端末の機能追加が不要な NAT 越え方式の提案

宮﨑 悠

A proposal of NAT-Traversal that does not force terminals to have any extra functions

Yutaka Miyazaki

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をグローバルアドレス空間に接続するためにアドレス変換装置(以下 NAT：Network Address Translation)が使用される．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は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へと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ネットワーク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，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 (UDP) Through Network Address Translators)[1] ， AVES(Address Virtualization Enabling Service)[2]や 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 サーバと NAT 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．本方式では一般家庭でコンピュータを使う人がアドレス空間の違いによる影響を意識することなく，通信することができることを目標としている．

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 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うことによって 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要する．

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．動作手順は以下の通りである．

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，WEB サーバの情報(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 ルータの持つ NAT テーブルにはルーティング情報が登録される．

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，PN に関する情報を得る．

GN は得た情報を元に PN 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．

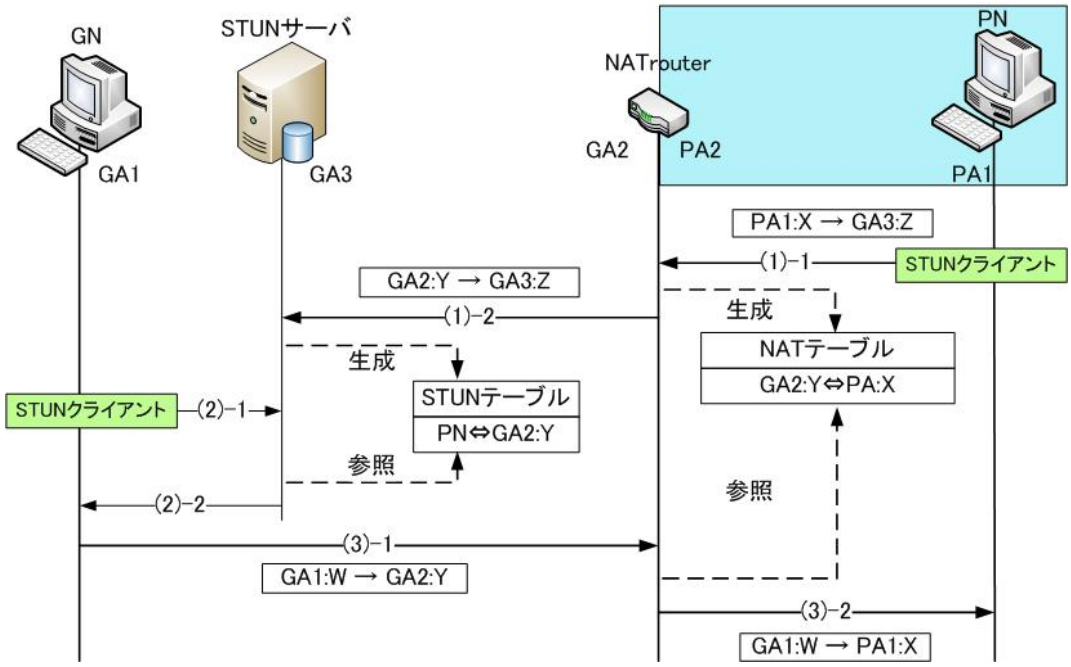


図 1　STUN の動作

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．

初めに①GN は DNS に WEB サーバについて問い合わせると，②DNS は waypoint に WEB サーバまでのルートを確認する．次に③Waypoint は情報が正しければ応答し，④DNS は GN に waypoint のアドレスを教える．⑤GN は waypoint に対して通信を開始する．⑥waypoint はパケットの宛先アドレスをプライベート空間で用いるアドレスに変換し，グローバルアドレス空間で用いるアドレスで IP in IP カプセリングし，NAT ルータへ送信する．⑦NAT は上記パケットを受信すると，デカプセリングし WEB サーバへ送信する．⑧WEB サーバは GN へ応答すると，⑨返答はそのまま GN へ届けられる．以後，⑤から⑨の手順による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，DNS サーバ，NAT ルータの改良が必要である．また経路が冗長になる，IP in IP カプセリングによるパケット冗長などの課題がある．

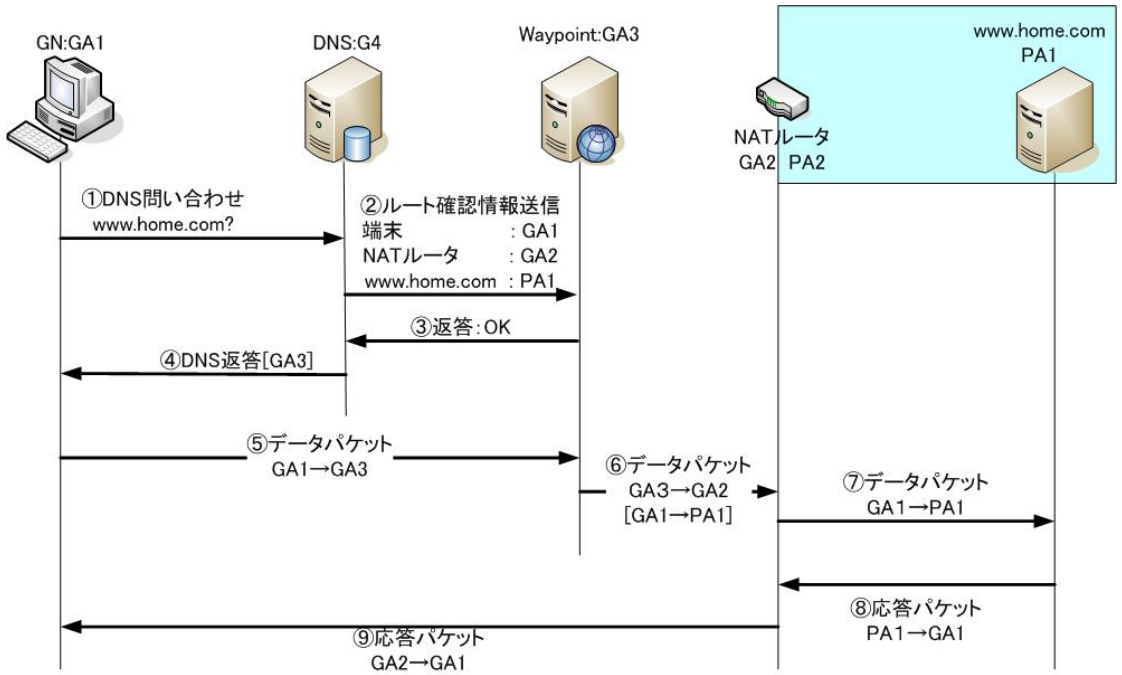


図 2　AVES の動作

2.3.　NAT-f

我々はP2P通信を崩さずNAT越えを実現する手段として，NAT-f と呼ぶプロトコルを提案している．NAT-f では機能を実装した GN と NAT-f 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かつ強制的に NAT テーブルを生成し，NAT 越えを実現する．以下に動作を説明する．

GN が PN と通信を開始する祭，NAT-f ルータの FQDN”sun.example.net”の先頭に PN のホスト名”bob”を付加して DDNS サーバに名前解決依頼を行う. DDNS サーバは GN に対し，ワイルドカード機能により NAT-f ルータの IP アドレス”G2”を返す．GN のカーネルにおいて PN のホスト名と NAT-f ルータの IP アドレスを取得する．更に NAT-f ルータの IP アドレスを仮想 IP アドレス”V1”に書き換え，これらを名前関連テーブル(NRT：Name Relation Table)へ対応付ける．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仮想 IP アドレス”V1”を PN の IP アドレスとして報告する．

次に，NAT-f ネゴシエーションを説明する．GN は NAT-f ルータ宛てのパケットを送信する際，カーネルにおいて送信元/宛先 IP アドレスとポート番号，およびプロトコルタイプより仮想アドレス変換(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-f 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，NAT-f 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 に従ってパケットの内容を変換し，存在しなければ相手をランダムな仮想アドレスと DNS からの情報と対応づけて登録する．

GN からのパケットは一時的にカーネル内に退避させてから NAT-f ネゴシエーションを実行する．

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”G1,V1”とポート番号”s,d”, プロトコルタイプ”TCP”, および NRT から取得した NAT-f ルータのグローバル IP アドレス”G2”と PN1 のプライベートホスト名“bob”を NAT-f ルータに通知する．

NAT-f ルータがこの通知を受信すると受信した情報と該当する PN のプライベート IP アドレスから NAT テーブルを強制的に生成する．

NAT-f ルータは先ほど GN から受信した送信元／宛先 IP アドレスとポート番号, プロトコルタイプ, NAT-f 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-f 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，TCP/UDP のどちらの通信にも対応でき，カプセル化の必要もないのでオーバヘッドが少ない．更には NAT の種類にも左右されないという利点がある．

しかし，GN に NAT-f 機能の実装を行う必要があるという課題がある．

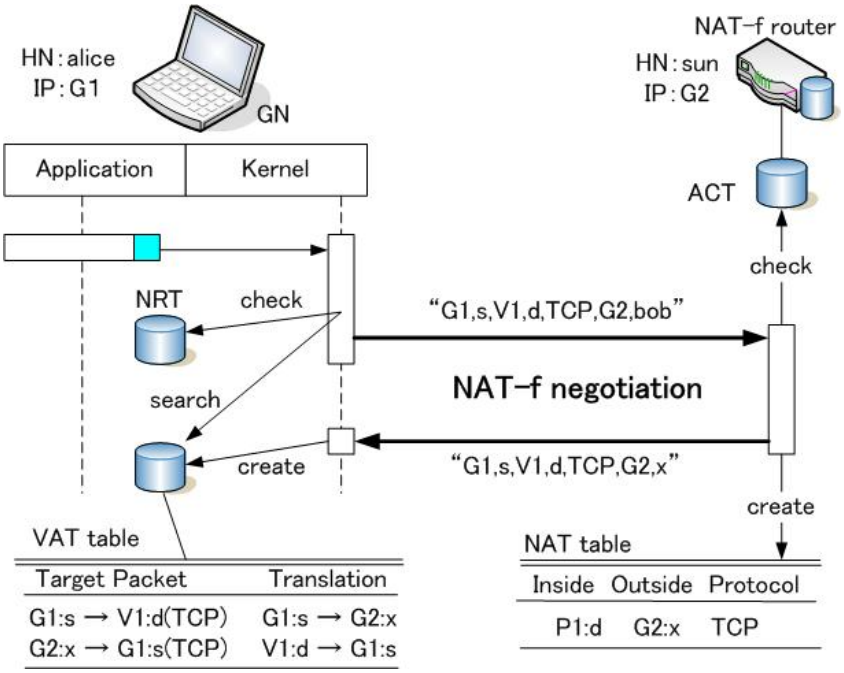


図 3　NAT-f ネゴシエーションの動作

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．

図 4 に本方式で考えられるネットワーク構成の例を示す．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 1･2, その NAT ルータと協調する拡張 DNS サーバの TSN(Transfer Supported by Name-system)サーバ，一般の DDNS(Dynamic DNS)が存在する．グローバルアドレス空間には GN，NAT ルータを介したプライベートアドレス空間には PN が存在する．

本方式では GN および PN に特別な機能追加をする必要はない．TSN サーバと NAT router1･2 には本方式の機能が実装されている必要がある．

以下の動作説明では GN1 から PN1(bob)へ通信を開始する場合の例を，3.2 事前設定，3.3 名前解決，3.4 通信にわけ，それぞれ説明する．

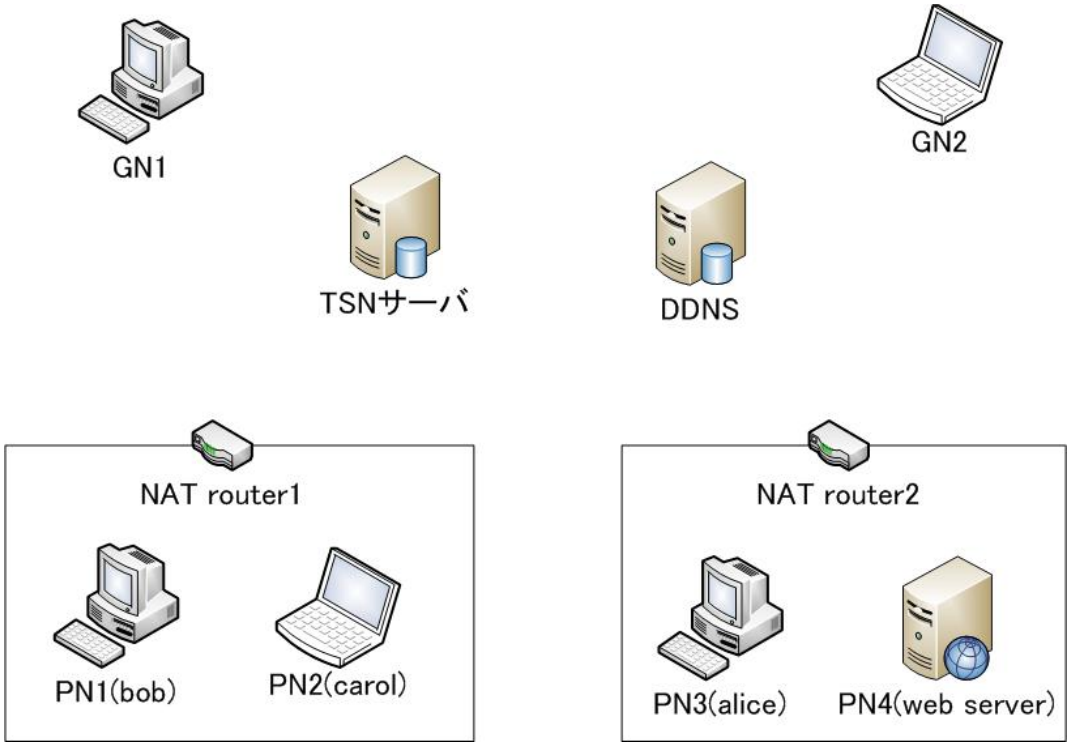


図 4　提案方式のネットワーク構成

3.2.　事前設定

外部から通信開始を許可するにあたり，予め PN は FQDN(Fully Qualified Domain Name:完全修飾ドメイン名)と NAT ルータのアドレスを DDNS 登録しておく．これは本方式に限ったことではなく，一般の DNS 登録と同様である．

上記の DNS 登録時に，PN から DNS への名前登録パケットを受け取った NAT ルータは，GT(Guide Table：表１)を作成する．GT には送信元･宛先の IP アドレス(Source･Destination IP)とポート番号(Source・Destination Port)，および宛先 IP アドレスに対応した PN のホスト名(Host Name)が保持される．その中で，DNS 登録パケットから現段階でわかる PN のプライベート IP アドレスとホスト名をテーブルに書き込む．

また，本方式を使って NAT 越えを実現するために，GN はプライマリ DNS として任意の TSN サーバを登録しておく必要がある．

表 1　Guide Table

Source IP (32bits)	Destination IP (32bits)	Source Port	Destination Port	Host Name

3.3.　動作概要（名前解決）

動作概要の名前解決シーケンスを図５で説明する．初めに①GN は bob.example.net の名前解決を TSN サーバへ依頼する．②依頼を受けた TSN サーバは自レコードに bob がないため，フォワーダにより他の DNS へ名前解決を依頼し，情報を得る．③TSN サーバは GN から bob 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 Guide Table に送信元 IP アドレス(SIP)と宛先 IP アドレス(DIP)，ホスト名 HN にそれぞれ G3，P1，bob を記入し作成する．④GT を作成した NAT ルータは TSN サーバへ応答する．⑤TSN サーバは GN へ名前解決される．

3.4.　動作概要(通信)

図６に通信シーケンスを示す．⑥GN は取得した IP アドレス G2(NAT ルータの IP アドレス)へ通信を開始する．　⑦NAT ルータは GN からのパケットの情報を元に宛先･送信元ポート番号(SP,DP)を GT へ付け加えてテーブルを完成させる．次に GT に基づきパケットを強制的に bob に転送する．⑧これに対する bob からの応答パケットは⑨GT

を参照することにより GN へ送信される．以後は⑥から⑨の手順により通信を行う．

NAT ルータはパケットが通過する度に GT を参照する．TSN サーバを利用していない通信は GT にデータが存在しないため，通常の NAT 機能により NAT テーブルが作成されアドレス変換されて通信を行う．

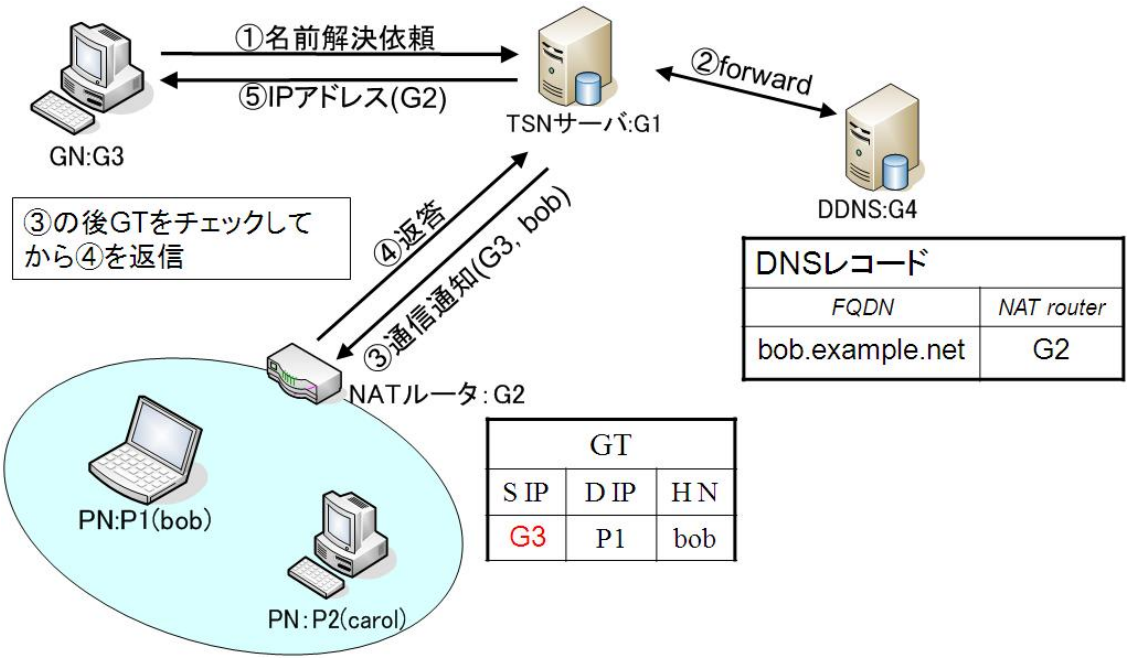


図 5　提案方式の動作(名前解決)

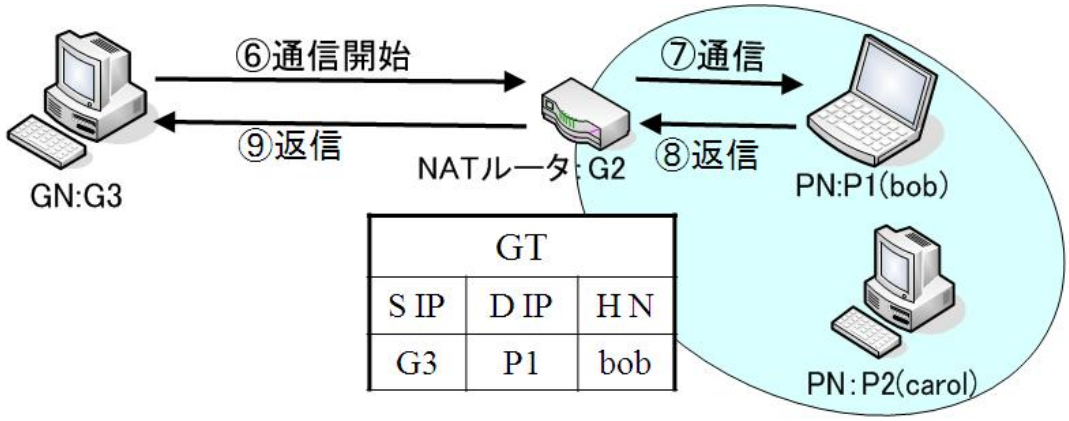


図 6　提案方式の動作(通信)

3.5.　異なるプライベートネットワークに存在する端末同士の通信

TSN サーバからの通信通知は NAT ルータが通信端末を確定する情報として，送信元のグローバル IP アドレスと宛先の端末のホスト名のみを通知する．しかし第一章でも説明したとおり，ほとんどの端末はプライベート IP アドレスを割り当てられており，プライベート IP アドレスを持つ端末は NAT ルータのグローバル IP アドレスが使われる．よって，同じネットワークの端末が同じグローバル IP アドレスへ通信を行った場合は，NAT ルータがどちらの通信か判断できなくなってしまう問題が発生する．しかし GN の名前解決依頼時に GT は作成され，GN からの通信を受信した時にポート番号によって識別される．そのため，この問題は同時に名前解解決･通信通知がなければ発生しない．

例えば先に図 5･6 のように通信があった場合，GT には表 2 のようにテーブルが作成される．ここで alice が carol へ通信を行う場合の動作を図 7 で説明する．NAT router1 は先ほどの通信とは違うので違うポート番

号より通信を開始する．その通信を受け取った NAT router2 は GT を参照し, Source Port が違うので先に来ているはずの通信通知によりできた GT で carol に通信を転送することができる．

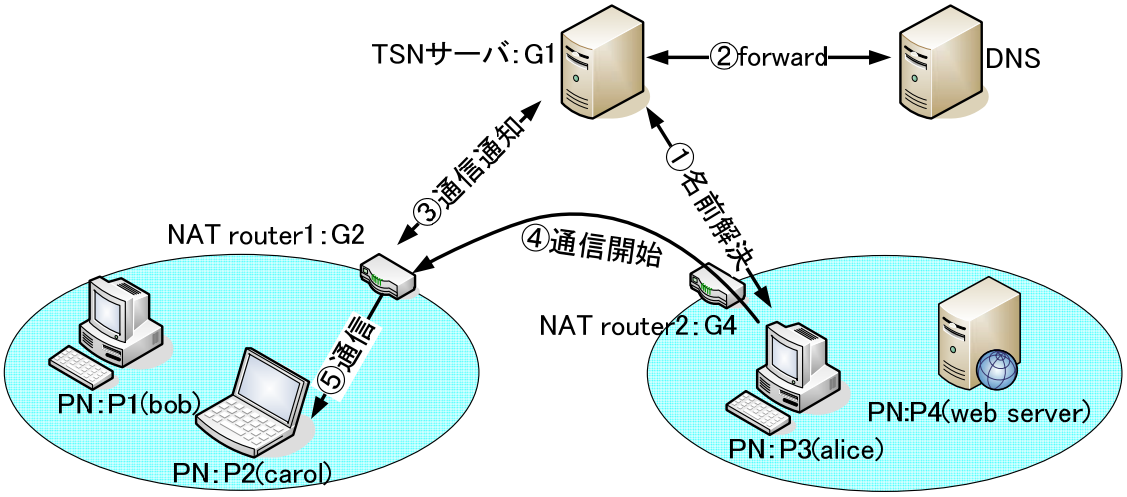


図 7　PN-PN による動作手順

表 2　Guide Table(通信通知受信後)

Source IP (32bits)	Destination IP (32bits)	Source Port	Destination Port	Host Name
G2	P4	X	Y	web server

3.6.　DNS 変更

本方式では GN からの名前解決の際には必ず TSN サーバを使用しなければならない．よって GN のプライマリ DNS 設定を変える必要がある．しかしこれは本方式に限らず，DNS を改良する通信方式には必須のことで，一般ユーザでも DNS を独自に運用している場合にもしているので，大きな問題ではない．また，セカンダリ DNS に元の DNS を設定しておくことにより，何らかの原因により TSN サーバのサービスが停止した時も通常の通信は問題なく行うことができる．

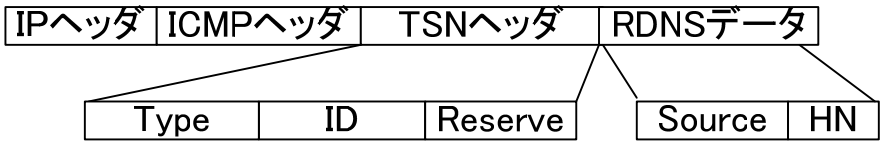
最終的にはインターネットのサービスプロバイダが TSN サーバを運用することができれば，ユーザはその設定を変える必要もなくなる．

3.7.　通信通知パケット

パケットの詳細は表 3 に明記する．

TSN サーバと NAT router の間でやり取りされる通信通知パケットは ICMP-ECHO パケットを使用する．TSN サーバは通信相手が自分のレコードに登録されていない場合，相手が本方式対応かどうかがわからないため，通信通知を毎回行う必要がある．ICMP 通信の場合は相手が本方式対応でなくても，パケットが到着すればエコーパケットが返ってくるため，相手の端末に関わらず対応か非対応かを判断することができる．

表 3　通信通知パケット



- IP ヘッダ(20Bytes)
- ICMP ヘッダ(24Bytes)
- TSN ヘッダ(4Bytes)

- Type(8bits)　　：パケットのタイプが通知③か応答④かを判断
- ID(16bits)　　：DNS が名前解決の際に使用する，トランザクション ID 同じ値．TSN サーバが NAT ルータからの返信を受信した際に，どの名前解決に対応する通信通知か応答わかるようにする
- Reserve(8bits)　：予備

● TSN サーバデータ(68Bytes)

- Origin IP(32bits)　：要求元 IP アドレス
- HN(64Bytes)　　：Host Name

4. 評価

4.1. 技術比較

表 4 に NAT 越えの既存技術と提案方式の比較を示す．

比較項目 GN，PN，NAT ルータはそれぞれに機能を実装する必要があるかどうか，第三装置は通信においてエンド端末以外の第三の装置が必要であるかどうか通信冗長は通信パケットに情報を付加する必要があるかを表す．

提案方式と AVES は端末に手を加えずに実現しているので GN と PN をともに○である． NAT-f では GN と NAT ルータがネゴシエーションをして P2P 通信を可能としているので第三装置は必要ない．また，提案方式，4+4，NATs では DNS サーバを改良するが， DNS サーバを使った通信は一般的であるため第三の装置とは言わないため△である．NAT ルータをそのまま利用できる方式は STUN だけである．しかし，STUN の原理により NAT の処理の方式に制限があるため△とする．提案方式，NAT-f，STUN は通信に先だってネゴシエーションや hole punching のパケットは必要となるが，AVES や 4+4 の様に実際の通信パケットにはデータ付加などがないので○とする．

本方式はユーザ端末を改造することなく NAT 越えを実現できるため，通信を行うユーザは NAT の存在を意識する必要はない．よって，コンピュータや通信の知識がない人が存在する家庭や企業で一番効果を発揮する方式だといえる． AVES でも同様に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 を中継して NAT 内に転送されるため，パケットの経路が冗長となる．また，GN は waypoint へ通信を行っているため，通信相手は waypoint となってしまう課題もある． しかし，本方式では NAT 越えに必要な処理は初めの名前解決時に全て完了しているので，各ユーザ端末は P2P で通信を行える．

表 4　NAT 越え技術の比較

比較項目	提案方式	STUN	AVES	NAT-f	4+4	NATs
GN	○	×	○	×	×	×
PN	○	×	○	○	×	○
第三装置	△	×	×	○	△	△
DNS サーバ	×	○	×	○	×	×
NAT ルータ	×	△	×	×	×	×
通信冗長	○	○	×	○	×	○

5. むすび

本論文では各ユーザ端末には一切の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．本方式の機能を追加した TSN サーバと NAT ルータが通信端末を通知し，独自のテーブルにより一意にすることで NAT 越え問題を回避する．

今後は実際に TSN 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] 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.
[4] Z. Tur´anyi, A. Valk´o : IPv4+4,
[5]Shiang-Ming Huang, Quincy Wu, Yi-Bing Lin :Tunneling IPv6 through NAT with Teredo Mecanism,

・謝辞

本研究を行うに当たり，多大なるご指導・ご鞭撻を頂きました渡邊晃教授に心より感謝いたします．また，有益な助言及び検討を頂いた渡邊研究室の皆様に深く感謝します．

・附録

6. NAT の動作

NAT には，IP アドレスのみを変換する NAT と IP アドレス変換に加え，ポート番号変換も行う NAPT(Network Address Port Translation)がある．NAT はグローバル IP アドレスとプライベート IP アドレスを対応づけるだけなので，複数のプライベートアドレス空間の端末が，同時にグローバルアドレス空間上の端末と通信ができるのは NAT の保持するグローバル IP アドレスの数だけに制限される．一方，NAPT はポート番号を用いて通信の判別を行うため， NAPT に 1 つだけグローバル IP アドレスを割り当てれば，複数のプライベートアドレス空間の端末がグローバルアドレス空間の端末と同時に接続できる．NAPT は NAT より汎用性が高いので多く使われているが，NAPT は広義の NAT に含まれるため，以後 NAPT を含めて NAT と呼ぶ．ただし，本稿における NAT の動作説明は全て NAPT のそれを指すものとする．

NAT の動作説明の例として，クライアント端末から異なるアドレス空間に所属する WEB サーバへの HTTP 通信を挙げる．NAT router は NAT 機能が搭載された装置である．PA はプライベート IP アドレス，GA はグローバル IP アドレスを示す．

まずプライベートアドレス空間に所属する端末からグローバルアドレス空間に所属する WEB サーバに通信を開始する場合の NAT の動作を図 7 に示す．はじめにクライアントは宛先を IP アドレス GA1，ポート番号を 80，送信元を IP アドレス PA1，ポート番号を X として送信する(1)．X はクライアントの OS が動的に選んだ任意のポート番号である． NAT router では送信元を NAT router の IP アドレス GA2，ポート番号 Y へと変換して中継する(2)．Y は NAT router が動的に選んだ任意のポート番号である．このとき NAT router はこの変換の関係を記した NAT テーブルを生成する．このパケットを受信した WEB サーバは，応答パケットを宛先 IP アドレス GA2，宛先ポート番号 Y，送信元 IP アドレス GA1，送信元ポート番号 80 として返信する(3)．このパケットは NAT router が受信し，NAT テーブルに従って宛先を IP アドレス PA1，ポート番号 X に書き換えて中継し(4)，クライアントがこれを受信する．以後の通信は NAT テーブルに従って，NAT router がアドレス変換を行うことにより，通信が行われる．

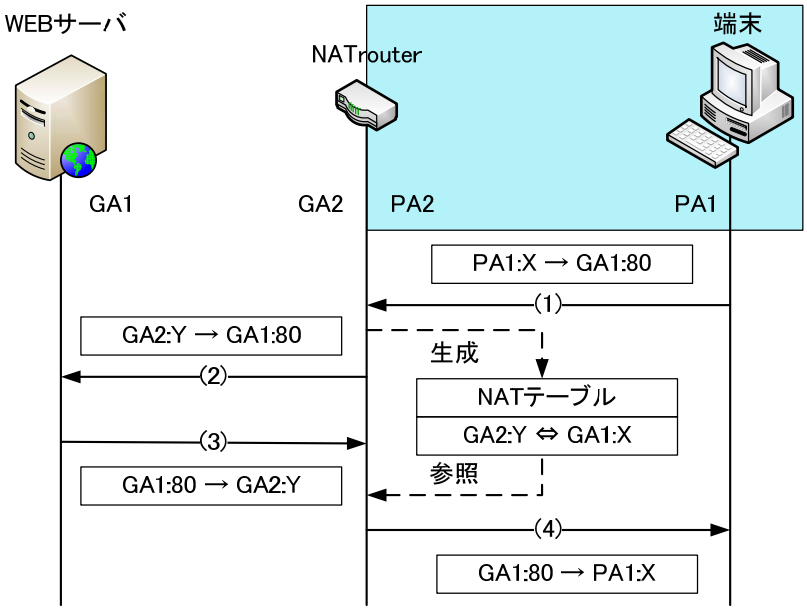


図 8　NAT の動作（内→外）

次に，グローバルアドレス空間に所属する端末がプライベートアドレス空間に所属する WEB サーバへ HTTP 通信を開始する場合の NAT の動作を図 8 に示す．まず WEB サーバはプライベート IP アドレスであるため，グローバルアドレス空間から見ると無効な値であり，インターネット上に送信ができない(1)．また，仮に NAT router のグローバル IP アドレスを知ることができて，NAT router までパケットを送信できたとしても，NAT router には，まだ NAT テーブルが存在しないため NAT router はどこにパケットを中継すれば良いのか判断できないため，破棄される(2)．即ちプライベートアドレス空間にサーバ，異なるアドレス空間にクライアントが存在するシステムは一般的に構築できない．ただし，NAT で静的にあらかじめ NAT テーブルを手動で記述しておく IP フォワードと呼ぶ機能を利用すればこの限りではない．しかしこの方法では，1 つのポートに対して 1 台しか設定できないことや動的に変更が不可能なため柔軟性に欠けるなどの欠点がある．

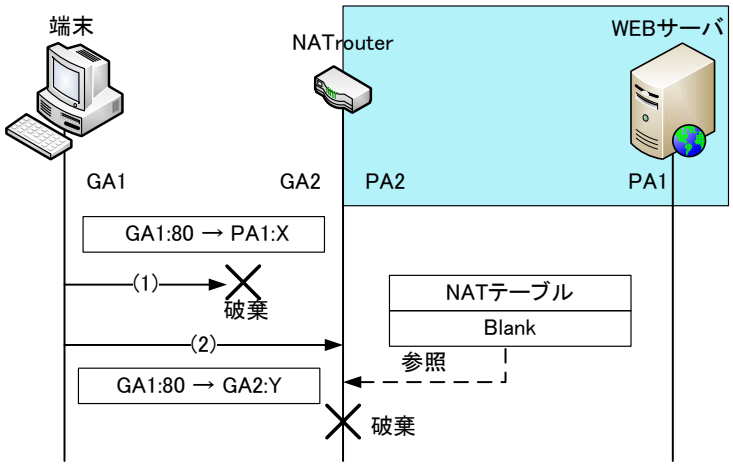


図 9　NAT の動作（外→内）

7. その他の NAT 越え既存技術

7.1. UPnP(Universal Plug and Play)

コンピューターや周辺機器などネットワークに接続された機器が．相互に認識し機能するための互換自動認識方式のことで、ネットワークにプラグするだけで簡単に動作を行えるネットワーク上の仕組みを呼ぶ．言わばプラグアンドプレイのネットワーク版である．TCP/IP ベースのホームネットワーク向けのプロトコルを使用し **UPnP** 対応の機器がネットワークに接続されると互いに認識しあい，また物理的に異なるネットワークに存在するデバイスであっても，新たな機器が接続されたことやその機能内容を通知し，その後も一定時間ごとに自らの存在を LAN に通知することになっている．

7.2. IPv4+4

IP アドレスは IPv4 では 32bit だが, IPv4+4 は IPv4 ヘッダをカプセル化することで更に 32bit 追加する．IP アドレスを複数扱えるようにすることで，異なるアドレス空間を跨いだ時にその空間で有効なアドレスに変換して通信を行う技術である．図 9 に IPv4+4 の動作を示す．この方式では各端末，ルータ，および DNS サーバなど通信に関係する全ての装置に IPv4+4 機能を追加する．IPv4+4 では IP アドレスの代わりに，端末と端末が所属するネットワークのゲートウェイの IP アドレスをくみとした IPv4+4 アドレスが用いられる．IPv4+4 アドレスは IP アドレスを”.”で区切った形で表記される．

- グローバルアドレス空間に存在する端末 GN は，通信に先だって DNS に問い合わせる
- DNS サーバから宛先 IPv4+4 アドレス(GA2.PA1)を取得

- GN は送信元(GA1,0)，宛先(GA2,PA1)としてパケットを送信
- これを受け取った NAT ルータは宛先(PA1,GA2)として PN へ転送

このようにして GN の通信は PN に到達する．以降は(3)(4)のように NAT ルータに変換されて通信を継続する．IPv4+4 では通信を行う各端末と介する NAT に機能の追加が必要なため，導入が難しいという課題がある．

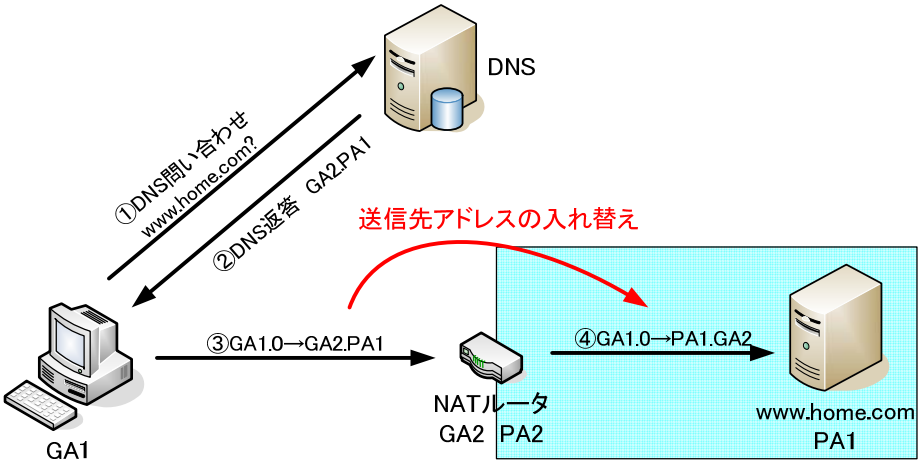


図 10　IPv4+4

7.3.　NATS(Network Address Translation with Sub-Address)

サブアドレスと呼ばれる新しい IP アドレス体系を定義し，ポート変換の変わりに IPinIP Tunneling を用いてパケットをカプセル化し，NAT を通過させる．

グローバル空間に端末(GA1)，プライベート空間に WEB サーバ(PA1)，その間に NATS BOX(GA2,PA2)を配置．

- 端末は DNS に IP アドレスと共にサブアドレスを取得
- 取得したサブアドレスを元に宛先 PA1 送信元 GA1 のパケットを宛先 GA2 送信元 GA1 の IP ヘッダでカプセル化し，送信
- これを受信した NATS BOX はカプセル解放処理を行い，WEB サーバへと転送
- WEB サーバは応答パケットを宛先 GA2 送信元 PA1 として送信
- NATS BOX がこのパケットを受け取ると，送信元を PA1 から GA2 へと書き換えた IP ヘッダでカプセル化し，端末へと転送

以後同様の処理によって通信される．

NATS では端末，DNS サーバ，NATS BOX を改良する必要があり，NATS BOX が端末に変わってカプセル化することで，NATS BOX に処理が集中する．また，サブアドレスを DNS サーバに登録する必要があり，サブアドレス取得のために DNS シーケンスに変更を加える必要もあるなどの課題もある．

7.4.　Teredo

IPv4 環境で IPv6 ネットワークを透過的に実現するために，Microsoft を中心に進められている技術である．Teredo クライアント(PN)には Teredo サーバから IPv6 アドレスが与えられ，仮想ネットワーク端末として認識される．

- PN は Teredo サーバに Teredo アドドレスを要求し，UDP 通信を行う(STUN の要領で NAT テーブルを生成)
- IPv6host は IPv6 パケットを Teredo サーバへ送信
- IPv6host のパケットは Teredo サーバにより，UDP パケットでカプセリングされ PN へ代理送信
- NAT は UDP パケットを受信し，予め作成されている NAT テーブルより PN へ転送
- PN は受信したパケットと同様に IPv6 パケットを UDP でカプセリングし，Teredo サーバへ返信
- Teredo サーバは受信したパケットをデカプセリングし，IPv6host へ転送

以上のように通信が行われる．Teredo では STUN 同様 NAT や DNS はそのままの装置を利用できるが，PN にアプリケーションを導入し，特殊な第 3 のサーバが必要という課題がある．

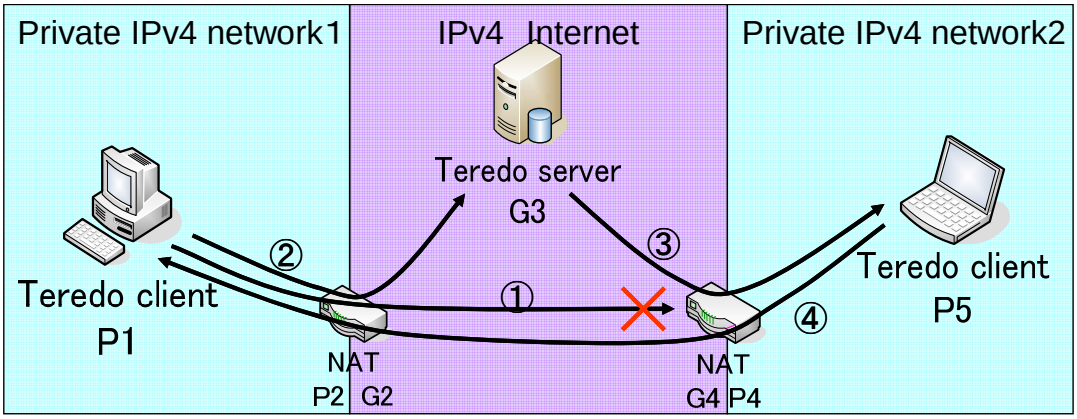


図 11　Teredo による IPv4 の NAT 越え