RL-007

SA46T-AS:アドレス変換を用いずに IPv4 アドレス共有を実現するカプセル化技術

SA46T-AS: Encapsulation Technology Enable IPv4 address sharing without Network Address Translation

松平直樹 †
Naoki Matsuhira

1. まえがき

IPv4 アドレスの枯渇以後の状況を踏まえた IPv4 継続利用技術として、SA46T-AS (Stateless Automatic IPv4 over IPv6 Tunneling with Address Sharing) と呼ぶ技術を提案する。SA46T-AS は、同じ IPv4 アドレスを共有するが利用可能なポート番号を排他的に用いるようなサーバの利用形態を、従来技術では必須であったアドレス変換なしに実現する。

本論では、まず、IPv4 アドレス枯渇による環境変化と従来技術の問題点について述べた後、SA46T-AS 技術について述べる。続いて、実装と実証実験について述べ、SA46T-AS を用いたサービスを展望する。最後に、本技術を評価する。

2.IPv4 アドレス枯渇後の課題と本研究の位置づけ

IPv6 の導入がはじまっているが、まだまだ IPv4 が主流であり、IPv4 を置き換えられる程 IPv6 が普及したとは言えない状況にある。

一方、2011 年 2 月に IANA(Internet Assigned Numbers Authority) で、2011 年 4 月に APNIC(Asia Pacific Network Information Centre) で、そして 2012 年 9 月には RIPE NCC(Reseaux IP Europeens Network Coordination Centre) で IPv4 アドレスが枯渇した。そして、ARIN(American Registry for Internet Numbers) に於けるアドレス枯渇予測時期も 2014 年 3 月と、あと 1 年を満たない状況になった [1]。IPv4 アドレス移転も行われるようになっているが、事業者の保有する IPv4 アドレスが枯渇するのは時間の問題とみられる。

円滑な Internet の成長には IPv6 の導入が欠かせないが、一方で、IPv4 アドレス枯渇後の、現行の IPv4 によるネットワークの継続利用が新たな課題となる。なお、ここで言う IPv4 ネットワークの継続利用とは、IPv4 デバイスの追加が一切無しの状況を指すのではなく、制限が生じるかもしれないが、若干の拡張性を提供することにより、IPv4 によるサービス継続のための創意工夫の余地を残し、IPv6 への移行のための時間稼ぎを可能とすることを指す。

このような IPv4 の継続利用を実現するには、二つのアプローチが考えられる。ひとつは IPv4 アドレスの再利用 (Reuse) であり、もうひとつは、IPv4 アドレスの共有 (Share) である。IPv4 アドレスの再利用を実現する技術として、筆者は SA46T(Stateless Automatic IPv4 over IPv6 Encapsulation / Decapsulation Technology) を提案している [2][3]。本論では、もう一方のアプローチである、IPv4 アドレスの共有 (Share) を実現する SA46T-AS を提案する。

表 1: SA46T-AS の位置づけ

移行技術	IPv4 アドレス	
	再利用 (Reuse)	共有 (Share)
Dual Stack	-	-
カプセル化	SA46T	SA46T-AS
IPv4-IPv6 変換		

なお、表 1 に、SA46T と SA46T-AS の位置づけを示す。

3. 従来技術とその問題点

3.1. 既存の IPv4 アドレス共有技術

1 個の IP アドレスを複数のホストで共有する技術として古くから NAT(Network Address Translator)[4] が良く知られている。より厳密に言えば、NAPT(Network Address Port Translator) と言うべきだが、NAT には各種バリエーションがあり、なおかつ、その表現も様々であるため、ここでは、これら技術を総称して NAT と表現する。

この技術は先ず企業の Firewall で用いられ、その後、SOHO ルータと呼ばれる家庭内機種で用いられてから一般化した。SOHO ルータの場合、NAT は PPP[5] で割り当てられる 1 個の IPv4 グローバルアドレスを、複数のホストで共有するための技術として用いられる。SOHO ルータには DHCP[6] サーバが内蔵され、ホストに IPv4 プライベートアドレスを割り当てる。NAT(厳密には NAPT) は、ホストに割り当てた IPv4 プライベートアドレスと、そのクライアントソフトが用いるポート番号の組に対応する、PPP で割り当てられた IPv4 グローバルアドレスと未使用のポート番号を動的に割り当て、以後この対応に従って変換する。こうして 1 個の IPv4 グローバルアドレスを複数のホストで共有する。

一方、サーバ負荷分散技術も 1 個の IPv4 アドレスを複数のサーバで共有しているのでアドレス共有である。このサーバ負荷分散の実現でも、NAT が用いられている。これは、負荷分散装置のバックエンドに複数台のサーバが配置され、負荷分散装置がパケットを複数台のサーバのどれか 1 台に振り分けることにより負荷を分散する。この振り分けを、宛先 IP アドレスを振り分け先のサーバの IP アドレスに書き換えて実現するのである。この負荷分散装置の処理も一種の NAT である。クライアントからサーバに送信される方向のパケット

†富士通株式会社, FUJITSU LIMITED

で見た場合、SOHO ルータで用いられている NAT はソースアドレスを変換することに対し、負荷分散装置では宛先アドレスを変換する点が違いである。

その後、IPv4 アドレス枯渇を意識し、A+P[7] と呼ばれる技術が検討されている。この技術では、ポート番号も意識したルーティングがなされるが、そのために、Port-Range Router と呼ぶ、TCP/UDP ヘッダのポート番号を見てルーティングを行う、これまでに無い特殊なルータを必要とすることが特徴である。この技術は、3 つの構成要素、具体的に、(1) カプセル化/デカプセル化、(2)NAT、及び (3) シグナリングから構成される。カプセル化/デカプセル化は、IPv4 に加え、IPv6 についても可能になっている。つまり、IPv4 over IPv4 もしくは、IPv4 over IPv6 である。この Inner の IPv4 パケットに対しては、アドレス及びポート番号が変換される。

3.2. 既存の IPv4 アドレス共有技術の問題点

これら IPv4 アドレス共有技術に共通するのは、NAT を使用する点である。NAT は、IP アドレスをアプリケーションのデータとしてやりとりするようなアプリケーションを、そのままで動作させることはできない。さらに、NAT による処理は、改ざんそのものであり、IPsec[8] が通らない問題もある。これら NAT が孕む問題は、インターネットのアーキテクチャである End to End 原則 [9] を NAT が破壊する [10] ことが理由である。

また、P2P 対戦ゲームなど P2P 型アプリケーションとの相性に関する課題 [11][12] もあり、NAT の実装は複雑さを増している。

これらは、NAT-Unfriendly Protocol または NAT-Unfriendly Application と呼ばれる。具体的には、FTP[13]、SIP[14]、PPTP[15] などが挙げられる。

また、IETF 標準でなく、商用のアプリケーションでも NAT 越しに利用できないものも存在する。

これら NAT-Unfriendly Protocol に対応するためには、NAT 機器内部で個別の Protocol 毎の対応が必要になる。しかし、全てに於いて対応が可能とは限らないし、対応させるための検討も複雑で、それが容易とは限らない。

4.SA46T-AS 技術

SA46T-AS は、NAT を用いずにアドレス共有を可能とする技術である。この技術は、SA46T 技術を拡張したものである。そのため、SA46T-AS の説明にあたり、まず、SA46T のポイントを整理した後、それを踏まえ、SA46T-AS を説明する。

4.1.SA46T アドレス

SA46T では、IPv4 over IPv6 の、Outer header に格納される IPv6 アドレスを、SA46T アドレスと呼ぶ。SA46T のアドレスの形式を図 1 に示す。

SA46T アドレスは、SA46T prefix、 IPv4 network plane ID、 IPv4 アドレスから構成される。

SA46T prefix
SA46T アドレスの prefix

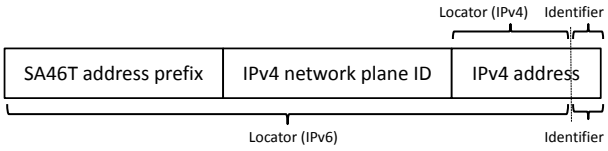

図 1: SA46T アドレス

IPv4 network plane ID
IPv4 ネットワークの識別子

IPv4 address
Inner header の IPv4 アドレス

IP アドレスはロケータとアイデンティファイアの 2 つの情報の組み合わせからなる。この関係を踏まえてみると、SA46T アドレスは、IPv4 アドレスのロケータ部を、IP アドレス全体で 128 ビットまで拡張したアドレスと見ることができる。このとき、IPv4 アドレスのロケータ部はそのままで変わりがない。IPv4 アドレスのロケータに割り当てるビット数を IPv6 アドレス空間に整合するように増やしたアドレスが SA46T アドレスと考えることができる。

4.2.SA46T-AS アドレス

SA46T-AS も、SA46T と同様の IPv4 over IPv6 カプセル化技術である。IPv4 over IPv6 の、Outer header に格納される IPv6 アドレスを、SA46T-AS アドレスと呼ぶ。SA46T-AS アドレスの形式を図 2 に示す。

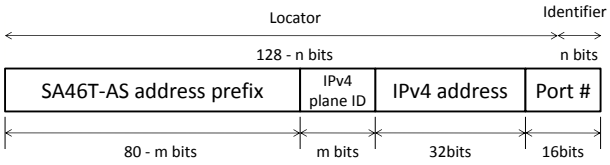

図 2: SA46T-AS アドレス

SA46T-AS アドレスは、SA46T-AS prefix、 IPv4 network plane ID、 IPv4 アドレス、Port 番号から構成される。SA46T との違いは Port 番号の有無である。

SA46T-AS prefix
SA46T アドレスの prefix

IPv4 network plane ID
IPv4 ネットワークの識別子

IPv4 address
Inner header の IPv4 アドレス

Port number
TCP/UDP Protocol の Port 番号

SA46T-AS アドレスは、IPv4 アドレスのアイデンティファイア部を、Port 番号を用いることにより拡張したアドレスと見ることができる。ロケータ部の拡張は SA46T と同様である。

4.3.SA46T-AS の経路広告

SA46T-AS では、1 個の IPv4 アドレスをどのように共有するかを経路制御を用いて実現する。

例えば、1 個の IPv4 アドレスを 1 台のホストで占有する場合、そのホストは、/112、つまり、128 ビットの IPv6 アドレスからポート番号長の 16 ビットを減算した経路を広告することにより実現できる。/112 は全ポート番号を表現する。

逆に、1 個の IPv4 アドレスをホストあたりポート番号を 1 個、つまり、65536 台[1]で共有する場合、それぞれのホストは、/128 の経路を広告すればよい。

例えば、その中間となる 1 個の IPv4 アドレスを、256 台のホストで、各ホストあたり 256 ポートで共有する場合、それぞれのホストは、/120 の経路を広告すれば良い。このように、ロケータとアイデンティファイアの境界は任意の位置に置くことができる。

なお、ホストあたりのポート数は異なっても良い。例えば、1 台のホストが、ポート番号空間の半分の 32768 個のポートを用い、残りのポート番号を、各ホスト 1 個で、32768 台のホストで共有するような割り当ても可能である。この場合、前者のホストは、/113 の経路広告を行い、残りの 32768 台のホストは、/128 の経路広告を行うことにより実現できる。

また、ホストで使用可能なポート番号は、必ずしも連続している必要は無い。連続していれば、経路の集約が期待されるが、集約を考えなければ、全て/128 の経路を、利用可能なポート番号分広告しても良い。

このように、ポート番号による割り振りをポート番号を IPv6 アドレスに含めること、より厳密に言えばポート番号の一部または全体を IPv6 の経路情報に含めることにより、ポート番号も含めて経路制御することが SA46T-AS の特徴である。

このように、経路制御のみで IPv4 アドレス共有が実現できるので、NAT を用いずに実現できるのである。

4.4.SA46T と SA46T-AS との関係

SA46T-AS は、SA46T-AS アドレスに、SA46T アドレスと TCP/UDP のポート番号を追加した技術である。従って、SA46T-AS は SA46T として動作させることも可能である。具体的には、経路広告の設定により可能となる。ロケータとアイデンティファイアの境界を IPv4 アドレスを格納している部分にすれば SA46T として動作するし、ポート番号を格納している部分にすれば SA46T-AS として動作する。

但し、SA46T-AS はポート番号の存在が前提となるため、ポート番号を持たないプロトコル、例えば、ICMP[16] などは扱えない。このような場合、SA46T-AS アドレスのポート番号部にゼロを格納してしまうなど処理を決めてしまえば、SA46T と同様に、ICMP なども扱えるようにすることは可能となる。

しかし、技術の目的が、SA46T が IPv4 アドレスの再利用で SA46T-AS が共有で異なること、そして、SA46T が IPv4 ネットワークのオーバレイによる構築が主観点であることに対して、SA46T-AS がホストが主観点であることなどから、別の技術として位置づけることとした。

[1]ポート番号がゼロと 65535 はルーティングは可能だが、ポート番号として使用出来ないので実際に利用可能であるのは 65534 台となる

5.SA46T-AS の適用対象

SA46T-AS の適用対象は、(1) クライアント、(2) サーバ、(3) P2P が考えられる。本論では、まず、サーバを対象とした。その理由は、サーバにはグローバルアドレスが必須であること、サーバでは、使用するポートを特定あるいは限定できるため、実用的と考えられるためである。

なお、クライアントを対象としたアドレス共有技術として SA46T-AS を用いる際には、SOHO ルータと同様に、複数台のクライアントが用いる IPv4 アドレス及びポート番号と、実際に利用可能な IPv4 アドレスとポート番号の整合を取るために変換が必要となるため、現実的には、NAT(厳密には NAPT) が必要となる。従って、この形態では NAT が不要という SA46T-AS の持つメリットを活かせないため、まずは、サーバを適用対象として検討を行った。

6.SA46T-AS によるシステム構成

図 3 は、SA46T-AS によるサーバ IPv4 アドレス共有を実現するシステム構成図である。本論ではこれを、SA46T-AS サーバ IPv4 アドレス共有システムと呼ぶ。SA46T-AS は、その役割から、フロント側とバックエンド側の 2 種で構成される。これらを、それぞれ、SA46T-AS フロントエンド、SA46T-AS バックエンドと呼ぶ。

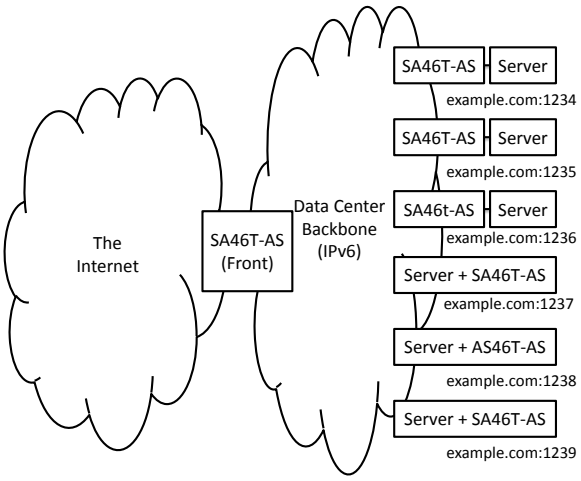

図 3: SA46T-AS サーバ IPv4 アドレス共有システムの構成図

SA46T-AS サーバ IPv4 アドレス共有システムは、SA46T-AS フロントエンドと SA46T-AS バックエンドを IPv6 バックボーンネットワークで接続した構成から成る。

SA46T-AS バックエンドは、サーバと一体化した形態と、サーバと分離した形態の二種類の実装形態がある。

バックボーンネットワークは、IPv6 only の運用が可能、つまり希少となった IPv4 グローバルアドレスを消

費しない運用も可能である。

インターネット上のクライアントは、SA46T-AS フロントエンドと通信しているように見えるが、実際は、クライアントから送信された IPv4 パケットは、SA46T-AS フロントエンドにて SA46T-AS のカプセル化がなされた後、このバックボーンネットワークで IPv6 の経路情報、より特定すれば経路情報のポート番号の情報に基づいてルーティングされる。この IPv6 パケットは、SA46T-AS バックエンドが受信し、デカプセル化されて取り出された IPv4 パケットはサーバに渡される。

インターネット上のクライアントからは、例えば、URL 指定に於いて、

```
http://example.com:1234
```

とポート番号も含めて指定すれば、該当ポート番号が割り当てられているサーバを指定した通信が可能になる。この例では、ホスト example.com のポート番号 1234 番に HTTP プロトコルを用いてアクセスすることを意味する。

7.SA46T-AS の特徴

(1) Stateless
状態を持たないため、状態管理対象の上限など、数の制限が無く、かつ、状態不一致がないので信頼性も高い。例えば、SA46T-AS フロントエンドが何らかの理由でリブートしても、SA46T-AS バックエンドをリブートさせる必要は無い。同様に、SA46T-AS バックエンドのどれか 1 台がリブートしても、SA46T-AS フロントエンド、あるいは、他の SA46T-AS バックエンドをリブートさせる必要も無い。

(2) SA46T-AS フロントエンドの冗長構成が可能
SA46T-AS フロントエンドを複数台用いて冗長構成を実現できる。状態を持たないので、SA46T-AS フロントエンド間での特別な情報の同期も不要である。どの SA46T-AS フロントエンドが用いられるかはルーティングプロトコルが決める。よって、ある SA46T-AS フロントエンドのそのものの故障もしくは、SA46T-AS フロントエンドに接続されるリンクが故障しても、他の SA46T-AS フロントエンドを経由しての利用が可能となる。さらに、ECMP(Equal-Cost Multi-Path) によるトラフィックの負荷分散も可能である。

(3) 特殊なプロトコルを必要としない
SA46T-AS を動作させるためには IPv6 が必要となる。その際、何か独自のプロトコルや既存プロトコルの拡張等不要である。将来、IPv6 への移行が完了した際には、SA46T-AS のみ停止すれば良く、他はそのまま継続して利用できる。SA46T-AS の導入に際し、無駄な投資は必要ない。

(4) 段階的な増設が可能
いつでも、SA46T-AS バックエンド及びサーバの増設が可能となる。よって、段階的な増設が可能となる。

(5) 利用可能なポート番号数を自由に決められる
あるサーバで利用可能なポート番号数を任意に決められるし、それらを混在させても良いし、必ずしも連続している必要も無い。ポート番号が排他でありさえすれば良い。

(6) サーバに於いて IPv6 の利用も可能
サーバで IPv6 を利用できる。IPv4 ではポート番号制限されているが IPv6 なら全ポート利用できる。IPv4 での制限されたポート、及び IPv6 双方でサービス提供することもできれば、IPv4 での制限されたポートのみでサービスを行うが、その運用管理を IPv6 を用いて行うようなことも可能となる。

(7) トラブルシューティングの容易さ
SA46T-AS でカプセル化された IPv6 パケットの IPv6 アドレスを見れば、そこに IPv4 アドレスとポート番号がそのまま格納されているので、判り易く、トラブルシューティングしやすい。

(8) サーバの入れ替えが容易
現用の SA46T-AS Plane と保守用 SA46T-AS Plane を SA46T-AS サーバ IPv4 アドレス共有システム上に共存させることができる。このとき、現用と保守用で共有する IPv4 アドレスは同じにできる。そして、これらの間での切り替えを、IPv4 Network Plane ID の操作のみででき、サーバの入れ替えを容易にできる。

8.SA46T-AS の制限とその対策案

8.1. ポート番号使用が条件

SA46T-AS はポート番号を利用するので、ポート番号を持つトランスポート層を使用するアプリケーションにしか対応できない。具体的には、ICMP や IPsec には対応できない。

但し、このような場合には SA46T-AS フロントエンドで応答することにより対応できる可能性がある。

カプセル化ではよく MTU(Maximum Transmission Unit) の扱いで問題になることがある。SA46T-AS フロントエンドが、SA46T-AS バックエンドに確実に到達できる Path MTU 値を知っていれば、Path MTU Discovery[17] に対応できそうである。具体的には、SA46T-AS フロントエンドが、この値に基づいて、Tunnel MTU を超えるような IPv4 パケットを受信した際には、もし Don't Fragment bit がオフの場合は IPv6 にカプセル化する前に IPv4 パケットをフラグメント化すれば良いが、もし Don't Fragment bit がオンの場合、ICMP エラー Type 3 Code 4 の Fragment needed and DF set を送信元に返送すれば良い。なおこの Path MTU 値は、実際のシステム構成に置ける値を調べてスタティック設定する方法もあれば、IPv6 の Path MTU Discovery を用いて学習して、その値をベースに IPv4 の Tunnel MTU を決める方法も考えられる。その他の対応策として、バックボーンで Jumbo Frame を用いることによってそもそもフラグメント化の必要を無くするという解決策もあり得る。

また、ping の応答についても SA46T-AS フロントエンドが返信すれば良い。

Path MTU Discovery や ping 応答は上記アプローチで対応可能と考えられる。IPsec など、その他のプロトコル等については今後の検討課題である。

8.2.IP アドレス共有ホスト間の通信は不可

一般に、ホストは自身の IP アドレス宛のパケットを外部に送信することはできない。従って、同一 IP アドレスを共有しているホスト間の通信は不可能である。これは、SA46T-AS そのものの制限ではないが、SA46T-AS の実用性に関連する事項である。サーバ間で通信するような場合、それを同一の IP アドレスを共有するがポート番号が異なるサーバを用いて実現することはできない。しかし、異なる IPv4 アドレスが割り当てられ、それら IPv4 アドレスがそれぞれ SA46T-AS で共有されるような場合は、サーバ間通信を可能にできる。

9.SA46T-AS 技術の標準化提案と実証

本技術を通じて広くインターネットコミュニティに貢献すべく、IETF に標準化提案を行っている。IETF での標準化では実装でき、動くことが重視されており、これら条件を満たすための、実装開発、実証実験等を進めている。

9.1. 標準化提案

IETF に対して、これまでに 1 件の Internet Draft[18] を提出している。はじめての提出は、2010 年 10 月 17 日で、以後、改版を行っている。

9.2. 実装

実装は SA46T の実装をベースにした。SA46T の実装規模は C 言語で約 300 ステップである。

図 4 に SA46T-AS の実装モジュール構成を示す。このモジュール構成は SA46T と同一である。SA46T と同様、CentOS5.5 をプラットフォームに用いた。具体的には、SA46T-AS のカプセル化機能、デカプセル化機能を疑似ネットワークインタフェースとしてカーネル空間に実装するアーキテクチャとした。

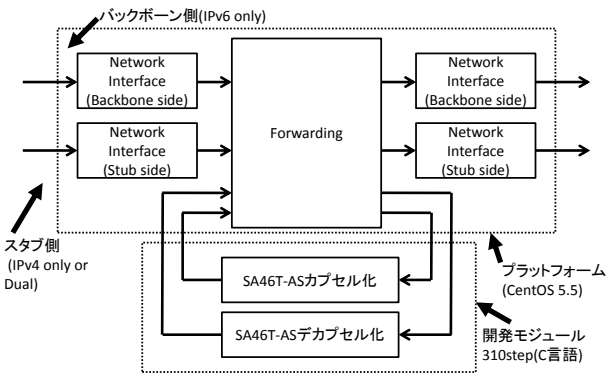

図 4: SA46T-AS の実装モジュール構成

SA46T-AS の実装は、SA46T に於いて、SA46T アドレスを生成する部分を、ポート番号を含むよう変更したのみである。具体的には、TCP と UDP で、ポート番号格納位置が異なるためその判別及びポート番号のコピーが差分で、約 10 ステップと僅かであった。合計すると 310step であり、実装はほとんど変わりがない。

9.3. 設定の考え方

SA46T-AS の実装は、SA46T-AS フロントエンド、SA46T-AS バックエンド共に同一である。その違いは設定による。以下、設定の考え方を示す。

9.3.1.SA46T-AS フロントエンドの設定

SA46T-AS フロントエンドでは、ルーティングテーブルに、カプセル化すべき宛先 IPv4 アドレスの経路に一致した場合、カプセル化を行う疑似ネットワークインタフェースに経路選択されるようなエントリを設定する。判りやすく言えば、共有する IPv4 アドレスの設定であり、その設定により SA46T-AS のカプセル化が起動される。

同様に、デカプセル化を行うネットワークインタフェースに経路選択されるようなエントリを設定するが、こちらは、デフォルト経路を設定することとなる。判り易く言えば、IPv4 パケットがカプセル化されていればデカプセル化するので、IPv4 のデフォルト経路相当を表現する IPv6 経路、つまり SA46T-AS プレフィックスを指定する。

9.3.2.SA46T-AS バックエンドの設定

SA46T-AS バックエンドでは、自身の SA46T-AS アドレスと一致したらデカプセル化を行う疑似ネットワークインタフェースに経路制御されるようなエントリを設定する。同様に、カプセル化を行うネットワークインタフェースに経路選択されるようなエントリを設定するが、こちらは、IPv4 のデフォルト経路を設定することとなる。さらに、各 SA46T-AS アドレスの経路を広告するような設定を行う。

SA46T-AS バックエンドで SA46T-AS モジュールとサーバが一体の場合、このサーバには、共有する IPv4 アドレスを割り当てる。デカプセル化され、IPv4 パケットが取り出されると、自ホスト宛のパケットとなるため、そのパケットはアプリケーションに渡される。

SA46T-AS バックエンドで SA46T-AS モジュールとサーバが別の場合、サーバには、共有する IPv4 アドレスを割り当てるが、SA46T-AS バックエンドには、サーバに割り当てる IPv4 アドレスと同一のサブネットになるような別の IPv4 アドレスを割り当てる。この設定により、SA46T-AS は、接続するサーバに IPv4 パケットを転送する。サーバから見た場合、SA46T-AS に割り当てた IPv4 アドレスがデフォルトルータとなる。

なお、SA46T-AS バックエンドには、サーバを 1 台のみしか接続出来ない。何故なら、同じ IPv4 アドレスを割り当てられたホストを同一サブネットに接続することはできないためである。裏返すと、SA46T-AS バックエンドに割り当てる IPv4 アドレスも共有できる。このアドレスは経路広告されないので、再利用可能となる。アドレスの節約にもなるし、設定の共通化も果たせる。

仮想環境でなおかつ SA46T-AS とサーバを一体化した形態が最も使い勝手が良さそうだが、物理のサーバを外付けする形態も必要となる。これは、このサーバに、SA46T-AS 機能を組み込めないような場合でも、アドレス共有を可能とするためである。

9.4. 実証実験

方式の有効性を証明するために、まずは、小規模な実証実験を Interop 2012 Tokyo でのデモンストレーションとして一般公開の場で実施した。

9.4.1. 機器構成とネットワークトポロジ

本実証実験では、サーバと SA46T-AS バックエンドを一体化したもので行うこととし、VMware ESXi 上のバーチャルアプライアンスとして実現した。なお、SA46T-AS フロントエンドについても VMware ESXi のバーチャルアプライアンスとして実現した。

FUJITSU PRIMERGY RX200S6 の IA サーバを 2 台用い、1 台で SA46T-AS フロントエンドを動作させ、もう 1 台で、SA46T-AS バックエンド込みのサーバの仮想マシンを 4 台動作させた。これらサーバには、同一の IPv4 アドレスを割り当て、かつ、ポート番号は、各 1 個のみ割り当てた。用いたポート番号は、1000 番、1001 番、1002 番、1003 番の 4 つである。

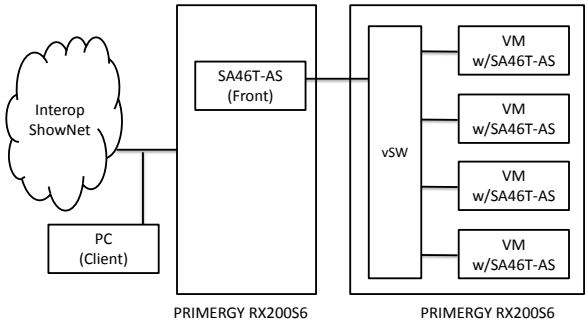

図 5: ネットワーク構成

デモンストレーション用のクライアント PC は、SA46T-AS フロントエンドの IPv4 側のサブネットに接続した。この PC からアドレス共有されたホストにアクセス可能とするために、SA46T-AS フロントエンドの IPv4 側で、Proxy ARP[19] を動作させた。

9.4.2. 設定

設定は、SA46T-AS フロントエンドと、SA46T-AS バックエンドで若干考え方が異なることは既に述べた。ここでは、具体的な設定について述べる。なお、本実証実験では、SA46T-AS の方式評価が主目的であることから、ダイナミックルーティングプロトコルは用いず、経路は全てスタティック設定とした。

SA46T-AS フロントエンドでは、

1. SA46T-AS モジュールの組み込み
2. SA46T-AS 疑似ネットワークインタフェースの up
3. SA46T-AS 疑似ネットワークインタフェースへのアドレス割り当て
4. IPv4 デフォルト経路の設定
5. IPv4 サーバ (共有アドレス) を SA46T 疑似ネットワークインタフェースに経路選択するエントリの追加
6. IPv6 デフォルト経路の設定
7. 各 SA46T-AS バックエンドへの経路情報の設定 (SA46T-AS バックエンドへの経路数分)

ここで、ダイナミックルーティングプロトコルを用いれば、7 行目の設定は不要となり、6 行のみの設定で良くなる。7 行目の設定は、ダイナミックルーティングプロトコルが自動で行う。今回は、SA46T-AS バックエンドに対応する経路数は 4 であったので、合計で 10 行の設定となった。

一方、SA46T-AS バックエンドでは、

1. SA46T-AS モジュールの組み込み
2. SA46T-AS 疑似ネットワークインタフェースの up
3. SA46T-AS 疑似ネットワークインタフェースへのアドレス割り当て
4. IPv4 デフォルト経路を SA46T-AS 疑似ネットワークインタフェースとするエントリの追加
5. IPv4 サーバ (共有アドレス) に該当する SA46T-AS アドレスを持つ IPv6 パケットを SA46T 疑似ネットワークインタフェースに経路選択するエントリの追加
6. IPv6 デフォルト経路の設定

の 6 行のみである。このうち、5 行目のデカプセル化処理を起動する際の IPv6 アドレス (SA46T-AS アドレス) の記載のみがサーバに依存して異なるが、あとの設定は同一となる。

以上のように、SA46T-AS フロントエンド、SA46T-AS バックエンド共に、このようにデフォルト経路を旨く活用することにより、設定数を少なく保つことが可能になる。

9.4.3. デモンストレーション用アプリケーション

デモンストレーション用のアプリケーションには、WWW を用いた。WWW サーバでは、そのサーバに割り当てられている IPv4 アドレスとポート番号が表示されるアプリケーションを動作させた。図 6 は、Interop のデモンストレーションの際のものではないが、その後実際に動作させて WWW サーバアクセスの画面をキャプチャしたものである。このサーバには、IPv4 アドレスは

共有の 10.21.107.222 が割り当てられ使用可能なポートは 1004 番で、なおかつ IPv6 アドレス 2001:db8:0:66::6 が割り当てられている。IPv6 でアクセスする際は、全ポート使用可能であり、ポート番号を指定すること無しにアクセスすれば良い。ウェルノウンな 80 番ポートにアクセスする。

図 6 の左側は IPv4 を用いて、右側は IPv6 を用いてアクセスしたものだが、サーバは同一であり、同じ結果が得られている。

図 6: デモンストレーションの web アクセス画面

Interop の際は、IPv4 グローバルアドレスを用いたので、Interop 会場内はもちろん、Interop 会場外からもアクセス可能であった。

10. 評価

ここでは、方式設計、実装開発、実証実験から得られた結果に基づいて、SA46T-AS 技術の評価を行う。

まず、実装可能であることを証明した。そして、この実装を用いて、仮想環境で、サーバ台数 4 台と小規模ながら実証実験を行い、成功した。これらを通し、方式の有効性を証明出来たと言える。

特に、サーバに於いて、IPv6 ならフルアクセス可能だが、IPv4 の場合、ポート番号制限があるものの IPv4 グローバルアドレスで指定できることを両立できたことを実証できたことは重要である。

本実験では負荷を掛ける等の実験は行わなかったが、SA46T と比べさほど違いが無いことから、SA46T 相当の性能は達成できると考えられる。むしろ、大規模に展開するための技術が今後の鍵となると考えられる。

11.SA46T-AS を用いたサービスの展望

IPv4 アドレスが枯渇する前に IPv6 が普及し、IPv4 を置き換えられることが理想的である。実際、このような移行がなされる可能性もある。このような移行、つまり、実際に IPv4 アドレスが枯渇する状況が発生しなければ、SA46T-AS の出番は訪れないかもしれない。実は筆者は、インターネットの健全な発展のためには SA46T-AS の出番が来ないことが望ましいと考えており、その意味で、SA46T-AS を保険的な技術と位置づけている。

しかし、IPv4 アドレスが実際に枯渇し、それでも IPv6 が普及していない状況も想定できる。このような状況に陥れば、SA46T-AS が役立つ可能性が高まる。この段階になれば、より具体的な用途が問われることになるだろうが、その可用性は、技術の汎用性が支えることとなる。

IPv4 アドレス枯渇の抜本解は IPv6 である。IPv4 アドレス共有でしのぐために、SA46T-AS を利用するためにも IPv6 が必要となる。いずれにせよ、IPv6 は欠かせない。そのため、SA46T-AS は、IPv6 の移行と、IPv4 の継続利用を両立する技術と言えそうである。IPv6 が導入されていなければ、SA46T-AS の利用もできない。移行が順調に進むにせよ、そうでないにせよ、IPv6 を導入しておくべきである。

さて、本技術はサーバを対象としているので、主として貢献できるのはデータセンターである。サーバに於いては、必ずしも全てのポートを使っている訳ではないので、まず最初に、ウェルノウンなポート番号だけを対象にしてサーバを分離するのは有効な手段かもしれない。具体的に、WWW サーバは 80 番ポートがあれば良く、FTP サーバは、20 番ポートと 21 番ポートがあれば良い。このサーバは、サービスによって物理サーバを分離出来るし、NAT を用いないので FTP もそのまま通る。

まずは、このような運用から開始し、SA46T-AS の実績が得られれば、ウェルノウン以外のポート番号を用いた共有に展開するのも容易になるであろう。

このような段階的な運用を想定すれば、仮想サーバの提供方法にも、いくつかのオプション、あるいはサービスメニューを用意できることが明らかになる。

1. IPv4 グローバルアドレスのみ (IPv4 only)
2. IPv6 グローバルアドレス及び IPv4 グローバルアドレス (Dual Stack)
3. IPv6 グローバルアドレス及び IPv4 の特定ウェルノウンポートのみに制限
4. IPv6 グローバルアドレス及び IPv4 の非ウェルノウンポート数個
5. IPv6 グローバルアドレスのみ (IPv6 only)

上記に於いて、3 及び 4 が SA46T-AS で提供可能なオプションである。SA46T-AS が無ければ、IPv4 only, Dual Stack, IPv6 only しか提供できない。IPv4 アドレスが枯渇したら、IPv6 only しか取り様が無くなるのである。

SA46T-AS は、IPv6 グローバルアドレス及び IPv4 グローバルアドレスだが利用可能なポート数数個、というオプションを提供できる。IPv4 アドレスの有効活用のために、IPv4 アドレスが枯渇する前からポート番号数数個のオプションを用意することは有効かもしれない。IPv4 によるポート番号制限が無いものに比べ、ポート制限があるものの方が安価であれば、ポート制限されていてもそれで十分なサービスが利用する可能性もある。そうなれば、IPv4 アドレスの消費速度を遅くできる可能性もある。

いずれにせよ、このようなオプションを提供可能とするためにも、まずは、IPv6 を導入することが欠かせないと言える。

12. まとめ

IPv4 アドレス枯渇後の IPv4 アドレス共有技術として SA46T-AS を提案した。そして、実装を開発しそれを用いた実証実験を通じ、方式の有効性を実証した。

次に実証すべきは大規模化など運用技術と考えている。もし、IPv6 への移行がなかなか進まず、SA46T-AS による IPv4 の継続利用が必要になった際は、具体的にアプリケーションを絞った動作検証が必要になると考えられる。

枯渇の状況を見ながら、インターネットの健全な発展に寄与すべく、今後も標準化、実用化、そして普及に向けて、取り組んでいく所存である。

謝辞

SA46T 及び SA46T-AS の開発、及び実証実験で協力頂いた (株) 富士通コンピュータテクノロジーズの御手洗正道氏、蛭子恵一氏に感謝します。また、実証実験にあたり、様々なご支援を頂きました、Interop Tokyo 2012 ShowNet NOC チームの皆様に感謝します。

参考文献

[1] *"IPv4 Address Report"* `http://www.potaroo.net/tools/ipv4/index.html`

[2] 松平直樹 *"SA46T:IPv4 アドレス枯渇後の IPv6 移行と IPv4 継続利用を両立するカプセル化技術"* IC2012, 2012 年 11 月

[3] N. Matsuhira *"Stateless Automatic IPv4 over IPv6 Encapsulation / Decapsulation Technology: Specification"* draft-matsuhira-sa46t-spec-06.txt, Internet-Draft, January 2013

[4] K. Egevang, P.Francis *"The IP Network Address Translator (NAT)"* RFC1631, May 1994

[5] W. Simpson, Editor *"Point to Point Protocol"* RFC1661, July 1994

[6] R. Droms *"Dynamic Host Configuration Protocol"* RFC2131, March 1997

[7] R.Bush, ED. *"The Address plus Port (A+P) Approach to the IPv4 Address Shortage"* RFC6346, August 2011

[8] S. Kent, K. Seo *"Security Architecture for the Internet Protocol"* RFC2401, December 2005

[9] B. Carpenter, Editor *"Architectural Principle of the Internet"* RFC1958, June 1996

[10] T.Hain *"Architectural Implications of NAT"* RFC2993, November 2000

[11] 佐藤良 "「IPv6 時代の IPv4 を考える」〜第二章〜 共存/移行技術と P2P 対戦ゲームの相性" JANOG30, 2012 年 7 月

[12] F. Audet, Ed. *"Network Address Translation (NAT) Behavioral Requirements for Unicast UDP"* RFC4787, January 2007

[13] J. Postel, J. Reynolds *"FILE TRANSFER PROTOCOL (FTP)"* RFC959, October 1985

[14] J. Rosenberg et. al. *"SIP: Session Initiation Protocol"* RFC3261, June 2002

[15] K. Hamzeh, G. Pall, W.Verthein, J. Taarud, W. Little, G. Zorn *"Point-to-Point Tunneling Protocol (PPTP)"* RFC2637, July 1999

[16] J. Postel *"INTERNET CONTROL MESSAGE PROTOCOL"* RFC792, September 1981

[17] J.Mogul, S. Deucing *"Path MTU Discovery"* RFC1191, November 1990

[18] N. Matsuhira *"Stateless Automatic IPv4 over IPv6 Tunneling with IPv4 Address Sharing"* draft-matsuhira-sa46t-as-00.txt, Internet-Draft, October 2010

[19] Smoot Carl-Mitcgell, John S. Quarterman *"Using ARP to Implement Transparent Subnet Gateways"* RFC1027, October 1987