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，鈴木 秀和，旭 健作，渡邊 晃

名城大学大学院 理工学研究科

Proposal of a NAT traversal Communication System Requiring No Changes in the Terminal

Tatsuya Matsuo and Hidekazu Suzuki and Kensaku Asahi and Akira Watanabe

Graduate school of Science and engineering, Meijo University

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 はグローバル側の端末からプライベート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．以前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していることが一般的となりつつある．そのため，グローバルアドレス空間側からプライベートアドレスを持つ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ため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 などのネットワーク機器に手を加える．外部端末と NAT 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．

端末非依存方式は，DNS サーバ，NAT，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 はグローバル側の端末が名前解決のために使用する DNS キャッシュサーバ，及び NAT 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 ではグローバル側の端末においてキャッシュサーバの登録変更をしなければならず，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，DNS キャッシュサーバには一切改造を加えず，プライベート側の端末のアドレスを管理する DNS 権威サーバを改造するように機能を見直した NTSSv2 を提案する．この方式により，両エンドの端末の変更，及び設定変更が一切不要な NAT 越えシステムが実現できる．

以下 2 章で NTSS，3 章で NTSSv2 を説明し，4 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）をグローバル側からアクセスする端末，IN（Internal Node）をプライベートアドレス空間に存在し，EN からアクセスされる端末とする．また，DNS サーバが提供する機能の違いにより，ホスト名を管理する DNS サーバを権威サーバ，ホスト名を問い合わせる DNS サーバをキャッシュサーバと呼ぶ．NTSS では，EN のキャッシュサーバと NAT を改造し，そこに NTSS を実現させるための NTS プロトコルを実装していた．改造したキャッシュサーバを NTS サーバ，改造した NAT 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．

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 のキャッシュサーバとなる NTS サーバと，IN の権威サーバとなる DDNS（Dynamic DNS）を設置する．DDNS 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 サーバをキャッシュサーバとなるように登録変更しておく．また，DDNS 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．

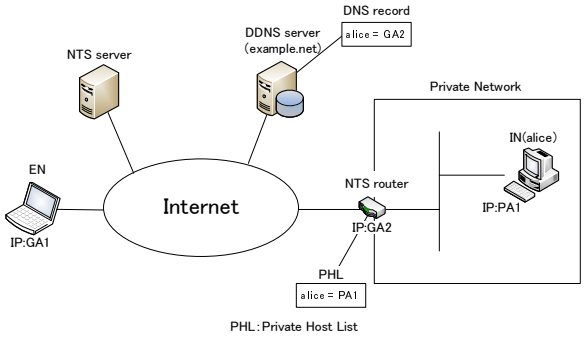


図 1: NTSS の構成

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）のプライベート IP アドレスを PA1 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 の権威サーバである DDNS サーバより NTS ルータのグローバル IP アドレス（GA2）を取得する．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，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．

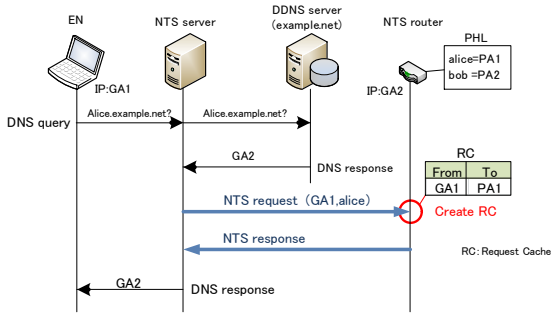


図 2: NTSS の名前解決シーケンス

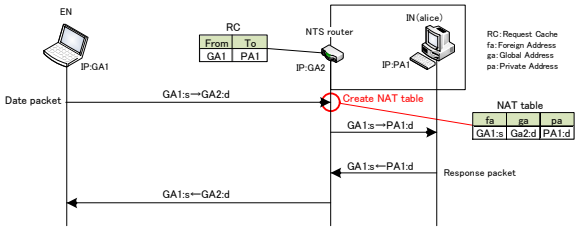


図 3: NTSS の通信開始シーケンス

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

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 を使用するユーザは，各自で使用するキャッシュサーバの設定を NTS サーバに変更する必要がある．NTSS において，EN 側のキャッシュ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．しかし，EN 側は一般端末であることから設定変更が必要であることは望ましくない．EN の設定変更を不要とするためには，通常利用しているキャッシュサーバを NTS サーバに置き換えれば良いが，一般ユーザが利用する全てのキャッシュサーバを置き換える必要があり現実的ではない．

3 NTSSv2

本章では，2.4 節の課題を解決するために，NTSS を実現する構成機器の見直しを行った NTSSv2 を提案する．NTSSv2 では EN のキャッシュサーバは改造せず，代わりに IN 側の権威サーバとなる DDNS を NTSv2 サーバとして改造する．権威サーバは

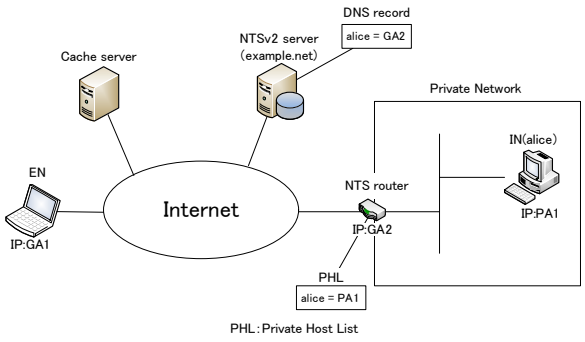


図 4: NTSSv2 の構成

プライベートアドレス側の装置であるため，改造は 1 ヶ所で良いという利点がある．これに伴い，NTS ルータの処理動作を見直した．

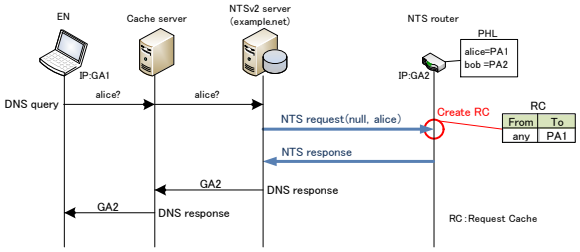


図 5: NTSSv2 の名前解決シーケンス

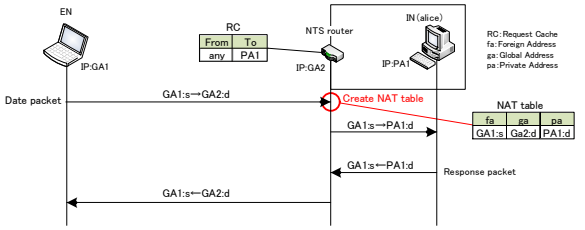


図 6: NTSSv2 の通信開始シーケンス

3.1 構成

図 4 に NTSSv2 の構成を示す．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 は既存のキャッシュサーバをそのまま使うので設定変更が不要である．

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 はキャッシュサーバに IN の名前解決を依頼する．キャッシュサーバは通常の DNS の仕組みにより，IN の権威サーバとなる 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

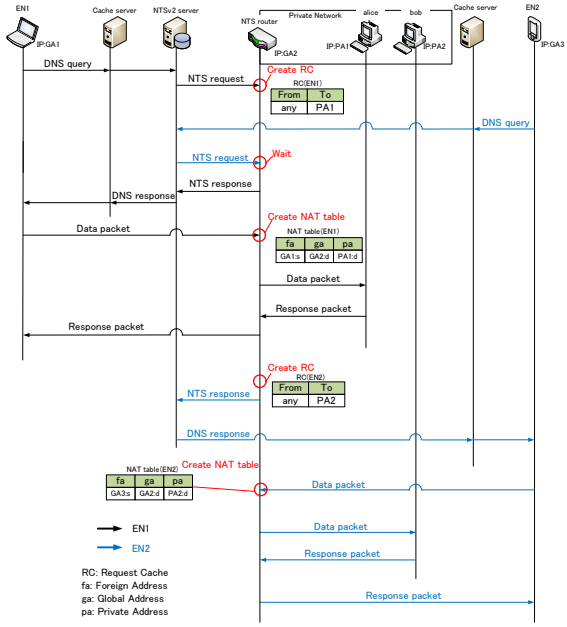


図 7: 同時問合せ時の動作シーケンス

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．

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

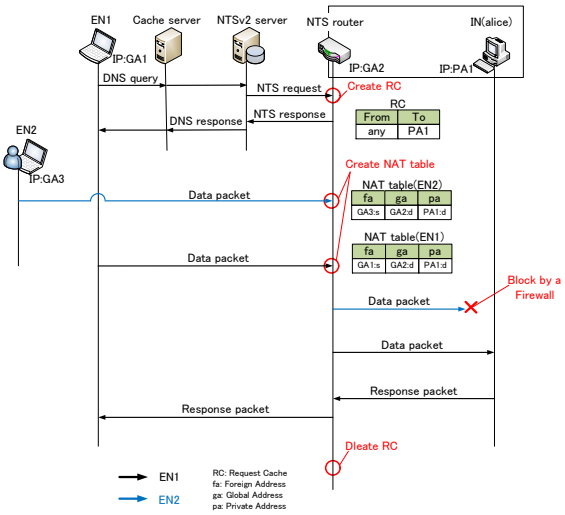


図 8: 第三者による通信の妨害

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ようにした．

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，EN2 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ができる．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．

4 まとめ

NTSS は端末の改造が不要であるが，キャッシュサーバの改造や EN の設定の変更が必要であった．そこで，これらの課題を解決するために，IN の権威サーバを 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課題を解決した．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 Protocol 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　旭 健作　渡邊 晃

Watanabe Lab.

研究背景

- IPv4アドレスの枯渇
  - アドレスの確保が困難となっている
  - プライベートアドレスの利用が一般的

- NAT（Network Adress Translation）
  - プライベートアドレスによりIPv4アドレスを大幅に節約できる
  - NATの外側から内側に通信を開始できない

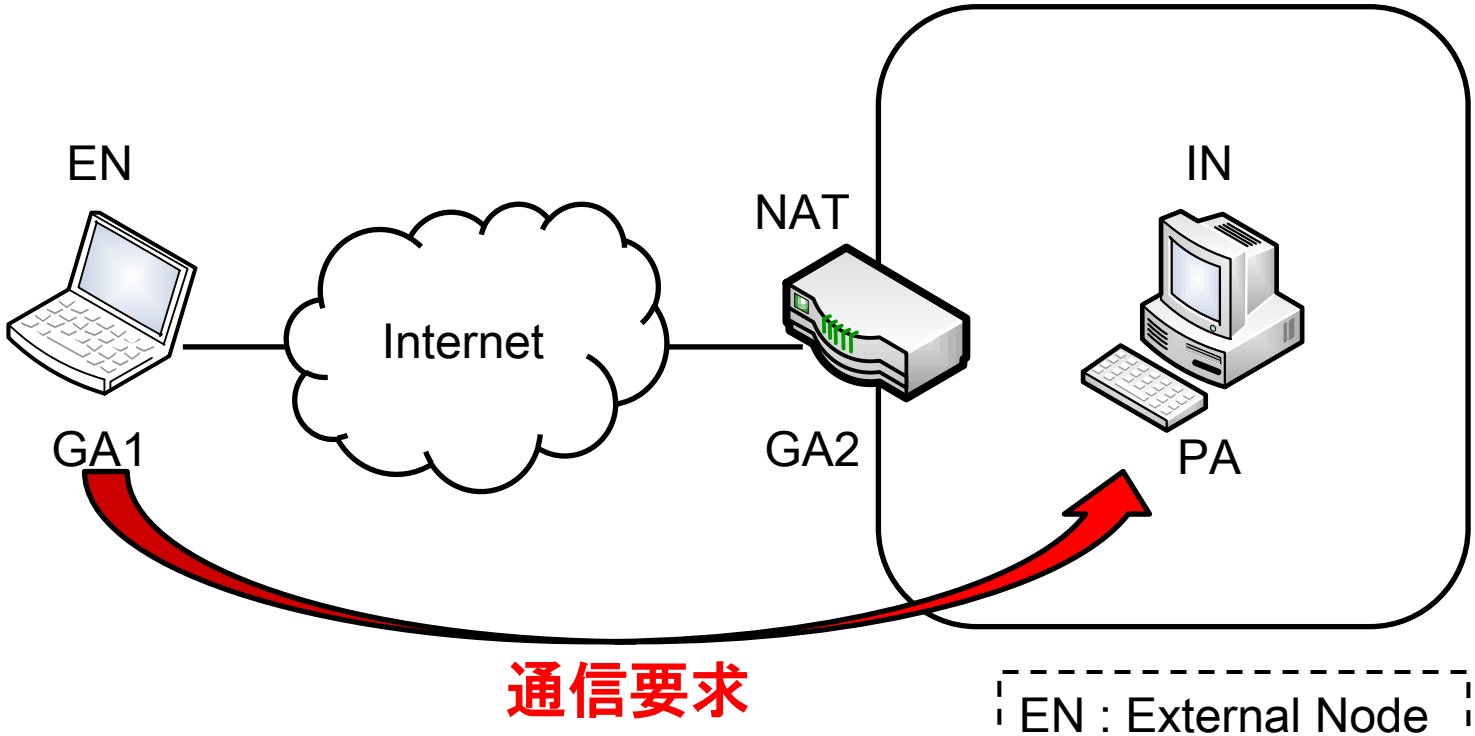
NAT越え問題

・インターネット利用方法の変化により問題化

Watanabe Lab.

NAT越え問題

- ENはINに通信を開始したい

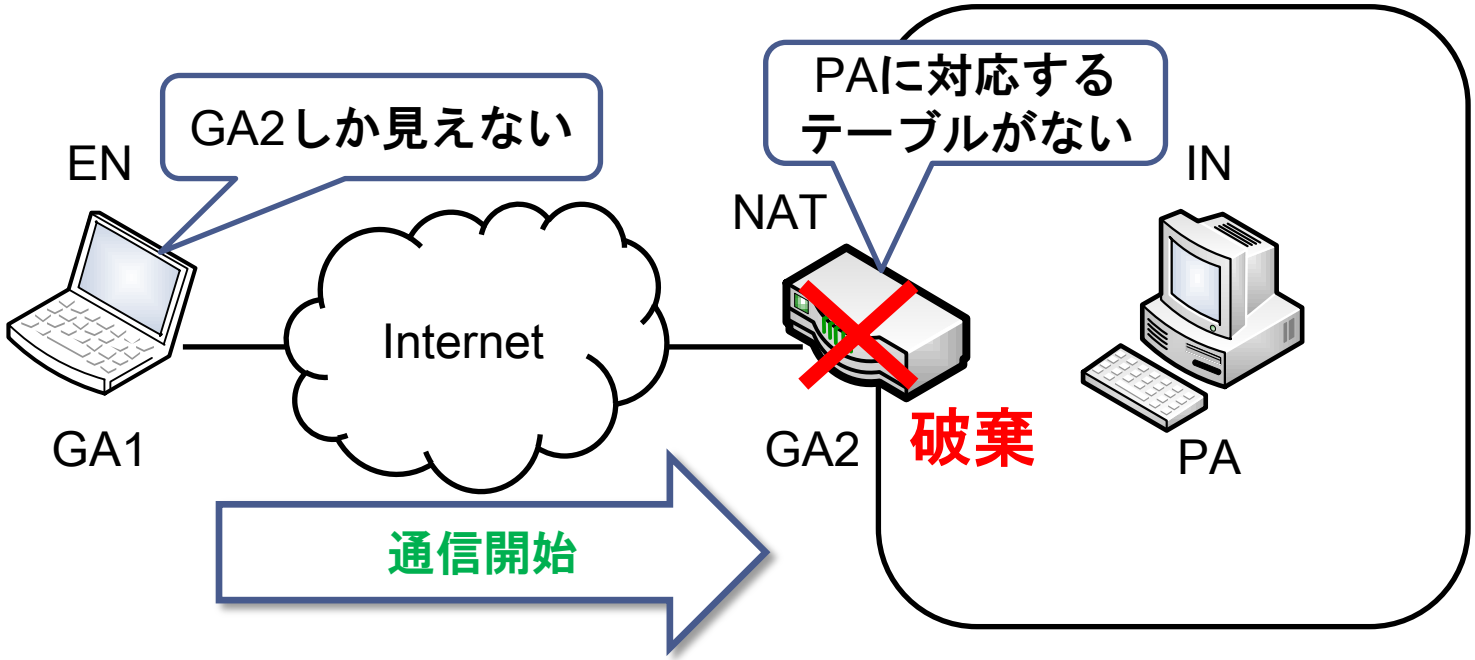


EN : External Node
IN : Internal Node
GA : Global Adress
PA : Private Adress

Watanabe Lab.

NAT越え問題

- NATによりINは隠蔽される



ENはINに通信を開始することができない

EN : External Node
IN : Internal Node
GA : Global Adress
PA : Private Adress

Watanabe Lab.

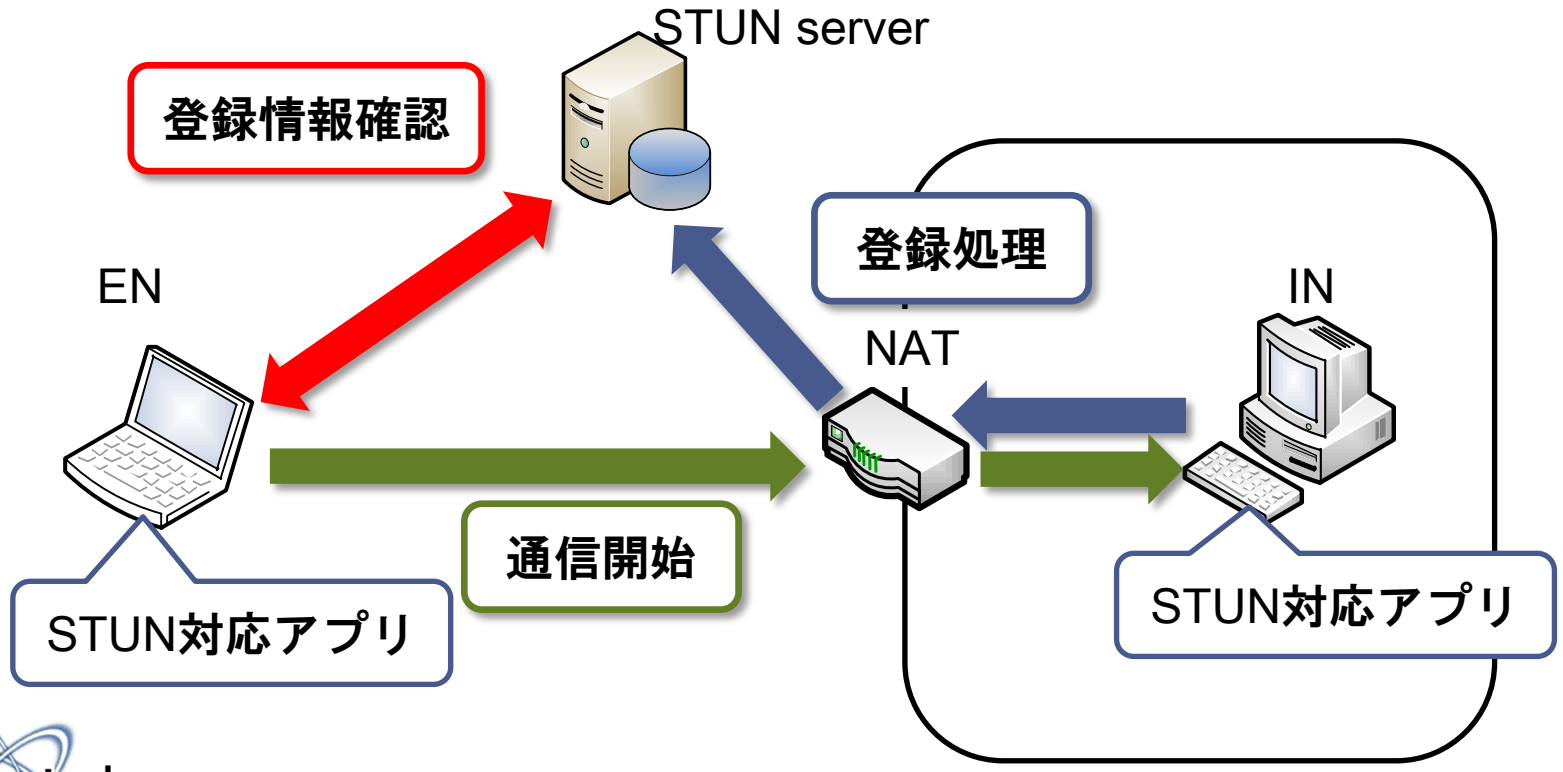
既存研究

- アプリケーションレベル改造方式
  - 既存のNATをそのまま使える
- ネットワークレイヤ改造方式
  - 既存のアプリケーションをそのまま使える
- 端末非依存方式
  - エンド端末の改造が不要

Watanabe Lab.

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
- 既存方式：STUNなど

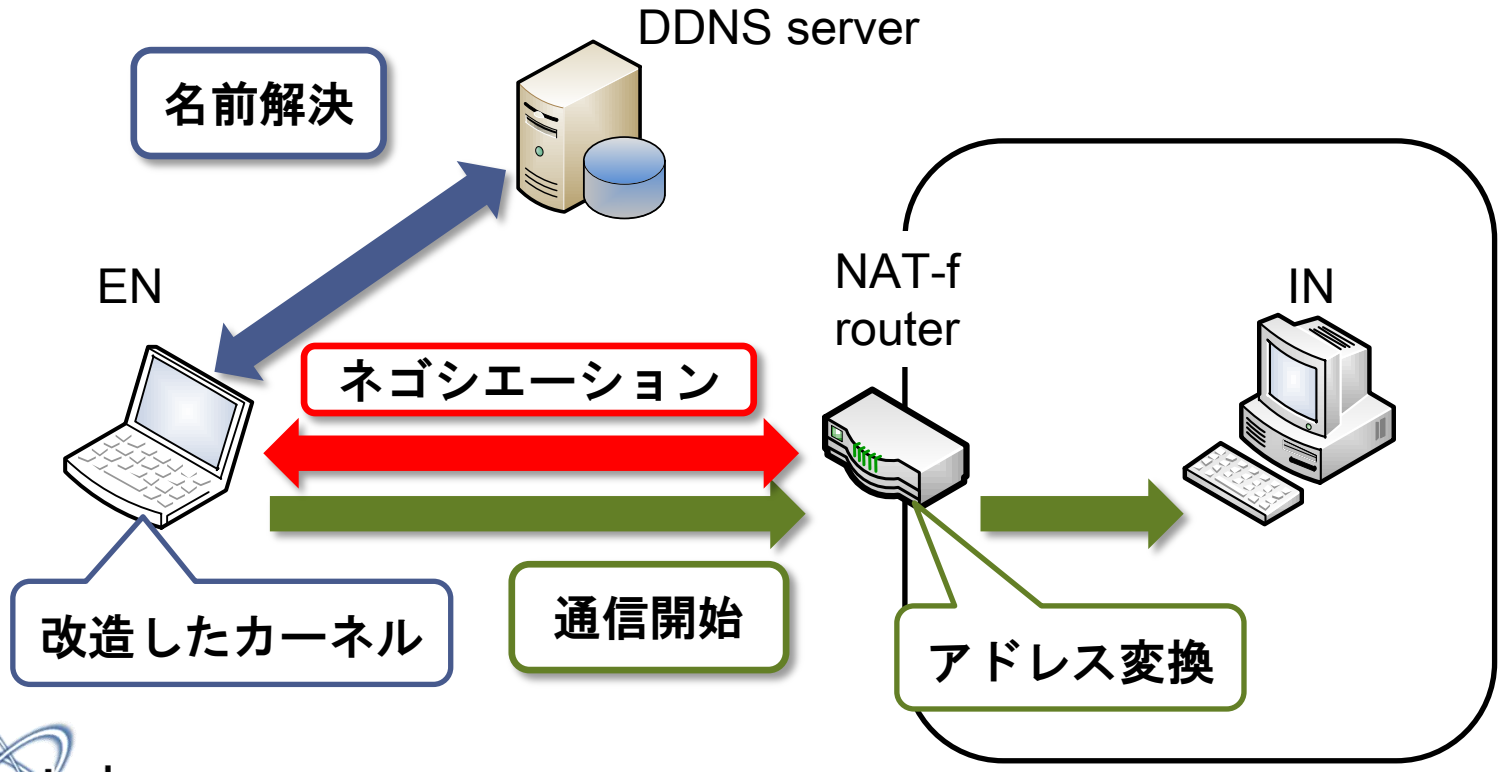


Watanabe Lab.

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

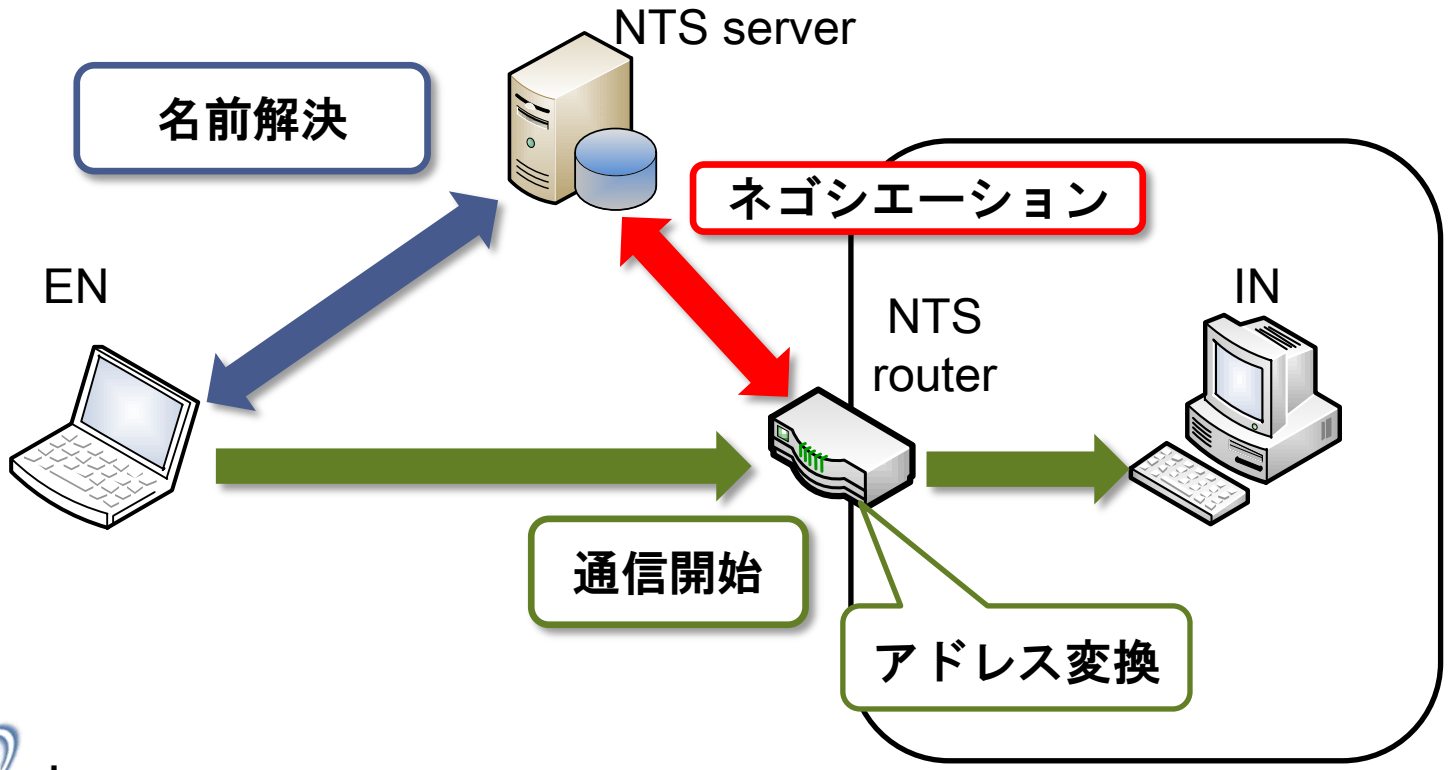
- ENのカーネルやNATを改造し，協調動作
- 既存方式 : NAT-fなど



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やNATなどを改造し，協調動作
- **既存方式**：NTSS, AVES



Watanabe Lab.

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.

研究の目的

- 接続場所や使用OSに限定されない
  - スマートフォン，タブレットPC，etc…
- 多くのユーザが容易に利用できる
  - 上記端末の急速な普及により，インターネット利用層が拡大

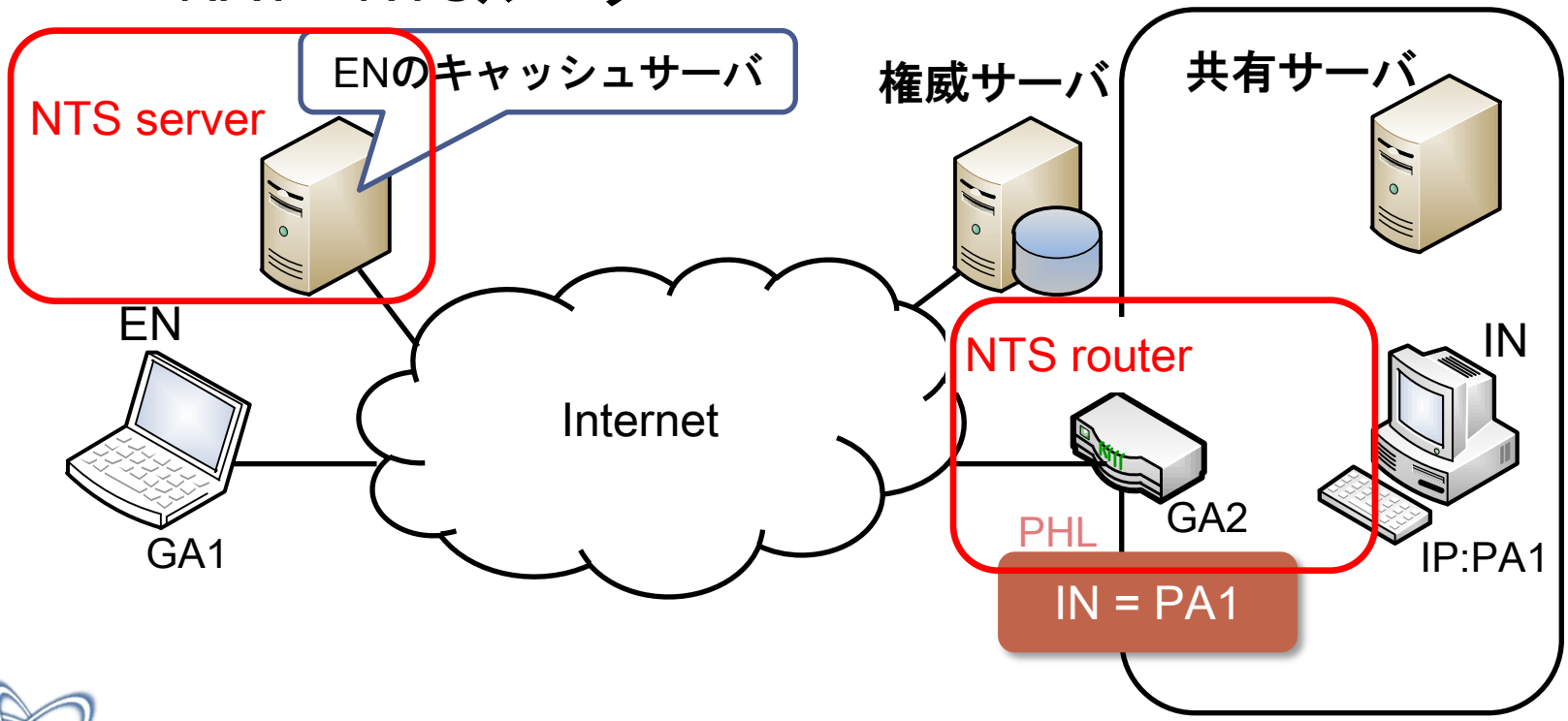
端末に手を加えずにNAT越えを実現

→端末非依存方式に着目

Watanabe Lab.

NTSS(NAT Traversal Support System)

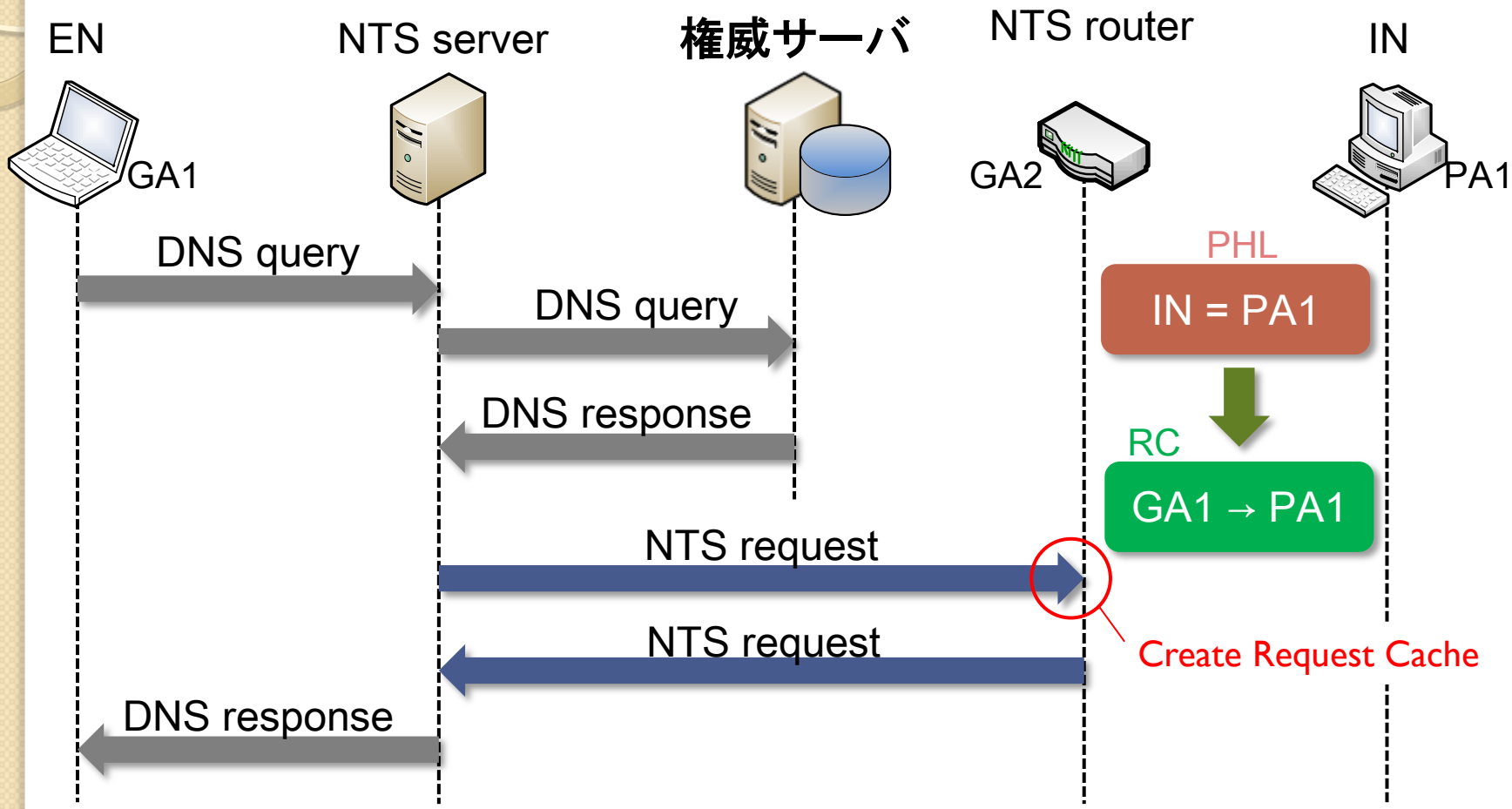
- ENのキャッシュサーバとNATを改造
  - キャッシュサーバ：NTSサーバ
  - NAT：NTSルータ



キャッシュサーバ：ホスト名を問い合わせるDNS
権威サーバ：ホスト名を管理するDNS

NTSS (名前解決)

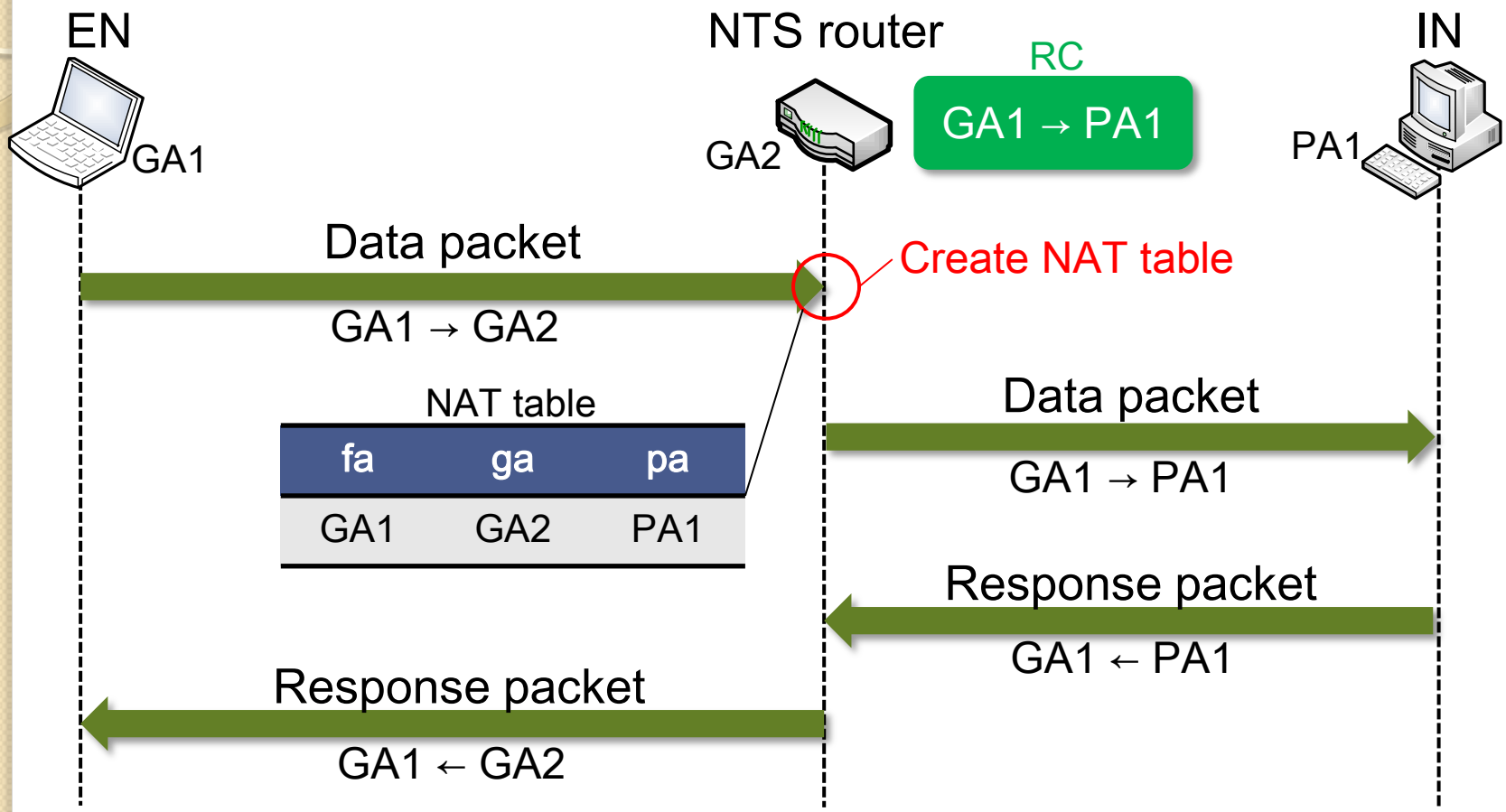
EN → INの通信



PHL(Private Host List)：INのFQDNとプライベートIPの対応関係を記したテーブル
RC(Request Cache)：ENとINのIPの関係を記したキャッシュ

NTSS (通信開始)

EN → INの通信



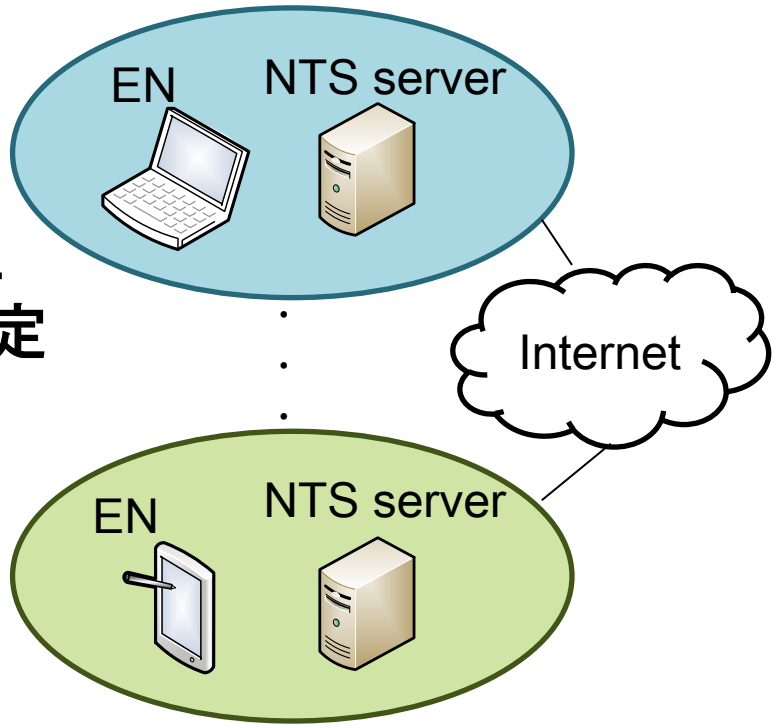
fa: foreign address
ga: global address
pa: private address

Watanabe Lab.

NTSSの課題

- ENの設定変更
  - ENが利用するキャッシュサーバをNTSサーバに指定
  - 使えるユーザが限られる

多くのユーザが利用できるようにしたい



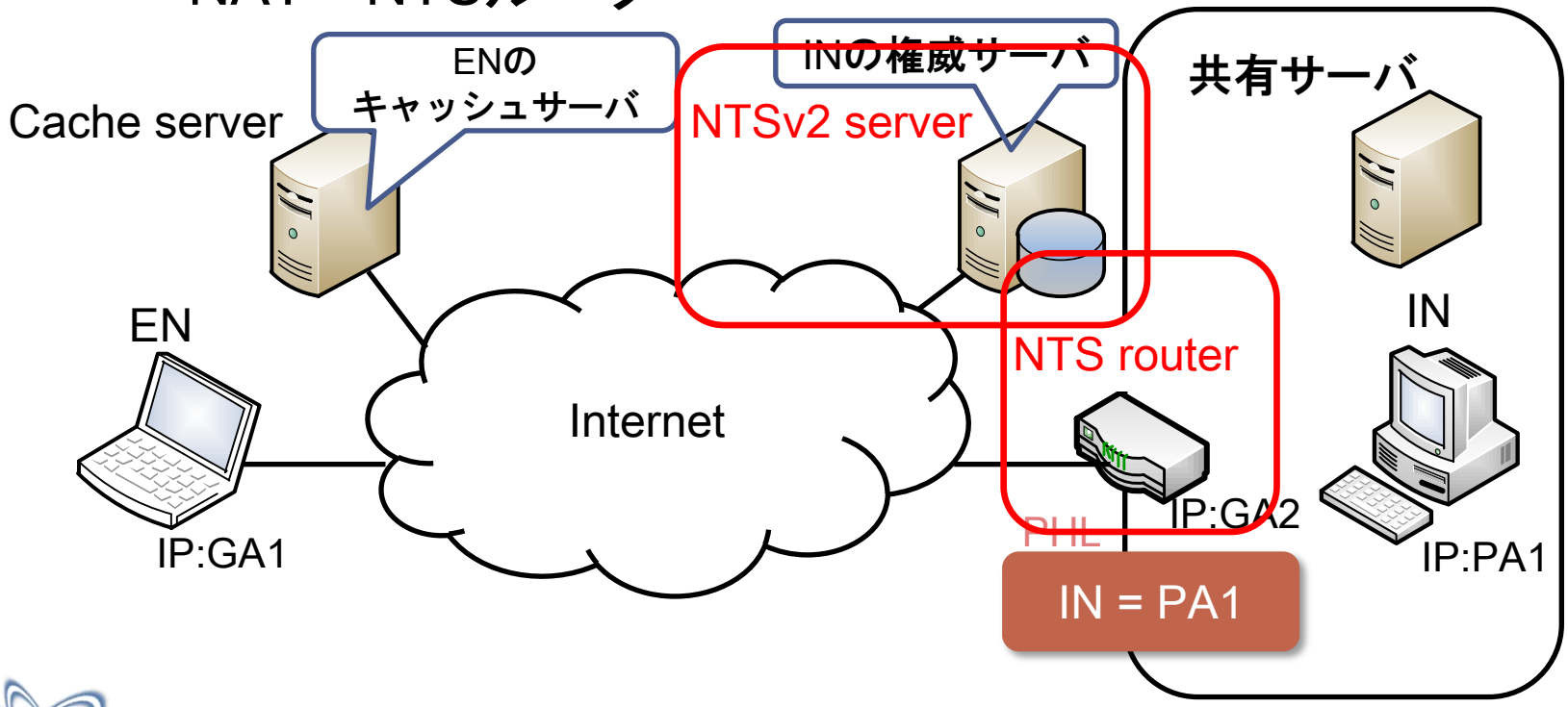
端末の設定変更も不要な方式

Watanabe Lab.

提案方式

NTSSv2

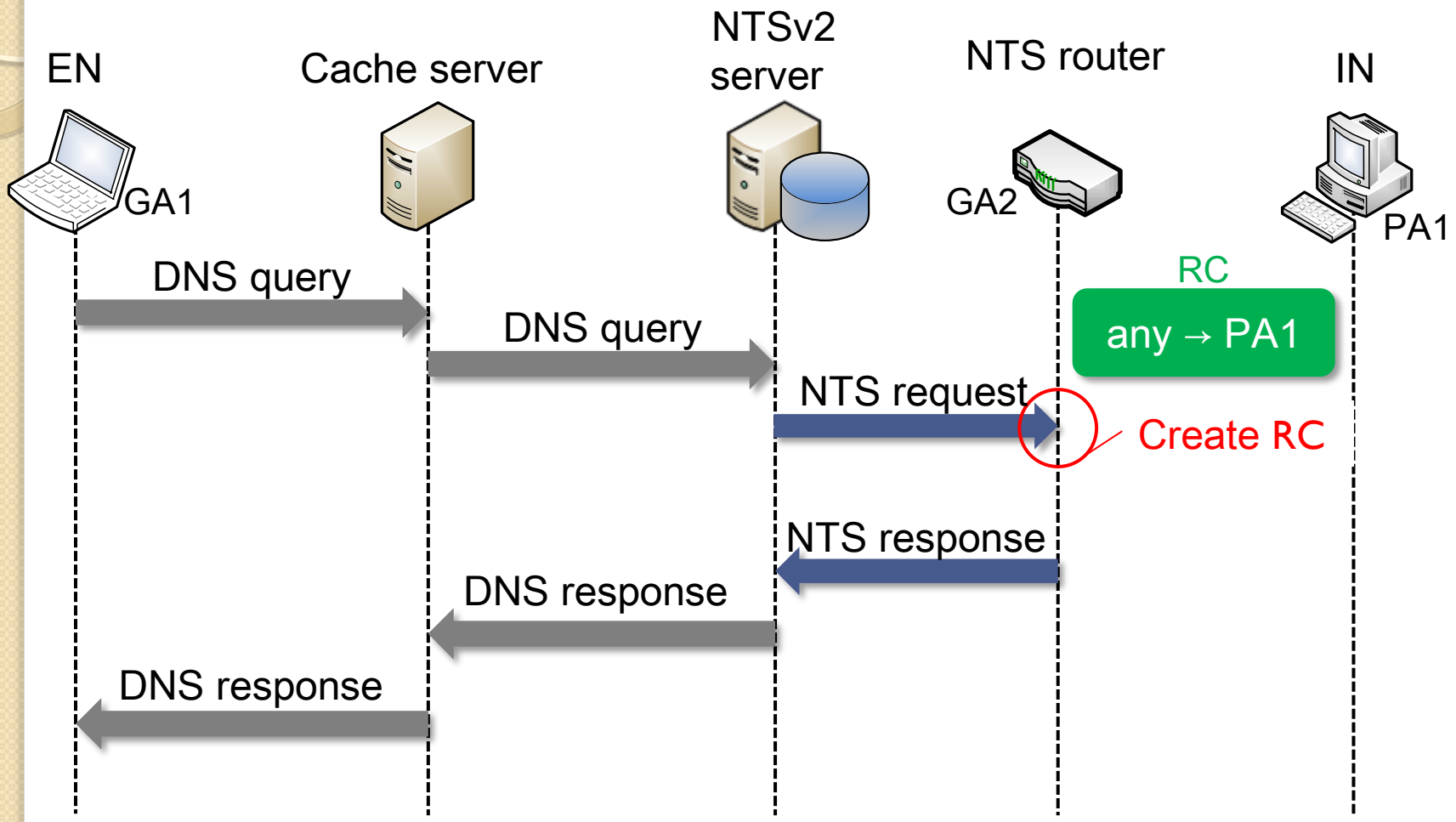
- INの権威サーバとNATを改造
  - 権威サーバ：NTSv2サーバ
  - NAT：NTSルータ



キャッシュサーバ：ホスト名を問い合わせるDNS
権威サーバ：ホスト名を管理するDNS

NTSSv2 (名前解決)

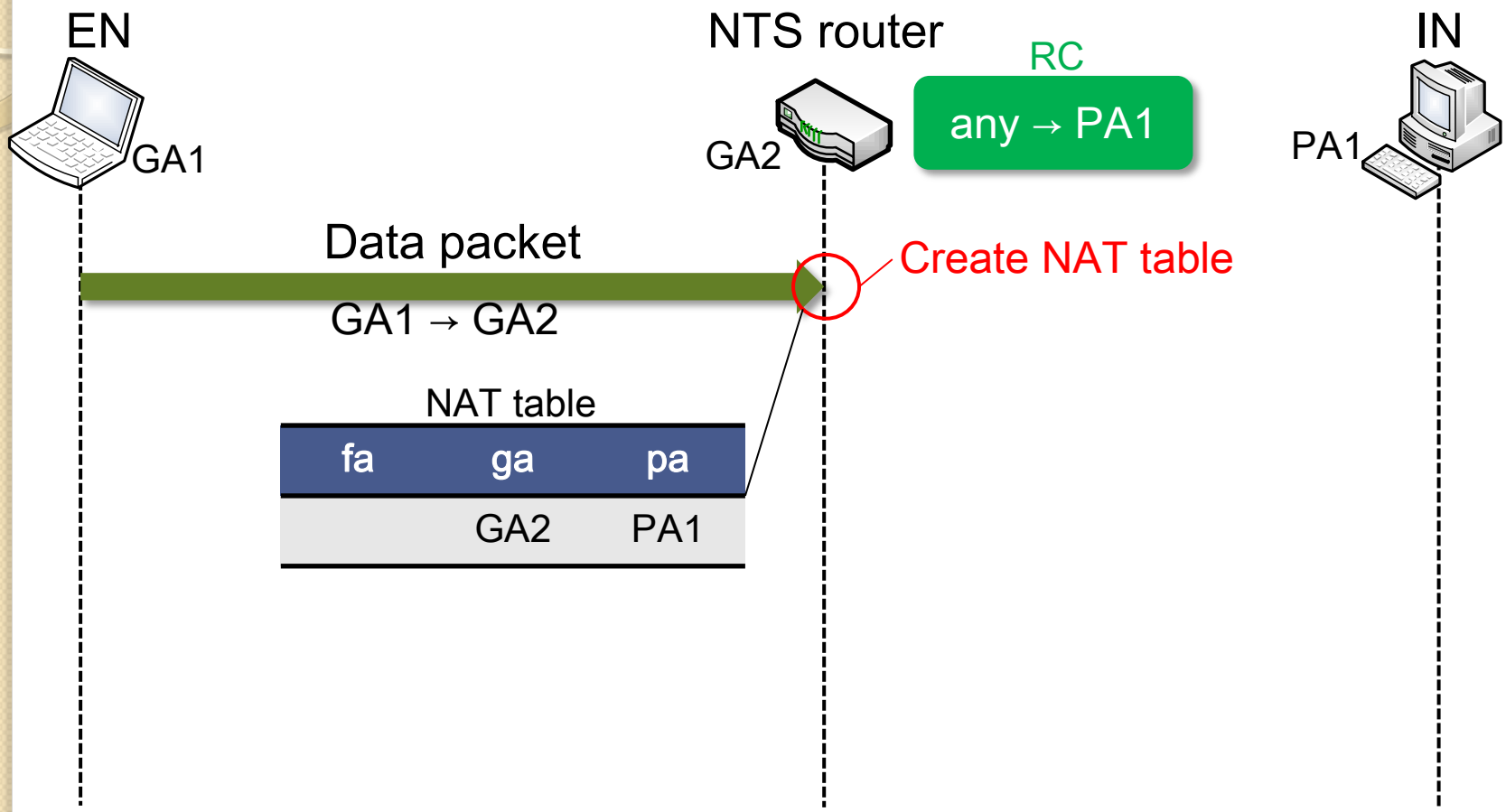
EN → INの通信



PHL(Private Host List)：INのFQDNとプライベートIPの対応関係を記したテーブル
RC(Request Cache)：ENとINのIPの関係を記したキャッシュ

NTSSv2 (通信開始)

EN → INの通信

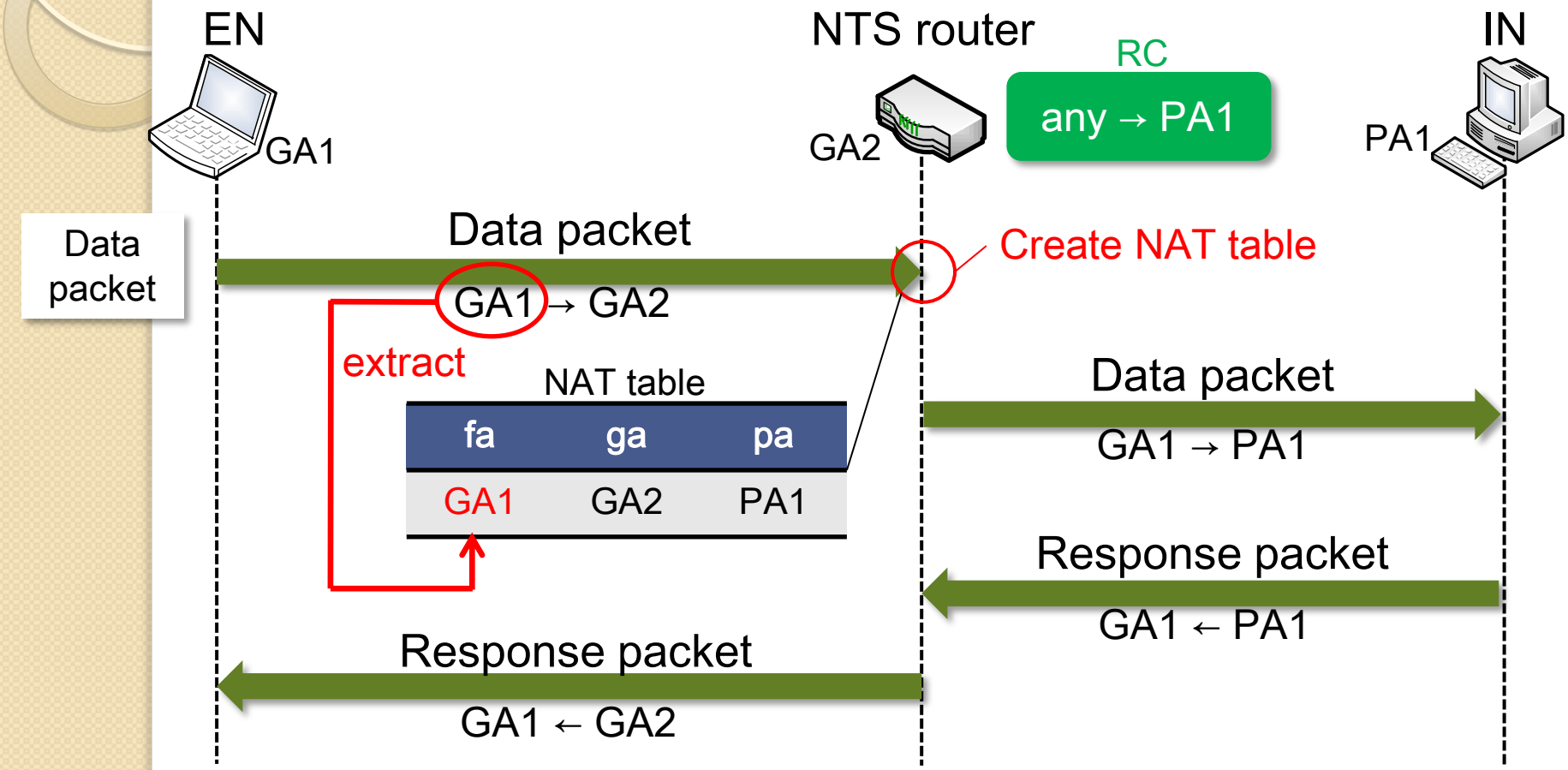


fa: foreign address
ga: global address
pa: private address

Watanabe Lab.

NTSSv2 (通信開始)

EN → INの通信



fa: foreign address
ga: global address
pa: private address

Watanabe Lab.

課題と対策

- 権威サーバを改造することにより，ENの情報をNTSルータに通知できなくなった

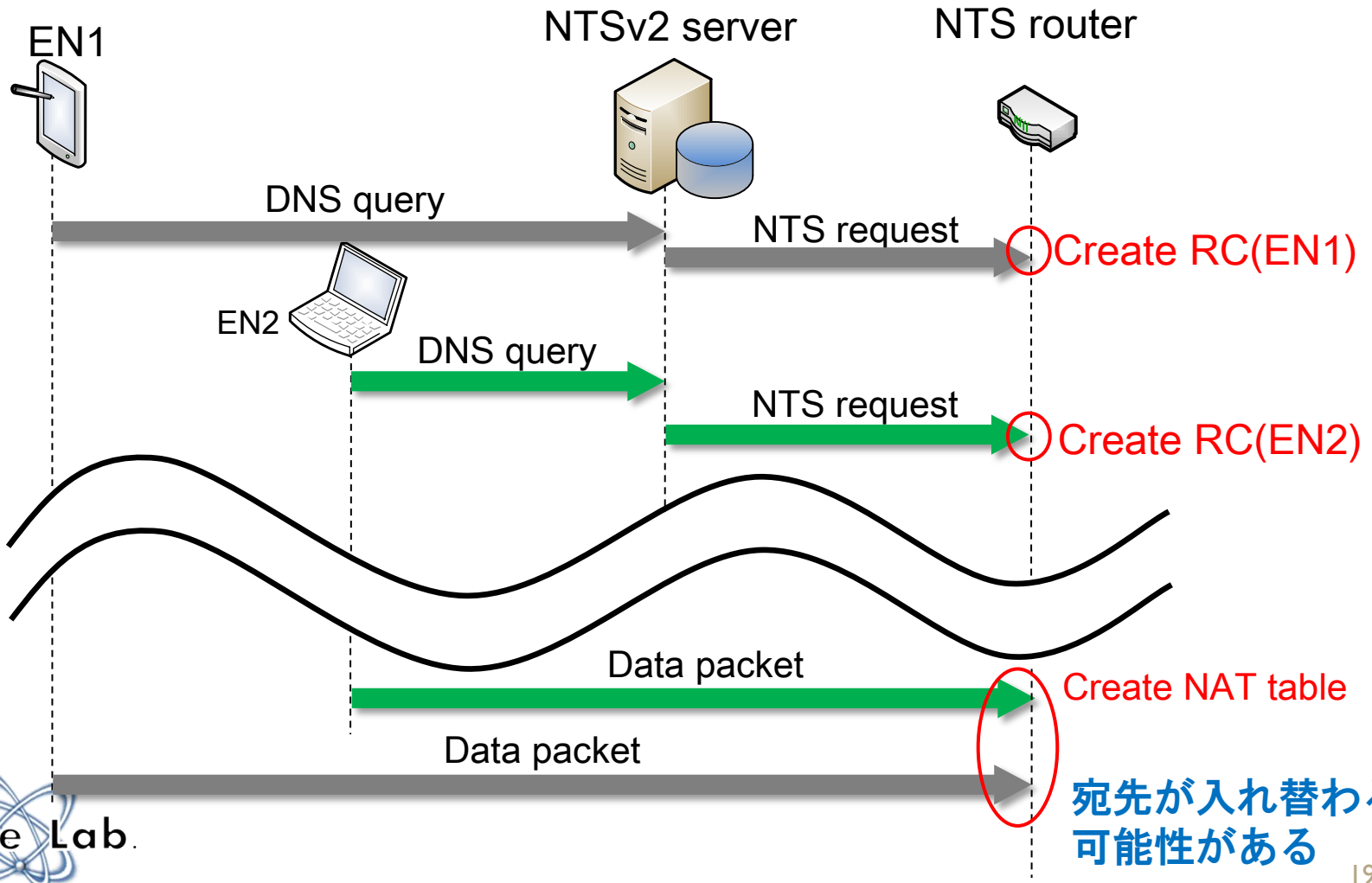
- 考えられる課題
  - 同時問い合わせ
  - 第三者による通信の妨害

Watanabe Lab.

同時問合せ（1/2）

EN1, EN2が同時問合せ

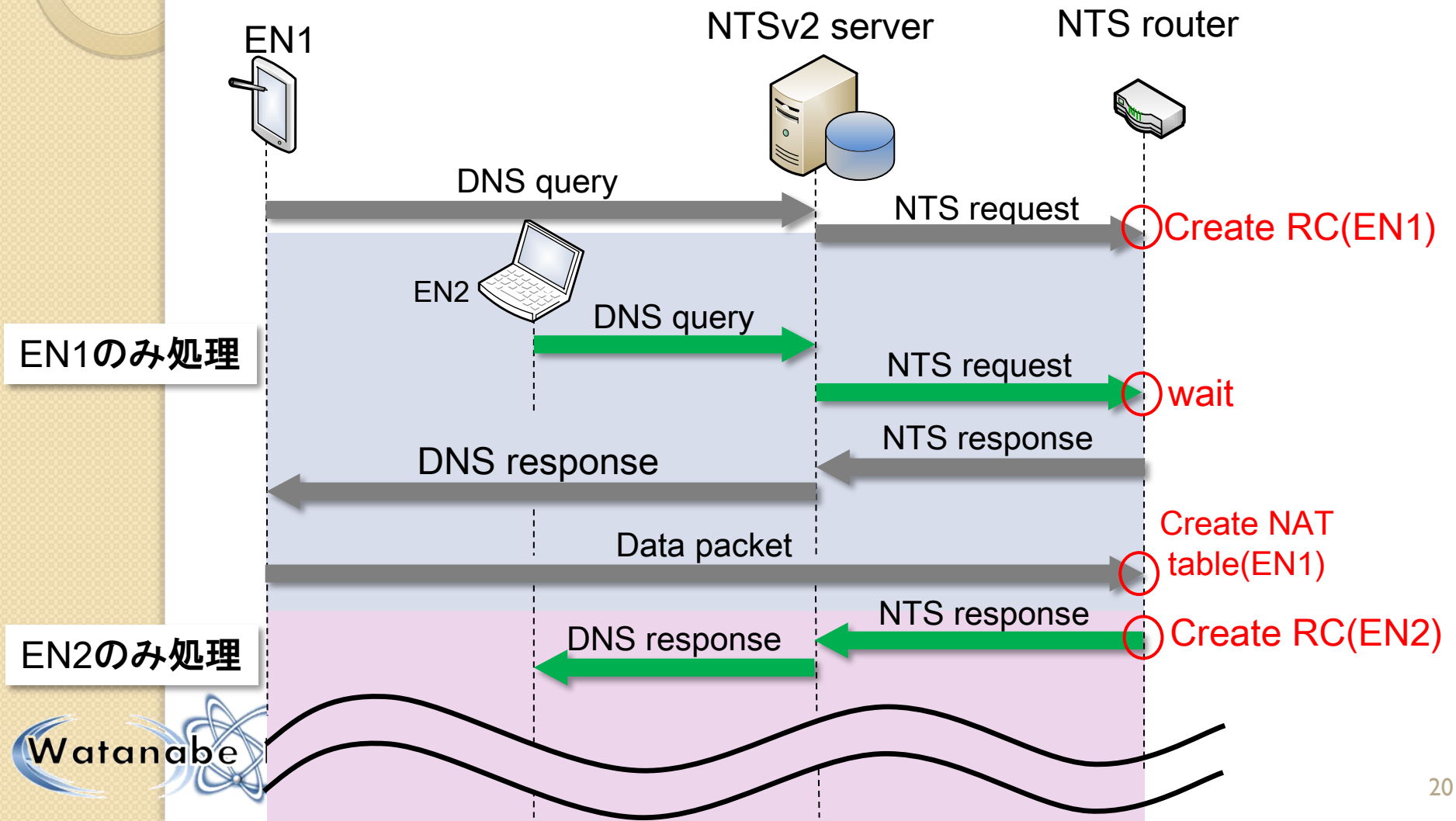
- 経路上の遅延などにより，宛先が違うNATテーブルを生成する可能性がある



同時問合せ（2/2）

EN1, EN2が同時問合せ

対策：NATが各々のリクエストに対し，
シリアライズに処理することで対応

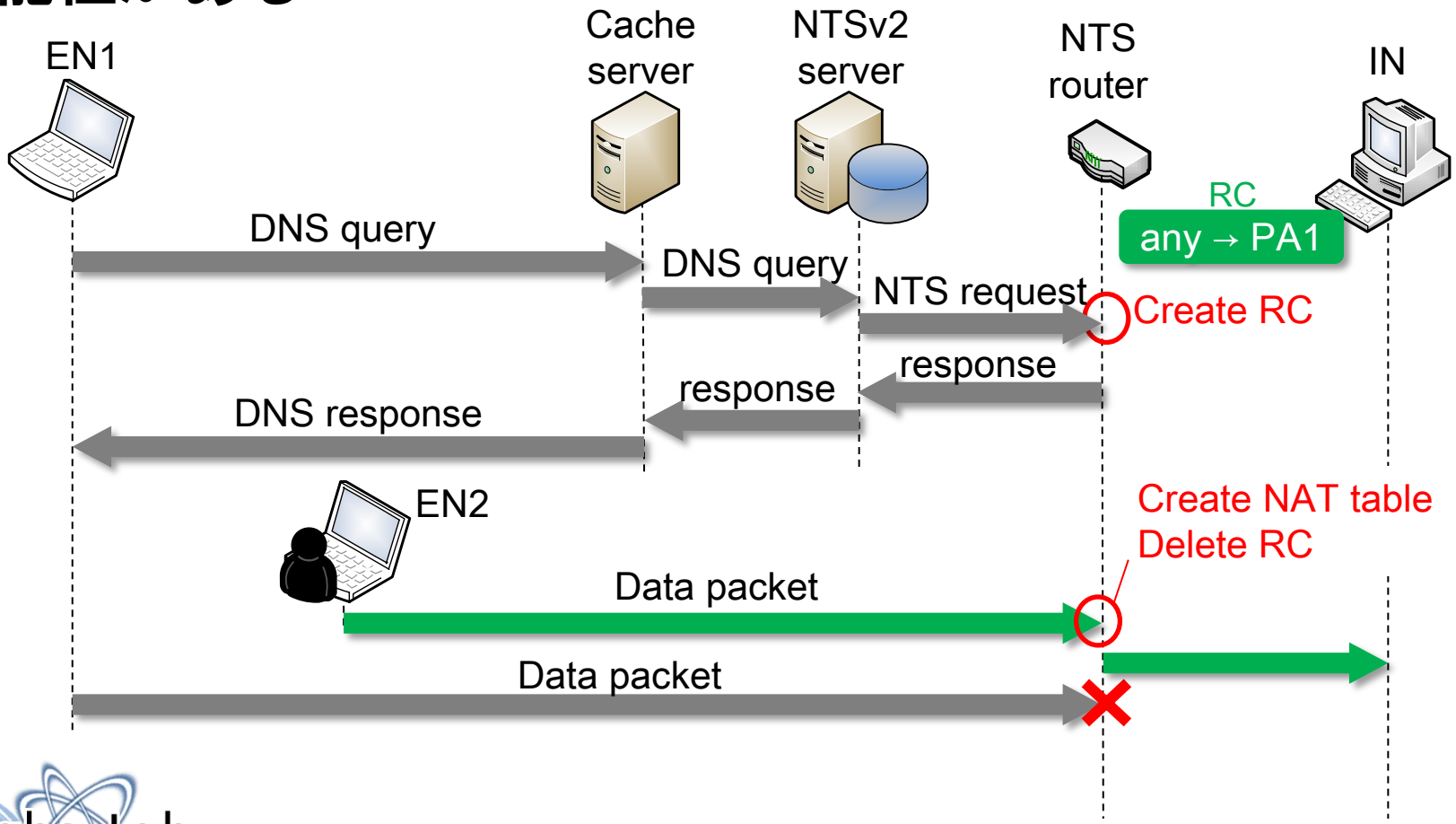


通信の妨害（1/2）

EN1の通信確立中にEN2が割込む

- NTSS：NATテーブル生成完了時にRCを削除

→第三者（EN2）によって，通信の妨害をされる可能性がある

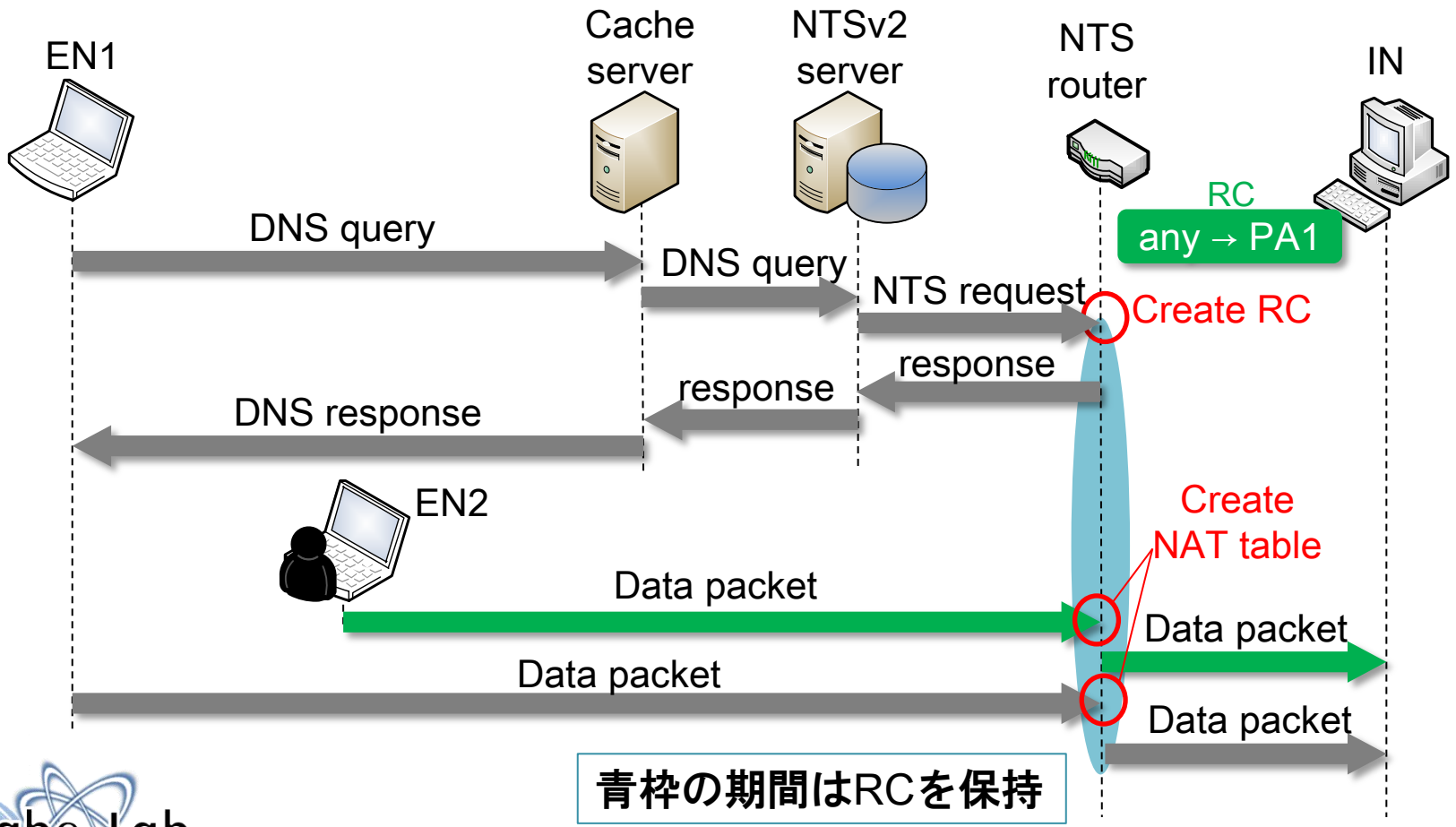


*一部処理は省略

通信の妨害（2/2）

EN1の通信確立中に
EN2が割込む

対策：RCを一定期間保持させる
→正規ユーザの通信の確立を保証



青枠の期間はRCを保持

Watanabe Lab.

むすび

- NTSSv2
  - NTSSを改良した方式
  - NTSv2サーバとNTSルータの連携により，NAT越えを実現
  - エンド端末の設定変更が不要
  - 考えられる課題に対応

- 今後
  - 実装を完了させる
  - ストレステストなどによる評価

Watanabe Lab.


Watanabe Lab.

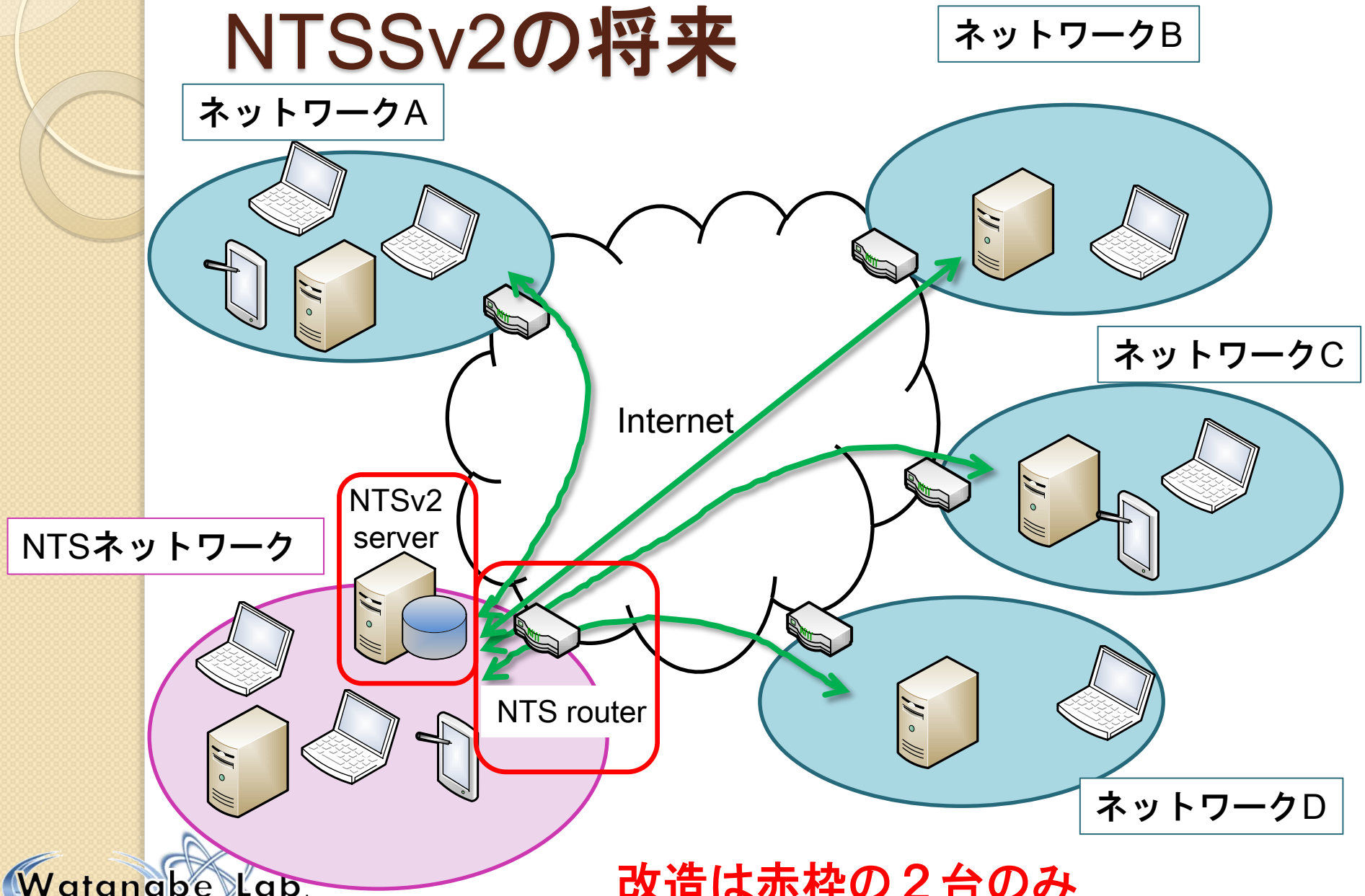
RC保持時間

- シリアライズ処理と連動させる

- EN-NTS router間のRTTを目安に設定
  - 端末や環境により異なる
  - 保持期間を短くする
    - 対応端末：少　スループット：高
  - 保持期間を長くする
    - 対応端末：多　スループット：低

Watanabe Lab.

NTSSv2の将来



改造は赤枠の２台のみ

Watanabe Lab.