

ラベルスイッチング技術を利用した仮想 IP 層の提案

Virtual IP Layer Based On Label Switching

内田 良隆[†] 三瓶 史彦[‡] 石川 憲洋[†]

Yoshitaka Uchida Humihiko Sanpei Norihiro Ishikawa

[†]株式会社 NTT ドコモ [‡]NTT アドバンステクノロジー株式会社

1. はじめに

近年、インターネットの急速な発展に伴い、ネットワークに接続する端末が増加し、IP アドレスの枯渇が問題になっている。そこで、NAT 機能を搭載したルータ装置等を用いてプライベート空間を構築している家庭や企業が多い。NAT (Network Address Translation) はグローバルアドレスとプライベートアドレス、ポート番号の変換を行うため、1つのグローバルアドレスがあればプライベート空間の複数端末がインターネット接続できる。しかし、両方の通信端末が異なるプライベート空間にいる場合、この NAT が障壁となりポート番号を保持した完全な end-to-end 通信の実現は難しい。プライベートアドレスはそのプライベート空間内に閉じたアドレスであり、グローバル空間では処理できず通信を確立できないため、NAT 越え問題とも呼ばれている。

本稿では、IP 層の上に定義した仮想 IP 層でラベルスイッチング技術を応用して、ラベルとルーティングテーブルを用いて IP アドレス変換を行うトランスペアレントな end-to-end 通信方式を提案する。本方式はマルチキャスト通信、IPv4-IPv6 相互変換、モビリティなどにも適用可能である。

2. 現状の課題

NAT 越え問題に対し、IETF で標準化されている STUN(Simple Traversal UDP through NAT)[1]などでは、UDP hole Punching 技術が利用されている。これはまず NAT 内にいる両方の端末が end-to-end 通信に利用する NAT 装置のグローバル IP アドレス、ポート番号をサーバに登録し、それを各端末が取得する。その後、各端末が一度通信を試みることによって NAT 装置がその IP アドレス、ポート番号を記憶し、NAT 装置に穴を開ける技術で UDP 通信を実

現する。しかし、アドレス、ポートなどのマッピング方法の違いから 4 種類に分類される NAT 全てに適用できるわけではなく、その際にパケット自身をサーバが中継して通信しなければならない。また、サーバを利用している点もフォールトトレランスなものとは言えない。そして、UDP 通信のみであるため、TCP 通信に適用できないことも課題と言える。

異なるアプローチとして、アドレス自体を拡張する IPv6 ネットワークの構築も考えられているが、現時点であまり進んでいない。

3. 提案方式の概要

図 1 に示すように、IP 層の上に仮想 IP 層を定義する。この仮想 IP 層において MPLS(Multi Protocol Label Switching)[2]で利用されているようなラベルスイッチング技術を応用し IP パケットのルーティングを行う方式が本稿の提案方式である。また、この仮想 IP 層でラベルスイッチを行うルータをバーチャル IP ルータ (VIP ルータ: Virtual IP Router) と呼ぶ。

VIP ルータは、アドレス空間の異なる IP パケットを中継する。中継には、ラベルと IP アドレスを関連付けたルーティングテーブルを利用する。グローバル空間に接している VIP ルータは端末から DNS への名前登録要求を代行する役割を負う。以下では、VIP ルータ R1 についてグローバル空間側のアドレスを R1、プライベート空間側のアドレスを小文字で r1 と表記する。

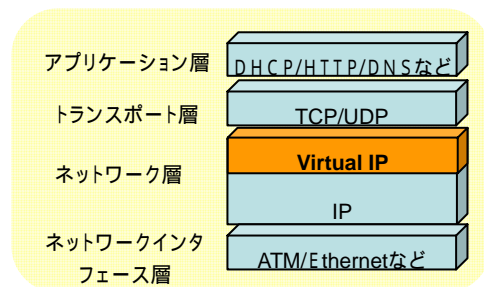


図 1 仮想 IP 層

[†] NTT DoCoMo, Inc.
[‡] NTT Advanced Technology Corporation
 { uchidayo, ishikawanor }@nttdocomo.co.jp

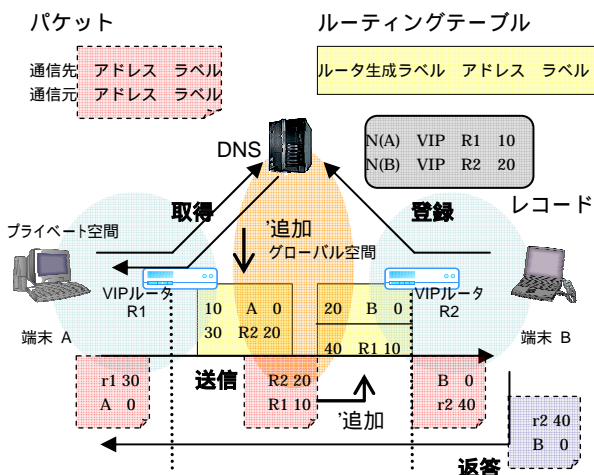


図2 提案方式の概要図

domain name	VIP	IP Address	VIP Label
例) A.vip.com	VIP	123.123....	10

図3 VIP レコード

図2は提案方式の概要図であり、IPパケットのヘッダ情報、手続きの流れを示している。また、提案方式は片方の端末がグローバル環境にある場合にも適用できるが、本稿では両方の端末がNAT下にいる場合について示す。下記に手続きについて説明する。

Phase 1: 名前登録

各端末は、ネットワークに接続すると示すように、VIPルータを介してDNSに一意的な名前(B)と対応するラベルを登録する。VIPルータは端末から受け取った情報(B,0)を動的に作成したラベル(20)と対応付けてルーティングテーブルに格納し、DNSに名前(B)、アドレス(R2)、生成したラベル(20)を登録する。情報は、図3のような新たに定義したVIPレコードをDynamicDNS方式[3]によりDNSに追加し、登録する。

Phase 2: ラベル・IPアドレスの取得

通信を開始する場合は、のようにVIPルータを介しDNSに通信先端末Bの名前を問い合わせ、ラベルとアドレスを得る。なお、VIPルータはラベル(30)を生成しDNSからの返答(R2,20)に関連付け、ルーティングテーブルに格納する。そして通信元

端末へアドレス(r1)・生成したラベル(30)を送信する。

Phase 3: 通信の開始

アドレス(r1)・ラベル(30)を取得した通信元端末はパケットヘッダにその情報を設定し、VIPルータに送信する。VIPルータR1は送信先ラベル(30)をルーティングテーブルと照合し次に転送する宛先のアドレス(R2)、ラベル(20)を得て、通信先情報に設定する。そして通信元情報には中継するアドレス空間側のアドレス(R2)と通信用に生成したラベル(10)を設定し、中継する。VIPルータR2はルーティングテーブルを参照し通信先端末Bに中継する。また、その際に新たなラベル(40)を生成し、送信元情報(R1,10)と関連付けルーティングテーブルに追加する。

Phase 4: 応答パケットの返信

通信先端末Bは、パケットを受信すると送信元、送信先情報を入れ替えて応答パケットを送信する。パケットが辿ってきた経路を中継し、通信元端末Aに応答パケットを送信することができる。

4. まとめ

本稿で提案した方式は、NATなどを介し異なるアドレス空間をまたぐ通信において、ポート番号は変更せず、トランスペアレントなend-to-end通信を実現する方式である。複雑な処理はなく、容易にルータへ実装できるものと考えられる。上記の現状の課題でも示した中継サーバが不要であり、TCP通信の確立を実現できる。また、1つのラベルを複数のアドレスに関連付けることによって、マルチキャスト通信へも適用可能とする。その他にIPv4-IPv6相互変換、モビリティなど、アドレス変換を必要とする機能に対して汎用的に適用できることが特徴である。

今後、実証実験環境を構築し本方式の有効性を検証する。

参考文献

- [1] J. Rosenberg, J. Weinberger, et al. *STUN - Simple Traversal of User Datagram Protocol(UDP) Through Network Address Translators(NATs)*, March 2003. RFC3489.
- [2] E. Rosen, A. Viswanathan, and R. Callon. *Multiprotocol Label Switching Architecture*, January 2001. RFC 3031.
- [3] P. Vixie, S. Thomson, Y. Rekhter, and J. Bound. *Dynamic Updates in the Domain Name System(DNS UPDATE)*. April 1997. RFC 2136.