社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2007－ＤＳＭ－46／2007－ＱＡＩ－24（13）
2007／7／20

サービス指向型ルーティングを目的としたエンドホストへの動的なIPv6割当て手法の提案

吉田 薫† 江崎 浩†

† 東京大学 大学院 情報理工学系研究科 〒113-8656 東京都 文京区 本郷 7-3-1
E-mail: †kaoru@hongo.wide.ad.jp, †hiroshi@wide.ad.jp

あらまし 近年，ブロードバンドな通信環境が一般家庭にまで広く普及してきており，この環境下，種々に異なる通信品質を要求するサービスが提案，利用されるようになってきている．こうしたサービスを利用するホストには，通常一意の IP アドレスが割り当てられており，その IP アドレスを基に通信経路が決定される．そのため，あるホストと別のホストが通信を行う際には，IP アドレスを基に一意の通信経路が決定されることになる．これは，一般に通信品質要求の異なる複数のアプリケーションの通信も，通信相手が同一の場合には同じ経路を介して通信が行われるということである．つまり，サービスの通信特性に応じて通信経路を選択するということは，事実上不可能である．本論文の目的は，ユーザやそのユーザが利用するサービスの品質要求に応じて，自由度の高い通信経路を選択可能とする仕組みを提供することである．これを実現するため，通常一つのホストが一つのみ保持する IP アドレスに，広範囲なアドレス空間を持つ IPv6 アドレスを利用し，サービス毎に IPv6 アドレスの動的な割当てを行うことで，一つのホストが容易に複数のアドレスを保持可能とする．そして，その IPv6 アドレス毎に柔軟な経路制御を実現するための手法の提案を行う．

キーワード IPv6，ルーティング，アドレス割当て

Dynamic IPv6 address Allocation to End Hosts for Service Orientied Routing

Kaoru YOSHIDA† and Hiroshi ESAKI†

† The University of Tokyo, 7-3-1 Hongo Bunkyo-ku, Tokyo 113-8656, Japan
E-mail: †kaoru@hongo.wide.ad.jp, †hiroshi@wide.ad.jp

Abstract According to wide deployment of broadband Internet environment both to offices and residences, wide variety of new applications has developed and deployed. QoS requirements of those applications differ based on their communication characteristics. But forwarding paths of various applications between two nodes are same, even QoS requirements of them are different. This is because, each node running such applications can only have a single IP address in general, and forwarding path from/to the node is uniquely selected using the IP address. As far as each node has a single IP address, it is practically impossible to use multi paths for the purpose of QoS. The objective of this paper is to offer users more flexible forwarding path selection based on their needs or their applications' requirements. To do that, we dynamically assign multiple IPv6 addresses, which have a huge address space, to a node based on their requirements, and provide different forwarding path to each IPv6 address.

Key words IPv6, Routing, Address assignment

1. はじめに

近年，ブロードバンドな通信環境が一般家庭にまで広く普及してきており，この環境下，種々に異なる通信品質を要求するサービスが提案，利用されるようになってきている．こうしたサービスを利用するホスト (計算機) には通常一意の IP アドレスが割り当てられており，インターネットのコアネットワーク (ISP の内部ネットワークなど) ではその IP アドレスを基に通信経路が決定される．つまり，あるホストと別のホストが通信を行う際には，それぞれが持つ IP アドレスを基に一意の通信経路が決定されることになる．これは，一般に通信品質要求の異なる複数のサービスの通信も，通信相手同一の場合には同じ通信経路を介して通信が行われるということである．つまり，サービスの通信特性に応じた通信経路をユーザが選択するということは，事実上不可能である．

現在のインターネットでサービス毎に通信経路を変更するためには，現状の通信経路識別子である IP アドレスの他に，サービス識別子であるポート番号も考慮する必要性があるが，サービスの中には利用するポートが予め定められていないものも数多く存在する．そのようなサービスに対して配送制御を行う場合には，パケットのペイロードも確認する必要が出てくるが，これはネットワーク内の機器の処理負荷を増大させる原因となる．通信品質が重要な VoIP 通信の場合，通信を優先制御するために IP ヘッダの TOS ビットを立てることにより，優先制御するという仕組みは存在するが，これは TOS ビットが立っているかどうかのみが優先度の唯一の指標である．また，この TOS ビットが立っている場合でも，それを優先制御するかどうかはコアネットワーク側の判断である．つまり，一般的に優先度を決定する権利はユーザ側には存在しない．また，ユーザが複数のネットワークに接続し，マルチホーム環境を作ることで，サービス毎に違うネットワークを利用するということは可能ではあるが，接続コストの面での問題が存在し，本論文では対象としない．

本論文の目的は，ユーザやそのユーザが利用するサービスの品質要求に応じて，自由度の高い通信経路を選択可能とする仕組みを提供することである．これを実現するため，通常一つのホストが一つのみ保持する IP アドレスに，広範囲なアドレス空間を持つ IPv6 アドレスを利用し，サービス毎に IPv6 アドレスの動的な割当てを行うことで，一つのホストが容易に複数のアドレスを保持可能とする．そして，その IPv6 アドレス毎に柔軟な経路制御を実現するための手法の提案を行う．

2. IPv6 の現状

数年後の IPv4 アドレスの枯渇の指摘 [1] を受け，グローバルに IPv6 アドレスを利用できる環境の構築が急務となり，また実際に進められている．本論文では，IPv6 の数年後の本格運用を見据え，またその広範囲なアドレス空間を効率的に利用することで，前節で述べた課題の解決を図ることを目的としている．そこで，現状の IPv6 アドレスの利用方法について簡単に述べる．

現在 IPv6 アドレスは，各 AS(Autonomous System) に対して /32 を最小割当て単位として，割り振りが行われている．各 AS は，割り当てられたアドレスを基に，自ネットワーク内のサイト (末端ネットワーク) に対して，通常 /64 を最小単位として更なる割当てを行う (図 1)．他方，IPv4 アドレスの場合には，各サイトには /24 を最大単位として割当てを行うのが一般的である (割当てアドレスがプライベートアドレスの場合もある)．各サイトの内部ネットワークでは，手動設定，DHCP や IPv6 の場合には EUI64(64-bit Extended Unique Identifier) などを利用して，各ホストへのアドレス割当てを行う．

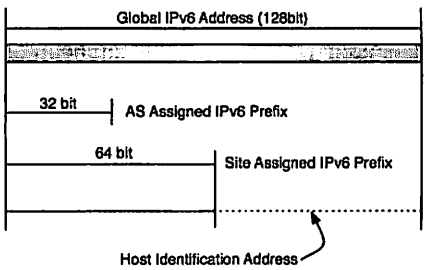

図 1　IPv6 アドレスの割当て方

つまり，IPv4 と IPv6 の双方が利用されているネットワークでは，/24 の IPv4 アドレスと /64 の IPv6 アドレスの割当てがなされることになる．そのネットワーク内部に存在するホストが IPv4 のアドレス空間で十分に収容できている場合には，IPv6 のアドレス空間はそれに比較して広範囲であり，未利用アドレス空間が多く存在することになる．そのようなネットワークでは，アドレスの効率的な利用ができていないと言うことができ，またそのようなネットワークは多数存在している．しかし，/64 を最小割当て単位としてサイトへの割当てを行う手法は既に一般的であり，これを変更するには各サイトへのドレスの再割当てが必要となり，現実的に困難である．また，/64 より小さいアドレス空間の割当ては，結果としてコアネットワーク内での経路数の増大を招くことになる．

3. 提案アーキテクチャ

3.1 アーキテクチャ概要

本論文では，第 1. 節で述べた課題を解決する一つの手法として，あるホストに対して，サービス毎にユーザが選択可能な IPv6 アドレスの動的な割当てを行い，その IPv6 アドレスを基に，より自由度の高いルーティングを実現する手法を提案する．また，この動的な IPv6 アドレスの割当てには，第 2. 節で述べたように各サイトに割り当てられながら利用されていない未利用アドレス空間を利用し，エンドユーザが個々の通信で必要とする通信品質要求に応じて IPv6 アドレ

スを選択可能とする仕組みの提案を行う．図2に，提案アーキテクチャの概念図を示す．

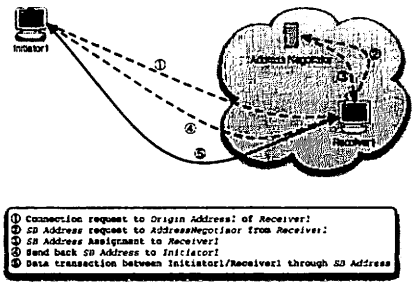

図2 動作概要

各ホスト (レシーバ 1:Receiver1) は，予めグローバルなIPv6 アドレス (Orign アドレス:Origin Address) を保持しており，そのアドレスはホストに対して付与される FQDN と対応しているものとする．外部 (イニシエータ 1:Initiator1) からレシーバ 1 へアクセスする際には，FQDN を基にアドレス解決を行い，Origin アドレスを宛先アドレスとして接続要求を行う．接続要求を受信したレシーバ 1 は，接続するネットワーク内に存在するアドレスネゴシエータ 1 から，利用するサービスの通信品質要求に見合う配送制御可能なアドレス空間の割当てを受け，そのアドレス (SB アドレス:Service Binded Address) をイニシエータ 1 へ送り返す．イニシエータ 1 は，改めてその SB アドレスを宛先アドレスとして通信を開始する．コアネットワーク側で Origin アドレス と SB アドレスを宛先とする通信の配送経路が異なるようにネットワークを設計しておくことで，通信品質の異なる配送経路を提供することが可能となる．

以下では，各サイトへ割り当てる IPv6 のプレフィックス長を /64 であるものとして議論を行うが，それ以外の場合でも一般性は失われないものとする．

3.2 Origin / SB アドレス

あるホストが予め保持し，FQDN を基に DNS などを利用して名前解決可能なアドレスを Origin アドレスと呼ぶ．また，ホストが通信を行う際に，その通信品質に見合うよう動的にアドレスネゴシエータによって割り当てされるアドレスを Service Binded(SB) アドレスと呼ぶ．SB アドレスは，Origin アドレスを基に Network Routing Label(第 3.3 節参照) を利用して設定される．Origin アドレスと SB アドレスは，配送経路が異なっていることが望ましいが，実際にどのような配送経路が選択されるかは，コアネットワーク内のルータが Network Routing Label をどのように扱うかに依存する．

3.3 Network Routing Label

AS 内部での OSPF [2], [3] や AS 間の BGP [4] をはじめとする現在のインターネットの配送制御手法は，ルータが保持するルーティングテーブルに書かれているプレフィックスと宛先アドレスの最長一致 (ロンゲストマッチ) を取ることにより，配送経路を決定している．この場合，サイト内に存在するホストが，その通信経路として複数の経路を保持するためには，ホストに対し複数のアドレスを付与し，そのアドレス毎に違う配送経路が選択されるように，それぞれに異なるプレフィックスを付与する必要がある．しかしながら，あるサイトに対して複数の任意のプレフィックスを割り当てることは，コアネットワーク内で交換される経路数の増大を招くことになる．通常，あるサイト内に複数のプレフィックスを割り当てる場合には，ネットワークを予め注意深く設計しプレフィックスの経路の集約化を行うことで，経路数の増大を防ぐのが一般的である．この場合，包括されるプレフィックス内に存在するアドレスを宛先とする通信の配送経路は同一のものとなり，互いに異なる配送経路を提供することはできない．つまり，現状ではネットワーク経路数とホストが選択可能な配送経路の数はトレードオフの関係にあり，両者を満足させる手法は存在しない．また，あるサイトに対して，経路の集約化の有無に関わらず，複数のプレフィックスを割り当てることは，第 2. 節で述べたように，現状の IPv6 割当てによって既に多くの未利用アドレス空間が存在することを考慮すれば，より多くの未利用アドレス空間を生じさせることを意味する．

そこで，本論文では，各サイトに割り当てられるプレフィックスの割り当て数及び大きさを保持したまま，複数の異なる配送経路を提供するための機構として，Network Routing Label(NR Label) の概念を導入する (図 3)．NR Label は，現在各サイトへ割り当てられている /64 のアドレス空間に固定長で割り当てられる配送経路識別子である．

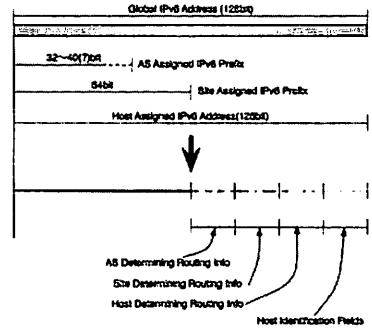

図3 NR Label

第 2. 節で述べたように，現状多くの場合，あるサイトに存在するホスト数は IPv4 アドレスの /24，つまり 8bit 分の空間，で十分に賄うことができる．そこで，将来的に各サイトに収容されるホスト数が増加する可能性を考慮し，各サイトへ割りあわてるプレフィックス /64 のうち，下位 16bit 分の空間をホスト識別空間 (HI: Host Idefication) として定義する．HI は，サイト内の各ホストを一意に識別するための識別子である．残りの 48bit 分の空間のうち，上位 16bit

分の空間を AS 決定配送制御識別空間 (ASNR Label)，次の 16bit 空間をネットワーク決定配送制御識別空間 (NNR Label)，その次の 16bit 空間をサイト決定配送制御識別空間 (SNR Label) と定義する．なお，ASNR/NNR/SNR Label 及び HI の空間の広さは，そのネットワーク毎に同意が取れた固定長であればよく，上述の長さではなくても一般性は失われない．

NNR Label は，AS 内部の各ルータが任意に設定可能なラベルである．ルータは，収容しているサイトに対して異なる通信品質を提供するための通信経路を確保したい場合には，プレフィックス単位で NNR Label を複数設定し，それらが異なる経路を通るように設定する．ASNR Label は AS 境界上のルータが，SNR Label はサイト内に存在するルータが，それぞれ任意に設定可能なラベルである．

NR Label を配送制御識別子として利用することで，既存の配送制御手法に比べ，図 4 に示すように配送制御空間を拡張することができる．つまり，現在はプレフィックス単位という一次元でのみ可能な配送制御を，プレフィックスと NR Label という二次元に拡張することができる．また，NR Label を利用することにより，あるルータが複数のサイトを収容し，それらのプレフィックスを集約して経路広告している場合であっても，収容しているホストに対してサービス毎に異なる配送経路を提供することが可能となる．

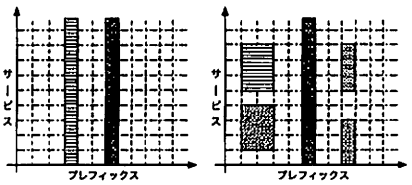

図 4　配送経路の選択のされ方

3.4 イニシエータ・レシーバ

イニシエータがレシーバへの通信を開始する際には，DNS などを利用して FQDN から Origin アドレスの取得を行い，その Origin アドレスを宛先アドレスとしてレシーバへ接続要求を行う (図 5)．接続要求を受信したレシーバは，イニシエータに提供しようとする通信品質に見合うアドレスをすでに保持しているかを，現在自らが保持している SB アドレスとその通信品質情報から検索する．もし，条件に合う SB アドレスを既に保持している場合には，その SB アドレスをイニシエータへ送り返す．条件に見合う SB アドレスが存在しない場合には，アドレスネゴシエータに対してアドレス空間の取得要求を行い，新たな SB アドレスを取得し，そのアドレスをイニシエータへ送り返す．SB アドレスを取得したイニシエータは，SB アドレスを宛先アドレスとしてデータ通信を開始する．

現在の通信モデルでは，通信を開始する際には FQDN から名前解決を行い，そのアドレスを利用して当該ホストとのデータ通信を開始することができる．これに対して提案アーキテクチャの場合には，名前解決を行った後，当該ホストへアクセスし SB アドレスの取得を行ってから，データ通信を開始する必要がある．これは，初期段階でのデータ通信の開始を遅らせることになるが，サービスに合った配送経路を行うことができるので，結果として必要なデータ通信を迅速に終了することが可能である．

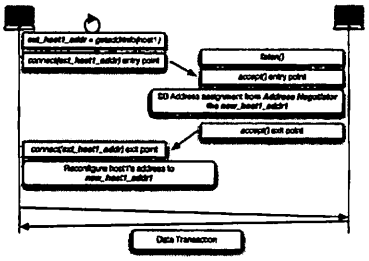

図 5　New TCP Connection

3.5 アドレスネゴシエータ

前節で述べたように，あるホストは，ユーザがネットワークを利用するサービスを開始するなどの理由によって，新たな通信を開始する際，その通信品質要求に見合う配送制御を実現可能な SB アドレスの取得要求をアドレスネゴシエータに対して行う．要求を受信したアドレスネゴシエータは，そのネットワークの配送制御を行っているルータに対して利用可能な NR Label の情報，及びそれぞれのラベルの通信品質情報を取得する．これらの情報を基に，ホストが要求する通信品質に見合った NR Label に当該ホストの HI を付与したアドレスを SB アドレスとして，ホストへ通知する．この際，NR Label の情報をキャッシュしておくことで，通知時間を短縮することができる．

3.6 提案アーキテクチャの特長

現在のインターネットでトラヒックエンジニアリングを行う場合には，配送制御識別子である IP アドレスとは別の情報 (サービスのポート番号など) を利用する必要がある．これは，配送制御識別空間が一次元から二次元以上に膨張することになり，管理が複雑化し運用コストを上昇してしまう．それに対して，本論文が提案する手法の場合，サービスに結び付けられたアドレス空間を構築し，それを基に配送制御を行っているので，配送制御識別子を IP アドレスの一次元に抑えたまま柔軟な配送制御を実現することができる．

また，既存のトラヒックエンジニアリング技術は，コアネットワークでの効率的な配送制御に主眼をおいているのに対し，提案アーキテクチャでは，コアネットワークとエンドホストが協調することで，エンドホストが必要とする通信品質に見合う通信を提供することが可能となる．

本手法の導入により，現在グローバル IPv6 アドレスのホストへの割当てとして広く利用されている EUI64 方式は利用できなくなるが，DHCPv6 [5] などの代替手段が存在して

おり，ここではその優劣に関しては議論しない．また，リンクローカルアドレスに対して EUI64 方式を利用することは，そのアドレスがグローバルな通信に利用されることがないので問題ない．

4. 機能要求

本節では，前章で提案したアーキテクチャを実現するために必要な以下の二つの機能について述べる．

- エンドホストアドレス変換
- NR Label を利用した配送制御

4.1 エンドホストアドレス変換

Origin アドレスを基に接続要求を出し，SB アドレスを取得後にデータ通信を開始するという本提案手法を実現する場合，その実現方法は以下の二通りが考えられる．

一つ目の方法は，イニシエータが getaddrinfo() 関数などを利用してレシーバの Origin アドレスを取得した際に，明示的にレシーバへの問い合わせを行い，SB アドレスを取得する方法である．例えば SIP(Session Initiation Protocol) [6] を利用して，通信の開始時に通信するアドレスのやり取りを予め行うことによりこれを実現できる．もう一つの方法は，TCP や SCTP [7] などのように通信の開始時に初期化を行う通信の場合，その初期化時に Origin アドレスと SB アドレスの書き換えをサービスに透過な形で変換する方法である．本論文では，後者の方法について議論する．

広く知られたアドレスを変換する機構としては，NAT [8], [9] が存在する．NAT の場合，あるサイト内のホストが syn パケットを送出すると，NAT ルータは送信元アドレスを自らが持つアドレスに書き替えた後，通信相手へ向かってパケットの転送を行う．その syn パケットを受信した通信相手は，NAT ルータが持つアドレスを宛先アドレスとした syn/ack パケットを返送する．NAT ルータでは，syn/ack パケットの宛先アドレスを syn パケットを送出したホストのアドレスへ書き替えパケットを転送し，そのパケットを当該ホストが受信することで接続が確立される．

この考え方を利用すれば，レシーバでは Origin アドレスを送信元アドレスとした syn パケットを受信し，それに対応する syn/ack パケットを生成した後，NAT の機能により送信元アドレスを Origin アドレスから SB アドレスへ変換することができる (図 6)．接続確立後には，SB アドレスを宛先アドレスとしたパケットを受信すると，その宛先アドレスを Origin アドレスに書き換えてホスト内のサービスへ転送する．こうすることで，サービスからは，常に Origin アドレスを用いてサービスを提供しているように見せることができる．イニシエータでも，基本的には同様の機構の導入によりサービスに対して透過なアドレス変換を行うことができるようになる．ただ，イニシータ側で Origin アドレスと SB アドレスの変換を行う際には，予めその情報を持っておくことができないので，syn cookies [10] のような機構により，syn と syn/ack の対応付けをする必要がある．

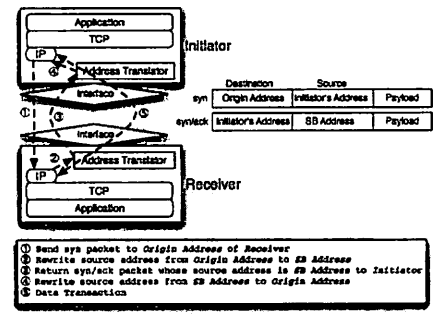

図 6 ホストアドレス変換機構

本提案の手法は，通常の NAT ルータとは異なり，syn パケットに対してはアドレス変換は行わず，syn パケットの宛先アドレスと syn/ack パケットの送信元アドレスの対を基にアドレス変換を行う．こうすることで，サービスからは最初の syn パケットのアドレス対を基にサービスを利用，提供しているように見えながら，実体として通信品質を考慮した SB アドレスを利用した配送制御を行うことができるようになる．

4.2 NR Label を利用した配送制御

第 3.3 節で述べたように，提案アーキテクチャを実現するためには，ルータがプレフィックスの最長一致による配送制御に加え，NR Label を識別し，それに応じた配送制御を行う必要がある．

以下では，AS 内部のネットワークを例に取り，NNR Label が設定されたネットワークでのルータが持つべき機能について説明する．Host1 が持つ Origin アドレスを XXXX:XXXX:XXXX:XXXX::ZZ/64 (Prefix1: XXX:XXX:XXX:XXXX::/64, HI1: ZZ) とする (図 7)．既存の配送制御手法では，Host1 を収容している Router1 は，OSPF 等を利用して Router2,3 に対して Prefix1 を広告する．Router1 から Prefix1 の経路情報を受け取った Router2,3 は，更に Router4,5,6 へと逐次的に経路情報を広告する．Router6 では，Router4,5 から受け取った情報を基に，Prefix1 への配送経路を決定する．この時，Router4,2 経由の配送経路が選択されるものとする．

提案アーキテクチャでは，Router1 から Prefix1 の経路広告をする際に，上述した通常の経路広告に加え，Router2 へ広告する経路情報には AAAA という NNR Label を，Router3 へ広告する経路情報には BBBB という NNR Label を付与して広告する．この情報は OSPF の Opaque LSA などを利用して広告する．Router4,5 を介して広告されたこの経路情報を取得した Router6 では，図 7 のようなルーティングテーブルを作成する．通常の最長一致で決定されるプレフィックスごとの配送経路に加え，そのプレフィックスに付与される NNR Label 毎の次に配送されるべき (ネクストホップ) ルータ情報がルーティングテーブルに記載

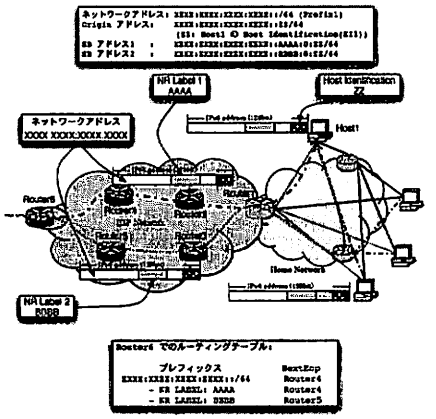

図 7 NR Label を用いた配送制御

されることになる．通常は，アドレスの最長一致によりネクストホップを決定するが，本手法では最長一致を取った後，NNR Label の値をさらに見てネクストホップを決定する．この時，Router1 が予め広告していない NNR Label が付与されたアドレスを宛先とした通信が行われる可能性が存在するが，その場合には通常の最長一致に基づいて配送経路が選択される．また，宛先アドレスの ASNR/SNR Label にも同様に情報が記載されている可能性もあるが，AS 内部の配送制御では，これらのラベルの値は無視される．つまり，XXXX:XXXX:XXXX:XXXX:1111:AAAA::ZZ と XXXX:XXXX:XXXX:XXXX:2222:AAAA::ZZ の様に異なる ASNR Label を付与されたアドレスを宛先とする通信であっても，プレフィックスと NNR Label が同一の場合には，AS 内部では同一の配送経路が選択されることになる．

仮にネクストホップの検索が radix tree に基づいて行われているとすると，ネットワークアドレス (XXXX:XXXX:XXXX:XXXX::/64) を検索した後，NNR Label である 80〜96bit 目の空間を再度検索することになる．NNR Lable の存在する位置が予め定められていれば，最大 80(64 + 16) 段の検索でネクストホップ決定することが可能である．現在の配送制御で 96bit 目までをネットワークアドレスとして利用している場合，最大 96 段の検索が必要となる．経路集約方法によって検索すべき段数は異なるが，ASNR Label の分だけ検索空間は小さくなる．

サイトを収容しているルータが，一つの上流接続を持たないなどの理由により，異なる NR Label を異なる配送経路で広告をできない場合には，誘導経路情報を用いた配送制御手法 [11] などを利用することで，複数の配送経路を広告することが可能である．

5. おわりに

本論文では，広範囲なブロードバンド環境の実現，及びそのネットワークを利用した様々通信品質要求の異なるサービスが利用されるようになってきた現在のインターネットにおいて，ユーザの要求に応じてサービス毎に動的な IPv6 アドレスの割当てを行い，そのアドレスを基により自由度の高い配送制御を実現するための手法の提案を行った．また，この手法を実現するために必要な，エンドホストにおけるアドレス変化機構，及び配送制御手法の拡張技術の提案も行った．本論文が提案する手法はユーザに対して通信経路選択の自由度を与えるという点で今まで提案されてきたトラヒックエンジニアリング手法とは異なる．今後は提案手法の実装及び評価を行う予定である．

文 献

[1] Geoff Huston. *IPv4 Address Report.* `http://www.potaroo.net/tools/ipv4/`.
[2] J. Moy. *OSPF Version 2.* RFC 2328, April 1998.
[3] R. Coltun, D. Ferguson and J. Moy. *OSPF for IPv6.* RFC 2740, December 1999.
[4] Y. Rekhter and T. Li. *A Border Gateway Protocol 4 (BGP-4).* RFC1771, March 1995.
[5] R Droms, Ed., J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney. *Dynamic Host Configuration Protocol for IPv6 (DHCPv6).* RFC3315, July 2003.
[6] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peerson, R. Sparks, M. Handley, and E. Schooler. *SIP: Session Initiation Protocol.* RFC3261, June 2002.
[7] R. Stewart, Q. Xie, K. Morneault, C. Sharp, H. Schwarzbauer, T. Taylor, I. Rytina, M. Kalla, L. Zhang and V. Paxson. *Stream Control Transmission Protocol.* RFC2960, January 2001.
[8] K. Egevang and P. Francis. *Traditional IP Network Address Translator (Traditional NAT).* RFC1631, May 1994.
[9] P. Srisuresh and K. Egevang. *Traditional IP Network Address Translator (Traditional NAT).* RFC3022, January 2001.
[10] *SYN cookies.* `http://cr.yp.to/syncookies.html`.
[11] 吉田薫. OSPF ネットワークにおける誘導経路情報を用いた動的経路選択手法. Master's thesis, 東京大学大学院情報理工学系研究科, February 2005.