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

松尾　辰也†　　鈴木　秀和†　　旭　健作†　　渡邊　晃†

†名城大学理工学部

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えることが可能となる．

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．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．

図 1 に NTSS の構成を示す．NTS サーバは EN のプライマリ DNS を改造した装置，NTS ルータは NAT を NTSS 用に改造した装置である．DDNS（Dynamic DNS）サーバは IN（Internal Node）のアドレス登録用で，既存の装置を使用する．

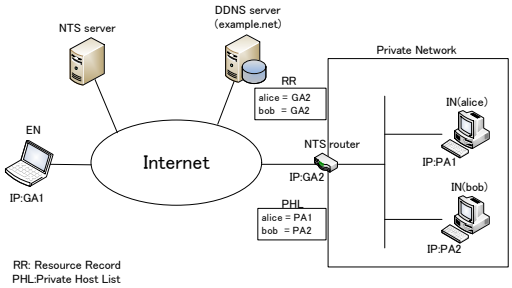


図 1: NTSS の構成

事前設定として，DDNS サーバには IN の名前と NTS ルータのグローバル IP アドレスの対応関係を RR（Resorce Record）として登録し，NTS ルータには 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）と呼ぶテーブルに登録しておく必要がある．また，EN のプライマリ DNS として NTS サーバを登録しておく．

図 2 に NTSS の動作シーケンスを示す．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 DNS の再帰検索により，alice の管理する DDNS サーバより NTS ルータの IP アドレス（GA2）を取得する．この時，NTS サーバは EN から alice への接続要求を NTS request として NTS ルータへ送信する．この通知を受け取った NTS ルータは PHL を参照し，alice のプライベート IP アドレス（PA1）を取得する．そして，EN と IN の IP アドレスの対応関係を RC（Request Cache）へ記憶して，NTS サーバへ NTS response を返信する．NTS response 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 に応答する．

名前解決後，EN は IP アドレスが ”GA2 ”である 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 の内容を確認する．RC に該当するデータがあれば，NTS ルータは NAT テーブルを動的に生成する．以後の通信は図 2 に示すように IP アドレスが変換されて alice へ パケットが送信される．

Interconnections between the Internet of the wireless mesh network in which two-way communication is possible

†Tatsuya Matsuo, †Hidekazu Suzuki, †Kensaku Asahi, †Akira Watanabe

†Faculty of Science and Technology, Meijo University

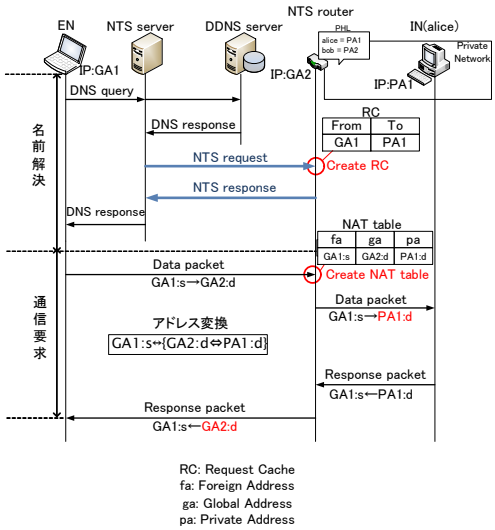


図 2: NTSS の動作シーケンス

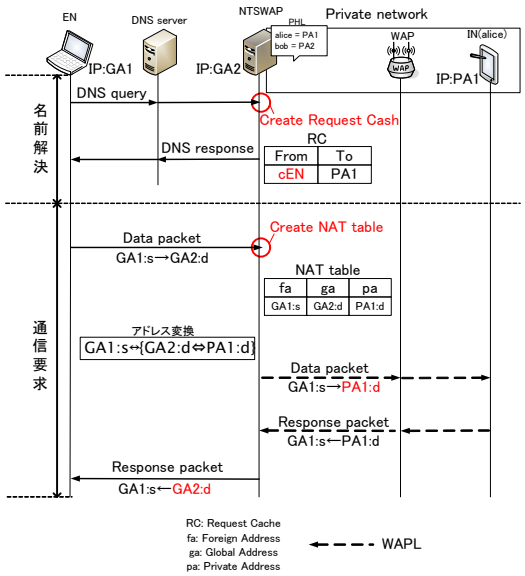


図 3: NTSSv2 のシーケンス

3 提案方式

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装置を設置することにより，双方向の通信を可能とする．

3.1 NTSS の改造

提案方式で利用するに当たり，NTSS の見直しを行った．NTSS では EN 側の DNS サーバを改造することにより NAT 越えを実現させていたが，NTSSv2 では DDNS 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，動的に RR と PHL を作成するようにした．

これにより，ユーザは環境設定を変更する必要が無くなるので，NTSSv2 を容易に利用することができる．

3.2 NTSSv2 のシーケンス

図 3 に提案方式のシーケンスを示す．EN のプライマリ DNS は既存の装置を使用している．NTS WAP は DDNS に改造を行った装置である．また，NTS WAP 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 IN の名前解決を依頼する．NTS WAP はこれを受けて NTSS と同様に RC を作成する．ただし，図 3 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ある EN からの通信要求として ”cEN ”とする．EN には NTS WAP のグローバルアドレスである（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 RC を参照して ”cEN ”の部分を NTS WAP にパケットを送信した EN の IP アドレスをソースとして 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．

3.3 セキュリティ

この方法によると，複数の端末が同時に 1 つの NTS WAP を経由して通信要求を行った時，EN は正しい相手と通信を行うことができない場合がある．これは，NTS WAP にパケットが到着する時間のずれによって，間違った RC を参照して NAT テーブルを作成してしまうためである．このため，NTS WAP は RC 作成からアドレス変換までの一連処理をクエリ到着順に 1 つずつ行うようにした．これにより，一定時間は 1 つの端末だけが通信要求を行っていると見なせるので，セキュリティ上の問題にならないと判断した．

4 まとめ

本稿では WAPL と NTSS を組み合わせ，かつ NTSS の動作を見直すことにより，被災地に容易に無線メッシュネットワーク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のインターネット接続方法

名城大学
松尾辰也　鈴木秀和　旭健作　渡邊晃

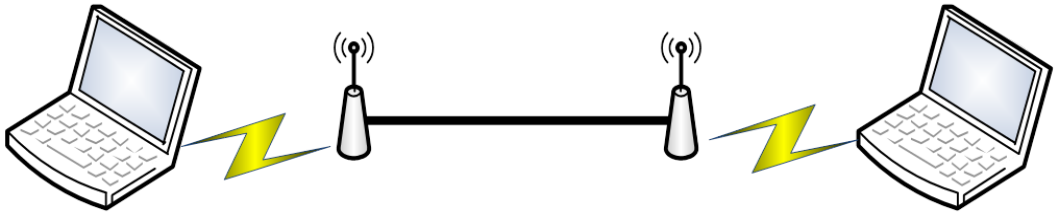
Watanabe Lab.

研究背景

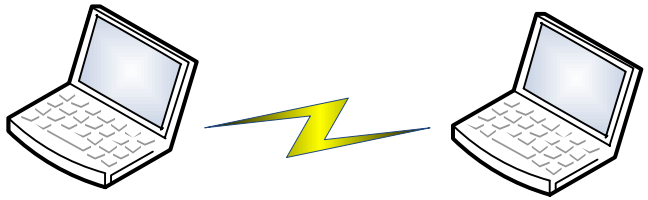
- 災害発生時
  - ネットワークインフラが破壊される場合がある
  - 迅速に通信インフラを再構築する必要がある
- 無線LANの普及
  - 配線が不要
  - 無線メッシュネットワーク技術の発展

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

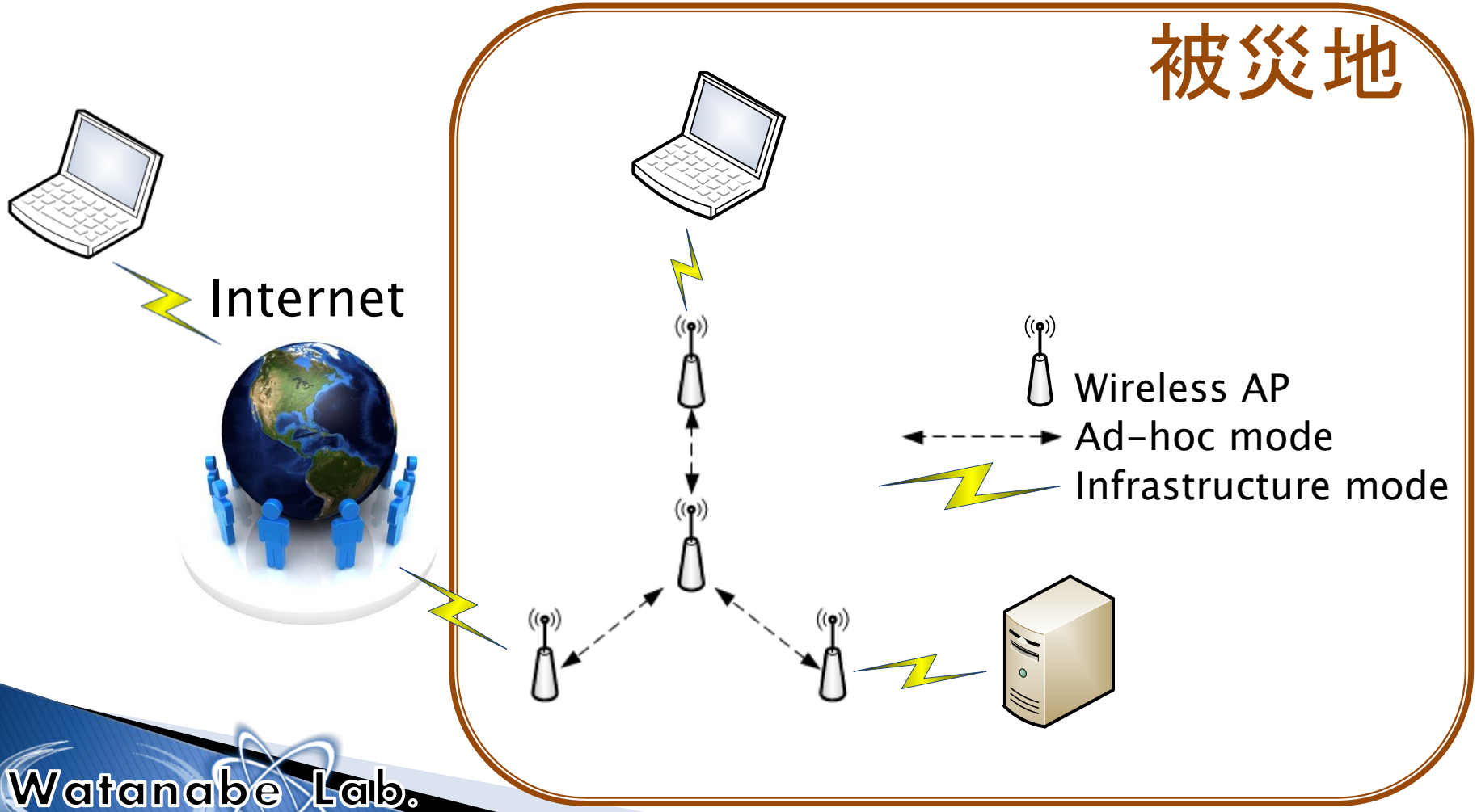


- アドホックモード
  - 端末同士が電波が届く範囲で直接通信を行う



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)

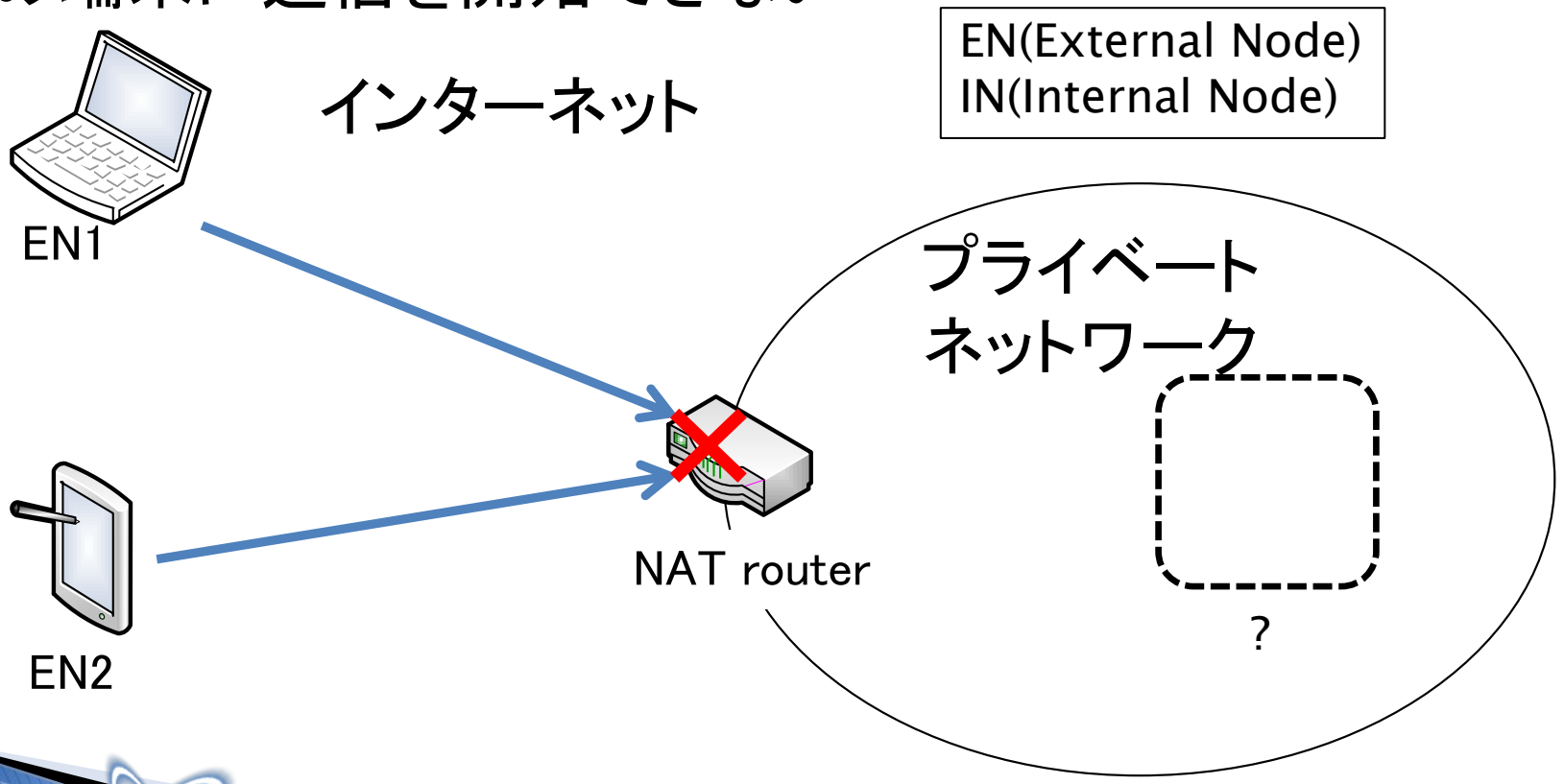
- 無線メッシュネットワークはプライベートアドレスで構築する(グローバルアドレスが枯渇しているため)

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



要件(2/2)

- 外部の人は既存のシステムをそのまま使える

端末の改造が困難　　ライトユーザ

→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

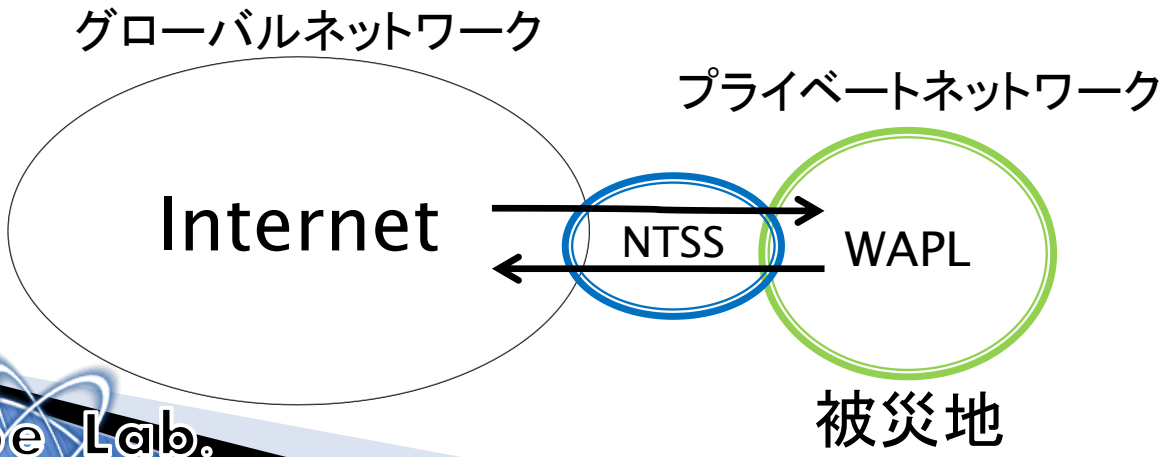
無線メッシュネットワーク

＋

NAT越えシステム

WAPL（Wireless Access Point Link）

NTSS（NAT Traversal Support System）

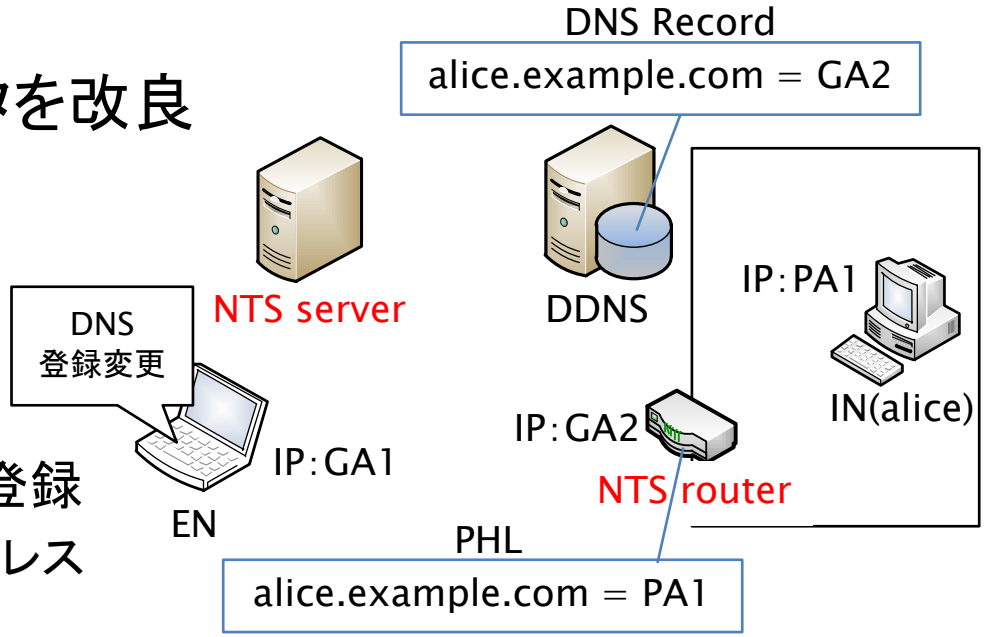


要素技術

- 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

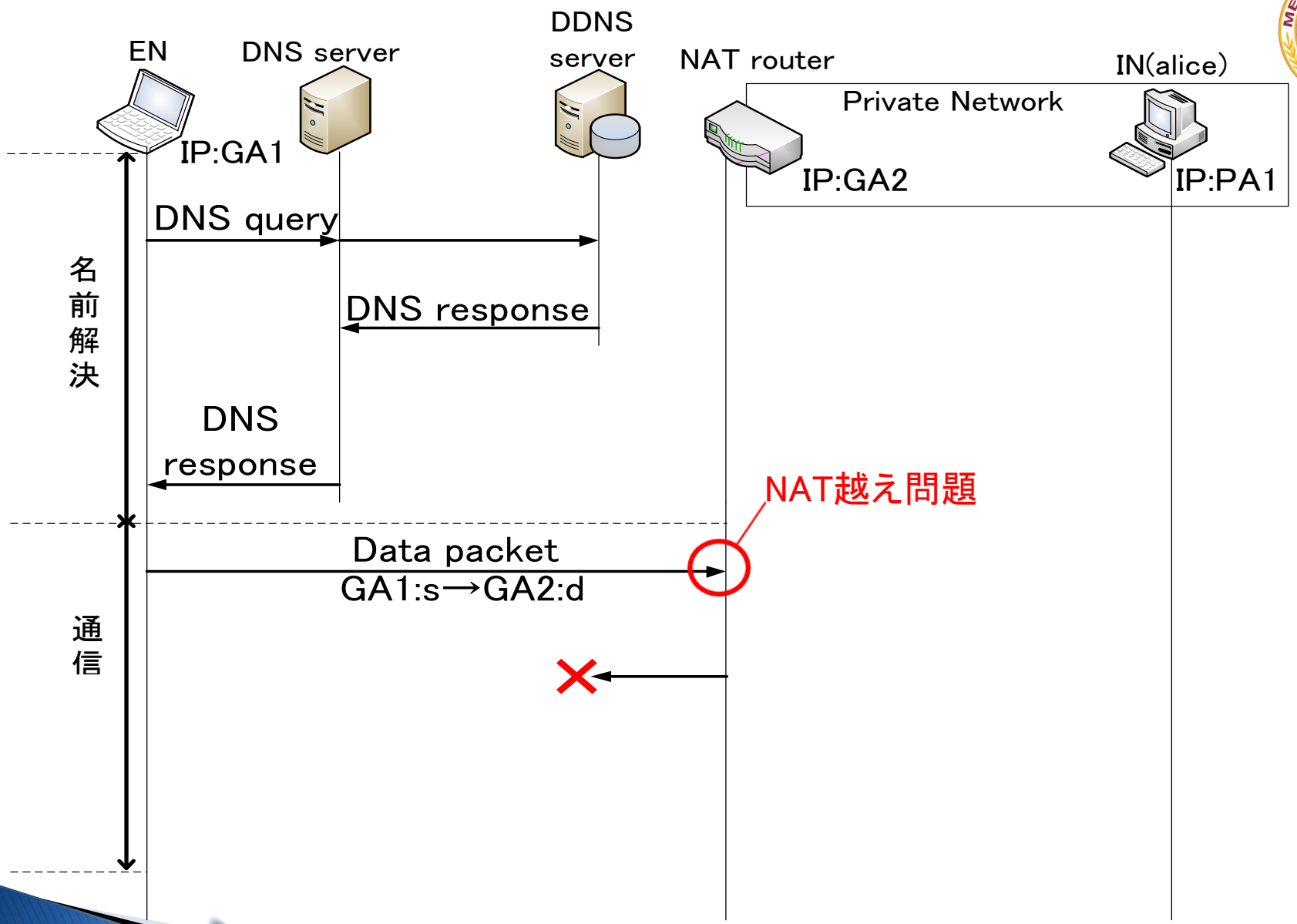
NTSSの構成

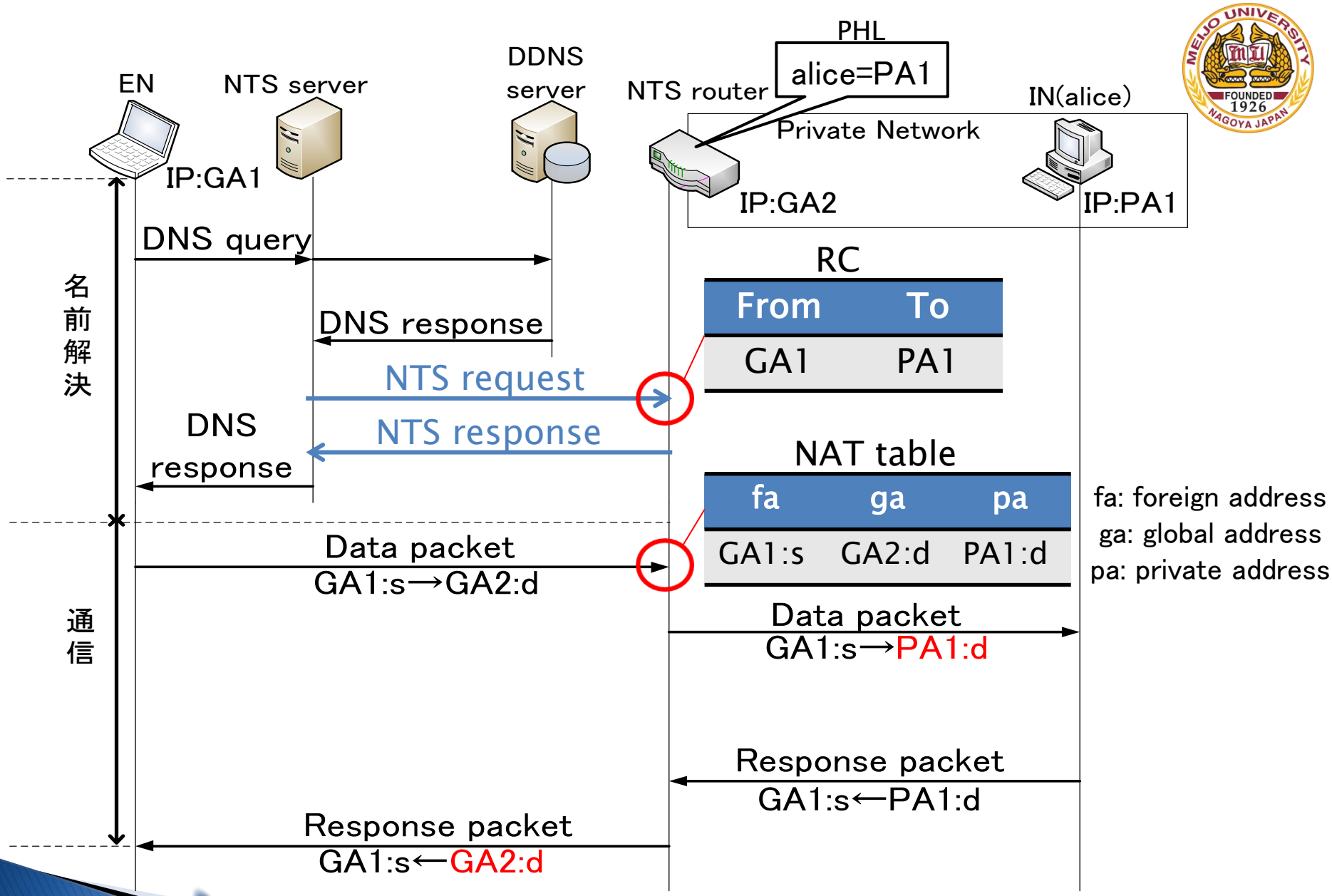
- DNSサーバとNATルータを改良
  - DNSサーバ：NTSサーバ
  - NATルータ：NTSルータ
- 事前設定
  - DDNS(Dynamic DNS)へ登録
    - FQDNとNTSルータのIPアドレス
  - NTSルータへ登録
    - FQDNとINのプライベートアドレス
    - PHL(Private Host List)
  - ENのプライマリDNSをNTSサーバに設定



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.

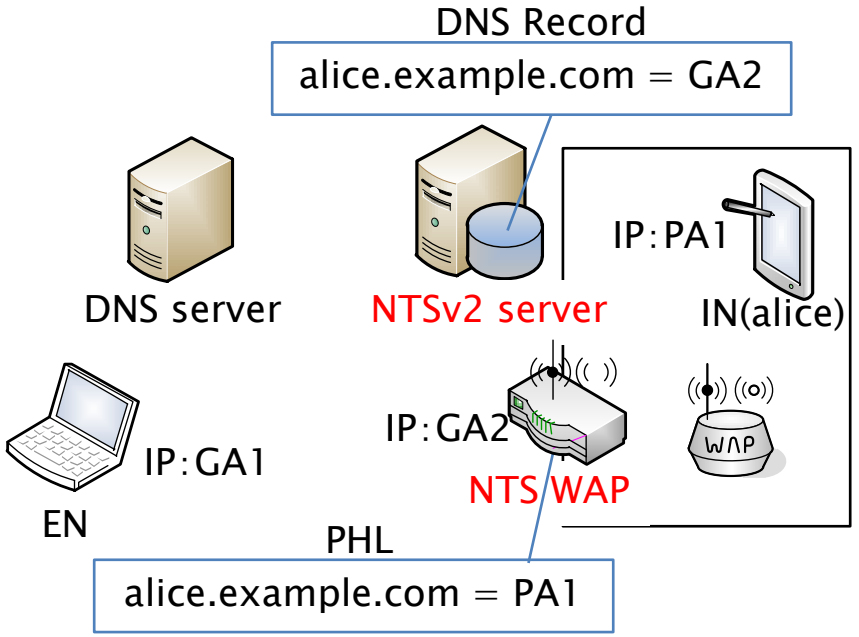
NTSSの動作シーケンス


EN
DNS server
DDNS server
NAT router
IN(alice)
Private Network
IP:GA1
IP:GA2
IP:PA1
DNS query
DNS response
名前解決
DNS response
NAT越え問題
Data packet
GA1:s→GA2:d
通信


EN
NTS server
DDNS server
NTS router
PHL
alice=PA1
IN(alice)
Private Network
IP:GA1
IP:GA2
IP:PA1
DNS query
DNS response
NTS request
NTS response
DNS response
名前解決
通信
RC
From
To
GA1
PA1
NAT table
fa
ga
pa
GA1:s
GA2:d
PA1:d
fa: foreign address
ga: global address
pa: private address
Data packet
GA1:s→GA2:d
Data packet
GA1:s→PA1:d
Response packet
GA1:s←PA1:d
Response packet
GA1:s←GA2:d

提案方式の構成

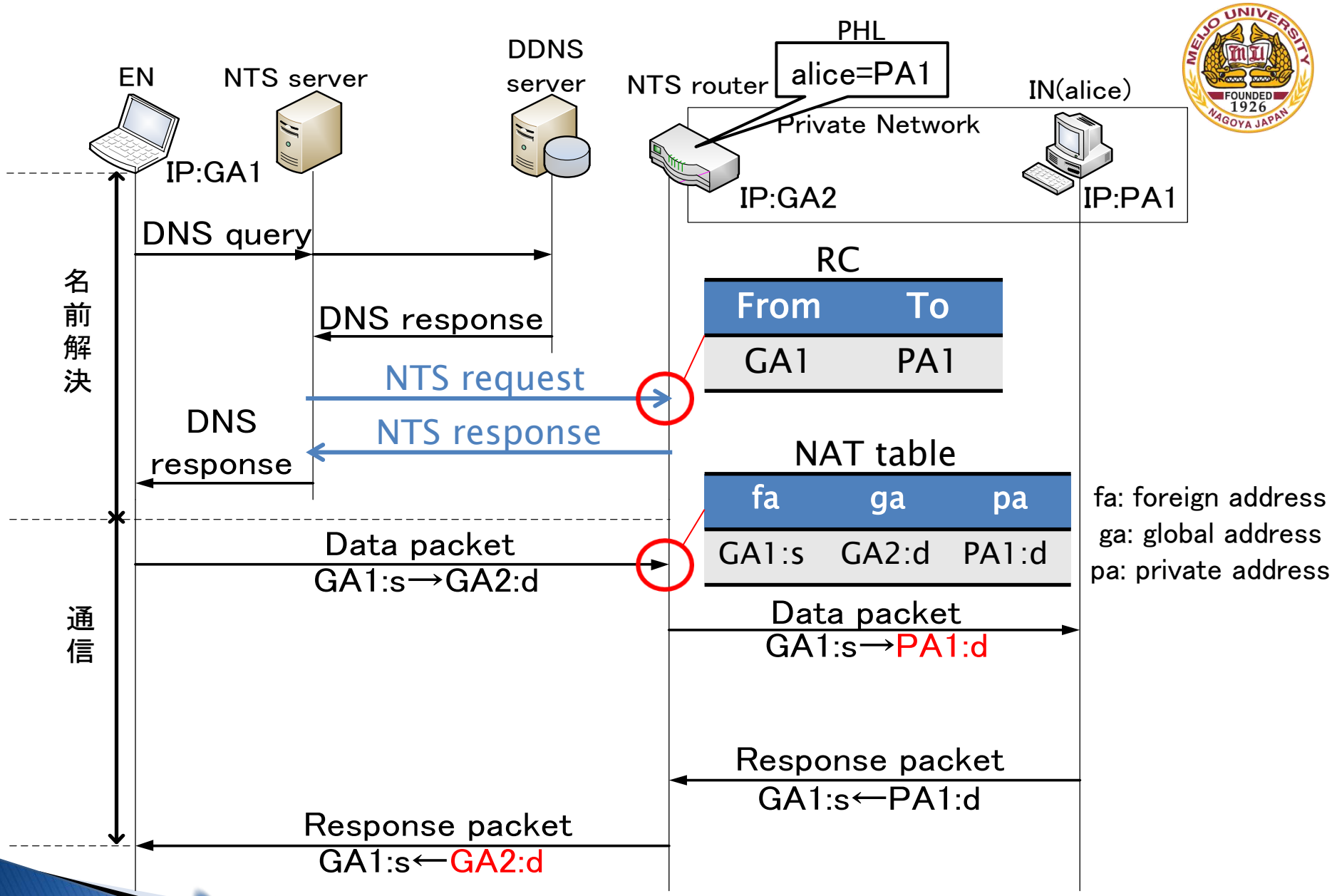
- NTSSv2
  - DDNSサーバ：NTSv2サーバ
  - NATルータ：NTS WAP
- NTSSとの違い
  - DNS登録変更が不要
  - WAPLに対応

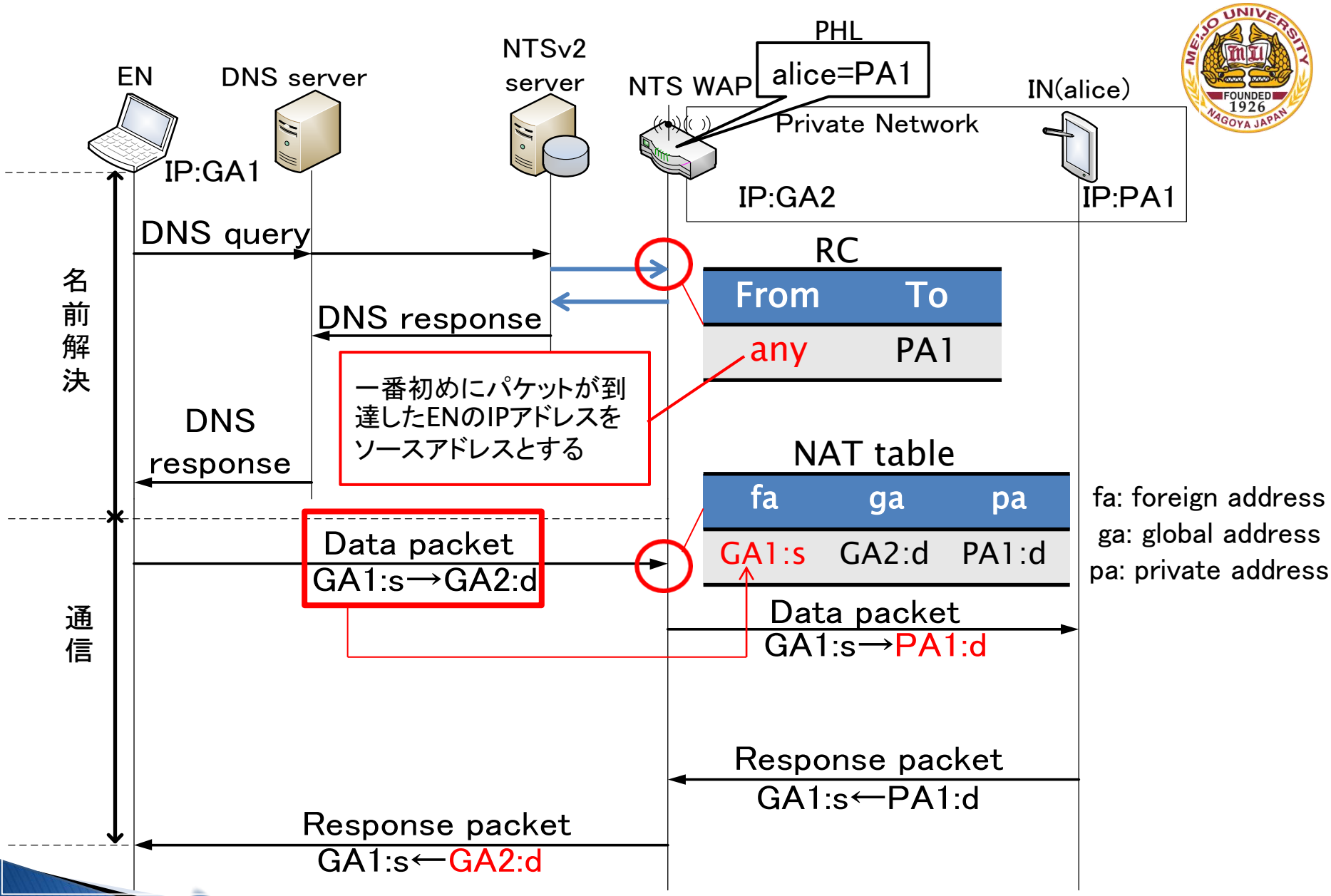


要件達成

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.

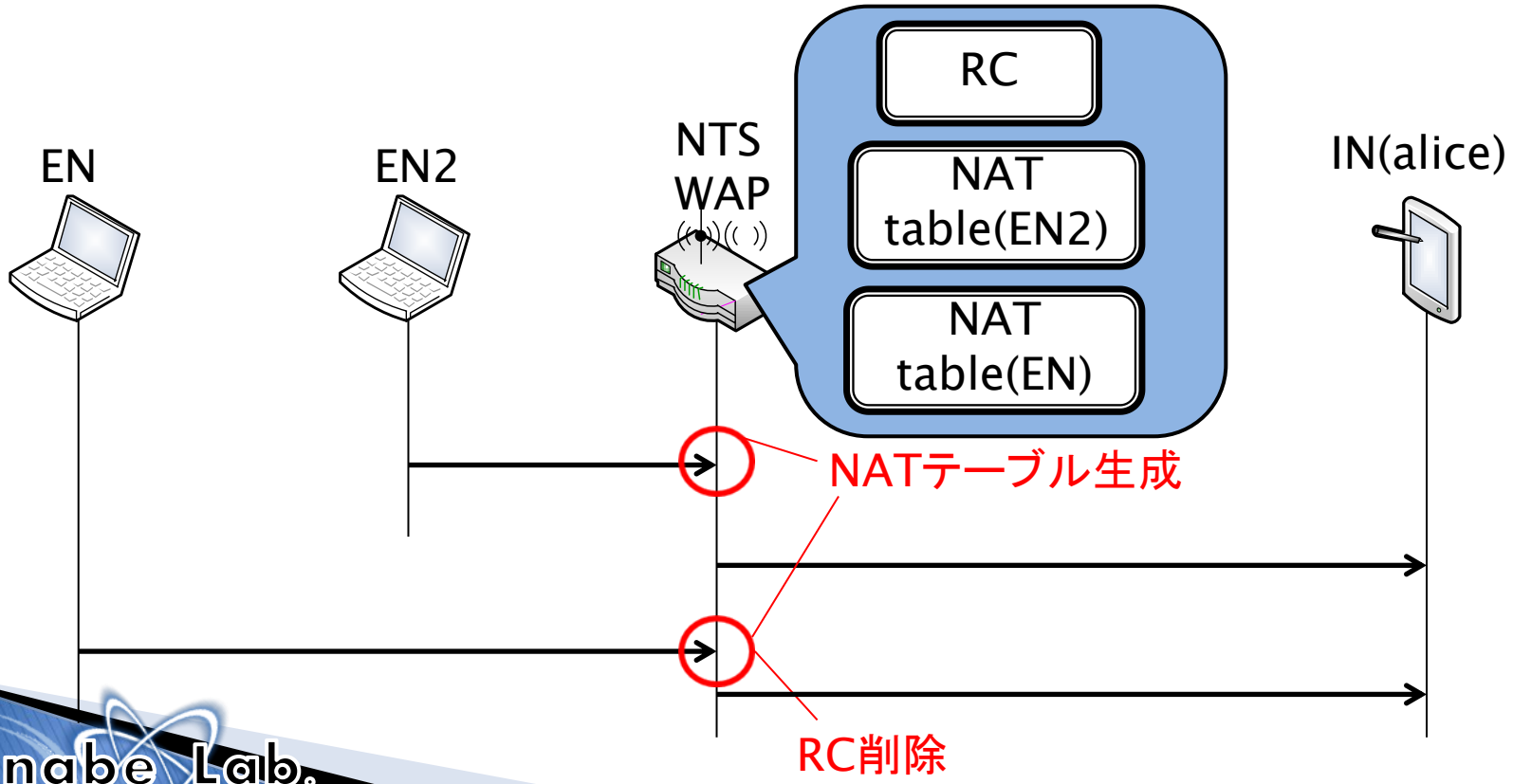
NTSSv2の動作シーケンス


EN
NTS server
DDNS server
PHL
alice=PA1
NTS router
IN(alice)
Private Network
IP:GA1
IP:GA2
IP:PA1
DNS query
DNS response
NTS request
NTS response
DNS response
名前解決
通信
RC
From
To
GA1
PA1
NAT table
fa
ga
pa
GA1:s
GA2:d
PA1:d
fa: foreign address
ga: global address
pa: private address
Data packet
GA1:s→GA2:d
Data packet
GA1:s→PA1:d
Response packet
GA1:s←PA1:d
Response packet
GA1:s←GA2:d


EN
DNS server
NTSv2 server
NTS WAP
PHL
alice=PA1
IN(alice)
Private Network
IP:GA1
IP:GA2
IP:PA1
名前解決
DNS query
DNS response
DNS response
RC
From
To
any
PA1
一番初めにパケットが到達したENのIPアドレスをソースアドレスとする
NAT table
fa
ga
pa
GA1:s
GA2:d
PA1:d
fa: foreign address
ga: global address
pa: private address
Data packet
GA1:s→GA2:d
通信
Data packet
GA1:s→PA1:d
Response packet
GA1:s←PA1:d
Response packet
GA1:s←GA2:d

セキュリティ

- 懸念
  - 正規のENがNATテーブルを作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



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

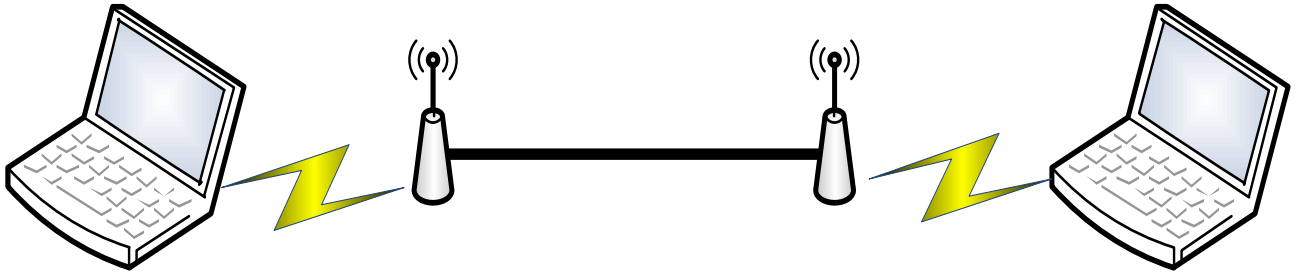
御清聴ありがとうございました

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

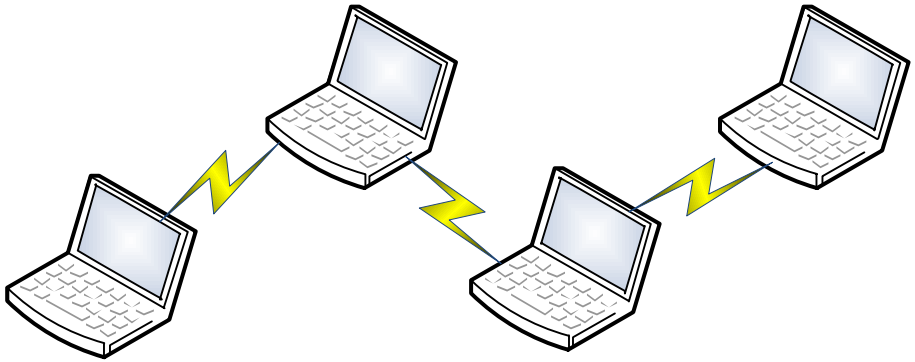


アドホックモード

- 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

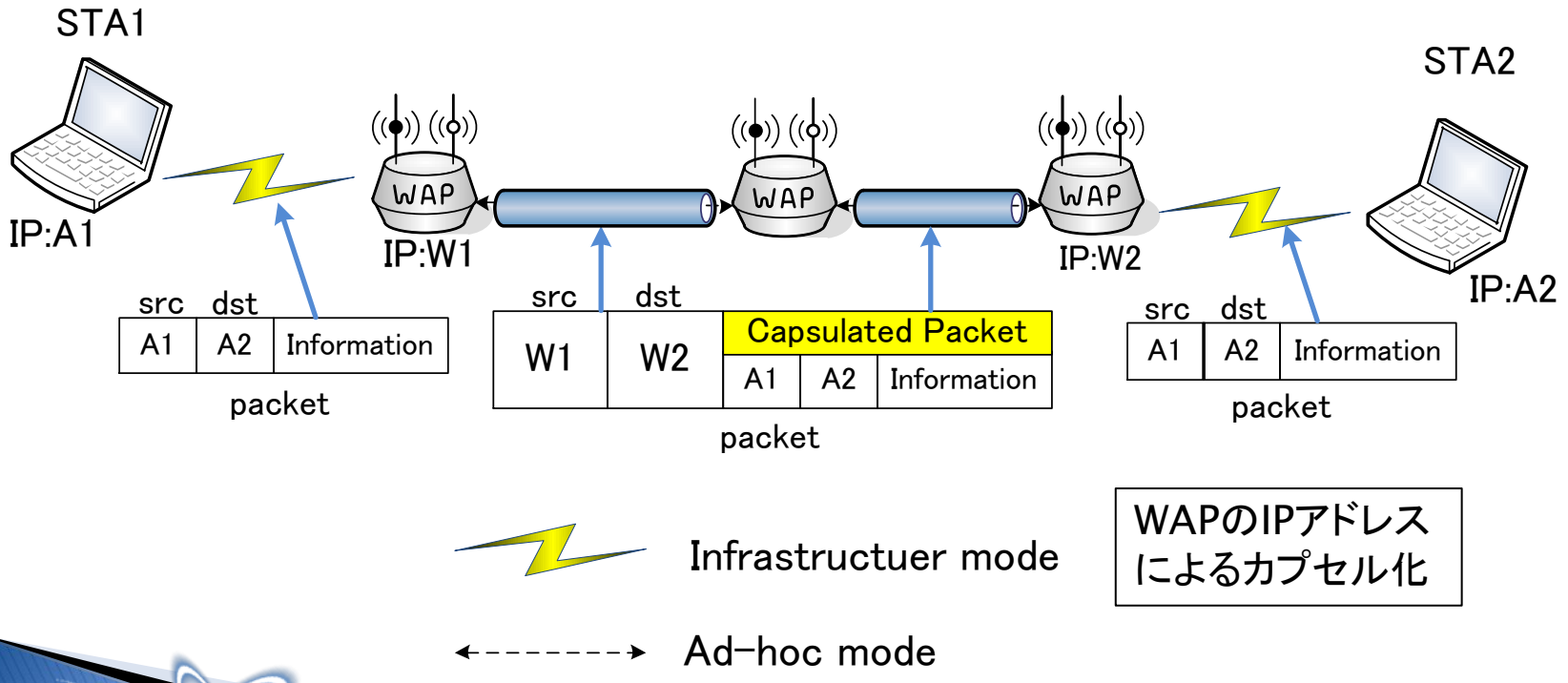
→経由された端末は、電力を消耗したりパフォーマンスが低下する

- 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



伊藤将志,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,No.6,pp.1859-1871,Jun.2008

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

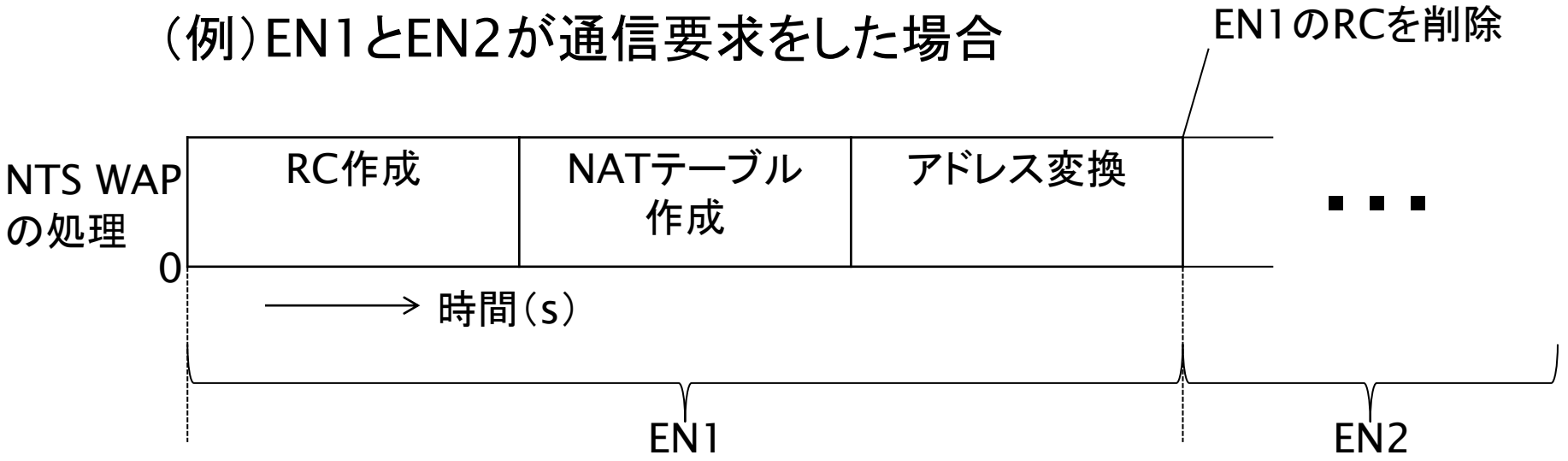
→通信が乗っ取られたり，宛先を間違って送信してしまう可能性がある

- 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