IPv6時代のIPv4アドレス共有技術

「ステートフル方式」と「ステートレス方式」。
これらのアドレス共有技術にどのような特徴があるのか概観し、IIR Vol.13[*1]でご紹介した
SEIL[*2]シリーズによる4rd試験実装の経験をふまえてIPv4アドレス共有技術の現状をご紹介します。

3.1 IPv4アドレス枯渇後の世界

既に発表されたとおり、IANA(Internet Assigned Numbers Authority)[*3]の保有するIPv4アドレスの在庫は2011年2月3日に尽き、次いで2011年4月15日にアジアのRIR(Regional Internet Registry)であるAPNICにおいても在庫がなくなりました。これを受けてJPNICが提示した対応策[*4]は、以下の3つの軸からなります。

1. 分配済みのIPv4アドレスについて、効率的な利用を推進
2. NAT技術を利用し、グローバルアドレスを使わずに新たなホストを収容
3. IPv6を導入し、新たなホストを収容

3.のIPv6への移行が根本的な解決策であるとされていますが、現時点ではビジネスの大半はIPv4上で行われており、1.及び2.の対策が早急に必要です。1.については、大量のアドレスを保有する組織ではアドレス空間の整理が積極的になされており、ある程度大きなアドレスブロックであれば組織間での移転も可能となりました。グローバルアドレスがどうしても必要となるケースについては、この枠組を利用することになるでしょう。今までと比較すると時間もお金もかかりますが、アドレスを取得できてしまえば差異はあまりありません。クライアントでの利用については2.の対策によりグローバルアドレスの消費を最小限に抑えつつインターネットに接続できる可能性があります。

3.2 ステートフル方式？ステートレス方式？

IPv4の大規模なアドレス共有技術の最古参としてCGN/LSN[*5]があります。CGN/LSNでは、ISPがIPv4グローバルアドレスを直接配布する代わりにNAT変換した後のプライベートアドレスを配布することで、IPv4グローバルアドレスの消費を最小限に押さえます。CGN/LSNの利用モデルとして、IPv4のアクセス網を利用する「NAT444[*6]」、IPv6のアクセス網を利用する「DS-Lite[*7]」が標準として合意されつつあります。

これらCGN/LSN系列の技術に対して、「ステートレス方式」と呼ばれるアプローチが多数提案され、定期的に話題になっています。ステートフル対ステートレスという大雑把な区分については、耳にしたことがある方も多いと思います。「ステートレス方式」は現在多数の提案が存在し、標準化の行方はまだ見えない状況ですが、何らかの標準が合意されることは間違いなさそうです。

本稿では、IIR Vol.13でご紹介したSEILシリーズでの4rd試験実装の経験から、CGN/LSNのような「ステートフル方式」と、4rdのような「ステートレス方式」にどのような特徴があるのかを概観し、ルータ開発者の視点からIPv4アドレス共有技術の現状をご紹介します。

＊1　IIR Vol.13「インターネットトピック：IIJ独自ルータ『SEIL』における4rdの実証実験」(http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol13.pdf)。
＊2　ISPのノウハウを結集してIIJが開発した高機能ルータ「SEIL(ザイル)」のポータルサイト(http://www.seil.jp/)。
＊3　ICANNが運用するインターネット資源の管理、調整機能。
＊4　「IPv4アドレスの在庫枯渇に関して」(http://www.nic.ad.jp/ja/ip/ipv4pool/)。
＊5　CGN = Carrier Grade NAT, LSN = Large Scale NAT。ISPでIPv4アドレスのNAT変換をする仕組み。CGNもLSNの2種類の用語が提案されているが同じ技術を指す。
＊6　"NAT444 addressing models draft-shirasaki-nat444-isp-shared-addr-07"(http://tools.ietf.org/html/draft-shirasaki-nat444-isp-shared-addr-07)。
＊7　"Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion"(http://tools.ietf.org/html/rfc6333)。

3.3 各方式を比較する試み

各IPv4アドレス共有技術の比較検討をする際、ステートフル方式とステートレス方式という区分がよく使われます。この区分は技術の詳細を比較する上では必ずしも十分とは言えません。そのため、詳細に技術を比較する際には、以下の軸を加えて議論されることが多いようです。

- NAT装置は、どこに配置されるのか？
- 通信主体の識別は、どのように行うのか？
- 顧客同士の通信手段は、どうなるのか？
- パケットフォーマットは、どうするのか？

3.3.1 NAT装置の配置を考える

NAT装置の配置（図-1）は、ステートレス方式、ステートフル方式という区分にもっとも近い尺度です。選択肢としては、ISPに配置するか、顧客ネットワークに配置するか、その両方か、の3つがあります。ISP側にNAT装置を配置する場合、ISPは巨大な共有資源をまとめて管理する必要がありますが、細かな制御が可能となります。顧客ネットワークにNAT装置を配置する場合、ISPでの資源管理は簡略化できますが、その分柔軟性は低くなります。

3.3.2 通信主体の識別方法を考える

不正アクセスを検知したような場合に、問題となる通信主体がログから識別できるかどうかはISPやサーバの運用管理者にとって重要な問題です。アドレス共有が行われる場合には、IPアドレスの記録からだけでは通信主体は識別できないため、ポート番号を誰が使っていたのか追跡する仕組みが必要になります。

ステートフル方式ではこの作業にNATセッションの情報が必要となり、ステートレス方式では静的な割り当てルールがあれば十分であることが、両者の大きな違いの一つと言われています。

3.3.3 顧客同士の通信手段を考える

顧客同士がどのように通信できるかは、IP電話のようなP2P通信において特に重要となります。P2P通信は本質的にNATとは相性が悪い技術ですが、現在では様々なNAT超え技術により実用的に利用されています。この既存のNAT超え技術が引き続き利用できるのであれば、通信の効率化が期待できます。遠隔会議アプリケーションがP2P通信モードで動作するか、中継サーバ経由で動作するかでは、ネットワークの利用効率もユーザの快適性も大きく変わってくるでしょう。

3.3.4 パケットフォーマットを考える

パケットフォーマットは、大まかにはIPv4パケットをそのままIPv4ネットワークで転送するか、IPv6にトランスレートしてIPv6ネットワークで転送するか、IPv6でカプセル化してIPv6ネットワークで転送するか、という選択肢が考えられます。IPv6を利用すると、IPv4アドレスが重複していたとしても、IPv6のアドレス情報をヒントに適切なネットワークに配送することが可能となります。これによりNAT装置の設置場所を柔軟に選択できます。

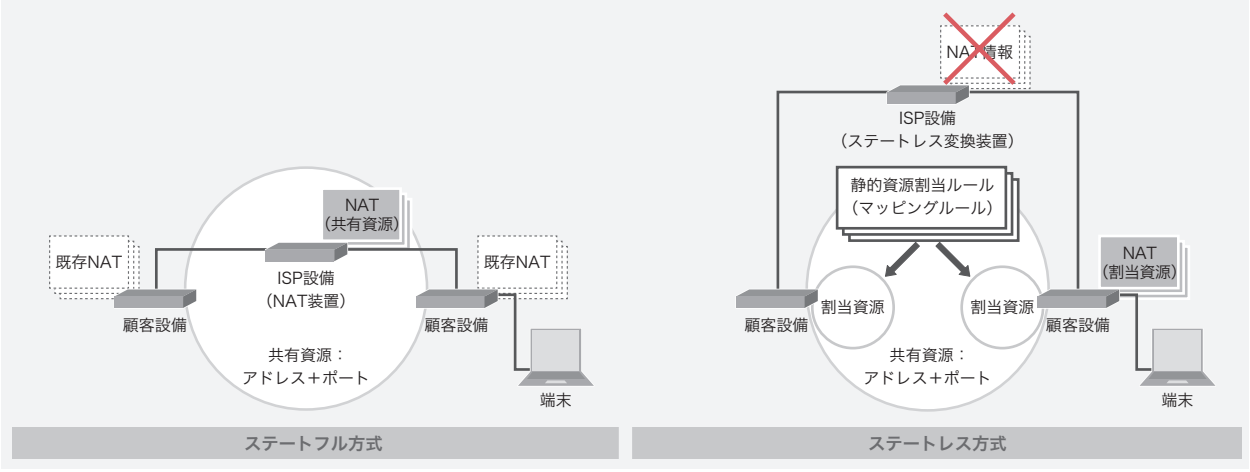

図-1 NAT装置の配置

3.4 ステートフル方式を概観する

ステートフル方式に分類されるアドレス共有方式の代表としてNAT444とDS-Liteをピックアップして比較してみました(表-1)。

3.4.1 ステートフル方式の具体例：DS-Lite

CGN/LSMベースの技術で、IPv6アクセス網を利用する技術です。ISPのCGN/LSN装置とCPEとの間をIPv4 over IPv6トンネルで結びます。NAT変換においては、表-2のようなIPv6グローバルアドレスを含めた変換を行います。

CPEからアクセス網にパケットを転送する際にはIPv6によるカプセル化を行うのみで、CPEでのNATは必要ありません。インターネットからの戻りパケットは、NATセッションに記録されたIPv6グローバルアドレスを利用してIPv6でカプセル化します。IPv6アドレスによりCPEを区別できるため、CPEのプライベートアドレスは、ISP内で重複していても構いません。

3.5 ステートレス方式を概観する

ステートレス方式は、現在のところ多数の提案が平行しており、どの方式が最終的に残るのかは不明です。ここでは、2011年11月のIETF 82で触れられた方式をピックアップしました(表-3)。

表-1 アドレス共有方式(NAT444、DS-Lite)

方式	アクセス網	NAT	通信主体の識別	顧客間通信	パケット形式
NAT444	IPv4	ISP、顧客	NATセッション情報を参照	ISP側機器を経由*8	IPv4 native
DS-Lite	IPv6	ISP	NATセッション情報を参照	ISP側機器を経由*9	IPv4 over IPv6 tunnel*10

表-2 NAT変換

プライベート側(CPE)	グローバル側(IPv4 Internet)
IPv6グローバルアドレス IPv4プライベートアドレス ポート番号	IPv4グローバルアドレス ポート番号

表-3 ステートレス方式

方式	アクセス網	NAT	通信主体の識別	顧客間通信	パケット形式
4rd-E*11	IPv6	顧客	静的ルール ・プリフィックス×2 ・整数値×1	直接可能	IPv4 over IPv6 tunnel
4rd-U*12	IPv6	顧客	静的ルール ・プリフィックス×2 ・整数値×1	直接可能	IPV4 - IPv6 double translation w/ IPv6 option header
SA46T-AS*13	IPv6	顧客	静的ルール ・整数値×2	直接可能	IPv4 over IPv6 tunnel
dIVI*14	IPv6	顧客	静的ルール ・整数値×2	直接可能	IPv4-IPv6 double translation
SD-NAT*15	IPv4 IPv6	顧客(ISP)	静的ルール ・アドレス×2 ・整数値×2	ISP側機器を経由	IPv4 native IPv4 over IPv6 tunnel
Stateless 4over6*16	IPv6	顧客	静的ルール ・dIVI準拠	ISP側機器を経由*17	IPv4 over IPv6 tunnel

*8 ただし、NATが多段となるため既存のNAT越え技術は適用が困難である。
*9 拡張仕様も標準化をしている。
*10 特定のパケット形式は仮定していないが、典型的なケースとして単純なIPv4 over IPv6 tunnelが考えられる。
*11 http://tools.ietf.org/html/draft-murakami-softwire-4rd-01
*12 http://tools.ietf.org/html/draft-despres-softwire-4rd-u-02
*13 http://tools.ietf.org/html/draft-matsuhira-sa46t-as-02
*14 http://tools.ietf.org/html/draft-xli-behave-divi-04
*15 http://tools.ietf.org/html/draft-penno-softwire-sdnat-01
*16 http://tools.ietf.org/html/draft-sun-softwire-stateless-4over6-00
*17 経路を最適化する装置を追加することも可能である。

ステートレス方式では、通信主体の識別の際にISPは静的に決めたルールを参照します。これによりNATセッションの記録が不要となるため運用コストが下がります。現在のところ、ルールの定義の仕方は各方式の特徴の一つとなっていますが、個々の方式とは独立して標準化する動きもあります。

3.5.1 ステートレス方式の具体例：4rd(4rd-E)

ここでは、SEILで試験実装を行っている4rd(4rd-E)を例にとり、ステートレス方式と呼ばれている仕組みの具体的な動作を簡単に追ってみます。

4rdでは、CPE(4rdの用語ではCE)はIPv6アクセス網に接続されており、IPv6グローバルアドレスが付与されます。同時に、CPEにはIPv4グローバルアドレスとIPv4通信で利用可能なポート番号の範囲も付与されます。付与されたIPv6アドレスの一部には、顧客の識別子(EA-bits)が埋め込まれています。また、IPv4グローバルアドレスとポート番号にまたがるように、IPv6と同様の識別子が埋め込まれています。この識別子(EA-bits)、IPv6グローバルアドレス、IPv4グローバルアドレス、ポート番号の静的な対応関係が4rdにおけるマッピングルールとなります。このIPv4グローバルアドレスは異なるCPE間で共有することがありますが、ポート番号を組み合わせるとCPEを一意に識別できます。

IPv4のネットワークでポート番号を参照して経路を選択することは、一般的には不可能です。そこで、4rdではパケットの配送にIPv6を利用します。先に述べたようにCPEの「IPv4アドレスとポート番号の組」と「IPv6アドレス」は静的な対応関係にありますので、変換後の「IPv6アドレス」を利用してパケットをカプセル化することで、IPv4パケットのポート番号に基づいた経路選択を実現します。

■ 4rdにおけるNAT

CPEには、IPv4グローバルアドレスとポート番号が割り当てられます。このリソースをCPE配下の端末で共有する段階で、NAT(NAPT)を利用します。通常のIPv4 NATとは、ポート番号の割り当てに制限があるという点が異なります。それ以外は従来のNATと異なるところは特にありません。

■ サーバログの解析

サーバに残されたIPアドレスとポート番号から通信主体を知りたい場合、必要な情報はマッピングルールと、IPv6アドレスの払い出し情報です。前者はアクセス網に固有の設定値で、動的に変化するものではありません。後者はアクセス網の接続ログを参照することで判明します。接続ログについては、現在のIPv4接続ログと同じ仕組みでログ管理が可能です。

3.6 おわりに

駆け足となりましたが、IPv4のアドレス共有技術について特徴的な箇所をピックアップしてみました。今後の標準化により変わる部分も多数あると思いますが、本稿が将来のIPv4環境について思いを巡らすきっかけになれば幸いです。

執筆者:
末永 洋樹（すえなが ひろき）
IIJ SEIL事業部 製品開発部 製品技術課 テクニカルマネージャ。2004年入社時より、一貫してSEILシリーズ及びSMFv2の開発に従事。NGNを見据えた研究開発の1つとして、4rdの試験実装と実証実験に携わっている。