あなたは誰？

IPにおけるアイデンティティとロケーション

Geoff Huston
Chief Scientist
APNIC

本資料について

本資料はGeoff Huston氏の発表資料

- “Who Are You? Identity and Location in IP”
  http://www3.ietf.org/proceedings/06nov/slides/intarea-1/intarea-1.ppt

をもとに、翻訳したものです。

JPNICはこの翻訳を参考のために提供しますが、その品質に責任を負いません。

IPアドレスとIPアーキテクチャー

構造上、IPアドレスとは:

- 一定のグローバルな空間から選ばれるものである
- 一意であるコンテキストにおける利用を意図している

IPアーキテクチャの観点からのアドレスとは:

- エンドポイント(※)の識別子
- ルーティングの対象
- 転送先検索(Forwarding Lookup)におけるキーとなる値

(※)トランズポート層での通信を行う片側

IPアドレスとは:

ネットワークに接続された機器のインターフェースを一意に識別する手段

- **エンドポイントの識別子**(Endpoint identifier)

ネットワーク内で機器の位置を特定する手段

- **ロケーションの識別子**(Location identifier)

ローカルでのスイッチングの判断を行うにあたっての、フォワーディングテーブルにおける検索キー

- **フォワーディングの識別子**(Forwarding identifier)

以上のように、異なった役割をもった機能を意図的に詰め込んだものがIPアーキテクチャにおける基本的な特性である

IPアドレスモデルにおける挑戦

- ローミングのエンドポイント - Nomadism
- モバイルなエンドポイント – Home and Away
- モバイルネットワーク
- セッションのハイジャックおよび混乱
- マルチホームを行っているエンドポイントと柔軟性のあるセッションの扱い
- 閉じたアドレス領域
- NATおよびALG
- VOIP
- ピア・ツー・ピア・アプリケーション
- 経路の複雑さと規模
- ミドルウェア、DNSおよびリナンバ

もしこんなことが実現できたら…

- ロケーションに依存しない一定のアイデンティティ
- 移動しながらのセッションの維持
- ローカルコネクティビティの変更を横断したセッションの維持
- 長期的に安定したアイデンティティを保つダイナミックなロケーターの利用

つまり、誰もがいつでもどこでもあなた(特定のポイント)へ到達できる。そして、あなた(特定のポイント)から誰に対してもいつでも、どこでも到達できる。

もしこんなことが実現できたら…

IPv6はエンドポイントの「アイデンティティ」を、ロケーションとフォワーディングの機能と切り離すことで解決策を提供してきた

"Second-Comer" (次に来る技術)シンドローム:
この観点は次のように述べることができる：IPv4が非常に複雑なソリューション空間として、実装環境の様々な面を圧迫している根本的な課題を、もしIPv6で直接取り組むことができないのであれば、残念ながらIPv6における実質的な進展は非常に小さい。IPv4より多くのロケーター識別子(locator identifier)をもっただけのものを作り直すことは大きな進歩ではない – むしろ小さく横道にそれることである。

"すでに検討したこと" であることに基づいた警戒:
もちろん、数年にわたる結集した努力の結果、IPv4において解決が困難であることが証明された非常に複雑なネットワーク構築における課題への解を見つけようとすることはIPv6にとっても悩ましい問題である。もしIPv4環境において難しい問題だったのであれば、IPv6においても状況が変わるわけではない。これを理由にこの空間におけるさらなる探求を止めるべきではないが解決策の検証にあたって、ちょっとした慎重さは加えられるべきである。

アイデンティティに求められるものは?

様々な程度での以下の特性:

- 一意性
- 持続性
- 構造
- 明確な適用範囲
- 有効性と正当性
- 権限の明確化

- アイデンティティとは一方的に定められるものではない
  – むしろ、一般に理解されている文脈において生み出された一意性の認知と捉えた方がよいだろう

現在提供されている技術:

- モバイルIPv4
- モバイルIPv6
- アドホックネットワーキング
- NEMO
- HIP
- SCTP
- SHIM6
- Teredo
- ダイナミックDNS
- NAPTR および SNAPTR DNS RRs

選択肢をあげてみよう

プロトコルスタックモデルのどのレベルにおいてもアイデンティティオブジェクト(アイデンティティ情報)を注入することは可能

- トランスポートセッションをまたがる「アプリケーションアイデンティティ」
- スタックロケーションの変更を吸収できる「トランスポートアイデンティティ」
- 保持しているすべてのセッションにおけるロケーションの違いを吸収した「ホストアイデンティティ」

ここでいう「アイデンティティ」とは、通信の両(もしくは複数)サイドにおいて、複数のロケーターが、単一の通信状態にあることを認識するためのトークンである

選択肢をあげてみよう

アプリケーションレベルでのアイデンティティ

- (DNSを使って)ロケーター(位置を示すもの)とマッピングがされている一定のネーム空間の利用
  - ダイナミックなDNSの差分更新
  - DNS NAPTRレコードを使った間接または直接参照(indirection and referral)
  - 一般的なアイデンティティに、サービスに特化したマッピングを加えたもの
  - ENUM
- 一定のランデブー・ポイント(rendevous point)を提供するためのアプリケーションエージェントの利用
  - 例: *sip:gih@sip.apnic.net*
- 課題:
  - DNSは適切な規模とスピードでダイナミックなやりとりに対応できるのか?
  - それぞれのアプリケーションに特化した多様なアイデンティティ群を設けることは望ましいのか (アプリケーション間での照会とハンドオーバー)
  - アプリケーションに特化したアイデンティティ空間において、アプリケーションに特化しながらNAT対応に優れたロケーター非依存のソリューションを、アプリケーションデザイナーが開発することを止めることはできるのか?

選択肢をあげてみよう

トランスポートレベルでのアイデンティティ

- セッション層にてアイデンティティとロケーターを切り離したメカニズムを提供することは可能か?
  - アプリケーションは、セッションを特定するトークン(セッションアイデンティティトークン)の生成と併せてセッションを開始する
  - アイデンティティトークンはロケーターのペアと動的に紐付けられている
  - ロケーターが変更してもセッションのトークンは変更しない
- 階層化の実装
  - アイデンティティアソシエーション(アイデンティティの連携)を行う体制をアプリケーションで担えるようにする
  - プロトコルスタックのより低い層において、アイデンティティとロケーターの紐付けを行う
  - 限定されたコンテキストでセッションの完全性を維持する役割を持った「便宜的なアイデンティティ(opportunistic identity)」の値を利用する
  - 一貫したAPIを提供することによるレガシーアプリケーション(古くからあるアプリケーション)への対応

選択肢をあげてみよう

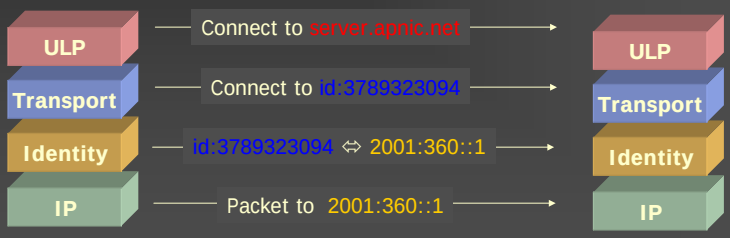
IPレベルでのアイデンティティ

アイデンティティとロケーターの紐付けを複数のセッションで共有することはできるか?

- 共通のエンドポイントに向かうすべてのセッションがマッピングされている状態を実現するための、アイデンティティとロケーターのマッピング(紐付け)によるオーバーヘッドの削減
- セッション指向(session oriented)のトランスポートプロトコルと(可能性としては)データグラムトランザクションの両方に対応した、より包括的なアイデンティティを提供できるようにしたい
- アプリケーションおよびトランズポート層におけるセッションの複雑さを軽減し、IPレベルでエンドポイント単位でのマッピングができる機能を備える

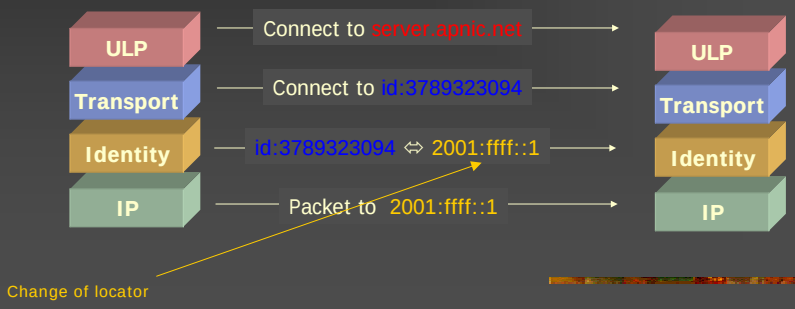
アイデンティティにおける課題

アイデンティティのマッピングはどのように機能するのか?



アイデンティティにおける課題

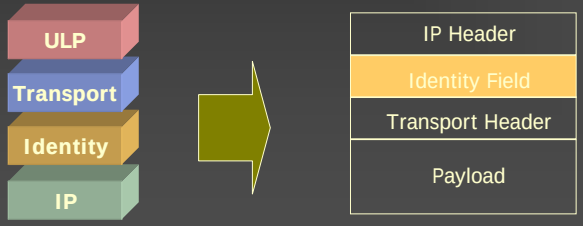
アイデンティティのマッピングはどのように機能するのか?



アイデンティティの実装

従来型

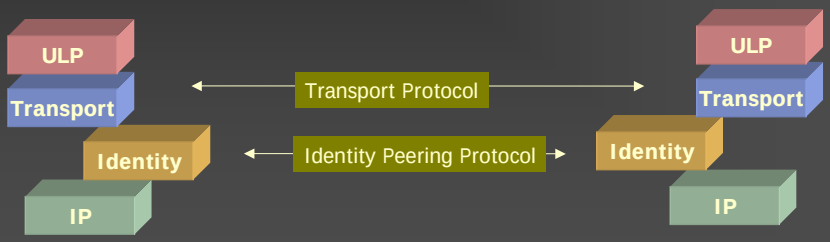
- 上位層のプロトコルデータユニット(PDU)に対してwrapper(包むもの)を加え、インバンド空間を利用して 同じレイヤーでの通信相手(ピアエレメント)と通信を行う



アイデンティティの実装

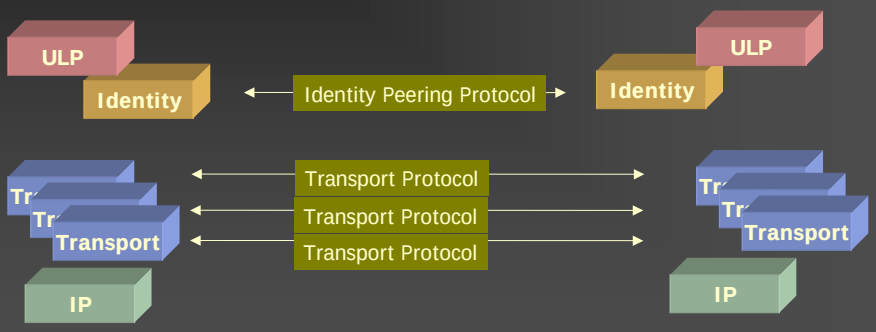
アウトオブバンド型

- プロトコルエレメント(プロトコル階層における各要素)がピア(通信相手)と情報交換できるよう、それぞれ別個のプロトコルを利用する



アイデンティティの実装

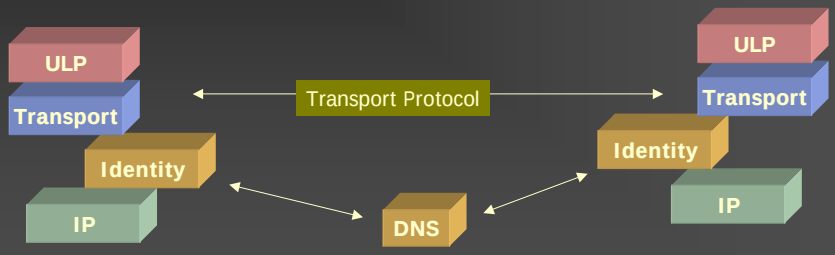
アプリケーションのアイデンティティ: セッション層の上で実現



アイデンティティの実装

参照型

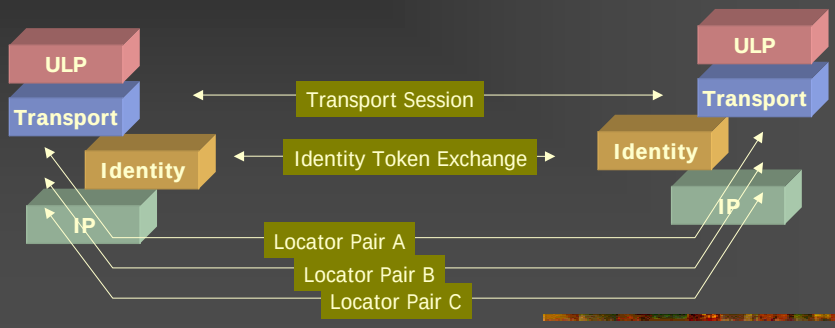
- ピアリングの手段として、第三の参照ポイントを利用(例. DNSの識別子)



アイデンティティの実装

自己参照型

- ロケーター群に該当するトークンとしてその時々に応じた便宜上のアイデンティティを利用する



アイデンティティの種別

- プロトコルの“アドレス空間”より抽出されたアイデンティティトークンを利用する
  - DNS, Appns, “特定のアドレス”をトランスポートが操作
  - IPの機能でロケーターに対応
  - プロトコルスタックエレメント(プロトコルスタックの各要素)でマッピングを実施
- FQDN をアイデンティティトークンとする
  - これは循環依存を生み出すか?
  - これはDNSの機能に対して無理な要求を強いることになるか？
- 体系化されたトークン
  - 新たなトークン空間の、上記の方法と区別される固有の特性はどんなものになるか？
- 体系化されていないトークン
  - 世界的な一意性は必ずしも保証されないアイデンティティ・トークンの自己生成（便宜的なトークン）
  - 検索機能を利用してアイデンティティトークンとロケーターのマッピングをどのように行うか？またはそのようなマッピング機能の実装を回避する術はあるか？

アィデンティティとして利用できそうなもの

- IPv4アドレス
- Centrally Assigned IPv6 Unique Local Addresses(IPv6 ULA)
- 暗号技術を使った公開鍵のハッシュ値
- 暗号技術を使ったロケータのハッシュ値
- 通信の開始にあたり、IPv6アドレスを利用する
- IPv6アドレス
- DNS名
- URI
- 電話番号

アィデンティティを取り巻く課題

- アィデンティティとロケーターを結びつけるもの
  - セッション単位かホスト単位か？
  - 動的か静的か？
  - 設定されているのか、状況に応じて変わるのか？
- アイデンティティ機能の範囲
  - ロケーターに依存しないアイデンティティ
  - 複数ロケーターとの紐付け(Equivalence binding)

ロケーターの選択

- アプリケーションによるアイデンティティ機能の識別
- 一定の領域/文脈におけるアイデンティティ
- アイデンティティの照会とハンドオーバー
- 第三者によるロケーターの書き換え
- バインディング(結合)のセキュリティ
- 意味的な解釈を決定するにあたっての文脈

アイデンティティ分野における高レベルの問題

- エンドポイントの識別子として新たにグローバルに一意であるトークンの分配体系を維持するには多大な労力とコストがかかる
  - 一意性は安くない!
- 既存のトークンセットをアイデンティティセットとして利用した場合の影響
  - リサイクルは危険!
- ロケーターとアイデンティティのダイナミックな紐付けへの対応
  - スピード vs 正確性
- データグラム通信におけるアイデンティティ・ハンドシェイクのためのプロトコルのオーバーヘッド
- アイデンティティの完全性を保つためのセキュリティ

IPv6 とアイデンティティ

64ビットのインターフェース識別子は便宜的なアイデンティティに対応するにあたって豊富なロケーションであるか？

Flow-Id fieldを利用する余地はあるか？

ヘッダーの拡張やオプションは有効か？

パケットインフレーション(パケットの膨張)は必要か?

IPv6はIPレベルにおけるアイデンティティを実現するにあたっての唯一のプロトコルなのか?

- トラスポートセッションでの試みに効果はあるか？
- また、そのような取り組みはIPのバージョンに依存しないことはできるか?

百花齊放，百家爭鳴 *

現在は様々な分野で並行してソリューションを開発する方向に進んでいる:

- 複数人のコミュニケーション向けのアプリケーション(Multi-party Application)
- アプリケーション･エージェント
- ランデブー･プロトコル
- DNSの差分更新およびDNSSEC
- DNSの間接および直接照会(indirection and referral)
- トランスポート層におけるSCTP, HIP
- Shim6
- モバイルIPv6
- モバイルIPv4
- そしておそらくその他多数!

* *百通りの花を咲かせよう、百通りの学説を論争させよう*
毛沢東, 1956

一花独放，一家主鳴 *

- アイデンティティモデルは単一であるべきか?
  - すべての要求を強制的に単一のアイデンティティ体系にまとめることはできるのか？
  - もしくはアイデンティティとして望ましい性質が多用であるがため、それらが衝突することもあり、ひとつの解決策はないのか？
  - これまで考察してきた方法の多くは特定のひとつのアイデンティティ体系のみに重点を置き、他のアイデンティティ体系が並行して実装されていた場合の影響は考慮していない
  - 一方、今日のIPアーキテクチャにアイデンティティ機能に改造を加えようとした場合、例えそれが他のアイデンティティ機能に枝分かれしないとしても、古くからの要求にも対応することがすでに充分に厄介である

* ひとつの花を咲かせよう：*ひとつの学説を主流としよう*

では今後どうすればよいか？

もっと学ばなければいけないことは多いようだ

- ルーティングにおけるスケーリング、リナンバやマルチホームの回避に留まらない
- IPv4、IPv6に留まらない
- 多様なコミュニケーションの環境やサービスへの対応にあたり、敏捷で柔軟なパケットネットワークモデルをもし望むのであれば、発信者の意図が、可能な通信方法とどれほど乖離しているか理解する必要がある