大規模NAT（Large Scale NAT:LSN）あるいはキャリアグレードNAT（CGN）

今回の10分講座は、IPv4アドレスの在庫枯渇の時期が迫るとともに注目を集めている大規模NATあるいはキャリアグレードNATと呼ばれる技術について解説します。

■IPv4アドレス在庫枯渇とスムースなIPv6移行に向けて

最近、あちこちで言われていることではありますが、IPv4アドレスの新規割り当てが、あとどんなに遅くても数年以内には、非常に困難になるであろうという予測は、やはり残念ながらと言うべきでしょうけれども、だんだんと確定的になってきています。

もちろん、この問題への根源的な対策は、インターネット全体をIPv6へと移行させることであることはまったく論を待ちませんが、その一方で、既に実社会に広く深く浸透している既存の設備や運用といったものを一気に変更することも、現実的とは言えません。

筆者は、長年IPv6プロトコルの開発および実装・標準化に関連した仕事をさせていただいており、IPv6という技術自体はおおよそ完成した技術であると思っているのですが、それであればこそ、今こそ、どのようにしたら既存のインターネットを現実的な手順でIPv6対応へと移行できるのかという問題に、一定の解答を与えたいと考えています。今回ご紹介するキャリアグレードNAT（Carrier Grade NAT:CGN）あるいは単に大規模NAT（Large Scale NAT:LSN）と呼ばれる技術は、その中でとても重要な役割を果たす可能性があります。

■完全IPv6化への遠い道

さて、近日中にIPv4が限界に達したとして、その代替手段であるIPv6という技術を搭載している機器は、現在どのくらい普及しているのでしょうか？

例えば、既に、皆様の手元のPCやサーバが、BSDやLinux、あるいは、SolarisやHP-UNIX、AIXなどといったものであれば、ほぼ間違いなくIPv6を使うことができます。

一方、主要なルータは、かなり前からIPv6対応をうたっている物が多く、また、Windows Vistaは、IPv6がデフォルトでONになっており、IPv4機能をGUIを使って削除することができる反面、IPv6を止めるのはとても難しいOSです。

そして、これらのような最新のIP機器では、IPv6「だけ」での動作も可能であることが普通です。しかしながら、だからといって問題が解決するわけではありません。

まず、サーバのほうからいきましょう。

サーバ本体やルータは大丈夫としても、実は、いまだにファイアウォールやロードバランサーの機器といった類は、IPv6に対応していないものが多く、たとえ対応していても、IPv4はハードウェア処理でもIPv6はソフトウェア処理に留まるなど、機能上の制限やパフォーマンス上の問題を持っている場合が多いようです。

となると、例えば、実際に現在使っている機材のソフトウェアを最新にするなどして、あるWebサービスをIPv6対応させようと思っても、十分なIPv6対応ができないという事態が考えられます。

また、使用する機器がすべてIPv6に対応していたとしても、URLやCGIなどにIPv4アドレスの数値が入ってくることが暗黙の内に仮定されていたり、バックエンドで動いているデータベースがログをIPv4でしか対応していないといった、「コンテンツのIPv6対応」ができていない場合も考えられます。

また、DNSサーバのコンフィギュレーションも問題です。時代の最先端を行くサイトはもちろん違いますが、世の中のほとんどのDNSサーバにおいて、それをIPv4でもIPv6でもアクセスすることができ、すべてのアドレスがAAAAとAの両方のレコードを持っているということは、まず期待できません。

すなわち、「サーバ側のIPv6対応はまだまだ途上である」ということになります。

言い換えれば、インターネット上のサーバが、ある短い期間の間にIPv6に対応することが極めて難しいのです。

一方で、クライアントはどうでしょうか。

先に述べましたように最新のOSであるVistaは、IPv6はきちんと対応しているのですが、同時にセキュリティ機能が高く、大変に良いOSではあるものの、それであればこそ、CPUに高い性能を要求するものとなっており、最近、非常に人気の高い5万円以下のPCでは、Vistaではなく、Windows XPベースのOSを搭載して販売されているものが大変多く見受けられます。

これが、問題をややこしくします。

実は、Windows XPそのものは、現在SP3となっていますが、IPv6に対応しています。ですが、この「対応」というものがくせもので、HTTPなどの通常のTCP通信はIPv6で行うことができるのですが、名前解決に使うDNSシステムが、IPv4でしか通信できないようになっています。すなわち、IPv6の通信に先立つ名前解決は、IPv4の中でしなければならないのです。

例えば、www.afo.comというDNS名がIPv6アドレスとしてのAAAAレコードを持っていたとしても、そのAAAAレコードに対するクエリ自体はIPv4の通信で行うということです。

では、Windows XP以前のOSが使用停止となり、Windows Vista以後のOSだけを相手にすれば実効上問題ないということが言えるのは、いつのことになるのでしょう。

筆者の知る限り、西暦2009年の現在でも、Windows 2000を現役で使用しているサイトは非常に多いですし、Windows 98などの古いOSを使い続けている人もまだいると思われます。

となると、自然な類推としては、あと10年くらい、すなわち2020年くらいまでは、Windows XPを端末として仮定する必要があると思います。

このように、サーバ側、また、クライアント側のIPv6への移行には、まだまだ問題があるにもかかわらず、一方で、IPv4の在庫枯渇時期をどんなに遅く見積もったとしても、古いマシンを引退させることのできる2020年という期限の数年前には、IPv4アドレスの新規割り当ては不可能になってしまっていると考えざるを得ず、まさに「あちらを立てればこちらが立たず」ということになっており、問題が非常に深刻であることがわかります。

■IPv4「延命」とIPv6への段階的移行の同時進行こそが解

このような状況では、IPv4の「延命」を考えないと、大変な資産の無駄が発生してしまうことがわかります。

仮に、インターネットを運用している世界中の主要なISPが合意を形成し、IPv4アドレス割り当てが不可能になる以前の、ある近未来の日付をもってIPv4通信の停止を決定するというシナリオは、すなわち現在販売されているPCのインターネット通信機能をあっという間に奪うことにもなりかねず、まったくもって現実的ではありません。

すなわち、IPv4を何らかの形で機能制限してでも延命を行うと同時に、一刻も速いIPv6の展開を実施することが、唯一の解なのです。

では、IPv4の延命とはどのようなものなのでしょうか？

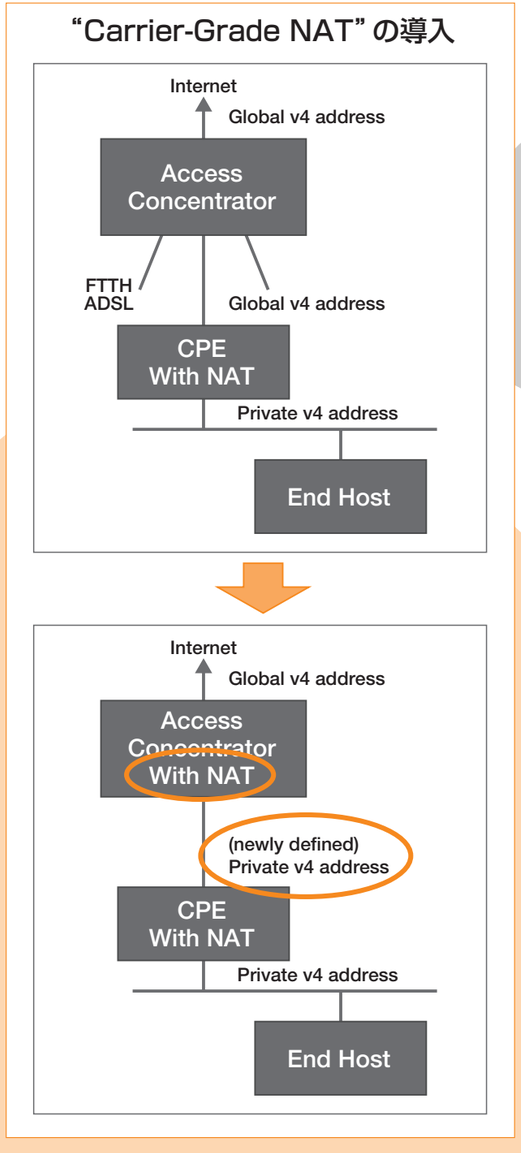
非常に簡単な答ですが、それは「共有」ということにつきます。すなわち、今まで一つのマシンに割り当てられていたIPアドレスを、複数のマシンで共有することです。

例を挙げると、一つのFTTH回線に一つのグローバルアドレスが今までだとしたら、これからは、複数のFTTH回線に一つのグローバルアドレスを割り当てる、ということです。

大規模NAT（Large Scale NAT：LSN）あるいはキャリアグレードNAT（CGN）

つまり、NATを上流に入れることが必要になる、というアイデアです。このアイデアは、FTTHやADSLの集約装置のところに大規模なNATを設置することから、キャリアグレードNAT（CGN）あるいは単にLarge Scale NAT（LSN）と呼んでいます（図1）。

図1：キャリアグレードNAT



※ CPE…Customer Premises Equipment

■LSN（CGN）には限界があるし、どうも高価になりそうだ

LSNを導入することにより、残り少なくなったIPv4アドレス空間を、より多くのユーザーで使うことができるようになります。

しかし、いまだに勘違いする方がたくさんいらっしゃるので、ここで大変に大事なポイントとして申し上げておきたいことは、LSNを使うと、NATを通過するトラフィックは、さまざまな障害に直面しますので、アプリケーションの利用に深刻な影響がでることが予想されるのです。

まず最初に認識すべきは、一つのマシンで同時に使用できるTCPの数には限界があるということです。

TCPのPort番号は2byteですので、同じ行き先アドレス、同じポート番号に対しては、一つの始点IPアドレスからは、最大で6万5,000強のセッションまで扱えるということになるのですが、この6万5,000を、共有するユーザー数で割算することになることから起因する問題です（ここでは仕様上の制限としての非常に厳密な言い方をしていますが、実際の実装では複数の行き先アドレスに対して、同じポート番号を使えないものもあるので、より厳しい割り当てとなる可能性もあります）。

ここで、仮に一つのIPアドレスを4,000ユーザーで共有することにしましょう。そうすると、6万5,000を4,000で割りますので、1人あたりは約16個のセッションが割り当てられることになります。

最近のリッチなWebページは、Ajaxの機能を利用して多数のTCPを同時並行的に張ることにより、高速でスムースな動作をさせているものがたくさん見受けられます。図2に、このような例として、我々の実験環境で、TCP数を15に制限するデバイスを通過させた通信環境において、Google社の地図を見ている様子を示します。

右図の図2からおわかりいただけるように、四角い空白がいくつも出てしまい、実用に耐えるとはとても言い難い状態です。

一つの四角形を表示するのに一つのTCPが使われているものと思われますが、TCPの同時制限数に引っかかってしまい、表示ができなくなる部分があるのです。我々の調査では、有名なWebページの中には、数十から、中には数百のTCPを同時に使用するものも見受けられるため、そのようなページの表示に深刻な支障が出ないように、共有するユーザー数を小さくする（例えば10ユーザーで共有することで6,500セッションを確保する）といったことが必要になりますが、その場合、IPv4が「いつまで」延命できるかという余命が短くなるという欠点と出てしまうので、頭の痛いところです。

また、多くのアプリケーションをスムースに透過させるために、NAT透過性に気をつけた実装にする必要もあり、まだ市中製品で完成された域に達したものはないのですが、我々が見聞きしているところでは、非常に高価な製品になってしまいそうな雲行きでもありますので、ベンダーの方により一層の努力をいただかなくては、実用化できない、という危険性もあります。

■なるべく早いIPv6の導入を。LSNは単なる「つなぎ」の技術です

したがって、IPv6の導入により、制限のある環境からの脱出と、低コスト化を同時に達成できることになりますので、かならずLSNの導入にあたって、IPv6への移行を強く念頭においたプランにする必要があるということを、忘れないでいただきたいと思っています。

我々の考える一つの道筋として、より詳細なストーリーにつきましては、筆者が2008年にダブリンで開催された第72回IETFのテクニカルプレナリで行った発表がありますので、そちらをご参照ください。

また、我々の考えているLSNの実装以外にも、CPEデバイスをIPv6対応にすることと同時にIPv4もサポートするテクニックとしてA+P（Address + Port）、Dual Stack Liteなどと言われている提案もありますので、あわせてご参考にしてください。

■ 参考

・標準化について
LSN（CGN）の標準化はIETFのBEHAVEおよびInt-AREAにおいて行われています。
http://www.ietf.org/html.charters/wg-dir.html
から必要なリンクを辿ってください。

・IETF72での宮川の発表資料
http://www.ietf.org/proceedings/08jul/slides/plenaryw-2/sld1.htm

（エヌ・ティ・ティ・コミュニケーションズ株式会社　宮川晋）

図2：TCP数を15に制限した状態でのGoogle Mapsの表示例