IETF RAMの動向

～新しいネットワークアーキテクチャ・アドレス割当て方式～

NTT 情報流通プラットフォーム研究所

松本存史

arifumi@nttv6.net

Copyright(C) NTT Information Sharing Platform Laboratories.
Copyright(C) NTT Information Sharing Platform Laboratories.

RAMとは

- 背景
  - Oct. 2006, IAB “Routing Workshop”
    - 経路表増大などについて問題提起
  - IETF Shim6の反省
    - Nanogからの反発 “TEができない”等
  - Mar. 2007, IETF “ ID-Loc Separation BoF”
    - ID-Loc分離にフォーカスして議論
- 現在の活動状況
  - WG形成には至っていない
  - MLにて活動(Routing and Addressing Mailing List)
    - 複数の提案が提出さて議論中

Copyright(C) NTT Information Sharing Platform Laboratories.
Copyright(C) NTT Information Sharing Platform Laboratories.

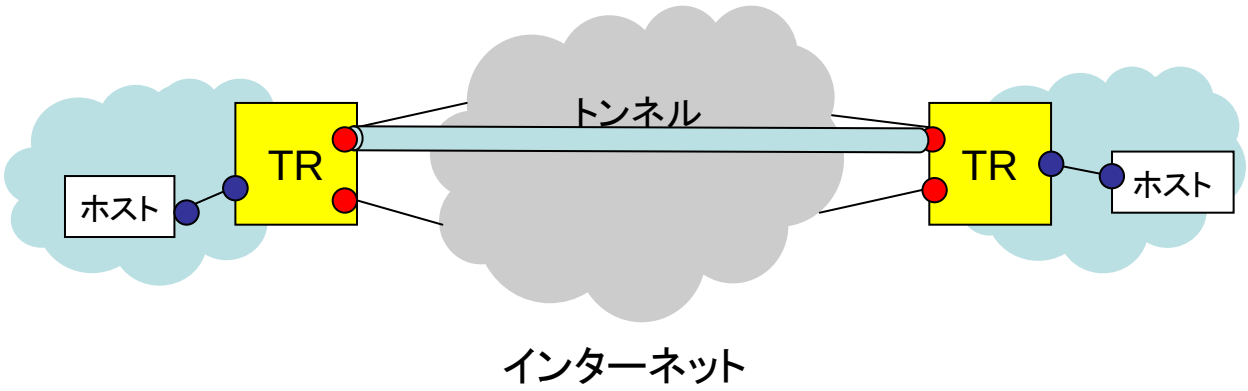
ID-Loc Separation BoFの模様

- **Routing Scalability問題に端を発するID/Loc分割,階層化Locator方式の設計に関する議論**
  - **ID/Loc分割: IPアドレスの持つIdentifier(個体識別子)とLocator(位置識別子)を分割することにより、通信冗長化(マルチホーム)を実現する**
  - **過去の議論を忘れて、一から議論をやり直す**
    - **既存方式(HIP,Shim6)はTE、Routing Scalability等のオペレータからの要求を満たせていない**
  - **要求条件及びデザインスペースについて議論が行われた**
    - **work for both IPv4 and IPv6**
    - **unmodified hosts**
    - **not change the core Internet routing infrastructure**
    - **not expect changes from applications**
    - **have support for dealing with referrals**
    - **incrementally deployable.**
  - **議論継続：2007.5に中間ミーティング開催？→結局開催されず**

Copyright(C) NTT Information Sharing Platform Laboratories.
Copyright(C) NTT Information Sharing Platform Laboratories.

RAM Approaches

- **Middlebox方式が隆盛**
  - **LISP(Locator/ID Separation Protocol)**
    - **Router-based solutionの1つ**
      - **端末には一切手を加える必要が無い**
  - **PASH(Proxying Approach to SHIM6 and HIP)**
    - **Shim6やHIP等のHost-based方式をProxy-boxで実現する**
  - **IPvLX(IP with virtual Link eXtension)**
    - **IPv6 over IPv4トンネル(LISPと類似？)**



Copyright(C) NTT Information Sharing Platform Laboratories.
Copyright(C) NTT Information Sharing Platform Laboratories.

LISP
(Locator/ID Separation Protocol)

Dino Farinacci
Vince Fuller
Dave Oran
Dave Meyer

Cisco Systems

Copyright(C) NTT Information Sharing Platform Laboratories.
Copyright(C) NTT Information Sharing Platform Laboratories.

ID/Loc分離が肝

- IPアドレスの二面性
  - EID(EndpointID): 個体識別子
  - Rloc(RoutingLocator): 位置識別子
- 今まではEID=Rloc
  - BGPで<位置情報＋個体情報>を管理
- EIDとRlocを分離することで
  - BGPで<位置情報>だけを管理
  - <位置情報→個体情報>の関連付けを別方式にて管理
  - 位置情報=PAアドレス、個体情報=PIアドレスとすれば、BGPで管理するのはPAアドレスだけになる
  - マルチホーム/TEはBGPから切り離して別方式にて実現

Copyright(C) NTT Information Sharing Platform Laboratories.
Copyright(C) NTT Information Sharing Platform Laboratories.

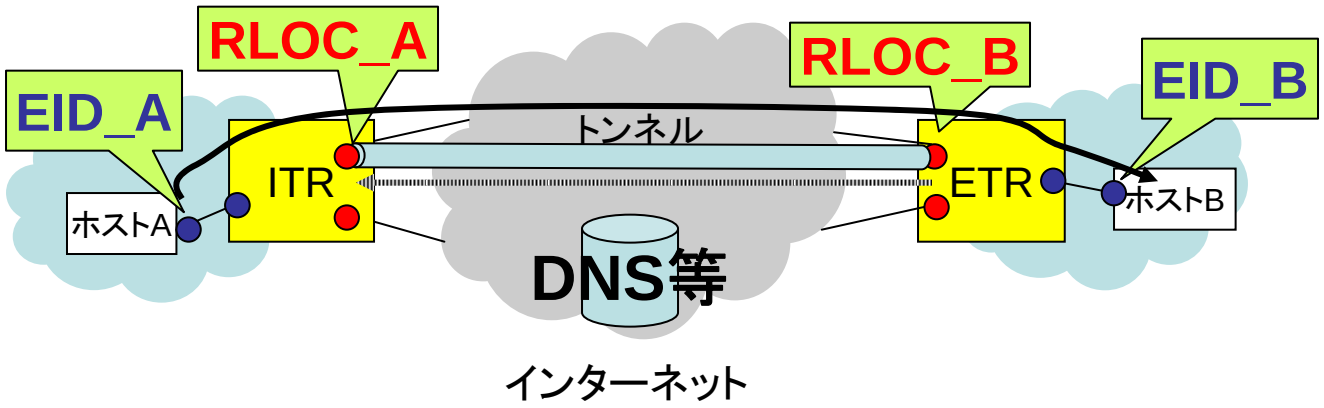
LISPのメリット

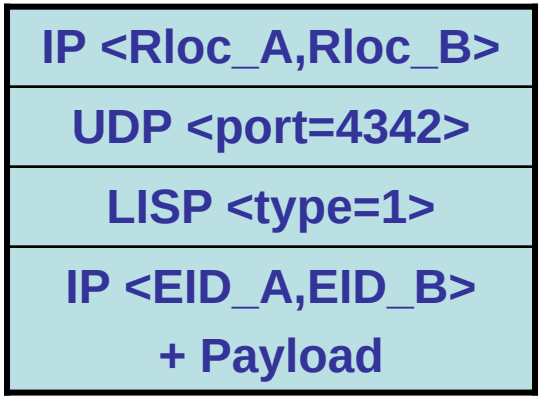
- 経路表を増大させずにマルチホーム/TEを実現
  - BGPでは位置識別子のみ管理
- エンドノードには変更不要
  - サイトGWルータのみ変更
- モビリティを実現可能
  - セッションを切らずに移動可能
- サイトリナンバリングも容易に
  - サイト内のアドレスは変わらない
- IPバージョン非依存
  - IPv4,IPv6両方対応可能
- Incremental Deploymentを想定
  - いきなりアドレス全部付け替え、ではなく徐々に導入可能

Copyright(C) NTT Information Sharing Platform Laboratories.
Copyright(C) NTT Information Sharing Platform Laboratories.

LISP基本動作

- 一言で言うと”サイト間動的UDPトンネリングプロトコル”
  1. ホストAはDNSを参照しホストBのEIDに対して通信開始
  2. ITR(トンネルルータ)がホストBのRloc (Rloc_B)を解決
  3. ITRがアドレス対<Rloc_A,Rloc_B>でカプセル化し転送
  4. ETRはデカプセルしてホストBにパケット転送
  5. ETRはMap_ReplyをITRに送信し、EID_B→Rloc_Bを通知
     ETRに於いてEID_A→Rloc_Aのマッピングキャッシュを保持
  6. ITRでEID_B→Rloc_Bのマッピングキャッシュを保持





LISPデータパケット

Copyright(C) NTT Information Sharing Platform Laboratories.
Copyright(C) NTT Information Sharing Platform Laboratories.

LISP制御パケット

- マッピング(誰が何処にいるのか)情報の管理
  - EIDとRlocの対応関係
    - EID → Rloc1,Rloc2,…
  - Map_Request
    - ETRに、EID(prefix)に対応するRloc群を問い合わせる
  - Map_Reply
    - ETR配下のEID(prefix)とRloc群を返す
    - 優先Rlocの指定, 負荷分散する場合は分散割合の指定
- 到達性情報の管理
  - Map_Request/Replyは到達性確認にも使われる
    - Map_Request/Replyのトランスポートに使われたアドレスの到達性を確認
- 制御パケットは1ppsでrate limit

Copyright(C) NTT Information Sharing Platform Laboratories.
Copyright(C) NTT Information Sharing Platform Laboratories.

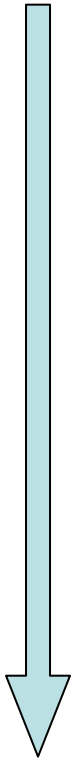
LISPの到達性確認

- 到達性検出方法
  - 制御パケットでの到達性確認
    - Map_Request/Replyにより確認
  - ICMPエラーにより障害検出
    - ICMP Host/NetUnreachはRlocが到達性無し
    - ICMP PortUnreachを受信したらETRがダウン
- 到達性情報の伝達
  - Dataパケット中のLoc-Reach-Bitsにより、ITRからETRに経路の到達性を伝達

Copyright(C) NTT Information Sharing Platform Laboratories.
Copyright(C) NTT Information Sharing Platform Laboratories.

LISPのDeployment方式

- EIDの特性,マッピング管理方式で複数バリエーションが存在
  - LISP1
    - EIDはRoutable (EID=RLOC,外部DB不要)
  - LISP1.5
    - EIDのRoutingは別トポロジーで実現
  - LISP2
    - EIDは非Routable, DNSでマッピング管理
  - LISP3
    - EIDは非Routable, DHT/CONS/NERDによりマッピング管理



Copyright(C) NTT Information Sharing Platform Laboratories.
Copyright(C) NTT Information Sharing Platform Laboratories.

LISPのトラフィックエンジニエアリング

- TR(Tunnel Router)での制御によってTEを実現
  - ホストではなく、中継網によりTEを実現可能
  - TEの制御により、柔軟なTEを実現可能
- エンドサイト,ISP等各レベルでのTEを可能に
  - 再帰的トンネルをサポート
    - 下位NWのTEポリシーをOverride可能
    - VPNでも使える
  - トンネルのリダイレクトが可能
    - 中継ポイントが設定できトラフィック監視/制御等に利用可能

- →以上により、TE権限をネットワークサイドに
  - shim6はエンドノードでのTEが基本だった

Copyright(C) NTT Information Sharing Platform Laboratories.
Copyright(C) NTT Information Sharing Platform Laboratories.

LISPのセキュリティ

- 偽マッピング情報対策
  - 偽Dataパケットによるアドレス注入
    - Map-Request/ReplyによるReturn-Routablity チェック
  - 偽Map-Replyによるアドレス注入
    - Map-Requestに対応していないものは受け付けない
- DoS対策
  - 制御パケット、DataパケットによるMap-Replyの受信にRate-limitを設定

Copyright(C) NTT Information Sharing Platform Laboratories.
Copyright(C) NTT Information Sharing Platform Laboratories.

今後の動向

- IETF69(7/22～27)にてミーティング開催
  - Rrg(routing research group)セッションにて
  - ドラフト(lisp-01)の大枠決定
  - 実装レポートの開始
  - WGになるか？
- IETF70(2007秋)
  - 実証実験結果報告
  - マルチベンダーでの相互接続実験
  - 他のDB方式のプロトタイプについて検討

Copyright(C) NTT Information Sharing Platform Laboratories.
Copyright(C) NTT Information Sharing Platform Laboratories.

LISP3方式の各種提案

- **DHT**
  - Distributed Hash Table をマッピング情報DBに用いる
- **LISP-CONS**
  - A Content distribution Overlay Network Service for LISP
  - 階層化オーバレイネットワークでマッピング情報を管理
- **NERD:A Not-so-novel EID to RLOC Database**
  - 認証されたサーバ群でデータベースを分散管理

Copyright(C) NTT Information Sharing Platform Laboratories.
Copyright(C) NTT Information Sharing Platform Laboratories.

その他の提案

- Ivip (Internet Vastly Improved Plumbing)
  - LISP3に類似
    - IP-in-IPトンネルを用いる
    - TR間の到達性確認は行わない
- APT (A Practical Transit Mapping Service)
  - IDとRlocのマッピング方式
- eFIT (A Proposal for Scalable Internet Routing & Addressing)
  - LISPと類似、Mapping方式の検討

Copyright(C) NTT Information Sharing Platform Laboratories.
Copyright(C) NTT Information Sharing Platform Laboratories.