JANOG23 DAY2

「IPv4/IPv6 共存環境におけるサービス移行 私たちは今何をすべきか」議論ログ

議論の目的

検証、サービスなどの経験談などの各種問題点を JANOG で共有することで IPv6 のサービス対応をスピードアップする。皆が同じ体験談を共有することで、迅速に展開していきたい。

経験談

- デュアルスタックの SMTP サーバを運用していたら、ある特定の IPv4 Only のサーバからメールが届かなかったりしたことがある。これは設定次第で MX レコードの設定で回避することが可能であるが不思議な現象である。デュアルスタックで運用する人は要注意。

- /48 の IPv6 環境下で PC にスタティックでアドレスを書くと通信できるが RA は聞いてくれなかった。アナライザでパケットを見ると/48 の RA は出している。
  プロトコル上は記述可能であるが/64 でしか聞いてくれない。WindowsXP も Mac も/64 でしか聞いてくれない。RA は/48 で出してはいけない。

- IPv4 サーバの前にトランスレータ、ロードバランサーなどミドルボックスをおいてクライントからの IPv6 アクセスを IPv4 に変化しサーバにアクセスした場合、サーバ側で IPv6 のソースアドレスが分からなくなる。
  Web サービスを提供する場合はアクセスログを出すが、ソースアドレスなどで制御する場合があるので、接続元の IPv6 アドレスが分からない場合はサービスレベルを IPv4 と同等のレベルで提供するとした場合、致命傷になると思う。
  また、接続元のソースアドレスを Web 以外のメールなどのプロトコルで箱を使ってアドレス変換をする場合は、ミドルボックスとサーバのログを突き合わせてチェックするのは大変なので考える必要がある。

  - IPv6 に対応した初期のころは量が少ないハズなのでログの突き合わせで何とかなると思っているが、IPv6 アクセスが増えてきた場合のことを考えると、初期と本格的な対応でフェーズを分けて考える必要があると思っている。

- 今の Web サービスホスティング事業者に限らずインターネットとの接続に関して、ログを採るということはクリティカルに要求されているので、最初の実装から取り入れてほしいという声を積極的に上げていきたい。
  初期の段階でサービスを作る人、社内、コミュニティ、ベンダー、メーカなどに「こういうことができないとこの先やっていけない」と相談することが重要で急務であると考えている。

- ログの省略形はログを取得する際にどのような表現、標記方法が良いのか？
  「::」にすればよいのか？「0000」にすれば良いのか？それとも両方？
  RFC にはなっていないよね？Web のアクセスログは省略系がまちまち。

  - アドレスの表現形式を正規化するライブラリ、フィルタなどで対処しては如何？

- サーバ OS あるいはサーバとして動作していてプロトコル上はクライアントとして振舞うことがある。例えば、メールサーバが相手にメールを送るときは送る側はメールクライアントになる。その時に、DNS を引いて AAAA があると IPv4 でもアクセスできたとしても IPv6 が優先されることが多いが、現実的には IPv4 のネットワークの方が IPv6 ネットワークよりしっかりしている場合が多いので、そういう場合はアプリケーション、スタックを少し改造している。

- OSPF は IPv6 では Authentication に IPSec を使うが、異なるベンダー（機器）間でのインターオペラビリティが少し良くない。neighbor が上がらないことがあるので注意が必要。ベンダーさんに異機種間でもつながるように調整していただきたい。

- 一部ルータで Path MTU Discovery を行なわないものがある。自発のパケットで問題になるので iBGP などで網内の MTU が異なる場合は特に注意が必要。

- イベントなどで IPv6 の環境を作る際に重要なのは RA の監視。
  オレオレ RA が発生し、通信可能な人と不可能な人が発生し騒ぎ出す。

- IPv6 対応のコード（アプリ）を作った時、テストをどのような環境でやればいいのか分からない。今まではルータ 1 台かませてクライアントのテスト環境で良かった。IPv6 の場合のモデル的なテスト環境が分からないので情報をして頂けるとありがたい。また、推奨、モデル的なテスト環境はあるのか？

- 参考までに、IPv6 協議会 サービス移行 SWG 第 1 回テストの環境は Web に掲載されているので参照お願いします。

- ICMP を止めないで下さい。
  デュアルスタックで SMTP を運用しているときに特定のところに通信できなかった。メールの場合、短いメールは届くが大きなメールは届かないことがあった。これは要注意。

- ちょっと古い CentOS などでは突然、デフォルトルートが消える、動かなくなることがあるバグがある模様。netstat などで経路情報を見てもデフォルトルートは設定されているが、フォワーディングテーブルも設定されているが、デフォルトルートにパケットが飛ばない。リブートしないと解決しなかった。

  - 数ヶ月以内にリリースされるものは改修されていると期待している。

- IPv6 環境に不用意に機器を接続してうっかり RA を送出してしまうと知らないうちにルートを奪ってしまったり、アドレスがついちゃったり。
  そのセグメントに接続していると気が付かないうちに複数のプレフィックスが付いている。

  - デフォルトで RA は聞かない設定を入れるべき

- IPv4 で ARP を見るコマンド名はどの装置でも「arp」でだいたい統一されているが、IPv6 のそれ相当のコマンドはバラバラである。オペレーションしている際は知っているので困ることはないが、お客さまとの会話などの際は、解説に困る。Neighbor Discovery と言ってよいのか？上手い伝え方がないのか？日々悩んでいる。会話で苦労している。

- 先にログに関わる話題があったが・・・
  Web サーバ、トランスレータなどのログの一致は絶対に必要。
  事業の証拠・証跡を追うためにはログがないと困る。
  更に言えば、事業に関わるところで、ログの保管・保全性・一意性を保障する、できる仕掛け、を作って欲しい。もしくは、その知見を持っている人は情報の共有をしてほしい。また、これらの運用のオペレーションの共有もして欲しい。

- DNS キャッシュサーバで、デュアルスタックサーバの BIND を使う際は最新の BIND を使うべき。IPv6 のリーチャビリティが多少悪くても、相手がデュアルであっても、意外と接続する。最新の BIND 以外は接続が良くないことがある。前回の DNSOPS の資料を参照のこと。

- 人が書いた Web-CGI を移植する際に、きっと何かあるだろうと思いつつ試しに移植したところ上手くいって気が付かなかった例を紹介。
  ソース IP アドレスで認証していたりする場合に、上位 32bit だけ見るように作られていると、IPv6 であっても動作はするけど、認証として意味がなくなったりすることもある。誰かが書いた Web-CGI は IP アドレスとかチェックが必要。