端末の機能追加が不要なNAT越え方式の提案

宮崎　悠[†]　鈴木秀和[†]　渡邊　晃[†]

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．

A Proposal for a NAT Traversal System that Does Not Require Additional Functions at Terminals

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

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.

1. はじめに

インターネットでは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され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)]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，企業ネットワークにおいてはファイアーウォールが設置され，内側からの通信開始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，そこでは企業のような厳しいセキュリティポリシーは必要とならない．よって，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ため，上記のようなNATの制約を除去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越えの既存技術として，STUN (Simple Traversal of User Datagram Protocol Through Network Address Translators)[2)]，AVES(Address Virtualization Enabling Service)[3)]やNAT-f (NAT-free protocol)[4)]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越えを実現しているが，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，経路冗長が発生するという課題がある．我々はSTUNやAVESの課題を解決するため，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NAT越えを実現できるNAT-fと呼ぶプロトコルを提案している．しかし，端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．そこで本稿ではDNSサーバ[5),6)]とNAT

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

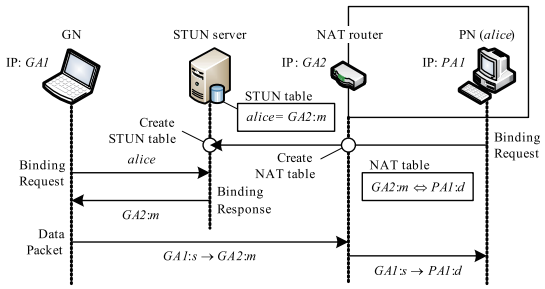


図 1 STUN の動作
Fig. 1 Flow of STUN.

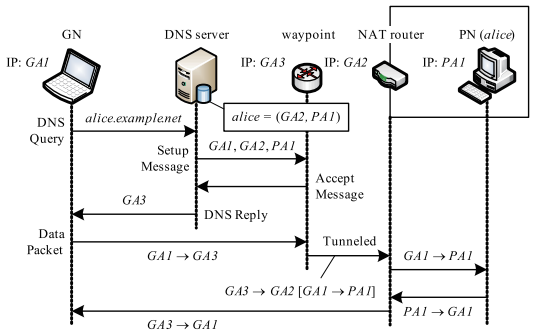


図 2 AVES の動作
Fig. 2 Flow of AVES.

ルータが協調することにより，一般のユーザ端末でも NAT 越えを可能とする方式を提案する．以降，第 2 章では NAT 越えの既存技術についてより詳しく解説し，第 3 章で提案方式を説明し，第 4 章でまとめる．

2. 既 存 技 術

2.1 STUN

STUN とは UDP Hole Punching[7] 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 に通り道を用意しておき，そこを通して外部から内部に通信を開始する方法である．STUN を利用するにあたり，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，登録された情報を得る．GN は上記で得た情報を元に NAT ルータへパケットを送信すると， 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．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うえ，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 アドレスと PN の所属する 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，PN の 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アドレス 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 WEB サーバへ送信する．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 ”sun.example.net” の先頭に PN のホスト名 ”alice” を付加して DDNS サーバに名前解決依頼を行う．DDNS(Dynamic DNS) サーバ[8] 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

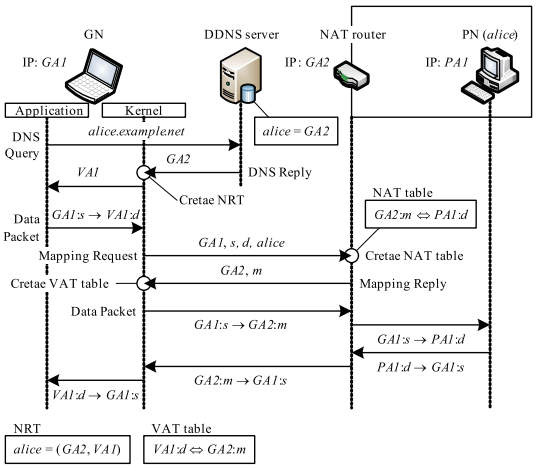


図 3 NAT-f の動作
Fig. 3 Flow of NAT-f.

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”とおよび 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 ルータは先ほど GN から受信した送信元／宛先 IP アドレス，ポート番号，プロトコルタイプ， NAT ルータのグローバル IP アドレス，および NAT テーブルに生成された変換後の送信元ポート番号”x”を GN へ応答する．GN が NAT ルータからの応答を受信すると，取得した情報から VAT テーブルを生成する．その後，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．

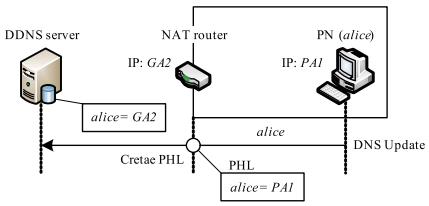


図 4 DNS 名前登録
Fig. 4 DNS registration.

3. 提 案 方 式

3.1 ネットワーク構成

本提案方式は DNS サーバと NAT ルータに機能を追加することにより NAT 越えを実現する．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 NAT ルータ，その NAT ルータと協調する NTS(NAT-Traversal Support) サーバ，DDNS サーバが存在する． NTS サーバは DNS サーバの仕様を拡張したもので，NTS サーバと NAT router には本方式の機能が実装されている必要がある．GN，NAT ルータのグローバル IP アドレスをそれぞれ GA1，GA2 とする．また 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 GN1 から PN1(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

本方式を適用するに当たり，GN はプライマリ DNS として任意の 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 のユーザは予め FQDN(Fully Qualified Domain Name) と NAT ルータのアドレスを DDNS 登録する必要があ

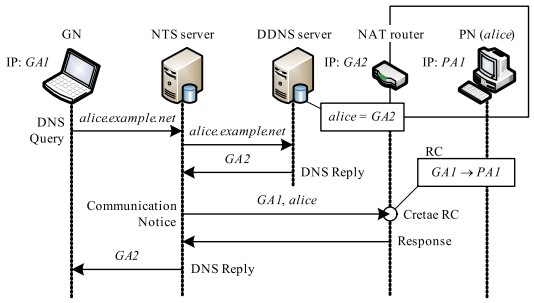


図 5 名前解決シーケンス
Fig. 5 Sequence of name resolution.

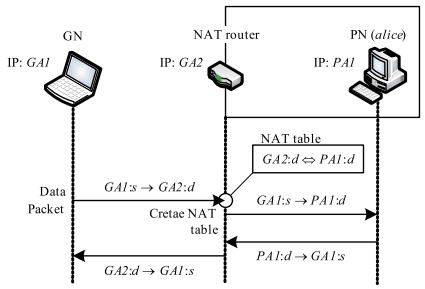


図 6 通信開始シーケンス
Fig. 6 Sequence of the start of communications.

る．これは一般の DDNS 登録と同様である．図 4 に名前登録シーケンスを示す．DDNS 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．これを受け取った NAT 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させて 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) への通信を開始する場合の名前解決シーケンスの例を示す．GN は PN(alice) に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により上位 DNS へ名前解決を依頼する．次に NTS サーバは GN から alice への接続依頼があることを NAT ルータに通知する．この通知を受け取った NAT ルータは PHL を参照し，GA2 から PA1 へ通信があるということをキャッシュしておく．これは RC(Request Cache) として保持しておく．そして NAT ルータは NTS サーバへ通知応答を返す．NTS サーバは GN の名前解決に対して NAT 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 へ通信を開始する．NAT ルータはパケットを受け取るとキャッシュを確認する．キャッシュに該当するデータがあれば，受け取ったパケットとキャッシュ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．NAT ルータは生成した NAT テーブルに従いパケットを 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．以後は上記の手順を繰り返すことにより通信を行う．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の動作である．

4. 評　　価

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．提案方式では，NTS サーバは特殊な装置ではあるが，DNS サーバを改造することで実現できるので”第三装置”の欄は△とした． しかし，実際に名前解決を行う DNS サーバ自体は改造してないので，”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をそのまま利用できるが，第三の装置が必要で，アプリケーションが限定される．AVES ではユーザ端末に機能を実装する必要はないが， 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しないが，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．アプリケーショ

表 1 NAT 越え技術比較

Table 1 Comparison of NAT Traversal Technologies

	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	○	×	○	○

ンに制約がなく，P2P 通信が可能である．また，自端末だけでなく，外出先のコンピュータを利用しても容易に NAT 越えを実現できる．さらには ISP(Internet Service Provider) が提案方式を利用し，例えばプライベート IP アドレス空間を用いた無線 LAN を展開するなどのサービスが可能になるものと考えられる．

5. むすび

本論文では各ユーザ端末には機能を追加することなく 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 NAT ルータが協調することにより NAT ルータが動的に NAT テーブルを生成する．各端末間の通信は P2P で行うことができる．今後は実際に NTS サーバと NAT ルータを実装し，更なる検討・評価を行う．

参考文献

1) Srisuresh, P. and Egevang, K.: Traditional IP Network Address Translator (Traditional NAT), RFC 3022 (2001).
2) Rosenberg, J., Weinberger, J., Huitema, C. and Mahy, R.: STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs), RFC 3489 (2003).
3) Ng, T. S. E., Stoica, I. and Zhang, H.: A Waypoint Service Approach to Connect Heterogeneous Internet Address Spaces, *Proc. USENIX Annual Technical Conference*, pp. 319–332 (2001).
4) 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).
5) P.Mockapetris: DOMAIN NAMES - CONCEPTS AND FACILITIES, RFC 1034 (1987).
6) P.Mockapetris: DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION, RFC 1035 (1987).
7) Ford, B., Srisuresh, P. and Kegel, D.: Peer-to-Peer Communication Across Network Address Translators, *Proc. USENIX Annual Technical Conference*, Anaheim, CA, pp.179–192 (2005).
8) Vixie, P., Thomson, S., Rekhter, Y. and Bound, J.: Dynamic Updates in the Domain Name System (DNS UPDATE), RFC 2136 (1997).

端末の機能追加が不要なNAT越え方式の提案

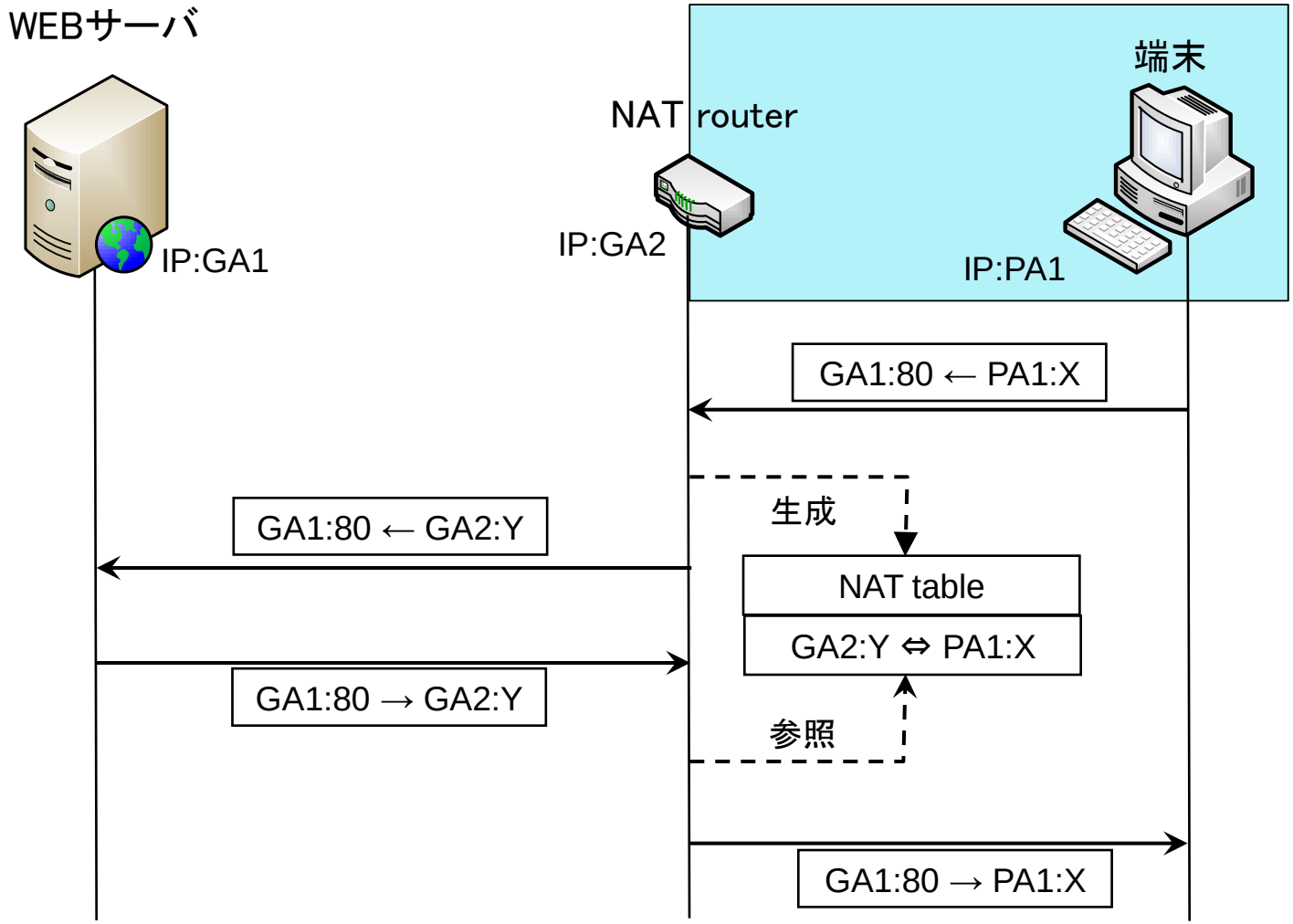
名城大学大学院　理工学研究科
宮﨑 悠　鈴木 秀和　渡邊 晃

研究背景

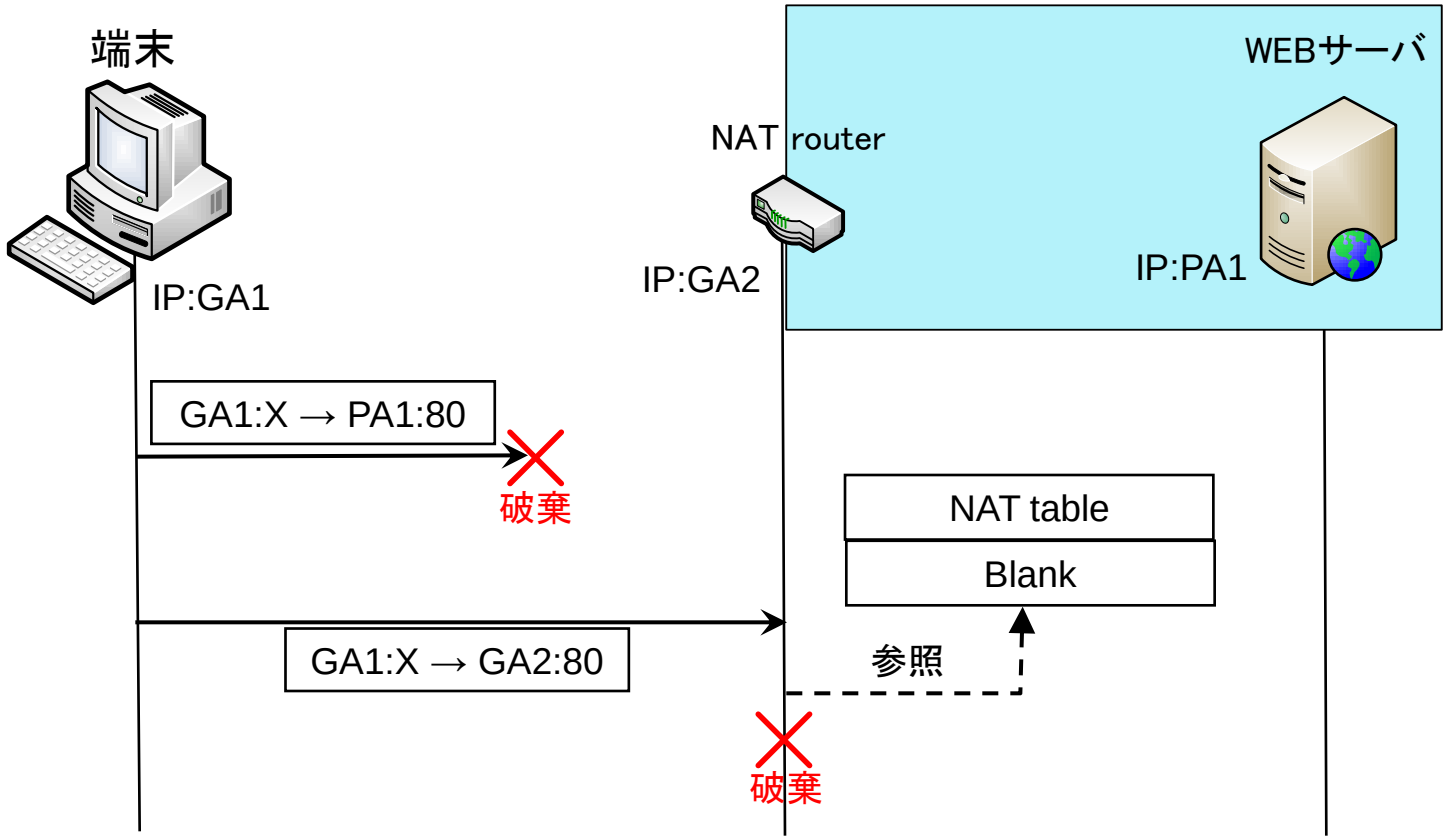
- インターネットの普及に伴ない，ユビキタス社会化が進んでいる
  →いつでもどこからでも通信したい

- 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）

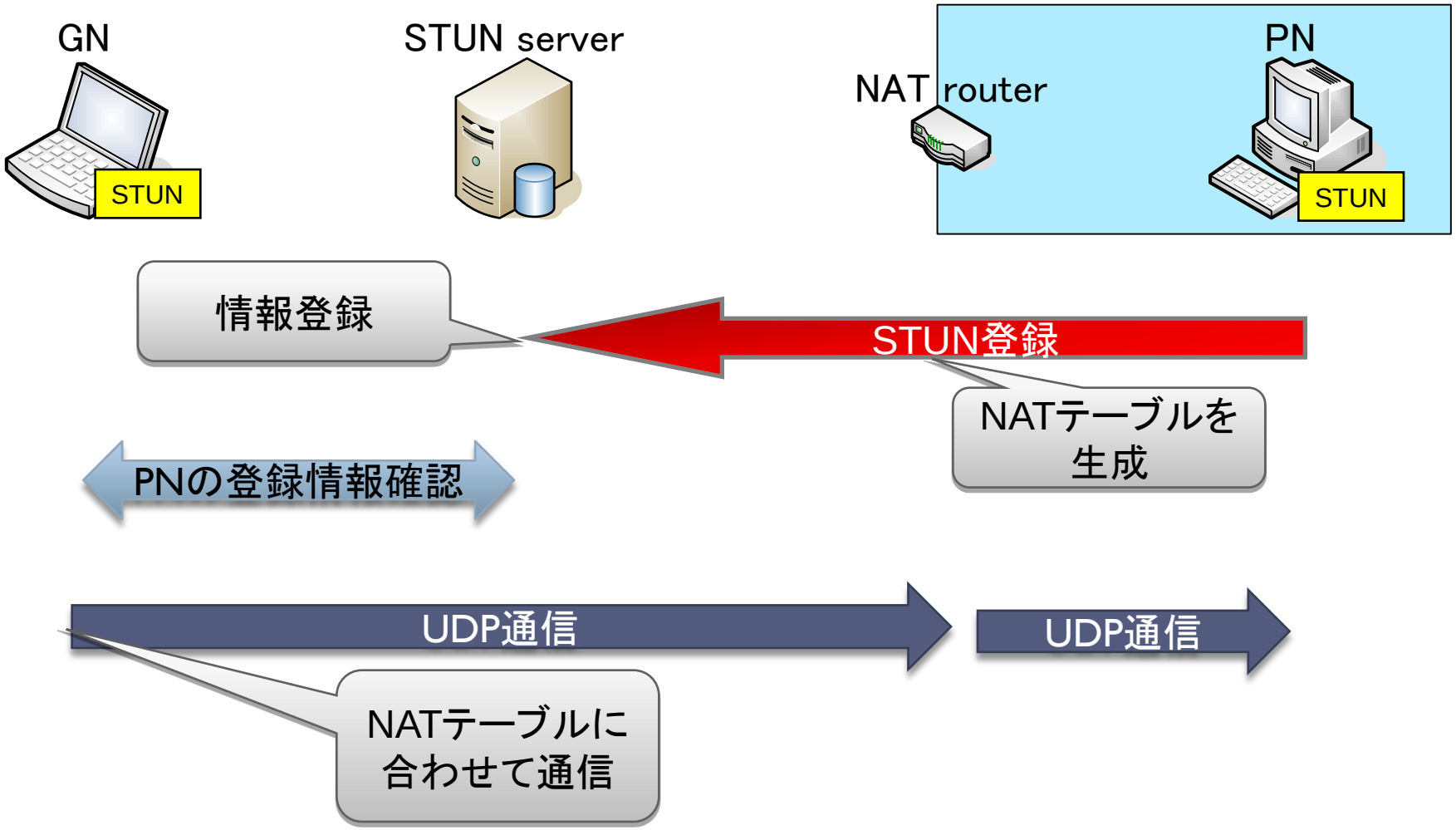

WEBサーバ
IP:GA1
NAT router
IP:GA2
端末
IP:PA1
GA1:80 ← PA1:X
生成
GA1:80 ← GA2:Y
NAT table
GA2:Y ⇔ PA1:X
GA1:80 → GA2:Y
参照
GA1:80 → PA1:X

NATの動作（外→内）

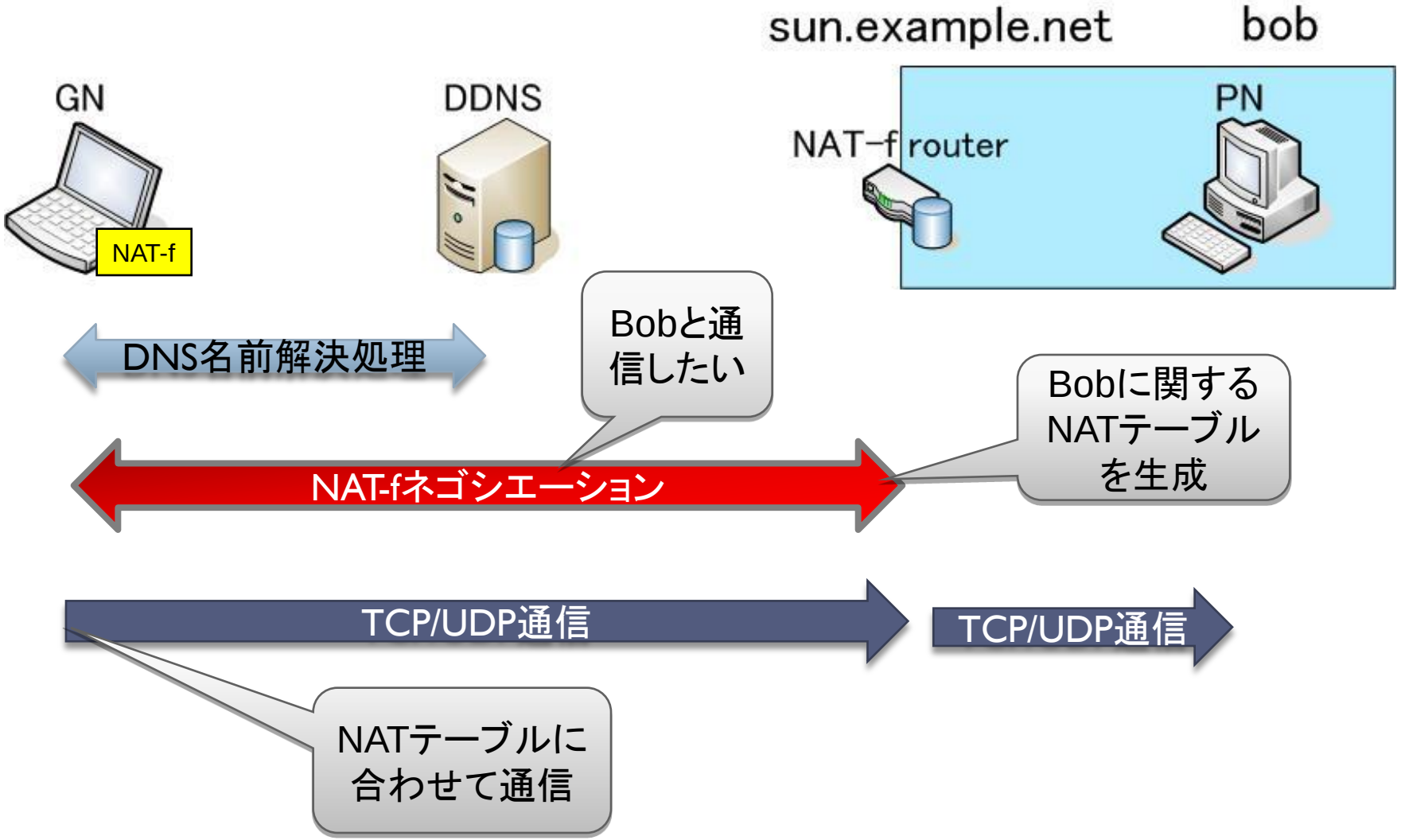


NAT越え問題

STUN(Simple Traversal of UDP Through NATs)



NAT-f（NAT-free）protocol



新たなNAT越え方式の提案

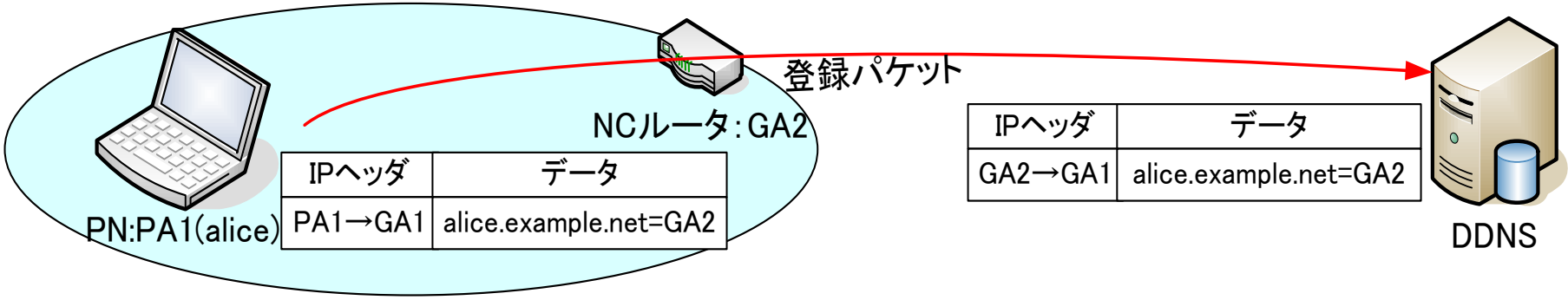
端末には手を加えずに問題を解決したい

本方式ではNATルータとDDNSサーバを改造し，それらが連携をとることにより問題を解決する

NCルータ：NAT with Cache router
NTSサーバ： NAT-Traversal Support server

提案方式（事前設定）

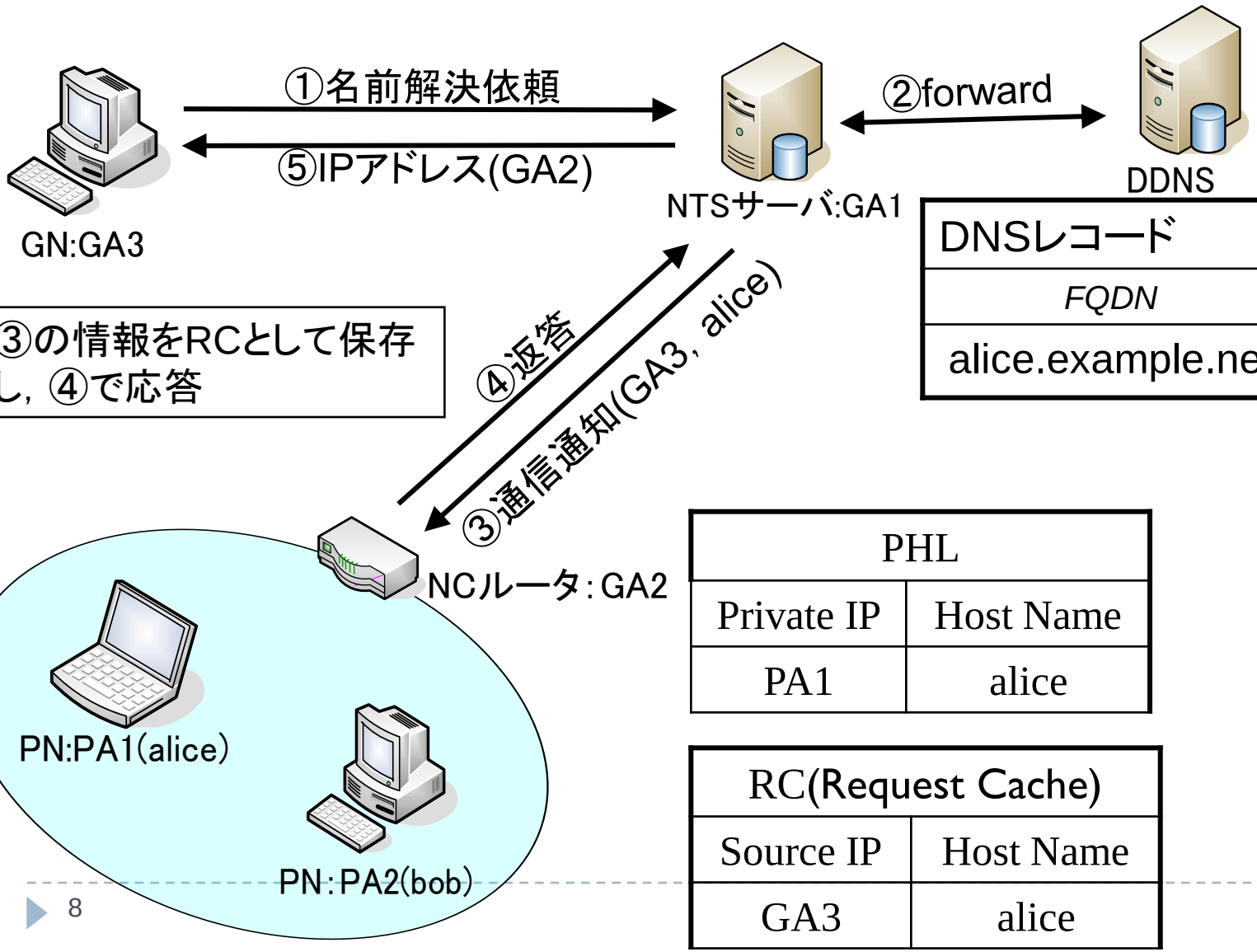
- 予めプライベートアドレス空間内の端末PNの名前とNATルータのアドレスがDDNSへ登録される



- 登録時にNCルータでPHL(Private Host List)を作成する

PHL	
Private IP	Host Name
PA1	alice

提案方式(名前解決)



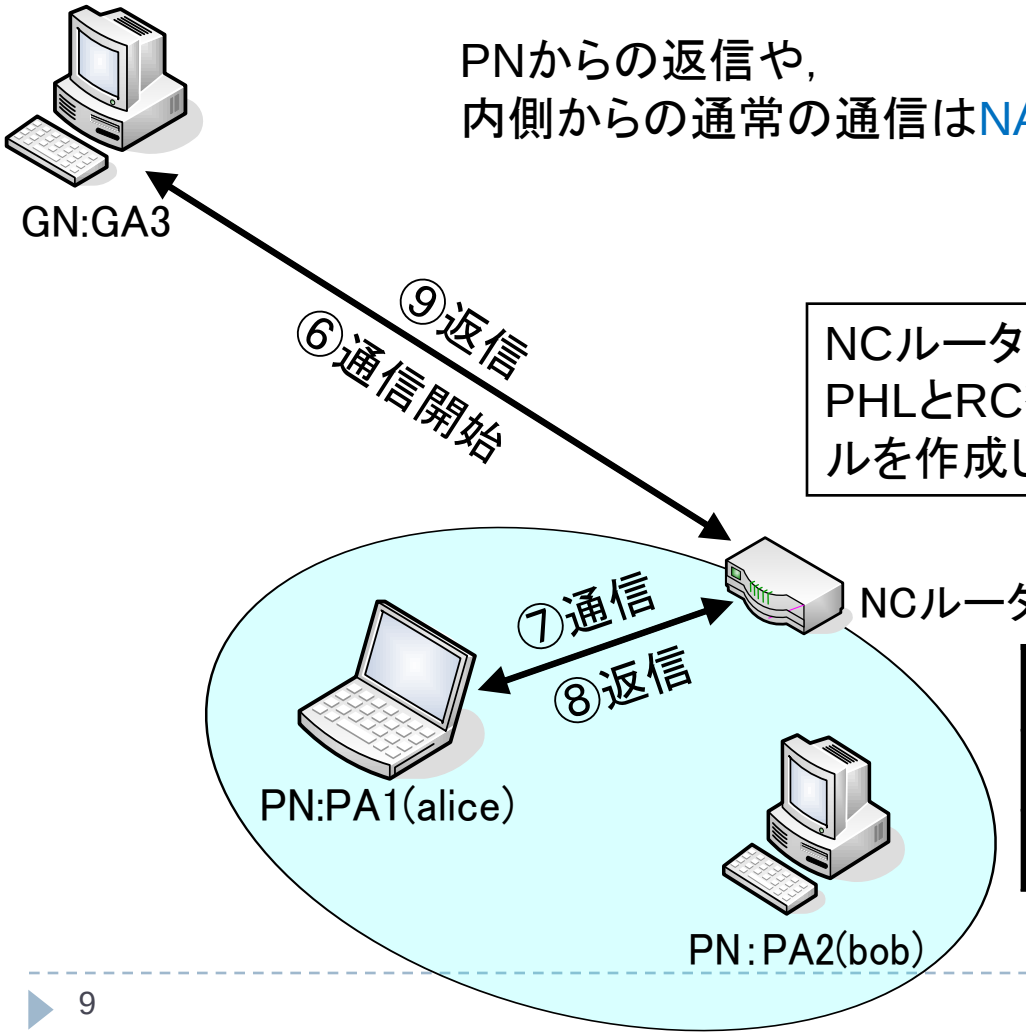
DNSレコード	
FQDN	*NAT router*
alice.example.net	GA2

PHL	
Private IP	Host Name
PA1	alice

RC(Request Cache)	
Source IP	Host Name
GA3	alice

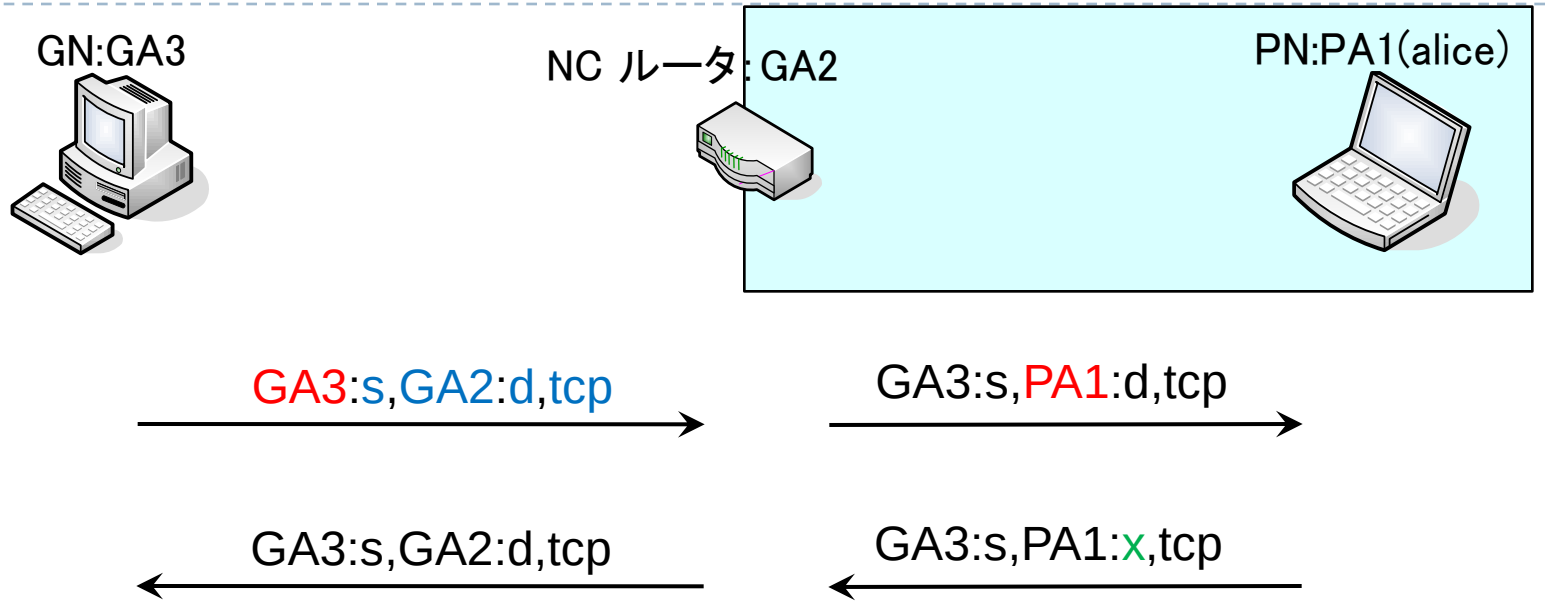
提案方式(通信)

PNからの返信や，
内側からの通常の通信はNATテーブルを使用して通信する



PHL + RC		
Private IP	Host Name	Source IP
PA1	alice	GA3

NATテーブル作成方法



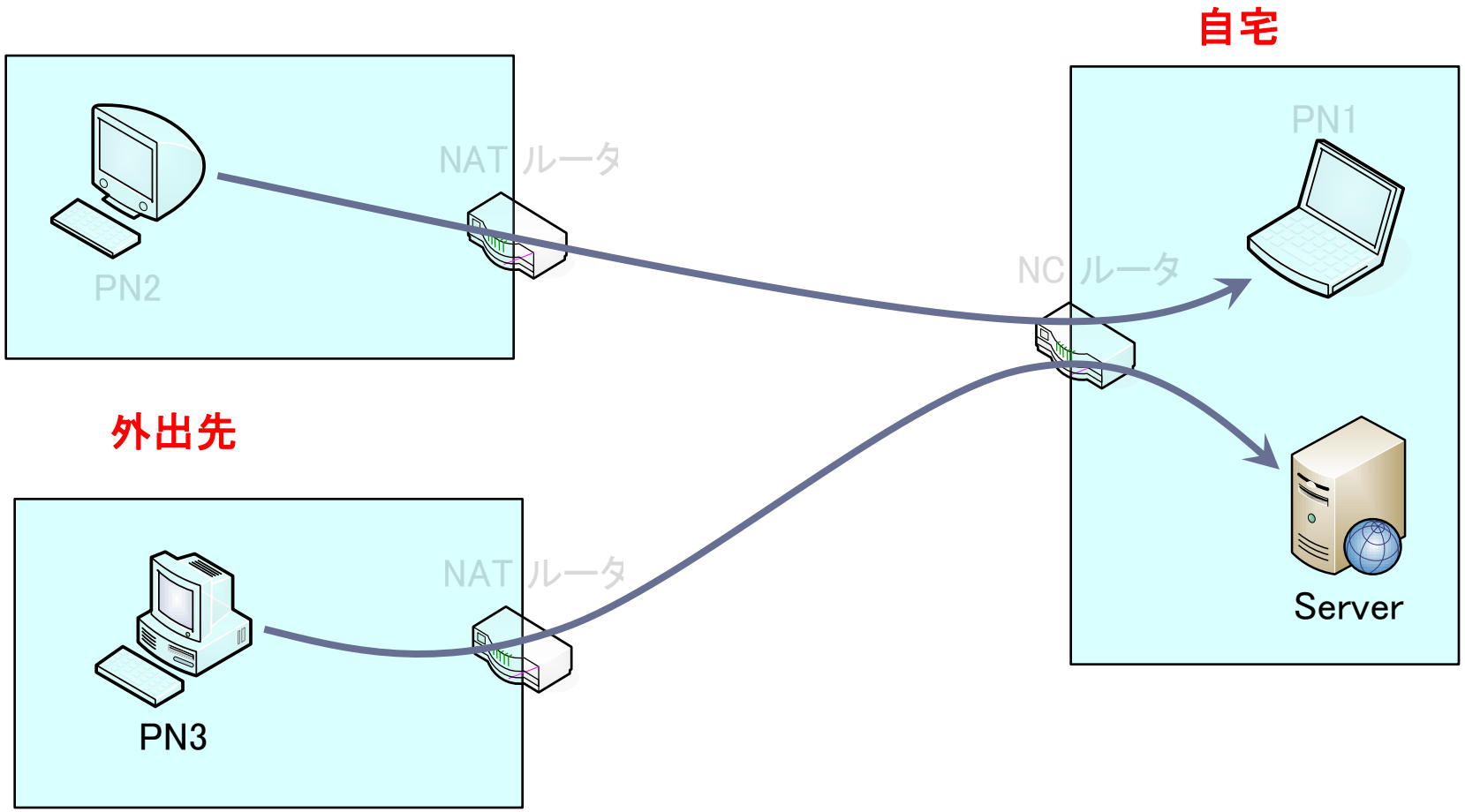
PHL + RC	
Private IP	Source IP
PA1	GA3

NAT table

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

利用場面

- ユーザはNATを意識せず，外出先の端末を利用可能



むすび

- 提案技術
  - 改良したNCルータとNTSサーバにより、端末に手を加えることなくNAT越え問題を解決する方法
  - NC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テーブルを作成する
- 今後の展開
  - 提案方法の実現

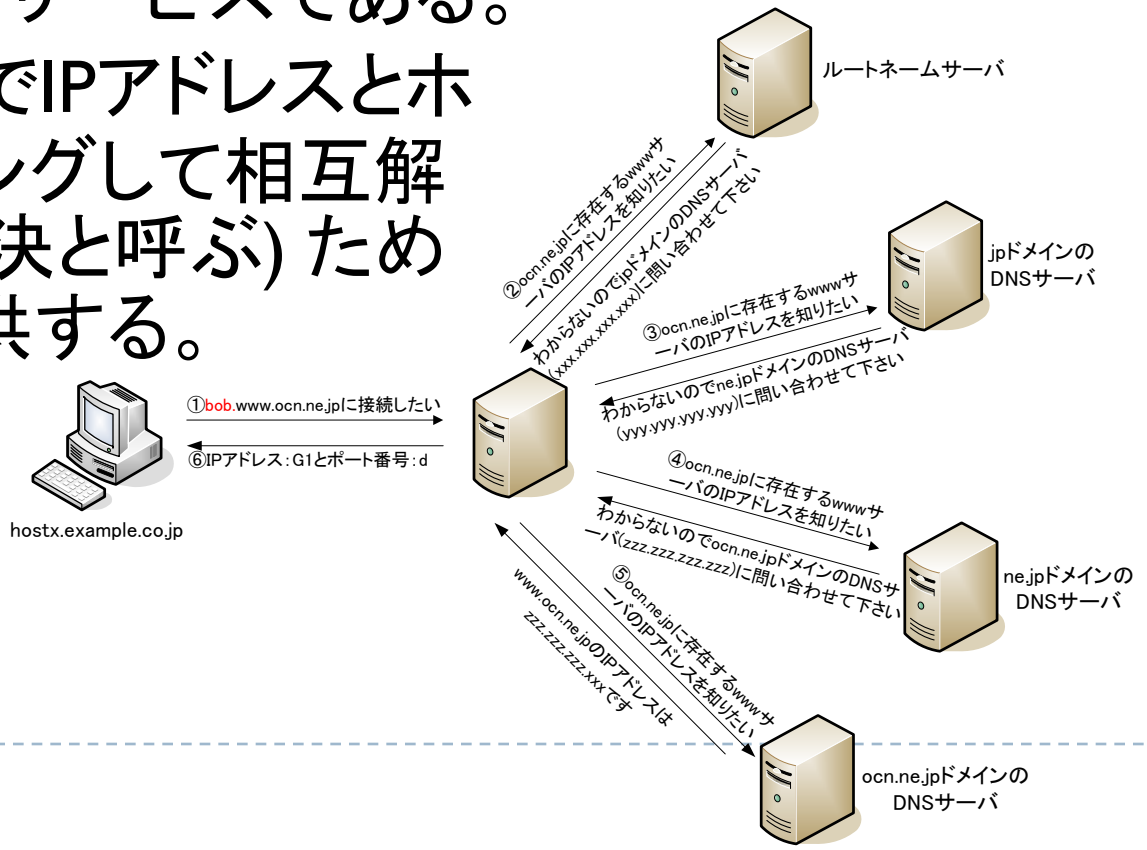
補足説明

NAT越え既存技術例

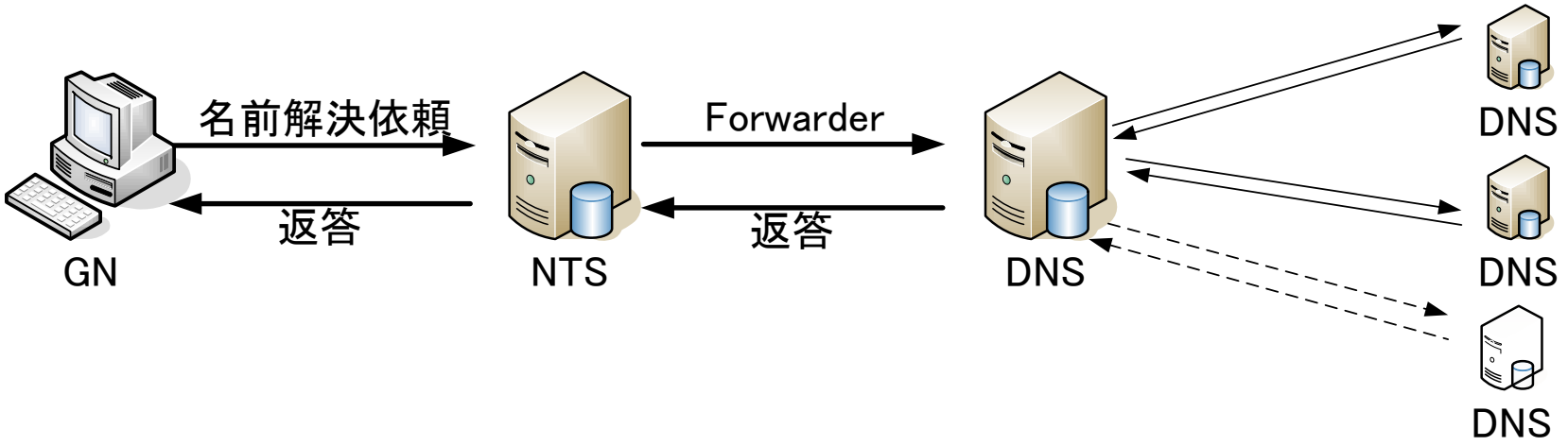
技術名	実装箇所	概略
STUN (Simple Traversal of UDP Through NATs	GN PN STUNサーバ	UDP Hole Punchingを使ってNATを通過する方法 。 UDP Hole Punching：UDPを用いて予め内部より外部に通信を行うことでNATに通り道を用意しておき、そこを通して外部より内部に通信を行う方式。
IPv4+4	GN PN NATルータ	IPv4ヘッダを拡張することで更に32bit追加する。 グローバルアドレスとプライベートアドレスを両方保持し、NAT通過時にこのヘッダを見て二つのアドレスを入れ替えることにより通信が可能となる。
NATS (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、1つの（グローバル）IPアドレスに対して16bitsのサブ・アドレスを割り当てることで、NAT／NAPT内のホストを特定する手段を提供
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。

RFC1034,1035
DNS（Domain Name system）

- ポート番号：53/udp and 53/tcp
- DNSは分散型データベースによるディレクトリサービスである。
- ネットワーク上でIPアドレスとホスト名をマッピングして相互解決する(名前解決と呼ぶ) ための仕組みを提供する。



NTSとDNSの関係



- GNは予めプライマリDNSに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
- 異なるアドレス空間のPNが増大するとNTSの対応が悪くなる可能性がある。
- 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

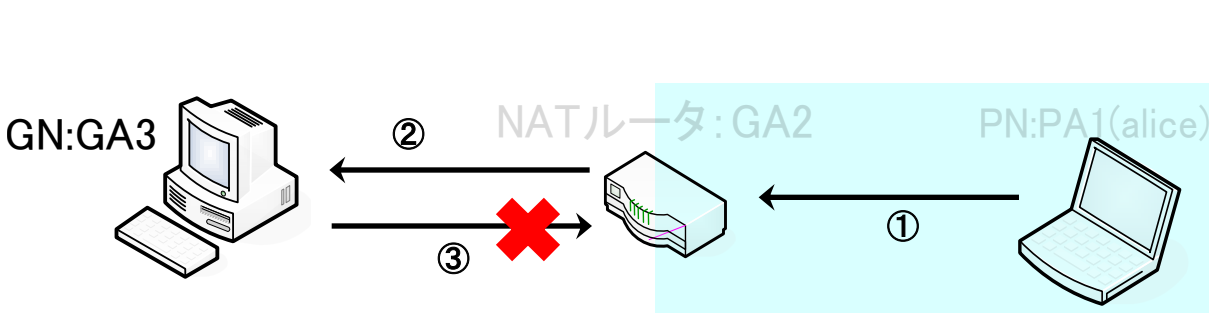
対応できないケース

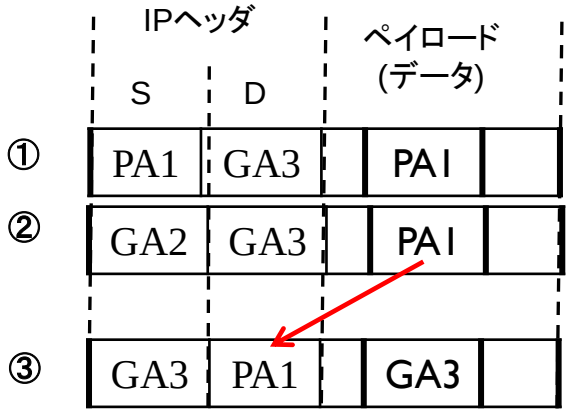
- IPアドレスやポートを制御するアプリケーション
  - FTP
  - SIP
- パケットのデータ部にIPアドレス・ポートの情報が記載されており，NAT通過時に変換されない

ALG(Application Layer Gateway)
をNATルータに実装して解決

ALG(Application Layer Gateway)

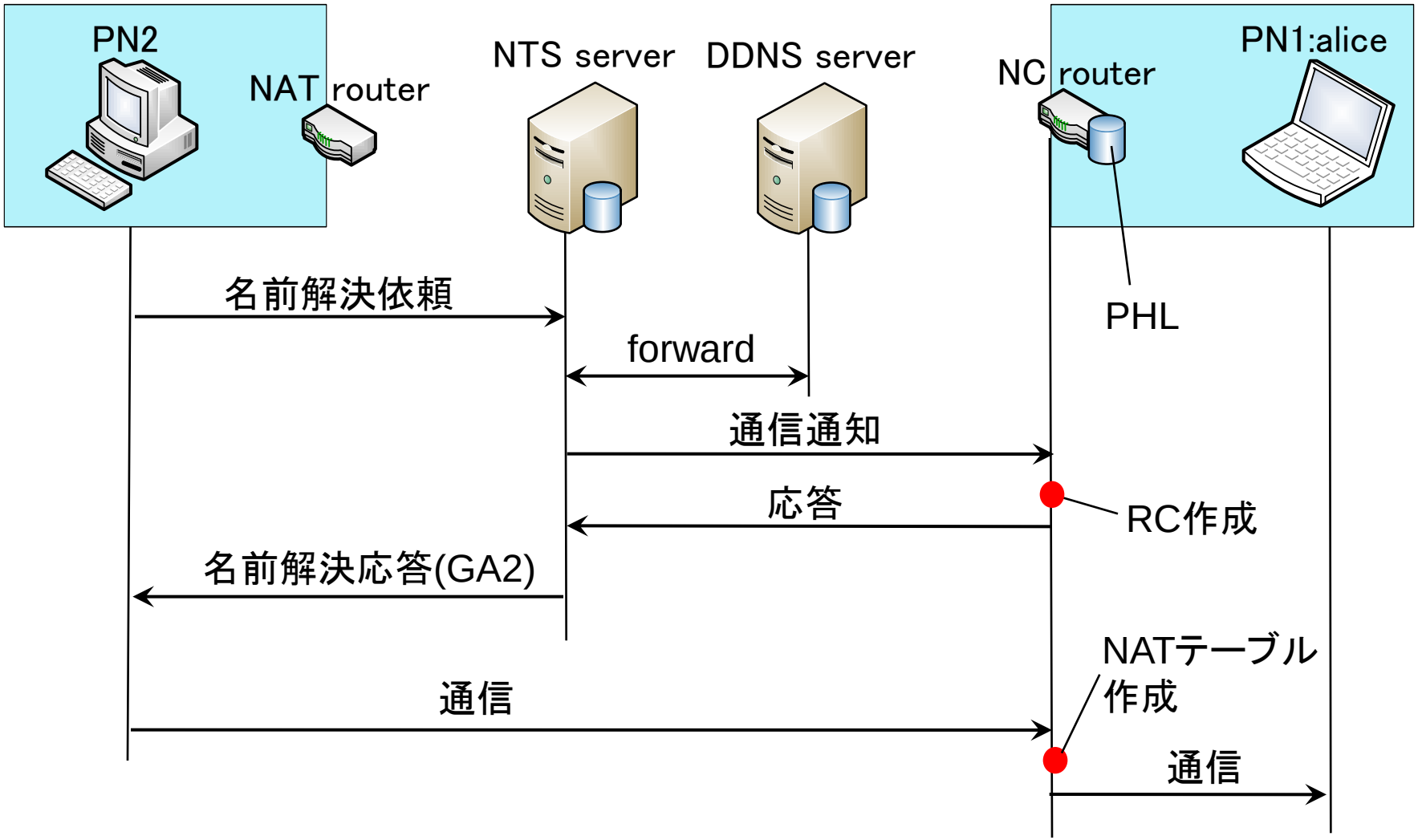
- NATによる異種ネットワーク間でのセッション確立





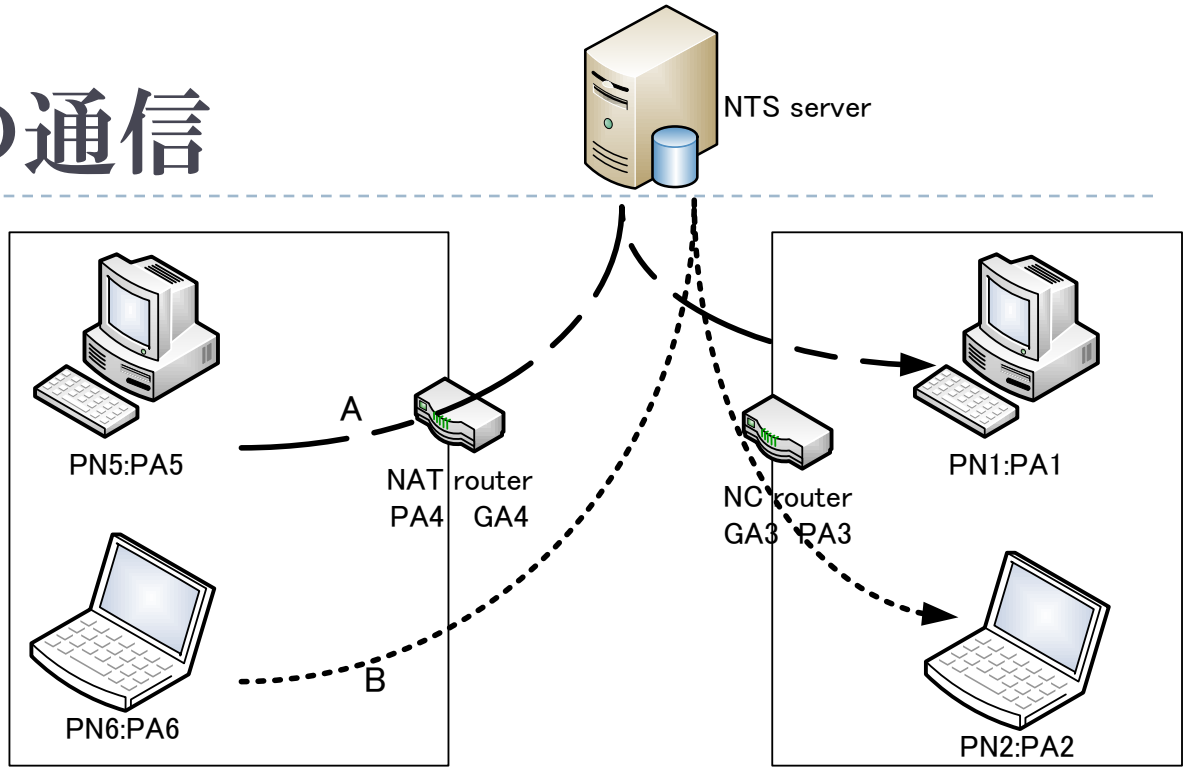
- NATではIPおよびTCP/UDPヘッダに記述されるアドレスを書き換えるが，ペイロード部には関知しない
- そこで，ALGによりアプリケーション内のアドレスも書き換える

GNがNAT配下にいる場合



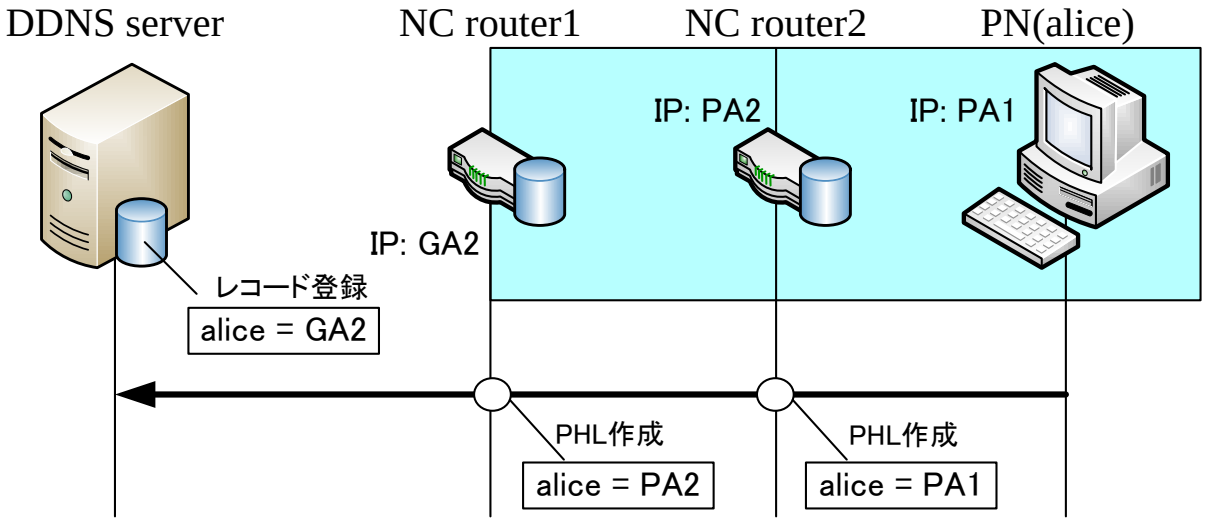
同NATからの通信

通信A：PN5→PN1
通信B：PN6→PN2



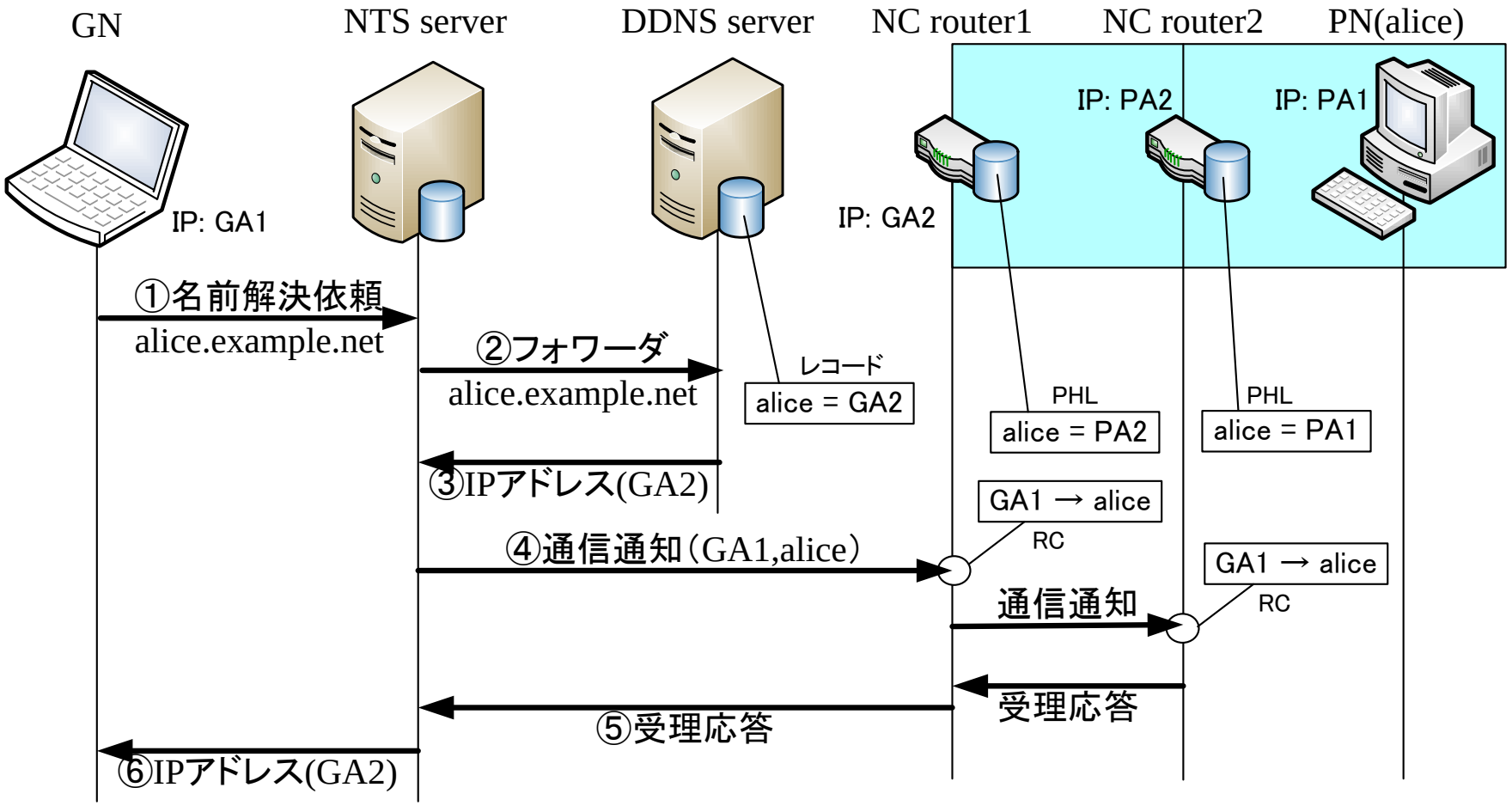
- PN5からPN1，PN6からPN2に通信があった場合
  - NCルータのキャッシュにはGA4からPA1･2という情報が書かれるため，AとBの通信が同時にあった場合，NCルータが混同してしまう可能性がある
  - NCルータが同じアドレスから通信通知を受け取った場合，後に来た方を遅らせて応答することで解決

二重NATの場合(名前登録)



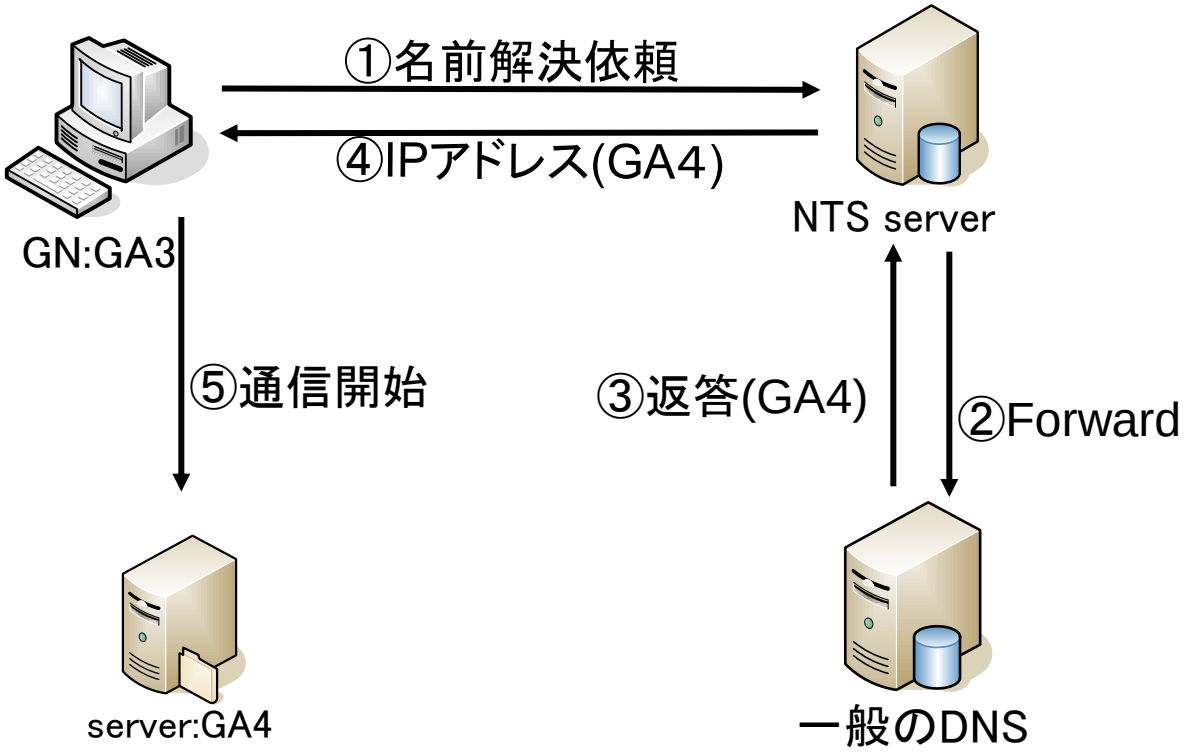
- NC routerはそれぞれ名前登録パケットが内側から通過した時にPHLを作成する.
- NATは内側からのパケットを自分の外側で使えるIPアドレスに書き換えて送信するので, NC router1と2ではそれぞれのネットワークに対応したアドレスのPHLが作成される.

二重NATの場合(名前解決)

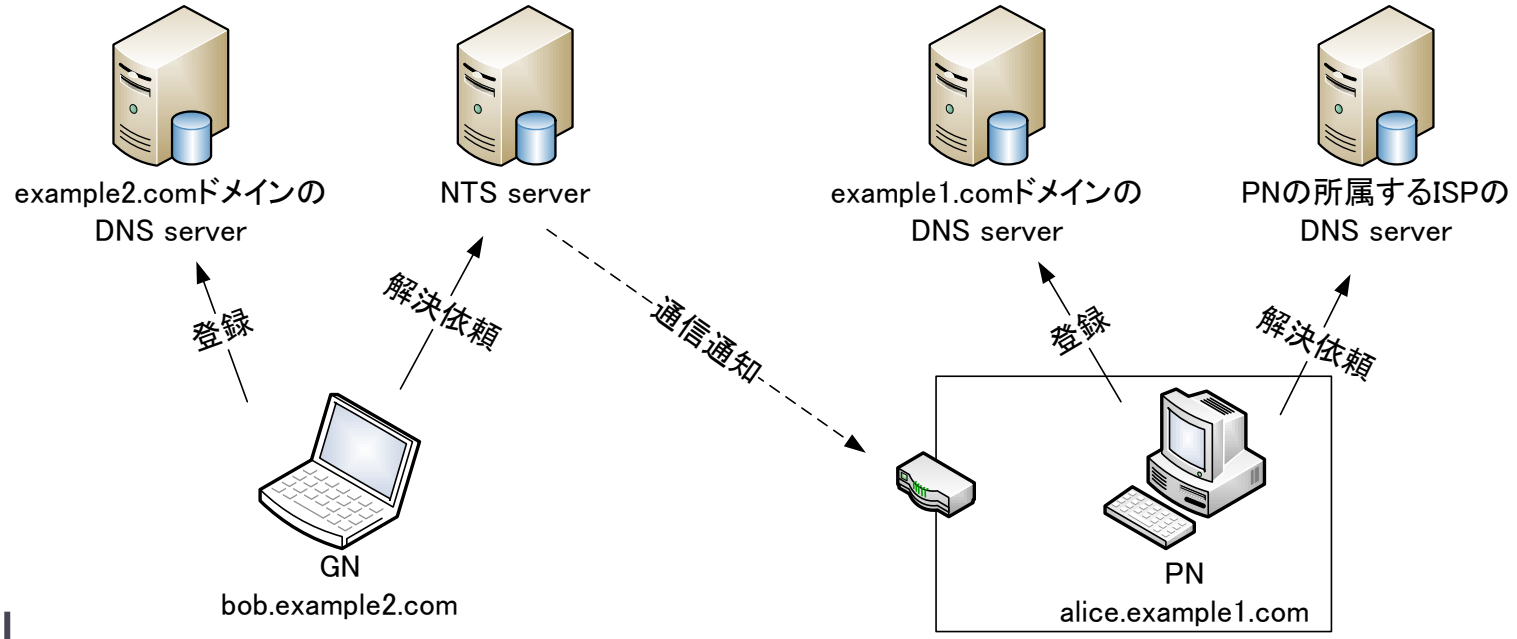


提案方式(対GN)

- 本方式を採用した端末GNがグローバルアドレス空間にあるサーバー等にアクセスしたい場合

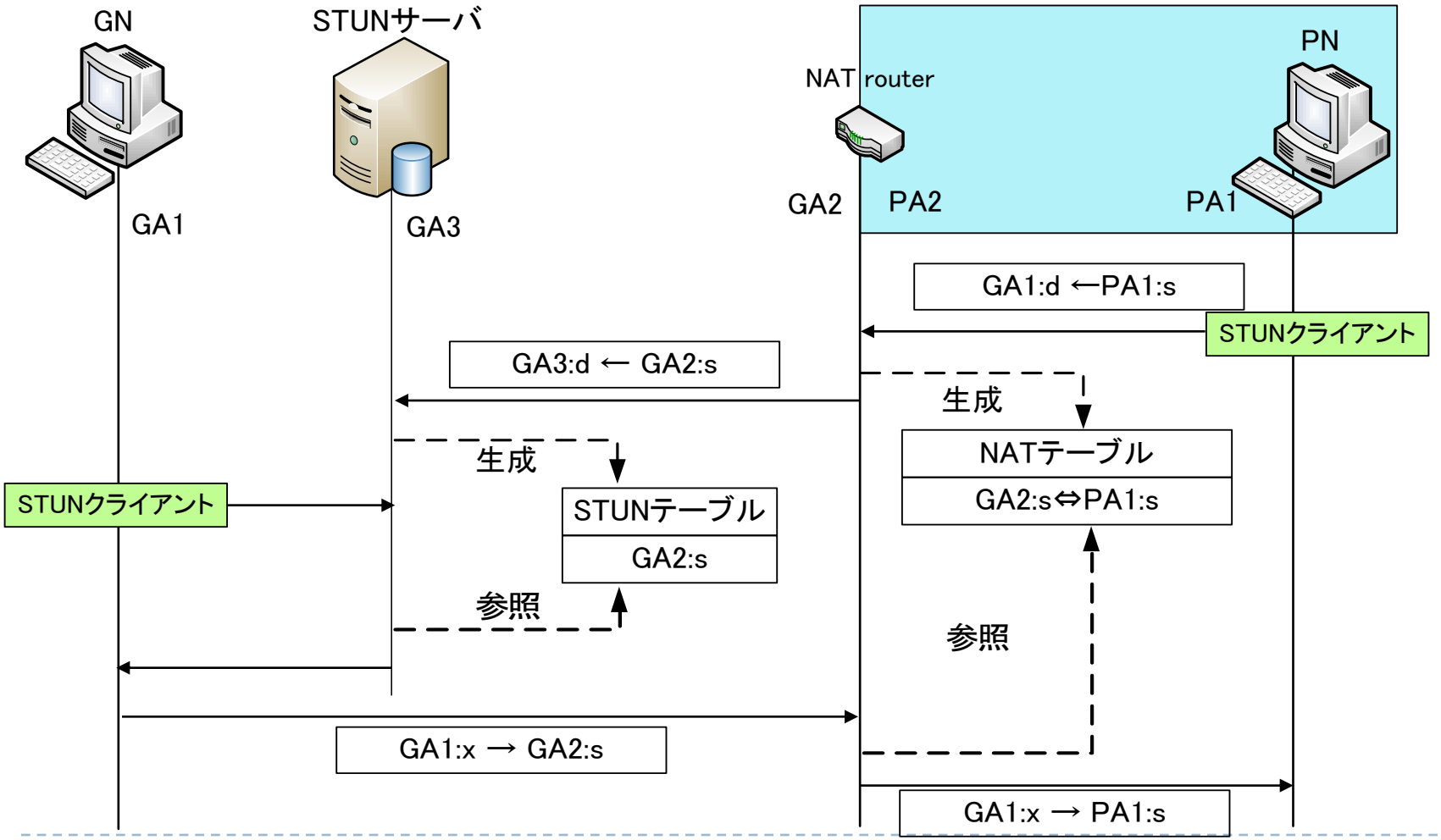


DNS対応関係



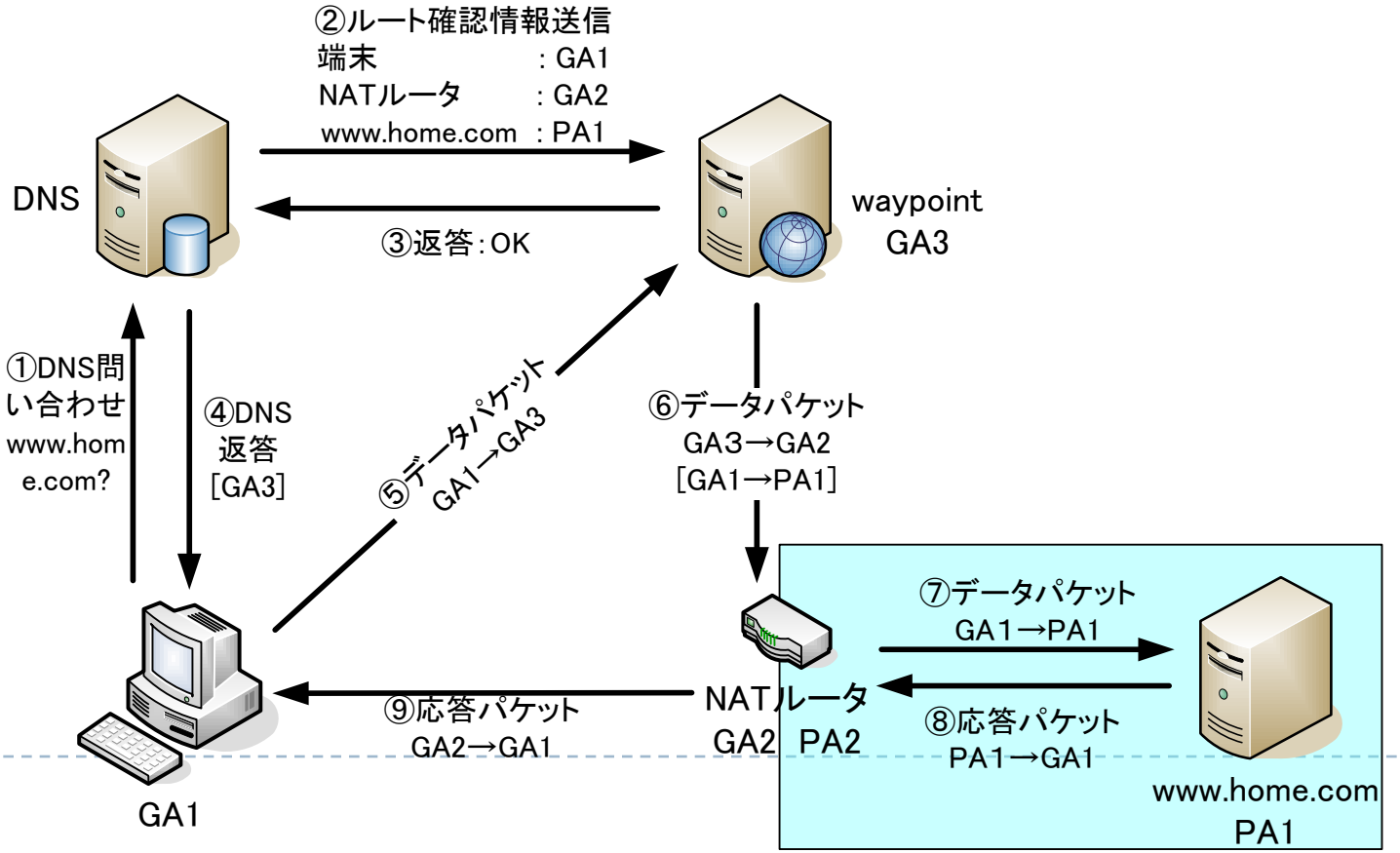
- GN
  - 登録先：自ドメインを管理するDNSサーバ
  - 名前解決依頼先：NTSサーバ
- PN
  - 登録先：自ドメインを管理するDNSサーバ
  - 名前解決依頼先：自分の所属するISPのDNSサーバ

STUN
(Simple Traversal of UDP Through NATs)

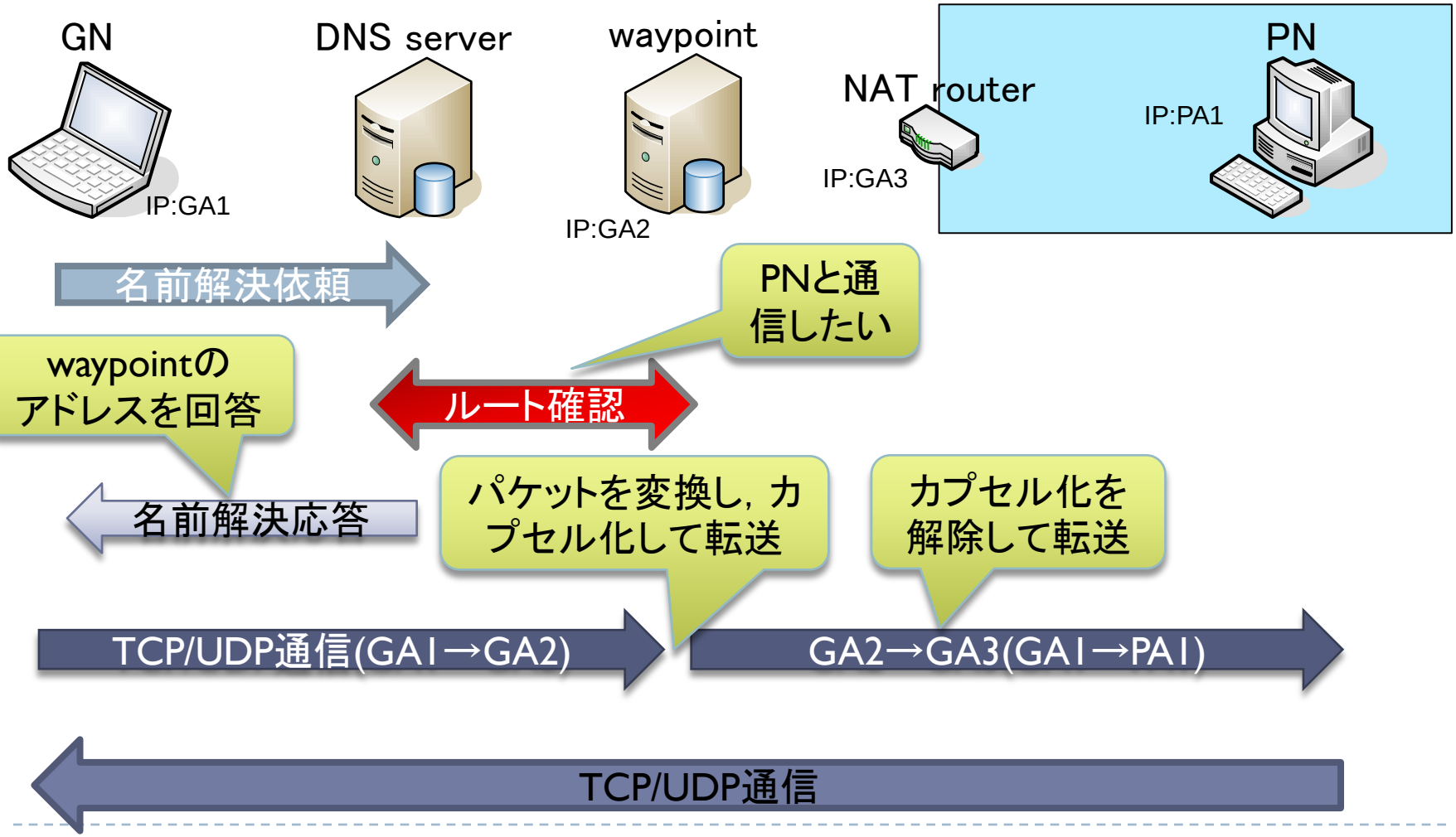


NAT越え既存技術例：AVES

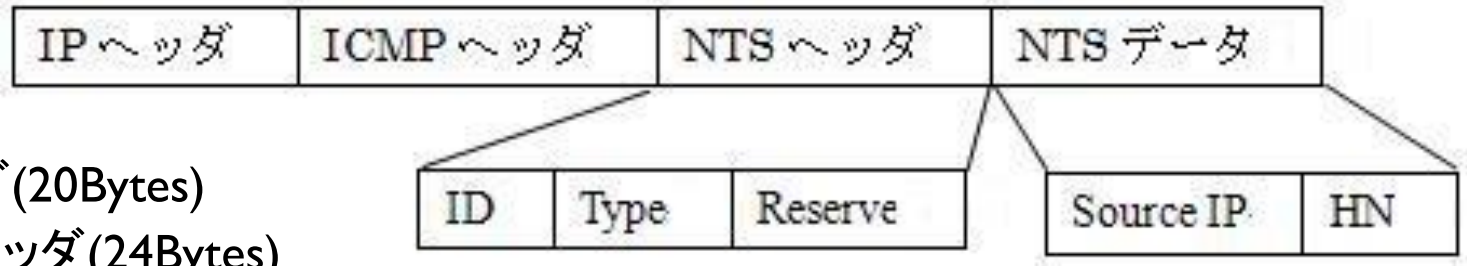
- DNS,NATルータ,waypointサーバを改良・設置
- 外側の端末は内側の端末への通信に全てwaypointを中継する
  →三角経路



AVES
(Address Virtualization Enabling Service)



NTS-NATルータ間パケット



- IPヘッダ(20Bytes)
- ICMPヘッダ(24Bytes)
- NTSヘッダ(4Bytes)
  - Type　　：パケットのタイプが通知③か応答④かを判断(8bits)
  - ID　：DNSが名前解決の際に使用するトランザクションIDと対応させ，NTSが受信した際に，名前解決①に対応する応答④だとわかるようにする(16bits)
- Reserve　　：予備 (8bits)
- NTSデータ(68Bytes)
  - Source IP　　：要求元IPアドレス(32bits)
  - HN　：Host Name (64Bytes：これ以上は有り得ない為固定)

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、NATルータへのパケットを生成・送信
3. NATルータからの返事に従いGNへ名前解決を送信

＊bindとは名前解決を行うDNSアプリケーション

NCルータの処理

- 内側からパケットが通過した時
  1. DNS登録パケットなら退避し，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へ一時キャッシュする
  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

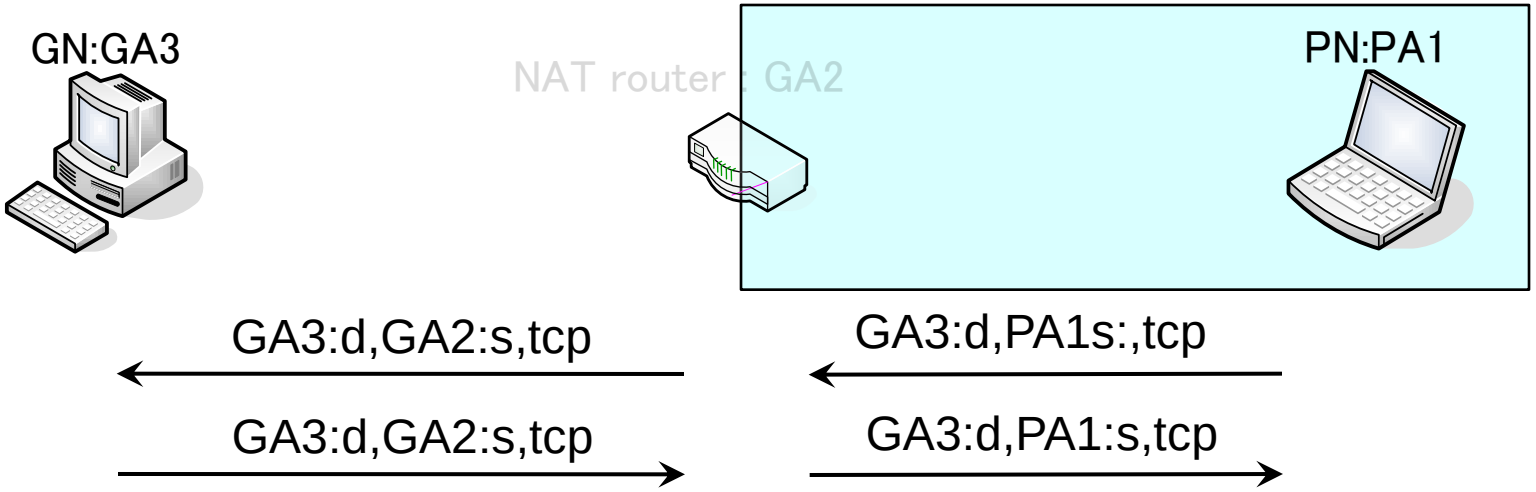
- NAPT(Network Address Port Translator)
  - 広義のNAT
  - NAT tableでIPアドレスとポート番号を対応させることで，一つのIPアドレスを複数の端末で共有することができる

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
  - Restricted Cone NAT
  - Port Restricted Cone NAT
  - Symmetric NAT

Full Cone NAT

- NATの外部portと内部端末をマッピング

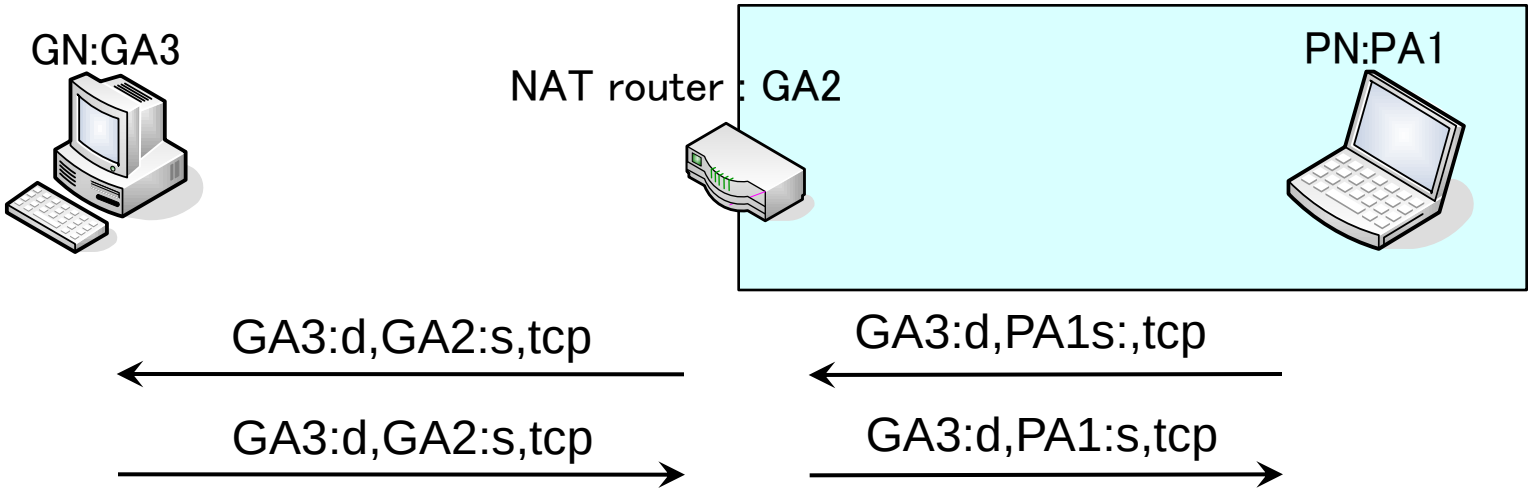


NAT table

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

Restricted Cone NAT

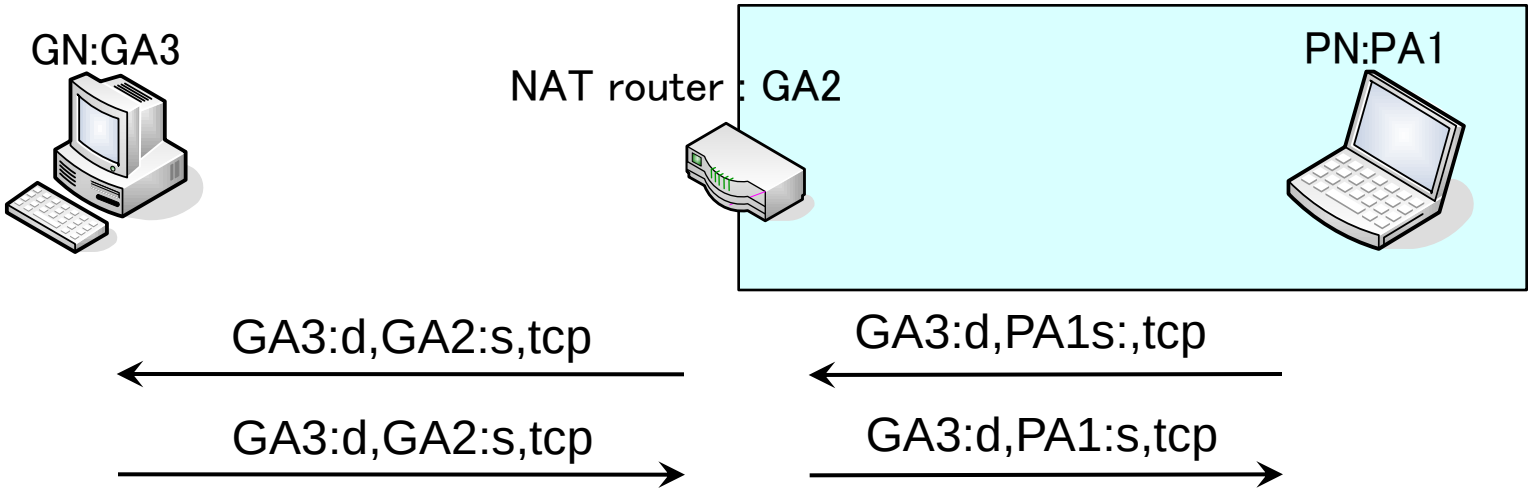
- NATの外部portと内部端末のマッピングだけでなく，リモート端末のIPアドレスも対応付ける



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

Port Restricted Cone NAT

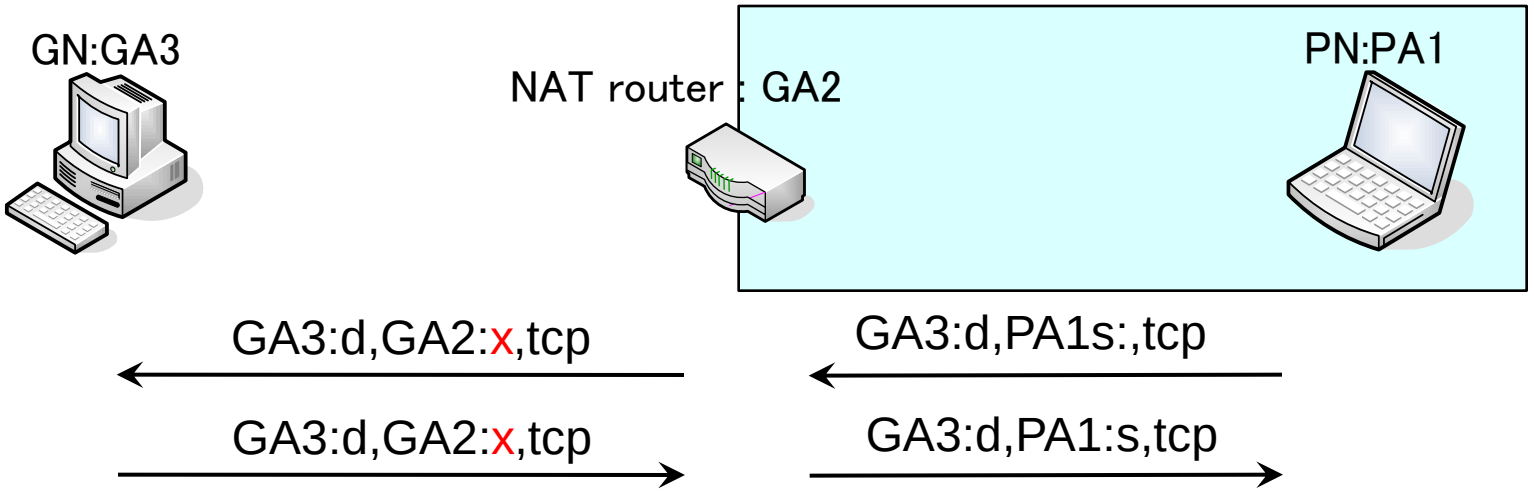
- Restricted Cone NATに加え，リモート端末のportも対応づけてマッピングする



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