

# 双方向通信が可能な無線メッシュネットワークのインターネット接続方法

080430093 松尾 辰也  
渡邊研究室

## 1. はじめに

近年、無線通信の需要が高まっている。中でも無線メッシュネットワークは無線 LAN インフラを容易に構築できる有用な技術である。無線メッシュネットワークは災害発生時に被災地などに展開することにより、迅速にネットワークを再構築できる。このとき、ネットワークのグローバルアドレスの数が十分に確保できない可能性があるため、メッシュネットワークはプライベートアドレスを使用できることが望ましい。プライベートアドレスを使用するためには NAT を設置する必要があるが、NAT 越え問題によりインターネット側から通信を開始することができなくなるという課題がある。そこで、本稿ではこの課題を解決するために無線メッシュネットワーク WAPL (Wireless Access Point Link) [1] と NAT 越え技術 NTSS (NAT Traversal Support System) [2] を組み合わせる方式を提案する。この方法により、被災地に WAPL を展開し、外部ネットワークと自由に通信を行うことが可能となる。

## 2. 要素技術

### 2.1 WAPL

WAPL はシームレスハンドオーバが実現できる独自の無線メッシュネットワークである。アドホックルーティングプロトコルと WAPL の機能を完全に独立させることにより、ルーティングプロトコルを自由に選択することができる。また、WAP と呼ばれる各 AP が近隣 WAP の通信状況を常に把握しておくことにより、ハンドオーバ時のパケットロスを大幅に低減させている。

### 2.2 NTSS

NTSS はユーザ端末の改造が不要な独自の NAT 越え技術である。NTSS は外部ノード EN (External Node) のプライマリ DNS サーバと NAT ルータを改造し、両者が協調することにより、NAT テーブルを強制的に生成することで NAT 越え通信を実現する。

## 3. 提案方式

提案方式では、WAPL をプライベートアドレスで展開し、WAPL のゲートウェイに NTSS と類似機能を搭載した機器を設置することにより、双方向の通信を可能とする。

### 3.1 NTSSv2

NTSS は EN 側の DNS サーバを改造することにより NAT 越えを実現していたが、NTSSv2 では IN (Internal Node) のアドレスを管理する DDNS (Dynamic DNS) 側を改造することにより、EN 側のプライマリ DNS 登録変更を不要とした。また、DHCP と DDNS と WAP を一体化させた NTS WAP という装置により、動的に IN の名前と NTS WAP のグローバル IP アドレスの対応関係を RR (Resource Record) に登録し、IN の名前とプライベート IP アドレスの対応関係を PHL (Private Host List) と呼ぶテーブルに生成できるようにした。

### 3.2 NTSSv2 のシーケンス

図 1 に NTSSv2 のシーケンスを示す。NTS WAP は IN 側の DDNS に改造を行った装置である。また、NTSWAP の配下は WAPL で構成されている。

EN はプライマリ DNS に対して alice の名前解決を依頼する。NTS WAP はプライマリ DNS からの問合せを受けて EN が IN に通信要求したいことを NTS モジュールに通知するために、EN と IN の IP アドレス関係を RC (Request Cash) として生成する。ただし、図 1 の DNS query では EN 側の IP アドレスを特定できないので、ソースアドレスの部分は "any" としておく。EN には NTS WAP のグローバルアドレス (GA2) が報告される。

名前解決後、EN は NTS WAP にむけてパケットを送信する。NTS WAP は NTS モジュールにより RC を参照して "any" の部分を EN の IP アドレスとして NAT テーブルを作成する。これにより、パケットはアドレス変換されて、WAPL によるアドホック通信によりエンドエンドで通信が可能となる。

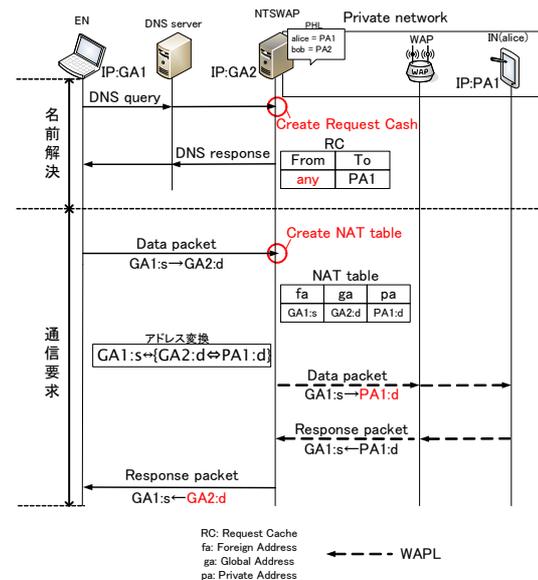


図 1: NTSSv2 のシーケンス

## 4. まとめ

本稿では NTSSv2 により、被災地に容易に WAPL を展開できる方式を提案した。今後は実装を進めていく予定である。

### 参考文献

- [1] 伊藤, 他. 無線メッシュネットワーク "WAPL" の提案とシミュレーション評価, 情報処理学会論文誌, Vol. 49, pp. 1859-1871, Jun.2008.
- [2] 宮崎, 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, pp. 1873-1880, Sep.2010.



# 双方向通信が可能な無線メッシュネットワーク ワークのインターネット接続方法

名城大学 理工学部 情報工学科  
渡邊研究室  
080430093  
松尾辰也

Watanabe Lab.



# 研究背景

## ▶ 災害発生時

- ネットワークインフラが破壊される場合がある
- 迅速に通信インフラを再構築する必要がある

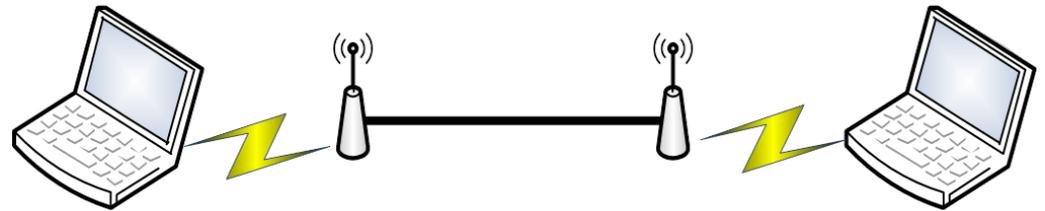
## ▶ 無線ネットワークの普及

- 配線が不要
- 無線メッシュネットワーク技術の発展

# 無線LAN

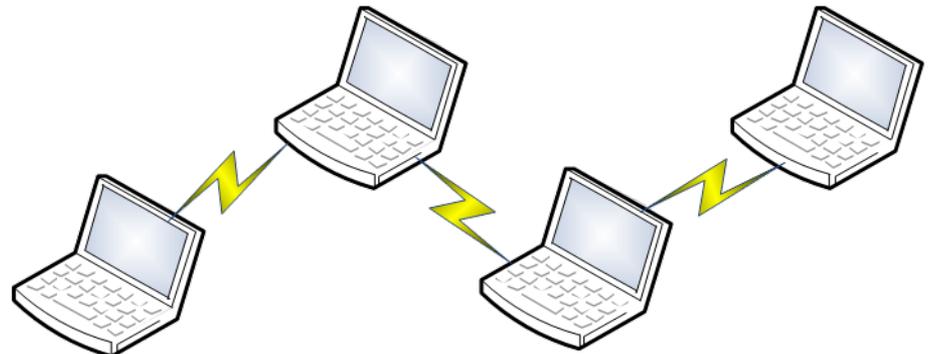
## ▶ インフラストラクチャーモード

- 一般的な無線LANの方式
- AP(アクセスポイント)間は有線で接続



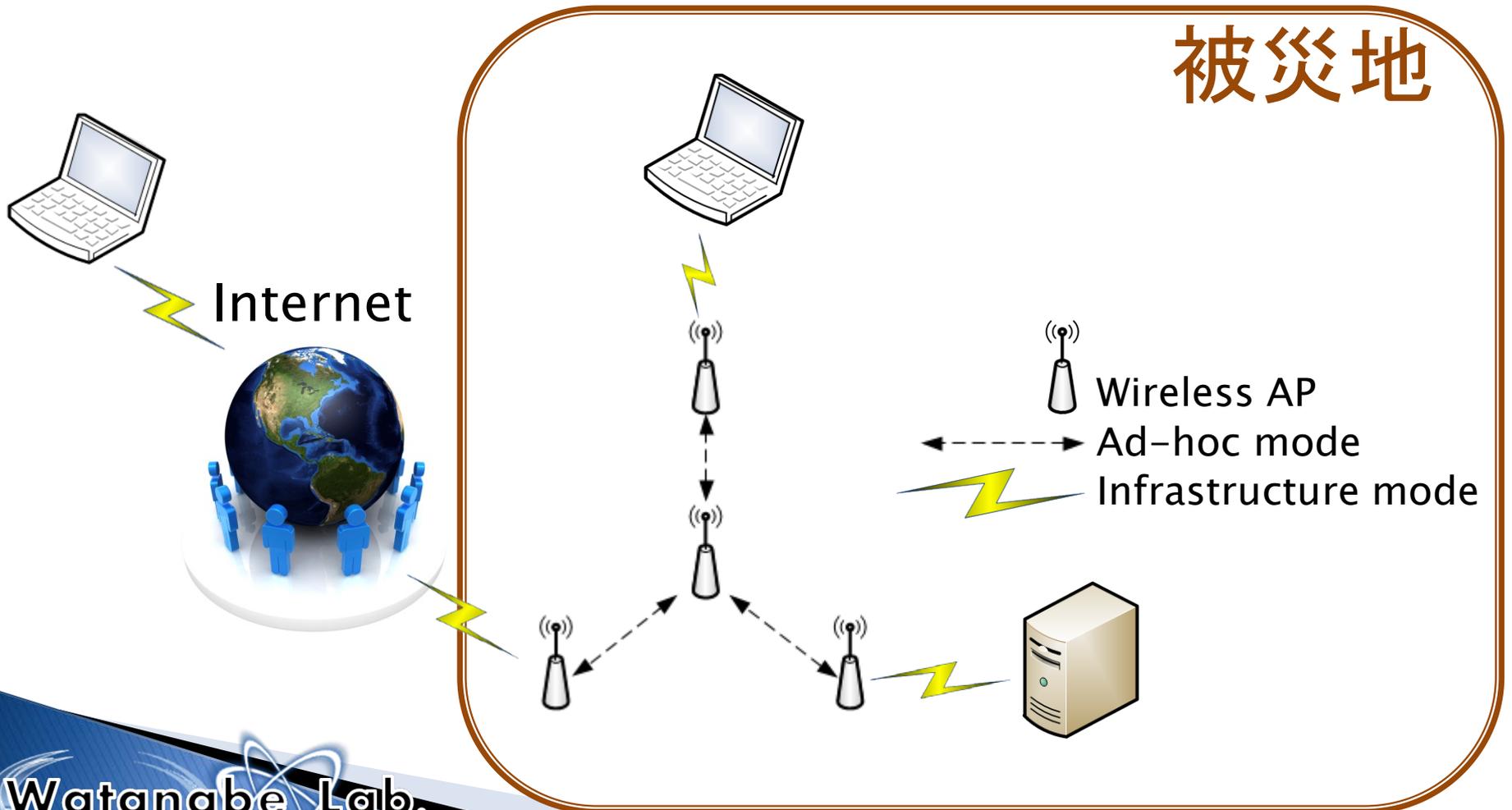
## ▶ アドホックモード

- 端末同士が直接通信を行い構築するネットワーク



# 研究目的

- ▶ 無線メッシュネットワークで迅速に通信インフラを再構築する



# 要件(1/2)

- ▶ 無線メッシュネットワークはプライベートアドレスで構築する(グローバルアドレスが枯渇しているため)

NAT(Network Address Translation)を使用

- アドレスが不足する心配がない
- 設置が簡単 → 被災地などに適している

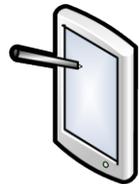
# NAT越え問題

- ▶ 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

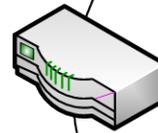


EN1

インターネット

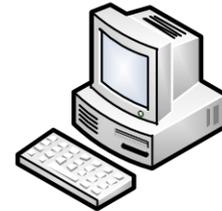


EN2



NAT router

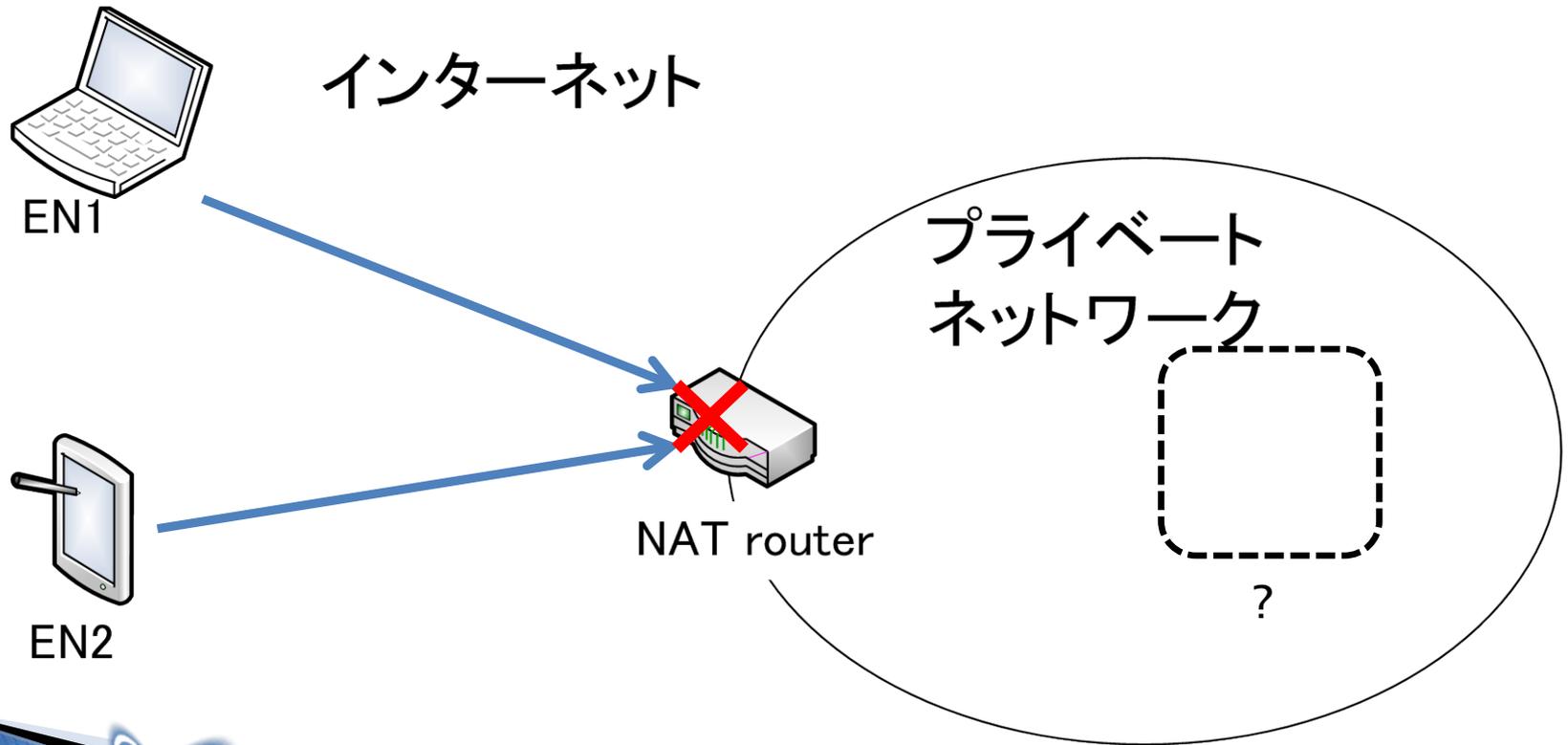
プライベート  
ネットワーク



IN

# 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



# 要件(2/2)

- ▶ 外部の人は既存のシステムをそのまま使える  
→ 端末は改造しない



端末を改造しないでいかにNAT越えを実現するか



# 提案

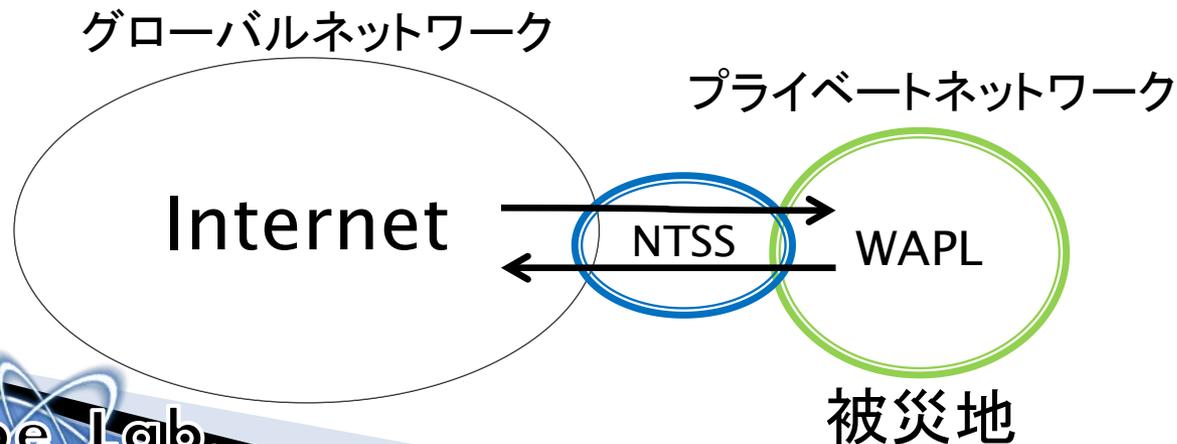
無線メッシュネットワーク

+

NAT越えシステム

WAPL (Wireless Access Point Link)

NTSS (NAT Traversal Support System)



# 要素技術

## ▶ WAPL

- 独自のメッシュネットワーク
- シームレスハンドオーバ

## ▶ NTSS

- 独自のNAT越え技術
- 端末を改造しない

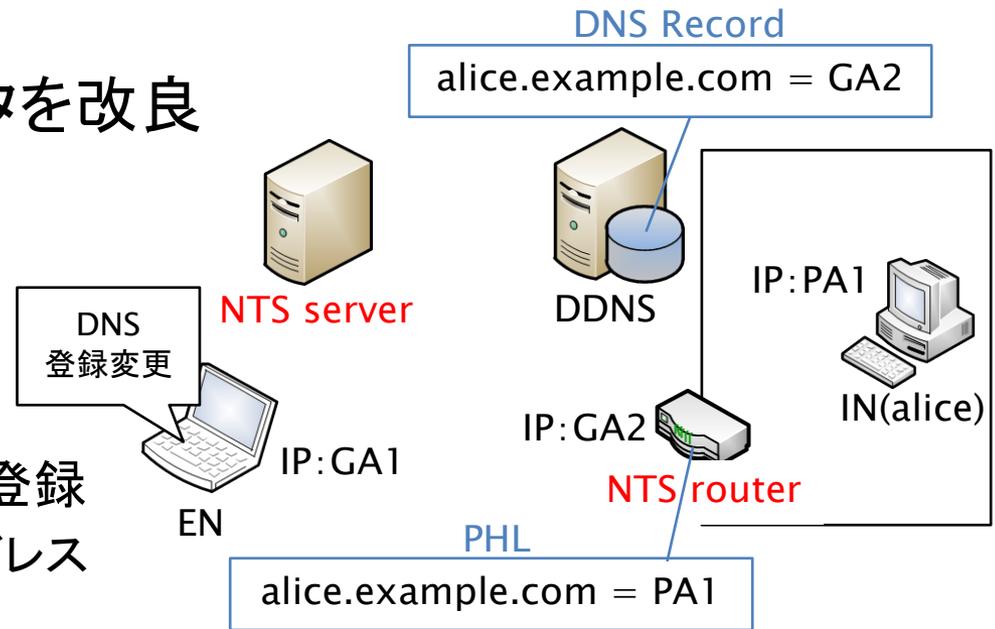
# NTSSの構成

## ▶ DNSサーバとNATルータを改良

- DNSサーバ:NTSサーバ
- NATルータ:NTSルータ

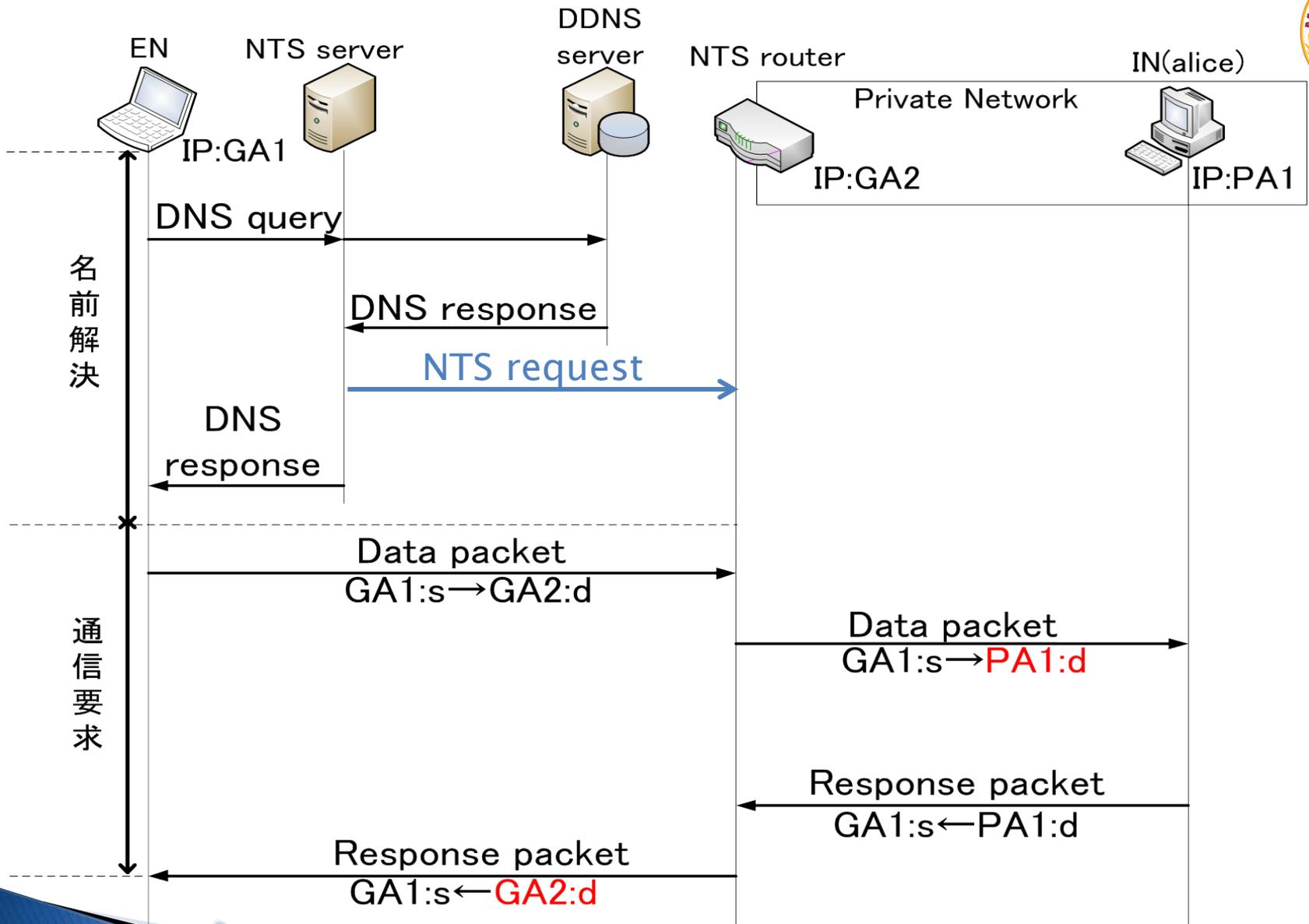
## ▶ 事前設定

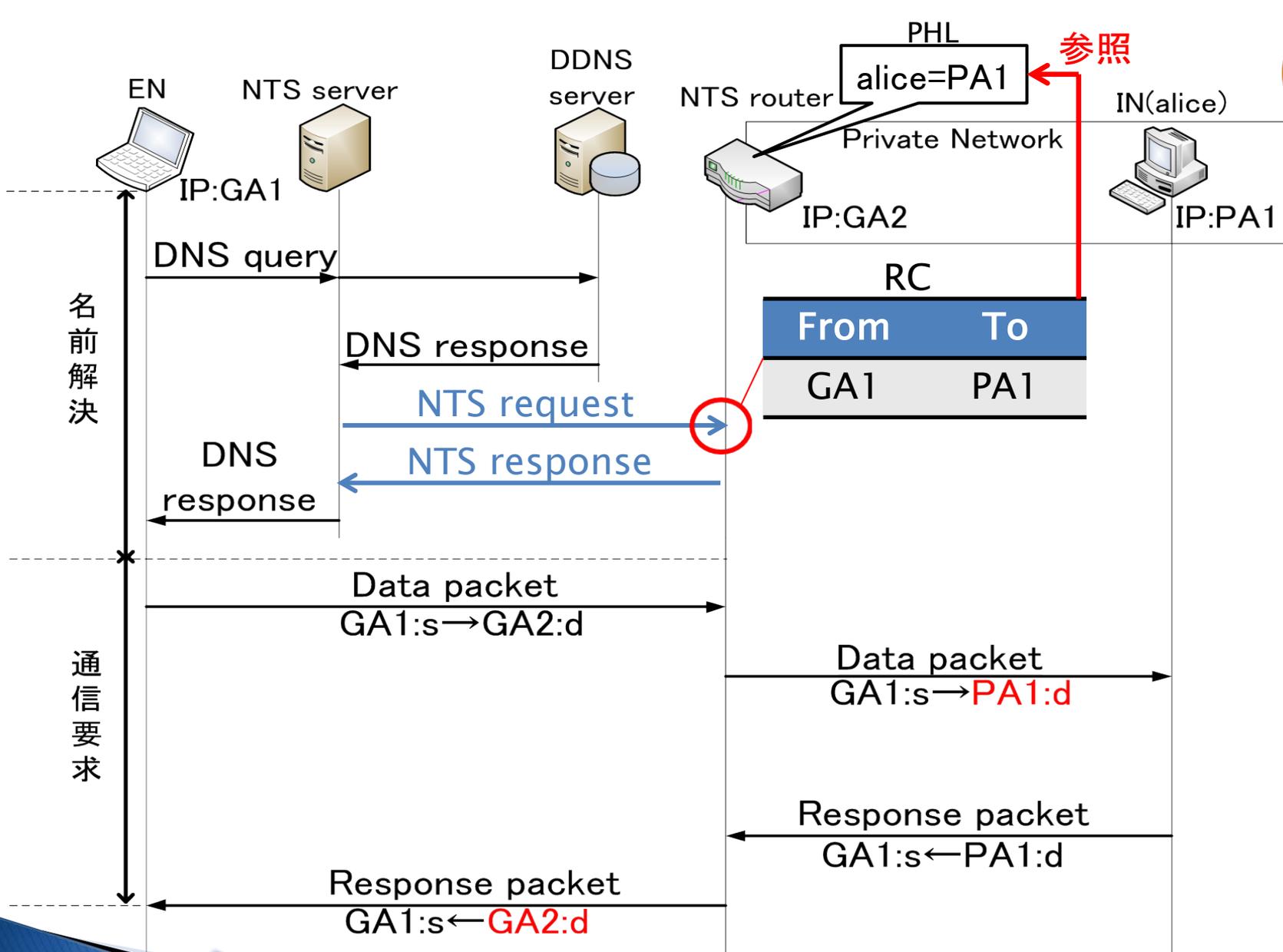
- DDNS(Dynamic DNS)へ登録
  - FQDNとNTSルータのIPアドレス
- NTSルータへ登録
  - FQDNとINのプライベートアドレス
  - PHL(Private Host List)
- ENのプライマリDNSをNTSサーバに設定

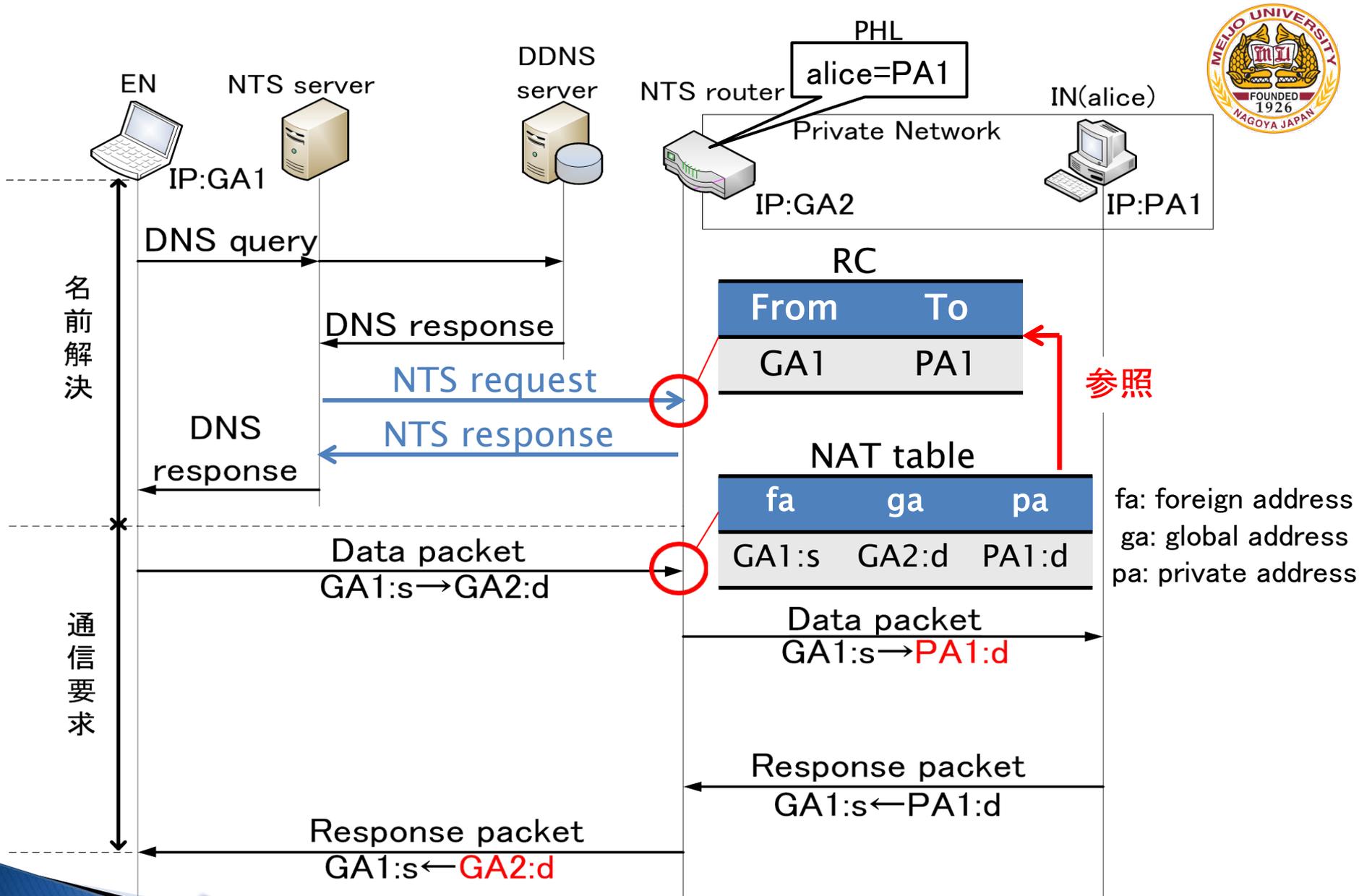




# NTSSの動作シーケンス



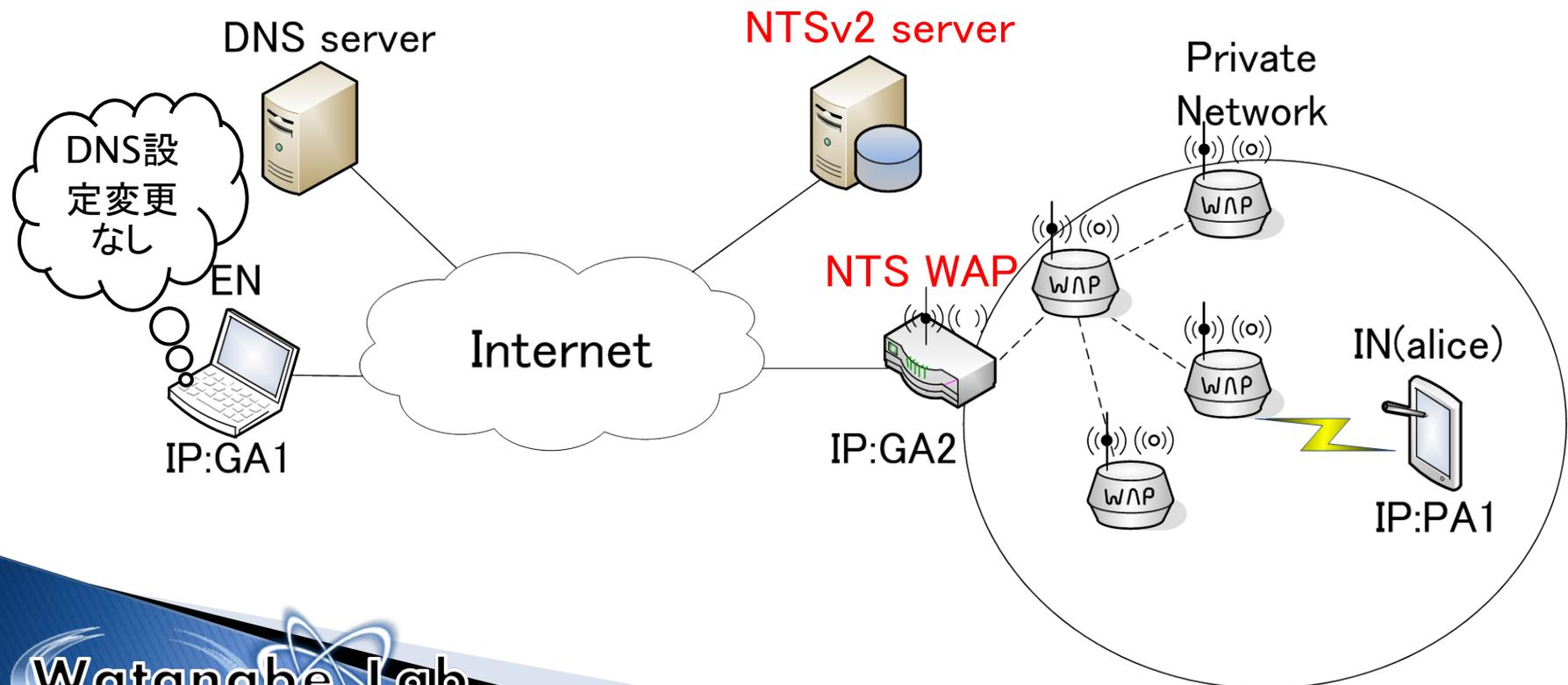




# 提案方式の概要

## ▶ NTSSv2

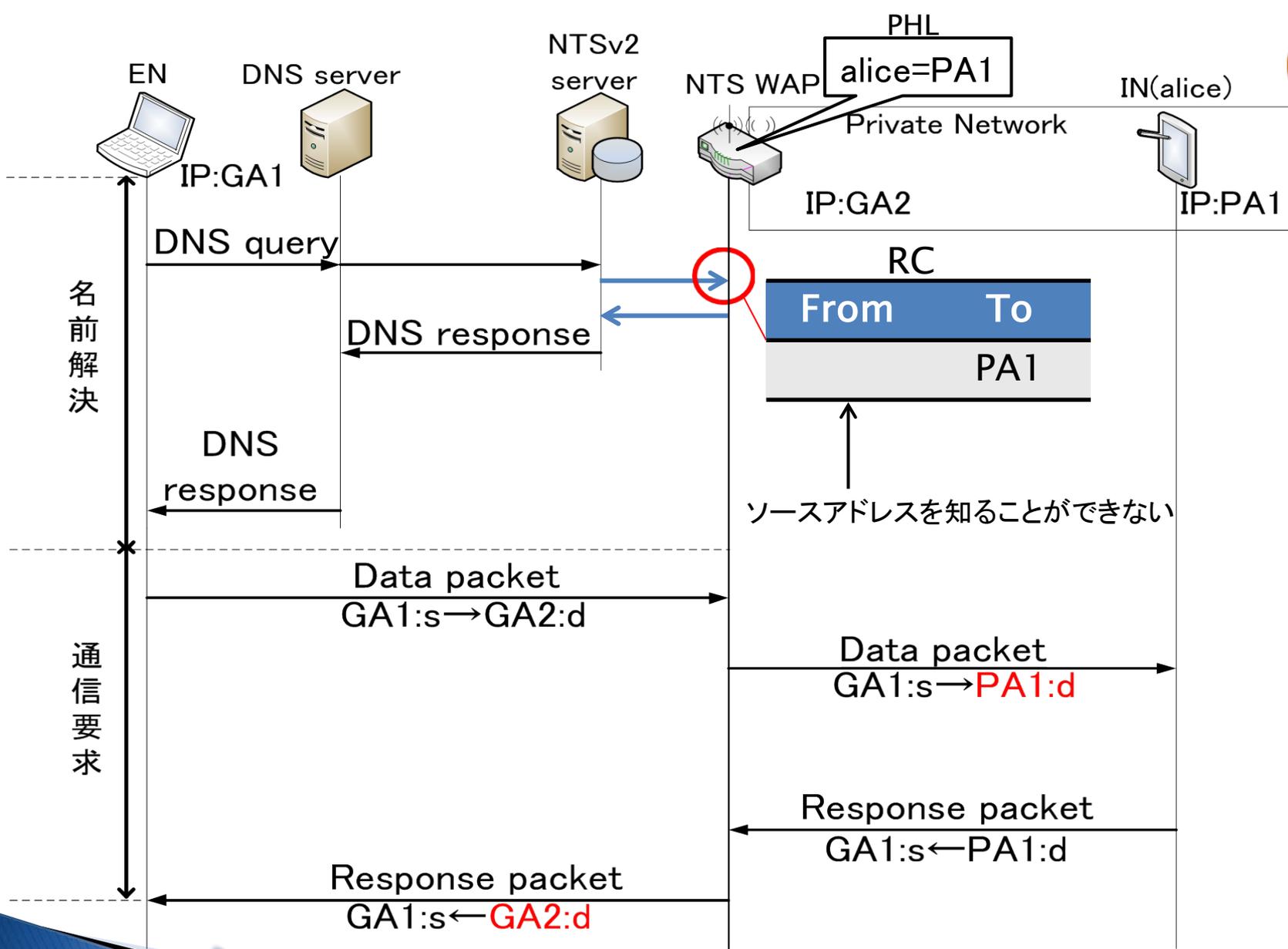
- INのアドレスを管理するDDNSを改造:NTSv2サーバ
- NTSルータにWAPの機能を統合:NTS WAP

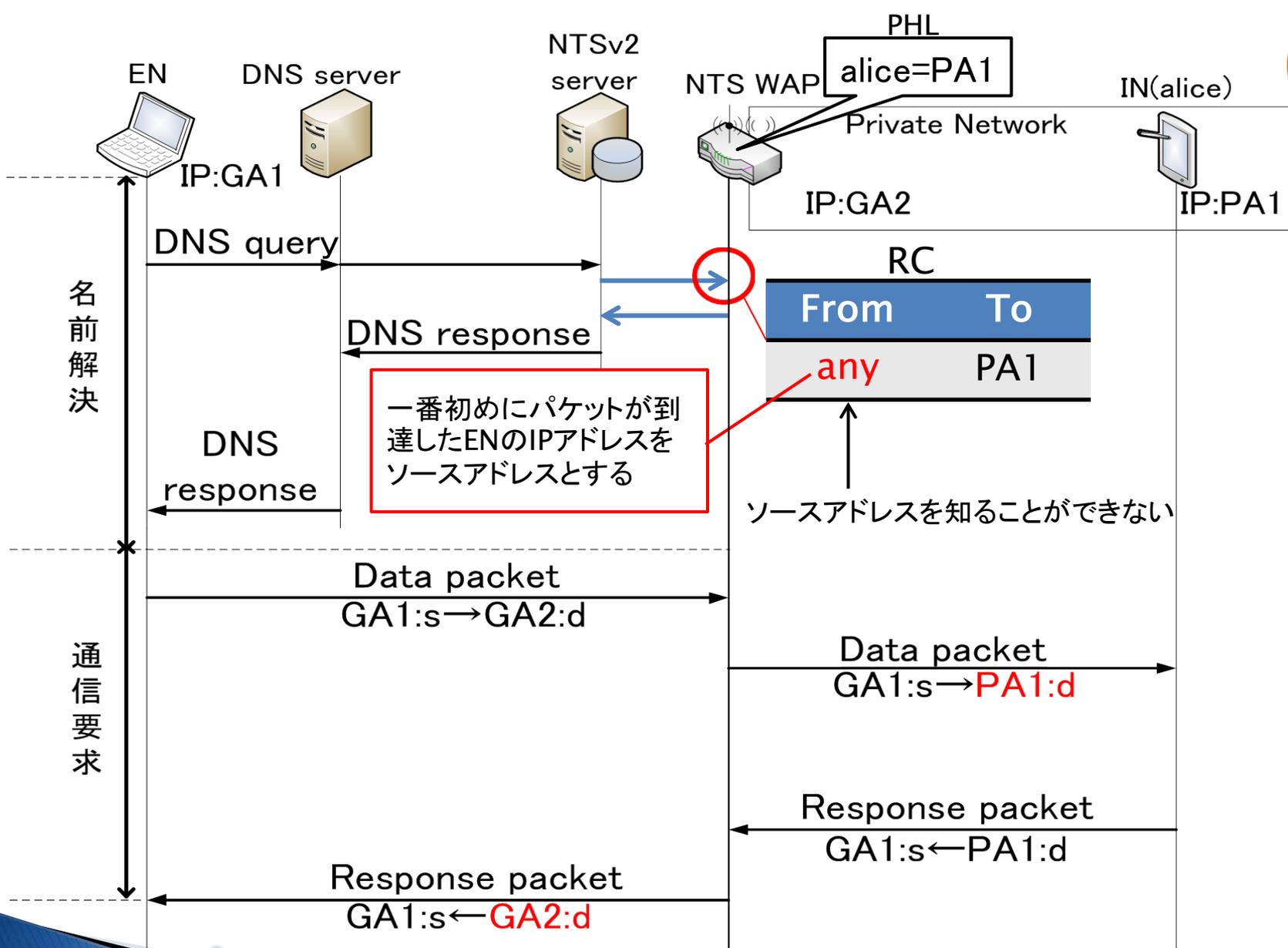


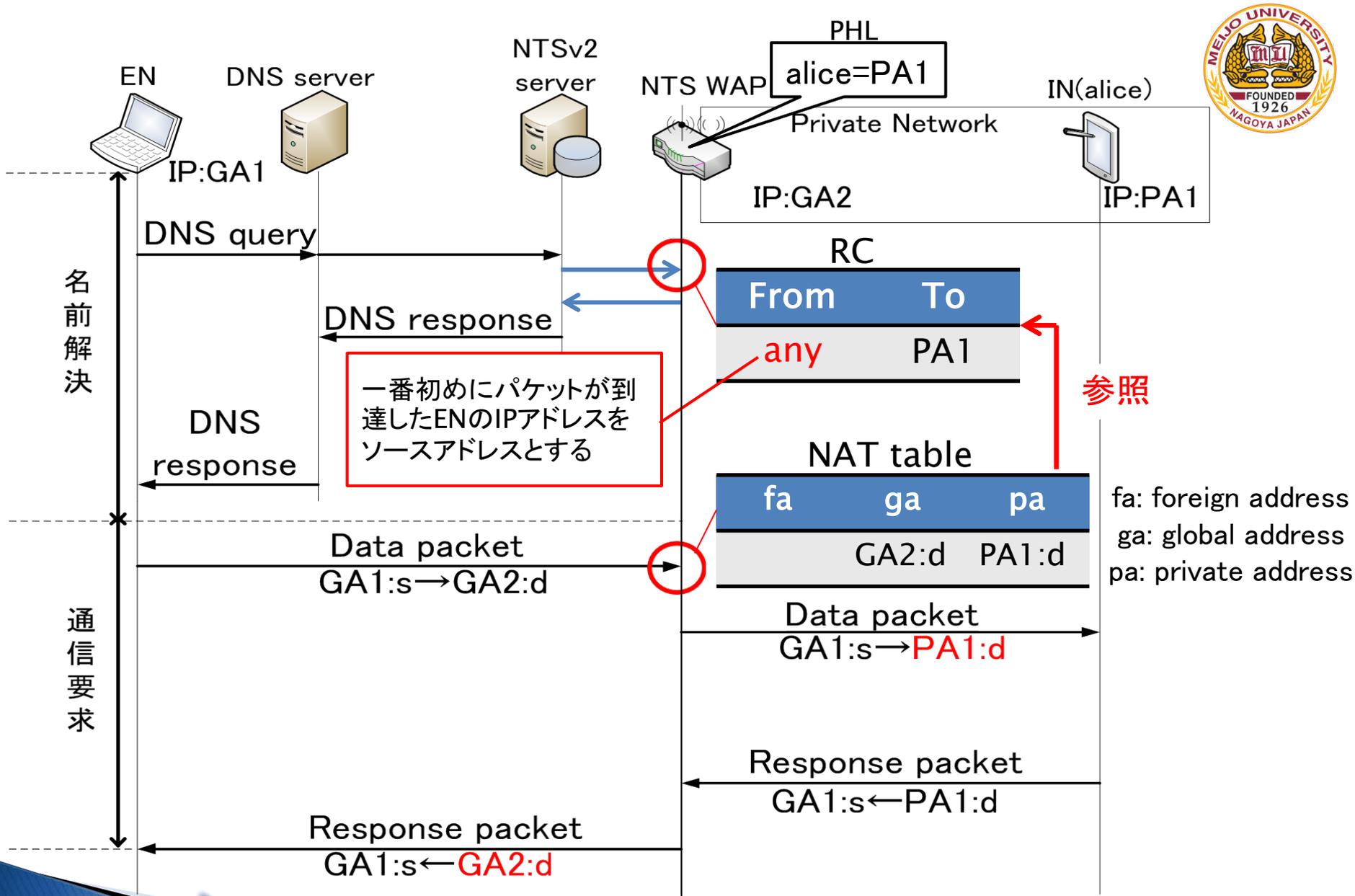


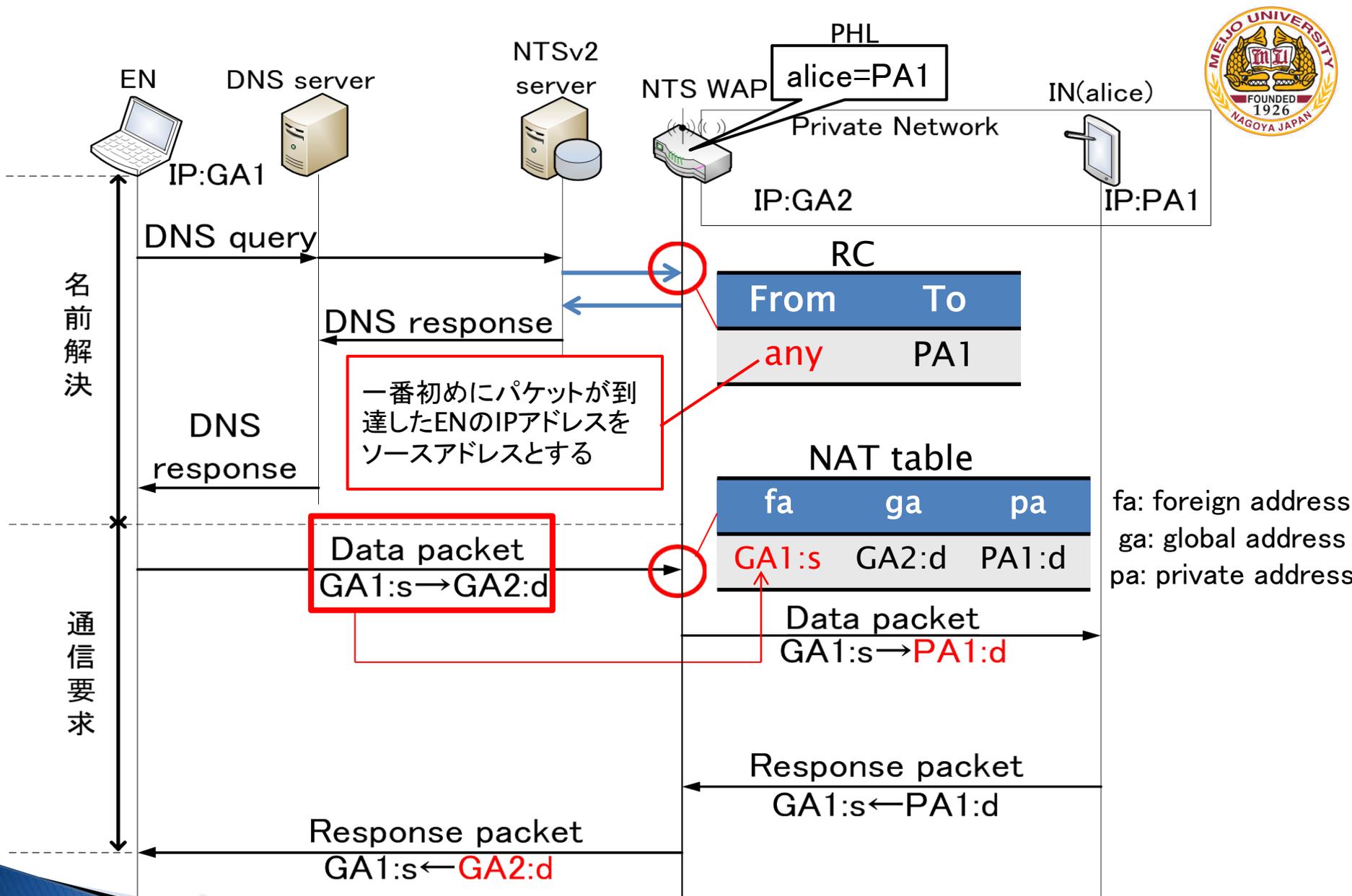
# NTSSv2の動作シーケンス







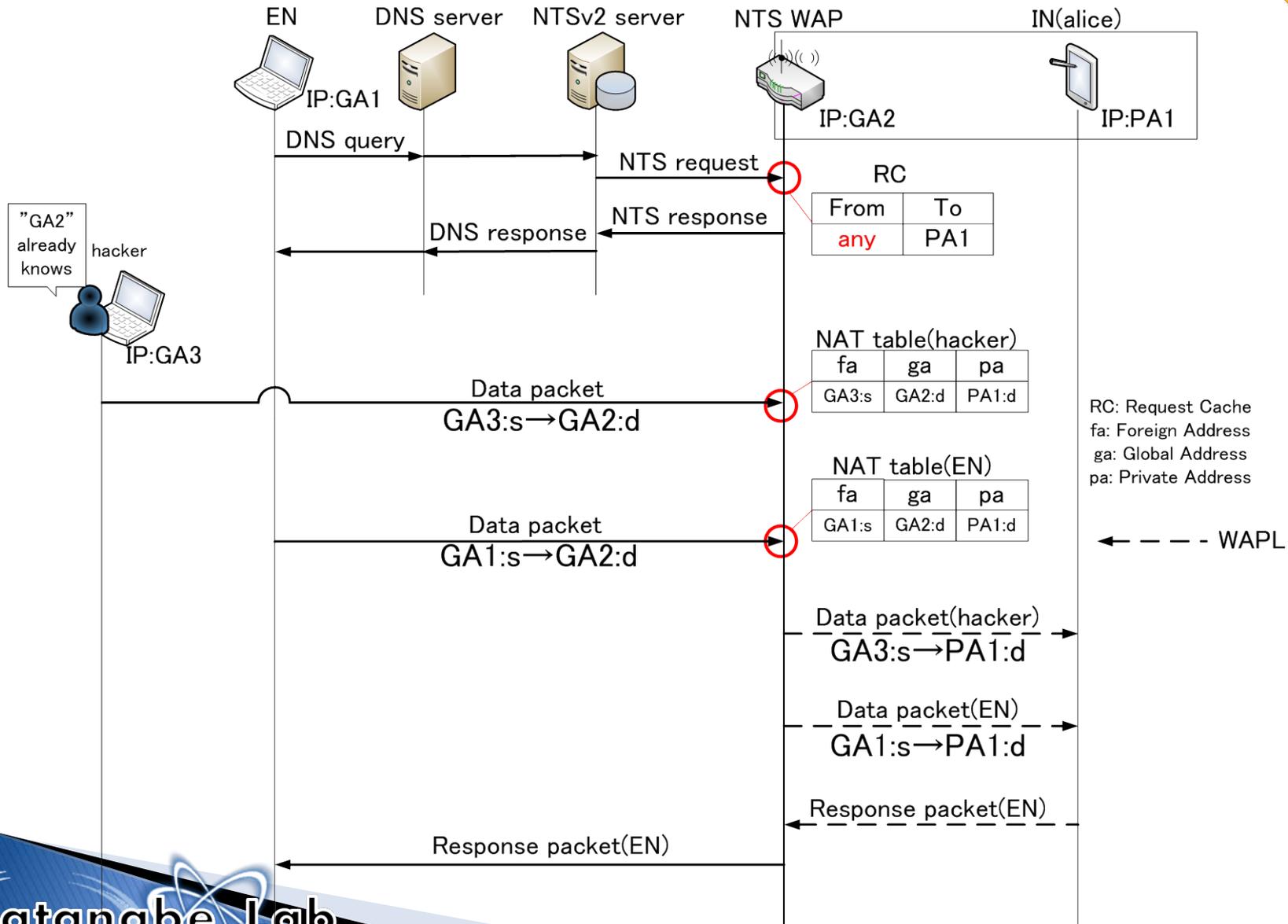




# セキュリティ

- ▶ NTS WAPはENから通信要求を受けるまでソースアドレスを特定できない
- ▶ (例) ENがRC作成後、NTS WAPにパケットを送信する前に第三者がパケットを送信
  - 第三者に通信が乗っ取られ、ENはNATテーブルを生成できない可能性がある
- ▶ 対策
  - 正規のENがNATテーブルを生成するまでRC参照を有効にする

# 第三者が入介入した場合のシーケンス



# まとめ

- ▶ NTSSv2により、被災地に容易にWAPLを展開できる方式を提案した.
- ▶ 今後は実装、動作確認及び性能評価を行う予定である



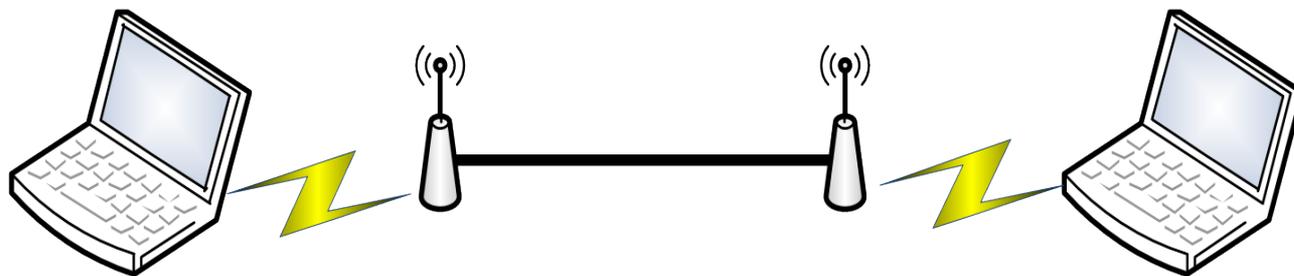
御清聴ありがとうございました

# 補足



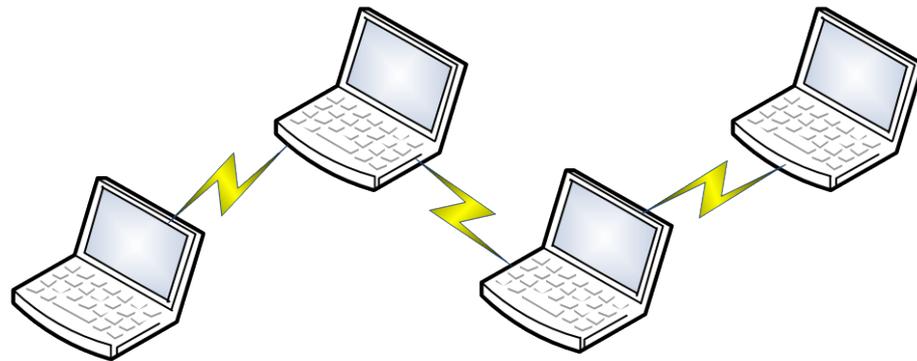
# インフラストラクチャーモード

- ▶ 一般的な無線LANの方式
- ▶ AP間は有線で接続
- ▶ 通信は必ずAPを介して行う  
→ 端末間は直接通信しない



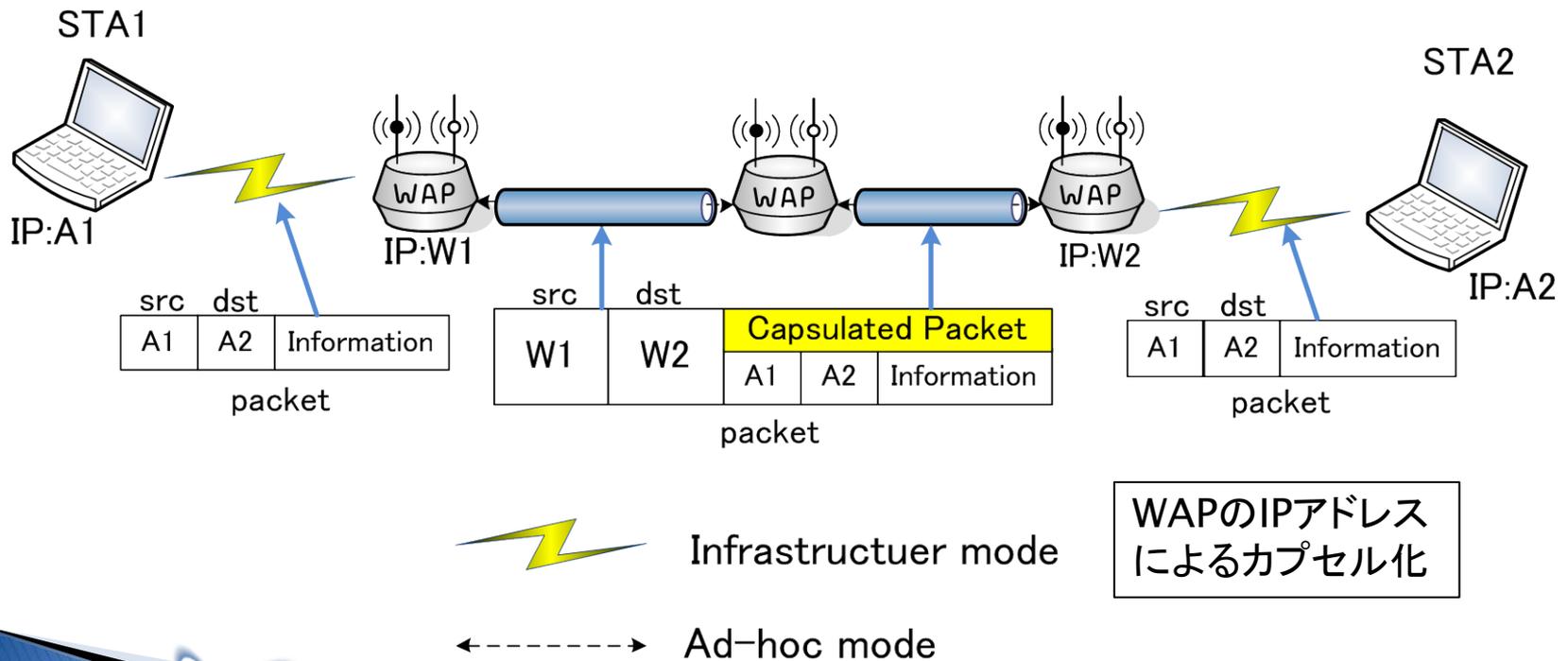
# アドホックモード

- ▶ 端末同士が直接通信を行い構築するネットワーク
- ▶ 同時に2台以上の通信ができない
- ▶ 通信する端末が遠くの場合、複数の端末を経由  
→ 経由された端末は、電力を消耗したりパフォーマンスが低下する
- ▶ 研究段階の技術



# WAPLの概要

- ▶ WAP間を移動してもパケットロスなく通信できる  
→ シームレスハンドオーバ
- ▶ アドホックルーティングプロトコルとWAPLの機能を独立  
→ アドホックルーティングプロトコルを自由に選択できる



# セキュリティ

- ▶ NTSSv2では名前解決の時点でIPアドレスを特定できない
  - 通信が乗っ取られたり, 宛先を間違っって送信してしまう可能性がある
  
- ▶ 原因
  - NATテーブル作成時にRCを削除してしまう
  - IPアドレスを特定できないのに複数の処理を同時に行う

# セキュリティ - 解決方法 -

## ▶ 解決方法

- RCをタイマーで消去
- RC作成からアドレス変換までを先着順に単一処理する

## ▶ 解決例

(例) EN1とEN2が通信要求をした場合



一定時間はNTS WAPとENは1対1で対応：  
確実に通信要求ができる