2005 年 IPv6 移行ガイドライン

ISP セグメント

2005 年 3 月

IPv6 普及・高度化推進協議会

移行 WG　ISP SWG

目次

はじめに

本ドキュメントは、中小 ISP 及びアクセス網の構築運営に携わる Operator、SIer を対象に、中小 ISP 及びアクセス網事業者が今後 IPv6 を導入するにあたり、検討すべき一般的な項目、指針、方法について記述しています。

ここで記載される内容は、考え方の例を示すものであり、唯一の解ではありません。読者が、自らの指針により IPv6 の導入を検討する際、このドキュメントを参考に応用が図れるよう記述しました。

概要

セグメントの特徴

・中小 ISP セグメントの特徴を分析、記述しました。

・アクセス網と顧客、及び ISP との接続方法の特徴を分析、記述しました。

アクセス網と顧客間接続　Site 型、Host 型

アクセス網と ISP 間接続　P2P、PTA、LAA

中小 ISP における移行

・中小 ISP バックボーンにおける、ネットワーク、ルーティング、アドレッシングに関する移行方法について記述しました。

アクセス網における移行

・下記アクセス網形態における移行方法検討を行いました。

ADSL/FTTH、CATV、無線 LAN、携帯、トンネルアクセス

中小 ISP の IPv6 移行ケーススタディ

・IPv4 中小 ISP が IPv6 試験サービスを行うと想定したケーススタディを記述しました。

1.セグメントの特徴

対象

提供対象：ホールセール（Flet’s、eAccess、ACCA など）、リテール（OCN、ODN、DION、@Nifty、BIGLOBE、Yahoo! BB など）
地理的範囲：グローバル（UUNET、VERIO など）、ナショナル（OCN、ODN、 DION、 @Nifty、BIGLOBE、Yahoo! BB など）、リージョナル（地域 ISP）
サービス内容：IP コネクティビティ、アプリケーション（ASP）、運用管理代行（MSP）

このドキュメントでは、以下のような特徴を持った、一般的な中小 ISP を対象として議論を進めます。

・構成要素の一部を他事業者から購入し、一般コンシューマを顧客としている（リテール）
・全国規模まではいかない準大手（ナショナル～リージョナル）
・IP コネクティビティと基本的なアプリケーション（DNS、Web、電子メール）を提供

対象となるアクセス網

また、本ガイドラインが対象とするアクセス網は、顧客ネットワークがインターネット接続性を得るために、ISP コアネットワークとの接続を提供するためのネットワークです。

本ガイドラインでは、物理的形態により分類しています（ADSL、FTTH、CATV、無線 LAN、携帯、IPv4 インターネット上での IPv6トンネリングによる接続）。PSTN、FWA などは本資料では検討対象外としています。

中小 ISP、及びアクセス網事業者にとっての IPv6 移行とは

中小 ISP およびアクセス網事業者にとっての IPv6 移行の動機は、

・先進サービスへの早期対応
・利用者をひきつける機器、アプリケーションの出現への対応
・国家施策、ISP 業界動向への対応

などです。

したがって、これらの事業者が実行しやすい移行プランとしては、既存サービスの置換えではなく、新サービスの開始と考えた方がよいと思われます。新サービスがよいものであれば、結果としてユーザはそちらに移行していくはずです（例：ダイヤルアップ⇒ADSL、一般電話⇒一般電話/IP電話）。

新サービス開始にあたり、中小 ISP 及びアクセス網事業者が気にする点は、以下のような点です。

- 新サービス（IPv6 サービス）に関わるコスト（ペイする時期の予測が難しい現状ではスモールスタートが望ましい）
- オペレーションコスト
- 機器のアップグレードコスト
- ユーザサポートコスト等
- 既存サービス(IPv4 サービス)への影響（既存サービス（IPv4 サービス）への影響があっては困る。また、アクセス網事業者は、各ネットワーク固有の条件により、IPv6 移行への敷居は ISP と比較して多少高く、移行に当たっては十分な事前検討が必要であろう）
- 新サービスに必要なリソース（人材、ノウハウ）（中小 ISP は少人数で運用している ISP が多いため、他社のアウトソースメニュの活用や、実験サービスなどを通じた本格オペレーションに必要な人材育成、ノウハウ蓄積も必要となるであろう）

IPv6 対応の 3 つの方法

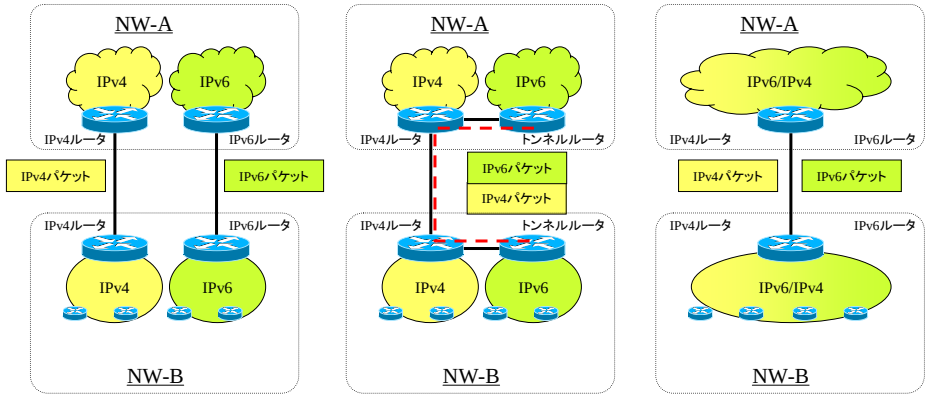
IPv6 対応の接続方法には、ネイティブ、トンネル、デュアルの 3 種類があります。ISP における IPv6 対応とは、この 3 つの手法のうちいずれか（または複数）を使って、上位接続、自社バックボーン、ユーザとの接続について、IPv6 通信を実現することです。

ネイティブは、IPv4 環境に全く影響を与えずに IPv6 を導入可能ですが、ISP にとっての移行コストは 3 つのうち最大となります。これは、IPv4 環境の安定性がクリティカルなケース向けと言えます。

トンネルでは、IPv4 環境にほとんど影響を与えずに IPv6 を導入可能です。コストは中程度で、既存の IPv4 環境を利用しつつ、IPv4 環境に大きな影響を与えたくないケース向けです。

デュアルは IPv6/IPv4 の両方のプロトコルを混在して利用できる理想的な方式で、コストは最も小さいと考えられます。しかし、ISP 内部で使われるルータ/ファイアウォール等、L3 ノードを全て IPv6/IPv4 デュアル対応にする必要があります。

IPv6対応の3つの方法



ネイティブ
- IPv4環境に全く影響を与えずにIPv6を導入可能
- コストは最も大きい
- IPv4環境の安定性がクリティカルなケース向け

トンネル
- IPv4環境にほとんど影響を与えずにIPv6を導入可能
- コストは中程度
- 既存のIPv4環境を利用しつつ、IPv4環境に大きな影響を与えたくないケース向け

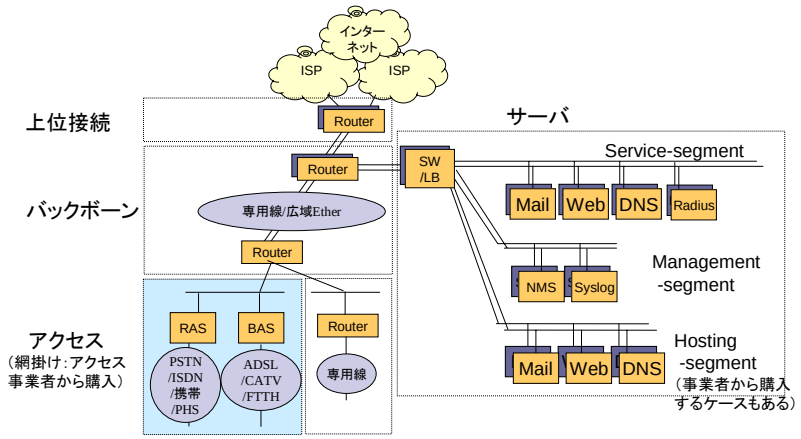
デュアル
- IPv6/IPv4の両方のプロトコルを混在して利用できる理想的な方式
- コストは最も小さい
- ルータ/ファイアウォール等、L3ノードを全てIPv6/IPv4デュアル対応にできるケース向け

中小 ISP の構成要素

一般的な中小 ISP のネットワーク構成は、図のようになっています。ダイヤルアップ、ADSL、FTTH といったアクセスサービスについては、アクセス事業者から購入し、ユーザからの直接専用線接続とともに、専用線や広域イーサネットで構成された自社のネットワークバックボーンにつなぎこみ、これを上位の ISP 経由でインターネットに接続しています。

バックボーンにはサーバセグメントを接続、このサーバセグメントは、サービス全体を対象とした DNS、電子メールサーバ、Web サーバを配置したサービスセグメント、さらにネットワーク管理システムや syslog サーバを配置した管理セグメント、そしてユーザに対するホスティングサービスのための Web サーバ、電子メールサーバ、DNS を運用するホスティングセグメントで構成されています。

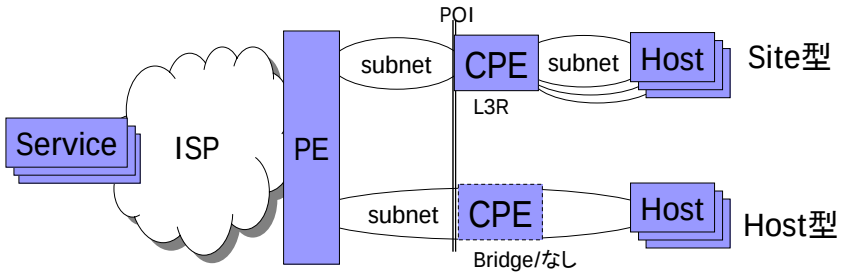
中小ISPの構成要素



アクセス網構成

現在のIPv4 サービスのアクセス網は、顧客の接続形態により、Site 型、Host 型の大きく 2 つの形態に分別することができます。

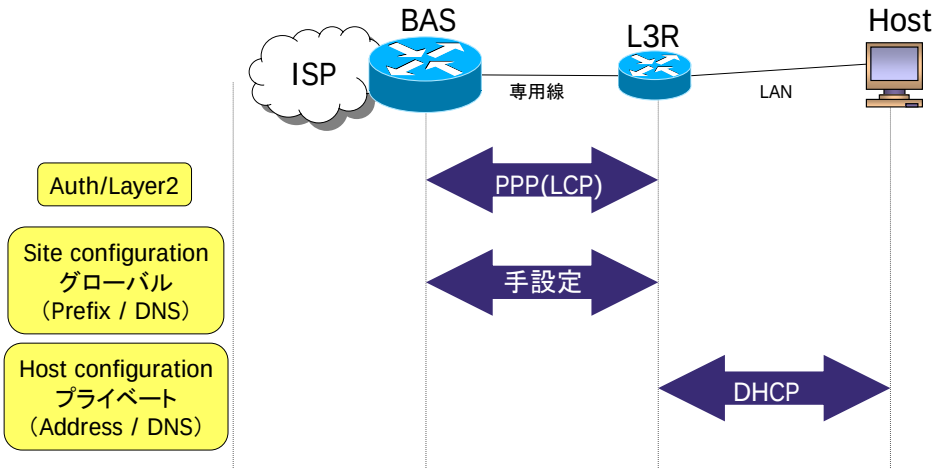
IPv4のモデル（2つの型）



	CPEの種類	例
Site型	L3R(Router)	エコノミー型サービス、企業向け専用線型サービス
Host型	L2 Bridge/なし	ダイアルアップ接続型サービス、ADSL/FTTHサービスも多くはこのモデル（Host=NAT/Router）、Hotspot

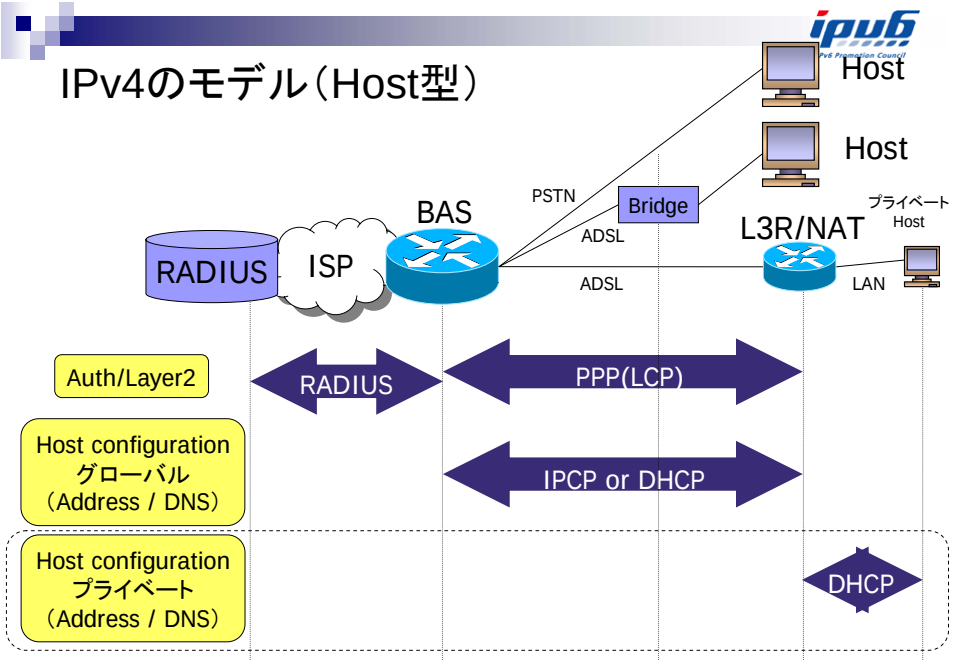
Site 型は、ユーザ拠点にルータを配置するものです。企業向けの回線サービスではこの形態になります。認証やレイヤ 2 接続は、PPP を通じて行います。

IPv4のモデル（Site型）



Host 型は、ADSL、FTTH、無線LANを含め、ほとんどの消費者向けサービスの提供形態で

す。


IPv4のモデル（Host型）
Host
Host
PSTN
Bridge
BAS
ADSL
L3R/NAT
プライベート
Host
RADIUS
ISP
ADSL
LAN
Auth/Layer2
RADIUS
PPP(LCP)
Host configuration
グローバル
（Address / DNS）
IPCP or DHCP
Host configuration
プライベート
（Address / DNS）
DHCP

2. 今すぐできること（Best Current Practice）

BCP の範囲と検討方針

以下では、今すぐできること、つまり BCP について検討します。中小 ISP、及びアクセス網事業者が今すぐ自力で可能な方法（実験、商用）を解説します。

対象となる ISP は、現在外部インターネットへのコネクティビティ、およびアプリケーションサービス(DNS、Web、Mail)を提供しているものとします。また、アクセス事業者については、ISP へのコネクティビティを提供しているものとします。

検討方針は、IPv4 サービスへの影響の考慮、コスト合理性の考慮、選択肢とメリットデメリットの例示、移行モデルケースの例示です。

IPv6 コネクティビティサービスの現状

現在提供されている IPv6 接続サービスは、以下の通りです。

ISP サービス(法人向け)

専用線（ATM、STM）：ネイティブ、デュアル、トンネル

LAN（DC）：トンネル、ネイティブ

ISP サービス(個人向け)

ADSL ：トンネル、デュアル

FTTH ：トンネル、デュアル

CATV ：デュアル（実験）、ネイティブ（実験）

無線 LAN ：デュアル（実験）

PSTN ：デュアル（実験）

携帯(PHS)： デュアル （実験）

他に、トンネル ASP サービス

中小 ISP における移行

推奨移行方法の概要

ここでは、アドレッシング、ルーティング、ネットワークの 3 つの観点から、推奨できる移行方法について紹介します。その概要は以下のようになります。

アドレッシング

sTLA を取得することを推奨

サイトに対しては/48 Prefix の割り当てを行う

ルーティング

IPv4 で利用していたルーティングプロトコルの採用を推奨

IPv6 と IPv4 のルーティングトポロジーを別々に構築することが可能

ISIS を採用している場合には、IPv6 と IPv4 のルーティングトポロジーをあわせる必要がある場合がある

ネットワーク

導入期は、IPv6 を IPv4 と独立して構築する方がインパクトが少ない

IPv6 ネットワーク拡大期において、IPv6 と IPv4 のネットワークを統合する

アドレッシング

アドレスの初期割り振りサイズ

事業者のアドレスの用途には、

・顧客に対して配布するアドレス空間（ユーザ用）
・自ネットワーク運用管理のためのアドレス空間（インフラ用）

の 2 通りがあります。

取得アドレス空間は、取得手段によって変わります。

	サイズ	取得手段
sTLA	/32(/35)	APNIC からの割り振り

NLA	/33～/47 /32	保有者からの再割り振り

各事業者が、sTLA と NLA のどちらの取得手段を使うかに関しては、ネットワーク規模、接続要件、運用管理のしやすさ等によって選択します。(※)

※ 現在 sTLA、NLA という標記は行われておらず、ここでは便宜上使用しています。

sTLA、NLA の比較

下の表は、ISP にとっての sTLA と NLA のアドレス空間のメリットやデメリットを比較したものです。

sTLA、NLAの比較

	sTLA	NLA
BGP4+	●インタネットとの経路制御が可能(マルチホーム) ▲取得申請に一定の条件 ▲下位ISP含め/48登録義務 ▲取得空間のDNS逆引き管理義務	●上位ISPの配布条件によっては取得、運用は容易 ●Peer(隣接ISPのアドレス空間に対する経路の交換)は可能 ▲インターネットとの冗長性経路の確保は制限を受ける ▲sTLAへの移行工数大
nonBGP4+	●運用が簡単(後にBGP4+も可能) ▲取得申請に一定の条件 ▲インターネットとの冗長性経路の確保が困難 ▲下位ISP含め/48管理義務 ▲取得空間のDNS逆引き管理義務	●上位ISPの配布条件によっては取得、運用は容易 ●運用が簡単 ▲インターネットとの冗長性経路の確保が困難 ▲sTLAへの移行工数大

- sTLAを取得/運用するハードルは高くなく、中小ISPもsTLAを取得するケースが一般的となるであろう

2005.1 IPv6PC TransitionWG ISPSWG 24

アドレス取得条件

sTLA と NLA のアドレス取得条件を、次にまとめます。sTLA を取得・運用するハードルは高くなく、中小 ISP も sTLA を取得するケースが一般的となると考えられます。

sTLA

APNIC 会員、もしくは JPNIC アドレス管理指定事業者であることと、以下の APNIC アドレスポリシーに合致することが必要。

IPv6 アドレス（sTLA）の初期割り振り資格

a) LIR であること

b) エンドサイトでないこと

c) /48を割り当てた組織に対し，IPv6インターネットへの接続性を 提供する計画があること。その際、インターネットに対する経路広告は、割り振られたアドレス一つに集成すること。

d) 2 年以内に最低でも 200 の/48 の割り当てを行う計画があること。

NLA

NLA は、上位のISPから取得するアドレスです。上位 ISP（/32 保有 ISP 等）の割り振りポリシーを満たすことが条件となります。通常、上位 ISP の IPv6 接続サービス利用とセットになります。

割り振られるアドレス空間は、上位 ISP のポリシーによりますが、1 年後（及び 2 年後）の/48 予定数に基づくケースが多く見られます。したがって、割り振られるアドレス空間、接続要件などを勘案して上位 ISP を決定する必要があります。

sTLA での経路制御方法

sTLA の場合、選択可能なルーティングプロトコルは BGP4+とスタティックの 2 種類です。

BGP4+では、IPv6 インターネットとの経路制御が可能です。上位 ISP が一つの場合はスタティックで十分ですが、将来の BGP4+ 運用への備えも必要となります。

sTLA 保持者の義務

sTLA を取得、運用する場合には、次の義務が発生します。

顧客への Prefix 割り当て報告

顧客に/48 の Prefix 空間を割り当てた際には、APNIC にその情報を登録する義務が生じます。APNIC への/48 報告は、メールで行います（Tech-c、Admin-c のための Person Object を登録と inet6num Object の登録）

sTLA 空間 DNS 逆引き

取得した sTLA の DNS 逆引き空間を管理する義務が生じます。

NLA 取得方法

NLA のアドレスは、上位 ISP(sTLA 、NLA) より取得します。 アドレスの割り振りは、通常、上位 ISP の IPv6 接続サービス利用とセットになります。 IPv6 接続における上位 ISP は、IPv4 の上位 ISP と同一である必要はありません。

割り振られるアドレス空間の大きさは、上位 ISP のポリシーによりますが、割り振り対象者の 1 年後(及び 2 年後)の/48 予定数に基づくケースが多く見られます。 割り振られるアドレス空間、接続要件など勘案して上位 ISP を決定するのがよいと考えられます。

NLA での経路制御方法

NLA の場合、IPv6 インターネットへの接続性は、NLA を取得した上位 ISP から取得します。

現状日本ではインターネット全体の経路集約の観点から、多くの AS で/35 より長い prefix のフィルタが一般的に行われています。なお、IPv6 実験ネットワーク 6bone の運用規則を定めた RFC2772(6Bone Backbone Routing Guidelines)ではパンチングホールを禁止しています。

ルーティングについても、上位 ISP のポリシーによって異なります。上位 ISP へのデフォルト経路をスタティックで設定する場合と、BGP4+で IPv6 フル経路を受領できる場合があります。インターネットエクスチェンジ(IX)やプライベートピアリング経由で、特定の ISP に対する経路の冗長化は可能です。将来 AS 間の暗黙のコンセンサスが崩れれば、パンチングホールによる経路数肥大の影響が危惧されます。

NLA から sTLA への移行

当初 NLA でスタートした ISP が sTLA に移行する契機としては、経路の安定性からマルチホームを導入する場合と、NLA のアドレス消費が進み、より大きなアドレス空間(sTLA)が必要になった場合が考えられます。

移行は、たとえばまず sTLA を取得、次に上位 ISP、IX との接続、および sTLA 経路広告を行い、リナンバリング作業を実施します。この際、自社のネットワークだけでなく顧客サイトにおいてアドレス移行作業が生じます。具体的な作業については 4 章の Tips を参照してください。

アドレッシング手法

顧客へのアドレッシング

エンドユーザ顧客に対するアドレスの割り当ては、RIR(APNIC)の IPv6 アドレスポリシー

（http://ftp.apnic.net/apnic/docs/ipv6-address-policy）に準拠して行ってください。このアドレスポリシーでは、原則的に 1 接続に対して/48 を割り当てることとなっていますが、顧客環境が 1 セグメントのみの場合に/64 を割り当てたり、1 端末のみの場合には/128 を割り当てることも選択肢として記述されています。現状の IPv6 接続サービスでは、(ADSL 等) コンシューマ向け接続は/48 あるいは/64 の割り当てが一般的となっています。

留意点としては、/48 の場合には RIR への whois 登録が必要であること、一方/64 の場合、エンドユーザへの追加割り当て処理への対応（事務処理、経路集成）が必要になること、等があげられます。

ネットワークインフラにおけるアドレッシング

IPv6 では、IPv4 と比べ、アドレス空間が広大であるため、容易で余裕を持ったプランニングが可能となります。まず、ホスト数を意識する必要がなく、サブネットはすべて/64 で構成するのが一般的です。この他、ISP では、インフラ用として POP 毎に/48 を割り当てることができます。全般的に、アドレス利用効率より、ISP 内部経路の集成を優先して考えることができます。

sTLA（/32）の場合 7132 個の/48（利用率 10.9%)を割り当てれば、追加割り振りを受けられます（HD-Ratio（利用率 0.8 の場合）より）。

ISP は/48 単位で APNIC データベースに登録する必要がありますが、登録数が HD-Ratio：0.8 を超えれば、申請によりただちに、アドレス空間が 2 倍となる追加割り振りが受けられます。

顧客用アドレスも経路集成が行えるように、接続 POP 毎に集約してアサインすることが望ましいと考えられます（IPv4 と考え方は同じ）。当初、センターのサーバで顧客向けトンネルを終端するケースでは、顧客がデュアルサービスに移行する（エッジへ収容替え）際のリナンバを考慮しておく必要はあります。

サーバセグメントにおけるアドレッシング

サーバセグメント用のアドレス空間確保では、1 つの LAN セグメントに対して、/64 を割り当てます。将来予想される使われ方（ソースアドレス選択等）に対応できるよう、1 つの LAN セグメントに複数の/64 を確保するのもよいと考えられます。

ルーティング

EGP

EGP には BGP4+（eBGP、iBGP）を利用します。フルメッシュ、ルートリフレクタ、コンフェデレーション等、IPv4 BGP と同じ技術の使用が可能です。

BGP ルーティングトポロジー

外部接続(eBGP)では、プロトコル毎に回線を分ける（IPv6 ネイティブリンクを追加）か、デュアルセグメント上で IPv4、IPv6 それぞれ別のルータでピアリングするかについては、接続先のポリシーに従います。内部接続(iBGP)におけるピアトポロジーも IPv4 のそれとは独立にできます。

IPv6 ルータの BGP 実装における注意

注意点としては、中小 ISP の場合、特殊な事情を除き IPv6/IPv4 とも同一の AS が一般的ですが、仮に異なった場合、ルータによっては同一ルータで 2AS の BGP プロセスが起動できない場合があります。

1 つの BGP4+プロセスで IPv4、IPv6 経路交換を行う実装の場合、iBGP 構成において下記のような点に注意する必要があります。

・IPv6、IPv4 で同一 AS 番号を利用する必要があります。
・IPv4、IPv6 で同一 RR 構成をとる必要があります（Route Reflector Cluster-ID が同一）。
・IPv4、IPv6 で同一 SubAS 構成をとる必要があります（Confederation SubAS が同一）。

BGP Peer

BGP Peer については、次の 2 点に注意が必要です。

NLRI （Network Layer Reachability Information）の受領

到達性情報を他のプロトコルに依存するべきではないという理由から、IPv6 NLRI を IPv4 Peer で扱わないことをお勧めします。 つまり、IPv4 ルーティングは IPv4 アドレスで Peer し、IPv6 ルーティングは IPv6 アドレスで Peer すべきです。

Peer アドレス

Peer アドレスは、グローバルアドレスとリンクローカルアドレスが考えられます。eBGP では、基本は IX、接続先のポリシーに従うべきですが、アドレスポリシーでは、IX に non-routable な IX 用グローバルアドレスを割り当て可能であることが決まっています。eBGP の仕様上、リンクローカルアドレスでの安定動作が難しい場合があるため、選択が可能な場合は、グローバルアドレスの利用を推奨します。iBGP では、グローバルアドレスを使用します。

BGP ルーティングポリシー

ルーティングフィルタについては、各ピアの設定にプレフィックスフィルタを導入し、s/pTLA 以外をフィルタアウトすべきです。また、AS Path フィルタを併用することが望まれます。6to4 プレフィックス（2002: :/16）は通しますが、/32 保有 ISP で/35 のパンチングホールは行わないようにすべきです。すでに利用廃止となったサイトローカルアドレスの通信は、念のため外部接続インタフェースでフィルタリングすることが望まれます。
IPv6 におけるプレフィックスの正当性確認については、s/pTLA の情報を、各 RIR あるいは 6bone のデータベースで確認します。

フル経路の受領

IPv6 フル経路の受領は、上位 ISP の IPv6 接続サービス（商用、実験）の利用か、WIDE 等の実験研究組織との接続によって実現できます。経路の安定性の点から、一定の接続サービスレベルを保ちたい場合、1 つは商用の IPv6 サービスの利用を推奨します。

IGP

IGP の選択肢としては、OSPFv3、i/IS-ISv6、RIPng、Static がありますが、コアとなる IGP は、IPv4 と同様に Link State 方式の動的ルーティングを推奨（OSPFv3 は既に大手 ISP での運用実績もある）します。Link State 方式では、経路収束が早い、経路集成が可能であるという 2 つの利点があるからです。

ただし、初期導入（トンネルのみ）等の小規模のケースでは Static、RIPng 利用もありえます。まず Static か RIPng で始め、将来、HOP 数や扱うルータ台数が増えた場合に OSPFv3 へ切り替えることもできます。

IGP の選択

IPv6 における IGP の選択に関しては、IPv4 で使用しているプロトコルの IPv6 版を選ぶことが運用経験の観点でベターです。つまり IPv4 で RIP を使っている場合は RIPng を選択し、OSPFv2 を運用している場合は OSPFv3 を選ぶということです。

ただし、i/IS-IS → i/IS-ISv6 の場合、次の 2 つの制約があり、段階的な移行には向きません。

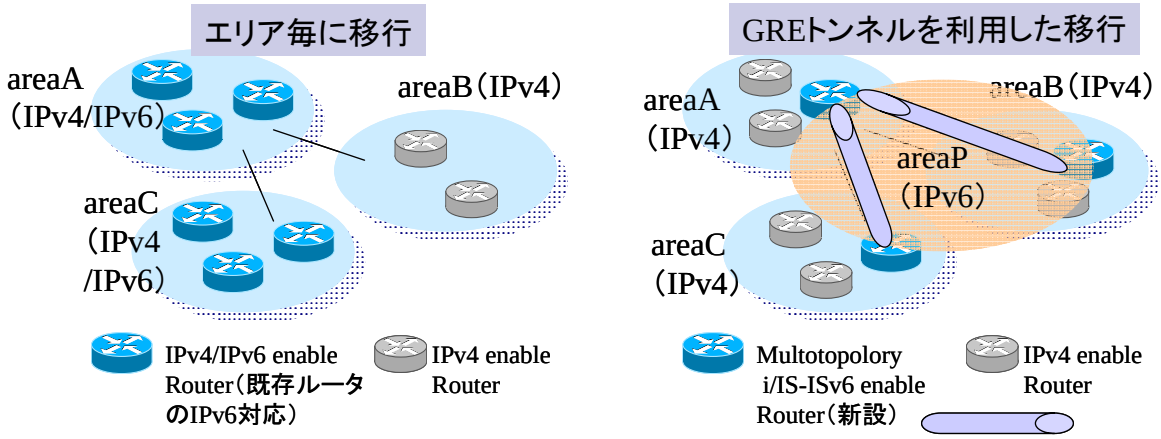
・同一 area 内で、IPv6 ルーティングトポロジーと IPv4 ルーティングトポロジーとを独立させるためには、multitopology i/IS-IS の採用が必要（i/IS-IS を用いて IPv6 対応するためには、同一 area 内で動作している IPv4 の i/IS-IS ルータ全てを IPv6 でも動作させる必要がある）

・ルーティング情報のトランスポートが OSI プロトコルであるため、IPv6 over IPv4 トンネルでは扱えない。従って、GRE トンネル等 IP プロトコルに依存しないトンネル技術の採用が必要となるが、その場合、IPv6、GRE、IPv4 のトリプルスタック構成となりオーバーヘッドが増加する。

これらが問題となるケースでは、i/IS-IS → OSPFv3 がよいと思われます。

IGP のルーティングトポロジー

RIPng、OSPFv3 のルーティングトポロジーは、IPv4 と IPv6 で独立して設計できます。i/IS-ISv6 の場合は、前項の条件から次の 2 パターンの段階的な移行手段がとり得ます。



エンドユーザとの経路制御

IPv6 では、IPv4 と比べエンドユーザがプレフィックスを持つケースが増えるため経路制御が必要な割合が増えます。

ダイナミックルーティングを使用する場合、ユーザから広告される経路が ISP 内部に影響を与えないようフィルタする必要があります。

また、複数ユーザが共有するセグメント上で RA を使用する場合、あるユーザが誤って RA を出しても、他ユーザに伝播しないよう、スイッチやモデム等でフィルタする、もしくは完全な策ではありませんが、上位ルータでは router-preference を high に設定する必要があります。

ネットワーク

上位接続

上位 ISP が提供するメニューは、以下のように分類できます。

接続方式:トンネル型、ネイティブ型、L2 共有型、デュアル型
ルーティングプロトコル:BGP4+、Static

上位接続用ルータの構成パターンは、IPv6 サービス専用、あるいは IPv4 サービスと v6 サービスで共用が考えられます。ここで言う「専用」の意味は、IPv4 サービスユーザのトラフィックを乗せないという意味であり、そのルータで IPv6 しか動かさないという意味ではありません。当面、ルータ管理(SNMP など)のため、IPv6 サービス専用ルータもデュアルスタックで動かすことにならざるをえません。

上位接続 各パターン説明

上位 ISP の提供メニューには、それぞれ以下の特徴があります。

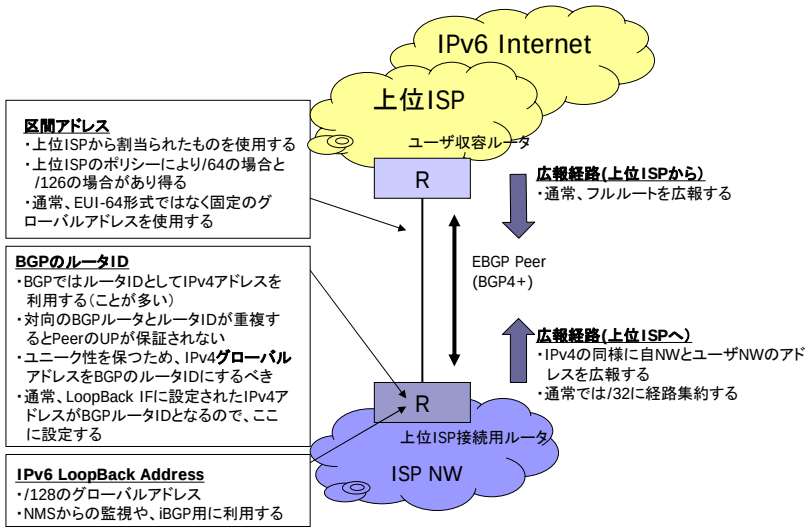
・トンネル型、L2 共用型
IPv4 の付加サービスとして課金される場合が多い
・デュアル型
新たに回線は必要なく、IPv4 と IPv6 サービスを両方購入するより安い
・ネイティブ型
IPv6 用に回線が必要なため、上位 ISP との接続点が地理的に離れているとコスト高になる。

以上に加え、使用可能なルーティングプロトコル(BGP4+、Static)、料金、将来のメニュー変更への対応等を検討し、上位 ISP を選択することになります。
ISP 側の上位接続用ルータについては、上位接続ルータの不具合が既存サービスすべてに影響を及ぼすということから、新サービス(IPv6)と安定運用が必須な既存サービス(IPv4)ではルータを分離しておいた方が運用上の安心感はある(デュアル型以外で可能)と言えます。IPv6 サービス専用のルータを設置する場合には、その設備投資がデメリットとして挙げられます。

上位接続の構成例(BGP4+)

中小 ISP における上位接続の構成例としては、図のようなものが考えられます。

上位接続の構成例(BGP4+)



ピア接続

ピア接続は、BGP4+で行います。

パブリックピア(IX 経由でのピア)は、一般的にはレイヤ 2 スイッチへの接続となります。レイヤ 3(ルータ)IX への接続は一般的ではありません。また、トンネル経由の IX 接続も一般的ではありません。

一方、プライベートピア(ISP 間での直接接続によるピア)では、トンネルによるピア形態もあります。

したがって、ピア接続の構成パターンは、ネイティブ、デュアルスタック、トンネルの 3 種類が考えられます。

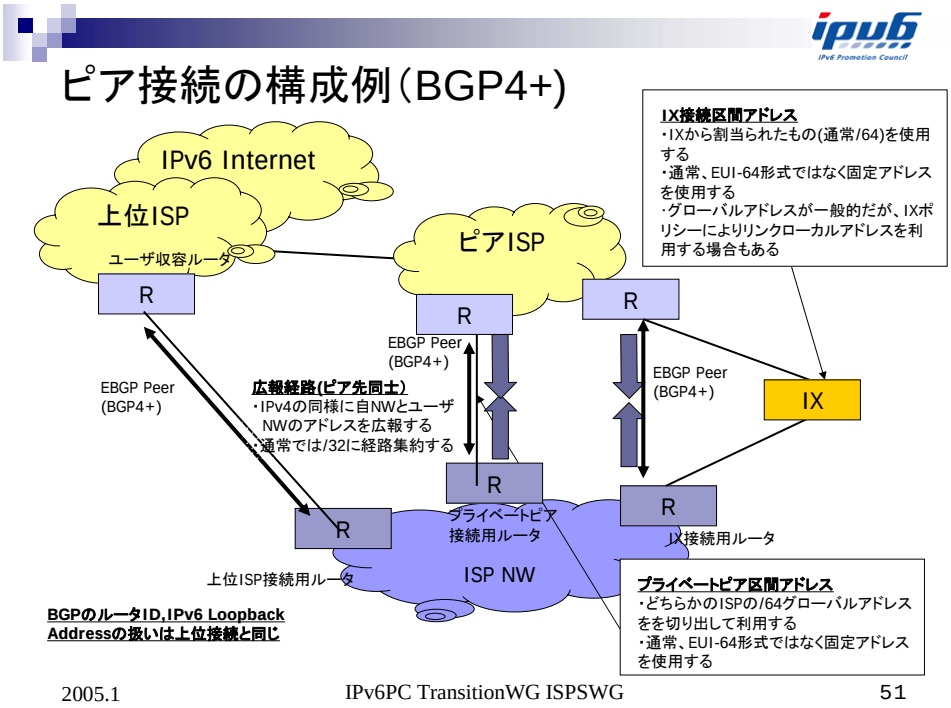
トンネルを利用したピア接続は、プライベートピアで用いられることがあります。IPv4 で直接接続されている ISP との IPv6 ピアに利用する場合が考えられます。

この場合の「直接接続」には、IPv4 プライベートピア、IPv4 パブリックピア、IPv4 上流/ 顧客接続があります。

他の ISP ネットワークをまたがったトンネルピアを設定することは推奨しません。トンネルの到達性に障害があった場合の状況把握、対応が困難だからです。

ピア接続の構成例(BGP4+)

中小 ISP におけるピア接続の構成例としては、図のようなものが考えられます。



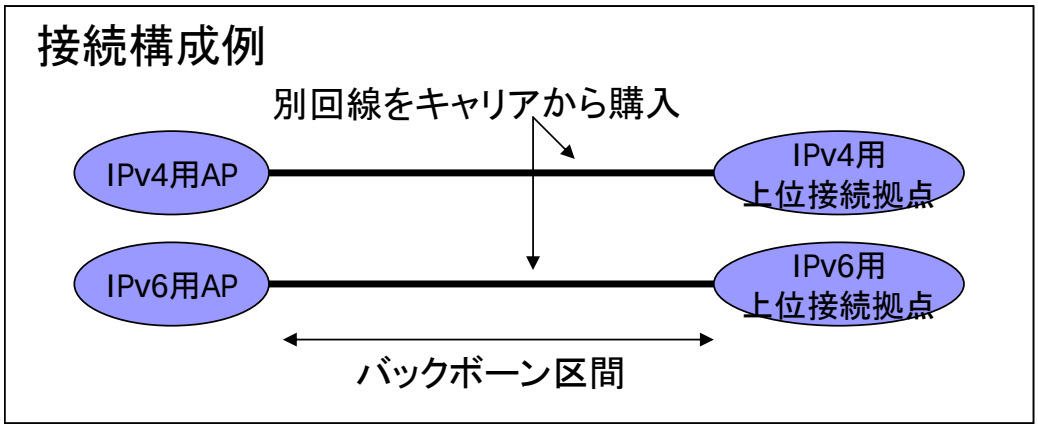
バックボーン

中小 ISP のバックボーンは、「上位接続ルータ設置拠点とアクセスポイントを接続する回線」と定義できます。ここでの「アクセスポイント」とは、アクセス回線業者との接続点を意味します。この場合、アクセスポイントにルータがあるとはかぎりません。中小 ISP では一般に、バックボーン回線を他の通信事業者から購入しています。最近では、広域イーサネットサービスを購入する場合が多く見られます。バックボーン用回線購入がバックボーン構築と同義となる場合もあります。

バックボーン構成は、別回線(IPv6 サービス専用)型、トンネル型、回線共用(L2 分離)型、デュアル型の 4 つに分類することが可能です。

別回線(IPv6 サービス専用)型

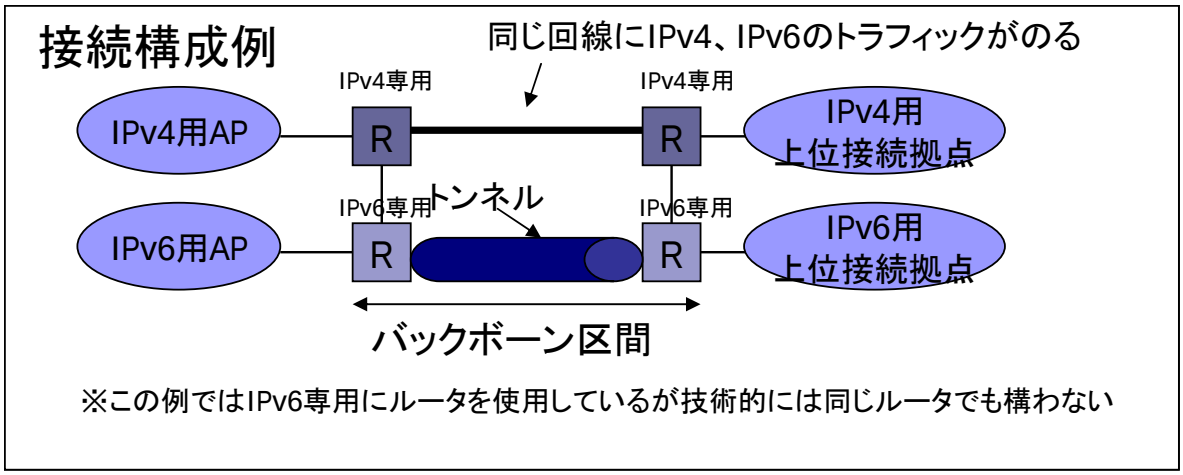
これは、IPv6 用に別回線を購入するパターンで、別サービスのトラフィックの影響を受けない点がメリットです。しかし、新たに回線を引くことになるので回線コストが高くなる点がデメリットとなります。



トンネル型

従来からよく言われている移行時の構成ですが、中小 ISP を対象とした場合には次のような問題点があります。

- 中小 ISP ではアクセスポイントにルータがあるとは限らない
- ルータがあったとしても IPv6 対応とは限らない
- 運良く IPv6 対応にできるルータがあったとしても既存サービスへの影響を見積もる必要がある
- アクセスポイントの数にもよるが、トンネル用のルータを新設するにはそれなりの設備投資が必要



トンネルでのネットワーク構築時の注意

MTU サイズ

トンネルインタフェースの MTU サイズは両端で合わせることを推奨します。トンネル区間での Path MTU サイズが不明の場合には、トンネルインタフェースの MTU を 1280byte にあわせま

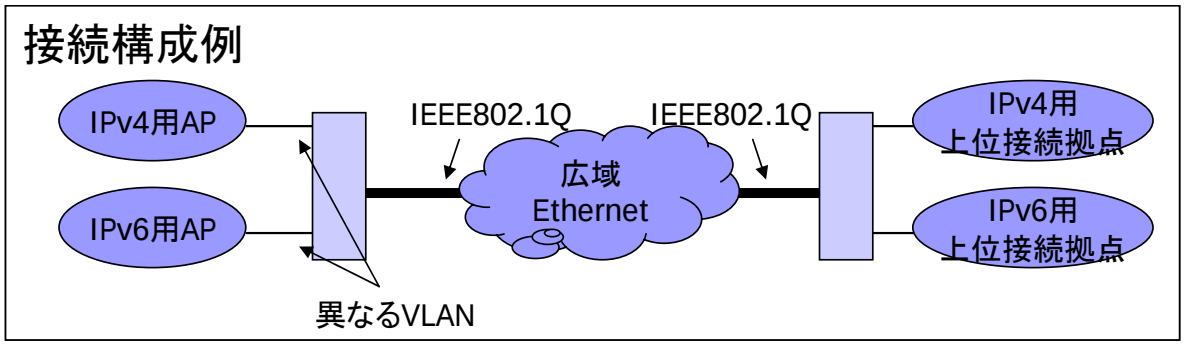
す。Path MTU 値が判明している場合には、それにあわせてトンネルインタフェースの MTU サイズを調整してもよいです。

トンネルインタフェースの死活監視

一般的な実装では、トンネルインタフェースの死活はトンネルの端点となる IPv4 アドレスの死活に連動しません。トンネル端点の IPv4 アドレスへの到達性がなくなっても、トンネルインタフェース自体はダウンしません。特に、トンネルの IPv4 アドレスへの到達性を静的経路設定で確保している場合には、動的に対応できないので注意を要します。トンネル端点の IPv4 アドレスの死活監視も行うことが望まれます。

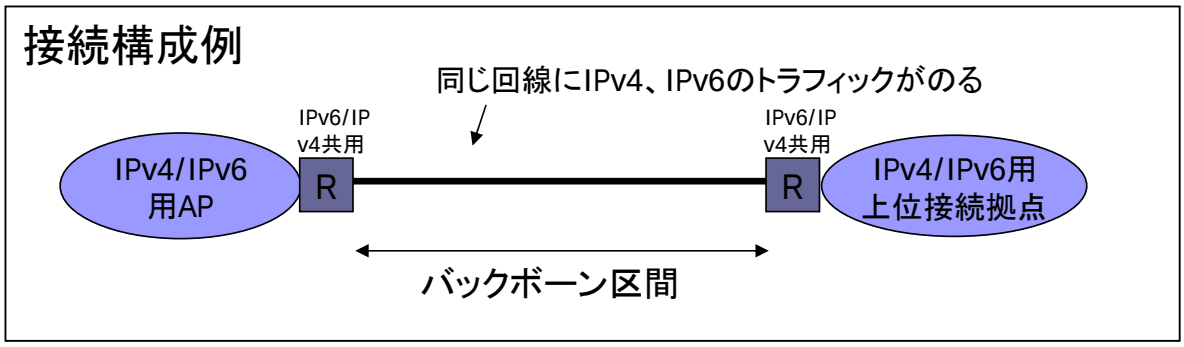
回線共用(L2 分離)型

レイヤ 2 の技術を利用し IPv4 の既存サービスと IPv6 サービスを論理的に分離するもので、イーサネットでは VLAN、ATM では VP/VC などを利用します。バックボーン用回線を IPv4 サービスと IPv6 サービスで共用することにより、回線コストを低く抑えられるメリットがあります。



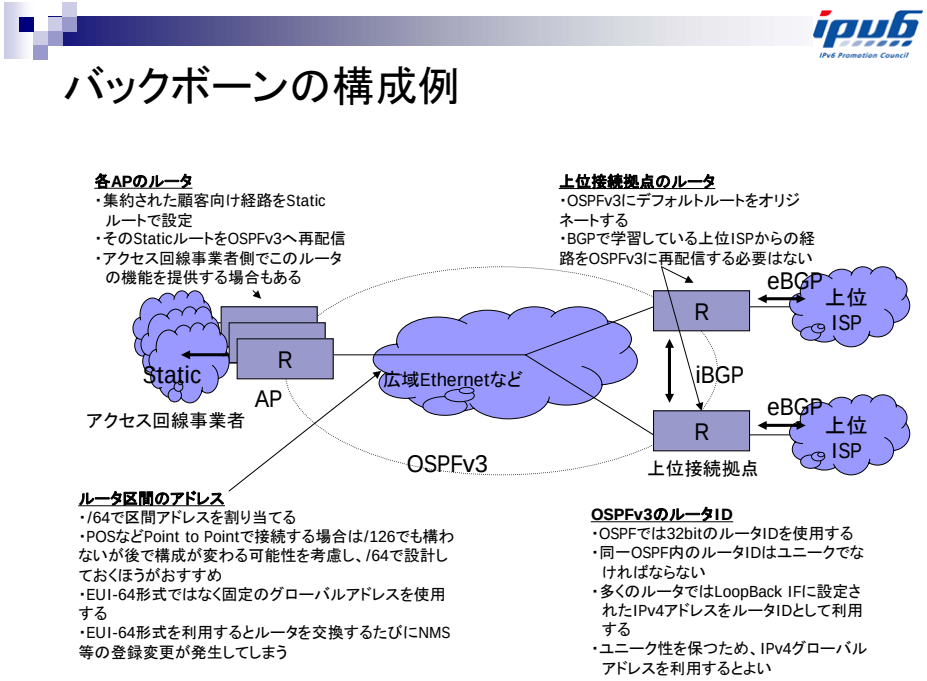
デュアル型

IPv4 サービスと IPv6 サービスを統合的に提供するものです。バックボーン回線を共用でき回線コストを下げられるほか、ルータも共用するため最もコストメリットが高い方法です。IPv4 サービスへの影響が危惧されますが、大手 ISP の一部ではこの構成が始まっています。ただし、中小 ISP の場合、アクセスポイントにルータがあるとは限らないため、この構成が無理なケースもあります。



バックボーンの構成例

中小 ISP のバックボーンは、図のような形で構成することができます。



アクセス網における移行

概要

アクセス網のアドレッシングについては、基本的には IPv4 と同様ですが、固定 Prefix 配布方式については検討が必要となります。

ルーティングについては、基本的には IPv4 と同様です。

ネットワーク形態は、基本的には IPv4 と同様の構成ですが、Site 型構成を推奨します。ただし、外出先などでの利用が想定される形態(無線 LAN、携帯)については Host 型とします。

IPv6 対応のために、構成機器の IPv6/IPv4 デュアルスタック対応を進める必要があります。ADSL/FTTH、無線 LAN でこれがあてはまります。

デュアルスタック対応機器が進んでいない場合にはトンネルによる接続を行います。たとえば CATV、携帯(、トンネルアクセス)などです。

アクセス網

中小 ISP が提供する IPv6 サービスのアクセス回線としては、ADSL や FTTH などが想定されます。中小 ISP では、これらをアクセス回線事業者から購入しサービスを提供する形態が一般的となっており、本ドキュメントでも、この形態を対象として扱います。

内容

アクセス網の移行に関して記述する内容は、以下の通りです。

<u>共通項目</u>

ネットワーク

- ・顧客との接続モデル
- ・ISP との接続モデル

アドレッシング、ルーティング

- ・アドレス設計
- ・ルーティング設計
- ・固定 Prefix 配布に関する議論

<u>個別項目</u>

ADSL/FTTH、CATV、無線 LAN、携帯、トンネルアクセスのそれぞれのアクセス網形態について、「各機器の要件」「接続方法」を記述します。

共通項目

概要

ネットワーク

顧客接続については、Site 型、Host 型の 2 つの形態があります。顧客宅内ネットワークのセキュリティ確保の観点から、可能な限り、Site 型の採用が望まれます。

ISP 接続については、P2P、PTA、LAA の 3 つの形態があります。IPv4 と同じ方式を採用することを推奨します。

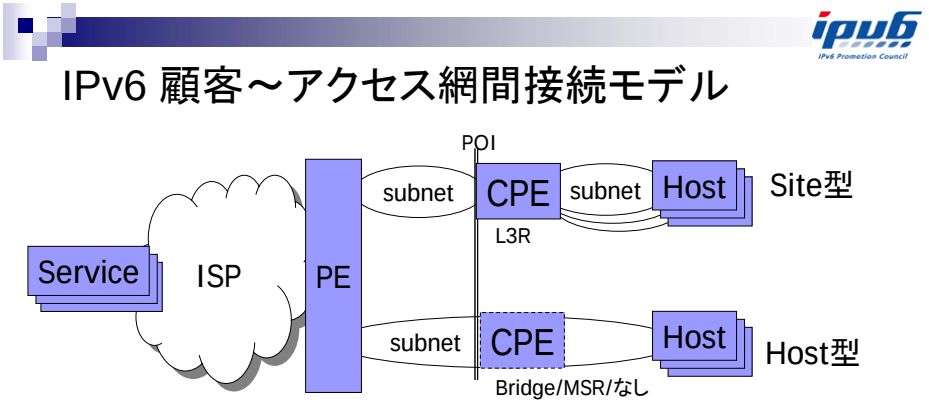
アドレッシング、ルーティング

基本的には IPv4 の場合と同様です。固定 Prefix の割り当てをする場合には検討が必要となります。

ネットワーク

IPv6 顧客～アクセス網間接続モデル

Site 型、あるいは Host 型でアクセス網からエンドユーザに接続するモデルは、下図のようになります。



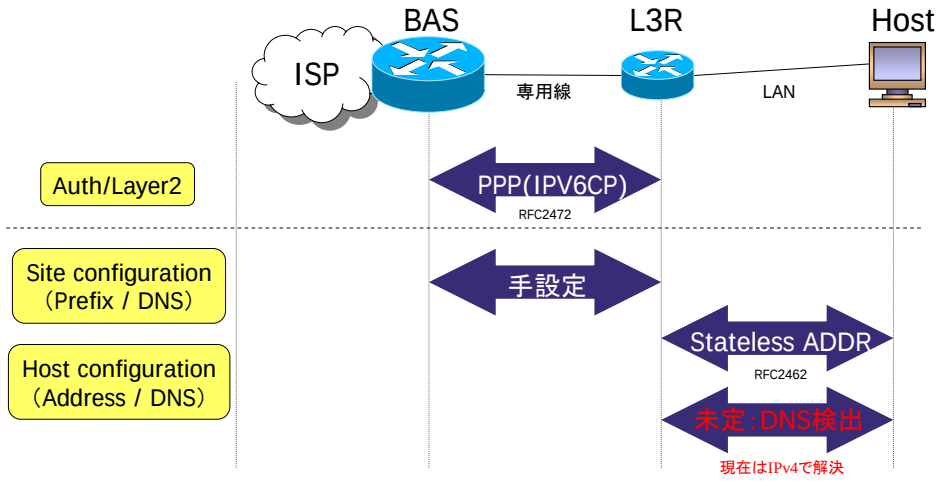
	CPEの種類	Prefix	例
Site型	L3R(Router)	/48,/64	企業向け専用線型サービス、ADSL/FTTHサービス
Host型	L2 Bridge/MSR/なし	/64	ダイアルアップ接続型サービス、3Gモバイルデータサービス、ADSL/FTTHサービス（/64限定）、Hotspot

MSR=Multi-link Subnet Router

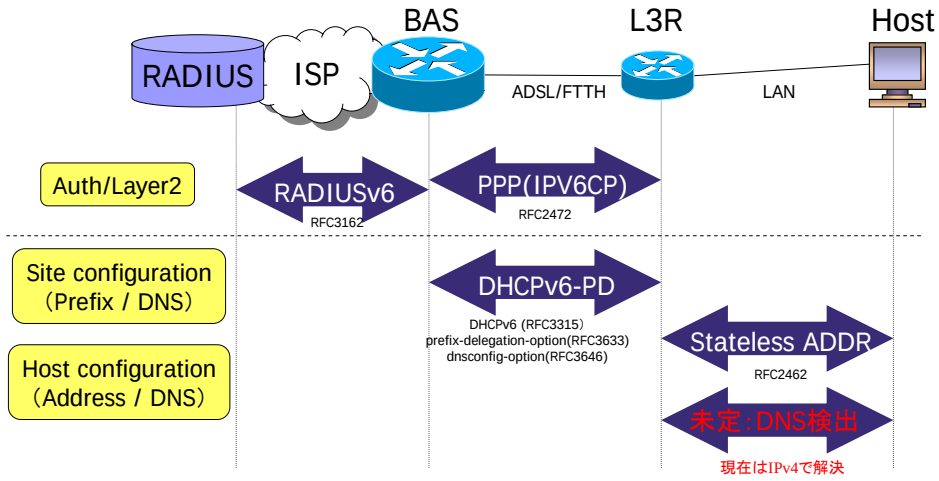
Site 型の構成

Site 型では、2 つの形態が考えられます。違いは、ユーザ拠点の構成を、手設定で行うか、DHCPv6 を利用するかという点にあります。

Site型その1

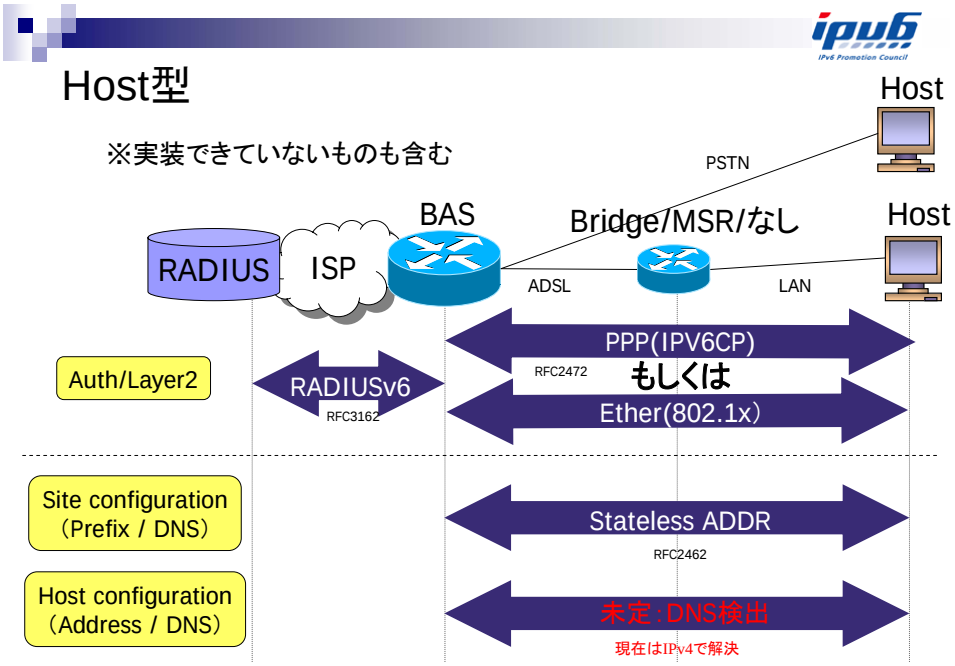


Site型その2



Host 型

Host 型の構成は下図のようになります。



IPv6 アクセス網～ISP 間接続モデル

アクセス網～ISP 網間の接続は、顧客トラフィックの接続方法によって下記の 3 つに大別されます。

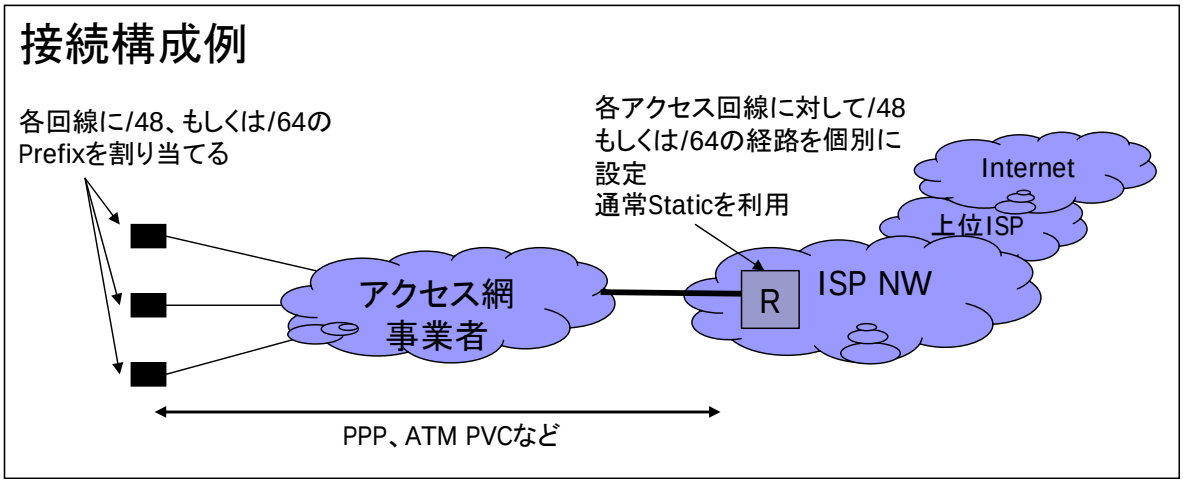
・Point-to-Point (P2P) 型
・PPP Termination Aggregation (PTA) 型
・L2TP Access Aggregation (LAA) 型

プロトコル毎の運用方式負荷の低減のため、基本的には IPv6/IPv4 両者とも同じ接続方式に揃えるとよいですが、アクセス網事業者(及び ISP)の展開方針によっては、IPv6/IPv4 で異なる型を取らざるを得ない場合もあります。

ISP 網がユーザ認証、およびネットワーク接続性を提供する形態が一般的ですが、両者を分け、ネットワーク接続性を他事業者にアウトソースする形態もあります。

Point-to-Point 接続型

この場合、IP パケットのパイプとして、アクセス網をレイヤ 2 網として利用します。各回線(PPP、ATM PVC 等)を ISP で直接終端します。アクセス網内はレイヤ 2 構成であるため、IP レイヤでのルーティングは必要ありません。

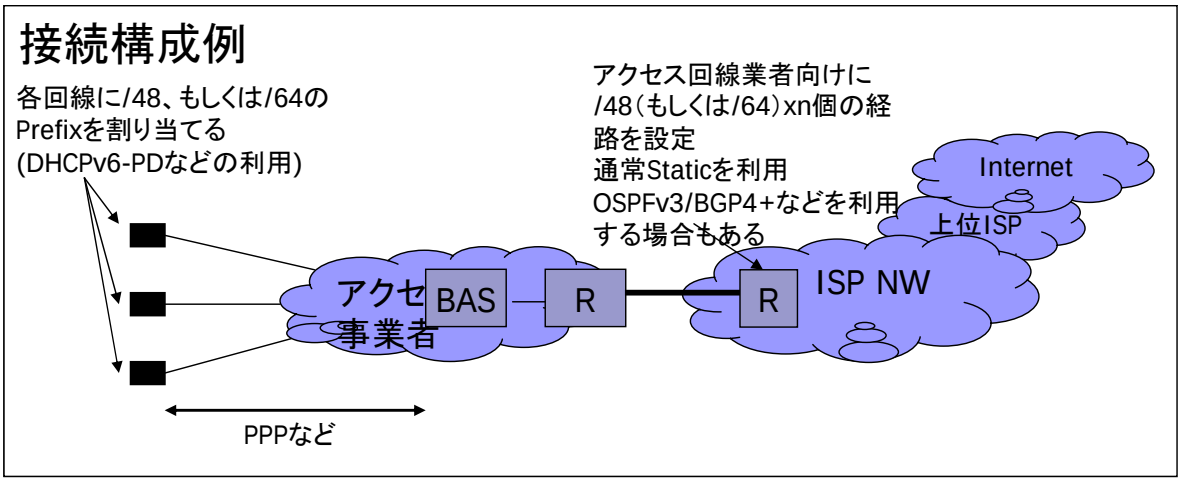


PPP Termination Aggregation 型

この場合、各回線(PPP 等)をアクセス網で終端し、IPv6 および IPv4 パケットを ISP に渡します。スケーラビリティなどを考慮し、アクセス網内で L2TP 構成をとることもあります。

アクセス網で PPP を終端する機器(一般的は BAS)と ISP 網間のルーティングが必要となります。アクセス網内で L2TP 構成をとる場合には、L2TP パケットのルーティングも必要です。

これは、現在、一般的に用いられている利用形態です。



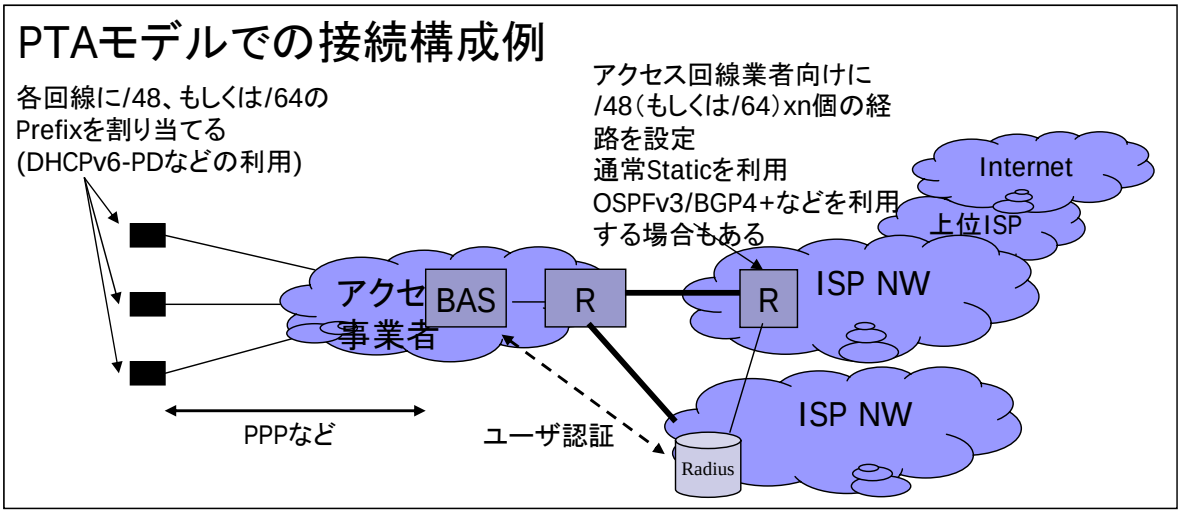
L2TP Access Aggregation 型

各アクセス回線(PPP 等)を L2TP にカプセル化し、ISP に渡す方式です。PPP は ISP で終端します。L2TP は IPv4 トランスポートでよく、アクセス網では顧客トラフィックのルーティングは必要

ありません。ただし、L2TP パケットのルーティングは必要です。

ネットワーク接続のアウトソース形態

ISP は RADIUS 等による顧客認証のみを実施し、顧客の IPv6 および IPv4 接続性は他 ISP(もしくはアクセス事業者)にアウトソースすることができます。自社で IPv6 接続性を持たなくても、IPv6 サービスの開始が可能です。



IPv6 アクセス網～ISP 網間接続構成

IPv6 によるアクセス網と ISP 間の物理的接続方式について、以下の点が指摘できます。

P2P 型と LAA 型

・顧客トラフィックのプロトコルには依存しないため、基本的に IPv4 と同様

・LAA 型の場合には、顧客 IPv6/IPv4 パケットとも、IPv4 L2TP で接続を行う

PTA 型

・IPv6 パケットを直接交換するために、考慮が必要

・レイヤ 3 的接続方法の区分としては、ネイティブ、デュアル、トンネル

・レイヤ 2 的接続方法の区分としては、シングルホーム接続とマルチホーム接続

それぞれの接続に関する留意点は、ISP コア網～上流 ISP 接続と同様です。

アクセス事業者内網構成

アクセス事業者の内部における網構成は、基本的には IPv4 と同様です。

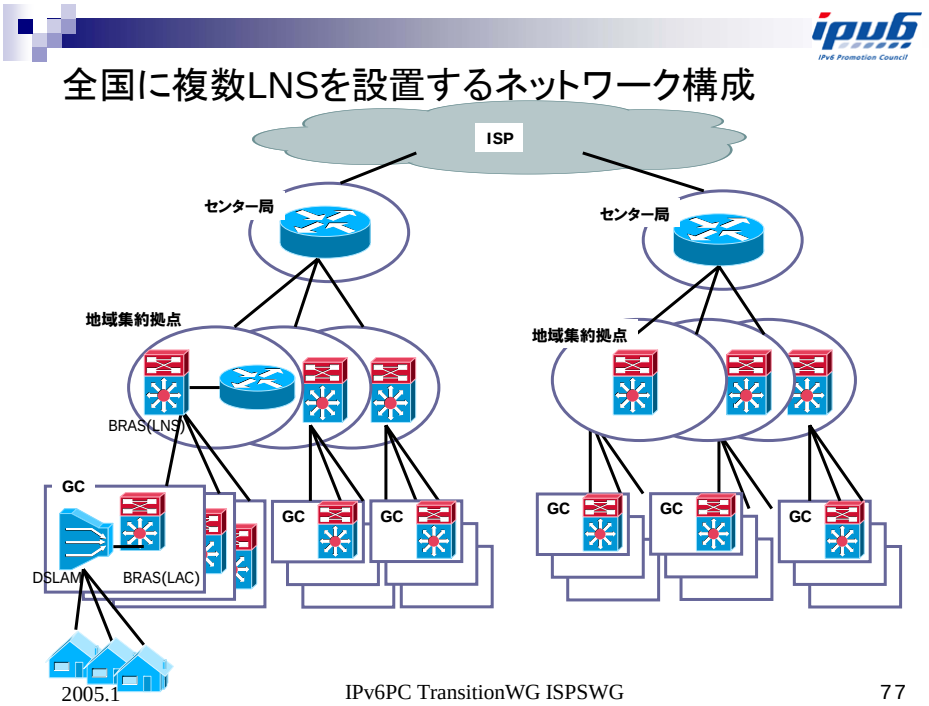
ブロードバンド事業者(一般的なホールセール型 ADSL 事業者)のネットワークには、加入者を地域単位で集約し BRAS(LAC/LNS)で PPP 終端する、PPP 終端後に IP ルーティングによりセンター局で ISP と相互接続する、という特徴があります。

PPP 終端ポイントから ISP 相互接続点をもつセンター局までのネットワークでは次の 2 つの構成が挙げられます。

・全国複数拠点で PPP を終端しセンター局まで IP ルーティングを行う NW 構成 → 全国に複数の LNS を設置

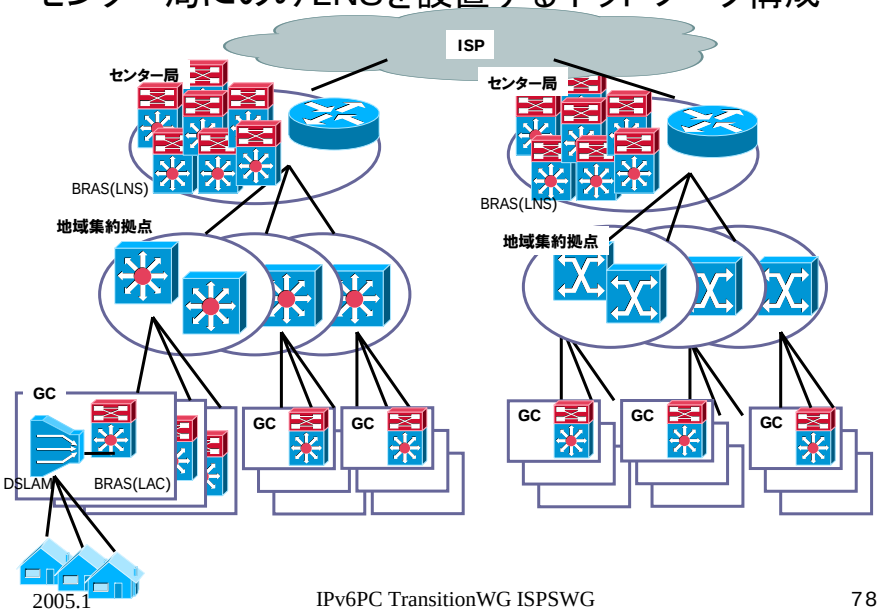
・センター局で集中的に PPP を終端し、局内で ISP に相互接続を行う NW 構成 → センター局にのみ LNS を設置

全国に複数 LNS を設置するネットワーク構成



センター局にのみ LNS を設置するネットワーク構成

センター局にのみLNSを設置するネットワーク構成



アドレッシング、ルーティング

アドレス設計

ここでは、顧客用アドレス、事業者インフラ用アドレスの各用途におけるアドレス設計、そしてアクセス網事業者、ISP 事業者の各事業者におけるアドレス設計を考えます。

顧客用アドレスの配布方法の定義

顧客用アドレスについては、可変、固定、完全固定の 3 種類の配布方法が考えられます。

可変

BAS などに IPv6 Prefix をプールし、接続毎にプールからアドレスを払い出すもので、接続毎に Prefix が変わる可能性があります。

固定

毎回同一 Prefix で接続する方法ですが、接続場所が変われば Prefix が変わります。

完全固定

どこに行っても同一 Prefix を使えるようにします。

顧客用アドレスの配布方法

顧客用アドレスの配布については、BCP としては「固定」Prefix 配布を推奨します。

現在のアクセスサービスでは「固定」方式が一般的であり、「完全固定」は一般的ではありません。

今後は「可変」Prefix 配布の出現もあり得ますが、「可変」Prefix 配布については、事業者側の提供コスト、ASP サービスやユーザのニーズなどの精査、議論が必要と思われます。

アクセス網におけるアドレス設計

アクセス網でのアドレス設計は、基本的には IPv4 と同じです。

顧客用アドレス

ISP から接続アドレスが提供されます。ISP からは接続回線毎に Prefix 束で渡され、配布 Prefix と RA により、IPv6 アドレスが提供されます。

ネットワーク構成における考慮点として、センター局にのみ LNS を設置するネットワーク構成では、センター局 LNS で Prefix 集約可能となります。全国に複数 LNS を設置するネットワーク構成では、地方拠点毎の Prefix 集約は可能です。固定 Prefix 配布サービスを行う場合、ISP からの Prefix 束をどのような大きさに分けるか、ISP 側も把握しておく必要があります。

事業者インフラ用アドレス

事業者インフラ用アドレスは、ISP バックボーンに準じます。IPv6 を PPP や L2TP でトンネリングするネットワークにおいては、機器には IPv4 アドレスのみを振ります（DSLAM～BRAS 間網など）。IPv6 パケットを扱うネットワークにおいては、IPv6/IPv4 アドレスを振る必要があります（BRAS～ISP 接続ルータ間網など）。

ISP 網からみたアドレス設計

ISP 網からみたアドレス設計も、基本は IPv4 と同様です。

顧客用アドレス

接続毎に必要分の Prefix プールを渡します。

固定 Prefix 提供の場合の考慮点として、アクセス事業者の網構成を意識した Prefix 設計が

必要です。基本は LNS 毎の Prefix 集約で、LNS 設置場所を意識した Prefix 計画が求められます。

事業者インフラ用アドレス

これについては、バックボーンのアドレッシングの項目を参照してください。

IPv6 アクセス網～ISP 網間ルーティング

基本的な考えは、ISP コア網～上流 ISP 網接続と同様です。ISP 網からみるとアクセス網は顧客として見え、アクセス網から見ると、ISP 網は上流 ISP 網として見えます。

経路制御は、各接続で経路集約されているものと想定します（動的 Prefix 配布で BAS に Prefix がプールされている場合）。集約できない経路が発生する場合には、動的ルーティングなどの検討が必要となります。

接続は、シングルホームの場合、スタティックルーティングです。複数リンクで接続する場合には、障害時の自動切換え、冗長、負荷分散などの考慮が必要となります。

マルチホームの場合は動的ルーティングが必要となります。複数リンクに対するケアも、動的ルーティング+α で対応します。

ADSL/FTTH

推奨移行方法

推奨移行方法の概要としては、顧客宅内の CPE 、及びアクセス網事業者の BAS (LNS BAS)を IPv6 に対応させることになります。IPv6/IPv4 デュアルスタックによる接続で、顧客トラフィックは IPv6 、IPv4 とも同一 BAS で終端されます。

顧客接続方式は Site 型が一般的です。Host 型の場合、IPv6 通信のパケットフィルタリングなどの考慮が必要となります。

各機器の要件

・BAS の IPv6 対応要件

BAS とは、Broadband Access Server、または BRAS:Broadband Remote Access Server で、ブロードバンド接続を集線する装置のことです。一般的には PPP を終端しています。機能により、LNS(L2TP Network Server)、及び LAC(L2TP Access Concentrator)に分けられま

す。
　IPv6 対応　LNS BAS の要件は次の通りです。

L2 層
PPPoE/oA を終端する
L2TP(IPv6 を扱う場合には LNS 機能)をサポート
PPP IPv6NCP(IPV6CP)をサポート

L3 層
IPv6 アドレッシング、ルーティング対応
PPP リンク接続先に対して RA、及び DHCPv6-PD を送る

上位層
認証
PPP 認証は IPv4 と同様
RADIUS IPv6 Attribute を扱うこと（IPv6 Prefix）
IPv6リンク（IPV6CP）アップ後に、アカウントとIPv6 Prefix情報を元に、PPPリンク接続先にRA、DHCPv6-PD を送る
BAS の IPv6 対応要件(続き)

IPv6 対応　LAC BAS の要件は次の通りです。

L2 層
PPPoE/oA を扱う
L2TP LAC 機能をサポート
ユーザアカウントサフィックスに対して、適切な LNS BAS に L2TPトンネルを設定する（サフィックス情報は LAC 手動設定、もしくは RADIUS などの機能を利用する）
IPV6CP のサポートは必要なし(PPP をトンネルするため)

L3 層
IPv6 のサポートは必要なし(ユーザの L3　層データは扱わないため)

上位層
必要であれば PPP 認証
RADIUS との連携(必要があれば)

BAS 接続構成

BAS 接続ネットワークは、(LNS)BAS が IPv6 に対応すれば、その他は基本的に IPv4 の場合と同様に構成可能です(L2TP トポロジーなど)。

ルーティングは次のように構成します。

上流(ISP)では静的、もしくは動的なルーティングです。アクセス事業者のネットワークポリシーに依存します。直接 ISP に接続する場合には、冗長性を高めるルーティングの採用が望まれます。 BAS で経路集約をすることが望ましいですが、アドレス設計の項を参照してください。

Home 側は、各 CPE リンク(PPP 等) への静的ルーティングです。

CPE の IPv6 対応要件

CPE の IPv6 対応要件については、Site 型モデル、Host 型モデル、Host 型モデル(機能追加)のモデルごとに検討します。

注意点として、CPE における Path MTU Discovery の実装などがあります。CPE に求められる機能には、CPE のマルチキャスト対応などがあり、接続認証についても検討が必要です。

■Site 型モデルの CPE

·IPv6 パケット転送

IPv6 ネットワークを終端、ルーティングします。

·アドレス割り当て

家庭内機器に対するアドレス割り当てを行います。

網→CPE は DHCPv6 PD と RA を使用します。

CPE→家庭内機器は、DHCPv6PD Prefix 情報から RA を生成します。/48 Prefix の通知を受けた場合には、CPE で任意の/64 を 1 つ切り出し、RA Prefix を生成し、網側 RA を Proxy (RA Proxy)します。

CPE の網側アドレスについては、リンクローカル接続、RA などで設定します。

·ルーティング

ルーティングについては、ISP 網への静的デフォルトルーティングを行います。Home 側 Prefix への静的ルーティング(Connected)となり、Home 側でのダイナミックルーティングはオプションです。ISP 網へのダイナミックルーティングは通常行いません。

·セキュリティ

IPv4 と同様のフィルタリングを行います。

■Host 型モデルの CPE

·IPv6 パケット転送

IPv6 パケットのみブリッジ(IPv4 はルータとして機能)、しかしこれは情報家電接続の観点からは望ましくありません。RA Proxy 対応ルータが望ましいです(後述)。

·アドレス割り当て

網からの RA を転送することになり、アドレス割り当てはありません。

·ルーティング

ありません(そのまま通過)。

·セキュリティ

フィルタリングは行われません。

■Host 型モデルの CPE(機能追加)

これは、Host 型モデルの CPE を高機能化するものです。CPE を RA Proxy 実装ルータとします。情報家電対応の要望にしたがい、CPE でセキュリティを確保します。

・IPv6 パケット転送

IPv6 ネットワークを(擬似的に)終端、IPv6 ルーティングします。網側からは同一ネットワークであり、Home 側からは分断しているように見えることになります。

アドレス割り当て

網→端末(及び CPE)で、RA Proxy を行います。

ルーティング

ルーティングについては Site 型と同様です。

セキュリティ

一般的なフィルタリングを実施します。

CPE における Path MTU Discovery(PMTUD)

IPv6 PMTUD は、IP を扱う機器(ブロードバンドネットワークでは CPE、(LNS)BAS など)が

実装する機能です。下位レイヤでは PMTUD は扱いません(扱えません)。

ブロードバンド事業者網では、PPPoE、L2TP などの構成が一般的であり、PPP、L2TP ヘッダ等のオーバーヘッドのため、Ethernet での一般的なサイズ(1500byte)より MTU サイズが小さくなります。PPP などで MTU 情報を網(BAS)から CPE 通知、CPE インタフェースに MTU 設定します(LCP MRU オプション)。

しかし、MTU 情報通知や、CPE での MTU サイズ設定に失敗した場合、CPE と ADSL 網で MTU の扱いに違いが生じます。CPE ではパケットを通し、ADSL 網でオーバーサイズのパケットとして廃棄します。すると、永久に MTU を学習できず、パケットが通りません。

そのため、PPP ネゴシエーション時に MTU サイズの情報を通知する必要があります。MRU オプション利用と、MRU 情報からのインタフェース MTU サイズ設定の適切な実装が推奨されます。

また、ICMP Packet Too Big Message を扱う適切な実装が求められます。ICMP Message パケットをフィルタしないことが必要です。

さらに、PPP 接続でない場合、かつ CPE～IPv6 ルータ間での網側下位レイヤで MTU サイズが変わる場合、CPE に適切な MTU サイズを通知する機能が必要です(一般的な PMTUD の適切な実装が求められます)。

CPE のマルチキャスト対応

ネットワークモデル別に考えると、以下の 2 通りが考えられます。

·BAS で集約するモデル(サイト型、ホスト型 PPP 接続の場合など)

マルチキャストパケットは、L3 を終端するデバイス(BAS)に集約されます。可用性は、一般的に BAS の性能に依存します。

·フラットなモデル(ホスト型 L2 接続の場合など)

VLAN を設定する場合には上記と同様の問題があります。フラットな空間の場合、PrivateVLAN などとマルチキャストとの共存が必要で、ND 時のマルチキャストの扱いの方法が問題となるかもしれません。

デバイス別には、CPE が IPv6 を扱う必要があるかどうかで区別できます。

·CPE が IPv6 を扱う場合

CPE が MLD/IPv6 マルチキャストルーティング、MLD プロキシに対応します。

·CPE が IPv6 を扱えない/扱わない場合

L3 接続先(BAS 等)で MLD をサポートする必要があります。

接続認証

リンク接続時に PPP LCP 等で認証を行います。アドレス払い出し時に改めて認証は行いません。

·Site 型

CPE～BAS 間の接続認証については、ユーザ認証、ユーザ特定は PPP 認証が一般的です。PPP 認証後はユーザに対して認証はありません。アドレス払い出し時などに改めて認証はしません。

·Host 型

端末～BAS 間の接続認証は、物理的紐付けによる認証、もしくは端末での PPP 認証です。

接続方法

Site 型(その 1)

これはプロバイダルータ(BAS 含む)の IPv6 対応で実現する IPv6 接続です。個人向けサービスでは一般的ではありませんが、SOHO 接続などではあり得ます。顧客収容ルータに物理回線が紐づいているので、固定アドレスのサービスは提供しやすいといえます。

CPE～プロバイダルータ間接続は、PPPoA/PPPoE(、専用線、ATM)、など、何らかの土管的な接続を行います。

CPE への IPv6 設定は手動設定が一般的です。

CPE～端末間は、一般的に Ethernet 接続 (IPv6 over Ethernet)で、IPv6 自動アドレス設定を利用します。端末での IPv6 DNS Cache アドレス検出(DNS アドレス通知等)の手法が課題となります。

認証については、回線などの設定を固定にすることでユーザを特定するため、認証のためのシーケンスはありません。

Site 型(その 2)

こちらは(LNS)BAS の IPv6 対応により実現するものです。個人向けサービスでは一般的な形態です。

BAS～CPE 間接続は、PPP NCP(IPV6CP)による接続となります。同一 LCP 上で IPCP と IPV6CP を同時に起動する方法が一般的です。

Prefix 配布では、DHCPv6 Prefix Delegation Option を利用します。サイズは、/64、/48 の配布が一般的です。同じスキームで DNS Cache アドレス等の通知も可能です。

CPE～端末間は、一般的に Ethernet 接続 (IPv6 over Ethernet)です。IPv6 自動アドレス設定を利用します。端末での IPv6 DNS Cache アドレス検出(DNS アドレス通知等)の手法が課題です。

認証は、PPP 認証（CPE でのアカウント設定）を行います。BAS～RADIUS は、通常と同様の認証です。固定 Prefix が必要であれば、IPv6 Prefix の Attribute 対応が求められます。

(LNS)BAS の IPv6 対応に関しては、L2TP 形態の場合、LAC BAS は IPv6 に対応する必要はありません。

アカウントは IPv4 と同様、接続認証に利用します。IPv4 サービスと、IPv6(もしくはデュアルスタックサービス) で Suffix を別にします。つまり、Suffix で IPv6 対応 BAS 収容と IPv4 対応 BAS 収容を分けます。

Host 型 L2 接続

・BAS～CPE 間

この場合、BAS～CPE 間は、端末側から見ると、ネットワーク側は Ethernet 同一セグメントに見えます。

アドレス付与は、BAS から RA を送付して実施しますが、BAS～CPE 間のセグメント形態により実現方法が異なります。

BAS～CPE が 1 セグメントの LAN の場合、RA は 1 つを共有します。同一 BAS に収容される端末が直接通信できますが、一般的には不具合があることが多い方法です。何らかの対策(PrivateVLAN など)が必要となります。

BAS～CPE 間がユーザ毎に別セグメントの場合は、BAS～CPE 間に VLAN を設定するなどを実施します。RA はユーザ毎に別個となります。同一 BAS 収容端末間同士の通信においても必ず BAS を介します。

・CPE～端末間

CPE～端末間は一般的に Ethernet 接続 (IPv6 over Ethernet)となります。IPv6 自動アドレス設定を利用しますが、端末での IPv6 DNS Cache アドレス検出(DNS アドレス通知等) の手法が課題となります。

CPE ですべての Ethernet フレームをブリッジする形態と IPv6 パケットの Etheret フレームの

みをブリッジする形態があります。後者の場合、IPv4 パケットはモデムで終端します。
端末側から見ると、ネットワーク側は Ethernet の同一セグメントに見えます。

・L2 接続のモデルでの認証機構

アドレス付与に対する認証はなく、下位レイヤでの接続認証に依存します。CPE がない場合、顧客を収容するスイッチが、VLAN 終端など CPE 的な役目を果たします。認証は特になく、必要であれば CPE～網間で L2 の認証を行います。回線と Prefxix を紐付けします。

Host 型 PPPoE 接続

·BAS～CPE 間

この場合、PPP NCP(IPV6CP)による接続となります。同一 LCP 上で IPCP と IPV6CP を同時に起動する方法が一般的です。PPP 接続時にユーザ認証を行います。
Prefix 配布には RA が利用され、ユーザ毎に/64 を配布します。同一 BAS 収容端末間同士の通信においても必ず BAS を介します。
BAS～CPE 間のセグメント形態には依存しません。

·CPE～端末間

CPE と端末の間は一般的に Ethernet 接続 (IPv6 over Ethernet)です。CPE ですべての Ethernet フレームをブリッジする形態と、IPv6 パケットの Etheret フレームのみをブリッジする形態があります。後者では、IPv4 パケットはモデムで終端します。
端末側から見ると、ネットワーク側は Ethernet 同一セグメントに見えます。BAS からの RA による IPv6 自動アドレス設定が実施されます。
端末での IPv6 DNS Cache アドレス検出(DNS アドレス通知等)の手法が課題となります。
CPE がない場合についてですが、L2 的には BAS～端末が PPP で直接接続される形態であるため、CPE の有無には依存しません。

·認証

PPP 認証では、端末でのアカウント設定が行われます。
BAS ～RADIUS 間は、通常と同様の認証です。固定 Prefix が必要であれば、IPv6 Prefix の Attribute 対応が必要です。

Home ネットワークでの問題点

Home 内マルチプレフィックス

家庭内で利用されるマルチプレフィックスには、ISP 間マルチプレフィックスと ISP 内マルチプレフィックスの 2 通りがあります。

ISP 間マルチプレフィックスとは、異なる上位 ISP に対するマルチホームです。ISP 接続（CPE）がひとつであれば割に容易ですが、ISP 接続（CPE）が複数になった場合には適切な出口を選択する機構が必要です。

検討事項としては、SOHO などの需要はあるか、そしてアドレスフィルタリングなどとの関係の確認が必要です。また、マルチホームの標準化動向(IETF multi6 WG)を注視する必要があります。

ISP 内マルチプレフィックスは、同一 ISP でのサービス分けを行う手段としての利用が想定されます（インターネット接続、VoIP、放送型ストリーミング、情報家電接続など）。

Prefix により、外部接続のありなし、固定アドレスのありなし、QoS のありなし、などの網要件を変えることができます。

Prefix の渡し方には、複数の Prefix として渡すか、ひとまとまりの Prefix として渡して内部分断するか、の 2 通りが考えられます。後者の場合、CPE に Prefix の意味を知ってもらう必要がありますが、サービスモデルによって分断方法も異なり、CPE では対応しにくいと言えます。

技術的には、アドレスセレクション/ルーティングセレクションの問題となります。ソースアドレスセレクションは RFC となっています。あて先セレクションは名前解決で実施することができるため、ソースルーティング技術の必要性の有無を検討する必要があります。

情報家電で、マルチプレフィックスを扱うことが可能かどうかも検討課題です。

Home 内プレフィックス管理とその方針

家庭内で利用されるプレフィックスの管理については、まず網からのプレフィックス通知をどうするかが検討課題となります。つまり、太束(/48) で受け、Home で分割するか、/64 を複数受けるかという問題です。どちらにしても、CPE でマルチプレフィックスの扱いが必要となります。

もう 1 つの課題は、プレフィックス利用について、用途毎にサブネットに分けるかどうかという点です。 用途が重なる場合には、同一リンクに複数プレフィックスを流すことに意味があります。

Home 内マルチリンク

別の検討課題としては、Home 内でのダイナミックルーティングサポートがあります。ただし、これは Home がマルチリンクになった場合に検討対象となります。したがって、Home がマルチリン

クになること、ISP がそれをサポートすることはあり得るかをまず考える必要があります。この問題には、ISP 的立場とユーザ的立場があります。

ISP の立場としては、ISP 側から Home 内の1つ以上のリンクを管理することは困難なため、マルチプレフィックスを配布して、Home の責任で分割して利用してほしいということになります。

ユーザの立場としては、特に一般ユーザの場合、サービスであればサポートはしてほしいということになります。ISP でマルチリンクをサポートする仕組みが必要かどうかが焦点となります。

その場合、各ルータ間の情報連携（特にアドレス配布に関して）が求められ、そのときこそ MSR(Multilink Subnet Router)が必要となるかもしれません。

情報家電をサポートする CPE に求められる機能

情報家電機器に欠けているネットワーク関係機能の補完は今後の重要なテーマの 1 つです。

ネットワークデバイスとしての情報家電の機能は当面飛躍が期待できません。特にセキュア通信や名前解決の手段などにこれが当てはまります。したがって、これらの機能をネットワークで補完することが期待されます。

すると、ネットワーク機器として家庭に存在する CPE がキーになってきます。外部端末～家庭ネットワーク(CPE)間セキュア通信の実現、情報家電機器の名前解決を補佐する手段(DDNS/SIP など)の実装等が求められます。

CPE で実現するセキュリティ

CPE で実現することの求められるセキュリティ機能には、パケットフィルタリング、セキュア通信への対応などがあります。

パケットフィルタリングについては、IPv4 と同機能のものについては、BCP で対応済みです。したがって、IPv6 独自の機能として、求められる機能があるかどうかということになります。たとえば、情報家電との連携の可能性はあります。UPnP など、情報家電と CPE の情報のやり取りを行うことが考えられます。

セキュア通信への要求については、CPE への IPsec、SSL/TLS 実装などがあります。

IPsec では、鍵交換インフラが問題となります。SSL/TLS では、各 CPE への証明書発行、インストールが問題となります。

これらについては、ASP 的対応が必要です。

CATV

推奨移行方法

CATV に関する概要として、現状では、宅内ルータとセンター間のトンネル接続の形態を推奨します。 宅内にデュアルスタック(トンネル)ルータ を置き、センターにトンネル終端ルータを置くというモデルです。

顧客接続方式は一般的に Site 型です。CATV インターネットの IPv6 対応標準化は進行中といえます。

CATV インターネットの IPv6 移行モデル

CATV インターネットでの IPv6 対応の現状としては、DOCSIS での IPv6 対応は検討中であり、CATV インターネット設備で IPv6 を実装したものはまだ少ない状況です。

CATV ネットワークでの IPv6 対応の課題点として、CM や Bridged CMTS 上での ND 動作の問題(マルチキャストの扱い、ND Proxy)、IPv6 トラフィックの Classfication(IPv6 はすべて BestEffort 扱いのため、IPv6 電話パケットなどの優先制御が不可能)が挙げられます。

以上の制限より現状多くの CATV がトンネルで IPv6 を提供しています。DOCSIS の IPv6 対応が待たれるところです。

移行モデルとしては、以下の 2 つが考えられます。

·Bridged CMTS

·Routed CMTS

いずれのモデルも CM、CMTS は管理目的でいくつかの L3 機能を有します。

各機器の要件

CATV インターネットの構成要素には、以下のものがあります。

·Edge Router (ER)

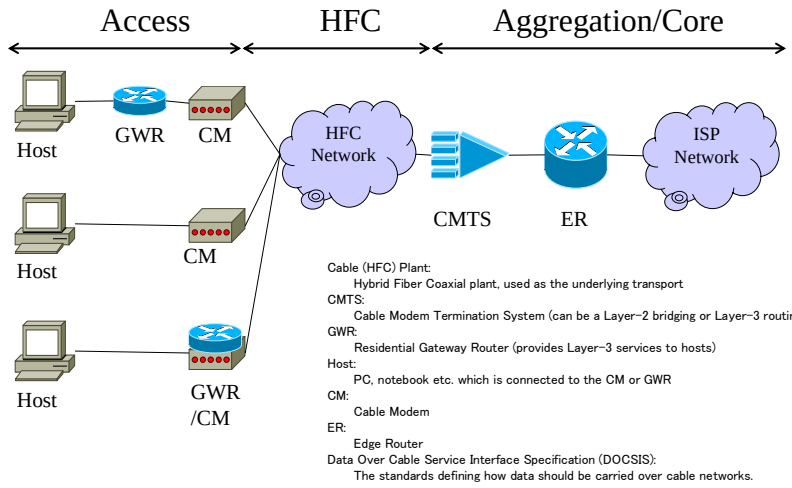
·CMTS (Cable Modem Termination System)

·CM (Cable Modem)

·GWR (Residential GateWay Router)

IPv6 移行に影響するこれらの要素は、以下のように図示することができます。

影響するケーブルネットワークの要素



接続方法

以下では、下記の接続方法において、各機器の要件を示します。

・Bridged CMTS

Site 型

Host 型

・Routed CMTS

Site 型

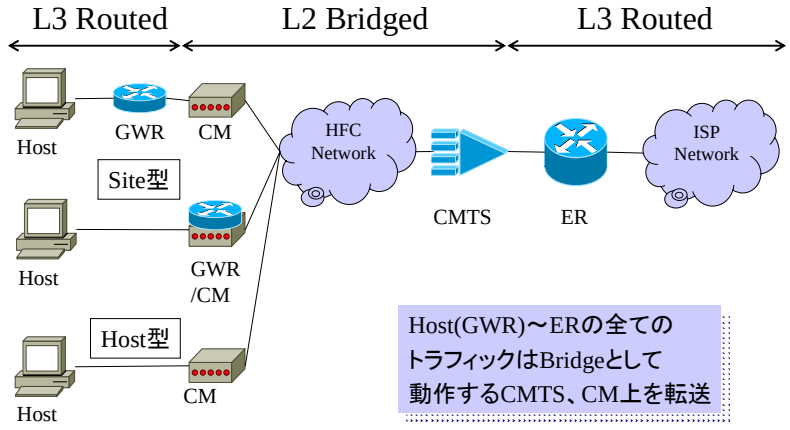
Host 型

CATV インターネット網は一般的に、本ドキュメントで言うところのアクセス網と ISP 網が一体ですが、ここでは顧客～アクセス網接続を議論します。上流 ISP への接続は、ISP の上流接続の項目を参照してください。

Bridged CMTS での IPv6 対応

Bridged CMTSでのIPv6対応

■ モデル



Bridged CMTS での IPv6 対応（Site 型）

・インフラ

インフラについては、Host、GWR(GWR/CM)、ER の IPv6 ルーティング対応が必要となります。CM および CMTS は IPv6 ルーティング対応が必要なく、IPv6 Packet のブリッジが必要です。これについては、データ転送の項目を参照してください。IPv6 Unicast/Multicast パケットについても、この Bridge 区間（CMTS～CM）で転送される必要があります。

・アドレシング

アドレシングについては、CM に対し、管理目的で DHCPv4 により IPv4 アドレスが割り当てられます。Host については、GWR に DHCP-PD で/64 以上（一般的には/48）を割り当てます。固定アドレス払い出しの場合には、DHCPv6-PD の MAC アドレス認証などが利用可能です。

・データ転送

CMTS では、IPv6 パケットのブリッジを行います。CMTS では、ND パケットの転送、もしくは ND Proxy を実装する必要があります。異なるサイト間の通信は、CMTS、CM が正確に Multicast IPv6 ND を転送するかどうかに依存します。NDは Link Local Multicast を利用します。どちらを利用するにしても、IPv6 Link Local Multicast の対応が必要となります。

CM では、IPv6 パケットのブリッジを行います。異なる CM 配下の Host は必ず CMTS を介し

て通信します。CM についても、ND パケットの転送、もしくは ND Proxy を実装する必要があります。DOCSIS Cable Network を跨いで IPv6 Multicast アプリを使う場合、CMTS と CM は、IGMPv3/MLDv2 の Snooping をサポートする必要があります。

・ルーティング

ルーティングに関しては、Host では ER へのデフォルトルーティングの静的設定を行います。ER では、Host に対する静的ルーティング設定を行います。DHCP-PD を使用する場合、Host に委譲された Prefix に対する Static ルートが定義されます。

上流への経路制御は IGP を利用します。上流に対して Host 経路の集約を行うことが望ましく、上位の経路制御によっては ER が iBGP を扱います。

Bridged CMTS での IPv6 対応（Host 型）

・インフラ

Host、ER の IPv6 ルーティング対応が必要です。一方、CM/CMTS は IPv6 ルーティング対応が必要なく、IPv6 Packet Bridging が必要です。これについては、データ転送の項目を参照してください。IPv6 Unicast/Multicast パケットもこの Bridge 区間（CMTS～CM）で転送される必要があります。

・アドレシング

アドレシングについては、CM に対し、管理目的で DHCPv4 により IPv4 アドレスが割り当てられます。Host については、CM 配下に RA もしくは DHCPv6 により/64 を割り当てます。固定アドレス払い出しの場合には、固定 RA+固定端末(固定 MAC アドレス)による方法、 DHCPv6-PD の MAC アドレス認証などが利用可能です。

・データ転送

CMTS では、IPv6 パケットのブリッジを行います。ND パケットの転送、もしくは ND Proxy を実装する必要があります。異なるサイト間の通信は、CMTS、CM が正確に Multicast IPv6 ND を転送するかどうかに依存します。NDは Link Local Multicast を利用します。どちらを利用するにしても、IPv6 Link Local Multicast の対応が必要です。

CM でも、IPv6 パケットのブリッジを行います。異なる CM 配下の Host は必ず CMTS を介して通信します。CM にも、ND パケットの転送、もしくは ND Proxy を実装する必要があります。DOCSIS Cable Network を跨いで IPv6 Multicast アプリを使う場合、CMTS と CM は、IGMPv3/MLDv2 の Snooping をサポートする必要があります。

・ルーティング

ルーティングに関しては、Host では ER へのデフォルトルーティングの静的設定を行います。ER では、Host に対する静的ルーティング設定を行います。DHCP-PD を使用する場合、Host に委譲された Prefix に対する Static ルートが定義されます。

上流への経路制御は IGP を利用します。上流に対して Host 経路の集約を行うことが望ましく、上位の経路制御によっては ER が iBGP を扱います。

Bridged CMTS 共通事項

Bridged CMTS に共通の事項としては、接続認証に、既存の認証方法の流用が可能だという点が挙げられます。 CM の MAC アドレスによる DHCP 認証が一般的です。

Proxy ARP を利用する CM の IPv6 対応

CM における端末の MAC アドレス認証では、Proxy ARP を利用する可能性があります。これは、CM がブリッジとして動作する場合、かつ MAC アドレス認証を行っている場合に当てはまります。Ethernet フレームの発 MAC アドレスを見てフレームを通すか判断します。CM は Ethernet フレーム透過のため、いったん CM でフレームを受けて再度反対のインタフェースに送信し直します。CM が Ethernet MAC アドレスを持つ場合、かつルータとして動作しない場合には Proxy ARP の動作を行います。同じことは Bridged CMTS にも適用できます。

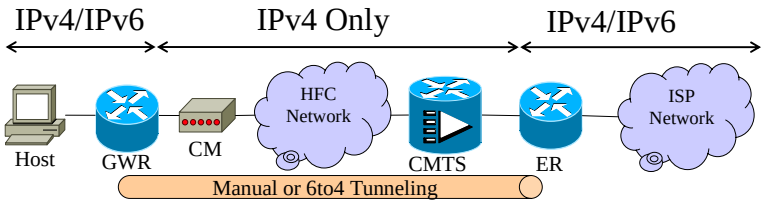
この場合の IPv6 対応は、CM が端末から IPv6 パケットを含む Ethernet フレームを受け取ります。CM でいったん受けて、再度ルータに送り直します。ルータ宛の IPv6 パケットの MAC アドレスは CM の Ethernet MAC アドレスに変換する必要があります。したがって、IPv6 ND Proxy などの対応が必要です。

Routed CMTS での IPv6 対応（Site 型）

・GWR～Routed CMTS 間トンネル接続

CM、CMTS は IPv4 装置のままで、ER、Host、GWR がデュアルスタック対応になります。

Site型: GWR～Routed CMTS間トンネル接続

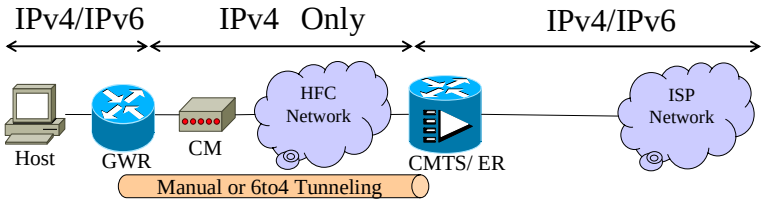


- IPv6対象機器
  - Host、GWR、ER
- アドレッシング
  - GWR～ER間
    - リンクはERからの/64 RA
    - DHCPv6 PDによるPrefix配布
  - GWR～Host間
    - RA
- データ転送
  - GWR～ER間トンネル
  - CM、CMTSはIPv4の扱いのみで良い
- ルーティング
  - Host
    - RAによるデフォルト設定
  - GWR
    - RAもしくは静的デフォルト設定
    - LAN側Prefixルーティング
  - ER
    - IGP等
    - 経路集約

·GWR～Routed CMTS/ER 間トンネル接続

CMTS と GWR が IPv6 対応します。CM は IPv6 を通す必要がありません。CMTS と GWR の IPv6 対応には、HW,SW のアップグレードが必要になるでしょう。

Site型: GWR～Routed CMTS/ER間トンネル接続

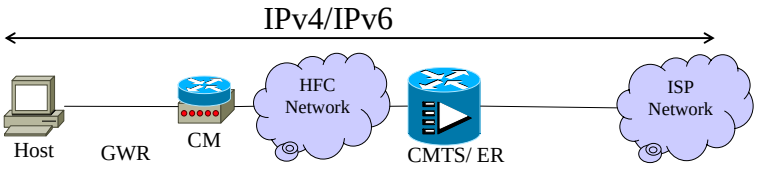


- IPv6対象機器
  - Host、GWR、CMTS/ER
- アドレッシング
  - GWR～CMTS/ER間
    - リンクはCMT?S/Rからの/64 RA
    - DHCPv6 PDによるPrefix配布
  - GWR～Host間
    - RA
- データ転送
  - GWR～ER間トンネル
  - CMはIPv4の扱いのみで良い
- ルーティング
  - Host
    - RAによるデフォルト設定
  - GWR
    - RAもしくは静的デフォルト設定
    - LAN側Prefixルーティング
  - ER
    - IGP等
    - 経路集約

·GWR/CM～Routed CMTS/ER ネイティブ接続

GWR と CM が一体型で IPv6 対応し、CMTS も IPv6 対応します。埋め込み CM/GWR と CMTS の変更が生じるため、今日展開させるのは難しい状況です。埋め込み CM/GWR への DOCSIS の仕様変更も必要になります。

Site型: GWR/CM～Routed CMTS/ERネイティブ接続



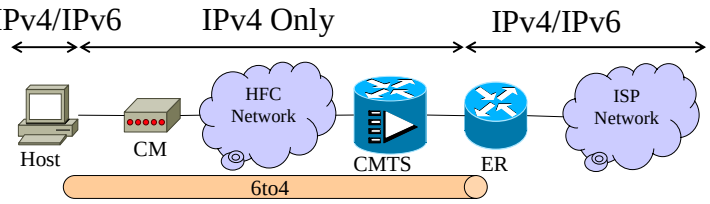
- IPv6対象機器
  - Host、CM/GWR、CMTS/ER
- アドレッシング
  - CM/GWR～CMTS/ER間
    - リンクはERからの/64 RA
    - DHCPv6 PDによるPrefix配布
    - CMTS/ERはDHCPv6 Relayをサポートする必要
  - CM/GWR～Host間
    - RA
- データ転送
  - IPv6ネイティブ転送
  - CM/CMTSはIPv6ルーティングを行うのでNDやMulticastはルータとして対応
- ルーティング
  - Host
    - RAによるデフォルト設定
  - CM/GWR
    - RAもしくは静的デフォルト設定
    - LAN側Prefixルーティング
  - CMTS/ER
    - IGP等
    - 経路集約

Routed CMTS での IPv6 対応（Host 型）

·Host～ER 間トンネル接続

CM、CMTS は IPv4 装置のままで、ER と Host のみがデュアルスタック対応になります。

Host型: Host～ER間トンネル接続

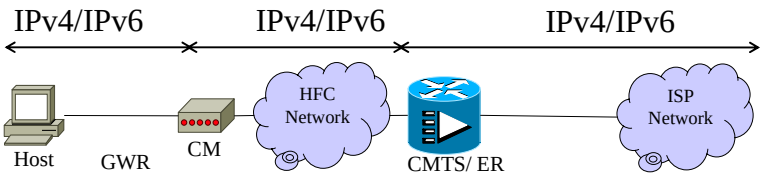


- IPv6対象機器
  - Host、ER
- アドレッシング
  - 静的、もしくはRA/DHCPv6
- データ転送
  - Host～ER間トンネル
  - CM、CMTSはIPv4の扱いのみで良い
- ルーティング
  - Host
    - 静的デフォルト設定
  - ER
    - IGP等
    - 経路集約

·Host～CMTS/ER 間ネイティブ接続

CMTS が IPv6 対応するとともに、CM が IPv6 Unicast/Multicast をブリッジします。これは DOCSIS の IPv6 対応を意味するため容易ではありません。CMTS の IPv6 対応には、ハードウェア、ソフトウェアのアップグレードが必要となるでしょう。

Host型: Host～CMTS/ER間ネイティブ接続



- IPv6対象機器
  - Host、CMTS/ER
  - CMはIPv6ブリッジ
- アドレッシング
  - CMTS/ER～Host間
    - RA
    - DHCPv6で配布する場合には、CMTS/ERはDHCP Relayをサポートする必要あり
- データ転送
  - IPv6ネイティブ転送
  - CMでのND(RS/RA含む)Proxyなどの実装が必要
- ルーティング
  - Host
    - RAによるデフォルト設定
  - CMTS/ER
    - IGP等
    - 経路集約

CMTS での DHCP Relay の挙動

DHCP パケットリレーの扱いについては、DHCP Discover パケットに対して、Option に CM の MAC アドレスを付与してリレーします。再リース時の unicast DHCP パケットに対しても CM の MAC アドレスを付与することが望ましいと考えられます。

Bridged/Routed CMTS 共通課題

・IPv6 Multicast

CM、bridged CMTS は IGMPv3/MLDv2 snooping に対応する必要があります。現在の CM は Multicast 通過に関して問題のある実装が多く見られます。Multicast を適切に扱う実装が必要であり、DOCSIS に IPv6 Multicast の扱いの明記の働きかけが必要となります。

・IPv6 QoS

現状は、DOCSIS で IPv6 のクラス分けが未定義です。IPv6 の Unicast/Multicast トラフィックを DOCSIS ネットワーク上で適切に分類する基準が必要となります。以下の項目について、128bit の IPv6 アドレスをサポートする必要があります。

·IP source address
·IP source mask
·IP destination address
·IP destination mask
·IP traffic class (DSCP)

次の 2 つの分類も IPv6 で新たに必要となります。

·IP version
·Flow label (optional)

・セキュリティ

DOCSIS 内では BLP+（Baseline Privacy Plus）で提供しています。暗号化された Multicast のみが IP アドレスに依存します。IPv6 の暗号化 Multicast に対応するために、DOCSIS の仕様を適切に拡張する必要があります。

もう一つの方法として、IPv6 では実装が必須の IPsec を利用する方法がありますが、鍵配布の仕組みが課題です。

・パケットフィルタリング

CM、もしくはCMTSでIPv6パケットフィルタリングを行います。レイヤをまたがるフィルタリングの設定が可能です（ブリッジ動作するCM/CMTSでのIPパケットフィルタリング）

パケットフィルタリングは通常、CM で行います。フィルタするパケットの種類はファイル共有(Windows/AppleTalk)、ウィルス対策、意図しない（故意にネットワークに流された)RA やDHCPv6応答などです。DOCSIS規定によって、MACアドレスによるユーザ端末接続台数制限も行います。

IPv6を扱うL3機器(GWR、Host、Routed CMTS、ER)でのパケットフィルタリングも可能ですが、CM(/CMTS)フィルタとの整合性を取る必要があります。必要に応じて Host において匿名アドレスを利用します。

・内部攻撃などへの対処

CMTS Bridged Modelの場合、同一CMTSに収容される別顧客のHostが同一セグメントとして収容されてしまいます。このため、網側でのパケット制御が不可能となり、無意識のファイル共有、悪意あるユーザからの内部の攻撃などから守れません。この場合、CM(/CMTS)でのフィルタリングが有効です。

IPv6 を扱うL3 機器(GWR 、Host 、Routed CMTS 、ER) でのパケットフィルタリングも可能です。ただし、CM(/CMTS) フィルタの整合性を取る必要があります。

・IPv6 ネットワーク管理

DOCSIS、PacketCable、CableHome MIB は、IPv6 対応を既に検討しています。全てのSNMPオブジェクトに対し、IPバージョンを識別するオブジェクト、InetAddressTypeが関連付けられています。これにより、SNMP経由で顧客CMの状態を監視することが可能となります。

しかし、必ずしもSNMPプロトコルをIPv6に対応させる必要はありません。CM/SNMPマネージャサーバともCATV事業者でコントロール可能で、顧客のIPv6トラフィックを乗せるわけではありません。

CM 管理用トラフィックについては、DOCSIS で運用をサポートする場合、ユーザデータとは別波長で管理を行う可能性もあります（DHCPによるCMへのアドレス割り当て、tftp、SNMP等）。

・Provisioning

tftpを利用して顧客CMに対してリモートで設定の更新を行います。これはDOCSIS で規定されています。これを利用してIPv6 サービス開始時に、適切な設定にアップデートします。

しかし、必ずしもtftp プロトコルをIPv6 に対応させる必要はありません。CM/tftp サーバともCATV 事業者でコントロール可能であり、顧客の IPv6 トラフィックを乗せるわけではありません。

参考資料

ISP IPv6 Deployment Scenarios in Broadband Access Networks

(Draft-asadullah-v6ops-bb-deployment-scenarios-00.txt)

5. Broadband Cable Networks

無線 LAN

推奨移行方法

無線 LAN における IPv6 移行の概要は以下の通りです。

街頭ボックスは、既存の無線 LAN 機器をそのまま利用します。既設無線 LAN AP の IPv6 パケットの扱いを確認する必要があります。バックボーンへの接続は、導入時は IPv6 と IPv4 を分離して構築したほうが既存ネットワークへのインパクトが小さいということを指摘することができます。

顧客接続方式は、顧客からみると Host 型です。

無線 LAN の特徴

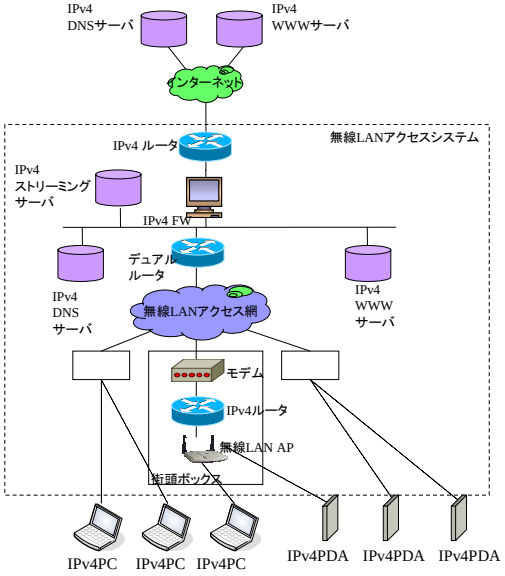
無線 LAN は、街頭ボックスと無線 LAN アクセスシステムで構成されます。

街頭ボックスは、モデム（ADSL などを利用して無線 LAN アクセスシステムに接続）、ルータ、無線 LAN アクセスポイントで構成されます。

一方、無線 LAN アクセスシステムは、内部ルータ（街頭ボックスなどの収容）、外部接続ルータ、サーバ群（WWW サーバ、DNS サーバ、ストリーミングサーバ、ファイアウォール）で構成されます。

IPv4 対応の無線 LAN ネットワークでは、IPv4 対応である無線 LAN アクセスシステムに対して、一般利用者は IPv4 端末で接続し、サービス提供側も IPv4 サーバで接続します。

無線LANネットワークの特徴



各機器の要件

街頭ボックス

街頭ボックスでは、モデムには既設モデムをそのまま利用します。ルータは、IPv6 対応する必要があります。無線 LAN アクセスポイントについても、既設無線 LAN アクセスポイントをそのまま利用しますが、IPv6 パケットの扱いについて確認する必要があります（後述）。

バックボーン

IPv6 を扱うことが可能なネットワークに移行します。下記の理由などから、IPv6/IPv4 を分離した形で実現します。

・ファイアウォール

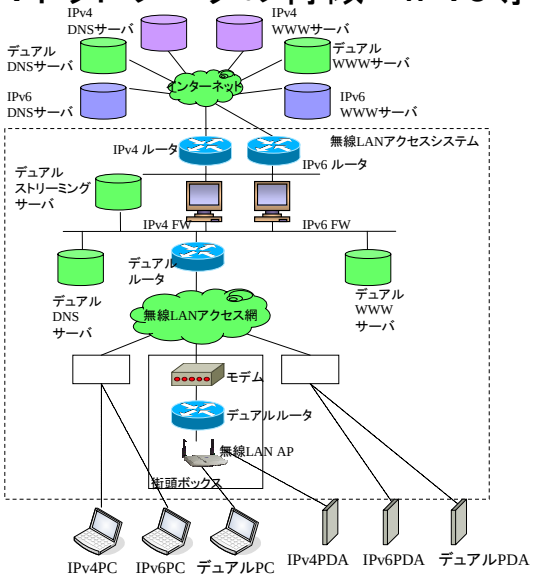
IPv4 ネットワークでは全端末用にグローバルアドレスの配布をすることが難しくネットワークアドレス変換（NAT）するのに対して、IPv6 ネットワークでは、全て一意のグローバルアドレスを配布できるためアドレス変換をする必要がない。これは、IPv4 ネットワークでは、一般利用者の端末は NAT 機器でアドレスがマスクされるためにインターネット側からの直接接続性を遮断できるのに対し、IPv6 では、全ての端末にインターネットからの接続性が提供できるためフィルタなどのセキュリティポリシーの記述が複雑になる可能性があることから、IPv4 サービスのパフォーマンスへの影響を排除する意味で分離する。

・ルータ

上位接続ルータの不具合は既存サービスの全てに影響を及ぼすため、安定運用が必須な既存サービスの IPv4 ルータとは分離する。

上記の課題が解決した段階で、同一機器/ネットワークで IPv6 を扱う(デュアルスタック)ネットワークに移行します。

無線LANネットワークの特徴 - IPv6導入時



接続方法(端末～バックボーン間)

概要

一般的に Site 型接続となります。無線 LAN スポットに情報ボックスを設置、情報ボックス内にモデム、ルータ、およびアクセスポイントがあるという構成です。ルータは IPv6 対応します。Ethernet フレームを基本とした Layer2 セグメントであるため、一般的に IPv6 通信に問題はありません。

アドレス配布

各街頭ボックスへのアドレス配布では、IPv6 アドレス自動設定(RS/RA)がそのまま利用可能です。通常はイーサネット 1 セグメントの Site 型接続として、固定/64 Prefix を割り当てます。街頭ボックスの WAN 側アドレスは静的、もしくはセンタールータからの RA で設定します。

Host へのアドレス配布は、各街頭ボックス内ルータからの固定 Prefix+RA で実施します。同

ー AP 内では通常固定アドレスとなりますが、匿名アドレスの利用による可変アドレスも許容できます。ただし、端末実装及び設定依存のため、無線 LAN 事業者からの固定/可変の強制は困難です。

アドレス配布時認証、対策など

MAC アドレスフィルタ認証の場合には、認証終了まで IPv6 通信が不可能であり、IPv6 通信をベースとしたアドレス自動設定の機能も認証終了時まで利用できません。

RADIUS 認証を使うには、IPv6 Attribute の対応が必要です。RADIUS トランスポート自体は IPv4 が利用できます。

ルーティング

IPv6 接続が実現された後の IPv6 ルーティングは通常通りです。

Host では、ルータへのデフォルトルーティング(RA/静的)、街頭ボックスルータでは静的です。ルータでは IGP は静的ルーティングで、アクセスポイント経路の集約を行う必要があります。

接続方法(バックボーン～ISP 間)

ISP への接続は、ネイティブ、デュアルスタックの 2 通りがあります。

さらに、ルーティング構成は静的ルーティング、動的ルーティングが考えられますが、冗長性確保のためには動的ルーティングが望まれます。IGP は BGP を使います。

トンネルの場合、トンネルルータを設置し、ISP とのトンネルを行います。ルーティングは上記と同様ですが、トンネルを 2 本つくり、ルーティング的に冗長を取ることも可能です。

確認すべき項目には、以下の点があります。

IPv6 Ethernet フレームの扱い

無線 LAN アクセスポイント、および無線 LAN カードが IPv6 Ethernet フレーム(プロトコル番号 0x86DD) を通すか確認する必要があります。 Unicast については一般的な Wi-Fi 証を受けた機器であれば問題はないと思われます。

特に、IPv6 ND の扱いを確認する必要があります。IPv6 ND(Ethernet Multicast フレーム) 、もしくは ND Proxy の対応を確認しなければなりません。特に、アクセスポイントで MAC 認証などを行っている場合は、これが重要です。

Multicast を扱う場合、Multicast Ethernet フレームの扱いの確認が必要です。Broadcast のみ通し、Multicast を通さないアクセスポイントの存在などが考えられます。

嘘つき RA/DHCP への対策

対策としては、ルータ RA の優先度を上げることも考えられます。DHCP についてはどうするかについては、IPv4 の問題として考えます。

アクセスポイント・セグメント内の”うそつき”RA/MLD 端末対策が必要

これについても、ルータの RA の優先度を上げることが考えられますが、完璧な対処法ではありません。

Proxy ARP を利用するアクセスポイントへの対策

アクセスポイントで MAC アドレス認証を行う場合に Proxy ARP を利用する可能性があります。このようなアクセスポイントでは、IPv6 ND への対応ができない可能性があります。ND Proxy などの対応が必要で、事前確認が必要となります。

Broadcast フレームを通し、Multicast フレームを通さないアクセスポイントへの対策

この場合、IPv6 ND などが扱えない可能性がありますので、必要な Multicast フレームを通す事前確認が必要です。

無線区間でのパケット落ち問題

ND や MLD パケットが引っかかると問題となります。Transmission of IPv6 Packets over 802.11/WLAN Networks(Draft-daniel-ipv6-over-wifi-01.txt)で指摘されています。

このなかで、DAD の扱い(Section 4.)について、WLAN では、”Source Address Based Packet Filtering At Layer2”が必須とされています。つまり、自ノードの MAC アドレスがソースとなるフィルタについては、アクセスポイントで L2 的にフィルタリングするということです。

ここでの問題は、DAD 時に同一 Link Local Address(=同一 MAC アドレス)を持つパケットを受信できず、アドレス重複を許してしまうことにあります。

解決策については、Source Address Filtering をはずすことは難しいですが、DAD パケット(NS/NA)の Source MAC アドレスは全て unspecified(All 0)にすることが考えられます。

また、検討項目としては、以下の点が考えられます。

ネットワークセキュリティ

無線 LAN ネットワークに接続するための認証は、既存の仕組みをそのまま利用することが可能です。これは、接続認証が IP プロトコルレイヤでは行われないためです。

SSID

接続先のアクセスポイントを指定する ID で、同じ SSID を設定した無線 LAN 端末だけが接

続可能となります。

IEEE802.1x 認証

センター側に設置している Radius サーバと無線アクセスポイントが連携して無線 LAN 上に接続されるユーザごとで認証を行いアクセス制御するため、高いセキュリティを確保することが可能となります。認証方法として、WPA のような事前共有鍵による認証、証明書ベースによる認証などがあります。

VLAN 認証

無線 LAN アクセスポイント上で認証されたユーザのみ、特定のサーバ、特定のネットワークへのアクセスを許可する VLAN への接続を提供し、限定されたユーザに対してのサービスを提供することが可能となります。

マルチキャスト

マルチキャストは MLD、マルチキャストルーティング(PIM-SM など)で既存の仕組みが利用できます。

しかし、IPv6 ルータがマルチキャストに対応する必要があります。特に、無線 LAN セグメントが ADSL 事業者回線などを利用した場合、事業者側 IPv6 設備(一般的には BAS)が IPv6 マルチキャスト伝送をサポートしていないことが考えられます。その際には、マルチキャストパケットを IPv6 トンネル等で上位マルチキャストネットワークまで直接接続するなどの工夫が必要となります。

また、無線 LAN セグメントに付随する L2 機器について、MLD Snoop などをサポートすることが望まれます。

無線 LAN ネットワークにおける移動透過性

同一無線 LAN セグメント上を移動する場合には、アドレスなどを含めて移動透過性が確保されます。しかし、無線 LAN の電波が補足できない箇所では一時接続性が切れます。このため、再認証、タイムアウトなどに関する対策が求められます。

異なる無線 LAN ネットワークを移動する場合には、MoblieIPv6 の適用が必要です。この場合、接続再認証などのタイミング、機器の MobileIPv6 対応、HA はどこに設置されるべきかといった点を検討しなければなりません。

IPv6 普及期の検討課題

IPv6 普及期には、IP サービス提供インフラのデュアルスタック化という検討課題が生まれます。この時期には、IPv4 設備と IPv6 設備の統合を進めることになるからです。

参考文献

ISP IPv6 Deployment Scenarios in Broadband Access Networks
（Draft-asadullah-v6ops-bb-deployment-scenarios-00.txt 8. Wireless LAN）

Transmission of IPv6 Packets over 802.11/WLAN Networks
（Draft-daniel-ipv6-over-wifi-01.txt）

携帯

推奨移行方法

携帯における IPv6 対応の概要は、以下の通りです。

まず、携帯データカードを接続した PC より、トンネルで接続します。IPv6 対応 OS の PC を利用しますが、トンネル方式（Configured / ISP Provisioned / Automatic Tunnel のどれを使うか）は、OS のサポート、及びサービス形式により異なります。

顧客の接続方式は、一般的に Host 型です。携帯データカードによる IPv6 ネイティブな接続は、携帯事業者設備の IPv6 接続対応が必要となります。また、携帯電話端末そのものの IPv6 接続は端末の対応も必要となります。

ここでは、携帯網そのものの IPv6 対応ではなく、携帯ユーザの IPv6 移行について検討します。つまり、ネットワークについては、端末～携帯網間インタフェースと携帯網～ISP 間インタフェースを検討します。 携帯網自体の作り方は（インタフェース部分などを除き）議論しません。

端末は、PC（ノート PC）+携帯（カードもしくは携帯端末）の構成で、IPv6 スタックは PC の OS を用います。携帯端末そのものの IPv6 対応については議論しません。

Best Current Practice として推奨できるのは、携帯を接続した（PC などの）端末の IPv6 対応を検討することです。接続携帯端末自身の IPv6 化は IPv6 普及期の課題となります。

接続方法は、携帯網を利用した接続の場合には、一般的には Host 型の接続となります。

端末～携帯網間の接続方法には、トンネル接続とネイティブ接続があります。

セグメントの特徴

機器

機器としては、以下のものを利用します。

端末	PC+携帯接続用カード
ネットワーク	PPP 終端機器
	IPv4 ルータ
	認証システム

接続モデル

接続モデルとしては、PTA モデルと LAA モデルが考えられます。

・PTA(PPP Terminated Aggregation)モデル

端末～携帯網間は PPP(IPCP NCP)接続、携帯網内 PPP 終端装置で PPP を終端

携帯網～ISP 間は IPv4 接続

·LAA(L2TP Acces Aggregation)モデル

端末～携帯網間は PPP(IPCP NCP)接続、携帯網で PPP パケットを L2TP でカプセル化

携帯網～ISP 間は IPv4 接続、L2TP でカプセル化された PPP パケットを ISP に渡す。ISP 内 PPP 終端装置で PPP 終端

アドレッシング

アドレッシングは、PPP で IPv4 アドレス一個を払い出します。固定、可変の両方がありえます。

アドレスプール

アドレスは、ISP から RADIUS 等で払い出しします。ISP からアドレスプールを固定に割り当てし、携帯網認証設備から払い出します。

認証

一般的な PPP 認証を行います。固定アドレス払い出しの場合には、これでユーザ特定も兼ねます。

ルーティング

端末～携帯網間は、静的デフォルトルーティングを使います。

携帯網内は、一般的には動的ルーティングです。

携帯網～ISP 間は、静的か動的ルーティングです。

セキュリティ

携帯接続カード等で IP パケットフィルタリングを行います。ファイル共有パケットのフィルタリン

グなどを TCP/UDP のポート番号などでチェックします。レイヤを超えたチェック機能も考えられます。端末における IP パケットフィルタリングが可能です。

トンネル接続

機器

ネットワーク機器は、IPv4 接続に必要な機器と、IPv6 トンネル終端ルータです。

接続モデル

IPv4 接続については PPP 接続（現状と同様）です。

IPv6 接続については、トンネルの終端位置で、携帯網トンネル終端モデル、ISP トンネル終端モデルの 2 つのモデルが存在します。

・携帯網トンネル終端モデル

携帯網（の一部）で IPv6 を扱うことが可能である必要があります。

端末～携帯網間は、端末で IPv6 トンネルを行います。携帯網でトンネル終端ルータを用意し、トンネルを終端します。トンネル手法は、IPv4 固定アドレスを利用する場合、Configured Tunnel、IPv4 可変アドレスを利用する場合、ISP Provisioned Tunnel、もしくは Automatic Tunnel となります。

携帯網～ISP 間は、デュアルスタック接続（IPv6/IPv4 同一リンク）、IPv6 ネイティブ接続（IPv6/IPv4 別リンク）、トンネル接続が考えられます。

・ISP トンネル終端モデル

これは、携帯網で IPv6 が扱えない場合です。

端末～携帯網間は端末で IPv6 トンネルを行います。IPv4 固定アドレスを利用する場合、Configured Tunnel、IPv4 可変アドレスを利用する場合、ISP Provisioned Tunnel、もしくは Automatic Tunnel となります。

携帯網～ISP 間は通常の IPv4 接続で、ISP でトンネル終端ルータを用意し、トンネルを終端します。

アドレッシング

IPv4 については、PPP で IPv4 アドレス一個を払い出します（IPCP NCP）。

IPv6 の場合のアドレス配布は、トンネル仕様に依存します。

6to4	/48
ISATAP、Teredo	/64+IPv4 アドレス
その他	任意

IPv6 の場合、余計なシグナリングを抑えることが重要となります（無線区間の有効利用のため）。

認証

認証は、IPv4 では通常の PPP 認証を行います。

IPv6 の場合、ISP Provisioned Tunnel では認証を行いますが、その他のトンネルでは通常認証は行いません。

ルーティング

端末～携帯網間はトンネル仕様に依存します。通常は携帯網に向けて静的デフォルトルーティングとなります。携帯網～ISP 間は、IPv6 も IPv4 と同様です。動的ルーティングは IPv6 に対応している必要があります。

セキュリティ

セキュリティについては、端末で IP パケットフィルタリングを行います。

ネイティブ接続

機器

ネットワークについては、機器としては同一形態です。

接続モデル

IPv4 接続については、現状と同様、PPP 接続です。

IPv6 接続についても、IPv4 は同じ方式(PPP)で接続します。

3GPP 仕様では、インタフェース ID は携帯網側から通知されたものを利用し、網側で制御することによりインタフェース ID の重複を避けます。これによって ID がリンクで一意であることが保証されるので、DAD が行われません（正確には DAD が無視されます）。

・PTA(PPP Terminated Aggregation)モデル

端末～携帯網間は PPP(IPV6CP NCP)接続です。

携帯網では、PPP 終端装置で PPP を終端します。

携帯網～ISP 間は、デュアルスタック接続（IPv6/IPv4 同一リンク）、IPv6 ネイティブ接続(IPv6/IPv4 別リンク)、トンネル接続があります。

・LAA(L2TP Acces Aggregation)モデル

端末～携帯網間は PPP(IPV6CP NCP)接続です。

携帯網では、PPP パケットを L2TP でカプセル化します。

携帯網～ISP 間は IPv4 接続で、L2TP でカプセル化された PPP パケットを ISP に渡し、ISP 内 PPP 終端装置で PPP を終端します。

アドレッシング

IPv4 については、PPP で IPv4 アドレス一個を払い出します(IPCP NCP)。

IPv6 については、RA で/64 Prefix を通知します。この場合、Unsolicited RA の送出タイミングが問題となります。大量に流さないように制限する必要があり、送出間隔、Prefix 生存期間の最適化が問題となります。

3GPP 仕様については、現状ではマルチプレフィックスには未対応という問題があります。1 リンクに 1 アドレス利用の制限が加わっています。

匿名アドレス（Privacy Extension）の利用を推奨しますが、アドレスの頻繁な変更は推奨しません。これは、SIP シグナリングの利用などにおける問題を回避するためです。

DHCPv6 も利用可能です。通常の利用方法でよく、網側で DHCP Proxy/Relay などを利用し、適切にハンドリングすることが求められます。

アドレスプールについては、ISP の RADIUS 等の情報より、携帯網から RA で静的(もしくは動的)に払い出します。携帯網側でアドレスプールを固定に割り当て、RA で動的に払い出しも可能です。

認証

認証については、一般的な PPP 認証を行います。固定アドレス払い出しの場合には、ユーザ特定も兼ねます。IPv4 と同一の仕組みで、PPP LCP 認証を行います。

ルーティング

ルーティングに関しては、IPv6 も IPv4 と同様です。動的ルーティングは IPv6 に対応している必要があります。

端末～携帯網間はデフォルトルータへの静的ルーティングです。

携帯網～ISP 間では、動的ルーティングを利用することが一般的です。

セキュリティ

携帯接続カード等で IP パケットフィルタリングを行います。IPv6/IPv4 とも同一の仕組みであることが望まれます。また、端末で IP パケットフィルタリングを行います。

IPv6 普及期の想定形態と課題

課題は、携帯端末の IPv6 対応です。携帯端末ネットワークスタックの PPP における IPv6 対応(IPV6CP NCP)が問題となります。3GPP の場合には、PPP スタックに若干の対応が必要です。

トンネルアクセス

推奨移行方法

概要

法人向けトンネルアクセスは、Configured Tunnel を利用します。これは、既に一般的に用いられている手法です。

個人向けトンネルアクセスは、ISP Provisioned Tunnel(TSP、DTCP 等)を利用することを推奨します。この場合、CPE がトンネルを終端します。ユーザ接続管理が可能、アドレッシングなどの制御が可能、といった特徴があります。

顧客接続方式は、両者とも Site 型が一般的です。個人向けトンネルアクセスの場合には、端末が直接トンネルを終端する場合(Host 型)もあります。

セグメントの特徴

一般的な IPv4 接続全般が対象となります。

グローバル IPv4 アドレス接続(IPv4 アドレス固定、IPv4 アドレス可変) 、プライベート IPv4 アドレス接続(家庭内、企業内)がすべて含まれます。

Best Current Practice

このセクションでは、トンネルの実現方法(Configured Tunnel、ISP Provisioned Tunnel、Automatic Tunnel)により分類して検討します。

各実現方法の概要は以下の通りです。

・Configured Tunnel

主に Site 型接続で利用されます。IPv4 トンネル終端が固定アドレスの場合有効です。(固定アドレス利用の)法人ユーザ向けサービスとして一般的に利用されています。ISP 側でのユーザプロビジョニングが可能という特徴があります。

・ISP Provisioned Tunnel

この場合は、Site 型、Host 型接続とも可能です。TSP や DTCP などのプロトコルを利用します。個人ユーザ、法人ユーザの双方を対象とすることができます。ユーザ認証によるトンネルセットアップが行え、ISP 側でのユーザプロビジョニングが可能です。

・Automatic Tunnel

これは主に Host 型接続で利用されます。6to4、ISATAP、Teredo などのプロトコルが利用できます。一般的には個人ユーザ向けで、通常は認証機構がありません。ISP 内部で全ユーザー律に提供する場合などには有効ですが、誰が IPv6 を利用しているかを知る手段や、IPv6 を利用したくないユーザに対するケアに関する課題があります。

Configured Tunnel

・ネットワーク機器対応

ユーザ側では、Configured Tunnel 終端ルータが必要です。IPv6 対応ホストでのトンネル終端も不可能ではないですが、一般的ではありません。

ISP 側ではトンネル終端ルータが必要です。IPv6/IPv4 ネットワークに同時に接続している必要があります。

・アドレッシング

アドレスは事前設定であり、固定的に Prefix をアサイン(一接続毎に/48 が一般的)します。

・ルーティング

ユーザ側では、静的(トンネルインタフェースへのデフォルト設定)、外部ルーティング(BGP4+)などを用います。

ISP 側は、ユーザに対しては、静的、外部ルーティングなどを用い、経路集約ができるようなアドレスを割り振ります。上流(コア)接続は、静的/IGP/iBGP などを用います。

ISP Provisioned Tunnel

・ネットワーク機器対応

ユーザ側では、Site 型の場合、ルータでトンネルを終端し、Host 型の場合は端末でトンネルを終端します。

ISP 側では、トンネル終端システムを運用します。この場合、IPv6/IPv4 ネットワークに同時に接続している必要があります。トンネル終端サーバ、認証機能サーバなど、機能的に分けることが多く見られます。

・アドレッシング

ユーザアカウント毎に固定 Prefix を提供します。

Host 型の場合、/128 Prefix を配布、もしくは/64 などを配布し、端末側で Prefix 内の任意のアドレスを利用します。ユーザ認証により、ユーザ情報と Prefix 情報を紐付けることが可能です。

・ルーティング

ユーザ側は、静的(トンネルインタフェースへのデフォルト設定)です。外部ルーティング(BGP4+)は一般的ではありません。

ISP 側は、ユーザに対しては、静的ルーティングで、経路集約ができるようなアドレス割り振りを行います。上流(コア)接続は、静的/IGP/iBGP などを用います。

Automatic Tunnel

・ネットワーク機器対応

ユーザ側では、各トンネル終端ホストの対応のみが求められます。ただし、6to4 の場合にはルータも利用可能です。

ISP 側では、トンネル終端ルータ/システムを運用します。この場合、IPv6/IPv4 ネットワークに同時に接続している必要があります。

・アドレッシング

IPv4 アドレスから IPv6 アドレスを生成するため、IPv4 アドレスに依存します。IPv4 アドレスが固定なら、IPv6 アドレスも固定されます。IPv4 アドレスが固定ならば、Configured Tunnel を用いることが普通です。

・ルーティング

ユーザ側は静的(トンネルインタフェースへのデフォルト設定)です。外部ルーティングは一般的ではありません。

ISP 側は、ユーザに対しては、静的ルーティングを行います。経路集約ができるようなアドレスを割り振ります。上流(コア)接続は、静的/IGP/iBGP などを用います。

・その他

接続ユーザの制限を行う場合、トンネル端点の ACL 設定を行います。

プライベートネットワークでのトンネル接続

・サイト間接続

これは、主に企業で行われます。通常、Configured Tunnel 接続で、両端が IPv4 固定アドレスです。

VPN 接続としては、IPsec-VPN、IPv6 対応 IP-VPN サービス(MPLS 6PE など)、広域

Ethernet サービスが考えられます。

・サイト内部ホスト接続

これは企業、家庭とも利用されます。ISATAP と Teredo が代表的です。

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)では、外部ネットワーク境界に ISATAP ルータを設置します。

Teredo では、IPv6 パケットを UDP over IPv4 パケットでカプセル化し、NAT の内側からトンネルします。

・リモートアクセス(サイト外部から特定サイトへの接続)

現在は主に企業で行われていますが、将来的には家庭も考えられます。IPsec-VPN、SSL-VPN が代表的です。いずれも、IPv6 トランスポート対応の必要があり、IPv6 固有の問題の解決が必要です。

・その他

その他、L2TP などの利用が考えられます。

IPv6 アドレス固定/可変

上記のトンネル手法を IPv6 アドレスが固定か可変かによって分類すると、次のようになります。

固定

Configured Tunnel

ISP Provisioned Tunnel(ISP のポリシーに依存)

可変

ISP Provisioned Tunnel(ISP のポリシーに依存)

Automatic Tunnel(IPv4 アドレスの固定/ 可変に依存)

IPv6 普及期の想定形態と課題

ここでは、トンネルを利用していたネットワークのネイティブ/デュアルスタックネットワークへの移行について補足します。

移行の動機は、IPv6 トラフィック増加に伴うトンネル処理のオーバーヘッドを避けることにあります。

Tips として、IPv4 Protocol No.41 パケット(IPv6 カプセル化パケット)の扱いに関し、説明します。

トンネルサービスを行う場合には、ISP ネットワーク内ではこのパケットをフィルタリングしません。サービスを行わない場合でも、6to4 などの利用を妨げるので、可能な限りフィルタリングを行わないことを推奨します。

ただし、フィルタリングをしないことから、セキュリティ的な考慮が必要となります。トンネルによる内部ネットワークへの攻撃の可能性や、トンネルルータへの DoS 攻撃の可能性があります。これらについては、セキュリティ SWG (I1)/(I2)を参照してください。

サーバ運用管理

これについては、データセンターSWG を参照してください。

3. IPv6 普及期の想定形態と課題

IPv6 普及期の想定形態と課題

IPv6 普及期には、次のような状況と課題が考えられます。

1.機器のデュアル比率の増加

デュアルシステムとしての安定動作と、アプリケーションの IPv6 から IPv4 へのフォールバック動作が問題なく動作すること（WIDE IPv6Fix Project で検討中）が必要となります。

また、現在 IPv4 でできて IPv6 でできていないことへの対策、つまり、DNS 自動検出方法、SNMP の IPv6トランスポート対応、ウィルスソフトの IPv6 対応、Stateful な AutoConfiguration（DHCPv6）、エンドサイトのマルチホーム接続、PI アドレスによるマルチホーム接続、ICMPv6 のフィルタリングが課題になります。

2.IPv6 トラフィックの増加

ルータ、スイッチ、IDS、ファイアウォール、負荷分散装置の処理パフォーマンスの向上が求められます。

3.IPv6 オンリー機器の出現

IPv6 しか話さない機器が登場した場合には、IPv4 オンリー機器との通信の有無と、通信する場合の手法について確認する必要があります。また後述しますが、IP 電話の IPv6 移行も考えられます。トランスレータが必要となる場合、その種類と設置場所を考える必要があります。

4.nonPC 機器のインターネット利用

Zero-conf の内容整理と実現手段を考えるとともに、簡便なセキュリティ確保手段を生み出さなくてはなりません。

5.外から中へのアクセス

外から中へのアクセスでは、動的な穴あけプロトコルの標準化が望まれます。また、IPsec の相互接続性向上と、ISP によるセキュリティマネジメント手法の確立（後述）も求められている一つです。さらに、遠隔からのメンテナンスや計測に必要な、狭帯域ですが重要な制御系トラフィックの保護手法を見出す必要があります。

6.P2P トラフィックの増加

P2P トラフィックの増大に伴い、トラフィックコントロール手法（ファイル交換と IP 電話の区別など）が要求されるようになっていきます。

7.放送と通信の融合

家庭までのマルチキャストのデフォルト化に向けた段階的なプランを考える必要があります。また、ベストエフォートサービスとの品質差別化手法（QoS、ポリシールーティング（後述）等）も確立する必要が出てくるでしょう。

8.モバイル機器との IP 通信

特に、リンク変更時のシームレスな Mobile IPv6 の動作が求められます。

9.その他

名前解決技術（DNS、UPnP、SIP 等）とそれらの使い（分け）方や、Privacy Extension の使い方、運用過程で出てくる問題への ISP 間コンセンサスの形成（パンチングホールの基準確立やプロバイダエッジでの Ingres フィルタの推奨など）が課題となります。さらに、各セグメント（Home、Unmanaged、Managed）が想定する形態へ ISP としての対応が求められます。

IPv6 普及時の技術的課題

以下では、IPv6 普及期の技術的課題として、IP 電話の IPv6 移行の課題、MultiPrefix 実現への課題、IPv6 Multicast 対応の課題、IPv6 上での QoS 実現の課題を取り上げます。

IP 電話の IPv6 移行の課題

電話の IPv6 移行に関する ISP にとっての課題には、ISP の提供している IP 電話サービスの移行と、企業 IP Centrex との相互接続の 2 つがあります。

具体的には、まず IP 電話サービスの移行の過程でデュアル電話機は存在しうるかどうかにより、課題となる点が異なってきます。

もしデュアル電話機が出たときには SIP サーバ、クライアント間のプロトコル選択のメカニズムとフォールバックを含めたオペレーションの信頼性は十分かという問題があります。

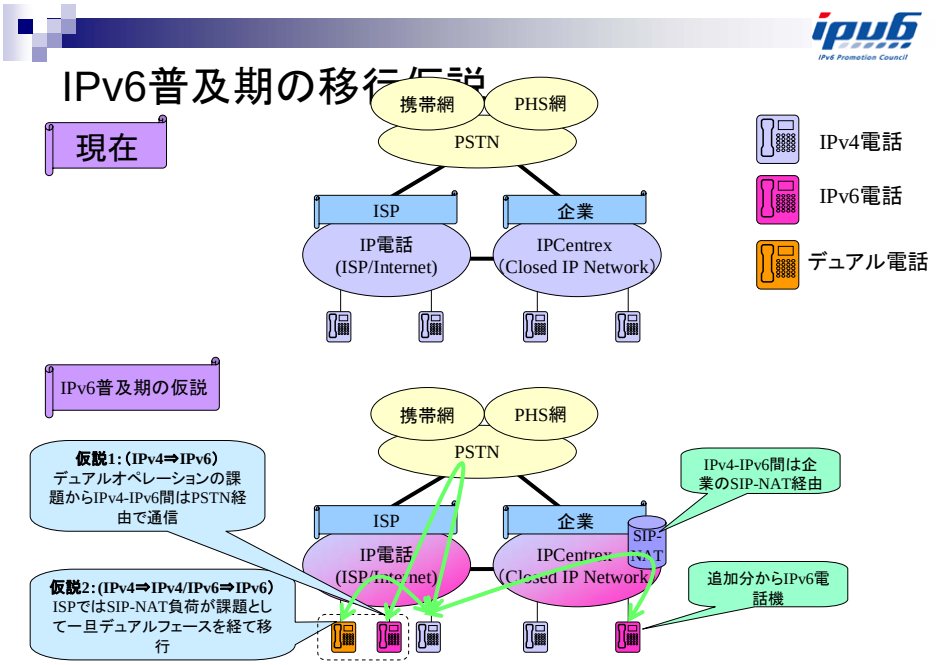
また、IPv6 オンリーの電話機が出たときには、IPv4 機器との接続方法をどうするかという問題があり、特に SIP-NAT などのトランスレータが負荷に十分耐えられるかという点が課題になりま

す。

現状では、中小 ISP の多くが大手 ISP の IP 電話サービスを購入（SIP サーバをアウトソース）しており、中小 ISP が IP 電話の IPv6 移行を意識するケースは少ないと考えられます。

しかし、ISP の IP 電話サービスの品質保持について、アクセス網での QoS 確保が求められるかもしれません。

IPv6 普及期の移行仮説



対象

ここで検討の対象とするのは、IP 電話のプロトコルスタックの IPv6 への移行と SIP の利用、そして IP 電話以外の用途での SIP の応用、特に機器の名前解決プロトコルとしての利用です。

現状

ここでは、SIP プロトコルの採用されたシステムを対象とします。H. 323/MEGACO なども利用されていますが、ここでは検討対象外とします。

適用領域としては、企業向け、公衆(一般家庭)向けの 2 つが考えられます。

企業向け IP 電話は、主に内線電話の置き換えを目的としています。一部 IPv6 の採用が進んでいます。IP 電話専用端末が、SIP 端末としての機能を果たし、SIP サーバは、企業毎個別か ISP などへのアウトソースとなっています。通常、他の IP 電話システムとの相互接続は考えず、外部へは PSTN 経由で接続されます。

公衆(一般家庭)向け IP 電話は、家庭の電話の置き換えです。SIP 端末としては、CPE に SIP クライアントを実装し、この CPE を VoIP ターミナルとしても利用します。これによって、IPv4 グローバルアドレス問題の回避を狙っています。

SIP サーバについては、ISP 間の SIP 相互接続が問題となります。SIP 方言の問題があるためです。SIP サーバ間のインタフェースで吸収できるかどうかが課題です。未提携 ISP、一般 PSTN 電話端末とは PSTN 経由での通信で回避します。

IPv6 への移行

IPv4 から IPv6 への移行では、デュアルスタック期間があるかないかが 1 つの分かれ目となります。

IPv4 → IPv4/IPv6 → IPv6

IPv4 → IPv6

このどちらの移行形態になるかによりますが、後者の場合、プロトコル間の差異はシステムで吸収することも可能かもしれません。しかし、いずれにしろ、UUI 相互接続(SIP 端末同士の通信、RTP など)の確認は必須です。IPv6⇔IPv4 プロトコル間通信は無理である可能性も考えられます。

IPv6⇔IPv4 相互接続については、サーバ間はシステムで吸収できる可能性はあります。しかし、上記 UUI の相互接続は問題です。デュアルスタックは厳しいかもしれません。

(ISP システム間)相互接続の問題に関して、SIP 方言は SIP サーバで吸収できる可能性もあります。また、相互接続の推進に関し、各種の活動が推進されています。IPv6 に関するものとしては、総務省の移行実証実験、IPv6 CertWG / TAHI 等があります。それでも、相互接続の問題は、IPv6 時代にも引きずると思われます。IPv6 移行に際しての特有の問題点があるかどうかは確認しなければなりません。

必要な実装としては、端末、CPE、ルータ、その他 SIP サーバなどのシステムがあります。

MultiPrefix 実現への課題（Source Address Selection）

IPv6 上での MultiPrefix

MultiPrefix へのモチベーション

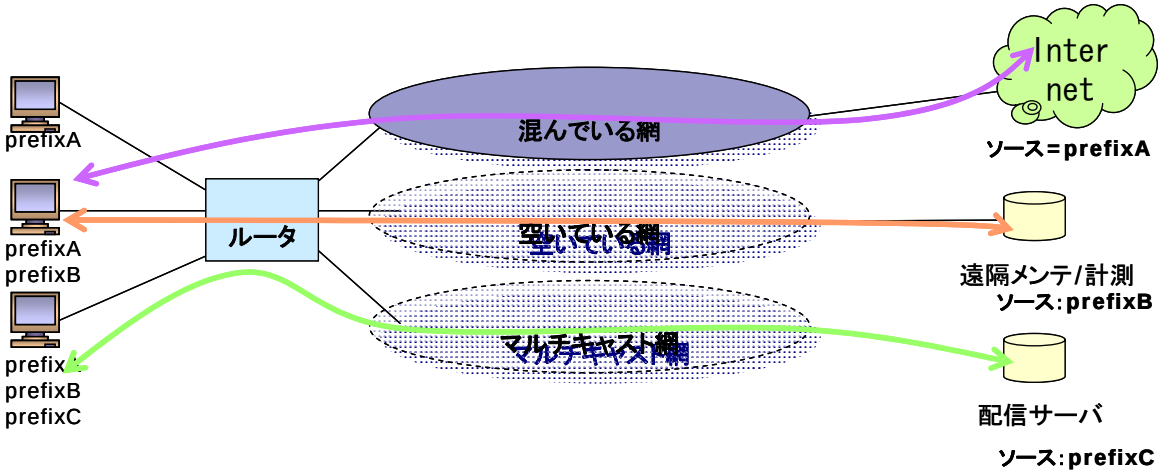
MultiPrefix のニーズとしては、おもに QoS 実現（Prefix による QoS 区別など。QoS の項目も参照）、サービス重畳（IPv6 グローバル接続サービスと ISP IPv6 プライベートネットワーク接続サービスとの共存など）、サイトマルチホームが考えられます。

関連する技術

関連技術としては、IPv6 アドレッシング（IPv6 は1つのインタフェースで複数 IPv6 アドレスの扱いを前提としている）、ルーティングセレクション（ポリシールーティングなど）、ソースアドレスセレクション（RFC3484 など）があります。MultiPrefix はこれらの技術によるところが大きくあります。

ポリシールーティング

IPv6 の特徴である MultiPrefix 環境下において、通信元端末が、宛先アドレスに対して longest-match なソースアドレス選択し通信を行うことを利用し、経由する IP 面を分ける手法が考えられます。



MultiPrefix 実現のための端末サポート

MultiPrefix に関しては、端末でサポートしているかどうかで 2 つのケースが考えられます。

・端末側でサポートしている場合

高機能端末（一般的な PC 端末）等ではサポートする可能性があります。OS レベルでのサポートが考えられます。

・端末側でサポートできない場合

複数アドレスをつけること自体はそれほど問題ではありませんが、 アドレスセレクション、ルーティングセレクションが適切にできない可能性が高い端末として、情報家電機器などが考えられます。

端末側でサポートしている場合

・端末側でサポートすべき項目

高機能端末(一般的な PC)の場合、複数アドレスがつけられることと、アドレスセレクションの機能をサポートすべきです。

・CPE でサポートすべき項目

CPE は、アカウントサーバからの情報を受けることができ、適切なアドレス配布、適切なルーティング、フィルタリングを実現すべきです。ここでは、MAC 情報の吸い上げ、登録はどうするかという課題があります。

・ネットワークでサポートすべき項目

ネットワークでは、アカウントサーバを運用し、適切なルーティング、フィルタリングを実施しなければなりません。

・端末上アプリのソースアドレスセレクション

これは、一度誤ったアドレスを選択しても、コネクション確立に失敗して最終的に正しいアドレスが選択できるようにする機能です。Getaddrinfo() を使ってコネクションをリトライするアプリケーションであればよいでしょう。ただし、コネクション確立に失敗したことをアプリケーションに伝える仕組みが必要です。ネットワークで ICMPv6 Error を弾いてしまうと、確立失敗の認識に時間が掛かってしまいます。

端末側でサポートできない場合

・端末側でサポートすべき項目

端末側で、MultiPrefix をサポートできない場合（情報家電機器など）でも、通常のアドレス設定、ルーティングのサポートは必要です。

・CPE でサポートすべき項目

アカウントサーバからの情報は DHCP 経由で受け取ります。受け取る情報は、MAC アドレスと対応する Prefix などです。

タイミングとしては、事前、RS 受信時が考えられますが、Unsolicited RA はどうするかという課題があります。

適切なアドレス配布は、MAC アドレスベースで行います。ただし、ND の扱いが複雑です。適切なルーティングについては、ソースアドレスによるルーティングセレクションが可能です。フィルタリングでは、適切でないアドレスからのパケット処理を行います。

この一連の手順では、MAC 情報の吸い上げ、登録はどうするかという課題があります。

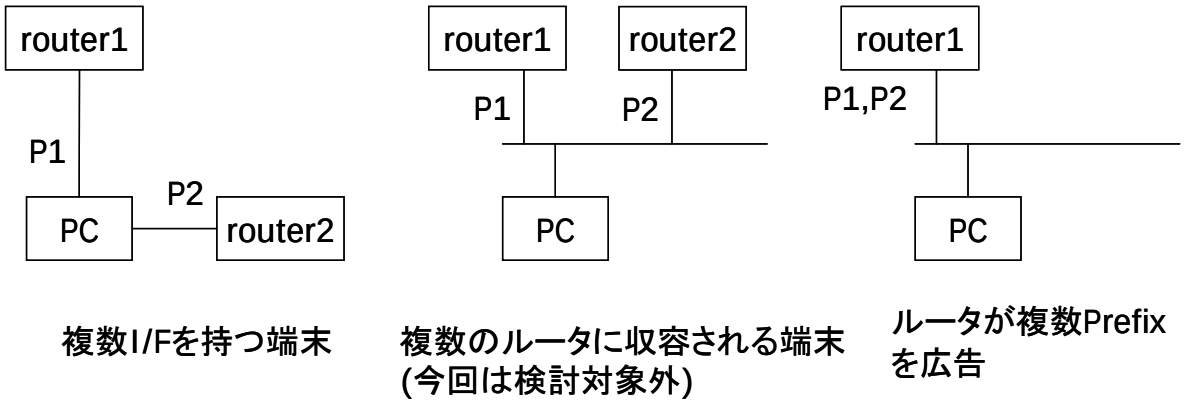
・ネットワークでサポートすべき項目

アカウントサーバは DHCPv6 ベースで運営します。適切なルーティングについては、場合によってはソースルーティングを行います。フィルタリングは、ルータ/サーバなどでケアします。

Multi-Prefix 環境における Source Address Selection

端末が複数 Prefix を持つ条件

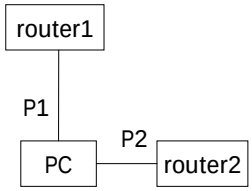
これには、実質的に、複数インタフェースを持つ端末が機能する場合、ルータが複数 Prefix を広告する場合の 2 パターンがあります。ここでは、「複数のルータに収容される端末」は「ルータが複数 Prefix を広告する場合」に包含します。



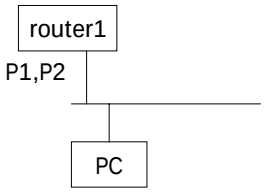
Source Address Selection に失敗する条件

Source Address Selectionに失敗する条件

- Nexthop Selectionには成功していると仮定



いつも成功
(RFC3484 Rule.5
“Prefer outgoing interface)

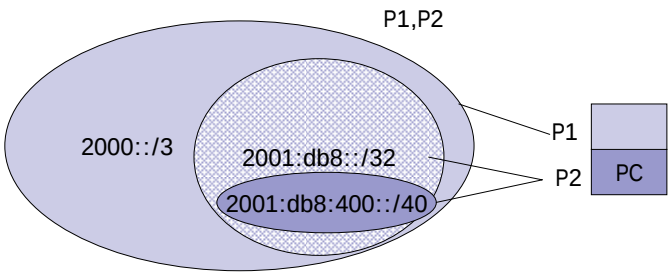


大体RFC3484 Rule 8で成功
(“Using the longest matching prefix”)
しかしうまくいかないときはRule 6が必要
(“Prefer Same label”)

Source Address Selection に失敗する例

Source Address Selectionに失敗する例

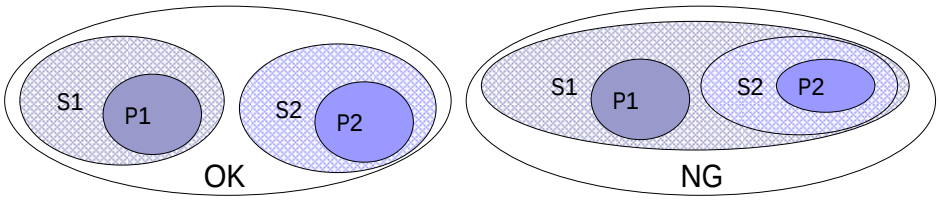
- e.g.)
  - P1=2001:db8:420:1::/64
  - P2=2001:0:165:10::/64
  - インターネット(2000::/3)通信時はP2を，イントラネット(2001:db8:400::/40)通信時にはP1を使用
  - 2001:db8::1に通信するとき、イントラネットプレフィックスP1が用いられる



どうすれば Source Address Selection に失敗しないで済むか

どうすればSource Address Selectionに失敗しないで済むか

- 前提
  - P1を使って通信すべき通信先∀x1∈S1
  - P2を使って通信すべき通信先∀x2∈S2
  - P1⊆S1, P2⊆S2
- 条件
  - S1∩S2＝φ⇔RFC3484 Rule 8(Longest Match Prefix)でうまくいく
  - これが保障できないときは、RFC3484 Rule 6(Prefer Same Label)が必要



IPv6 Multicast 対応の課題

Multicast の扱い

基本的な考え方は IPv4 と同様です。端末からの Multicast グループ参加/脱退をシグナリングするのが Multicast です。IPv4 では IGMP、IPv6 では ICMPv6、MLD を用います。

マルチキャストルーティングのプロトコルは変わりません（PIM-SM/SSM/DM など）。

IPv6 Multicast

IPv6 Multicast では、グローバル性を活かして、エンド端末までのマルチキャスト配信が簡便に実現可能です（PIM-SSM の利用）。Multicast の NAT 越えなど、このメリットをどう活かすかが課題です。

Dualstack Multicast

デュアルスタックの場合、マルチキャストルーティングは、IPv4/IPv6 で別テーブルが構築可能

でなければなりません。

特に PIM など Unicast ルーティングテーブルの RPF(Reverse Path Forwarding) に依存するプロトコルの場合は、IPv4/IPv6 Unicast ルーティングトポロジーが同一であるとは限らないため、両者の Multicast ルーティングテーブルも別トポロジーになります。

Multicast グループでは、グループ空間の違い、スコープの違いがありますが、これらが何かに影響するかどうかを確認する必要があります。

IPv6⇔IPv4 相互接続性

IPv6 と IPv4 では、まずアドレスの違いがあります。ここでアドレス相互変換 → Multicast Translation を行うのかどうかという問題があります。

また、ルーティングにおける相互接続については、その必要性をまず確認する必要があります。

グループ空間の違いについては、グループ相互変換をするのかどうかという問題があります。

機器に対するマルチキャスト機能実装

端末

端末では、MLD を利用します。PC では実装しているものが多く見られます。

CPE

CPE はスタティックマルチキャストルーティングを実行します。個人向けサービスユーザ内環境にダイナミックルーティングを行わせることは現実的ではない可能性があります。

MLD and/or MLD Proxy については、MLD Proxy+ISP 側で MLD を扱えることが求められるかもしれません。

ルータ

マルチキャストルーティング、MLD への対応が求められますが、実装は多く存在しています(PIM-SM)。

L2 スイッチ

MLD Snooping 機能が求められます。

IPv6 上での QoS 実現の課題

本文書での QoS の範囲

ここで検討する QoS は、同一ネットワーク上でのトラフィック差別化機構です。同一ネットワークでの差別化には、インタフェースのキューイング、Diffserv が利用できます。

しかし、ここでは、別面を構築することによる差別化を行います。MultiPrefix による別面運用で、物理面を分けます。そして、Prefix により扱いを分け、ポリシールーティングなどを利用します。

応用例としては、ストリーム系トラフィックの優先制御、たとえば IP 電話や画像ストリーミング等があります。

QoS の扱い

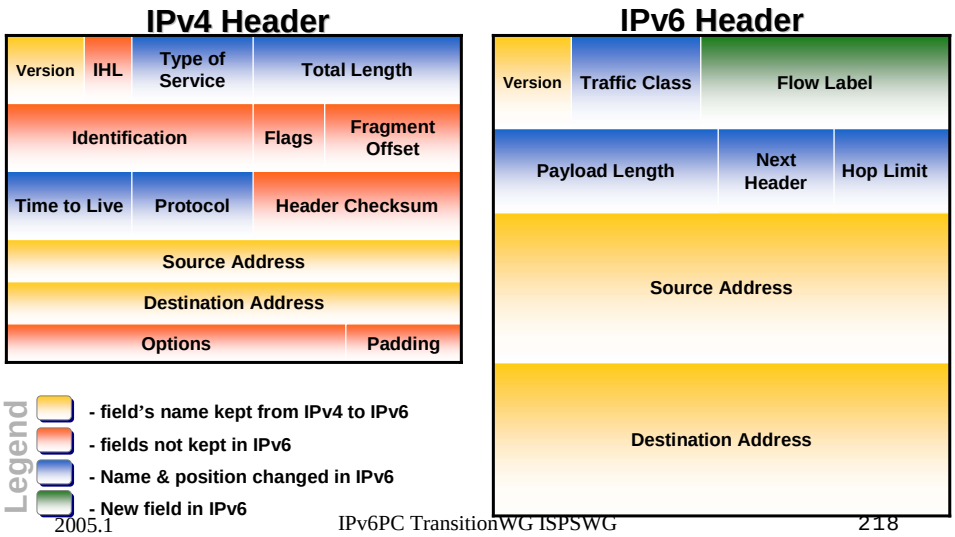
下に、IPv4 Header と IPv6 Header の比較図を掲載します。

IPv6 Traffic Class フィールドの扱いは IPv4 ToS フィールドと同様です。IPv4 との違いは“FlowLabel”にあります。したがって、IPv6 の独自性を出すためには、FlowLabel に対する応用の実現が必要です。

Layer2 QoS とのマッピングについては、IPv4 と同様、MPLS 等との関連付けが考えられます。

IPv6⇔IPv4 QoS の相互互換については、必要か、いつの時点で必要になるかを検討する必要があります。

参考:IPv4ヘッダとIPv6基本ヘッダ比較



機器に対して期待される QoS 機能

CPE

CPE では、Traffic Class フィールドの扱い、Queuing の機能が求められます。

ルータ

ルータでは、Traffic Class フィールドの扱い、Queuing

その他

QoS ポリシー制御システム等

4. Tips

アドレス関連

ルータ、サーバのアドレスはマニュアル設定すべきです。EUI-64 は、NIC が変わるとアドレスも変わりますので、DNS 登録、フィルタリング設定の手間を軽減する意味から固定すべきです。

便利なネーミングルール例には、以下のようなものがあります。

・ ::1 、::53 、::80 、::cafe

・ :c726:a00:3:82 これを東京 03 - 広島 082 間の ATM リンク に割り当てる

ただし、これらのアドレスは攻撃対象になりやすいことも考慮したほうがよいと思われます。

リナンバリング方法

実行しやすい手動リナンバリングの方法を解説します。これは、同一インタフェースに複数の IPv6 アドレスが付与可能であることを利用したものです。

手順は以下の通りです。

1. 新アドレス取得
2. 新アドレス接続性(ルーティング)設定
3. IPv6 ノード(ルータ及び端末)へ新アドレス付与
   - 旧アドレスも削除せずに付与しておく
   - 端末レベルでは AddressAutoConfiguration により自動設定
4. あわせて、DNS 登録変更作業等を行う
5. 旧アドレスを削除
6. 旧アドレス接続性(ルーティング)削除

IPv6 では、こうした方法でリナンバリングを実施すると、IPv4 のリナンバと比べ、サービス断の影響が少なく段階的なリナンバが可能です。

この手順については、以下のドラフトに示されています。

Procedures for Renumbering an IPv6 Network without a Flag Day
(Draft-ietf-v6ops-renumbering-procedure-01.txt)

sTLA 割り当ての歴史的経緯

最初(1999)は、初期割り当てが/35 となっていました。

改定後(2002 . 7 . 1)は初期割り当てが/32 となりました。ただし、既存/35 取得の sTLA 保持者の/32 へのアップグレードは任意であるため、新ポリシー後も/35 を保持する sTLA が存在します。 現在は、/32 、/35 の sTLA が共存している状況です。

Appendix

中小 ISP の IPv6 移行ケーススタディ

目的、前提とする ISP の形態

ここでは、ガイドラインの記述を元に、中小 ISP に対する典型的な IPv6 導入モデルについて記述します。目的は、運用経験の蓄積とサービス対応への布石です。

前提とする中小 ISP の形態は、以下の通りです。

ネットワーク

IPv4 ネットワークを構築し、 ISP サービスを行っている。

アドレス

アドレス指定事業者として、JPNIC より IPv4 アドレス割り振りを受けている。

ルーティング

(JPNIC 等から)AS 番号を取得しており、BGP で IPv4 の外部接続を行っている。内部ルーティングは OSPFv2 を利用している。内部 BGP(iBGP)は Confederation、RR などは利用していない。

本項の前提は、IPv4 の接続性確保は今までの手法をそのまま利用することです。そして IPv6 に特化した部分のみを本項で記述します。

IPv6 ネットワーク導入方針

アドレス

IPv6 で独自にアドレスを取得します（/32 Prefix 空間)。管理用に IPv4 のアドレス、接続性は確保しますが、ユーザの IPv4 トラフィックは扱いません。IPv6 試験サービスとして、顧客に対して /48 Prefix を提供することを想定します。

ネットワーク

既存ネットワークとは独立に IPv6 別ネットワークを構築します。基本的な構成の考え方は IPv6/IPv4 同一です。バックボーン、外部接続、アクセス接続、サーバセグメントで、将来のデュアルスタックネットワークへの移行を行いやすくすることを心がけます。

バックボーンは、場合によってはトンネルを利用することもありえます。IPv6 試験サービスとして、顧客に対してトンネル接続を提供することを想定しています。

ルーティング

既存ネットワークと可能な限り整合性を取ります。ここでは、将来の IPv6/IPv4 ネットワーク統合を見据えて検討します。IPv6/IPv4 ルーティングプロトコルの整合性、IPv6/IPv4 ルーティングトポロジーの整合性をとります。IPv6 試験サービスとして、顧客に対して静的ルーティングを設定することを想定します。

参考：上位 ISP からアドレスを取得する場合

アドレスを独自に取得する場合との差分を示します。

ネットワーク

外部接続は、通常上流 ISP のみとなります。上流を 2 本以上接続することは困難です。冗長性確保などのため、上流 ISP と複数本接続することはあり得ます。

アドレス

IPv6 アドレス空間は上位 ISP より取得します。この場合、アドレス空間は APNIC より取得する場合(最低/32)より小さくなります。取得可能なアドレス空間の大きさは上位 ISP のポリシーによって異なります。

ルーティング

通常は上流 ISP をデフォルトネットワークとしたスタティック接続です。冗長性確保、もしくは他 ISP との Peering のために、動的ルーティング(BGP4+等)での接続もあり得ます。

Peer を行う場合には、自分の経路を Peer 先から外部ネットワークに広報してはなりません(IPv6 Prefix パンチングホールを避けるため)。プライベート AS を利用する場合には、Peering 先と利用する AS 番号についての調整などが必要です。(通常はこの形態は推奨しません)。

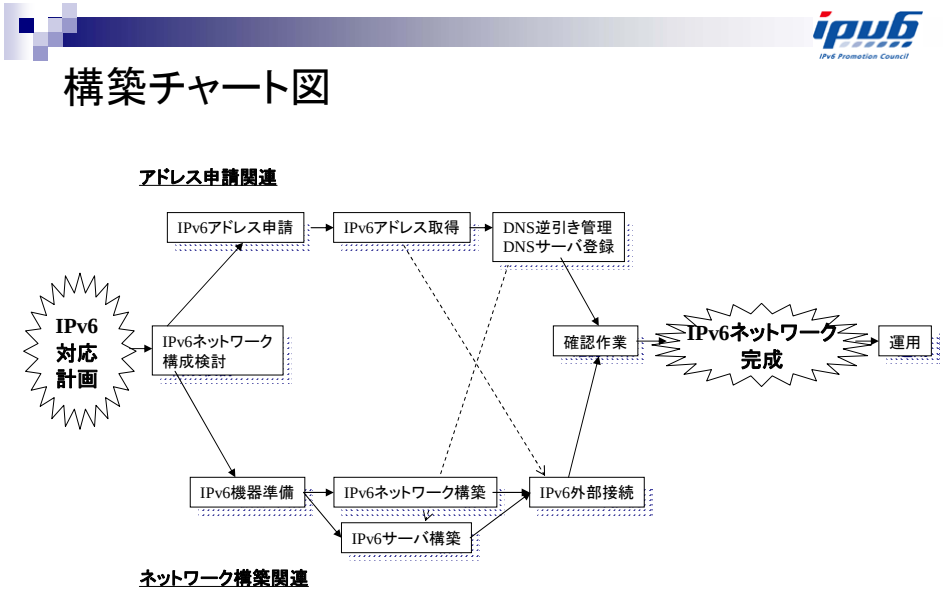
導入手順

以下では、次の点で、導入手順を解説します。

1. ネットワーク構成検討（物理構成、論理構成）
2. アドレス取得
3. 機器準備
4. ネットワーク構築
5. 運用

   アドレス取得に伴う義務（アドレス割り振りに伴う RIR データベース登録、取得アドレスの DNS 逆引き設定の管理）

構築チャート図



1. ネットワーク構成検討

アドレス取得時に IPv6 ネットワーク展開計画のヒアリングが行われる場合があるため、最初に検討しておきます。

物理構成

ネットワーク、バックボーン、外部接続、アクセス、サーバセグメントの構成です。

試験ネットワーク段階ではネットワーク及び設備の二重化は必須ではありませんが、サービス対応時と同様なネットワークを構築しておくことが望まれます。

論理構成

アドレッシング設計

顧客用、POP 用の用途に合わせた Prefix 計画を立てます。経路集約を行いやすいように、POP 毎に大きな Prefix 領域を確保するなどの留意をします。

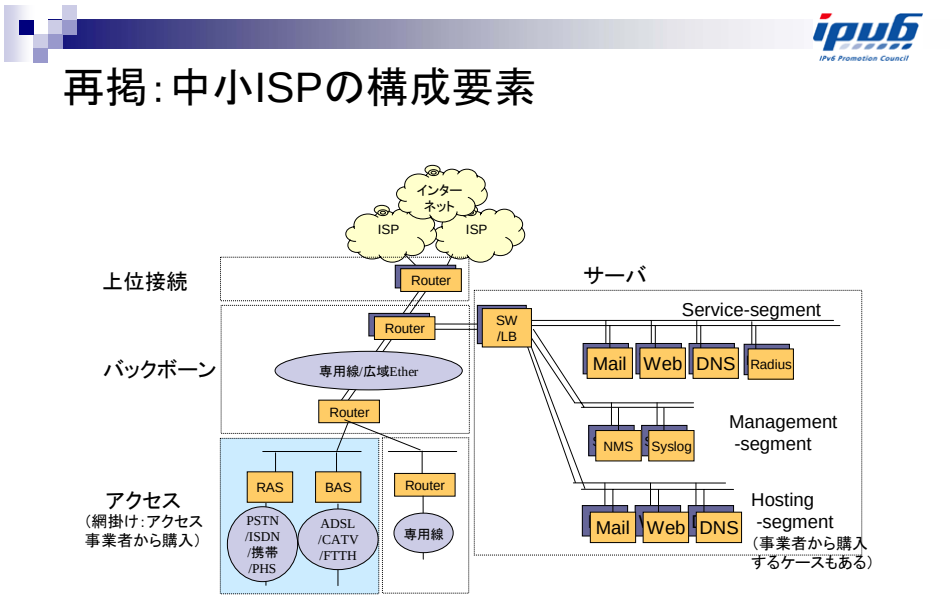
IPv6 のデータ転送のみを扱う場合でも、必ず IPv4 アドレスを各インタフェースに付与します。これは、運用を既存システムで行うためです。

ルーティング設計

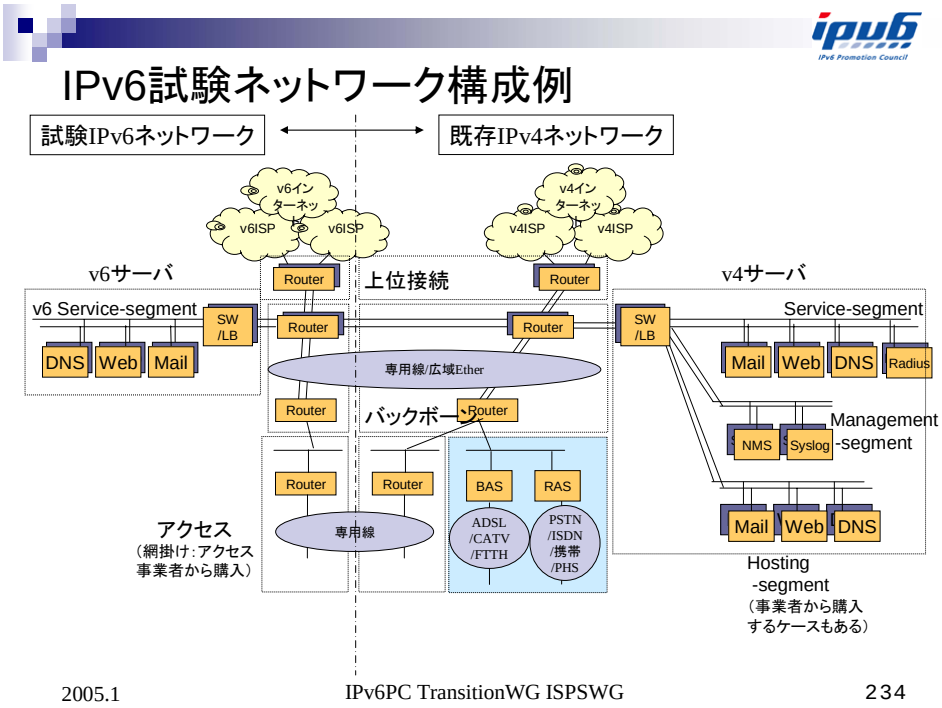
外部経路は、BGP Mulitprotocol Extension、内部経路は OSPFv3 を使います。

顧客経路設定は静的ルーティング、内部経路への再配布を行います。

再掲：中小 ISP の構成要素



IPv6 試験ネットワーク構成例



2. アドレス取得

JPNIC 指定事業者の場合、「JPNIC IPv6 アドレス申請取り次ぎサービス」を利用してアドレス申請を行います。http://www.nic.ad.jp/ja/ipv6/index.html (JPNIC)を参照してください。

申請時に必要な内容

IPv6 アドレス申請の流れは http://www.nic.ad.jp/doc/ipv6-alloc-process.html を参照してください。

申請記述内容

これについては、下記の申請記述例をご覧ください。

料金

IPv6 アドレス割り振り手数料

・1 サイト(/48)につき 4.2 円(税込)

・/32 の場合、調整により 7132 サイトとして算出し、29954 円(税込)

IPv6 アドレス維持手数料

・/32 の場合、262,500 円/年(税込)

IPv4 /20 以上のアドレス管理を行っている(割り振りを受けている)場合には、/32 IPv6 アドレス維持手数料は免除されます。(IPv4 アドレス維持手数料と IPv6 アドレス維持手数料の高い方が適用されます)。

詳細は、JPNIC ドキュメント JPNIC-00937「IP アドレス割り当てなどに関する規則」を参照してください(http://www.nic.ad.jp/doc/ip-rule.html)。

JPNIC および APNIC で申請内容の確認作業終了後、1 ヶ月前後で IPv6 Prefix 割り振りが行われます。

IPv6 アドレス申請

IPv6 アドレス申請(例後述※)を作成し、request@ipv6.nic.ad.jp にメールで送付します(Subject 等は任意)。

※IP アドレス管理指定事業者定例説明会資料より抜粋
(http://www.nic.ad.jp/ja/materials/ip/4beginers20040910.pdf)

申請内容は JPNIC で確認後、APNIC に送付されます。内容確認時に JPNIC、及び APNIC(JPNIC 経由)より問い合わせがある場合があります。

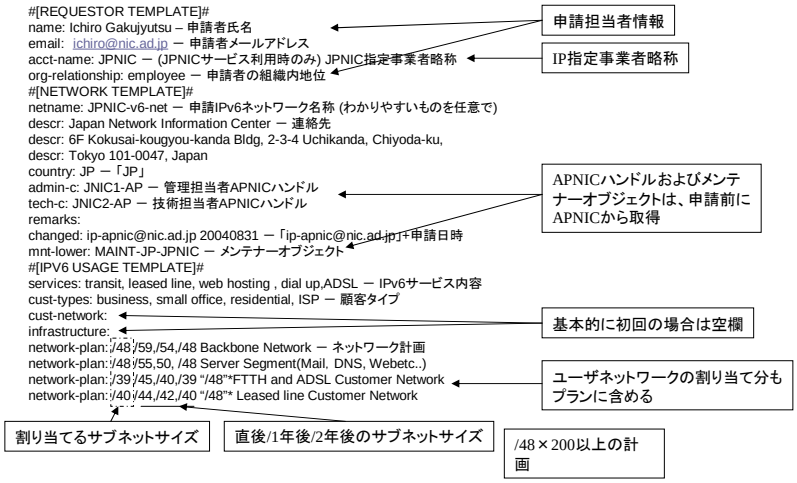
個々のネットワークの状況にあわせた記述については、下記のガイドラインを参照してください。

http://www.nic.ad.jp/ja/translation/ipv6/ipv6-alloc-form-guide.html

IPv6 アドレス申請前に、Maintainer Object(ネットワーク情報)、Person Object(ネットワーク管理者情報)を APNIC に申請、取得します。申請方法は後述します。

IPv6 アドレス申請記述例

IPv6アドレス申請記述例



上記申請を補足情報として、IPv6サービス展開のプランなどがあるとよい

Maintainer Object、Person Object 申請方法

IPv6アドレス申請時に必要なMaintainer Object(ネットワーク情報)、Person Object(ネットワーク管理者情報)を申請します。

Maintainer/Person Object 申請(例後述)を作成し、maint-request@apnic.net (Maintainer Object 申請アドレス)にメールで送付します。Subject には APNIC アカウントを含めます。 JPNIC 指定事業者の場合、Subject に「JPNIC-JP」を必ず含めます。

申請方法(および内容変更方法)の説明は、下記をご覧ください。

http://www.nic.ad.jp/ja/translation/apnic/apnic-102-j.html

http://www.nic.ad.jp/ja/translation/apnic/20021217.html

問題がなければ、数日中にメールでMaintainer Object承認・登録、Person Object登録情報を示す APNIC NIC ハンドルが連絡されます。

Maintainer Object、Person Object 申請記述例

Maintainer Object、Person Object申請記述例

```
#[MAINTAINER TEMPLATE V:3.0]#

mntner: MAINT-JP-JPNIC              ー MAINT-JP-「組織名」、組織名は任意 (指定事業者略称を推奨)
descr: Maintainer for JPNIC         ー 組織の簡単な概要
descr: Webhosting, dialup, leased line
descr: Japan
admin-c: AUTO-1                     ー Person Objectと同時申請の場合は「AUTO-数字」と記述し、Person Objectの記述とあわせる
tech-c: AUTO-2                      ー admin-c、及びtech-cは同一人物でもよい
                                      Admin-c、Tech-cはそれぞれ複数登録することが可能、その際は必要分を列記する
upd-to: noc@nic.ad.jp               ー Maintainer Objectに関する情報の連絡先(Person ObjectやDomain Object(後述)更新情報が送られる)
auth:  CRYPT-PW JPNIC-v6v6          ー Maintainer Object利用時の認証方法
                                      平文認証　ー 「CRYPT-PW」＋平文パスワード
remarks:                            ー 注記 (特に必要なし)

[PERSON TEMPLATE V:4.0]#

Person: Ichiro Gakujyutsu           ー 名前
address: 6F Kokusai-kougyou-kanda Bldg, 2-3-4 Uchikanda, Chiyoda-ku,  ー 住所
address: Tokyo 101-0047, Japan
country:  JP                        ー 所在国、JPNIC指定事業者の場合は「JP」
phone:  +81-3-1234-5678             ー 電話連絡先
fax-no:  +81-3-1234-9876            ー Fax連絡先(任意)
e-mail: ichiro@nic.ad.jp            ー e-mailアドレス
nic-hdl: AUTO-1                     ー NICハンドル
                                      Maintainer Objectと同時申請の場合は「AUTO-数字」と記述し、Maintainer Objectの記述とあわせる
remarks:                            ー 注記 (特に必要なし)

#[PERSON TEMPLATE V:4.0]#

person: Hanako Gakujyutsu
address: 6F Kokusai-kougyou-kanda Bldg, 2-3-4 Uchikanda, Chiyoda-ku,
address: Tokyo 101-0047, Japan
country:  JP
phone:  +81-3-1234-5678
fax-no: +81-3-1234-9876
e-mail: hanako@nic.ad.jp
nic-hdl: AUTO-2
remarks:

#[TEMPLATES END]#
```


3. 機器準備

必要な機器は、おもにサーバとルータです。

ルータ

外部接続（上流接続、IX やプライベートピアの Peer 接続、バックボーン、アクセス、顧客収容）に使用します。本ケーススタディでは、トンネル終端ルータを想定しています。

サーバ

DNS サーバの設置は、取得アドレスの逆引き管理を行うために必須です。AAAA を扱うサーバにする必要があります。必ずしも IPv6 トランスポートをサポートする必要はないですが、サポートしていることが望まれます。

その他、経験蓄積のためにも、基本的な Mail や Web の IPv6 対応サーバなども構築しておくことが望まれます。IPv6 ネットワークの日常管理を行うためのサーバ、もしくは IPv6 端末を用意することが望まれます。Ping6 や tracertoute6 などを行うなどの管理を行います。

機器、サーバアプリケーション選定

機器選定

現在利用している機器で IPv6 対応していれば、可能な限り同一機器の利用を推奨します。理由は、デュアルスタックネットワークへの移行のためです。

必要な機能

IPv6 Logo Phase I 相当の IPv6 機能を具有することが求められます。可能な限り、IPv6 Logo Mark 取得機器の利用を推奨します。IPv6 Logo Mark 取得機器リストについては後述します。

ルータの場合、上記に加えて必要なルーティングプロトコル(ここでは BGP4+、OFPFv3、スタティック)をサポートすることが必要です。

サーバアプリケーション選定

OS は、現在利用しているサーバ OS が IPv6 に対応していれば、可能な限り同一 OS の利用を推奨します(BSD、Linux(USAGI の適用を推奨)、Solaris、HP-UX など)。

サーバは、現在利用しているサーバアプリケーションで IPv6 対応していれば、可能な限り同一アプリケーションの利用を推奨します。

IPv6 対応サーバアプリケーション例としては、DNS が Bind9 など、Web で Apache2 など、電子メールは SMTP サーバが Sendmail、postfix、qmail など、POP3 サーバが qpopper、cyrus-IMAPd(IMAP サーバとしても)、などです。

「IPv6 Style」に IPv6 対応 OS およびアプリケーションサーバ情報が掲載されています。

http://www.ipv6style.jp/jp/statistics/ipv6unix/index.shtml

機器認証

機器認証プログラムとして IPv6 Ready Logo プログラム(http://cf.v6pc.jp/frames.html)があります。IPv6 Forum が主催する機器導入のガイドラインとなる認定プログラムです。通過基準を制定しており、現在は PhaseI プログラム、PhaseII プログラムの一部が制定されています。

対象機器はルータ、端末、スペシャルデバイスです。可能な限り IPv6 Ready Logo 認定品の利用を推奨します。

最新の IPv6 Logo Mark 認定品リストは、以下の URL にあります。

http://cf.v6pc.jp/logo_db/approved_list.php

4. ネットワーク構築

ネットワーク構築方法に関しては、既存ネットワークと変わるところはありません。デュアルスタックネットワーク移行のため、可能な限り既存ネットワークと同一形態で構築することが望まれま

す。

・外部接続

安定的な接続を確保するために、グローバル IPv6 接続の確保は ISP の IPv6 ゲートウェイサービス等を利用することが望まれます。上流接続のみでも国内的な接続性は確保されます。

国内 ISP との IPv6 接続性は、IPv6 対応 IX などで Peer を行うことにより確保するとよいと思われます。

・顧客接続

静的経路設定による接続を行います。顧客静的経路を、ISP 内部経路に再配布し接続性を確保します。顧客トンネルルータとの Configured Tunnel の設定を行います。

さらに、ルータ設定、サーバ設定（サーバセグメント構築、サーバ構築）を行います。

ルータ構築

IPv6 アドレッシングは、通常、リンクに対して/64 Prefix をアサインします。/126 Prefix でもよいですが、/127 は薦めません。また、リンクの死活監視などの観点から、unnumbered とすることは薦めません。

ルータインタフェースに付与する IPv6 アドレスは通常固定とします。 RA などは利用しません。リンクローカルアドレスは、通常そのまま(fe80::(EUI-64)) で問題ありません。

IPv4 アドレッシングは既存ポリシーを踏襲します。

外部接続例- IPv6 対応 IX(NSPIXP6)への接続

NSPIXP6 は、 WIDE Project が運営する IPv6 対応 IX です。

DIXIE のようなプロダクションレベルではなく実験的なレベルであることを理解する 必要があります。KDDI 大手町ビル、NTT 大手町ビル、NTT 堂島ビルなどに接続ポイントを持っています。詳細は下記 URL を参照してください。

http://www.wide.ad.jp/nspixp6/

NSPIXP6 への接続手順例

NSPIXP6 への接続については、東京大学 加藤先生に相談します（メール、NSPIXP 会合など）。特に決まったフォーマットはありませんが、下記の情報があると判断がつきやすいと思われます。

・組織
・組織の概要
・接続の目的
・AS
・(取得していれば)IPv6 Prefix
・接続場所、など

NSPIXP6 への接続は、接続許可が下りた後に作業を行います。NSPIXP6 運用担当へ事前に作業時間などを連絡しておくことが望まれます。

通常は FastEthernet(100BASE-TX/FX)で接続します。IPv6 Peer アドレスは一定の法則によりアサインされます。fe80::ASN:ID あるいは (NSPIXP6 IPv6 Prefix) ::ASN:ID となります。http://www.wide.ad.jp/nspixp6/peering-address.txt を参照してください。

接続作業完了後、NSPIXP6 への接続後、運用担当へご連絡し、下記情報を連絡します。

接続場所、接続スイッチポート番号、IPv6 Prefix、組織名、AS 番号(10 進、及び 16 進)、Peer アドレス、IX 接続ルータ実装、コンタクト先

これで、コンタクトリストへの追加などが行われます。

Peer の交渉、設定

NSPIXP6 接続後、各 Peer 連絡先へコンタクトし、Peer を打診します。コンタクトの際には、下記の接続情報を連絡することが望ましいと考えられます。

・IPv6 アドレス (上記の方針により生成されたアドレス)
・広報する AS Path (自 AS,もしあれば配下の AS Path も)
・広報する Prefix (自 Prefix、もしあれば配下の Prefix も)
・運用に関するコンタクトポイント (メール、電話番号、Fax 番号など)
・必要であれば、MD5 パスワード、覚書の取り交わし、等

Peer に合意した後、IX 接続ルータに Peer の設定を投入します。Peer セッションが立ち上がり、経路交換が正しく行われていることを確認します。

ネットワーク構築 Tips

ICMPv6 パケットに対するアクセスリスト

IPv6では、ICMPv6パケットを通過させても大きなセキュリティ的脅威となることはありません。PMTUD動作のため、特にType2(Packet Too Big)パケットは必ず通過させなければなりません。Type1(Destination Unreachable)、Type3(Time Exceedes)、Type4(Parameter Problem)も通過させたほうがよいと考えられます。

また、IPv6では、IPv4のような外部からのブロードキャストICMPパケットを利用した内部セグメントへの攻撃の心配がありません。Neigbor Discovery関連のICMPv6パケットはリンクローカルのみで利用されます。

ICMPv6 パケットフィルタは、ネットワークポリシーにあわせて必要に応じて設定します（内部ホストの存在を確認するための Type129/130(Echo Request/Reply) パケットの遮断、Type138(Router Renumbering)、Type139/140(Node Information Query)など）。

APNIC のデータベースに登録された IPv6 アドレスは、到達可能になっていなければなりません（DNS サーバの IPv6 アドレスなど）

トンネルに対するフィルタリング

IPv6トンネルパケットが通過するIPv4セグメントでは、IP Protocol 41番のパケットを通過させる必要があります。

<u>サーバセグメントネットワーク構築</u>

・アドレッシング

サーバセグメントにおけるアドレッシングは以下のように行います。

IPv6の場合、セグメントに対し、/64 Prefix を割り当てます。サーバアドレスは通常固定割り当てとし、RA は利用しません。場合によっては RA による割り当てもあり得ます。

IPv4 の場合、接続に必要な大きさの Prefix を割り当てます。サーバアドレスは、通常固定割り当てとします。

・ルーティング

通常 IPv6/IPv4 ともデフォルトでは静的ルーティングです。 冗長性確保などの目的で動的ルーティングや VRRP 等を設定する場合もあります。

<u>サーバ構築</u>

DNS サーバ

DNS サーバはデュアルスタックで構築します。

逆引き Zone 情報を管理する DNS の場合の設定では、逆引き Zone の SOA レコードを競っています。

2001:db8::/32 の場合 → 8.b.d.0.1.0.0.2.ip6.arpa

必要に応じて登録レコードを作製します。それは、上位サーバが IPv6 問い合わせに対応しているとは限らないためです。特に、ルートサーバは現状 IPv6 問い合わせには対応していません。

メールサーバ

SMTP サーバは、通常デュアルスタックで構築します。これは、接続元サーバから IPv6/IPv4 両方で接続される可能性があるものの、接続先サーバが IPv4 しか接続を受け付けない可能性があるからです。そして、MX レコードは IPv6/IPv4 に分けて登録することはできません。

POP3/IMAP サーバなどは、クライアントの IPv6 対応状況によります。

DNS Zone 情報設定例

DNS Zone情報設定例 (bind9)

- named.conf
  - 正引き

```
zone “test.com” {
type master;
file “test.com.zone”
};
```

  - 逆引き

```
zone “8.b.d.0.1.0.0.2.ip6.arpa” {
type master;
file “8.b.d.0.1.0.0.2.ip6.arpa.rev”;
};
```

- test.com.zone

```
@                IN    SOA    ns.test.com. Admin.test.com. (
                                                2004122101
                                                3600
                                                900
                                                3600000
                                                3600 )
                 IN    NS     ns.test.com.
ns               IN    A      192.168.0.1
                 IN    AAAA   2001:db8::53
```

- 8.b.d.0.1.0.0.2.ip6.arpa.rev

```
@                IN    SOA    ns.test.com. Admin.test.com. (
                                                2004122101
                                                3600
                                                900
                                                3600000
                                                3600 )
                 IN    NS     ns.test.com.
3.5.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0   IN   PTR   ns.test..com.
```


接続試験

接続試験で確認すべき事項は、以下の通りです。

·IPv6 インターネットへの接続性

ルーティングテーブルの確認

内部から外部 IPv6 ネットワークへの到達性確認

内部ルータ等から、Ping6、traceroute6 などで到達性を確認します。ターゲットホストとして、www.v6pc.jp (IPv6 普及・高度化推進協議会)、www.kame.net(KAME Project)などが使えます。

外部から内部 IPv6 ネットワークへの到達性など確認

外部 IPv6 対応 Looking Glass で自 IPv6Prefix 広報の状況、内部ネットワーク(内部ルータの IPv6 アドレスなど)への ping6 や、traceroute6 などで到達性を確認します。

http://www.v6.mfeed.ad.jp/ipv6/lg.html

http://query.freak.ne.jp/

http://www.v6.dren.net/lg/index.html、など

擬似顧客環境を用意し、顧客ネットワークからの IPv6 ネットワーク接続性を確認する

Ping6 のパケットサイズを変更(大きく)し、PMTUD がネットワーク内で正常に動作することを確認する

通常の Ethernet での最大 MTU 値(1500byte)以上にして確認する、など

・サーバ動作

DNS の設定及び APNIC への IPv6 アドレス空間逆引き管理権限委譲の申請を行う

申請方法は後述します。

Web、Mail サーバなどの動作を確認

·管理

既設システムより IPv6 機器の管理が行えるか

IPv4 と IPv6 の両方で管理できることが望ましい

ログインサーバからの到達性確認

IPv6 Prefix DNS 逆引き情報の RIR データベース登録

登録時に、DNS サーバのインターネット接続性 (アドレス、DNS サーバ動作)および逆引き Zone 情報 (SOA レコード)の確認が APNIC のシステムより行われるため、事前に DNS サーバの構築、及び逆引き Zone 情報の設定を行っておきます。

割り当て Prefix の管理担当者(admin-c)、技術運用担当者(tech-c)、及びゾーン管理者(zone-c)の Person Object 申請(例後述)を作成し、auto-dbm@apnic.net にメールで送付します(通常は Maintainer Object と同一)。

問題がなければ、数日中にメールで Person Object 登録情報を示す APNIC NIC ハンドルが連絡されます。

さらに、DNS 逆引き情報の domain Object 申請(例後述)を作成し、auto-dbm@apnic.net にメールで送付します。

申請方法(及び内容変更方法)の説明は、以下の URL を参照してください。

http://www.nic.ad.jp/ja/translation/apnic/apnic-database-update-info.html

問題がなければ、数日中にメールで登録終了が連絡されます。

Person Object 登録申請記述例

Person Object登録申請記述例

person: Ichiro Gakujyutsu	ー 名前
address: 6F Kokusai-kougyou-kanda Bldg, 2-3-4 Uchikanda, Chiyoda-ku,	ー 住所
address: Tokyo 101-0047, Japan	
country: JP	ー 所在国 (日本の場合「JP」)
phone: +81-3-1234-5678	ー 電話連絡先
fax-no: +81-3-1234-9876	ー Fax連絡先(任意)
e-mail: ichiro@nic.ad.jp	ー e-mailアドレス
nic-hdl: AUTO-1	ー NICハンドル (未決定状態なので「AUTO-1」と記述)
remarks:	ー 注記 (特に必要なし)
notify:	ー 連絡先アドレス (e-mailと同じであれば必要なし)
mnt-by: MAINT-JP-JPNIC	ー ISPのMaintainer Objectを記述
changed: noc@nic.ad.jp	ー ISPの申請担当者アドレス 通常Maintainer Objectのupd-to:を記述
source: APNIC	ー 情報ソースを記述 JPNIC指定事業者の場合「APNIC」

IPv6 Prefix DNS 逆引き情報登録申請記述例

IPv6 Prefix DNS逆引き情報登録申請記述例

domain: 8.b.d.0.1.0.0.2.ip6.arpa	－逆引きドメイン名
descr: Reverse Delegation of 2001:db8::/32	－ ドメインの説明
admin-c: IG100-AP	－ 管理者NICハンドル
tech-c: HG200-AP	－運用者NICハンドル
zone-c: HG200-AP	－ ゾーン管理者NICハンドル
nserver: dns-ipv6-1.nic.ad.jp	－ 逆引きゾーン管理を行うDNSサーバ名(FQDN)を記述
nserver: dns-ipv6-2.nic.ad.jp	DNSサーバ名は複数記述可能 DNSサーバ名のデータベース登録は無いため、事前にアドレス正引きを行えるように設定しておく
sub-dom:	－ サブドメインリスト (IPv6逆引き登録においては必要なし)
dom-net:	－ドメイン中のアドレスリスト (IPv6逆引き登録においては必要なし)
remarks:	－ 注記 (特に必要なし)
notify: noc@nic.ad.jp	－ ISPの申請担当者アドレス 通常Maintainer Objectのupd-to:を記述
mnt-by: MAINT-JP-JPNIC	－ ISPのMaintainer Objectを記述
mnt-lower:	－ mnt-byにて認証されない場合の下位Maint. Object (特に必要なし)
refer:	－DNSサーバへの参照 (IPv6逆引き登録においては必要なし)
changed	－ 情報変更者のアドレス 通常Maintainer Objectのupd-to:を記述
source:	－ 登録データベース名を記述 JPNIC指定事業者の場合「APNIC」

5. 運用

・日々の管理

ネットワーク監視については、IPv6 ICMPv6 による機器インタフェース死活監視を行います。IPv6 対応 NMS などを利用します。

また、既存 IPv4 管理システムからも、機器インタフェース死活監視(ICMPv4)、プロセス監視(syslog)、トラフィック状況監視(snmp)などの管理を行います。

・プロビジョニング

これは、アドレス取得に伴う義務です。

アドレス割り当てに伴う RIR データベース登録（登録方法は後述）を実施します。

また、取得アドレスの DNS 逆引き設定の管理を行います。必要に応じて、割り当て Prefix の逆引き zone の権限委譲の設定を行います。

顧客収容時のプロビジョニングとしては、トンネル設定、静的経路設定があります。

・外部接続

Peering 情報のアップデートを行います。

IPv6 アドレス割り当て情報の RIR データベース登録

割り当て Prefix の管理担当者(admin-c)、及び技術運用担当者(tech-c)の Person Object 申請(例先述)を作成し、auto-dbm@apnic.net にメールで送付します。問題がなければ、数日中にメールで Person Object 登録情報を示す APNIC NIC ハンドルが連絡されます。

また、割り当て Prefix 情報の inet6num Object 申請(例後述)を作成し、auto-dbm@apnic.net にメールで送付します。

申請方法(及び内容変更方法)の説明は、以下を参照してください。

http://www.nic.ad.jp/ja/translation/apnic/apnic-database-update-info.html

問題がなければ、数日中にメールで登録終了が連絡されます。

inet6num Object 登録申請記述例

inet6num Object登録申請記述例

inet6num: 2001:db8:1::/48	ー IPv6 Prefix
netname: JPNICTESTNET	ー ネットワーク名(大文字で任意)
descr: JPNIC IPv6 Test Network	ー ネットワークの説明
country: JP	ー所在国 (日本の場合「JP」)
admin-c: IG100-AP	ー 管理者NICハンドル
tech-c: HG200-AP	ー 運用者NICハンドル
ev-srv:	ー DNSサーバ名 (inet6numでは特に必要なし)
status: ALLOCATED NON-PORTABLE	ー ネットワークの状態 アドレス割り当ての場合には「ALLOCATED NON-PORTABLE」
remarks:	ー 注記 (特に必要なし)
notify: noc@nic.ad.jp	ー ISPの申請担当者アドレス 通常Maintainer Objectのupd-to:を記述
mnt-by: MAINT-JP-JPNIC	ー ISPのMaintainer Objectを記述
mnt-lower:	ー mnt-byにて認証されない場合の下位Maint. Object (特に必要なし)
mnt-irt:	ーComputer Security Incident Response Team (CSIRT) セキュリティインシデント用 (現時点では特に必要なし)
changed: noc@nic.ad.jp	ー 情報変更者のアドレス 通常Maintainer Objectのupd-to:を記述
source: APNIC	ー 登録データベース名を記述 JPNIC指定事業者の場合「APNIC」

LIR 向け IPv6 アドレス管理ツール

これは、IPv6 アドレス取得組織(LIR)で IPv6 アドレスの取得から管理までをサポートする管理ツールです。IPv6 普及・高度化推進協議会で開発されたもので、これから IPv6 アドレスを取得し、IPv6 管理を必要とする組織に有用です。

アドレスの申請方法から/48 Prefix サイトのデータベース登録まで、アドレス申請に関する事項が網羅されたドキュメントも付属しています。すでに IPv6 アドレス管理システムを持っている組織、

既設置システム(IPv4 管理システム)で IPv6 アドレス管理を行う組織においても有用です。
詳細は下記 URL を参照してください。

http://www.v6nic.net/system/index.html

トラブルシューティング

ルーティング

Q: peer へ広告する経路はどうすればいいのでしょうか？
A: AS は通常/32 Prefix でアグリゲートしたものを広告します（歴史的経緯で/35 Prefix を持つ AS、もしくはそれより短い Prefix を持つ AS もあります）。自 AS で持っている Prefix から/48 や/64 といった Prefix を切り出してバラバラ流すことは通常お勧めできません。

Q: お隣の ISP から見かけない/48 や/64 が流れてくるのですが？
A: 特殊な用途として、APNIC などがそのような Prefix を割り当てているケースが見られます。RIR のデータベースを whois などで調査し、あやしいルートでなければそのままで特に問題ありません。
特殊用途を含めた、各 RIR での IPv6 Prefix 割り当て状況は下記 URL にも情報があります。

http://www.ripe.net/ripencc/mem-services/registration/ipv6/ipv6allocs.html

明らかに/32 などから切り出した細かい Prefix を流しているようなケースでは、当該 Prefix を BGP 設定の In 側でフィルタしてもよいでしょう。

アドレッシング

Q: アドレッシング割り当てで困っているのですが？
A: 例えば、データセンターを/56 単位で管理する場合、2001:DB8:0:0000::/56 をネットワーク機器のセグメント 2001:DB8:0:0A00::/56 をサーバ用セグメントとすると/64 の管理表も大きくなりすぎず、頭を見るだけでサーバなのかルータなのかが一目でわかります。
IPv6 では階層的に IPv6 Prefix を管理する事が重要なノウハウです。トラブルシュートもやりやすいというメリットもあります。

運用

Q: 障害の疑いがある場合、運用者がサービス正常性確認を行うにあたって、どこに Ping、もしくは HTTP Get などを試すのがよいでしょうか？

A: ピアとの接続点を考慮しながら選択する事をお勧めします。一般的には www.v6pc.jp や www.kame.net などが使われたりしています。

一般的な Web サイトに対しての Ping は特別な技術を持った運用者を必要としませんが、経路障害などを検知しにくいというデメリットがあります。自分のネットワークがどこでピアを行っているか、という事を考慮しながら、サービス正常性確認を行う事が大切です。また、traceroute による確認もお勧めします。

なお、HTTP Get については IPv6 の世界ではリテラル形式(※)でのアドレス直接指定ができない事が多いので注意が必要です。

Internet Explorer のエンジンを利用しているブラウザでは、現在リテラル形式でアクセスができなくなっています。但し、Mozilla エンジンを利用するブラウザである Firefox1.0 など本形式がサポートされているものもあります。

(※) リテラル形式とは、http://[IPv6 address]/という形式です(例. http://[2001:DB8::1])。

APNIC 登録

Q: 逆引き DNS サーバの登録ができません。

A: APNIC の逆引きドメイン登録はスクリプトで DNS の挙動の確認を行います。もし登録が最後まで終了しない場合には、DNS サーバの下記の項目を確認してください。

- DNS サーバの FQDN に対して IP アドレスが引ける状態になっていますでしょうか
- DNS サーバへのインターネット接続性はあるでしょうか
- DNS サーバが起動していますでしょうか
- 逆引きドメインに対する SOA レコードが設定されてますでしょうか

エラーメッセージにも内容が記述されますので、コメントを確認して対処して再度登録作業を行ってください。

移行 WG ISP セグメント 検討メンバ

（敬称略）

2003 年度メンバ

SWG チェア

中井哲也（NTT コミュニケーションズ）

リーダ

アドレス＆ルーティング担当

石原（KDDI）

ネットワーク担当

石川（NTTPC コミュニケーションズ）

松平（富士通）

サーバ担当

橘（あにあにどっとこむ）

検討メンバ（敬称略・50 音順）

荒野（インテックネットコア）

石原（東芝）

猪俣（富士通）

岡本（eAccess）

金山（インテックネットコア）

国武（RINT）

鈴木（日立）

須田（知多メディアスネットワーク）

竹山（eAccess）

中原（NEC）

難波（古河電工）

松岡（NTT PF 研）

2004 年度メンバ

SWG チェア

石原清輝（KDDI）

検討メンバ（敬称略・50 音順）

荒木(日本テレコム)
荒野（インテックネットコア）
飯塚(パワードコム)
石井(インターネットマルチフィード)
石原（東芝）
伊藤(IPv6 普及･高度化推進協議会)
稲葉(TOKAI)
太田(NTT 東日本)
大塚(NTT 西日本)
岡(東芝ソリューション)
沖本(NTT 西日本)
小山(倉敷ケーブルテレビ)
川島（NEC アクセステクニカ）
川島(シスコシステムズ)
川村(NEC)
北村(NTT 西日本)
鬼頭(アライドテレシス)
国武（アンカーテクノロジー）
後藤(富士通)
佐藤(アライドテレシス)
佐藤(NTT 東日本)
鈴木(IIJ テクノロジー)
鈴木(NTT コミュニケーションズ)
鈴木（日立）
須田（知多メディアスネットワーク）
富川(IIJ テクノロジー)
中井（NTT コミュニケーションズ）
中原（NEC）
難波（古河電工）
西野(イー・アクセス)

西本(イー・アクセス)
廣海(インテックネットコア)
細野(NTT 東日本)
松本(インテックネットコア)
松本(日本テレコム)
水谷(シスコシステムズ)
湊(富士通アクセス)
毛利(NTT コミュニケーションズ)
山本(NTT 東日本)

お問い合わせ先

本ガイドラインに関するお問い合わせは、以下のアドレスまでメールでご連絡下さい。
IPv6 普及・高度化推進協議会移行 WG／e-mail: wg-dp-comment@v6pc.jp