平成23年度　卒 業 論 文

邦文題目

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

英文題目

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

情報工学科　渡邊研究室
(学籍番号: 080430093)

松尾　辰也

提出日: 平成 24 年 2 月 9 日

名城大学理工学部

内容要旨

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）と NAT 越え技術 NTSS（NAT Traversal Support System）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．

Abstract

A wireless mesh network is the useful technology in which a wireless LAN infrastructure can be built easily. By developing to a stricken area etc. at the time of disaster generating, the wireless mesh network can reconstruct a network quickly. As for a mesh network, since the number of network global addresses may fully be unable to secure at this time, it is desirable that a private address can be used. In order to use a private address, it is necessary to install NAT but, and the subject of it becoming impossible to start communication from the Internet side by an NAT traversal problem occurs. So, in this paper, in order to solve this subject, the system which combines wireless mesh network WAPL(Wireless Access Point Link) and the NAT traversal technology NTSS(NAT Traversal Support System) is proposed.WAPL is developed to a stricken area and this method enables it to be able to communicate to an external network and freedom.

目 次

第1章　はじめに

近年，スマートフォンやタブレット端末の普及により，無線通信の需要が高まっている．しかし，無線通信で使われる無線 LAN の AP（Access Point）は，有線で接続されることが一般的であり，AP の設置場所が限定されたり，配線に多大なコストを要する．

この問題を解決するために，無線 LAN の AP を網目状に展開し，AP 間をアドホックモードで接続する無線メッシュネットワークが提案されている．これは AP 間を無線で接続しているので，無線 LAN インフラを容易に構築することができる．また，無線メッシュネットワークにおける端末／ AP 間の通信はインフラストラクチャモードのため，既存の端末は容易にネットワークに参加することが可能である．そのため，災害発生時の被災地ような有線インフラを構築することが困難な場合や，有線の維持費を捻出できないイベントで運用されることが期待される．

そこで，無線メッシュネットワークを災害発生時に被災地などに展開する場合，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．このため，無線メッシュネットワークは NAT（Network Address Translation）によるプライベートアドレスを使用できることが望ましい．NAT は一つのグローバルで IP アドレスを複数のコンピュータで共有する技術であり，プライベートアドレスを使用することで IP アドレスを十分に確保することができる．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に存在する端末側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をする例があるため，インターネット側から無線メッシュネットワークを介して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考えられる．

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．

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している．また，NTSS の機能をプライベートネットワークを管理する DDNS（Dynamic DNS）を改造して実現することにより，NAT テーブル生成に必要な事前登録処理を不要とした．

以降，第 2 章では要素技術である WAPL と NTSS の解説を行い，第 3 章で提案方式の説明，第 4 章で実装について検討を示し，第 5 章でまとめる．

第2章　要素技術

2.1　WAPL

WAPL と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できる．また WAP と呼ばれる各 AP が近隣 WAP の通信状況を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．

図 2.1 に WAPL によるカプセル化通信を示す．WAPL はルーティングテーブルとは独立した LT（Link Table）と呼ばれる WAP 間の経路制御用テーブルを必要に応じてオンデマンドに生成する．通信を開始する際，送信端末は ARP request を送信する．メッシュネットワーク上の各 WAP は端末からの ARP request を受信すると，LT が生成されていない他の WAP へ生成要求をフラッディングにより通知する．このフラッディングにより各 WAP に LT が生成され，宛先端末に ARP request が送信される．その後，パケットはハンドオーバの実現のために WAP 間で MAC ヘッダを含めてカプセル化されて，宛先端末にパケットが送信される．

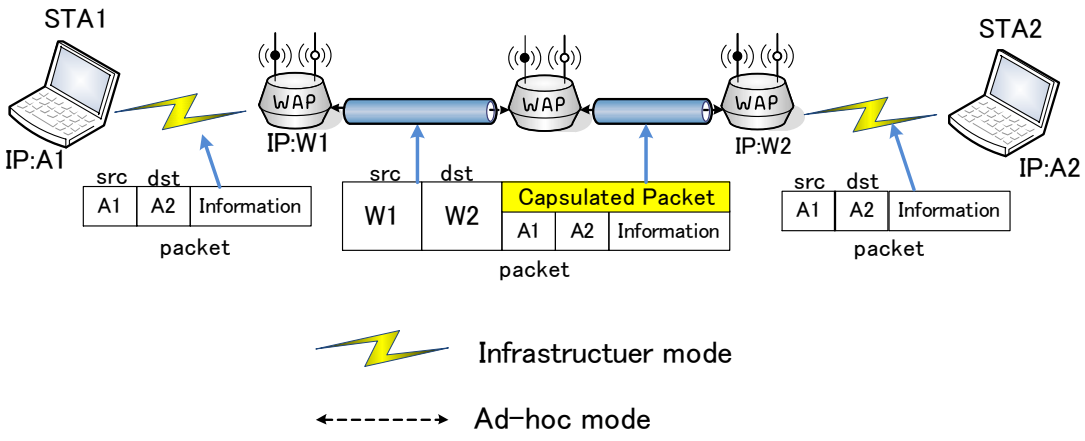


図 2.1　WAPL の構成

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．EN（External Node）のプライマリ DNS と NAT ルータを改造し，この両者が協調動作をすることにより，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 2.2 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 ルータを NTSS 用に改造した装置である．DDNS サーバは IN（Internal Node）のアドレス登録用サーバで既存の装置を使用する．

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）に登録し，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 2.3 に動作シーケンスを示す．EN から IN（alice）への通信を例に説明する．EN は通信を開始するにあたり，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 サーバは名前解決結果を EN へ応答する前に，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 Cash）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 ルータは以下のような NAT テーブルを動的に作成する．

GA1:s ↔ { GA2:d ⇔ PA1:d }

上記 NAT テーブルの意味は，EN との通信はでは NAT と IN の IP アドレスとポート番号が対応していることを意味する．s は EN のカーネルが選択した任意のポート番号，d は IN がサービスを提供しているポート番号である．

NAT テーブルが作成されると，パケットはアドレス変換処理が施され，alice にパケットが送信される．以後，EN と alice はエンドエンドの通信を行うことが可能となる．

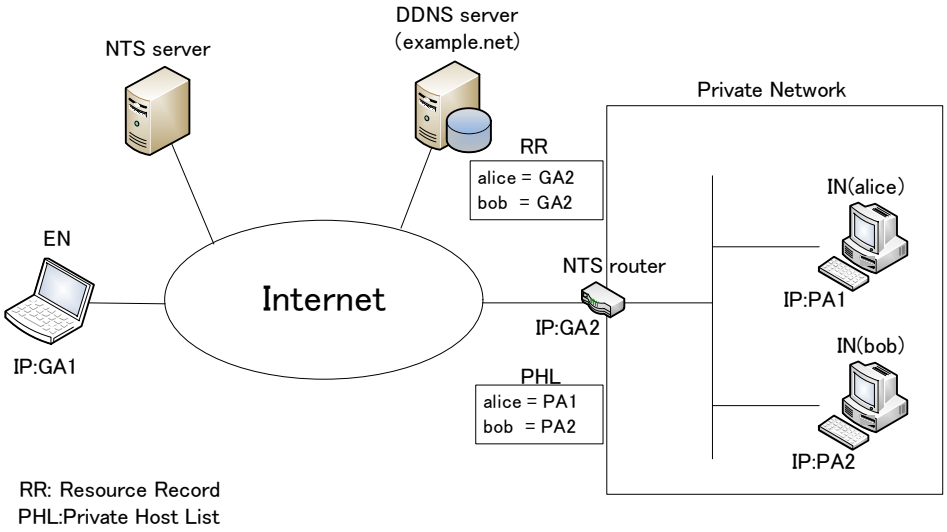
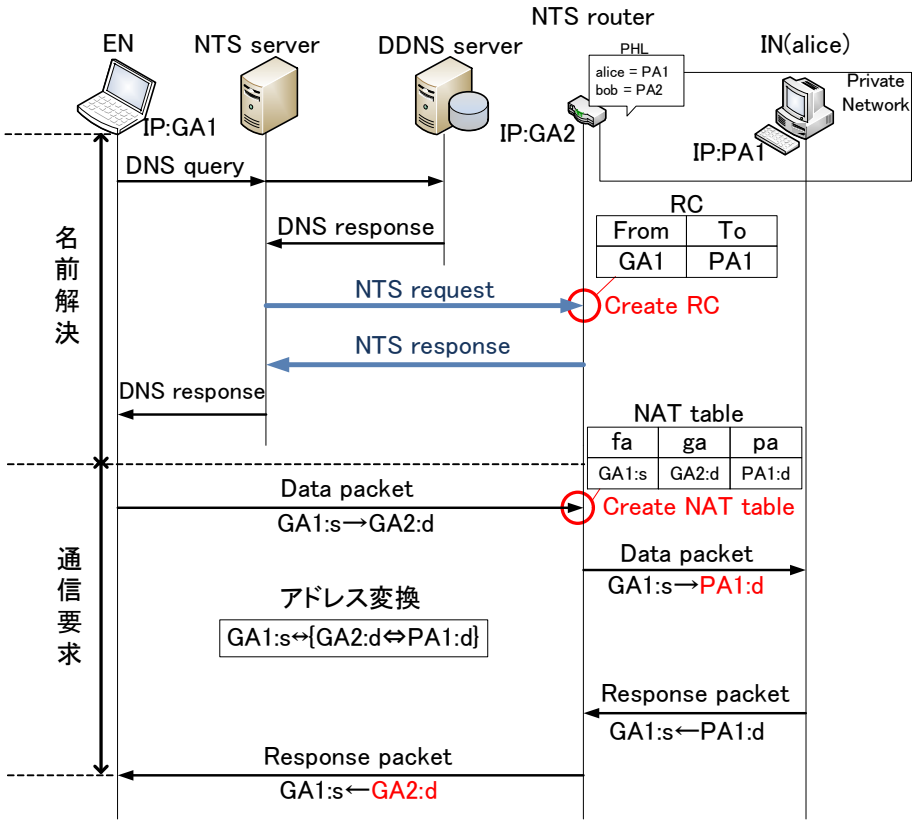


図 2.2　NTSS の構成



RC: Request Cache
fa: Foreign Address
ga: Global Address
pa: Private Address

図 2.3　NTSS の動作シーケンス

第3章　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機器を設置することにより，双方向の通信を可能とする方式である．

3.1　NTSS の改造

NTSS では EN 側の DNS サーバを改造することにより NAT 越えを実現している．そのため，EN はあらかじめ NTS サーバをプライマリ DNS として登録しておく必要がある．しかし，プライマリ DNS の登録変更はいくつかの操作を行う必要があるため，一般ユーザが容易に変更することができない可能性がある．そこで，提案方式である 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．DDNS は DHCP と DDNS と WAP を一体化させた NTS WAP という装置として改造することにより，動的に RR と PHL を生成するようにした．これにより，ユーザは事前登録や DNS 登録変更を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

図 3.1 に提案方式の構成, 図 3.2 に NTSSv2 のシーケンスを示す．EN のプライマリ DNS は既存の DNS サーバを使用している．NTS WAP は DDNS を改造した装置であり，NTS WAP の配下は WAPL で構成されている．動作シーケンスは NTSS と同様に EN から IN（alice）への通信を例に説明する．

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 を生成する．しかし，この段階では 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．この ”any ” は RC 生成後，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して NAT テーブルを生成することを意味する．そして，名前解決結果として 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 に向けてパケットを送信する．NTS WAP は RC を参照し，先ほど述べたように ”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，NTSS と同様に EN の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 EN と alice はエンドエンドで通信が可能となる．

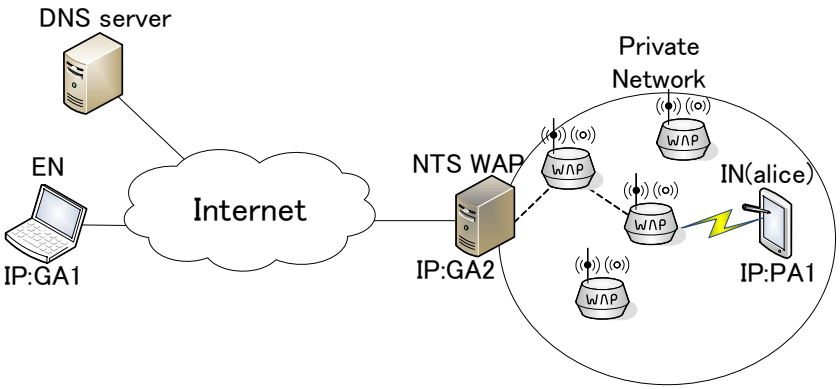


図 3.1　NTSSv2 の構成

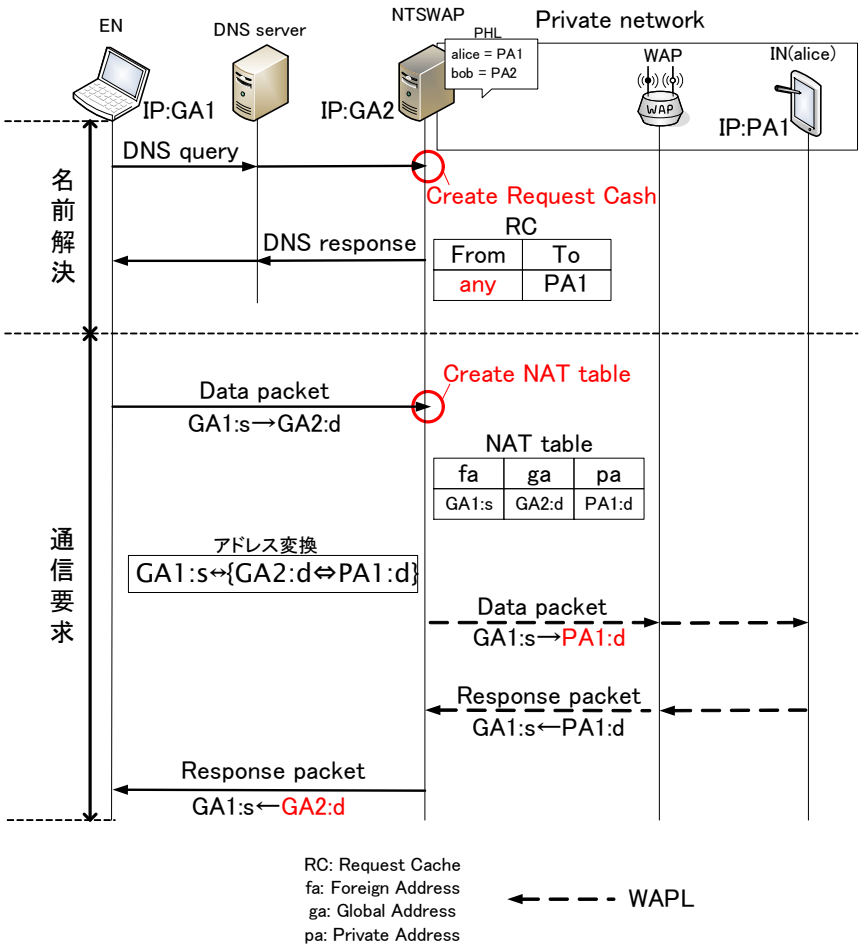


図 3.2　NTSSv2 のシーケンス

3.3 セキュリティ

NTSSv2 では，NTS WAP が EN 側の IP アドレスを特定することができないため，NTSS で生成される RC とは中身が異なったものになる．そのため，NTSSv2 では以下の項目が懸念される．

1. 名前解決を行った EN が NTS WAP に通信要求を行う前に，第三者が通信要求をした場合（乗っ取り）
2. 複数の EN が同時に 1 つの NTS WAP を経由して通信した場合（同時通信）

以下，これらの項目の説明し，現状の解決策を示す．

3.3.1 乗っ取り

この場合の例として，図 3.3 の通信に第三者であるハッカーが参加した場合を想定する．ハッカーは NTS WAP の IP アドレス（GA2）を既知とする．

EN は通常のシーケンス通りに名前解決を行い，名前解決結果（GA2）を得る．そして，EN は NTS WAP に向けて通信要求を行うが，その前にハッカーが NTS WAP に通信要求をすると，NTS WAP はハッカーの IP アドレスである ”GA3 ”をソースとした NAT テーブルを生成し，IN（alice）に通信要求をしてしまう．この時，NTSS では同時に RC を削除してしまうので，EN が通信要求をする時には，既にハッカーにより RC が削除されている可能性がため，NAT テーブルの生成ができなくなる問題が発生する．

この問題の原因は，NTSS では NAT テーブル生成時と同時に RC を削除してしまうため，EN が RC を参照できなくなってしまうことにある．そこで図 3.3 のように，NTSSv2 では RC に適切な有効時間決めてタイマーによって削除するようにした．これにより，第三者によって RC が勝手に削除される心配がなくなるので，EN は確実に RC を参照することができる．

またハッカーが通信できてしまう問題は，NTSSv2 に限って発生した問題ではなく通常の NAT による UDP 通信にも発生する問題である．これを防ぐために通常のセキュリティ対策として，NTS WAP に予めフィルタを掛ければ防げるのではないかというものがあるが，NTS WAP は名前解決時に IP アドレスを特定することができないため困難である．そのため，NTSSv2 ではハッカーによる通信をスルーし，各端末に搭載されているファイアーウォールによって怪しい通信をブロックするという方針で考えている．

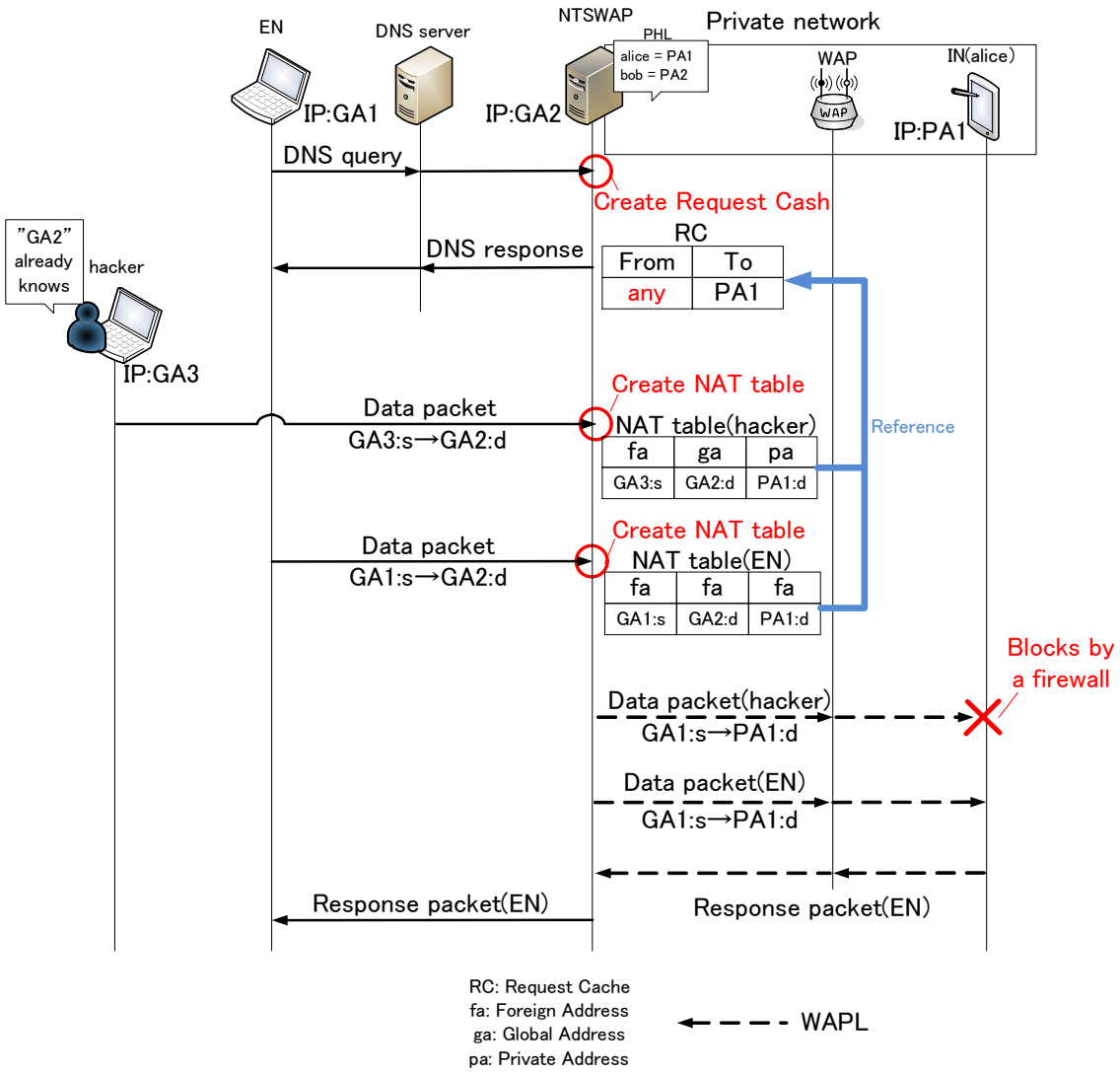


図 3.3　1. を解決した場合のシーケンス

3.3.2 同時通信

この場合の例として，EN1 は IN（alice）に，EN2 は IN（bob）にそれぞれ通信したい場合を例とする．NTS WAP は複数のシーケンスを受けた時には先着順に処理を行うものとし，RC は複数個生成できるものとする．

EN1 と EN2 はほぼ同時に名前解決を行うと，それぞれの問い合わせが僅かな時間差で NTS WAP に到着する．このとき，EN1 の問い合わせが先に到着したとすると，NTS WAP は EN1 の RC を先に生成し，その後 EN2 の RC を生成する．RC 作成後，EN1 と EN2 に名前解決結果（GA2）が応答される．

名前解決後，EN1 と EN2 は NTS WAP に向けてパケットを送信する．このとき，通信路の遅延や送信タイミングなどにより，EN1 より EN2 のパケットが先に到着したとする．そうすると，NTS WAP は最初に作成された EN1 用の RC を参照して ”any ”の部分を EN2 の IP アドレスとして NAT テーブルを作成する．これにより，EN2 は名前解決を行っていない IN（alice）に通信要求をしてしまう．同様に EN1 も名前解決を行っていない IN（bob）に通信要求をしてしまうことになるので，正しい相手と通信できない状態が発生してしまう．

この問題の原因は，NTS WAP は EN を特定できないにも関わらず，複数の端末を同時に処理することにある．NTSS において NTS ルータは EN の IP アドレスが通知されるため，RC を複数個保持していても EN を特定することが可能であった．しかし，NTSSv2 では EN の IP アドレスが通知されないので，複数の端末を同時に処理すること適切でないと考えた．

そこで解決策として，図 3.4 は NTS WAP が RC 生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 台の EN だけが通信要求を行っていると見なせるので，間違った RC を参照してしまうという心配はなくなる．この方法により，スループットが多少低下する可能性があるが，EN は正しい宛先と確実に通信を行うことができる．

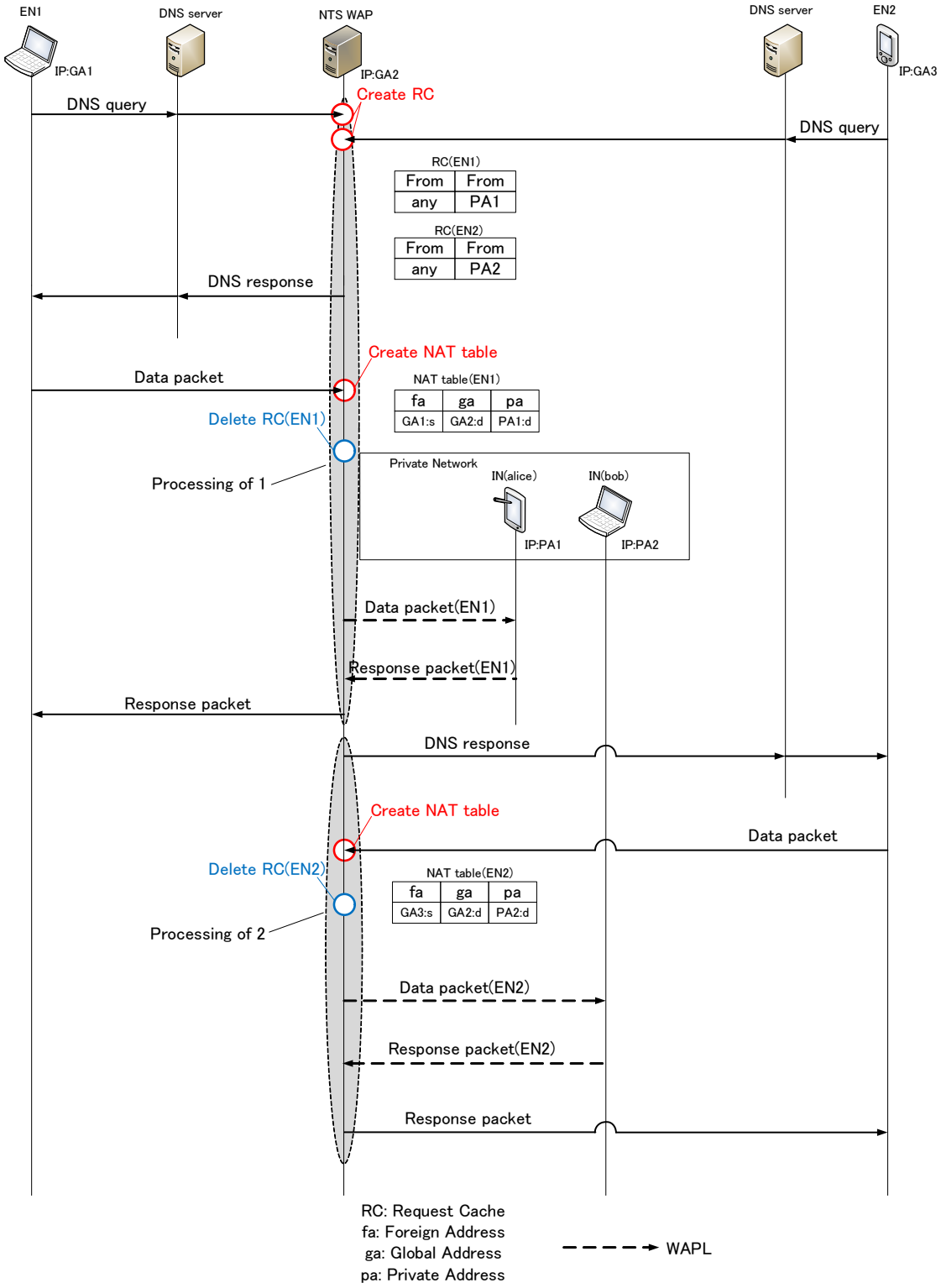


図 3.4　2. を解決した場合のシーケンス

第4章　実装

実装に向けて NTS WAP のモジュール構成を以下のように検討した．NTS sever module は NTSS における NTS サーバが搭載しているモジュールに改良を加えたもので，名前解決を BIND（DDNS）に依頼し，BIND から返される名前解決結果を元に RC 生成を行う．NTS router module は NTS ルータが搭載しているモジュールに改良を加えたもので，RC を参照して疑似パケットを作成し，NAT テーブルを生成する．BIND は DDNS のアプリケーションであり，natd は NAT のデーモンである．Create table module は DHCP と協調して RR，PHL を作成するモジュールである．WAPL は WAPL を実現するためのモジュール構成群を示している．

図 4.1 にモジュール構成を示す．NTS router module は NAT デーモン内に実装し，その他のモジュールは独立したものである．矢印はモジュール間で通信を行うことを示している．今後は実装に向けて，Create table module の詳細構成や NTS sever module，NTS router module の改良箇所の検討，WAPL との連携方法を検討をしていく予定である．

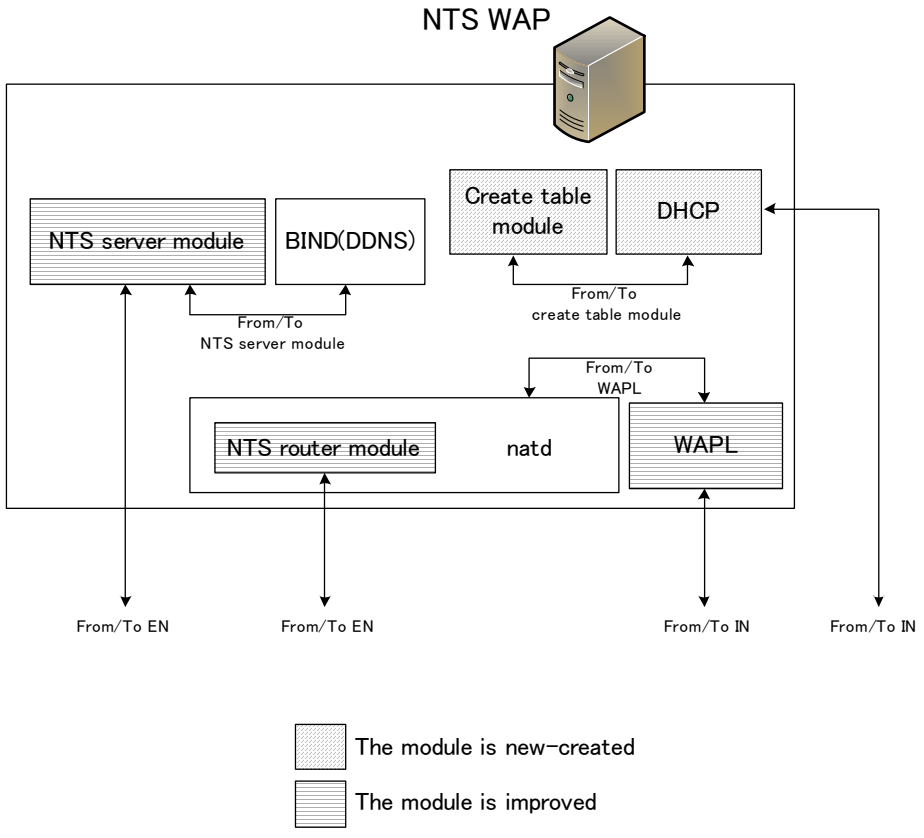


図 4.1　NTS WAP のモジュール構成

第5章　まとめ

本論文では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．提案方式ではDDNS側を改造することにより，ENのプライマリDNS登録変更を不要とした．またNTSSの類似機能を搭載し，DHCPとDDNSとWAPを一体化させたNTS WAPという装置として改造することにより，動的にRRとPHLを生成するようにした．これにより，ユーザは環境設定を変更する必要無くなるのでNTSSv2を容易に利用することができる．また提案方式の具体的な構成と動作シーケンスを示し，それに関するセキュリティについて考えられる課題と解決策を述べた．また実装に向けてNTS WAPのモジュール構成を検討した．今後は実装を進めていきたいと考えている．

謝辞

本研究にあたり，多大なる御指導と御教授を賜りました，渡邊晃教授には心から感謝いたします．
本研究にあたり，快く査読を引き受けて下さり，熱心にご指摘を頂きました，鈴木秀和教授には心から感謝いたします．
本研究にあたり，快く査読を引き受けて下さり，熱心にご指摘を頂きました，旭健作教授には心から感謝いたします．
最後に，本研究を進めるにあたり，数々の有益なご助言や御討論を賜りました，渡邊研究室，鈴木研究室の諸氏に感謝します．

参考文献

[1] 伊藤将志，鹿間敏弘，渡邊晃．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.