

IPv6技術動向

IPv6 Technical Summit 2005

アラクサラ ネットワークス株式会社

ALAXALA Networks Corporation / KAME Project
SUZUKI, Shinsuke <suz@alaxala.net>

Alaxala

- 基本仕様
- 運用ノウハウ
- 移行技術
- アドレッシング
- マルチホーム
- モビリティ

■ ほぼFixした

- IETF ipv6 WGのface-to-face meetingは、2005/11が最後
 - ◆ IPv6は、IPv4と同様に、全プロトコルの基本要素である
- KAME Projectの完成宣言
 - ◆ <http://www.wide.ad.jp/news/press/20051107-KAME-j.html>
 - ◆ <http://www.kame.net/newsletter/20051107/>
- 細かい話題が若干残っている程度
 - ◆ Router Advertisementメッセージ内のM bit/O bitの定義
 - ◆ IPv6 DNSサーバアドレス通知方式
 - ◆ 仕様更新 (IPv6 over PPP, Source Address Selection, ...)

■ 非IP系通信媒体でのIPv6通信方法の標準化

- IETF IPv6 over Low Power WPAN WG
 - ◆ センサネットワーク
- IETF IPv6 over IEEE 802.16(e) Networks BoF
 - ◆ WiMax

■ 運用ノウハウを文書化 (IETF v6ops WG)

- ◆ リナンバリング手順 (RFC4192)
- ◆ IPv6 Security概論 (draft-ietf-v6ops-security-overview-04.txt)
- ◆ ICMPv6フィルタガイドライン (draft-ietf-v6ops-icmp-filtering-bcp-02.txt)
- ◆ Network Architecture Protection (draft-ietf-v6ops-nap-04.txt)
 - NAT相当の機能を、NAT箱なしで実現する方法
- ◆ IPv6アドレスのDNS問い合わせに対する誤応答事例集 (RFC4074)
 - WIDE v6fix WG <http://www.v6fix.net/>

...

■ 時には運用観点から仕様変更も提案

- On-link assumption廃止
 - ◆ 「端末にDefault経路がない」全ての端末は同一リンク上に存在すると思え」
 - ◆ 最新のIPv6基本仕様からは、この仮定が廃棄される
- Stateless DHCPv6での情報更新方法のRequirement (RFC4076)
- Stateless DHCPv6での情報更新方法 (RFC4242)

■ 大まかに3段階

● 事前準備

◆ 事前に新アドレスを確保

- アドレスブロックの割当, DNS逆引き委譲

◆ DNSレコードのTTLを短めに設定

● 新規プレフィックスに基づくアドレス追加

◆ 古いプレフィックスのアドレスはまだ消さない X-dayなしのリナンバリング

● 古いプレフィックスを削除

◆ 古いプレフィックスのDNSレコードを削除

◆ 古いアドレス割り振りを削除

■ ポイント

● 思わぬところにアドレス情報は潜んでいる

◆ フィルタ (e.g. パケット中継、経路制御メッセージ)

◆ アプリケーション内部 (e.g. DHCPv6で広告するサーバアドレス)

■ 背景

- ICMPv6パケットをフィルタすると、IPv6通信自体が出来なくなることがある (e.g. path MTU discovery失敗)
- だからといって、ICMPv6パケットを無制限に通すのは怖い

	廃棄不可	通常は廃棄不可	Don't Care	管理者のポリシー次第	通常廃棄可
中継		MIP6	NDP, MLD, SEND, MR-disc.	Seamoby	NI-Query/Reply, Router Renum.
共通	Dst Unreach(全code) Packet-Too-Big Time-Exceed (code0) Param.Prob. (code1,2) Echo-Request Echo-Reply	Time-Exceed. (code 1) Param.Prob. (code0)		未割当 ICMPv6 エラー タイプ (Type5-99, 102-126)	試験割当 ICMPv6 タイプ (Type100-101, 200-1) 未割当ICMPv6 情報タイプ (Type159-254)
自分宛	NDP, MLD, SEND, MR-disc		Router Renum., MIP6, Seamoby	Redirect, NI- Query/Reply	

■ NATで提供したい機能

- Intranet-Internet間のゲートウェイ機能
- Stateful Filter Inspection
- ユーザ/アプリケーションのトラッキング
- 端末/トポロジー隠蔽
- ISP非依存なアドレッシング
- グローバルアドレス枯渇対策
- マルチホーム

■ IPv6で等価な機能を提供する方法の整理

- Privacy Address Extension
- ULA
- Prefix-Delegation
- Untraceable IPv6 address
- Mobile-IPv6
- Shim6

■ IETF v6ops WG

- IPv6導入ノウハウを文書化

- ◆ ケース別のIPv6導入手順分析 (RFC4029, 4038, 4057, 4213, 4215)

■ IETF softwire WG

- 自動トンネリングプロトコルの標準化

- 現在は以下の2ケースに関する要求事項の整理中

- ◆ ホスト~ ルータ

- Last one-mileのIPv6対応

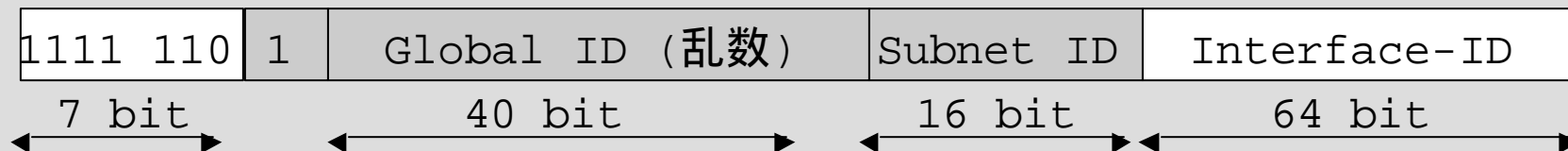
- ◆ ルータ~ ルータ

- Coreネットワーク内のIPv6対応

- 不要なアドレス空間の廃止
 - サイトローカルアドレス (RFC3879)
 - NSAP互換アドレス (RFC4048)
 - IPv4互換アドレス (draft-ietf-ipv6-addr-arch-v4-04.txt)
 - IPv6実験網(6bone)の廃止 (2006年6月6日)
 - ◆ 3ffe::/16 (RFC3701), ip6.int (RFC4159)
- 新規アドレスの標準化
 - アドレススコープの明確化 (RFC4007)
 - Unique Local Address (RFC4193)
 - Embedded-RP (RFC3956)
- アドレス割当ポリシー
 - IETF IAB - IANA間で随時議論 (詳細は次の発表で)

■ 閉域網向けの/48アドレス空間

- Registryへの申請は不要 (FD00::/8)
 - ◆ IPv4 Private Addressと同じ感覚で使える
 - ◆ 40bitの乱数計算が必須
 - e.g. “時刻+EUI-64”のSHA-1ハッシュ値の下40bit
- <http://www.kame.net/~suz/gen-ula.html>



- IPv4 Private Addressとは違い、重複の可能性は低い
 - ◆ N個のULAアドレスブロックのうちどれか2つ以上が重複する確率 $1 - (1-1/2^{40}) \times (1-2/2^{40}) \times \dots \times (1-N/2^{40})$
 - N= 1,000 約0.00005%
 - N= 10,000 約0.005%
 - N=150,000 約1%
- Registryで割当を管理するULA(FC00::/8)は、標準化未完了
 - ◆ 運用体制に関する議論が収束していないため

■ 背景

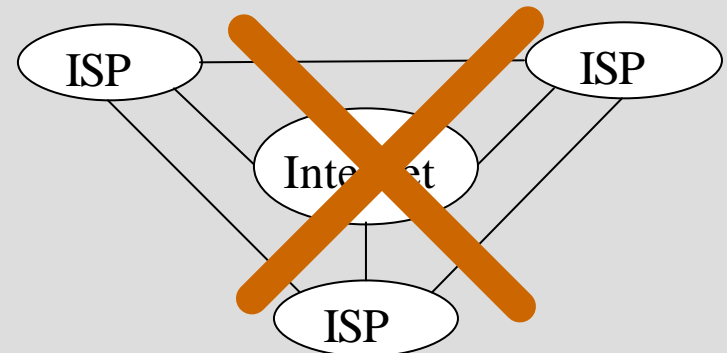
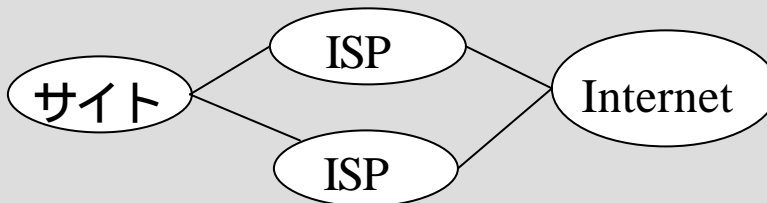
- IPv4マルチホームでは“Punching Hole”が経路エントリ数増大の原因
- IPv6で同じ流儀でマルチホームすると、インターネットは破綻する

■ 課題整理 (IETF multi6 WG)

- RFC4177 アーキテクチャ整理
- RFC4218 想定される脅威の分析
- RFC4219 想定される課題の分析

■ 「マルチホーム」にも色々

- ここでは「サイトマルチホーム」が考察の対象
 - ◆ 現在“Punching Hole”の原因になっているケース
- ISP間マルチホームは考察対象外
 - ◆ BGPによるポリシー制御で十分



■ Shim6=端末ベースのサイトマルチホーム技術 (IETF shim6 WG)

- 端末に振られたアドレスを2種類に分類
 - ◆ Identifierアドレス 端末の一意性を示すアドレス
 - ◆ Locatorアドレス ルーティングするための場所を示すアドレス
- IPv6層の間にShim層を導入
 - ◆ Shim層の上からは、Identifierアドレスで通信しているように見える
 - ◆ Shim層の下からは、Locatorアドレスで通信しているように見える
- 本質的には端末内NAT
 - ◆ アプリケーションからNATを隠蔽し、端末外NATの抱える問題を回避

アプリケーション	
TCP/UDP	
IPv4	IPv6(2)
	Shim
	IPv6(1)
物理層	

IPv6(2) = IP end-point sub-layer

- IPsec, Fragment, Destination Option処理

Shim

- Locator/Identifier対応付け
- Locator/IdentifierのIPv6アドレス付替

IPv6(1) = IP routing sub-layer

- NDP, IPv6パケット送受信処理

ISP1/2の両方からアドレス取得
src/dstにより、用いられるISPが決める

- 一見Mobile-IPv6に似ているが...
 - Identifier(Mobile-IPv6ではHome Address)への到達性がなくなる事態も考慮
 - アプリケーション単位に経路選択可能
- 到達性がなくなったら、どのような処理をすべきか
 - 到達性がなくなった」という判断基準は?
 - Identifierの付替は必要?
- Locator選択アルゴリズムはどうあるべきか
 - 到達性だけで評価して本当によいのか?
- Shim6がサイトマルチホーミングの課題を全て解決するか?
 - 端末がマルチホームポリシーを決める設計 ネットワーク管理者は、端末に対してマルチホームポリシーを強要しにくい

- 基本プロトコルの標準化は終了
- 運用を想定した議論が活発に行われている
 - 特に高速ハンドオーバ
 - ◆ 運用階層型MIPv6 (RFC4140)
 - ◆ ネットワーク接続検出技術の要求事項 (RFC4135)
 - ◆ MIPv6での高速ハンドオーバ (RFC4068)

- 基本仕様
 - ほぼ完了
- 運用ノウハウ
 - ドキュメントの蓄積中
 - 見つかった課題は随時仕様にフィードバック
- 移行技術
 - Last one-mile/Backboneにおける自動トンネリングプロトコルの標準化が始まった
- アドレッシング
 - 不要なアドレス空間の廃止
 - 有用なアドレス空間の追加 (ULA, Embedded-RP)
- マルチホーム
 - 端末でのサイトマルチホーム技術(shim6)の設計が急速に進む
- モビリティ
 - 運用を想定した議論へ

Thanks you!

Alaxaia