

DNSのv6対応

2009年3月5日

IPv6オペレーションズフォーラム

株式会社インターネット総合研究所

伊藤 高一

- authoritativeサーバ

- v6関連のRRを設定する。

- AAAA

- `www IN AAAA 2001:db8::80`

- PTR

- `0.8.略.ip6.arpa. IN PTR www.example.jp.`

- recursiveサーバ/authoritativeサーバとも
 - v6トランスポートを経由してquery/responseをやりとりできるようにする。
 - OS/サーバソフトウェアは今どき困らないのでは?
 - v6コネクティビティの確保:がんばれ!
- recursiveサーバ
 - v6 reachableなrootサーバは存在する。
 - root hintにもAAAAは載っている。
 - でも、まだしばらくはv6 onlyでは検索できない部分木もあるだろう。
- authoritativeサーバ
 - authoritativeサーバ自身のAAAAを書く。
 - glueも忘れずに。

枯渇までに、このフェーズは済ませておかなきゃいけない。

- v6トランスポートでquery/responseできることと、v6関連のRRを設定することとは独立。
 - v4 onlyのauthoritativeサーバがv6アドレスのPTRを応答してもよい。
 - dual stackのクライアントがv4トランスポートでAAAAをqueryしてもよい。
 - それどころかIPトランスポートで
 - % dig version.bind TXT CHとかするでしょ?

- 疑問
 - dual stackのrecursiveサーバは、authoritativeサーバへのqueryにv4/v6どちらを優先的に使うの？

- 自サイトのv6トランスポートの質が心配なら、よくなるまでv4 onlyで待った方がDNSサービスのレスポンス/安定性はいいかも。
 - recursiveサーバにはv6でqueryさせない。
 - authoritativeサーバのAAAAは書かない。
- あくまで過渡的な話。今日は後ろ向き禁止!
- エンドユーザーに「やっぱv6ダメちゃん」と言わせたら負け。

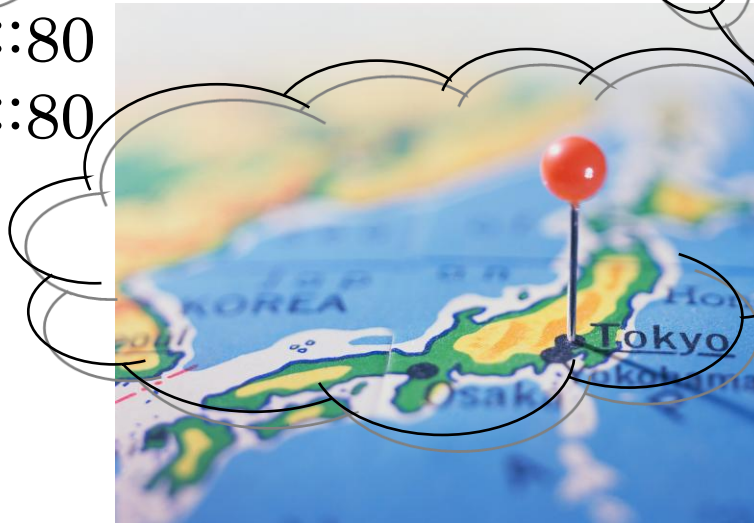
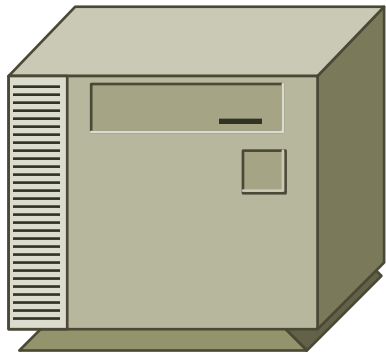
- `www.v6.example.jp`
 - アプリケーション層(とユーザ)にトランスポートを意識させるためのhack = layer violation
 - v6コネクティビティの質に不安がある間は意味はある。
 - かめが踊ることを喜べるヒトにも意味はある。
 - 気づいたらv6を使っていた、には逆行。
 - v6が当たり前の時代になったら、「v6」って入ってるの、はづかしくない?

1つのインターフェースに複数のアドレスを振れる

単純にAAAAを2つ設定して
ラウンドロビンして
幸せになれるか?

実在の会社・団体とは無関係デス

2001:db8:2914::80
2001:db8:2500::80



- AAAAとPTRを設定すればよい。
- 外からアクセスされるサーバ(MX、Web、NSなど)のAAAAは、なきや話にならん。
- サーバ類のPTRって何に使う? 必要かなあ?
 - v4では「設定するでしょ、ふつ～」な面がある。
- ルータのPTRは、設定しておくのとtracerouteしたときに幸せ。
 - 利便性より情報隠蔽を重んじる選択もあり得る。
- 整合性をチェックするツールは?
 - dnswalkは非対応のまま進化していない。

- DNSという仕掛けができた。
- 正索き/逆索きともキチンと設定することが定着。
- 逆索きできないアドレスからは接続させない
anonymous FTPやIRCのサーバが出てきた。
 - バリエーション:さらに正索きして元に戻らないとダメ。
- という状況で、動的割当されるIPアドレスが登場。

- DNSに登録しないと、anonymous FTPやIRCに接続できない(既成事実)。
- プール空間を網羅して設定することで解決したのか?
 - カ技
 - v4では現実的なオーダーだった。
- 動的割当のアドレスもDNSに登録されていることが既成事実になった。
- アドレスの素性はDNSに載ったが、ホストの素性はDNSから失われた。

君に、胃がキュン
弱気なぼくら

- 力技、再び...か?
 - /64だとしても16nibbleある。
 - 網羅したらゾーンデータの寸法が大変なことに...
- では特定のホストだけ登録する?
 - オフィスなどなら、まだ現実味もあるけど、アドレスはPnPなのに、それをDNSには手で設定するって間違っていない?
 - 不特定のホストがつながってくるISPでは無理。
 - RtSol+dynamic updateの実装っていないのかな?

- どうも、v4のやり方をそのままv6に持ち込むのは無理っぽい。
- v6での身元確認はDNSに頼るべきではない、という意見もある。
- 仕掛けとしてDNSを使うとしても、具体的な方法は変わるだろう。
 - ワイルドカードにPTRを設定するという案もある。
 - ホストアドレスではなくprefixにPTRを設定するという案もある。
 - いずれにしても、正索きしたって元には戻らない。

- たかがアドレスが長くなるだけでしょ？
 - v6トランスポートを有効にしてAAAAとPTRを設定すればいいんだろ？

• 間違いでした ;_;



- 新しいコモンセンスを形成しなきゃいけない気がする～う。