを受け取った BIND は通常の DNS 機能により名前解決を行い，NTS サーバモジュールへ DNS レスポンスパケットを返す．NTS サーバモジュールは応答された IP アドレスへ EN から通信要求があることを通知する．このネゴシエーション後，NTS サーバは EN に対して DNS レスポンスパケットを返信する．上記手順により，EN にとって NTS サーバはあたかも通常の DNS サーバの様に振る舞う．

4.2 NTS ルータ

図 4 に NTS ルータの実装概要を示す．natd（NAT デーモン）は NAT 機能を持つ FreeBSD のデーモンであり，NTS ルータはこれを最大限利用する．通常の NAT の動作は以下の通りである．受信したパケットは下位層から IP 層の

[1]図 1 では NTS サーバと DDNS サーバ間の DNS シーケンスは省略してある．

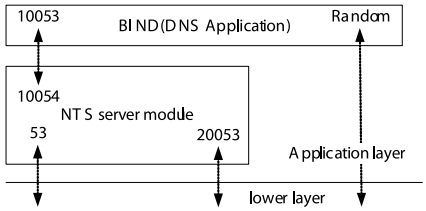


図 3: NTS サーバの実装概要

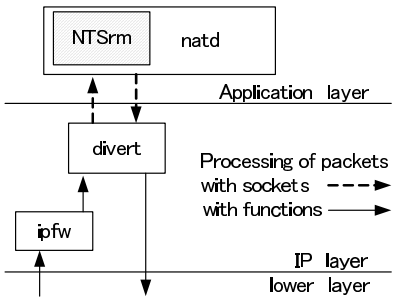


図 4: NTS ルータの実装概要

ファイアウォールモジュール ipfw に渡される．次に natd は divert ソケットを介してパケットを取り出し，NAT 処理を行う．その後パケットを divert ソケットを介して下位層に渡し，アドレス変換されたパケットが送信される．NTS ルータの実装では，natd にパケットを操作する NTS ルータモジュールを挿入する．NTS ルータモジュールでは NTS サーバとの通信や，NAT テーブルを生成する為に必要な処理を行う．

5 動作検証

EN から IN へ FTP 接続を開始した結果，ファイル転送が NAT を越えて実行できることを確認した．また複数の IN に対して，同時に HTTP 通信ができることを確認した．その結果，EN と IN の間で自由な双方向通信が可能であることを実証できた．

6 まとめ

本論文ではユーザ端末の改造が不要な NAT 越えを実現する方式を提案した．提案方式では EN の通信開始に先駆けて，NTS サーバと NTS ルータが協調することにより NTS ルータが動的に NAT テーブルを生成することにより NAT 越え通信を可能にする．各端末間の通信はエンドエンドで行うことができ，今後のユビキタス社会に有益なシステムと考えられる．

プロトタイプシステムの実装を行い，動作を検証した．

参考文献

[1] Rosenberg, J., Weinberger, J., Huitema, C. and Mahy, R.: STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs), RFC 3489, IETF (2003).

[2] 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).

[3] 鈴木秀和，　渡邊晃：アドレス空間透過性を実現する NAT-f の実装と評価，マルチメディア，分散，協調とモバイル（DICOMO2006）シンポジウム論文集，Vol.2006, Vol. 2006, No. 6, pp. 453–456 (2006).

端末依存しないNAT越え通信に関する研究

名城大学大学院　理工学研究科　情報科学専攻
073432029　宮﨑 悠

研究背景

- インターネットの普及に伴ない，ユビキタス社会化が進んでいる

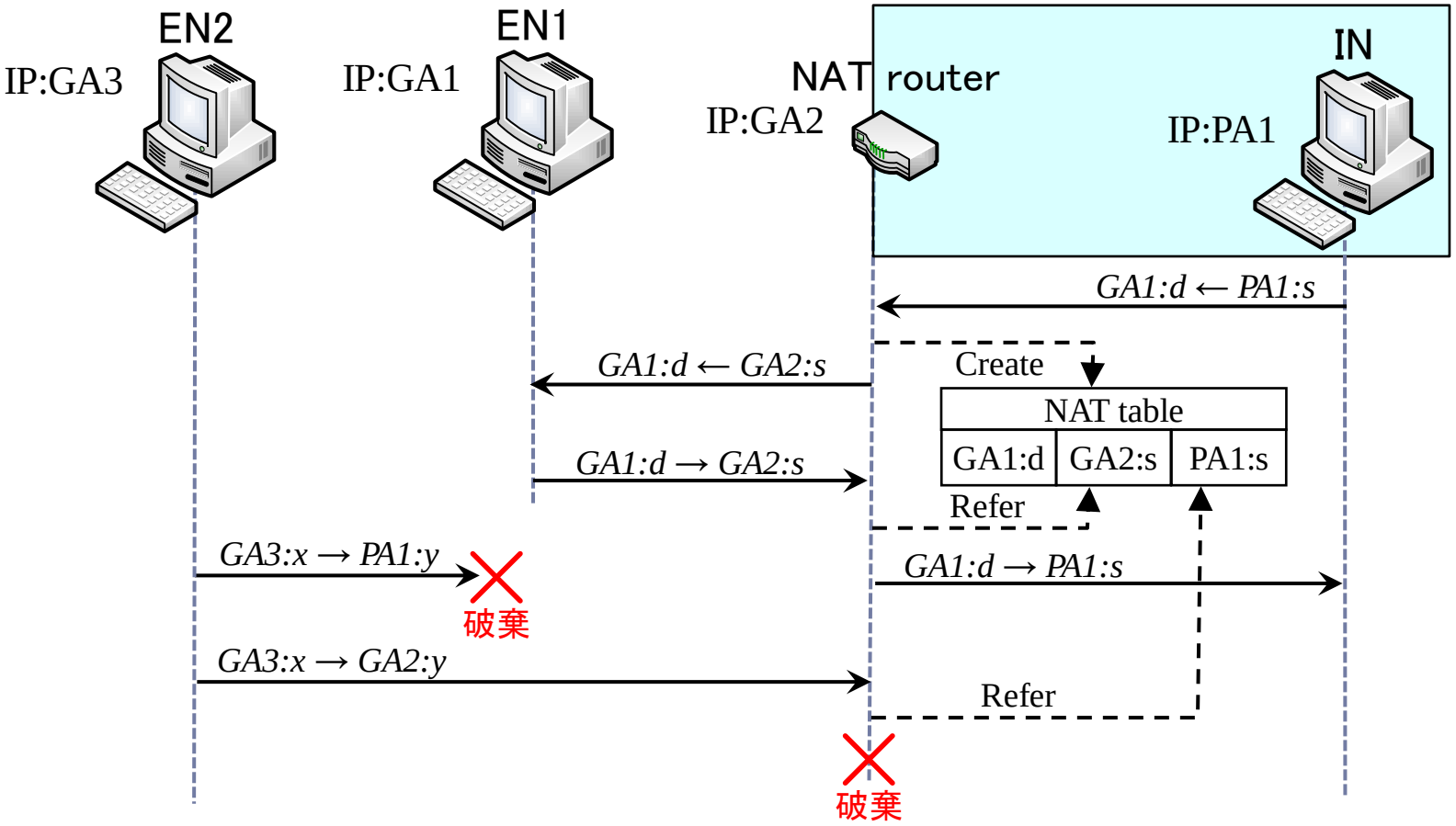
  →いつでもどこからでも通信したい

- 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される場合が多い

  →NAT(Network Address Translator)が使用される

NATの動作

- 通常はNATの内側からは通信を開始



NAT越え問題

インターネット環境の変化

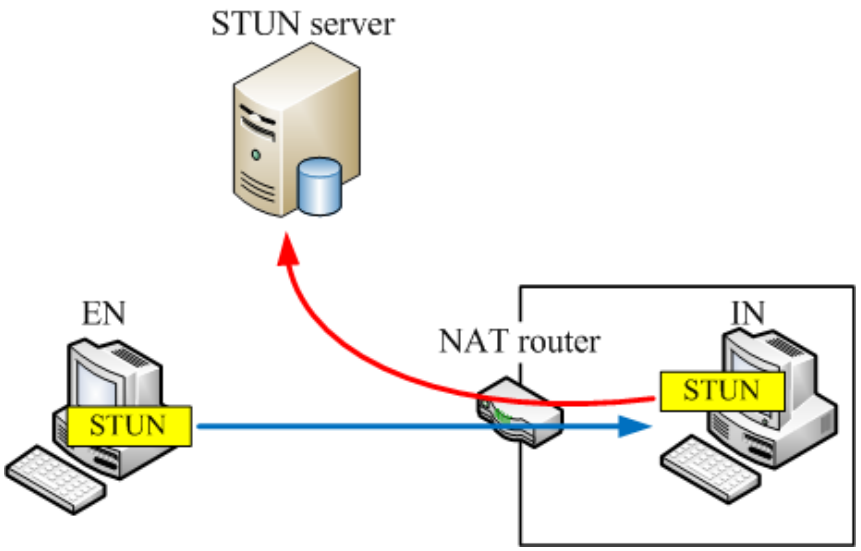
- 通常はNATの外側から通信を開始することはない
  - サーバ・クライアントモデル
- 今後考えられる進展
  - 情報家電
  - モバイル端末
- NAT越え通信を実現することは有益である.
  - アドレス空間の違いに影響されない通信
  - P2P通信

NAT越え通信における主な既存技術

- STUN :RFC5389

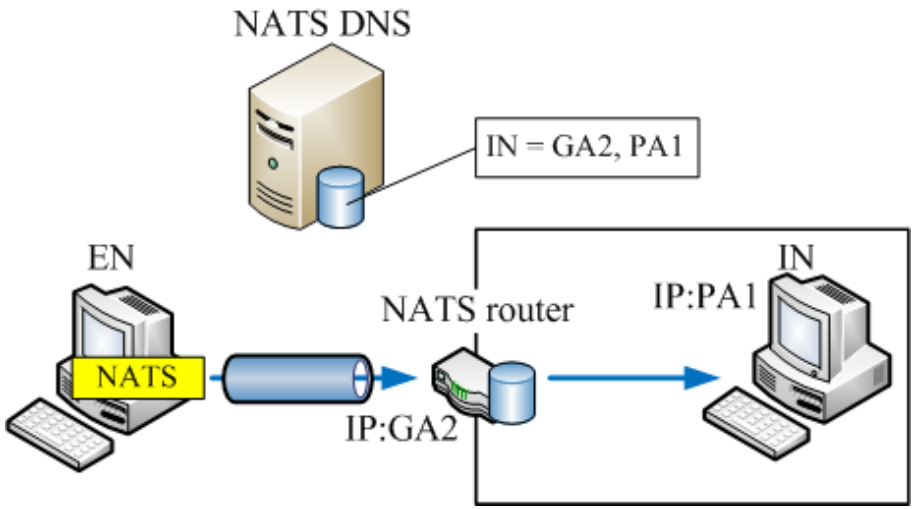
(Session Traversal Utilities for NAT)

  - EN,INへアプリケーション
  - 専用サーバ



  - 利点:実現容易
  - 欠点:通信の限定

- NATS (NAT with Sub-Address)
  - EN,NAT,DNSサーバへ実装
  - 通信をカプセル化



  - 利点:自由な通信
  - 欠点:導入難易度，スループットの低下

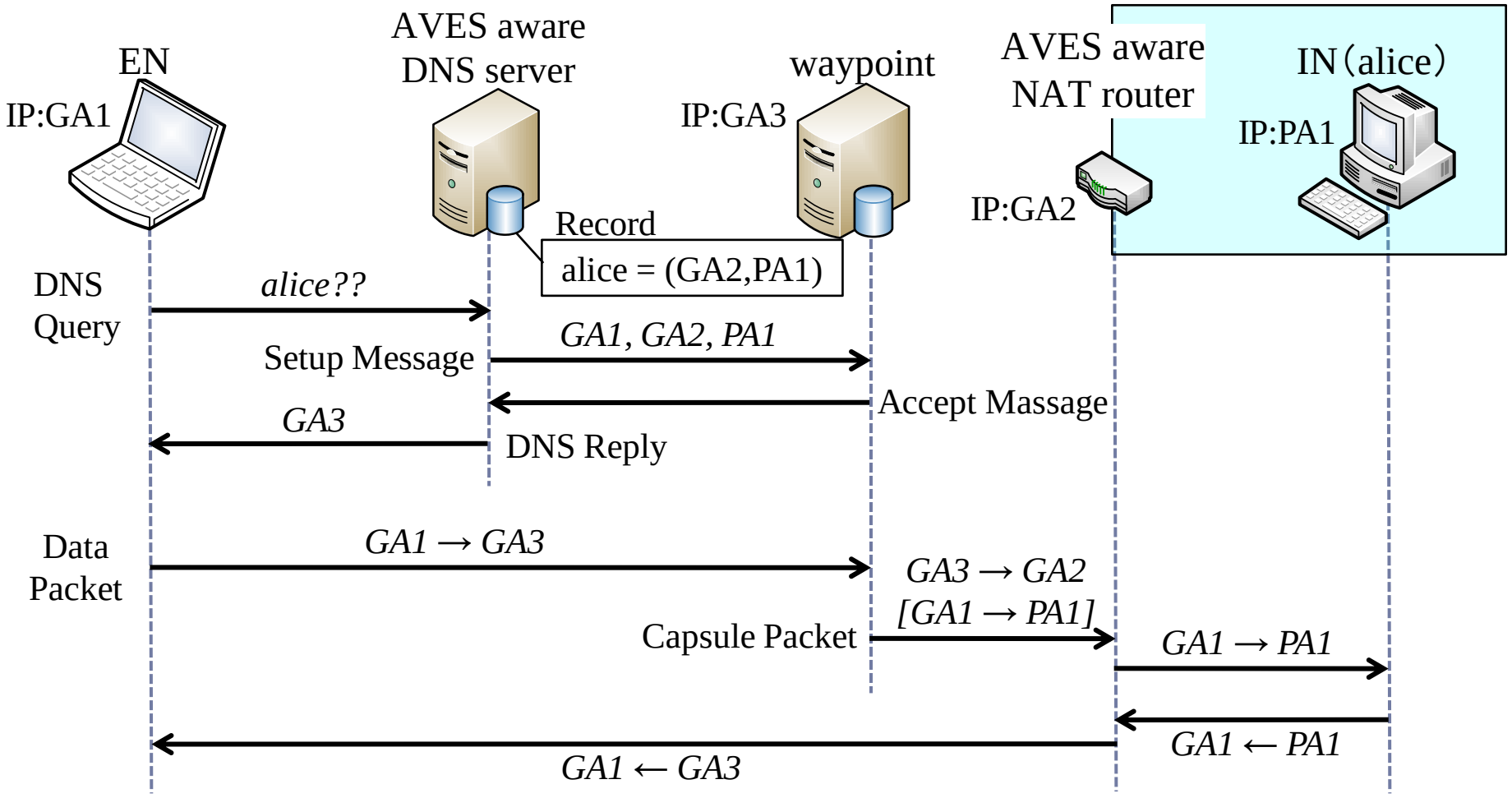
研究目的

端末に機能を加えることなく
NAT越えを実現したい

- ユーザはNATの存在を意識する必要はない
  - 出掛け先の端末から，会社や自宅のプライベートネットワークへ通信を行うことができる
- 利用端末を選ばない
  - モバイル端末から家庭内の情報家電へアクセス

端末への実装不要なNAT越え既存技術

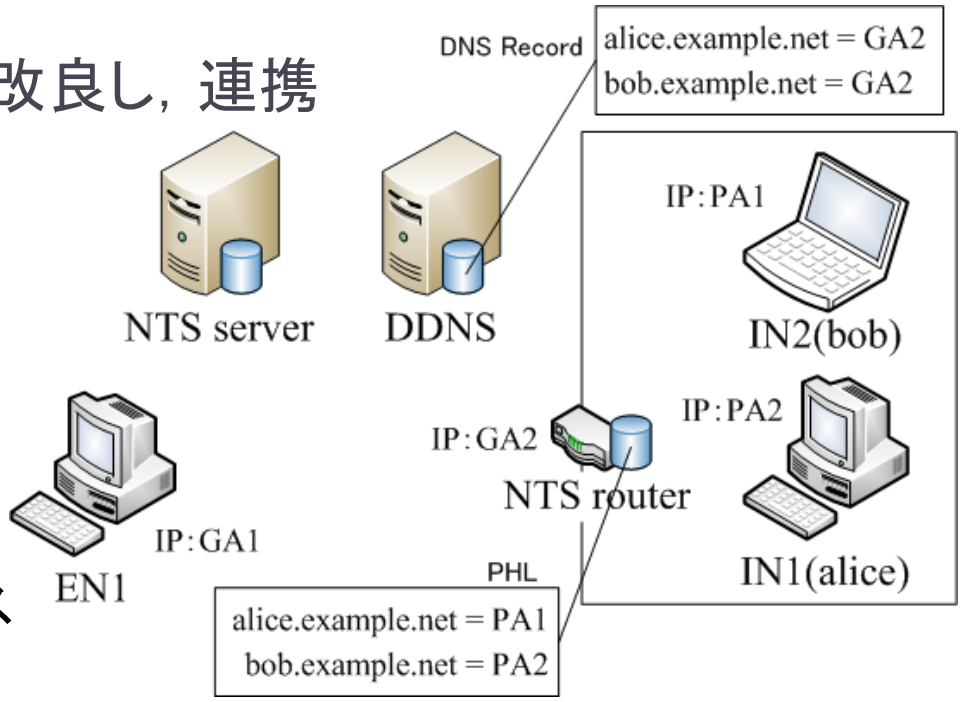
AVES(Address Virtualization Enabling Service)



提案方式（構成と事前設定）

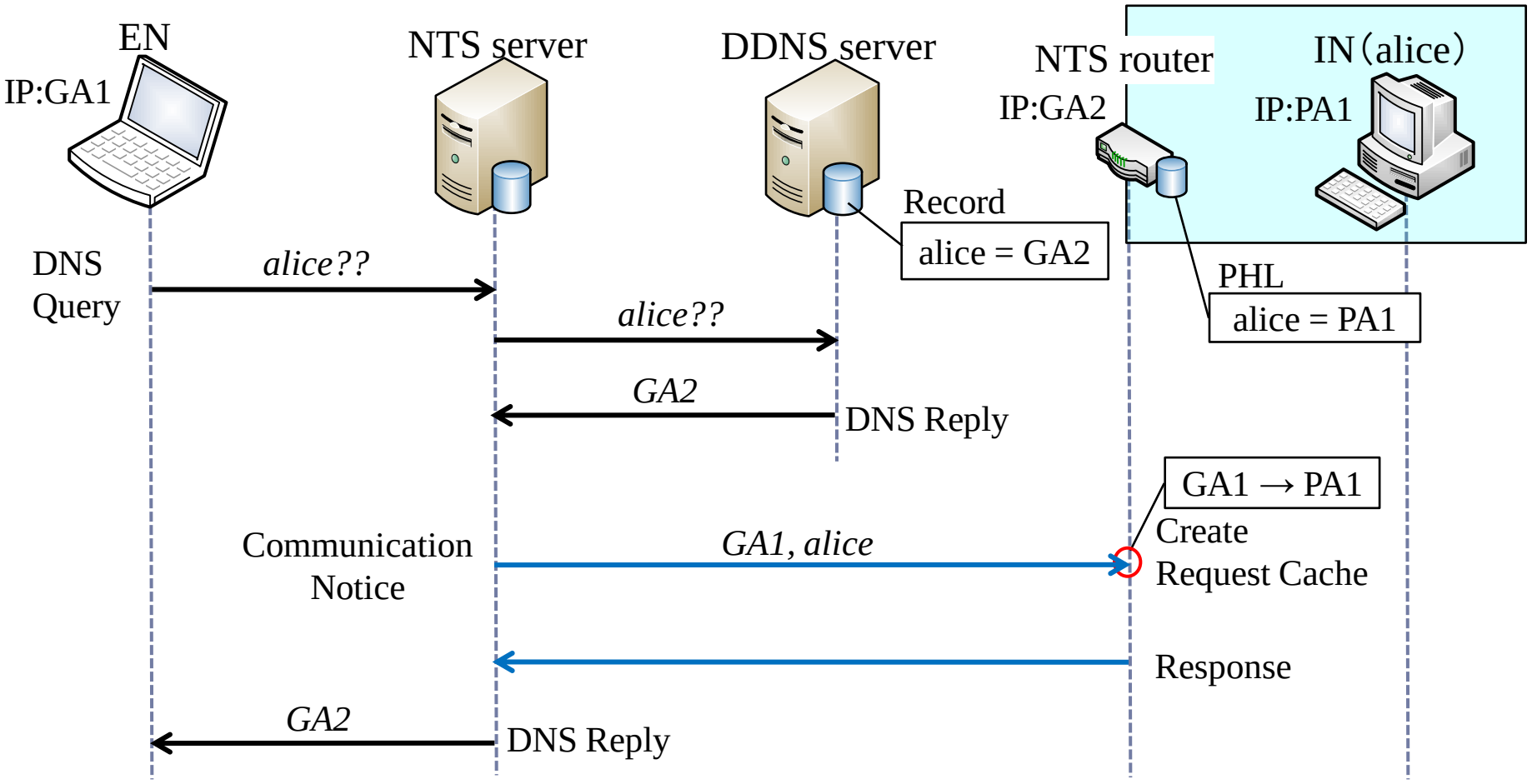
- 構成
  - DNSサーバとNATルータを改良し，連携
    - DNSサーバ：NTSサーバ
    - NATルータ：NTSルータ

(NAT-Traversal Support)

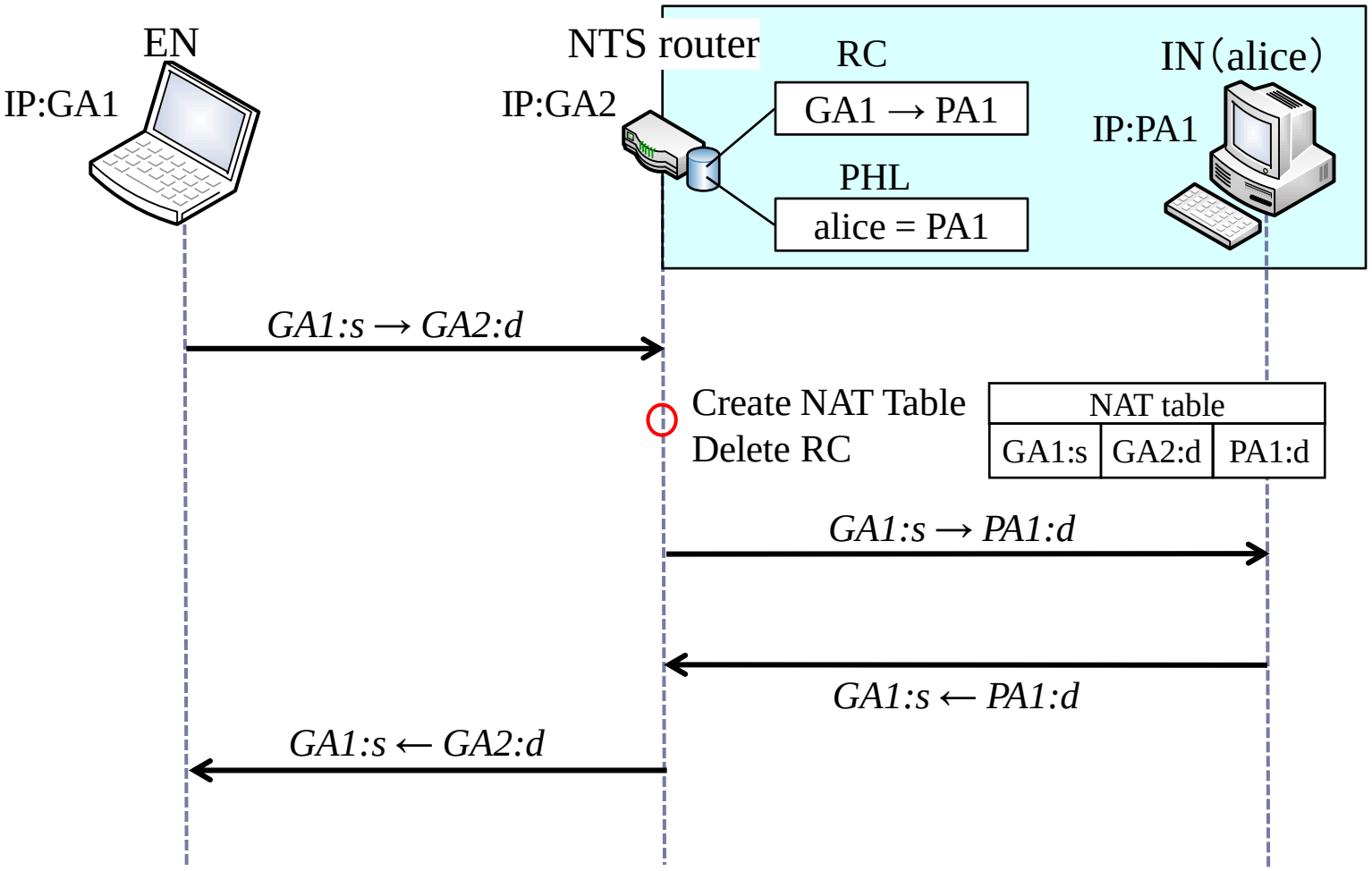


- 事前設定
  - DDNSへ登録
    - FQDNとNTSルータのIPアドレス
  - NTSルータへ登録
    - FQDNとINのプライベートIPアドレス
    - PHL(Private Host List)
  - ENのプライマリDNSをNTSサーバに設定

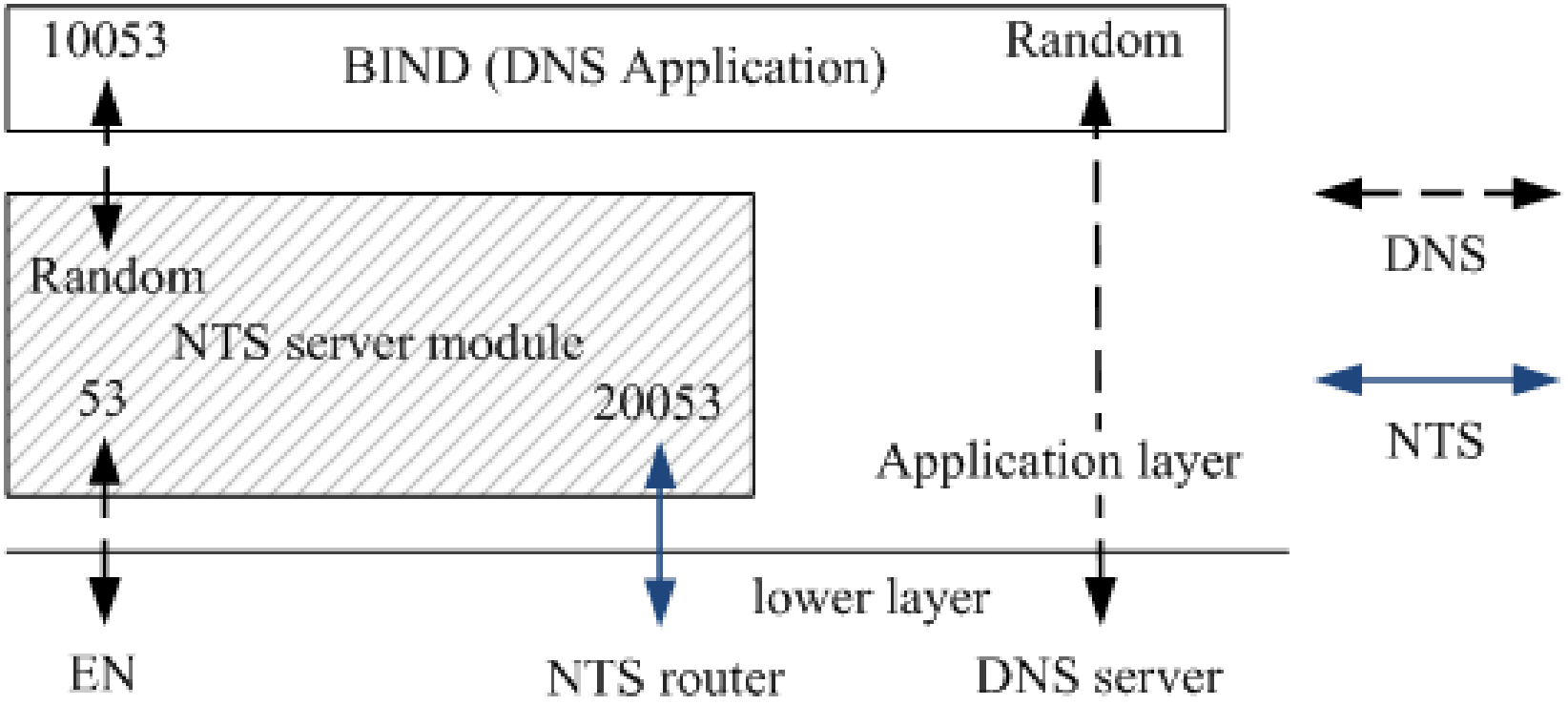
提案方式（名前解決）


EN
IP:GA1
NTS server
DDNS server
NTS router
IP:GA2
IN（alice）
IP:PA1
Record
alice = GA2
PHL
alice = PA1
DNS
Query
alice??
alice??
GA2
DNS Reply
GA1 → PA1
Create
Request Cache
Communication
Notice
GA1, alice
Response
GA2
DNS Reply

提案方式（通信開始）


EN
IP:GA1
NTS router
IP:GA2
RC
GA1 → PA1
PHL
alice = PA1
IN（alice）
IP:PA1
GA1:s → GA2:d
Create NAT Table
Delete RC
NAT table
GA1:s
GA2:d
PA1:d
GA1:s → PA1:d
GA1:s ← PA1:d
GA1:s ← GA2:d

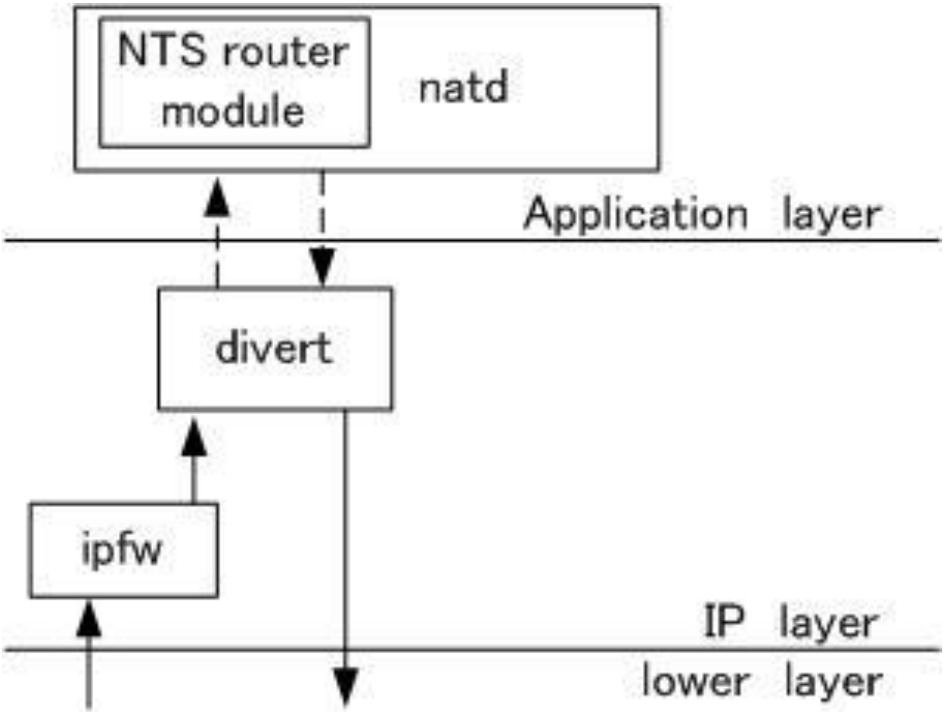
実装概要（NTS Server on FreeBSD）



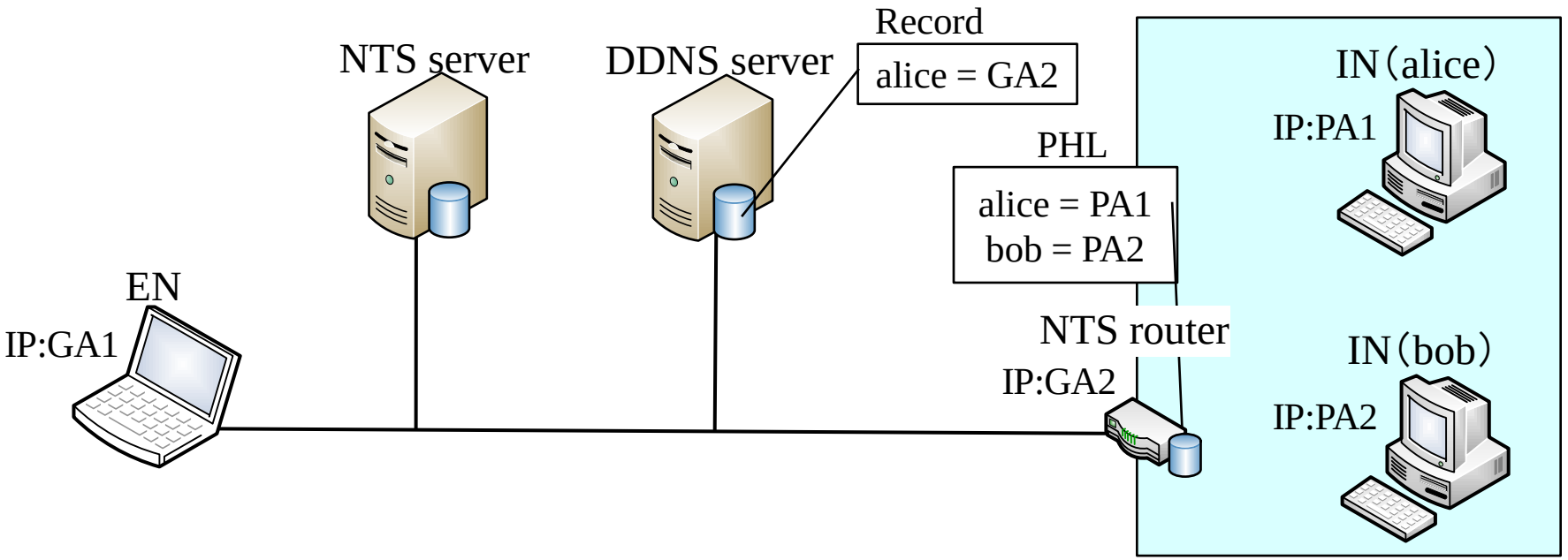
- NTSが53番で待ち，DNS-requestを受け取る
- 役割はDNSパケットを中継・解析してNTSネゴシエーションを行うのみ

実装概要（NTS Router on FreeBSD）

- ipfw：ファイアウォールの動作モジュール
- divert：natdのパケット取り出しをサポートするソケット
- natd：NAT機能を持つデーモン



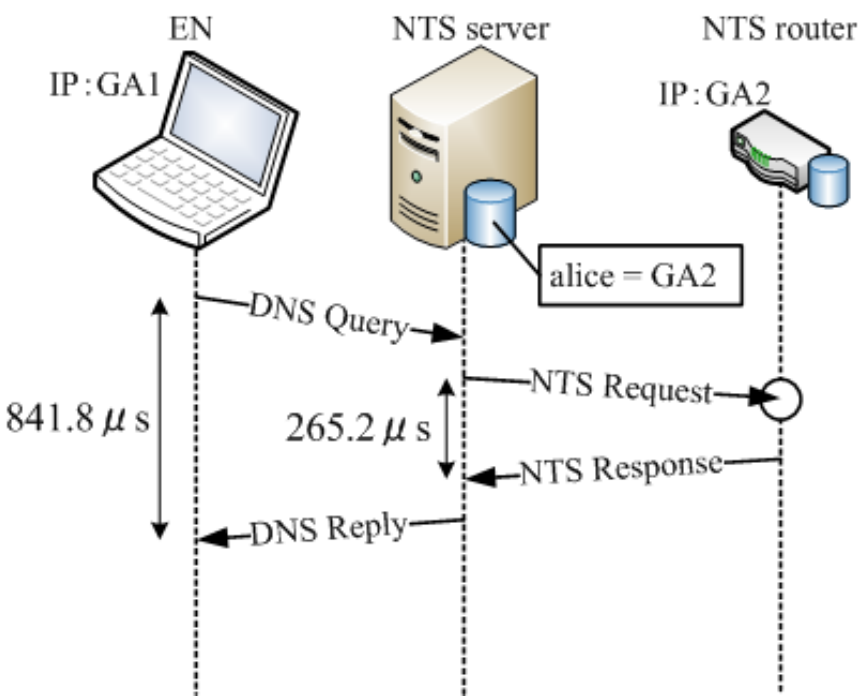
動作検証

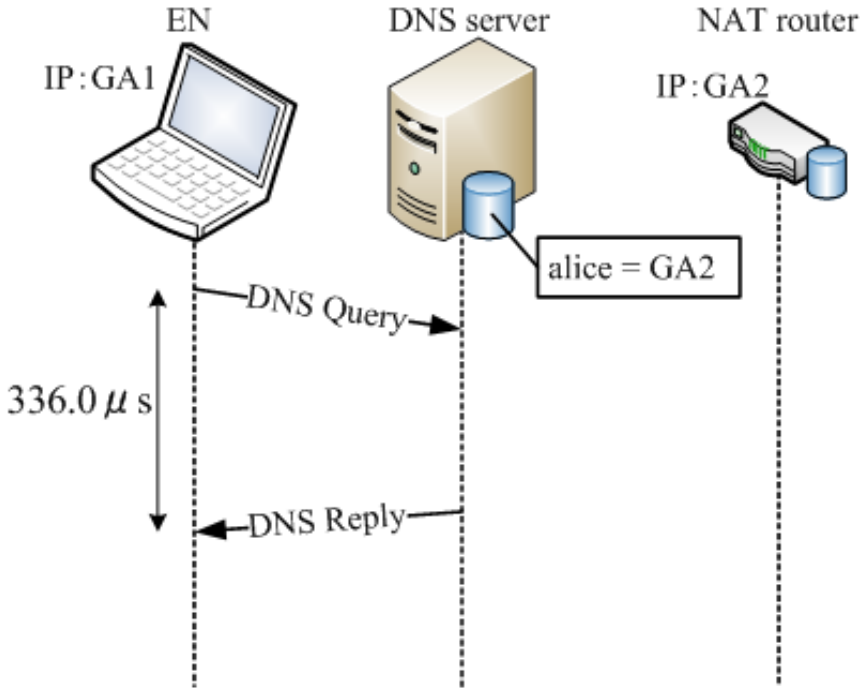


- EN，NTSルータ，NTSサーバ，DNSサーバをスイッチで接続
  - 100BASE-TX
- ENからINへFTP接続
- 複数のINに対して，同時HTTP通信

性能測定 (Overheads)

- 名前解決時のオーバヘッドを測定（Ethereal，10回試行平均）
  - NTS server，DNS serverそれぞれがaliceのレコードを所持





  - ＊　RTTの短い実験的な環境

性能測定 (Throughputs)

- スループットを測定（netperf，10回試行平均）
  - 通常のNATを介した通信と比較するため，
    通常NATの内側から外側への通信も測定

スループットを測定（Mbps）				
Message Size	TCP		UDP	
(Bytes)	NTS	NAT	NTS	NAT
64	94.1	94.1	49.3	49.3
128	94.1	94.1	66.0	66.0
256	94.1	94.1	79.6	79.6
512	94.1	94.1	88.9	88.9
1024	94.1	94.1	94.4	94.4

測定環境	
CPU	Pentium4 3.0GHz
Memory	512MB
Ethernet	100BASE-TX

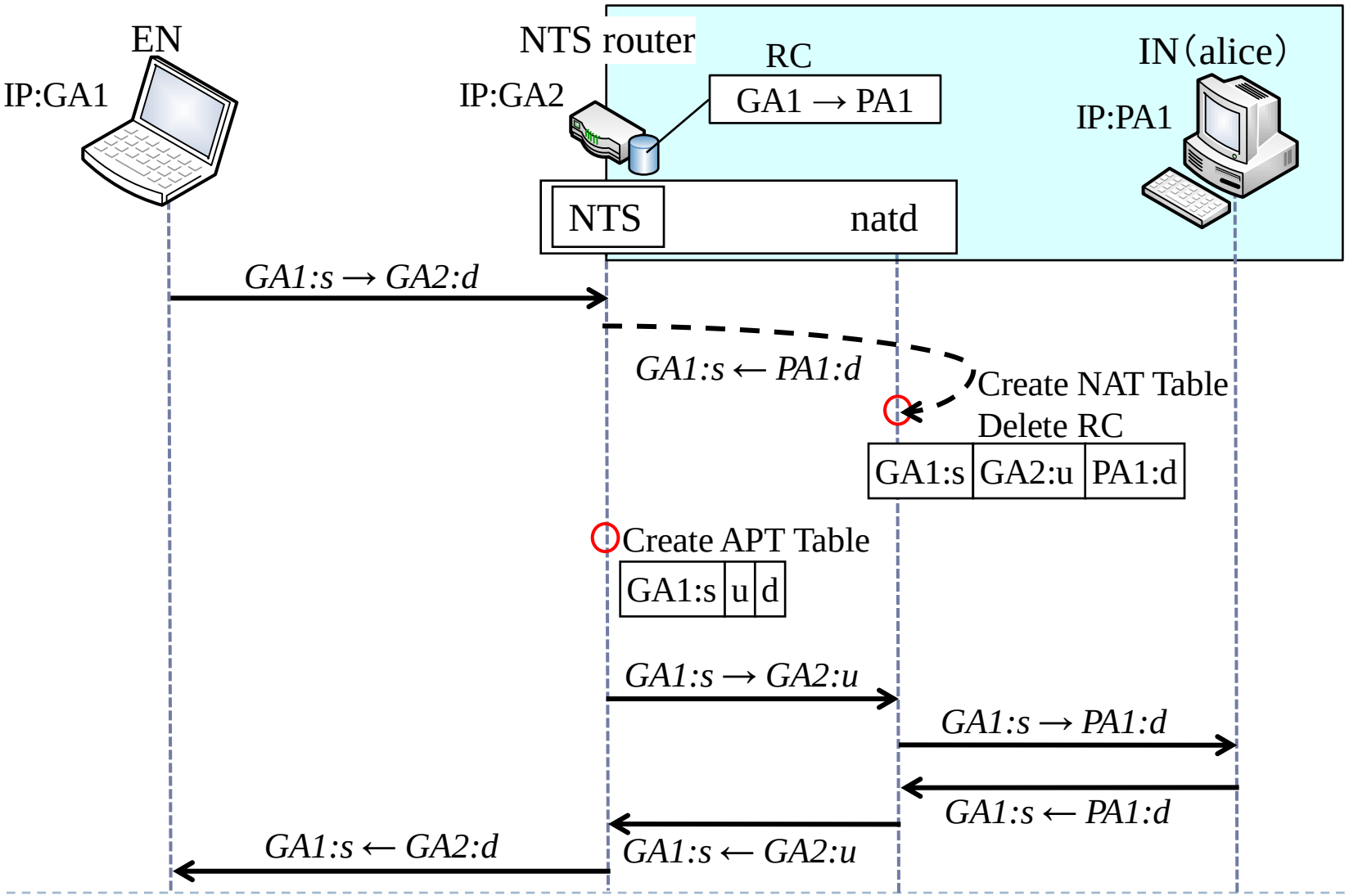
むすび

- 提案技術
  - NTSサーバとNTSルータの連携により，端末に手を加えることなくNAT越え問題を解決する方法
  - NTSルータがENからの通信より先に情報を得ることにより，外部からの通信でNATテーブルを作成
  - 実用に問題ない性能

- 今後の課題
  - セキュリティ確保
  - SIPへの対応

補足説明

提案方式（NATテーブル作成方法）



NAT越えによるセキュリティについて

- 元々NAT越えをさせるということは，その端末をインターネットに直接繋ぐことと同意なので，絶対にアクセスされたくない端末にはほん方式を利用しない
- NATはセキュリティのためにも使われることがあるが，元来アドレス枯渇を解消するための装置であり，セキュリティはその副産物なので，セキュリティに関しては個々の端末で実施する
- それでも侵入されたくないネットワークがある場合は二重NATなどの対応をとる

セキュリティ課題(1)

- 名前解決を行ったGNより先に，第三者がIPスプーフィングにより通信を開始した場合，通信を乗っ取られる可能性がある

  - IPスプーフィング
    - 偽のIPアドレスを送信元にセットしたパケットを送り込む攻撃手法
  - Ingress Filteringによる解決（RFC2827）
    - ISPのルータが，プリフィックスの範囲内の発信元アドレスからのものだけを許すようにトラフィックを制限し，攻撃者がこのプリフィックスの範囲外の「不正な」発信元アドレスを使用することを防ぐ

セキュリティ課題(2)

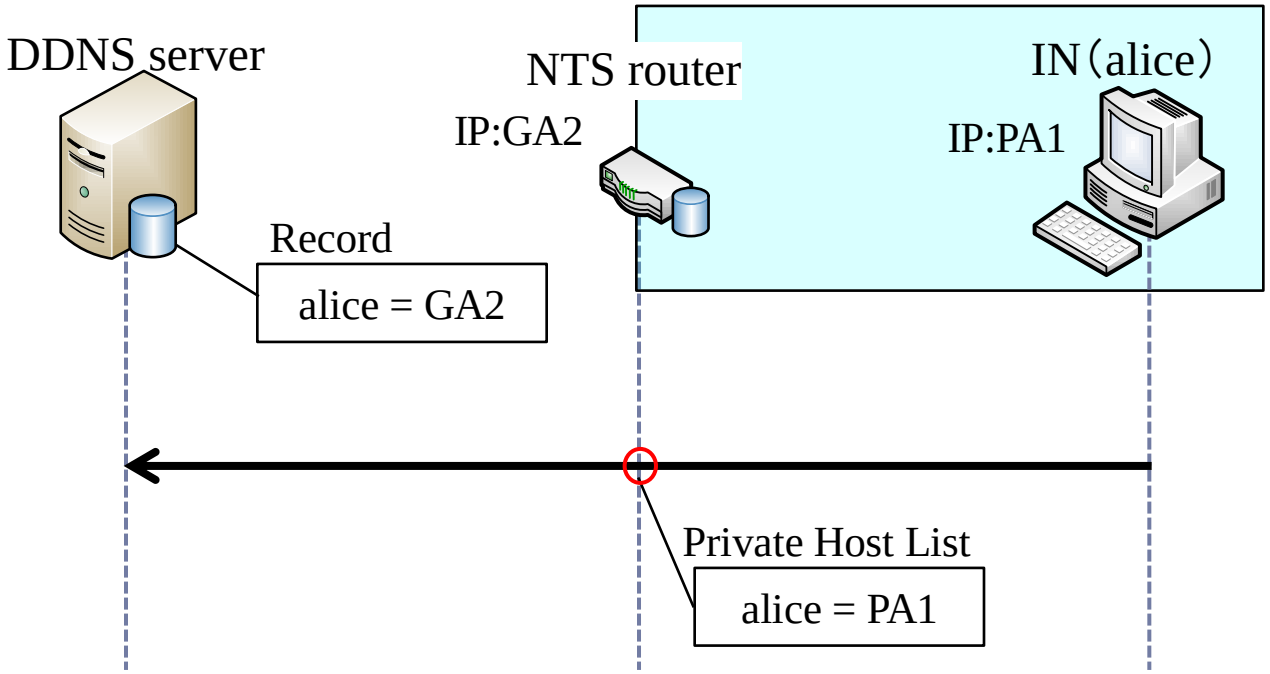
- 通信を開始したENと同じネットワーク内から，同じネットワーク内の端末に本方式を利用した場合
  - 元から通信があった場合
    - NATが使用する送信元のポートが違うため，通信を区別することができる
  - 同時に開始された場合
    - 名前解決の時点であれば，NTSルータからの返信を遅らせることで，通信を混同することを防ぐ
  - 故意に通信を乗っ取ろうとした場合

（ENの名前解決に合わせて，第三者が名前解決を行わずに先に通信を開始した場合）

- タイミング的に難しいが，不可能ではない
- 元々その第三者も本方式を利用できるので，ルーティングを奪われたENも開始し損ねただけなので，もう一度行えば良い

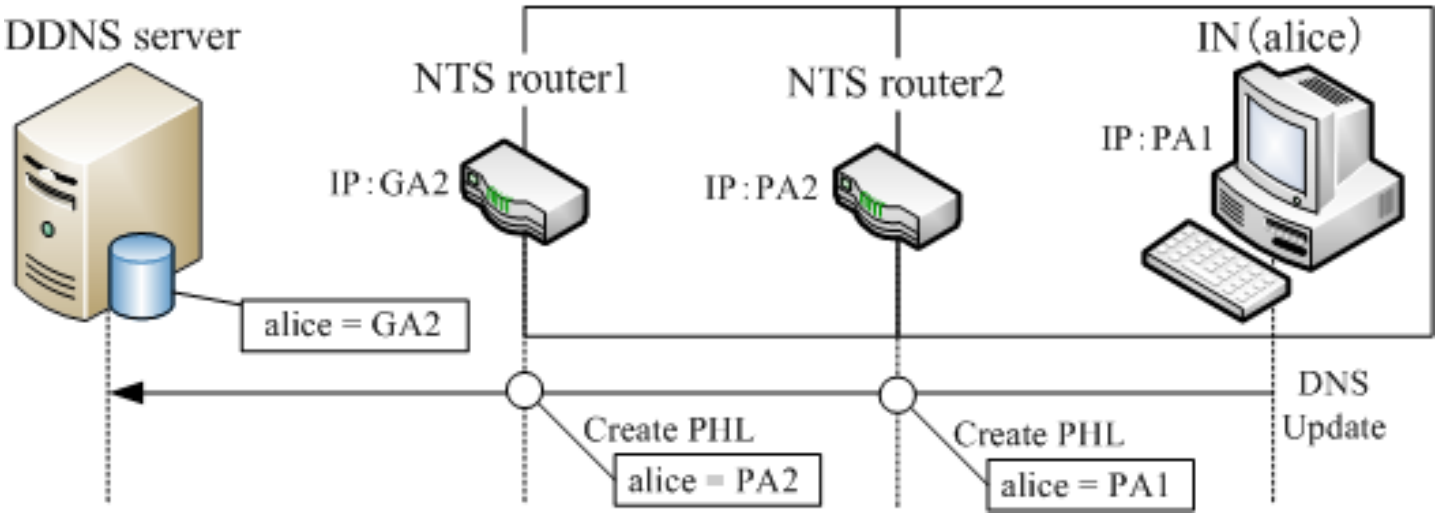
PHLの自動生成

- INのFQDN(alice)とNTSルータのアドレスをDNSサーバへ登録



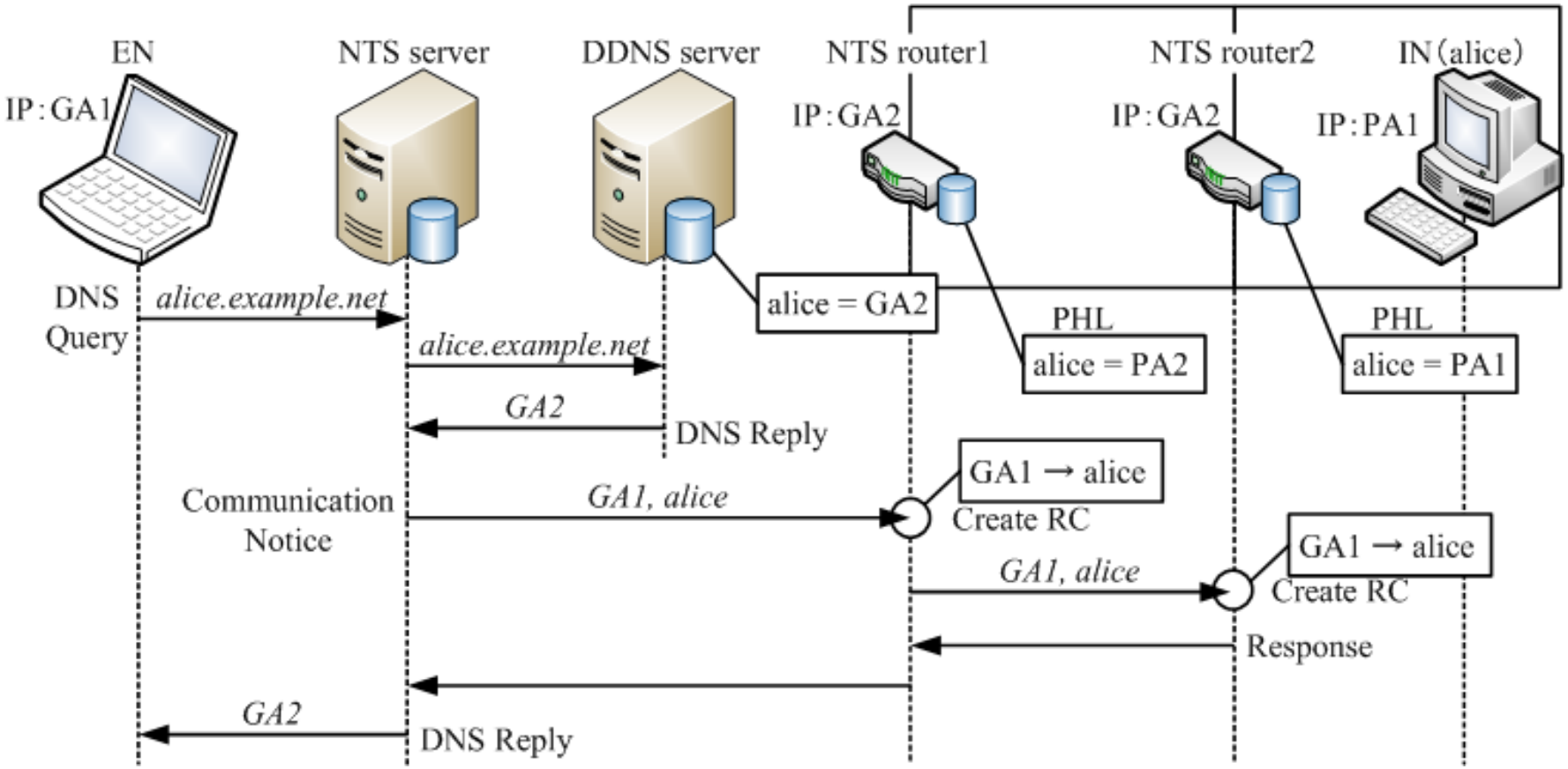
- DNS updateパケットがNTSルータを通過時，PHLとしてその情報を保持しておく

二重NATの場合(名前登録)

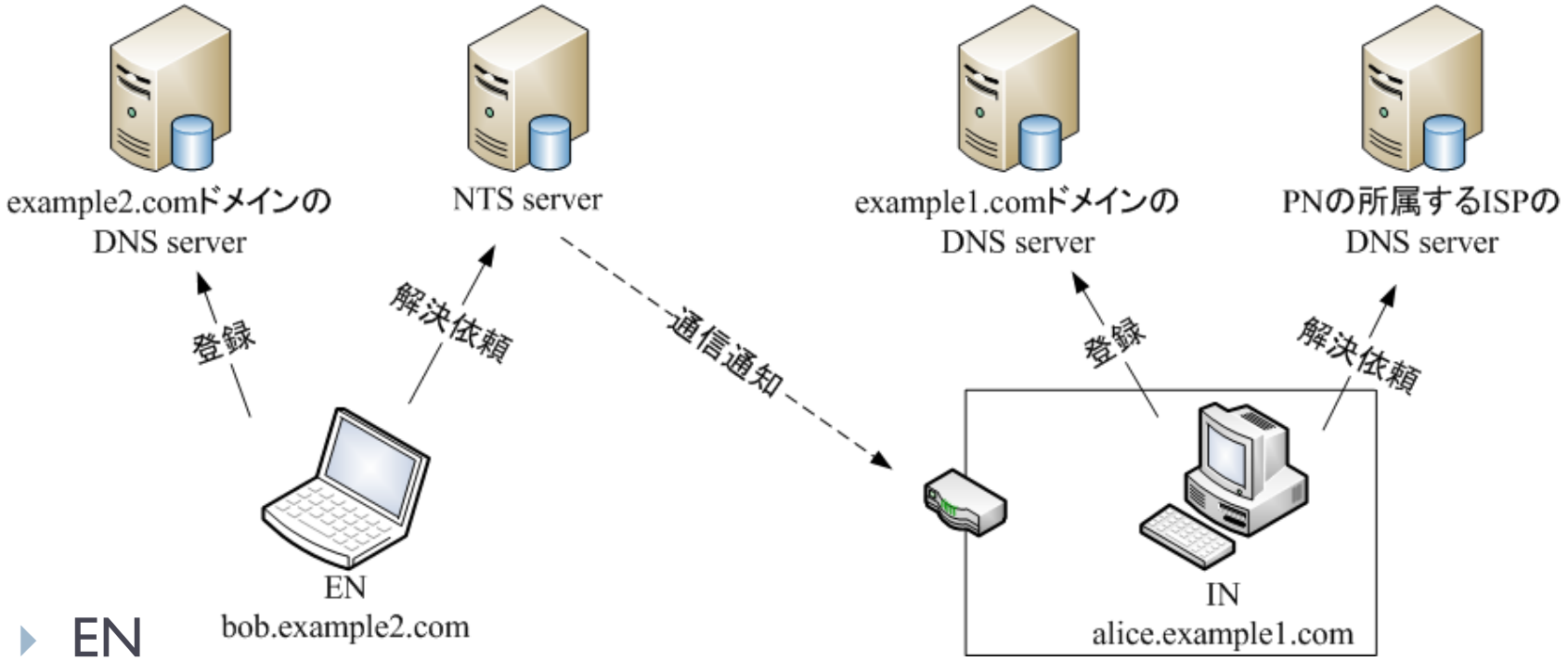


- NTS routerはそれぞれ名前登録パケットが内側から通過した時にPHLを作成する.
- NATは内側からのパケットを自分の外側で使えるIPアドレスに書き換えて送信するので, NTS router1と2ではそれぞれのネットワークに対応したアドレスのPHLが作成される.

二重NATの場合(名前解決)

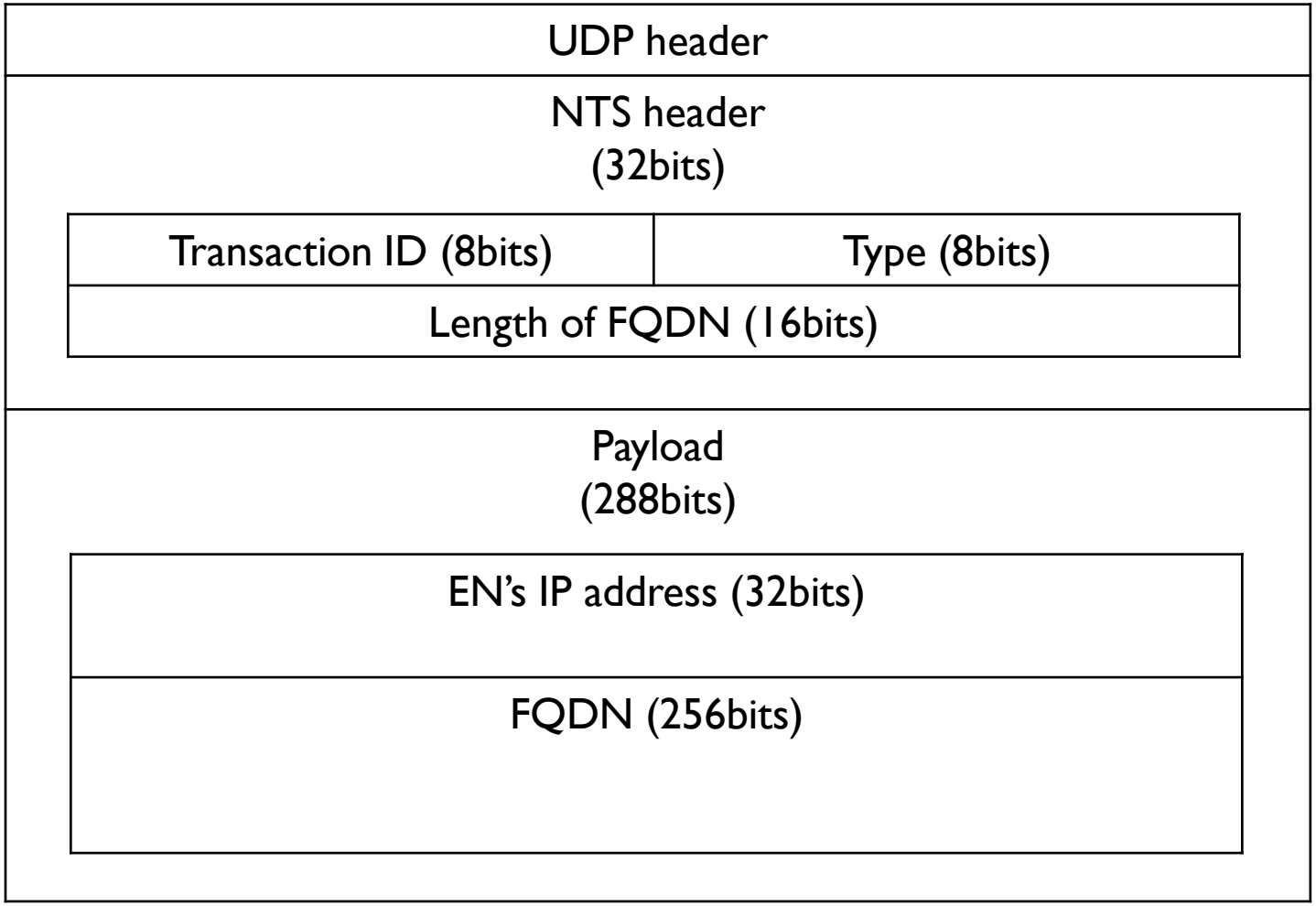


DNS対応関係



- EN
  - 登録先：自ドメインを管理するDNSサーバ
  - 名前解決依頼先：NTSサーバ
- IN
  - 登録先：自ドメインを管理するDNSサーバ
  - 名前解決依頼先：自分の所属するISPのDNSサーバ

NTS-Negoパケットフォーマット



プライマリDNSの設定方法

- Windows XPの場合
  - 「スタート」-「コントロールパネル」-「ネットワークとインターネット接続」-「ネットワーク接続」-「ローカルエリア接続」を開く
  - 全般タブのプロパティからインターネットプロトコル(TCP/IP)のプロパティ
- Windows Vistaの場合
  - 「スタート」-「コントロールパネル」-「ネットワークとインターネット」-「ネットワークと共有センター」-「ネットワークの管理」-「ローカルエリア接続」を開く
  - ローカルエリア接続の状態のプロパティにあるネットワークタブのインターネットプロトコルバージョン4(TCP/IPv4)のプロパティ

NAT(Network Address Translator)

- IPアドレスの枯渇
- プライベートIPアドレス
  - クローズなネットワーク内のみで利用できるIPアドレス

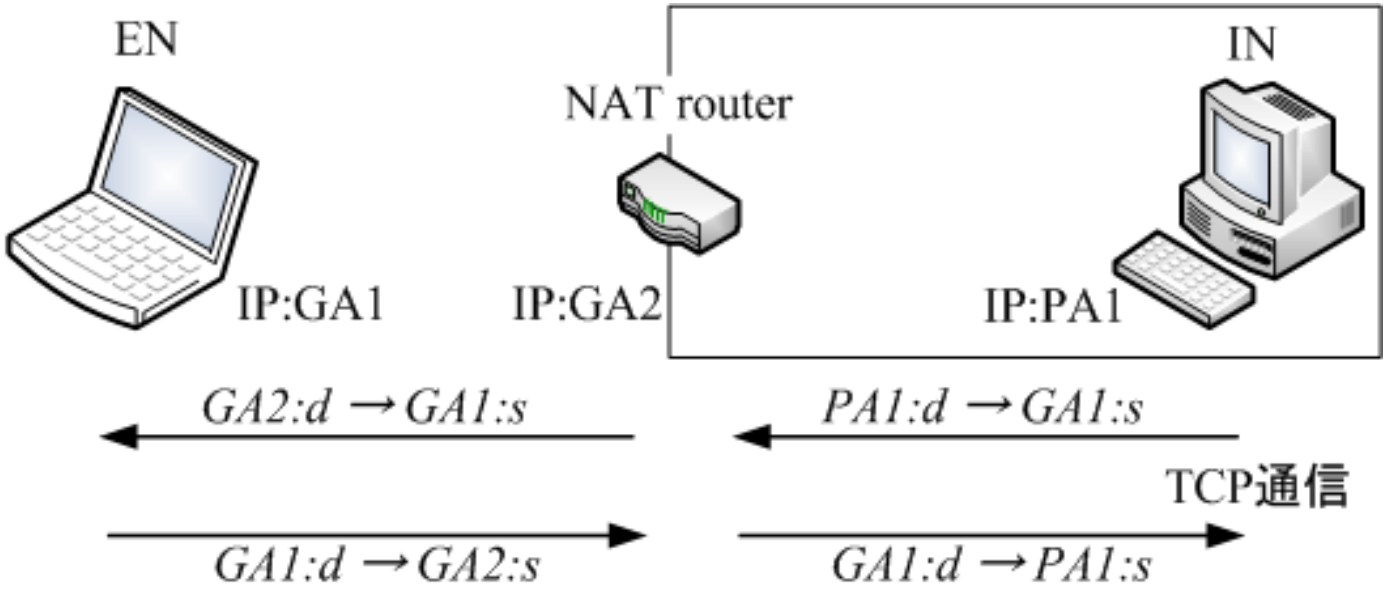
- NAPT(Network Address Port Translator)
  - 広義のNAT
  - NAT tableでIPアドレスとポート番号を対応させることで，一つのIPアドレスを複数の端末で共有することができる

NATのマッピング方法

- マッピングの仕方で四つに分類
  - Full Cone NAT
    - NATの外部portと内部端末をマッピング
  - Restricted Cone NAT
    - リモート端末のIPアドレスも対応付ける
  - Port Restricted Cone NAT
    - リモート端末のportも対応づけてマッピングする
  - Symmetric NAT
    - 内部と外部で異なるportをマッピングする

Full Cone NAT

- NATの外部portと内部端末をマッピング

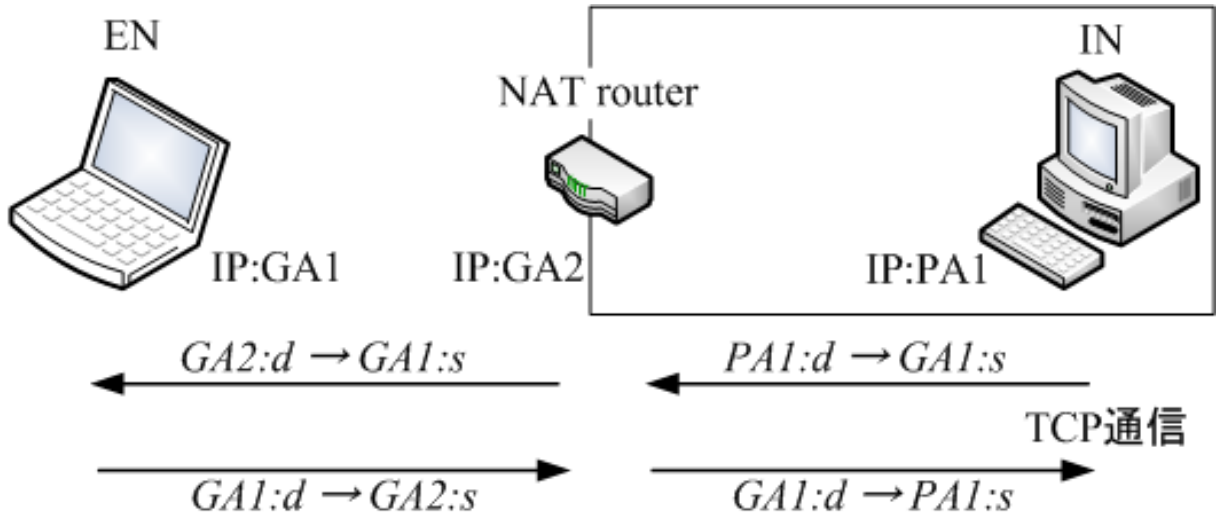


NAT Table

Remote		*Global*		*Local*		*Protocol*
address	*port*	*address*	*port*	*address*	*port*	
		GA2	s	PA1	s	TCP

Restricted Cone NAT

- NATの外部portと内部端末のマッピングだけでなく，リモート端末のIPアドレスも対応付ける

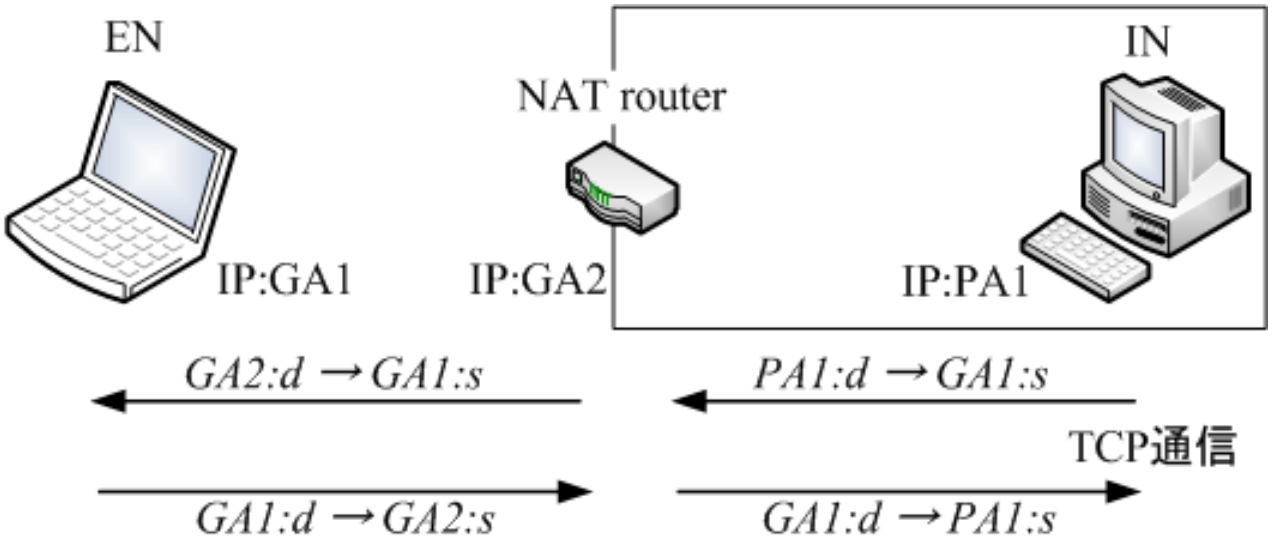


NAT Table

Remote		*Global*		*Local*		*Protocol*
address	*port*	*address*	*port*	*address*	*port*	
GA1		GA2	s	PA1	s	TCP

Port Restricted Cone NAT

- Restricted Cone NATに加え，リモート端末のportも対応づけてマッピングする

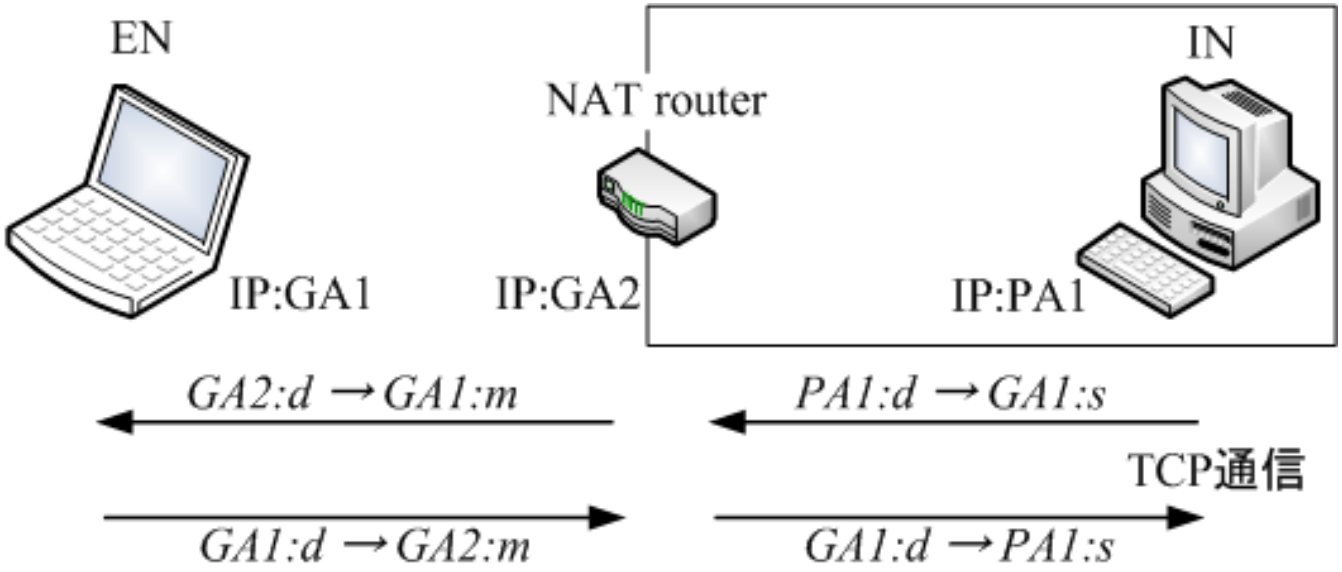


NAT Table

Remote		*Global*		*Local*		*Protocol*
address	*port*	*address*	*port*	*address*	*port*	
GA1	d	GA2	s	PA1	s	TCP

Symmetric NAT

- 内部と外部で異なるportをマッピングする



NAT Table

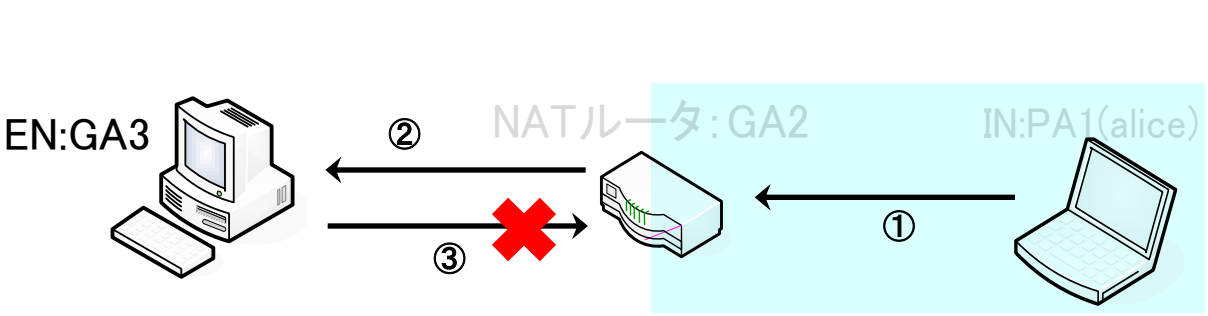
Remote		*Global*		*Local*		*Protocol*
address	*port*	*address*	*port*	*address*	*port*	
GA1	d	GA2	m	PA1	s	TCP

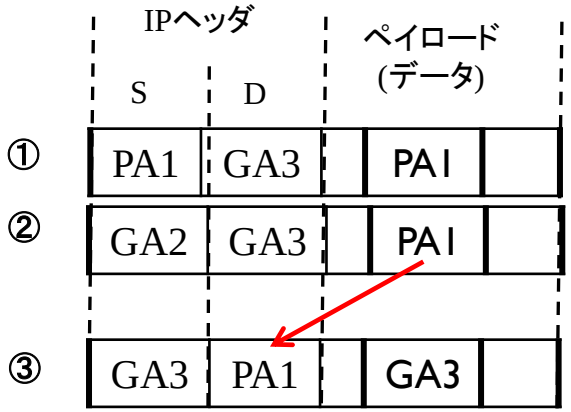
NATによる別の課題と解決方法

- IPアドレスやポートを制御するアプリケーションが利用不可（SIP・FTP）
  - Application Level Gateway
    - パケットのペイロードにあるIPアドレスやポートの情報も変換する
  - Universal Plug and Play
    - 内側の端末からNATに開けるべきポートを通知する

ALG(Application Layer Gateway)

- NATによる異種ネットワーク間でのセッション確立





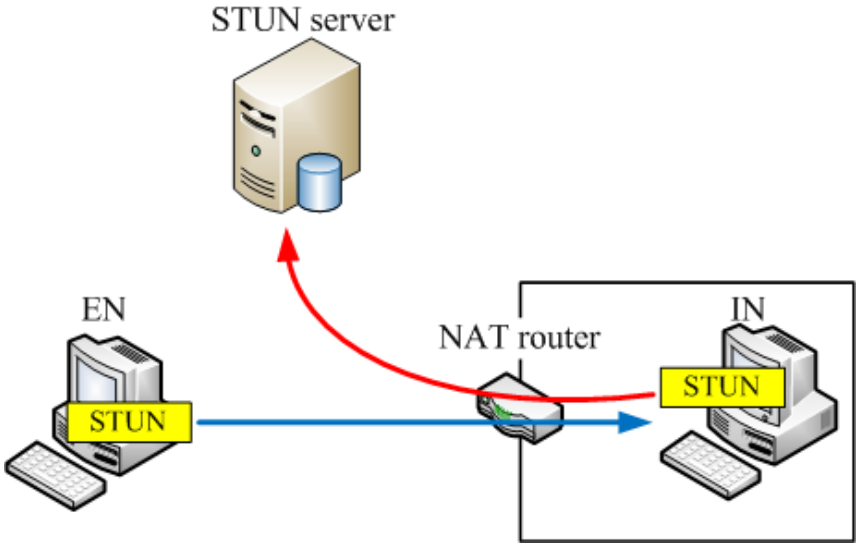
- NATではIPおよびTCP/UDPヘッダに記述されるアドレスを書き換えるが，ペイロード部は関知しない
- そこで，ALGによりアプリケーション内のアドレスも書き換える

NAT越え通信における主な既存技術

- STUN

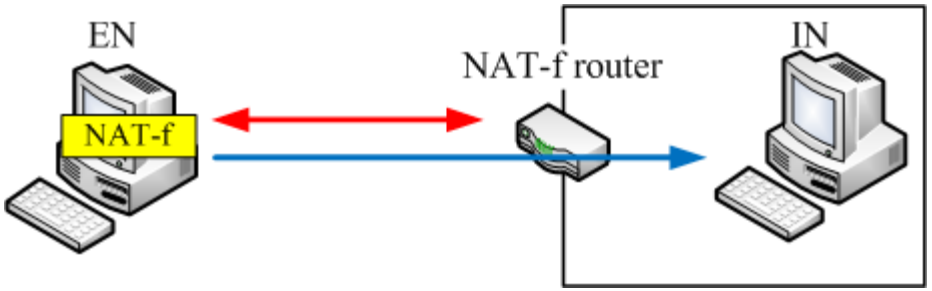
(Simple Traversal of UDP Through NATs)

  - EN,INへアプリケーション
  - 専用サーバ



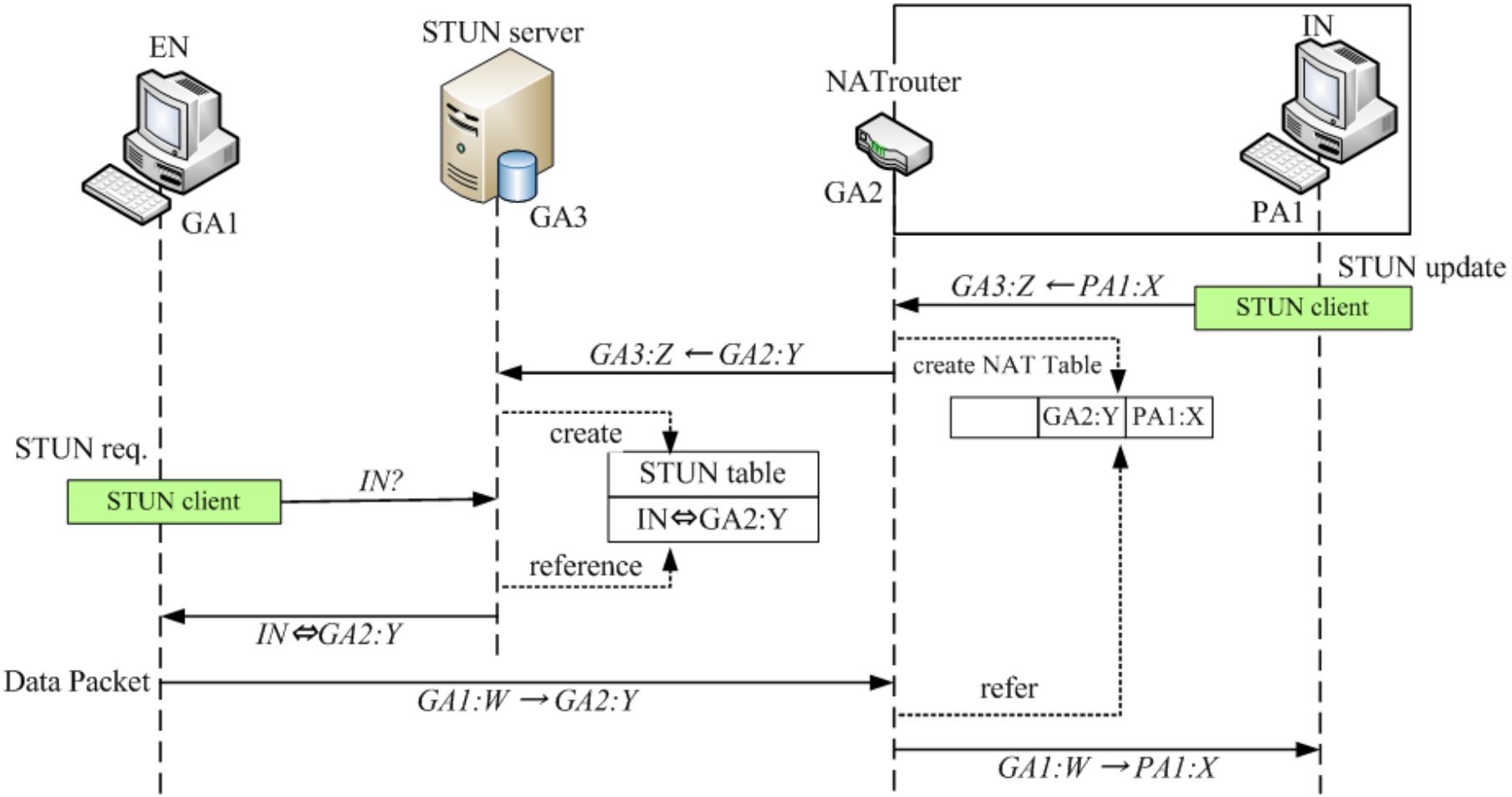
  - 利点：実現容易
  - 欠点：通信の限定

- NAT-f (NAT-free protocol)
  - EN,NATルータへ実装
  - 事前ネゴシエーション

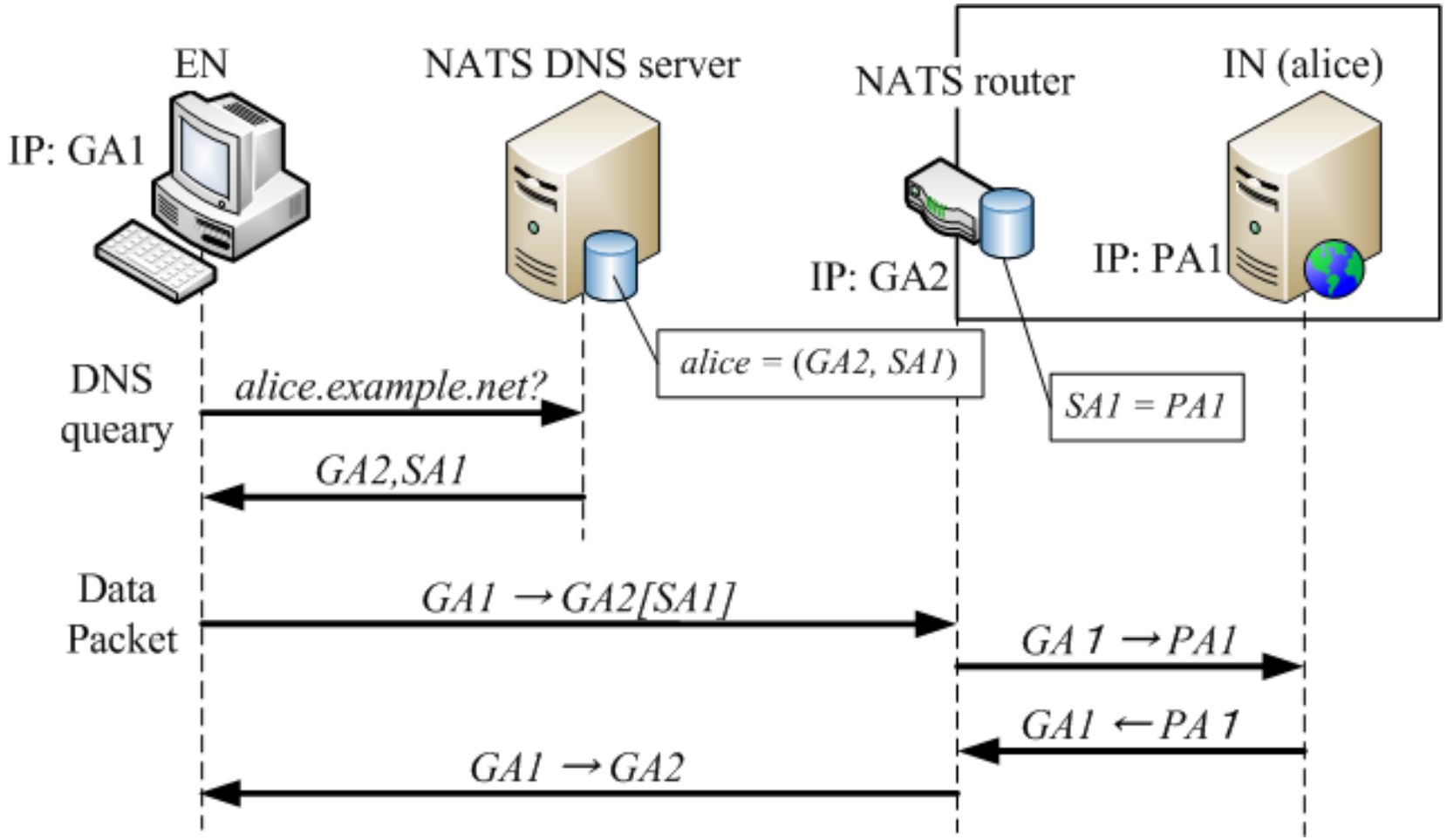


  - 利点：自由な通信
  - 欠点：導入難易度

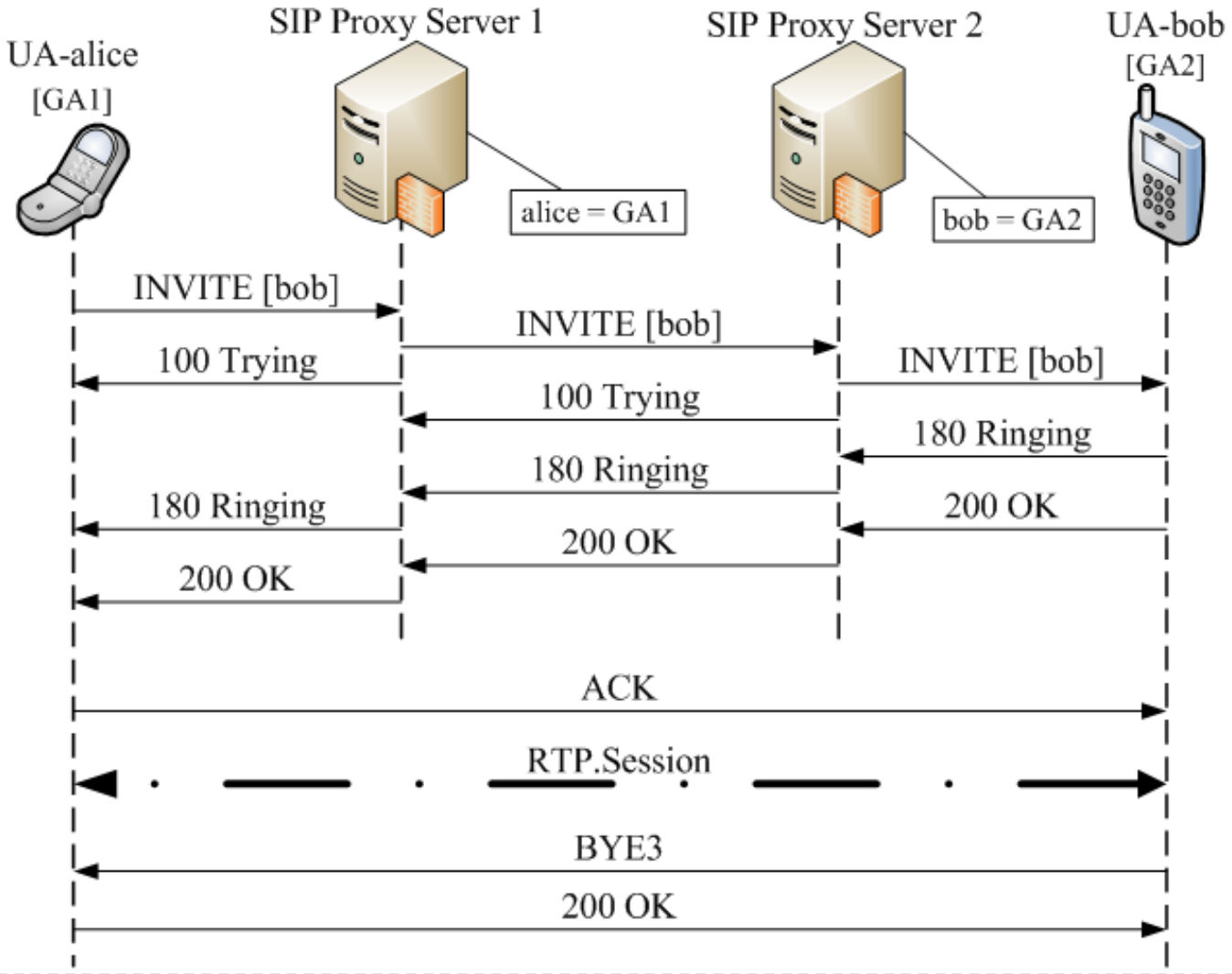
STUN
(Simple Traversal of UDP Through NATs)



NATS(NAT with Sub-Address)



SIP (Session Initiation Protocol)



NTSのSIP対応時，INVITEシーケンス