端末に依存しないNAT越えシステムの提案と実装

宮崎　悠[†1]　鈴木秀和[†1]　渡邊　晃[†1]

ユビキタス社会の到来に向けて，いつでもどこからでもネットワークにアクセスしたいという需要が高まっている．そこでは外出先からでも家庭内や企業内の端末に自由にアクセスしたいというニーズが考えられる．しかし，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一般であり，通信経路上に必ずNATが存在する．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の端末に対して通信を開始するためにNAT越え問題を解決する必要がある．本稿では，DNSサーバとNATルータを改造し，両者を協調させることによりNAT越えを実現する方式を提案する．また，提案方式を実現するためのサーバとルータの実装方法について説明する．

Installation of the NAT traversal system independent of user terminals

Yutaka Miyazaki,[†1] Hidekazu Suzuki[†1] and Watanabe Akira[†1]

Demand for users accessing networks anytime and from anywhere has been increasing in the forthcoming advent of ubiquitous society. Users would strongly desire to acquire the capability of accessing to their own terminals of the home or company networks from the outside. However, networks are usually constructed with private IP addresses, and a NAT stands on the way of a communication path. In such an environment, communication cannot be initiated from terminals in the Internet. This is called "NAT traversal problem". To solve this problem, we propose a new NAT traversal system based on the modified DNS server and NAT router and concerted work between them. Moreover, we explain the installation method of server and router for realizing a proposal system.

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アドレス変換装置 (以下NAT : Network Address Translator)[1),2)]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，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．

この課題を解決する為に様々な解決手法が提案されている．NAT越え問題を解決する既存技術として，STUN (Simple Traversal of User Datagram Protocol Through Network Address Translators)[3)]，AVES(Address Virtualization Enabling Service)[4)]およびNAT-f (NAT-free protocol)[5)]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

†1 名城大学大学院理工学研究科
Graduate School of Science and Technology, Meijo University

末の機能追加が必要であることから，一般ユーザがNAT 越えを行うのは難しいという課題がある．そこで本稿では DNS サーバ[6),7)] と NAT ルータが協調することにより，一般のユーザ端末に機能を追加することなく，かつエンドエンドで NAT 越えを実現できる方式を提案する．

以降，第 2 章で既存技術について解説し，第 3 章で提案方式を説明する．第 4 章に実装内容を説明し，第 5 章で既存技術との比較をして第 6 章でまとめる．

2. 既存技術

2.1 STUN

STUN は UDP Hole Punching[8)] を使って NAT 越えを実現する技術である．UDP Hole Punching とは UDP を用いて予め内部より外部に通信を行っておくことによって NAT 内に経路を生成しておき，その経路を利用して外部から内部に通信を開始する方法である．通信を行う各端末には STUN に対応したアプリケーションを必要とし，インターネット上には STUN サーバという特殊なサーバを必要とする．例として，グローバルアドレス空間の端末 GN(Global Node) からプライベートアドレス空間にいる端末 PN(Private Node) へ通信を開始する例を挙げる．動作手順は**図 1** の通りである．予め PN はインターネット上に存在する SUTN サーバに通信を行い，PN に対応する NAT ルータの IP アドレスとポート番号を STUN サーバの STUN テーブルに登録する．その時に NAT 内の NAT テーブルにはアドレス変換情報が登録される．次に PN へ通信を行いたい GN は，STUN サーバへ PN に関する問い合わせを行い，登録された情報を取得する．GN はこの情報を元に NAT テーブルに合わせたパケットを生成して NAT ルータへパケットを送信する．パケットを受け取った NAT ルータは NAT テーブルを参照し，PN へパケットを転送することが可能となる．

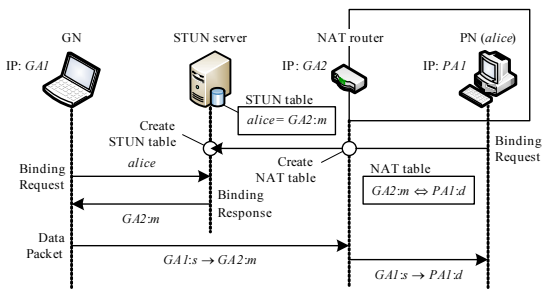


図 1 STUN の動作
Fig. 1 Flow of STUN.

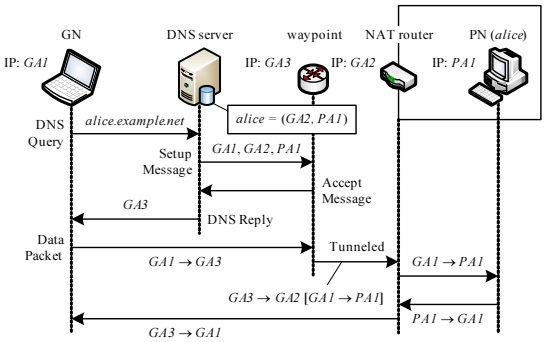


図 2 AVES の動作
Fig. 2 Flow of AVES.

STUN は既存の NAT ルータを使用できるという利点がある．しかし，インターネット上に第三の特殊な装置 STUN サーバが必要で，アプリケーションが限定される．また NAT の種類によっては利用できないなどの制約がある．

2.2 AVES

AVES ではグローバルアドレス空間に waypoint と呼ばれる機器を配置し，それを経由して通信を行う．**図 2** に AVES の動作を示す．GN が DNS サーバに PN について問い合わせると，DNS サーバは waypoint に PN についてのルート確認情報を送信する．ルート確認情報には PN のプライベート IP アドレス ”PA1” とその NAT ルータのグローバル IP アドレス ”GA2” が含まれる．Waypoint はこれを受理したら DNS に肯定応答を返す．DNS サーバが waypoint から受理メッセージを受け取ると，waypoint の IP アドレス ”GA3 ” を GN に応答する．次に GN は waypoint に対して通信を開始する．waypoint はパケットの宛先アドレスを PN のプライベート IP アドレス PA1 に変換し，NAT ルータのグローバル IP アドレス GA2 で IP in IP カプセル化し，NAT ルータへ送信する．NAT は上記パケットを受信すると，カプセル化を解除し PN へ送信する．PN からの応答は直接 GN 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 はユーザ端末には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．

2.3 NAT-f

NAT-f は第三の装置を必要とせず，P2P 通信による NAT 越えを実現できる方式である．NAT-f では機能を実装した GN と NAT ルータが，通信に先だって

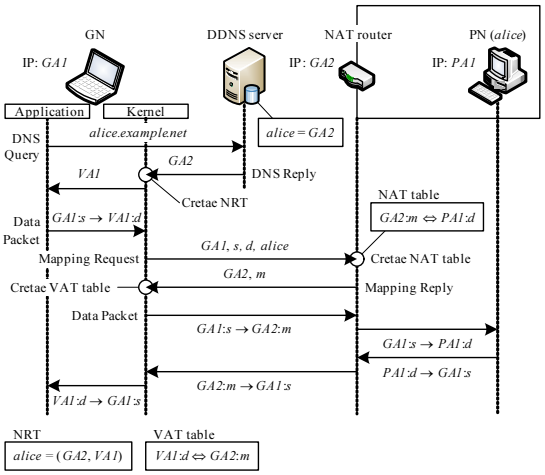


図 3 NAT-f の動作
Fig. 3 Flow of NAT-f.

ネゴシエーションを行うことにより動的に NAT テーブルを生成し，NAT 越えを実現する．**図 3** に NAT-f の動作を説明する．GN が PN と通信を開始する際，NAT ルータの FQDN ”example.net ” の先頭に PN のホスト名 ”alice ” を付加して DDNS サーバに名前解決を依頼する．DDNS(Dynamic DNS) サーバ[9] は GN に対し，ワイルドカード機能により NAT ルータの IP アドレス ”GA2 ” を返す．GN はカーネルにおいて DDNS サーバからの応答をフッキングし，PN のホスト名と NAT ルータの IP アドレスを取得する．更に NAT ルータの IP アドレスを仮想 IP アドレス ”VA1 ” に書き換え，これらを名前関連テーブル (NRT : Name Relation Table) へ記憶する．仮想 IP アドレスは通信相手となる PN を一意に特定するために割り当てる IP アドレスであり，GN の内部でのみ有効な値である．GN のアプリケーションへは PN の IP アドレスとして仮想 IP アドレス ”VA1 ” が報告される．次に，GN が NAT ルータ宛てのパケットを送信する際，GN のカーネルにおいて仮想アドレス変換 (VAT : Virtual Address Translation) テーブルを参照する．VAT テーブルとは PN に対応づけられた仮想 IP アドレス，ポート番号と NAT ルータの IP アドレス，ポート番号の相互変換関係が記されたテーブルで，GN と NAT ルータとのネゴシエーション完了時に作成される．該当する VAT が存在すれば VAT テーブルに従ってパケットの内容を変換してパケットを送信する．VAT テーブルの内容が存在しなければ，送信する通信パケットを一時的にカーネル内に退避させ，NAT-f ネゴシエーションを開始する．GN はネゴシエーションのトリガーとなった TCP/UDP パケットの送信元／宛先 IP アドレス ”GA1,VA1 ”，ポート番号 ”s,d ”，プロトコルタイプ ”TCP ”，NRT から取得した NAT ルータのグローバル IP アドレス ”GA2 ” および PN1 のプライベートホスト名 “alice ” を NAT ルータに通知する．NAT ルータはこの通知を受信すると該当する PN のプライベート IP アドレスから NAT テーブルを生成する．NAT ルータはグローバル IP アドレスと NAT テーブルに生成された変換後の送信元ポート番号 ”m ” を GN へ応答する．GN はその応答を受信すると，取得した情報から VAT テーブルを生成し，一時的に待避していた TCP/UDP パケットを復帰させて NAT-f ネゴシエーションを完了する．以後は生成された VAT と NAT テーブルで IP アドレスとポート番号が変換されることにより通信が実行される．

NAT-f によれば，エンドエンドの通信が可能で，カプセル化の必要もないのでオーバヘッドが少ない．また，第三の装置が不要であるという利点がある．しかし，GN に NAT-f 機能を実装する必要があるという課題がある．

3. 提 案 方 式

3.1 ネットワーク構成

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．GN と PN 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，その NTS ルータと協調する NTS サーバ，PN の名前解決に使用する DDNS サーバが存在する．NTS サーバは DNS サーバの機能を包含し，拡張したものである．ここで GN，NTS ルータのグローバル IP アドレスをそれぞれ GA1，GA2，PN(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 GN から PN(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．

3.2 事 前 設 定

提案方式を適用するに当たり，GN はプライマリ DNS として NTS サーバを登録しておく必要がある．外部からの通信を許可するにあたり，PN は予め FQDN(Fully Qualified Domain Name) と NTS ルータのアドレスを DDNS 登録する．これは一般の DDNS 登録と同様である．**図 4** に提案方式の DDNS 名前登

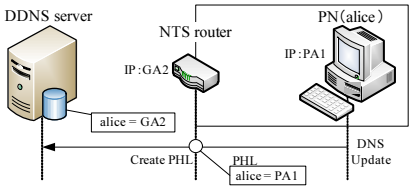


図 4 DDNS 名前登録シーケンス
Fig. 4 Sequence of DDNS registration.

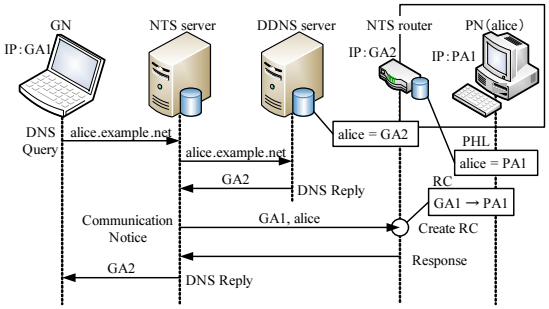


図 5 名前解決シーケンス
Fig. 5 Sequence of name resolution.

録シーケンスを示す．DDNS 名前登録時に，PN から DDNS サーバへ名前登録パケットが送信される．このとき NTS ルータは，そのパケットの情報からプライベート IP アドレスとホスト名を対応づけて PHL(Private Host List) へ記憶しておく．

3.3 名 前 解 決

図 5 に GN から PN(alice) へ通信を開始する場合の名前解決シーケンスを示す．GN は PN(alice) と通信を開始するに当たり，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 サーバはフォワード機能などを利用して上位 DNS へ名前解決を依頼し，NTS ルータの IP アドレス GA2 を取得する．次に NTS サーバは GN から alice への接続依頼があることを NTS ルータに通知する．この通知を受け取った NTS ルータは 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 ルータは NTS サーバへ通知応答を返すと，NTS サーバは GN に対して NTS ルータのアドレス GA2 を応答する．

3.4 通 信 開 始

図 6 に通信開始シーケンスを示す．GN は取得した IP アドレス GA2 への通信を開始する．NTS ルータはパケットを受け取ると RC の内容を確認する．RC に該当するデータがあれば，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，プロトコルタイプがわかるので，NAT テーブルを動的に生成する．NTS ルータは生成した NAT テーブルに

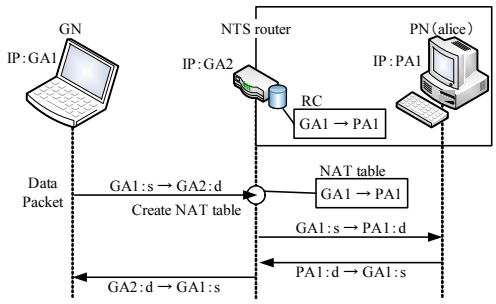


図 6 通信開始シーケンス
Fig. 6 Sequence of the start of communications.

従いパケットを PN(alice) に転送する．これに対する alice からの応答パケットは通常の NAT 処理に従い内側から外側へ転送される．以後は通常の NAT 動作により通信を行うことができる．内側から始まる通信に関しては，従来の NAT を介する通信と同様である．

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 のルータに実装する方法を検討した．

図 7 に NTS サーバの実装概要を示す．NTS サーバには DNS サーバ機能として BIND をインストールし，これを任意 (ここでは 10053 番) の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．その際，NTS サーバモジュールは受け取った DNS パケットと後のルータとのネゴシエーションの整合を取るために，トランザクション ID と送信元 IP，リクエストされた FQDN をリクエストテーブルとして保持する．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

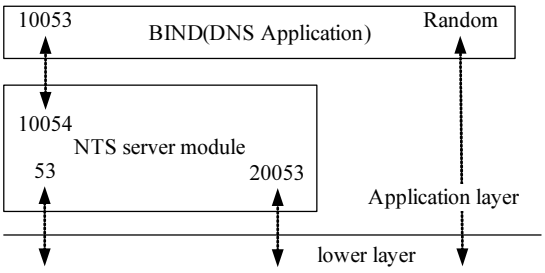


図 7 NTS サーバの実装概要
Fig. 7 Implementation on NTS server.

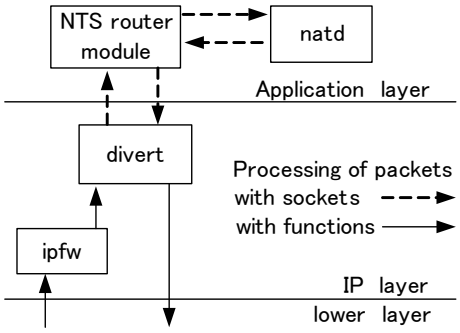


図 8 NTS ルータの実装概要
Fig. 8 Implementation on NTS router.

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上記 DNS レスポンスパケットのトランザクション ID で，リクエストテーブルと DNS パケット情報とのマッチングを行い，FQDN に対応する IP アドレスへ GN から通信要求があることを通知する．ネゴシエーション後，NTS サーバは GN（DNS 名前解決依頼元）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，NTS サーバはあたかも通常の DNS サーバの様に振る舞う．

次に**図 8** に NTS ルータの実装概要を示す．natd（NAT デーモン）は NAT 機能を持つデーモンであり，NTS ルータもこれを利用する．ipfw はファイアウォールの動作を行うモジュールである．divert は natd のパケット取り出しをサポートするソケットである．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 ipfw に渡され，ipfw はそのパケットを divert に渡す．次に natd は divert からソケットを介してパケットを取り出し，テーブル生成やパケットのアドレス変換など NAT に関わる動作を行った後に，ソケットを介して divert に戻す．divert はパケットを下位層に渡し，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 と divert の間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 サーバとのネゴや，受信パケットが RC に一致するか等の処理を行う．

5. 既存技術との比較

表 1 に NAT 越えに関する既存技術と提案方式の比較を示す．比較項目 ”GN”，”PN”，”DNS サーバ”，”NAT ルータ” はそれぞれに機能を実装する必要がない場合を ◯，必要がある場合を×とした．”第三装置” は通信において第三の装置が必要ない場合を ◯，必要な場合を×とした．”アプリケーション” は通信を行うアプリケーションに制約がない場合を ◯，制約がある場合を×とした．

表 1 NAT 越え技術比較
Table 1 Comparison of NAT Traversal Technologies

比較項目	提案方式	STUN	AVES	NAT-f
GN	◯	×	◯	×
PN	◯	×	◯	◯
第三装置	◯	×	×	◯
DNS サーバ	△	◯	×	◯
NAT ルータ	×	△	×	×
アプリケーション	◯	×	×	◯

提案方式では，NTS サーバは DNS サーバを改造することで実現でき，通信経路冗長などはないので ”第三装置” の欄は ◯ とした． また，GN はプライマリ DNS の設定を変更する必要があるが，名前解決を行う DNS サーバ自体は改造しないので ”DNS サーバ” は △ とした．

STUN は NAT ルータに手を加えずに NAT 越えを実現できるが，NAT の種類によっては使えない場合もあるため，NAT ルータの欄は △ とした．STUN は既存のネットワーク環境を変更せずに利用できる利点があるが，第三の装置が必要で，通信するアプリケーションが限定される．

AVES はユーザ端末に機能を実装する必要はないが，DNS サーバを改造する必要があり，NAT 越え通信は必ず waypoint を中継した通信となるため，パケットの経路が冗長となる．また，アプリケーションに制約がある．

NAT-f は第三装置を必要とせず既存の DNS サーバを使用できるが，GN と NAT ルータに手を加える必要がある．

提案方式はユーザ端末に手を加える必要がない．そのためアプリケーションに制約がなく，P2P 通信が可能である．アプリケーションを勝手にインストールすることができない，大学やネットカフェなどの外出先のコンピュータを利用することが可能である．また無線 LAN サービスを提供する ISP(Internet Service Provider) が提案方式を利用することにより，アドレス空間の違いを意識しないネットワークを構築することができる．例えば無線 LAN のアドレスをプライベート IP アドレス空間とすることができる．IPv4 のグローバルアドレスを消費することなくサービスエリアを拡大できるため，有用な方法と考えられる．

6. むすび

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 GN 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で 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．今後は NTS サーバと NAT ルータの実装を行い，更なる検討・評価を行う．

参 考 文 献

1) K.Egevang and P.Francis: The IP Network Address Translator (NAT), RFC 1631 (1994).
2) Srisuresh, P. and Holdrege, M.: IP Network Address Translator (NAT) Terminology and Considerations, RFC 2663 (1999).
3) J.Rosenberg, J.Weinberger, C.Huitema and R.Mahy: STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs), RFC 3489 (2003).
4) 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).
5) 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).
6) P.Mockapetris: DOMAIN NAMES - CONCEPTS AND FACILITIES, RFC 1034 (1987).
7) P.Mockapetris: DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION, RFC 1035 (1987).
8) B.Ford, P.Srisuresh and D.Kegel: Peer-to-Peer Communication Across Network Address Translators, *Proc. USENIX Annual Technical Conference*, Anaheim, CA, pp.179–192 (2005).
9) P.Vixie, S.Thomson, Y.Rekhter and J.Bound: Dynamic Updates in the Domain Name System (DNS UPDATE), RFC 2136 (1997).

端末依存しないNAT越え方式の提案と実装

名城大学大学院　理工学研究科
宮﨑 悠　鈴木 秀和　渡邊 晃

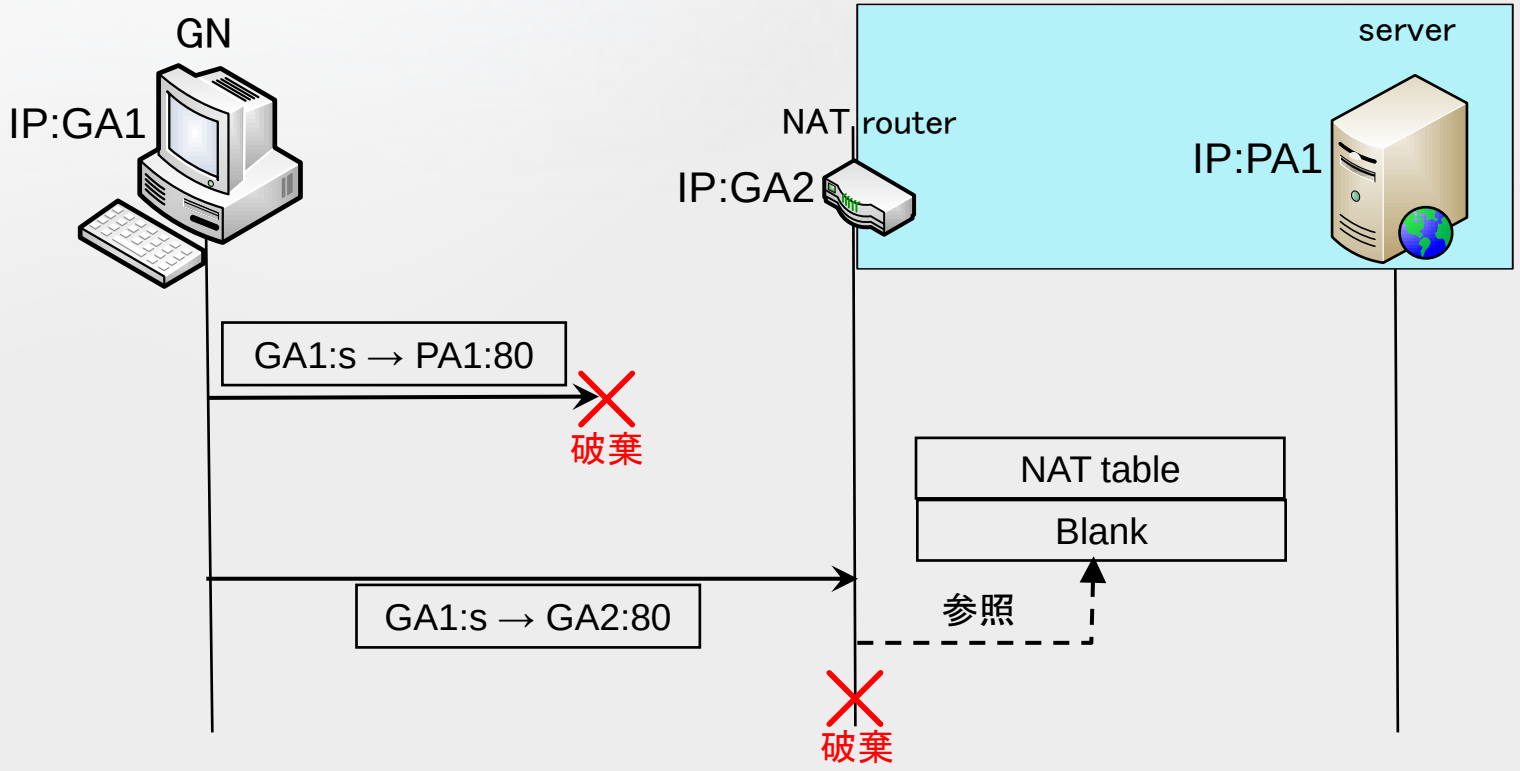
研究背景

- 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

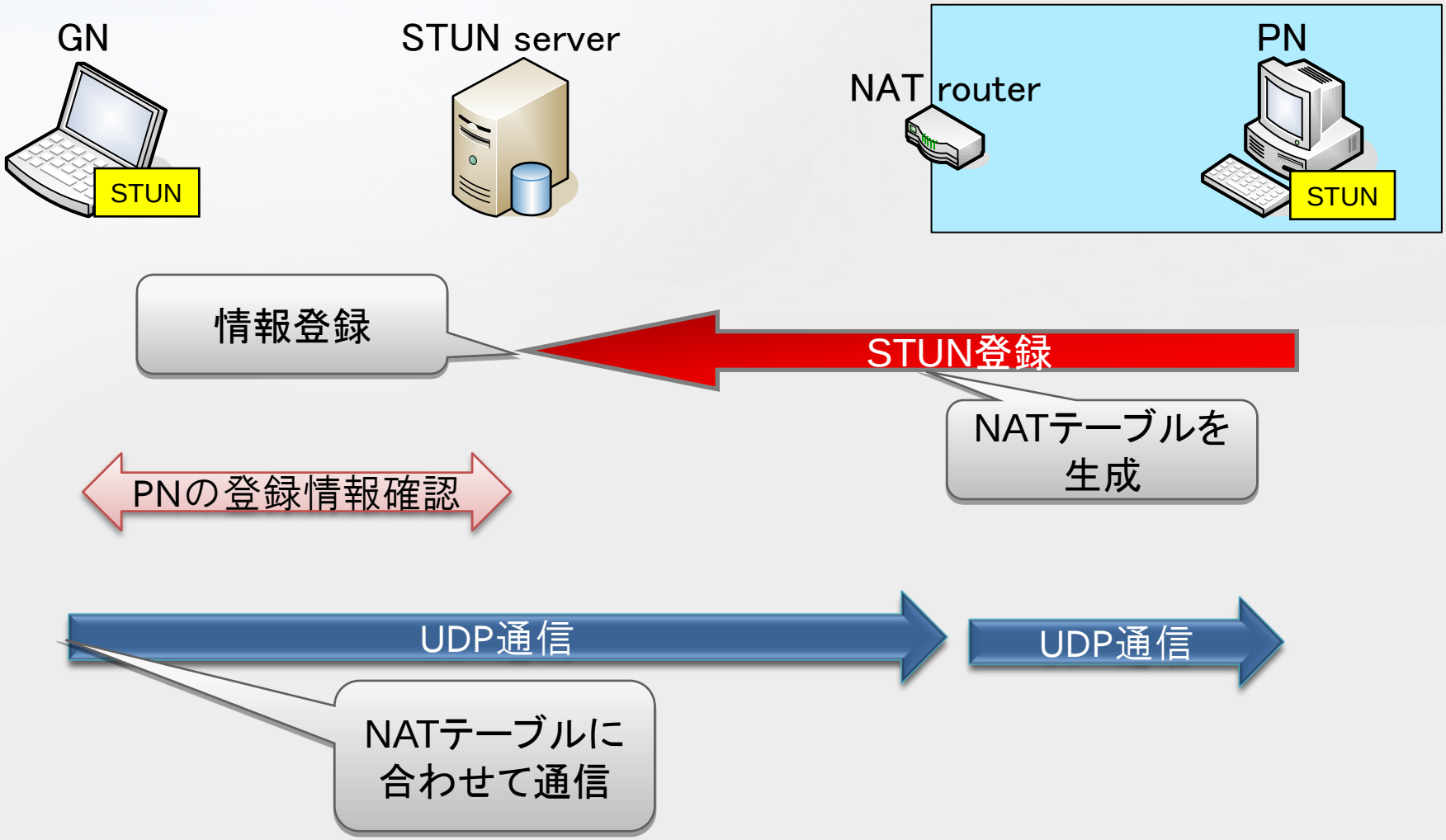
- 家庭内や企業内のネットワークはプライベートアドレスで構築される場合が多い
  →NAT(Network Address Translator)が使用される

NAT越え問題

- NATの外側にある端末からは通信を開始できない

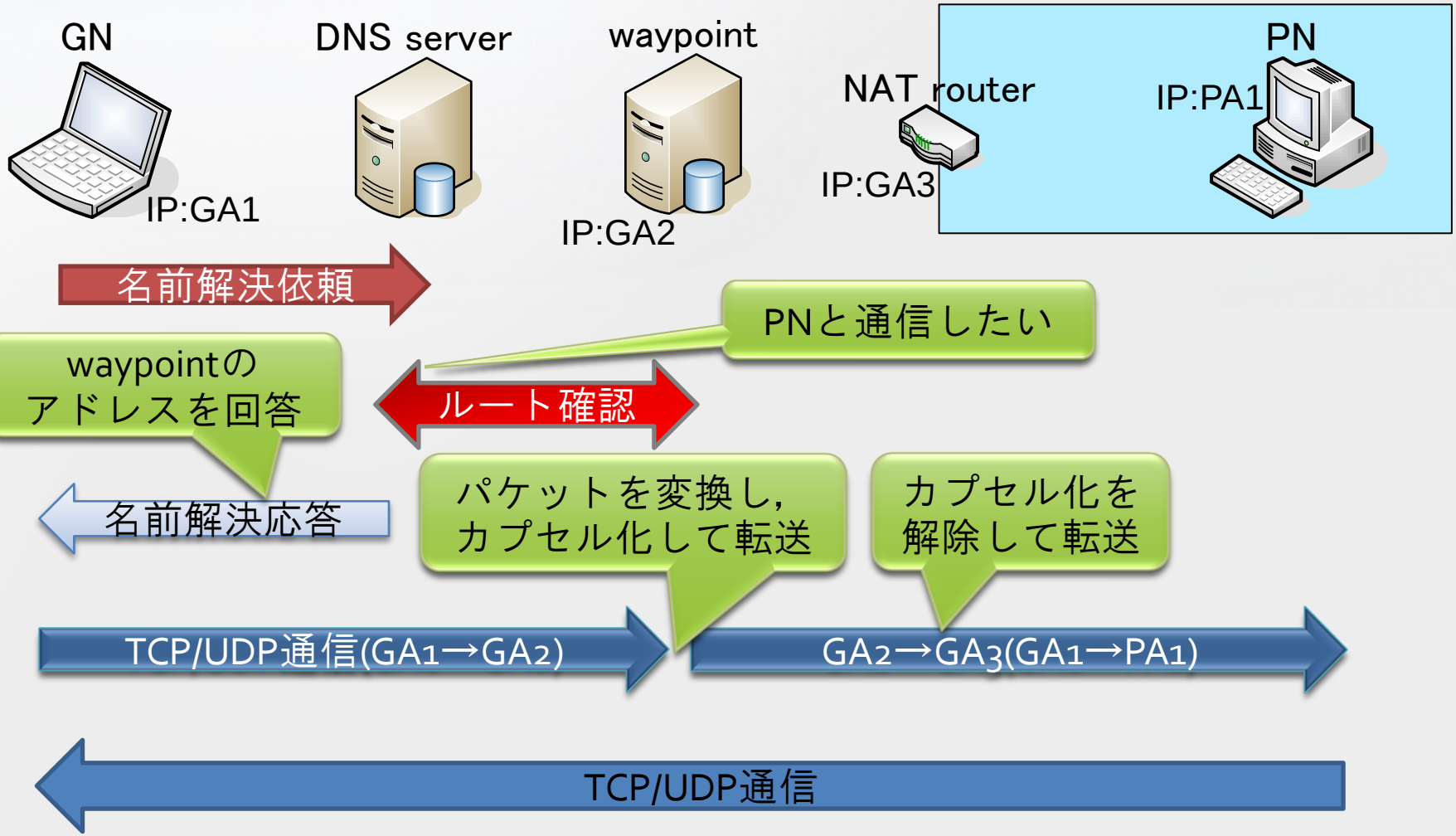


STUN(Simple Traversal of UDP Through NATs)



AVES

(Address Virtualization Enabling Service)



提案技術

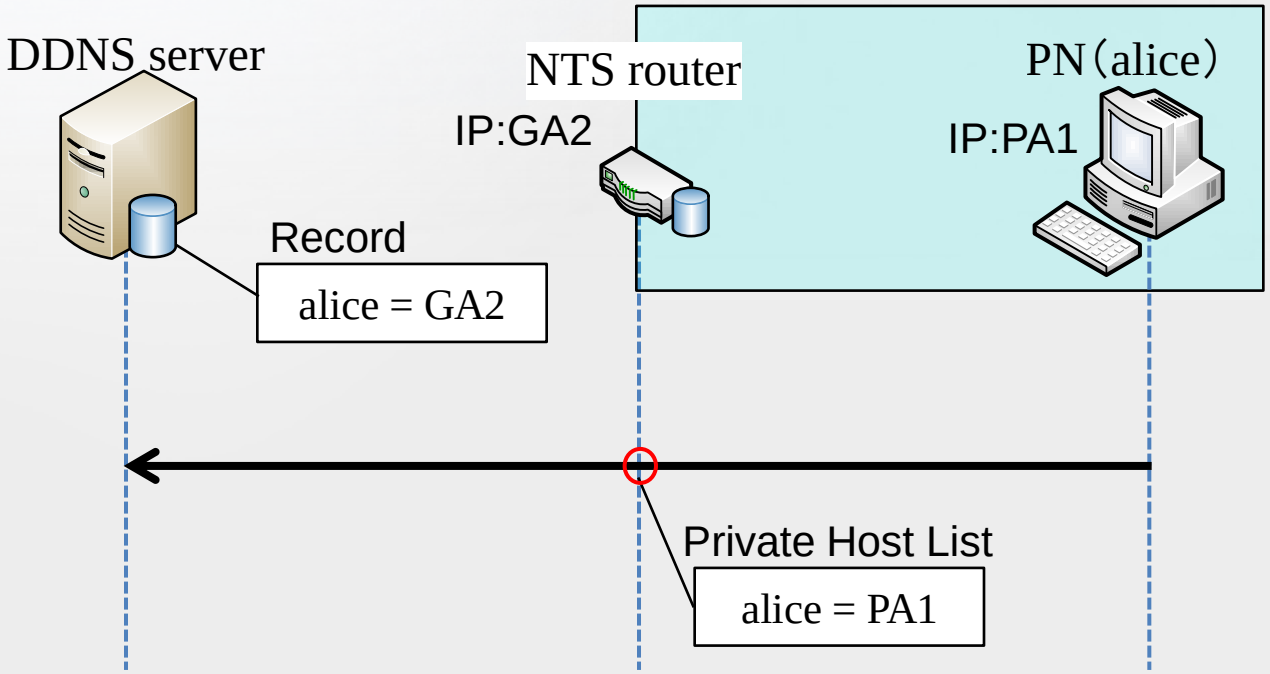
端末に機能を加えることなく
NAT越えを実現したい

- 端末は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

- DNSサーバ：NTSサーバ
- NATルータ ：NTSルータ
  - が連携をとることにより問題を解決する

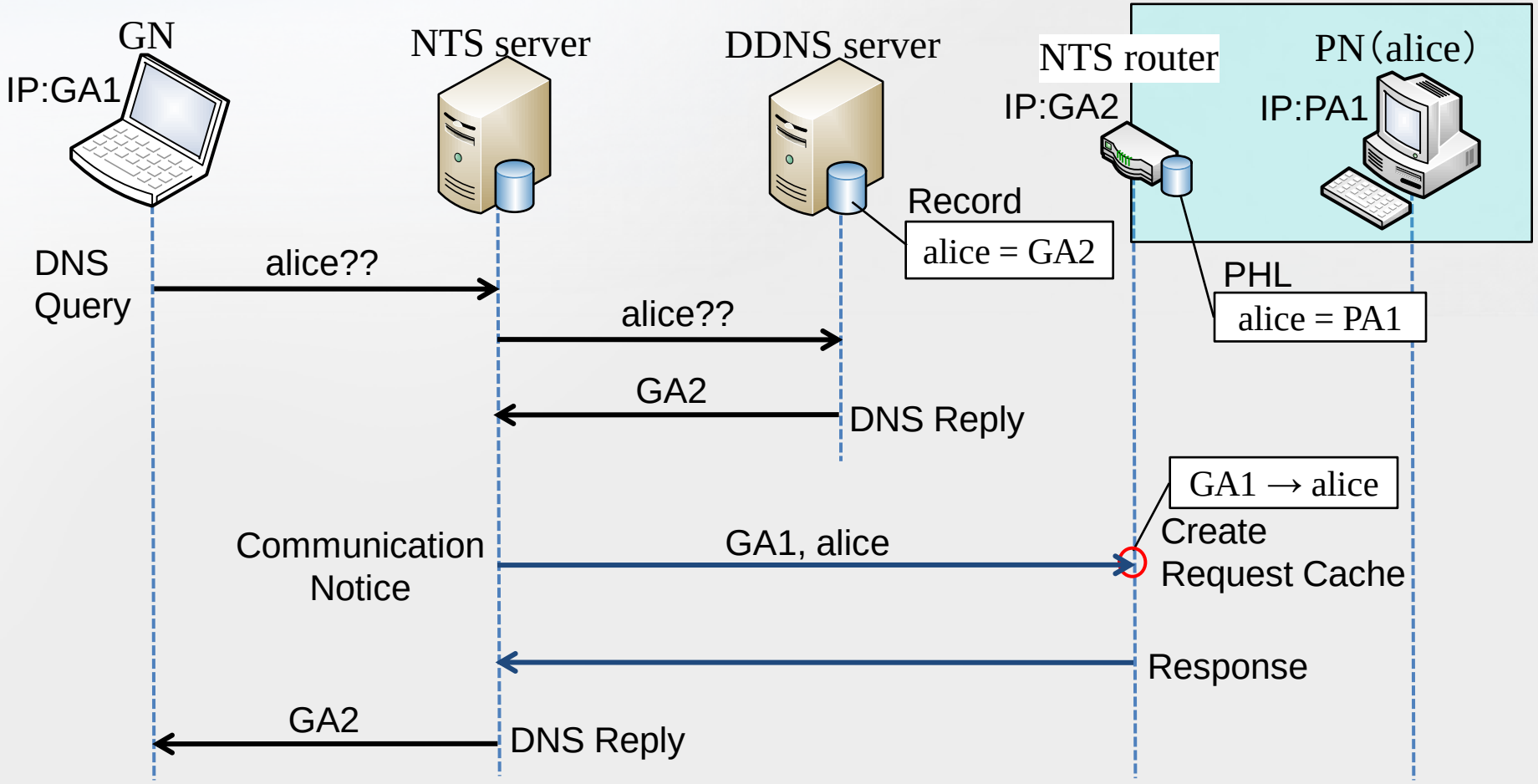
提案方式（事前準備）

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

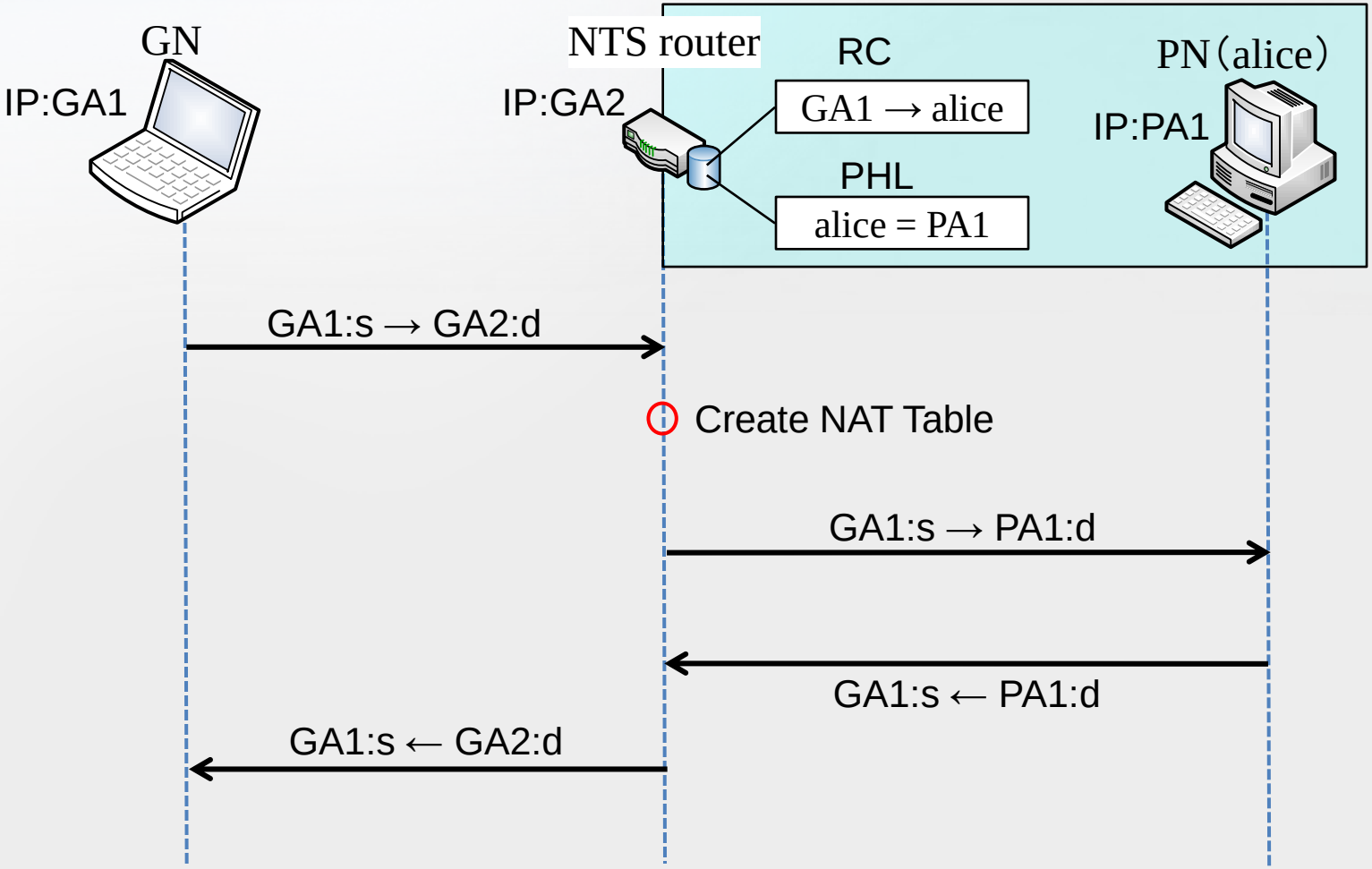


- DNS updateパケットがNTSルータを通過時，PHLとしてその情報を保持しておく

提案方式（名前解決）


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

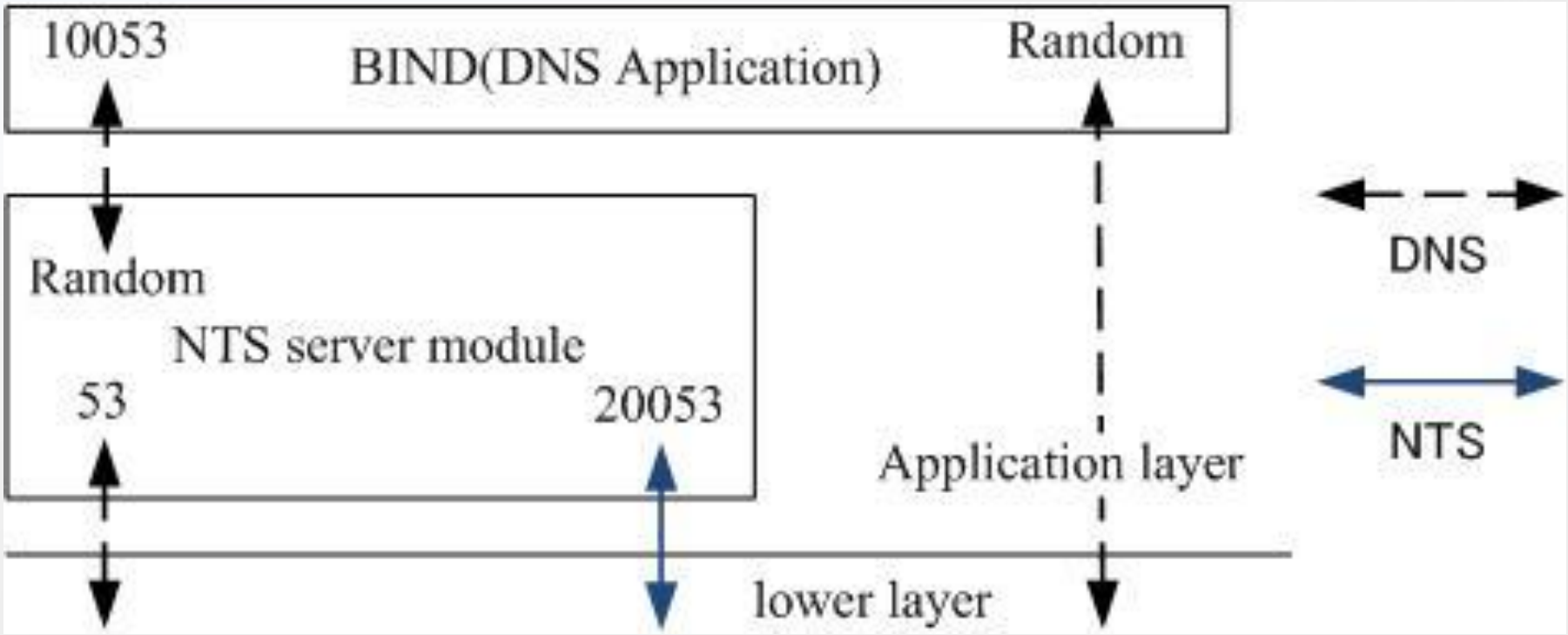
提案方式（通信開始）


GN
IP:GA1
NTS router
IP:GA2
RC
GA1 → alice
PHL
alice = PA1
PN（alice）
IP:PA1
GA1:s → GA2:d
Create NAT Table
GA1:s → PA1:d
GA1:s ← PA1:d
GA1:s ← GA2:d

実装状況

- FreeBSDに実装中
- Server
  - ほぼ実装済み
- Router
  - 実装中

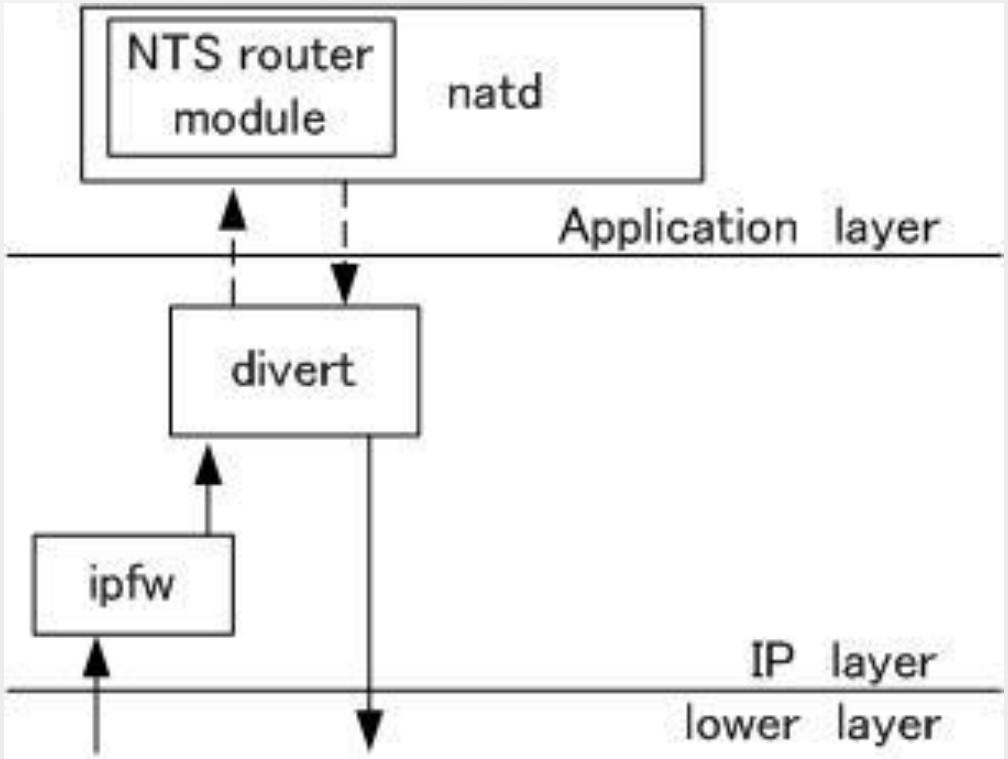
実装概要（NTS Server）



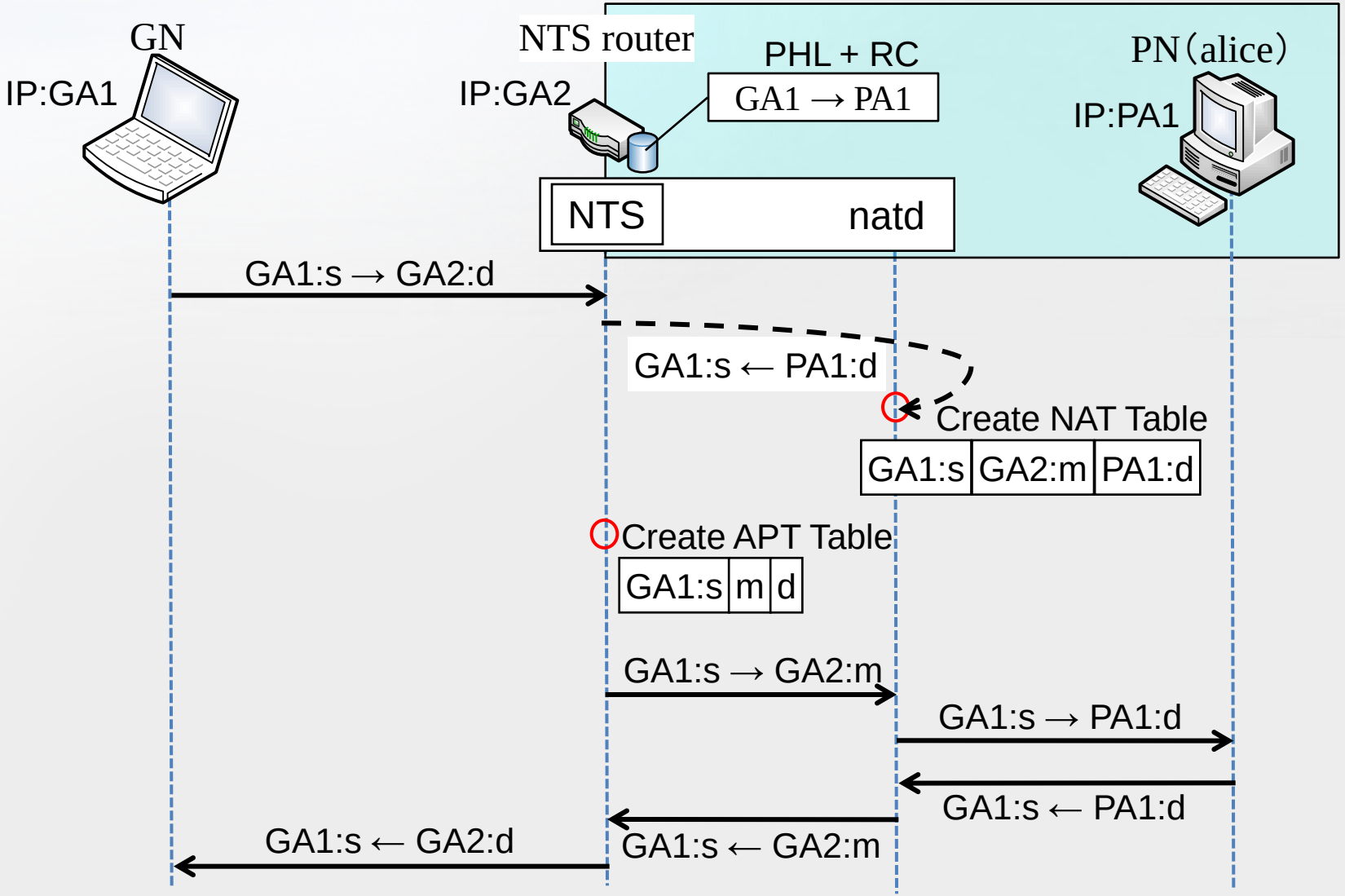
- NTSが53番で待ち，DNS-requestを受け取る
- 役割はDNSパケットを中継・解析してNTSネゴシエーションを行うのみ

実装概要（NTS Router）

- 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



提案方式（NATテーブル作成方法）



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GN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

- 今後の展開
  - 提案方法の実現
  - 技術比較と性能評価

補足説明

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GN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
    （GN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GNも開始し損ねただけなので，もう一度行えば良い

NAT越え既存技術例

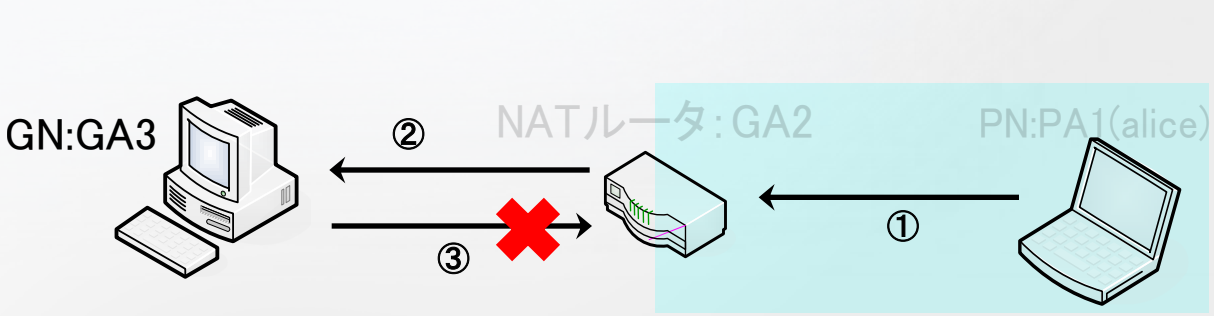
技術名	実装箇所	概略
STUN (Simple Traversal of UDP Through NATs)	GN PN STUNサーバ	UDP Hole Punchingを使ってNATを通過する方法． UDP Hole Punching：UDPを用いて予め内部より外部に通信を行うことでNATに通り道を用意しておき，そこを通して外部より内部に通信を行う方式.
IPv4+4	GN PN NATルータ	IPv4ヘッダを拡張することで更に32bit追加する. グローバルアドレスとプライベートアドレスを両方保持し、NAT通過時にこのヘッダを見て二つのアドレスを入れ替えることにより通信が可能となる.
NATS (NAT with Sub-Address)	GN NATルータ DNS	IPアドレスとは別に16bitsのサブアドレスを定義し，NAT／NAPT内のホストを特定する手段.
AVES （Address Virtualization Enabling Service）	Waypoint DNS NATルータ	グローバル空間にwaypointと呼ばれる機器を配置し，それを経由してグローバルアドレス空間の端末はプライベートアドレス空間の端末に通信を行う.
NAT-f	GN NATルータ	GNとNATルータが情報交換し，FQDNから内部端末を特定し，パケットを通す

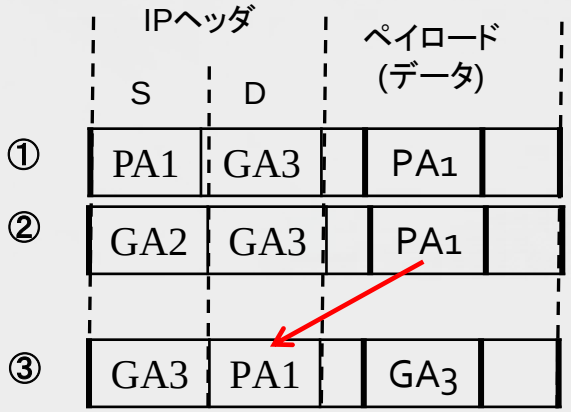
NATによる別の課題と解決方法

- 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

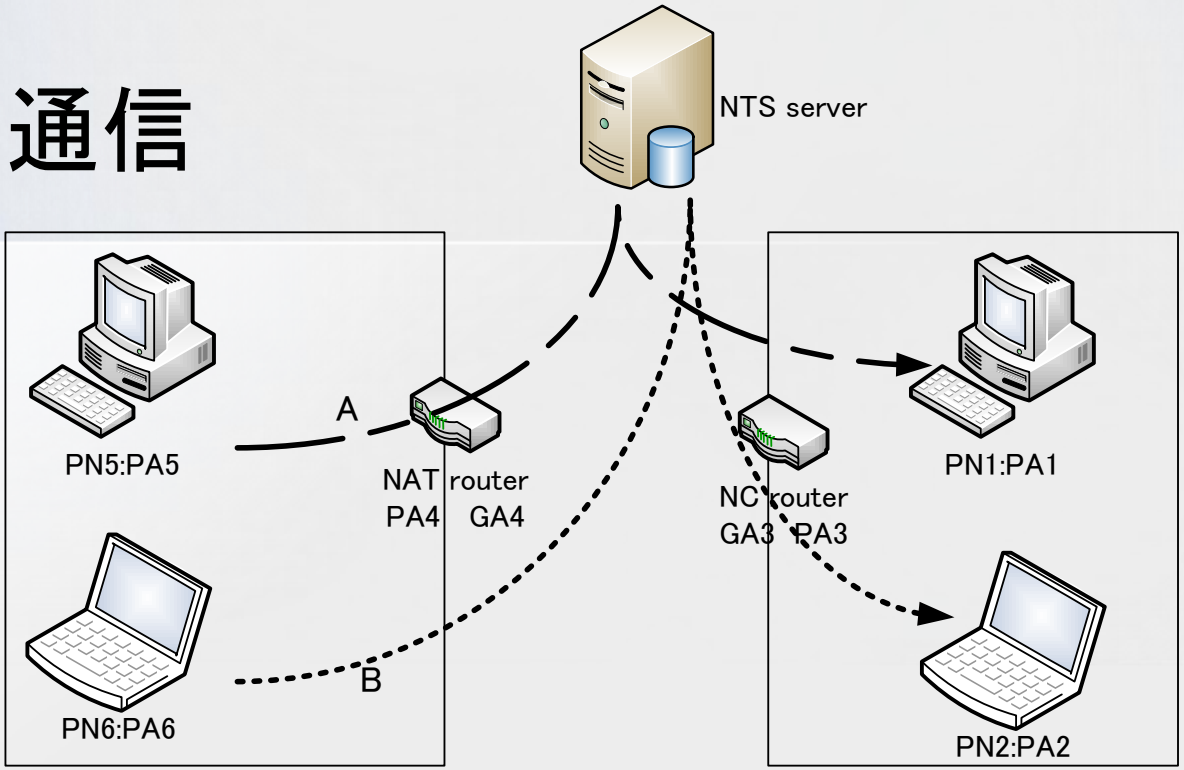




- NATではIPおよびTCP/UDPヘッダに記述されるアドレスを書き換えるが，ペイロード部は関知しない
- そこで，ALGによりアプリケーション内のアドレスも書き換える

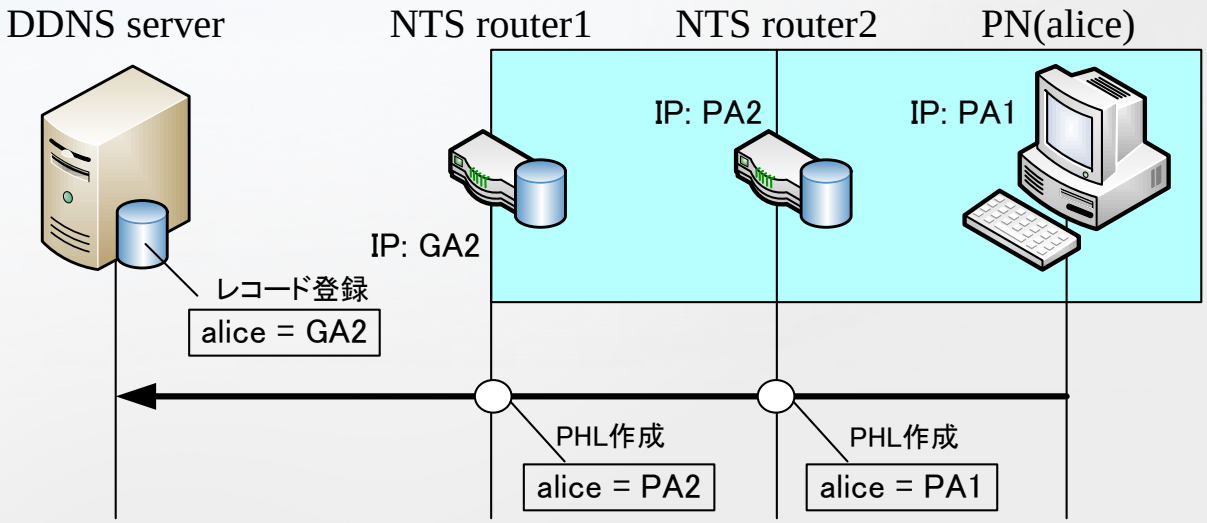
同NATからの通信

通信A：PN5→PN1
通信B：PN6→PN2



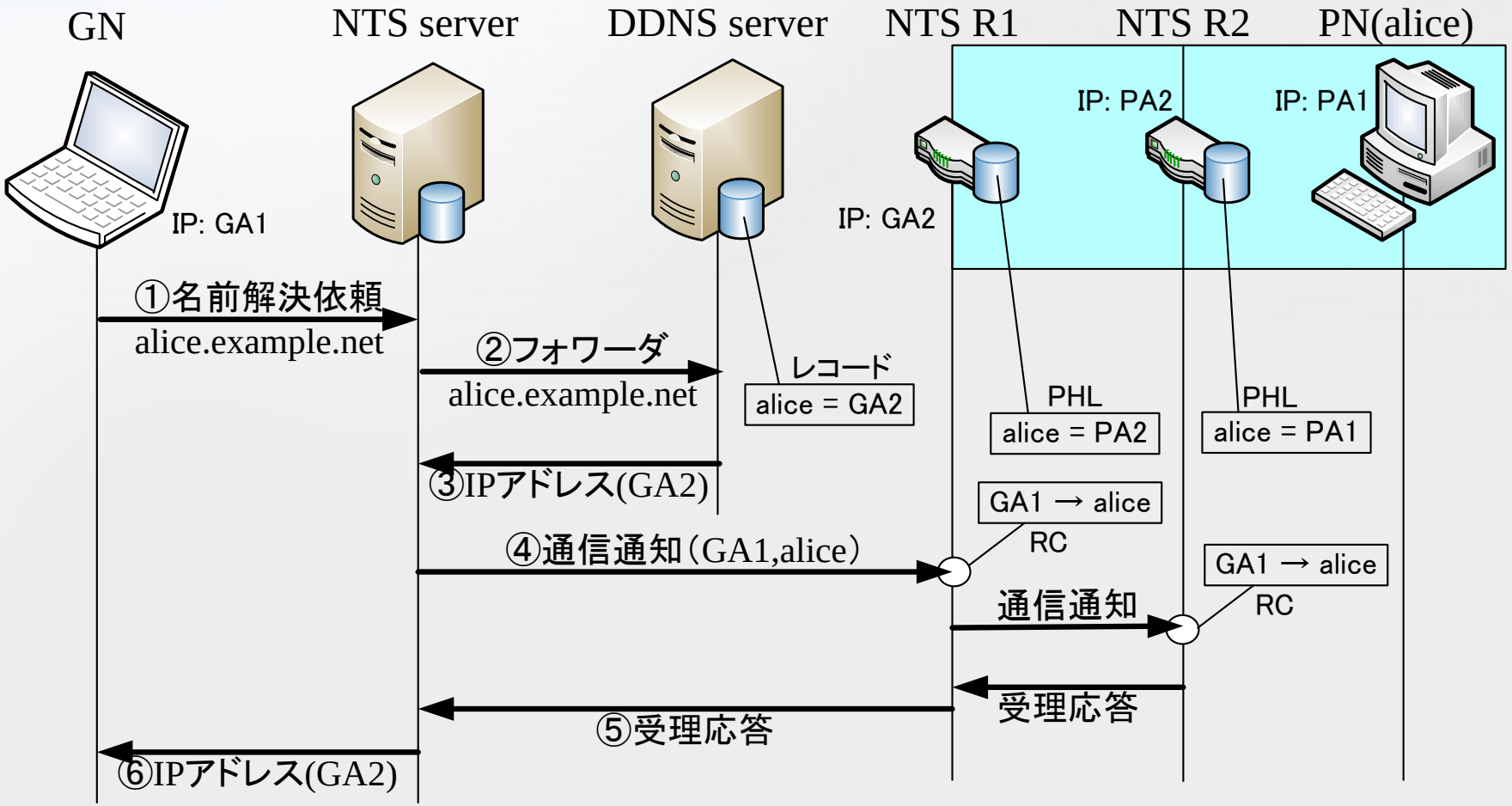
- PN5からPN1，PN6からPN2に通信があった場合
  - NTSルータのキャッシュにはGA4からPA1･2という情報が書かれるため，AとBの通信が同時にあった場合，NTSルータが混同してしまう可能性がある
  - NTSルータが同じアドレスから通信通知を受け取った場合，後に来た方を遅らせて応答することで解決

二重NATの場合(名前登録)

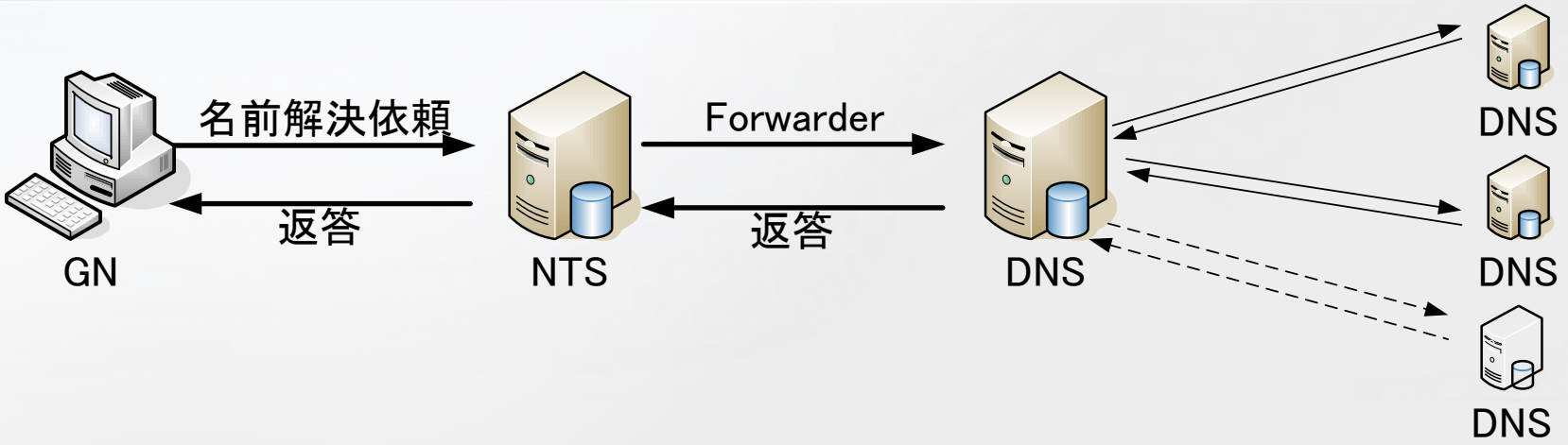


- NTS routerはそれぞれ名前登録パケットが内側から通過した時にPHLを作成する.
- NATは内側からのパケットを自分の外側で使えるIPアドレスに書き換えて送信するので，NTS router１と２ではそれぞれのネットワークに対応したアドレスのPHLが作成される.

二重NATの場合(名前解決)

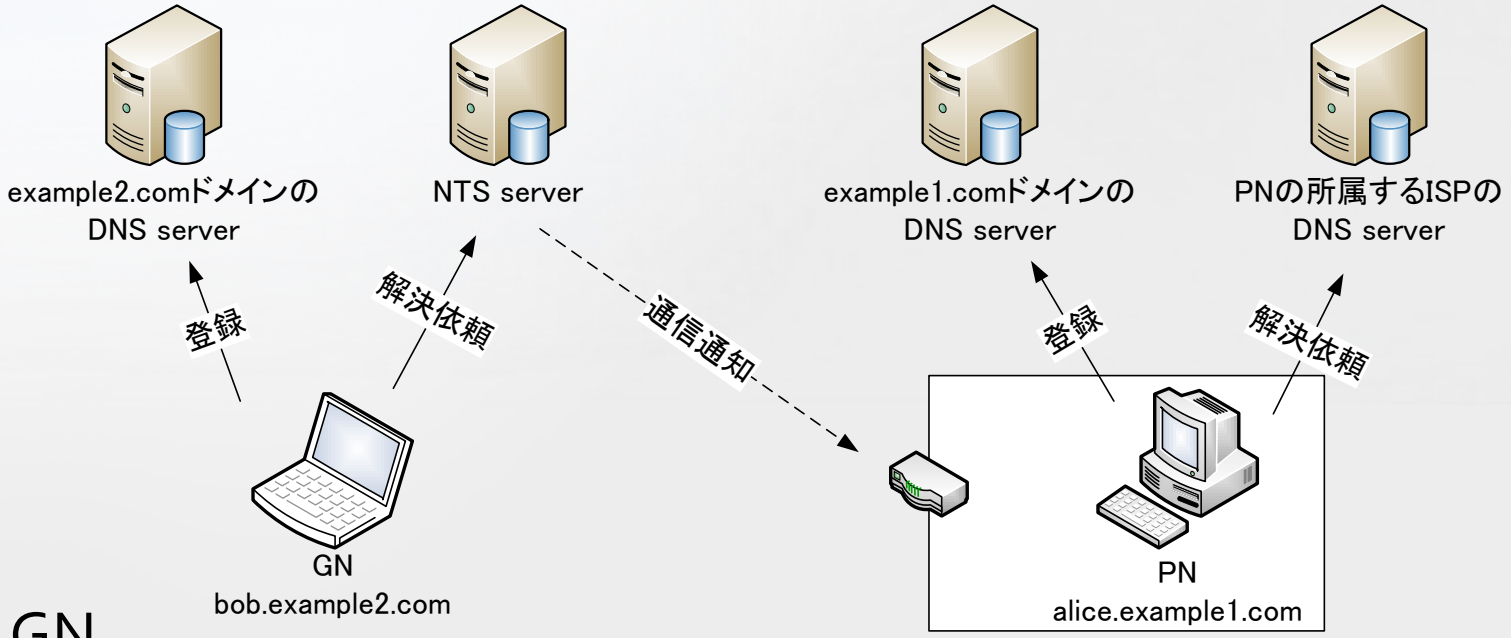


NTSとDNSの関係



- GNは予めプライマリDNSとしてNTSを登録しておく必要がある
  →NTSは直接GNと通信を行うことでGNのIPアドレスを得る
- この方式が普及し，一般のDNSにNTSの様なルータとやり取りする機能が実装されれば，GNはプライマリDNSを変換することなく実現できる

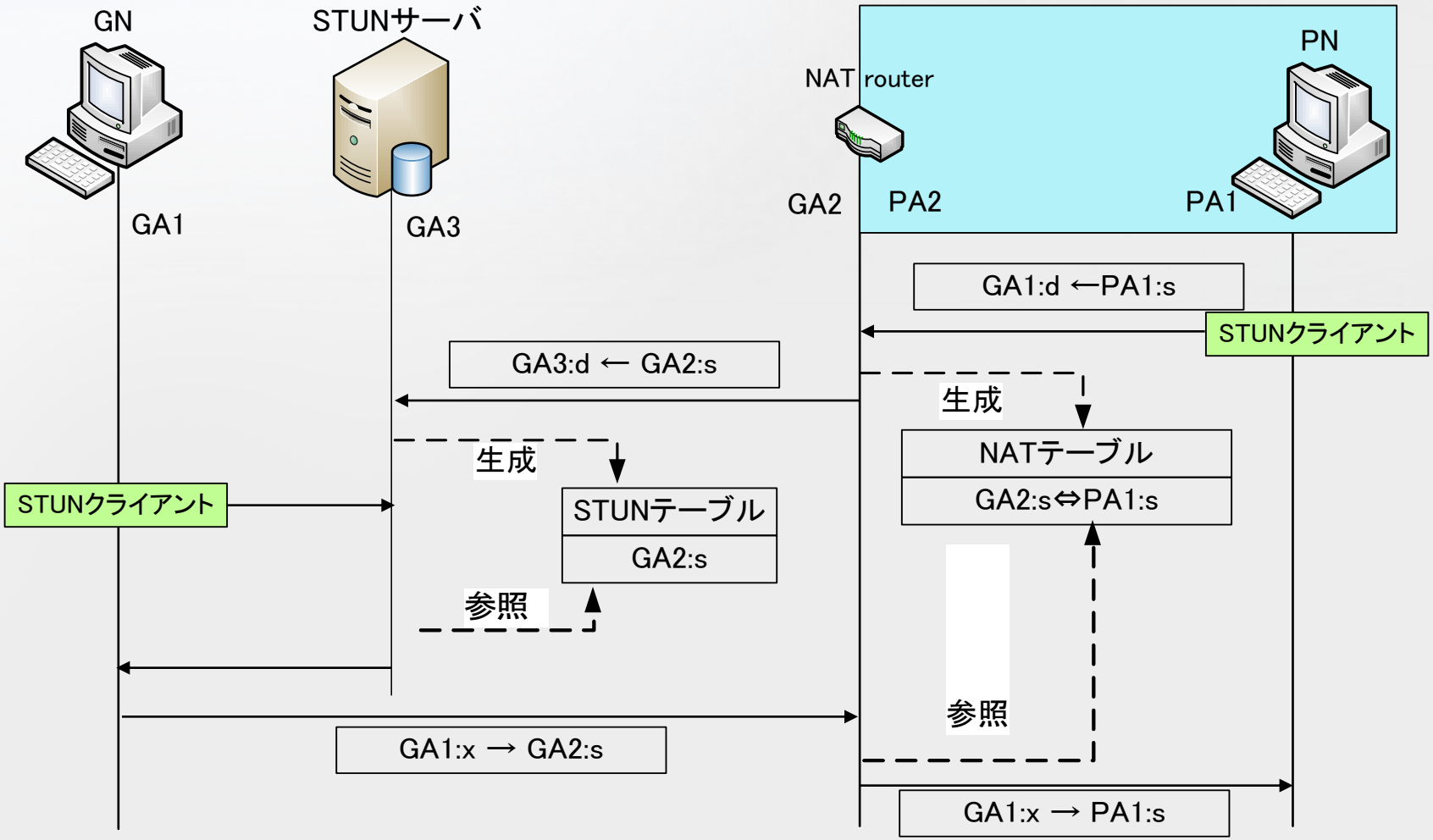
DNS対応関係



- GN
  - 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
- PN
  - 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

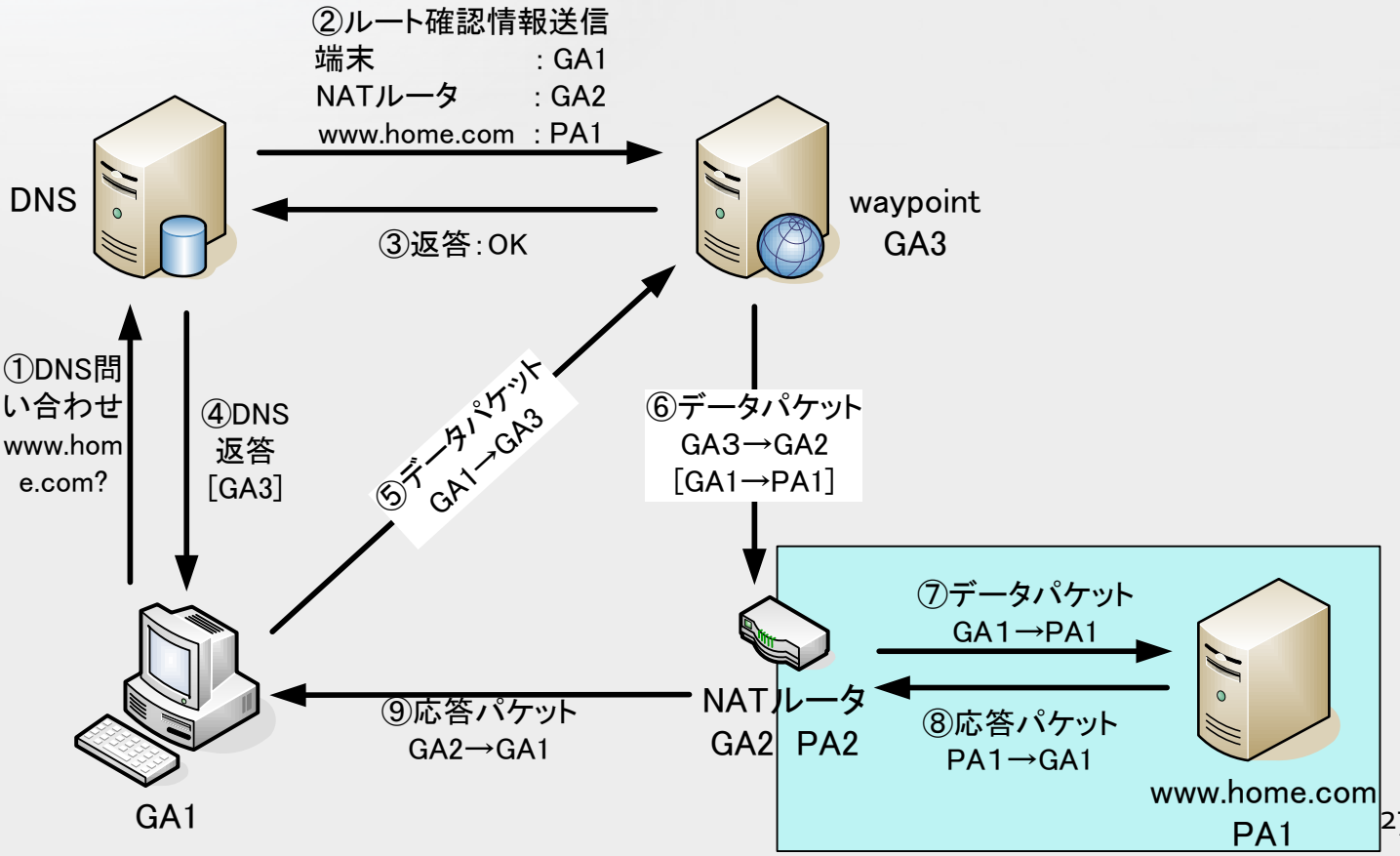
STUN

(Simple Traversal of UDP Through NATs)

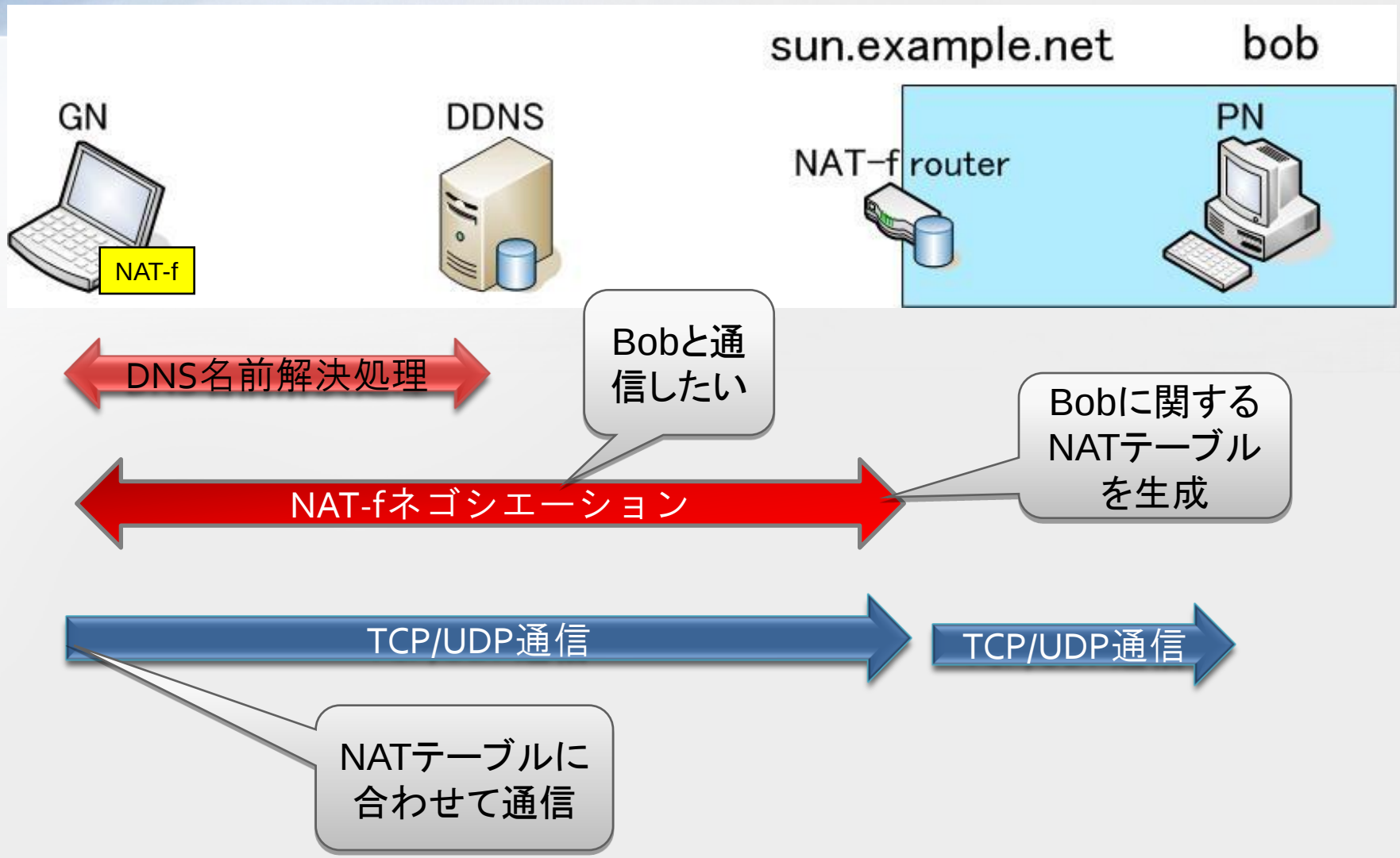


NAT越え既存技術例：AVES

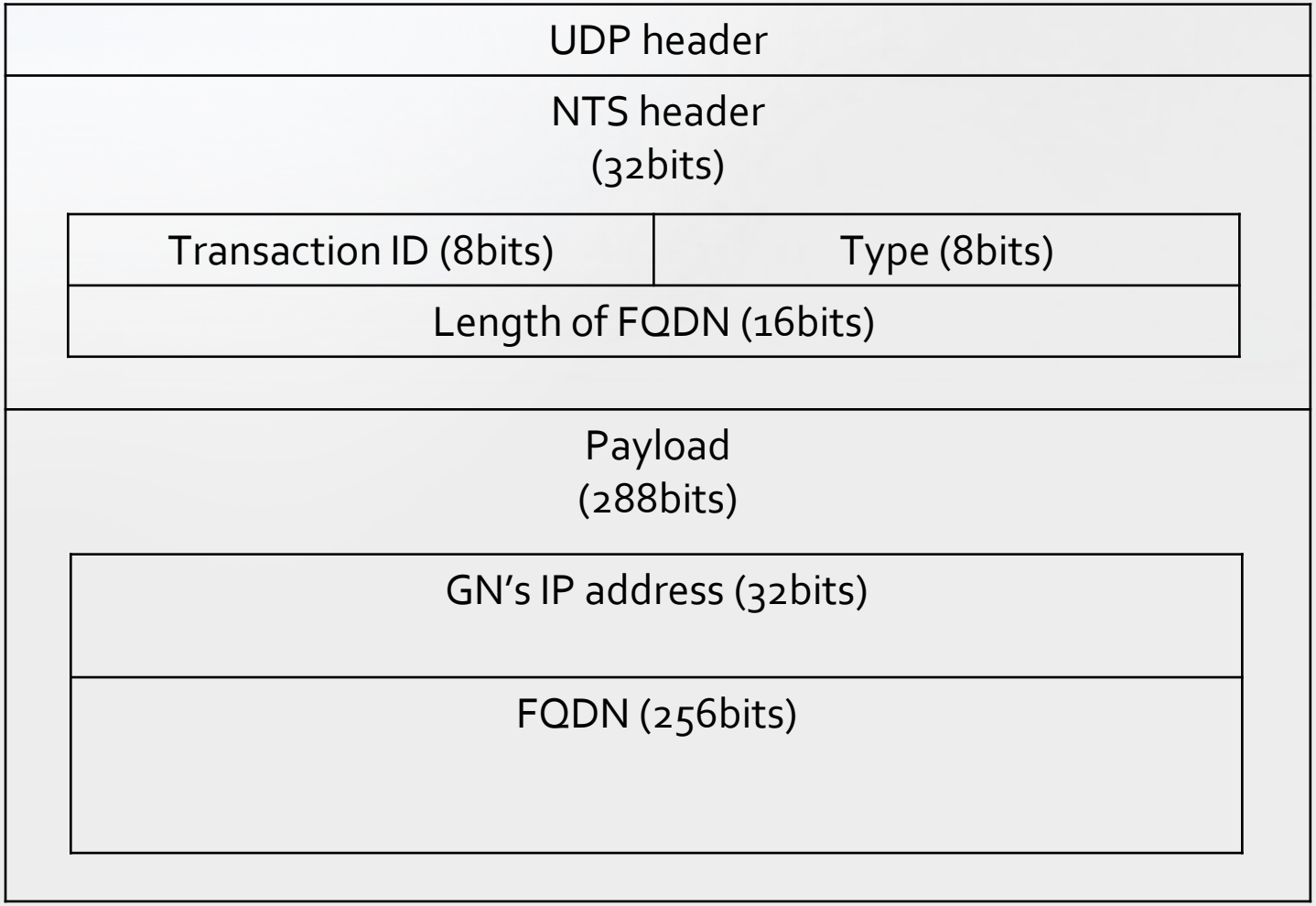
- DNS,NATルータ,waypointサーバを改良・設置
- 外側の端末は内側の端末への通信に全てwaypointを中継する
  →三角経路



NAT-f（NAT-free）protocol



NTS-Negoパケットフォーマット



NTSサーバの処理

1. 受けた通信が名前解決依頼(53番ポート宛)であった場合、bindに渡す(forwardして解決)
2. bindから返って来たパケットを解析・待避し、NTSルータへの通知パケットを生成・送信
3. GNへ名前解決を返信

＊bindとは名前解決を行うDNSアプリケーション

NTSルータの処理

- 内側からパケットが通過した時
  1. DNS登録パケットのupdateなら解析する
  2. パケット内容に合わせてPHLを作成
  3. 登録パケットを通す
- 外側から通信を受けた時
  1. NATテーブルに対応があるなら本来のNAT動作
  2. NTSサーバからの通信なら，内容をRCとして保持
  3. その他の通信ならRCとPHLを参照し，該当すればNATテーブルを作成し，RCを消去
  4. 該当しなければ通常通りのNATルータの処理

プライマリDNSの設定方法

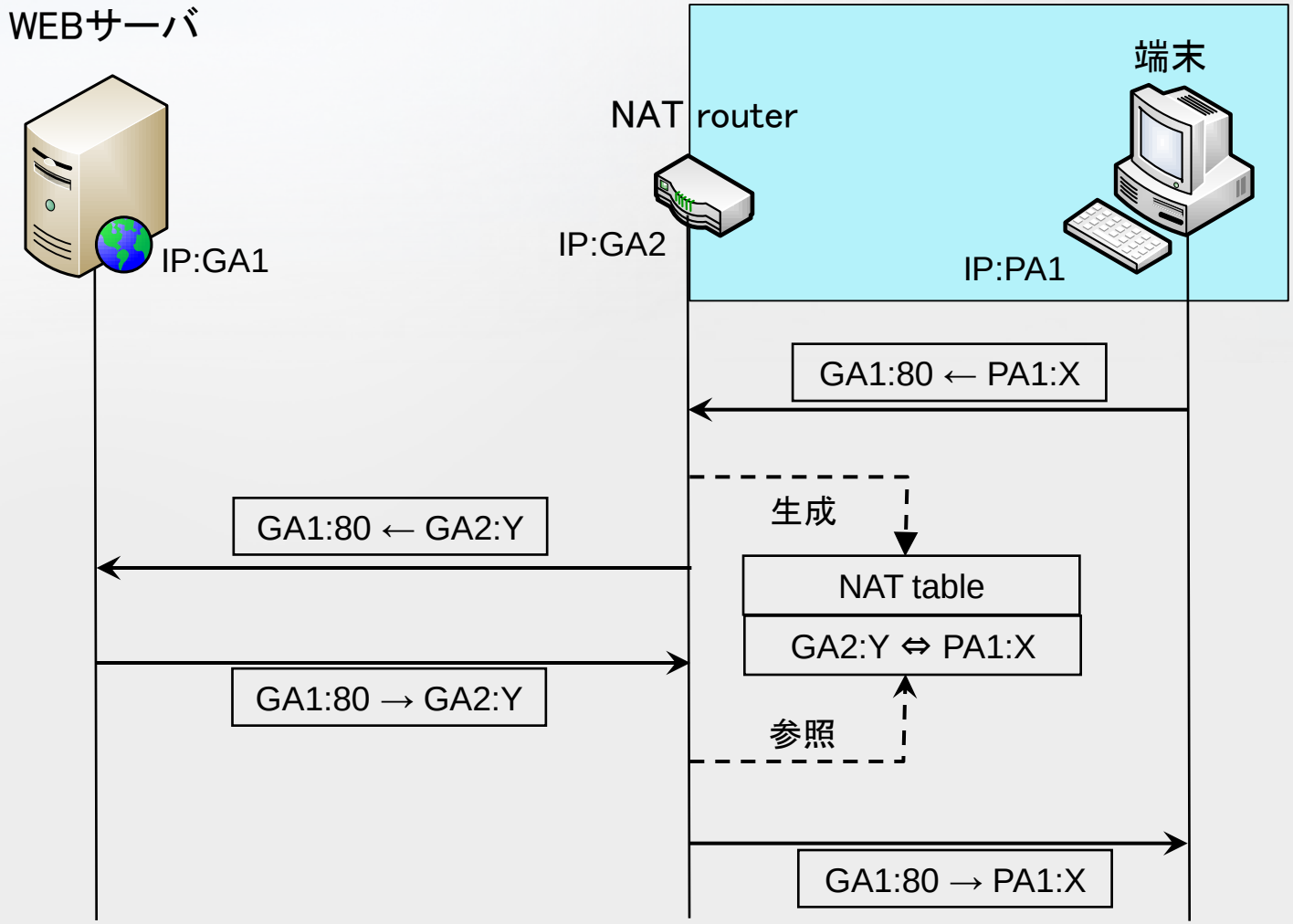
- Windows XPの場合
  - 「スタート」-「コントロールパネル」-「ネットワークとインターネット接続」-「ネットワーク接続」-「ローカルエリア接続」を開く
  - 全般タブのプロパティからインターネットプロトコル(TCP/IP)のプロパティ
- Windows Vistaの場合
  - 「スタート」-「コントロールパネル」-「ネットワークとインターネット」-「ネットワークと共有センター」-「ネットワークの管理」-「ローカルエリア接続」を開く
  - ローカルエリア接続の状態のプロパティにあるネットワークタブのインターネットプロトコルバージョン４(TCP/IPv4)のプロパティ

NAT(Network Address Translator)

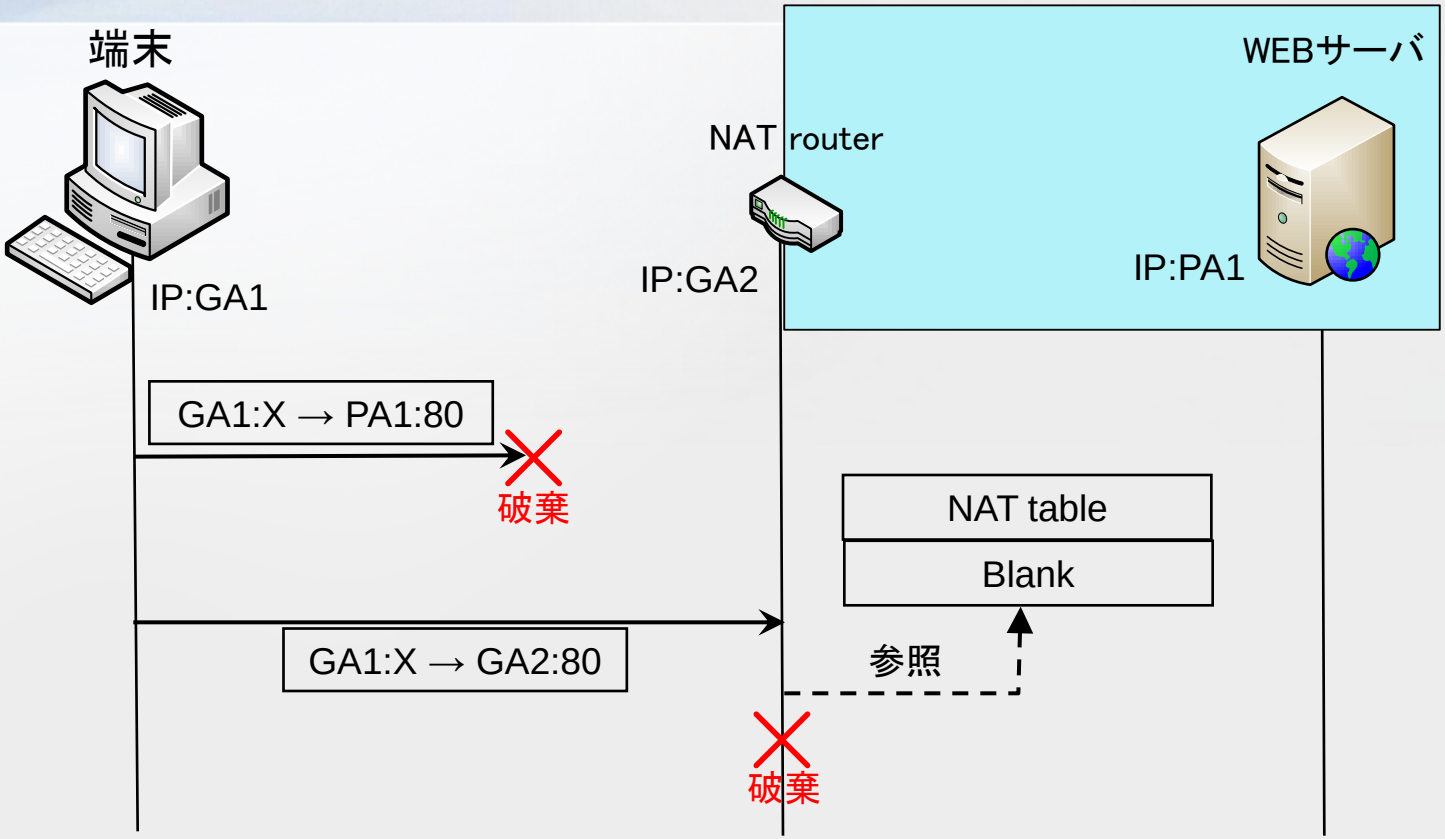
- IPアドレスの枯渇
- プライベートIPアドレス
  - クローズなネットワーク内のみで利用できるIPアドレス

- 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の動作（内→外）


WEBサーバ
IP:GA1
NAT router
IP:GA2
端末
IP:PA1
GA1:80 ← PA1:X
生成
GA1:80 ← GA2:Y
NAT table
GA2:Y ⇔ PA1:X
GA1:80 → GA2:Y
参照
GA1:80 → PA1:X

NATの動作（外→内）



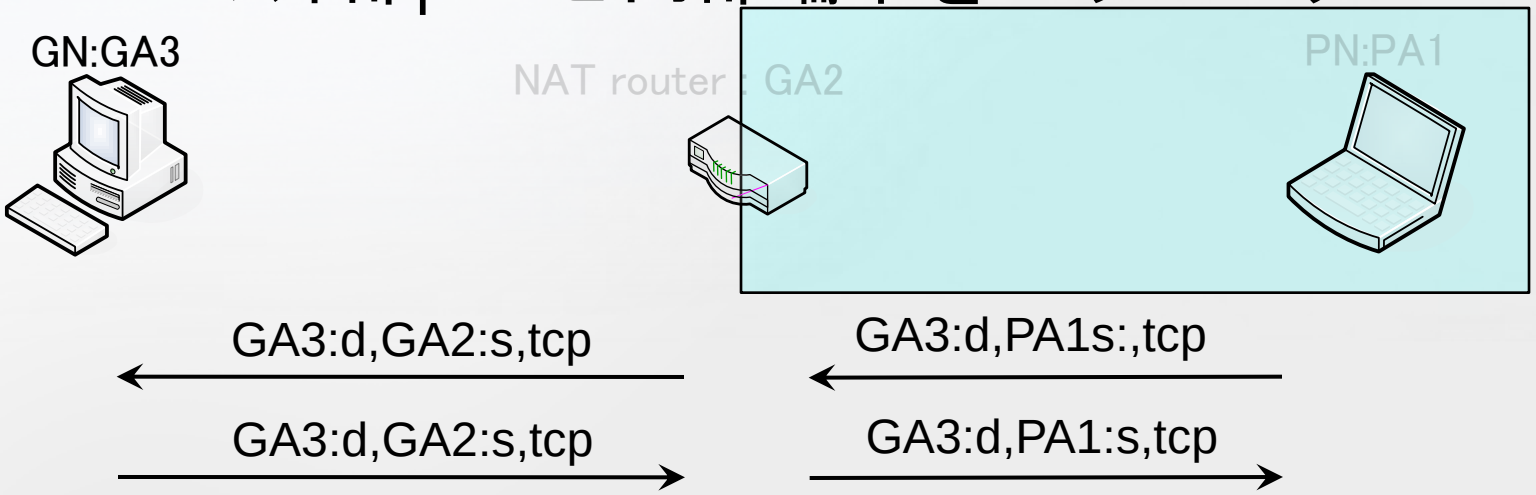
NAT越え問題

NATのマッピング方法

- マッピングの仕方で四つに分類できる
  - 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

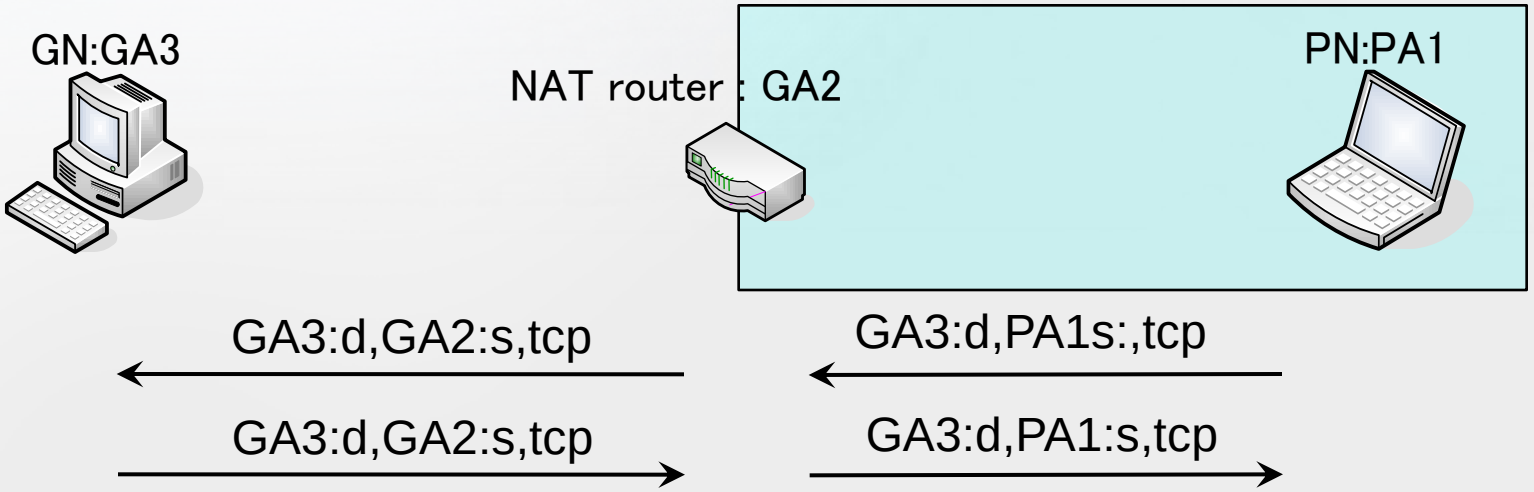
- NATの外部portと内部端末をマッピング



NAT table						
Remote		Global		Local		Protcol
address	port	address	port	address	Port	
		GA2	s	PA1	s	tcp

Restricted Cone NAT

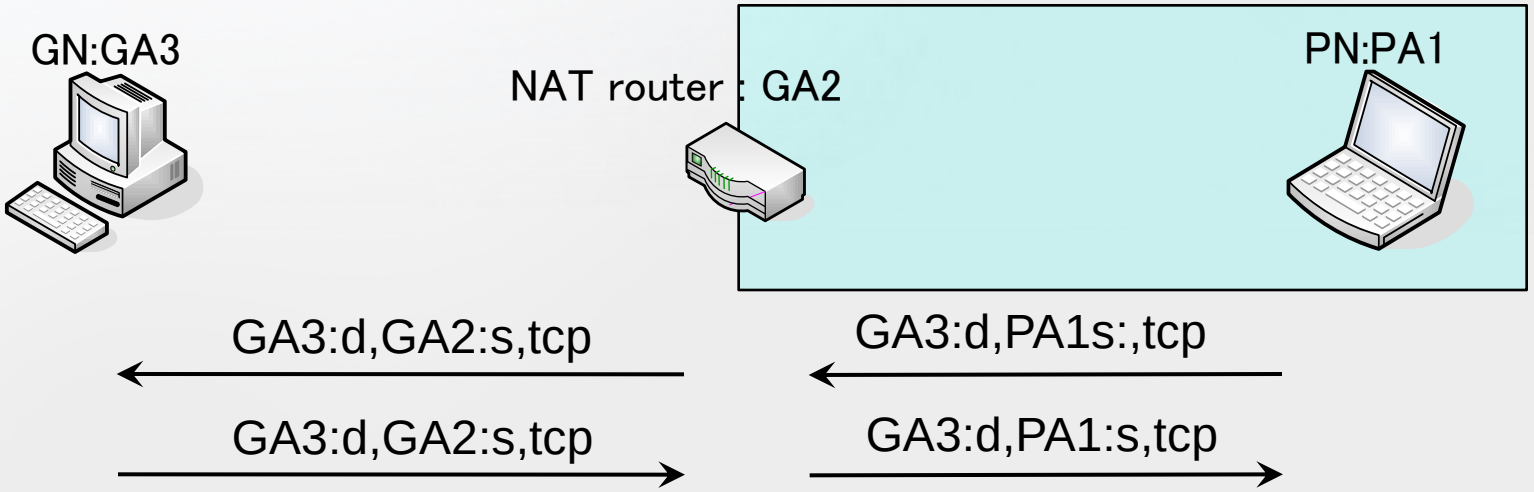
- NATの外部portと内部端末のマッピングだけでなく，リモート端末のIPアドレスも対応付ける



NAT table						
Remote		Global		Local		Protcol
address	port	address	port	address	Port	
GA3		GA2	s	PA1	s	tcp

Port Restricted Cone NAT

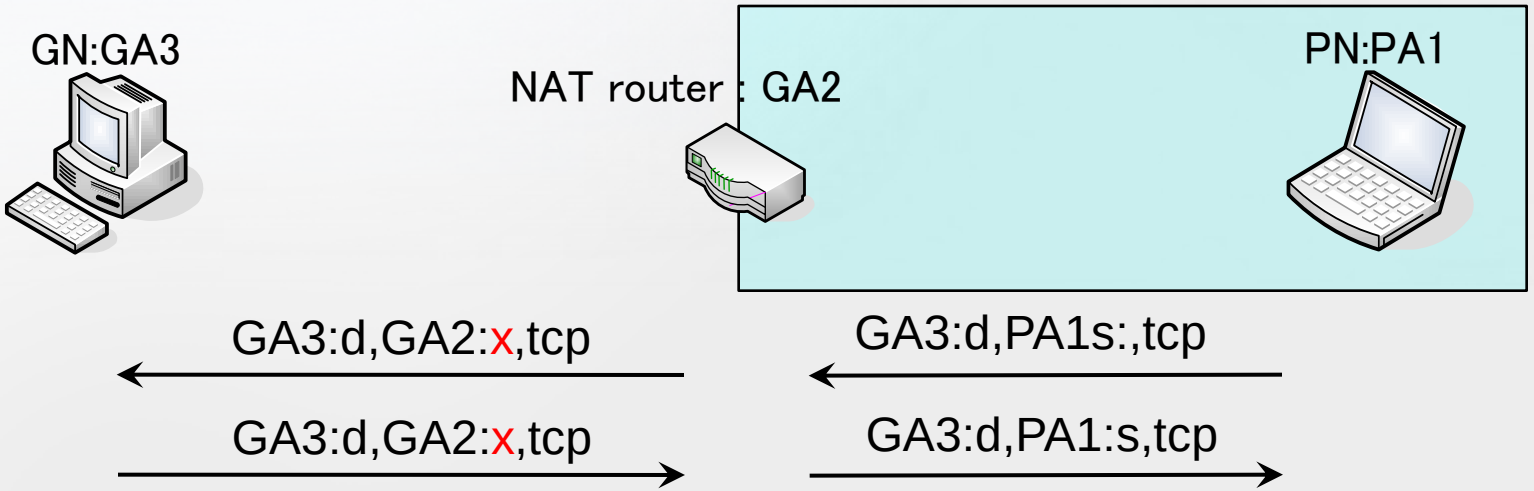
- Restricted Cone NATに加え，リモート端末のportも対応づけてマッピングする



NAT table						
Remote		Global		Local		Protcol
address	port	address	port	address	Port	
GA3	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		Protcol
address	port	address	port	address	Port	
GA3	d	GA2	x	PA1	s	tcp