端末の機能追加が不要な NAT 越え方式の提案

030432106　宮﨑悠
渡邊研究室

1. はじめに

IPv4 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ている．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空間の端末に対して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．しかし，従来の解決手法はユーザ端末に機能を追加する場合が多い．本稿では DNS サーバと NAT ルータが協調することにより，一般のユーザ端末をそのまま使用できる NAT 越え方式を提案する．

2. 既存技術

NAT 越えの既存技術として，STUN[1]，AVES[2]や NAT-f [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 越えを実現しているが，専用のアプリケーションや UDP 通信でしか利用できないという制約がある．

AVES では 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という課題があった．

3. 提案方式

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．通信を行うエンド端末に対して特殊な機能を実装する必要がないという特徴がある．その為，一般ユーザは NAT 問題を意識することなく NAT 越え通信を実現できる．また，特殊な第 3 の装置が不要で P2P 通信を実現することができる．

図 1 に提案方式の動作概要を示す．本手法における専用の DNS サーバを RDNS（Remodeled DNS）と呼ぶ．RDNS には予めプライベートアドレス空間内の端末 PN の名前と NAT ルータのグローバル IP アドレスの関係が登録されている．グローバルアドレス空間の端末 GN はプライマリ DNS として RDNS を設定する．

GN から PN（bob）へ通信を開始する場合の動作手順を以下に示す．

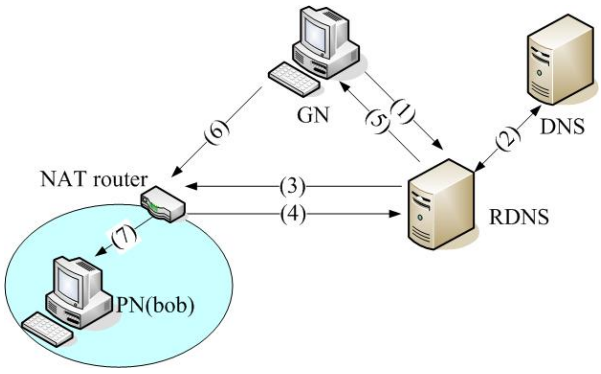


図 1　提案方式の動作概要

(1)GN は RDNS に bob の名前解決を依頼
依頼を受けた RDNS はリソースレコードから bob を検索
→存在しないなら(2)
→存在するなら(3)
(2)RDNS は上位 DNS に名前解決を依頼
(3)RDNS は GN から bob への接続依頼があることを NAT ルータに通知
(4)(3)に対する応答
(5)RDNS は GN に NAT ルータのアドレスを応答
(6)GN は取得したアドレスに対して通信を開始
(7)NAT ルータは GN からのパケットを(3)の情報に基づき強制的に bob に転送

bob からの応答パケットは，NAT テーブルとは別に独自のテーブルを作成し GN へ送信される．通常の通信は従来の NAT と同様，NAT によりアドレス変換され通信を行う．

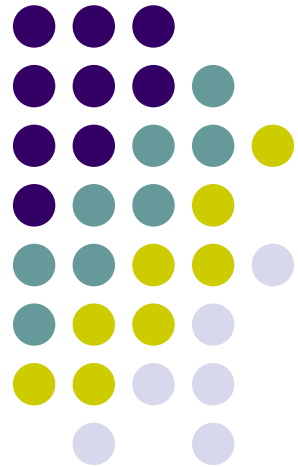
4. むすび

端末の機能追加が不要な NAT 越え方式を提案した．今後は RDNS と NAT ルータを実装し，動作検証を行う．

参考文献

[1] J. Rosenberg, J. et al: STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs), RFC3489, Mar.2003
[2] T.S.Eugene Ng, I.Stoica, H.Zhang:A Waypoint Service Approach to Connect Heterogeneous Internet Address Spaces", USENIX 2001 (Jun.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，DICOMO2006 シンポジウム論文集(Ⅰ)，Vol.2006，No.6，pp.453-456，Jul.2006.

端末の機能追加が不要なNAT越え方式の提案



渡邊研究室
030432106
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が使用される

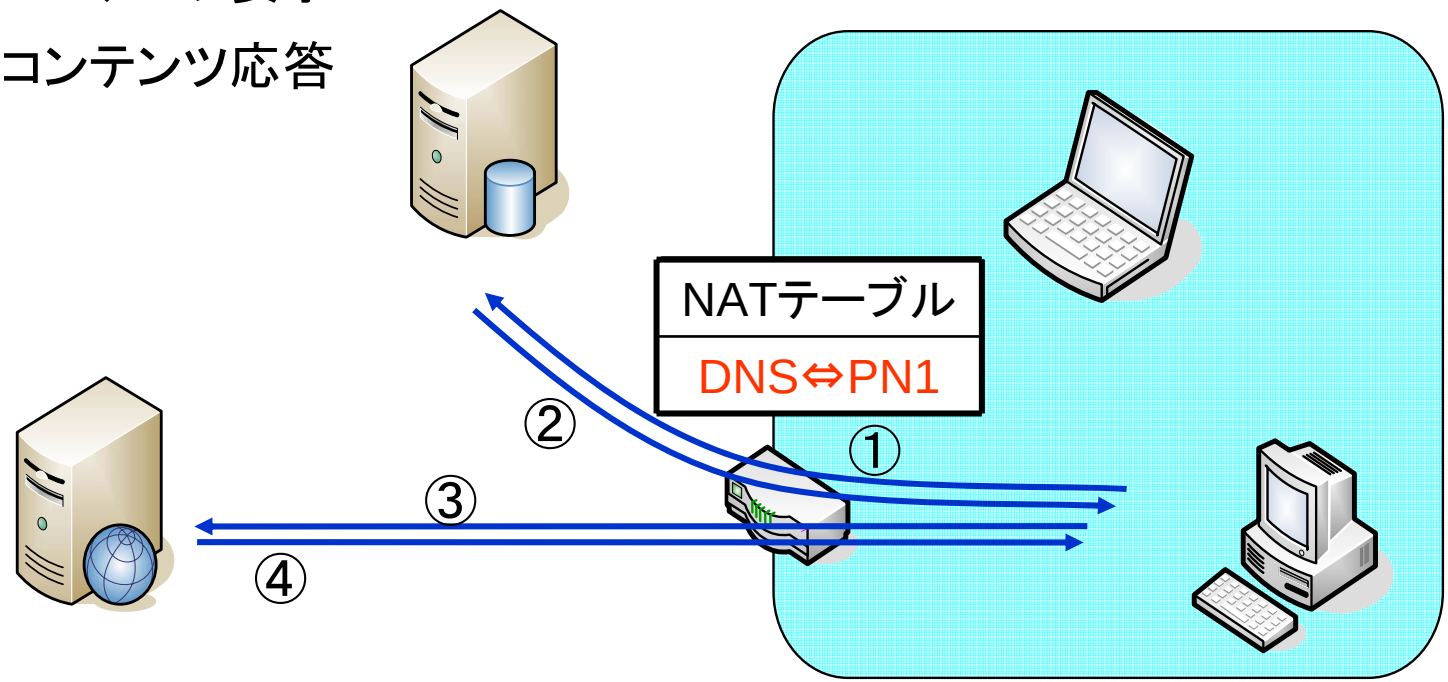
一般のネットワーク

①WEB serverのアドレス要求

②WEB serverのアドレス応答

③WEB コンテンツ要求

④WEB コンテンツ応答

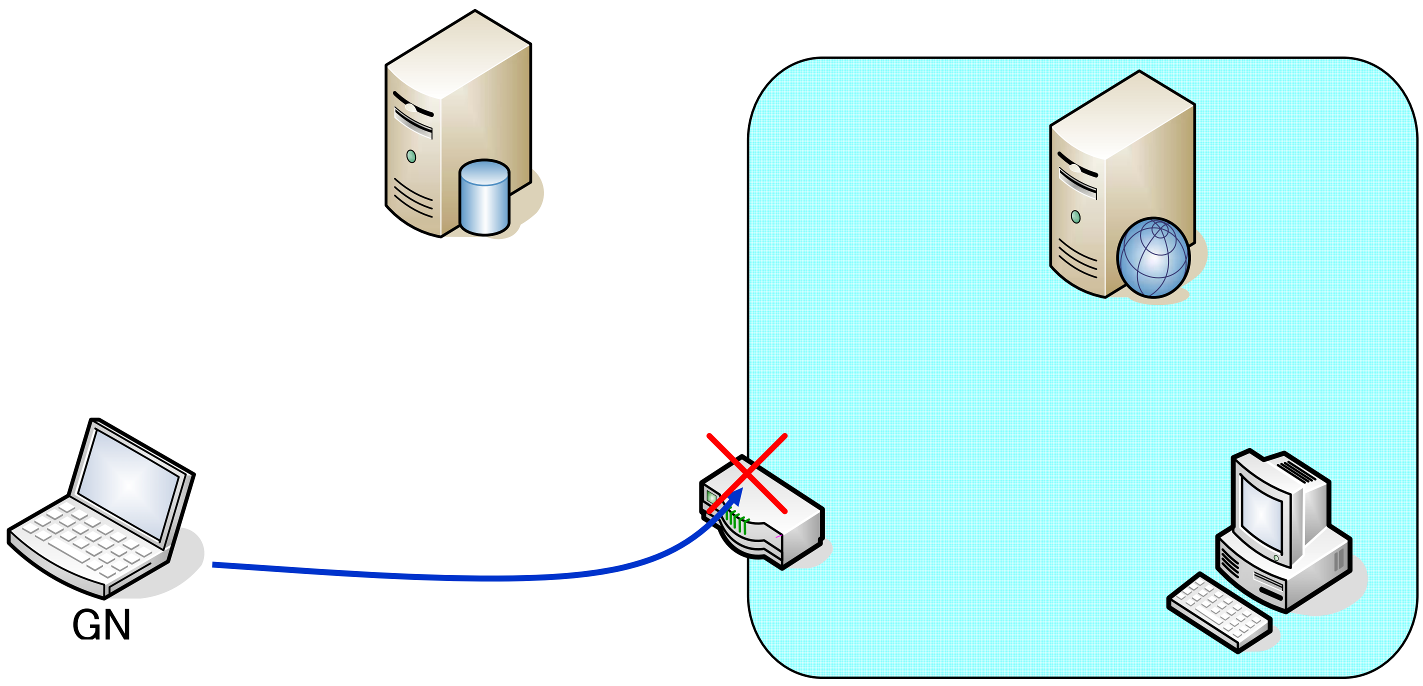


今後考えられるネットワーク

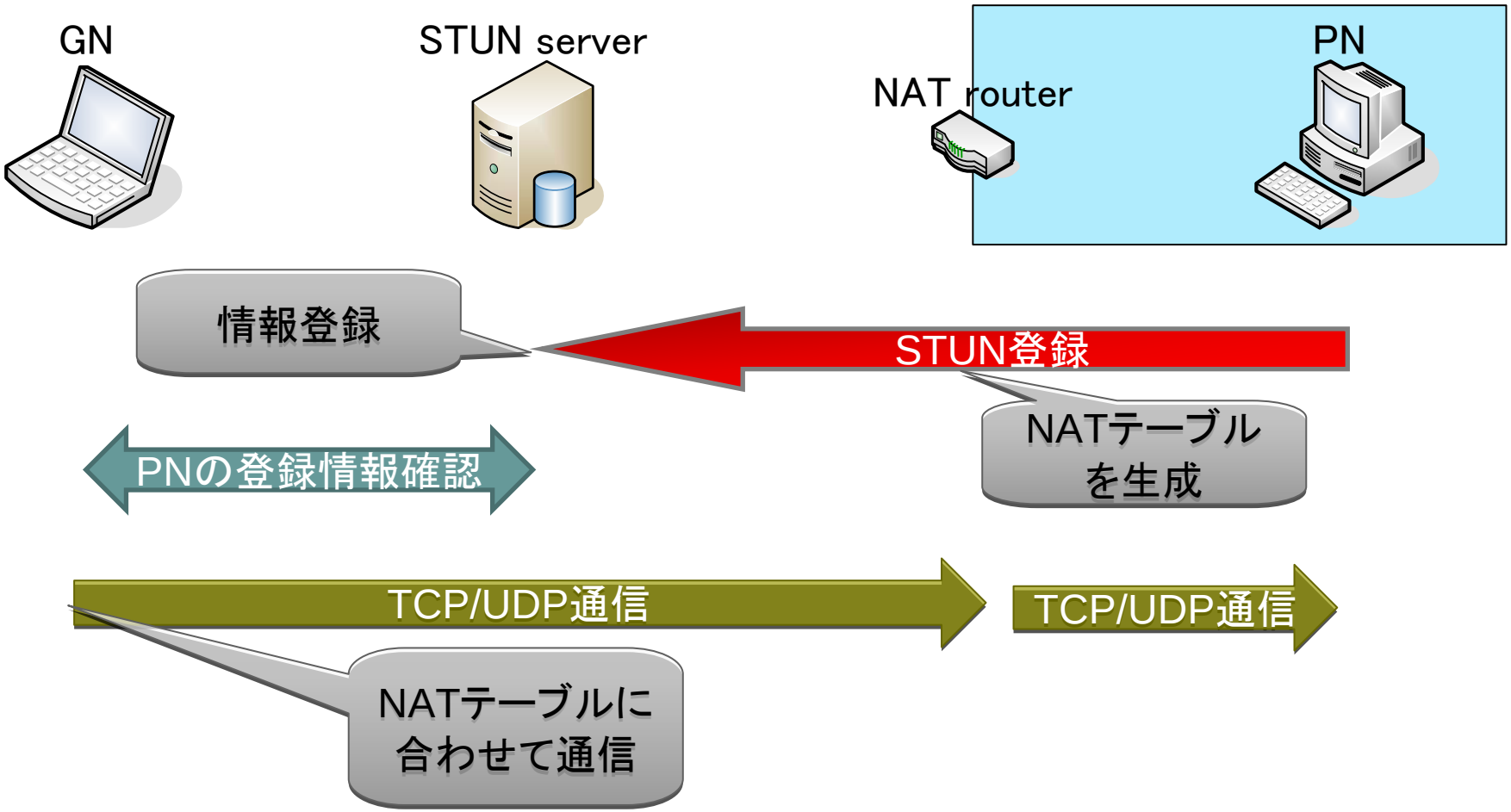
- 家庭・企業ネットワーク内(サーバがある)

NATの原理(GNはプライベートネットワーク内と環境が異なる)
により外側から内側にアクセスすることができない

- プライベートネットワーク内の端末にアクセスしたい　**NAT越え問題**

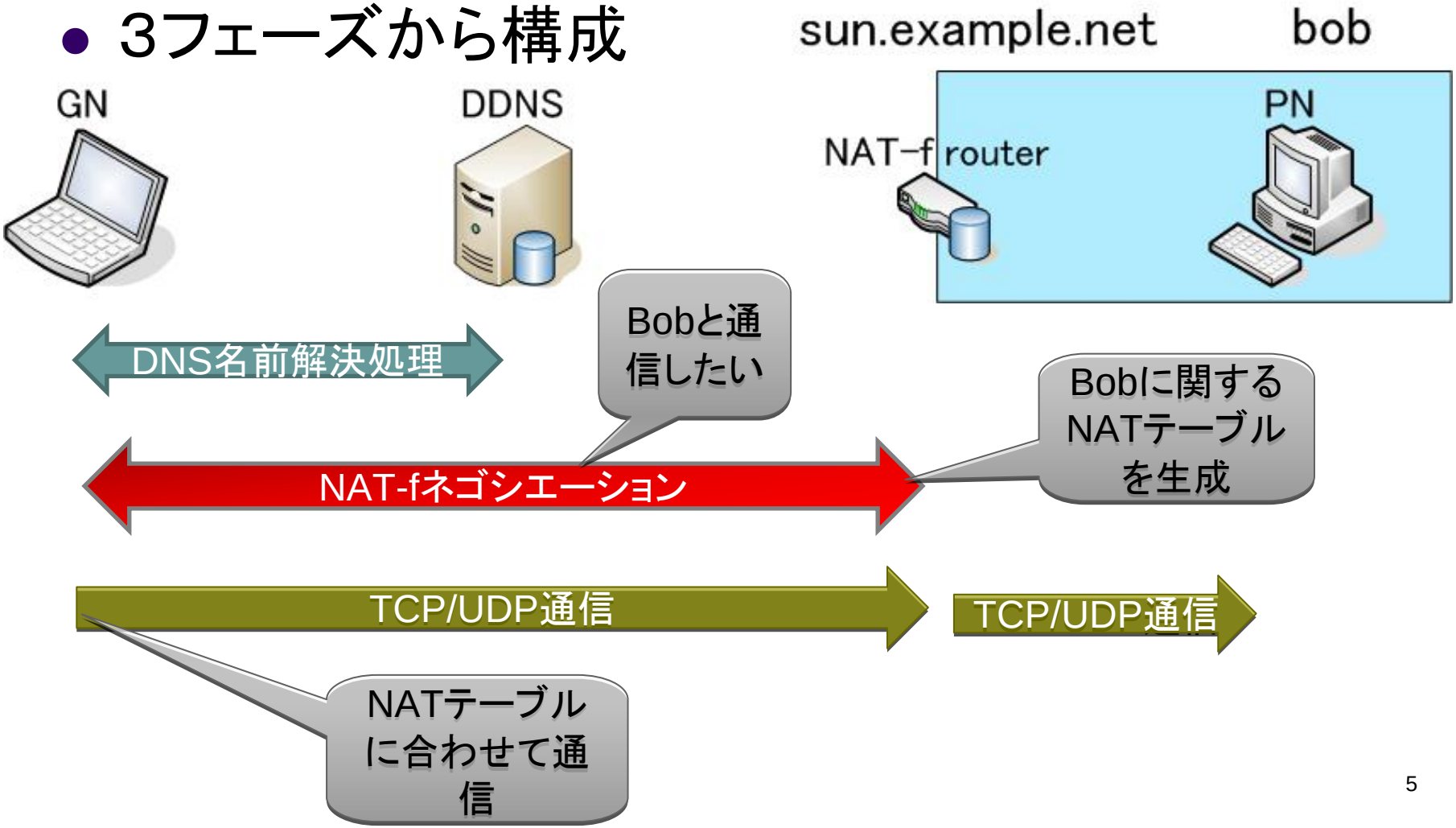


STUN
(Simple Traversal of UDP Through NATs)



NAT-f（NAT-free）protocol

- 3フェーズから構成



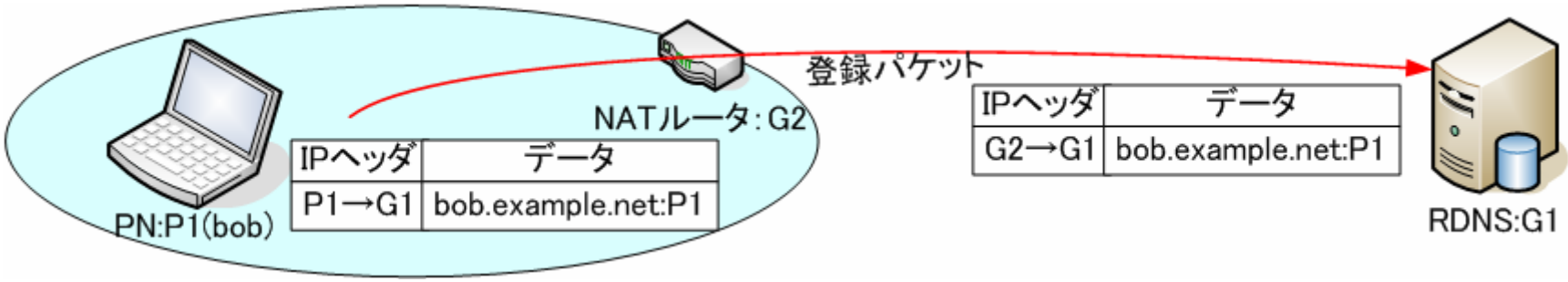
新たなNAT越え方式の提案

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、そのNATルータとDDNSサーバ(RDNS：Remodeled DNS)が連携をとることにより問題を解決する

提案方式

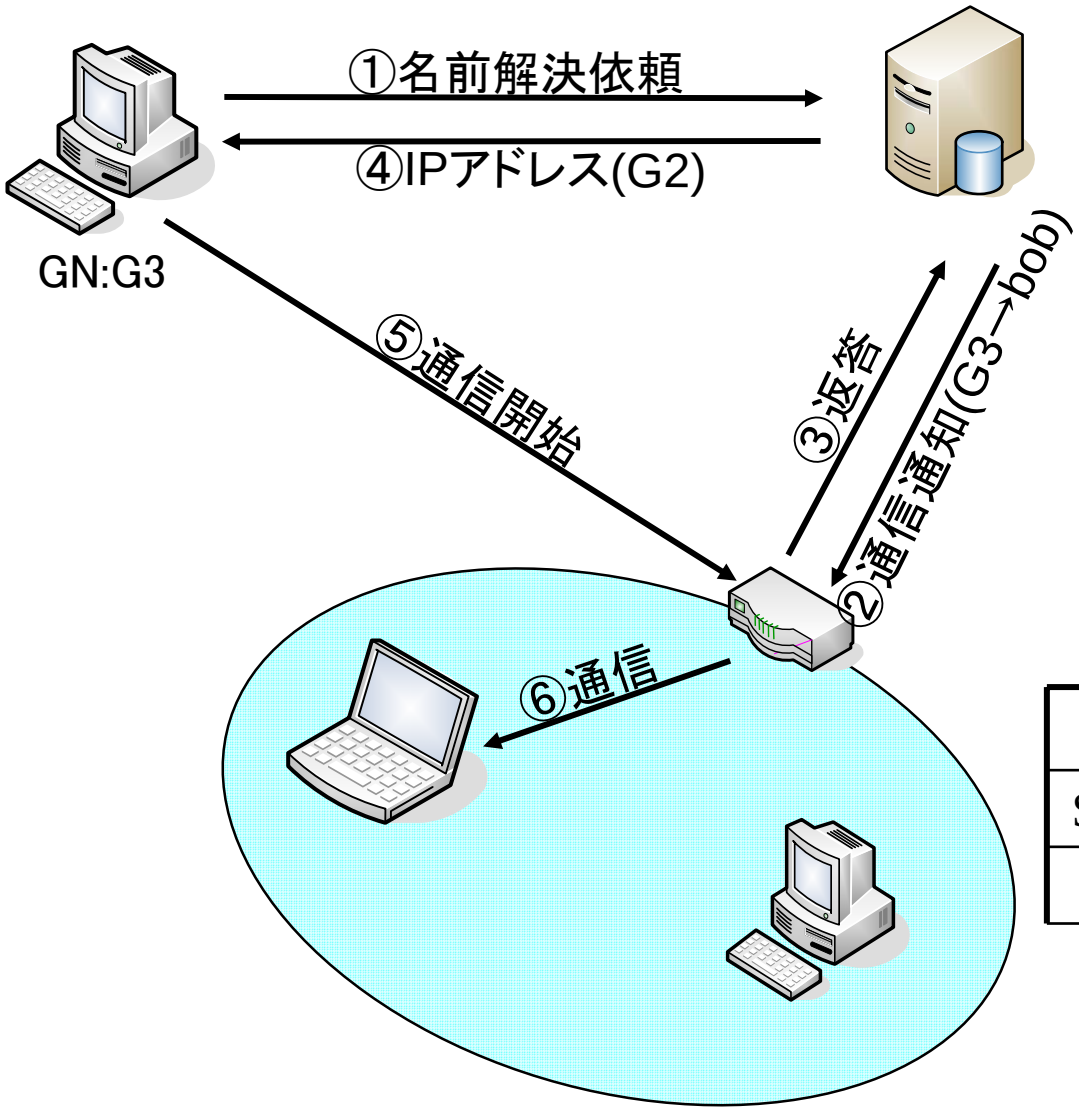
- 予めプライベートアドレス空間内の端末PNの名前とNATルータのアドレスがRDNSへ登録される



- 登録時にNATルータでGuide Table(GT)を作成する

GT		
Source IP	Destination IP	Host Name
	P1	bob

提案方式(動作手順)



DNSレコード	
FQDN	*NAT router*
bob.example.net	G2

②の後GTをチェックして
から③を返信

GT		
S IP	D IP	H N
G3	P1	bob

NATルータは⑤を受信後，
②とGTを元に通信を転送

実装状況

- 仕様決定
  - RDNS-NATルータ間のパケットフォーマット決定
  - RDNSの処理手順決定
  - NATルータの転送処理手順決定
- 一般のDDNSを設定（BIND9）

- RDNSアプリケーション作成中
- NATルータ未着手

むすび

- 提案技術
  - 改良したNATルータとRDNS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を提案
  - 実装段階
- 今後の展開
  - 提案方法の実現

補足説明

NAT：Network Address Translation（RFC1631）

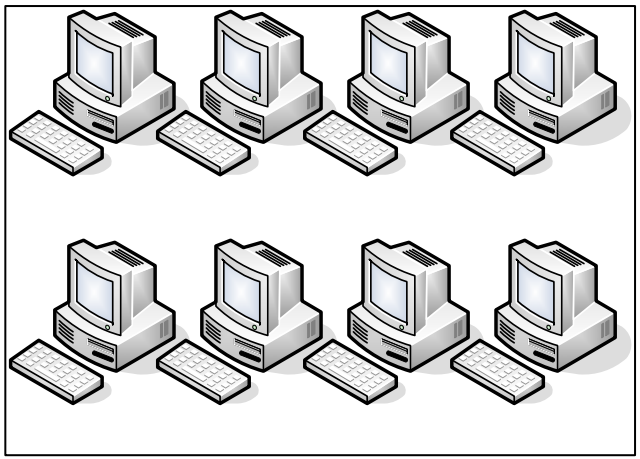
- Private IP Address (RFC1918)

10.0.0.0/8

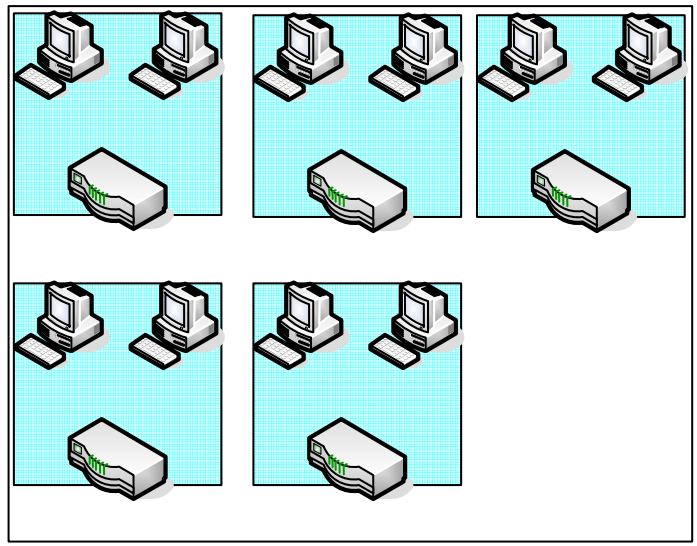
172.16.0.0/12

192.168.0.0/16

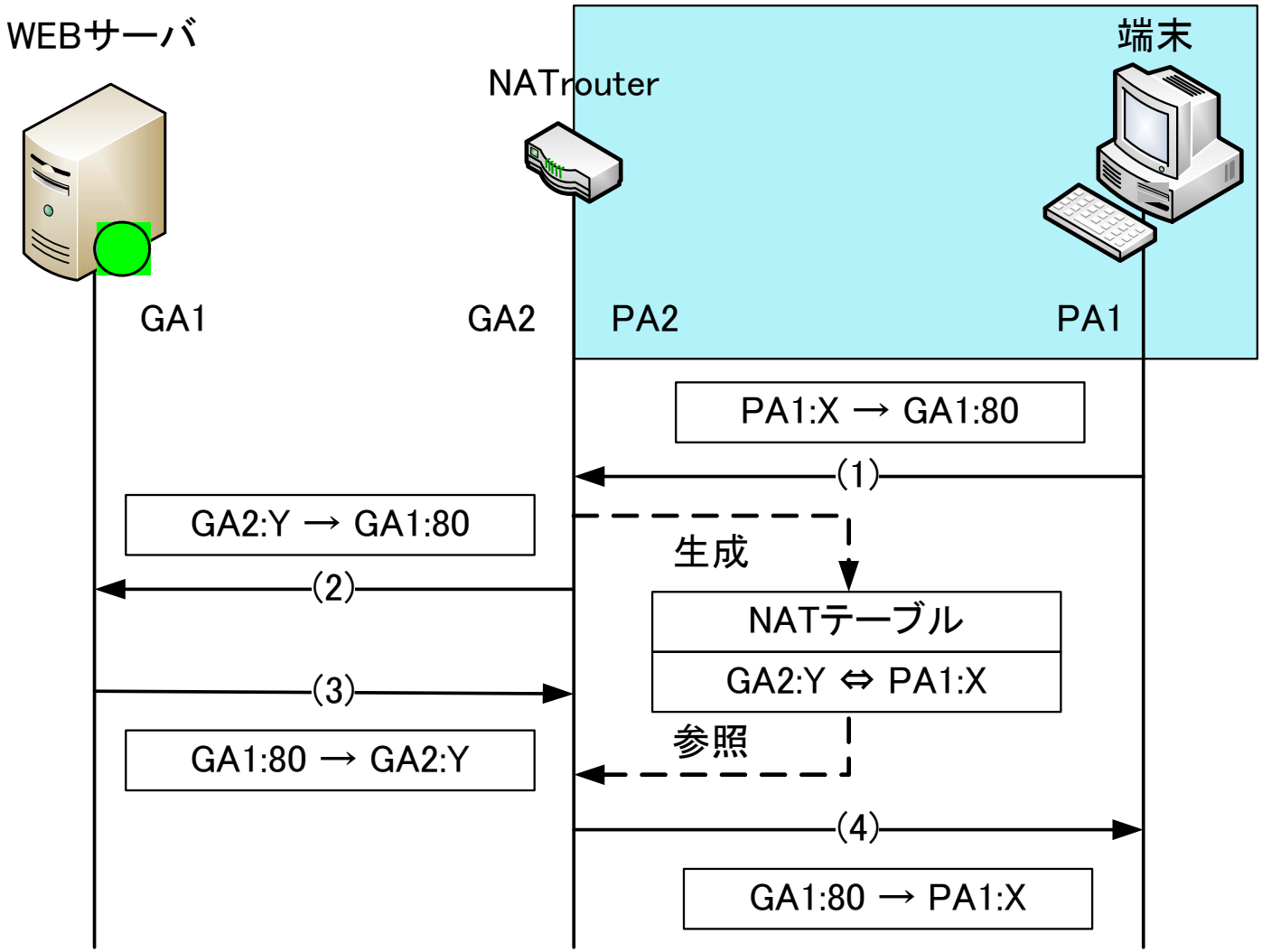
Global IP Address：1-8



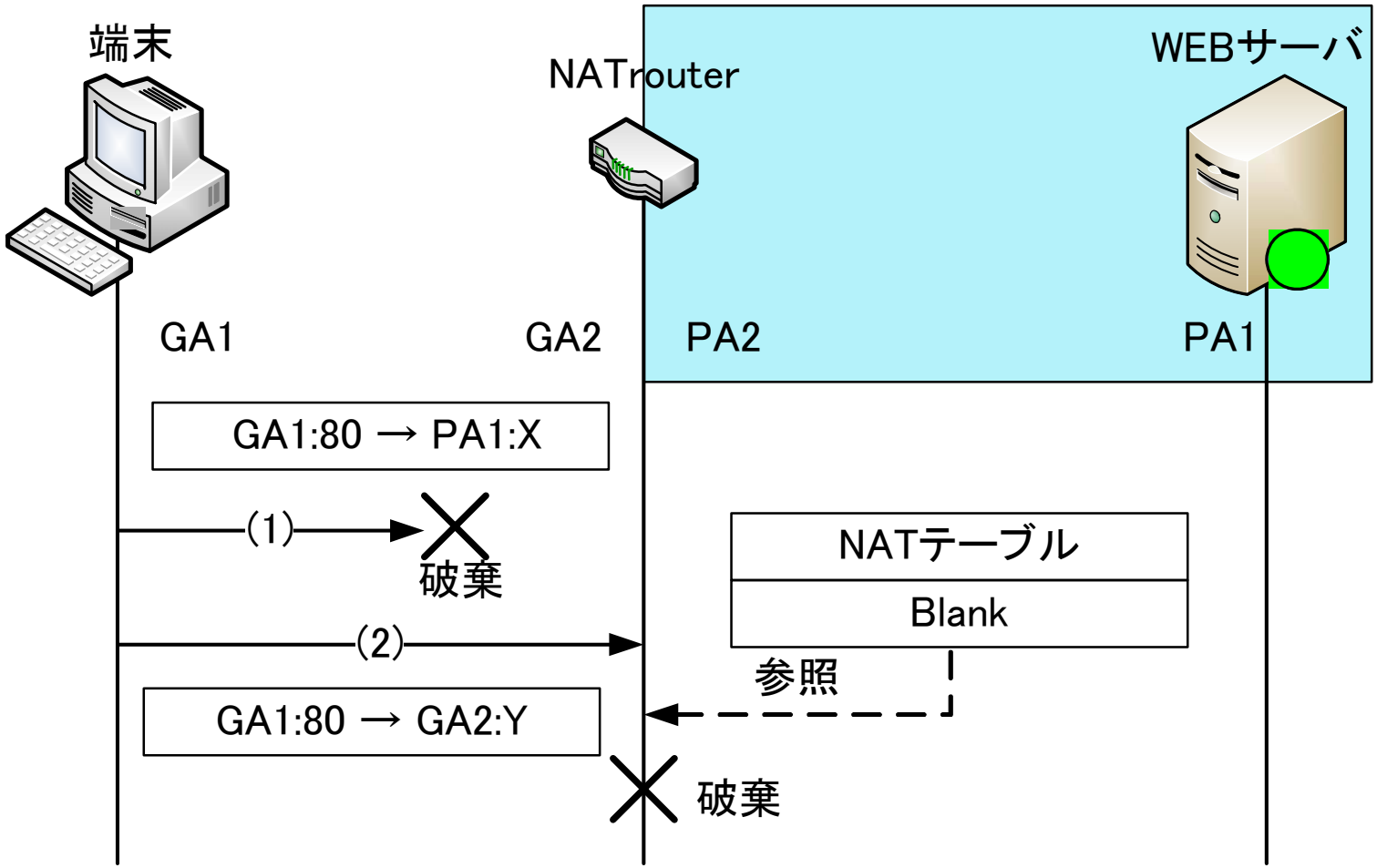
G IP A：1-5 ， P IP A：6-8



NATの動作（内→外）


WEBサーバ
NATrouter
端末
GA1
GA2
PA2
PA1
PA1:X → GA1:80
(1)
GA2:Y → GA1:80
生成
(2)
NATテーブル
GA2:Y ⇔ PA1:X
(3)
参照
GA1:80 → GA2:Y
(4)
GA1:80 → PA1:X

NATの動作（外→内）


端末
NATrouter
WEBサーバ
GA1
GA2
PA2
PA1
GA1:80 → PA1:X
(1)
破棄
NATテーブル
Blank
(2)
参照
GA1:80 → GA2:Y
破棄

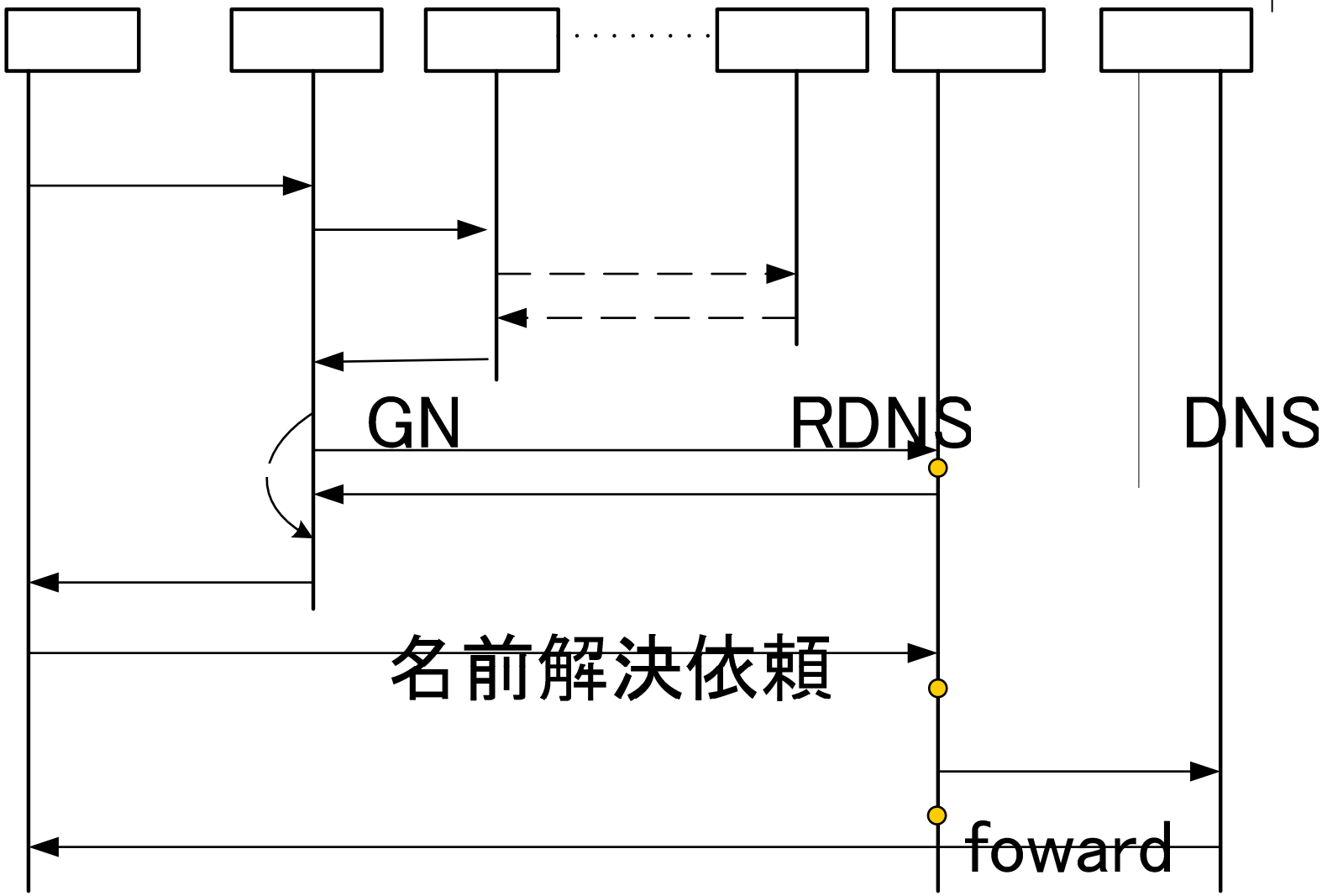
NAT越え既存技術例

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。

提案方式動作

①GNはRDNSにbobの名前解決を依頼する
　RDNSはソースレコードからbobを検索する
　→ない場合は本方式対応ではないと判断して，一般のDNSにフォワーダする
②RDNSはNATルータにG3からbobへ通信要求があったことを通知する
③②に対しての返答
④RDNSはGNにbobのアドレスを応答する
　（実際はNATルータのアドレスG2）
⑤GNは取得したアドレス(G2)に対して通信を開始する
⑥NATルータは得ている情報からNATテーブルを生成し，GNからの通信パケットをbob(P1)に転送する

提案方式時間的流れ



考えられる問題点

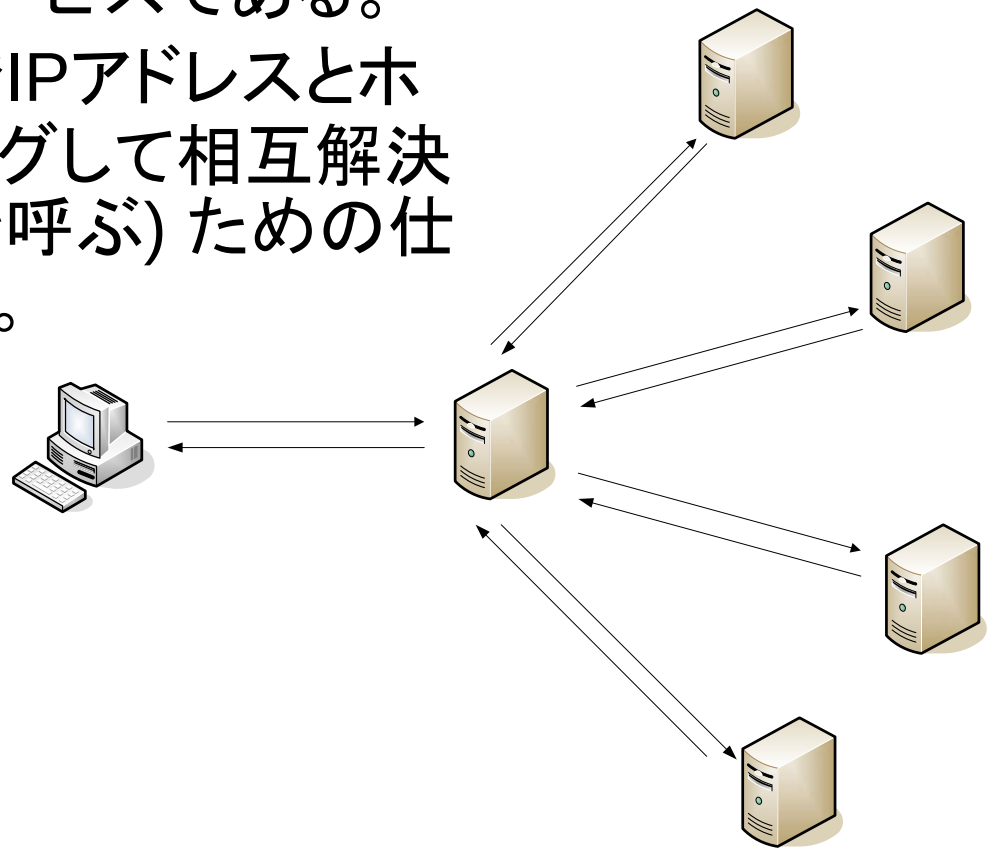
- 通信の乗っ取り

他のGNからIPアドレスを装ってNATルータ宛に通信が開始された時，NATルータは誤ってPNに通信を通してしまう可能性がある

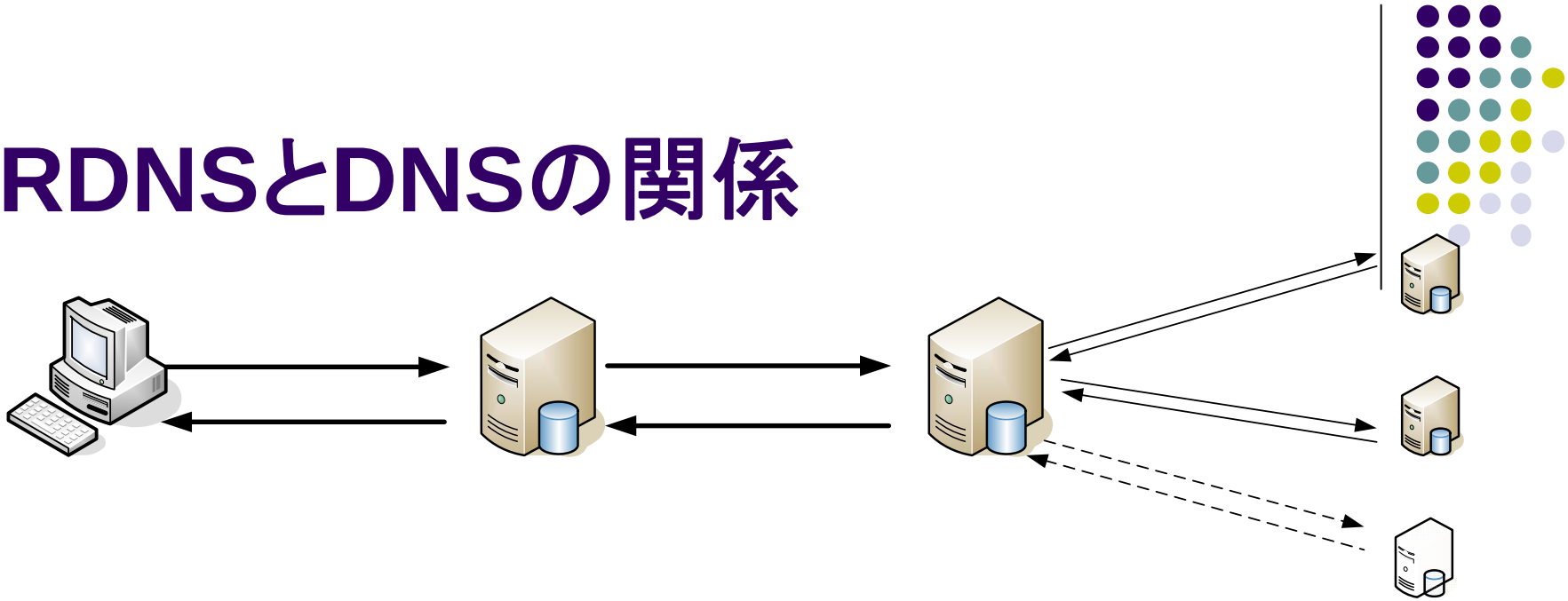
→RDNSとNATルータに事前に鍵を持たせておけば，盗聴される可能性があるのは④か⑤の為，危険性は軽減できる

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。



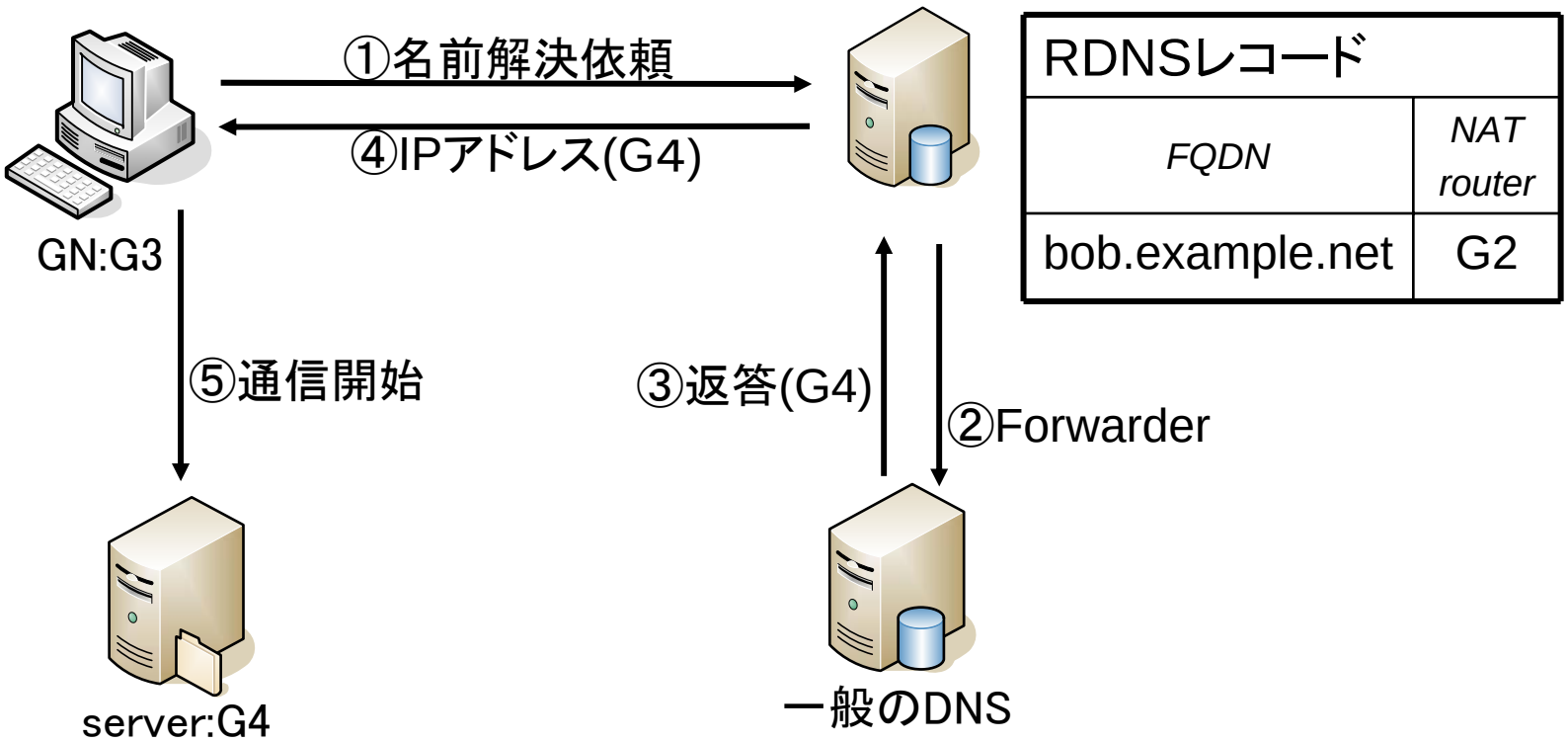
RDNSとDNSの関係



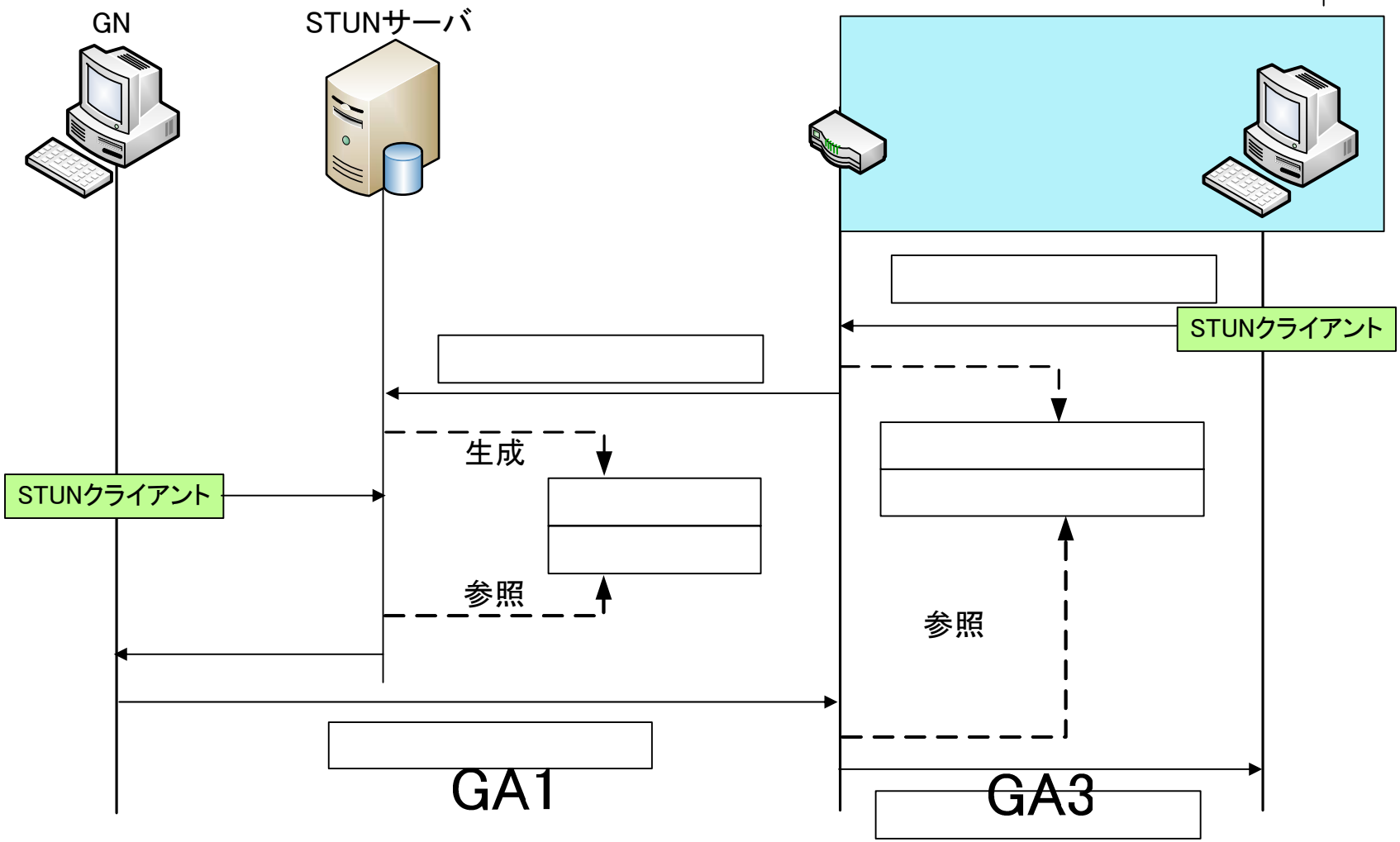
- GNは予めプライマリDNSにRDNSを登録しておく必要がある
  →RDNSは直接GNと通信を行うことでGNのIPアドレスを得る
- 異なるアドレス空間のPNが増大するとRDNSの対応が悪くなる可能性がある。
- この方式が普及し、一般のDNSにRDNSの様なルータをやり取りする機能が(ブリッジ等で)実装されれば、GNはプライマリDNSを変換することなく実現できる

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

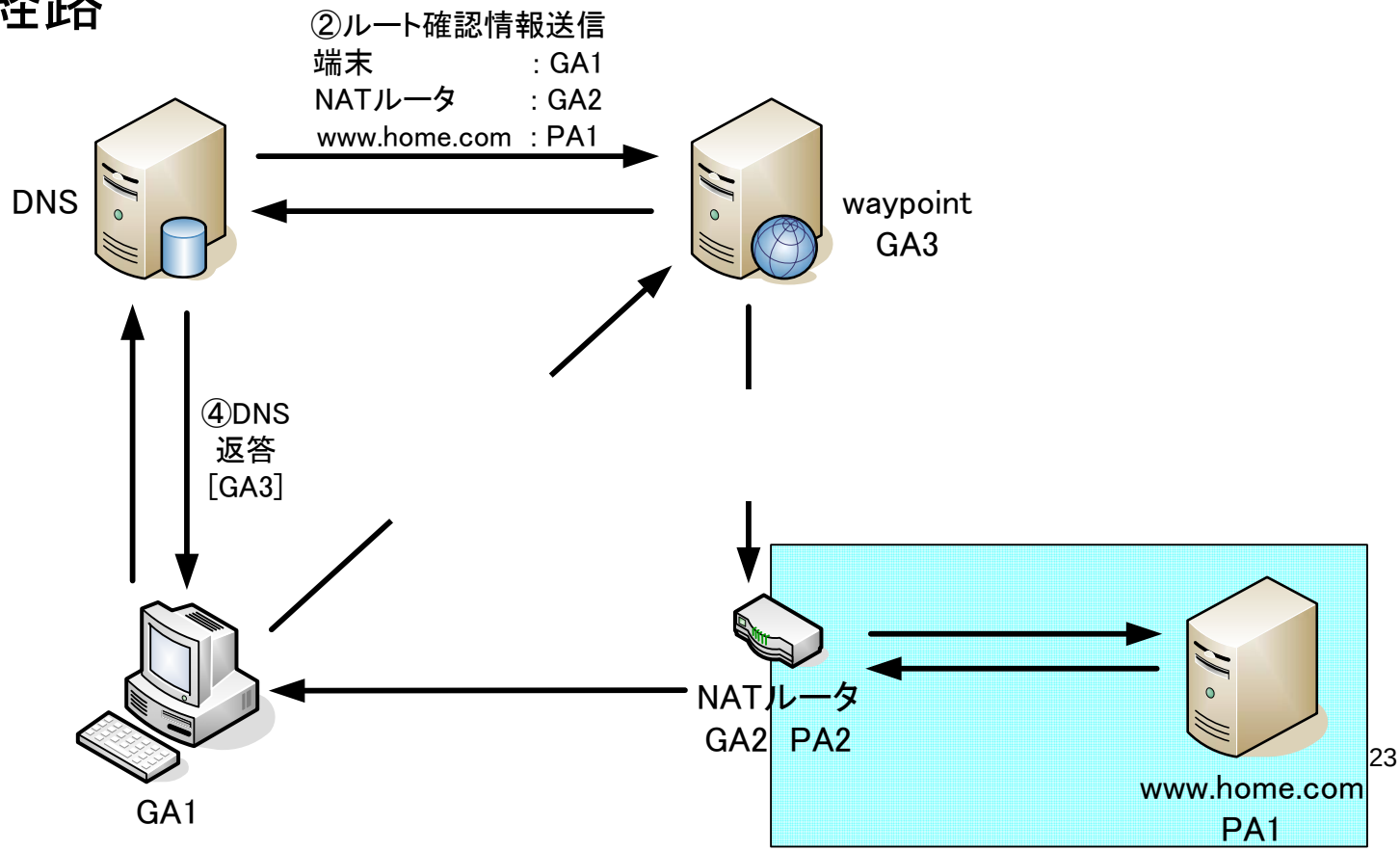


STUN
(Simple Traversal of UDP Through NATs)

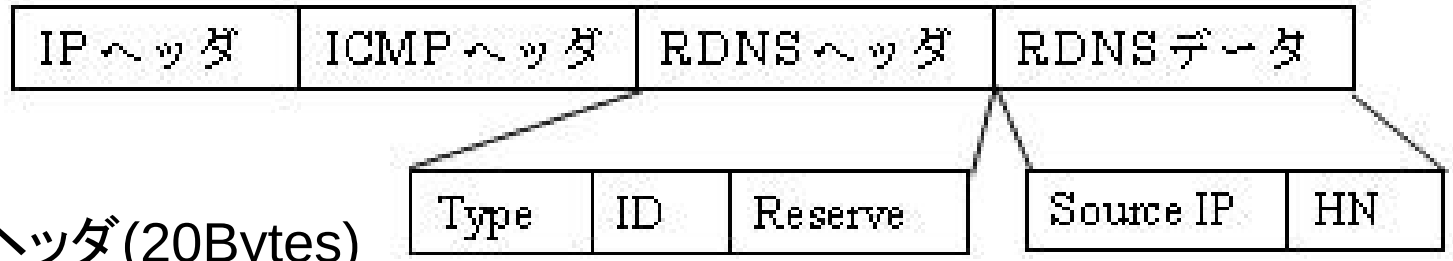


NAT越え既存技術例：AVES

- 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



RDNS-NATルータ間パケット



- IPヘッダ(20Bytes)
- ICMPヘッダ(24Bytes)
- RDNS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，RDNSが受信した際に，①に対応する④だとわかるようにする．(16bits)
- Reserve　　:予備 (8bits)
- RDNS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)

RDNSの処理

- DNSの53番ポートで名前解決依頼があった場合、bindに渡す
- 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
- 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

NATルータの処理