IPv6 Update

SUZUKI, Shinsuke

Hitachi, Ltd. / KAME Project

suz@crl.hitachi.co.jp

Abstract

- IETFにおけるIPv6関連動向の最新状況
  - 基本仕様
  - 経路制御
  - DNS関連
  - IPv4→IPv6移行
  - セキュリティ関連

基本仕様

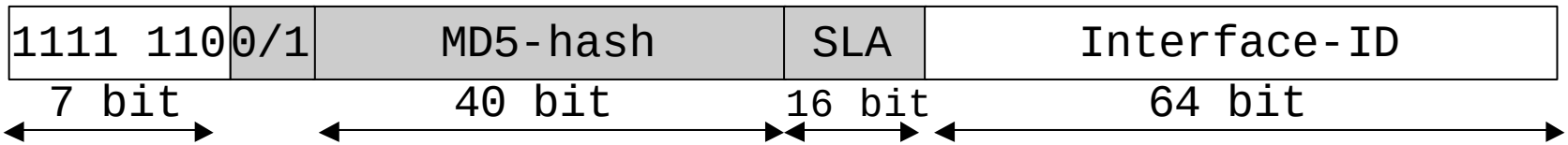
- Site-Local Address
- Prefix Delegation
- RFC2461bis, 2462bis
- Router Renumbering
- Mobile-IPv6

Site-local Addressの問題

- Site-local address の特徴
  - ローカルな使用OK (192.168.0.0/16)
  - サイト境界ルータは、異なるサイトのアドレスを別物扱い
    - e.g. FEC0::1%site1 and FEC0::1%site2
- 課題
  - 重複するため、運用上不便
    - 例. 2つのネットワークを統合したら、両方fec0:1:2::/48を使っていた
  - サイト境界ルータは厄介者
    - ベンダー、オペレータ、標準化

Site-local Addressの見直し

- 現状のSite-localを廃止して、新しい策を考える
  - 「サイト境界」は廃止するが、一意性とローカル使用は認める。
- Global-Unique Local Address (FC00::/7)
  - ローカル使用OKな、一意性のあるアドレス
    - 2^{40}個の/48
    - インターネットへ広告してはならない
  - 2種類
    - FC00::/8=レジストリ経由でアサイン
    - FD00::/8=レジストリなしにアサイン
- 標準化
  - Site-local Addressを廃止すること→WG Last call
  - Global-Unique Local Address→まだ議論中

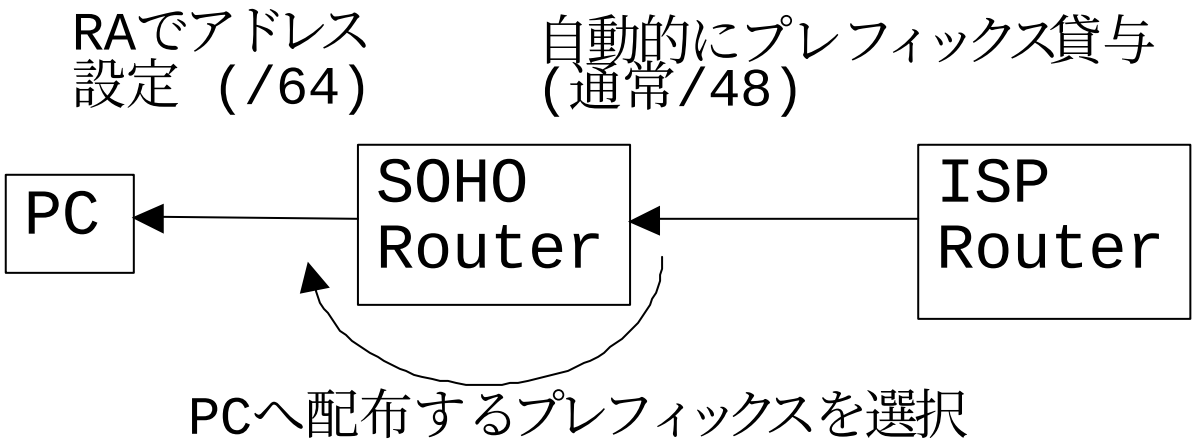


FC00::/7の残課題

- IPv6-NATが必要になる?
  - グローバルアドレスとFC00::/7の併用で十分ではないか?
- Source address selection
  - Longest-match algorithm (RFC3484)で十分ではないか?
- DNSサーバ
  - IPv4プライベートアドレス同様、内向けDNSと外向けDNSとを分ける必要あり
- Well-known address?
  - 例. DNS server address
- FC00::/8を配布する「レジストリ」とは?
- 2^{40}個で本当に十分?

Prefix Delegation (概要)

- 特にSOHO Router向けのPlug & Play
- プロトコルを使って、プレフィックスを上流から下流へ自動的に通達



Prefix Delegation (状況)

- 標準化: ほぼ完了
  - コンセプト/要求事項: IESGレビュー中
  - プロトコル: いろいろあるが、DHCPv6-PDがメジャー
    - IPv4 DHCPとは異なり、IPv6アドレスは配らない
    - DHCPv6プロトコルの枠組を流用して、IPv6プレフィックスを配布
    - 他の情報(e.g. DNSサーバ)も同時に配布可能
    - RFCとして承認済。正式なDHCPオプション番号も割当済。

Prefix Delegation (実装)

- 実装
  - CPE側
    - 6Wind, Allied-Telesis, Cisco, IIJ, KAME, NEC, USAGI, Yamaha
  - PE側
    - Cisco, 富士通, 日立, KAME, NEC, USAGI
- 相互接続試験も多数行われている
  - TAHI, Connectathon, IPv6 Showcase, DHCPv6-Interop
- 一部のISPで運用試験中

RFC2461bis, 2462bis

- 課題
  - NDP, RAを使ってみると、いろいろ不便な点がある
    - default routeがないとき、全てのアドレスはonlink
  - NDP, RAを作ってみると、仕様が不明確な点もある
    - セキュリティ面
    - モバイルIPv6との関連
    - その他諸々 (valid-lifetime > preferred-lifetime)
- 状況
  - ICMPv6の仕様修正作業中
    - 実装者には楽になる方向な修正
    - ユーザにも便利になる方向の修正

Router Renumbering

- 概要
  - Router Renumberingプロトコル(RFC2894)は、現実に役に立つ?
- 状況
  - あまり役に立たない
    - アプリに埋め込まれたIPv6アドレスを書き換えられない
      - DNSレコード
      - パケットフィルタ
      - IPv4/v6 トランスレータ
      - 組み込みアプリ (e.g. OSのインストーラ)
  - あるX-dayに一気にrenumberingしなくてもよい
    - 旧プレフィックスと新プレフィックスを共存させながら、手動でrenumberingする手順を明確化

Router Renumbering (cont.)

- 4ステップの手動動作によるRenumbering手順
  1. 新しいアドレスをネットワーク上のルータに設定
     - 古いアドレスも継続使用
  2. アプリケーションを新しいアドレスで動かす
     - 古いアドレスでも動くようにしたまま

     e.g. DNSレコードに新しいアドレスを設定
  3. アプリケーションを古いアプリで動かなくする

     e.g. 古いアドレスのDNSレコードを削除
  4. 古いアドレスをネットワーク上のルータから削除
- 参考
  - `draft-baker-ipv6-renumber-procedure-01.txt`

Mobile-IPv6

- 現状
  - 基本仕様はRFC化承認済
    - RFC発行待ち
    - ICMPv6オプション番号も正式割当済
  - 実運用上の課題を検討中
    - 高速ハンドオーバ
    - ホームプレフィックスの自動割当方法
    - IPsecとの相性

経路制御関連

- 概要
- マルチホーム

経路制御プロトコル全般

- IPv6固有なプロトコル課題は稀
  - IPv6でプロトコル課題が見つかったら、大抵同じ課題がIPv4にもある
- 「複数のプロトコルを同時に扱う」という点での課題はいくつかある
  - ベンダー向けの課題
  - オペレータはほとんど気にする必要はない

マルチホーム

- 概要
  - あるサイトが複数の上流ISPとつなぎたいときには、どうすればいいのか?
    - 1. AS番号を取得して、E-BGP運用
    - 2. 各ISPからプレフィックスを取得し、宛先に応じて適切なソースアドレスを選択
  - 今のIPv4の流儀でマルチホームをしたとして、経路表エントリ数は多くなりすぎないか?
- 状況
  - Multi6 WGで議論中
    - マルチホームをするにあたっての要求事項を整理
      - Locator/Identifierの分離
      - モビリティを考慮するか否か
    - それに基づき様々な提案を分析

DNS関連の課題

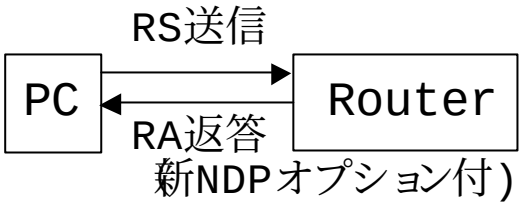
- DNSサーバ検出
- AAAA vs A6
- ip6.int vs ip6.arpa
- PTR recordの使い方
- IPv6問合せ処理の典型的なバグ

DNSサーバ検出(概要)

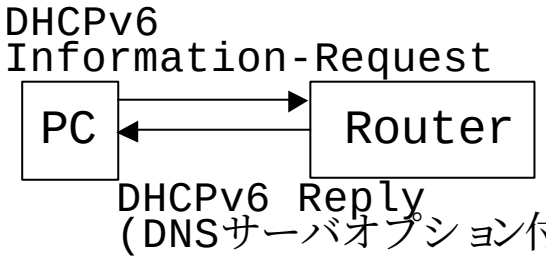
- RAではIPv6アドレス以外の情報を自動設定不能
  - e.g. DNS server, NTP server, ...
- 特にDNS関連は、IPv6アドレス長を考えると大切
  - DNSサーバアドレス
  - DNSドメインサーチパス
- DNSOP WGで議論中

DNSサーバ検出(現状)

- 3種類の候補
  - well-knownな固定アドレス
    - 具体的なアドレスは未定
  - RA拡張
  - stateless DHCPv6
- どうするかは未定
  - 1候補に絞る?
  - 複数候補使い、使い分ける?
- 主な課題
  - DNSサーバアドレス更新方法
  - 複数サーバ存在時の挙動
  - 他のDNSサーバ自動設定(e.g. DHCPv4)との競合



**DNSサーバアドレス
=新NDPオプション内のアドレス**



**DNSサーバアドレス
=DNSサーバオプションのアドレス**

AAAA vs A6

- 概要
  - 2種類のDNSレコードが存在
    - AAAA: Aレコードを IPv6向けに単純拡張
    - A6: Router Renumberingを考慮したIPv6レコード
- 結論
  - 通常運用ではAAAAのみ使う
  - Renumberingは運用でカバー

ip6.int vs ip6.arpa

- 概要
  - かつては、IPv6逆引きレコード=“ip6.int”
  - “ip6.int”は国際TLDとして予約された
- 現状
  - “ip6.arpa”を用いる
    - 2001::/16については、“ip6.arpa”を使用
    - 3ffe::/16は、“ip6.int”を使用
      - “ip6.arpa”導入は計画中
- 参考
  - `draft-ymbk-6bone-arpa-delegation-01.txt`

逆引きレコードの使い方

- DNSの逆引きレコードを認証に使うアプリ・プロトコルが存在
  - ソースアドレスの逆引きレコードがあれば、信頼できる
- 本当に実用的?
  - 全てのIPv6アドレスが逆引き登録されるわけではない
    - Link-localアドレス
    - RAで生成されたIPv6アドレス
    - Privacy address extension
  - 単にアドレスから名前を引きたいだけならば、ICMPv6でも実現可能(Node-Information-Query)

IPv6問合せ処理の典型的バグ

- 概要
  - DNSサーバがIPv6レコード問合せを処理するときの典型的なバグをリストアップ:
    - (IPv6レコードの有無にかかわらず)IPv4レコードがなければ、常に「エントリなし」エラーを返す
    - IPv6アドレス問合せを無視する
    - AレコードでIPv6アドレスを答える
- 参考
  - draft-morishita-dnsop-misbehavior-against-aaaa-00.txt

移行メカニズムの課題

- 分類
- 課題
- v6ops WG

移行メカニズムの分類

- Tunnelベース
  - トンネルセッションプロトコル
    - DTCP, TSP
  - 自動トンネルプロトコル
    - 6to4, ISATAP, Teredo, DSTM
- Translatorベース
  - NAT-PT, SIIT, FAITH
- Proxyベース
  - アプリケーションレベルゲートウェイ(HTTP proxy, SMTP gatewayなど)

課題

- 完全なメカニズムは存在しない
  - Tunnelベース
    - IPv6 network topology ≠ IPv4 network topology
    - IPv4アドレス必須
      - i.e. IPv4アドレス不足の根本解ではない
    - NAT経由では動かない
      - (Teredoは唯一の例外だが、複雑すぎ)
  - Translatorベース
    - IPv4→IPv6変換は困難
    - アプリケーションデータ内に埋め込まれたアドレスは変換不能
      - link
  - Proxyベース
    - 特定のプロトコルについてしか動かない
- 結局何をいつ使えばいい?

V6ops WG

- 概要
  - 適用場面ごとに、移行に必要な技術要素を解析
    - 携帯
    - ISP
    - Unmanaged(家庭/SOHOネットワーク)
    - Managed(企業/エンタープライズネットワーク)
- 現状
  - 具体的なソリューションの議論は、上記解析が済んでから
    - 現在は解析を進めている段階
- 参考
  - v6ops WG
    - `http://www.6bone.net/v6ops`
  - Issue Tracker
    - `https://rt.psg.com/` (id=ietf/passwd=ietf)

セキュリティ関連の課題

- Securing Neighbor Discovery
- 自動トンネルのセキュリティ課題
- IPv6 Firewall Architecture

Securing Neighbor Discovery

- 概要
  - Plug & Playは不正ネットワーク使用につながりうる
    - NA spoofingによる、偽NDPキャッシュ生成
    - RA spoofingによる、誤ったRA広告
- 現状
  - CGA (Cryptographically-Generated Address)
    - 公開鍵のハッシュから生成されたリンクローカルアドレスを用いてNDP通信
    - SEND WGで議論中
  - L2認証
    - PAP/CHAP (PPP), 802.1x (Ethernet)...
- 参考
  - `draft-ietf-send-psreq-04.txt`
  - `draft-ietf-send-cga-02.txt`

自動トンネルのセキュリティ課題

- 概要
  - 自動トンネル(e.g. 6to4)
    - IPv6アドレスに埋め込まれたIPv4アドレスを、IPv6 over IPv4トンネリングに使用
  - 自動トンネルリレーを悪用すると、攻撃も可能
    - Source spoofing
    - IPv4/v6 DoS attack
- 現状
  - 起こりうる攻撃とその対策の分析
- 参考
  - `draft-ietf-v6ops-6to4-security-00.txt`

IPv6 Firewall Architecture

- 2種類の課題
  - IPv6プロトコル由来の課題
    - 数珠繋ぎの拡張ヘッダスキャン, Privacy Address Extension...
  - ‘End-to-End’通信との相性の悪さ
    - IPsec, P2P ...
- 現状
  - 問題点の洗い出しを開始
  - 具体的な方策については未定
    - 本当にIPv6WGやv6ops WGで行うべき仕事?
- 参考
  - `draft-savola-v6ops-firewalling-02.txt`

まとめ
IETFにおけるIPv6関連動向の最新状況

- 基本仕様
  - ICMPv6, RAなどの仕様の不明点の明確化
- 経路制御関連
  - マルチホーム関連の議論方針で紛糾中
- DNS関連
  - DNSサーバ検出方法の標準化がホットトピック
- IPv4→IPv6移行
  - どの移行技術をどの場面で使うかの整理中
- セキュリティ関連
  - プロトコル別のセキュリティ課題の洗い出し中