日本ケーブルラボ資料

IPv6 対応ケーブルインターネット アクセス技術仕様ガイドライン

Guideline of technical specifications for cable internet access IPv6-enabled

JLabs DOC-009 3.0 版

2020 年 3 月 26 日

一般社団法人　日本ケーブルラボ

Japan Cable Laboratories

まえがき

本ガイドラインは、ケーブル事業者が IPv6 を導入するにあたり、想定される IPv6 アドレスの実装方法やアドレス配布方法、ケーブルインターネット特有の注意点などを策定したものである。

ケーブル事業者の IPv6 アドレス対応は IPv4 アドレスの枯渇対策の検討から始まり、本ガイドラインは 3 回目の改定になる。

2009 年 1 月、社団法人日本ケーブルテレビ連盟日本ケーブルラボによって IPv4 アドレス枯渇対応プロジェクトが発足された。

2010 年 6 月にその配下に設置した IPv6 対応 CATV アクセス仕様策定タスクグループによって「IPv6 対応ケーブルインターネットアクセス技術仕様ガイドライン：JLabs DOC-009-00 1.0 版」が発行されケーブル事業者に向けて周知広報した。

その後、一般社団法人日本ケーブルラボにて継承し、本格的な IPv6 導入に向けて、より詳細にさまざまなネットワーク形態に対応するべく、2012 年 9 月に 2.0 版として改定を行った。その後、インターネットを取り巻く環境の変化に伴う対応や導入事例の追加を行い、2015 年 3 月に 2.1 版として改定を行った。

前回の改定から約 5 年が経過しており、その間に IPv6 を取り巻く環境が大きく変化してきた。総務省の「IPv6 によるインターネットの利用高度化に関する研究会」が平成 30 年 3 月に発行した最終報告書では、IPv6 対応の究極的な目標として IPv6 ディプロイメント（利用環境整備）から、IPv6 マイグレーション（IPv6 の利用促進による IPv6 シングルスタック化の実現）に改めて設定された。

ケーブルテレビ業界においても、IPv6 マイグレーション、つまり IPv6 シングルスタック化に向けた課題を検討すべく、IPv6 検討 WG で議論された内容を元にガイドラインの改定を行った。また、今回の改定では、章構成の見直しや古くなった情報の削除なども合わせて行った。

本ガイドラインがケーブル事業者のインターネット運用を担っている技術者に積極的に活用されることを期待する。

（空白）

目次

第1章　はじめに

1.1　ガイドライン策定の目的

本ガイドラインは、IPv6 接続環境を提供するケーブルインターネットアクセスの技術的な注意点を提示し、IPv6 の導入を促すことを目的としている。

1.2　ガイドライン改定の背景

IPv6 化には、IPv4・IPv6 デュアルスタックおよび IPv6 シングルスタックの 2 種類があり、いずれの方式もユーザの宅内端末（CPE）での IPv6 接続環境を提供する必要がある。

IPv6 接続環境の提供に重要な要素の 1 つに IPv6 アドレス割り当て方式があり、ケーブルテレビ業界で主流になっている DHCPv6 方式から DHCPv6-PD 方式による家庭用ルータ（CE-Router）の LAN 側へのアドレス配布が推奨される風潮となった。これは、対応可能な機器の種類や運用の容易さ、セキュリティ面や家庭用 IoT 機器の増加を見越したためである。特に、セキュリティ面では CE-Router の IPv6 をブリッジする方式は、加入者内部のネットワークと事業者のネットワークを厳密に分離することができず、一定のセキュリティを担保することが困難になると予想される。このことから、市販の CE-Router の LAN 側は DHCPv6-PD によるアドレス割当てのみに対応する動きがある。

一方で、本ガイドライン（DOC-009）の 2.1 版では、アクセス網を中心に DHCPv6 方式の提供に必要な情報を主に記載しており、CE-Router の LAN 側について DHCPv6-PD 方式を推奨する内容にはなっていなかった。

また、総務省の「IPv6 によるインターネットの利用高度化に関する研究会」では、IPv6 シングルスタック化が目標として掲げられているが、DOC-009 2.1 版では、IPv6 シングルスタックについては記載されていないため、IPv6 シングルスタックで使われる IPv4 over IPv6 通信技術について調査、分析する必要があった。

1.3　用語と略語の定義

本ガイドラインでは用語と略語を以下のとおり定義する。

用語	内容
ACL	Access Control List の略。個々のネットワーク利用者が持つアクセス権限やアクセス可能なサーバやファイルなどの資源を列挙したリスト。
AP	Access Point の略。
APC	Access Point Controller の略。無線 LAN の AP と常に通信を行い集中的に AP の管理や各種制御を行うシステム。

用語	内容
APM	Alternative Provisioning Mode の略。最初に IPv6 アドレスを割り当てるプロビジョニングを試みて成功すれば IPv6 で、失敗した場合は IPv4 アドレスを割り当てる方式。
ARP	Address resolution Protocol の略。TCP/IP ネットワークにおいて IP アドレスから Ethernet の MAC アドレスを求めるためのプロトコル。
CE-Router	Customer Edge router の略。本書では CE-Router を指す。
CLI	Command Line Interface の略。情報の表示を文字によって行うユーザインタフェイス。
CM	Cable Modem の略。
CM プロビジョニング	単にプロビジョニングと呼ぶ場合もある。CM に必要な情報を与えて契約内容に応じた設定を行い利用可能にすること。
CMTS	Cable Modem Termination System の略。
CPE	Customer Premises Equipment の略。通信回線において顧客側の端末設備。CM に接続される加入者の PC や CE-Router が相当する。
DAD	Duplicate Address Detection の略。重複アドレス検出。
DHCP、DHCPv4	Dynamic Host Configuration Protocol の略。RFC2131 で規定される動的に IPv4 ノードを設定するためのプロトコル。IPv6 用の DHCPv6 と区別するため RFC2131 DHCP を DHCPv4 と表記することがある。
DHCPv6	RFC3315 で規定される IPv6 ノード用の DHCP。DHCPv4 と互換性はなく、default route を通知する場合は SLAAC(RA)を併用する。
DHCPv6-PD	DHCPv6-Prefix Delegation の略。DHCPv6 プロトコルを用いて prefix を取得すること。
Direct Hosting of SMB	Windows2000 以降採用された、Windows ネットワークにおける接続されたコンピュータや、ファイル・サービスなどの各種ネットワーク・サービスなどを識別可能にするもの。

用語	内容
DNS	Domain Name System の略。インターネット上のホスト名と IP アドレスを対応させるシステム。
DOCSIS	Data Over Cable Service Interface Specifications の略。
DoS	Denial of Service の略。コンピュータやルータなどに不正な データを送信して使用不能に陥らせたり、トラヒックを増大させたりして相手のネットワークを麻痺させる攻撃。
DPM	Dual-stack Provisioning Mode の略。DOCSIS3.0 CM に IPv4 アドレスと IPv6 アドレスの両方を割り当てるプロビジョニング方式。
eRouter	米国 CableLabs によって規定される標準規格 DHCPv6-PD に対応した IPv6 ルータ機能搭載の CM。
G-PON	Gigabit PON の略。ITU-T 標準の GTC(G-PON Transmission Convergence)フレーム等で構成された FTTH 向けの通信方式。1Gbps の G-PON（ITU-T G.983）だけでなく 10Gbps の XG-PON（ITU-T G.987）等がある。
GE-PON	Gigabit Ethernet-PON の略。IEEE 標準の Gigabit Ethernet をプロトコルとして用いた FTTH 向けの通信方式。1Gbps の GE-PON（IEEE802.3ah）だけでなく 10Gbps の 10G-EPON（IEEE 802.3av）等がある。
GW	GateWay の略。ネットワーク上で媒体やプロトコルが異なるデータを相互に変換して通信を可能にする機器。
HE	Head End の略。
HFC	Hybrid Fiber Coaxial の略。
HGW	Home Gate Way の略。本書ではプライマリ IP 電話サービスに使用する宅内設置端末を指す。
IPv4 over IPv6	IPv6 ネットワーク上で IPv4 の接続性を提供するサービスを指す。IPv4aaS（IPv4 as a Service）と呼ばれることもある。
IPv6 ブリッジ	ルータ機能を介さず IPv6 パケットを転送する機能。IPv6 パススルーとも呼ばれることがある。
IP 電話サービス	番号形式が 050 IP 電話と 0AB～J IP 電話に分けられ、それぞれでサービスを行っており両方を指す。

用語	内容
ISP	Internet Service Provider の略。
IX	Internet eXchange の略。複数の ISP を相互に接続するインターネット上の相互接続ポイント。
LLC	Logical Link Contorol の略。LAN などで利用される伝送制御手順。
LSN（CGN）	Large Scale NAT（Carrier Grade NAT）の略。ISP などの電気通信事業者が自社内のネットワークと他社のネットワークの分界点付近で NAT を行う技術。
MAX-CPE	Maximum Number of CPEs の略。インターネット接続が可能な加入者端末の台数を MAC アドレスによって制限する方式のことをいう。
MAC アドレス	Media Access Control アドレスの略。Ethernet カードに割り当てられる固有の ID。
MDD	Mac Domain Descriptor の略。DOCSIS3.0 において導入された、CMTS から CM に対して送信されるメッセージフィールド。
MDF	Multicast DSID Forwarding の略。DOCSIS3.0 において導入された、下り方向のマルチキャスト転送を制御する機能。
MIB	Management Information Base の略。通信ネットワークにおけるデバイス管理するためのデータベース。
MSO	Multiple System Operator の略。
NA	Neighbor Advertisement の略。アドレス情報などを広告するための NDP メッセージ。
NAT	Network Address Translation の略。1 つのグローバル IP アドレスを複数のローカルアドレスで共有する技術。
NDP	Neighbor Discovery Protocol の略。同一リンク上のノードに対する動作を扱うプロトコル。ルータ探索、アドレス自動設定などをサポートする。
NetBIOS	Windows ネットワークにおいて、接続されたコンピュータやファイルなどを識別可能にするもの。
NS	Neighbor Solicitation の略。近隣ノードのリンク層アドレスを決定するためなどに利用される NDP メッセージ。

用語	内容
OLT	Optical Line Terminal の略。事業者側に設置される光回線終端装置のこと。
ONU	Optical Network Unit の略。加入者側に設置される光回線終端装置のこと。G-PON においては、ONT（Optical Network Terminal）と呼ばれる。
OSPF,OSPFv3	Open Shortest Path First の略。TCP/IP における経路選択プロトコルの１つ。
PE-Router	Provider Edge router の略。本書では CE-Router が接続する事業者側に設置されたルータを指す。
PON	Passive Optical Network の略。1 本の光ファイバーを光受動素子で分岐させる FTTH ネットワーク形態の一種。標準化されている PON 方式には、IEEE 標準の GE-PON と ITU-T 標準の G-PON がある。 また、1Gbps の GE-PON(IEEE802.3ah)だけでなく、10Gbps の 10G-EPON（IEEE 802.3av）等があり、G-PON には 1Gbps の G-PON(ITU-T G.983), 10Gbps の XG-PON（ITU-T G.987）等がある。
Prefix	ネットワーク ID、インタフェース ID で構成される IPv6 アドレス構造のネットワーク ID を指す。
RA	RouterAdvertisement の略。IPv6 のステートレスアドレス自動設定において用いるパケット。
Route Injection	ネットワークおよびホストのルーティングプロセスに、スタティックルートを自動的に組み込む機能。
SLAAC	StatelessAddressAutoConfiguration の略。IPv6 における自動アドレス構成を実現する方法で、ルータ広告で配布される prefix 設定から自身で自動的に IPv6 アドレスを生成する。
SNMP	Simple Network Management Protocol の略。通信機器をネットワーク経由で監視・制御するためのプロトコル。
Solicit	DHCPv6 においてクライアントがサーバの場所を突き止めるためのメッセージ。
SSH	Secure Shell の略。ネットワークを介してコンピュータにログインしたりコマンドを実行したりするためのプログラム。

用語	内容
TFTP	Trivial File Transfer Protocol の略。コンピュータ間でファイルを転送するためのプロトコル。
TLV	Type-Length-Value の略。CM のコンフィグレーションファイル内に書かれるメッセージデータ、およびそれを格納するフィールドの指定形式。
UDC	Upstream Drop Classifier の略。CM における上り方向のパケットフィルタとして用いられる。
VLAN	Virtual LAN の略。仮想的な LAN 接続を意味し、物理的な 1 つのスイッチ上に、複数の LAN を構成できる仕組み。
VoD	Video on Demand の略。
Wi-Fi	無線 LAN 機器が標準規格である IEEE 802.11 シリーズに準拠していることを示すブランド名。
チャネルボンディング	DOCSIS3.0 で導入された高速化技術。256QAM では 1 チャンネル(6MHz 幅)あたり 42Mbps が上限となるが、複数のチャンネルを使って同時伝送する。ワイドバンドと呼称される場合もある。
不正 DHCP server 対策	ネットワーク上に不正に接続された DHCP サーバを防止すること。例：CE-Router の逆接続など不正な DHCP サーバがネットワーク上にあると、加入者は意図しないサーバから IP アドレスを払い出されることとなり、加入者のインターネット接続が不安定になる。

1.4 参考文献

- DOCSIS®1.0 ANSI/SCTE 22-1 2002R2007,22-3 2002R2007
- DOCSIS®1.1 CM-SP-RFIv1.1-C01-050907,OSSIv1.1-C01-050907
- DOCSIS®2.0 CM-SP-RFIv2.0-C02-090422,OSSIv2.0-C01-081104,IPv6-I01-090518
- DOCSIS®3.0 CM-SP-MULPIv3.0-I19-120809,OSSIv3.0-I19-120809
- RFC2131　Dynamic Host Configuration Protocol
- RFC3315　Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC3633　IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6
- RFC4649　Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option

- RFC5007　DHCPv6 Leasequery
- RFC5460　DHCPv6 Bulk Leasequery
- RFC6145　IP/ICMP Translation Algorithm
- RFC6146　Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers
- RFC6333　Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion
- RFC6877　464XLAT: Combination of Stateful and Stateless Translation
- RFC7596　Lightweight 4over6: An Extension to the Dual-Stack Lite Architecture
- RFC7597　Mapping of Address and Port with Encapsulation (MAP-E)
- RFC7599　Mapping of Address and Port using Translation (MAP-T)
- RFC8106　IPv6 Router Advertisement Options for DNS Configuration
- RFC8273　Unique IPv6 Prefix per Host
- RFC8415　Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- 情報処理学会デジタルプラクティス掲載論文「クライアント OS の IPv6 実装検証から見たネットワーク運用における課題の考察」
- 一般社団法人 日本インターネットプロバイダー「ブロードバンド関連用語の標準化に向けた検討会」

第2章　ガイドラインの対象者と適用範囲

2.1　ガイドラインの対象者

本ガイドラインでは、以下のようにケーブル事業者はもちろんのことケーブルインターネットの設備構築やシステム運用を請負うシステムインテグレータやネットワークインテグレータまで、ある程度広い範囲をガイドラインの対象としており、特にケーブルインターネットの設計や構築、運用保守を行う技術者を対象者としている。

(1)　ケーブル事業者（MSO 含む）

(2)　行政が運営するケーブル事業

(3)　ケーブルインターネット接続用設備の構築・運用事業会社

- ケーブルインターネットシステムインテグレータ
- ネットワークインテグレータ

(4)　その他上記以外のケーブルインターネットに関連する事業者

2.2　適用範囲

2.2.1　適用範囲

本ガイドラインでは、ケーブル事業者のネットワークを IPv6 対応にするために必要な技術仕様を策定するため、DOCSIS および PON を用いたインターネットアクセスサービスを対象としている。対象サービスの適用範囲を第 4 章に示す。

サービスモデルは、ケーブル事業者が通常サービスとして提供していると想定される方式について言及しており、法人向けサービスなどの特殊なケースは言及しない。

2.2.2　適用範囲外としたケース

本ガイドラインでは以下のケースを適用範囲外とする。

(1) DOCSIS 以外の非標準ケーブルモデムシステム

(2) DOCSIS、PON 以外の通信サービスや集合住宅向けソリューション

- G.hn や LAN 配線方式、EoC

(3) フレッツネクストなどのホールセラーを使ったサービス

(4) インターネットアクセス以外の通信サービス

- IP 電話サービス
- VoD など放送サービスに関する通信機能 など

本ガイドラインは、0AB-J IP 電話や VLAN・専用線サービスなど基本的にインターネット接続性のないサービスは適用範囲外とする。また、標準規格に準拠あるいは参照して作成しており、ルータや CPE の仕様はそれに準拠していることを前提としている。

2.3 本ガイドラインと外部団体との連携について

本ガイドラインは、IPv6 普及・高度化推進協議会のサブワーキンググループとして活動している IPv6 家庭用ルータ SWG と意見交換を行い策定している。

2.3.1 IPv6 家庭用ルータ SWG について

IPv6 家庭用ルータ SWG の趣旨は「インターネット利用者がスムーズに IPv6 環境に対応できるように ISP の IPv6 サービス提供に必要な家庭内ルータ機能のベースライン（最小限の共通認識）をインターネット利用者の視点からまとめる」ことであり、国内の主要な家庭用ルータメーカが参加している。

IPv6 普及・高度化推進協議会と IPv6 家庭用ルータ SWG で策定される「IPv6 家庭用ルータガイドライン」については、次のリンクから確認ができる。

- IPv6 普及・高度化推進協議会のホームページ
  http://www.v6pc.jp/jp/index.phtml
- IPv6 家庭用ルータ SWG の詳細
  http://www.v6pc.jp/jp/wg/coexistenceWG/v6hgw-swg.phtml

2.3.2 連携の背景

ケーブルインターネット環境での DHCPv6-PD 方式は、国際標準に準拠しない、もしくは国際動向を把握しない形で独自の IPv6 サービス設計が行われていたため、市販されている CE-Router がケーブル事業者の想定する動作を行わないケースが確認されていた。

そこで、DHCPv6-PD 方式をサポートした市販 CE-Router が増加してきている状況を踏まえ、日本ケーブルラボと IPv6 家庭用ルータ SWG とで、DHCPv6-PD 方式提供時の適切な動作仕様について、合同でとりまとめを行った。

2.3.3 連携による効果

IPv6 家庭用ルータ SWG には国内の主要な家庭用ルータメーカが参加しているため、ケーブル事業者は本ガイドラインに従うことで、ケーブルインターネットと市販 CE-Router の仕様の整合性を保つことが可能となり、市販 CE-Router を活用できる可能性が広がる。

第3章　IPv6 の概要

IP（Internet protocol）は、インターネットに接続するために必要なプロトコル（手順）である。これまでは IPv4 アドレスが利用されてきたが、近年、インターネットが世界的に普及したことにより、アドレス枯渇問題が取り出されてきた。IPv6 は IPv4 の持つ根本的なアドレス空間問題を解決し、人のインターネットから IoT 等の物のインターネットにシフトする現在において、非常に重要かつ必要なインターネットプロトコルといえる。

なお、IPv4 と IPv6 は互換性がないため、相互に通信する必要がある場合はトランスレーション（変換）する機器や仕組みが必要となる。また、IPv4 前提で作られたプログラムでは IPv6 の処理ができない問題などが発生するため考慮が必要である。

3.1　IPv6 の基礎

3.1.1　IPv6 アドレスについて

インターネットに接続している機器には、一意の識別番号（IP アドレス)を設定して通信するのが基本である（ルータ等の機器を用いて、1 つの IP アドレスを複数の機器で共有することはありえる)。この IP アドレスは、一般的に広く利用されている IPv4（IP バージョン 4）では 32 ビット幅、IPv6（IP バージョン 6）では 128 ビット幅で構成されている。そもそも IPv6 が開発された経緯は、IPv4 環境において機器に割り当てる IP アドレスが不足することが予想されたためである。

IPv4 アドレスの絶対数は約 43 億個（2 の 32 乗）であり、インターネットが通信基盤のひとつとなって世界中で利用されている。現在の 70 億を越える世界人口を考えてみてもその不足は明らかであり、新たな IPv6 の 128 ビットというアドレス幅（約 340 澗個）は、今後のインターネットの発展による接続機器の増大にも十分に耐えられるよう考慮され決定されている。

3.1.2　IPv4 アドレスの課題

- 機能の仕組みが複雑になった

  現在主流となっているインターネット利用用途や規模が、IPv4 アドレス決定時に想定できていないことから、機能の追加やサービス構築が複雑化している。

  例）セキュリティ対策

  　　マルチキャスト型情報配信

- ネットワークの仕組みが複雑になった

  IP アドレス割り当てを節約する必要性から、ネットワーク構成が複雑化しアプリケーション利用に支障が出ている。

  IP アドレスブロックの分割により、ネットワーク管理者にとっては監視しづらい、利用者にとっては機器設定が複雑となる。

例）細かな IP アドレスブロックの分割
アドレス変換（NAT）技術

3.1.3 IPv6 アドレスの概略

3.1.3.1 IPv6 アドレスの種類

IPv6 アドレスは IPv4 アドレスと同じく、機器の持つネットワークインタフェースに付与される。1 つのインタフェースに複数の IPv6 アドレスが付与されることも、複数のインタフェースに単一の IPv6 アドレスが付与されることもあり、次の 3 種類に分類される。なお、IPv6 は IPv4 とは異なり、ブロードキャストアドレスは存在せず、マルチキャストアドレスが同様の役割を果たす。

(1) ユニキャストアドレス
単一インタフェースの識別番号で、ユニキャストアドレス宛のパケットはそのアドレスを持つインタフェースに配送される。

(2) エニーキャストアドレス
インタフェースの集合の識別番号で、一般的には複数の別機器に付与される。エニーキャストアドレス宛のパケットは、そのアドレスを持つ「一番近くにある」機器のインタフェースに配送される。エニーキャストアドレスはユニキャストアドレス空間から割り当てられ、表記上、エニーキャストアドレスとユニキャストアドレスの区別はつかない。

(3) マルチキャストアドレス
インタフェースの集合の識別番号で、通常は別の機器となる。マルチキャストアドレス宛のパケットはそのアドレスを持つすべてのインタフェースに配送される。

3.1.3.2 IPv6 アドレスの表記法

IPv4 アドレスでは、32 ビットを 8 ビットずつ 4 つに“.” （ピリオド)で区切った数値列を“192.168.0.1”のように 10 進数で記述される。対して IPv6 アドレスでは、128 ビットを 16 ビットずつ 8 つに“:”（コロン)で区切った数値列を、16 進数で表記する。IPv4 に比べ、2 の 96 乗倍の大きさとなるアドレス空間を扱うことが可能となる。連続する“0”は省略可能で、“::”は 16 ビットの 0 が複数連続していることを示す。

例：

2001:0db8:0000:0000:0008:0800:200c:417a （省略）→　2001:db8:0:0:8:800:200c:417a
2001:db8:0:0:8:800:200c:417a （省略）→　2001:db8::8:800:200c:417a

これにより長い IPv6 アドレスを短く表記することができる。また、IPv6 アドレス Prefix の表記法は IPv4 における CIDR 表記と同一であり、「[IPv6 アドレス] ／ [Prefix 長]」のように表記し、IPv6 アドレスと Prefix を同時に表記することもある。

例：

2001:0db8:0:cd30:123:4567:89ab:cdef/60 というアドレス表記は

ノードアドレス　2001:db8:0:cd30:123:4567:8 9 ab:cdef

サブネット番号　2001:db8:0:cd30::/60

を同時に表記する。

3.1.3.3 IPv6 アドレスの型

IPv6 アドレスは、上位ビットにより、未指定アドレス、ループバックアドレス、マルチキャストアドレス、リンクローカルユニキャストアドレス、およびグローバルユニキャストアドレスに分類される。

例：

アドレスの型	表記
未指定（Unspecified）	::/128
ループバック	::1/128
マルチキャスト	ff00::/8
リンクローカルユニキャスト	fe80::/10
グローバルユニキャスト	上記以外

3.1.3.4 パケット形式

IPv4 アドレスと IPv6 アドレスはパケット形式やプロトコルが備える機能が異なる。パケットヘッダーの全体長が可変だった IPv4 に比べ、IPv6 は 40 バイトに固定されている。それは、ヘッダー内容を簡素化することにより、ネットワーク機器処理効率の向上が可能となるためである。

3.1.3.5 クライアントの IP アドレス

IPv4 では 1 つのインタフェースに対して 1 つの IPv4 アドレスしか持てなかったが、IPv6 においては、1 つのインタフェースに、Link Local Address やグローバルユニキャストアドレスなど、同時に複数の IPv6 アドレスを持つことが可能となった。

3.2 IPv6 払い出し方式

IPv6 においてクライアント端末へのアドレス払い出しの方法は複数あるが、運用上使われるケースが多い手法は、ネットワーク機器自体が Prefix を払い出す SLAAC（StateLess Address AutoConfiguration)方式と、DHCPv6 サーバー（機能）を利用し、サーバからアドレスを払い出すステートフル DHCPv6 方式の 2 つがある。

SLAAC では、ルータ広告（RA : Router Advertisement）に含まれる Prefix 情報（PIO : Prefix Information Option）を利用し、クライアントの MAC アドレスをもとにアドレスを生成する（現在はセキュリティの観点から MAC アドレスをもとにした生成は推奨されていない）。加入者宅内に CE-Router がある場合、事業者が管理するアドレスは CE-Router の WAN 側アドレスのため、CE-Router が接続端末に対して SLAAC でアドレス配布することは問題ない。スマートフォンなどのモバイル端末は、OS によっては、SLAAC でないと接続できない端末があるため、CE-Router の選定、設定時に注意が必要である。

SLAAC の概要を図 3.1 に示す。RA は NDP（Neighbor Discovery Protocol）の 1 つで、NDP には NS（Neighbor Solicitation）や NA（Neighbor Advertisement）、RS（Router Solicitation）が含まれるがここでは詳細な説明は割愛する。

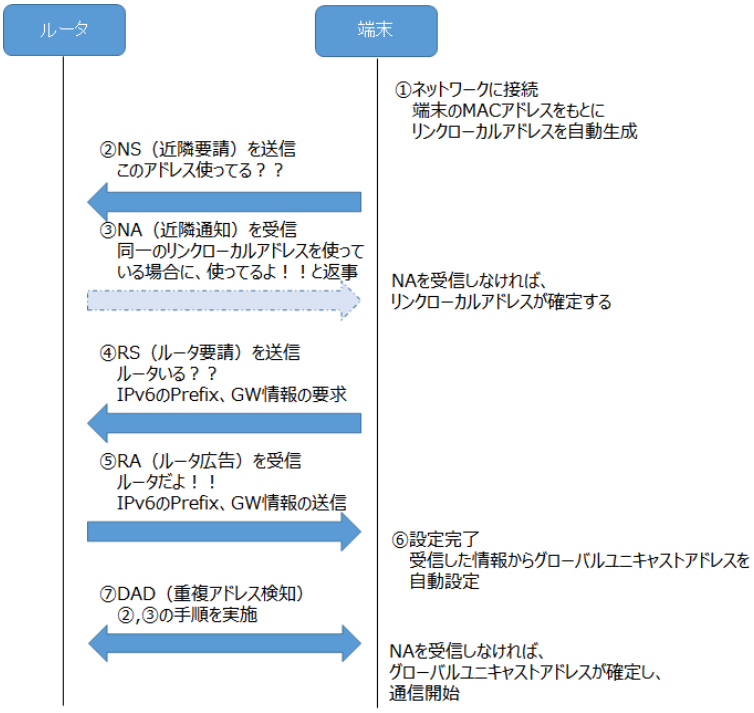


図 3.1 SLAAC の概要

ステートフル DHCPv6 では、クライアントが RA の M フラグ（Managed Flag）を受信した場合に、DHCP クライアントとしてアドレス要求を行う。アドレス要求には IA_NA オプション、または IA_PD オプションを使用する。DHCPv6 サーバに対して、IA_NA オプションで要求した場合は、クライアント（ノード）アドレスを要求するが、IA_PD オプションで要求した場合は、Prefix（ネットワーク）を要求する。なお、RA のフラグにはもう 1 つ O フラグ（Other Flag）が存在するが、こちらは IPv6 アドレス以外のパラメータ（DNS 等）を DHCPv6 から取得するか否かを指定するものである。

ステートフル DHCPv6 の概要を図 3.2 に示す。

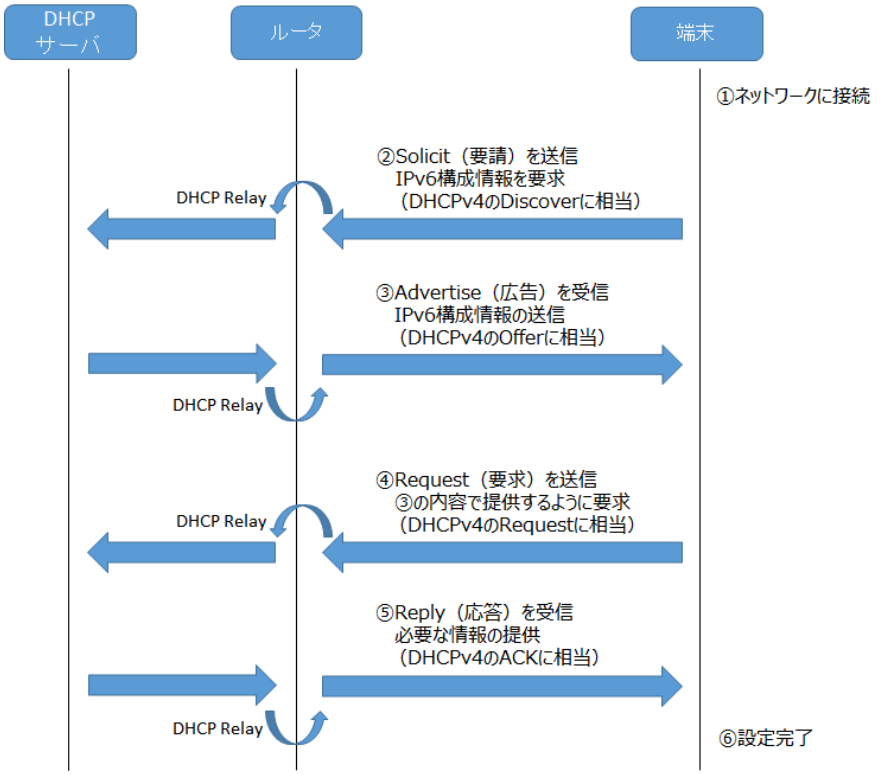


図 3.2 ステートフル DHCPv6 の概要

IA_NA オプションを利用する方式は、DHCPv6 方式と呼ばれ IPv4 アドレスと同様の方式であり、ネットワーク構成としては簡易的である。しかし、IPv4 から IPv6 へアドレス枯渇対策とはなるが、アドレス形態としてはインテグレーションがされていない。今後の多種多様な機器がネットワークに接続されることを考えると、管理するアドレス数が非常に多くなる可能性がある。加入者の IP アドレスは DHCP から割り振られるが、IPv6 の仕様上、基本的にはすべてグローバルアドレスとなる。これにより、ネットワーク内部の構成が予測される可能性がある。その点に抵抗のある事業者では、NAT66 の導入を検討する可能性があり、IETF で非推奨とされている NAT66 を助長する懸念がある。また、セキュリティに関しては、1.2 に記載した通りであり、セキュリティ上のリスクも高いため、IA_PD オプションを想定した設計が望ましい。

IA_PD オプションを利用する方式は、DHCPv6-PD 方式と呼ばれ、加入者宅 CE-Router に対し Prefix を割り当て、CE-Router から配下の端末へアドレス配布を行う。事業者が管理すべきアドレスは CE-Router に通知する Prefix のみであり、IA_NA（DHCPv6）と違い接続端末すべてのアドレスを管理する必要がない。PE-Router が DHCP Snooping することで、加入者使用 IPv6 アドレスの Prefix を確認することによりユーザトレースが可能で

ある。CE-Router にて DHCPv6-PD の設定が必要で、CE-Router によっては DHCPv6-PD に対応していない機種も存在するため CE-Router の選定には注意が必要である。

3.3 IPv6 管理手法

クライアントに対する IPv6 DNS アドレスの通知方法については、これまでは DHCPv6 による通知が基本であった。しかしながら、Android など一部のデバイスや OS が DHCPv6 に対応していないことから、RDNSS（Recursive DNS Server）オプションを利用し、RA で DNS アドレスを通知することも可能となってきている。

IPv4 の DHCP においては DHCP リレーエージェントの情報（リモート ID）を DHCP 要求に付加するオプションとして Option82 が用いられるが、DHCPv6 においてはリモート ID を DHCP サーバ側に伝達する手段として Option18/Option37 が RFC4649 に定義されているので運用に注意が必要である。

第4章　CATV における IPv6 ネットワーク概要

4.1　定義

4.1.1　IPv6 ネットワーク概要

ケーブルテレビにおけるネットワークを図 4.1 に示す。ケーブルインターネットは上位ネットワーク、サーバ、アクセス網で構成されており、各構成要素の概要は 4.1.2　以降で解説する。

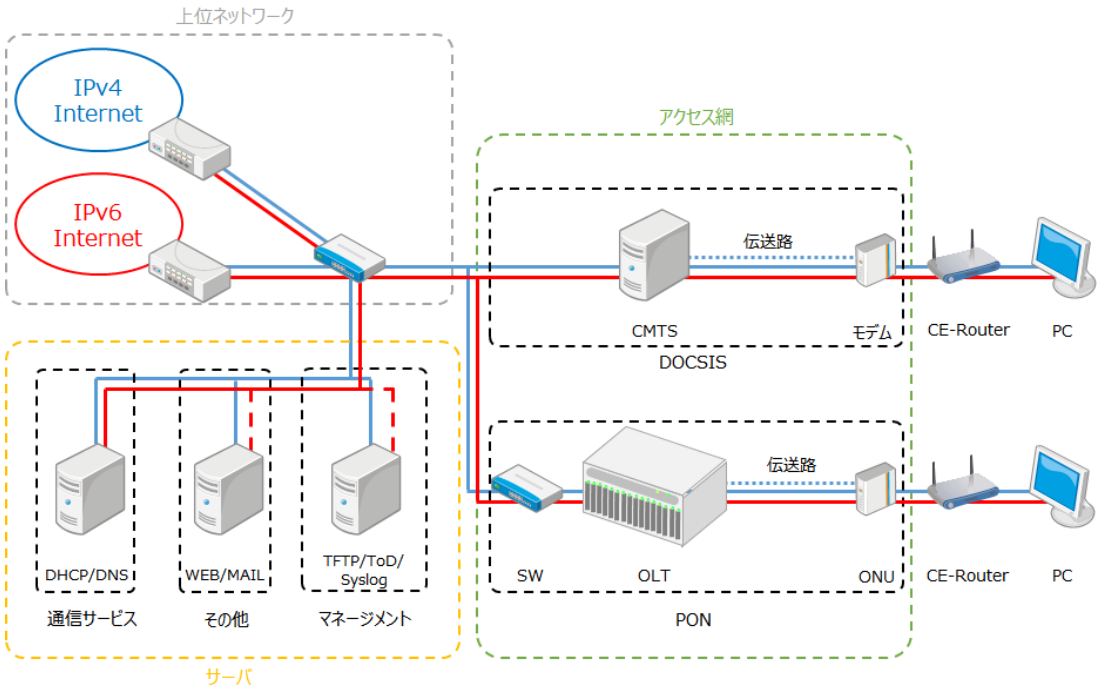


図 4.1 ケーブルインターネットの概要図

4.1.2　IPv6 ネットワーク設計

本書では、IPv6 アドレスの払い出し設計やルーティング、DNS などユーザ端末のネットワークへの接続性に関する設計や、オペレーションに必要なユーザトレースなどの留意事項を「IPv6 ネットワーク設計」として第 5 章に記載する。

4.1.3　アクセス網

(1) DOCSIS 構成

DOCSIS におけるアクセス網の定義範囲は図 4.1 に示したとおりである。DOCSIS の場合は一般的に CMTS が L3 動作を行うため CMTS から CM までがアクセス網となる。詳細は第 6 章に記載する。

(2) PON 構成

PON におけるアクセス網の定義範囲は図 4.1 に示したとおりである。OLT は L2 機器が多いため、L3SW までがアクセス網となる。CMTS-CM の役割を L3SW-OLT/ONU の組み合わせで実現するため、L3SW に要求される MAC アドレス数の設計やアクセス網内のセキュリティ機能を L3SW と OLT/ONU のどちらで持たせるのかなどの考慮が必要である。OLT は、筐体に L2、L3 機能を搭載する機器もあるため、FTTH ベンダおよびネットワークベンダと相談してネットワーク構成の検討および機器の選定することが望ましい。詳細は第 7 章に記載する。

4.1.4 上位ネットワーク

上位ネットワークの定義範囲は図 4.1 に示したとおりである。

(1) DOCSIS の場合

上位ネットワークは CMTS より上位のネットワークを指し、ISP や IX 等に接続されるネットワークを指す。

(2) FTTH の場合

OLT に接続される L3 よりも上位のネットワークを指し、ISP や IX 等に接続されるネットワークを指す。

4.1.5 サーバ

(1) 通信サービス用サーバ

DHCP や DNS サーバ等、通信サービスの提供に直接必要となるサーバである。IPv6 化にあたっては、DHCP サーバ、DNS サーバの IPv6 対応は欠かせない。しかし、デュアルスタック環境の DNS キャッシュサーバは、AAAA レコードの管理ができていれば、DNS リクエストを IPv4 で受け付ける設計とすることも可能である。

(2) マネージメント用サーバ

マネージメント系サーバとは、TFTP/ToD/Syslog サーバ等ユーザの通信サービス提供に間接的に必要となるサーバである。

(3) その他サービス用サーバ

その他サービス用サーバとは、Web サービスや Mail サービス等インターネット接続以外の通信サービス以外に用いられるサーバである。

4.2 Internet Protocol によるネットワーク分類

本ガイドラインでは、ケーブルインターネットのアクセス網で用いられる Internet Protocol（IPv4/IPv6）で、IPv4 シングルスタックと IPv4/IPv6 デュアルスタック、IPv6 シングルスタックを分類する。

(1) IPv4 シングルスタック

アクセス網を IPv4 のみで構築したネットワークであり、ユーザには IPv4 接続環境を提供する。IPv6 接続環境は提供されない。

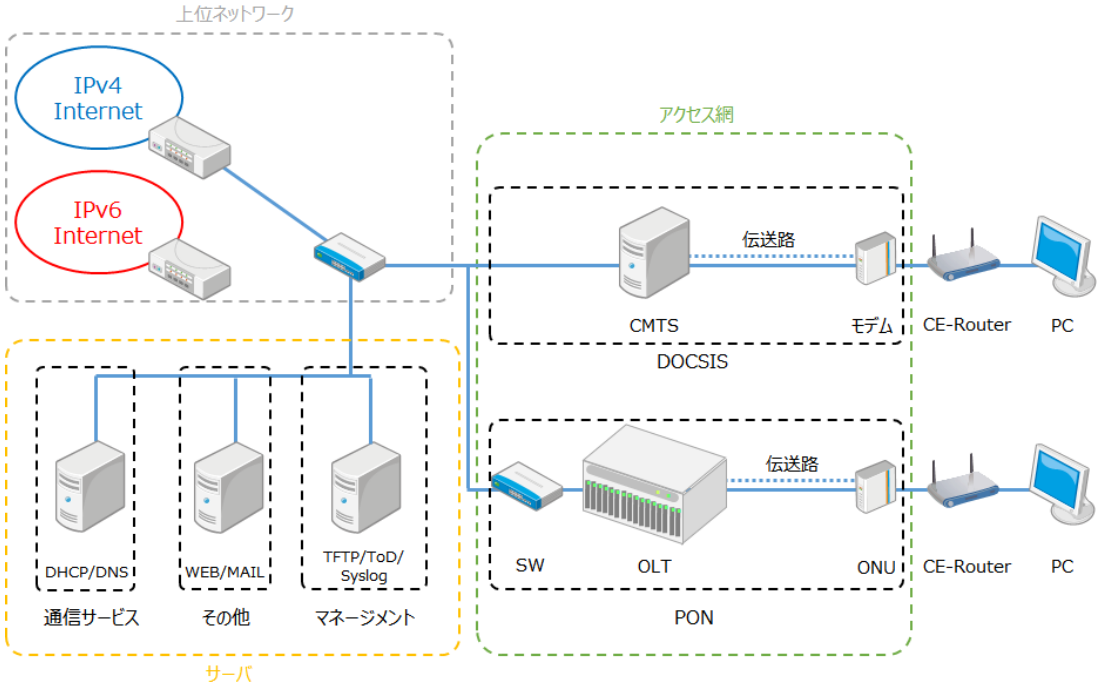


図 4.2 IPv4 シングルスタック

(2) IPv4/IPv6 デュアルスタック

アクセス網を IPv4 と IPv6 を共存させて構築したネットワークであり、ユーザには IPv4 接続環境と IPv6 接続環境を提供する。

なお、上位ネットワークと DHCP/DNS サーバについても、IPv4 と IPv6 を共存させて構築する必要がある。その他サーバについては、運用に合わせた構築が必要となるため、本ガイドラインでは考慮しない。

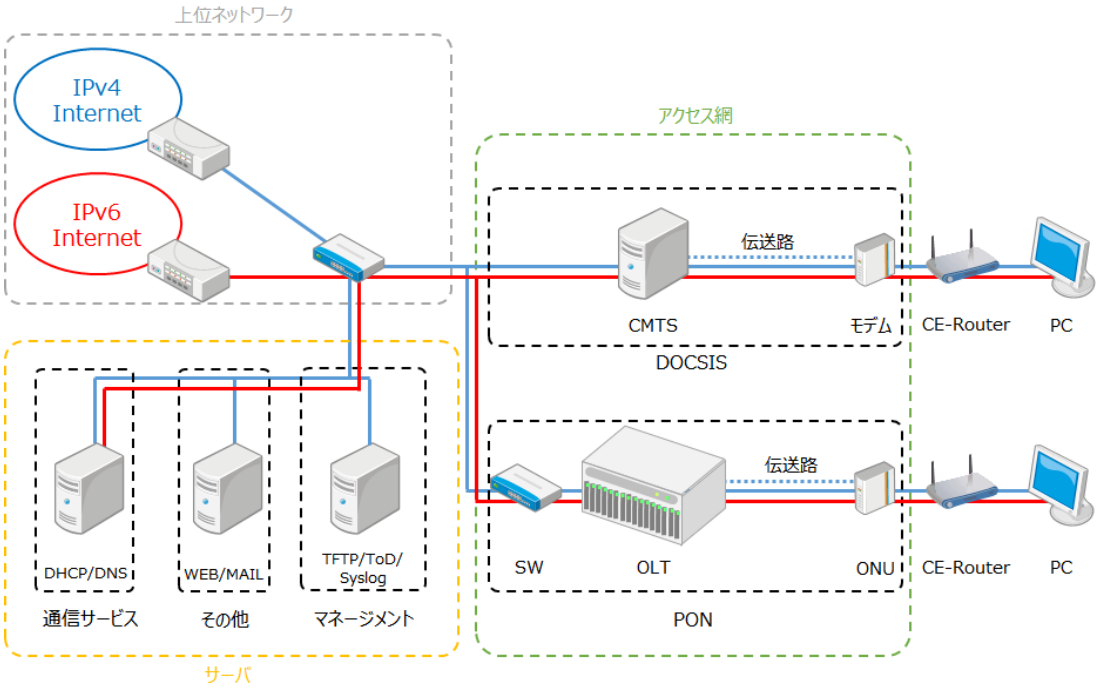


図 4.3 IPv4/IPv6 デュアルスタック

(3) IPv6 シングルスタック

アクセス網を IPv6 のみで構築したネットワークであり、ユーザには IPv4 接続環境と IPv6 接続環境を提供する。IPv4 ネットワークへの接続性は、IPv4 over IPv6 通信技術を用いて提供することが一般的である。本ガイドラインでは、IPv6 シングルスタック上で IPv4 接続を提供する技術を IPv4 over IPv6 通信技術と総称する。IPv4 over IPv6 通信技術の詳細は、第 8 章に記載する。

なお、上位ネットワークと DHCP/DNS サーバについても、IPv4 と IPv6 を共存させて構築する必要がある。その他サーバについては、運用に合わせた構築が必要となるため、本ガイドラインでは考慮しない。

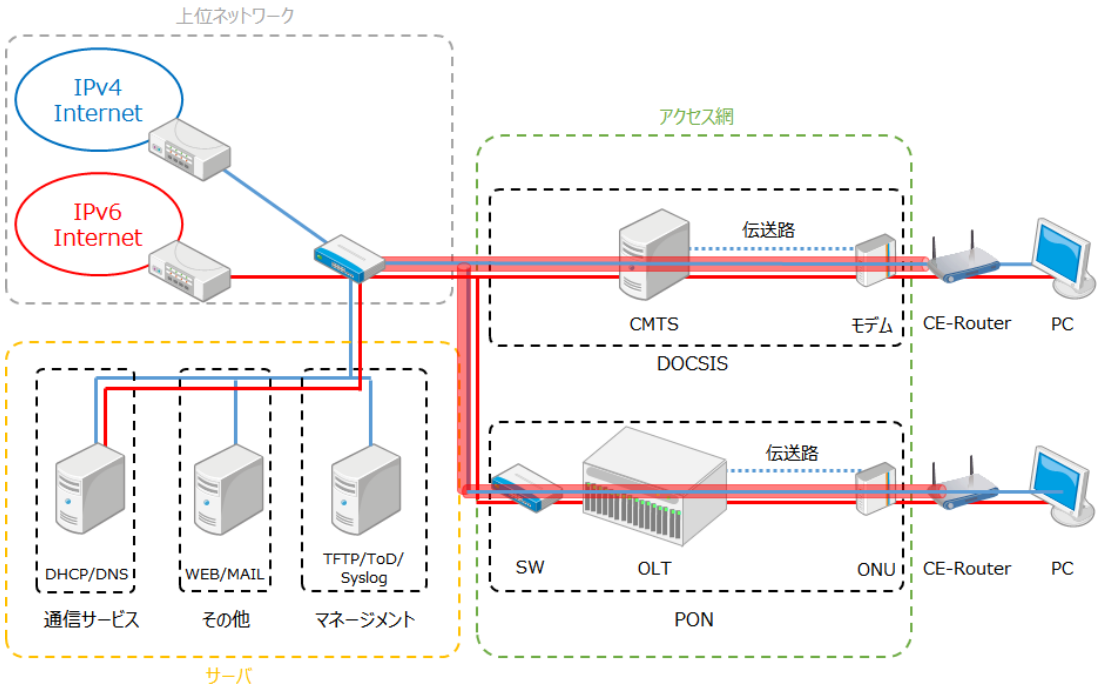


図 4.4 IPv6 シングルスタック

第5章　IPv6 ネットワーク設計

5.1　インフラ設計

本章では主にケーブルインターネットの IPv4 ネットワークで用いられている同一 L2 リンク内での DHCP 環境において、デュアルスタックにて IPv6 ネットワークを構築する場合の IP アドレス配布方式について述べる。

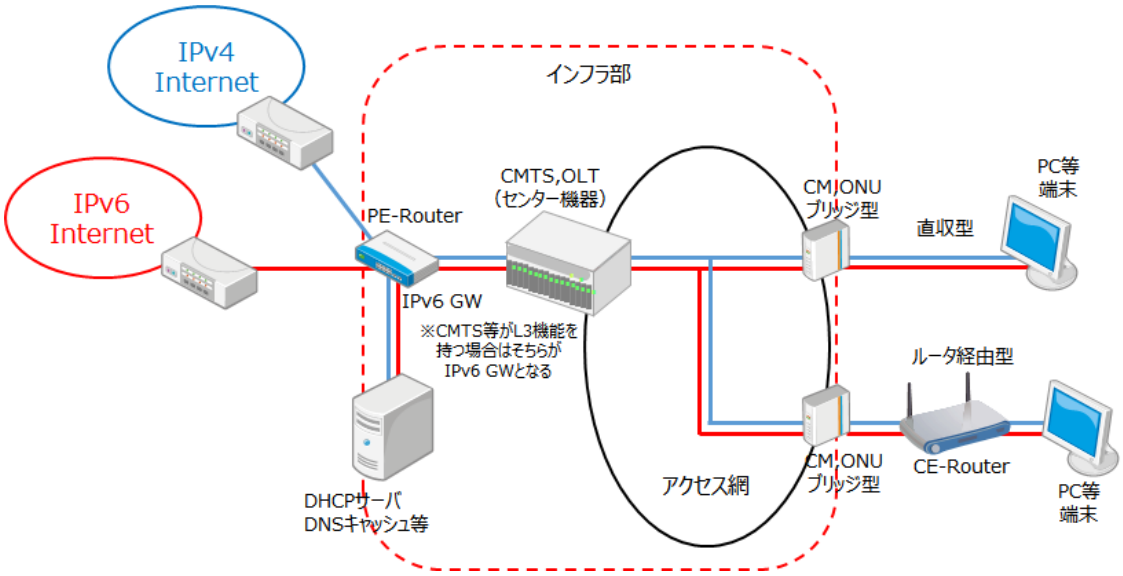


図 5.1 想定するネットワーク構成

IPv6 ネットワークでの IP アドレスの配布方法は、基本的に DHCP で完結していた IPv4 と異なり、DHCPv6（IA_NA）、DHCPv6-PD（IA_PD）、SLAAC 等の複数の設定方法が規定されている。また、基本的に NAT を行わずグローバルユニキャストアドレスを端末まで付与しルーティングする必要がある。近年では無線 LAN の普及によりユーザ側に無線 LAN ルータ等の CE-Router（Customer Edge Router）が設置されていることが多く、ルータ配下の端末まで IPv6 グローバルユニキャストアドレスを配布するためには CE-Router の実装機能との組み合わせを考慮してインフラ側の仕様を決定する必要がある。

以下に「IPv6 家庭用ルータ SWG」にて想定されているインフラ側機能とルータ機能の組み合わせを表 5.1 に示し、各ケースの詳細を表の下に記載する。

本ガイドラインとしては、ケース 1 およびケース 2 を推奨ケースとする。

表 5.1 インフラ側機能とルータ機能の組み合わせ

		ケース 1	ケース 2	ケース 3
インフラ側	DHCPv6 （IA_NA）	○	×	×
	DHCPv6-PD （IA_PD）	○	○	○
	RA フラグ等	M/O※1	M/O	M/O
	事業者のアドレス管理	IA_NA、 IA_PD	IA_PD	IA_PD
ユーザ側	CE-Router WAN 側アドレス	IA_NA※2 LLA※3	LLA	IA_PD（Prefix 長 /64） LLA
	CE-Router LAN 側アドレス	IA_PD※4	IA_PD	IA_PD
	CE-Router 実装機能	IA_NA、 IA_PD	IA_PD	IA_PD

		ケース 4	ケース 5	ケース 6
インフラ側	DHCPv6 （IA_NA）	×	○	×
	DHCPv6-PD （IA_PD）	○	×	×
	RA フラグ等	M/O,PIO※5	M/O	M/O,PIO
	事業者のアドレス管理	IA_NA、RA PIO	IA_NA	RA PIO
ユーザ側	CE-Router WAN 側アドレス	SLAAC※6 LLA	IA_NA LLA	SLAAC LLA
	CE-Router LAN 側アドレス	IA_PD	ULA※7	SLAAC
	CE-Router 実装機能	IA_PD	IA_NA、 NAT66	ND-Proxy

出展：IPv6 家庭用ルータ SWG 資料

※1 RA の Managed フラグと OtherConfig フラグが両方ともオンになっていることを示す
※2 DHCPv6 によって取得するグローバルユニキャストアドレス
※3 自動生成されるリンクローカルアドレス
※4 DHCPv6-PD によって取得する Prefix から生成されるアドレス
※5 RA の Prefix Information Option。SLAAC 動作に必要な Prefix を渡す。
※6 Stateless Address Auto Configuration
※7 ユニークローカルアドレス

(1) ケース 1

インフラ側では DHCPv6（IA_NA）と DHCPv6-PD（IA_PD）が両方とも動作しているが、RA に PIO を含まないため SLAAC は動作しない。

この設計の意図として、DHCPv6（IA_NA）と DHCPv6-PD（IA_PD）を両方とも動作させることで端末の CE-Router 接続と CE-Router を設置しない回線直収を両方とも考慮している。また CE-Router の機能実装にもよるが、WAN 側にもグローバルユニキャストアドレスを持つため、CE-Router 自体の遠隔管理などの管理に活用できる。

CE-Router を使用していても IPv6 ブリッジなどの IPv6 ブリッジ接続機能を使用しているユーザの場合は CE-Router を設置しない回線直収と同様に DHCPv6（IA_NA）で接続可能である。ただし DHCPv6 に対応していない端末も存在するため留意が必要である。

インフラ側で SLAAC を動作させないことによりユーザトレーサビリティや IP ソースガード等の運用面も考慮している。

本ガイドラインの推奨ケースとする。

(2) ケース 2

インフラ側では DHCPv6-PD（IA_PD）のみ動作している。DHCPv6（IA_NA）と SLAAC は動作しない。

実質的に DHCPv6-PD（IA_PD）対応の CE-Router 経由での接続のみの考慮となり、CE-Router を設置しない回線直収（IPv6 ブリッジ含む）での端末接続は考慮しないことになる。ユーザへの CE-Router の提供に課題はあるものの、ユーザトレーサビリティや IP ソースガードについては DHCPv6-PD（IA_PD）で割り当てた Prefix のみを対象として運用すれば良いため管理性に優れるといえる。ただし CE-Router の WAN 側アドレスは自動生成された Link Local Address となり CE-Router 自体の遠隔管理に不都合をきたす懸念がある。

インフラ側で SLAAC を動作させないことによりユーザトレーサビリティや IP ソースガード等の運用面も考慮している。

本ガイドラインの推奨ケースとする。

(3) ケース 3

インフラ側では DHCPv6-PD（IA_PD）のみ動作している。DHCPv6（IA_NA）は動作せず、CE-Router の WAN 側には、LAN 側と同じく PD Prefix によりアドレス生成を実施し、Prefix 長は/64 で配布する。ケース 3 の方式の場合、ケース 2 と同様に回線直収は考慮されておらず、PE ルータに DHCPv6（IA_PD）を実装する必要がある。CE-Router を介さずに加入者が端末を直結すると、ユーザトレースができなくなることが課題となる。

(4) ケース 4

インフラ側では DHCPv6-PD（IA_PD）と SLAAC が動作している。DHCPv6（IA_NA）は動作しない。

CE-Router の WAN 側は RA PIO で取得した Prefix から SLAAC により自動生成される。LAN 側は DHCPv6-PD（IA_PD）で取得した Prefix から生成されることを想定している。

インフラ側で SLAAC が動作しているため、端末を回線直収した場合にステートレスなグローバルユニキャストアドレスで接続されてしまうためユーザトレーサビリティや IP ソースガードの観点で課題がある。

(5) ケース 5

インフラ側では DHCPv6（IA_NA）のみ動作している。DHCPv6-PD（IA_PD）は動作しておらず、CE-Router の LAN 側ネットワークを ULA（ユニークローカルアドレス）で構築することを想定している。

ULA はプライベートなネットワーク空間内のみでの使用が想定された IPv6 アドレス帯であり、インターネット空間へのルーティングは禁止されている。そのため CE-Router ではルーティングではなく NAT66 を行う必要がある。NAT66 は IETF でも推奨されていない上、「IPv6 家庭用ルータ SWG」でもベンダ独自仕様になる可能性が高いという見解もある。

(6) ケース 6

CE-Router の WAN 側、LAN 側とも SLAAC により IP アドレスが生成される。WAN 側 LAN 側が同一 Prefix となりルーティングは行われないが、ND-Proxy により WAN 側と LAN 側の Neighbor Discovery に代理応答することにより通信が可能となっている。IPv6 ブリッジとは異なり CE-Router でパケットフィルタリングが行えることが利点であり、ただし日本では電話系事業者回線で利用されているが、日本特有の実装である。

SLAAC でのアドレス生成となるためケーブルインターネットではユーザトレーサビリティや IP ソースガードの観点で課題がある。

5.2 利用者側設備のネットワーク管理

本ガイドラインの推奨ケースであるケース 1、ケース 2 について、CE Router 実装機能（IA_NA・IA_PD）の違いや回線直収（IPv6 ブリッジも含む）の場合の想定されるネットワーク情報取得動作の違いについてまとめる。

説明にあたり、利用者側設備から見て IPv6 ゲートウェイとなる同一リンク上のインフラ側装置（CMTS、L3 機能付き OLT、L3SW 等）をまとめて「PE-Router」と呼称する。

(1) ケース 1 のインフラ設計の場合

- CE-Router（IA_NA・IA_PD 機能有り）経由で端末を接続する場合

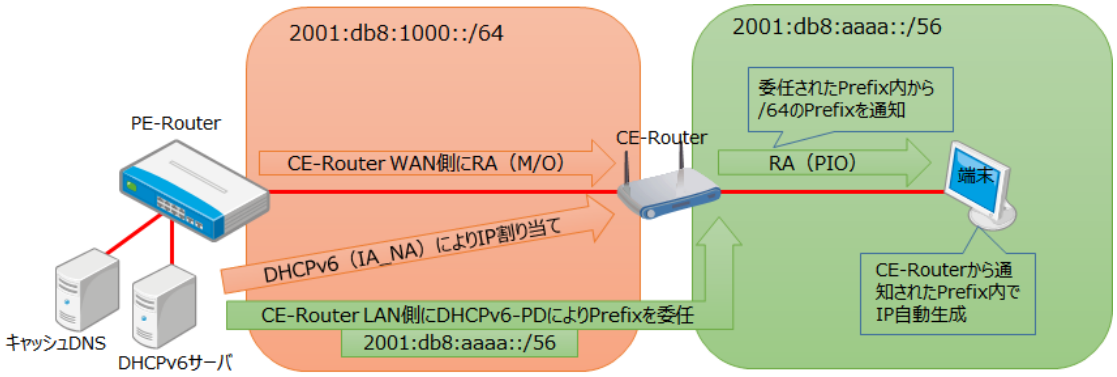


図 5.2 CE-Router（IA_NA・IA_PD 機能有りの構成

この場合の CE-Router、端末に設定されるネットワーク情報は表 5.2 のとおりとなる。

表 5.2 ケース 1 と CE-Router（IA_NA・IA_PD 機能有り）の組み合わせ

CE-Router	WAN 側 IP アドレス	・LLA ・DHCPv6 （IA_NA）サーバにより割り当てられるグローバルユニキャストアドレス
	LAN 側 IP アドレス	・LLA ・DHCPv6-PD により委任された Prefix 内から生成
	デフォルトゲートウェイ	・PE-Router の LLA が設定される（RA から取得）
	遠隔管理	WAN 側のグローバルユニキャストアドレスは、ユーザトレースによりユーザとの紐づけが可能であるので、遠隔アクセスが可能
端末	IP アドレス	・LLA ・CE-Router から通知された Prefix 内で SLAAC により生成
	デフォルトゲートウェイ	・CE-Router LAN 側の LLA が設定される（RA から取得）
キャッシュ DNS 情報		・RA 内の RDNSS オプションから取得 ・CE-Router は DHCPv6 サーバからも取得可能

- CE-Router（IA_PD 機能のみ）経由で端末を接続する場合

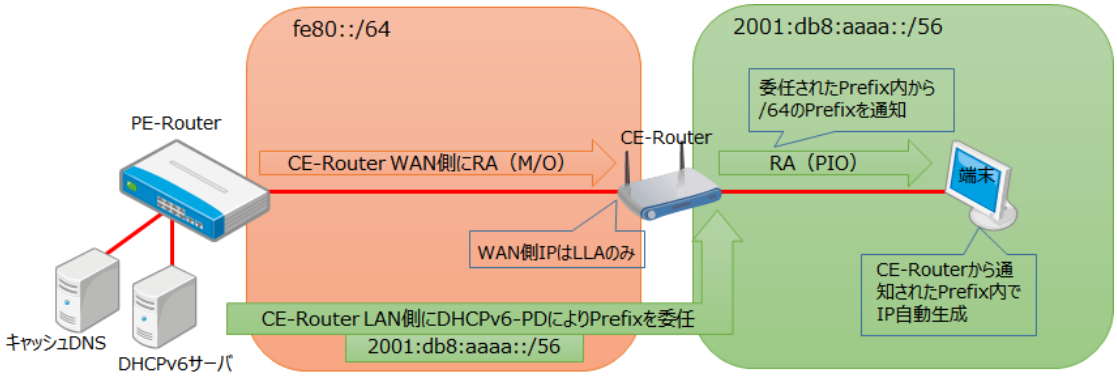


図 5.3 CE-Router（IA_PD 機能のみ）の構成

この場合の CE-Router、端末に設定されるネットワーク情報は表 5.3 のとおりとなる。

表 5.3 ケース 1 と CE-Router（IA_PD 機能のみ）の組み合わせ

CE-Router	WAN 側 IP アドレス	・LLA
	LAN 側 IP アドレス	・LLA ・DHCPv6-PD により委任された Prefix 内から生成
	デフォルトゲートウェイ	・PE-Router の LLA が設定される（RA から取得）
	遠隔管理	WAN 側は LLA しか持たないため外部から到達不可能。LAN 側には委任された Prefix から生成されたグローバルユニキャストアドレスが付与されるが、ユーザトレースでは Prefix 単位での紐づけになるのでこのアドレス自体は分からない。端末側から CE Router にログインしてアドレスを調べるなどの手段が必要となり、遠隔管理という面では適さない。
端末	IP アドレス	・LLA ・CE-Router から通知された Prefix 内で SLAAC によりグローバルユニキャストアドレスを生成
	デフォルトゲートウェイ	・CE-Router LAN 側の LLA が設定される（RA から取得）
キャッシュ DNS 情報		・RA 内の RDNSS オプションから取得 ・CE-Router は DHCPv6 サーバからも取得可能

- 回線直収（IPv6 ブリッジ含む）で端末を接続する場合

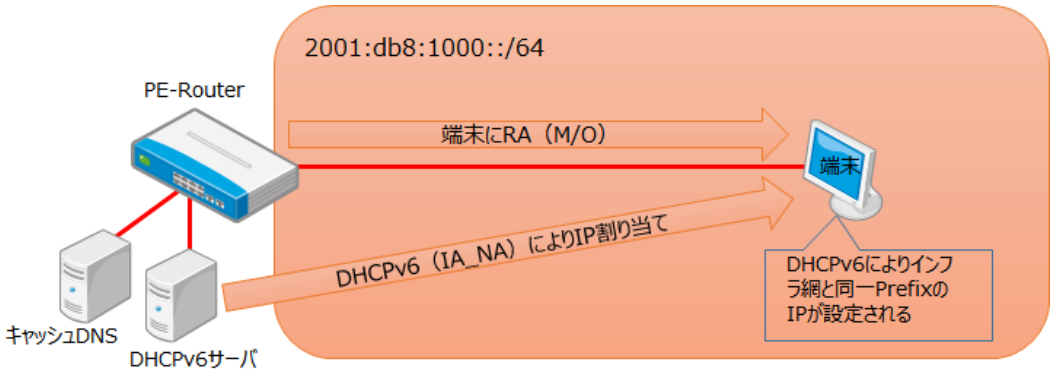


図 5.4 回線直収（IPv6 ブリッジ含む）の構成

この場合の端末に設定されるネットワーク情報は表 5.4 のとおりとなる。

表 5.4 ケース 1 と回線直収（IPv6 ブリッジ含む）の組み合わせ

端末	IP アドレス	・LLA ・DHCPv6 （IA_NA）サーバにより割り当てられるグローバルユニキャストアドレス※
	デフォルトゲートウェイ	・PE-Router の LLA が設定される（RA から取得）
	キャッシュ DNS 情報	・RA 内の RDNSS オプションまたは、DHCPv6 サーバから取得

※ DHCPv6 に未対応の端末は接続できないことに注意

(2) ケース 2 のインフラ設計の場合

- CE-Router（IA_NA・IA_PD 機能有り）経由で端末を接続する場合

  インフラ側で DHCPv6（IA_NA）が動作していなので、実質的に次の「CE-Router（IA_PD 機能のみ）経由で接続する場合」と同様の動作になる。

- CE-Router（IA_PD 機能のみ）経由で端末を接続する場合

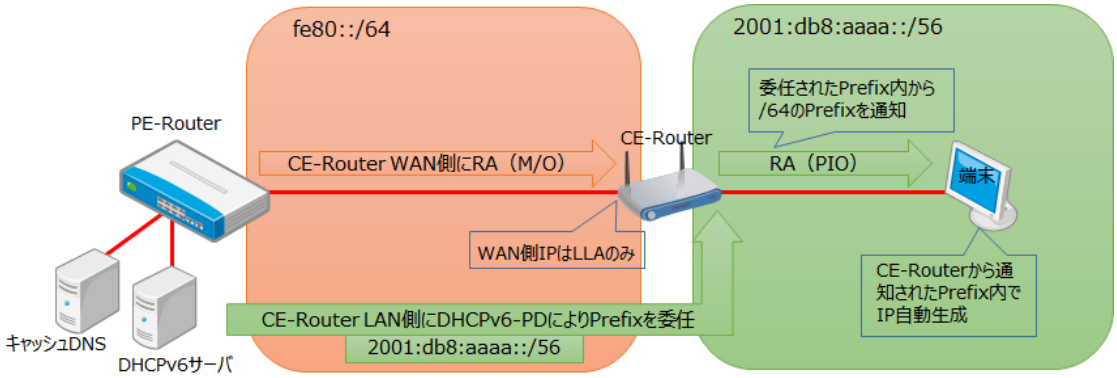


図 5.5 CE-Router（IA_PD 機能のみ）の構成

この場合の CE-Router に設定されるネットワーク情報は表 5.5 のとおりとなる。

表 5.5 ケース 2 と CE-Router（IA_PD 機能のみ）の組み合わせ

CE-Router	WAN 側 IP アドレス	・LLA
	LAN 側 IP アドレス	・LLA ・DHCPv6-PD により委任された Prefix 内から生成
	デフォルトゲートウェイ	・PE-Router の LLA が設定される（RA から取得）
端末	IP アドレス	・LLA ・CE-Router から通知された Prefix 内で SLAAC によりグローバルユニキャストアドレスを生成
	デフォルトゲートウェイ	・CE-Router LAN 側の LLA が設定される（RA から取得）
キャッシュ DNS 情報		・RA 内の RDNSS オプションから取得 ・CE-Router は DHCPv6 サーバからも取得可能

- 回線直収（IPv6 ブリッジ含む）で端末を接続する場合
  インフラ側で DHCPv6（IA_NA）も SLAAC も動作していないため、アドレス自動生成の仕組みが提供されないので接続不可能となる。

5.3 その他の考慮事項

IPv6 ネットワークを構成するうえで設計、運用時に考慮すべき事項をまとめる。

5.3.1 ネットワーク移行時の変更箇所

(1) ISP との接続性を確認する（IPv4/IPv6 の対応）。
(2) インフラ側装置（CMTS、L3 機能付き OLT、L3SW 等)に付随する OSS（プロビジョニングサーバーや DHCP サーバ等)がインフラ側装置の IPv6 対応に追従できるようにソフトウェアのバージョンアップもしくは入れ替えを行う。
(3) ユーザ側の端末（CM や ONU)が CPE へ IPv6 を転送可能なファームウェアへのバージョンアップ、もしくは対応機種へ入れ替えを行う。
(4) CPE は IPv6 プロトコルに対応した製品にする。
(5) IPv6 機器より IPv4 設備へ接続できるよう、HE・コアネットワーク内、ルータないし NAT 追加、もしくは CGN を経由し IPv4 の接続性を確保する。

＜留意点・注意点＞

- 機器のファームウェア・バージョンアップにおける、性能インパクトを検証する
- IPv6 導入における各機器キャパシティ状況を確認する。
- IPv6 化移行に関する、段取りをする。

①アクセス装置のみを IPv6 対応（バージョンアップ、または新規導入）にする
②ユーザ側の端末のファームウェア・バージョンアップ、または対応機種への入れ替えを行う

上記①、②を同時に進めるか個別に進めるかはサービス切り替えのタイミングと展開方法を充分に検討する必要がある。また、IPv6 導入にあたっての各機器の選定は製品の性能・評価試験等を事前に各ベンダ、メーカ等と検証することが必要である。

5.3.2 フィルタリング設定への考慮すべき事項

(1) 設備に設定するフィルタ

IPv4 でセキュリティフィルタを設定している場合、IPv6 でも同様の要件を満たすセキュリティレベルの設定が必要である。また、セキュリティフィルタを適用する機器も IPv4 と同様の箇所で設定することが保守・運用上望ましい。以下にケーブル事業者設備で設定している IPv4 の主なセキュリティフィルタを示す。

① 不正 DHCP Server 対策（DHCP 逆接続対策）
② Windows 共有対策（NetBIOS/Direct Hosting of SMB）
③ ウイルス対策（option 1434,4444,5000,など）
④ OP25B（Outbound Port 25 Blocking）

昨今の DDoS 等の不正アクセスの状況により、以下のフィルタが考えられる。

⑤ IP53B（Inbound Port 25 Blocking）
⑥ IP123B（Inbound Port 123 Blocking）

また、IPv6 で新たに考慮すべきセキュリティフィルタについて以下に例を示す。

⑦ 不正 RA（Router Advertisement）対策
⑧ 不正 DHCPv6 Server 対策（DHCPv6 逆接続対策）

さらに、IPv6 においてフィルタすべきではないものについて以下に示す。

⑨ ICMPv6
⑩ IPv6 のマルチキャスト

以上を考慮してセキュリティフィルタの適用をする。しかし、IPv6 のセキュリティフィルタに関してはその仕様上課題も多いことから以下の点について注意する。

(2) ネットワーク事業者間におけるパケットフィルタ

IPv6 のフィルタについては、ケーブル業界のみならずバックボーンを含めた関係各所で議論がなされている。その中でもネットワーク事業者間におけるパケットフ

ィルタに関しては、JANOG（JApan Network Operators’Group）から公表されている内容が参考となる。

（参考 http://www.janog.gr.jp/doc/janog-comment/jc1006.txt）

今後、ネットワーク事業者間にて IPv6 フィルタを設定する場合、本資料を参考に精査を進めていくことが望ましい。

5.3.3 監視に関する考慮すべき事項

IPv4 サービスで監視を行っている場合、IPv6 でも同様の項目を監視する必要がある。監視サーバについては、既存のサーバを IPv6 化させるか新規に IPv6 用のサーバが必要となる。また、監視ソフトウェアも IPv6 に対応しているかどうか確認する必要がある。オープンソースの監視ソフトウェアはすでに IPv6 対応されているものが多い。

＜具体例＞

- Nagios（統合監視ツール）http://www.nagios.org/
- Smokeping（ネットワーク latency を計測）http://oss.oetiker.ch/smokeping/ など

また、ベンダまたはメーカ独自で監視ソフトウェアを用意している場合にも IPv6 に対応しているかどうか確認する必要がある。アクセス装置についても同様に IPv6 に対応する MIB がサポートされているか確認しておく必要がある。

5.3.4 DHCPv6-PD（Route Injection）導入時に考慮するべき事項

ケーブルネットワークにおける DHCPv6-PD では、IPv6 ゲートウェイとなる同一リンク上の PE-Router において DHCPv6-PD パケットを Snoop し、動的に Route Table を生成する必要がある。

DHCPv6-PD を導入する際に考慮するべき点として以下が挙げられる。

(1) 上位ネットワークへのルート広報

1 台の CE Router へ prefix を配布すると、上位ネットワークへ割り当てた prefix が経路広報され、IPv6 の FIB（Routing）テーブルを 1 経路分消費することになる。

DHCPv6-PD の提供前に払い出し Prefix 数（＝上位ネットワークへ広報される経路数）を事前に想定し、上位ネットワークおよび PE-Router のキャパシティや FIB テーブルが枯渇しないよう考慮する必要がある。

※ IPv6（DHCPv6-PD ユーザ）の普及によって上位ネットワークの Routing テーブルを圧迫しないよう、PE-Router で IPv6 ルートをサマライズして広報するなどネットワーク設計上考慮することが推奨される。

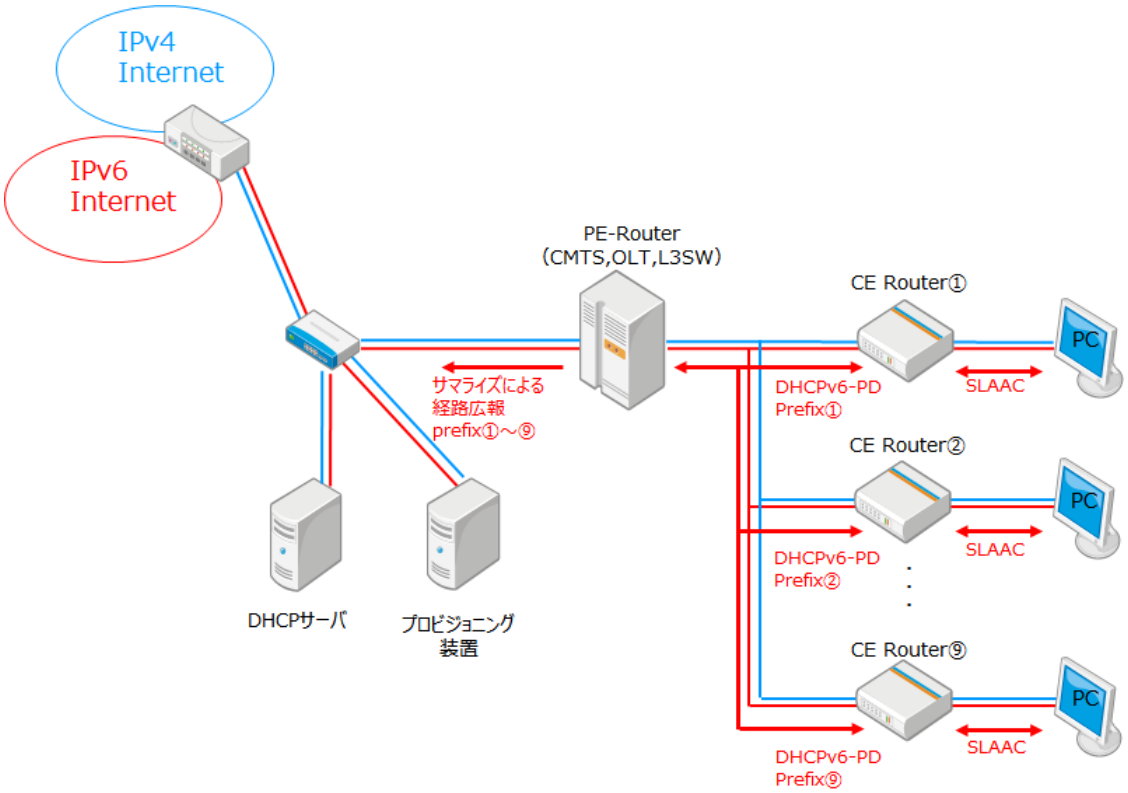


図 5.6 DHCPv6PD を PE-Router でサマライズし広報する実装例

(2) ルート冗長

OLT が L2 で構成され、PE-Router を冗長で構成する場合は、DHCPv6-PD パケットが通過した PE-Router にのみ経路エントリされることに留意する必要がある。

※ 図 5.7 のとおり、副系側 PE-Router には IPv6 Route がエントリされないため、障害やメンテナンスによって経路の切替わりが発生すると IPv6 アドレスで通信ができない状況が発生する。

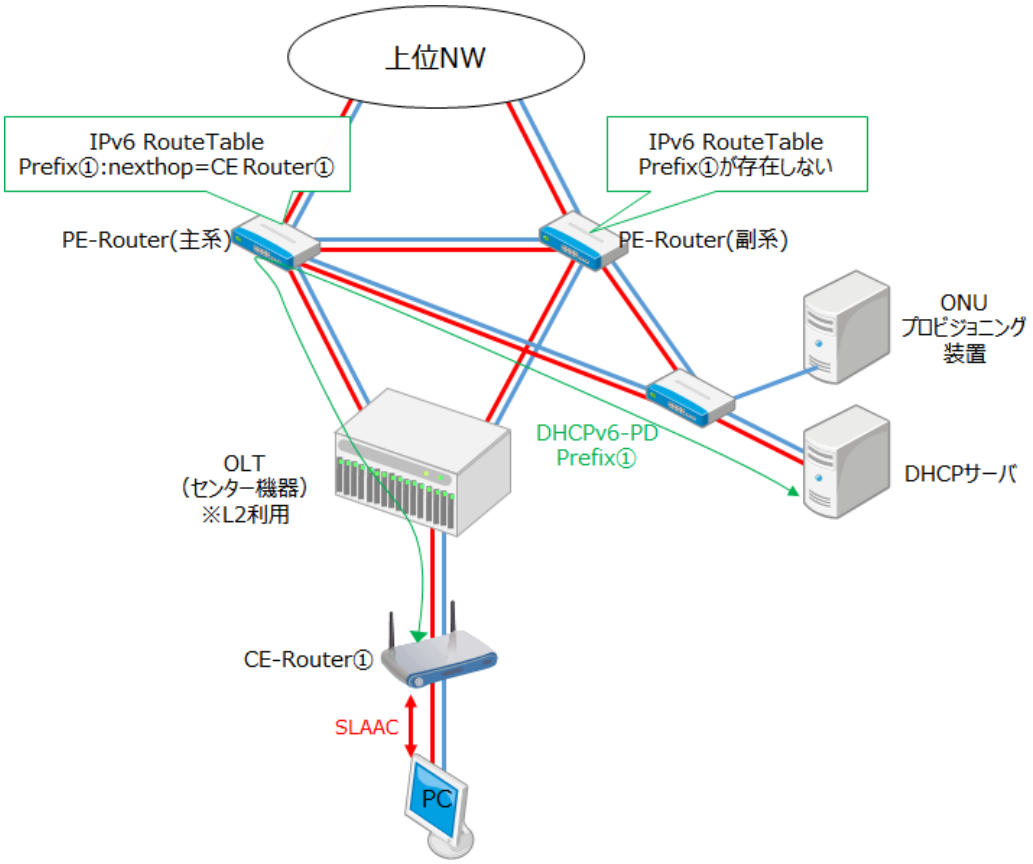


図 5.7 DHCPv6PD を PE-Router でサマライズし広報する実装例

PE-Router を冗長構成で設計する場合には、図 5.8 のとおり、仮想的に PE-Router を 1 台に見せる技術を利用することを推奨する。1 台の物理 PE-Router で構成する場合は、筐体内で CPU(ルーティングエンジンが)冗長を確保し、OLT との接続についても接続インタフェースを別ラインカードにするなどの考慮が必要である。

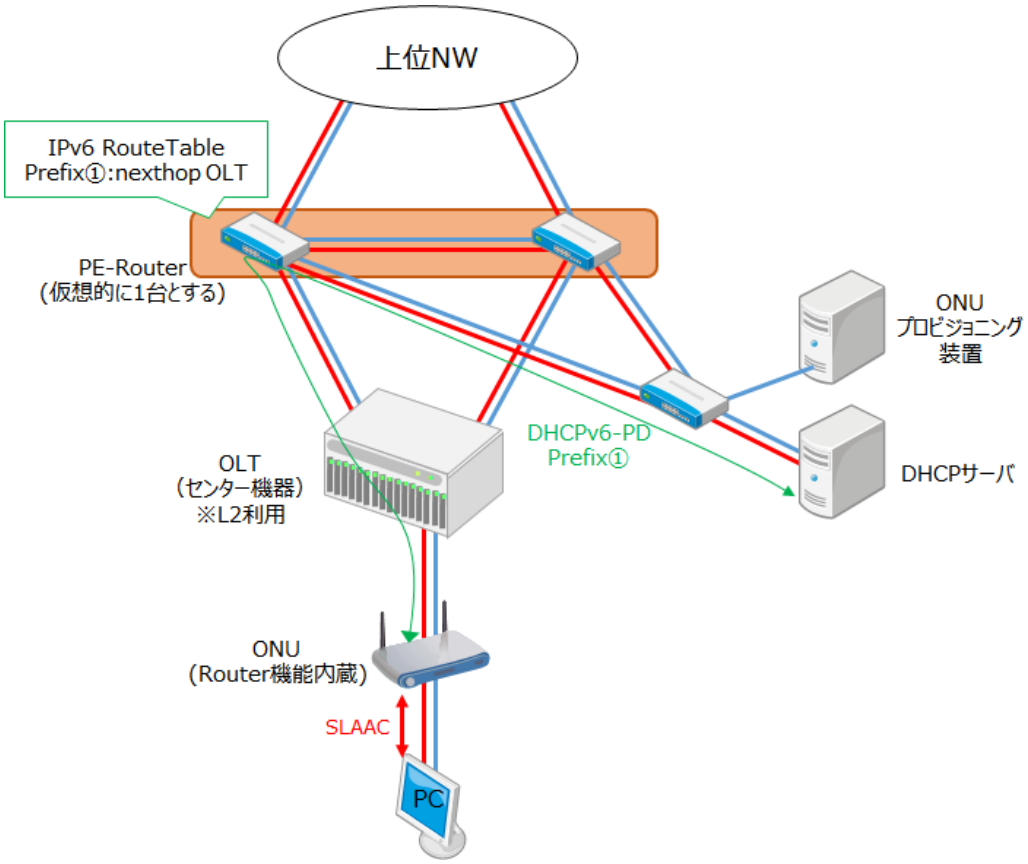


図 5.8 L3SW の冗長構成

(3) その他

市場には Route Injection 機能を非搭載の L3SW が多く存在するため、PE-Router に Route Injection 機能搭載機種を選定する必要がある。特に、FTTH ネットワークの機器選定では、処理 VLAN 数を優先して Route Injection 非搭載のデータセンター向けの機種が選定されることがあるため、注意が必要である。

すでに Route Injection 非搭載の PE-Router を採用している場合は、ルート情報を PE-Router に記述する仕組みを導入する必要がある。具体的には次の 2 パターンを挙げることができる。その他の方法も検討したが課題が残る結果となった。詳細は Appendix II に記載する。

①専用設備により PE-Router へ Dynamic Routing で配布する。
②専用プログラムにより PE-Router に Static Route コマンドで投入する。

なお、本対応は暫定的な対応であり、機器更新のタイミングなどで Route Injection 機能搭載 PE-Router を導入することを推奨する。また、あくまで机上検討によるもので実機を用いた試験等は行っていない点にご留意いただきたい。

5.3.5 折り返し通信に関する考慮事項

IPv6 ネットワークで L2 折り返し通信を実現させるためには、PE-Router に IPv4 の local-proxy-arp に相当する IPv6 ND-Proxy 機能が必要となる。

コンシューマ向けのインターネット接続サービスであれば、セキュリティリスクの観点から ND-Proxy の実装は必須ではないと考えるが、法人向けなどサービスごとに L2 折り返し通信を制御する場合には必要な機能となる。

※ ND-Proxy を具備していない場合は、DHCPv6-PD でネットワークを分けてルーティングするなど折り返しを考慮する必要がある。

5.3.6 ユーザトレーサビリティにおける考慮するべき事項

IPv4 アドレスと同様に、abuse 対応として、IPv6 アドレスにおいても使用時刻から利用者を特定する環境を構築する必要がある。

IPv4 アドレス運用におけるユーザトレーサビリティでは、一般的に DHCP ログ等から特定を行う場合が多いが、5.1 インフラ設計のケース 1,2 で実装する場合は IPv4 同様に DHCPv6 サーバの割り当てログから利用者を特定する環境を構築しておくことが運用オペレーション上望ましい。

一方ケース 4、もしくはケース 6 で示す構成で実装する場合、RA で PIO を配布していることによって、ユーザ側に設置されている端末がブリッジ CM/ONU 端末かつ LLC フィルタによる IPv6 通過許可を行っている環境において、CPE（PC やスマートフォン等）が回線直収されると SLAAC によって IPv6 アドレスを生成することが考えられる。

ケース 3 の構成で実装を行う場合のユーザトレーサビリティ確保として、PE-Router で CPE の MAC アドレスと CM/ONU の紐づけ情報を定期的に取得するなどの実装が必要となる。

※ 取得間隔としては IPv6 アドレスを自動生成した際に PE-Router 側で生成される ND-Cache および MAC アドレステーブルのエージングタイムよりも短い間隔で取得するなどの考慮が必要となる。

5.3.7 DHCPv6-PD における推奨要件

DHCPv6-PD の実装を行う場合、以下の払い出し仕様で Prefix 配布を行うことが推奨される。

(1) prefix サイズ：/48～/60

理由としては以下が挙げられる。

- /64 では Prefix Per Host（RFC 8273）を実装する端末への対応ができない。また、将来の CPE 管理に関する拡張性がないため採用すべきではない。
- TR-177 では、/56 を推奨、少なくとも/60 が望ましいとしている。
  ※ すでに/64 で配布している事業者についてはネットワーク更改や機器入れ替えのタイミング等で推奨 prefix サイズに変更することが望ましい。

(2) DNS 配布方法

DNS キャッシュ情報の配布は、CE Router は DHCPv6、 CE Router の LAN 側は RDNSS を利用する。

5.3.8 アクセス網のセキュリティ確保

アクセス網は、PE Router は未知のアドレス解決のため Neighbor Solicit を利用するが、アクセス網側の Prefix を大きくしてしまうと、悪意を持った機器が外部より(ping sweep 等)アドレス解決をするようなパケットを大量に発行することにより、PE Router やネットワークが高負荷な状態にできる可能性が考えられる。

このため、アクセス網は端末設備を収容するのに十分な Prefix を準備し、必要以上に大きな Prefix を適用しないようにすることが望ましい。

第6章　DOCSIS 構成の IPv6 対応

6.1　既存の IPv4 サービス仕様

DOCSIS ネットワークは図 6.1 に示す設備構成が基本となる。IPv4 サービスでは、DOCSIS に準拠したケーブルモデムシステムが用いられる事が多く、家庭内に 設置された CM を HE に設置された CMTS で終端している。

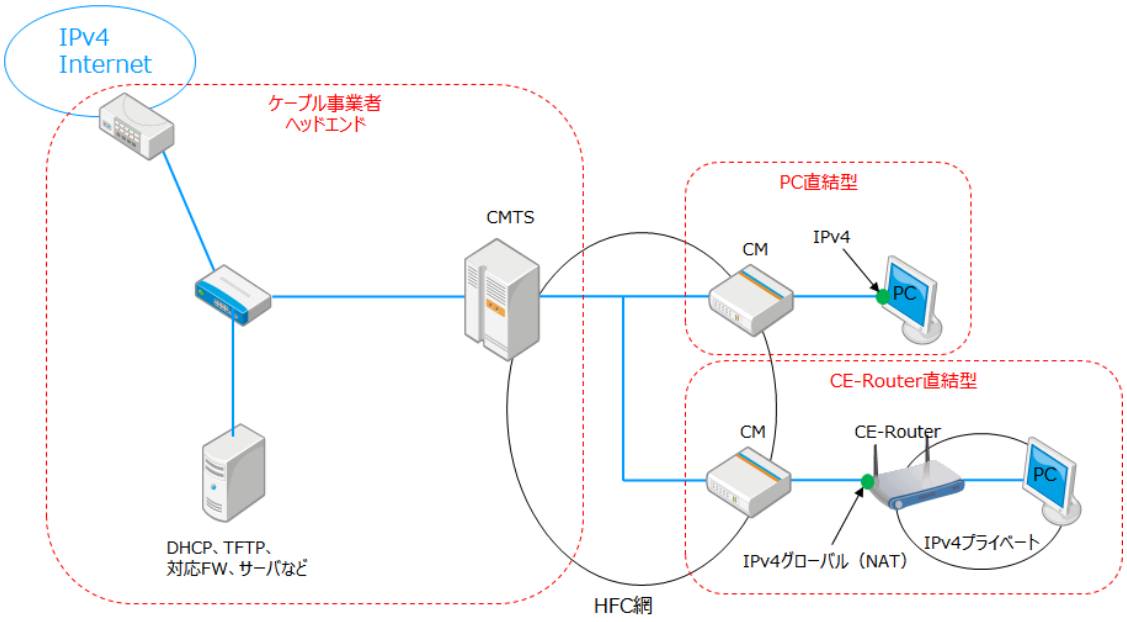


図 6.1 一般的な DOCSIS IPv4 サービス設備構成例

CPE への IP アドレス割り当て方法やその他オプションに関しては、DHCPv4 (RFC2131)により、以下のような項目を自動で割り当てる。

- IPv4 address, Netmask,（Global／Private：Private の場合 NAT）
- Default route
- DNS cache server address
- Domain name (option)

ケーブル事業者側でのセキュリティフィルタは、ケーブルインターネットの特性上、CMTS や CM で、以下のセキュリティフィルタを加入者保護ならびに自社設備保護として実施している事業者が多い。

- 不正 DHCP server 対策
- NetBIOS / Direct Hosting of SMB
- ウイルス対策　(option,1434,4444,5000,など)

6.2 IPv6 対応後の想定されるサービス形態

DOCSIS 3.0 の IPv6 サービスは CM として DOCSIS 3.0 もしく DOCSIS 2.0+IPv6 仕様を用いて、CM に対して管理用に IPv4、IPv6、またはデュアルスタックでその両方を割り当て、さらに CM の先の加入者端末にデュアルスタックを対応させるものである。CM への IPv6 アドレスの割り当ては DOCSIS の規定により DHCPv6 で行われる。加入者端末へは第 3 章で述べたとおり、トンネル方式を推奨しないものとし、DHCPv6 にてアドレスを割り当てる。ルータ接続の場合には DHCPv6-PD によりルータ配下にケーブル事業者から Prefix を割り当てる。この形態を図 6.2 に示す。

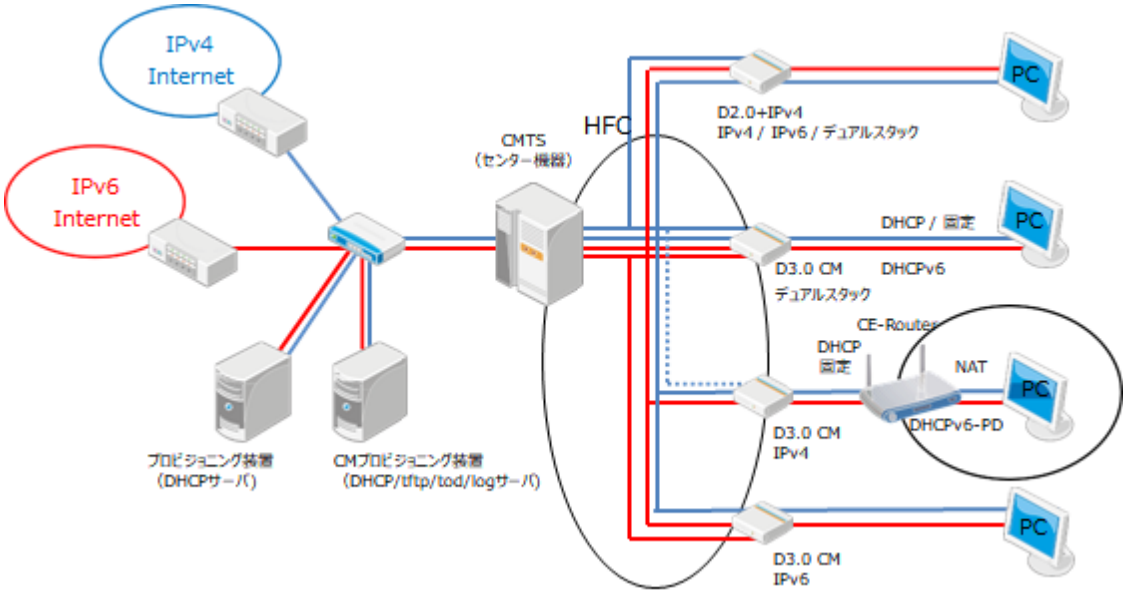


図 6.2 想定する IPv6 サービス形態

6.3 ネットワーク構成

基本的な構成を図 6.3 に示す。CMTS は上位のルータ/L3SW に接続される。上位接続のリンクをデュアルスタックとするために CMTS の上位接続ポートに IPv4 と IPv6 アドレスを割り当てる。Dynamic Routing を用いる場合、一般的に IPv4 は OSPFv2 で IPv6 は OSPFv3 を用い、両プロトコルで上位ルータと接続する。Cable インタフェースには CM 用の IPv4-Subnet、CM 用 IPv6-Prefix、CPE 用 IPv4-Subnet、CPE 用 IPv6-Prefix を割り当てる。CM を IPv4 でのみプロビジョングする場合には CM 用 IPv6-Prefix は不要となる。DHCPv6-PD で加入者宅のルータに対して Prefix を割り当てるために PD 用の Prefix を用意する。ここで PD にて割り当てられた Prefix は CMTS には直接接続されないが、ルータの先にある Prefix として CMTS では Routing Table で管理される。プロビジョニングサーバーとしては CPE のデュアルスタックのために CPE に IPv6 アドレスを割り当てら

れることができる DHCPv6 サーバを準備する。CM を IPv6 でプロビジョニングする場合には DHCPv6 サーバに加え IPv6 対応の TFTP/TOD サーバが必要になる。

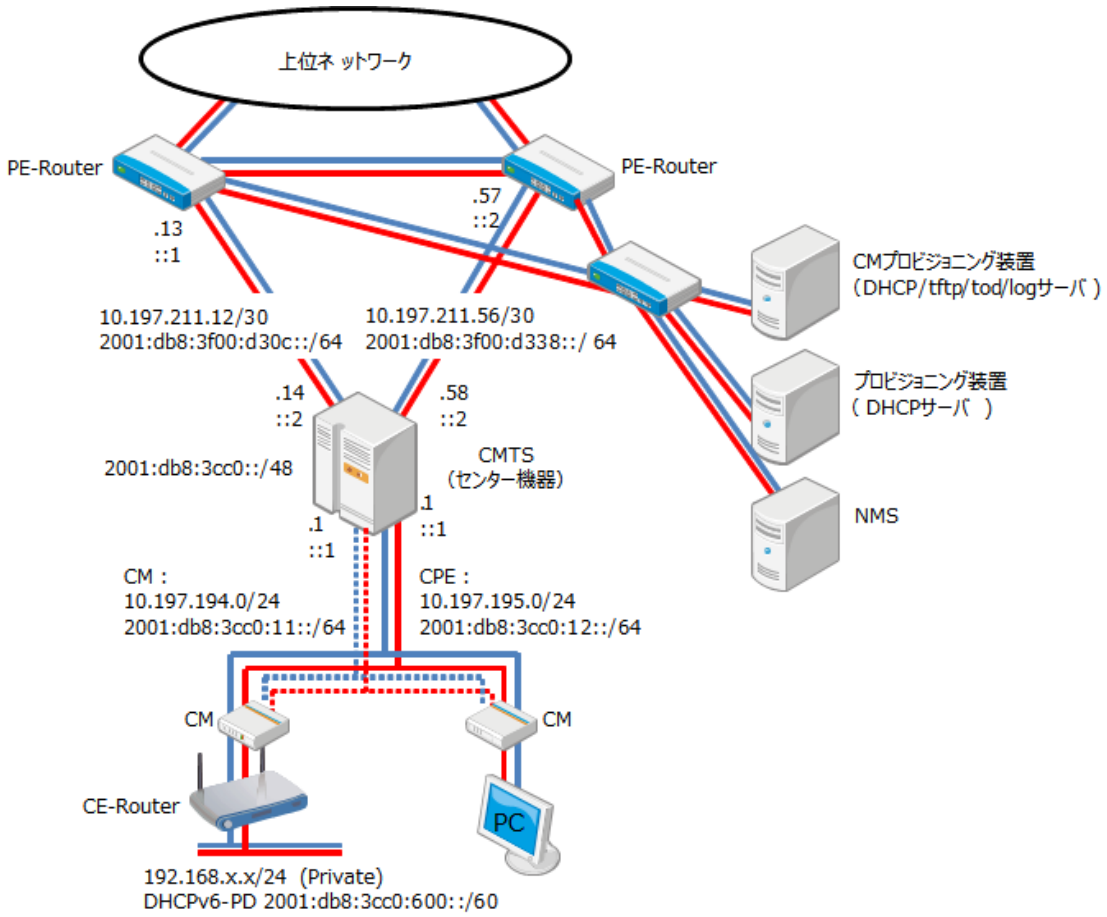


図 6.3 基本的なネットワーク構成

6.4 CPE の接続形態

6.4.1 CPE 接続形態の概要

IPv6 アドレス割り当て方法において CPE には DHCPv6 で、ルータには DHCPv6-PD で Prefix を割り当てるのかである。サービス面において IPv4/IPv6 アドレス割り当て数の制限について CPE 接続形態の概要と MAC 制限、IPv4 アドレス付与の方法、IPv6 アドレス付与の方法を表 6.1 にまとめた。

表 6.1 CPE 接続形態と運用について

接続形態	CPE 単体接続	CPE 複数台接続	CE-Router 接続型	eRouter 利用型
接続対象端末 接続許可台数	PC を 1 台接続するか CE-Router1 台接続。CE-Router 配下に事業者の設定した台数制限に関係なく CPE を接続できる。	HUB を介して複数台の PC を接続。PC の代わりに CE-Router を接続することもある。	DHCPv6-PD クライアントを実装する CE-Router のみを接続。	CM の代わりに eRouter を用い DHCPv6-PD クライアントを有効にする。
MAC	IPv4 のみサービスでは IPv6 は CE-Router でフィルタ、CM に流れない動きを想定。IPv6 は IPv6 ブリッジ機能により CPE から直接 CM に到達。IPv6 接続の場合は MAC 数の制限は現実的ではない。	接続許可数分の MAC が CM に認識されるため、MAX CPE は許可台数分を設定。CE-Router 接続を想定すると左記同様に MAC 数制限は現実的ではない。	ルータ1台接続を想定するため許可する MAC 数は 1。	
IPv4	CE-Router の WAN-IF に 1 つ付与。CPE は CE-Router の NAT 機能で複数 CPE を接続できる。	PC もしくは CE-Router の WAN-IF に 1 つずつ付与。CE-Router 配下の CPE は NAT 機能により許可 CPE 台数を超えて接続できる。	ルータの WAN-IF に 1 つ付与。CE-Router の NAT 機能で複数 CPE を接続できる。	
IPv6	CE-Router 配下に接続した CPE 台数分、IPv6 アドレスを付与される。IPv6 アドレス付与数の制限は現実的ではない。	CE-Router 配下に接続した CPE 台数分、IPv6 アドレスを付与される。IPv6 アドレス付与数の制限は現実的ではない。	ルータの WAN-IF に 1 つ付与。DHCPv6-PD で取得した Prefix で IPv6 アドレスを CPE に付与するため、複数台の CPE を接続できる。	

6.4.2 CPE 単体接続

(1) CPE 単体接続の概要

PC を 1 台のみ接続するか、もしくは CE-Router1 台を接続する。CE-Router を接続した際にはその配下にケーブル事業者の設定した接続台数制限に関係なく CPE を接続できる形態である。現在のケーブルインターネットで最も多い形態である。実際にはケーブル事業者は CM の配下に接続できる端末数を MAC Address 数で制限する方法で許可、MAC Address=1 としている。この形態では加入者が CE-Router を利用するか 1 台の CPE を接続するかについては管理しない。

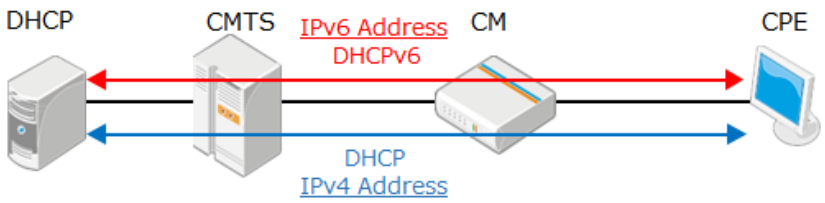


図 6.4 CPE 単体接続型

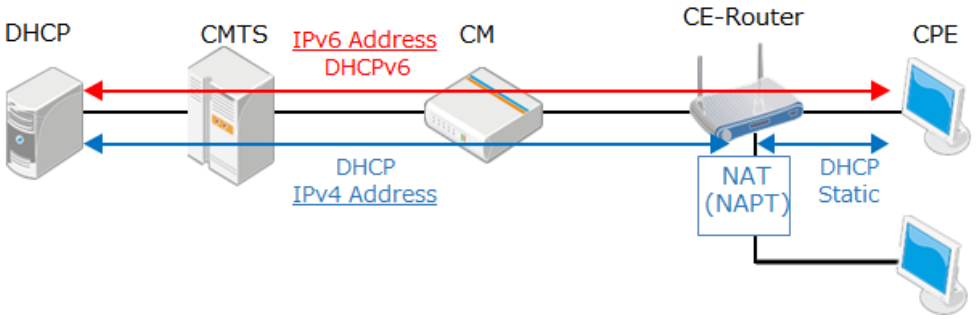


図 6.5 CPE 単体接続(CE-Router を接続した場合)

(2) IPv4 アドレス割り当て方法

PC、もしくは CE-Router の WAN インタフェースへの IPv4 アドレスは DHCP により事業者が保有するアドレス空間から割り当てる。また、固定でアドレスをマニュアルで割り当てる場合もある。

(3) IPv6 アドレス割り当て方法

PC への IPv6 アドレス割り当てはステートフル DHCPv6 にてケーブル事業者が保有するアドレス空間から割り当てる。この際、DHCPv6 サーバは Advertise および Reply で DNS cache server address Option 他、必要なオプションを含める。CPE の OS によってステートフル DHCPv6 が利用できない場合がある。この場合でもユーザトレーサビリティの観点で SLAAC を利用することは好ましくない。CPE における制限を取り除くためにルータ接続型モデルを用いてルータ配下での SLAAC 利

用を検討すべきである。CPE が DHCPv6 でアドレスを取得する場合、CMTS はリレー時にそれら CPE が接続される CM の MAC アドレスを以下の Option として付加する。

“Option 17 (Vender Specific Option) → Enterprise ID 4491 → Sub-Option 1026”この Option を DHCPv6 サーバで利用することで CM を特定することができ、特定の Prefix に属するアドレスを CPE に割り当てるなどのサービスが可能となる。ただし、この設定に関しては CM 障害時などにおいて、ケーブル事業者側にて設定変更が必要になるため（設定ツールを公開している場合は該当しない)、その運用も含めて検討する必要がある。

(4) ユーザトレーサビリティ

IPv4 と同様、IPv6 アドレスから利用者を特定するユーザトレーサビリティについても必要となる。abuse 対応をするときなど、利用時間と IPv6 アドレスから利用者を特定する環境を構築することが必要である。DHCPv6 サーバの割り当てログや、CMTS 等の Neighbor Cache 情報を利用することが考えられる。

(5) CPE 数の制限

IPv4 のみのサービスで CM に接続される CPE 数の制限を行う際、CM Config File での MAX CPE を用い MAC Address をカウントして制限する方法が一般的だった。デュアルスタックにおいて CPE 数を制限する際も、IPv4/IPv6 ともブリッジ接続となる場合には CPE 数制限として MAC Address をカウントすることで問題はない。多くの加入者で CE-Router を利用しており、IPv4 は NAT(NAPT)で IPv6 はブリッジするタイプがある。ブリッジ型接続でもその仕様の CE-Router を用いていることを前提として CPE 数の制限を考えることが望ましい。CPE 数制限の方法として、現時点の検討では以下の方法が最良の方法といえる。

サービス		設定
IPv4 アドレス許可数	1	CM Config File で TLV 35 = 1 を設定 もしくは SNMP：docsDevCpeIpMax = 1 を設定
IPv6 アドレス接続台数	n	CM Config File で TLV 18 = n を設定

ここでは CM に CPE が 1 台、もしくは CE-Router1 台接続を想定している。IPv4 アドレスはこれらのいずれか 1 つ付与されれば良いため、TLV35=1 や SNMP：docsDevCpeIpMax で制限する。IPv6 アドレスは 1 台の CPE に複数割り当てられることもあり、IPv6 アドレス数で制限する方法は得策ではないので、ここでは TLV 18 で CE-Router をスルーして IPv6 通信を行うことができる CPE 数を制限する。

なお、IPv6 アドレス数を制限する TLV63 で設定する場合の問題点として、TLV63=n と設定した場合にも n 台の CPE の Link local Address を CM が学習し、

実際には Global Address が学習できずフォワードされない点が例として挙げられる。一般的に Link local Address をソースとした通信が Global Address をソースとした通信よりも先に行われるため、n をいかに設定したとしてもどこかの段階で Link local Address のみが学習されることは発生しうるので TLV63 による制御は実質的に不可能といえる。TLV35 に関しては、CMTS の実装によっては設定数を越えた PC を接続した場合に CMTS を越えての通信はできないものの、DHCP でのアドレス取得だけは CMTS がリレーするために行われてしまう場合がある。事前に CMTS での動作を確認し、そのような場合には DHCP サーバでのリースタイムをあまり長くしないよう IPv4 アドレス消費を抑える処置が必要である。

6.4.3 CPE 複数台接続

(1) CPE 複数台接続の概要

HUB を介して複数台の PC を接続する。PC の代わりに CE-Router を接続することもありうる。この形態は CM Config File の TLV18 において接続可能な MAC Address 数の制限を 2 以上の値に設定することで実現している。端末 1 台接続の場合と同じで HUB を介して PC のみを接続させるか、その一部に CE-Router を利用するかは事業者としては管理しない。

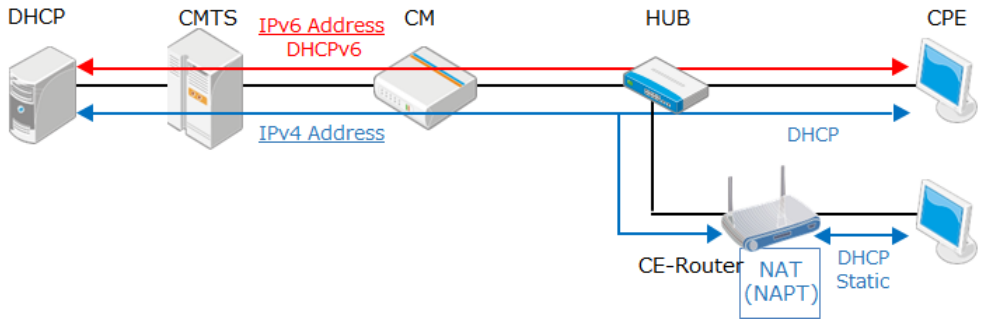


図 6.6 CPE 複数台接続

(2) IPv4 アドレス割り当て方法

PC もしくは CE-Router の WAN インタフェースへの IPv4 アドレスは DHCP により事業者が保有するアドレス空間から割り当てる。また別に DHCP は用いず、加入者が固定アドレスをマニュアルで割り当てる場合もある。

(3) IPv6 アドレス割り当て方法

PC への IPv6 アドレス割り当てはステートフル DHCPv6 にて、ケーブル事業者が保有するアドレス空間から割り当てる。この際、DHCPv6 サーバは Advertise および Reply で DNS cache server address Option 他、必要なオプションを含める。CPE の OS においてはステートフル DHCPv6 が利用できない場合がある。この場合もユ

ーザトレーサビリティの観点で SLAAC を利用しない。CPE における制限を取り除くためにルータ接続型モデルを用いてルータ配下での SLAAC の利用を検討すべきである。CPE が DHCPv6 でアドレスを取得する場合、CMTS はリレー時にそれら CPE が接続される CM の MAC アドレスを次の Option として付加する。“Option 17 (Vender Specific Option) → Enterprise ID 4491 → Sub-Option 1026”この Option を DHCPv6 サーバで利用することで、CM を特定することができ、たとえば特定の Prefix に属するアドレスを CPE に割り当てるなどのサービスが可能となる。ただし、この設定に関しては、CM 障害時などにおいて、ケーブル事業者側にて設定変更が必要になるため(設定ツールを公開している場合は該当しない)その運用も含めて検討する必要がある。

(4) ユーザトレーサビリティ

IPv4 と同様、IPv6 アドレスから利用者を特定するユーザトレーサビリティについても必要となる。abuse 対応をするときなど、利用時間と IPv6 アドレスから利用者を特定する環境を構築すること。IPv6 アドレスからの加入者特定は DHCPv6 サーバの割り当てログを利用することなどで可能である。

(5) CPE 数の制限

IPv4 のみのサービスで CM に接続される CPE 数の制限を行う際、CM Config File での MAX CPE を用い MAC Address をカウントして制限する方法が一般的だった。デュアルスタックにおいて CPE 数を制限する際も、IPv4/IPv6 ともブリッジ接続となる場合には CPE 数制限として MAC Address をカウントすることで問題はない。多くの加入者で CE-Router を利用しており、このうち IPv4 は NAT(NAPT)で IPv6 はブリッジするタイプがある。ブリッジ型接続でもその仕様の CE-Router を用いていることを前提として CPE 数の制限を考えることが望ましい。この形の CE-Router を考慮した CPE 数制限の方法として、現時点の検討では以下の方法が最良の方法といえる。

サービス		設定
IPv4 アドレス許可数	m	CM Config File で TLV 35 = m を設定 もしくは SNMP：docsDevCpeIpMax=m を設定
IPv6 アドレス接続台数	n	CM Config File で TLV 18 = n を設定

ただし m≦n

ここでは CM に直接 CPE が m 台接続され、その内には CE-Router も含まれることを想定している。IPv4 アドレスは契約の観点から m 台が付与されれば良いため TLV35=m で制限する。前項と同じく IPv6 アドレスは 1 台の CPE に複数割り当てられることもあり、IPv6 アドレス数で制限する方法は得策ではないため、TLV 18 で

CE-Router をスルーして IPv6 通信を行うことができる CPE 数を制限する。CE-Router の接続を考慮しなければ m=n でよいが、IPv6 をブリッジする CE-Router 配下の CPE から IPv6 通信するために n は m よりも大きい値が望ましく、CMTS でサポートできる最大数に設定することを推奨する。TLV35 に関しては CMTS の実装によっては設定数を越えた PC を接続した場合に、PC から CMTS を越えての通信はできないものの、DHCP でのアドレス取得だけは CMTS がリレーするために行われてしまう場合がある。事前に CMTS での動作を確認し、DHCP サーバでのリースタイムをあまり長くしないよう IPv4 アドレス消費を抑える処置が必要である。CMTS によっては TLV35 に代わる機能を別に持つ場合もある。

6.4.4 CE-Router 接続型

(1) CE-Router 接続型の概要

IPv4 としては NAT(NAPT)を実装し、IPv6 では DHCPv6-PD クライアントを実装するルータのみを接続する。

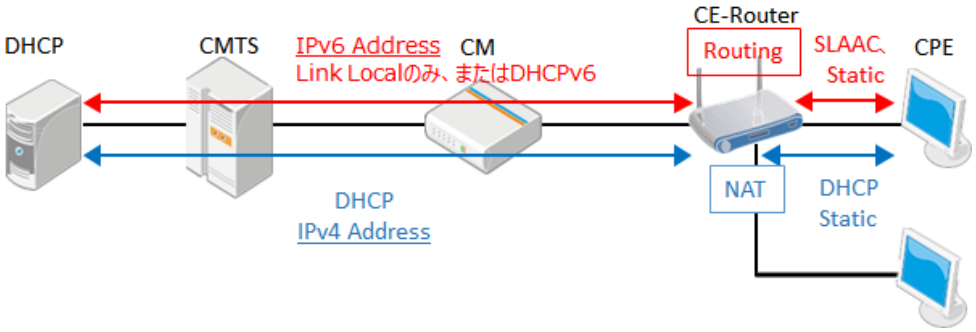


図 6.7 CE-Router 接続型

(2) IPv4 アドレス割り当て方法

CE-Router の WAN インタフェースへの IPv4 アドレスは DHCP によりケーブル事業者が保有するアドレス空間から割り当てる。固定でアドレスを割り当てる場合には加入者がアドレスをマニュアルで割り当てるため DHCP は必要ない。

(3) IPv6 アドレス割り当て方法

CE-Router の WAN インタフェースへの IPv6 アドレスは DHCP、または SLAAC によりケーブル事業者が保有するアドレス空間から割り当てる。

CE-Router の LAN インタフェースにあるネットワーク用として Prefix をケーブル事業者が保有するアドレス空間から DHCPv6-PD で割り当てる。CPE はルータの LAN 側に接続された LAN インタフェースからの RA に基づいて、SLAAC によりアドレスを生成することが可能となり、DHCPv6 をサポートしない OS においても

IPv6 を利用できるようになる。CE-Router の WAN 側インタフェースは Link Local Address のみでもかまわない。なお、Global Unicast Address を割り当てる場合には、CM に接続された CPE が SLAAC でアドレスを生成しないよう、CE-Router においても SLAAC を利用することは望ましくなく、ステートフル DHCPv6 を用いることが望ましい。RA に DNS Option を盛り込む仕様が RFC8106 で規定されている。CE-Router の LAN 側に設置された CPE が SLAAC で IPv6 アドレスを生成する際、この仕様に沿って DNS を RA で取得することを考え、DHCv6-PD の際にも DHCPv6 サーバは Advertise および Reply で DNS cache server address Option を含めるべきである。CE-Router が DHCPv6-PD において Prefix の割り当てを受ける際、CMTS はリレー時にそれら CPE、CE-Router が接続される CM の MAC アドレスを以下の Option として付加する。

- “Option 17 (Vender Specific Option) → Enterprise ID 4491 → Sub-Option 1026”

この Option を DHCPv6 サーバで利用することで、CM を特定することができ、たとえば固定の Prefix を割り当てるなどのサービスが可能となる。この設定に関しては、CM 障害時において、ケーブル事業者側にて設定変更が必要になるため(設定ツールを公開している場合は該当しない)、その運用も含めて検討する必要がある。

(4) ユーザトレーサビリティ

IPv4 と同様に IPv6 アドレスから利用者を特定するユーザトレーサビリティについても検討が必要である。abuse 対応をするときなど、利用時間と IPv6 アドレスから利用者を特定する環境を構築すること。CE-Router 接続型においては加入者ごとに Prefix を DHCPv6 サーバから割り当てるため、ソースアドレスの Prefix 部分を見ることで特定が可能になり、個々の CPE のアドレスまで管理する必要はない。Prefix からの特定は DHCPv6 サーバの割り当てログを利用することで可能である。

(5) CPE 数の制限

接続される端末は CE-Router に限られるため、CM Config File での TLV18 により MAX CPE を 1 として CPE の MAC Address 数を管理することが可能である。これにより接続できるルータ数を制限でき、合わせて DHCPv6-PD で割り当てる Prefix 数を制限できる。この場合、IPv4 アドレスは CE-Router の WAN インタフェースへ付与されるアドレスに限られ、複数 CPE においては CE-Router の LAN 側の Private アドレス領域を用いる IPv6 は割り当てられた Prefix の内のアドレスを、CE-Router の LAN 側に接続された CPE が利用する。DHCPv6-PD で IPv6 を割り当てた場合、CMTS における Prefix Delegation Route Injection が働くことで PD のルーティングは CMTS 内部に自動的に格納される。その際のネクストホップは Link Local Address となるため、CE-Router の WAN インタフェースへの IPv6 Global Unicast Address の付与は、運用上必ずしも必要ではないが、監視サービス

などを行う際には監視ネットワークからのルーティングを確保する必要性があるため、WAN 側にも IPv6 Global Unicast Address が必要になることも想定される。

(6) DHCPv6-PD で割り当てられた Prefix へのルートの広報

DHCPv6-PD で CE-Router への Prefix が割り当てられた際、その Prefix がどのルータ配下にあるかは CMTS が内部に Routing Table を生成して管理する。さらに CMTS の上位のルータに、その Prefix が当該 CMTS の先にあることが Routing 情報として広報されなければならない。OSPFv3 を利用する場合には、CMTS からの広報でこれが通知される。OSPFv3 等の Dynamic Routing を使用しない場合には、当該 CMTS の加入者に割り当てられる Prefix の領域を上位ルータに、Static Route として設定しておく必要がある。OSPFv3 を用いる場合には DHCPv6-PD で割り当てられた Prefix へのルートが、その Prefix の数だけ異なるルートとして CE-Router 接続型の加入者の数だけ広報される。この場合、上位ルータへ最大で数千から万の単位のルートが広報されるため、実際の運用では以下のような方法により広報するルート数を一定数に抑える方法が望ましい。

(a) CMTS 単位で割り当てる Prefix の範囲を上位ルータで Static Route として設定する。

(b) DHCPv6 サーバに Relay Address Option を用いるなどの方法で DHCPv6-PD で割り当 てる Prefix を(a)の範囲内になるようにする。

(c) CMTS の Null Interface を有効にし、(a)で設定された Prefix 範囲を Null Interface への Static Route を設定する。

CMTS が DHCPv6 Route Injection で個別 Prefix へのルート設定した場合にそのルートが(c)で設定された Static Route より優先することで、CE-Router へのルートが確保されるようにする。

(7) 割り当てサイズ

1 台の CE-Router に DHCPv6-PD で割り当てる Prefix 長は DHCPv6 サーバ側で設定される。CE-Router の LAN 側には/64 の Prefix を生成する。DHCPv6 サーバでの Prefix では/60～/48 を割り当てる。

6.4.5 eRouter タイプの CM を用いる場合

eRouter と 6.4.4 で記載したルータは同等なので運用の指針についても 6.4.4 と同様である。

6.5 IPv6 サービス構築上の検討ポイント

6.5.1 IPv6 サービスに必要な機能

加入者にデュアルスタックを提供する際にサービス品質を従来と同様に維持するため、表 6.2 にまとめる機能が必要となる。CMTS の管理に関しては DOCSIS 3.0 の規定では IPv6 をトランスポートとして管理される機能が必須となっているが、現実的には管理、監視は IPv4 トランスポートでも同一の内容を把握できる。管理システムを IPv6 化するには大きな負担がかかるため CMTS への CLI/SSH/SNMP アクセスは従来とおり IPv4 を使用するのが一般的である。よって現時点では CMTS の管理における SNMP、telnet、syslog 等のアクセスは、IPv6 対応となっても IPv4 で行うことを前提とする。

表 6.2 IPv6 サービスのために必要な機能

目的	機能	IPv4	IPv6
ユーザにデュアルスタックサービスを提供する	デュアルスタック	○	○
CMTS を管理する	管理するためのアドレス	○	△
	IPv6 関連の MIB、CLI を持つ	○	○
CM を管理する	管理するためのアドレス	○	△
	IPv6 関連の MIB を持つ	○	○
CPE へのアドレス割り当て	DHCP、DHCPv6	○	○
ユーザの PC の特定をする	DHCP Lease Table CMTS 上の DB	○	○
成りすましの防止	cable source verify DHCP lease query	○	○
不正なアクセスを防ぐ	Filtering	○	○
プロビジョニング	DHCP Server、TFTP Server	○	○
運用・管理	SNMP、Syslog	○	△

6.5.2 パケットフィルタに関して

(1) CMTS によるパケットフィルタ

CMTS に IPv6 のパケットフィルタを設定するには、拡張された Subscriber Management 機能、もしくはメーカ独自仕様の ACL 制御を行うことで可能となる。いずれの機能を使う場合でも、同一 CMTS 配下での加入者間の折り返し通信に対しても、フィルタリングを行うことが可能であるかを確認することが必要となる。また、このようなフィルタリング機能の実装は、メーカの機器仕様に依存するため、実際の設定方法なども含め、メーカまたはベンダに確認することが必要である。

(2) CM によるパケットフィルタ

CM で IPv6 のパケットフィルタをする方法は以下のとおり。

(ア) IP Filtering(docDevFilterEntry)

(イ) Subscriber Management Filter(TLV37)

(ウ) Upstream Drop Classifier(TLV60)

デュアルスタックにおいては個別のトラヒックに対して特定のポート番号のアクセスを禁止することができる Subscriber Management Filter、または UDC 機能で制御することが可能である。UDC は IPv4 のパケットフィルタにも対応している。だだし、UDC は上り方向のフィルタリングしかサポートしておらず、さらに従来から使用されている CM の config file による IPv4 の IP フィルタ機能を、同時に有効化することができないことに注意する必要がある。実装はメーカの仕様にも依存するため、実際の設定方法なども含めてメーカまたはベンダへ確認することが望ましい。また、現用の CM の config file において、LLC フィルタを用いて IPv4 と ARP のみ疎通を許可するような制限を実施している場合は、IPv6 の疎通も許可する設定を追加する必要がある。

6.5.3 プロビジョニング

IPv6 サービスを開始するにあたり CPE 用の DHCPv6 サーバは IPv6 対応を完了している必要があるが、CM のマネージメントを IPv4 でのみ行う場合、直ちに CM 用プロビジョニングシステムの IPv6 対応は必須ではない。ケーブル事業者の判断に委ねられるが、CM 管理用の IP アドレス空間の使用状況などを考慮し、将来的に CM のマネージメントを IPv6 で行う場合には対応を検討する必要がある。

6.6 IPv6 対応のための機能

IPv6 サービスを構成するための機能を、表 6.3 に示す。これらの個々の機能の解説を(1)～(9)で述べる。

表 6.3 DOCSIS システムにおける IPv6 機能

目的	機能	
CM プロビジョニング	CM Provisioning Mode	IPv4 Only
		IPv6 Only
		APM
		DPM
CPE デュアルスタック	Multicast DSID Forwarding	GMAC Promiscuous
		GMAC Explicit
	RA Off-Link	
	DAD Proxy	

目的	機能	
CPE への アドレス割り当て	DHCPv6 Relay	
	CM と CPE での Relay 先の使い分け	
	CM とCPE でRelay Link Address を分ける	
CPE 数制限	MAC Address 数	TLV18
	IPv4 Address 数	TLV35
		Default Subscriber Management
		SNMP : docsDevCpeIpMax
	IPv6 Address 数	TLV63
		Default Subscriber Management
ホームルータへの アドレス割り当て	DHCPv6 Prefix Delegation	
	Prefix Delegation Router Injection	
	Bulk Lease Query	
セキュリティ	Protocol Throttling	
	Cable Source Verify	
	Lease Query	
フィルタリング	Subscriber Management Filter	
	Data Plane 標準 ACL	
	Data Plane 拡張 ACL	
	Upstream Drop Classifier	
QOS	IPv6 Classification	
ルーティング	Static	
	IS-IS	
	OSPFv3	
マネージメント	MIB の IPv6 拡張	
	IPv6 での CLI、SNMP アクセス	
	IPv6 Lookback Interface	

(1) CMTS のインタフェースでの IPv6 アドレス割り当て

インタフェースはデュアルスタックにし、IPv6 側では/64 のアドレスを割り当てる。CPE へのアドレス割り当てポリシーは、Cable インタフェースでの RA パラメータが制御することになる。SLAAC を利用しないために、CPE 用の Prefix には no autoconfig flag の設定を有効にする。

(2) CM のプロビジョニングモード

DOCSIS 3.0、2.0+IPv6 では CM のプロビジョニングモードとして IPv4 Only、IPv6 Only、APM、DPM の 4 つが規定されている。モードの選択は Cable MAC ごととなり、その Cable MAC の Primary Capable DS Channel で伝送される MDD により、このプロビジョニングモードが CM に伝えられる。CM は MDD のプロビジョニングモードを受信して、起動時のモードを選択する。IPv4 Only モードでは DHCP で IPv4 アドレスを取得し、以降の起動プロセス、および管理トラヒックに IPv4 トランスポートを用い、IPv6 Only モードでは DHCPv6 により IPv6 アドレスを取得し、以降 IPv6 トランスポートを用いる。APM では 最初に IPv6 アドレスによる接続を試み、完了しなかった場合に IPv4 にフォールバックする。DPM は DHCP、DHCPv6 の両方でアドレスを取得し、IPv4/v6 の両トランスポートの管理に使用できる。なお、CM が IPv4 でプロビジョニングされているか、IPv6 でされているか、デュアルスタックとなり IPv4/v6 アドレスの両方を持つかは、CM に接続された CPE におけるデュアルスタックの可否とは関係ない。なお CM を IPv6 でプロビジョニングして管理する際には、CM が Link Local アドレス、Global アドレスを持つことから、CMTS の管理可能最大アドレス数を考慮した規模設計が必要となる。

(3) IPv6 サービスの許可、不許可

これまでは、CM Config File の LLC フィルタで、Ether Type =2048(IPv4) と Ether Type=2054(ARP)のみを通過させ、他のプロトコルをブロックする方法が一般的である。この場合、IPv6(Ether Type = 34525)はブロックされるので、CPE のデュアルスタックを提供することはできない。CPE にデュアルスタック を許可する場合には LLC フィルタに Ether Type = 34525 を追加する。また、反対にこの LLC フィルタを用いて デュアルスタックを許可する加入者と、許可しない加入者を分けることが可能である。

IPv6 をフィルタしない CM Config File の SNMP 設定

```
SnmpMib = docsDevFilterLLCUnmatchedAction.0 discard
SnmpMib = docsDevFilterLLCStatus.10 createAndGo
SnmpMib = docsDevFilterLLCIfIndex.10 0
SnmpMib = docsDevFilterLLCProtocolType.10 ethertype
SnmpMib = docsDevFilterLLCProtocol.10 2048
SnmpMib = docsDevFilterLLCStatus.20 createAndGo
SnmpMib = docsDevFilterLLCIfIndex.20 0
SnmpMib = docsDevFilterLLCProtocolType.20 ethertype
SnmpMib = docsDevFilterLLCProtocol.20 2054
SnmpMib = docsDevFilterLLCStatus.30 createAndGo
SnmpMib = docsDevFilterLLCIfIndex.30 0
SnmpMib = docsDevFilterLLCProtocolType.30 ethertype
SnmpMib = docsDevFilterLLCProtocol.30 34525
```

(4) CPE へのアドレス割り当ての方法

CM に直接接続された CPE は DHCPv6 でアドレスを取得する。DHCPv6 でのアドレス割り当てを用いる場合には、CMTS は DHCPv6 Relay が機能している必要があり、DHCPv6 サーバを Relay Destination で指定することで、CPE に DHCPv6 でのアドレスを割り当てることが可能である。

(5) DHCPv6-PD と Route Injection

IPv6 CE-Router への Prefix の割り当てには DHCPv6-PD を用いる。DHCPv6 でホストアド レスを割り当てる代わりに、CE-Router が必要とする Prefix を割り当てる。CE-Router からの Solicit に対して、たとえば DHCPv6 サーバは 2001:db8:3cc0:1ff0::/60 などの Prefix を割り当て、CE-Router は LAN インタフェースにその割り当てられた Prefix の中で/64 の Prefix を選択しアドレスを生成する。CE-Router の LAN 側に接続された CPE は、CE-Router LAN インタフェースからの RA によって SLAAC でアドレスを生成する。DHCPv6-PD で割り当てられた PrefixCPE が生成するアドレスの関係を図 6.8 に示す。

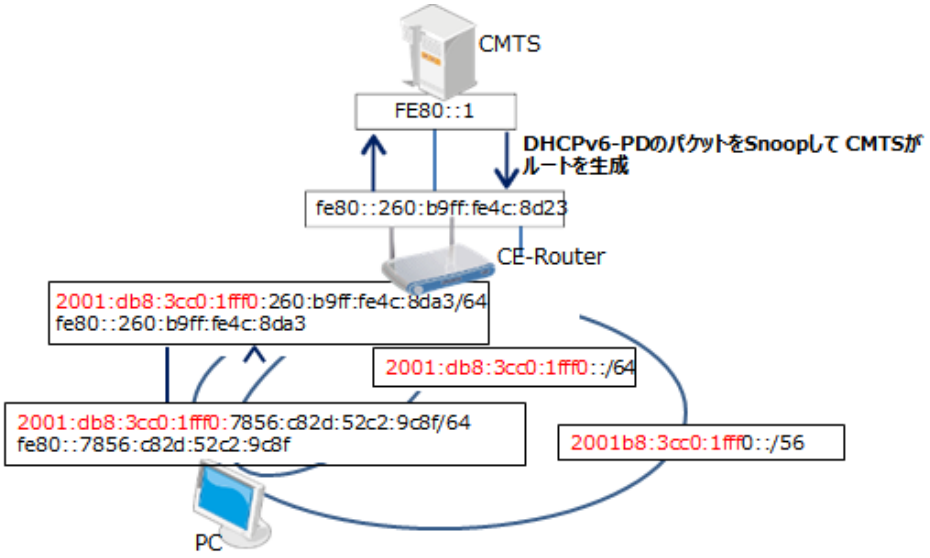


図 6.8 DHCPv6-PD で割り当てたアドレスの CPE での使用

CPE から見た default route は、CE-Router の LAN インタフェースからの RA で CPE に与えられる。また、CE-Router の default route は、CMTS の Cable インタフェースからの RA で与えられる。逆に DHCPv6-PD で割り当てた Prefix が、どの CE-Router の配下にあるかは動的に CMTS が Route Table として持つ必要がある。よって CMTS は DHCPv6-PD パケットを Snoop して動的に Route Table を生成する必要があり、これを DHCPv6-PD Route Injection という。DHCPv6-PD Route Injection で生成された Route Table (PD Route)は、OSPFv3 で上位ルータに広報することが可能である。しかしながら、CMTS が自ら持つ PD-Route は、外部ルータから OSPFv3 で CMTS に通知されることはないため、CMTS の再起動等により、PD-Route を再取得する必要がある場合には、DHCPv6 サーバに対して、Bulk Lease

Query (RFC5460)によって払い出された Prefix 情報を取得して、PD-Route を再構成する。

(6) MDF(Multicast DSID Forwarding)

IPv6 は、Link Layer アドレスの解決やルータ探索などに使用される Neighbor Discovery でマルチキャストが多く使用される。DOCSIS 3.0、または DOCSIS 2.0+IPv6 仕様ではマルチキャストパケットをフォワードするために MDF という機能が定義され、CPE での IPv6 通信を実現する。MDF では、GMAC Promiscuous Mode、GMAC Explicit Mode の 2 つがあり、DOCSIS 3.0 CM は、GMAC Promiscuous Mode、DOCSIS 2.0+IPv6 CM では、GMAC Explicit Mode を使用することになっている。MDF の Mode は、CM 起動時の Registration Request、Registration Response で交換され、お互いがサポートする Mode が一致した場合に、マルチキャストがフォワードされる。

表 6.4 DOCSIS 3.0/2.0+IPv6 で規定された MDF の Mode

CM / CMTS / REG-REQ / REG-RSP	DOCSIS2.0+IPv6		DOCSIS3.0
	MDF-incapable CM	MDF-capable CM	
	0	1	2
0	MDF-incapable CM (Multicast for IPv6 CPE are forwarded)	MDF-disabled	MDF-disabled
1	-	GMAC-Explicit (MDF-enabled)	-
2	-	-*1	GMAC-Promiscuous (MDF-enabled)

*1:GMAC−Promiscuous　Override 機能は対象外とする。

一方で、DOCSIS 2.0 CM は、IGMP のみによりマルチキャストを対応する仕様で、default では IPv6 で必要なマルチキャストを通さない。CM がマルチキャストを通さない場合に、CPE の IPv6 で次に示す 3 つの問題が発生する。

(ア) RA が CM を通過せず、CPE が IPv6 Default Gateway を受け取れない。

(イ) CMTS 同一 Cable MAC 内の CPE と通信しようとした場合に、相手先の CPE の MAC のアドレス解決ができない。

(ウ) IPv6 アドレス生成時の DAD において、DAD のための NS が、実際に重複アドレスがあった場合にも CM を通過せず、NA が戻らず重複を検出できない。

上記(ア)の問題は、CM Config File にて固定で RA を設定にするように、TLV42 に全ノード宛の Multicast MAC アドレス=33:33:00:00:00:01 を、記載することで多くの CM で RA を透過できるようになる。しかしながら、CM の先に接続された CPE の IPv6 Global アドレスを元に生成する要請ノードマルチキャストを通過させるためには、動的に CM に接続された CPE のアドレスに応じて、フォワーディングルールを変える必要があるため、CM Config File でこれに対応することはできない。また、フィルタリングを利用する際に、DOCSIS 2.0 では、IPv6 トラヒックをフィルタリングすることができない。これらの点から、IPv6 対応においては、DOCSIS 3.0 もしくは DOCSIS 2.0+IPv6 の CM を用いることが前提となる。

(7) Cable Source Verify

IPv4 と同じく IPv6 に対してもアドレスの不正利用を防止するために、CPE からの通信での Source IPv6 アドレスが、正しく DHCPv6 サーバから割り当てられたものであるのかを Lease Query を用いて判断する、Cable Source Verify 機能を用いる。IPv6 での Lease Query は RFC5007 に規定されている。

(8) フィルタリング

フィルタリングの方法として、インタフェースに Access List を適用する Network Side ACL と、DOCSIS 3.0 で規定されている以下の方法がある。

(ア) IP Filtering (docsDevFilterEntry)

(イ) Subscriber Management Filter (CM Config File：TLV37)

(ウ) Upstream Drop Classifier (CM Config File：TLV60)

IP フィルタリングは IPv4 のみに適用できる方法であるため、デュアルスタックには利用できない。よってデュアルスタックにおいては個別の加入者に対して特定のフィルタリングは Subscriber Management Filter または UDC となる。

(9) Protocol Throttling

IPv6 通信において、不必要な DHCPv6 と Neighbor Discovery パケットを制限することが、CMTS の安定運用のために必要であり、CMTS では Protocol Throttling の利用を推奨する。

6.7 IPv6 導入手順

(1) CMTS ソフトウェアバージョンアップ

DOCSIS3.0 対応のソフトウェアであっても、IPv6 に関わる機能が不十分である場合もあるため、ベンダおよびメーカへの確認が必要である。仮に対応していない場合、IPv6 による CM のプロビジョニングと、CPE に対する IPv6 転送を可能にするために、バージョンアップが必要である。通常、稼動中の CMTS はソフトウェアバージョンアップ時に再起動が必要な場合が多く、サービスを中断することになる。ベ

ンダによっては、一部のハードウェアとソフトウェアの組み合わせによって、シャーシ内で予備カードに切り替えながら、サービスへの影響を減らしてバージョンアップできるものも存在するが、IPv4 のみの状態からデュアルスタックをサポートするのは変更点が多いため、バージョンアップによるサービス中断を念頭において準備をすることが望ましい。

また、バージョンアップと同時に IPv6 を有効とするか、バージョンアップ後に IPv6 を有効とするかは状況により判断が必要と考えられる。図 6.9 に CMTS のみバージョンアップし、サービスは IPv4 のまま維持している状態を示す。

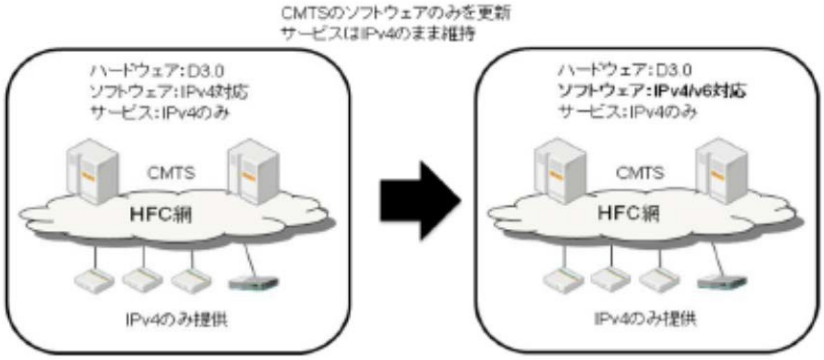


図 6.9 CMTS のみバージョンアップしサービスは IPv4 のまま維持

(2) CMTS の IPv6 設定

CMTS での IPv6 設定は Appendix に設定例を記載する。

通常は CMTS に IPv6 対応としてデュアルスタック化する場合、各インタフェースの IPv4 設定に IPv6 を追加する。この作業はサービス中断を伴わず実行できるが、実施に当たっては予備機等で手順を検証し、サービスへの影響を確認しておくことが望ましい。

(3) DHCPv6 サーバの準備

DOCSIS2.0 では CM/CPE への IPv4 アドレスの割り当てに、DHCPv4 サーバが用いられていた。DOCSIS3.0 では CM/CPE への IPv6 アドレス割り当てには、DHCPv6 サーバが用いられ、stateful DHCPv6 が必要である。

ネットワーク上に DHCPv6 サーバを準備する場合、次の 2 つの選択肢がある。

(ア) 既存の DHCPv4 サーバを DHCPv6 に対応にバージョンアップする。

商用かつ DOCSIS 向けに市販されている DHCP サーバの中には特定バージョン以降で DHCPv6 をサポートするものがあり、バージョンアップすることで DHCPv4 と DHCPv6 の両方が利用可能となる。

(イ) DHCPv4 サーバとは別に DHCPv6 サーバを用意する。

DHCPv4 と DHCPv6 は互換性のない独立したプロトコルであり、CMTS 上で DHCP ヘルパー、もしくは DHCP リレー先を各々個別に設定する。そのため、DHCPv4 サーバと DHCPv6 サーバは、同一ホストであっても別ホストであっても差し支えないため、既存の DHCPv4 サーバとは別に DHCPv6 サーバを設置してもよい。

いずれの方法でも問題はないが、サーバと各端末の接続性は IPv4、IPv6 それぞれで確保する必要がある。また、DHCP サーバ以外にも Firewall 等を設置している場合にはそれらも更新することが必要となる。

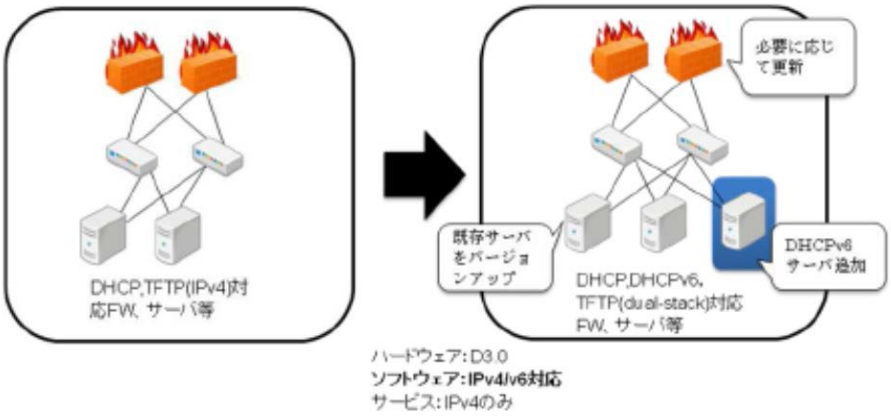


図 6.10 DHCP サーバを準備

(4) CM プロビジョニング方法の変更

上述した MDF が CMTS/CM ともに IPv6 運用に必要な機能となることから、IPv6 サービスでは、DOCSIS 3.0 か DOCSIC 2.0+IPv6 CM が必要である。しかし、DOCSIS3.0 および DOCSIS 2.0+IPv6 の CM は、実装状況が仕様と異なるなどの事象も一部確認されているために、必ずメーカやベンダに実装状況の確認を行うとともに、検証評価を実施することを推奨する。特に、MDF 関連については、仕様の解釈の違いによるサポート状況が CM により異なる可能性も あるので十分に注意が必要である。

(ア) DOCSIS 3.0、DOCSIS 2.0+IPv6 CM に使用する管理用 IP アドレスを、IPv4 のまま維持する。

(イ) DOCSIS 3.0、DOCSIS 2.0+IPv6 CM に管理用 IP アドレスとして IPv6 を割り当てる。またはデュアルスタックとする。

- CM は IPv4 アドレスのまま運用する場合

  上記（ア）の方法を選択する場合、CMTS の MDF を有効化することによりマルチキャストのサポート範囲が拡張されるだけでなく CPE プロビジョニングに必要な IPv6 マルチキャストが透過される。

- CM に IPv6 アドレスを割り当てる場合

  上記（イ）の方法を選択する場合、CMTS の MDF を有効化することによりマルチキャストのサポート範囲が拡張されるだけでなく CPE プロビジョニングに必要な IPv6 マルチキャストが透過される。次に以下の手順で CM に IPv6 アドレスを割り当てる。

  ① CMTS において CM を収容するインタフェースに CM 用の IPv6 アドレスを設定する。そして、ステートフル DHCPv6 が有効となるよう RA を設定し、CM のプロビジョニング方法を IPv6-only、APM、DPM のいずれかに設定する。

  ② DHCP サーバにおいて、対象となる CM に IPv6 アドレスが割り当てられるよう設定する。すなわち DHCPv6 サーバに登録する。

  ③ CM を再起動する。

(5) デュアルスタック サービス用の CM Config File の準備

一般的にはサービス分類上の都合、もしくは CM 側の都合により全加入者一律に IPv6 を許可せず、特定加入者および CM に対して IPv6 を許可することとなる。ここでは、上述した CM Config File の LLC Filter を用いて IPv6 通信の許可・不許可を設定する。デュアルスタックを提供する CM に対しては、IPv6 が LLC Filter 設定で通過する CM Config File を準備する。またサービス個別のフィルタリングを設定する場合は、CM Config File に IPv6 用フィルタリング設定も追加する。

(6) 段階的な適用

デュアルスタックを提供する加入者に関して、上項で作成した CM Config File をプロビジョニングで CM に適用し、CM を再起動することでこの設定を反映させる。

第7章　PON 構成の IPv6 対応

7.1　既存の IPv4 サービス仕様

現在、FTTH では GE-PON や G-PON 構成である事が多く、家庭内に設置された ONU を HE に設置された OLT にて終端している。

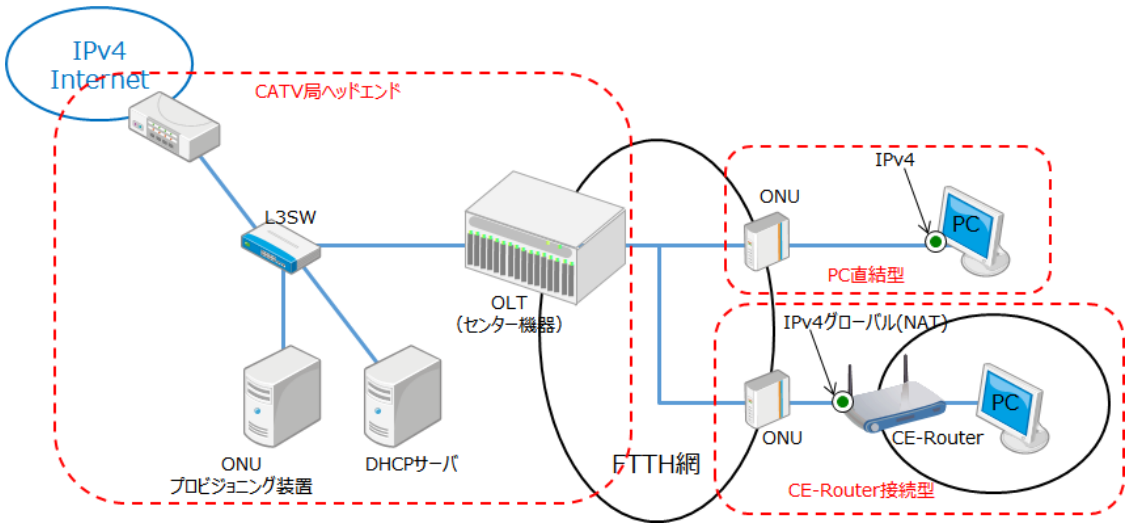


図 7.1 一般的な FTTH インターネット接続サービス設備構成例

(1) CPE への IP アドレス割り当て例

CPE への IP アドレス割り当て方法やその他の情報に関しては、DHCPv4（RFC2131）により以下のような項目を自動で割り当てる。

- IPv4 address, netmark,(Global／Private：Private の場合 NAT)
- Default Route
- DNS cache server Address
- Domain name (option)

また、サービス内容によっては DHCPv4 で IP アドレスを割り当てる事なく、CPE 固定の IP アドレスを指定することもある。

(2) ケーブル事業者側でのセキュリティフィルタ

OLT で以下のセキュリティフィルタを、加入者保護と自社設備保護として実施している事業者が多い。

- 不正 DHCP server 対策（DHCP 逆接続対策）
- NetBIOS／Direct Hosting of SMB（Windows 共有対策）
- ウイルス対策（UDP1434,TCP4444,TCP5000 など）

7.2 IPv6 対応後の想定されるサービス形態

5.1 で推奨したケース 1 およびケース 2 の PON 構成でのサービス方式について述べる。

7.2.1 推奨 IPv6 サービス

(1) ケース 1 DHCPv6 と DHCPv6-PD のデュアルスタックによる IPv6 サービス方式

CE-Router の WAN 側には、DHCPv6 でアドレスを配布し、LAN 側には、DHCPv6-PD によるアドレス配布を実施する。また、CE-Router のない加入者には、端末を直結しても、DHCPv6 による IPv6 アドレス配布がされ、すべての加入者へ、IPv6 を提供することが可能となる。加入者が接続する CE-Router によって IPv6 の対応状況が異なるため注意が必要である。

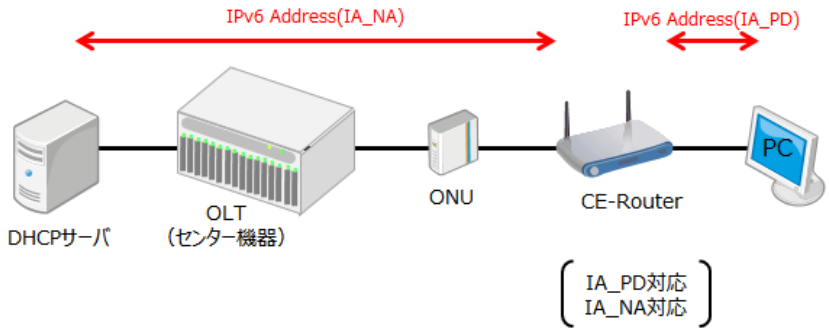


図 7.2 ケース 1 CE-Router (IA_PD/IA_NA 対応)

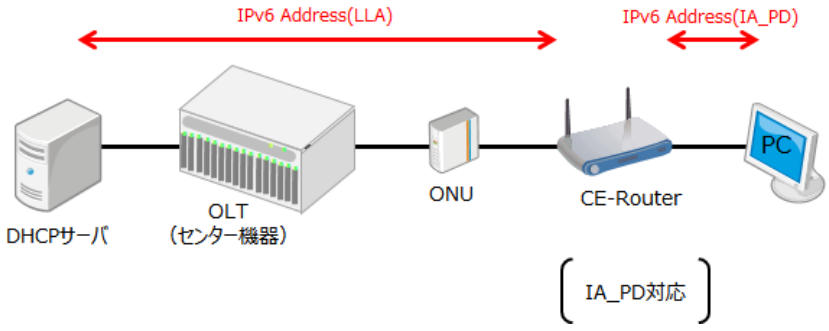


図 7.3 ケース 1 CE-Router（IA_PD にのみ対応）

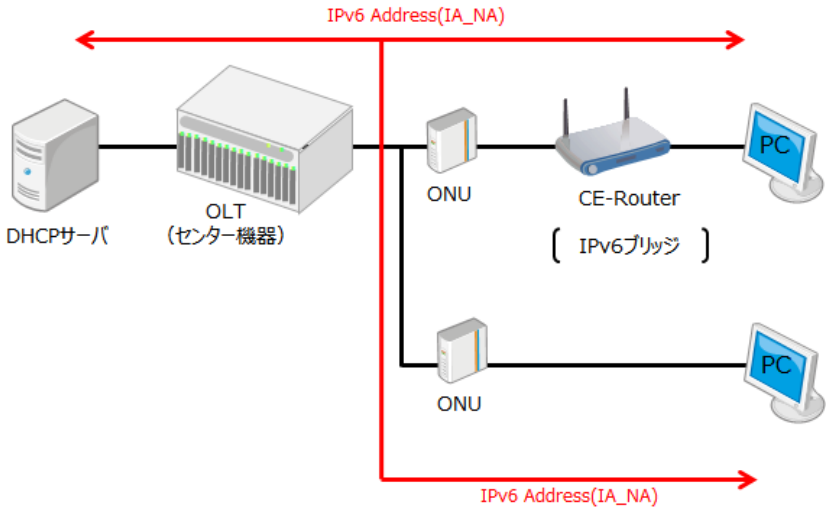


図 7.4 ケース 1 CE-Router（DHCPv6-PD 非対応）or ONU 直結

(2) ケース 2　DHCPv6-PD のみによる IPv6 サービス方式

CE-Router の WAN 側は、リンクローカルアドレスが生成されグローバルアドレスは持たない。LAN 側には、DHCPv6-PD によるアドレス配布を実施する。CE-Router のない加入者は、端末を直結してもアドレス配布はされず、リンクローカルアドレスの生成がされるだけである。また、加入者が接続する CE-Router によって IPv6 の対応状況が異なるため注意が必要である。

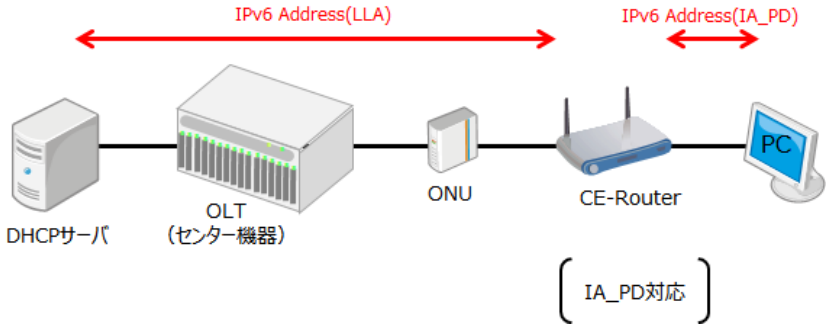


図 7.5 ケース 2 CE-Router（IA_PD 対応）

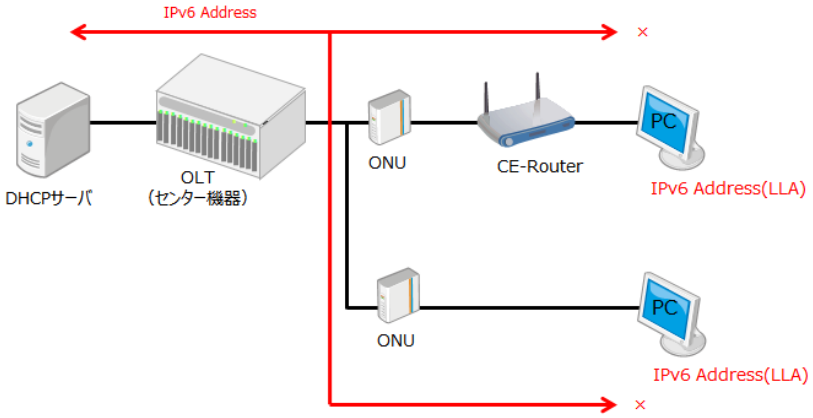


図 7.6 ケース 1 CE-Router（DHCPv6-PD 非対応）or ONU 直結

7.2.2 IPv4 と IPv6 のサービス形態

3 つの方式について注意点も含めて以下に述べる。

(1) デュアルスタック 方式

FTTH 網も含めてデュアルスタック化されている構成である。IPv4 の通信も IPv6 の通信も FTTH 網にそのまま流れるため、運用時に ONU 配下の PC 端末数等の制御が PON 装置で比較的容易に行える。本稿では FTTH を使用した恒常的な IPv6 ネットワーク構築の方式として本方式を推奨する。

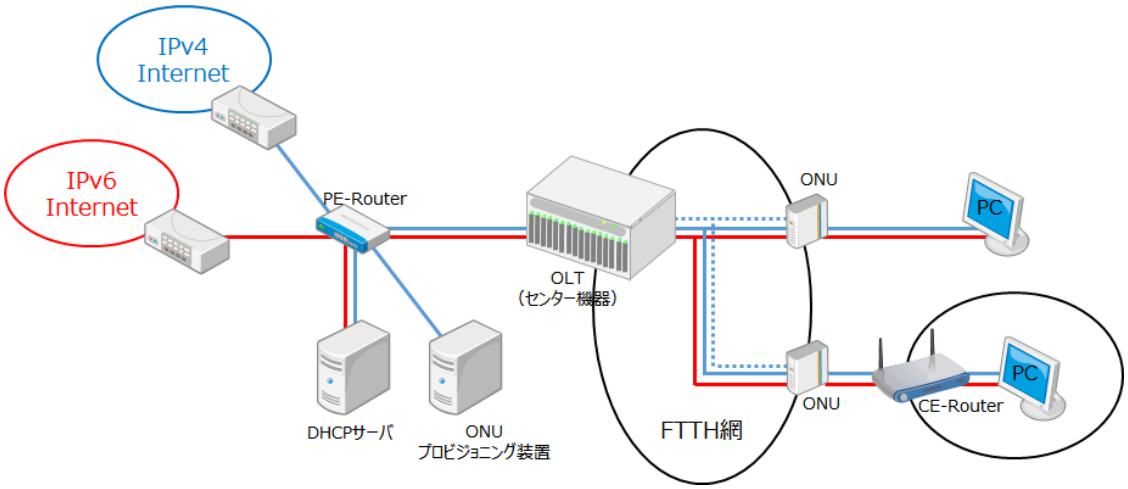


図 7.7 デュアルスタック方式の設備構成例

(2) IPv4 トンネル方式

OLT から加入者側の経路が IPv4 の方式である。IPv6 パケットも IPv4 の FTTH 網を通るので IPv4 パケットにカプセル化された IPv6 パケットが設定されたフィルタ等を正しく通過するかどうかを確認する必要がある。なお、本方式は納期などの問

題により IPv4 を使用したネットワークで IPv6 通信を先行して試したい場合に使用する事が考えられる。

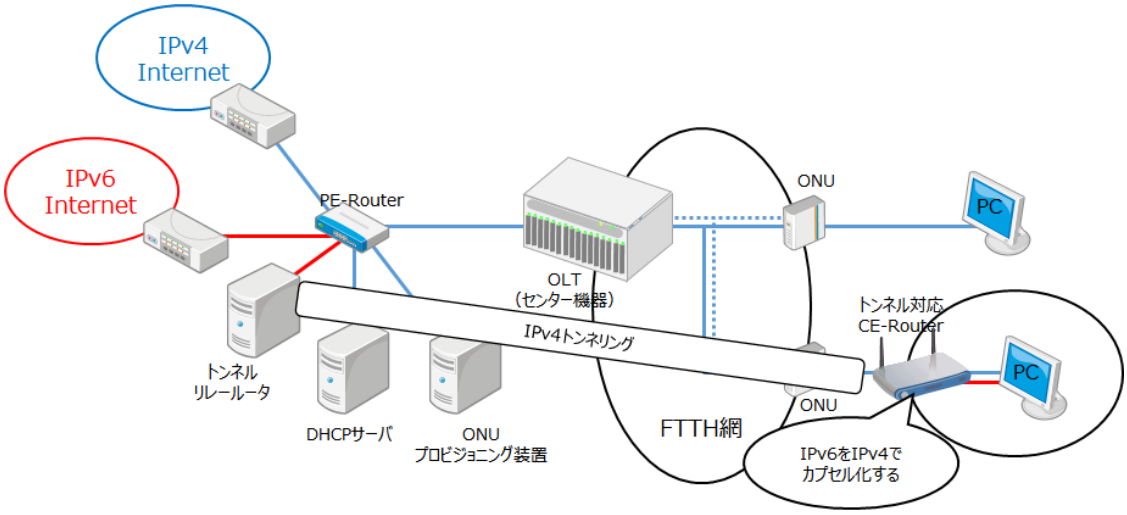


図 7.8 IPv4 トンネル方式の設備構成例

(3) IPv6 トンネル方式

OLT から加入者側のすべての経路が IPv6 の方式である。IPv4 パケットも IPv6 の FTTH 網を通るので IPv6 パケットにカプセル化された IPv4 パケットが FTTH 網内に設定されたフィルタなどを正しく通過するかどうかを確認する必要がある。本方式はデュアルスタックを構成した後、IPv4 アドレスが枯渇した場合に LSN の代わりに使用する事が考えられる。

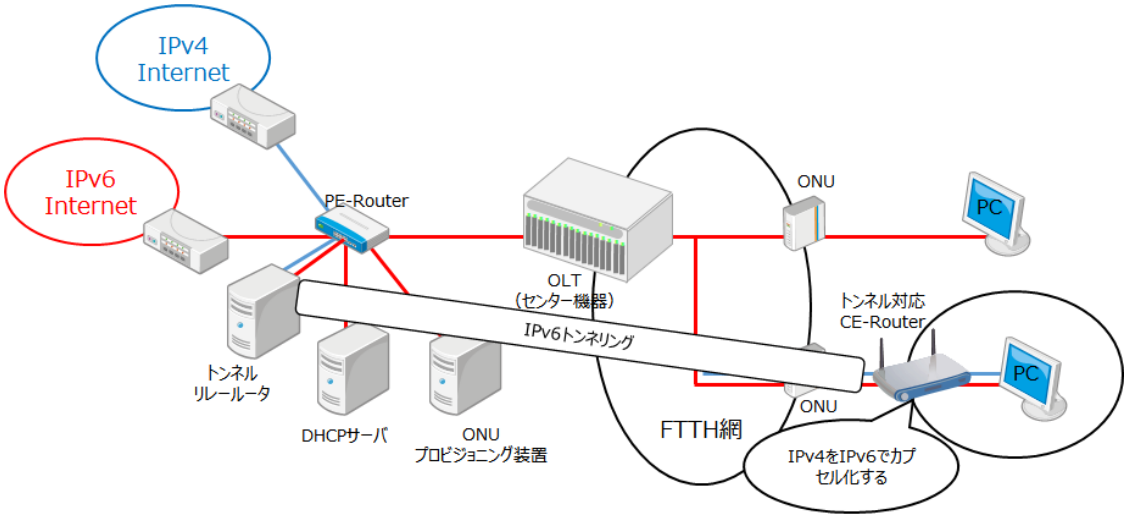


図 7.9 IPv6 トンネル方式の設備構成例

7.3 ネットワーク構成

基本的な構成を図 7.10 に示す。OLT は上位のルータ/L3SW に接続される。OLT は CMTS 同様に L3 機能を持つ装置と、L2 機能のみを持つ装置がある。ここでは L2 機能のみを持つものに関して述べる。

L2 OLT 環境では上位のルータ/L3SW が CPE のデフォルトゲートウェイとなる。IPv4 サービスで実施していた CPE 間通信の禁止や Windows 共有の防止、ルータ逆接続の禁止、デフォルトゲートウェイ乗っ取りの防止などのセキュリティコントロールは IPv6 でも同様に実施する必要がある。IPv4 で実施していたセキュリティ機能が IPv6 でも実装されているか、OLT とルータ/L3SW のいずれがどのセキュリティコントロールを担うかは改めて整理・検討が必要となる。

DHCPv6-PD サービスを行う場合、ルータ/L3SW 側で Route Injection を行う必要がある。L3SW の Route Injection 機能は CMTS ほど実績がなく、ローエンドの機種などは非サポートのものもある。Injection できる経路数が思いのほか少ない場合もあるため事前にベンダに仕様を確認する必要がある。

ルータ/L3SW で IPv6 デュアルスタックを利用する場合、IPv4 ARP エントリ数と比較して IPv6 ND エントリ数のキャパシティが大きく減る場合があるのであらかじめ仕様を確認しておいたほうがよい。その他、経路テーブル数、ACL エントリ数、ルータ逆接続防止のエントリ数など、各種リソースについてもデュアルスタック化することで IPv4 のみで利用した場合のカタログ値から大きく数を減らす場合があるので確認が必要である。IPv4/IPv6 の経路テーブル数は 1:2 などの割合で動的にエントリを消費する場合と、デュアルスタックを有効化した時点で固定的に割り当てられる場合がある。いずれの場合にもデュアルスタック化に伴い、IPv4 のみの場合と比べて各種エントリ容量が減ることが多いので確認することが必要である。

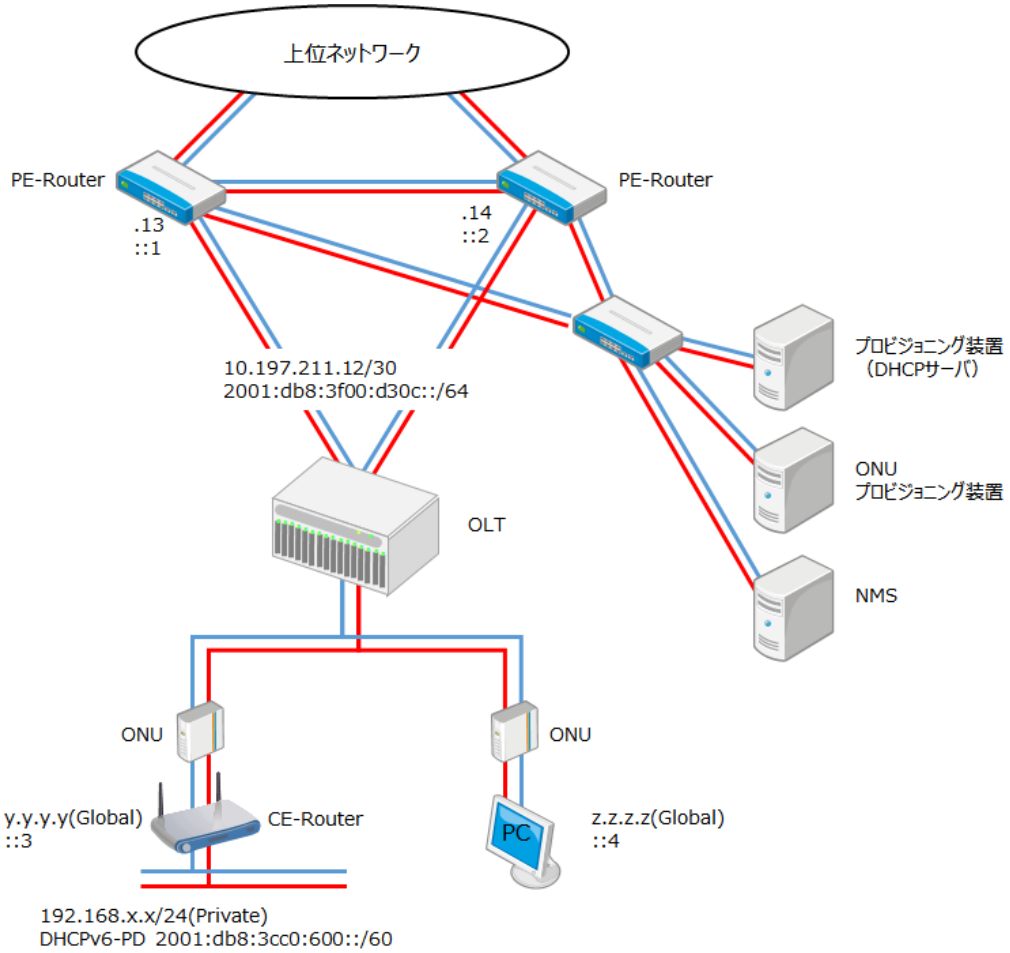


図 7.10 FTTH ネットワークの基本構成

7.4 CPE の接続形態

7.4.1 CPE 接続形態の概要

IPv6 アドレス割り当て方法において CPE には DHCPv6 で、ルータには DHCPv6-PD で Prefix を割り当てるかである。サービス面において IPv4/IPv6 アドレス割り当て数の制限について CPE 接続形態の概要と MAC 制限、IPv4 アドレス付与の方法、IPv6 アドレス付与の方法を表 7.1 にまとめた。

表 7.1 CPE 接続形態と運用について

接続形態	CPE 単体接続	CPE 複数台接続	CE-Router 接続型
接続対象端末接続許可台数	PC を 1 台のみ接続するか CE-Router 1 台接続。 CE-Router 配下に事業者の設定した台数制限に関係なく CPE を接続できる。	HUB を介して複数台の PC を接続。 PC の代わりに CE-Router を接続することもある。	DHCPv6-PD クライアントを実装する CE-Router のみを接続。
MAC	IPv4 のみサービスでは IPv6 は CE-Router でフィルタ、ONU に流れない動きを想定。 IPv6 は IPv6 ブリッジ機能により CPE から ONU に到達。 IPv6 接続の場合は MAC 数の制限は現実的ではない。	接続を許可する台数分の MAC が ONU に認識されるため、OLT または ONU で接続許可台数を設定。 CE-Router 接続を想定すると左記同様に MAC 数制限は現実的ではない。	CE-Router 1 台接続を想定するため許可する MAC は 1。
IPv4	CE-Router の WAN-IF に 1 つ付与。 CPE は CE-Router の NAT 機能で複数 CPE を接続できる。	PC もしくは CE-Router の WAN-IF に 1 つずつ付与。 CE-Router 配下の CPE は NAT 機能により許可 CPE 台数を超えて接続できる。	CE-Router の WAN-IF に対して 1 つ付与。
IPv6	CPE は ONU に接続。CPE へのアドレス付与は DHCPv6 となる。 接続可能 CPE 数は付与する Global アドレス数、もしくは CE-Router の WAN 側 MAC も含めた MAC アドレス数で設定する。	CPE が HUB を介して ONU に接続される。 CPE へのアドレス付与は DHCPv6 となる。 接続可能 CPE 数は付与する Global アドレス数、もしくは CE-Router の WAN 側 MAC も 含めた MAC アドレス数で設定する。	CE-Router の LAN-IF に/64 以上の Prefix を 付与。 WAN-IF では Link Local のみか、Global を付与するかについては CE-Router の実装によるが SLAAC は利用しない。

7.4.2 CPE 単体接続

(1) CPE1 台のみ接続の概要

PC を 1 台のみ接続するか、もしくは CE-Router1 台を接続する。CE-Router を接続した際にはその配下にケーブル事業者の設定した接続台数制限に関係なく CPE を接続できる形態である。現在のケーブルインターネットで最も多い形態である。実際にはケーブル事業者は ONU の配下に接続できる端末数を MAC Address

数の制限する方法で許可、MAC Address=1 としている。この形態では加入者が CE-Router を利用するか 1 台の CPE を接続するかについては管理しない。

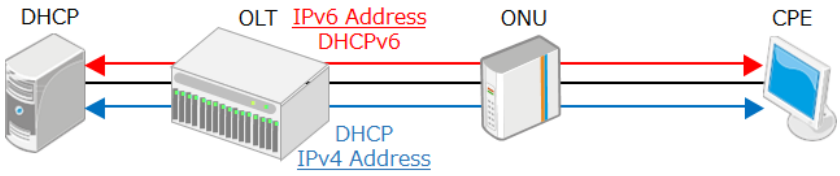


図 7.11 CPE 単体接続型

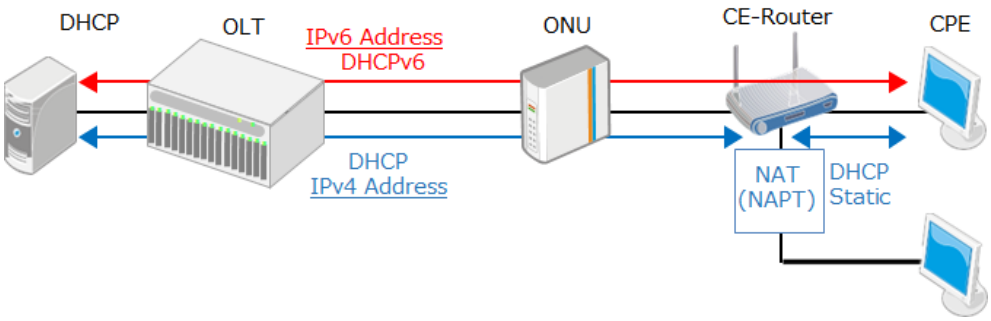


図 7.12 CPE 単体接続(CE-Router を接続した場合)

(2) IPv4 アドレス割り当て方法

ケース 1、ケース 2 ともに PC もしくは CE-Router の WAN インタフェースへの IPv4 アドレスは、DHCP によりケーブル事業者が保有するアドレス空間から割り当てる。また、固定でアドレスをマニュアルで割り当てる場合もある。

(3) IPv6 アドレス割り当て方法

(ア) ケース 1

IPv6 アドレス割り当てはステートフル DHCPv6 にてケーブル事業者が保有するアドレス空間から割り当てる。この際、DHCPv6 サーバは Advertise および Reply で DNS cache server address Option 他、必要なオプションを含める。CPE の OS によって Stateful DHCPv6 が利用できない場合がある。この場合でもユーザトレーサビリティの観点で SLAAC を利用することは好ましくない。

(イ) ケース 2

IPv6 アドレス割り当ては IA_PD が流れるのみで、PC は IPv6 アドレスを持たない。

(4) ユーザトレーサビリティ

IPv4 と同様、IPv6 アドレスから利用者を特定するユーザトレーサビリティについても必要となる。abuse 対応をするときなど、利用時間と IPv6 アドレスから利用者を特定する環境を構築することが必要である。DHCPv6 サーバの割り当てログや、FTTH ネットワークにおける上位 L3 機器などの Neighbor Cache 情報や OLT のログ情報を利用することが考えられる。

(5) CPE 数の制限

IPv4 のみのサービスで ONU に接続される CPE 数の制限を行う際、OLT／ONU の機能 を用い、MAC Address をカウントして制限する方法が一般的だった。デュアルスタックにおいて CPE 数を制限する場合も IPv4/IPv6 ともブリッジ接続となる場合には CPE 数制限として MAC Address をカウントすることで問題はない。多くの加入者では CE-Router を利用しており、このうち IPv4 は NAT(NAPT)で IPv6 はブリッジするタイプがある。ブリッジ型接続でもその仕様の CE-Router を用いていることを前提として CPE 数の制限を考えることが望ましい。CPE 数制限の方法については OLT/ONU の仕様を確認する必要がある。

7.4.3 CPE 複数台接続

(1) CPE 端末台接続の概要

HUB を介して複数台の PC を接続する。PC の代わりに CE-Router を接続することもありうる。この形態は OLT／ONU の機能において接続可能な MAC Address 数の制限を 2 以上の値に設定することで実現している。端末 1 台接続の場合と同じで HUB を介して PC のみを接続させるか、その一部に CE-Router を利用するかについては事業者として管理しない。

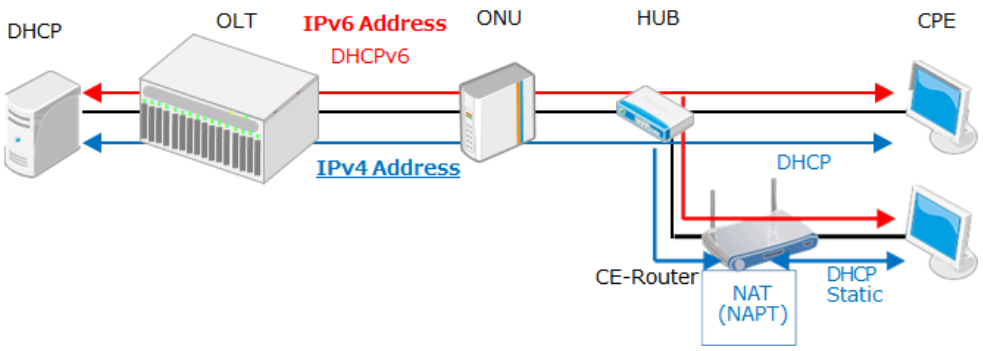


図 7.13 CPE 複数台接続

(2) IPv4 アドレス割り当て方法

ケース 1、ケース 2 ともに PC もしくは CE-Router の WAN インタフェースへの IPv4 アドレスは DHCP によりケーブル事業者が保有するアドレス空間から割り当てる。また、固定でアドレスをマニュアルで割り当てる場合もある。

(3) IPv6 アドレス割り当て方法

(ア) ケース 1

IPv6 アドレス割り当てはステートフル DHCPv6 にてケーブル事業者が保有するアドレス空間から割り当てる。この際、DHCPv6 サーバは Advertise および Reply で DNS cache server address Option 他、必要なオプションを含める。CPE の OS によって Stateful DHCPv6 が利用できない場合がある。この場合でもユーザトレーサビリティの観点で SLAAC を利用することは好ましくない。

(イ) ケース 2

IPv6 アドレス割り当ては IA_PD が流れるのみで、PC は IPv6 アドレスを持たない。

(4) ユーザトレーサビリティ

IPv4 と同様、IPv6 アドレスから利用者を特定するユーザトレーサビリティについても必要となる。abuse 対応をするときなど、利用時間と IPv6 アドレスから利用者を特定する環境を構築することが必要である。DHCPv6 サーバの割り当てログや、FTTH ネットワークにおける上位 L3 機器などの Neighbor Cache 情報や OLT のログ情報を利用することが考えられる。

(5) CPE 数の制限

IPv4 のみサービスで ONU に接続される CPE 数の制限を行う際、OLT/ONU の機能を用いて MAC Address をカウントして制限する方法が一般的だった。デュアルスタックにおいて CPE 数を制限する場合も IPv4/IPv6 ともブリッジ接続となる場合には CPE 数制限として MAC Address をカウントすることで問題はない。多くの加入者で CE-Router を利用しており、このうち IPv4 は NAT(NAPT)で IPv6 はブリッジするタイプがある。ブリッジ型接続でもその仕様の CE-Router を用いていることを前提として CPE 数の制限を考えることが望ましい。CPE 数制限の方法については OLT/ONU の仕様を確認する必要がある。

7.4.4 CE-Router 接続型

(1) CE-Router 接続型の概要

IPv4 としては NAT(NAPT)を実装し、IPv6 では DHCPv6-PD クライアントを実装する CE-Router のみを接続する。

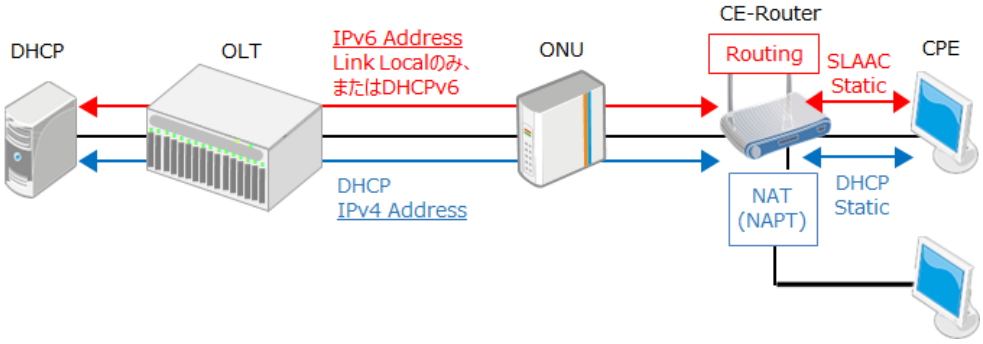


図 7.14 ルータ接続型

(2) IPv4 アドレス割り当て方法

CE-Router の WAN インタフェースへの IPv4 アドレスは DHCP によりケーブル事業者が保有するアドレス空間から割り当てる。固定でアドレスを割り当てる場合には加入者がアドレスをマニュアルで割り当てるため DHCP は必要ない。

(3) IPv6 アドレス割り当て方法

(ア) ケース 1

CE-Router において、WAN 側が IA_NA 対応であれば、ステートフル DHCPv6 による割り当て、非対応であれば LLA のアドレス生成がされる。

CE-Router の WAN 側インタフェースは、CPE が SLAAC でアドレスを生成しないよう CE-Router においても SLAAC を利用することは望ましくない。

CE-Router の LAN インタフェースのネットワーク用として Prefix を DHCPv6-PD で割り当てる。CPE は CE-Router の LAN 側に接続され LAN インタフェースからの RA に基づいて SLAAC によりアドレスを生成することが可能となり、DHCPv6 をサポートしない OS においても IPv6 を利用できるようになる。RA に DNS Option を盛り込む仕様が RFC8106 で規定されている。CE-Router の LAN 側に設置された CPE が SLAAC で IPv6 アドレスを生成する際、今後、この仕様に沿って DNS を RA で取得することを考え DHCv6-PD の際にも DHCPv6 サーバは

Advertise および Reply で DNS cache server address Option を含めるべきである。

（イ） ケース 2

CE-Router の WAN 側は LLA のアドレス生成がされる。

CE-Router の LAN インタフェースのネットワーク用として Prefix を DHCPv6-PD で割り当てる。CPE はルータの LAN 側に接続され LAN インタフェースからの RA に基づいて SLAAC によりアドレスを生成することが可能となり、DHCPv6 をサポートしない OS においても IPv6 を利用できるようになる。CE-Router の WAN 側インタフェースは Link Local Address のみでもかまわないが、Global Unicast Address を割り当てる場合には ONU に接続された CPE が SLAAC でアドレスを生成しないよう CE-Router においても SLAAC を利用せず、Stateful DHCPv6 を用いることが望ましい。RA に DNS Option を盛り込む仕様が RFC8106 で規定されている。CE-Router の LAN 側に設置された CPE が SLAAC で IPv6 アドレスを生成する際、今後、この仕様に沿って DNS を RA で取得することを考え DHCv6-PD の際にも DHCPv6 サーバは Advertise および Reply で DNS cache server address Option を含めるべきである。

(4) ユーザトレーサビリティ

IPv4 と同様、IPv6 アドレスから利用者を特定するユーザトレーサビリティについても必要となる。abuse 対応をするときなど、利用時間と IPv6 アドレスから利用者を特定する環境を構築することが必要である。DHCPv6 サーバの割り当てログや FTTH ネットワークにおける上位 L3 機器などの Neighbor Cache 情報や OLT のログ情報を利用することが考えられる。

(5) CPE 数の制限

接続される端末は CE-Router に限られるため OLT/ONU の機能により MAX CPE を 1 として CPE の MAC Address 数を管理することで可能である。これにより接続できる CE-Router 数を制限でき、合わせて DHCPv6-PD で割り当てる Prefix 数を制限できる。この場合、IPv4 アドレスは CE-Router の WAN インタフェースへ付与されるアドレスに限られ、複数 CPE においては CE-Router の LAN 側の Private アドレス領域を用いる。IPv6 は割り当てられた Prefix の内のアドレスを CE-Router の LAN 側に接続された CPE が利用する。

(6) DHCPv6-PD で割り当てられた Prefix へのルートの広報

DHCPv6-PD で CE-Router への Prefix が割り当てられた際、どの CE-Router 配下にあるかは OLT の上位のネットワーク機器にて Routing Table を生成して管理するが、さらに上位のルータに、その Prefix が当該の OLT の上位のルータの先にあることが Routing 情報として広報されなければならない。OSPFv3 を利用する場

合には OLT の上位のルータからの広報でこれが通知される。OSPFv3 等の Dynamic Routing を使用しない場合には、当該の OLT に割り当てられる Prefix の領域を PE-Router に Static Route として設定しておく必要がある。

(7) 割り当てサイズ

1 台の CE-Router に DHCPv6-PD で割り当てる Prefix 長は DHCPv6 サーバ側で設定される。CE-Router の LAN 側には/64 の Prefix を生成する。DHCPv6 サーバでは/60～/48 の Prefix を割り当てる。/48 で割り当てれば、IPv6 アドレスの第 3 オクテット目までを事業者で構成設計し、第 4 オクテット目を CE-Router が任意に設定することになるため、IPv6 アドレスの設計が容易になる。

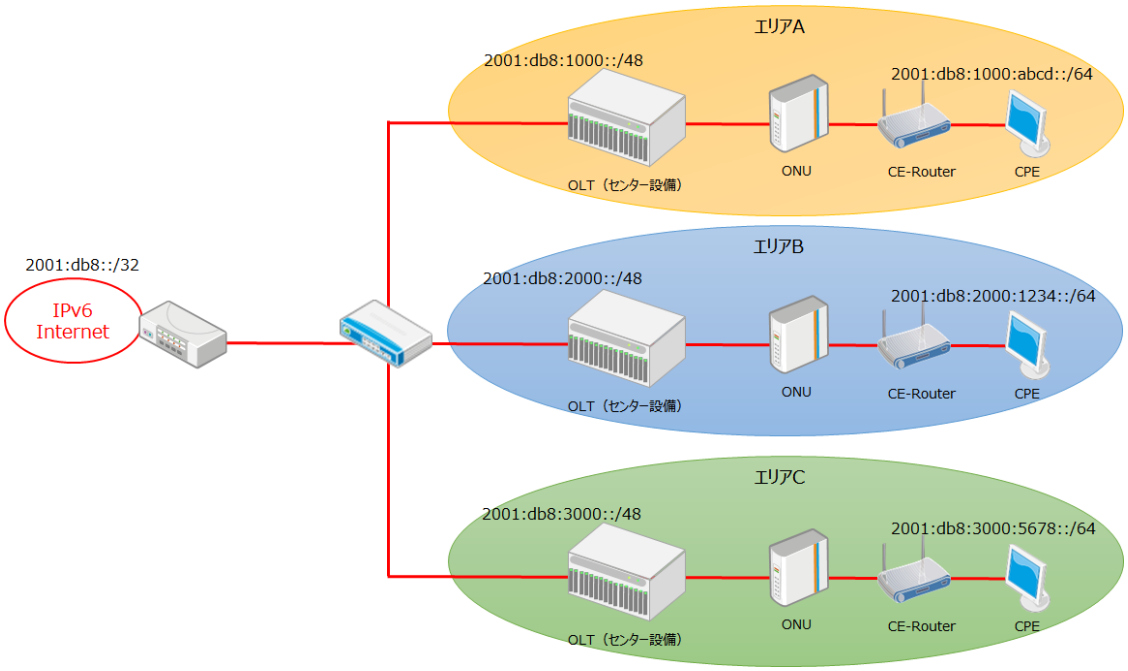


図 7.15 割り当てサイズ例（Prefix /48）

7.5 IPv6 サービス構築上の検討ポイント

7.5.1 CPE プロビジョニングに関して

(1) IPv4/IPv6 の CPE プロビジョニングの違い

PON 構成における CPE プロビジョニングは、IPv4 と IPv6 のいずれかの場合で、プロビジョニング方法が異なる。さらに、OLT の運用設定が L2 モードと L3 モードのいずれかの場合でも検討ポイントが異なる。本ガイドラインでは、CATV 事業者の OLT 導入事例としては比較的に一般的な L2 モードのケースを前提とする。OLT が L2 モードである場合、CPE プロビジョニングに必要な L3 機能を具備した装置（L3SW/ルータ）を OLT の上位へ接続したシステム構成とする必要がある。

また、DPoE（vCM）プロビジョニングについては、主要 PON チップベンダが開発を継続しないことを表明しており、将来性が不透明であることから本ガイドラインの対象外とする。その他にも、EoC など特殊な構成は対象外とする。

以上を踏まえ、IPv4 構成と IPv6 構成のそれぞれについて、DHCP を用いた CPE プロビジョニング例を示す。

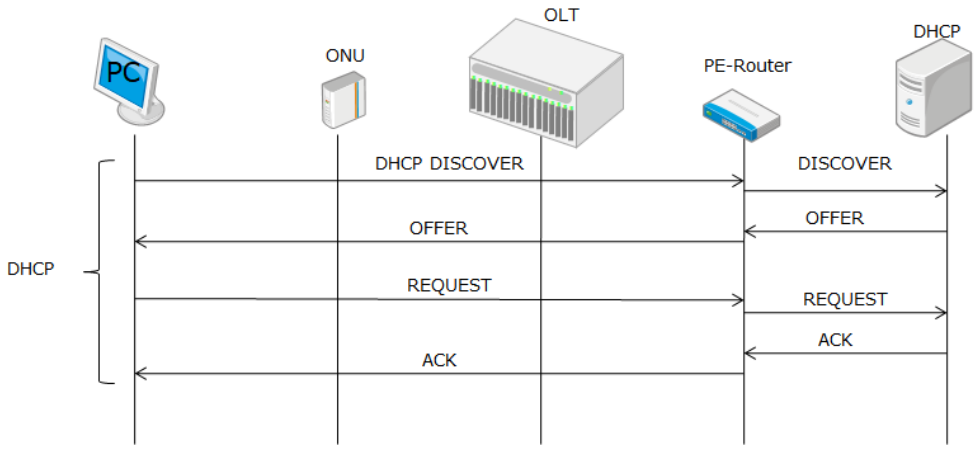


図 7.16 IPv4 構成時の CPE プロビジョニング例

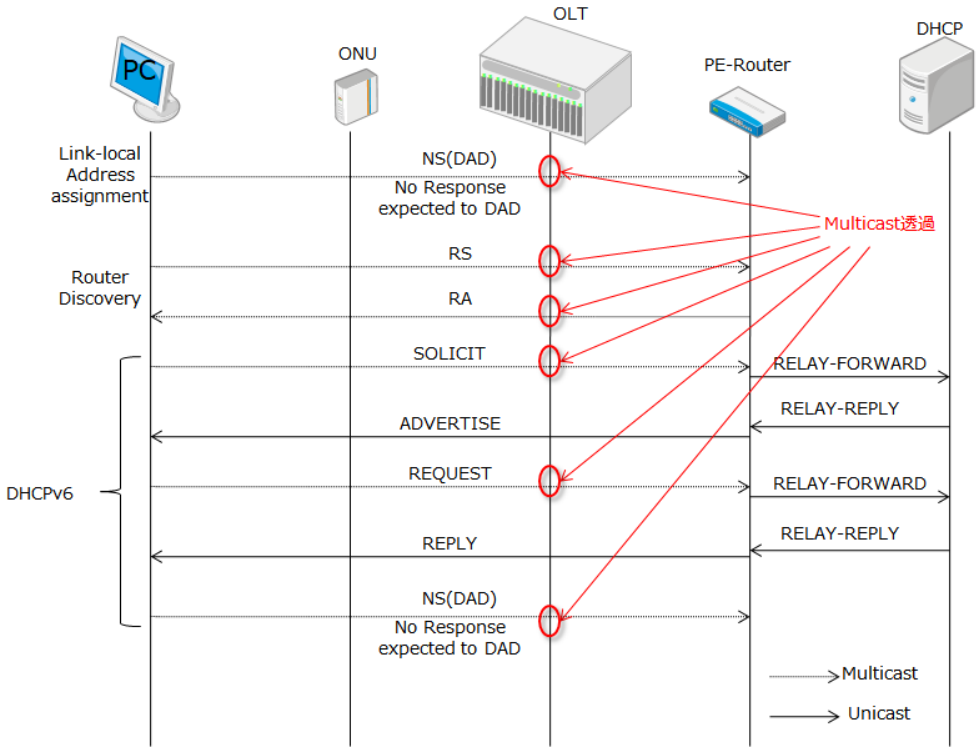


図 7.17 IPv6 構成時の CPE プロビジョニング例（DHCPv6 利用時）

IPv4 構成の CPE プロビジョニングは、CPE からの DHCP（Broadcast）パケットに対して、OLT は透過転送（必要に応じて DHCP Option82 を付与）し、L3SW は DHCP サーバへリレー転送する方式となる。一方、IPv6 では Broadcast は廃止されており、IPv6 マルチキャストへ統合されている。そのため、IPv6 構成の CPE プロビジョニングは、CPE からの DHCPv6（IPv6 マルチキャスト）パケットに対して、OLT は透過転送（必要に応じて DHCPv6 Option18/37 を付与）し、L3SW は DHCP サーバへリレー転送する方式となる。さらに、IPv6 構成では DHCP だけでなく、上り方向の RS（IPv6 マルチキャスト）や下り方向の RA（IPv6 マルチキャスト）の透過転送が必要となる。したがって、OLT および ONU については、対象 IPv6 マルチキャストパケットの転送仕様やフィルタ設定に注意が必要である。

また、DOCSIS 構成における CMTS の L3 モードによる運用は一般的であるが、PON 構成における OLT の L3 モード運用は比較的少数であるため、OLT は L2 モードで運用することが多い。この場合、OLT と L3SW の組み合わせが必須となり、L3SW に要求される IPv6 機能も重要な検討ポイントとなる。

(2) CPE プロビジョニング使用時の注意点

CPE プロビジョニングが IPv4 の場合、OLT が保持する MAC アドレスエントリのエージアウトタイマと PE-Router が保持する ARP エントリのエージアウトタイマに時間差があると、上位から CPE への通信不能となる不具合が発生することがある。例として、OLT の MAC アドレスエントリのエージアウトタイマが PE-Router の ARP エントリのエージアウトタイマよりも短い場合、OLT の MAC アドレスエントリからエージアウトした時点で対象 MAC アドレスの CPE への通信が不能となる（OLT が未学習ユニキャストフレームをフラッディング動作する場合は例外）。そのため、CPE プロビジョニングが IPv6 の場合も同様のことが発生するため、PE-Router の ND エントリのエージアウトタイマの設定値に注意が必要となる。

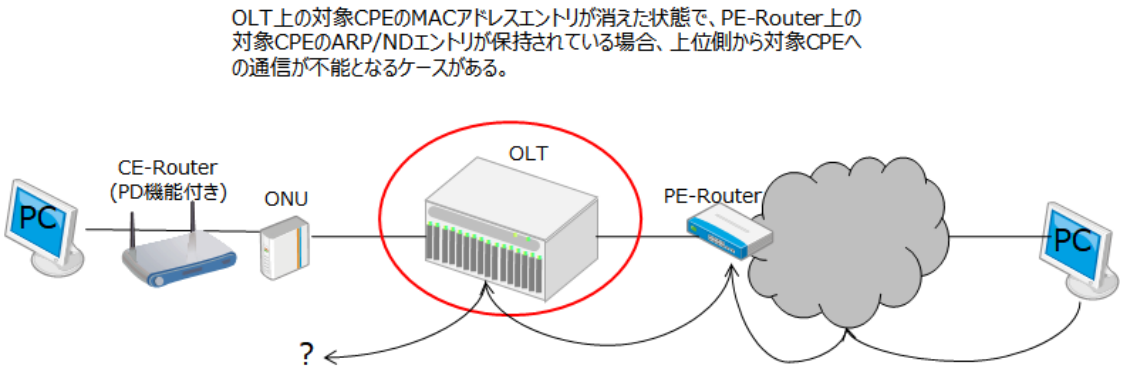


図 7.18 CPE プロビジョニング時の注意例

このような場合、OLT の MAC アドレスエントリのエージアウトタイマを PE-Router の ARP/ND エントリのエージアウトタイマよりも長く設定することで回避できる。

7.5.2 DHCPv6-PD 利用時の注意点

IPv6 による CPE プロビジョニングに DHCPv6-PD を利用する場合、OLT による DHCPv6 Option18/37 の挿入に注意が必要となる。OLT の旧機種では、DHCP リレーエージェントでないにも関わらず、DHCPv6 Option18/37 を挿入する際に、DHCPv6 Solicit/Reply を Relay-Forward でリレー転送する仕様の OLT が存在するためである。

このとき、OLT が L2 モードの場合は、PE-Route にて PD 経路の Route Injection が必要となるが、DHCPv6 パケットが Relay-Forward/Relay-Reply の場合は Route Injection が動作しない L3SW がある。Route Injection が動作しないと PD 経路が生成されないため、対象 DHCPv6-PD 端末はインターネット通信できない。このような環境では、DHCPv6-PD 端末を運用上使用できないことになる。

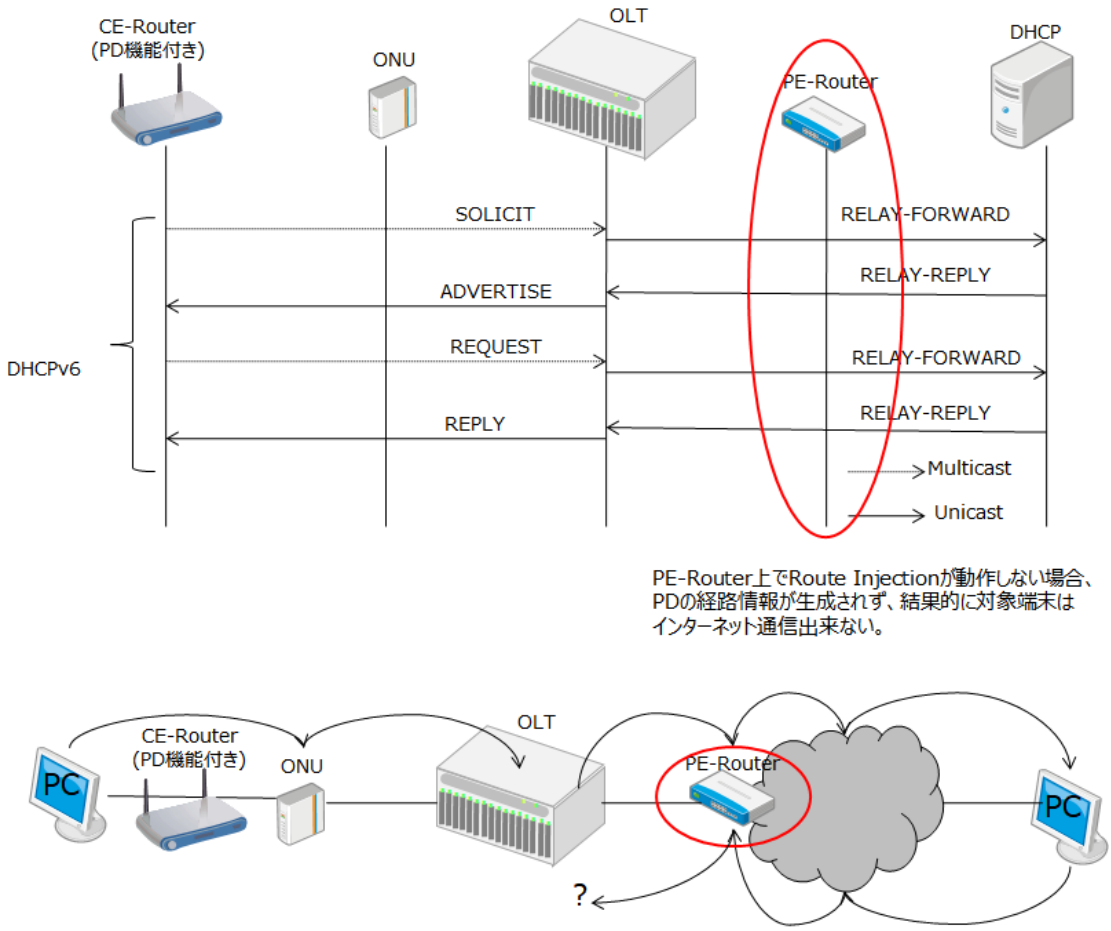


図 7.19 IPv6 構成時の OLT リレーエージェント設定時の注意点

OLT が L2 モードの場合、DHCPv6-PD を利用する際は、OLT だけでなく L3SW と組み合わせたシステム的な動作確認が重要である。また、このようなケースについては、OLT の DHCPv6 Option18/37 挿入機能を利用せず、OLT の DHCPv6 Snooping/DHCPv6-PD Snooping 機能による DHCPv6 バインディング情報の Syslog/SNMP Trap 送出機能によってユーザトレースを実現する方法もある。しかし、現在の主要な OLT は DHCPv6 Option18/37 を挿入する際、DHCPv6 Solicit/Advertise はそのまま転送する仕様となっているため、同様の問題は発生しない。

7.5.3 OLT と L3SW によるパケットフィルタ

フィルタ要件（逆 RA 対策、逆接続 DHCPv6 対策、Windows 共有対策、ウイルス対策、OP25B、IP53B、IP123B）については、OLT、もしくは L3SW にて対応が必要となるが、機器依存になるため機能実装有無について担当ベンダへの確認が必要である。本ガイドラインの前版発行時は OLT による対象機能の実装は少なかったが、10G 対応モデル等の比較

的新たな OLT には実装されていることが多い。また、このフィルタ要件の中で、逆 RA 対策機能は OLT に実装されているべきであり、現在では一般的に実装されている機能である。

7.6 IPv6 対応のための機能

FTTH ネットワークを IPv6 対応するためには、OLT などの PON 装置だけでなく、上位のネットワーク機器に関しても注意が必要である。上述したように OLT が L3 モード運用でない場合は、L3SW の IPv6 機能を効果的に活用する事が重要となる。以下に検討項目について述べる。

(1) デュアルスタックおよび IPv6 トンネルの際に使用する L3SW

OLT が L3 モード運用ではない場合、L3SW による IPv4/IPv6 通信の制御や RA の送出、RS への応答、DHCPv6 リレーエージェント機能、DHCPv6 Option18/37 の透過リレー転送機能が必要となる。また、DHCPv6-PD 運用のために、PD 経路の Route Injection 機能が必要である。Route Injection は、DHCPv6 パケット（IA-PD）を基に L3SW 自身のルーティングテーブルに PD 経路を挿入する機能である。Route Injection により挿入された PD 経路は、当該 DHCPv6（IA-PD）のリース期限が切れると同時に削除される。課題として、L3SW の再起動や対象インタフェースのダウンが発生すると、Route Injection によって挿入された PD 経路は、ルーティングテーブル上から削除され、DHCPv6-PD 端末は DHCP 再取得するまでインターネット通信が不能となる問題がある。これについては、Bulk Lease query（RFC5460）を利用したルーティングテーブルの再構築機能により回避できるが、機能実装した L3SW は少ない。仮に Bulk Lease query 機能を利用する場合は、DHCPv6 サーバも、この機能に対応する必要がある。

(2) PON のデュアルスタック対応

デュアルスタック運用にて IPv4 グローバルアドレスを加入者へ割り当てるサービスである場合、IPv4 グローバルアドレスは枯渇状況であるため、OLT には CPE への IPv4/IPv6 払出制限機能が必要となる。制限手法は機器依存となるが、一般的な手法について述べる。IPv4/IPv6 払出制限機能は、DHCPv4 snooping、DHCPv6/DHCPv6-PD snooping 機能の一部であり、当該 Snooping 機能により作成された DHCP Binding テーブルに基づき、IPv4 端末 n 台、IPv6 端末 m 台というように IPv4/IPv6 を識別して制御することが可能となる。これにより、IPv4 グローバルアドレスは消費を抑制し、IPv6 アドレスは多数払い出すことを同時に実現する機能である。このとき、DHCPv6-PD 端末の IPv6 アドレスについては、WAN 側と LAN 側は別々にカウントし、LAN 側は Prefix 単位でカウントする。そのため、WAN 側に IPv6 グローバルアドレスが 1 個割り当てられ、LAN 側に 1 個の Prefix が割り当てられた場合は、2 台とカウントする。

また、マルチキャストについては無制限に透過転送するわけではなく、IPv6 構成の CPE プロビジョニング時の上り RS、下り RA、DHCPv6 パケットや MLD snooping に基づいたマルチキャストストリーミングの転送など制限が必要である。

7.7 IPv6 導入手順

(1) IPv6 対応の PON の導入

FTTH ネットワークを IPv6 対応にする場合、7.2 で説明のあった 3 つの方式のうちデュアルスタックおよび IPv6 トンネルの場合は使用する PON で IPv6 のストリームが流れることが必要となる。またデュアルスタックで運用を行う場合、単に IPv4 と IPv6 のストリームが流れるだけでなく、現実的には IPv4 と IPv6 のネットワークをそれぞれ管理する必要がでてくる。そのため具体的には同じ物理ポートに対して IPv4 と IPv6 をそれぞれ設定する機能や DHCPv6-PD の Snooping を行える機能が必要となる。

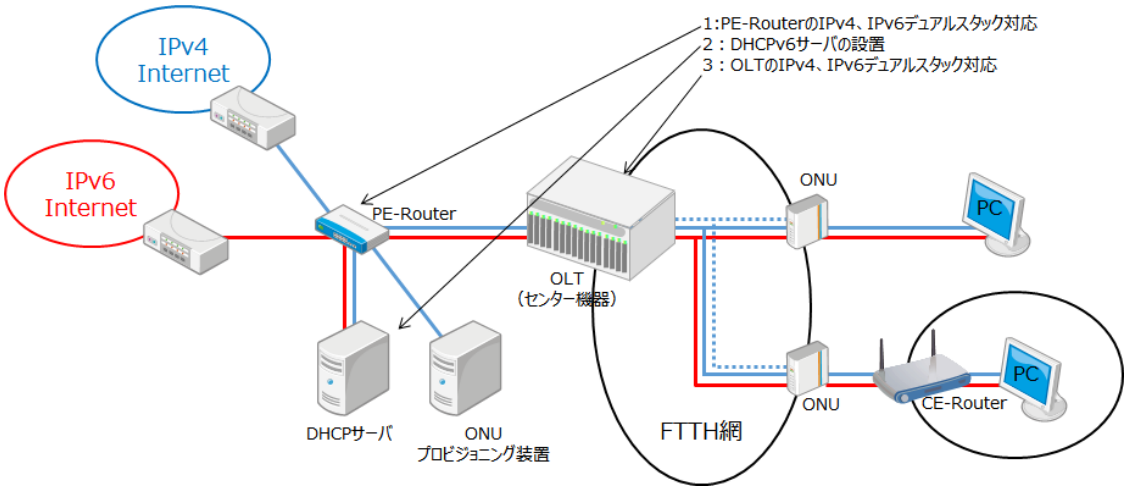


図 7.20 デュアルスタック方式の設備構成時の注意点

(2) DHCPv6 サーバの設置

FTTH 網に接続された PC は上位ネットワークから DHCPv6 によって IPv6 アドレスを割り当てられるので L3SW の配下に DHCPv6 に対応したサーバの設置が必要である。

(3) OLT の IPv4/IPv6 デュアルスタック対応

加入者トラヒックに対するセキュリティ機能が IPv6 に対応していることが必要である。必要に応じてソフトウェアのバージョンアップやハードウェアの更新を行う。OLT マネージャやプロビジョニング装置、SMS 連携などについても IPv6 に

対応しているかを確認する。IPv4 と同様のセキュリティを実現することが望ましい。

(4) PE-Router のデュアルスタック対応

ゲートウェイとなる PE-Router をデュアルスタック化する。7.3 で述べたように、IPv6 ルーティングテーブルのエントリ数、ND エントリ数、DHCPv6-PD Snooping、および Route Injection 経路数など、IPv6 関連のハードウェアキャパシティとデュアルスタック化にともなう IPv4 関連のハードウェアキャパシティの減少量はあらかじめ把握しておく。CMTS と同様にデュアルスタックの利用に際しては機能サポートの面などから、ソフトウェアの更新を必要とするケースがあること、またデュアルスタックを有効化するために筐体再起動を要することが多いことから、あらかじめサービス中断を念頭に置いて準備することが望ましい。

(5) PE-Router での IPv6 関連機能有効化

(6) PE-Router をデュアルスタック化したのち、IPv6 関連の設定を行う。セキュリティコントロール機能の設定などを IPv4 と同様に行う。必要に応じて Route Injection の有効化を行う。

(7) ONU の再起動

OLT/ONU に IPv6 関連のフィルタが入っている場合、削除を行い必要に応じて ONU の再起動を実施する。

第8章　IPv4 over IPv6 通信技術を使った IPv6 シングルスタック

8.1　IPv4 over IPv6 通信技術を使った IPv6 シングルスタック化について

ケーブル事業者のネットワークに IPv6 シングルスタックを採用した場合、事業者側のネットワーク（アクセス網）は IPv6 設備のみとなるが、この IPv4 over IPv6 通信技術を利用することでユーザに対しては IPv4 と IPv6 のデュアルスタックの接続を提供できる。これにより、デュアルスタックに比べネットワークの設備、運用コストを軽減することができる。以下に、IPv4 over IPv6 通信技術を利用した IPv6 シングルスタックのネットワーク構成について述べる。

8.1.1　IPv4 over IPv6 通信技術を利用した IPv6 シングルスタックのネットワーク構成

IPv6 シングルスタックでは、CATV 事業者設備に IPv4 over IPv6 通信技術を利用するための装置が必要となる。IPv4 over IPv6 通信サービスを提供するために、センター側に IPv4 over IPv6 通信技術装置を設置し、同様に CE-Router も IPv4 over IPv6 通信技術に対応する必要がある。このネットワーク構成を図 8.1 に示す。

宅内からの接続先が IPv4 インターネットの場合、センター側 IPv4 over IPv6 通信技術装置と対応する CE-Router 間は IPv6 で通信を行い、事業者側ネットワークも IPv6 通信となる。接続先が IPv6 インターネットであれば、CPE（PC）から IPv4 over IPv6 通信技術装置を介さず IPv6 で直接通信を行う。

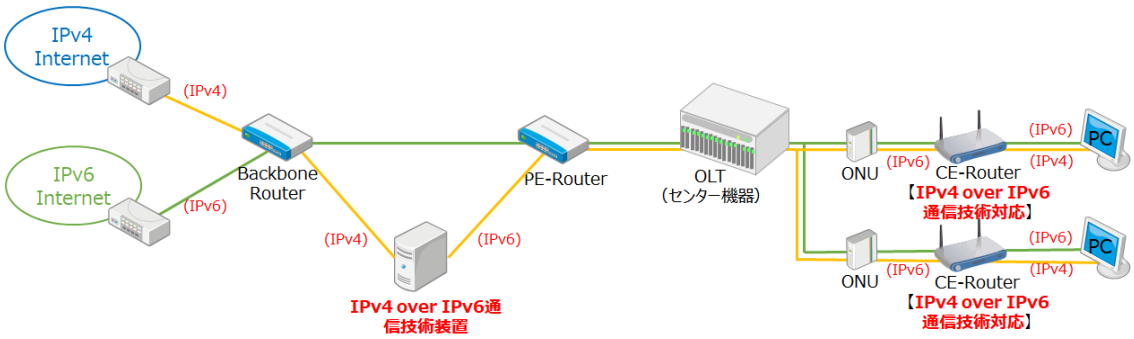


図 8.1 IPv6 シングルスタックネットワーク

8.1.2　IPv6 シングルスタックへの移行期間のネットワーク構成

既存（移行前）のネットワーク（IPv4 シングルスタックまたはデュアルスタック）から IPv6 シングルスタックへの移行は、ネットワーク側としては、基本的には移行前のネットワークに IPv4 over IPv6 通信技術装置を増設することで対応が可能であるが、CE-Router を IPv4 over IPv6 通信技術に対応した製品へ交換する必要があるため、完全移行には長期

間が必要になると想定される。なお、CGN 装置の機種によっては、ソフトウェアの入れ替えで同一筐体を IPv4 over IPv6 通信技術装置として動作させることが可能なものや、同一筐体の中で従来の CGN 装置の機能と IPv4 over IPv6 通信技術装置の機能を併用することが可能なものが存在する。

移行前（デュアルスタック）のネットワーク構成を図 8.2 に、移行期間のネットワークを図 8.3 に示す。

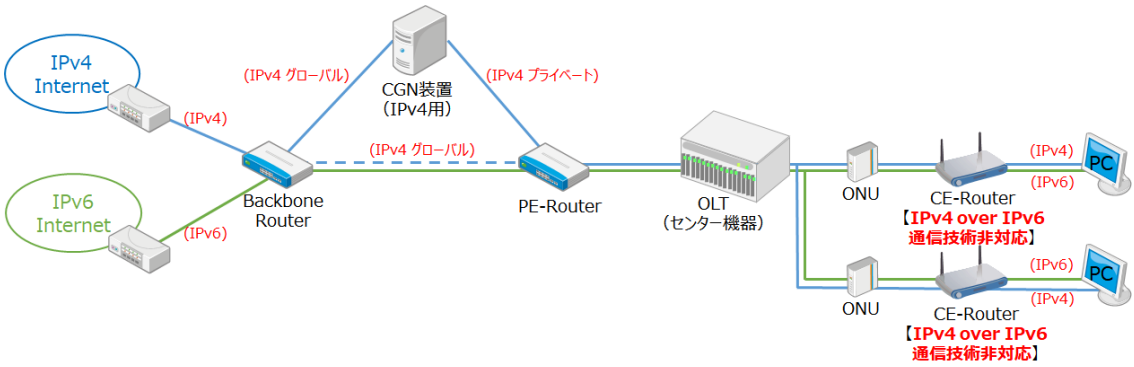


図 8.2 移行前（デュアルスタック） ネットワーク

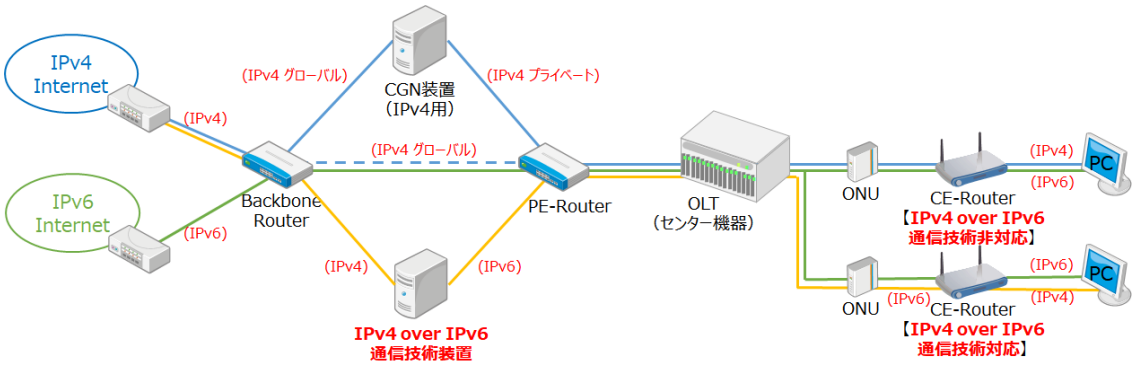


図 8.3 IPv6 シングルスタックへの移行期間ネットワーク

8.2 IPv4 over IPv6 通信サービスの技術

8.2.1 IPv4 over IPv6 で利用される技術

IPv4 over IPv6 通信サービスで利用される技術として DS-Lite、MAP-E など複数の技術があり、大きくトンネルと NAT の 2 つに分類できる。

この IPv4 over IPv6 通信技術の主要なものは RFC 標準化されており、国内や海外の ISP、モバイル事業者、CATV 事業者の実運用環境ですでに利用されている。

国内では、NTT 東西 IPoE サービスを提供する複数の事業者が DS-Lite、MAP-E などを利用している。

8.2.2 主要な IPv4 over IPv6 通信技術の紹介

(1) DS-Lite (RFC6333)

DS-Lite は Dual-Stack Lite の略で、CGN による IPv4 プライベートとグローバルの NAPT と IPv4 in IPv6 トンネルを組み合わせた技術である。宅内ネットワークからの IPv4 プライベートアドレスのトラヒックを CE-Router から IPv4 in IPv6 トンネルを使い IPv6 シングルスタックを経由して、センター側 IPv4 over IPv6 通信技術装置でグローバル IPv4 アドレスに NAPT を行う。DS-Lite における IPv4 over IPv6 通信技術対応 CE-Router を B4（Basic Bridging BroadBand）と呼び、CGN を行うセンター側 IPv4 over IPv6 通信技術装置を AFTR（Address Family Transition Router）と呼ぶ。

AFTR にユーザトラヒックを集約し、CGN により多対多 NAPT を行うため、NAPT 変換時の IPv4 アドレスの利用効率が良い。一方でユーザトラヒック追跡の観点から、CGN 同様に NAPT 時の変換ログの保存を考慮する必要がある。

海外の CATV で最も実績の多い IPv4 over IPv6 通信技術でもある。AFTR 製品としては、国内、海外では A10 ネットワークス製品が多く採用されている。

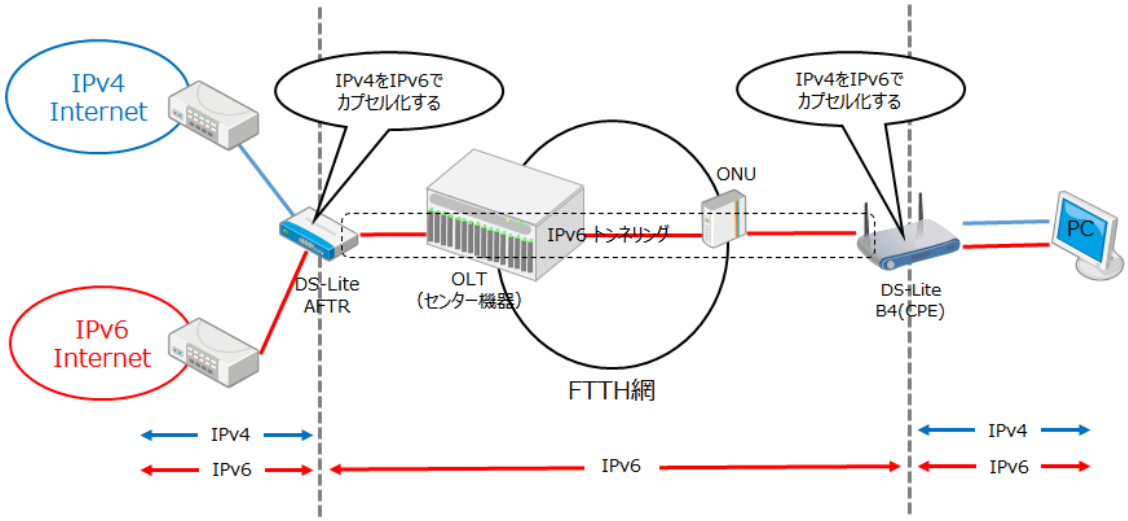


図 8.4 DS-Lite の概要図

(2) MAP-E (RFC7597)

MAP-E は Mapping of Address and Port Encapsulation の略で、DS-Lite と同様、IPv4 in IPv6 トンネルを利用するが、IPv4 グローバルアドレスへの NAPT を行うのは IPv4 over IPv6 通信技術に対応した CE-Router 側である。MAP-E では、CE-

Router を CE（Customer Edge）と呼び、センター装置を BR（Border Router）と呼ぶ。

CE がどの IPv4 グローバルアドレス、ポート番号を使い NAPT を行うかは、MAP-E サービス全体で設計、運用する必要がある。これを行うための仕組みが MAP-Rule で、事前に MAP-E サービス提供範囲（MAP Domain）内の BR、CE でこれを共有する必要がある。

ユーザの各 CE が利用できる IPv4 アドレスとポート番号は事前に MAP-Rule により固定化されており、MAP Domain 全体で固定の NAPT ポート数の割り当てを行い運用する形態が一般的である（たとえば、ユーザあたり 256 ポート、1024 ポートなど）。

事前に NAPT で割り当てる IPv4 グローバルアドレス、ポート番号の割り当てが固定化されているため、NAPT 時のアドレスの利用効率はあまり良くない。一方で、固定化されていることにより、NAPT 時の変換ログの保存を考慮する必要がない。

また、BR で NAPT を行なわないため、BR をルータとしてネットワークに配置でき、センター装置で IPv4 グローバルアドレスへの NAPT を行う DS-Lite などに比べ装置の拡張や冗長化が容易である。

海外の CATV では、NAPT のアドレス利用効率が良くないためか、現状ではあまり利用されていない。国内では、IPoE サービスの BR として古河電工製品が多く採用されている。

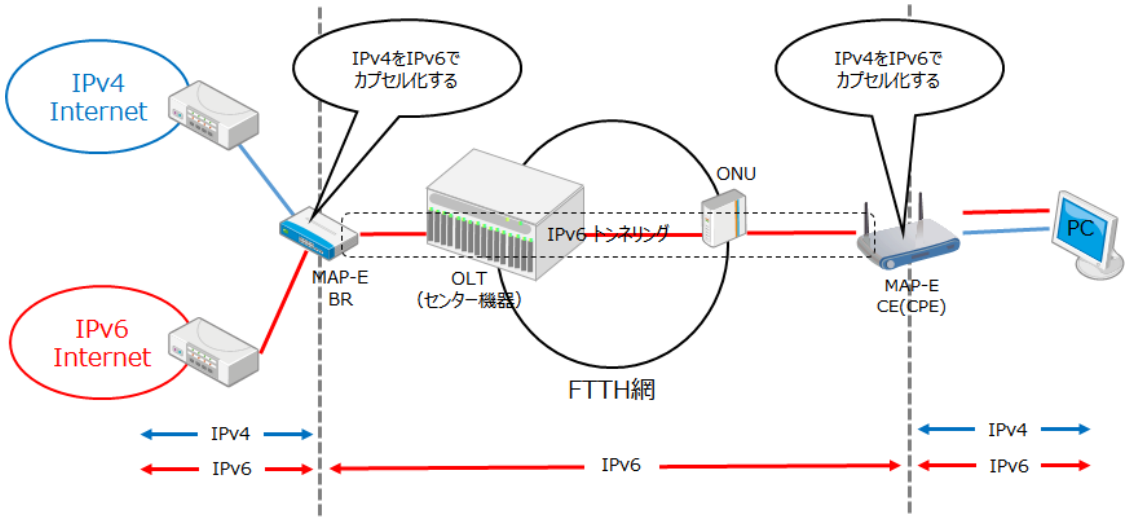


図 8.5 MAP-E の概要図

(3) MAP-T (RFC7599)

MAP-T は Mapping of Address and Port Translation の略で、MAP-E と同様、MAP-Rule の仕組みを利用し IPv4 over IPv6 通信サービスを提供する。MAP-E が

Encapslation（IPv4 in IPv6 トンネル）方式なのに対し、Translation（IPv4 と IPv6 の変換）を行う方式である。その他の特徴は MAP-E と共通である。

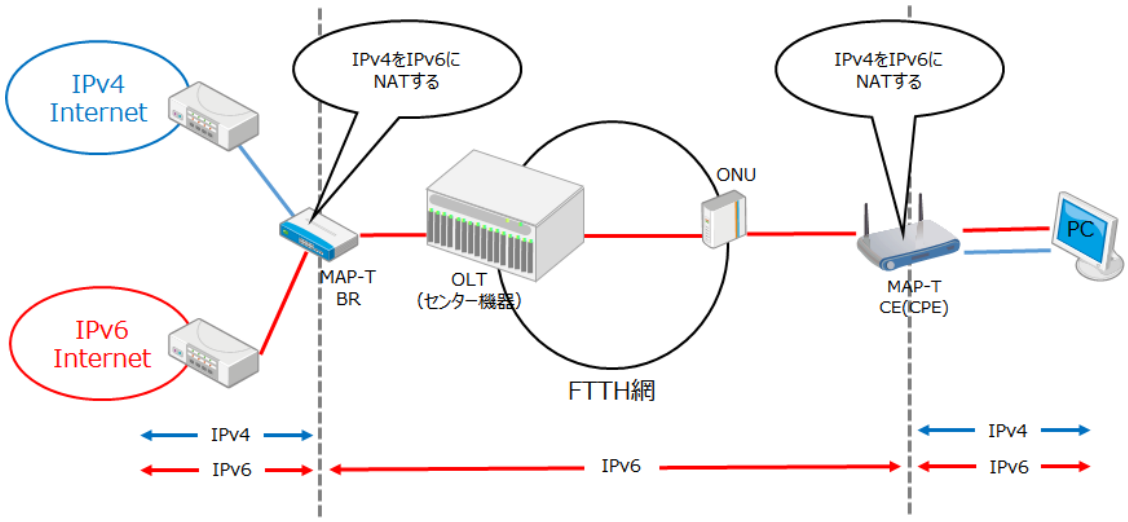


図 8.6 MAP-T の概要図

(4) Lw4o6 (RFC7596)

Lw4o6 は Light-weight 4 over 6 の略で、DS-Lite と同様、IPv4 in IPv6 トンネルを利用するが、IPv4 グローバルアドレスへの NAPT をセンター側の IPv4 over IPv6 通信技術装置ではなく、IPv4 over IPv6 通信技術対応 CE-Router で行う。DS-Lite 同様、IPv4 グローバルアドレスへの NAPT を行う CE-Router を B4 と呼び、センター側 IPv4 over IPv6 通信技術装置を AFTR と呼ぶ。

MAP-E/MAP-T における MAP-Rule のような仕組みがないため (PCP という動的にポート割り当てを行うプロトコルがあるが、IPv4 over IPv6 通信技術装置の対応や PCP サーバ設備などが必要となり国内では普及していない)、B4 へ固定の IPv4 グローバルアドレスを 1 対 1 で割り当てる運用が一般的である。

海外の CATV 事業者や国内の IPoE サービスで利用されている。AFTR 製品としては、A10 ネットワークス、ジュニパーネットワークス製品などが採用されている。

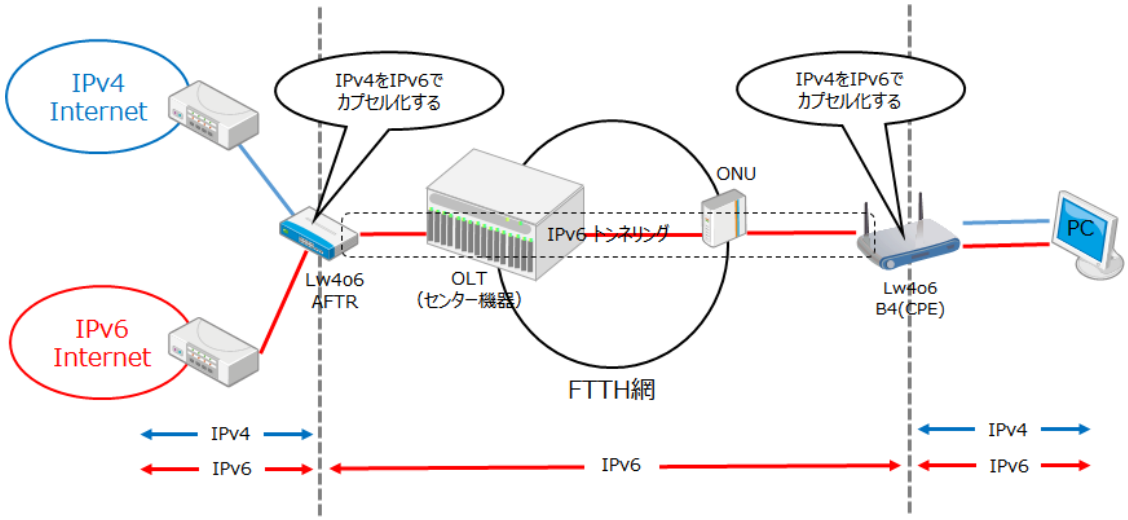


図 8.7 Lw4o6 の概要図

(5) 464 XLAT (RFC6877)

464XLAT は、NAT64 (RFC6146) による IPv6 と IPv4 の変換と、Stateless NAT46 (RFC6145) による IPv4 と IPv6 の変換を組み合わせた技術で、センター側 IPv4 over IPv6 通信技術装置の NAT64 で IPv4 グローバルアドレスへの NAPT も行う。Stateless NAT46 を行う CE-Router を CLAT と呼び、NAT64 を行うセンター側 IPv4 over IPv6 通信技術装置を PLAT と呼ぶ。

PLAT にユーザトラヒックを集約し NAT64 により IPv4 グローバルアドレスへの NAPT を行うため、DS-Lite と同様、NAPT 変換時の IPv4 グローバルアドレスの利用効率が良い。また、DS-Lite と同様、PLAT で NAPT 時の変換ログ保存を考慮する必要がある。

CATV などの固定網での利用はまだ多くはないが、北米の T-Mobile や韓国の主要なモバイル 3 キャリアなど海外のモバイル事業者での利用が非常に多い方式である。モバイルにおける IPv4 over IPv6 通信技術としては、海外におけるデファクトスタンダードになっているともいえる。

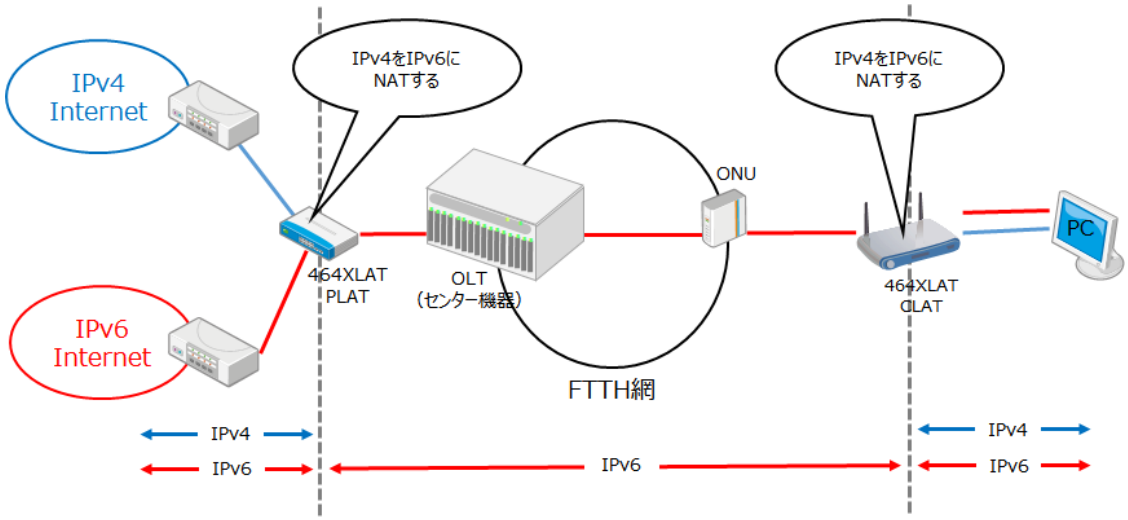


図 8.8 464XLAT の概要図

8.2.3 主要な IPv4 over IPv6 通信技術の特徴

紹介した主要な IPv4 over IPv6 通信技術を、あらためて先に述べたトンネル方式と NAT 方式に分類したものを表 8.1 に示す。

表 8.1 主要な IPv4 over IPv6 通信技術の整理

方式	IPv4 over IPv6 通信技術
トンネル	DS-Lite、MAP-E、Lw4o6
NAT	MAP-T、464XLAT

他にも、アドレス利用効率や拡張性など、技術ごとにそれぞれ特徴があり、採用する事業者のネットワーク規模や運用状況などにより適したものを選択すべきである。

IPv4 over IPv6 通信技術の利用事例としては、現在（2020 年 2 月時点）、国内の IPoE サービスでは DS-Lite や MAP-E などがあるが、MAP-T、464XLAT はまだ国内での利用事例はない。海外では、北米やアジア、ヨーロッパの CATV 事業者で DS-Lite や Lw4o6、MAP-T の利用事例がある。また、海外のモバイル事業者で 464XLAT が多く利用されている。

これらの IPv4 over IPv6 通信技術を実装しているネットワーク製品として、A10 ネットワークス、古河電工、シスコシステムズ、ジュニパーネットワークス、ファーウェイ、F5 ネットワークスの製品がある。

8.3 IPv4 over IPv6 通信技術採用時の考慮点

これまで述べたとおり、IPv4 over IPv6 通信技術にはそれぞれ特徴があるが、採用にあたっては特に以下の点の考慮が必要である。

8.3.1 必要な IPv4 グローバルアドレス

センター側 IPv4 over IPv6 通信技術装置で IPv4 グローバルアドレスへの NAPT を行う DS-Lite や 464XLAT に対して、MAP-Rule に従い固定のアドレスやポート割り当てを行う MAP-E/MAP-T では、IPv4 アドレスの利用効率に差がある。

MAP-E/MAP-T は、CE に割り当てるポート数が MAP-Rule 設計時に固定化されるため、ユーザ宅内におけるアプリケーションのポート利用状況によりポートの枯渇が発生しないよう、慎重にこの設計を行うべきである。一方で、割り当てポート数に余裕を持たせ余分に設定してしまうと、必要な IPv4 グローバルアドレス数が増加することになり、逆に割り当てポート数が少ないとポート枯渇の発生リスクが大きくなる。IPoE サービスで MAP-E を利用している事業者では、256 ポート割り当てと 1024 ポート割り当ての事業者が存在している。また、MAP-Rule で収容予定の CE 全体で利用する IPv4 アドレスは、MAP-E 初期導入時から確保しておく必要がある。

対して DS-Lite や 464XLAT は、動的に割り当てアドレスやポートを変更できるため、必要に応じてこの増減が可能で、ポート枯渇のリスクが小さく、必要 IPv4 グローバルアドレスの利用効率も良い。

Lw4o6 は 1 対 1 NAT での利用が多く、利用効率は悪いが、収容ユーザの増加に応じて利用アドレスを増やしていく事が可能である。

	DS-Lite	MAP-E	MAP-T	Lw4o6	464XLAT
初期時に必要な IPv4 グローバルアドレス	少	多		少	少
NAPT 時の IPv4 グローバルアドレスの利用効率	良い	悪い		悪い	良い

8.3.2 1 対 1 NAT の実装

収容ユーザによっては、IPv4 グローバルアドレスを 1 対 1 で割り当てをしたい場合がある。MAP-E、MAP-T、Lw4o6 はこの提供が可能だが、DS-Lite、464XLAT では難しい（製品ベンダ独自の拡張実装により対応しているケースは除く）。

この場合、DS-Lite では Lw4o6 と併用を行う方法が一般的である。Lw4o6 は元々DS-Lite の拡張を目的として策定されたプロトコルであり、DS-Lite との親和性が高く、製品ベンダもこの併用をサポートしているものが多い。

	DS-Lite	MAP-E	MAP-T	Lw4o6	464XLAT
1 対 1 NAT に対応	Lw4o6 と併用	対応		対応	未対応

8.3.3 家庭用ルータの IPv4 over IPv6 通信技術対応

IPv4 over IPv6 通信技術を利用するには各技術に対応した CE-Router が必要であるが、現時点（2020 年 2 月）では、国内の主要な製品は CATV 事業者での利用を想定した実装が行われていない。NTT 東西の IPoE サービスに対応した家庭用ルータも NTT 東西の設備利用を前提に開発されており、これをそのまま CATV に流用することはできない。

現在、IPv6 家庭用ルータ SWG にて、CE-Router の対応に関する標準化が進められており、これに対応した CE-Router が、今後、CATV でも利用可能になると考えられる。

8.3.4 MAP-E/MAP-T CE（CE-Router）への MAP-Rule 配布方法

これまで述べてきたように、MAP-E/MAP-T では MAP-Domain に所属するすべての BR、CE で MAP-Rule を共有する必要がある。運用中に変更の可能性がある MAP-Rule を CE の初期設定時にユーザが手動で設定することは運用上難しく、これを網内で CE に動的に配信する仕組みが必要になる。配信を行うサーバの準備と CE-Router でこれを取り込む実装を行うなど、相互の対応が必要になる。IPv6 家庭用ルータ SWG の標準化検討では、この実装に関しても検討がされている。

8.3.5 アプリケーションの透過性

どの技術も IPv4 グローバルアドレスへの NAPT を行うため、NAPT によるアプリケーション透過性への影響を考慮する必要がある。特に P2P アプリケーションや、CE-Router との UPnP を使ったポート開放を行うことを前提としているアプリケーションの場合、この影響を受けやすい。

P2P アプリケーションの透過性に対しては、DS-Lite、464XLAT では NAPT を行うセンター側 IPv4 over IPv6 通信技術装置で NAT の透過性の高い NAT Type である EIM/EIF（Endpoint Independent Mapping/Endpoint Independent Filtering）に対応しているため、

通信影響を受けないケースがほとんどだが、MAP-E/MAP-T は CE-Router で NAPT を行うため、CE-Router 側で透過性の高い NAT Type を実装している必要がある。ほとんどの CE-Router では EIM/EIF に対応しておらず、この影響を受ける可能性がある。

1 対 1 NAT の場合はこの影響を懸念する必要はない。1 対 1 NAT 以外の IPv4 over IPv6 通信技術では UPnP が利用できない（IPv4 over IPv6 通信技術では UPnP に対応するための標準技術もあるが、現状では CE-Router が未実装の状態で、今後も対応の可能性は低い）。そのため、アプリケーション側が UPnP による接続に依存している場合には通信に影響が出る可能性がある。アプリケーションが UPnP を使っていても、NAT トラバーサルにフォールバックできる実装であれば、問題ないと想定される。

<table>
<tr><th></th><th>DS-Lite</th><th colspan="2">MAP-E</th><th>MAP-T</th><th>Lw4o6</th><th>464XLAT</th></tr>
<tr><td>透過性の高い NAT Type への対応</td><td>○</td><td colspan="2">CE の実装に依存
対応していないルータも存在する</td><td></td><td rowspan="2">1 対 1 NAT であれば○</td><td>○</td></tr>
<tr><td>UPnP への対応</td><td>×</td><td colspan="2">×</td><td></td><td>×</td></tr>
</table>

8.3.6 変換ログ保存の有無

センター側 IPv4 over IPv6 通信技術装置で動的に NAPT を行う DS-Lite、464XLAT ではユーザ追跡の観点から、変換ログの保存を考慮する必要がある。一方、MAP-E、MAP-T は固定でアドレス、ポートを割り当てるため、考慮が不要となる。製品によっては、ログ出力回数や、ログのメッセージサイズを削減する実装を行っており、それらも考慮してストレージサイズなどの設備や運用コストを検討する必要がある。

8.3.7 まとめ

これらの点を考慮した上で、各 CATV 事業者は自社の設備にどの方式が適しているかを検討する必要がある。これまで述べてきな内容を表 8.2 にまとめた。

表 8.2 IPv4 over IPv6 通信技術の比較表

	DS-Lite	MAP-E	MAP-T	Lw4o6	464XLAT
初期時に必要な IPv4 グローバルアドレス	少	多		少	少
NAPT 時の IPv4 グローバルアドレスの利用効率	良い	悪い		悪い	良い
1 対 1 NAPT に対応	Lw4o6 と併用	対応		対応	未対応
家庭用ルータの対応	国内主要製品ベンダでは CATV 未対応				
透過性の高い NAT Type への対応	○	CE の実装に依存 対応していないルータも存在する		1:1 NAT であれば○	○
UPnP への対応	×	×			×
変換ログの保存	必要	不要		不要	必要
MAP-E/MAP-T MAP-Rule 配布方法		MAP-Rule 配布の仕組みが必要			

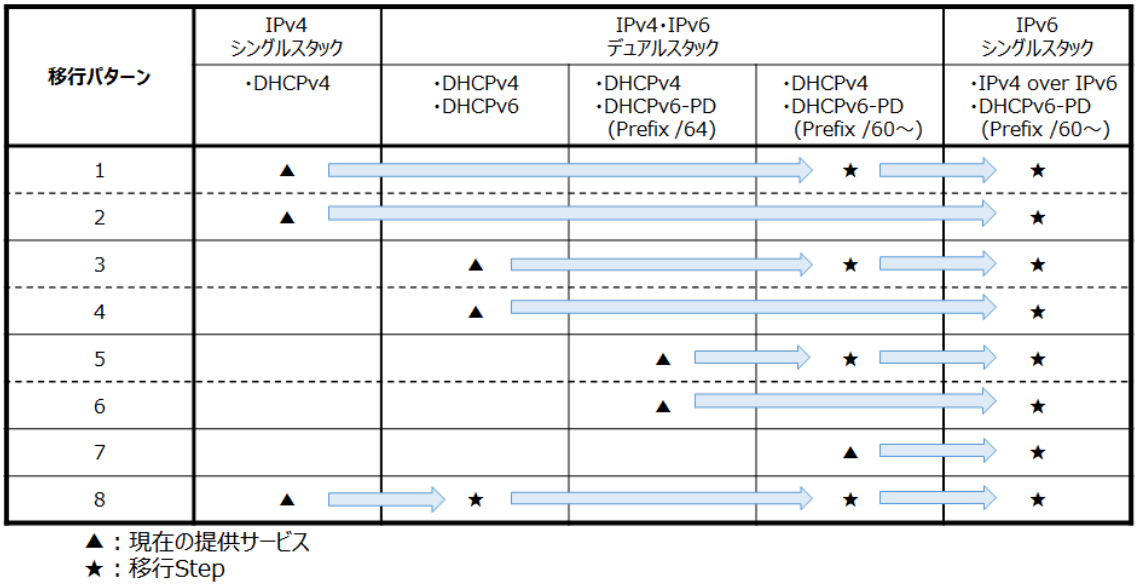
第9章　移行シナリオ

本ガイドラインが推奨する IPv6 アドレスサービスの提供方式は、「DHCPv6-PD(Prefix : /60、/56、/52、/48） IPv4 over IPv6 通信技術を利用したシングルスタック方式」とし、事業者のサービス形態ごとにネットワーク移行シナリオを表 9.1 に示す。現在のサービス形態が IPv4 シングルスタックであれば移行パターンの 1、2、8 が対象となる。IPv4・IPv6 デュアルスタックでサービス提供している場合は、移行パターンの 3～7 が対象となり、IPv6 アドレスの提供方式によって移行パターンが異なる。

推奨する移行シナリオとしては、いずれのサービス形態からも IPv4 over IPv6 通信技術を利用した IPv6 シングルスタックのネットワークを構築した上で、サービス（CE-Router）としてはデュアルスタックと IPv6 シングルスタックサービスを併用して提供し、徐々に IPv6 シングルスタックへ移行を行う方法である。

現在のサービス形態ごとに移行方法を述べる。

表 9.1 移行シナリオ



9.1 IPv4 シングルスタックからの移行

IPv6 サービスを行っていない場合の移行パターンであり、対象は移行パターン 1、2、8 である。ここでは、IPv6 サービス提供を DHCPv6 方式ではなく、DHCPv6-PD 方式で開始することを推奨する。

移行パターン	IPv4 シングルスタック	IPv4・IPv6 デュアルスタック			IPv6 シングルスタック	移行パターンの比較	
	・DHCPv4	・DHCPv4 ・DHCPv6	・DHCPv4 ・DHCPv6-PD (Prefix /64)	・DHCPv4 ・DHCPv6-PD (Prefix /60～)	・IPv4 over IPv6 ・DHCPv6-PD (Prefix /60～)	コスト	運用保守
1	▲			★	★	△	○
2	▲				★	○	×

▲：現在の提供サービス
★：移行Step

移行パターン	IPv4 シングルスタック	IPv4・IPv6 デュアルスタック			IPv6 シングルスタック	移行パターンの比較	
	・DHCPv4	・DHCPv4 ・DHCPv6	・DHCPv4 ・DHCPv6-PD (Prefix /64)	・DHCPv4 ・DHCPv6-PD (Prefix /60～)	・IPv4 over IPv6 ・DHCPv6-PD (Prefix /60～)	コスト	運用保守
8	▲	★		★	★	×	○

▲：現在の提供サービス
★：移行Step

9.1.1 移行パターンの解説

移行パターン 1 と 2 の大きな違いは、ユーザにデュアルスタックサービスを提供するか否かである。

ネットワークの観点でみると、移行パターン 1 は IPv4 シングルスタックの構成に IPv6 の設定を追加した後に、IPv4 over IPv6 通信技術装置を導入することになる。一方の移行パターン 2 は、IPv4 シングルスタックの構成に IPv4 over IPv6 通信技術装置と合わせて IPv6 の設定を追加することになる。そのため、コストの視点では、移行パターン 2 が優れているといえる。

CE-Router の観点でみると、移行パターン 1 はデュアルスタックへの移行時に DHCPv6-PD 方式に対応した製品への交換が必要となり、さらに IPv6 シングルスタックへの移行時に IPv4 over IPv6 通信技術に対応した製品への交換が必要となる。一方の移行パターン 2 は、IPv4 over IPv6 通信技術に対応した製品への交換の 1 回のみで済むため非常に効率的であるといえる。しかし、第 8 章で説明したとおり、IPv4 over IPv6 通信技術に対応した CE-Router が高価、機種が少ないという課題がある。

なお、移行パターン 8 は、ドコモ光タイプ C サービス提供開始など早急に IPv6 アドレスを提供する必要がある場合に対象となる。DHCPv6 方式は本ガイドラインでは推奨していないが、早急に IPv6 アドレスを提供する場合には暫定策としての導入は考えられる。

9.1.2 推奨する移行方法

- ネットワークは、移行パターン 2 のように IPv4 シングルスタックから IPv6 シングルスタックへ移行する。
- サービスは、デュアルスタックと IPv6 シングルスタックサービスを併用して提供し、徐々に IPv6 シングルスタックへ移行を行う。

9.2 IPv4・IPv6（DHCPv6 方式）デュアルスタックからの移行

DHCPv6 で IPv6 アドレスサービスを提供している場合の移行パターンであり、対象は移行パターン 3、4 である。すでに構築している上位ネットワーク機器が DHCPv6-PD 方式に対応しているかの確認が必要であり、対応していない場合は 5.3.4 を参考に検討いただきたい。

移行パターン	IPv4 シングルスタック	IPv4・IPv6 デュアルスタック			IPv6 シングルスタック	移行パターンの比較	
	・DHCPv4	・DHCPv4 ・DHCPv6	・DHCPv4 ・DHCPv6-PD (Prefix /64)	・DHCPv4 ・DHCPv6-PD (Prefix /60～)	・IPv4 over IPv6 ・DHCPv6-PD (Prefix /60～)	コスト	運用保守
3		▲ →	→	★ →	★	△	○
4		▲ →	→	→	★	○	△

▲：現在の提供サービス
★：移行Step

9.2.1 移行パターンの解説

移行パターン 3 と 4 の大きな違いは、ユーザにデュアルスタックサービスで DHCPv6-PD 方式を提供するか否かである。

ネットワークの観点ではどちらの移行パターンも大きな違いはないが、移行パターン 3 は作業が 2 回発生するのに対して、移行パターン 4 は作業が 1 回で済む。

CE-Router の観点でみると、9.1.1 でも述べたように、移行パターン 3 は CE-Router の交換が 2 回必要となり、移行パターン 4 は、CE-Router の交換が 1 回のみで済む。しかし、IPv4 over IPv6 通信技術に対応した CE-Router が高価、機種が少ないという課題がある。

9.2.2 推奨する移行方法

- ネットワークは、移行パターン 4 のように 1 度で IPv6 シングルスタックへ移行する。
- サービスは、デュアルスタックと IPv6 シングルスタックサービスを併用して提供し、徐々に IPv6 シングルスタックへ移行を行う。

9.3 IPv4・IPv6（DHCPv6-PD(Prefix：/64)方式）デュアルスタックからの移行

DHCPv6-PD で IPv6 アドレスサービスを提供しているが、CE-Router の LAN 側に委任する Prefix が/64 となっている場合は、推奨する Prefix(/60、/56、/52、/48)への変更を検討いただきたい。

使用している CE-Router が Prefix の/64～/48 に対応した製品であれば移行パターン 5 と 6 の違いはほとんどない。CE-Router が Prefix の/64 にしか対応していない場合は、CE-Router の交換が必要となるため、移行パターン 6 が推奨となる。

移行パターン	IPv4 シングルスタック	IPv4・IPv6 デュアルスタック			IPv6 シングルスタック	移行パターンの比較	
	・DHCPv4	・DHCPv4 ・DHCPv6	・DHCPv4 ・DHCPv6-PD (Prefix /64)	・DHCPv4 ・DHCPv6-PD (Prefix /60～)	・IPv4 over IPv6 ・DHCPv6-PD (Prefix /60～)	コスト	運用保守
5			▲ →	★ →	★	△	○
6			▲ →		★	○	○

▲：現在の提供サービス
★：移行Step

9.4 IPv4・IPv6（DHCPv6-PD(Prefix：/60～)方式）デュアルスタックからの移行

本ガイドラインで推奨する、DHCPv6-PD(Prefix：/60～)で提供している場合は、あとは IPv6 シングルスタックへ移行するのみである。CE-Router の状況を見極めて適切なタイミングでの移行を検討いただきたい。

移行パターン	IPv4 シングルスタック	IPv4・IPv6 デュアルスタック			IPv6 シングルスタック	移行パターンの比較	
	・DHCPv4	・DHCPv4 ・DHCPv6	・DHCPv4 ・DHCPv6-PD (Prefix /64)	・DHCPv4 ・DHCPv6-PD (Prefix /60～)	・IPv4 over IPv6 ・DHCPv6-PD (Prefix /60～)	コスト	運用保守
7				▲ →	★	-	-

▲：現在の提供サービス
★：移行Step

第10章 まとめ

CE-Router の LAN 側に接続される端末の IPv6 アドレス配布方式は DHCPv6 方式ではなく、CE-Router の出力する RA の Prefix オプションによって IP を自動生成できる DHCPv6-PD 方式が推奨されている。また、DHCPv6-PD 方式で CE-Router の LAN 側に割り当てる Prefix は世界的には/48 が推奨されているが、本ガイドラインでは現実的な運用を想定して/60、/56、/52、/48 を推奨とした。最終的には、ケーブルインターネットも IPv6 アドレスのサービス提供において、CE-Router の LAN 側は DHCPv6-PD 方式で Prefix は /48 を委任することが望ましい。

事業者側ネットワークについては、IPv4 over IPv6 通信技術を使った IPv6 シングルスタックと IPv4/IPv6 デュアルスタックを比較すると、ネットワークの設備や運用コストを軽減することができることから、IPv4 over IPv6 通信技術を使った IPv6 シングルスタックを目指すべきである。移行シナリオについては、第 9 章に記したとおりであるが、既存のネットワークに IPv4 over IPv6 通信技術を使った IPv6 シングルスタックのネットワークを構築した上で、サービス（CE-Router）としては IPv6 シングルスタックと IPv4/IPv6 デュアルスタックを併用して提供し、徐々に IPv6 シングルスタックへ移行していく方法を推奨とした。

DHCPv6-PD 方式を開始するにあたり、市販されている CE-Router（IPv6 家庭用ルータ SWG の仕様に準拠した製品）との接続性を担保することが非常に重要であり、これを実現するための情報は第 5 章を中心に第 6 章、第 7 章にとりまとめた。この中で大きな課題となるのが、事業者の既存 PE-Router が Route Injection などに対応していないケースである。この場合は、Route Injection 等に対応する PE-Router への更改、もしくは Route Injection などを代替する設備の新設が必要となる。必要に迫られて DHCPv6-PD 方式への対応のために設備の更改、新設を行うと膨大な費用が必要となるが、ネットワーク機器を更新する際に第 5 章を参照して設備を更改することにより、第 9 章のとおり IPv6 対応に要する費用は限りなく少なくなる。エッジコンピューティングや IoT 等の普及により、CE-Router の LAN 側に接続される端末数が大きく増加し、DHCPv6-PD 方式でのサービス提供が必要になる可能性がある。動静を注視し、計画的なネットワーク更改を検討することが重要である。

IPv4 over IPv6 通信技術を使った IPv6 シングルスタック化は、ネットワーク側の対応と CE-Router 側の対応が必要である。そのため、まずはネットワーク側を IPv4 over IPv6 通信技術に対応させ、その後に順次 IPv4 over IPv6 通信技術に対応した CE-Router へ交換する流れがベターとなる。CE-Router の交換が完了するまで IPv4/IPv6 デュアルスタックのネットワークを維持しなければ、IPv4 over IPv6 通信技術非対応の CE-Router 配下から IPv4 インターネットへの接続ができなくなるため、CE-Router 交換スケジュールがネット

ワーク更改のスケジュールにも大きな影響を与える。IPv6 シングルスタックに必要な技術は第 8 章で述べたとおりだが、現時点では CE-Router の実装に依存するところがあるため、実装状況を確認しながら採用する技術や移行計画を決定する必要がある。

Appendix I　事業者導入事例

I 1　国内 CATV 事業者の導入事例

I 1.1 iTSCOM（DOCSIS）導入事例

I 1.1.1 導入経緯

イッツ・コミュニケーションズ株式会社においては 2009 年より IPv6 対応について検証/検討を開始し、以下の導入ポリシーおよび設計ポリシーを定めた。

I 1.1.2 導入ポリシー

(1) IPv6 対応および導入にあたり既存サービスへ影響を発生させない。
- 問題が確認できた場合などは IPv6 導入を遅延させ、既存サービスへの影響ないことが確認できるまで導入は行わないこととした。

(2) 設備更新時に合わせて IPv6 対応を行う。
- IPv6 対応のために設備投資は行わず、設備更新時やアップグレード時などに要件として IPv6 対応を含めた。

(3) IPv6 導入の準備が整い次第払い出しを開始し、運用ノウハウを蓄積する。
- IPv6 が必要になってからの対応では後手となってしまうことから、IPv6 運用を開始し運用ノウハウ、ナレッジを蓄積することを目的とした。

(4) セキュリティに問題がないことを確認する。
- CMTS 配下の CPE 間通信でセキュリティ(主にファイル共有)が IPv4 同様担保されていることを検証する。

I 1.1.3 設計ポリシー

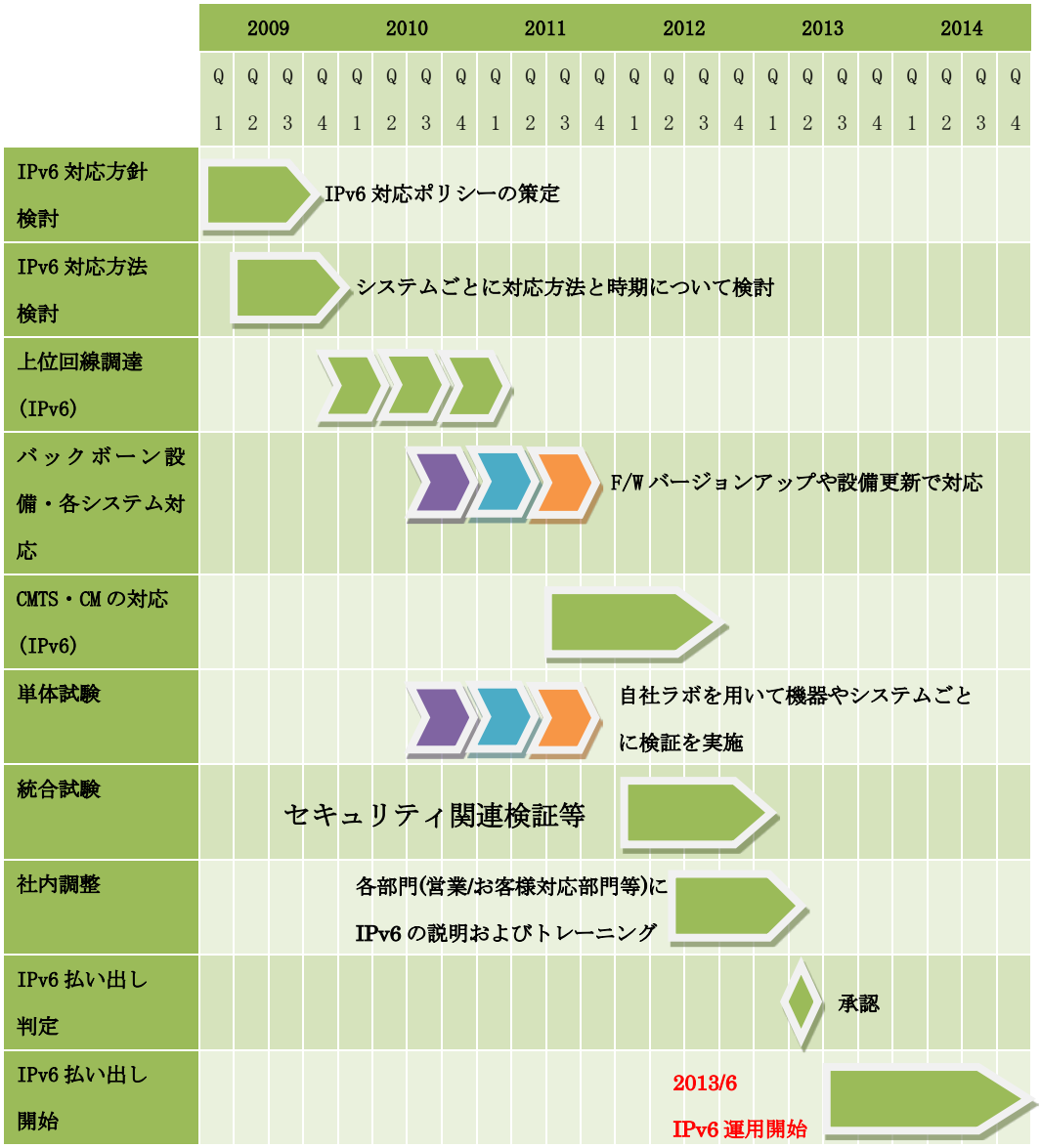
(1) デュアルスタック方式にて設計する。
- IPv4 におけるネットワーク構成と同じ設計とすることができ、運用性も優れていることから採用した。IPv6 で使用するルーティングプロトコルや冗長化方式については IPv4 で使用しているものと同じものを採用し、IPv4 と IPv6 が同様にオペレーションできるように導入を行った。

(2) シンプルな NW 構成となるよう設計する。
- IPv6 ではアドレス空間が膨大であるため、可能な限り経路集約を行うよう設計した。

(3) IP 割り当てポリシーの策定
- IPv6 の割り当てポリシーを策定しておくことで、経路集約や同一のルールに基づいてグローバルユニキャスト IPv6 アドレスや LinkLocal アドレスを割り当てできるよう策定した。

I 1.1.4 スケジュール

表 I.1 IPv6 サービス提供までの対応過程



同社では導入ポリシー検討時、IPv6 払い出しにおけるスケジュールは計画せず、準備が整い次第(IPv6 環境が整備完了次第)運用を開始することと定義したことから、本スケジュールは実績となる。

また、IPv6 運用開始に合わせて、CM へ適用していた LLC Filter(IPv6 Ether Type = 86DD)を解除することで IPv6 の払い出しを開始した。

I 1.1.5 導入前後のネットワーク構成

(1) 導入前のネットワーク構成

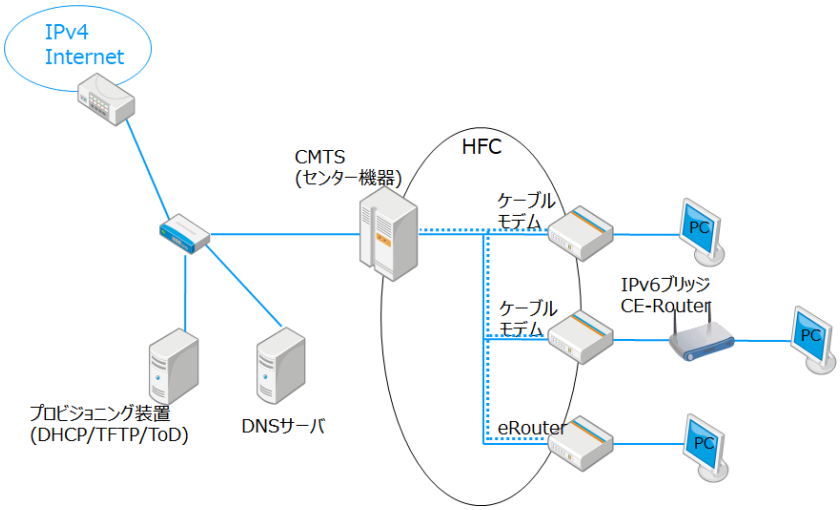


図 I.1 導入前のネットワーク構成図

(2) 導入後のネットワーク構成

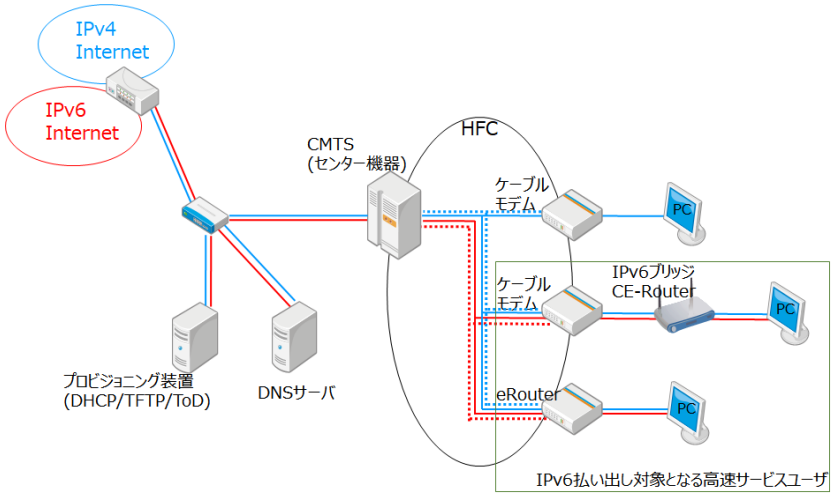


図 I.2 導入後のネットワーク構成図

I 1.1.6 IPv6 払い出し仕様

同社における IPv6 払い出し仕様は以下のとおり。

- DOCSIS3.0 を使用した高速サービスのみ IPv6 提供

  ※ 低速サービスにおいては DOCSIS1.1～3.0 の CM が使用されおり、運用上煩雑になること、設置モデムによって同じサービスでも内容に違いが生じることから IPv6 を提供していない。

- デフォルト IPv6 提供（※別途申し込み不要）
  ※ 同社では IPv6 払い出しをサービスとは考えていないため、追加料金や料金変更は発生しない。
- IPv6 アドレス（IANA）：15 個
  ※ IPv6 ブリッジルータ対応のため。
- IPv6 アドレス(IAPD)：「/56」を 1 個配布
  ※ Prefix Per Host を考慮。

I 1.1.7 IPv6 導入にあたり考慮した点

- 機器・システムにおける機能実装有無
  各種プロトコル機能検証（単体試験）
  セキュリティ関連の検証 . . . など
- 基本サービス（DNS/Mail/Webmail/Web/FTP/CGI）
  DNS および Web サービスについては IPv6 対応
- 専用 IPv6 接続確認 Web の作成
  お客様の IPv6 接続確認ツールとして作成
- 社外告知/社内調整
  プレスリリースの発行や FAQ 作成、約款改定など
- マネージメント関連（監視システム）
  機器の正常性監視や telnet 等のマネージメントは IPv4 で実施
- IPv6 監視対象
  （1）IPv6Routing 正常性
  お客様環境を模擬した仮想端末を設置し ICMPv6 による死活監視
  （2）IPv6 サービスの正常性
  お客様環境を模擬した仮想端末からテスト Web に HTTPGET
  （3）IPv6Traffic 量の取得
  SNMP や Netflow を活用

I 1.2 iTSCOM（PON）導入事例

I 1.2.1 導入経緯

2017 年 5 月より提供を開始した FTTH インフラを用いたインターネットサービスにおいても IPv6 対応を行った。

I 1.2.2 導入ポリシー

基本的な考え方は HFC インフラと同様であり、技術的に IPv6 の提供が可能かつオペレーションに影響が発生しないサービスで IPv6 対応を行うこととした。

※ FTTH インフラで提供されるインターネットサービスでは DOCSIS2.0 以下のモデムを使用したサービスを除くすべてのサービスで IPv6 の提供を行っている。

I 1.2.3 設計ポリシー

FTTH インフラでは、加入者宅に光回線を引き込み D-ONU を設置する方式(主に SDU 向けに提供)と集合住宅に EoC(C-DOCSIS)を設置し、加入者宅には DOCSIS モデムを設置する方式(主に MDU 向け)が存在する。

D-ONU が設置される方式ではすべてのコースで IPv6 の提供を行っている。

DOCSIS モデムが設置される方式では、HFC インフラと同様に DOCSIS3.0 モデムが設置される高速サービスのみで IPv6 の提供を行っている。

※ 理由は HFC インフラと同様である。

※ その他、設計ポリシーは「HFC インフラ導入事例」と同じ考え方となる。

(1) FTTH インフラネットワーク構成図

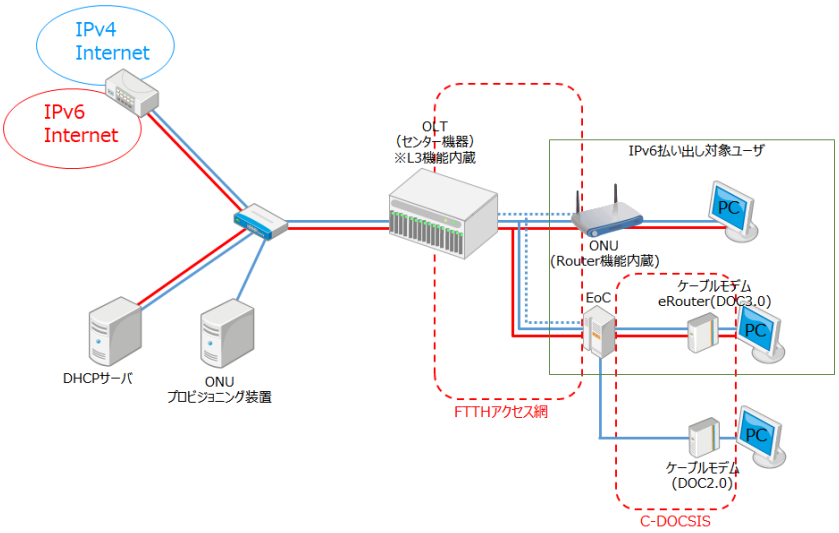


図 I.3 FTTH インフラネットワーク構成図

I 1.2.4 IPv6 払い出し仕様

(1) FTTH インフラ IPv6 払い出し仕様

- デフォルト IPv6 提供（※別途申し込み不要）

  ※ 同社では IPv6 払い出しをサービスとは考えていないため、追加料金や料金変更は発生しない。

- IPv6 アドレス（IANA）：15 個
  ※ IPv6 ブリッジルータ対応のため。
- IPv6 アドレス(IAPD)：「/64」を 1 個配布

※ HFC インフラにおける/56 の配布実績から、

※ 社ユーザにおける Prefix Per Host などの要望がなかったことから、/60 以上の割り当ては現在のところは不要と判断し/64 を配布することとなった。

※ 今後 IPv6 普及の状況やユーザからの要望によって、/60 以上の配布に変更することを検討。

I 1.2.5 IPv6 利用状況(払い出し状況)

HFC インフラでは IPv6 払い出し開始から約 6 年半、FTTH インフラではサービス開始から 2 年半経過したが、HFC インフラでは IPv6 払い出し対象モデムの内、約 50%が IPv6 アドレス(IANA/IAPD)を取得している。一方、FTTH インフラでの IPv6 取得率としては 80%以上となる。

I 1.2.6 その他

(1) 不具合

IPv6 に関するトラブル(サービスに影響があった事案)は IPv6 払い出し後、数件発生したものの散見はされておらず、比較的安定的に運用ができているものと考えられる。

(2) トラブル事例

- デュアルスタック環境にて特定の web ページが表示されない
  - AAAA を返すがコンテンツがないことが原因。web 管理者へ連絡し解決した。
- eRouter におけるバグにより、重複した v6PD を払い出す
  - FWupdate にて解決した。
- CMTS 切り替え時に DHCPv6PD の route summary の設定漏れによる経路溢れ
  - route summary にて解決した。

(3) 検討課題

- IPv6 未対応インフラへの導入検討
- IPv6 未対応サービス（法人向け・マンション LAN 向け）および、インフラ（フレッツ）への IPv6 導入の検討
- IPv6 移行後のシナリオ検討
- IPv6 移行が進み、Traffic 比率が IPv6<IPv4 となった際の IPv4 におけるインターネット接続性および効率的な NW 構成・運用方法の検討

I 1.3 J:COM（DOCSIS）導入事例

I 1.3.1 導入経緯

株式会社ジュピターテレコムでは、2013 年より IPv6 利用希望者に対して IPv4/IPv6(/128)デュアルスタックでのインターネットサービス(以下、旧 IPv6 サービス)提供を開始。

その後 IPv4 グローバル IP 枯渇対策検討において、DHCPv6-PD による IPv6 と IPv4 のデュアルスタックでのインターネットサービス(以下、DHCPv6-PD サービス)デフォルト提供の開始を決定。2021 年の提供開始に向け対応中。

I 1.3.2 DHCPv6-PD サービス導入ポリシー

IPv4 グローバル IP 枯渇対策検討において、以下の DHCPv6 サービス導入ポリシーを定めた。

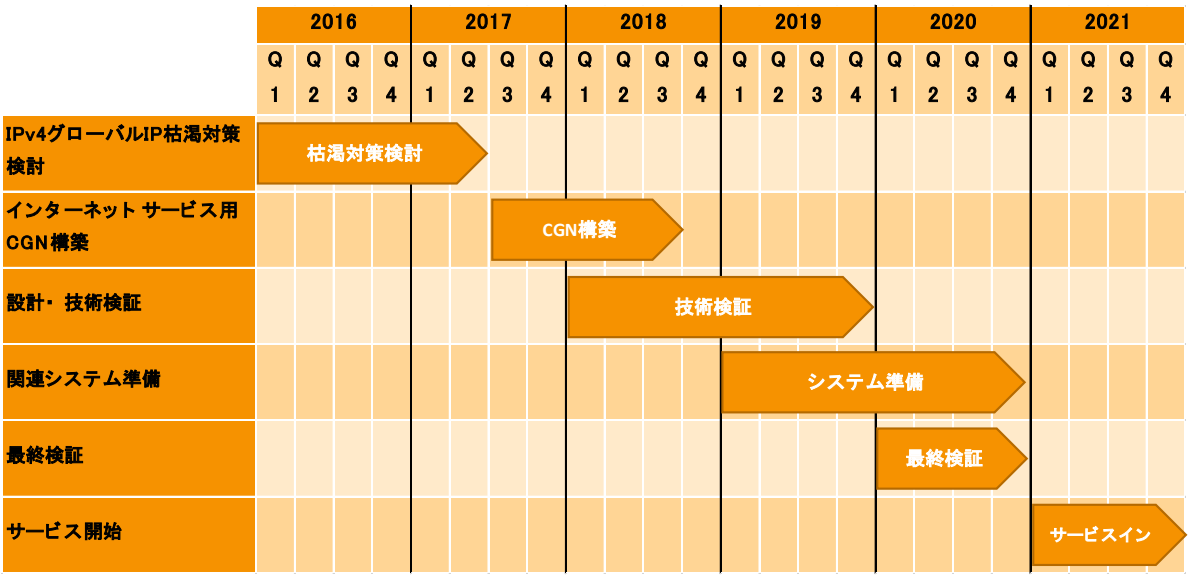
(1) 2021 年より全国の新規インターネットサービス加入者を対象に DHCPv6 サービスを提供する。
(2) DHCPv6 サービス開始と同時に、関東圏の新規インターネットサービス加入者を対象に CGN を介したインターネットサービスを提供する。

I 1.3.3 DHCPv6-PD サービス提供ポリシー

(1) 提供方法：新規インターネットサービス加入者に対してケーブルモデムのルータ LAN 側に DHCPv6-PD にて prefix を割り当てる
(2) 料金：無料提供
(3) 実装仕様：ルータ WAN 側／ステートフル DHCPv6
ルータ LAN 側／ステートフル DHCPv6-PD
(4) その他：2013 年から開始の申込制による旧 IPv6 サービスは DHCPv6-PD サービス開始前に提供終了とする

I 1.3.4 スケジュール

表 I.1 DHCPv6-PD サービス導入計画



(1) 2016 年

・IPv4 グローバル IP 枯渇対策の検討実施

(2) 2017 年

・インターネットサービス用 CGN 構築

・CGN 構築に伴うヘッドエンド設計見直しおよび設定変更作業実施

(3) 2018 年

・DHCPv6-PD 技術検証実施

(4) 2019 年

・DHCPv6-PD サービスに関連するシステムの DHCPv6-PD 対応

(5) 2020 年

・検証環境での一気通貫試験実施

・フィールド試験実施

(6) 2021 年

・トライアル実施

・DHCPv6-PD サービスおよび CGN 運用(関東圏)開始

I 1.3.5 ネットワーク構成

DHCPv6-PD サービス開始後のネットワーク構成を図 I.4 、図 I.5 に示す。

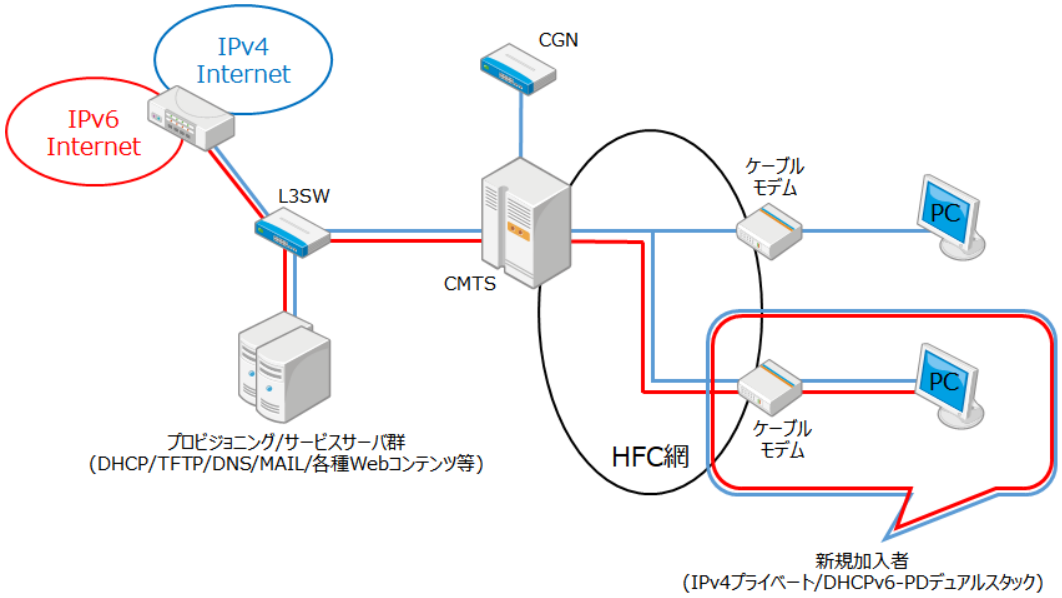


図 I.4 関東圏のネットワーク構成

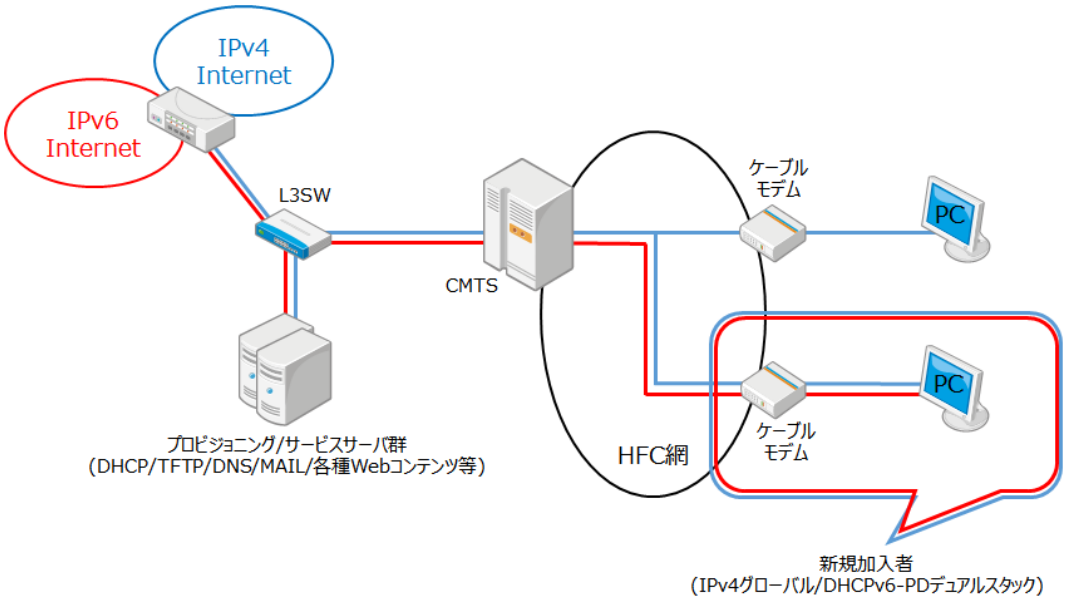


図 I.5 関東圏を除く全国のネットワーク構成

I 1.3.6 DHCPv6-PD サービス開始に向けた対応状況

(1) コアネットワーク

キャッシュサーバは 2020 年に IPv6 対応予定。

(2) 各種システム

プロビジョニングシステムは DHCPv6-PD サービスに対応した機能を 2020 年に実装予定。

(3) ヘッドエンドネットワーク

CMTS は DHCPv6-PD サービスを想定した検証を 2019 年に実施。

帯域制御装置は 2020 年に IPv6 対応予定。

IPv6 アサインメントポリシーについて 2020 年に再度見直しを実施予定。

(4) ケーブルモデム

DHCPv6-PD サービス対応ファームウェアへのバージョンアップを 2020 年に実施予定。

I 1.3.7 今後の課題

(1) DHCPv6-PD サービス開始前

- 構築要素が多いことから対応部署が多く、一部のスケジュール遅延が全体スケジュールに影響を与える。IPv4 グローバル IP 枯渇対策の対応項目について各部署との情報共有を図り、スケジュール管理する必要がある。
- 加入者への DHCPv6-PD に関するご案内を想定し、コールセンターに対して基本仕様について知識共有の場を設定する必要がある。

(2) DHCPv6-PD サービス開始後

- サービス開始後は 1 加入者あたり複数の IPv6 アドレスを利用することとなる。効果的に関連システム増強計画を行うために関連システムの負荷を注視しそのデータをもとに試算する体制を整える。
- DHCPv6-PD サービスと同時期に関東圏では CGN の運用が開始されるが、対象は新規加入者のみのため、IPv4 グローバル IP は徐々に使用率が縮小されていく。これにより各 CMTS で IPv4 グローバル IP の余剰が生じるため、IPv4 グローバル IP の回収作業を効率的に実行する仕組みを整理しておく必要がある。

I 2　海外事業者の導入事例

I 2.1　アジア CATV 事業者導入事例（IPv4 over IPv6 通信サービス）

I 2.1.1　導入の背景と経緯

東南アジアの大手 CATV 事業者（加入者 50 万人以上）では IPv4 インターネット接続サービスのみを提供していた。事業者側ネットワークの IPv6 化を進めていたが、この時点ではユーザに対しては IPv4 と IPv6 のデュアルスタックでのインターネット接続提供には至っていなかった。加入者増に伴い IPv4 グローバルアドレスの枯渇が懸念されたため、対策としてまずは CGN の導入が検討され、同時にユーザへの IPv6 インターネット接続の提供についても検討された。

検討の結果、既存回線のユーザに対しては CGN による IPv4 アドレス枯渇対策を行い、合わせて事業者側ネットワークの IPv6 対応に従い、新規回線のユーザには IPv4 over IPv6 通信サービスによるデュアルスタックのインターネット接続提供を行うことを決めた。これにより、IPv4 枯渇対策を行いつつ IPv6 対応を進めることができる。IPv4 over IPv6 通信技術はいくつか選択肢があったが、最初に導入する CGN との親和性の高さを重視し、DS-Lite が選択された。DS-Lite の NAPT は CGN を採用しており、EIF/EIM による NAPT の透過性、NAT アドレスの増減やユーザへのポート割り当ての柔軟性、CGN と同一の NAPT 変換ログ出力など、CGN 同様の運用が可能な点が重視された。これにより、IPv4 アドレス枯渇対策を行いながら、ユーザへの IPv6 インターネット接続提供も進めていけると考えた（DS-Lite の 44 NAPT は CGN を用いているため、IPv4 アドレス枯渇対策としても有効）。

IPv4 over IPv6 通信技術対応 CE-Router の展開は、新規回線ユーザの CE-Router として DS-Lite B4 機能対応のものを導入することで対応した。センター側 IPv4 over IPv6 通信技術装置は CGN と DS-Lite 両方を提供する必要があるが、それぞれ別々の筐体に分けて提供するのでなく、同一筐体で並行して提供できる A10 ネットワークス社製品を選定し導入した。これは、筐体を分ける事によるコストの増加、そして別々の運用を行うことによる運用負担を軽減することが目的である。また、同一筐体で提供が行えることで、既存回線ユーザの CGN から DS-Lite への移行が容易になる点も考慮されている。競合製品はシャーシ型が多い中、1 U ラックマウントサイズで省スペースである点も選定ポイントであった。

I 2.1.2 ネットワーク構成

(1) CGN 導入時構成

既存回線ユーザに対して CGN を提供。IPv4 グローバルアドレス枯渇対策を行う。

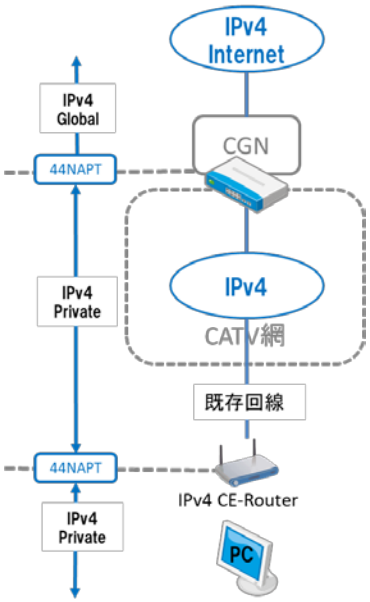


図 I.6 CGN 構成図

(2) DS-Lite 導入時構成（CGN/DS-Lite 併用構成）

続いて、新規回線ユーザに対して事業者側ネットワークの IPv6 対応に従い、DS-Lite による IPv4 over IPv6 通信サービスを提供し、ユーザに対しては IPv4 と IPv6 のデュアルスタックのインターネット接続環境の整備を進めていく。

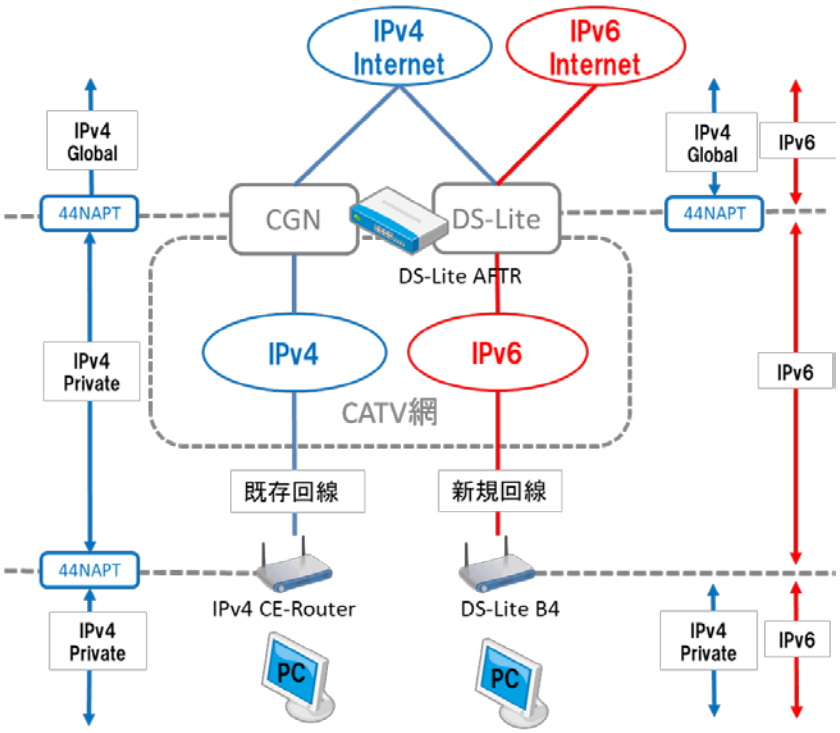


図 I.7 DS-Lite 構成図

Appendix II　PE-Router が Route Injection 機能非搭載の場合の暫定策

II 1　検討の背景

DHCPv6-PD サービスを提供する上で、PE-Router が DHCPv6 Snooping 機能と Route Injection 機能を搭載している必要がある。しかし、DHCPv6-PD サービスを提供するまでは必要となる機能では無かったため、本機能が搭載されていない機種を PE-Router として採用している事業者が多いという実態がある。PE-Router を本機能搭載の機種へ交換するには当然ながら新たな設備投資が発生するため、DHCPv6-PD サービスの普及拡大の妨げとなる。そのため、暫定的な対応として、本機能を非搭載の機種を PE-Router として採用している事業者に向けた対策を検討した。あくまで暫定的な対応であり、機器更改のタイミングなどで本機能を搭載した PE-Route を導入することを推奨する。

なお、本検討は机上での検討であり、実機を用いた試験などは行っていない点にご留意いただきたい。

II 2　検討結果

検討の結果、表 Ⅱ.1 に示す 5 つの手法が挙がった。その中でも、手法の 1 と 2 が現実的であるとの結論に至った。各手法の詳細については II 3 で記載する。

表 Ⅱ.1 検討結果

手法		ルート情報書き込みのタイミング	①誰が ②どのようにして	必要情報の参照元 ①Addr/Prefix 情報 ②NextHop(PE-Router) ③Gateway(CE-Router)
1	DHCPv6 Snooping / Route Injection 専用設備を増設 (専用設備を増設①)	CE-Router 接続後	①サーバ/ルータ ②Dynamic Routing	①DHCP Snooping(IA_PD) ②DHCP Snooping(IA_PD) ③Dynamic Routeing (iBGP,OSPF など) or RA
2	DHCPv6 Snooping のための専用設備を増設 (専用設備を増設②)	CE-Router 接続後	①サーバ ②コマンド	① DHCP ログ(Syslog or Leases)、OLT ログ(Syslog) ②PE-Router (Neighbor Addr) or OLT ログ(Syslog) ③DHCP(IA_PD)
3	Static route を手動設定	CE-Router 接続後	①オペレータ ②手入力	① DHCP ログ(Syslog or Leases)、OLT ログ(Syslog) ②PE-Router (Neighbor Addr) or OLT ログ(Syslog) ③DHCP(IA_PD)
4	Static route を事前設定	CE-Router 接続前	①オペレータ/サーバ ②手入力	①DHCP 設定(dhcpd.conf) ②DHCP 設定(dhcpd.conf) ③DHCP(IA_PD)
5	CE-Router で Dynamic Routing を実装	CE-Router 接続後	①CE-Router ②Dynamic Routing	①Dynamic Routeing (OSPF、RIPng etc…) ②Dynamic Routeing (OSPF、RIPng etc…) ③Dynamic Routeing (iBGP,OSPF etc…) or RA

II 3　各手法の詳細

各手法について詳細を示す。

II 3.1　手法 1

手法 1 は、DHCPv6 Snooping、および Route Injection を行う専用設備を増設し PE-Router へ Dynamic Routing で配布する方式である。専用設備のイメージは、ルータ型である。

本方式の技術的課題は、PE-Router に専用設備がどのようにゲートウェイ情報を渡すのかであるが、RA のルータオプションで実現できる可能性が有る。現時点で対応機器はない可能性が高いが、開発のハードルはあまり高くないと想定される。本方式は、専用設備の増設（投資）が必要となるが、PE-Router の交換と比べると経済的であると想定される。

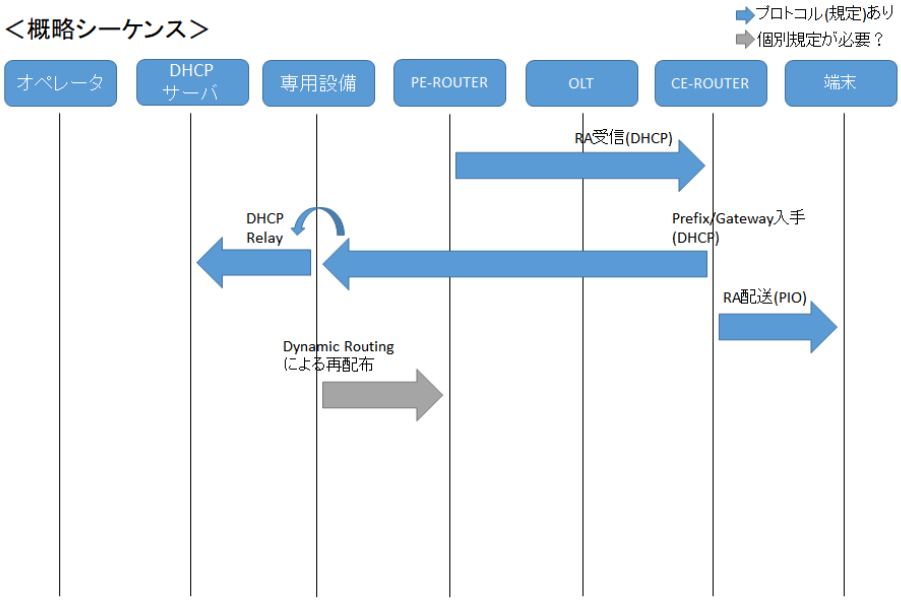


図 II.1 手法 1 のシーケンス

II 3.2 手法 2

手法 2 は、DHCPv6 Snooping を行う専用プログラム（スクリプト）により PE-Router に Static Route コマンドを投入する方式である。専用設備のイメージは、サーバ型である。また、設備増設をせずに DHCP サーバ内に専用プログラムを配置することも考えられる。

本方式は、専用プログラムの動作タイミング（DHCP の log から動作等）を検討する必要があるが実現性が高い。また、構成によっては専用プログラムの開発のみで実現できるため、投資が少なくてすむ可能性が有る。

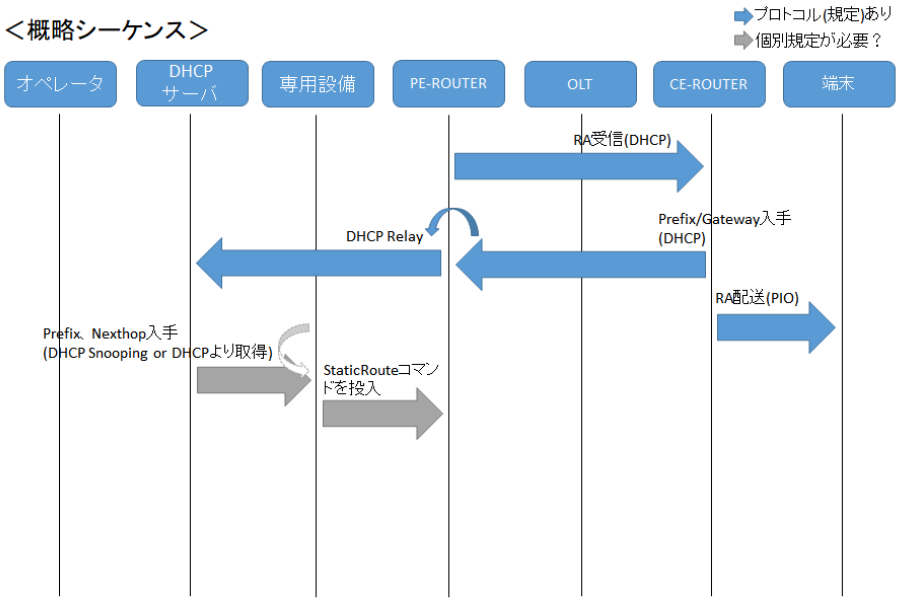


図 II.2 手法 2 のシーケンス

II 3.3 手法 3

手法 3 は、StaticRoute を手動設定する方式である。本方式の技術課題は、Prefix、Nexthop の情報の入手方法である。また、CE-Route が接続される都度、手動での設定が必要となることが、運用上致命的な問題となる。

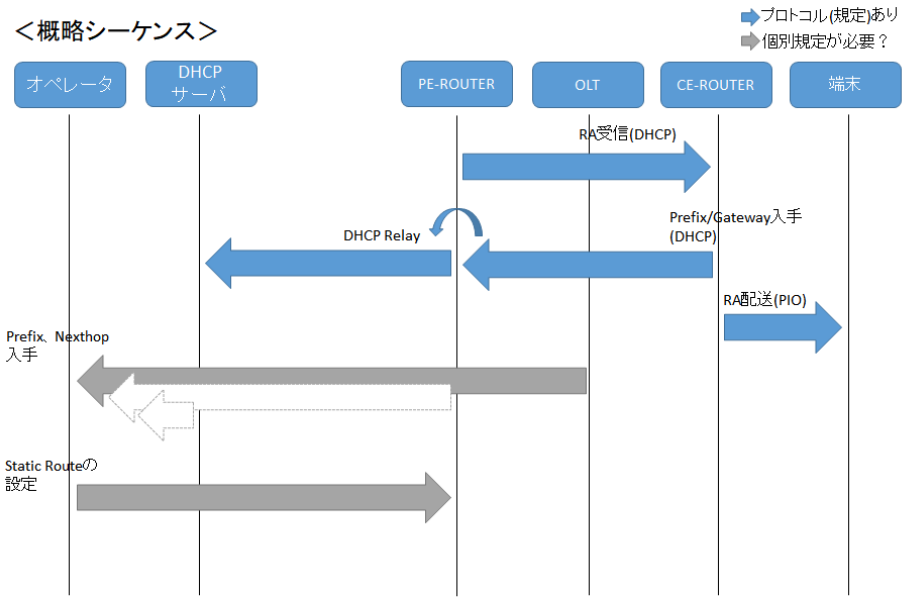


図 II.3 手法 3 のシーケンス

II 3.4 手法 4

手法 4 は、StaticRoute をあらかじめ設定しておく方式である。StaticRoute を固定にするためには、DHCPv6 サーバへ事前に払い出し、端末の DUID や IAID と払い出しアドレス情報を紐づけておく必要がある。本方式の課題は、DUID や IAID、Nexthop などの情報をオペレータがどのように入手するかである。特に、IAID は CE-Router と 1 対 1 ではないため、事前手法が最大の課題である。また、事業者が管理していない CE-Router（エンドユーザが購入した物など）への対応も検討が必要となる。

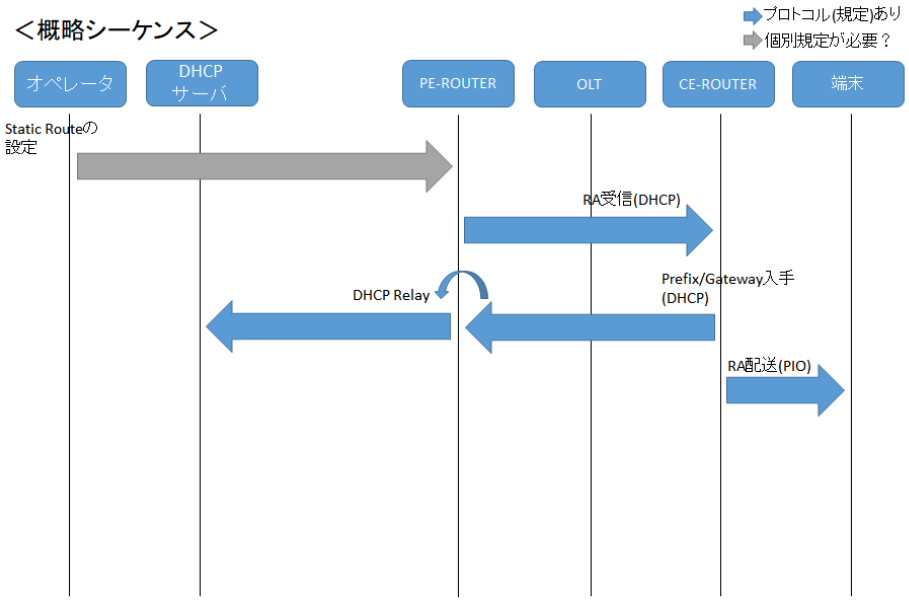


図 II.4 手法 4 のシーケンス

II 3.5 手法 5

手法 5 は、CE-Router から DynamicRouting で経路を PE-Router へ rouing する方式である。セキュリティリスクがあるため、ルータベンダが対応する可能性が低く、実現の可能性も低い。

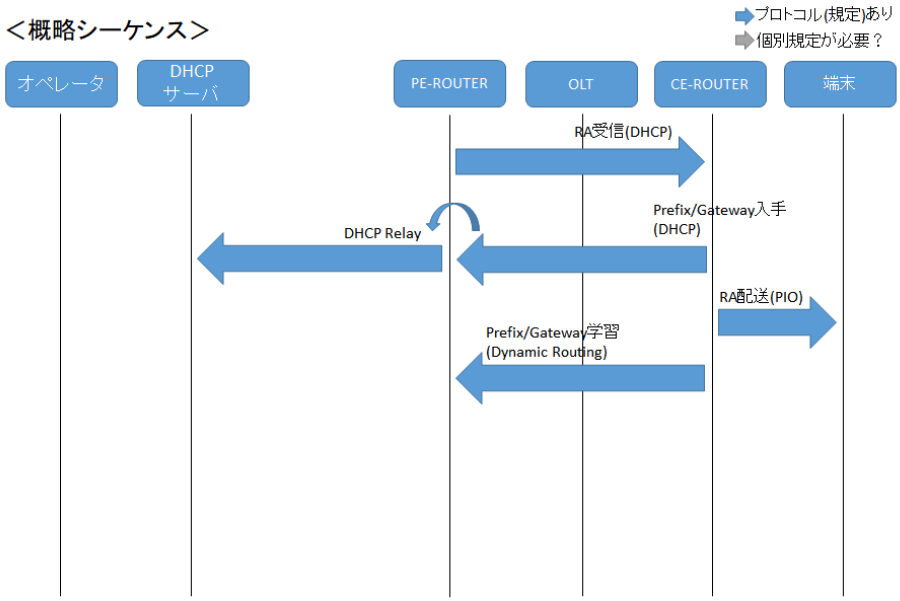


図 II.5 手法 5 のシーケンス

II 4 その他

これまでは、PE-Router に CE-Router へのルートを記述する方法について述べてきたが、検討の中では PE-Router と CE-Router の LAN 側まで同一サブネットとして、CE-Router に ND-Proxy 機能を実装させる手法も挙がった。しかし、PE-Router と CE-Router の LAN 側の同一 NW にすることは、セキュリティリスクが高いという結論に至った。たとえば、L3SW の同一セグメント内で大量の ICMPv6 が発行されたときに、大量の ND が発生することで、そのセグメント内の通信ができなくなる恐れがある。

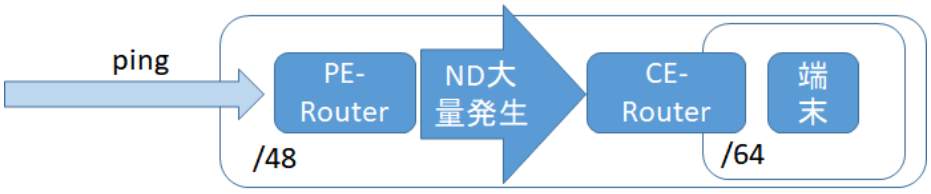


図 II.6 CE-Router に ND-Proxy を実装した場合のセキュリティリスク

日本ケーブルラボ資料

IPv6 対応ケーブルインターネット
アクセス技術仕様ガイドライン
JLabs DOC-009 3.0 版

2010 年 6 月 30 日 1.0 版
2012 年 9 月 14 日 2.0 版
2015 年 9 月 14 日 2.1 版
2020 年 3 月 26 日 3.0 版

発行　一般社団法人 日本ケーブルラボ
〒103-0025 東京都中央区日本橋茅場町 3-4-2
KDX 茅場町ビル 3 階
電話　03-5614-6100　FAX　03-5614-6101