

IPv6 - プロトコルと実装・運用状況

江崎 浩 (東京大学)

1999年12月15日

Internet Week 99 パシフィコ横浜

(社)日本ネットワークインフォメーションセンター編

この著作物は、Internet Week 99 における江崎 浩氏の講演をもとに当センターが編集を行った文書です。この文書の著作権は、江崎 浩氏および当センターに帰属しており、当センターの同意なく、この著作物を私的利用の範囲を超えて複製・使用することを禁止します。

©1999 Hiroshi Esaki, Japan Network Information Center

目次

1	概要	1
2	IPv6 の背景	2
3	IPv6 の基本仕様	4
4	IPv6 アドレス	10
5	経路制御	19
6	IPv6 への移行	20
7	IPv6 システムの現状	23
8	まとめ	26
9	参考	26

1 概要

かつて研究者のものであったインターネットは、誰もが使うネットワークへと変わってきました。現在、インターネットでは、ATM、サテライト、CATV 等、多種多様なデータリンクの上でアプリケーションが実行されており、それらを統一的に繋ぐものとして、TCP/IP が業界標準となっています。

これからのインターネットを考えると、重要なポイントが 2 つあります。

- Quantitative Scalability until Massive Scalability

大量のユーザ、大量のデータにも対応できるスケーラビリティを持つものであること。

- Qualitative Scalability

多様なメディアに対応し、ネットワークの品質が不均一であっても対応できるスケーラビリティを持つものであること。

この講演では、Massive Scalability に対応すべきプロトコルとして開発された IPv6 について、次の事柄を説明します。本講演は、IPv6 への移行に携わられるであろうネットワークオペレータの方を対象にしています。

- IPv6 の背景 (2 を参照)
- IPv6 の基本仕様 (3 を参照)
- IPv6 アドレス (4 を参照)
- 経路制御 (5 を参照)
- IPv6 への移行 (6 を参照)

2 IPv6 の背景

2.1 インターネットに対する要求

現在、インターネットには、「誰にでも（コンピュータに詳しくない人でも）使えること」、「情報家電も含め、どんな機器でも繋がれること」、「どこでも使えること」、「あらゆる目的のために使えること」が求められています。研究開発だけではなく、CALS や電子コマース等の産業活動基盤や生活基盤でも使えるものであり、また、End-to-End でセキュアなコネクティビティを持つものでなければならないのです。

インターネットに関する新しい適用分野、新しい要求と、それぞれに対応する技術をまとめます。

- プラグ & プレイ：IPv6
- モバイル：Mobile IP
- セキュリティ：IPSec
- リアルタイム：Diff-Serv、RSVP
- スケーラビリティ：DWDM、IPv6
- マルチホーム：IPv6
- マルチキャスト：PIM、MBGP
- 信頼性・運用性：MPLS

IETF では、上記のような要求に応えるために、1980 年後半から IPng (IP Next Generation) の検討を始めました。

2.2 現在のインターネットが抱える問題

新しい適用分野、要求に応えるというのもインターネットの課題ですが、インターネットの急激な成長に伴い、緊急に対応しなくてはならない問題が 2 つ出てきました。

- IPv4 アドレスの枯渇

利用者数・ホスト数の増加に伴い、32 ビット空間の IPv4 アドレス（約 43 億）が枯渇してきました。IPv4 での対応として、アドレス付け替えを含む Address Aggregation、NAT (Network Address Translation) / Masquerade、CIDR (Classless Inter-Domain Routing) による可変長ネットマスクが導入されましたが、根本的な解決にはなりません。

- 経路情報の爆発的な増加

80年代には「1組織1クラスBアドレス」の原則によって経路情報の抑制が図られていましたが、現在はCIDR(アドレス+マスク)によって経路情報の抑制を試みています。しかし、インターネットの急激な成長には追いつかず、2年ほど前、4～5万だった全経路数は今や7万に達しています。

2.3 IPv6 へ

IPv4 が直面している問題に対応するために、CIDR、NAT という技術が現在使われています。しかし、アドホックな解決でしかありません。

たとえば、NAT には次のような問題があります。企業内ではそれほどではないかもしれませんが、プロバイダとしては大きな問題と言えます。

- End-to-End モデルが崩れる
 - 出口が1つに限られてしまう。
 - NAT がリポートするとすべての通信が切れてしまう。
 - 通信の双方向性がなくなる。
- IPsec との相性が悪い
 - IPv4 のヘッダを書き換えてしまうので、認証ヘッダが機能しない。
 - ポートを書き換えてしまうので、暗号ペイロード中のポートが見えなくなってしまう。

また、結局のところ NAT では、アドレスも増えませんし、経路情報も減らないのです。十分なアドレス空間を確保し、経路情報を抑制し、セキュリティにも対応し、インターネットに対する要求に応えるためには、NAT やプロキシ等のアドホックな解決ではなく、IPv6 への移行が必要です。

IPv6 では、次に挙げるインターネットの基本原則が維持されます。

- End-to-End アーキテクチャモデル
- 自由な開発 (development)
- 展開 (Deployment)

これらの基本原則が維持されることによって、たとえば、アプリケーションを追加したら、それがネットワークからトランスペアレントにアクセスできるといった、インターネットが持つ「簡単でグローバル」という利点が活かされます。また、End-to-End モデルによって、トランスペアレントなファイアウォールとエンドホストでのセキュリティ機能実現も可能となります。

3 IPv6 の基本仕様

ここでは、次の事柄について説明します。

- IPng 選定の経緯 (3.1 を参照)
- IPv6 と IPv4 の違い (3.2 を参照)
- IPv6 のフォーマット (3.3 を参照)

3.1 IPng 選定の経緯

IPng (IP Next Generation) は IETF ワーキンググループの正式な名称であり、80 年代後半から活動を開始しました。IPng の目標は、「今後のインターネット成長に追従すること」、「新しい要求、市場の要求に対応すること」、「移行性を持つこと」の 3 点でした。そして、94 年 7 月の IETF トロント会議で、次の 3 つの候補が検討されました。

- CATNIP (Common Architecture for the Internet)

理想的ですが、未完成でした。

- SIPP (Simple Internet Protocol Plus)

シンプルですが、16 ビットアドレス空間が問題とされました。

- TUBA (TCP/UDP over CLNP-Addressed Network)

ISO のネットワークアドレスを使うことが、従来技術との整合性の点から疑問視されました。

会議の結果、SIPP のアドレス空間を 128 ビットに拡張した「SIPP16」が採択されました。SIPP16 では CLNP も記述できるので、TUBA の思想も吸収されたと言えるかもしれません。

SIPP16 をベースとして、次世代の IP として開発されたのが IPv6 です。IPv6 については、IPv4 からの移行手法も含め、図 1 に示す RFC が策定されています。

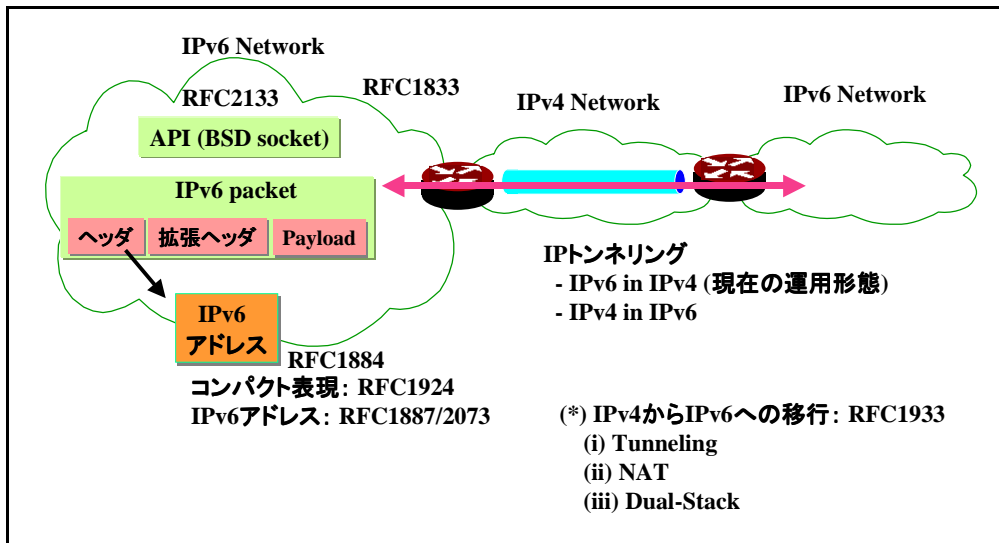


図 1 : IPv6 の RFC

3.2 IPv6 と IPv4 の違い

IPv6 と IPv4 の違いは次のとおりです。一部の項目については、後半で詳しく説明します。

- アドレス空間の拡大
 - 32 ビットから 128 ビットへ
 - アドレスハイアラキ
 - 各種タイプのサポート (Multi-Protocol)
- ヘッダフォーマットの簡略化 (3.3 を参照)
 - 拡張ヘッダのオプション化 (3.3.2 を参照)
 - 統一した形式による処理の単純化
 - 経路上での処理の軽減
- 単純化、処理高速化への対応
 - 8 バイトアライメント
 - IP チェックサムの廃止
 - TTL(Time to Live) から Hop Limit への変更
 - 経路上での細分化 (フラグメンテーション) 処理の廃止 (3.3.4 を参照)
- オプションと機能の拡張性 (3.3.3 を参照)
 - 柔軟性、拡張性を持つオプション形式

- フローラベル機能の導入
 - 詳細未定（ドラフトでは、通信品質の意味付けのためにパケットラベルを使用する、リアルタイム系で使用する等の案がある）
- セキュリティ（認証、プライバシー機能の導入）
 - 認証機構，改ざん防止機構
 - 機密機構
 - End-to-End での実現

ただし、セキュリティについては、IPsec が組み込まれるというだけで、実質的な内容としては IPv4 と同等です。IPv6 にしたからといって、現存するセキュリティの問題が解決されるわけではない点に注意してください。マルチキャストでの鍵配布をどのように行うか等、今後の検討課題が残っています（本講演ではセキュリティについては深く触れません）。

3.3 IPv6 のフォーマット

3.3.1 IPv6 の基本ヘッダフォーマット

IPv6 の基本ヘッダフォーマットを図 2 に、基本ヘッダの各要素を表 1 に示します。

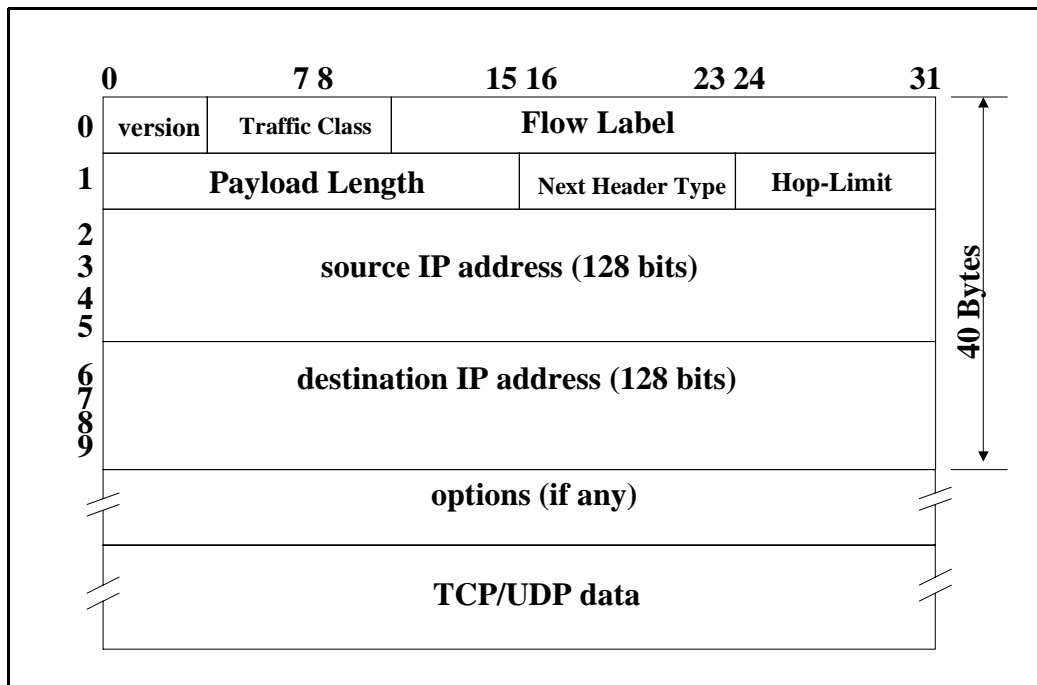


図 2 : IPv6 の基本ヘッダフォーマット

表 1 : IPv6 基本ヘッダの要素

要素名	内容
Version	版番号 6 (IPv6)
Traffic Class	トラフィッククラス。 IPv4 基本ヘッダの TOS は、IPv6 では Traffic Class となった。Diff-Serve が TOS で表現していた DSCP (Different Service Code Point) を表現するために、この 8 ビットを使用することがある。また、ネットワークの混み具合をエンドステーションに通知する、ECN (Explicit Congestion Notification) のために 2 ビットを使用することもある。
Flow Label	フローラベル (詳細は未定)
Payload Length	ペイロード長 (オクテット単位) IPv4 ではペイロード長ではなく、ヘッダ長であった。
Next Header	後続のヘッダのタイプ (RFC1700 で規定)
Hop Limit	中継ホスト数限界。 ルータを通過するごとに 1 減。0 でパケット破棄。 IPv4 基本ヘッダの TTL の名称が変わった。
Source Address	発信元アドレス (128 ビット)
Destination Address	宛先アドレス (128 ビット)

IPv6 の基本ヘッダは、表 1 に示した以外に、次の点が IPv4 の基本ヘッダと異なります。

- フラグメンテーションの情報は、基本ヘッダから拡張ヘッダへ移った。
- IP チェックサムが廃止された。伝送システムの品質が上がったので、データリンクレベルで対応するか、アプリケーションでチェックする。
- Protocol の情報は、Next Header に入れる。

3.3.2 IPv6 の拡張ヘッダ

IPv6 では拡張ヘッダはオプションとされます。IPv6 パケットにおける拡張ヘッダの位置と拡張ヘッダに含まれる情報を、図 3 に示します。

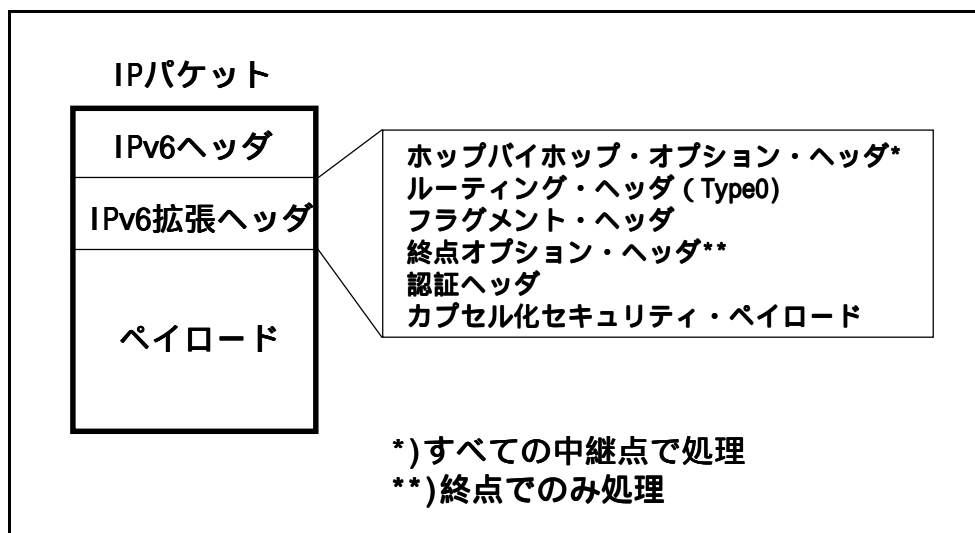


図 3 : IPv6 の拡張ヘッダ

拡張ヘッダに含める情報は、処理の効率化を期待して、図 3 に示した順序で並べることが推奨されています。ただし、この順序でなくても処理できなければいけないとされていますので、実質的には決まっていないのと同じです。

また、IPv6 の拡張ヘッダには、次の特徴があります。

- 拡張ヘッダ長は 8 オクテットの整数倍とする。
- すべてのノードで処理すべきものと、終点でのみ処理するものと、それ以外を分離することによって、処理を効率化する。
- 処理できないヘッダは、ICMP (Internet Control Management Protocol) でエラー返送する。

IPv6 の拡張ヘッダは、図 4 に示すようにチェーンして使用されます。NH (Next Header type) に、次の拡張ヘッダの種類が示されます。

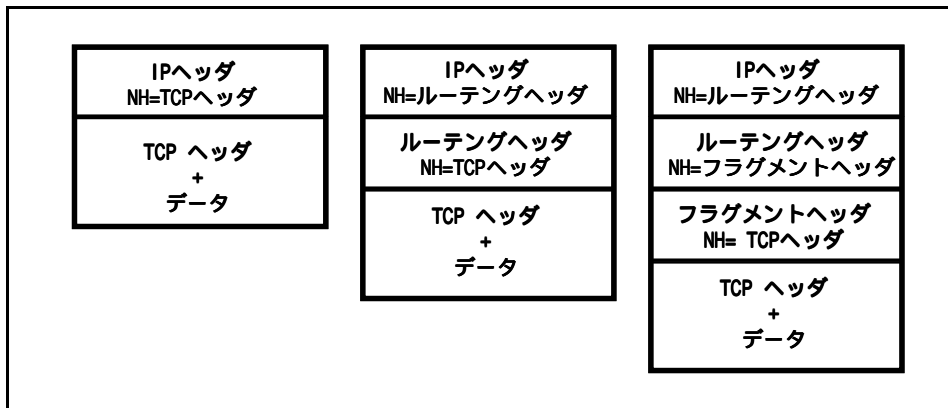


図 4 : IPv6 拡張ヘッダのチェーン

3.3.3 オプション

IPv6 パケットのオプション (options) フィールドは、図 5 に示すような TLV (Type-Length-Value) 形式の可変長フォーマットをとります。この TLV 形式により、高い汎用性をもって、情報を End-toEnd で伝えることが可能になります。さまざまな長さのデータを挿入できますし、Option Type を増やせば、新しいデータにも対応できるからです。

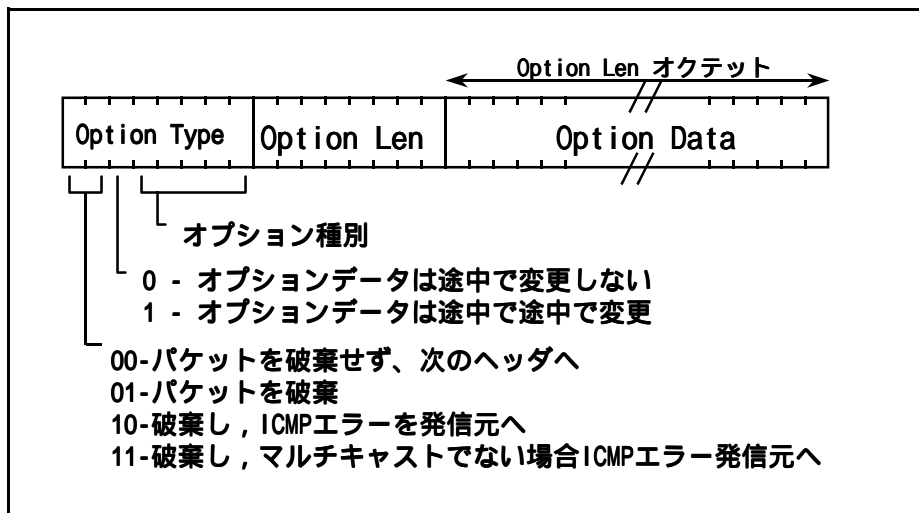


図 5 : TLV 形式のオプション

3.3.4 フラグメンテーション処理

負荷がかかるという理由から、IPv6 では経路上でのフラグメンテーションは行わなくなりました。IP パケットを投げる前にフラグメンテーションを行い、処理済みのものを経路に送出するようにするのです。このために、IPv6 では「パス MTU 発見プロトコルを標準で実装すること」とされています。

パス MTU 発見プロトコルは、動的にパス MTU を発見するもので、まず、最初のリンクの MTU を初期値として IP パケットを送出します。そして、ICMP の Too Big Message を受け取った時点で、フラグメンテーションを行います。また、それ以外にも、適当な周期で再調査を行います。

なお、マルチキャストの場合の最小パス MTU の問題は、現在は未解決です。

4 IPv6 アドレス

ここでは、次の事柄について説明します。

- アドレス空間 (4.1 を参照)
- アドレス体系 (4.2 を参照)
- ユニキャストアドレス (4.3 を参照)
- マルチキャストアドレス (4.4 を参照)
- 割り当ての現状と問題点 (4.5 を参照)
- NDP (4.6 を参照)
- DNS (4.7 を参照)

4.1 アドレス空間

IPv6 のアドレス空間は 128 ビットです。IPv4 と比較すると次のようになり、アドレス枯渇の問題は解決されます。

- IPv4 : $2^{32} = 4,294,967,296$
- IPv6 : $2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456$

4.2 アドレス体系

4.2.1 アドレス表記

IPv6 では、128 ビットアドレスを「8つの16進数を:(コロン)で区切る」表記で、次のように表現します。

```
3ffe:0501:0008:1234:0260:97ff:fe40:efab  
ff02:0000:0000:0000:0000:0000:0000:0001
```

連続する0については、「::」として省略することができます(1カ所のみ)。

```
FF01:0:0:0:0:0:0:43      FF01::43  
0:0:0:0:0:0:FF01:9123   ::FF01:9123
```

IPv4 の「*.*.*.*」表記も混合することができます。

IPv4/IPv6 ノードのアドレス

```
0:0:0:0:0:0:13.1.68.3
```

IPv4 オンリーノードのアドレス

```
0:0:0:0:0:FFFF:129.144.52.38
```

ただし、Web アドレスのように「:」を含む文字列におけるアドレス表記は少々困ります。まだ、最終決定されていませんが、[と]でアドレスを囲む表記がおそらく使用されることになるでしょう。

```
http://[3ffe:501:8:1234:260:97ff:fe40:efab]/foo/
```

4.2.2 アドレスタイプ

IPv6 のアドレスは、図6に示すように3種類あります。

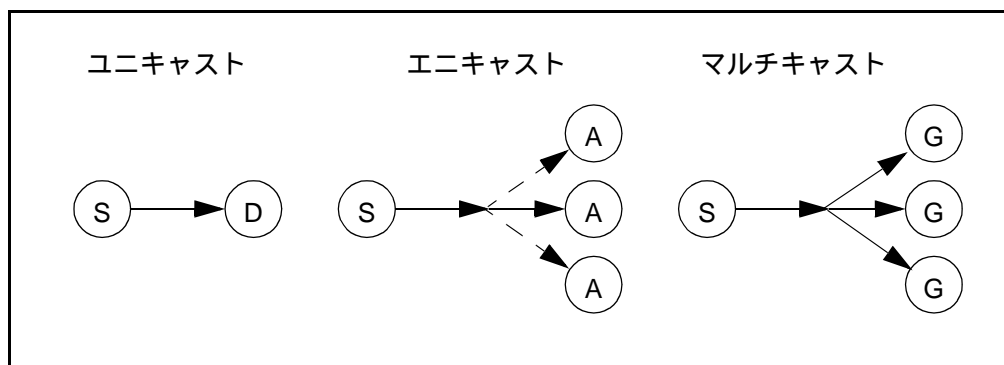


図6 : IPv6 の3種類のアドレス

- ユニキャスト (Unicast) アドレス

1 つのインタフェースを識別するアドレスです。IPv6 では「インタフェースにアドレス」という考え方が重要です。また、マルチホームアクセス等のために、1 つのインタフェースに複数のアドレスを割り当てることも可能です。詳細については、4.3 を参照してください。

- エニキャスト (Anycast) アドレス

グループのうち経路上一番近いインタフェースに配送するためのアドレスです。IPv4 では実現されませんでした。IPv6 では使用します。プラグ & プレイのために有用です。

- マルチキャスト (Multicast) アドレス

グループのすべてのインタフェースに配送するためのアドレスです。IPv4 のブロードキャストはマルチキャストの一種として処理します。詳細については、4.4 を参照してください。

アドレスタイプは FP (Format Prefix) で指定します。たとえば、マルチキャストアドレスの FP は「1111 1111」です。

4.3 ユニキャストアドレス

ユニキャストアドレスは、1 つのインタフェースを識別するアドレスであり、プリフィックスの最大長マッチによって経路を決定します。ルータは、一番深いところまでネットマスクが当たったところで、経路を探します。ユニキャストアドレスの経路決定の方法は、CIDR と同様です。

4.3.1 集成可能なユニキャストアドレスと TLA

IPv6 では、従来のプロバイダベースのアドレスに代わり、集成可能なユニキャストアドレス (Aggregatable Global Unicast Address) としてアドレスが階層的に割り当てられます。

ユニキャストアドレスのフォーマットを図 7 に示します。

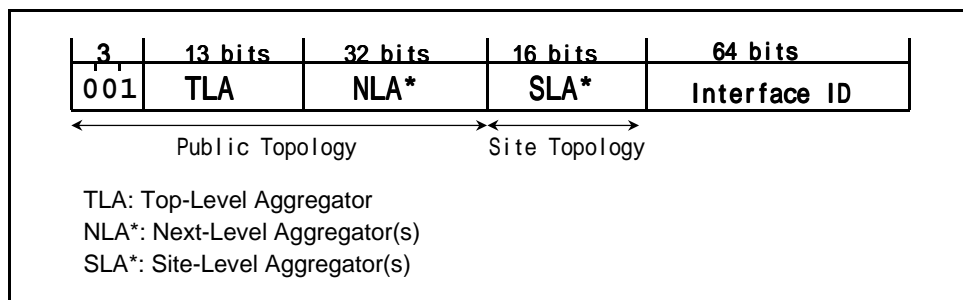


図 7 : 集成可能なユニキャストアドレス

ここで、TLA (Top-Level Aggregator) は 13 ビットなので、 $2^{13} = 8,192$ し
か割り当てることができません。プロバイダとしては、TLA が欲しいと
ころでしょうが、非常に限りがありますので、下記の BCP (Best Current
Practice) を定め、それを満たす場合にのみ TLA を割り当てることとして
います。

- 割り当てから 6 カ月以内に IPv6 のサービスを開始すること
- 他のプロバイダにトランジットすること (リーフでない)
- NLA アドレス割り当てを行うこと
- 他のすべての TLA と通信できること (フィルタしてはいけない)
- 利用統計情報の収集と報告を行うこと

4.3.2 インタフェース識別子

図 7 に示したインタフェース識別子 (Interface ID) は、ホストインタフェ
ースを識別するものであり、IEEE の 64 ビット識別子である EUI-64 をその
まま使用します。EUI-64 は、従来より使用されていた MAC アドレス (802
アドレス) が拡張されたものです。インタフェースが持つ識別子をその
まま使用することは、ブートした瞬間に IP アドレスが使用できることに
繋がります。

EUI-64 は、24 ビットの company_id と 40 ビットの extension_id から成り
ます。48 ビットの 802 アドレスを持つインタフェースについては、FFFE
を挿入することによってマッピングします。

34-56-78-9A-BC-DE 34-56-78-FF-FE-9A-BC-DE

4.3.3 ローカルなユニキャストアドレス

IPv6 では、ローカルなユニキャストアドレス (Local-use IPv6 Unicast
Addresses) が用意されています。これは、IPv4 におけるプライベートア
ドレスを一般化したもので、次の 2 種類があります。

- リンクローカル (同一リンク内でローカルなアドレス)
たとえば、家庭内でのネットワークで使用します。
- サイトローカル (同一サイト内でローカルなアドレス)
たとえば、キャンパス内で使用します。

ローカルなユニキャストアドレスは、NDP (従来の ARP) や DHCP のよ
うな、リンク内でのノード管理のために使用されます。また、インター
ネットに未接続のネットワークで、ローカルなユニキャストアドレスを
割り当てておき、後でプリフィックスを置き換えるだけでインターネッ
トに接続するという使い方もあります。

ローカルなユニキャストアドレスのフォーマットを図 8 に示します。

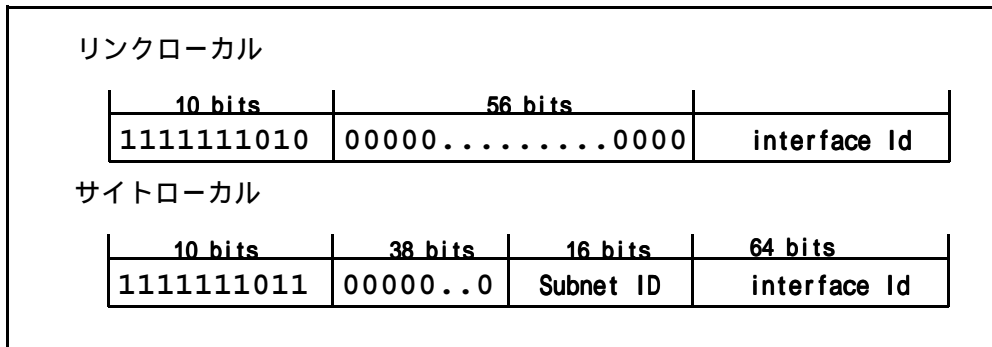


図 8 : ローカルなユニキャストアドレス

また、次の 2 つは、特別な目的のために使われるローカルなユニキャストアドレスです。

- 0:0:0:0:0:0:0

未指定アドレス (Unspecified Address) です。初期化前の IPv6 ノードの始点アドレスでのみ利用されるものです。
- 0:0:0:0:0:0:1

ループバックアドレスです。IPv6 データを自分自身に送るときにのみ使用します。

4.4 マルチキャストアドレス

マルチキャストアドレスは、複数のインタフェースを識別するためのアドレスです。マルチキャストアドレスのフォーマットを図 9 に、定義済みのマルチキャストアドレスを表 2 に示します。

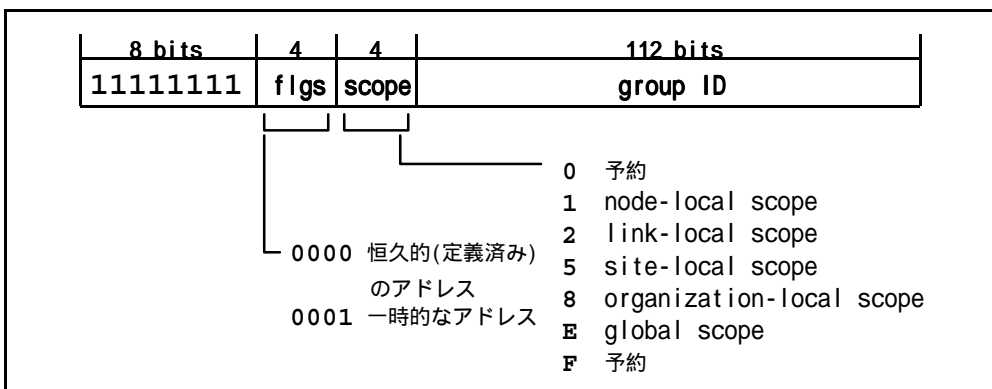


図 9 : マルチキャストアドレスのフォーマット

表 2：定義済みのマルチキャストアドレス

アドレス	機能
FF00:0:0:0:0:0:0:0	予約。
FF01:0:0:0:0:0:0:0 ~ FF0F:0:0:0:0:0:0:0	予約。
FF01:0:0:0:0:0:0:1	ノード内のすべての IPv6 ノード。
FF02:0:0:0:0:0:0:1	リンク内のすべての IPv6 ノード。
FF01:0:0:0:0:0:0:2	ノード内のすべての IP ルータ。
FF02:0:0:0:0:0:0:2	リンク内のすべての IP ルータ。
FF02:0:0:0:0:0:0:C	DHCP サーバ/リレーエージェント。
FF02:0:0:0:0:1:x:x	要請ノードアドレス。

なお、図 9 中の SCOPE は、「どこまでマルチキャストアドレスを伝搬させるか」という範囲を決めるものです。SCOPE の node-local は、たとえば、マルチプロセッサのために使用します。

4.5 割り当ての現状と問題点

ここで、IPv6 においてノードとルータが持つアドレスについて、それぞれまとめておきましょう。

- ノードの持つアドレス
 - 各インタフェースごとのリンクローカルアドレス
 - 割り当てられたユニキャストアドレス
 - ループバックアドレス
 - 全ノードマルチキャストアドレス
 - 要請ノードマルチキャストアドレス
 - ノードの属するその他のマルチキャストアドレス
- ルータの持つアドレス
 - 各インタフェースごとのリンクローカルアドレス
 - 割り当てられたユニキャストアドレス
 - ループバックアドレス
 - 接続されているリンクのサブネットルータ・ユニキャストアドレス
 - 設定されたユニキャストアドレス

- 全ノード・全ルータマルチキャストアドレス
- 要請マルチキャストアドレス
- ルータの属する、その他のマルチキャストアドレス

次に、IPv6 アドレスの割り当ての現状について説明します。IPv6 アドレスについては、p-TLA (pseudo-TLA) による実験的な割り当てが行われてきましたが、1999 年 9 月から商用割り当ても始まりました。ARIN、RIPE、APNIC が s-TLA (sub TLA) の割り当てを行っています (図 10)。

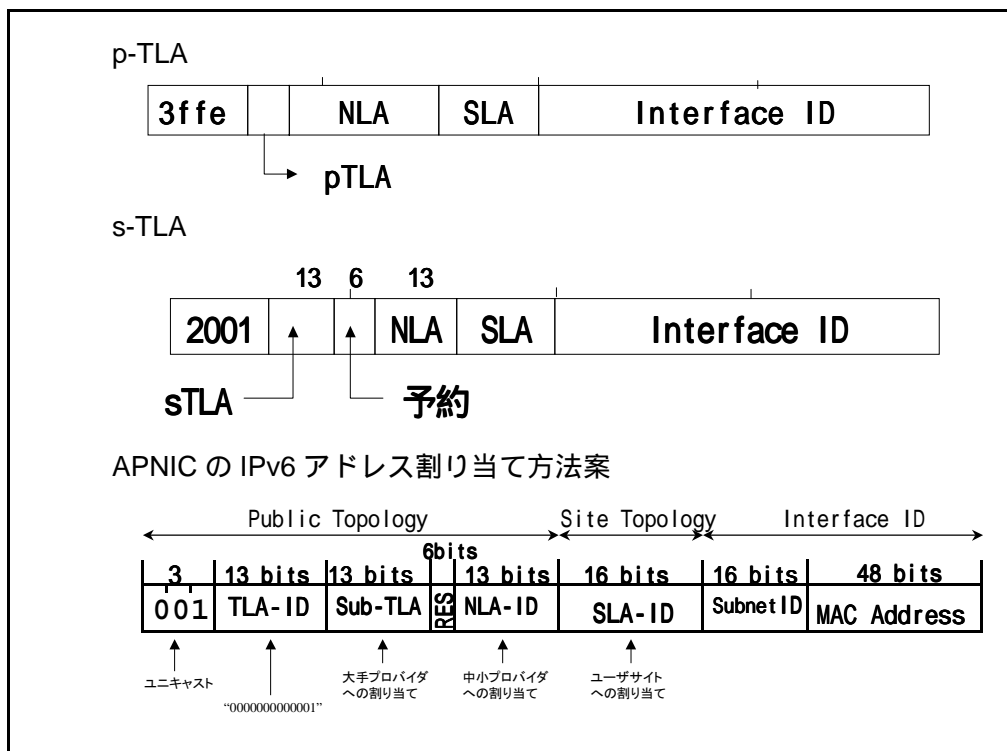


図 10：実際の IPv6 アドレス割り当て

IPv4 アドレスの抱える問題を解決すべくスタートした IPv6 アドレスですが、「TLA が本当に足りるのか」、「ユニキャストアドレスは、マルチホームの場合やプロバイダを変更した場合どうするのか」といった課題があります。

ユニキャストアドレスの課題については、「8 バイト (Routing Group と STP) + 8 バイト (End System Designator)」のフォーマットをとる GSE (Global Site End-system) が提案されました。GSE はモバイル IP にとってはメリットがあるのですが、Routing Group を境界ルータで書き換えなければならないことから、IETF では理解を得られませんでした。

4.6 NDP

NDP (Neighbor Discovery Protocol) は、隣接ノード、つまり同一リンクに接続されているノードを探すための機能です。NDP は ARP の機能を含んでおり、ICMP の一部として実装されます。NDP には、次の機能があります。

- Router Discovery
- Prefix Discovery
- Parameter Discovery
- Address Autoconfiguration
- Address Resolution
- Next-Hop determination
- Neighbor Unreachability Detection
- Duplicate Address Detection
- Redirect

NDP によって隣接ルータを見つけ出すことができるので、そのルータの周期的な情報広告を利用すれば、ホストは自分が属するネットワークのプリフィックス等の情報を得て、自アドレスを自動設定することができます。ホストがクライアントに、ルータがサーバとなるサーバ/クライアントモデルと言えます。

なお、ICMP と IGMP (Internet Group Management Protocol) については、IPv6 でも IPv4 と同様の機能が提供されます。たとえば、ping、traceroute、Router_Discovery 等のアプリケーションも、同じように使用できます。ICMP の機能を図 11 に示します。

NDP の実装を考えると、DHCP (Dynamic Host Configuration Protocol) は IPv6 では不要にも見えます。しかし、IPv6 においても DHCP は用意されており、ステートレス方式とステートフル方式という 2 種類の IP アドレス割り当て方法が定められています。

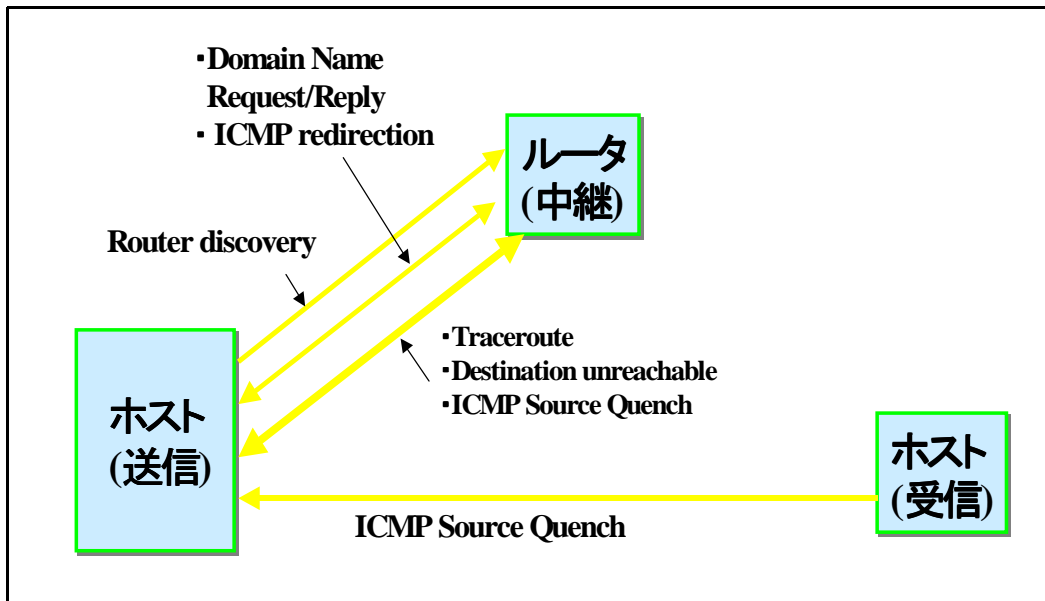


図 11 : ICMP

4.7 DNS

IP アドレスとドメイン名の対応付けを行う DNS (Domain Name System) は、IPv6 でも運用上、大変重要な機能です。ルートサーバのコミュニティで、現在運用が検討されていますが、たとえば、次のものが追加されます。

- 正引きのための AAAA レコード
- 逆引きのための IP6.INT ドメイン

4321:0:1:2:3:4:567:89ab

b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.

0.0.0.1.0.0.0.0.0.0.0.0.1.2.3.4.IP6.INT.

5 経路制御

IPv6 では、経路制御を CIDR によって行います。経路情報プロトコルについては、IPv4 で使用されていたものをアドレス拡張したりすることによって、IPv6 対応が進められました。現在運用されているネットワークは、RIPng と BGP4+ で運用されています。

- RIP は RIPng として IPv6 対応済み。
- OSPF も IPv6 対応済み。ゼブラ等、実装も出ている。
- BGP もマルチプロトコル化した際に、IPv6 対応済み。

IPv6 では、4.6 で説明したように NDP を利用できます。NDP によってエンドステーションは、ルータ通知による情報からグローバルなアドレスを生成できるほか、デフォルト経路の情報も得ます。

ここで、マルチホームにおける IPv6 の経路制御の例を見てみましょう。マルチホームネットワークでは、1つのインタフェースに複数のアドレスが割り当てられますが、たとえば、企業で冗長性のためにマルチホームネットワークを使用するのであれば、図 12 のような経路制御を行うように、ルータを設定する必要があります。こうすれば、ISP1 に障害が発生しても、トンネリングによって ISP2 経由の経路を確保することができます。これは、BGP の考え方を改造したオペレーションといえます。

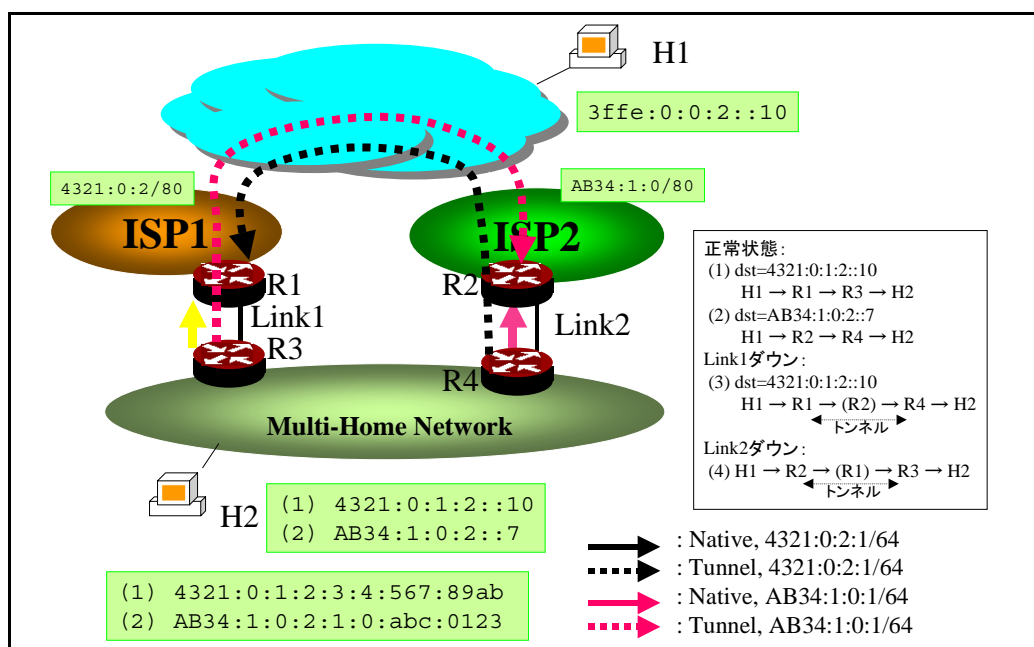


図 12：マルチホームネットワークの経路制御の例

6 IPv6 への移行

ここで、IPv4 から IPv6 への移行について考えてみましょう。移行にあたって検討、実施しなければいけない事柄には、次のものがあります。

- IPv4 と IPv6 アドレスの割り当て方法（完了）
- ホストやルータのアップグレードや展開
- IPv6 アドレスレコードタイプをサポートする、DNS サーバの展開方法
- 個々のインターネットサイトのIPv6への移行のためのオペレーション計画
- インターネット全体の IPv6 への移行のためのオペレーション計画

また、移行の際には、次の要求を満たさなければなりません。

- IPv6 ノードへのアップグレードは、現存する IPv4 ノードとは独立に行えること
- IPv4 と IPv6 の混在環境を実現できること
- 現存する IPv4 アドレスは、IPv6 でも利用可能とすること

IPv6 への移行ストーリーは、次の 3 ステージに分けることができます。

- 現在
 - IPv4 オンリーノードのみ
- 初期
 - IPv4/v6 デュアルノード
 - IPv6 アドレスフォーマットの IPv4 アドレス
 - IPv4 ネットワーク上での IPv6 のトンネリング
- 後期
 - IPv6 インフラと IPv4 インフラの混在
 - IPv4/v6 の相互変換（オプション）
 - IPv6 ノードの展開

上記の移行過程において重要なポイントは、IPv4 ノードと IPv6 ノードの通信をどのように行うかということです。もし、IPv4 オンリーノードのホストとIPv6オンリーノードのホストが通信する必要がないのであれば、図 13 に示すようなトンネリングによる接続でかまいません。

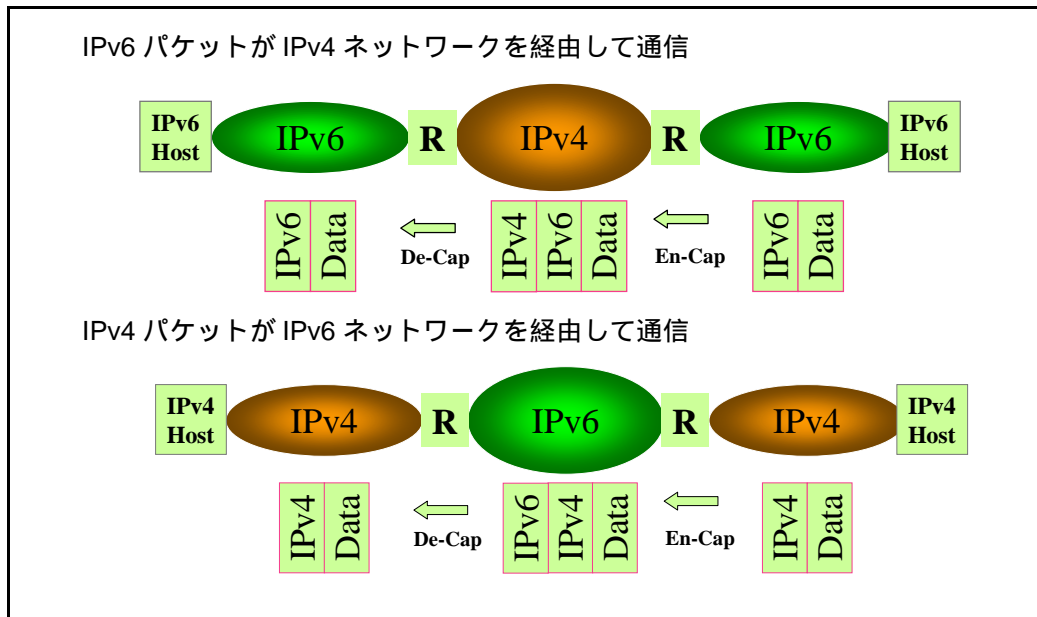


図 13 : トンネリングによる IPv4 ホストと IPv6 ホストの通信

しかし、IPv4 ホストと IPv6 ホストが通信する場合は、変換ルータを用意しなければなりません。変換には、次の 2 つの方法があります。

- NAT

ルータが IPv4 と IPv6 のアドレスを変換します。たとえば、図 14 (A) のように、IPv4 ホスト側では、ソースアドレスがルータアドレスになっているパケットを受け取ります。また、図 14 (B) のように、デスティネーションアドレスをルータのアドレスとしたパケットを、IPv6 ホスト側に投げます。

- SOCKS

プロキシサーバに近い、アプリケーションゲートウェイである SOCKS を利用する方法です (図 15)。考え方としてはファイアウォールと同じです。必要に応じて処理を外部 DNS、内部 DNS に振り分けます。

SOCKS は NAT ほど複雑な処理を行いません。スケーラビリティが高いことが実験からも証明されています。NAT と SOCKS の中間の方法とも言える RSIP もありますが、アドホックなものであり、スケーラブルかどうかは不明です。

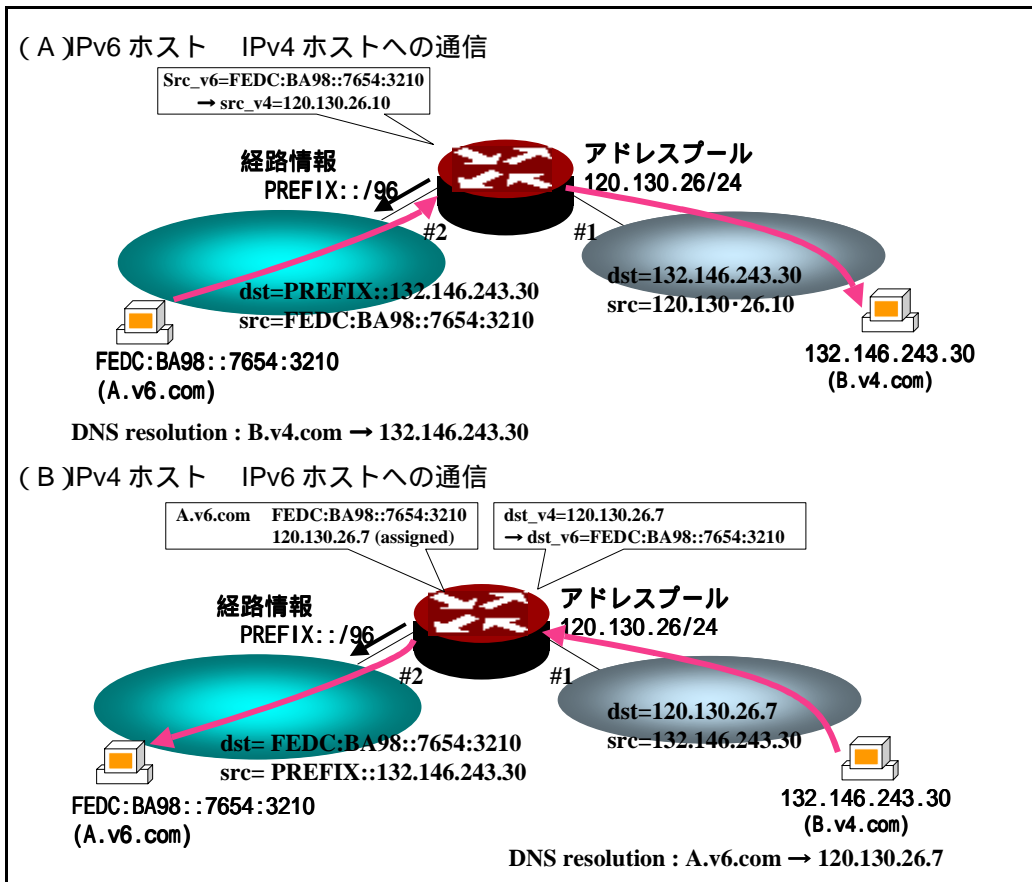


図 14 : NAT による IPv6 ホストと IPv4 ホストの相互接続

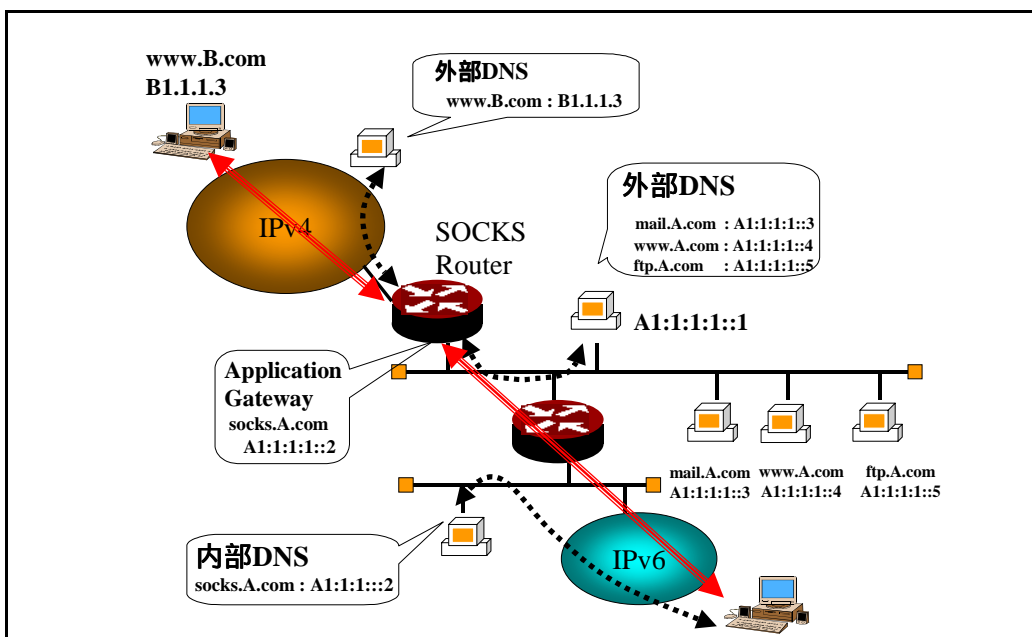


図 15 : SOCKS による IPv4 ホストと IPv6 ホストの相互接続

7 IPv6 システムの現状

ここでは、次の事柄について説明します。

- IPv6 の開発、実装の状況 (7.1 を参照)
- IPv6 の運用状況 (7.2 を参照)

7.1 IPv6 の開発、実装の状況

IPv6 については、RFC1883 (IPv6 Specification)、RFC1884 (IPv6 Addressing Architecture)、RFC1885 (ICMPv6)、RFC1886 (DNSv6) 等、基本的な機能は既に決定されています。アドレス割り当ての運用、セキュリティアルゴリズム、鍵管理等、検討が続けられている機能もかなりありますが、IPv6 は実装および相互接続検証のフェーズに入っていると言えます。

日本国内では、WIDE プロジェクトによる統合化実装 KAME において、複数ベンダーのコード統合が進められています。KAME の概要は次のとおりです。

- ルーティングプロトコル
 - マルチキャスト：PIM-SM & PIM-DM (開発終了)
 - ユニキャスト：OPSF for IPv6 (開発中)
- QoS/CoS コントロール
 - Diff-Serv Integration with ALTQ (Sony-CS) (開発終了)
 - BB (Bandwidth Broker) with COPS
- モバイル IP
 - エリクソンからの提供を受ける予定
- IPv6/v4 相互接続
 - NAT (Hitachi、KAME)
 - SOCKS (富士通、NEC、KAME)
- ラベルスイッチ (MPLS)
 - IPv6、PIM、Diff-Serve、BB

国際的には、IPsec による NRL、フランスの INRIA という実装もありましたが、NRL は予算の関係から、INRIA は方向性の変化から実装が進んでいません。このため、実質的には、UNIX 標準コードの実装は KAME で進んでいます。

また、エンドホスト、ルータへの IPv6 の実装も進んでいます。エンドホストについては、各 OS で IPv6 に次のように対応できるようになってきています。

- Microsoft Windows
 - Bump-In-The-Stack (日立製作所)
 - Windows 2000
- Apple MAC OS 9
- UNIX with KAME Stack
 - Free-BSD、BSDI、NetBSD、BSD/OS
- Solaris
- LINUX (オリジナルの v6 コードが動作)

図 16 に日立製作所の Bump-In-The-Stack のしくみを示します。Bump-In-The-Stack はデバイスドライバに変換モジュールを組み込む形のフリーソフトウェアであり、接続実験でも動作が確認されています。

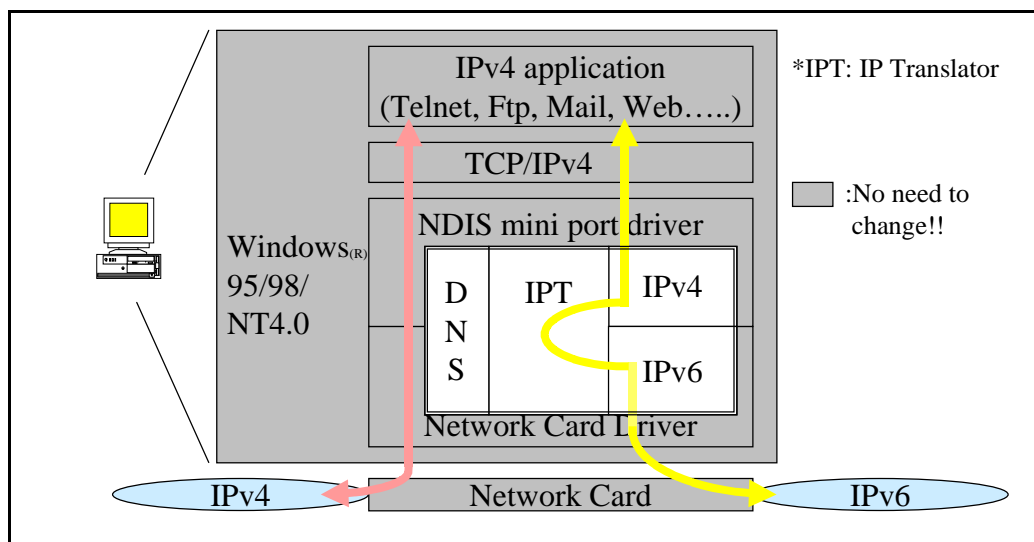


図 16 : Bump-In-The-Stack

現在、相互接続実験については、横河電機、YDC、WIDE による TAHI プロジェクトが活発に進められています。先行していたニューハンプシャー大学のプロジェクトは活動が止まっています。

7.2 IPv6 の運用状況

ネットワークの構成要素に関する実装がほぼ完了した今、IPv6 の運用は実験ネットワークから商用クオリティのネットワークへ移ろうとしています。s-TLA によるアドレス割り当ての開始もその流れの中の 1 つです。ルーティングレジストリ、アドレスレジストリの開発も進んでいます。IX for IPv6 については、6TAP のほか、NSPIX6 も 1999 年 9 月よりオペレーションを開始しています。

また、リサーチネットワークとして、6REN (IPv6 Research and Educational Network) の活動が始まりました。これはプロダクションクオリティのネットワークを作ろうという動きの 1 つです。業界では、Telebit が v6 フォーラムを設立したほか、日本では IJ が 1999 年 9 月から IPv6 サービス (IPv4 ユーザに対する IPv6 トンネリング) の提供を開始する等、新しい動きがあります。

日本の IPv6 ネットワークの状況を、図 17 に示します。

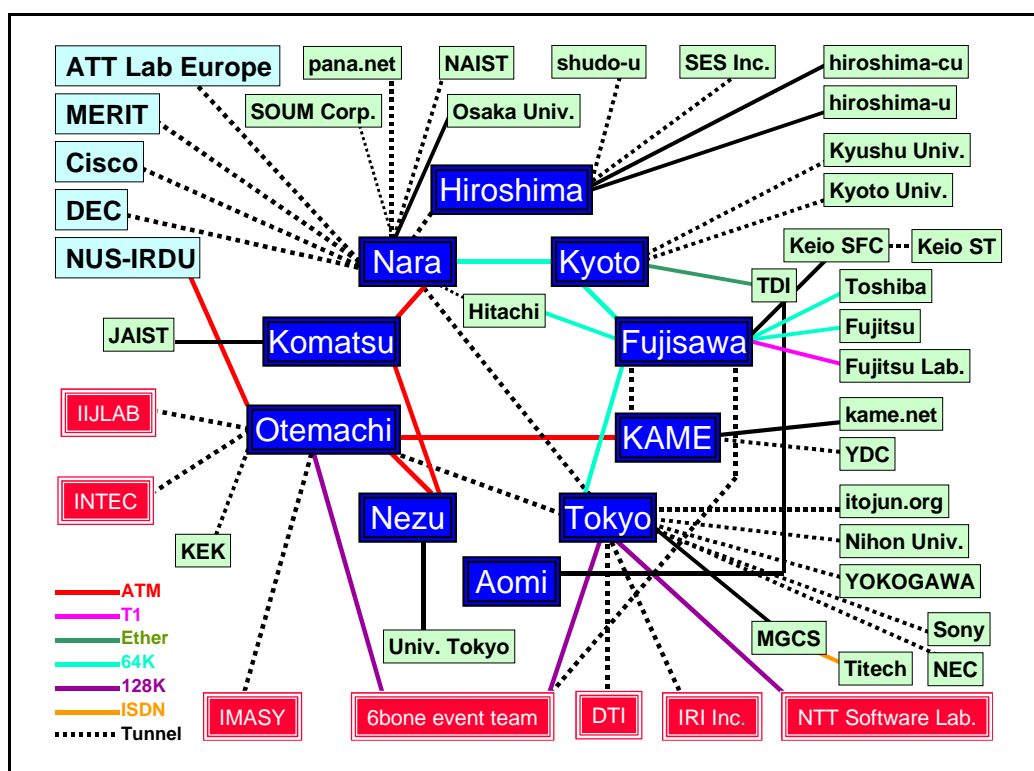


図 17 : 日本の IPv6 ネットワーク

8 まとめ

IPv6 への流れは、もう止められません。

IPv4 アドレスの枯渇や経路情報の抑制という差し迫った問題の解消はもとより、アドレス割り当てや構成管理を容易にするためにも、IPv6 化は必須であると言えます。ただし、セキュリティやモバイルについては、検討課題が残されています。

実装も進み、ルータでもエンドホストでも IPv6 化は Ready と言えます。実績を積み、スムーズな移行手順を考え、実行していくフェーズに入っているのです。その過程において、重要な役割を果たすのはネットワークオペレータの皆さんなのです。

9 参考

本講演の準備においては、次の文献を参考にしました。

- IPv6：佐野晋（日本電気） Networld+Interop96 チュートリアル資料
- RFC 事典：ASCII 出版
- 電子情報通信学会全国大会資料（1998 年 10 月）：村井純

また、次の URL に、本講演に関連する詳細情報があります。

- IPv6 実装について
<http://playground.sun.com/pub/ipng/html/>
<http://www.kame.net/>
- レジストリシステムほかの稼動状況について
<http://www.v6.sfc.wide.ad.jp/6bone/>