

平成25年度 卒業論文

邦文題目

**NTMobileにおける通信経路冗長化を抑制する
リレーサーバ選択手法の提案**

英文題目

**Proposal of Relay Server Selection Method
that Avoids Redundant Routes in NTMobile**

情報工学科 渡邊研究室
(学籍番号: 100430128)

若杉 純

提出日: 平成26年2月13日

名城大学理工学部

内容要旨

接続するネットワークの構成に関わらず通信を開始できる通信接続性と、ネットワークを切り替えても通信を継続できる移動透過性を実現する技術として、NTMobile (Network Traversal with Mobility) が提案されている。NTMobile では、端末どうしが直接通信を行うことが基本であるが、直接通信を行えない環境において通信接続性を確保するため、RS (Relay Server) と呼ばれる通信の中継装置を導入している。RS はグローバルネットワーク上に分散配置することが可能であり、通信の中継を行う RS は選択することができる。しかし、端末と RS のネットワーク上の位置を考慮せずに RS が選択されると、通信経路が冗長となる課題がある。

本論文では、NTMobile を実装した端末から RS までのルータ経由数を調査し、冗長化を最も抑制した通信経路を実現する RS 選択手法を提案する。提案方式のプロトタイプを実装し、仮想環境上で動作検証を行った結果、RS 選択手法によって通信端末間において最適な通信経路を構築できることを確認した。

目次

第1章	はじめに	1
第2章	関連研究	2
2.1	Mobile IPv4	2
2.2	Mobile IPv6	4
2.3	Dual Stack Mobile IPv6	6
第3章	NTMobile	8
3.1	NTMobileの構成	8
3.2	NTMobileの動作	9
3.3	RSの選択とRSを経由した通信経路の課題	11
第4章	RS選択手法	13
4.1	想定環境	13
4.2	RSの評価指標とホップ数調査	14
4.3	RSの選択	16
第5章	実装と評価	21
5.1	モジュール構成	21
5.2	動作検証	23
5.3	ホップ数調査の性能評価	24
第6章	関連研究との比較	27
6.1	IPv4ネットワークにおける比較	27
6.2	IPv6ネットワークにおける比較	28
6.3	IPv4/IPv6混在ネットワークにおける比較	29
第7章	まとめ	31
	謝辞	32
	参考文献	34
	研究業績	35

付録A	RTTとホップ数の関係	36
付録B	メッセージフォーマット	37
付録C	インターネットの構造	41
C.1	ISPのネットワーク	41
C.2	ASの接続形態	41

第1章 はじめに

近年，スマートフォンのような移動通信端末の普及や無線通信技術の発展により，あらゆるネットワークからインターネットに接続する需要が急激に増加している．そして，インターネット接続数に伴い増大するトラフィックを複数の無線回線に分散したり，通信を行いながら移動したいという要求が高まっている．IP ネットワークでは，IP アドレスがノード識別子と位置識別子の役割を担っており，通信端末がネットワークを移動すると IP アドレスが変化するため，通信を継続することができない．そのため，ネットワークを切り替えても通信を継続できる移動透過性と，接続しているネットワークの構成に関わらず通信を行うことができる通信接続性の実現が期待されている．

IPv4 グローバルアドレスの枯渇問題が深刻な状態となった今，NAT 機能によるプライベートネットワークを家庭や企業に導入し，通信端末にプライベートアドレスを割り当てること一般的となっている．しかし，グローバルネットワーク側からプライベートネットワーク側に対して通信を開始できない NAT 越え問題が発生し，端末の自由な双方向通信を妨げる要因となっている．長期的な解決策として，膨大なアドレス空間を持つ IPv6 ネットワークの普及活動が進められているが，IPv4 と IPv6 には互換性がないため，IPv4 と IPv6 のネットワークが共存する環境が長らく続くと考えられている．

移動透過性を実現する技術として，MIPv4 (Mobile IPv4) [1]，MIPv6 (Mobile IPv6) [2]，DSMIPv6 (Dual Stack Mobile IPv6) [3] が提案されている．これらの技術では通信端末の管理と通信の中継を行う HA (Home Agent) を導入することにより，NAT 越えや一般端末との通信を実現している．しかし，中継装置を経由した通信は経路が冗長となるため，なるべく冗長な経路を取らないように中継装置を選択することが望ましい．

通信接続性と移動透過性を IPv4/IPv6 混在環境において実現する NTMobile (Network Traversal with Mobility) が提案されている [4–8]．NTMobile では中継装置である RS (Relay Server) を導入している．RS はグローバルネットワーク上への自由な分散配置が可能であり，通信端末の通信相手毎に選択することができる．しかし，RS を選択する具体的な手法は検討されていない．

そこで，本論文では NTMobile を実装した通信端末から RS までのルータ経由数を調査し，冗長化を最も抑制した通信経路を実現する RS 選択手法を提案する．

以下，2 章で関連研究について，3 章では NTMobile について述べ，4 章で提案方式を説明する．そして，5 章では提案方式の実装と動作検証の結果を示し，6 章で関連研究との比較評価について示す．最後に 7 章でまとめる．

第2章 関連研究

本章では、一般端末との通信や NAT 越えを特殊な中継サーバを用いることにより可能とし、移動透過性と通信接続性を実現する関連研究について述べる。

2.1 Mobile IPv4

MIPv4 は、IPv4 ネットワークを対象とした移動透過技術である。本節においては、MIPv4 の機能を持つ移動端末を MN (Mobile Node)、MN の通信相手の端末を CN (Correspondent Node) と記述する。

2.1.1 Mobile IPv4 における通信

図 2.1, 図 2.2 に、MIPv4 における通信の様子を示す。MIPv4 では、ホームネットワークに HA (Home Agent) が配置され、訪問先ネットワークに FA (Foreign Agent) と呼ぶ装置を設置する必要がある。MN は起動時に利用する HA を決定し、HA から割り当てられた HoA (Home Address) を用いて通信を行う。HoA はホームネットワークと同様のプレフィックスを持つため、図 2.1 に示すように、ホームネットワーク内に存在する MN は、CN に対して通常の通信を行うことができる。しかし、MIPv4 において移動端末の通信接続性を確立する

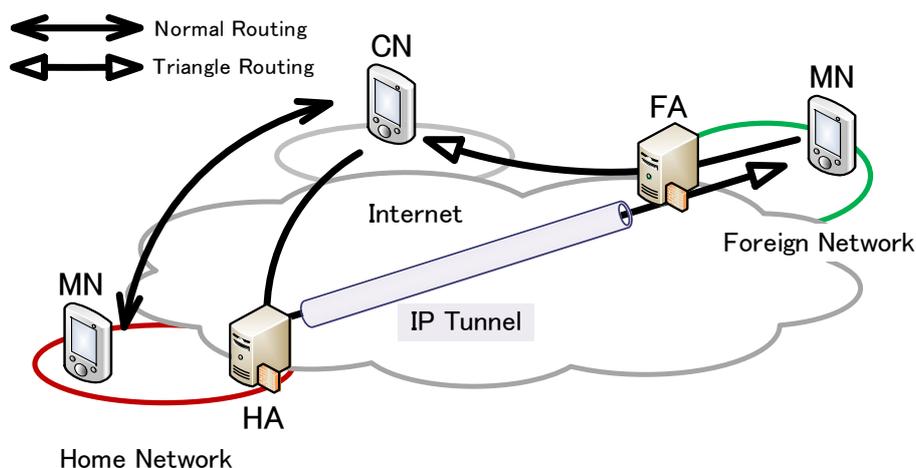


図 2.1 Mobile IPv4 における NAT が存在しない環境での通信経路

ためには、HA をグローバルネットワーク上に設置し、HoA をホームネットワークと同様のプレフィックスを持つ IPv4 グローバルアドレスにする必要がある。これは IPv4 におけるアドレス枯渇問題に逆行する致命的な課題である。

MN は FA が存在する訪問先ネットワークに移動すると、FA が送信する Agent Advertisement により FA の CoA (Care of Address) と MAC アドレス (Media Access Control address) を取得する。MN は HoA と CoA を FA を通して HA に登録し、HoA と CoA を関連付ける。HA は、HoA と HA の MAC アドレスを関連付ける ARP (Address Resolution Protocol) 処理を実行し、ホームネットワークに届けられる MN 宛てのパケットを受信する。HA が HoA 宛てのパケットを受信すると、CoA に対する IP トンネルを用いて、訪問先ネットワークにパケットを転送する。FA がパケットをデカプセル化し、MN に転送することにより、MN に HoA 宛てのパケットが到達する。MN は CN 宛てのパケットを、送信元 IP アドレスを HoA として送信する。以上のようにして、MN と CN は通信を行う。

MIPv4 における通信の課題として、三角経路と呼ばれる HA を経由する冗長な経路を取ることが挙げられる。更に、MN から CN までの経路上のルータがインGRESSフィルタリング [9] を行っている場合、送信元 IP アドレスを HoA に偽装した MN から CN 宛てのパケットが破棄される恐れがある。そのため、MN から CN 宛のパケットを、一度 HA に IP トンネルにより送信し、HA から CN に対して転送する Reverse Tunneling [10] と呼ばれる方法で通信を行うことが強く求められている。しかし MN と CN の通信は必ず HA を経由するため、ドッグレグ経路と呼ばれる、より冗長な通信経路となる。

図 2.2 に示すように、MN が NAT 配下の訪問先ネットワークに移動した場合における NAT 越えは、MN と HA との間に UDP トンネルを構築することにより実現している [11]。ただし Reverse Tunneling と同様に、MN と CN の通信パケットはすべて HA を経由するため、必

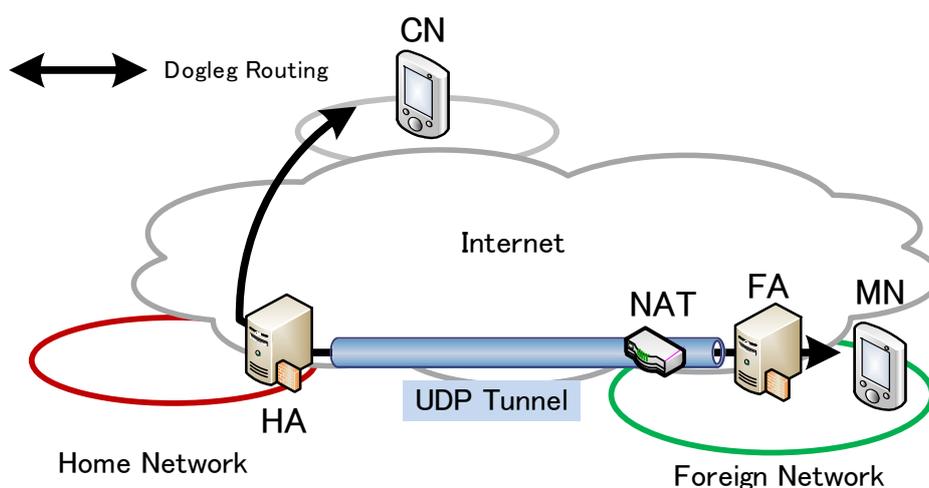


図 2.2 Mobile IPv4 における NAT が存在する環境でのドッグレグ経路

ずドッグレグ経路となる。

さらに、CN が MIPv4 機能を持つ端末であり、MN および CN の双方がホームネットワークとは異なるネットワークに移動している場合、MN と CN 間の通信は、MN 側および CN 側の 2 台の HA を経由するという一層冗長な通信経路となる。そのため、通信経路の伸長によってパケットの伝送遅延が増加し、スループットが低下すると考えられる。

2.1.2 Mobile IPv4 における HA 選択

HA が端末の位置管理や中継機能を一手に引き受けているため、HA の障害により MIPv4 の機能を利用することが一切不可能となる、一点障害と呼ばれる課題がある。また、三角経路では 3 つのすべての通信経路が正常であることが求められるため、通信経路の障害に対しても脆弱となる。よって HA を分散配置し、経路の冗長化を抑えた HA の割り当てや、負荷分散を行うことが求められる。

MN は起動時に、利用する HA を動的に選択可能であると規定されている [12]。動的 HA 選択処理において、MN は Requested HA と呼ばれる装置に HA の割り当て要求を行う。Requested HA は MN に割り当てる HA (Assigned HA と呼ぶ) を決定し、Assigned HA の IP アドレスを MN へ返答する。しかし Requested HA が複数の HA を評価し、Assigned HA を決定する具体的な手法は定められていない。また HA が HoA 宛てのパケットを代理受信するため、HA の設置個所はホームネットワーク内に限定されている。そのためインターネット上の広域に HA を分散配置することは不可能であり、負荷分散と経路冗長化の抑制は困難である。

また、MN はどのネットワークに接続したとしても、ホームネットワークと同一のプレフィックスである HoA を使い続けなければならない。つまり端末が利用する HA は、一度選択した HA から別の HA に変更できないため、移動した先がネットワーク的にホームネットワークから遠くなるにつれ、経路の冗長性が悪化することは避けられない。

2.2 Mobile IPv6

MIPv6 は、IPv6 ネットワークを対象とした移動透過技術であり、MIPv4 と同様に HoA と CoA の 2 つの IP アドレスを利用する。本節においては、MIPv6 の機能を持つ端末を MN、MN の通信相手の端末を CN と記述する。

2.2.1 Mobile IPv6 における通信

図 2.3 に、MIPv6 における通信の様子を示す。MIPv6 では MIPv4 と同様に、MN はホームネットワークに配置された HA から割り当てられた HoA を利用して通信を行うため、ホームネットワーク上においては通常の IP 通信が可能である。訪問先ネットワークに MN が移動すると、MN はルータが送信している Router Advertisement により移動を検知し、CoA を生

成, そして HA に登録を行う。その後, HA は Neighbor Advertisement を実施することにより, HA が HoA 宛ての packets を受信する。 packets は MN と HA 間の IP トンネルにより CoA 宛てとして転送され, MN 自身が packets のデカプセル化処理を行うことにより, MN は HoA 宛ての packets を受信する。 MIPv6 ではイングレスフィルタリングへの対応のため, MN から CN 方向の packets も HA への IP トンネルを経由して転送される。

MIPv6 では, Return Routability と呼ぶ認証機構を用いた Route Optimization (経路最適化) により, 端末どうしの直接通信を実現する。通信相手端末が経路最適化処理に対応していない場合, HA を経由した通信を継続する。

2.2.2 Mobile IPv6 における HA 選択

MIPv6 は MIPv4 と同様に, HA の設置個所がホームネットワーク内に限定されており, MN は HoA を管理する HA を利用し続けなければならない。そのため, 通信経路の冗長化によるスループットの低下や, HA における一点障害への対策として, 通信経路や負荷分散を考慮した HA の選択が要求される。しかし, MN が移動によって HA からネットワーク的に遠くなるにつれ, 経路の冗長性が悪化することは避けられない。

文献 [2] において, IP エニーキャスト [13] を利用した HA の動的発見手法が規定されている。 MN は, ホームネットワークの IP サブネットプレフィックスのエニーキャストアドレス [14] へ ICMP Home Agent Address Discovery Request Message を送信することにより, ネットワーク的に最も近い HA の IP アドレスの取得を試みる。 ICMP Home Agent Address Discovery Request Message を受信した HA は, サブネットに対応した HA のグローバルユニキャストアドレスを含めた ICMP Home Agent Address Discovery Reply Message を送信する。

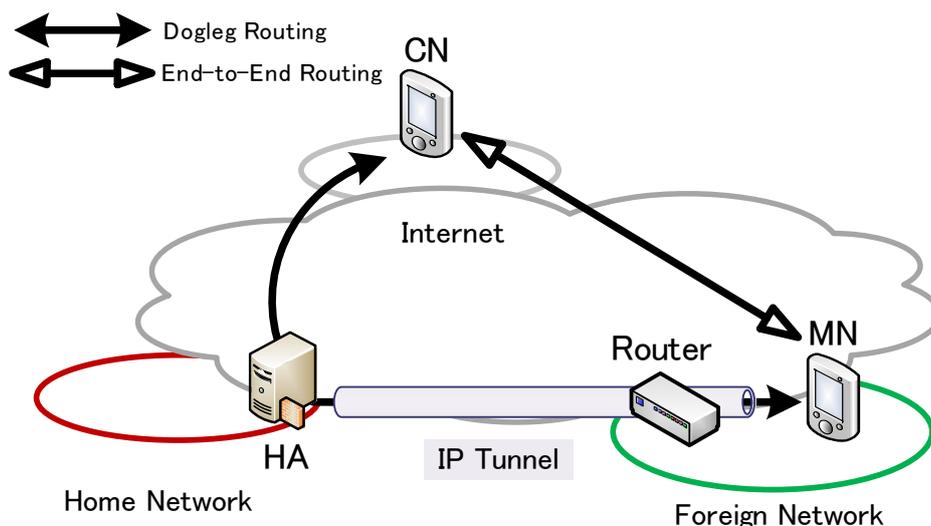


図 2.3 Mobile IPv6 における通信経路

IP エニーキャストによるパケットは最も近い宛先に到達するため、IP エニーキャストは経路の冗長化の抑制と負荷分散に用いられている。ホームネットワーク内部を対象として IP エニーキャストを行った場合、内部の HA のみが対象となるため、経路冗長化や一点障害への対策、負荷分散としては効果が薄い。IP エニーキャストを用いた分散配置を広範なグローバルネットワーク上で行う代表的な例として、権威ある DNS (Domain Name System) における運用 [15] が挙げられる。しかし IP エニーキャストを用いた場合の負荷分散は、端末が最もネットワーク的に近い HA に接続する性質によるものであり、HA が管理する端末数を制御するといった高度な負荷分散は行えない。

文献 [2] には、ホームネットワーク上に複数の HA が存在する場合、優先度が高い順に複数の HA の IP アドレスを MN に通知する手法が拡張的な仕様として規定されている。HA は Router Advertisement を送受信することにより、ホームネットワーク上にあるすべての HA の情報を記録した HA リスト (Home Agent List) を保持している。HA リストには、HA のリンクローカルアドレス、グローバルユニキャストアドレス、情報の有効期限 (Lifetime)、選択での優先度 (Preference) が記載される。優先度は値が高いほど望ましく、優先度が記載されていない場合は既定値 (0) を取る。しかし、HA の優先度の具体的な決定手法は定義されていない。

2.3 Dual Stack Mobile IPv6

DSMIPv6 は、MIPv6 を IPv4/IPv6 混在環境に対応するように仕様を拡張した移動透過技術である。本節においては、DSMIPv6 の機能を持つ端末を MN、MN の通信相手の端末を CN と記述する。

2.3.1 Dual Stack Mobile IPv6 における通信

図 2.4 に、DSMIPv6 における通信の様子を示す。DSMIPv6 では、ホームネットワークに配置した HA を IPv4/IPv6 デュアルスタック構成^{*1}としている。MN は IPv4/IPv6 の HoA を取得でき、IPv4/IPv6 双方のネットワークにおいて HA を利用した通信が可能である。また、HA と NAT 配下の MN との間に UDP トンネルを構築することにより NAT 越えを実現し、HA がプロトコルの違いを吸収することによって IPv4/IPv6 相互通信を可能としている。しかし、MIPv4 と同様に HoA はグローバルアドレスである必要があるため、IPv4 グローバルアドレスの枯渇問題に逆行するという課題がある。

MIPv6 において定められた Route Optimization は、MN が IPv6 ネットワークに接続し、CN と IPv6 アプリケーションによる通信を行っている場合のみ、適用可能である。しかし MN が IPv4 ネットワークに接続している場合や、IPv4 アプリケーションを用いて CN と通信するとき、HA を経由する冗長経路を取る。

^{*1}装置が IPv4/IPv6 ネットワーク双方に接続され、両プロトコルによる通信を可能とした形態

2.3.2 Dual Stack Mobile IPv6 における HA 選択

MIPv6 における動的 HA 選択は、MN のホームネットワークと同様のプレフィックスを持つエニーキャストアドレスを利用しているが、これは IPv6 ネットワークにおいてのみ動作する。仮に MN が IPv4 ネットワークに接続しているならば、DNS による HA の FQDN の名前解決を行うことにより、HA の IP アドレスを取得する。しかし、負荷分散や経路冗長化の抑制を考慮した HA の選択は議論されていない。

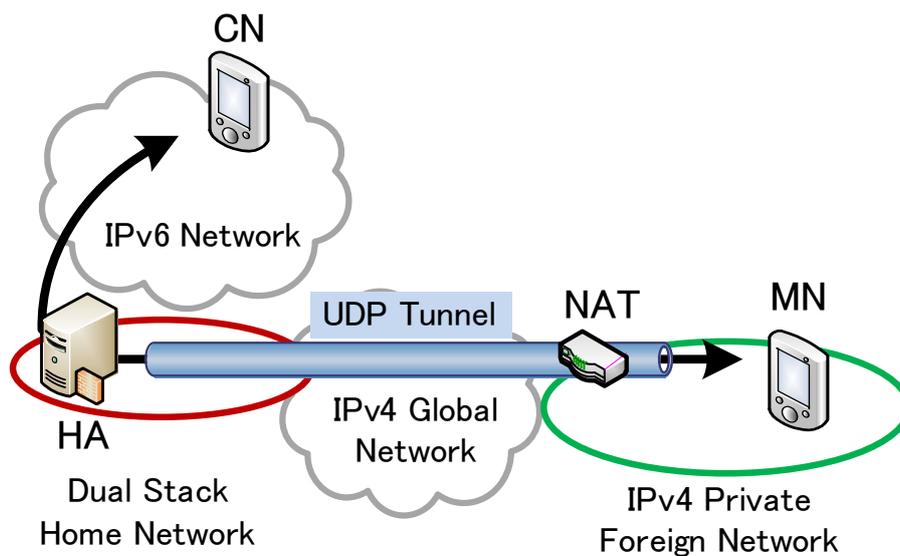


図 2.4 Dual Stack Mobile IPv6 における通信経路

第3章 NTMobile

本章では，提案方式を適用する NTMobile について説明する．

3.1 NTMobile の構成

図 3.1 に NTMobile のネットワーク構成を示す．NTMobile は，NTMobile を実装した通信端末（NTM 端末），NTM 端末が通信相手と直接通信を行えない場合に，NTM 端末の通信を中継する RS，NTM 端末のアドレス情報を管理する DC（Direction Coordinator）により構成される．DC は，NTM 端末へ仮想 IP アドレスを配布するほか，NTM 端末の通信において使用する RS を必要に応じて自由に選択し，NTM 端末と RS に対してトンネル構築の指示を行う装置である．DC と RS はグローバルネットワーク上に設置され，ネットワークの規模に応じて自由に分散配置することができる．また DC は RS の負荷情報を収集し，RS の負荷分散を行うことができる [16]．DC と RS はデュアルスタックネットワーク上に設置し，IPv4/IPv6 混在環境へ対応する．

通常，直接通信を実現できない通信環境は，NAT 配下に存在する NTM 端末どうしの通信

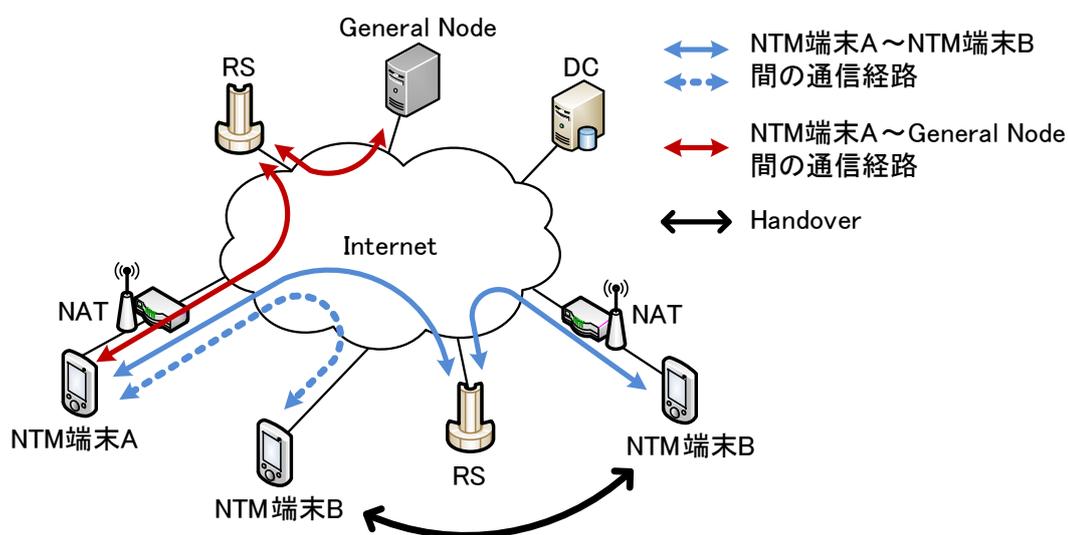


図 3.1 NTMobile のネットワーク構成

や、NTM 端末と一般端末 GN (General Node) との通信、IPv4/IPv6 の相互通信である。RS がこれらの通信を中継することにより、NTM 端末は接続しているネットワークに関わらず、通信を開始することができる。

NTM 端末は起動時に、DC に対して実 IP アドレスなどのアドレス情報の登録を行い、DC から仮想 IP アドレスを取得する。NTM 端末は仮想 IP アドレスをノード識別子、実 IP アドレスを位置識別子として利用する。NTM 端末のアプリケーションは仮想 IP アドレスを自身の IP アドレスであると認識する。

NTM 端末は通信開始時に、DC に対して経路指示を依頼する。DC は、通信相手が NTM 端末であるか判定し、更に NTM 端末と通信相手のネットワーク上の位置関係を識別し、通信経路を決定する。NTM 端末どうしが直接通信できる場合、DC は NTM 端末間で直接トンネルを構築するように、両 NTM 端末に指示する。RS を必要とする場合には、DC は利用する RS を選択し、NTM 端末と RS との間にトンネルを構築するように NTM 端末と RS に対して指示を行う。NTM 端末はトンネル構築指示に従い、NTM 端末との間、もしくは RS との間に UDP トンネルを構築し、通信経路を確立する。

NTM 端末はネットワークを移動すると、DC に対してアドレス情報の更新処理を行う。このとき DC の経路指示により新しいトンネルが構築されるが、仮想 IP アドレスは変化しないため、アプリケーションの通信は継続される。

NTMobile では、DC どうし、DC と RS 間、および DC と NTM 端末間には信頼関係があることを前提とする。NTMobile の制御メッセージはあらかじめ共有した共通鍵によって暗号化され、メッセージの改ざんを防ぐために MAC (Message Authentication Code) が付加される。NTM 端末間、NTM 端末と RS との間の通信は、トンネル構築時に DC から配布される共通鍵によって、暗号化と MAC の付加が行われる。

3.2 NTMobile の動作

以後の説明では、通信を開始する側の NTM 端末を MN (Mobile Node) とし、MN を管理する DC を DC_{MN} とする。また、通信相手となる NTM 端末を CN (Correspondent Node) とし、CN を管理する DC を DC_{CN} とする。

3.2.1 アドレス情報の登録

NTM 端末は自身のアドレス情報を DC に登録するため、NTM 端末の起動時とネットワーク移動時に、NTM 端末の実 IP アドレスや FQDNなどを記載した NTM Registration Request を DC に対して送信する。DC は NTM Registration Request を受信したとき、NTM 端末の実 IP アドレスと IP ヘッダの送信元 IP アドレスが異なれば NTM 端末が NAT 配下に存在すると判別し、送信元 IP アドレスを NAT ルータの IP アドレスとして取得する。DC は、NTM 端末の FQDN から NTM 端末の一意な識別子である Node ID を生成する。また、NTM 端末に仮

想 IP アドレスを割り当て、NTM 端末のアドレス情報をレコードとして記録する。その後、仮想 IP アドレスなどを記載した NTM Registration Response を NTM 端末に対して送信する。

NTM 端末のアドレス登録が完了した後、NTM 端末と DC は定期的にメッセージを交換する (Keep Alive)。Keep Alive により、DC から NAT 配下に存在する NTM 端末までの制御メッセージ用の通信経路を確保する。

3.2.2 名前解決とトンネル構築

図 3.2 に、MN および CN が NAT 配下に存在する場合に、MN から CN に対して通信を開始するときのトンネル構築シーケンスを示す。MN は CN の名前解決を行う DNS 問合せをトリガーとしトンネル構築シーケンスを開始する。MN は、CN の名前解決処理とトンネル構築指示を依頼するため、DC_{MN} に対して CN の FQDN (FQDN_{CN}) を記載した NTM Direction Request を送信する。DC_{MN} は、自身が CN のアドレス情報を管理していない場合、CN が NTM 端末であり、DC_{CN} に管理されていることを調査する。そして DC_{CN} に対して NTM Information Request を送信することにより、CN のアドレス情報を要求する。DC_{CN} は

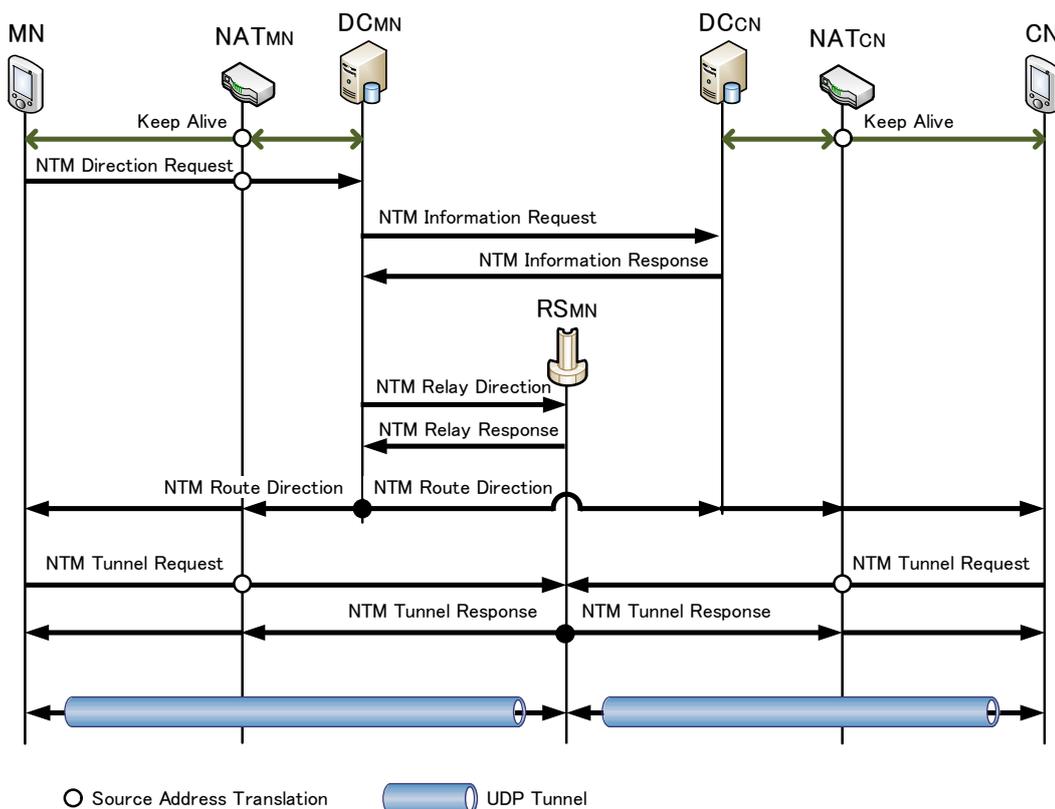


図 3.2 トンネル構築シーケンス

FQDN_{CN} のレコードを検索し、取得した CN のアドレス情報を記載した NTM Information Response を DCMN に送信する。

DCMN は、MN と CN のアドレス情報からネットワーク上の位置関係を判別する。この場合 MN と CN が NAT 配下に存在するため、DCMN は RS を経由した通信経路を構築することを決定する。そして、DCMN は自身の管理下にある RS の中から、利用する RSMN を選択する。

DCMN は、RSMN に対して NTM Relay Direction を送信し、MN との間、および CN との間にトンネルを構築するよう指示する。RSMN はトンネル構築を行えることを NTM Relay Response により DCMN に通知する。DCMN は MN に対して直接、および CN に対して DC_{CN} を経由して NTM Route Direction を送信し、RSMN に対してトンネル構築依頼を行うように指示する。その後、NAT 配下にある MN と CN から、グローバルネットワークにある RS に対して NTM Tunnel Request を送信する。そして RSMN が MN と CN に対して NTM Tunnel Response を返信することにより、MN と RSMN 間、および CN と RSMN 間でトンネルを構築する。

RS を経由する経路によって通信を確実に確立した後、自律的経路最適化処理を MN と CN 間で行うことにより、MN と CN 間で直接トンネルを構築する経路最適化が可能な場合がある [17]。最適化が行えない場合、RS を経由した通信を継続する。

MN が GN に対する通信を開始する場合には、GN についての名前解決とトンネル構築指示の依頼を受けた DCMN が、GN が一般端末であると判断し、RS を経由した通信経路を構築することを決定する。DCMN は MN と GN 間の通信で利用する RS を選択し、MN と RS の間でトンネルを構築するよう指示する。MN と GN 間の通信パケットは、RS においてカプセル化/デカプセル化を行い転送される。GN は通信相手を RS だと認識しているため、MN がネットワークを移動しても通信を継続することができる。

3.2.3 ネットワーク移動時のトンネル再構築

MN はネットワークを移動したことを検出すると、実 IP アドレスなどのアドレス情報を更新するため、DCMN に対して NTM Registration Request を送信する。また通信のトンネルを再構築するため、3.2.2 項に示したトンネル構築のシーケンスを再び行い、通信を継続する。

3.3 RS の選択と RS を経由した通信経路の課題

MN から CN までの最適な通信経路は、経路の冗長性がない直接通信である。直接通信を実現できない環境では、RS を経由した冗長な経路を取る。しかし NTMobile では、RS の選択手法が確立されていない。RS の選択が経路の冗長性を考慮して行われなければ、通信を行う端末からネットワーク上の位置が遠い RS を選択してしまう場合がある。よって、図 3.3 に示すように、端末が移動した先々において適切な RS を選択する手法の確立が望まれる。

通信経路の長さが伸びることによる課題として、パケット伝送遅延が増加すること、スループットが低下すること、ネットワーク負荷が増大することが挙げられる。

DCMN が選択することができる RS は、MN から CN への通信開始時においては自身の管理下にある RS に限られている。そのため、MN と CN の通信において DC_{CN} の管理下の RS が最適な位置にあったとしても、利用することができない課題がある。

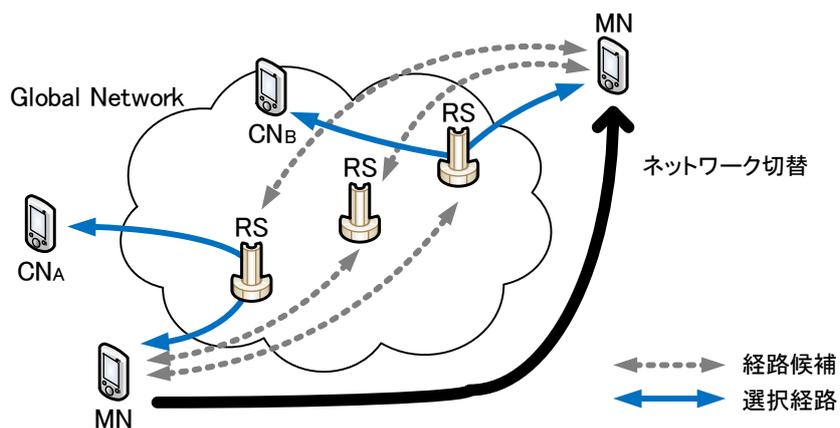


図 3.3 接続先に応じた最適な RS の選択

第4章 RS 選択手法

通信経路の冗長化を抑制するため、RS の負荷分散を行いつつ、通信経路のルータ経由数（ホップ数）を最小とする RS 選択手法を提案する。NTM 端末が DC へ実 IP アドレスの登録を行うと、その都度 DC は NTM 端末から RS までのホップ数の調査を実施する。DC は、NTM 端末が RS を必要とする通信を開始するとき、最もホップ数が少ない経路を構築するため各 RS を経由した場合の経路を比較し、最適な RS を選択する。

RS の選択処理においてホップ数による経路評価は必須とせず、DC は RS の負荷情報のみから選択可能とする。これによりホップ数の調査が、NTM Mobile における通信開始時のオーバーヘッドとなることを防止する。

4.1 想定環境

図 4.1 に、本提案において想定する NTM Mobile のシステム構成を示す。DC_{MN} は RS_A～RS_C を、DC_{CN} は RS_L～RS_N をそれぞれ占有して管理する形態であり、最もシンプルなシステム構成である。また、DC は管理下の RS の負荷分散を考慮するため、RS の負荷情報を収集していることを前提とする。DC と RS はグローバルネットワーク上に複数台分散配置され、その規模は運用実績が積まれるにつれて拡大していく。

ネットワーク規模の拡大に伴い、RS の資源の有効活用のために 1 台の RS を複数台の DC

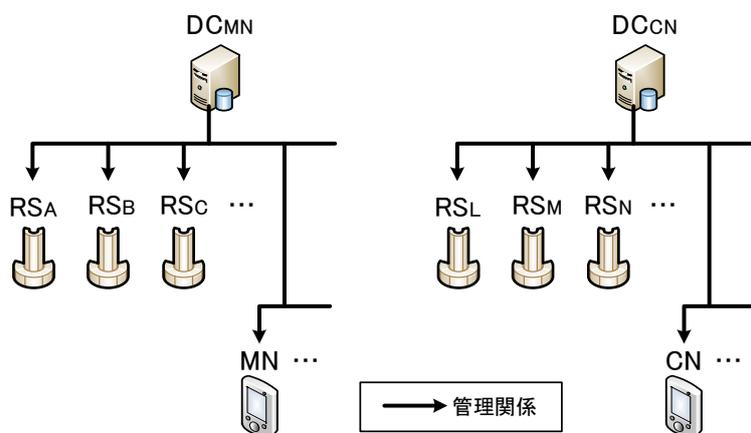


図 4.1 想定するシステム構成

が管理・利用する形態へ移行すると考えられる。提案手法はこの形態においても適用可能であり、かつネットワーク規模に関わらず安定的な動作が可能であるように検討を行う。

4.2 RSの評価指標とホップ数調査

4.2.1 RSの評価指標

DCはRSを、NTM端末から各RSまでの通信経路のホップ数と、各RSの負荷情報により評価する。IPv4ネットワークにおけるホップ数は、IPヘッダ内のTTL (Time to Live) を用いて調査する。TTLはIPパケットがルータを経由する度に減少するため、TTLの初期値との差を算出することによりホップ数が得られる。IPv6ネットワークにおいては、TTLと同様の仕様であるHop limitを用いる。NTM端末がネットワークに接続したとき、その都度NTM端末からDC管理下のすべてのRSまでの通信経路を調査する必要がある。

通信経路の評価指標として、パケットの往復遅延時間を示すRTT (Round Trip Time) が挙げられる。NTM端末が接続するネットワークは無線環境であることが想定されるが、第3世代移動通信システム (3G) のように回線の帯域が比較的狭いネットワークにおいては、多数の調査用の制御メッセージを送受信することは避けることが望ましい [18]。また3GはRTTが比較的長く、かつ振れ幅が大きい。そのため、NTM端末からRSまでのRTTを正確に測定するには多数の制御メッセージの往復が必須となり、ネットワークと端末に負荷が掛かる。この影響はNTM端末が頻繁な移動を行うほど大きくなるため、RTTはNTM端末から各RSまでの経路の評価指標として適さない。

CAIDA (The Cooperative Association for Internet Data Analysis) *² によるRTTとホップ数の関連性の調査 [19,20] により、ホップ数が増加するとRTTも共に上昇する傾向があることが分かっている。そのため、通信経路のホップ数を低く抑えることにより伝送遅延の低下、スループットの向上が期待できる。ホップ数は通信経路にある通信設備に依存した指標であるため、接続したネットワーク毎にNTM端末は各RSに対して1つずつパケットを送信するだけでよく、経路調査によるネットワークおよび端末の負荷を最小限に抑えることができる。

4.2.2 ホップ数の調査

図4.2に、新たに定義したUDPのメッセージによる、NTM端末からRSまでのホップ数調査のシーケンスを示す。NTM端末は、起動や移動を行い新たなネットワークに接続したとき、DCに対してアドレス情報の登録を行う。DCはアドレス情報の登録処理をトリガーとし、その位置にあるNTM端末から管理下にあるすべてのRSまでのホップ数の調査を開始する。このときDCは、登録されたNTM端末のアドレス情報から、NTM端末のIPv4お

*²インターネット・データ分析協会 <http://www.caida.org/home/>

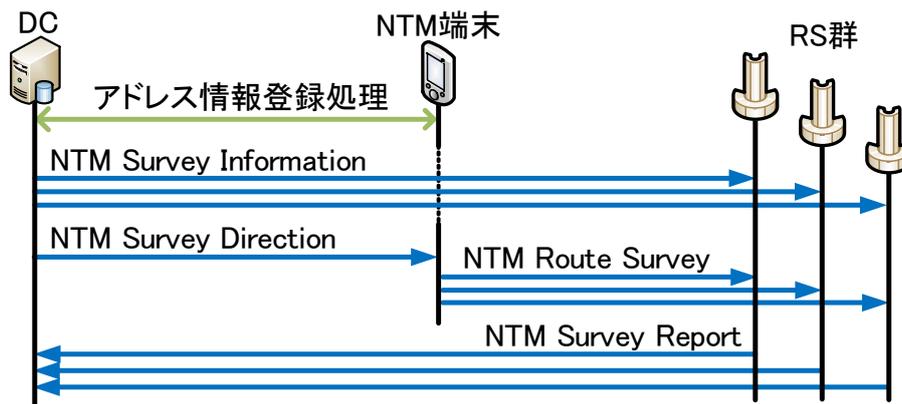


図 4.2 NTM 端末から RS までのホップ数調査

よび IPv6 のネットワークへの接続状態を識別し、接続している IP ネットワークにおける RS までのホップ数を調査する。

NTM Mobile の前提によると、NTM 端末と DC、DC と RS、DC と DC の間には信頼関係があるが、NTM 端末と RS の間には信頼関係がない。そのため両者と信頼関係がある DC が、調査毎に調査用の一時鍵 (Survey Temp Key) を生成・配布することにより、調査時において NTM 端末と RS の間に一時的な信頼関係を構築する。

DC は管理下の RS に対し NTM Survey Information を送信することにより、NTM 端末からホップ数調査が行われることを通知する。DC は NTM Survey Information に、調査を行う NTM 端末の識別に用いる Node ID、NTM 端末との間の一時鍵である Survey Temp Key、情報の期限を示す Timeout、ホップ数調査の結果を報告する DC を示す DC の IP アドレスを記載する。RS は NTM Survey Direction より得た情報をデータベースの Survey Information Table に記録する。Survey Information Table のレコードは、Timeout の期限を過ぎた場合削除する。

DC は NTM 端末に対し、調査対象となる RS の IP アドレスや Survey Temp Key を記載した NTM Survey Direction を送信し、各 RS までのホップ数調査を指示する。

NTM Route Survey は、NTM 端末から RS までの経路における、TTL または Hop limit の変化を確認するためのメッセージである。TTL の初期値は端末に実装されている OS (Operating System) のカーネルによって異なるため、NTM 端末は自身が生成する TTL、Hop limit の初期値を取得する。NTM Route Survey には、NTM 端末の TTL 初期値または Hop limit 初期値、NTM 端末の Node ID、調査指示を出した DC の IP アドレスを記載する。そして NTM 端末は、改ざん検知のために Survey Temp Key を用いた MAC を NTM Route Survey に付加し、各 RS へ送信する。NTM 端末は NTM Route Survey を送信し終わると、Survey Temp Key を破棄する。

RS は NTM Route Survey を受信すると、記載されている NTM 端末の Node ID と DC の IP アドレスをキーとして Survey Information Table を検索し、当該の Survey Temp Key を取

得する。RS は Survey Temp Key を用いて NTM Route Survey の MAC 認証を行う。認証に失敗した場合、RS は NTM Route Survey を破棄する。認証に成功し、正規のメッセージであると RS が判断したとき、IPv4 の場合にはメッセージの IP ヘッダ内の TTL と、NTM Route Survey メッセージ内の TTL 初期値の差をホップ数として取得する。IPv6 の場合では、TTL と同様にして、Hop limit の変化量をホップ数として取得する。

RS は NTM Survey Report に、NTM 端末の Node ID、調査対象とされた RS の IP アドレス、NTM 端末から RS までのホップ数を記載し、調査指示を行った DC へホップ数の調査結果を報告する。

DC は NTM Survey Report を受信すると、NTM 端末から管理下の RS までのホップ数を Hop Table に記録する。

ホップ数調査は UDP のメッセージを用いており、調査結果の報告は各 RS が個別に行うため、ホップ数の調査結果の一部が正常に報告されない場合があり得る。DC は NTM Survey Information から始まるホップ数調査自体にタイムアウトを設け、タイムアウト後にホップ数調査が完了していない RS へ対して、ホップ数の再調査を行う。

4.3 RS の選択

RS を必要とする通信は、通信を行う端末に着目すると次のように場合分けできる。

- 同一の DC に管理されている NTM 端末どうしの通信
- 異なる DC に管理されている NTM 端末どうしの通信
- 一般端末との通信

それぞれの場合において、最も経路冗長化を抑制できる RS を選択する。また、異なる DC に管理されている MN と CN の通信において、DC_{MN} 側に管理されている RS、および DC_{CN} 側に管理されている RS の双方の中から、DC_{MN} が最適な RS を選択可能する。これにより、NTM Mobile における RS の選択と RS を経由した通信経路の課題を解決する。

4.3.1 同一の DC に管理されている NTM 端末どうしの通信における RS 選択

以後の説明では、MN と CN を管理する DC を、DC_{MN-CN} と記述する。

図 4.3 に、MN と CN が DC_{MN-CN} に管理されている場合に、MN から CN に対する RS を経由した通信を開始するシーケンスを示す。MN は DC_{MN-CN} に対し、CN までの経路指示の依頼のため、NTM Direction Request を送信する。DC_{MN-CN} は、MN と CN の通信において最適な RS を選択する処理を行う。

この場合、MN と CN は DC_{MN-CN} 管理下の RS に対してホップ数調査を行っている。DC_{MN-CN} は負荷に問題がない RS_A~RS_C を選択の対象として抽出したとする。そして DC_{MN-CN} は

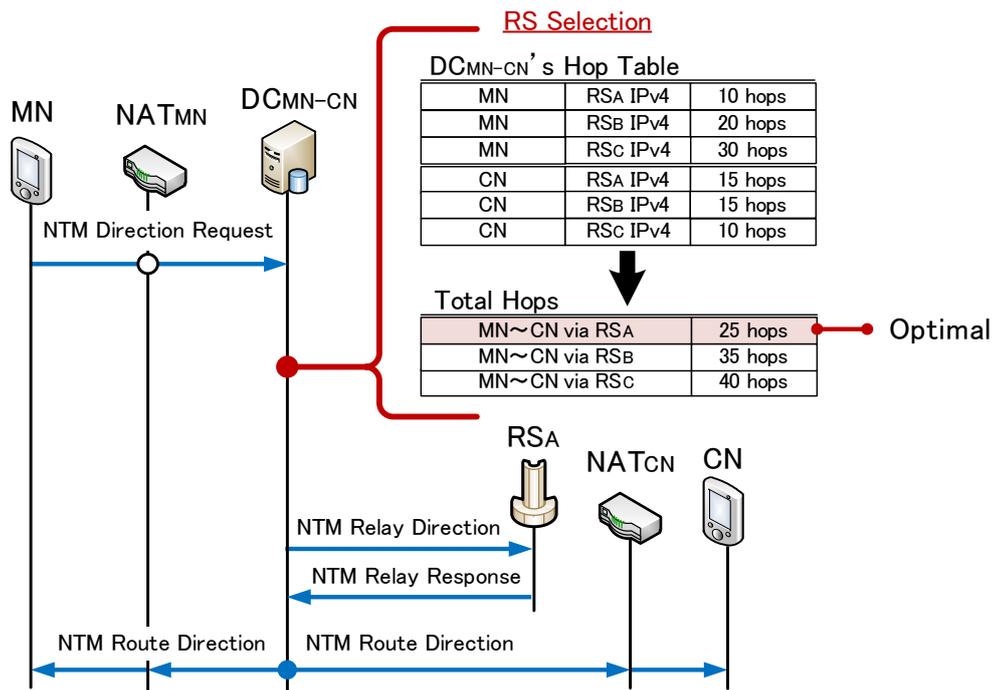


図 4.3 同一の DC に管理されている NTM 端末どうしの通信における RS 選択

MN から各 RS までのホップ数と CN から各 RS までのホップ数の両方の情報を、Hop Table から MN の Node ID, CN の Node ID, 選択対象の RS の IP アドレスなどをキーとして検索し、MN から各 RS を経由して CN に到達するまでの総経路のホップ数を算出する。DCMN-CN は総経路のホップ数が最少となる RSA を選択し、トンネル構築までの経路指示手順を実施する。以上により、経路の冗長化を最も抑えた MN から CN までの通信経路を実現する。

4.3.2 異なる DC に管理されている NTM 端末どうしの通信における RS 選択

MN と CN が異なる DC, それぞれ DCMN, DCCN に管理されている場合に、MN から CN への通信に用いる RS の選択手法を検討する。このとき DCMN が、MN と CN の通信において最適な RS が DCMN 管理下にある場合と、DCCN 管理下にある場合に分けられるため、それぞれの事例におけるトンネル構築シーケンスについて述べる。

以下の説明において、RSA, RSB, RSc は DCMN 管理下にあり、負荷状態に問題なく選択可能とされた RS である。RSL, RSM, RSN は DCCN 管理下にあり、同様に選択可能とされた RS である。

DCMN の RS を選択する場合

図 4.4 に、異なる DC に管理されている NTM 端末どうしの通信において、DCMN 管理下の RS を選択するときのトンネル構築シーケンスを示す。DCMN は CN までの経路指示依頼を MN から受けると、DCCN に対して既存の NTM Information Request を送信する。DCCN は NTM Information Request を受信すると、DCCN 管理下の負荷状態に問題のない RSL~RSN を抽出する。そして RSL~RSN の IP アドレスと CN の Node ID をキーとして Hop Table を検索し、RSL~RSN までの CN からのホップ数を取得する。

NTM Mobile の制御メッセージには、オプションヘッダを付加することにより追加情報を記載することができる。新たに定義したオプションヘッダである Route Information に、RSL~RSN までの CN からのホップ数と、RSL~RSN の IP アドレスを 1 つのレコードとして、ホップ数が昇順となるように記載する。ホップ数が同一の RS が存在する場合は、負荷状態を考慮した順序とする。すべての評価が同一となった RS は、ランダムな順序で記載する。DCCN は既存の NTM Information Response に Route Information を含め、DCMN に送信する。

DCMN は、MN にとって最も近い RS までのホップ数と、CN にとって最も近い RS までの

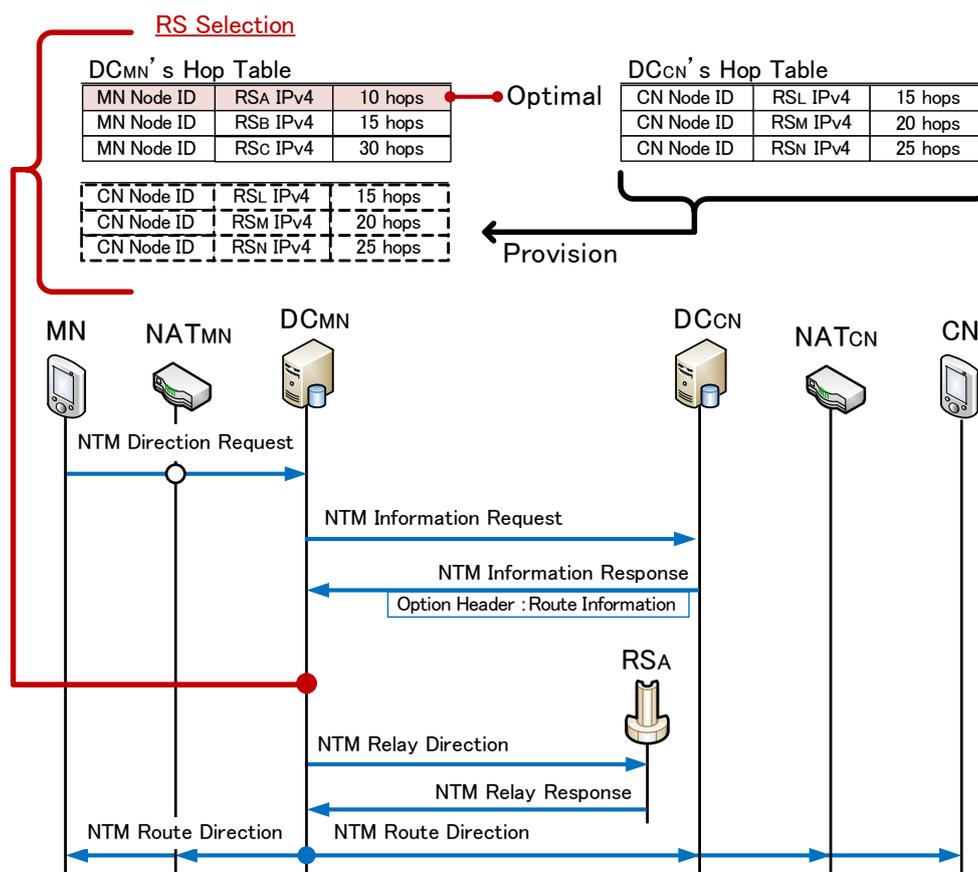


図 4.4 異なる DC に管理されている NTM 端末どうしの通信における DCMN 管理下の RS 選択

ホップ数を比較し、より NTM 端末に近い RS を最適な RS として選択する。このとき、ホップ数が同じ RS が存在した場合、MN が管理している RS を優先して利用する。

DCMN 管理下の RSA が最適だと判定された場合、以降、DCMN が RSA を利用した既存のトンネル構築シーケンスを行う。

NTM 端末から RS までのホップ数が小さいものから複数のレコードを Route Information に記載する理由は、1 台の RS を複数台の DC が管理・利用する形態に対応するためである。例えば RSx, RSy, RSz, が DCMN, DCCN に管理されている場合、DCMN は Route Information によって MN から CN まで、RSx, RSy, RSz をそれぞれ経由した場合の総経路ホップ数を算出し、最適な RS を選択する。

Route Information に記載するデータ数は、Route Information を含んだ NTM Information Response のパケットサイズがネットワークの MTU (Maximum Transmission Unit) を越えないように設定するべきである。

DCCN の RS を選択する場合

図 4.5 に、異なる DC に管理されている NTM 端末どうしの通信において、DCCN 管理下の RS を選択するときのトンネル構築シーケンスを示す。DCMN の RS を選択する場合と同様に NTM Information Response まで実施し、DCCN が、最適な RS として RSL を選択したとする。

DCMN は、RSL と信頼関係を持つ DCCN に MN と CN 間のトンネル構築指示を委任する。そのため、NTM Direction Delegation という制御メッセージを新たに定義した。NTM Direction Delegation は、トンネル構築を委任するための制御メッセージである。

DCMN は、NTM Direction Delegation を DCCN に対して送信する。NTM Direction Delegation には、最適だと判定された RSL の IP アドレスを記載しておく。DCCN はトンネル構築指示の委任を受け、以降、DCCN が RSL を利用した既存のトンネル構築シーケンスを行う。

4.3.3 一般端末との通信における RS 選択

図 4.6 に、MN が GN に対して通信を開始するときのトンネル構築シーケンスを示す。MN は DCMN に対して GN までの経路指示を要求する。DCMN は GN が一般端末であることを識別すると、DCMN の Hop Table を MN の Node ID で検索し、最もホップ数が少ない RSA を最適だと選択する。そして DCMN は、RSA までのトンネル構築を MN に指示する。以上の手順を踏まえることにより、MN は自身に最も近い RS を利用して、一般端末と通信を行うことができる。

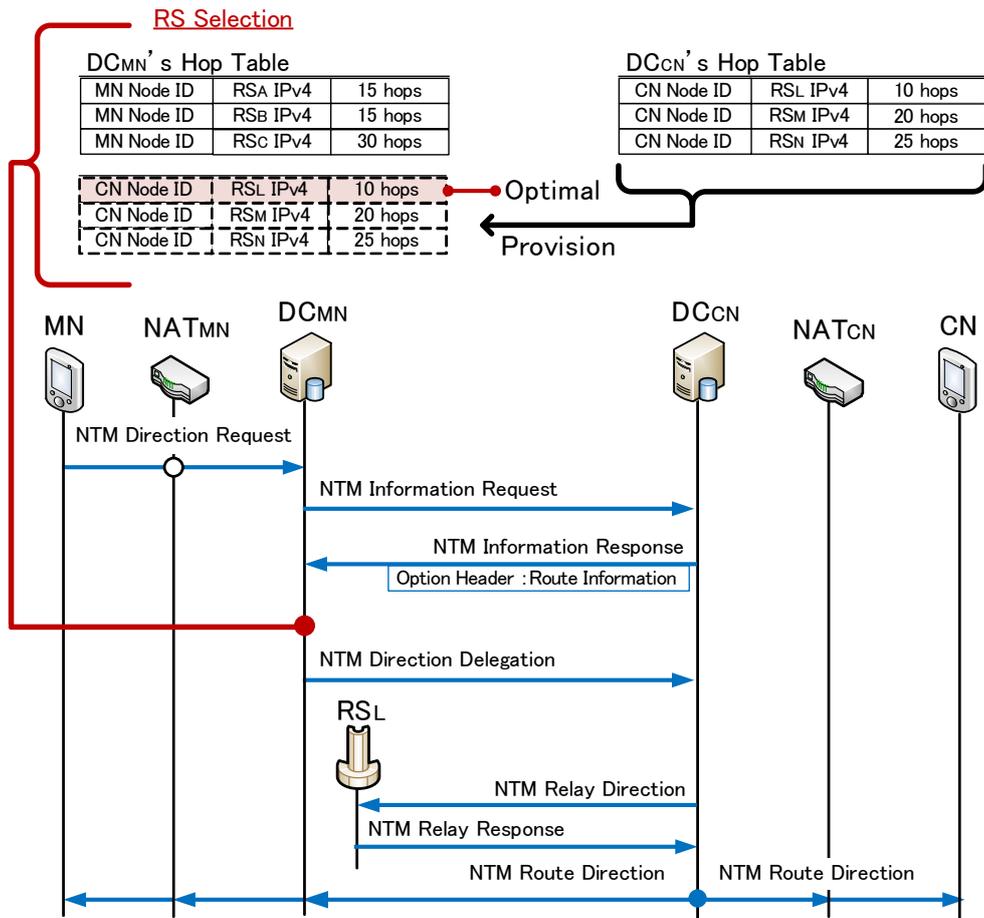


図 4.5 異なる DC に管理されている NTM 端末どうしの通信における DCCN 管理下の RS 選択

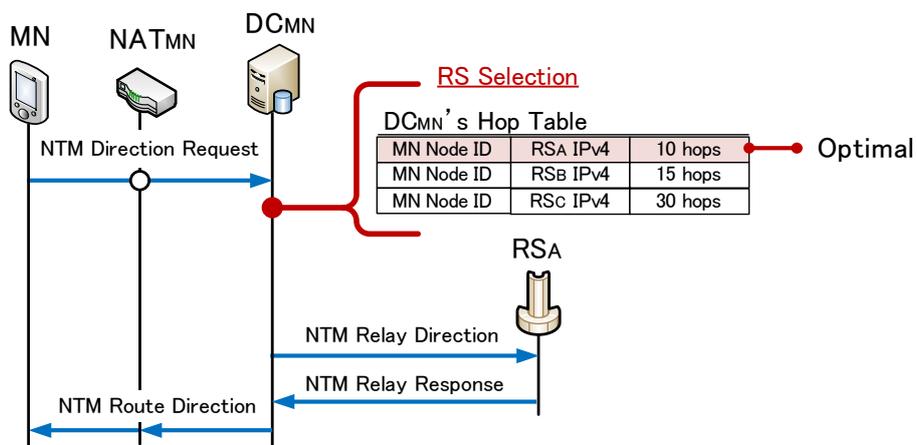


図 4.6 一般端末との通信における RS 選択

第5章 実装と評価

NTMobile は Linux 環境での実装が行われている。そこで、NTMobile のモジュールとして提案方式のプロトタイプを実装し、性能評価を行った。

5.1 モジュール構成

提案方式のプロトタイプの実装として、DC、RS、および NTM 端末に、既存モジュールの一部変更、およびプロトタイプモジュールの追加を行った。プロトタイプモジュールは IPv4 へのみ対応している。

5.1.1 DC のモジュール構成

図 5.1 に DC のモジュール構成を示す。DC はユーザ空間で動作する NTM デーモンと、DNS サーバで構成される。DNS サーバには BIND を利用している。DC の NTM デーモンには、新たにホップ数調査を行う経路調査モジュールのプロトタイプを追加実装した。NTM 端末のアドレス登録が正常に行われたとき、その NTM 端末に関するホップ数調査を開始する。動作検証のため、調査対象の RS の IP アドレスはプログラム内で静的に設定しており、

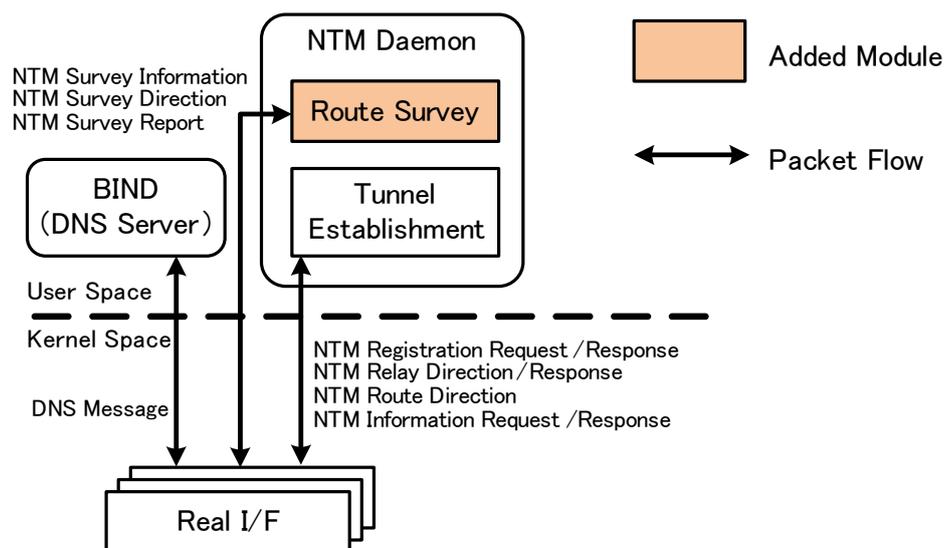


図 5.1 DC のモジュール構成

各 NTM 端末の調査毎に調査用一時鍵を生成し、各 RS と NTM 端末へ配布する。その後、RS から受信したホップ数調査結果は、NTM 端末と RS 毎に保持しておく。RS の選択処理は本来はトンネル構築モジュールにおいて、Hop Table を参照して必要な情報を取得することにより実施する予定であるが、本論文では、経路調査モジュールに組み込む形で RS 選択モジュールのプロトタイプを実装した。RS 選択モジュールのプロトタイプでは、MN および CN から各 RS までのホップ数調査の結果を基に、MN と CN の通信において経路冗長化を最も抑える RS を選択する処理を追加した。

5.1.2 RS のモジュール構成

図 5.2 に RS のモジュール構成を示す。RS は、ユーザ空間で動作する NTM デーモンと、カーネル空間で動作する NTM カーネルモジュールにより構成される。NTM デーモンにあるトンネル構築モジュールと、NTM カーネルモジュールの機能によりトンネル構築およびパケットの中継処理が行われる。RS の NTM デーモンには、新たに経路調査モジュールのプロトタイプを実装した。経路調査モジュールは、DC から送信された NTM Survey Information の情報を保持しておく。RS では NTM Route Survey を受信したとき、IP ヘッダ内の TTL を取得する必要がある。そのため RS ではデバイスレベルのパケットインタフェースである PF_PACKET を利用し、経路調査モジュールが IP ヘッダを含むパケットを受信可能とした。PF_PACKET を用いたことにより、実装範囲をユーザ空間に限定することが可能となり、プロトタイプ実装が容易となった。経路調査モジュールは、NTM Route Survey の MAC 認証を実施し、取得したホップ数を DC へ報告する。

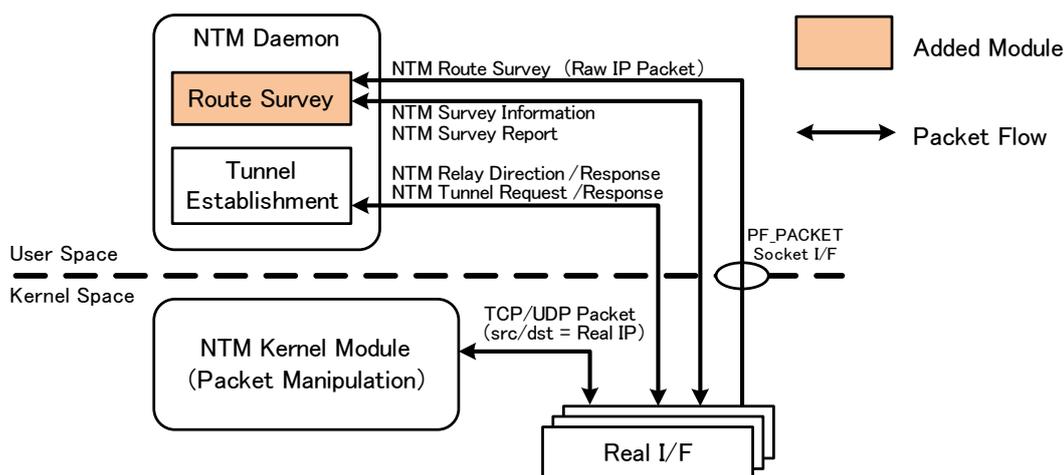


図 5.2 RS のモジュール構成

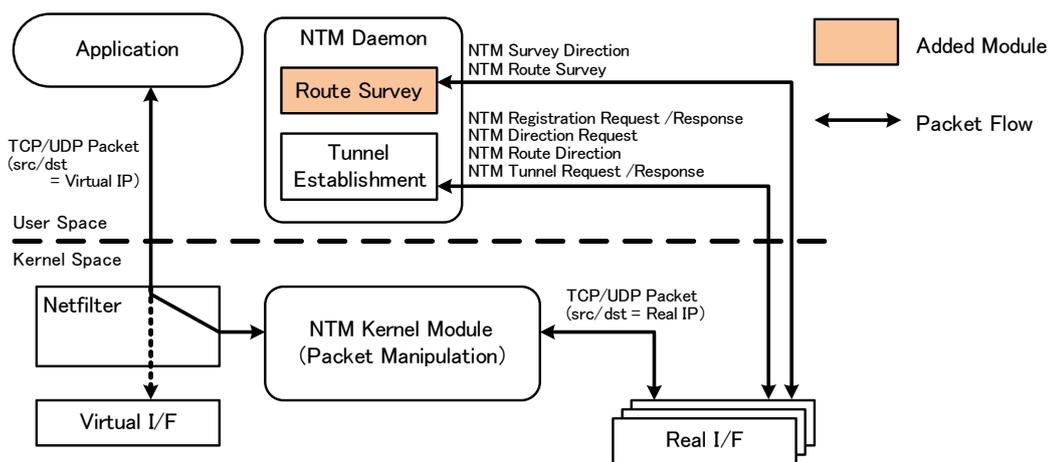


図 5.3 NTM 端末のモジュール構成

5.1.3 NTM 端末のモジュール構成

図 5.3 に NTM 端末のモジュール構成を示す。NTM 端末は、ユーザ空間で動作する NTM デーモンと、カーネル空間で動作する NTM カーネルモジュールにより構成される。NTM デーモンは DC に対するアドレス情報の登録や仮想 IP アドレスの取得、およびトンネル構築を行う。NTM カーネルモジュールは、NTM 端末が送受信するパケットのカプセル化/デカプセル化および暗号化処理を行う。NTM デーモンに、新たに経路調査モジュールのプロトタイプを実装した。経路調査モジュールは、NTM 端末の TTL 初期値を取得し、複数 RS までのホップ数調査を MAC 認証機構を利用して行う処理を追加した。

5.2 動作検証

ホスト PC 上に、VMware Player 6.0.1^{*3} を利用し、3 台の RS (RSA, RS_B, RS_C)、MN と CN、および 3 台のルータを構築し、動作検証を行った。表 5.1 にホスト PC の構成を、表 5.2 に各仮想マシンの構成を示す。

図 5.4 に、動作検証を行ったネットワークの構成を示す。IPv4 ネットワークにおいて、通信を行う MN と CN が NAT 配下に存在し、RSA が MN と CN の間において最も適切な RS である環境を想定した。そのため MN と CN は、VMware Player の機能により構成された NAT ルータ配下に接続した。また、DC および RSA はプライベートネットワークに直接接続し、RS_B は 1 つのルータを挟み、RS_C は 2 つのルータを挟んで接続した。ルータには IP フォワーディングを設定し、各装置には RS_B, RS_C までの経路情報を登録し、接続性を確保した。

^{*3}<http://www.vmware.com/jp>

表 5.1 ホスト PC の構成

	構成
OS	Windows 7 64 bit
CPU	Intel Core i7 870 @2.93 GHz
メモリ	8 GB

表 5.2 仮想 PC の構成

	DC, RSA, RS _B , RS _C , MN, CN	Router
OS	Ubuntu 10.04 32 bit	Ubuntu 10.04 32 bit
Kernel Version	2.6.32-24-generic	2.6.32-24-generic
CPU 割り当て	各 1 Core	各 1 Core
メモリ割り当て	各 1 GB	各 512 MB

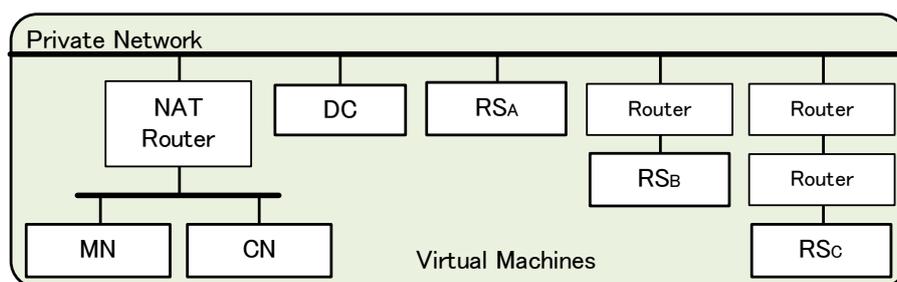


図 5.4 試験ネットワーク構成

DC および 3 台の RS を立ち上げた後、MN と CN を起動した。MN と CN からのホップ数調査が完了したことを確認した後、MN から CN までの到達性と通信経路の確認のため、MN から CN に対して ping を実行した。MN と CN の間において適切な RS として、DC は RSA を選択し、ping は RSA を経由して送受信された。以上により、ホップ数調査および RS の選択処理が正常に動作したことを確認した。

5.3 ホップ数調査の性能評価

図 5.5 に、図 5.4 に示した環境において実行されたホップ数調査の調査時間を、DC の仮想マシン内で Wireshark^{*4} により取得した結果を示す。表 5.3 に各装置間の RTT を示す。

図 5.5 は、NTM 端末が NTM Registration Response を受信し、NTM 端末のアドレス登録処理が正常に終了した時点からの様子を示している。動作検証は仮想環境内で実施している

^{*4}<http://www.wireshark.org/>

ため、装置間の RTT の平均は 2 ms 未満となっている。

RSA に対する NTM Survey Information は、アドレス登録終了後から 4.93 ms 後に送信された。続く RSB, RSc に対する NTM Survey Information, および NTM 端末に対する NTM Survey Direction では 0.60 ms 程度の遅延しか生じていないことから、ホップ数調査開始における DC でのホップ数調査用スレッドの生成処理および Survey Temp Key を生成する処理による遅延が発生していると考えられる。

NTM 端末は NTM Survey Direction を受信してから、RSA に対して NTM Route Survey を送信するまで 8.43 ms 経過している。理由としては、NTM 端末におけるホップ数調査用スレッドの生成による遅延、および DC~NTM 端末間での 2 回の NAT 処理により、DC でのパケットのキャプチャ間隔が拡大したとみられる。ただし、NTM Route Survey の送信間隔は比較的短いことから、Survey Temp Key による MAC 付加による処理遅延はほぼ発生しないことが分かる。

RSA, RSB, RSc が NTM Route Survey を受信してから DC に NTM Survey Report を送信するまで、それぞれ 3.76 ms, 5.17 ms, 8.22 ms 経過している。この遅延には、RS におけるホップ数調査用スレッドの生成時間、NTM Route Survey の MAC 認証およびホップ数の計算処理時間が含まれる。また NTM 端末から各 RS までの経路に存在するルータの個数が多い

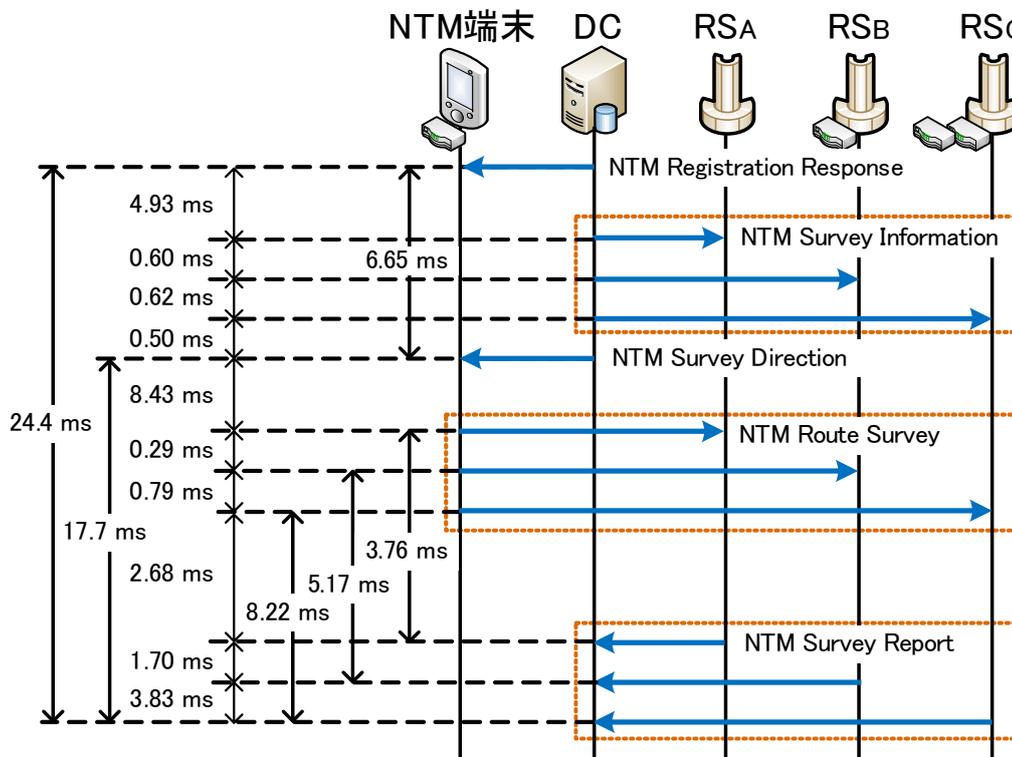


図 5.5 ホップ数調査時間の内訳

表 5.3 装置間の RTT

	RTT [ms]		
	min	avg.	max
DC-RSA	0.097	0.330	2.305
DC-RSB	0.188	0.610	1.398
DC-RSc	0.256	0.920	2.435
DC-MN	0.332	0.910	1.842
MN-RSA	0.285	0.939	2.185
MN-RSB	0.289	1.192	6.686
MN-RSc	0.463	1.551	8.824

くなるにつれて遅延時間が増加しているため、パケットがルータを経由することによる処理遅延の影響が存在することが見て取れる。

この環境において、ホップ数調査は総計 24.4 ms で正常に終了した。また DC が NTM 端末に調査指示を出してから、17.7 ms で完了することが確認できた。

実環境での調査時間の検討のため DC, 各 RS, および NTM 端末が日本国内に存在し、NTM 端末が 3G ネットワークに接続している環境を想定する。日本国内のグローバルネットワークにおいて発生する RTT を約 20 ms, 日本国内の 3G ネットワークでの RTT を約 120 ms と仮定すると、NTM Survey Direction, および NTM Survey Report の各送信時に 60 ms 程度、NTM Route Survey の送信時に 10 ms 程度の一方向の伝送遅延が発生する。実環境では NTM Survey Information の送信においても伝送遅延が発生するが、DC および RS はグローバルネットワーク上に有線で接続され、かつ NTM 端末は無線接続が主となると予想されるため、NTM Survey Direction および NTM Route Survey が NTM Survey Information を追い抜き、先に RS へ到達する状況は発生し難い。そして、NTM Survey Information と NTM Survey Direction は連続的に送信されるため、NTM Survey Information の伝送遅延はほぼ無視できる。よってホップ数調査は、NTM 端末が移動を行ってから 3 台の RS に対するホップ調査を完了するまで、おおよそ 154.4 ms 後に完了すると推測できる。

NTM 端末によるホップ数調査が完了していない場合であっても、DC による RS 選択処理は RS の負荷情報のみを用いて行うことができるため、ホップ数調査が通信開始時のオーバーヘッドとなることはない。

文献 [6] における通信断絶時間の調査によると、NTM 端末が接続するネットワークの切替えおよび IP アドレスの取得処理に 4.01~5.41 s 要している。NTM 端末が移動先のネットワークにおいて最適な RS を利用できることが求められる中、ネットワーク切替えからホップ数調査完了までにおけるホップ数調査時間は全体の 4% に満たないため、実用上問題ないと言える。

第6章 関連研究との比較

提案方式を取り入れた NTMobile と、MIPv4, MIPv6, DSMIPv6 を、IP ネットワークの構成毎に中継装置および通信経路に着目して比較した。

6.1 IPv4 ネットワークにおける比較

表 6.1 に、IPv4 ネットワークにおいて動作可能な、MIPv4, DSMIPv6, NTMobile について比較した結果を示す。

6.1.1 MIPv4

MIPv4 では HA を経由した通信を行う、実際の通信ではイングレスフィルタリングを考慮することが現実的であるため、冗長なドッグレグ経路で通信することとなる。HA を広く分散配置することは、設置個所がホームネットワーク内に限定されていることから困難である。動的 HA 発見手法は端末の起動時に実施され、HA の IP アドレスを取得する仕組みであるが、端末に割り当てる HA を評価し選択する具体的な手法が定められていない。また、端末は HoA に依存した通信を行っているため、端末がネットワークを移動したとしても、1 つの HA を利用し続ける必要がある。そのため MIPv4 のシステムは、HA の一点障害に脆弱である。NAT 配下に存在する端末は、HA との間にはのみ UDP トンネルを構築可能であり、通信端末間の経路最適化は定義されていない。よって、MIPv4 における通信経路の冗長化は避けられない。

表 6.1 IPv4 ネットワークにおける提案方式と関連研究の比較

比較項目	MIPv4	DSMIPv6	NTMobile
中継装置の分散配置	×	×	○
端末起動時の中継装置選択	△	×	○
端末移動後の中継装置再選択	×	×	○
通信毎の中継装置選択	×	×	○
中継装置の耐障害性	△	△	○
経路最適化	×	×	△
通信経路冗長化の抑制	×	×	○

6.1.2 DSMIPv6

DSMIPv6 では MIPv4 と同様に、HA はホームネットワーク内に設置する必要がある。DSMIPv6 は、IPv4 ネットワークにおいて HA の IP アドレスを取得する方法として DNS による名前解決を用いているが、通信経路の評価や負荷分散を行う具体的な手法は検討されていない。端末は 1 台の HA を利用し続けなければならないが、経路最適化もサポートされていないため、一点障害による機能停止や、冗長な通信経路を避けることができない。

6.1.3 NTMobile

NTMobile は IPv4 ネットワーク間の通信において、両通信端末が NAT 配下にいる場合と一般端末と通信を行う場合を除き、直接通信を行うことができる。中継装置である RS は、グローバルネットワーク上に自由に分散配置可能である。端末が通信を開始するとき、DC は端末が直接通信を行えないと判別すると、提案方式により、その通信において最適な RS を選択する。このとき DC が RS の負荷情報の収集を行っていることにより、RS の負荷分散が可能である。また端末の位置に依存せず、通信相手毎に自由に RS を割り当てることができる。RS を経由した通信経路を構築した後、移動端末と通信相手端末が自律的経路最適化を実施することにより、直接通信に切り替えることが可能である。よって NTMobile は、IPv4 ネットワークにおいても通信経路冗長化の抑制が可能である。

6.2 IPv6 ネットワークにおける比較

表 6.2 に、IPv6 ネットワークにおいて動作可能な、MIPv6、DSMIPv6、NTMobile について比較した結果を示す。

比較項目	MIPv6	DSMIPv6	NTMobile
中継装置の分散配置	△	△	○
端末起動時の中継装置選択	○	○	○
端末移動後の中継装置再選択	×	×	○
通信毎の中継装置選択	×	×	○
中継装置の耐障害性	△	△	○
経路最適化	○	○	○
通信経路冗長化の抑制	△	△	○

6.2.1 MIPv6

MIPv6では、IP エニーキャストを利用した HA の動的発見手法が規定されている。IP エニーキャストにより HA の負荷分散が可能であり、端末はネットワーク的な距離が近い HA に接続できる。しかし端末に割り当てた HA は基本的に変更できないため、端末が移動することによって経路がより冗長となることは避けられない。また、HA の一点障害により、MIPv6 の機能は利用できなくなる。耐障害性の向上のため、ホームネットワークを IP エニーキャストに対応させ、グローバルネットワーク上の広い範囲に配置することが求められる。

6.2.2 DSMIPv6

DSMIPv6 は MIPv6 を拡張した仕様であるため、IPv6 ネットワークにおいて IPv6 アプリケーションを用いる場合、MIPv6 と同様の動作が可能だと考えられる。

6.2.3 NTMobile

NTMobile は IPv6 ネットワークにおいても、IPv4 ネットワークと同様の動作を行う。IPv6 ネットワークでは NAT 環境が想定されないため、NTMobile では基本的に直接通信を行うことになる。

6.3 IPv4/IPv6 混在ネットワークにおける比較

表 6.3 に、IPv4/IPv6 混在ネットワークにおいて動作可能な、DSMIPv6、NTMobile について比較した結果を示す。

表 6.3 IPv4/IPv6 混在ネットワークにおける提案方式と関連研究の比較

比較項目	DSMIPv6	NTMobile
中継装置の分散配置	×	○
端末起動時の中継装置選択	△	○
端末移動後の中継装置再選択	×	○
通信毎の中継装置選択	×	○
中継装置の耐障害性	×	○
経路最適化	△	△
通信経路冗長化の抑制	×	○

6.3.1 DSMIPv6

DSMIPv6 は IPv4/IPv6 混在環境への対応のため、HA を IPv4/IPv6 のデュアルスタック構成とする。DSMIPv6 において、HA への端末の登録には、IPv6 ネットワークでは MIPv6 と同様に IP エニーキャストを利用する。IPv4 ネットワークでは、端末は DNS による名前解決を利用し HA に接続する。そのため HA の選択は DNS の設定によって行うこととなる。

IPv4 ネットワークに移動端末が存在する場合や、IPv4 アプリケーションを利用した通信は必ず HA を経由する。移動端末が移動先ネットワークにおいて IPv6 の IP アドレスを取得し、通信相手と IPv6 による通信を行っている場合のみ、経路最適化が可能である。

6.3.2 NTMobile

NTMobile では、中継装置である RS はデュアルスタック構成とした上で、分散配置が可能である。IPv4/IPv6 相互通信は必ず RS を経由した冗長経路を取るが、提案方式により最適な RS を選択することが可能である。

第7章 まとめ

本論文では、NTMobileにおいて中継装置を経由することにより発生する経路冗長化の課題を解決する手法について提案を行った。提案方式では、端末とネットワークの負荷を最小限に抑えた方法で、端末のカーネルや接続したネットワークの構成に関わらず、ネットワーク毎にNTM 端末からRS までのホップ数調査を行う手法を確立した。そしてNTM 端末の通信開始時には、利用可能なRS を通信開始側のDC 配下だけでなく通信相手側のDC 配下まで拡大し、端末間の通信経路のホップ数が最小となるようにRS を選択することによって、通信経路の冗長化を抑制した最適経路を構築可能とした。また提案方式のプロトタイプをNTM 端末、DC、RS に実装し、仮想環境内においてプロトタイプの動作検証を行った。その結果、IPv4 プライベートネットワークに存在する2 台のNTM 端末によるホップ数調査が正常に完了し、NTM 端末間の通信が最適なRS を経由して行われることを確認した。加えてホップ数の調査時間の性能評価の結果から、実環境において実用可能であることが確認できた。提案方式を適用したNTMobile と関連研究との比較評価を行い、IPv4、IPv6、IPv4/IPv6 混在のいずれのネットワークにおいても、提案方式は通信経路冗長化の抑制が可能であり、関連研究よりも優位にあることを示した。今後は、提案方式の実環境での有用性を検証する。

謝辞

本研究を進めるにあたり，終始丁寧かつ熱心なご指導を賜りました，指導教官である名城大学工学部情報工学科 渡邊晃教授に心から感謝致します。

本研究を進めるにあたり，様々なご指導を頂きました，名城大学工学部情報工学科 鈴木秀和助教に深く感謝致します。

本研究を進めるにあたり，ご意見並びにご助言を賜りました，三重大学大学院工学研究科 内藤克浩助教に深謝致します。

本研究を進めるにあたり，常日頃からご教示下さり，数々のご助言を賜りました，土井敏樹氏，上醉尾一真氏，清水皓平氏，金丸幸弘氏，津田一磨氏，廣瀬達也氏に心から感謝致します。また，研究に関して議論をさせて頂き，快くご助力を賜りました，早川顕太氏，上山雄輝氏に感謝致します。

最後に，本研究を進めるにあたり，多くの討論の場において有益なご意見を賜りました，渡邊研究室及び鈴木研究室の先輩方，そして同期の皆様に感謝致します。

参考文献

- [1] Perkins, C.: IP Mobility Support for IPv4, Revised, RFC 5944, IETF (2010).
- [2] Perkins, C., Johnson, D. and Arkko, J.: Mobility Support in IPv6, RFC 6275, IETF (2011).
- [3] Soliman, H.: Mobile IPv6 Support for Dual Stack Hosts and Routers, RFC 5555, IETF (2009).
- [4] 鈴木秀和, 上醉尾一真, 水谷智大, 西尾拓也, 内藤克浩, 渡邊 晃: NTMobile における通信接続性の確立手法と実装, 情報処理学会論文誌, Vol. 54, No. 1, pp. 367–379 (2013).
- [5] 内藤克浩, 上醉尾一真, 西尾拓也, 水谷智大, 鈴木秀和, 渡邊 晃, 森香津夫, 小林英雄: NTMobile における移動透過性の実現と実装, 情報処理学会論文誌, Vol. 54, No. 1, pp. 380–397 (2013).
- [6] 上醉尾一真, 鈴木秀和, 内藤克浩, 渡邊 晃: IPv4/IPv6 混在環境で移動透過性を実現する NTMobile の実装と評価, 情報処理学会論文誌, Vol. 54, No. 10, pp. 2288–2299 (2013).
- [7] 細尾幸宏, 鈴木秀和, 内藤克浩, 旭 健作, 渡邊 晃: NTMobile における DNS 実装の変更が不要なデータベース型端末情報管理手法の検討, 情報処理学会研究報告, Vol. 2012-MBL-64, No. 6, pp. 1–8 (2012).
- [8] 土井敏樹, 鈴木秀和, 内藤克浩, 渡邊 晃: NTMobile におけるアドレス変換型リレーサーバの実装と動作検証, 情報処理学会研究報告, Vol. 2013-MBL-67, No. 11, pp. 1–6 (2013).
- [9] Ferguson, P. and Senie, D.: Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, RFC 2827, IETF (2000).
- [10] Montenegro, G.: Reverse Tunneling for Mobile IP, revised, RFC 3024, IETF (2001).
- [11] Levkowitz, H. and Vaarala, S.: Mobile IP Traversal of Network Address Translation (NAT) Devices, RFC 3519, IETF (2003).
- [12] Kulkarni, M., Patel, A. and Leung, K.: Mobile IPv4 Dynamic Home Agent (HA) Assignment, RFC 4433, IETF (2006).
- [13] Abley, J. and Lindqvist, K.: Operation of Anycast Services, RFC 4786, IETF (2006).
- [14] Johnson, D. and Deering, S.: Reserved IPv6 Subnet Anycast Addresses, RFC 2526, IETF (1999).
- [15] Hardie, T.: Distributing Authoritative Name Servers via Shared Unicast Addresses, RFC 3258, IETF (2002).

- [16] 井貝友哉, 土井敏樹, 上醉尾一真, 鈴木秀和, 内藤克浩, 渡邊 晃: NTMobile における RS-N の二重化と状態管理手法の検討, 平成 25 年度電気関係学会東海支部連合大会論文集 (2013).
- [17] 納堂博史, 鈴木秀和, 内藤克浩, 渡邊 晃: NTMobile における自律的経路最適化の提案, 情報処理学会論文誌, Vol. 54, No. 1, pp. 394–403 (2013).
- [18] 藤川雅朗, 加藤雅浩, 根本浩之, 阿蘇和人, 久保田浩, 齊藤栄太郎, 中沢 智, 堀内かほり, 田村奈央 (編): 日経 NET | WORK 2008 年 7 月号, 日経 BP 社 (2008).
- [19] CAIDA: Archipelago Monitor Statistics, <http://www.caida.org/projects/ark/statistics/> (2014 年 2 月 7 日アクセス).
- [20] CAIDA: Med RTT per Hop, http://www.caida.org/projects/ark/statistics/nrt2-jp/med_rtt_per_hop.csv (2014 年 2 月 7 日アクセス).

研究業績

研究会・大会等

1. 若杉 純, 土井敏樹, 鈴木秀和, 内藤克浩, 渡邊 晃, “NTMobile における最適な RS 選択手法の検討”, 平成 25 年度電気関係学会東海支部連合大会論文集, 2013.
2. 若杉 純, 土井敏樹, 鈴木秀和, 内藤克浩, 渡邊 晃, “NTMobile における通信経路冗長化を抑制するリレーサーバ選択手法の提案”, 情報処理学会第 76 回全国大会講演論文集, 2014.

付録A RTTとホップ数の関係

図 A.1 に、CAIDA が公開しているデータ [19,20] を基に作成した、plala NTT broadband^{*5} における RTT とホップ数の関係を示す。ホップ数が増加すると共に、RTT の中央値と上側四分位数、下側四分位数が共に上昇していくことが分かる。

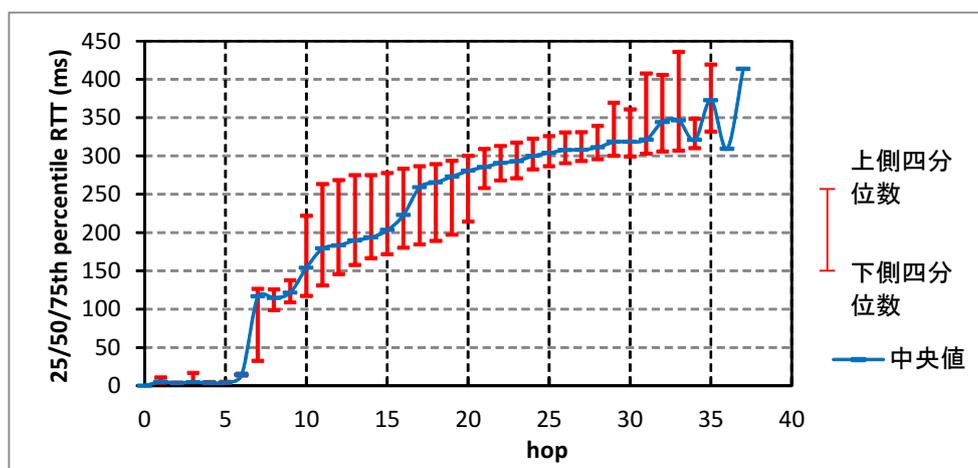


図 A.1 RTT 四分位数とホップ数の関係

^{*5}<http://www.plala.or.jp/>

付録B メッセージフォーマット

図 B.1 に、NTMobile のメッセージに付加される NTM ヘッダとヘッダオプションのフォーマットを示す。

図 B.2, 図 B.3, 図 B.4 に、4 章において新たに提案したメッセージのフォーマットを示す。提案メッセージは NTM Route Survey を除き、共通鍵により暗号化される。また、すべてのメッセージには MAC が付加される。

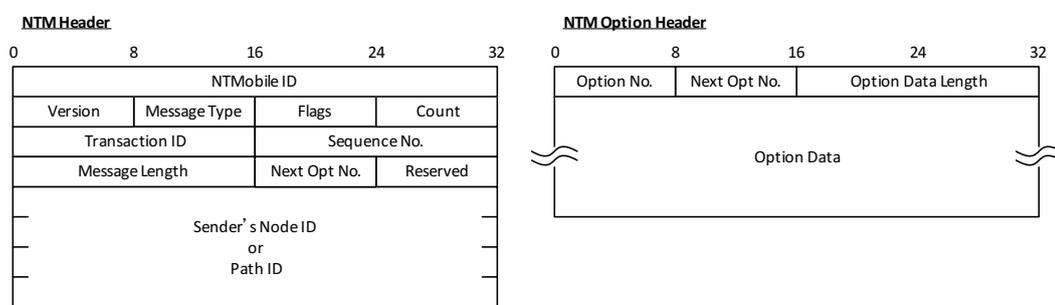


図 B.1 NTM ヘッダとヘッダオプション

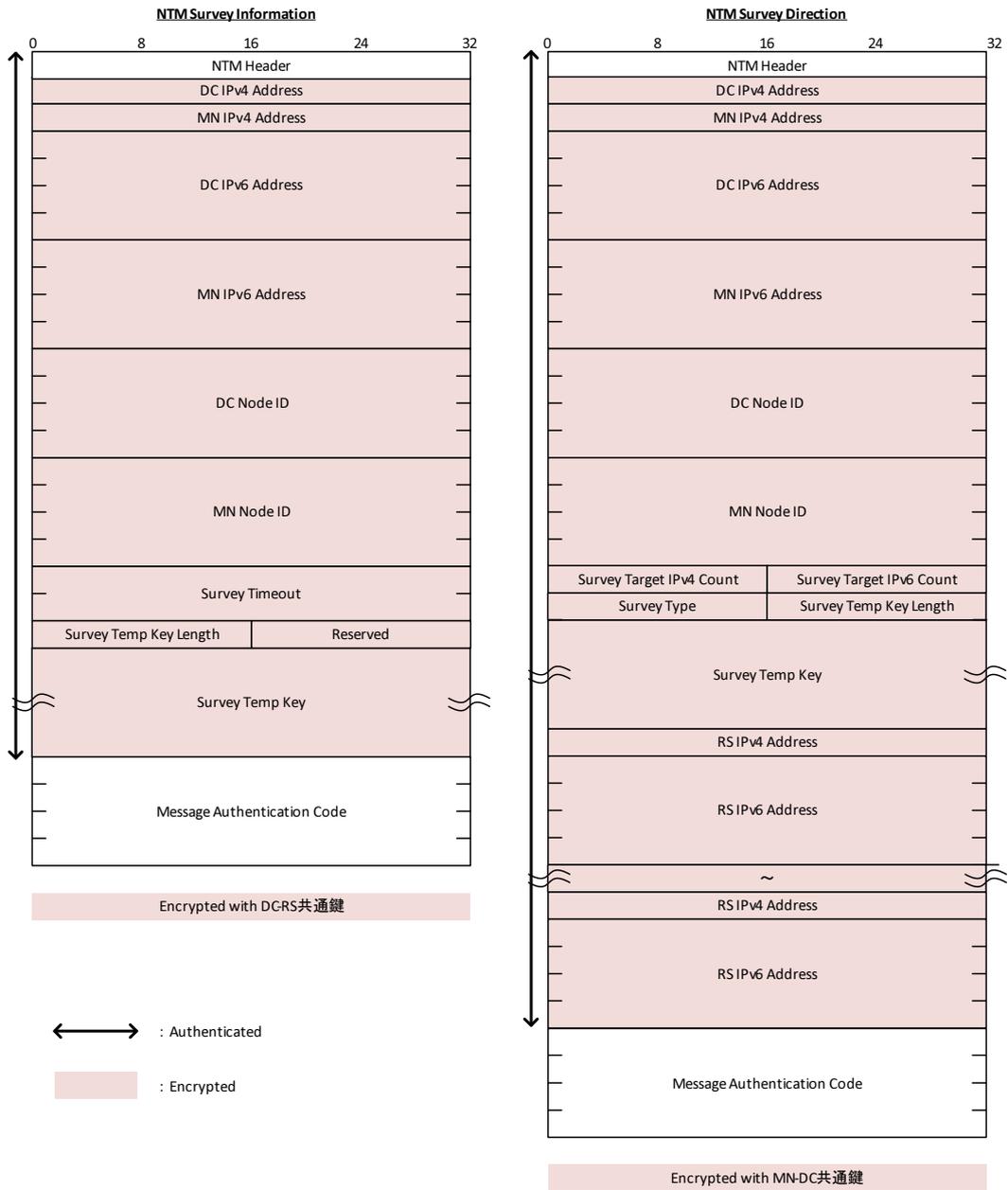


図 B.2 提案メッセージフォーマット 1

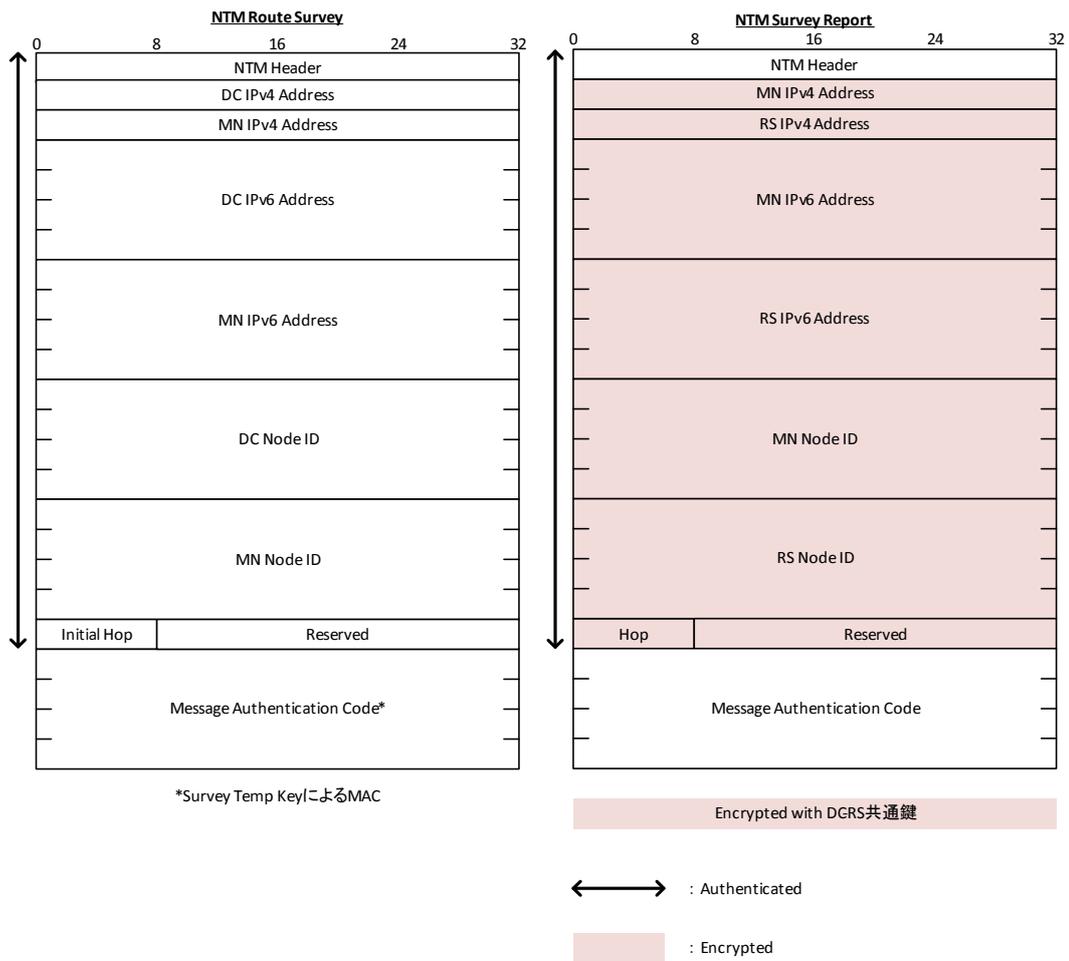


図 B.3 提案メッセージフォーマット 2

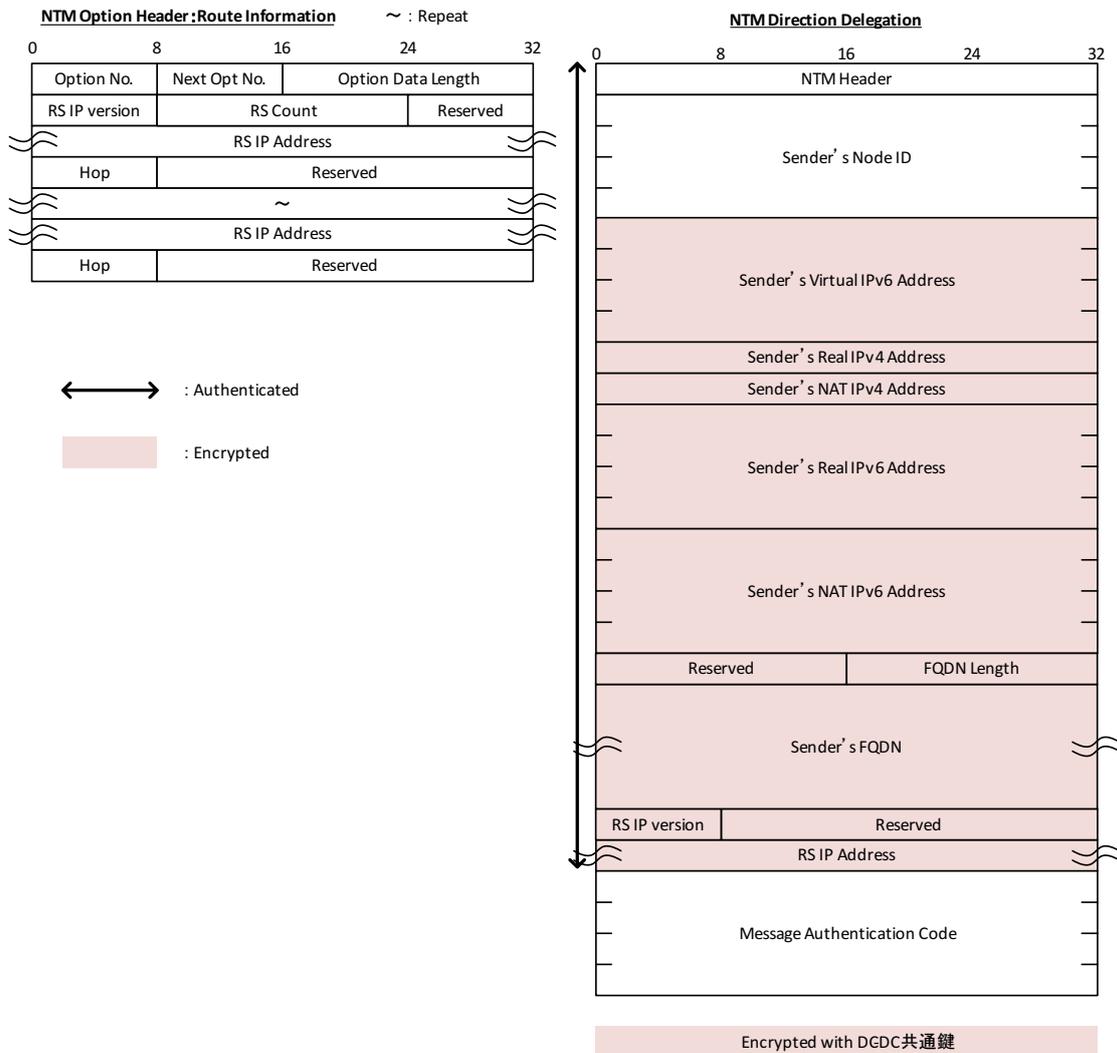


図 B.4 提案メッセージフォーマット 3

付録C インターネットの構造

インターネットは ISP (Internet Services Provider) がネットワークの相互接続を行うことにより成り立っている。インターネットを全世界に広げるためには、物理的にネットワークを世界中に張り巡らせる必要がある。そのため、1つの ISP が大規模なネットワークを構築することは難しい。いくつもの ISP が独自のネットワークを地域に構築し、ISP 同士が接続し合うことによりネットワークの規模を拡大させている。

端末が IP パケットを送信すると、インターネットを経由して目的のネットワークまで到達する。これは IP ネットワークを接続しているルータが、目的のネットワークの位置情報を示す経路情報をもとに、経路制御を行うことによって実現している。ISP 間でルータの経路情報を共有することにより、世界のどのネットワークにもパケットを伝送することができる経路情報（フルルート）が作られる。このフルルートを作る ISP は Tier1 と呼ばれ、世界に約 10 社存在する。

C.1 ISP のネットワーク

経路制御の方針が統一されたネットワークを AS (Autonomous System, 自律システム) と呼び、AS 毎に一意的な AS 番号が与えられている。IP アドレスが住所における番地だとすると、AS 番号は郵便番号に例えられる。AS 番号は各国の NIC (Network Information Center) によって管理・発行されており、日本は JPNIC の管轄となっている。

AS 番号は 0~65,535 という 2 バイトの数値を取っていたが、AS 番号の枯渇問題が発生したため、4 バイトの AS 番号の利用も始まった。4 バイト AS 番号は、2 バイト毎にピリオドで区切って表記される。4 バイト AS 番号の空間は 0.0~65,535.65,535(10 進数では 0~4,294,967,295) であり、約 43 億個分の空間がある。

C.2 AS の接続形態

AS の接続形態には、大きく分けてトランジット (Transit) とピアリング (Peering) がある。トランジットは、Tier1 に接続して自 AS の経路情報を渡しつつ、フルルートを手に入れることにより上位の ISP にトラフィックを運んでもらう形態である。トランジットにより、上位 AS を介して自 AS 配下の端末からインターネットへ接続できるようになり、また

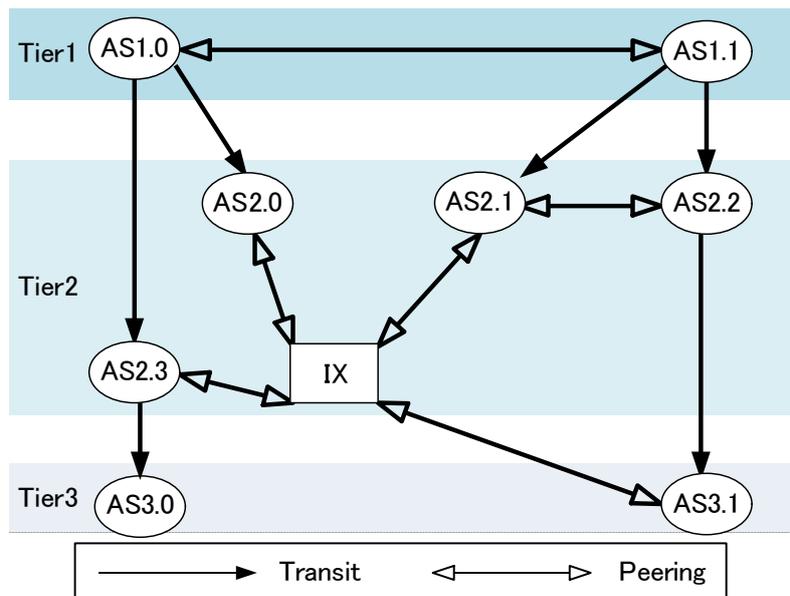


図 C.1 AS の接続

インターネット側から自ネットワークへトラフィックが流れるようになる。契約により、下位 ISP は上位 ISP に対してトランジット料を支払うことが一般的である。

図 C.1 に AS の接続を示す。Tier1 とトランジット接続した ISP は Tier2 と呼ばれ、その下にトランジット接続した ISP は Tier3 と呼ばれる。ISP はトランジットによる階層構造を成している。

トランジット接続のみをした異なる下位 AS 間で通信を行うと、トラフィックが常に上位 AS を介して流れることになる。AS 間のトラフィックを直接やり取りするために、自 AS の経路情報のみを交換し合う接続形態をピアリングと呼ぶ。ピアリングにおいて両 ISP は対等の関係にあるため、一般的に料金は発生しない。

Tier1 どうしの接続もピアリングである。ただし Tier1 のピアリングでは、Tier1 配下の AS から送られて来る経路情報も共有する。こうして全てのネットワークに接続できるフルルートが作られる。

ISP 間でピアリングを行う場合、ISP 毎のネットワーク設備の初期投資、運用・管理コストが必要となり、交渉に労力がかかる。このようなコストを削減し、より効率的にピアリングする場を提供する IX (Internet eXchange, インターネット相互接続点) がある。IX では複数の AS が物理的に接続される。ISP はピアリング交渉を行い、設定を行うことにより、IX を利用したピアリングが可能になる。ISP は IX を利用することにより、ピアリングにおいて IX に対し 1 つの接続点を持つだけで良い。