端末の変更が一切不要なNAT越え通信システムの提案

123430037　松尾 辰也
渡邊研究室

1. はじめに

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NAT（Network Address Translation）による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NAT越え問題が存在する．これまでに様々な方式が提案されてきたが，多くの方式では端末に特殊な機能を実装する必要があった．

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）[1]を提案し実現させた．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，それぞれが動作を協調することにより，NAT越えを実現する．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，誰でも利用できる訳ではなかった．

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，両エンド端末の変更，および設定変更が一切不要なNAT越えシステムが実現できる．

2. NTSSとその課題

2.1 NTSS

NTSSはエンド端末の改造を不要とした独自のNAT越え通信システムである．

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る．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．

ENからIN（alice）へ通信を開始する場合を例として，NTSSの事前設定と各処理の流れを説明する．

(1) **事前設定**　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，INの権威サーバとなるDDNS（Dynamic DNS）を設置し，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．

(2) **名前解決**　図1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，rootDNSサーバから始まる反復問合せを行い，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．NTSサーバはこの名前解決結果をENへ返信する前に，NTSルータとネゴシエーションを行う．この時，NTSルータは通知情報を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．

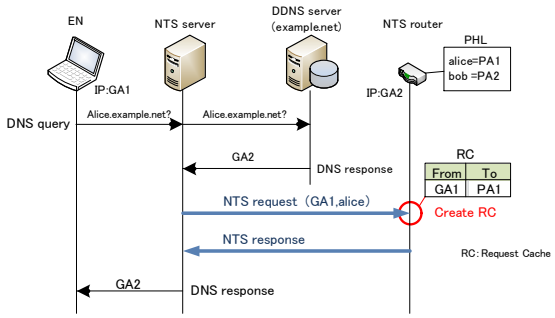


図 1: NTSSの名前解決シーケンス

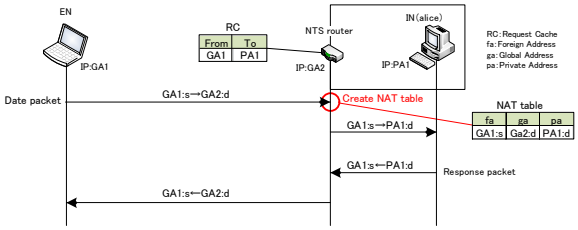


図 2: NTSSの通信開始シーケンス

(3) **通信開始**　図2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．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の内容から送信元IPアドレス（GA1），宛先IPアドレスを“PA1”に変換するNATテーブルを生成する．受信したパケットはNATテーブルに従ってアドレス変換し，aliceに送信する．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．

2.2 課題

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．しかし，EN側は一般端末であることから登録変更が必要であることは望ましくない．ENの登録変更を不要とするためには，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ればよいが，現実的な案ではない．

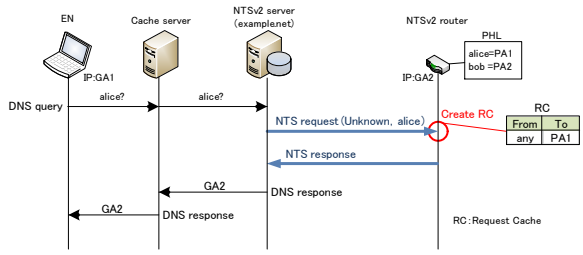


図 3: NTSSv2 の名前解決シーケンス

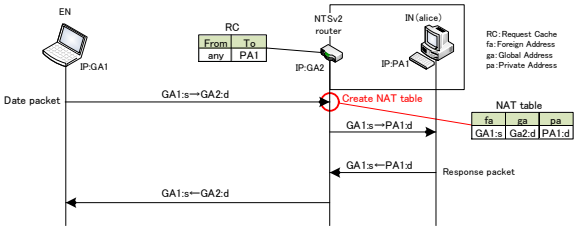


図 4: NTSSv2 の通信開始シーケンス

3. 提案方式

上記の課題を解決するために，NTSS を実現する構成機器とシーケンスの見直しを行った NTSS を NTSSv2 と呼ぶ．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，各装置の動作を見直した．

以降 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．事前設定は，キャッシュサーバの設定変更以外は NTSS と同様なので省略する．

(1) **名前解決**　図 3 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 サーバを発見する．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．

(2) **通信開始**　図 4 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．

4. 実装

提案方式の実装概要を図 5，図 6 に示す．NTSS と同様に，FreeBSD のアプリケーションとして，NTSv2 サーバと NTS ルータにそれぞれ NTS モジュールを追加させる．

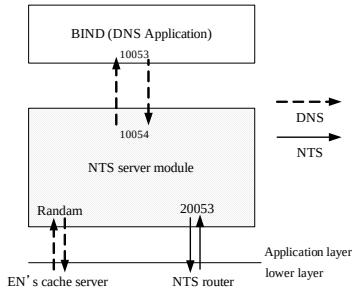


図 5: NTSv2 サーバの実装概要

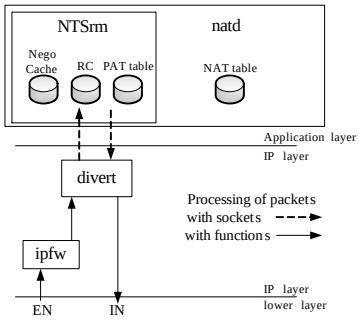


図 6: NTS ルータの実装概要

4.1 NTSv2 サーバ

NTSv2 サーバには，DNS アプリケーションである BIND をインストールし，これを 10053 番ポートでリッスンするように設定する．代わりに，NTS サーバモジュールを 53 番ポートでリッスンするように設定する．NTS サーバモジュールは，通常の名前解決処理は BIND に受け渡し，その処理結果を基に NTS ルータとネゴシエーションを行う．ネゴシエーションが完了すると，EN のキャッシュサーバに名前解決結果を返す．このような手順により，NTSv2 サーバは通常の権威サーバの様に振る舞う．

4.2 NTS ルータ

NTS ルータは，natd（NAT デーモン）と呼ぶ NAT 機能を持つ FreeBSD のデーモンに NTS ルータモジュールを内蔵させる．NTS ルータモジュールは，divert ソケットからパケットを受信すると，送信元と宛先を入れ替えたダミーパケットを生成する．更に，PAT テーブルという独自の変換テーブルにより，ポート番号の整合性を解消させ，natd に EN 用の NAT テーブルを強制的に生成させる．提案方式では異なる EN からの同時問合せ時対応するため，処理をシリアライズに行わせる必要がある．そのため，NTS リクエストを保存させるネゴキャッシュを新たに用意する．

5. まとめ

本論文では，既存方式の課題であった端末の改造や登録変更を無くし，一般端末でも利用できる NAT 越え方式を提案した．今後は実装を完了させ，評価を行う予定である

参考文献

[1] 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　情報工学専攻
渡邊研究室　123430037　松尾 辰也

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

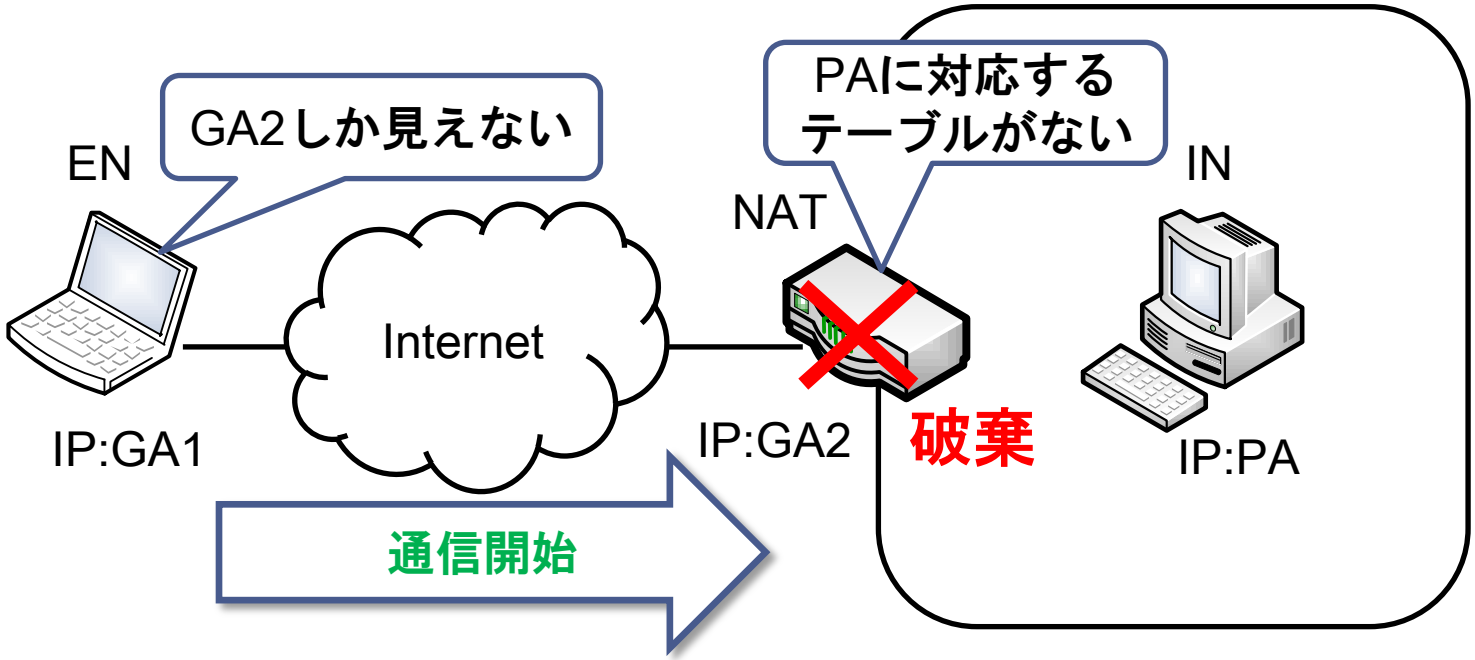
- NAT（Network Address Translation）
  - プライベートアドレスによりIPv4アドレスを大幅に節約できる
  - NATの外側から内側に通信を開始できない

NAT越え問題

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
  - エンド端末のアプリケーションを改造，専用サーバを設置
  - 特徴：既存のNATが利用できる
- ネットワークレイヤ改造方式
  - ENのカーネルとNATを改造
  - 特徴：既存のアプリケーションが利用できる
- 端末非依存方式
  - DNS (Domain Name Server) とNATを改造
  - 特徴：エンド端末の改造が不要

Watanabe Lab.

研究の目的

- モバイル端末，情報家電の多様化
- 一般ユーザでも容易に利用したい

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.

端末非依存方式の既存研究

- AVES(Address Virtualization Enabling Service)
  - 専用サーバとNATが協調動作
  - 第三の装置の設置，経路冗長

- NTSS(NAT Traversal Support System)
  - 本研究室が提案した独自の方式
  - DNSサーバとNATが協調動作

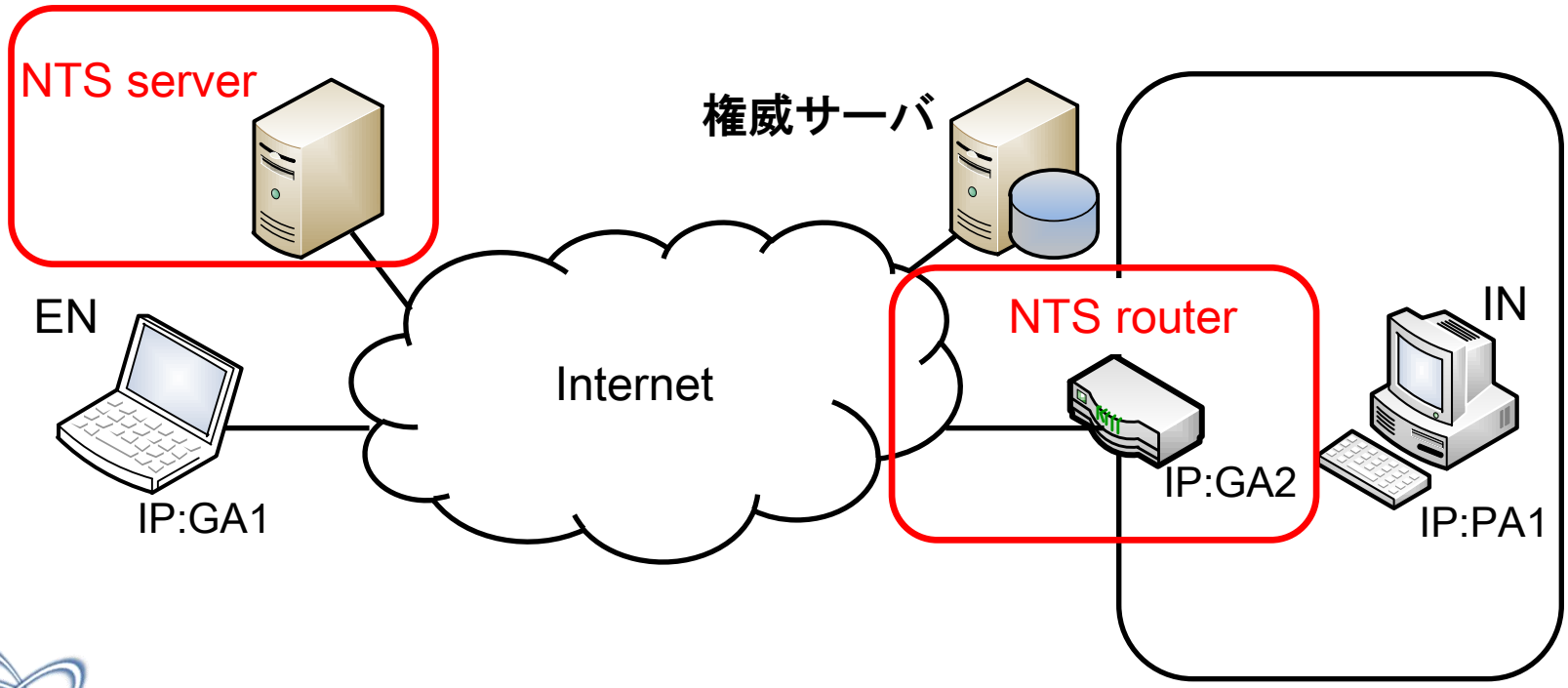
改良

AVESの課題
NTSSの課題
を解決

Watanabe Lab.

NTSS(NAT Traversal Support System)

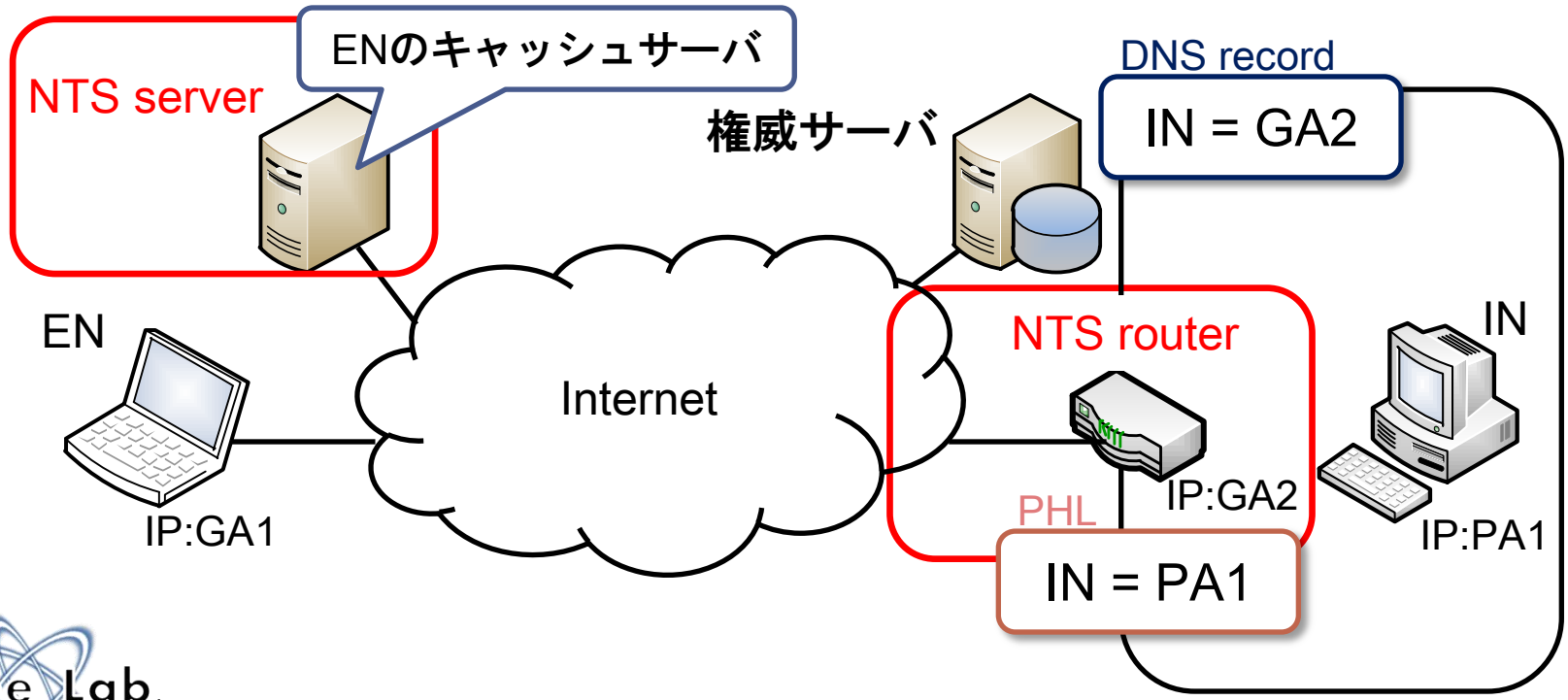
- キャッシュサーバとNATを改造
  - キャッシュサーバ：NTSサーバ
  - NAT：NTSルータ



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(事前設定)

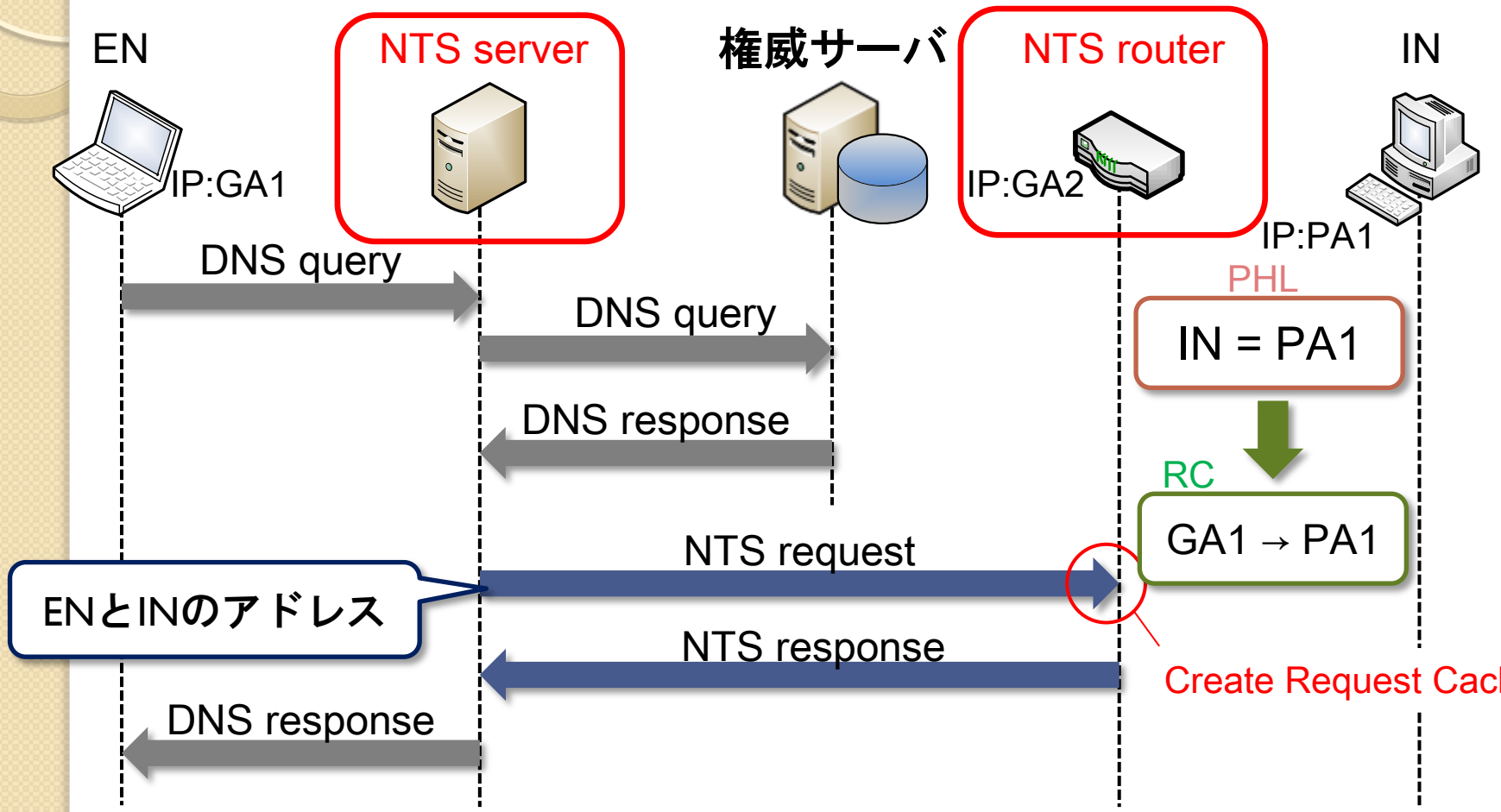
- NTSサーバをENのキャッシュサーバに指定
- **登録処理**
  - DNSレコード：INのFQDNとNTSルータのグローバルアドレスの対応関係
  - PHL(Private Host List)：INのFQDNとプライベートアドレスの対応関係



PHL(Private Host List) : **新たに定義した独自のテーブル**

NTSS (名前解決)

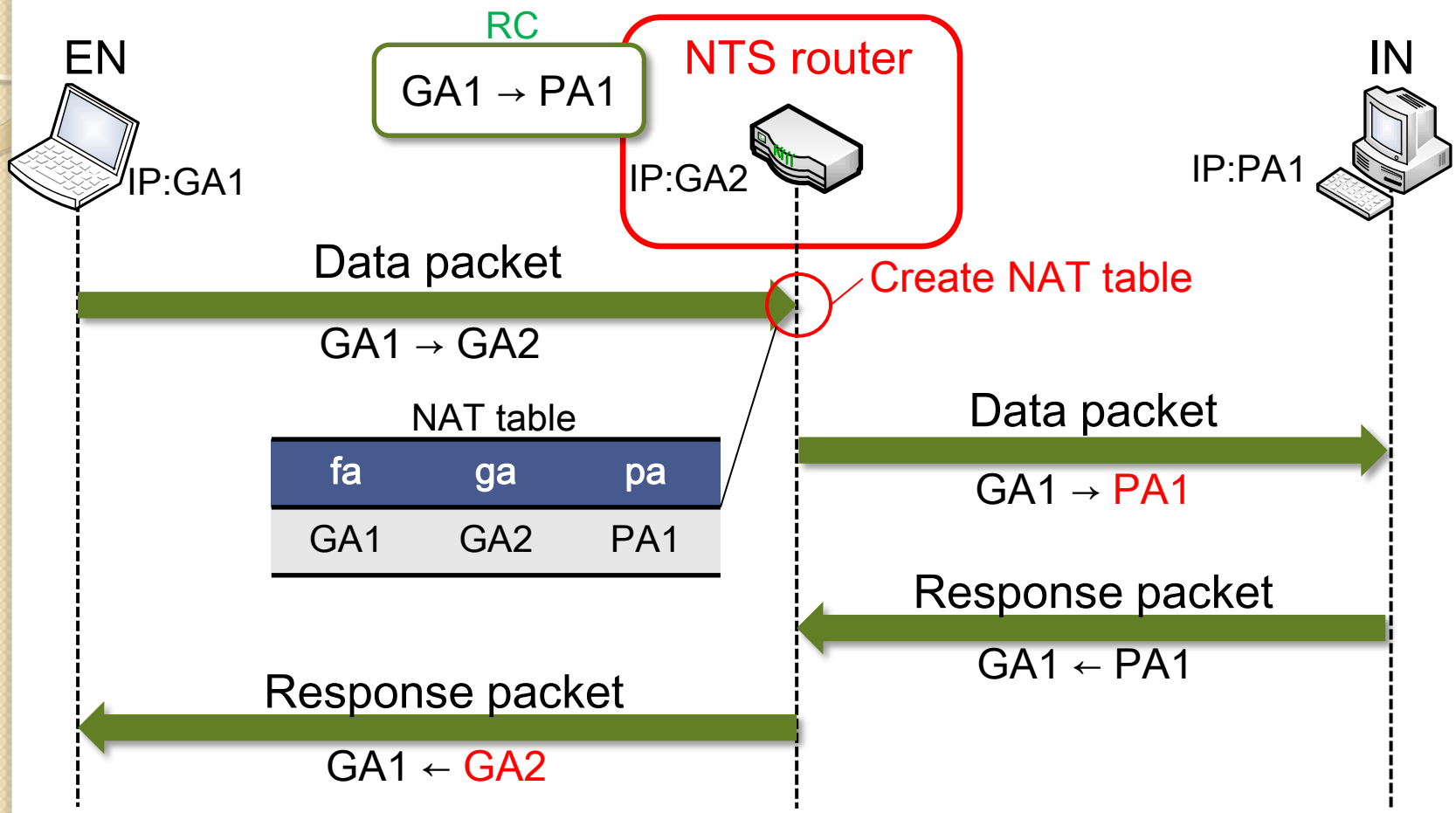
EN → INの通信



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

NTSS (通信開始)

EN → INの通信

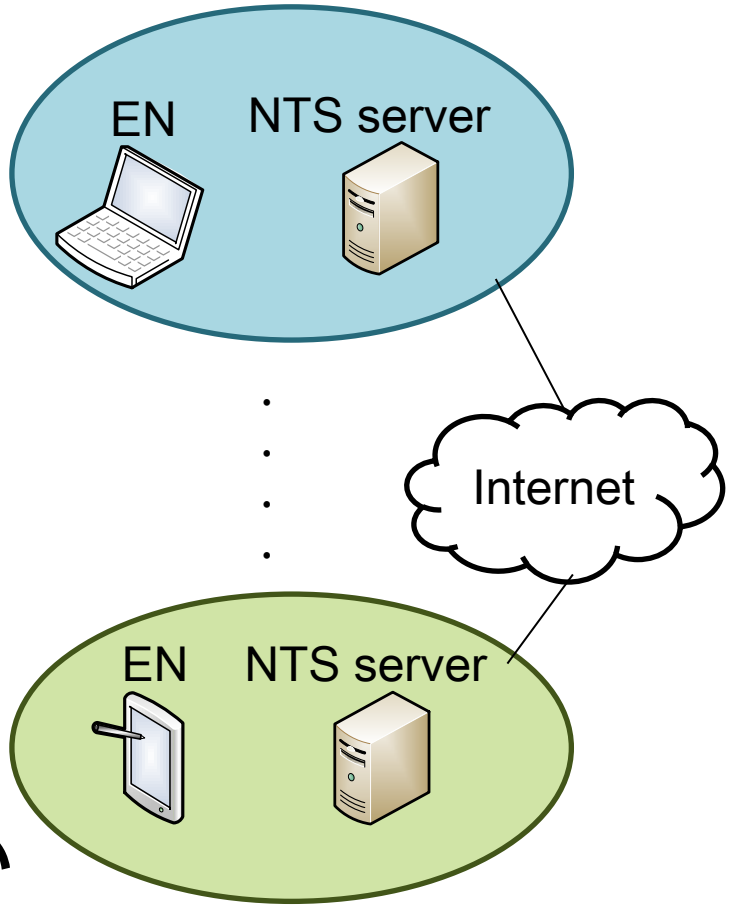


fa(foreign address)：ENのグローバルアドレス
ga(global address)：NTSルータのグローバルアドレス
pa(private address)：INのプライベートアドレス

Watanabe Lab.

NTSSの課題

- ENの登録変更
  - ENが利用するキャッシュサーバをNTSサーバに変更
  - **一般端末は利用できない**



解決方法

ENのキャッシュサーバを置き換える

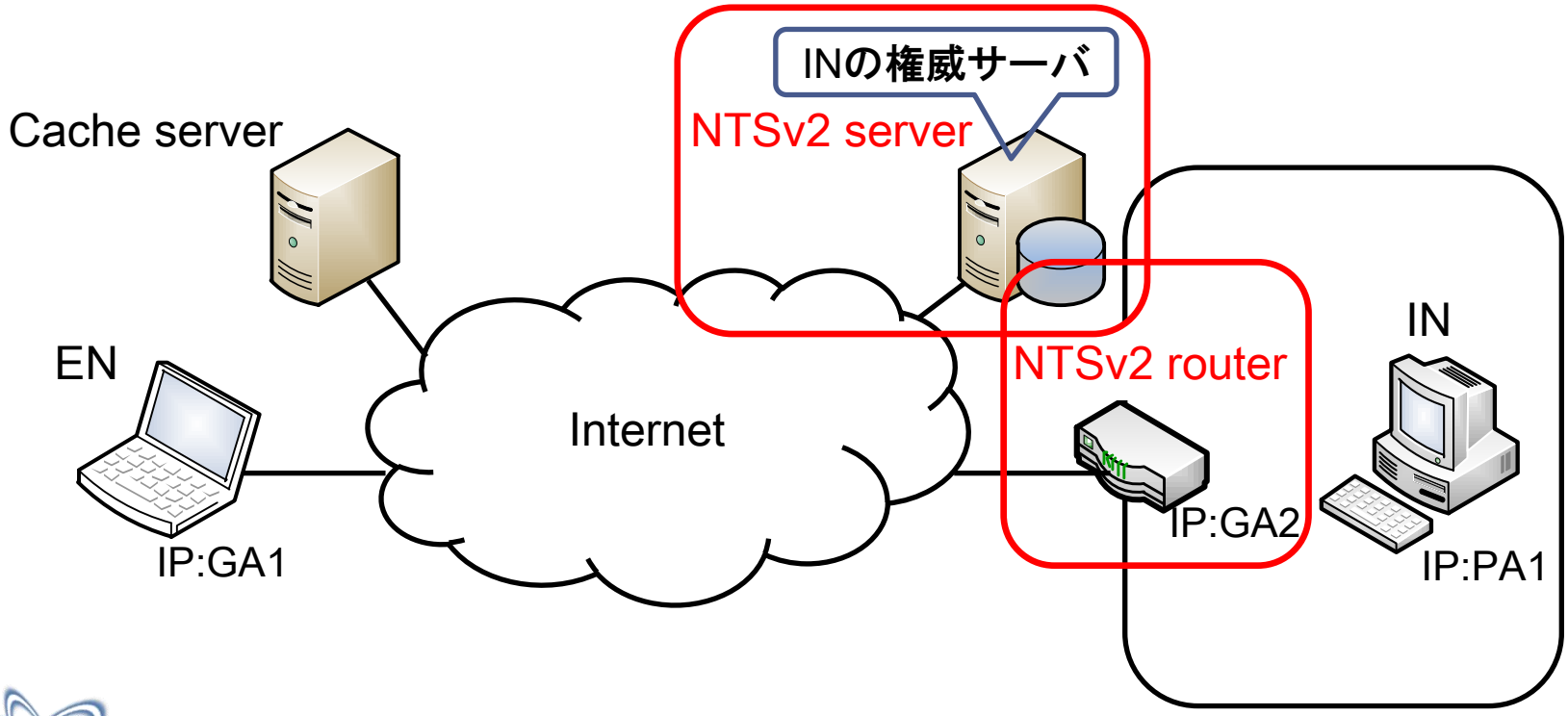
→規模が大きいと現実的ではない

端末の登録変更を不要にする方式

提案方式

NTSSv2

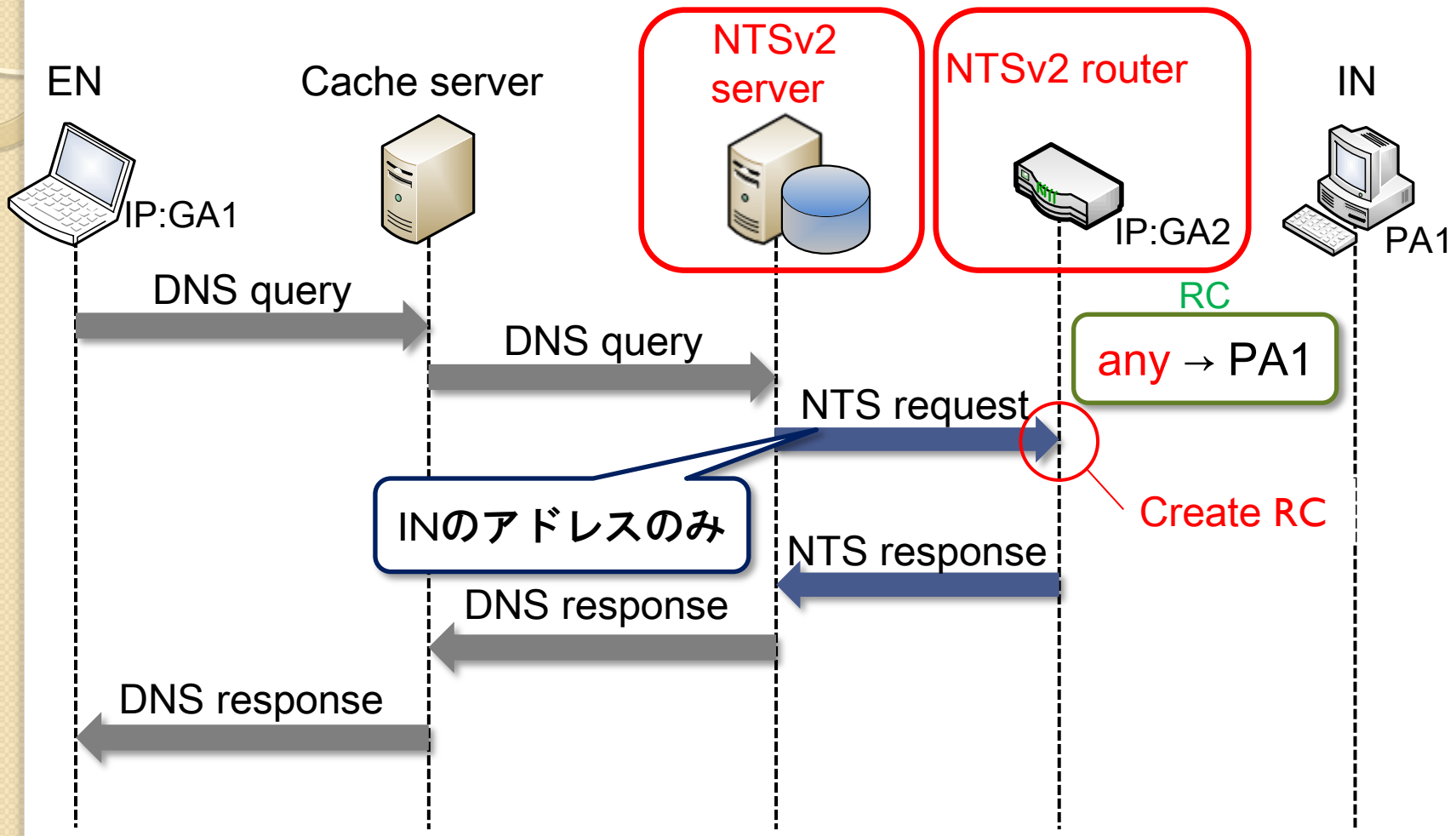
- INの権威サーバとNATを改造
  - 権威サーバ：NTSv2サーバ
  - NAT：NTSv2ルータ



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)

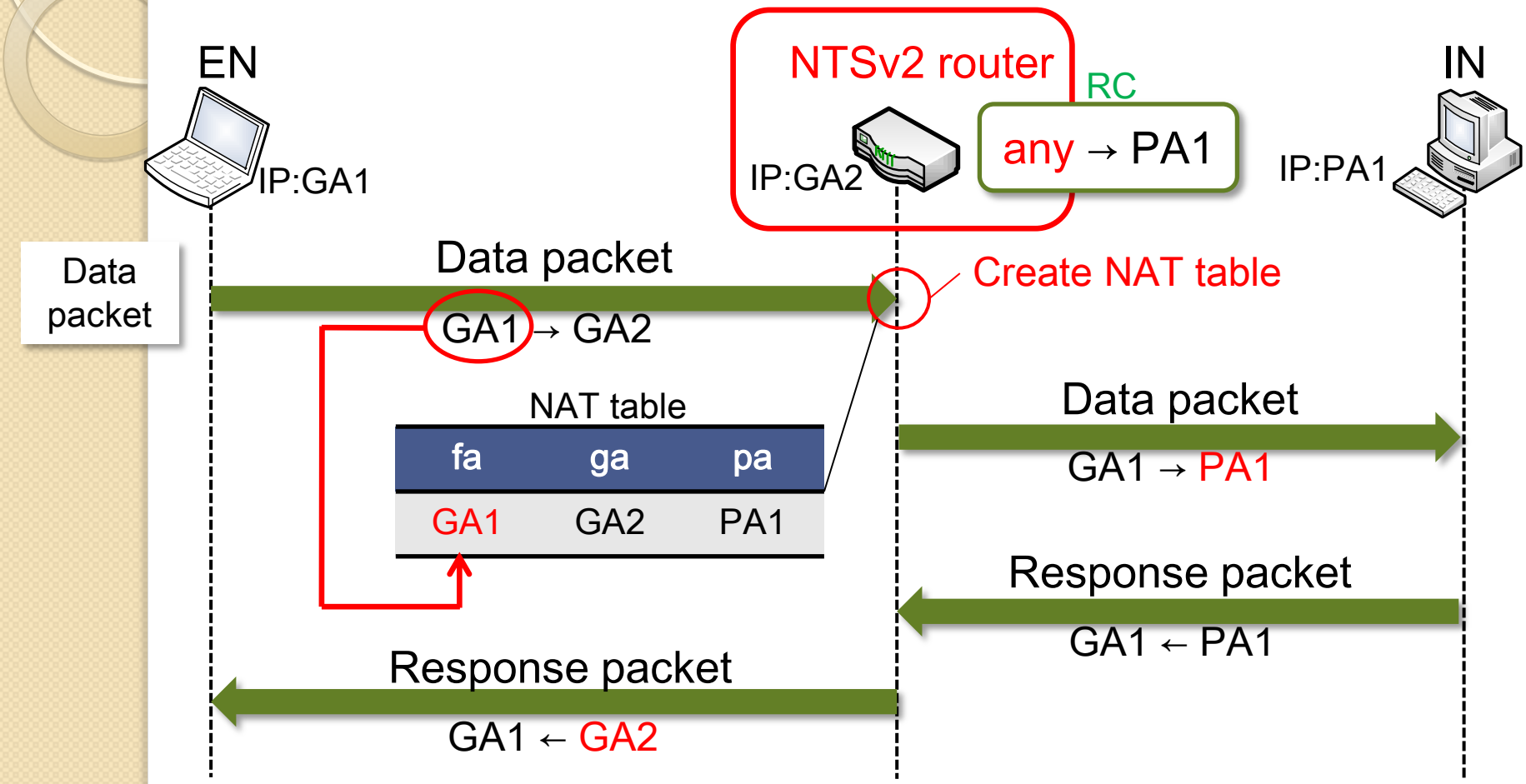
EN → INの通信



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

NTSSv2 (通信開始)

EN → INの通信



fa(foreign address)：ENのグローバルアドレス
ga(global address)：NTSルータのグローバルアドレス
pa(private address)：INのプライベートアドレス

Watanabe Lab.

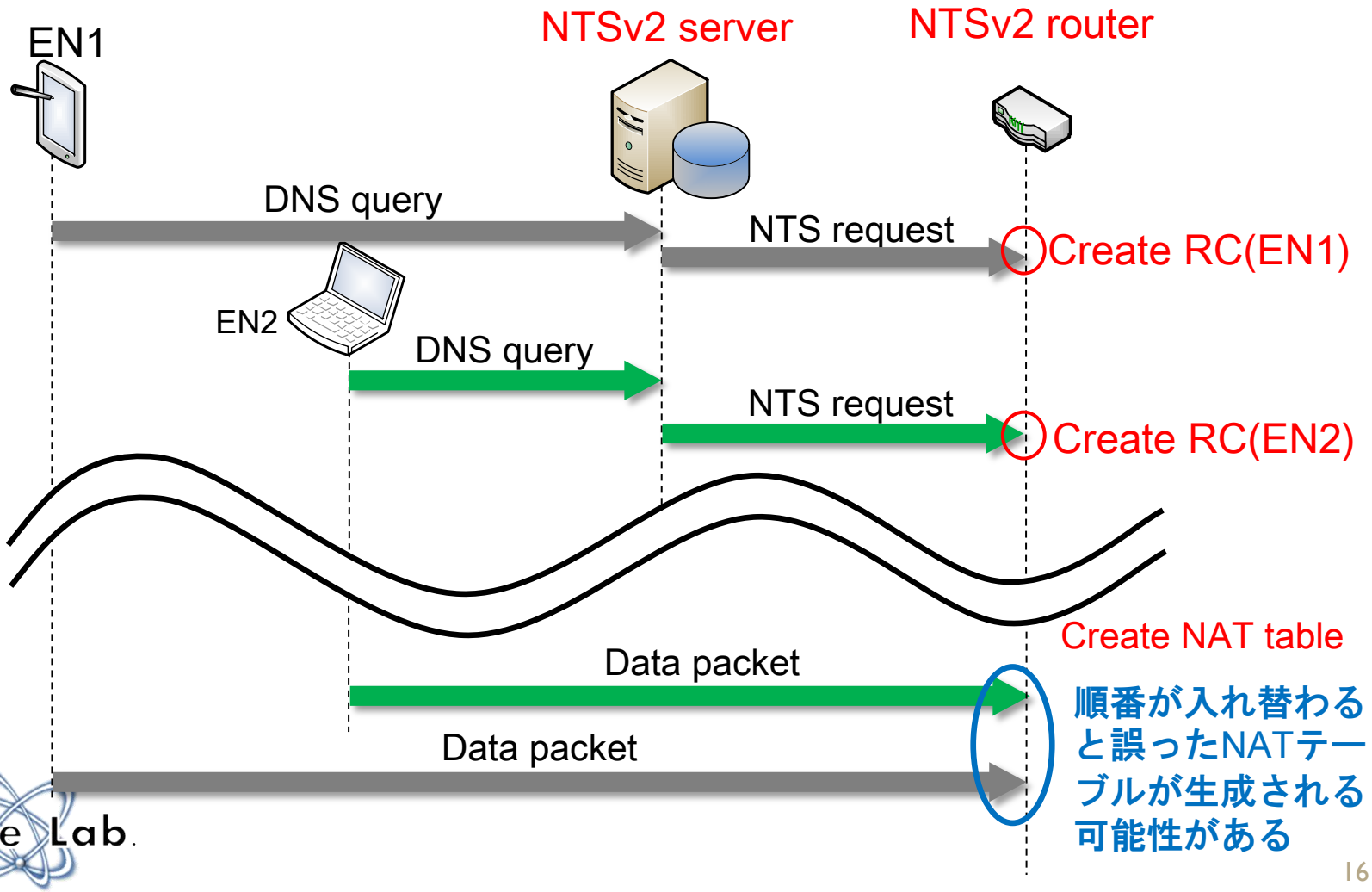
解決すべき課題

- 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

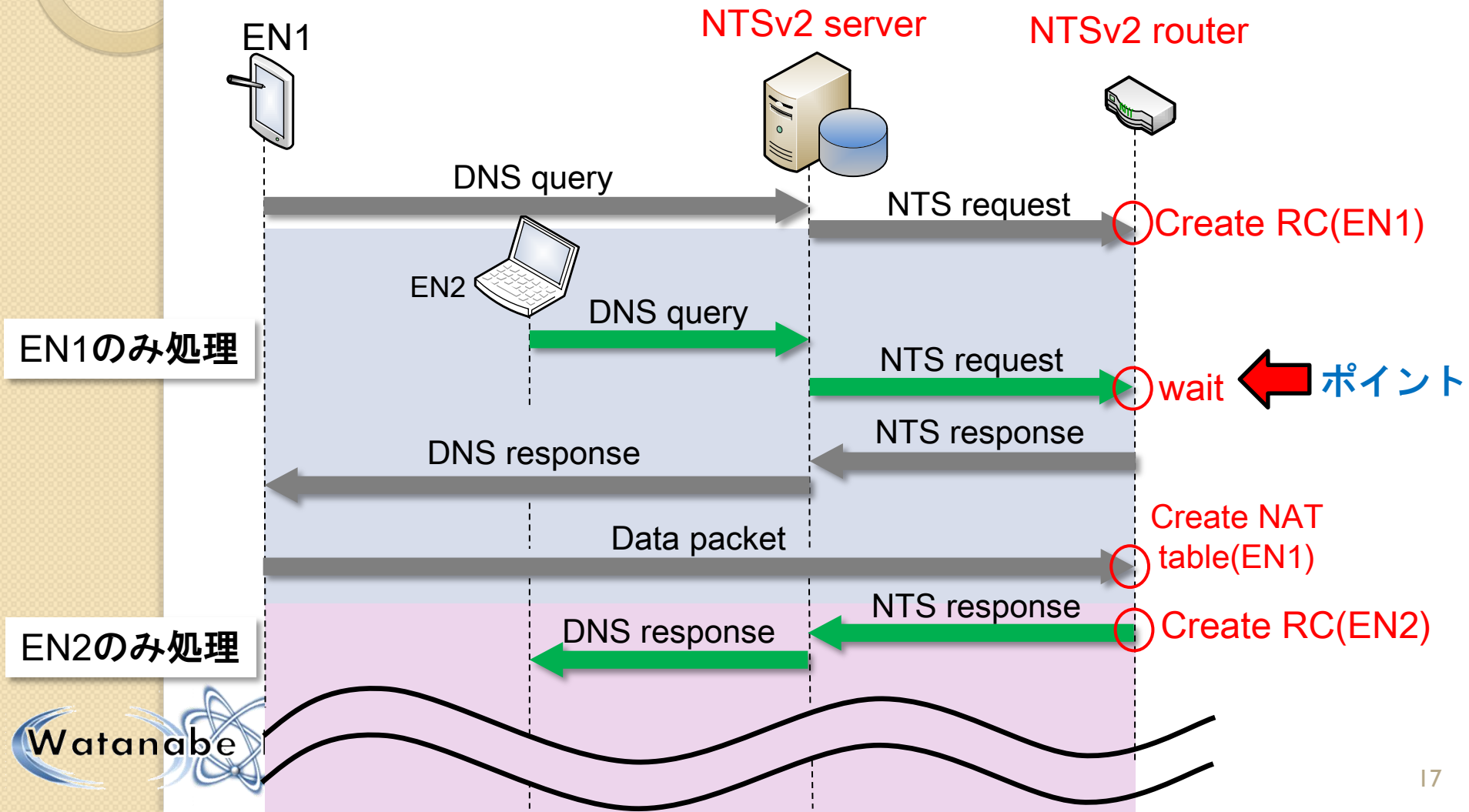
- 2台以上の端末（EN1,EN2）が同時に通信を開始すると，誤ったNATテーブルを生成する可能性がある



Watanabe Lab.

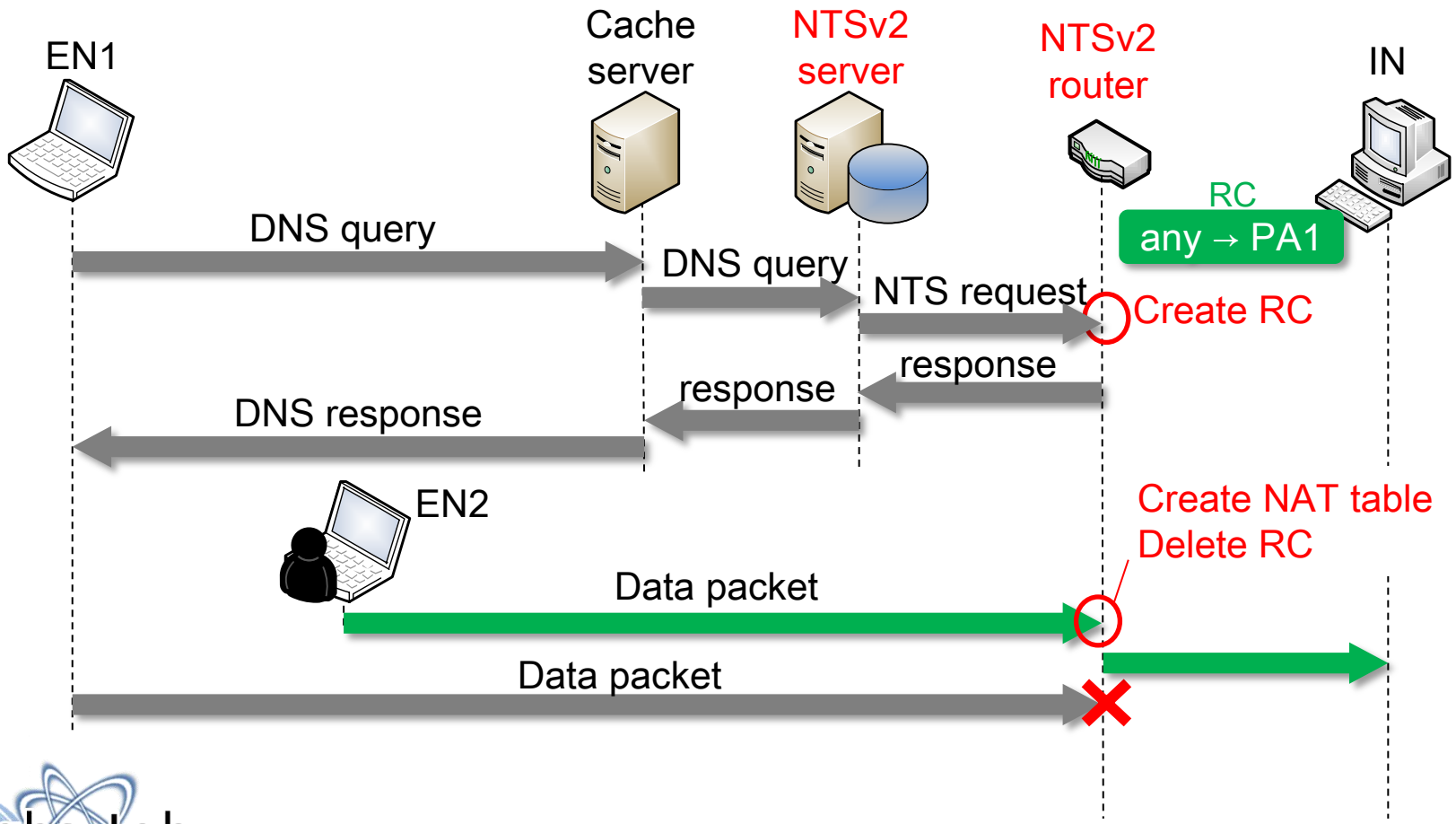
同時問合せ

対策：NTSv2ルータが各々のリクエストに対し，処理をシリアライズすることで解決



通信妨害の課題

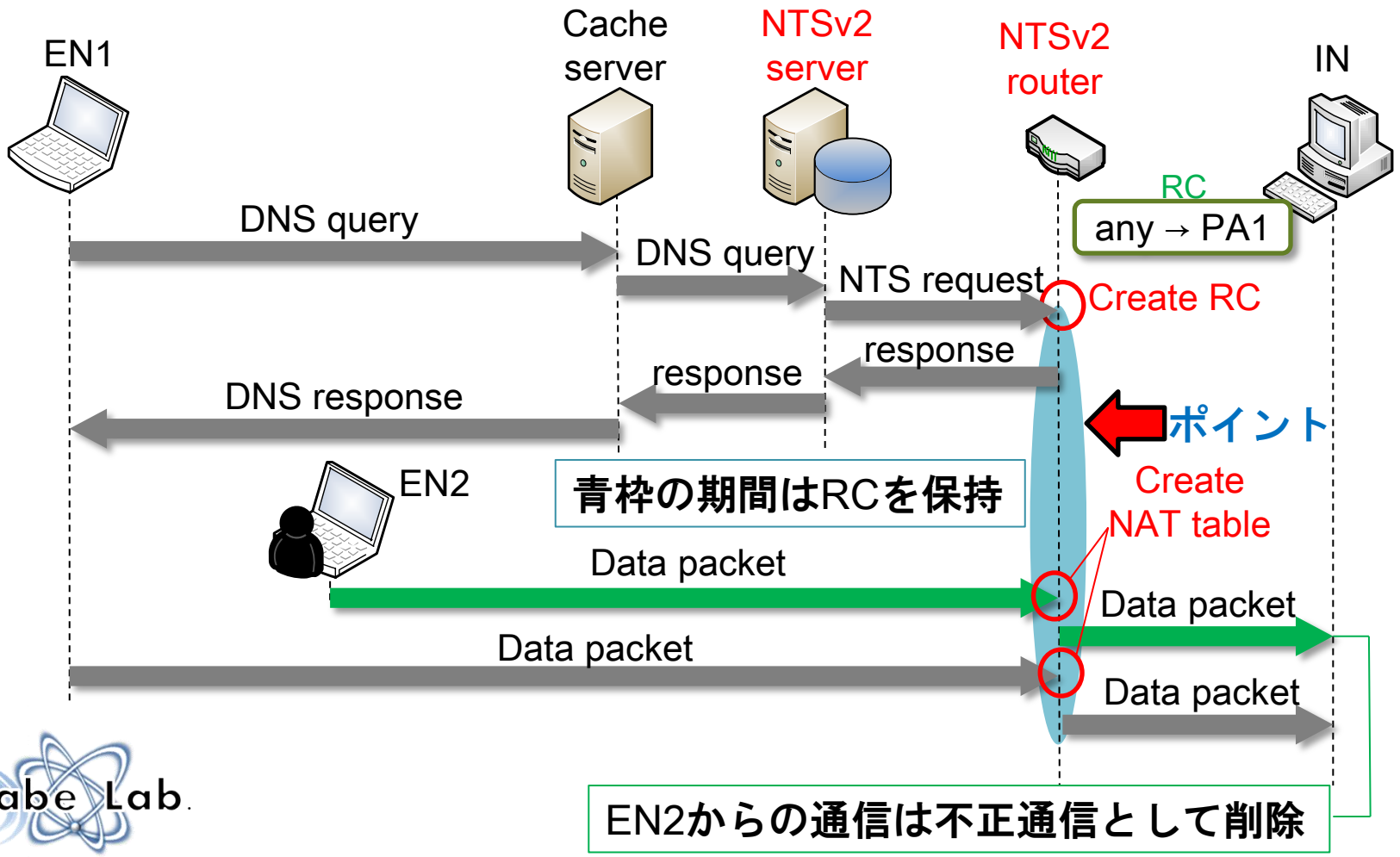
- EN1の通信確立中にEN2が割込むと，通信妨害をされる可能性がある



*一部処理は省略

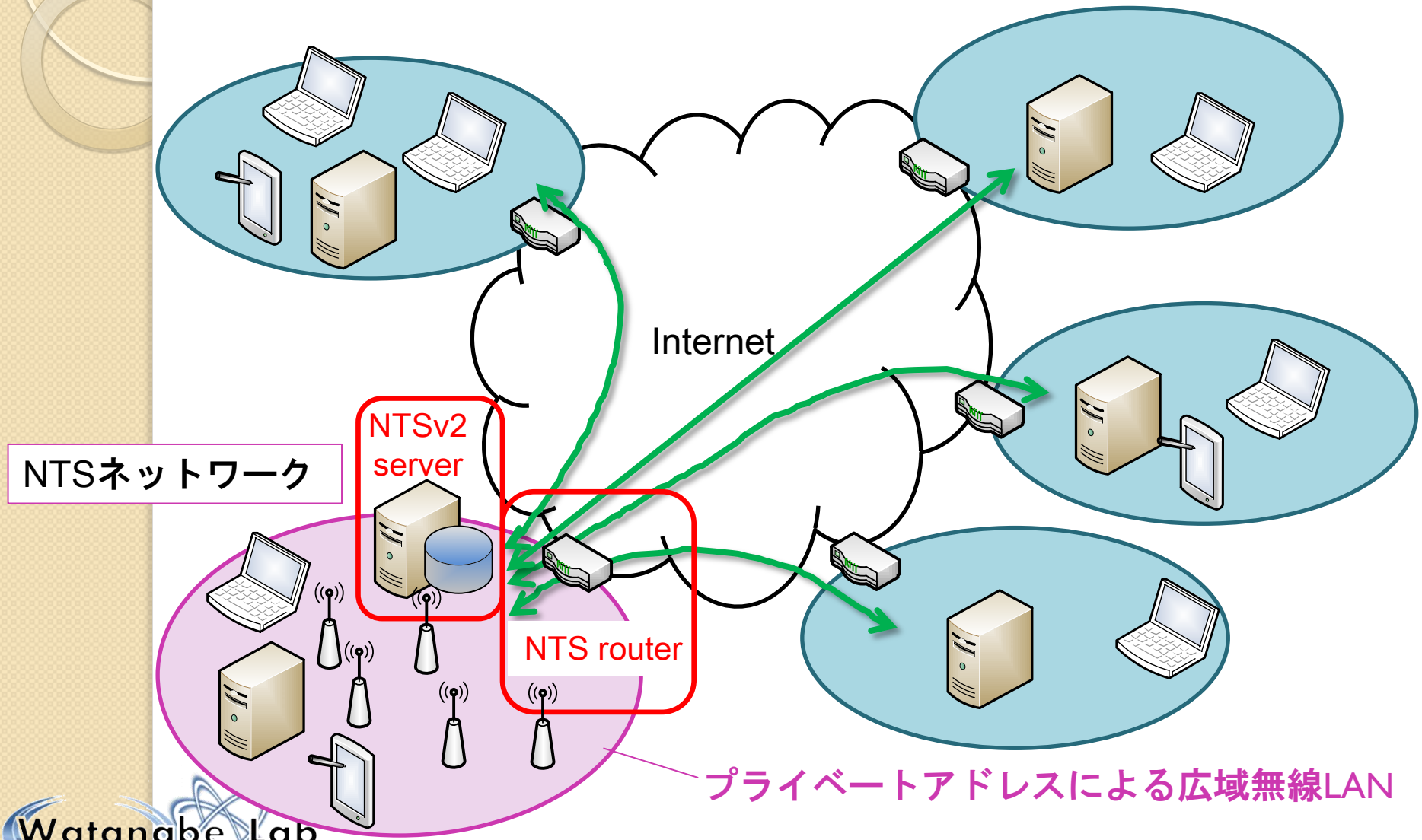
通信妨害

対策：RCを一定期間保持させる
→正規端末の通信の確立を保証



Watanabe Lab.

NTSSv2の適用例



改造は赤枠の２台のみ

Watanabe Lab.

むすび

- NTSv2サーバとNTSv2ルータの連携により，エンド端末の改造と登録変更が不要なNAT越えを実現
  - 同時通信と通信妨害の課題を解決
- 今後
  - 実装の完了
  - ストレステストなどによる評価

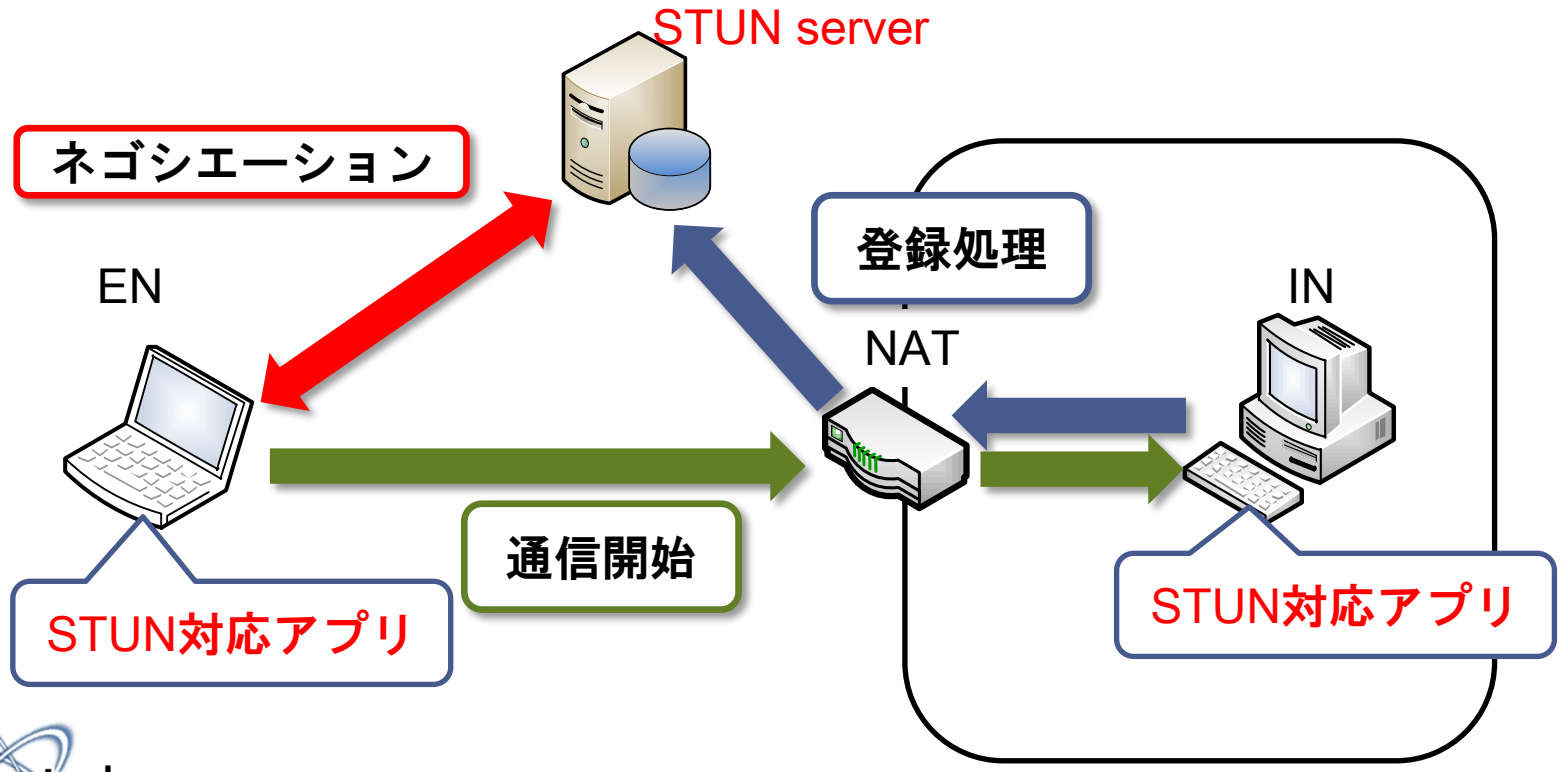
Watanabe Lab.


Watanabe Lab.

補足

STUN
(Simple Traversal of UDP through NATs)

- アプリケーションとSTUNサーバが協調動作

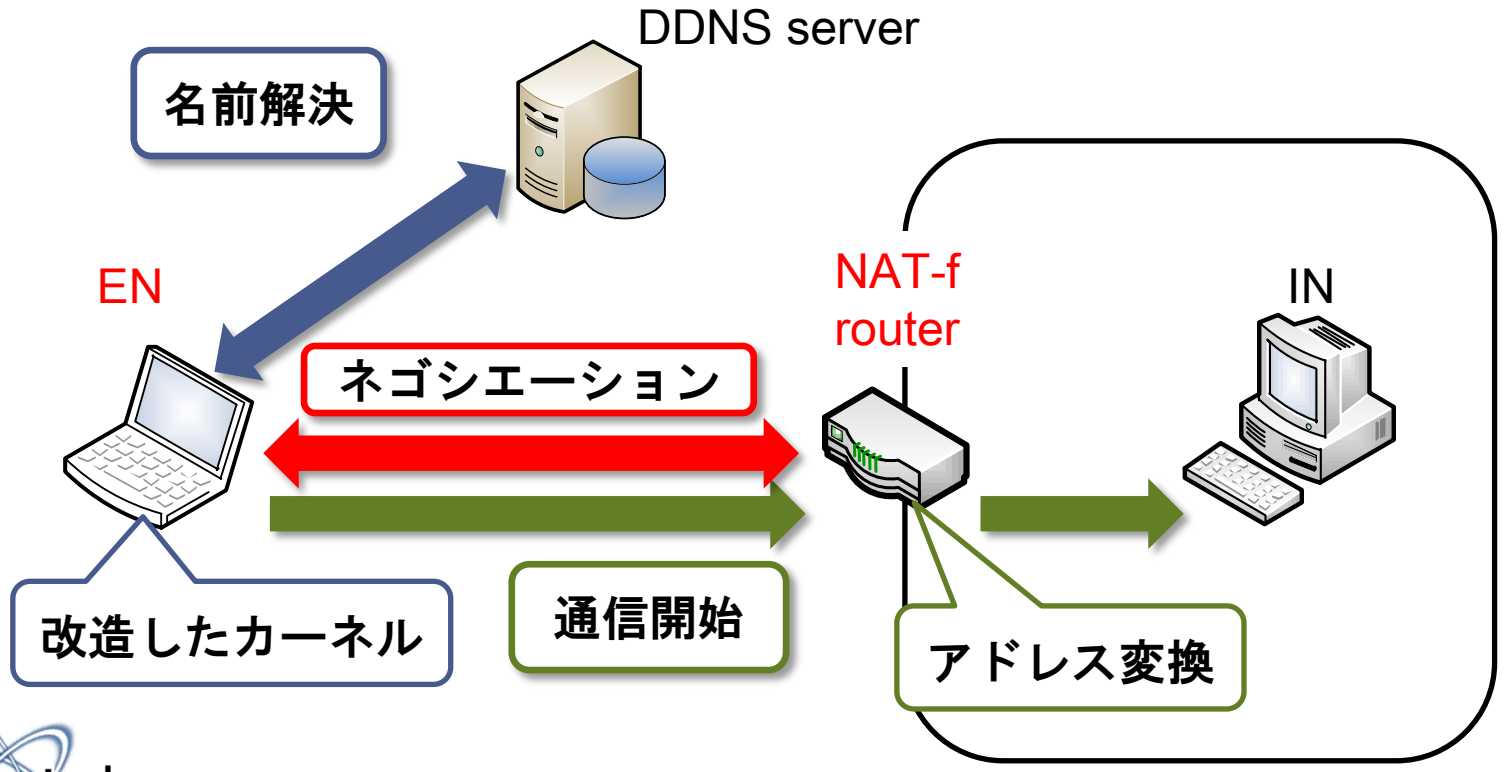


Watanabe Lab.

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

NAT-f (NAT-free protocol)

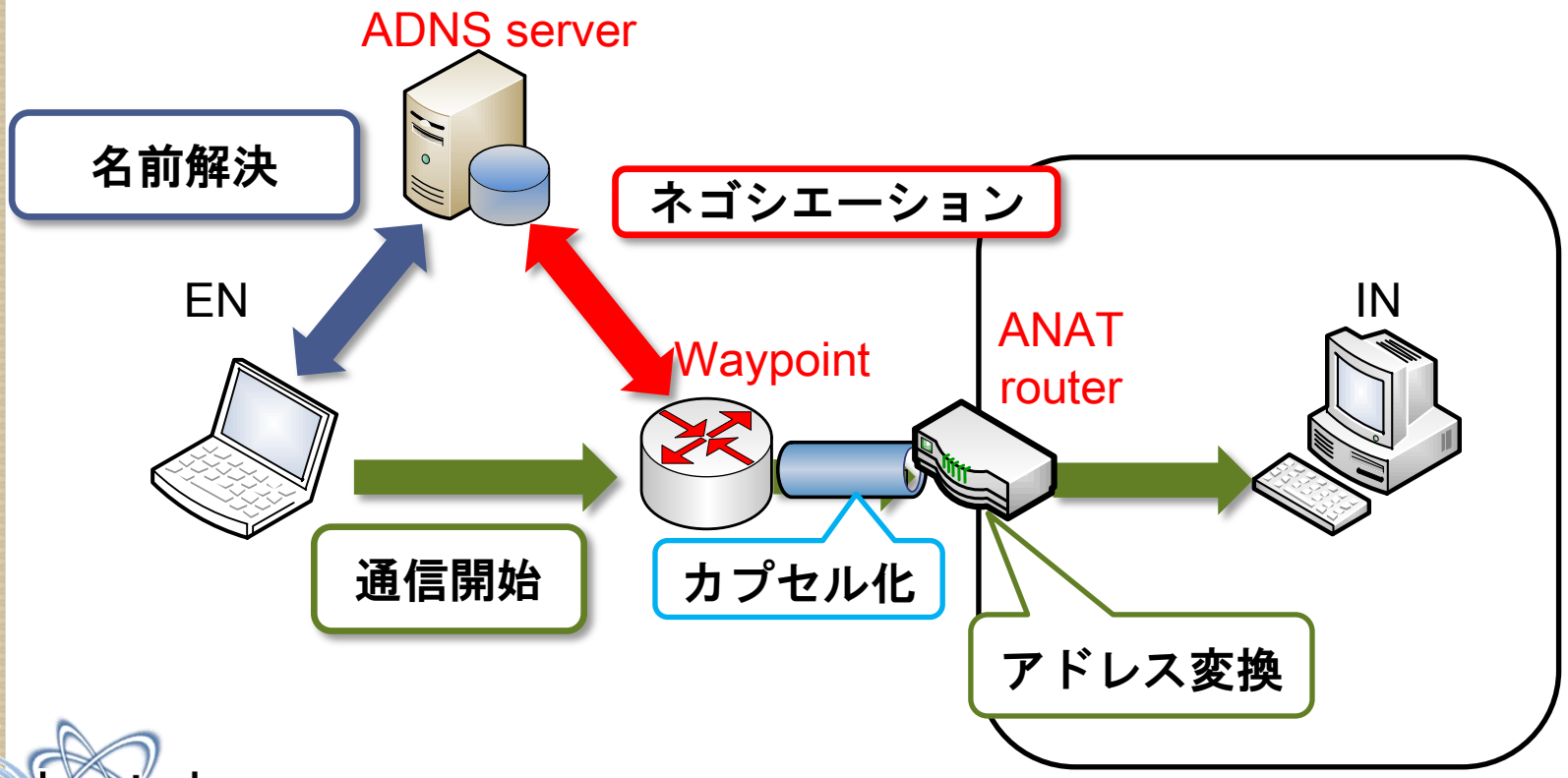
- ENのカーネルやNATを改造し，協調動作
- 既存方式 : NAT-fなど



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).

AVES
(Address Virtualization Enabling Service)

- DNSやNATなどを改造し，協調動作
- **既存方式**：AVES，NTSSなど



Watanabe Lab.

RC保持時間

- 単一リクエストの処理時間から見積もる

- 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

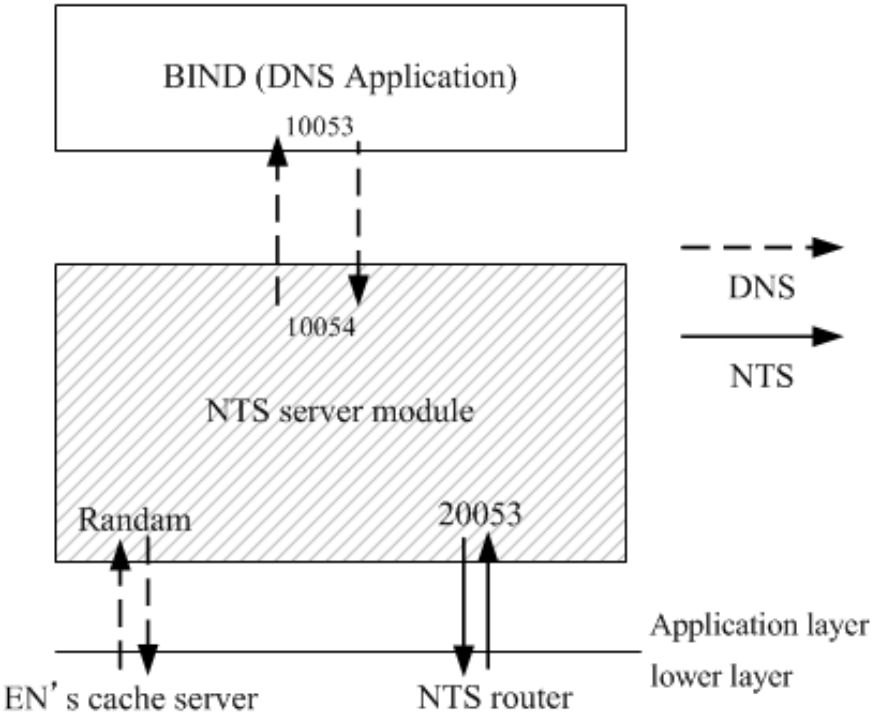
Watanabe Lab.

実装 I

- NTSv2サーバ（FreeBSD）
  - BINDとNTSサーバモジュールで構成する

NTSサーバモジュール：
DNSパケットの中継・解析，
NTSネゴシエーション

BIND：
DNSアプリケーション



Watanabe Lab.

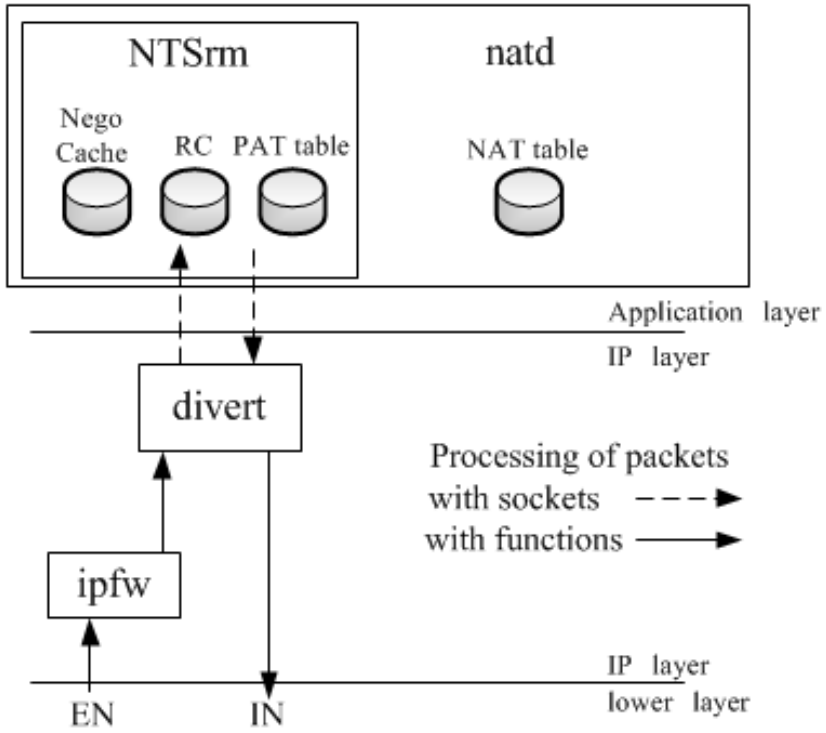
実装2

- NTSv2ルータ（FreeBSD）
  - natd(NAT機能を持つデーモン)にNTSルータモジュールを組み込む

NTSrm(NTSルータモジュール) :
NTSネゴシエーションの処理，RCの生成，ダミーパケットの生成

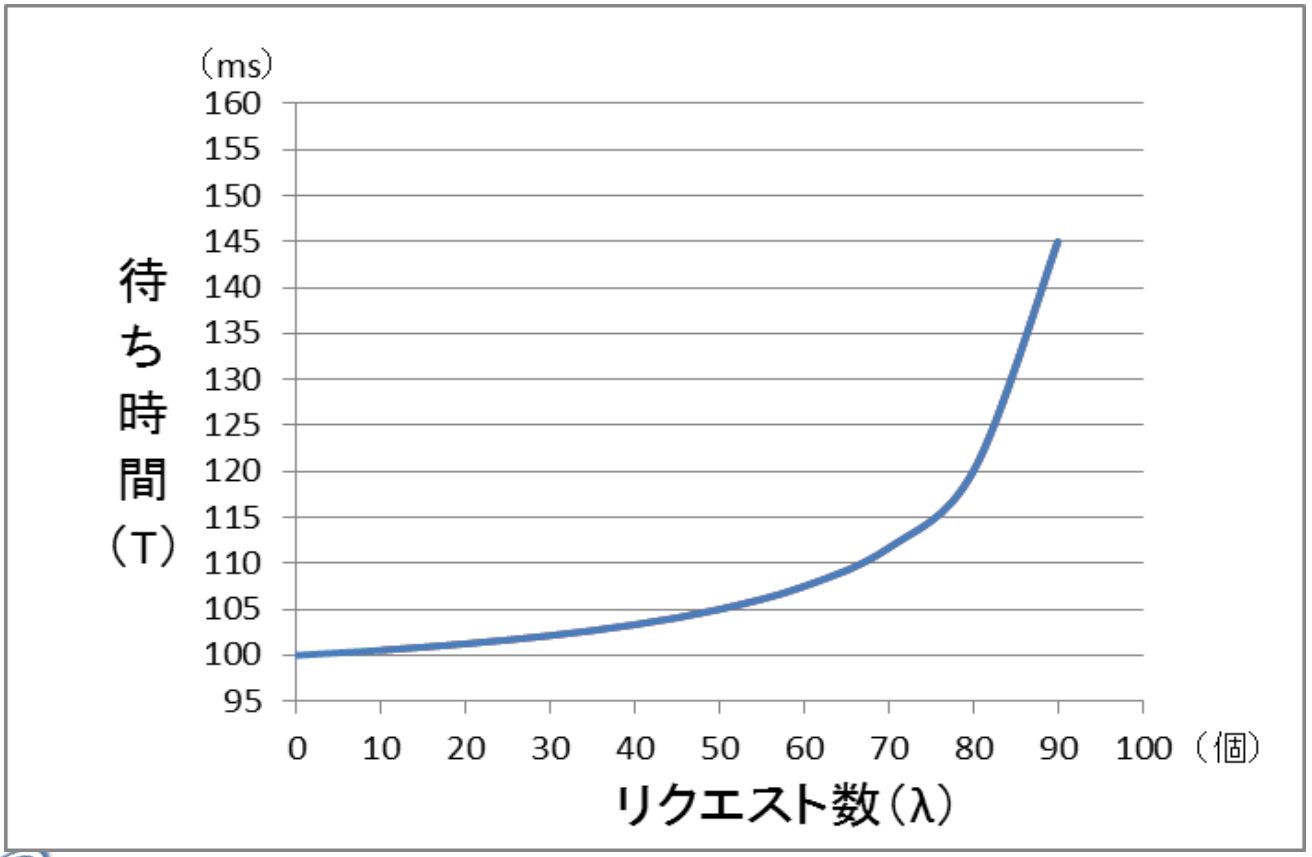
divert :
natdのパケット取り出しをサポートするソケット

ipfw :
ファイアウォールのモジュール



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）



Watanabe Lab.