IETF における標準化ディプロイメント状況

東京大学 情報基盤センター / WIDE Project
関谷 勇司

この 1年間 (2008) における IETF での動向

- この 1年間で活動があったWG から個人的に関心を持っているWGを抜粋して紹介
- Routing 関連
  - savi WG (INT)
  - rtgwg (RTG)
  - sidr WG (RTG)
  - idr WG (RTG)
  - grow WG (OPS)
- DNS 関連
  - dnsext WG (INT)
  - dnsop WG (OPS)
- IPv6 関連
  - v6ops WG (OPS)
  - 6MAN WG (INT)

ROUTING 関連

SAVI WG

- Source Address Validation Improvements WG
  - Source Address Validation
  - Path Validation
- Ingress Filtering を末端で行う
  - ブロードバンドルータやセットトップボックスも範疇
- Bridge Layer-3

- First-come-first-serve SAVI for IPv4 + IPv6
- SAVI for IPv6 Secure Neighbor Discovery

- まだ requirement を出している段階で
  具体的なプロトコルの話まで到達していない

SIDR WG

- Secure Inter Domain Routing WG

- RPKI Architecture / ROA format
  - RIR, LIR, NIR を中心とした RPKI
  - Routing Object の認証
  - ポリシー議論なのでいろいろ意見でます
  - まだ収束は先です
- 実用という意味では、まだ先の技術

- BGP Prefix Origin Validation
- RPSL and RPKI

BGP PREFIX ORIGIN VALIDATION

- Prefix に対する Origin AS のデータベースを保持
  - 手元にキャッシュし BGP update 毎に照会

- ROA Validation との関係
  - データベースは特に定義していない
  - RPKI の ROA を使ってもいいし、別のものでも良い

RPSL AND RPKI

inetnum: 193.0.0.0 - 193.0.7.255
netname: RIPE-NCC
descr: RIPE Network Coordination Centre
descr: Amsterdam, Netherlands
remarks: Used for RIPE NCC infrastructure.
country: NL
admin-c: AMR68-RIPE
admin-c: BRD-RIPE
tech-c: OPS4-RIPE
status: ASSIGNED PI
mnt-by: RIPE-NCC-MNT
mnt-lower: RIPE-NCC-MNT
signature: v=1; c=rsync://rpki.ripe.net/….cer; m=rsa-sha1; t=1234567890; a=inetnum+netname+country+status; b=<base64-data>
source: RIPE # Filtered

RTGWG

- Routing Area Working Group
- IP レベルの fast reroute に関するフレームワークの議論
  - Failure detection
  - Repair Paths
- あくまでフレームワークが中心
  - IS-IS / OSPF への適用までは言及
  - MPLS LDP も利用
  - BFD も利用

GROW WG

- Global Routing Operations WG

- MRT format
  - MRT フォーマットを標準化する文章
- BMP "BGP Monitoring Protocol”
  - BGP monitor のためのプロトコル定義
- LISP implementation
  - www.lisp4.net / www.lisp6.net
- LISP: Deployment and Experience

LISP

- Locator and Identifier Separation Protocol

- Locator (ネットワーク上での位置を示すアドレス)
- Identifier (ノード固有の識別子を示すアドレス)
  - 分離することにより、経路制御情報の削減を目指す
- Identifier に対して Locator をマッピングするデータベースが必要
- GRE を使ったトンネルによる通信

- www.lisp4.net / www.lisp6.net
  - プロトタイプ実装が存在 – OpenLisp
- Practice and Experience の報告
  - 実験段階に入りつつあるのかな、という段階

IDR WG

- Inter-Domain Routing WG

- Published
  - RFC5291: Outbound Route Filtering Capability BGP-4
  - RFC5292: Address-Prefix-Based Outbound Route Filter for BGP-4
- Ongoing
  - Flow-spec
    - Prefix に対する flow の性格を定義する NLRI
  - BGP4-mib

IDR - NEW WORKS

- Advertisement of Best External Route in BGP
  - iBGP での Best Route と eBGP での Best Route を用いた Fast Switchover

- Fast Connectivity Restoration using BGP Add-path
  - BGP path に ID をつけ、複数のパスを RR に渡すことで経路の切り替えを早める

DNS 関連

DNSEXT WG

- DNS extensions WG
  - DNS のプロトコル拡張に関して議論するWG
- DNSSEC
  - Kaminsky Attack により注目を集めた
  - DNSSECbis も仕様は固まり、実装も出始めた
    - RFC4033, RFC4034, RFC4035, RFC4956, RFC5155
    - Bind は 9.6 にて NSEC3 対応予定
  - DNSSEC の要求が高まりつつある
    - IAB, ICANN も声明を出す
- Forgery Resilience

FORGERY RESILIENCE

- キャッシュ汚染に対する耐性を高める

- Call for Ideas
  - Additional Entropy
  - Cache Overwrite
  - CNAME and DNAME chains
  - TCP
  - Multiple UDP queries
  - Do nothing and recommend DNSSEC deployment

FORGERY RESILIENCE (CONT.)

- Additional Entropy
- 0x20
  - 大文字小文字を利用して、Port / TID 以上に Entropy を上げる方式
- Cache Overwrite
- Cache の上書きに制限を設ける
- TCP
- TCP を使い名前を解決
- Multiple UDP
- 何回も問い合わせる
- Do Nothing
- DNSSEC を早く普及させる

DNSOP WG

- Domain Name System Operations WG

- Reflectors are evil
- Name Server Management
- DNSSEC trust anchors
- Priming
- Respsize
- AS112
- EDNS0 deployment

DNSOP WG (CONT.)

- Reflectors are evil
  - Open Resolver による Reflection 攻撃への注意
- Name Server Management
  - Name Server を運用管理するためのプロトコル
  - まずは Requirement を作成するためのデザインチーム
    - 完了
- DNSSEC trust anchor
  - DNSSEC 認証の起点となる trust anchor のフォーマットやメンテナンス方法に関する議論
- Priming
  - Resolver Server における Priming の定義
- Respsize
  - UDP 512 octets 制限に関する議論

DNSSEC

- NTIA (米国商務省 電気通信情報局)
  - http://www.ntia.doc.gov/dns/dnssec.html
  - Root zone を署名する
  - 誰が署名するのか？
    - Public comment
- IAB の声明
  - NTIA をサポートする
- ICANN の声明
  - 技術的に DNSSEC を deploy する方向

- Root zone の署名に関して動きが出ています

IPV6 関連

V6OPS WG

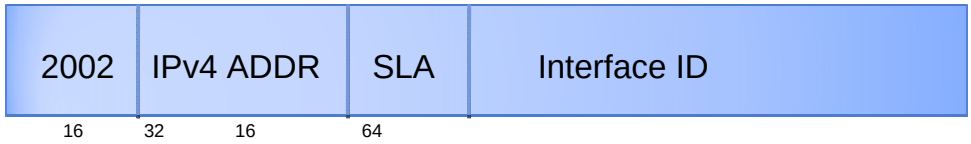
- IPv6 Operations WG
  - IPv6 運用に関する技術を議論
- IPv6 CPE
- Rouge RA / RA guard
- IPv6 usage in Sweden
  - 6to4 や Teredo でのトラフィックが 50M 程度
  - MAX では 6to4 が 100M、Teredo は 200M
- IPv6 statistics at Google
  - RIPE meeting でも報告があった

IPV6 移行のための技術

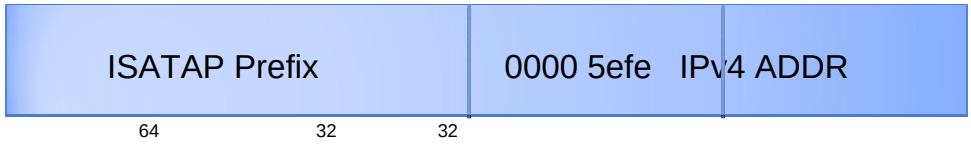
- 6to4 (RFC3056)
  - IPv4 → IPv6 へのアクセス
  - 6to4 サーバによるトンネル中継
  - Tokyo6to4.net Project
- ISATAP - Intra-Site Automatic Tunnel Addressing Protocol) (RFC5214)
  - 6to4 のイントラネット版
- Teredo (RFC4380)
  - UDP を使ったIPv6 over IPv4 tunnel
  - NAT の裏側からでも利用可能
  - Teredo リレーによる中継
- どれも Windows Vista には実装済み
- MacOS X では標準で 6to4 が利用可能

それぞれのアドレス形式

- 6to4



- ISATAP



- Teredo

GOOGLE から見た IPV6 アクセス状況

- www.google.* へのリクエストからそのホストが IPv6 ready であるか判定して latency 等を計測

- 国別に見ると
  - ロシア　: 0.76%
  - フランス : 0.65%
  - 米国　　: 0.45%
  - 日本　　: 0.15%
  - IPv6 を叫んでいる国の中では最下位っぽい

- IPv6 アクセス方法
  - 6to4　　: 67.9%
  - Native : 29.1%

6MAN WG

- IPv6 Maintenance WG
  - IPv6 に関して改訂が必要な仕様に関する議論を行う
- Node Requirements
  - IPv6 ノードへの要求事項をまとめた文章
  - MUST / SHOULD がわかる
- Overlap Fragment
  - オーバーラップしたフラグメントパケットが届いた場合の扱い
- Address Selection Model
  - Address Selection に関する解決モデルを提示
- v6ops とともに、CPE 系やカスタマー収容系の技術に関する話題が議論された