端末の変更が一切不要なNAT越え通信システムの提案

松尾辰也[†1]　鈴木秀和[†1]　渡邊晃[†1]

IPv4 アドレスの枯渇に対応するため，家庭内や企業のネットワークの端末はプライベートアドレスで実現するのが一般的である．しかし，NAT が存在するとインターネット側の端末からプライベートアドレス側の端末へ通信を開始できない NAT 越え問題が存在する．NAT 越え技術としてこれまで様々な方式が提案されているが，多くの方式では端末に特殊な機能を実装する必要がある．この課題を解決するために，我々は端末の改造が不要な NAT 越え技術 NTSS（NAT Traversal Support System）を提案しているが，端末の設定変更が必要という課題が残されていた．本論文では，NTSS を更に改良し，設定変更も不要とした NTSSv2 を提案する．

Proposal of NAT traversal communication systems do not require any change of the terminal

Tatsuya Matsuo,[†1] Hidekazu Suzuki[†1]
and Akira Watanabe[†1]

In order to cope with the situation where IPv4 addresses are about to be exhausted, it is now common that network terminals within homes or in offices are being handled with private addresses. However, in the case where NAT exists in between, we encounter a so called “NAT traversal problem”, meaning that it is not possible to initiate communication from a terminal on the side of the Internet toward a terminal with a private address. Although there have been a number of methods proposed as NAT traversal technologies, many of them require special function to be added at the terminal. In order to solve this problem, we have proposed a NAT Traversal Sipport System (NTSS), but there was a problem with this system, too; that is, that some modification of the setting was required at the terminal in advance. In this paper, we propose a system called “NTSSv2”, which is an improved version of NTSS. This NTSSv2 does not even require any modification of the setting at the terminal.

1. はじめに

IPv4 ネットワークは IP アドレスの枯渇を回避するため，家庭内や企業など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．プライベートアドレスはインターネット上では利用できないので，両ネットワークの間には NAT（Network Address Translation）[1)2)] を設置し，アドレス変換を行う必要がある．しかし，NAT はインターネット側の端末からプライベートアドレス側の端末へ通信を開始できないという課題があり，これを NAT 越え問題と呼ぶ．これまでのインターネットの利用形態は Web ページ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側の端末から通信を開始していたため，NAT 越え問題が表面化することはなかった．しかし，近年ではネットワークの普及に伴い，企業だけでなく一般家庭にもネットワークを構築することが一般的になると考えられる．そのため，インターネット側からプライベートアドレスのサーバなどに自由にアクセスしたいというニーズは十分にあると考えられる．

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きたが，その目的により以下のように分類することができる．すなわち，既存の NAT 装置をそのまま使えることを目的としたアプリケーションレベル改造方式，既存のアプリケーションをそのまま使えることを目的としたネットワークレイヤ改造方式，端末の改造を不要とすることを目的とした端末非依存方式である．

アプリケーションレベル改造方式は，エンド端末のアプリケーションとインターネット上に設置したサーバが NAT テーブルの情報を交換し，NAT に生成された NAT テーブルに合わせて，外部端末からパケットを送信する点が特徴である．この方式は，アプリケーションが限定されることと，第三の装置が必要になるという課題がある．代表例として，STUN[3)4)]，TURN[5]，UPnP[6] などがある．

ネットワークレイヤ改造方式は，アプリケーションを限定しないために，外部端末のカーネルや NAT ルータなどのネットワーク機器に手を加える．外部端末と NAT ルータが協調してパケットを内部に転送する点が特徴である．この方式は，端末の OS ごとに異なる対応が必要となる．代表例として，4+4[7]，NAT-f[8] などがある．

†1 名城大学
Meijo University

端末非依存方式は，DNS サーバ，NAT ルータ，あるいはインターネット上のサーバなどが情報交換し，一般端末が送信するパケットを通信経路上でアドレス変換し，プライベートアドレス空間の中に転送する点が特徴である．この方式は研究事例がそれほど多くないため，研究途上であるといえる．端末非依存方式の AVES[9] では，第三の装置が必要であること，通信経路が冗長になること，送信元アドレスが実際と異なるため経路上のルータで廃棄される可能性があるなどの課題がある．

これらの NAT 越え技術を用いると，共有サーバをプライベートアドレス空間に設置できるので，グローバル IP アドレスを大幅に節約することができる．このとき，情報家電やモバイル端末の多様化により，今後はユーザが自由に端末に機能を追加できない場合が考えられる．そこで，本論文では一般ユーザが容易に共有サーバを利用できるようにするため，端末に改造が不要な端末非依存方式に着目する．

我々はこれまで端末非依存方式として NTSS（NAT Traversal Support System）[10] を提案してきた．NTSS はアクセスする側が使用する DNS サーバおよびアクセスされる側の NAT ルータを改造し，それぞれを協調させることにより，NAT 越えを実現する．第三の装置が不要でエンドエンドで NAT 越え通信を行うことができ，AVES が抱えていた課題を解決できる．しかし，NTSS では一般ユーザのプライマリ DNS 登録変更をしなければならなく，この部分が負担となる可能性があった．そこで本論文では，プライマリ DNS には改造を加えず，アクセスされる側のアドレスを管理する DDNS（Dynamic DNS）サーバを改造するように機能を見直した NTSSv2 を提案する．この方式によると，端末の変更および設定変更が一切不要な NAT 越えが実現できる．

以下 2 章で NTSS，3 章で NTSSv2，4 章で NTS ルータの負荷予測を説明し，5 章でまとめる．

2. NTSS

本章では提案のベースとなる NTSS について，その実現手法と課題を示す．以後の説明では，EN（External Node）を NAT の外側からアクセスする端末，IN（Internal Node）を NAT の内側に存在し，EN からアクセスされる端末とする．EN のプライマリ DNS サーバと IN 側の NAT ルータを改造し，そこに NTSS を実現させるための NTS プロトコルを実装する．改造した DNS サーバを NTS サーバ，改造した NAT ルータを NTS ルータと呼ぶ．NTS ルータは NTS サーバと協調し，外部から送信されてくるパケットに合わせて NAT テーブルをオンデマンドに生成する特徴がある．

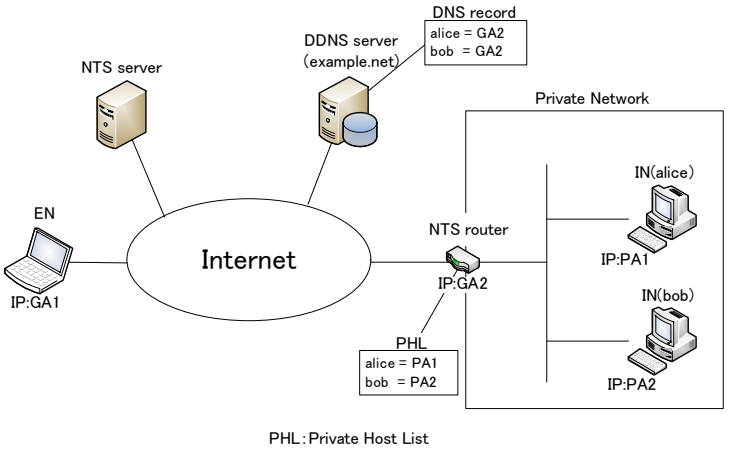


図 1 NTSS の構成

2.1 構成と事前設定

図 1 に NTSS の構成を示す．インターネット上に EN のプライマリ DNS サーバとなる NTS サーバと，IN のアドレス解決用 DNS サーバとなる DDNS サーバを設置する．DDNS サーバは既存のサービスプロバイダが使用しているものを利用できる．事前設定として，EN はあらかじめ，NTS サーバが自身のプライマリ DNS となるよう登録変更しておく．また，DDNS サーバには IN の FQDN と NTS ルータのグローバル IP アドレスの対応関係を DNS レコードに登録する．NTS ルータには IN の FQDN とプライベート IP アドレスの対応関係を独自のテーブル PHL（Private Host List）に登録する．

EN，NTS ルータのグローバル IP アドレスをそれぞれ GA1，GA2 とし，IN（alice）と IN（bob）のプライベート IP アドレスをそれぞれ PA1，PA2 とする．

EN から IN（alice）へ通信を開始する場合を例として，NTSS の動作を名前解決と通信開始時に分けて説明する．

2.2 名 前 解 決

図 2 に NTSS の名前解決シーケンスを示す．EN は通信を開始するに当たり，alice の名前解決を NTS サーバへ依頼する．NTS サーバは通常の DNS の仕組みにより，再帰検索を行い，alice を管理する DDNS サーバより NTS ルータのグローバル IP アドレス（GA2）を

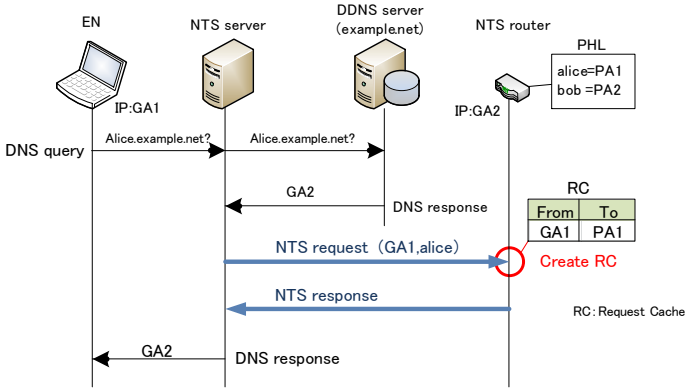


図 2 NTSS の名前解決シーケンス

取得する．図 2 は簡単のため NTS サーバの再帰検索の部分は省略して記述している．NTS サーバはこの名前解決を EN へ返信する前に，EN から alice への接続要求があることを通知する NTS リクエストを NTS ルータに送信する．このメッセージには，EN の IP アドレス（GA1）と alice の FQDN が含まれている．この通知を受け取った NTS ルータは事前に設定しておいた PHL を参照し，alice のプライベート IP アドレス（PA1）を取得する．その後，EN と IN の IP アドレスの関係を RC（Request Cache）と呼ぶキャッシュへ記憶して，NTS サーバへ NTS レスポンスを返信する．これを受信した NTS サーバは，先ほど取得した名前解決結果（GA2）を EN に返信する．

2.3 通 信 開 始

図 3 に名前解決後の通信開始シーケンスを示す．EN は名前解決の結果，alice の IP アドレスを“GA2”と認識しているため，NTS ルータに向けて通信を開始する．ここで，

$$GA1 : s \rightarrow GA2 : d \tag{1}$$

は送信元 IP アドレス GA1，送信元ポート番号 s，宛先 IP アドレス GA2，宛先ポート番号 d のパケットであることを示す．s は EN のカーネルが選択した任意のポート番号であり，d は IN がサービスを提供しているポート番号である．

NTS ルータはインターネット側からパケットを受け取ると，送信元 IP アドレスをキーとして RC を参照する．RC に該当するデータがあれば，NTS ルータは受信したパケットと RC の内容から次のような NAT テーブルを動的に生成する．

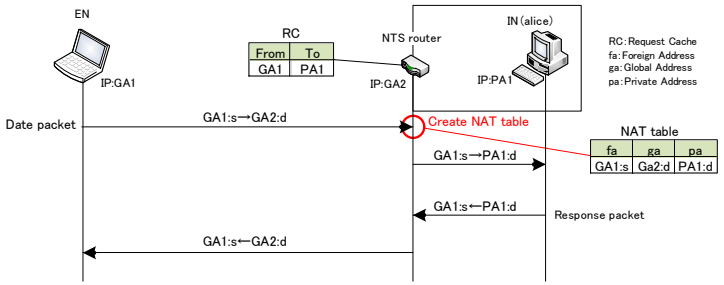


図 3 NTSS の通信開始シーケンス

$$GA1 : s \leftrightarrow \{GA2 : d \Leftrightarrow PA1 : d\} \tag{2}$$

上記 NAT テーブルの意味は，NTS ルータから見た外側トランスポートアドレス“GA1：s”との通信では NAT のトランスポートアドレス“GA2：d”と IN のトランスポートアドレス“PA1：d”が対応していることを意味する．即ち，“GA1：s”から“GA2：d”へ送信されたパケットは，NTS ルータの NAT 機能において宛先が“PA1：d”に変換されて alice へ転送される．これに対する alice からの応答パケットは上記と逆の変換を行い，EN へ送信される．RC は NAT テーブルを生成した時点で削除する．

2.4 課　　題

上記の手順により，EN は IN へ NAT を越えて通信を開始することができる．しかし，NTSS を実際のインターネット環境に適用する場合，EN にあたるユーザは，各自でプライマリ DNS の設定を NTS サーバに変更する必要がある．EN 側のプライマリ DNS サーバを改造の対象とした理由は，NTS ルータへ“GA1 から alice へ通信要求がある”ということを NTS リクエストで通知する時，EN の IP アドレス（GA1）も同時に通知できるためである．この方式では，ユーザが故意に DNS の設定を変える必要があるため，一般ユーザが利用できないという課題がある．

3. NTSSv2

EN のプライマリ DNS の設定変更をしなくてもよいように，NTSS を実現する構成機器の見直しを行った．NTSSv2 では EN のプライマリ DNS サーバは改造せず，代わりに IN のアドレス解決用 DDNS サーバを NTSv2 サーバとして改造する．これに伴い，NTS ルータの処理動作を見直した．

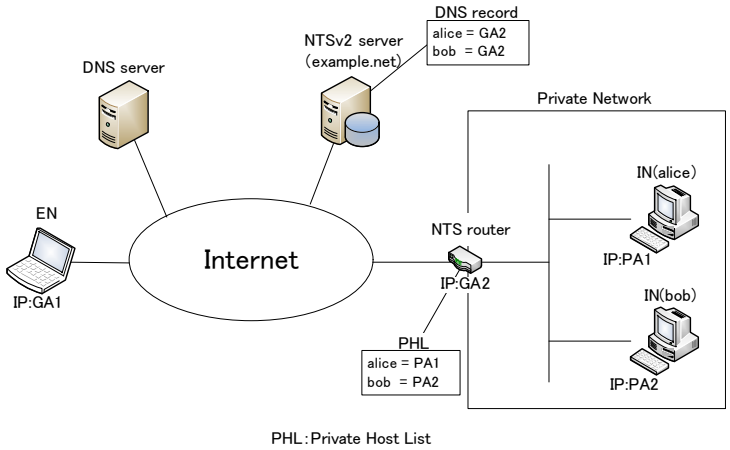


図 4 NTSSv2 の構成

3.1 構　　成

図 4 に NTSSv2 の構成を示す．IN を管理する DDNS サーバを改造し，NTSv2 サーバとする．NTSv2 サーバと NTS ルータが協調することにより，NAT 越えを実現する．EN はプライマリ DNS サーバをそのまま使うので設定の変更が不要である．

NTSS と同様に，EN から IN（alice）へ通信開始する場合を例として，名前解決と通信開始時に分けて説明する．

3.2 名 前 解 決

図 5 に NTSSv2 の名前解決シーケンスを示す．EN はプライマリ DNS サーバに IN の名前解決を依頼する．DNS サーバは通常の DNS の仕組みにより，IN を管理する NTSv2 サーバを再帰検索する．NTSv2 サーバは DNS 問合せを受け取ると，alice への接続要求を通知するために NTS リクエストを NTS ルータに送信する．この時，NTSv2 サーバが受信する DNS 問合せには，問合せを依頼したノードの情報が含まれていないため，EN の IP アドレスを特定することができない．そこで，NTS ルータは送信元 IP アドレスを“any”，宛先を alice とした RC を生成しておく．名前解決結果として EN には NTS ルータ のグローバル IP アドレス（GA2）が返信される．

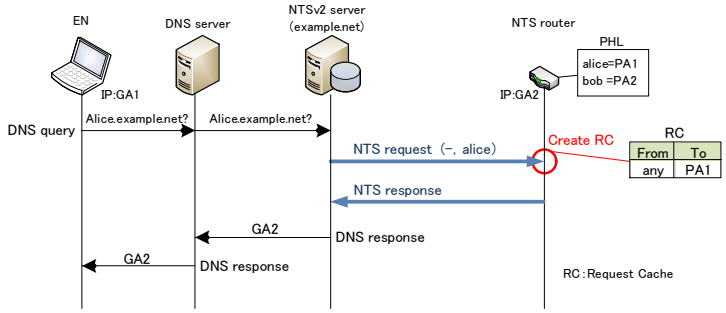


図 5 NTSSv2 の名前解決シーケンス

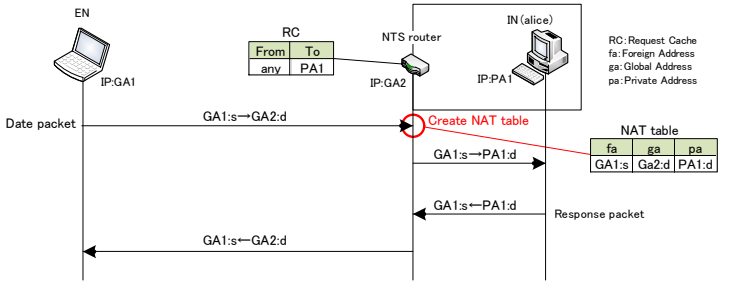


図 6 NTSSv2 の通信開始シーケンス

3.3 通 信 開 始

図 6 に NTSSv2 の通信開始シーケンスを示す．EN は名前解決後，NTS ルータに向けて通信を開始する．NTS ルータはデータパケットを受け取ると，既に生成されている RC の内容を参照する．RC の送信元 IP アドレスの部分が“any”なので，送られてきたパケットの送信元 IP アドレス（GA1）を抽出し，“GA1”をソースアドレスとする NAT テーブルを生成する．以後の処理は NTSS と同様にして，EN と IN の通信が開始される．

3.4 同時問合せ時の動作

同時問合せとは，2 つ以上の EN がほぼ同時に名前解決を開始し，NTS ルータに対して通信開始する場合を示す．この場合，ネットワークの遅延などの影響でパケット到着順が変わると，宛先を誤って NAT テーブルを生成してしまう可能性がある．これは，RC の送

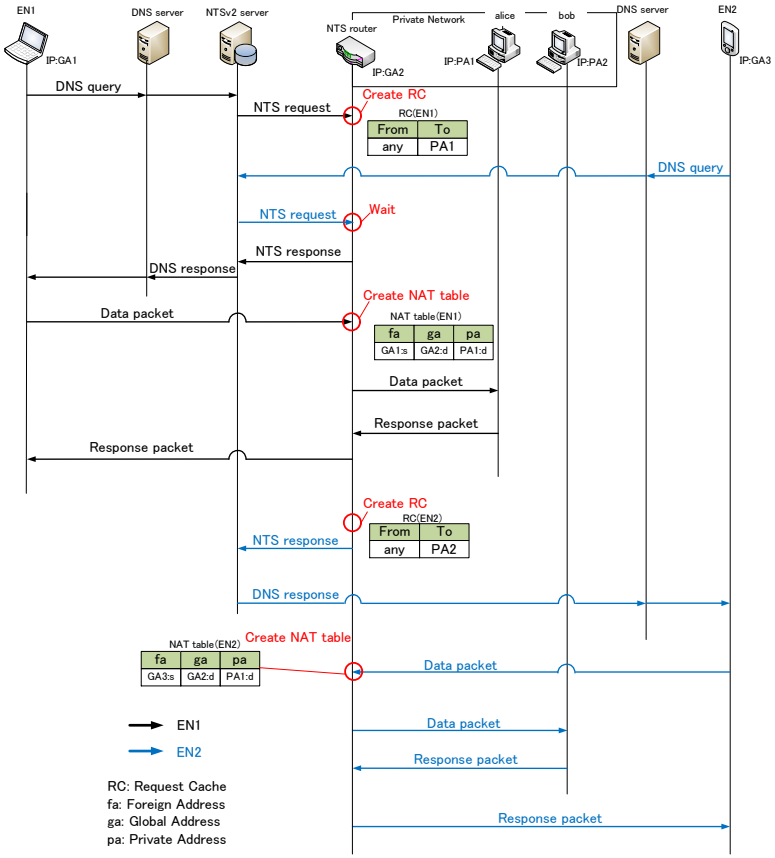


図 7　同時問合せ時の動作シーケンス

信元 IP アドレスが“ any ”のため発生する問題である．この問題を解決するために，NTS ルータは処理をシリアライズする．

図 7 に NTSSv2 の同時問合せ時のシーケンスを示す．EN1 が alice，EN2 が bob と通信を行いたい場合を例として説明する．EN1 が名前解決を行うと，NTS ルータに EN1 の NTS リクエストが届く．NTS ルータは alice と“ any を ”対応付けた RC を生成する．図 7 では，直後に EN2 からの問い合わせで EN2 の NTS リクエストが届いているが，NTS ルータはこのリクエストを待機状態とし，RC は生成しない．EN1 からのデータパケットが到着して EN1 のテーブルが完成した時点で EN2 の RC を生成し，NTS レスポンスを返信する．この他の問合せ要求があっても同様に先着順で待機させる．このように，NTS ルータは NTS リクエストを先着順で処理することにより，同時問合せに対応することができる．DNS 問合せに対する処理が遅れる可能性があるが，既に NAT テーブルが生成されている通信には全く影響しない．

3.5　通信の妨害に対する処置

通信の妨害とは，EN1 の通信開始シーケンスに EN2 の通信開始シーケンスが介入する場合を示す．この場合，EN2 のデータパケットが EN1 より先に NTS ルータに到着すると，RC が削除される可能性がある．これは，NTSS では NAT テーブルを生成した時点で削除していたため発生する．この問題を解決するために，NTS ルータは NAT テーブルを生成した時点で RC を削除せず，所定の時間保持しておく．

図 8 に第三者による通信の妨害を示す．EN1 が alice に通信を行いたい時，第三者である EN2 が通信に介入した場合を例として説明する．EN2 は NTS ルータの IP アドレス（GA2）を既に知っているものとする．EN1 は名前解決により NTS ルータの IP アドレス（GA2）を取得し．NTS ルータにデータパケットを送信する．このとき，図 8 のように EN2 は NTS ルータにデータパケットを送信する．NTS ルータはパケットを受け取ると EN1 用，EN2 用の NAT テーブルをそれぞれ生成する．EN1 と EN2 は両者とも NAT を越えて通信することができる．この方法では，EN1 による不正パケットが内部ネットワークに流れることになるが，EN1 による正常な通信が阻害されることはない．

NAT はその仕様上，ネットワーク構成が外部ネットワークから見えなくなる性質があるので，NAT をセキュリティ装置として考える場合がある．この観点から見ると図 8 に示す方法は，不正なパケットをネットワーク内部に流すことになるため，セキュリティホールになるという指摘がある．しかし，NAT は本来 IPv4 アドレス枯渇に対処するためのものであり，セキュリティは IN のパーソナルファイアウォールなどの別の方法でも確保することできる．また，NAT が存在しないネットワークの場合，不正なパケットは IP アドレスを直接指定して送信することができるため，不正なパケットが送られて来ることはありうる．このように，NTSSv2 は NAT 越えを実現するのが目的であるため，図 8 のようなケースが問題になる場合は別の手段で対策をとる必要がある．

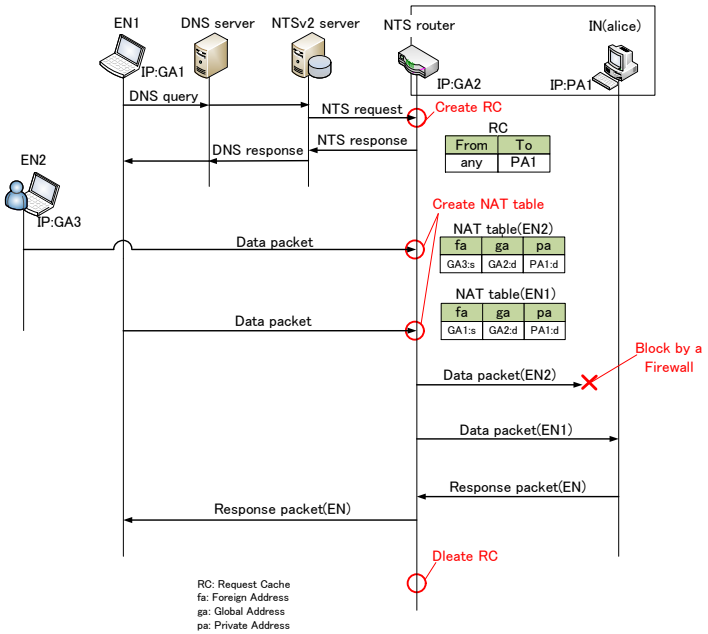


図 8　第三者による通信の妨害

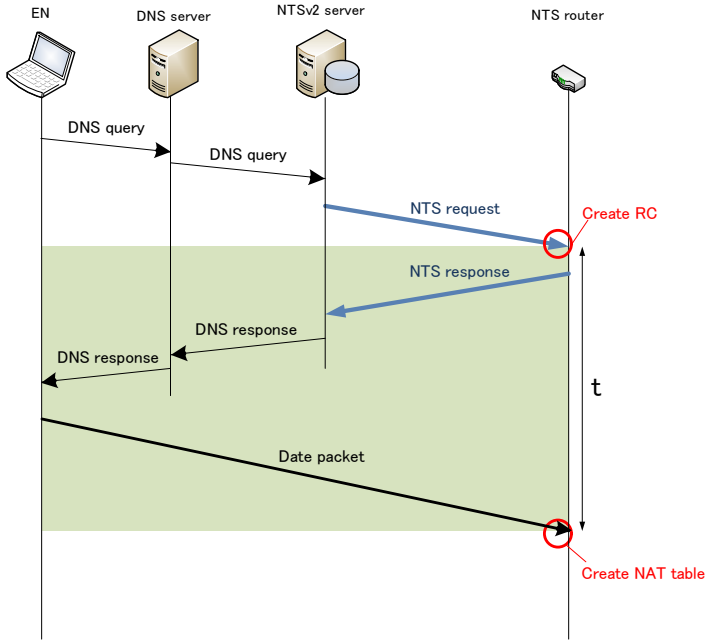


図 9　DNS 問合せに要する時間

4. NTS ルータの負荷予測

NTS ルータの NAT テーブル生成処理をシリアライズしたため，この処理が NTSSv2 のネックになる懸念がある．そこで NTS ルータの負荷予測を行った．この時間と DNS 要求のタイムアウト値から，NTS ルータの処理負荷を予測する．ここでいう NTS ルータの処理負荷とは，NTS ルータが同時にどのくらいの NTS リクエストを待機させることができるかを表す．

図 9 に NTSSv2 における DNS 問合せに要する時間を示す．EN と DNS サーバ，および NTSv2 サーバと NTS ルータは近隣のネットワークに設置できるものとする．図中のハッチング部分は他のリクエストを処理できないため，1 回のリクエストに対する NTS ルータの処理時間に相当する時間とし，この時間を t とする．また，EN は名前解決後，即座に通信開始することを前提とする．

NTSS の測定結果によると，NTSS の処理に要する時間は NTS サーバで 360.2 μ s，NTS ルータで 265.2 μ s であった．NTSSv2 では処理内容が大きく変わることがないので，同等の時間を要するものと想定できる．一方，実際のシステムにおいて ping の RTT を測定すると 10ms〜400ms ぐらいである．この値は NTSS の処理時間に比べて大きな値と言える．このようなことから，NTSS の処理時間は無視できる程小さいと考えられるので，t の値は RTT により見積ることができる．DNS タイムアウトをデフォルトの 5s，EN と NTS ルータ間の RTT を 20ms とすると，同時に 250 個までの DNS リクエストを処理できることになる．

実際には，DNS タイムアウト及び RTT は各々の環境により異なるので，正確な性能値を示すことはできない．しかし，RTT は RC の保持時間と見積もることができるため，最

悪値をとる必要がある．また，一般ユーザが DNS タイムアウトをデフォルトより低く設定を変える可能性は考えられないため，値はあらかじめ予想できる．そのため，事前に NTS ルータの負荷予測が可能となる．

5. ま と め

NTSS は EN の改造が不要であるが，設定の変更が必要であった．そこで，設定変更を無くすために，IN を管理する DDNS サーバを NTSv2 サーバとして改造した NTSSv2 を提案した．NTSSv2 サーバが受信する DNS 問合せにはノードの情報が含まれていないため，EN の IP アドレスを特定することができない．そこで，NTS ルータは送信元 IP アドレスを“ any ”とし，これを宛先と対応付けした RC を生成をすることにより，NTS ルータはデータパケットはデータパケットを受け取ると，送られてきたパケットの送信元 IP アドレスを抽出し，それをソースアドレスとする NAT テーブルを生成する．これにより，NTSS と同様の通信を可能とした．また，同時問い合わせや通信の妨害時の動作を再検討することにより問題にならないとした．今後は，NTSSv2 の実装を完成し評価を行う予定である．

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) 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).
4) Rosenberg, J., Mahy, R., Matthews, P. and Wing, D.: Session Traversal Utilities for NAT (STUN), RFC 5389, IETF (2008).
5) Rosenberg, J., Mahy, R. and Matthews, P.: Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN), Internet-draft, IETF (2009). http://tools.ietf.org/id/draft-ietf-behave-turn-16.txt
6) UPnP Forum: Internet Gateway Device (IGD) *Italic Standardized Device Control Pro- tocol V 1.0* (2001). http://www.upnp.org/standardizeddcps/igd.asp
7) Turanyi, Z., Valko, A. and Campbell, A.: 4+4: An Architecture for Evolving the Internet Address Space Back Toward Transparency,*Italic ACM SIGCOMM Computer Communication Review*, Vol.33, No.5, pp.43-54 (2003).
8) 鈴木秀和，宇佐見庄五，渡邊　晃 : 外部動的マッピングにより NAT 越え通信を実現する NAT-f の提案と実装，情報処理学会論文誌， Vol.48, No.12, pp.3949-3961 (2007).
9) Ng, T., Stoica, I. and Zhang, H.: A Waypoint Service Approach to Connect Heterogeneous Internet Address Spaces, *Italic Proc. USENIX Annual Technical Conference*, pp.319-332 (2001).
10) 宮崎悠，鈴木秀和，渡邊晃．端末の改造が不要な NAT 越え通信システム NTSS の提案と評価, 情報処理学会論文誌, Vol. 51, pp.1873-1880, Sep.2010.

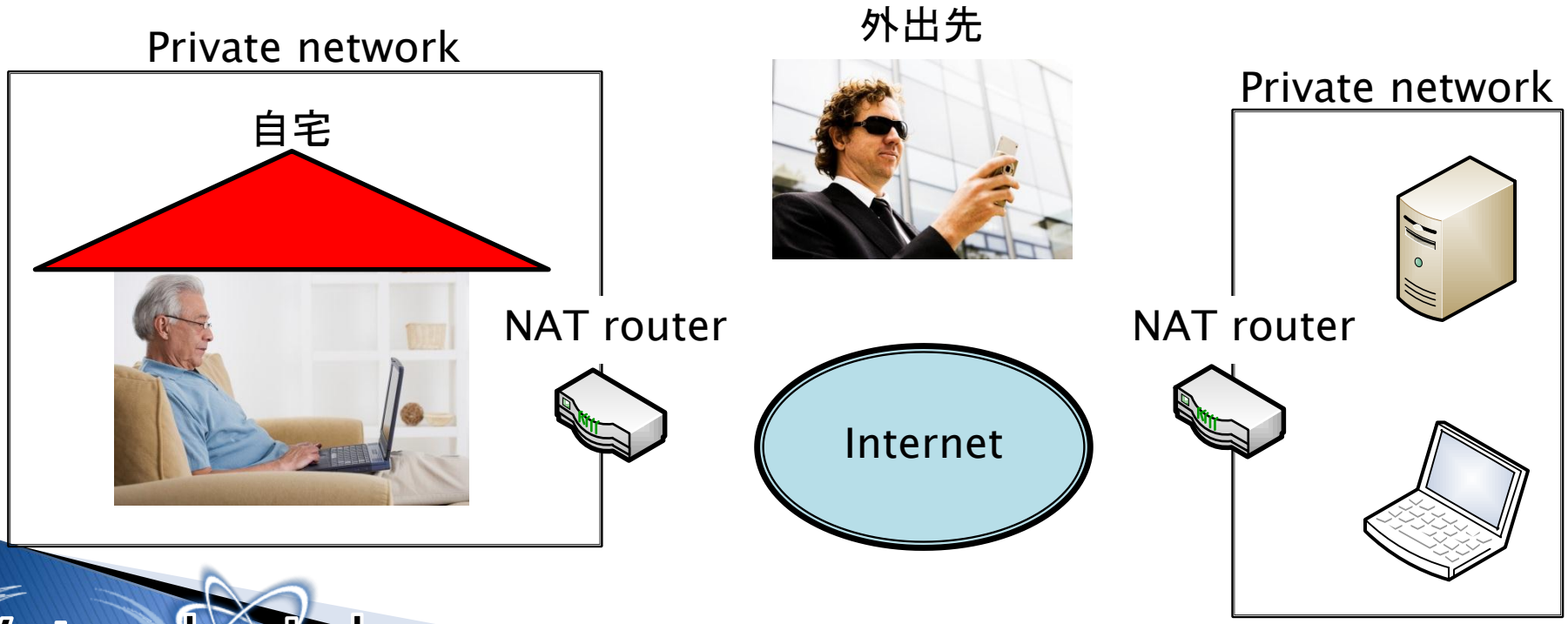
端末の変更が一切不要な NAT越え通信システムの提案

名城大学大学院　理工学研究科
松尾辰也　鈴木秀和　渡邊晃

Watanabe Lab.

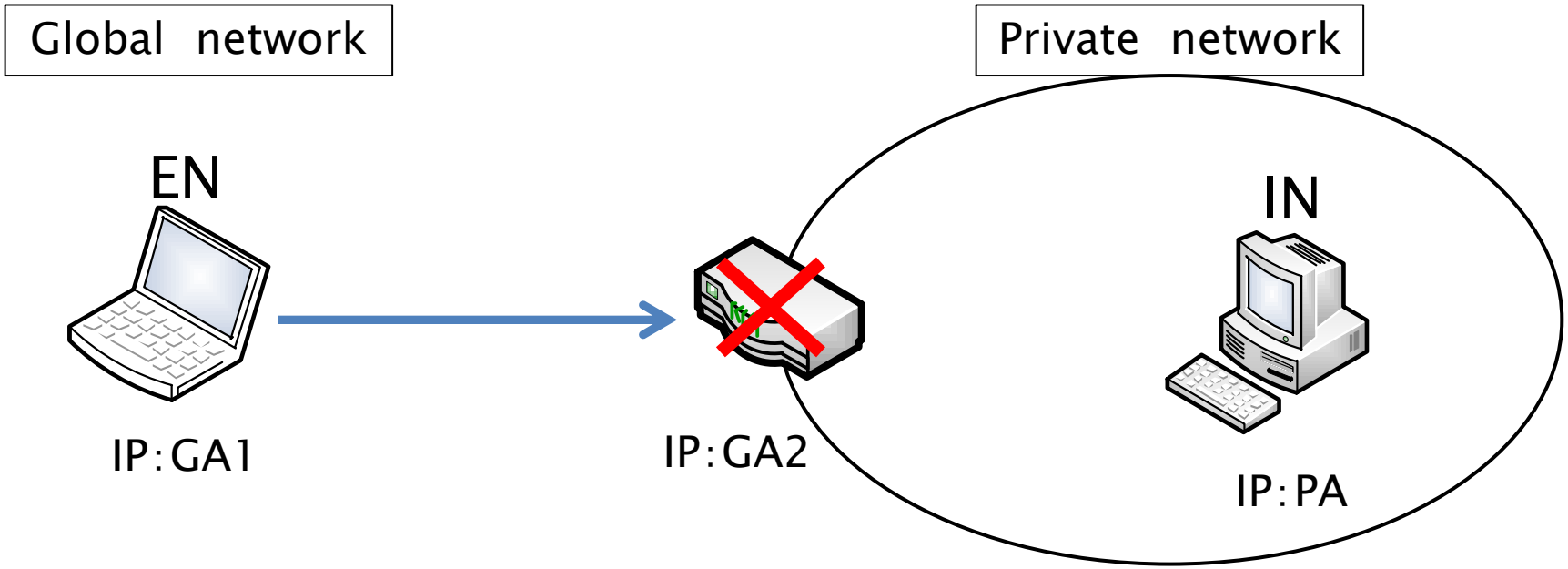
研究背景

- IPv4アドレスの枯渇
  - 現状：NAT(Network Address Translator)を使用
    →ネットワークをプライベートアドレスで構築



NAT越え問題

- インターネット側の端末はプライベートネットワーク内の端末に通信を開始できない



- 外側からはNATのIPアドレスしか見えない

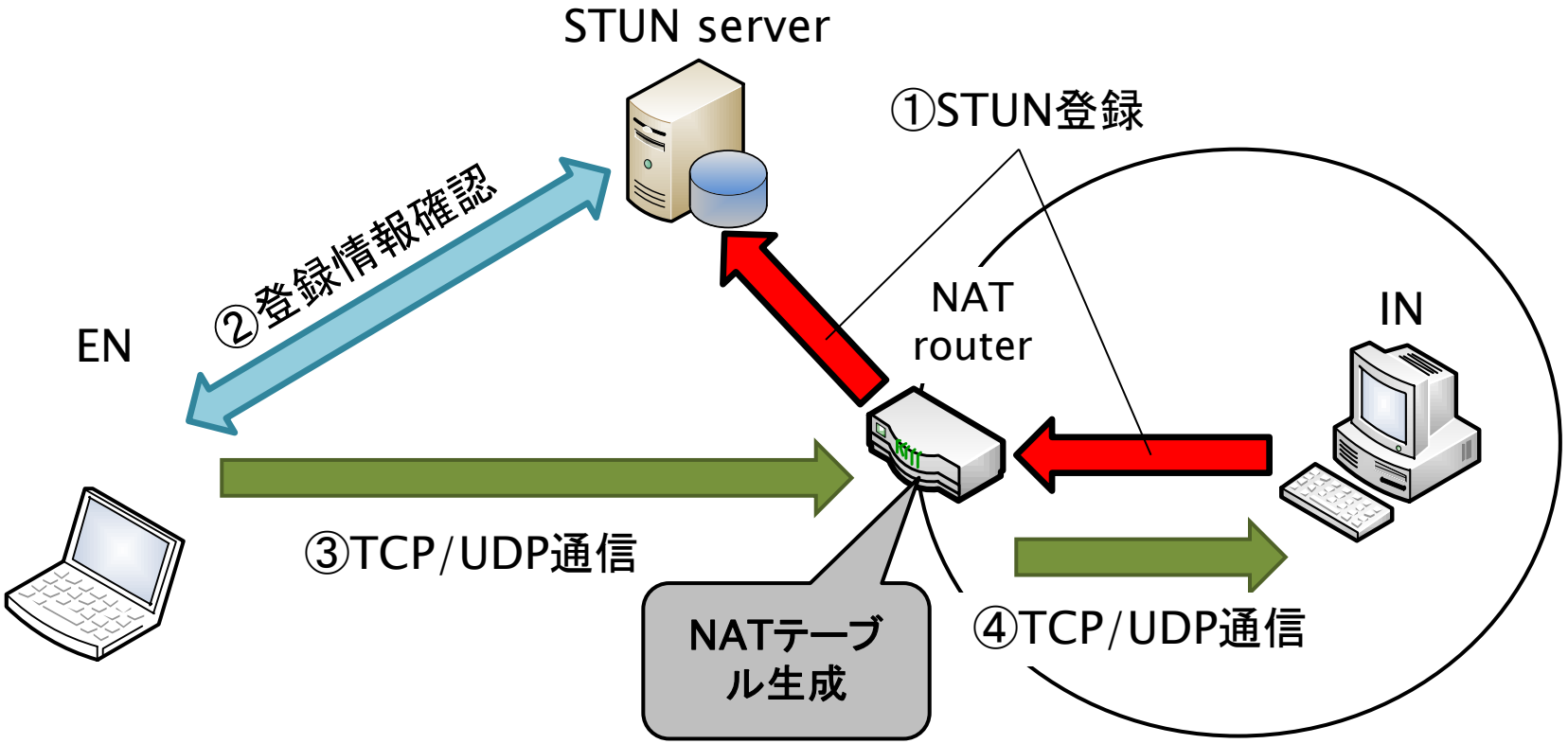
EN(External Node)
IN(Internal Node)

既存のNAT越え技術

- アプリケーションレベル改造方式
- ネットワークレイヤ改造方式
- 端末非依存方式

アプリケーションレベル改造方式

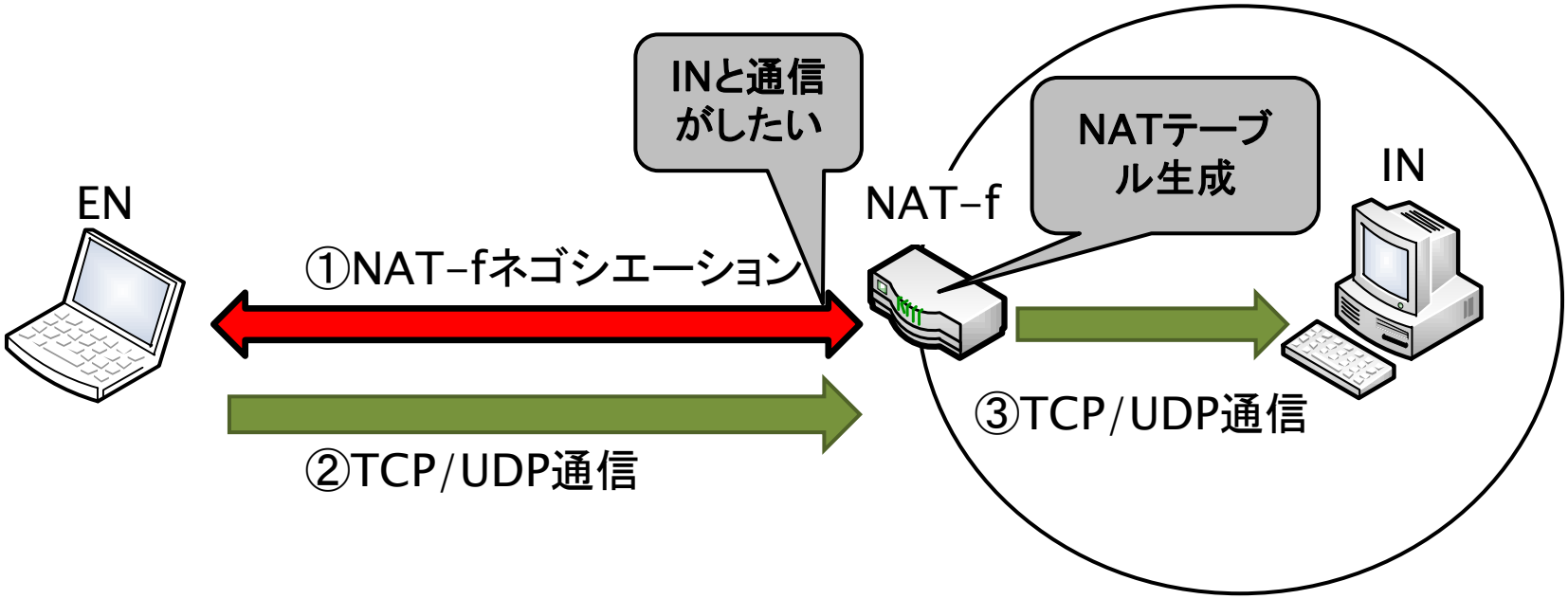
- アプリケーションと第三の装置が協調動作を行う
  - 既存方式：STUN，TURN，UPnP



Rosenberg, J.,Weinberger, J., Huitema, C. and Mahy, R.:
STUN – Simple Traversal of UDP Through NATs,RFC 3489, IETF (2003).

ネットワークレイヤ改造方式

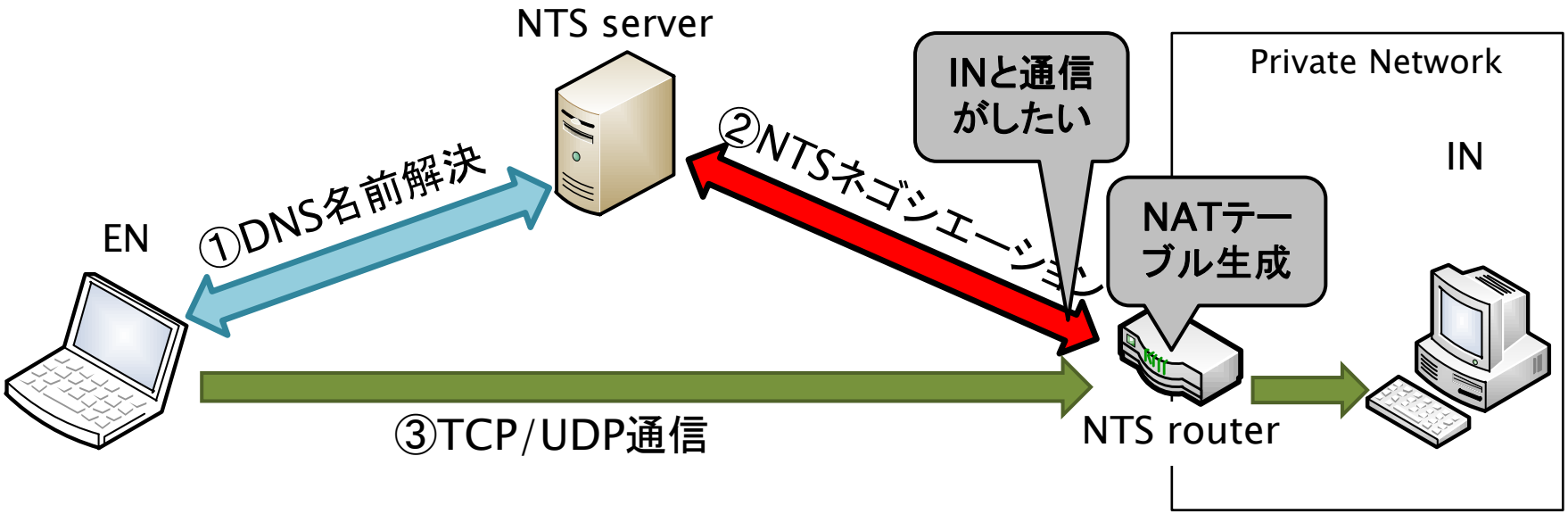
- ENのカーネルやNATルータを改造し，協調動作を行う
  - 既存方式：NAT-f



鈴木，他「外部動的マッピングによりNAT 越え通信を実現するNAT-f の提案と実装」情報処理学会論文誌， Vol.48, No.12, pp.3949-3961 (2007).

端末非依存方式

- DNSサーバ，NATルータなどを改造し，協調動作を行う
  - 既存方式：NTSS，AVES

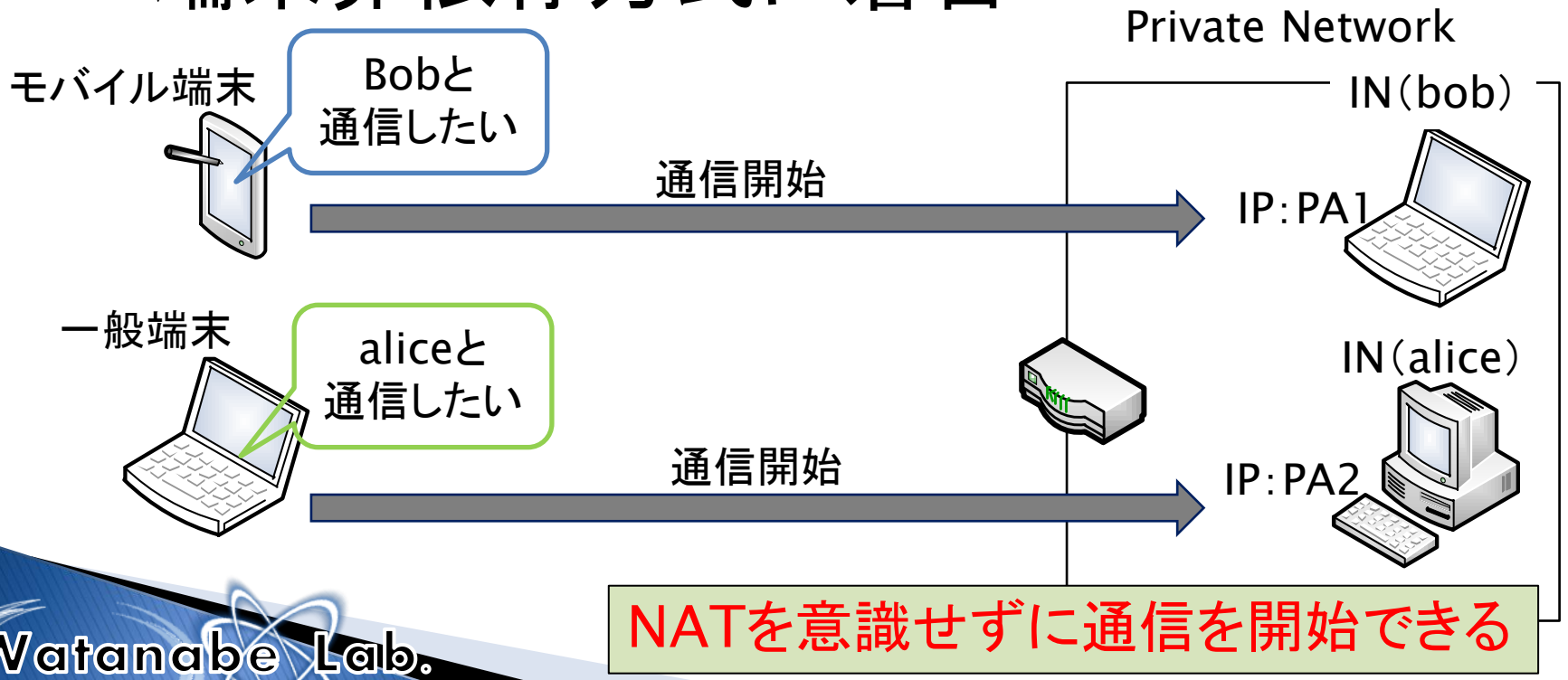


宮崎悠,他「端末の改造が不要なNAT越え通信システムNTSSの提案と評価」情報処理学会論文誌,Vol.51,No.9,pp.1873-1880,Sep.2010.

研究目的

端末に手を加えることなく
NAT越えを実現したい

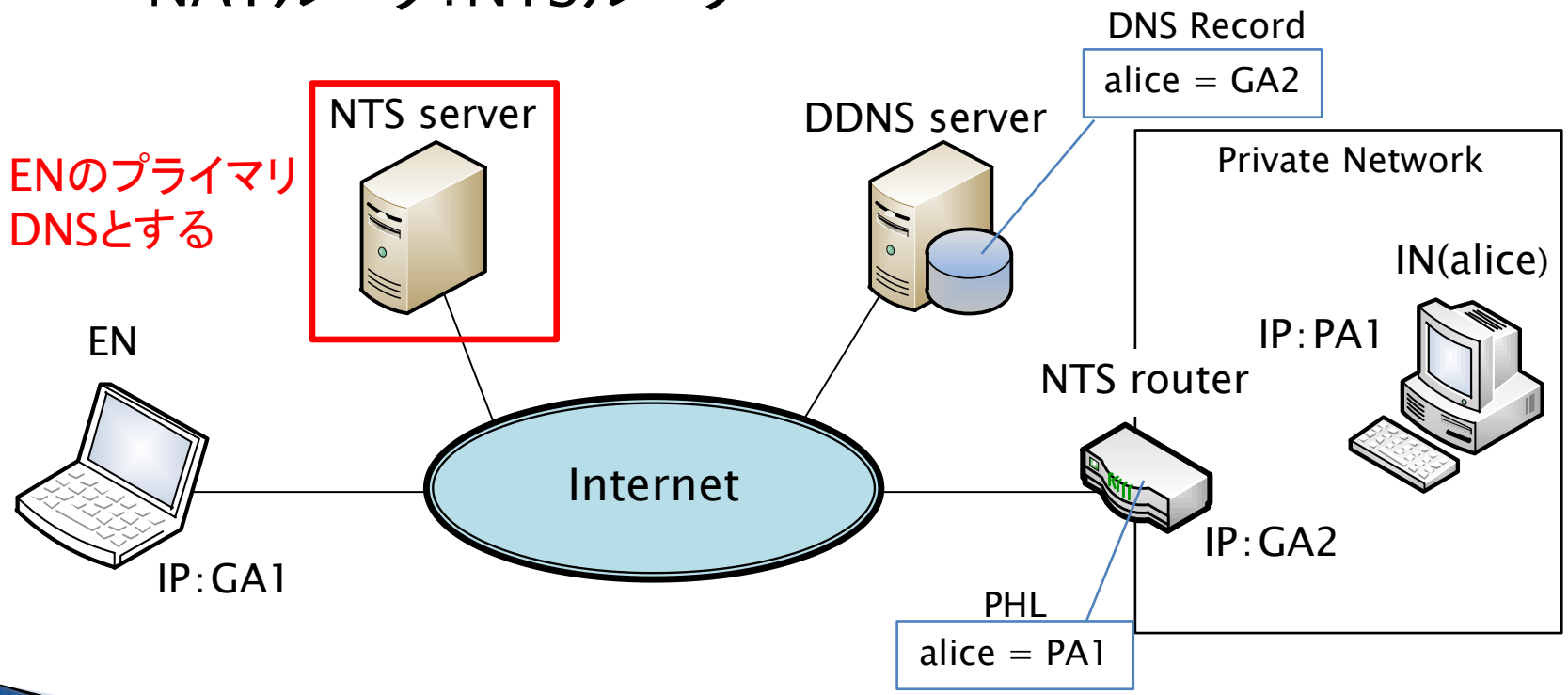
→端末非依存方式に着目



NTSS(NAT Traversal Support System)

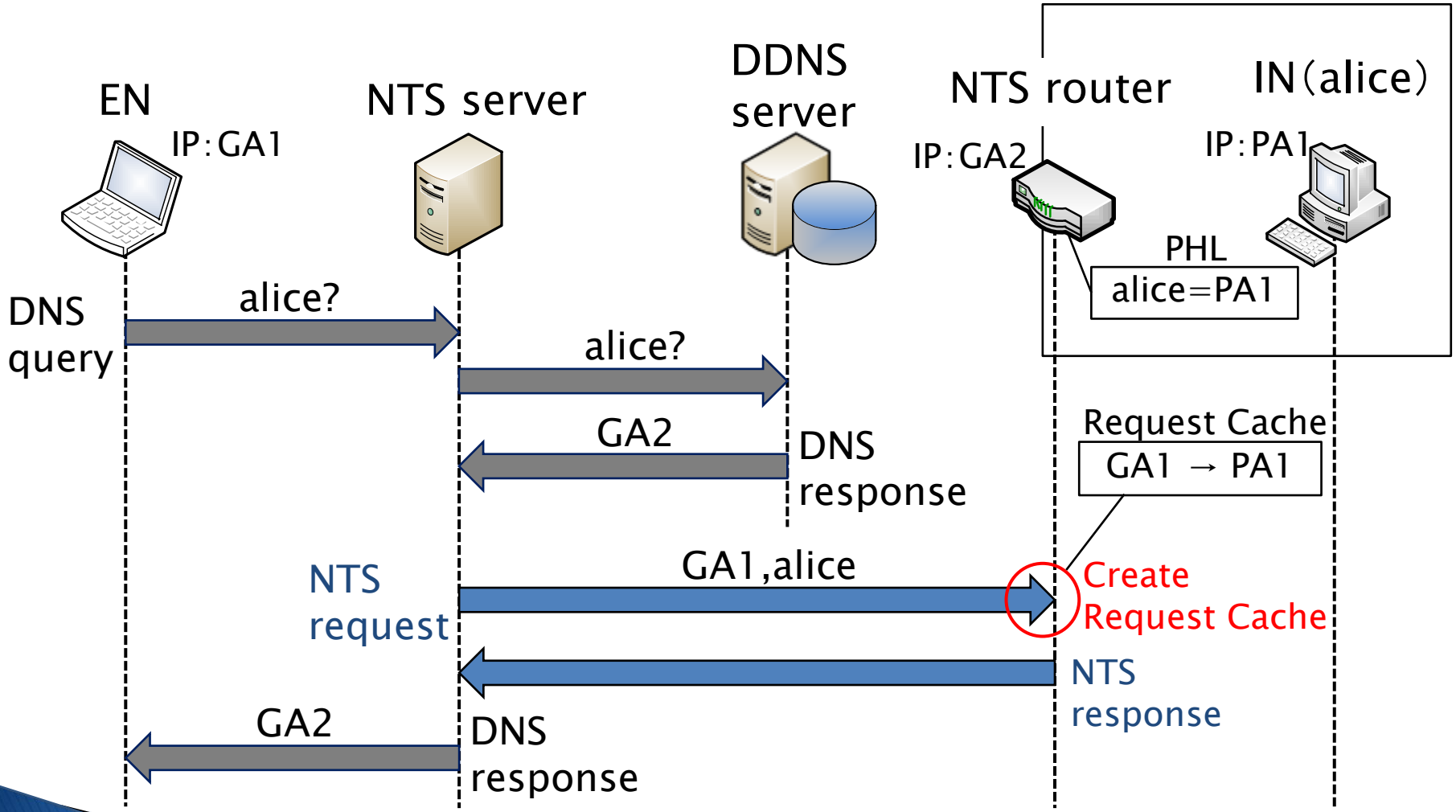
- DNSサーバとNATルータを改造
  - DNSサーバ:NTSサーバ
  - NATルータ:NTSルータ

PHL:Private Host List

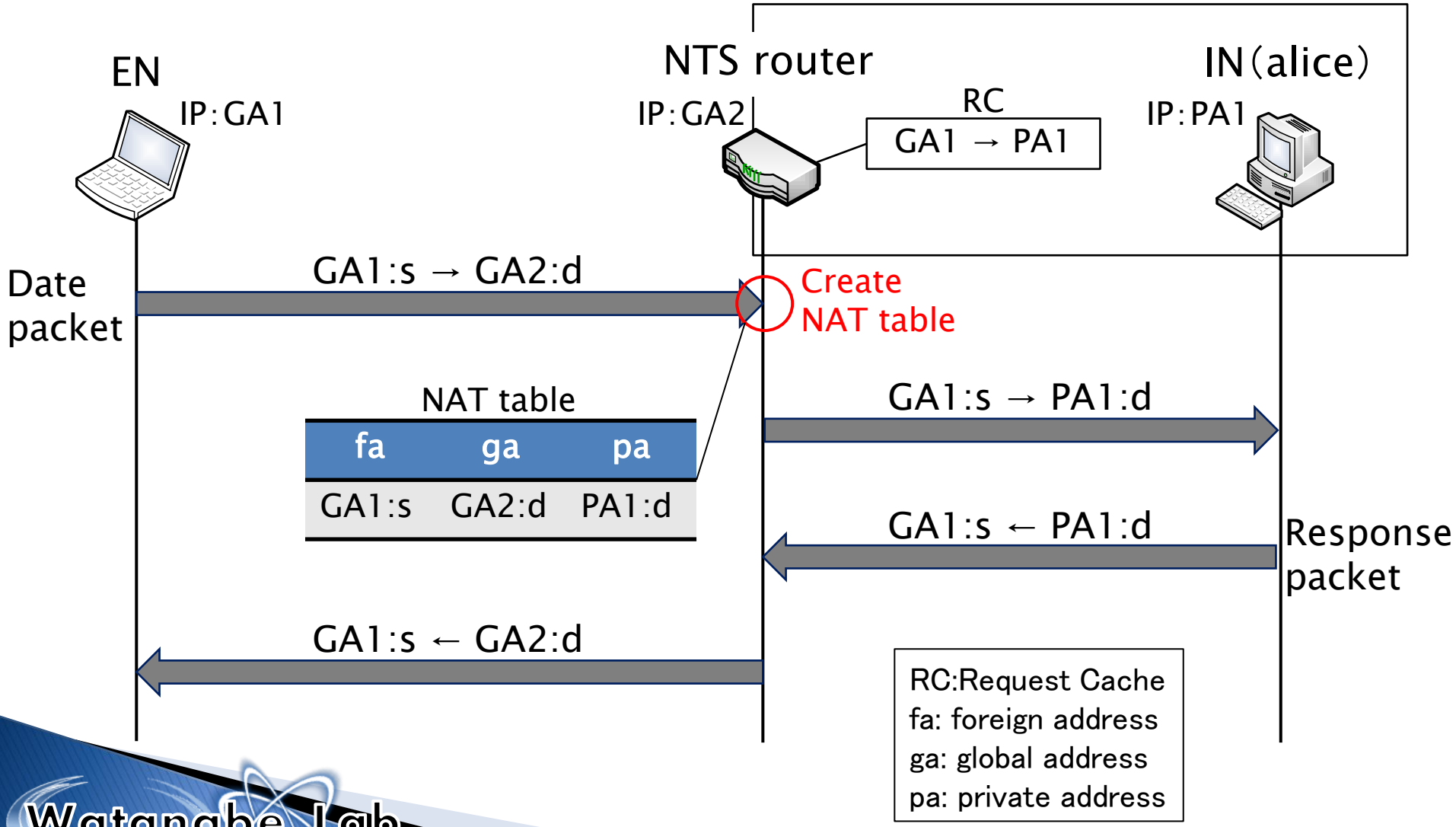


宮崎悠,他「端末の改造が不要なNAT越え通信システムNTSSの提案と評価」情報処理学会論文誌,Vol.51,No.9,pp.1873-1880,Sep.2010.

NTSSの動作(名前解決)



NTSSの動作（通信開始）



NTSSの課題

ENはNTSサーバを常に自身の
プライマリDNSサーバとする必要がある

- 例えば・・・
  - サービスを知らない
  - モバイル端末による移動

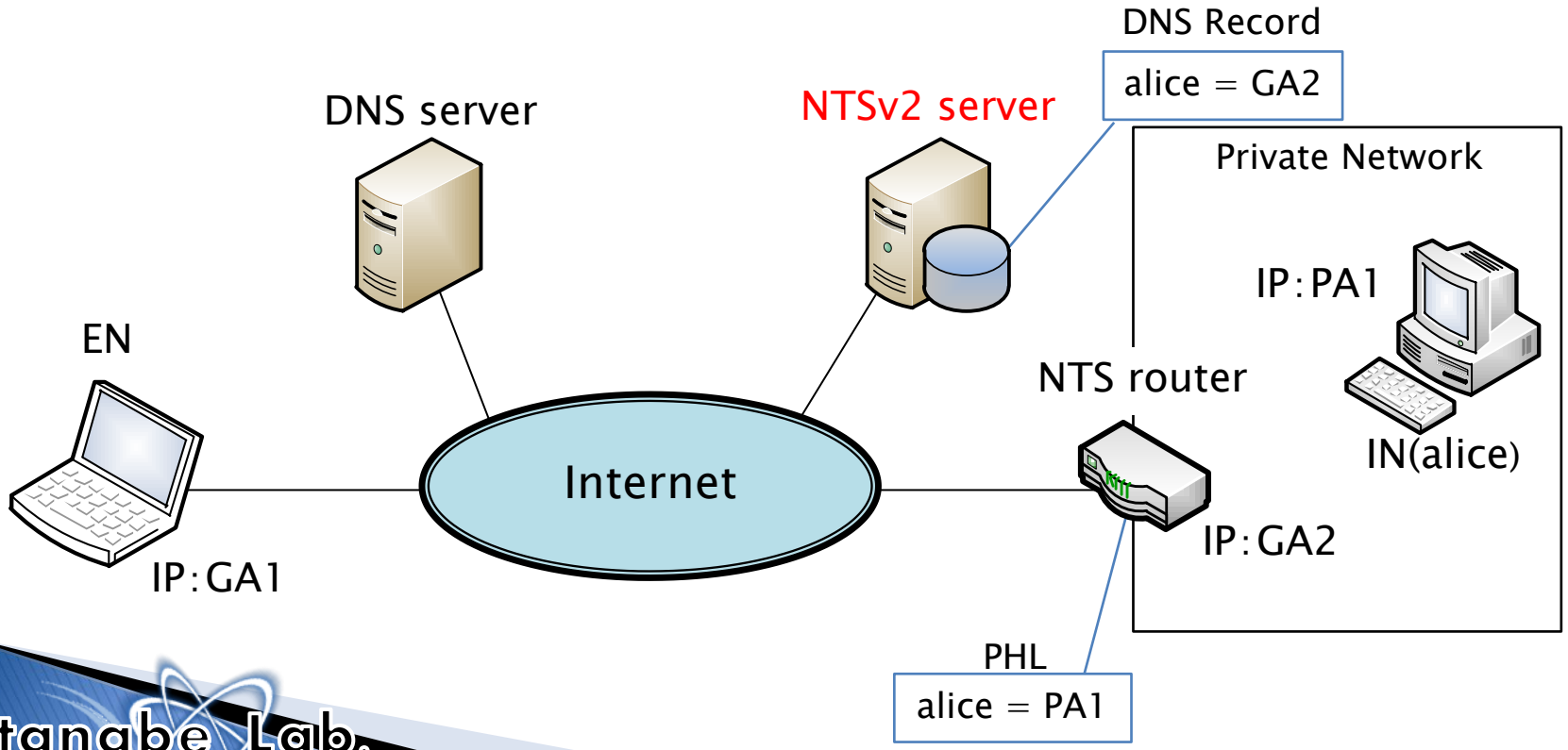
一般ユーザが利用できない可能性がある

提案方式

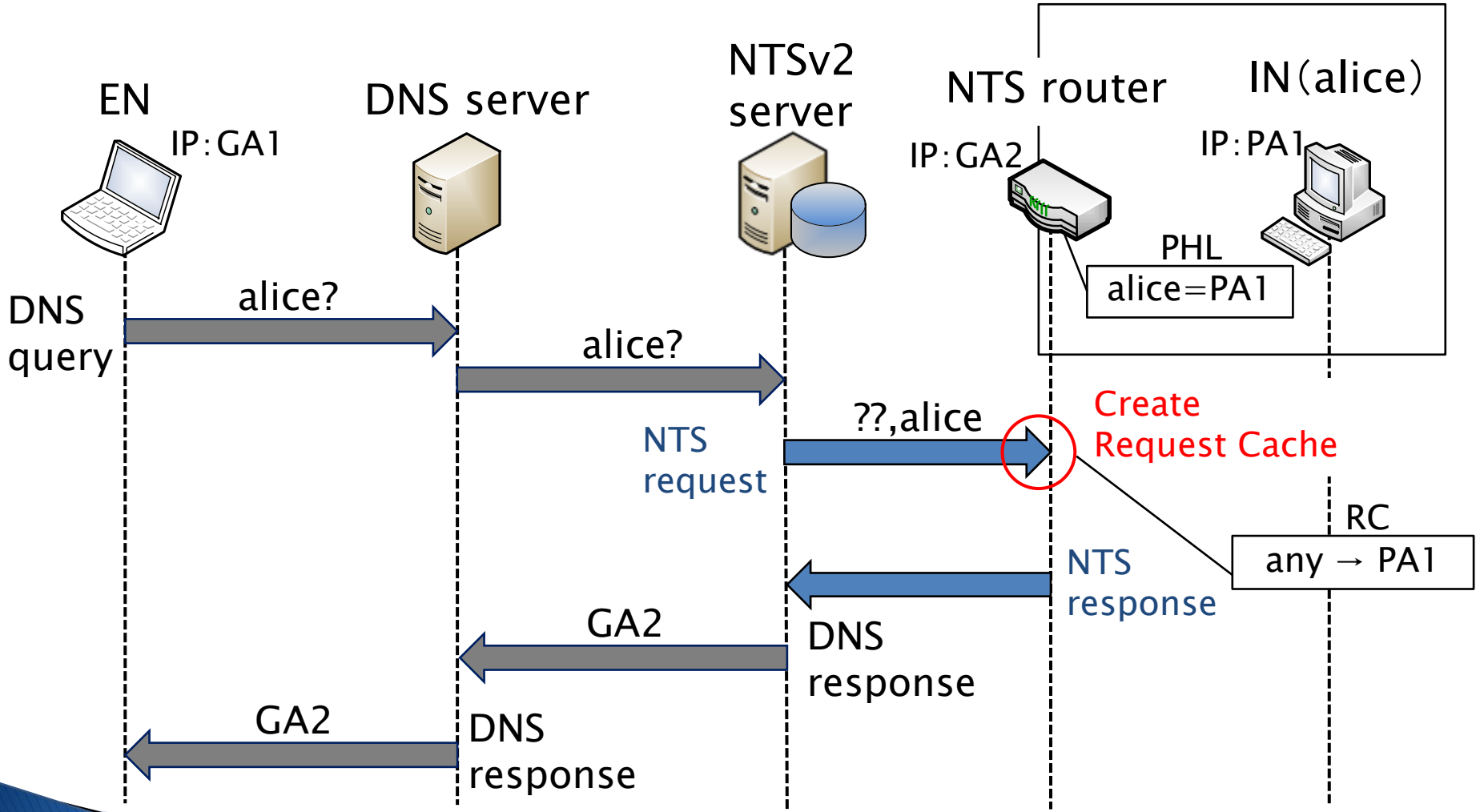
NTSSv2

- NTSSとの違い
  - ENは既存のDNSサーバを利用できる
  - DDNSサーバ：NTSv2サーバ

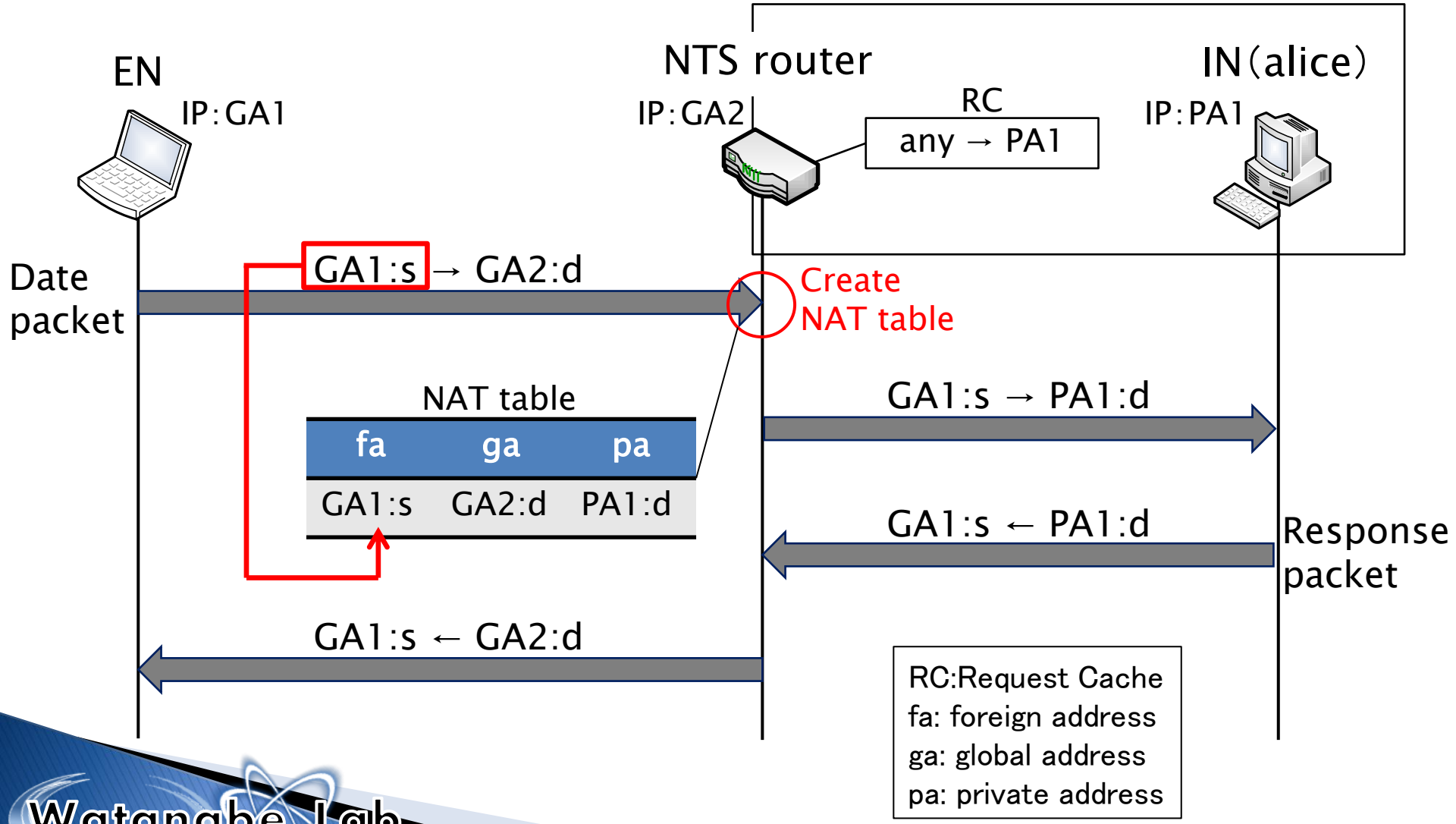
PHL：Private Host List



NTSSv2の動作(名前解決)

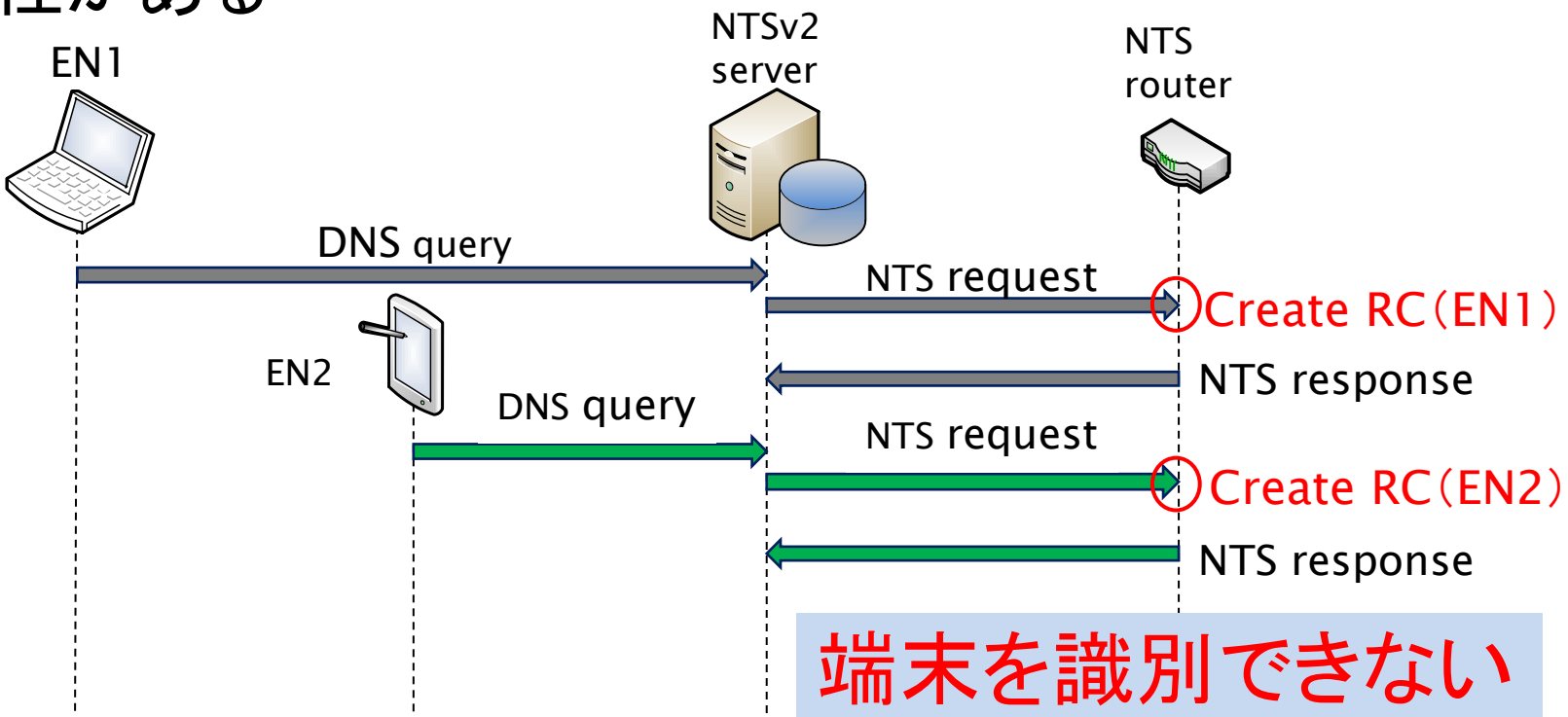


NTSSv2の動作（通信開始）



同時問合せ(1/2)

- ルータにノード情報を通知できないため，経路上の遅延などにより，宛先が違うNATテーブルを生成する可能性がある

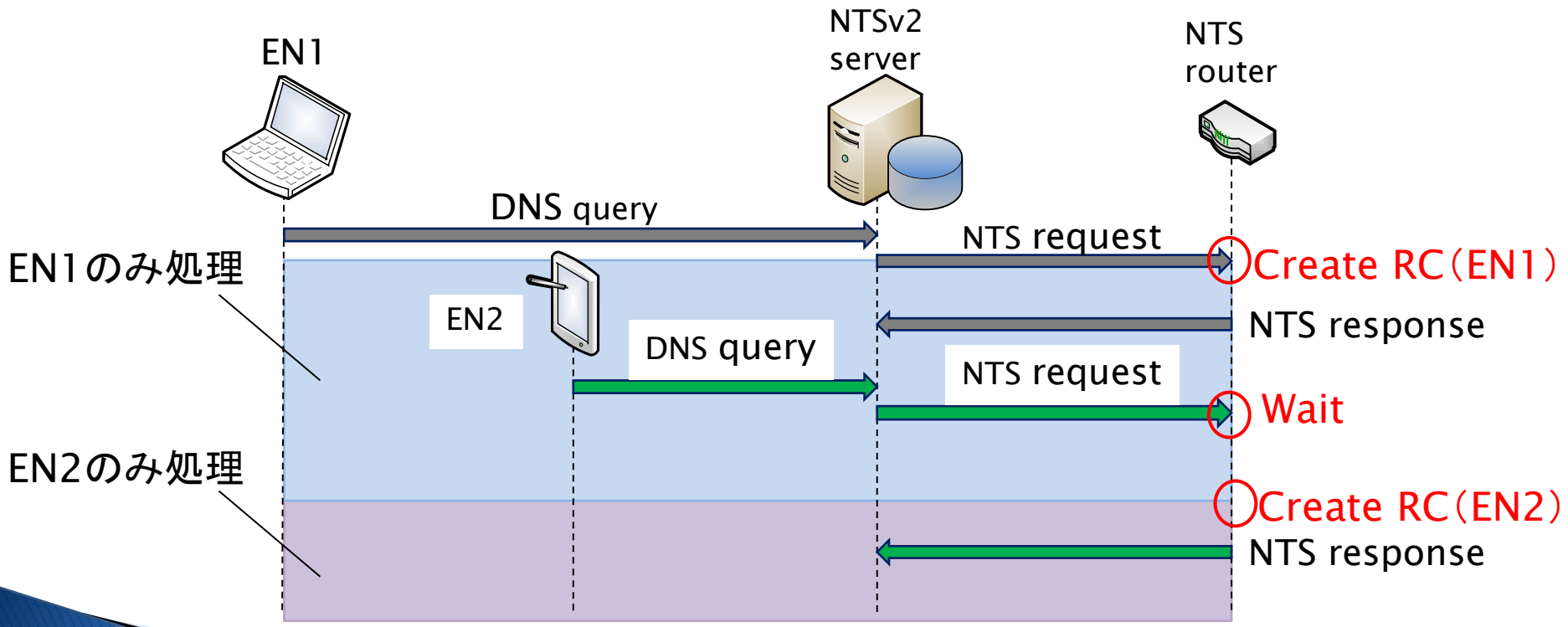


端末を識別できない

一部の処理は省略

同時問合せ(2/2)

- NATがリクエストに対し，シリアライズに処理することで対応

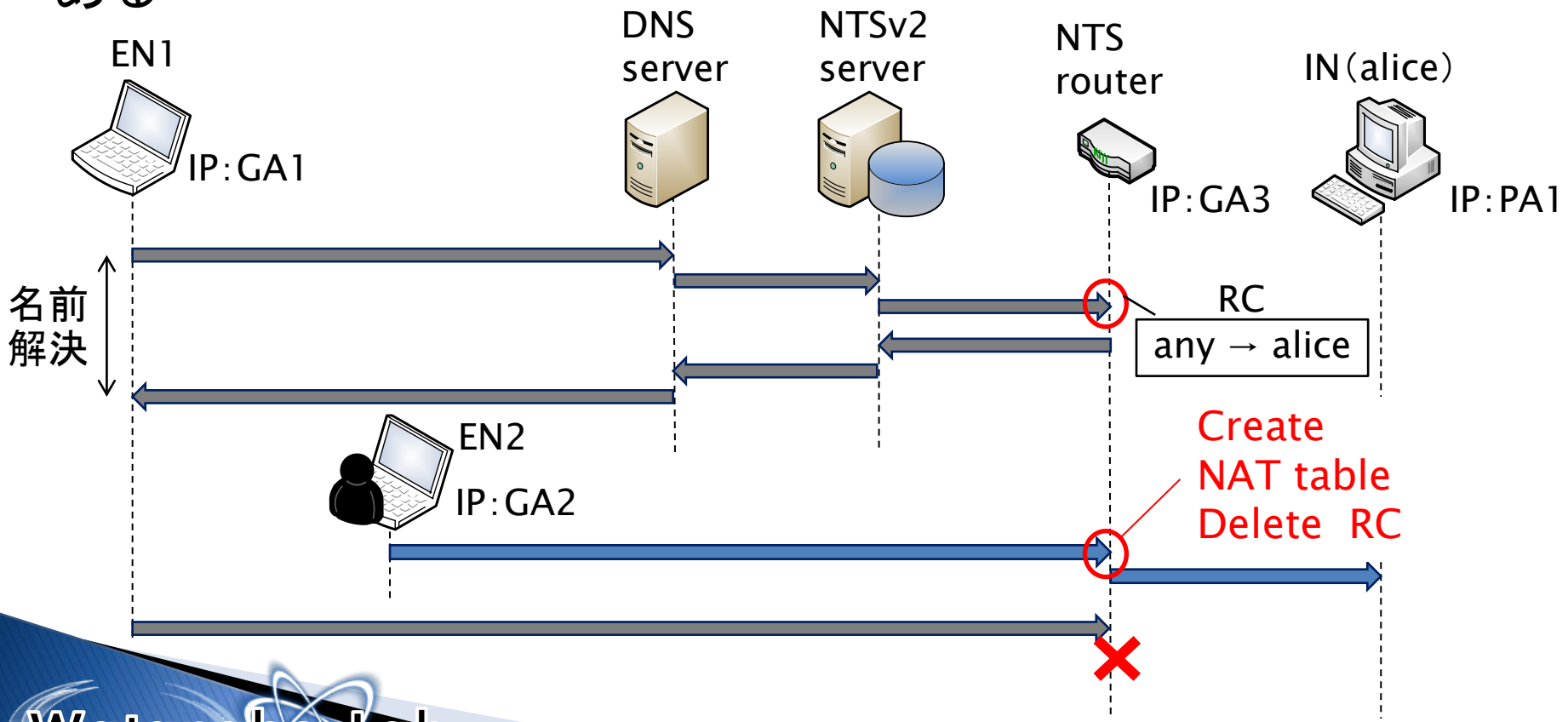


一部の処理は省略

通信妨害(1/2)

- 従来:NATテーブル生成時にRCを削除

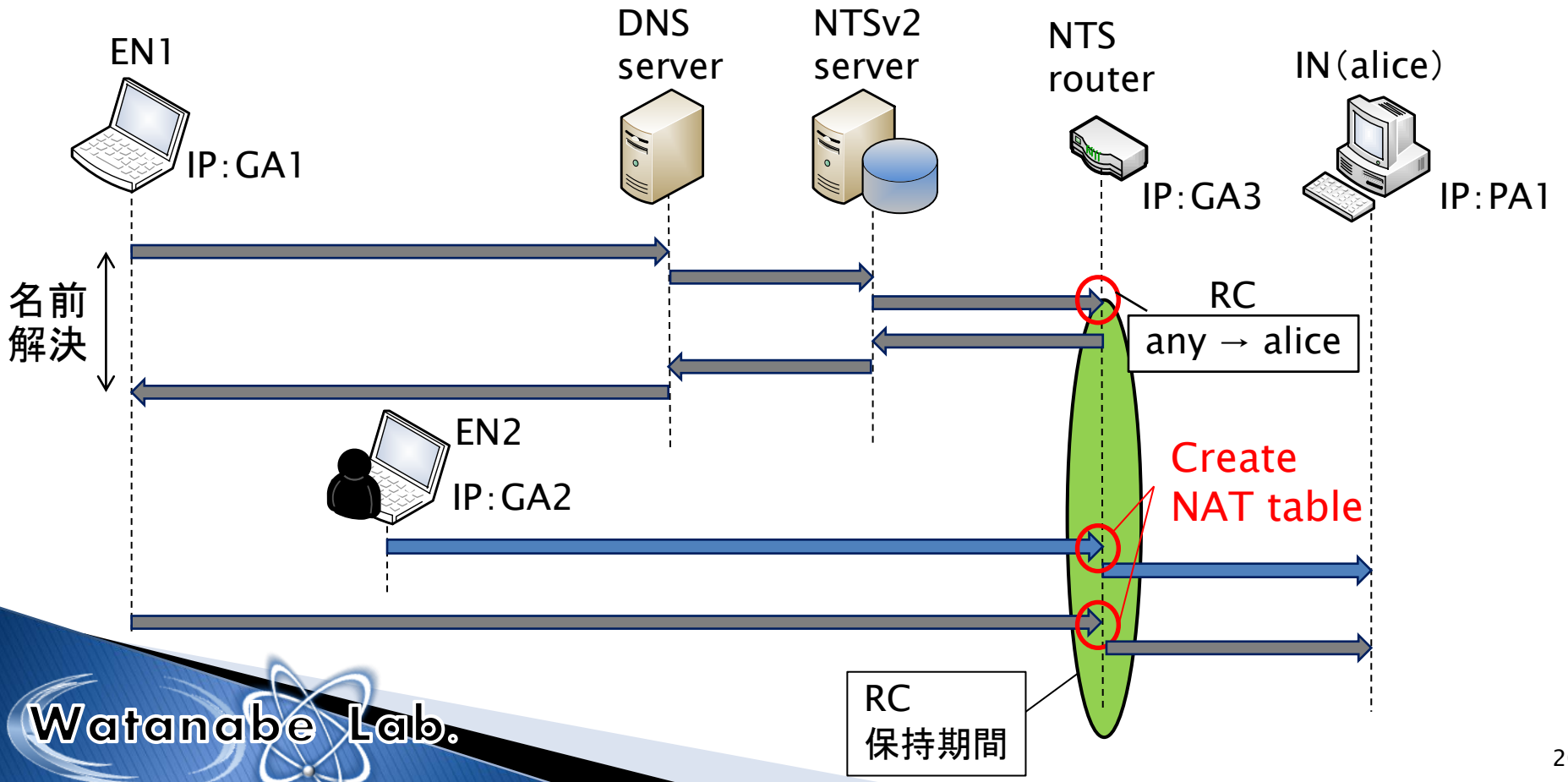
→第三者(EN2)によって，IN宛のRCが削除される可能性がある



通信妨害(2/2)

- 第三者(EN2)によって，IN宛のRCが削除される可能性がある

→RC生成後，一定期間保持することで対応



まとめ

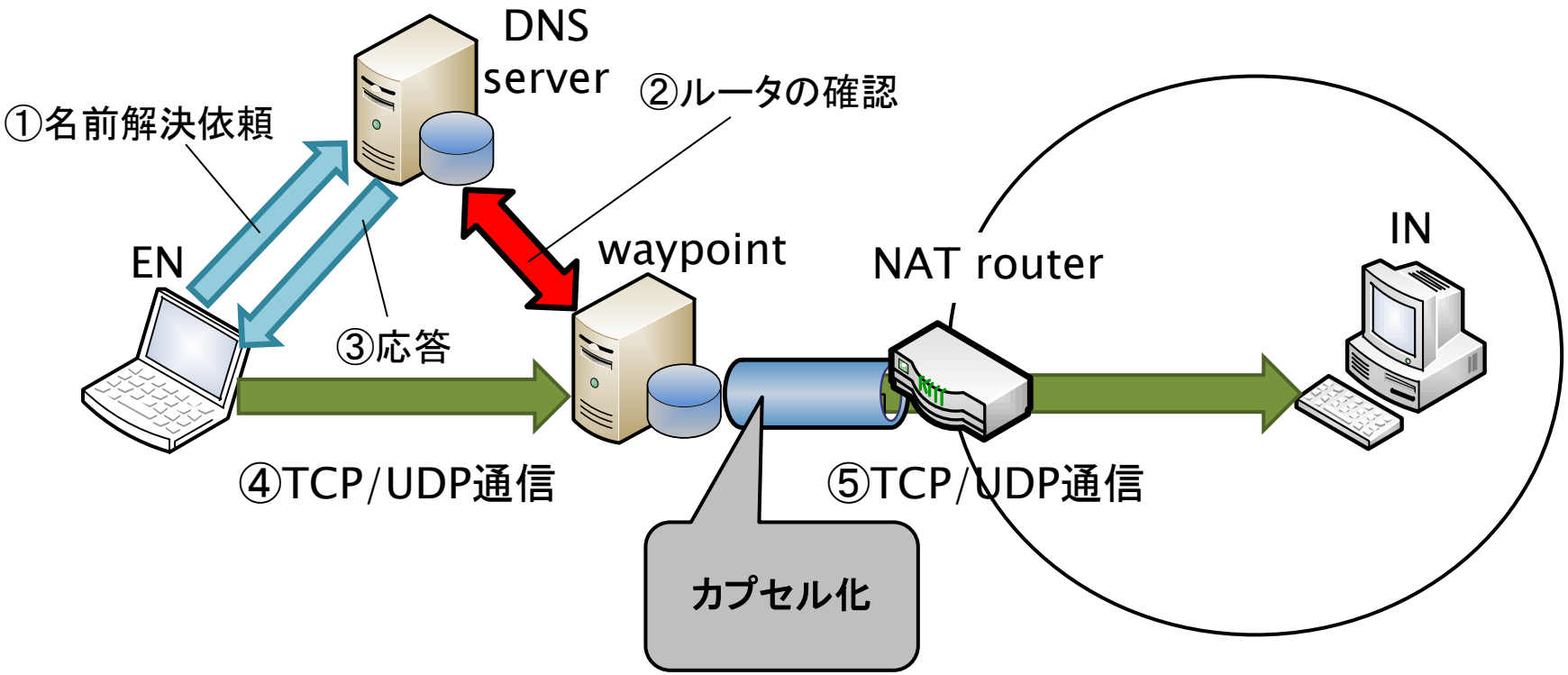
- NTSSを改良したNTSSv2を提案した
- NTSSv2は既存のDNSサーバを利用できるので、一般ユーザが問題なく利用できる．また，ルータの動作変更により、同時問合せと第三者による通信妨害に対応する
- 今後は実装を完了させ，動作確認及び評価を行う予定

ご清聴ありがとうございました

補足

端末非依存方式 -AVES-

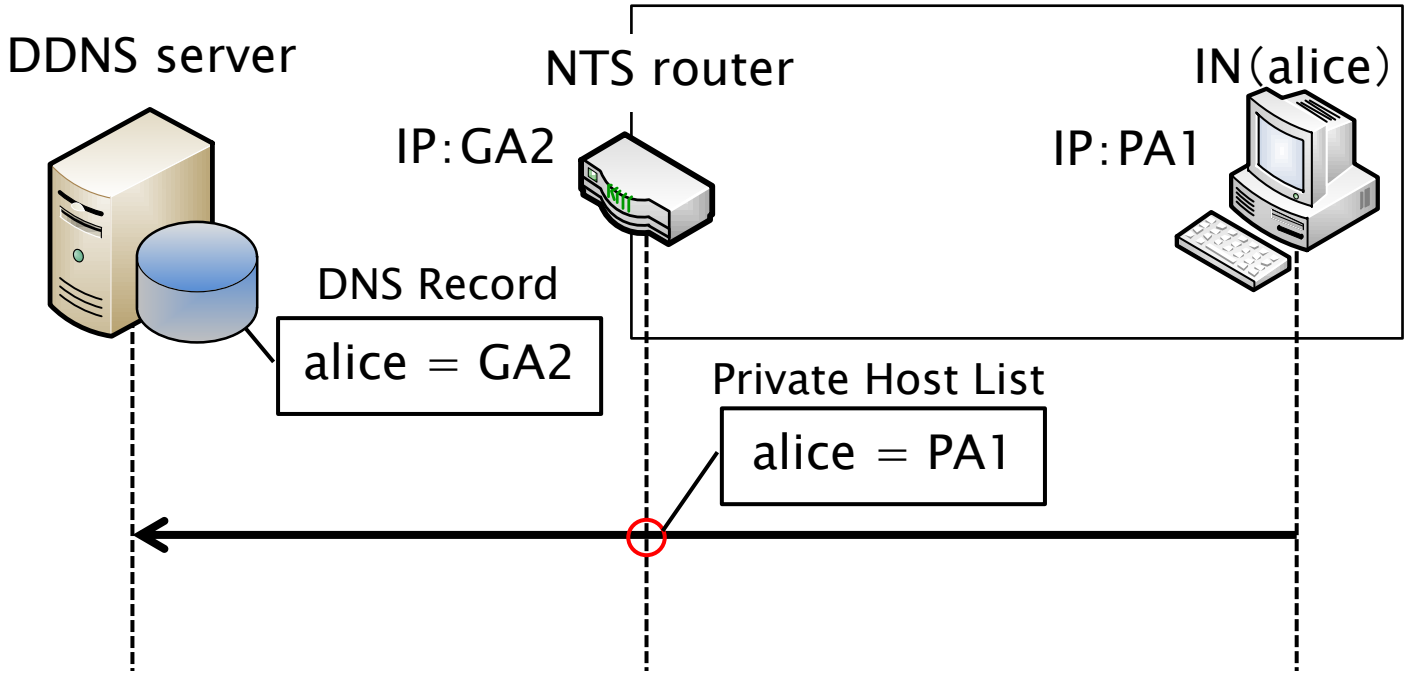
- ENはwaypointを経由してNAT越えを実現



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).

事前設定

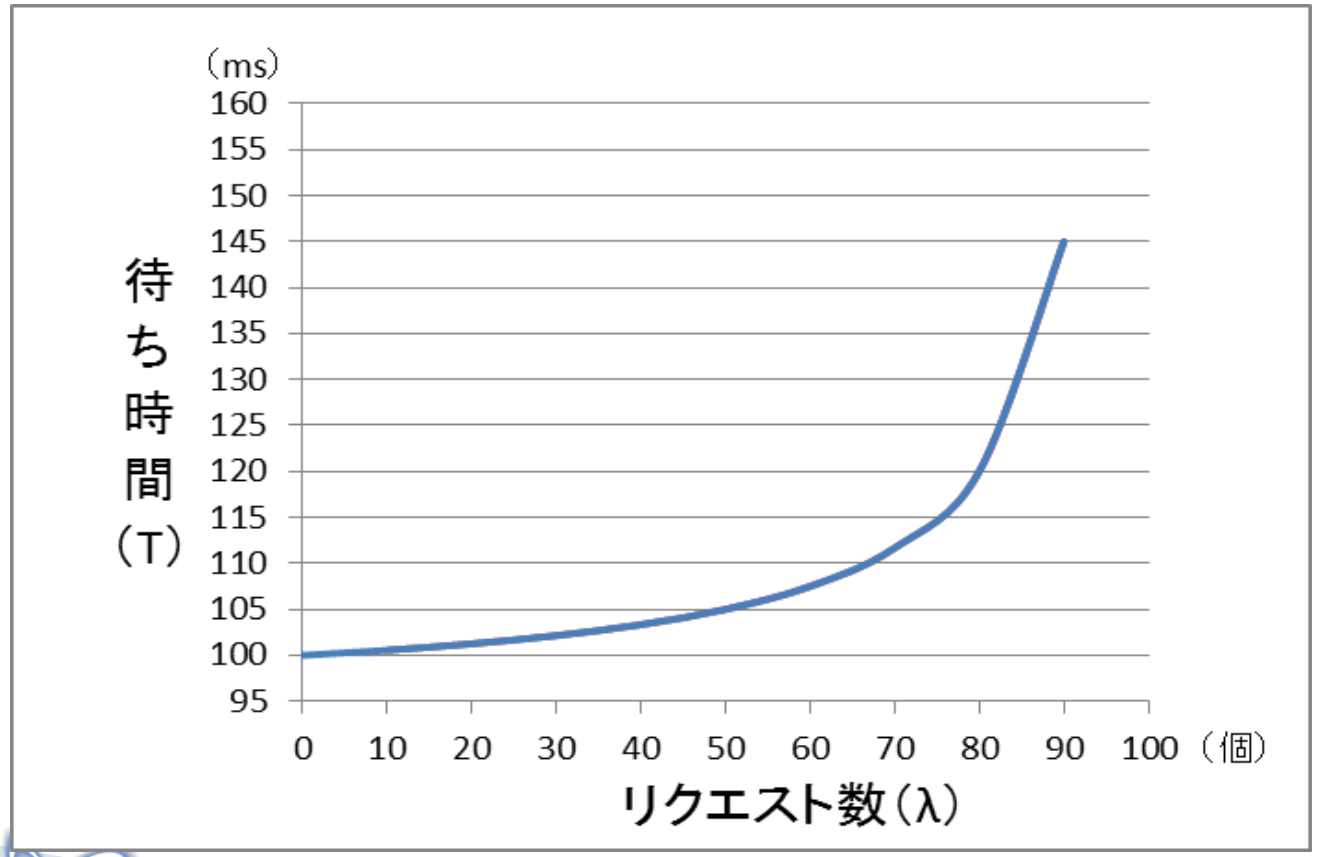
- INのFQDN(alice)とNATルータのIPアドレスを登録



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

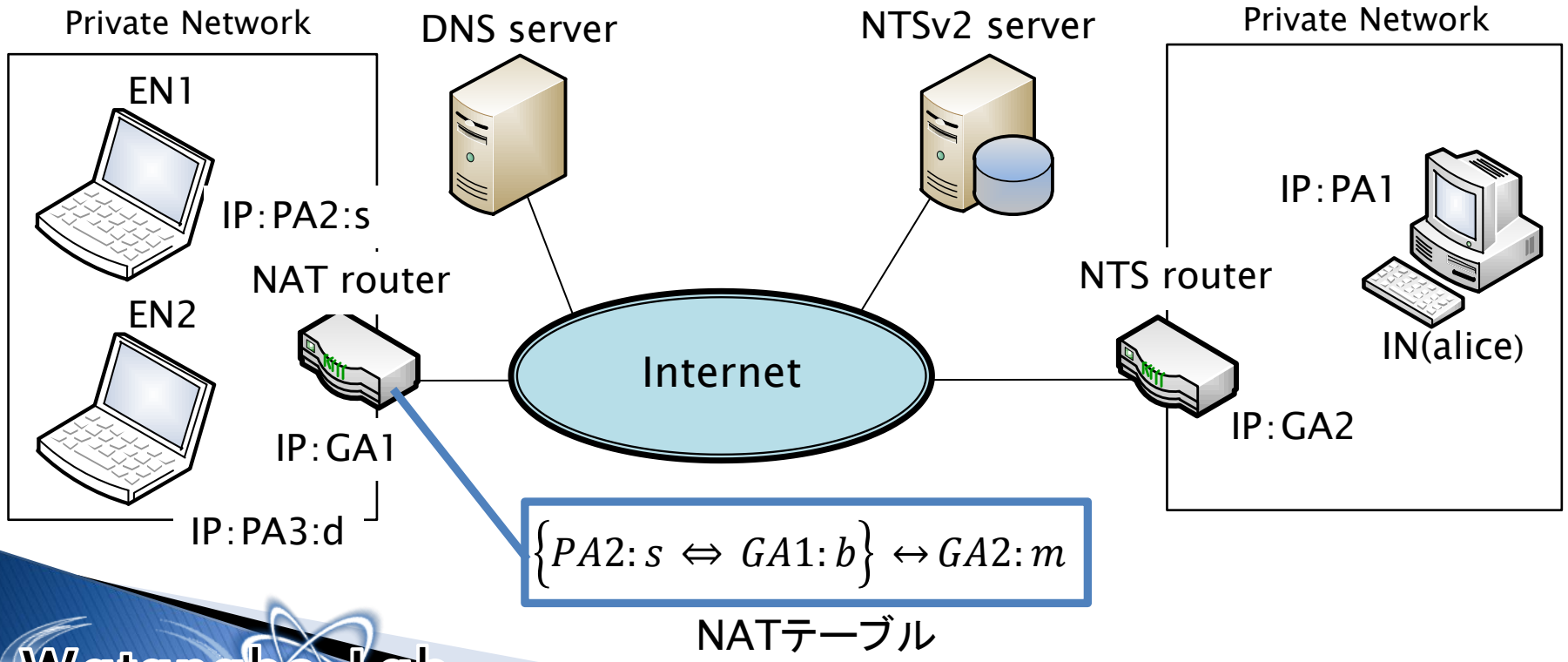
ルータの負荷予測

- 10秒当りのリクエスト数に対する平均待ち時間
  - リクエスト数（λ）：0～100（10刻みずつ計算）
  - 平均サービス率（μ）：100（リクエスト1個当たり約100msで処理）



Private to Private

- NATテーブル生成時にIPアドレスとポート番号が紐付されるため，端末の識別が可能



NATテーブル生成方法