RL-002

インバウンド接続に適用可能な NAT によるマルチホーム化手法

NAT-based Multihoming Method Applicable to Inbound Connection

山口 拓哉 † 金 勇 † 岡山 聖彦 ‡
Takuya Yamaguchi Yong Jin Kiyohiko Okayama
山井 成良 ‡ 中村 素典 §
Nariyoshi Yamai Motonori Nakamura

1. はじめに

近年，インターネットは社会的な情報基盤として広く利用され，WWW（World Wide Web），電子メールのようなサービスを単に提供するだけでなく，これらを高速かつ安定的に提供することが重要視されるようになってきている．このような要求に対処する一つの方法として，自組織ネットワークを複数のバックボーンネットワーク（以下，単にバックボーンと呼ぶ）と接続し，通信先や途中のネットワークの状態に応じて利用するバックボーンを使い分けることにより通信速度や耐障害性の向上を図るマルチホームネットワークが注目されている．

マルチホームネットワークの構成方法として，AS（Autonomous System）番号取得による方法 [1]，アプリケーションゲートウェイ（Application Level Gateway，以下 ALG）による方法 [2]，ネットワークアドレス変換（Network Address Translation，以下 NAT[3]）による方法 [4][5] などが挙げられる．このうち，NAT を利用する方法は他の方法と比較して，導入コストや運用コストが比較的小さい，利用可能な通信プロトコルの制約が少ない，などの利点がある点で優れている．

ところが，この方法では組織外から接続される通信（以下，インバウンド接続）において，復路すなわち組織内から組織外への経路が往路と一致せずに通信不能になるなどの問題があるため，インバウンド通信への適用が困難であった．

そこで本研究では NAT を利用しながらインバウンド接続についても適用可能なマルチホーム化手法を提案する．この手法では NAT ルータにおいてソースルーティング用 IP オプションの一つである LSRR（Loose Source Routing and Recording）オプションを付加することにより往復の経路の一致を可能にする．これにより NAT を用いたマルチホーム化方法の利点を活かしながら，インバウンド接続についてもマルチホームネットワークの利点を享受することが可能になる．

以下，まず 2 章では従来のマルチホーム化方法とその問題点について述べる．次に 3 章では NAT を利用したマルチホーム化手法の問題点を詳述し，またその解決手法を提案する．4 章では提案手法の評価及び考察を行う．最後に，5 章では結論と今後の課題について述べる．

†岡山大学大学院自然科学研究科, Graduate School of Natural Science and Technology, Okayama University
‡岡山大学情報統括センター, Center for Information Technology and Management, Okayama University
§国立情報学研究所, National Institute of Informatics

2. 従来のマルチホーム化方法とその問題点

マルチホームネットワークの構成方法としては，1 章で述べたように，AS 番号取得による方法（方法 1），ALG による方法（方法 2），NAT による方法（方法 3）が挙げられる．以下ではこれらの方法とその問題点について述べる．

2.1 AS 番号取得によるマルチホーム化

現在，インターネットではネットワーク全体を AS と呼ばれる部分ネットワークの集合として扱い，AS 間で BGP4(Border Gateway Protocol version 4)[6] を用いて経路情報をの交換を行う方法が一般的に用いられている．方法 1 は自組織のネットワークを AS として扱ってその識別番号（AS 番号）を取得し，各バックボーンとの間で経路情報を交換して経路制御を行う方法である．この方法は組織内ネットワークとインターネットとの通信はネットワーク層レベルで冗長化でき，組織内外のホストには一切変更を加える必要がないという利点を持つ．しかし，現状では BGP4 の運用が必須であり，これに関して次のような問題がある．

- BGP4 の運用には高い技術レベルと管理・運用コストが必要になるため，BGP4 による経路制御機能を提供していない ISP（Internet Service Provider）が多数存在する．また，同機能を提供している ISP を利用したとしても金銭的なコストが大きい．
- 経路制御が宛先アドレスにのみ依存して行われ，現在の通信量などバックボーンの利用状況が反映されないため，通信先に偏りがあった場合に特定のバックボーンにトラフィックが集中する可能性がある．

2.2 ALG によるマルチホーム化

方法 2 は，電子メールや WWW などの一部のアプリケーションにおいて，各バックボーンに属するアドレスを持つ ALG を導入し，これらの ALG を経由して組織内と組織外との間で通信することによりマルチホームネットワークを実現する方法である．この方法では，組織内から組織外へ接続される通信（アウトバウンド接続）については ALG が経路選択機能*を持つことにより適切なバックボーンを選択することが可能になる．また，インバウンド接続については，たとえば組織内サーバに関する DNS 問合せに対して適切な ALG の IP アドレスを応答する手法 [7][8] などにより適切なバッ

*通常の hop-by-hop の経路ではなく，end-to-end の経路を選択する機能であるため，本論文では経路選択と呼ぶことにする．

クボーンを選択させることが可能である．したがって，方法 1 の欠点である，管理・運用コストの問題は比較的低減され，また経路選択機能の工夫により効果的なトラフィック分散を行うことも可能である．

一方，この方法では次のような問題がある．

- 適用可能なアプリケーションが WWW, 電子メールなど ALG に対応した一部のものに限られる．一般に 1 台の ALG を経由して複数の相手と通信を行う場合があるため，たとえば電子メールにおける宛先メールアドレスと中継先メールサーバとの関係のように，最終的な通信先と経由する ALG とを個別に指定できるプロトコルしか利用できない．
- 特にインバウンド接続に適用する場合，組織内のサーバでは ALG がクライアントであると見なされ，実際のクライアントの情報の一部（IP アドレスなど）が失われる．その結果，たとえば IP アドレスに基づくアクセス制御に影響を及ぼす，あるいはサーバではクライアントの正しいアクセスログを記録できないなどの制約が生じる．

2.3 NAT によるマルチホーム化

方法 3 は，各バックボーンから個別の IP アドレスの割当てを受け，組織外と組織内との通信の際に NAT を用いて組織内の IP アドレスとバックボーンから割り当てられたアドレスとを相互変換することによりマルチホームネットワークを構成する方法である [4][5]．この方法では方法 2 と同様に管理・運用コストを方法 1 と比べて軽減することが可能になるだけでなく，適用可能なプロトコルの制約も方法 2 と比べて少ないため，広範囲に適用可能である．その意味で，この方法は他の方法より優れているといえる．

しかし，特にインバウンド接続に対しては，方法 1, 2 と比較して問題がある．すなわち，組織外から組織内への往路のパケットにはどちらのバックボーンを経由したかを示す情報が含まれていないため，組織内から組織外への復路のパケットをどちらのバックボーンに中継すればよいか判断が困難である．この問題の詳細については次章で述べる．

3. インバウンド接続に適用可能な NAT によるマルチホーム化

前章で述べたように，既存のマルチホーム化方法にはいずれも問題がある．そこで，本章ではこれらのうち最も適用範囲が広い方法 3 に基づき，これをインバウンド接続にも適用できるように拡張する手法を提案する．

3.1 対象となるシステム構成

対象とするマルチホームネットワークの典型的な構成例を図 1 に示す．この図では，組織内ネットワークは ISP A とは普通のルータ（図中の R）を介してインターネットに接続され，組織内ネットワークでは ISP A から割り当てられたグローバル IP アドレスが使用される．また，ISP B とは NAT 機能を持つルータ（図中の NAT．以下，NAT ルータ）を介して接続され，ISP

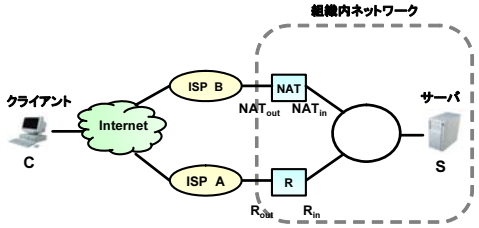

図 1: マルチホームネットワーク構成例

B から割り当てられたアドレスと組織内ネットワークで用いられるアドレスを相互変換する役割を果たす．ルータと NAT ルータは物理的に離れた場所に設置されていても構わない．

この構成において，組織内ネットワークではプライベート IP アドレスを用いてもよい．その場合，ISP A との接続にも NAT ルータが用いられ，また組織内ネットワークにおける組織外へのデフォルト経路は ISP A 経由になっているものとする．また，組織内ネットワークに設置されているホスト（図中のサーバなど）の管理者は組織内ネットワークの管理者とは必ずしも一致するとは限らないものとする．

このようなネットワーク構成は中小規模の組織では比較的よく見られるか，あるいは容易に採用できると思われる．

3.2 インバウンド接続における問題点

本論文ではこれ以降図 1 において，インターネットに接続されているクライアントから組織内ネットワークに接続されているサーバへの TCP インバウンド接続に対する経路選択について議論する．なお，UDP インバウンド接続については 4.3 節において考察する．

同図における経路選択機能は，方法 2 の場合には比較的容易に実現できる．すなわち，図 1 の NAT ルータの代わりに ALG を設置し，クライアントからサーバへのアクセスに先だって行われる DNS による名前解決において，サーバあるいは ALG のグローバル IP アドレスのうち適切なほうを応答する方法 [7][8] を適用すればよい．

方法 3 の場合においても，基本的には方法 2 と同様の手法を適用することが考えられる．この手法では，NAT ルータに対して ISP B から割り当てられているグローバル IP アドレスのうちの一つ（以下，$\mathrm{IP}_{\mathrm{NATout}}$）をサーバ用として選び，$\mathrm{IP}_{\mathrm{NATout}}$ とサーバのグローバル IP アドレス（以下，IP_{S}）とを 1 対 1 で相互変換するように予め NAT ルータを設定する．これにより，事前の名前解決において IP_{S} あるいは $\mathrm{IP}_{\mathrm{NATout}}$ のうちの適切なほうを組織内ネットワーク側の DNS サーバが応答すれば，往路については応答に応じて ISP A あるいは ISP B を経由させることができる．

しかし，この手法では復路についてはうまく経路選択を行うことができない．その場合の往復のパケットの流れを図 2 に示す．

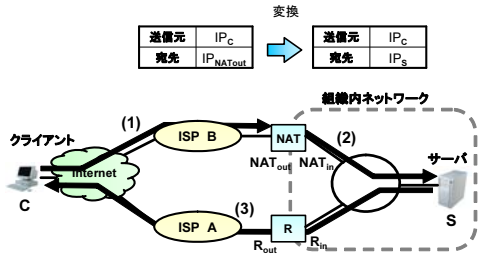

図 2: NAT 利用時のパケットの流れ（往復経路不一致例）

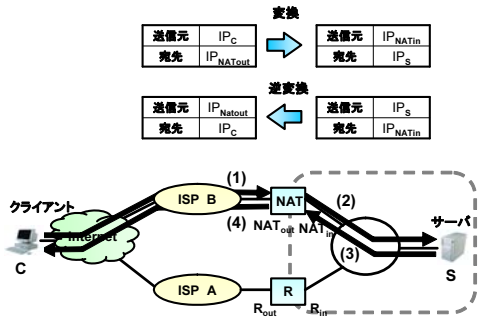

図 3: NAT 利用時のパケットの流れ（クライアント情報損失例）

同図において往路の経路として ISP B が選択された場合，クライアントの IP アドレスを IP_C とすると，クライアントからサーバへのパケットは送信元アドレスが IP_C，宛先アドレスが IP_{NATout} として NAT ルータに送られる（同図 (1)）．NAT ルータでは IP_{NATout} と IP_S との間で相互変換が行われるため，クライアントから受信したパケットは宛先アドレスが IP_S に変換され，サーバに中継される（同図 (2)）．このとき，送信元アドレスは IP_C のままであることに注意する．サーバでは応答として送信元アドレスが IP_S，宛先アドレスが IP_C であるパケットをクライアントに送信する．ところが，組織内ネットワークではインターネットへのデフォルト経路は ISP A 経由であるため，このパケットは NAT ルータを経由せずにクライアントに配送される（同図 (3)）．その結果，クライアントでは送信したパケットの宛先 IP_{NATout} とは異なる送信元 IP_S からパケットを受信することになり，クライアント・サーバ間で正しく通信が行われない．

一方，この問題に対して NAT ルータでクライアントのアドレスも変換する手法が考えられる．この手法では IP_{NATout} と IP_S との相互変換だけでなく，IP_C と NAT ルータの組織内ネットワーク側アドレス（以下，IP_{NATin}）との相互変換も行うようにする．その場合の往復のパケットの流れを図 3 に示す．

同図において往路の経路として ISP B が選択された場合，クライアントからサーバへのパケットは同様に送信元アドレスが IP_C，宛先アドレスが IP_{NATout} として NAT ルータに送られる（同図 (1)）．NAT ルータでは IP_{NATout} と IP_S との間および IP_C と IP_{NATin} との間で相互変換が行われるため，クライアントから受信したパケットは送信元アドレスが IP_{NATin}，宛先アドレスが IP_S に変換され，サーバに中継される（同図 (2)）．サーバでは応答として送信元アドレスが IP_S，宛先アドレスが IP_{NATin} であるパケットを送信する（同図 (3)）．このパケットは宛先である NAT ルータが受け取り，送信元アドレスが IP_{NATout}，宛先アドレスが IP_C に変換した後にクライアントに配送される（同図 (4)）．その結果，前例とは異なり，クライアント・サーバ間の通信自体は正しく行われる．

しかし，この手法では方法 2 と同様の問題が新たに生じる．すなわち，サーバではクライアントの IP アドレス情報が失われるため，アクセスログの記録やアクセス制御などに制約が生じる．

3.3 インバウンド接続における復路の経路選択

前節で述べた問題点の本質的な原因は，復路の経路選択がフロー単位で行えない点にある．組織内ネットワークの機器のうち，NAT ルータだけがフローを識別する機能を有するため，図 1 において NAT ルータが ISP A，B の両方に接続されている場合には NAT ルータが復路の経路選択を行うことが可能であるが，そうでない場合にはクライアントの IP アドレスを維持したままフロー単位で復路の経路を指定できる機能が必要になる．

そこで，本論文では前節で述べた問題点を解決する手法として，IP オプションの一つである LSRR（Loose Source and Record Route）オプション [9] を用いる手法を提案する．提案手法を用いた場合の動作を，図 4 を用いて説明する．

同図において往路の経路として ISP B が選択された場合，クライアントからサーバへのパケットは送信元アドレスが IP_C，宛先アドレスが IP_{NATout} として NAT ルータに送られる（同図 (1)）．ここで，従来と同様に NAT ルータでは IP_{NATout} と IP_S との間で相互変換が行われるため，クライアントから受信したパケットは宛先アドレスが IP_S に変換される．さらに NAT ルータはこのパケットに対して IP_{NATin} を経由してきた直後に見えるように LSRR オプションを付加した後，サーバに中継する（同図 (2)）．我々の調査の範囲では，このオプションはフロー単位で有効であり，サーバがクライアントに対して応答パケットを送出する際にはちょうど逆の経路をたどるように LSRR オプションを付加する．したがって，サーバが送出するパケットは送信元アドレスが IP_S，(最終の）宛先アドレスが IP_C となり，さらに LSRR オプションとして IP_{NATin} を経由するように指定されることになる（同図 (3)）．NAT ルータはこのパケットを受け取ると，まず LSRR オプションを削除し（同図 (4)），さらに送信元アドレスを IP_S から IP_{NATout} に変更してクライアントに配送する（同図 (5)）．

これにより，クライアント・サーバ間の通信はフロー単位で LSRR オプション中に経由した経路（LSRR オプションが存在しない場合にはデフォルト経路）が記録され，これに従って復路の経路選択に利用されるだけ

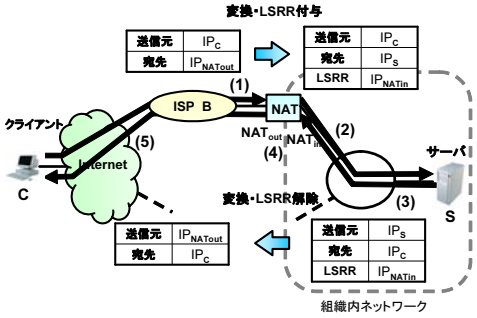

図 4: LSRR オプションによる復路の経路選択

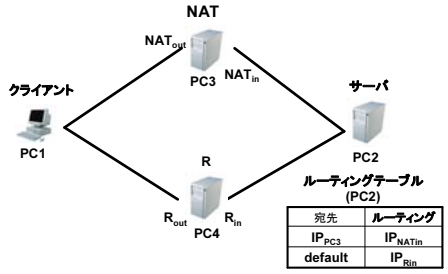

図 6: 実験環境

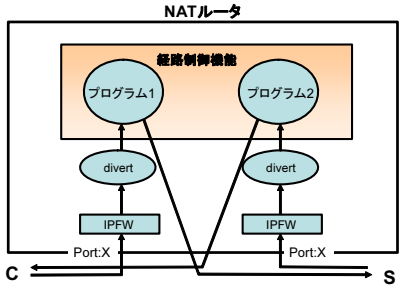

図 5: 試作 NAT ルータの構成

なく，クライアントの IP アドレスはパケット中にそのまま残されるため，これを用いてアクセス制御を行ったりアクセスログを残したりすることが可能となる．

3.4 NAT ルータの実装

前節で述べた手法に基づき，我々は LSRR オプションの付加・削除機能を持つ NAT ルータの試作を行った．本節ではその実装方法を述べる．

試作 NAT ルータは FreeBSD 7.2 上で自作プログラムとして実装した．試作 NAT ルータの構成を図 5 に示す．同図に示すように，内部には 2 つのプログラムがあり，プログラム 1 は宛先アドレスの変換と LSRR オプションの付加，プログラム 2 は送信元アドレスの変換と LSRR オプションの削除を行う．これらのプログラムへのパケットの受け渡しは，FreeBSD の IPFW(IP FireWall) 機能 [10] により divert ソケット [11] を介して行われる．

4. 試作 NAT ルータの評価と考察

本章では試作した NAT ルータの機能や性能を評価するために行った実験について述べる．また，提案手法の適用範囲について考察する．

4.1 動作確認実験

まず，試作した NAT ルータを用いてクライアント・サーバ間で正しく通信が行えるかどうかを確認するため，動作確認実験を行った．実験環境を図 6 に示す．この環境においてクライアント PC1，サーバ PC2 ともデフォルト経路はルータの役割を果たす PC4 を経由するように設定した．全ての PC には OS として FreeBSD 7.2 を用いた．また，サーバ PC2 では Web サーバプログラムとして apache[12] を動作させ，クライアント PC1 上では wget[13] を用いてサーバにアクセスさせた．

まず，クライアントからサーバを直接指定してアクセスさせたところ，正常にアクセスできた．また PC3, PC4 において tcpdump[14] を用いて各リンクのパケットを観測したところ，クライアント・サーバ間の通信は往路，復路とも PC4 を経由していることを確認した．

次に，クライアントから NAT ルータ PC3 の組織外側アドレス IP_{NATout} を指定してアクセスさせたところ，同様に正常にアクセスできた．また PC3，PC4 において各リンクのパケットを観測したところ，クライアント・サーバ間の通信は往路，復路とも PC3 を経由し，また PC3 で LSRR オプションの付加および削除が正しく行われていることを確認した．

また，いずれの実験においても PC2 において apache のアクセスログに PC1 の IP アドレスが記録されていることを確認した．

これらの結果により，LSRR オプション付加による復路の経路選択機能は有効に動作し，またサーバではいずれの経路を経由した場合でもクライアントの IP アドレスが保存されることが確認された．

4.2 性能評価実験

提案手法では NAT ルータにおいて 8 バイトの LSRR オプションの付加・削除が伴うため，通常の NAT ルータよりもオーバヘッドが大きいと予想される．そこで，試作 NAT ルータを用いた場合，通常のルータ，通常の NAT ルータと比較してどの程度のスループットが得られるかを調べるため，図 6 と同様の環境において性能評価実験を行った．また，クライアントからサーバへのパケットについては，8 バイトの LSRR オプションの付加により見かけ上の Path MTU（Maximum Transfer Unit）が 8 バイト分小さくなる．そこで，PC1 において MTU の値を通常の 1500 および 8 バイト分小さい 1492 の 2 通りに設定して Path MTU 減少によるスループット低下の影響についても調査を行った．

この実験では，図 6 における PC4 は用いず，PC3 を通常のルータ，通常の NAT ルータ，および試作 NAT ルータの 3 種類に切り替え，それぞれの場合において iperf[15] を用いて TCP スループットの測定を行った．用いたネットワークの種類は全て 100BaseT である．また，各 PC の諸元を表 1 に示す．

実験結果を表 2 に示す．この結果から MTU が 1500

表 1: 各 PC の諸元

PC	CPU	メモリ
PC1	Pentium3 864MHz	256MB
PC2	Pentium4 3GHz	1GB
PC3	Pentium4 3GHz	1GB

表 2: 性能評価実験結果

PC3 種別	MTU(byte)	スループット (Mbps)
通常ルータ	1500	94.3
通常ルータ	1492	92.7
通常 NAT ルータ	1500	94.2
通常 NAT ルータ	1492	92.6
試作 NAT ルータ	1492	92.5

の場合の通常ルータと比較すると，試作 NAT ルータは 1.8Mbps（約 1.9%）のスループットの低下が見られる．一方，通常ルータや通常 NAT ルータでは MTU が 1500 から 1492 に減少するといずれも 1.6Mbps（約 1.7%）のスループットの低下が見られる．したがって，試作 NAT ルータによるスループット低下の主たる原因は MTU の減少によると思われる．ただし，スループットの低下の割合は 2%以下であり，実用上は問題ないと思われる．

4.3 適用範囲に関する考察

提案手法の適用には様々な前提条件が必要となるため，対象や環境によっては提案手法が適用できない場合がある．そこで本節では提案手法の適用範囲について考察する．

4.3.1 LSRR オプション無効化による影響

現在，多くのネットワーク機器やホストでは，セキュリティ上の理由により LSRR オプションが標準的に無効化されている．したがって，提案手法はそのままでは多くの環境で利用することができず，ルータやホストで LSRR オプションを有効化するように設定変更を行う必要がある．しかし，その必要が生じるのは組織内ネットワークのルータおよびマルチホーム化のサービス対象となるホスト（サーバ）だけであり，組織外のネットワーク機器やクライアントでは設定変更の必要はない．

また，この手法を用いた場合でも組織外ネットワークから送信された LSRR オプション付きパケットは外部ネットワークとの接続部分で廃棄することが可能であるため，少なくとも組織外からの攻撃に対するセキュリティは低下しない．ただし，組織内ネットワークにおいては LSRR オプションの有効化により，たとえばアドレス広告のないネットワークにもゲートウェイの指定によりアクセスが可能になるなどの危険性が生じるため，ネットワークの構成や設定によっては注意が必要である．

4.3.2 Path MTU 減少が与える影響

提案手法では NAT ルータで 8 バイトの LSRR オプションを付加するため，見かけ上クライアント・サーバ間の Path MTU が減少する．そのため，ソフトウェアによっては Path MTU の減少を認識できず，通信に支障を来たす可能性がある [16]．しかし，Path MTU の減少はたとえば L2TP[17] などの IP トンネリング技術を用いる場合にも生じる問題で，提案手法特有の問題ではない．もし，この問題が解決できないようであれば，TCP 通信の開始時において NAT ルータが MSS（Maximum Segment Size）の値を変更，あるいは新たに指定する方法が有効に機能すると思われる．

4.3.3 UDP 通信への適用

UDP については TCP とは異なりコネクションの概念がないため，サーバからクライアントへ送信されるパケットが同一フローに属するかどうか判別することが通常は困難である．したがって，一般には UDP 通信については提案手法は適用できないと思われる．しかし，現在ではネットワーク上の多くのサービスがトランスポート層プロトコルとして TCP を用いており，この制約による影響は事実上それほど大きくないと思われる．

ただし，UDP を用いた重要なサービスとして DNS がある．NAT を用いたマルチホーム化手法では，インバウンド接続の経路選択に DNS を利用すると想定しているため，DNS プロトコルについては往復とも同一の経路を経由するように対応する必要がある．この問題に対しては，たとえば NAT ルータが DNS サーバを兼ねる，あるいは NAT ルータ経由での問合せのみを受信し，応答を必ず NAT ルータ経由で送信するような DNS サーバを用意する，などの方法で対応可能である．

4.3.4 複数のサーバへの適用

組織内ネットワークに複数のサーバが存在する場合，クライアントが NAT ルータ経由でこれらにアクセスするには原則として 1 台のサーバにつき一つの IP アドレスが必要である．現在，IPv4 のアドレスは枯渇しつつあるため，組織内に多数のサーバが存在する場合には IP アドレスの割当てが困難になることが今後予想される．

この問題については，ALG を用いたマルチホーム化でも同様であり，たとえば一つのアドレスに対してサービスの異なる複数のサーバを対応させ，宛先ポート番号に応じて変換後の宛先 IP アドレスを決定するような仕組みの導入などが対策方法として考えられる．

4.3.5 IPv6 環境への応用

IPv6 の場合には一般に各サーバは複数のアドレスを持つことができる．したがって，各 ISP から割り振ら

れたアドレスを一つのサーバに割り当て，NAT 機能を導入することなくマルチホーム化を実現することが可能である．しかし，この場合にも各バックボーンの流入フィルタリング（ingress filetering）を回避するために往復の経路を一致させる必要があり，たとえば組織内ネットワークにおいて送信元アドレスに基づく経路制御機能の導入が新たに必要になる [18].

この問題の一つの解決策として，提案手法の IPv6 環境への応用が考えられる．IPv6 においても routing header と呼ばれる拡張ヘッダ [19] を用いることにより，LSRR の指定と同様の効果を得ることが可能である．したがって，提案手法を IPv6 環境へ応用すれば，組織内ネットワークの広範囲に新たな経路制御機能を導入する必要がなく，提案手法に基づく NAT ルータの導入と既存のネットワーク機器および対象ホストでの routing header の有効化のみで往復の経路を一致させることができる．

5. まとめ

本論文では，NAT ルータへ LSRR オプションを付加・削除する機能を導入することにより，インバウンド接続についても復路の経路選択を可能にするマルチホーム化手法を提案した．またこのような機能を持つ NAT ルータを試作し，実際に通信が行えること，オーバヘッドは高々2%程度であることを確認した．これにより，導入コストや管理コストが比較的小さく利用可能な通信プロトコルの制約が少ないという NAT によるマルチホーム化方法の利点を活かしながらインバウンド接続についてもマルチホームネットワークの利点を享受することが可能になった．

今後の課題としては DNS を用いた動的トラフィック分散機能 [7][8] と組み合わせ，実環境において動作検証および性能評価を行うことが挙げられる．また，IPv6 環境においても適用できるように NAT ルータを拡張し，有効性を検証することも将来は行いたい．

参考文献

[1] Hawkinson, J.: Guidelines for creation, selection, and registration of an Autonomous System (AS), RFC1930, IETF (1996).

[2] 山井成良，土居正行，岡山聖彦，中村素典：マルチホームネットワークにおける電子メールシステムの高信頼化運用手法，第 6 回情報科学技術フォーラム情報技術レターズ，pp.373–376 (2007).

[3] Egevang, K. and Francis, P.: The IP Network Address Translator (NAT), RFC1631, IETF (1994).

[4] 岡山聖彦，山井成良，島本裕志，宮下卓也，岡本卓爾：マルチホームネットワークにおける透過的な動的トラヒック分散，情報処理学会論文誌，Vol.41, No.12, pp.3255–3264 (2000).

[5] 岡山聖彦，山井成良，久保武志，宮下卓也：マルチホームネットワークにおけるアプリケーションプロトコルの性質を考慮した動的トラフィック分散，情報処理学会論文誌，Vol.46, No.4, pp.1007–1016 (2005).

[6] Rekhter, Y., Li, T. and Hares, S. (Eds.): A Border Gateway Protocol 4 (BGP-4), RFC4271, IETF (2006).

[7] 金勇，山井成良，岡山聖彦，清家巧，中村素典：マルチホーム環境における DNS 応答の多重化による自組織宛メール配送の動的経路選択手法，情報処理学会論文誌，Vol.51, No.3, pp.998–1007 (2010).

[8] Jin, Y., Yamai, N., Okayama, K. and Nakamura, M.: An Adaptive Route Selection Mechanism Per Connection Based on Multipath DNS Round Trip Time on Multihomed Networks, Proceedings of 2010 10th Annual International Symposium on Applications and the Internet (SAINT 2010), pp.52–58, DOI:10.1109/SAINT.2010.21 (2010).

[9] Postel, J. (Ed.): Internet Protocol, RFC 791, IETF (1981).

[10] Antsilevich, U. J. S., Kamp, P.-H., Nash, A., Cobbs, A. and Rizzo, L.: IPFW(8), FreeBSD System Manager's Manual (online), available from ⟨http://www.freebsd.org/cgi/man.cgi?query=ipfw⟩ (accessed 2011-06-30).

[11] Cobbs, A.: DIVERT(4), FreeBSD Kernel Interfaces Manual (online), avaiable from ⟨http://www.freebsd.org/cgi/man.cgi?query=divert⟩ (accessed 2011-06-30).

[12] The Apache Software Foundation: Welcome! - The Apache HTTP Server Project (online), avaiable from ⟨http://httpd.apache.org/⟩ (accessed 2011-06-30).

[13] Free Software Foundation, Inc.: GNU Wget (online), avaiable from ⟨http://www.gnu.org/software/wget/⟩ (accessed 2011-06-30).

[14] Tcpdump/Libpcap: TCPDUMP/LIBPCAP public repository (online), avaiable from ⟨http://www.tcpdump.org/⟩ (accessed 2011-06-30).

[15] Iperf (online), available from ⟨http://iperf.sourceforge.net/⟩ (accessed 2011-06-30).

[16] Lahey, K.: TCP Problems with Path MTU Discovery, RFC2923, IETF (2000).

[17] Lau, J., Townsley, M. and Goyret, I. (Eds.): Layer Two Tunneling Protocol - Version 3 (L2TPv3), RFC3931, IETF (2005).

[18] Ohira, K. and Okabe, Y.: Host-Centric Site-Exit Router Selection in IPv6 Site Multihoming Environment, *Proceedings of 1st International Workshop on Protocols and Applications with Multi-Homing Support* (*PAMS 2011*), pp.696–703 (2011).

[19] Deering, S. and Hinden, R.: Internet Protocol, Version 6 (IPv6) Specification, RFC2460, IETF (1998).