日本ケーブルラボ仕様ガイドライン

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 2.0 版

2012 年 9 月 14 日

一般社団法人日本ケーブルラボ

Japan Cable Laboratories

.

まえがき

日本ケーブルラボ仕様ガイドラインは、ケーブル事業者施設の適正品質、互換性、相互運用性の確保等、加入者の利便を図る目的から策定される民間の指針である。

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、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むけて周知広報した。

一般社団法人日本ケーブルラボはそれらを継承して 2011 年 12 月 IPv4 アドレス枯渇対応プロジェクトメンバーを刷新し、「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」の内容更新のため改定作業に着手した。その成果物が本書である。

本ガイドラインは、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り、ケーブル事業者のインターネット運用担当者に積極的に活用されることを望んでいる。

（空白）

目　次

(空白)

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、IPv4 アドレス枯渇に対応した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 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。
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。
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。
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。
BB ルータ	本書ではブロードバンドルータをさす。
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 BB ルータが相当する。
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 と区別するために 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。
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、トラフィックを増大させ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。
GE-PON	Gigabit Ethernet-PON の略。Gigabit Ethernet をプロトコルとして用いた FTTH 向けの通信方式。
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。
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。
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。
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。
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
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 Multicast 転送を制御する機能。
MSO	Multiple System Operator の略。
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。
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。
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。
OSPF,OSPFv3	Open Shortest Path First の略。TCP/IP における経路選択プロトコルの一つ。

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。
Prefix	ネットワーク ID、インタフェイス ID で構成される IPv6 アドレス構造のネットワーク ID をさす。
RA	Router Advertisement 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。
SLAAC	Stateless Address Auto Configuration 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プログラム。
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、物理的な一つのスイッチ上に、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：BB ルータ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 アドレスを払いだ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。

1.3 参考文献

[1] DOCSIS® 1.0 ANSI/SCTE 22-1 2002R2007,22-3 2002R2007

[2] DOCSIS®1.1 CM-SP-RFIv1.1-C01-050907,OSSIv1.1-C01-050907

[3] DOCSIS®2.0 CM-SP-RFIv2.0-C02-090422,OSSIv2.0-C01-081104, IPv6-I01-090518

[4] DOCSIS®3.0 CM-SP-MULPIv3.0-I19-120809,OSSIv3.0-I19-120809

第 2 章 ガイドラインの対象者と適用範囲

2.1 ガイドライン対象者

本ガイドラインでは下記のとおり、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に及ぶまで、ある程度広い範囲をガイドライン対象者とする。

(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、第 3 章に示す対象サービスを適用範囲とした。

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)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

(3)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、作成中の既存標準規格に準拠、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ため、クライアント OS や家庭用ルータの対応状況までは言及しない。

第 3 章 IPv6 対応サービスプラン

3.1 対象サービス・アドレス割り当て方式

3.1.1. 対象となるサービス

ケーブル事業者が提供するサービスは様々であるが、本ガイドラインではケーブル事業者自らが構築し加入者に提供する下記のインターネット接続サービスについて言及する。なお、他社の設備を利用したサービスについては、自社でのポリシーが容易に適用できないことが想定されるため対象としない。

しかし、当ガイドラインに基づいた構築が可能である場合はサービス提供者と十分な調整をおこなった上で、当ガイドラインを適用すること。

(1) DOCSIS を利用して提供されるケーブルインターネット接続サービス
(2) CATV-FTTH によるケーブルインターネット接続サービス(GE-PON)
(3) ケーブル Wi-Fi（無線 LAN サービス）によるインターネット接続サービス
(4) 加入者宅内に設置される無線 LAN ルータ等の付加サービス

3.1.2. 想定される IPv6 アドレス割り当て方式

IPv6 アドレス割り当て方式は、IPv4 アドレスに比べ様々な方式が存在する。特に大きな特徴としては、IPv4 アドレスには存在しなかった SLAAC を使った IPv6 アドレス割り当てが可能となったことである。この方式は、DHCPv6 サーバなどを用いずに RA から IPv6 アドレスを生成する方式である。DHCPv6 サーバが不要となるために、一見効率的な割り当て方式に見えるが、RA を受信した端末自身が IPv6 アドレスを自身で生成するために、ケーブル事業者から端末の特定ができなくなり、運用上不都合が起こる可能性が高い。したがって、ケーブル事業者が提供する IPv6 サービスについては、SLAAC 方式は使わず、DHCPv6 方式を使用することが望ましい。以上を踏まえ、対象となるサービスの中で IPv4 を含めたアドレス割り当て方式について表 3-1 に示す。

表 3-1 想定される IPv4/v6 アドレス割り当て方式

名称	IPv6	IPv4
ケース 1 dual-stack 方式	途中経路も含めて全て IPv6 化	従来通り（ｸﾞﾛｰﾊﾞﾙ/ﾌﾟﾗｲﾍﾞｰﾄ） DHCP・固定含む
ケース 2 IPv4 トンネル方式	宅内端末や GW 等で IPv4 にカプセル化する（途中経路は IPv4）	従来通り（ｸﾞﾛｰﾊﾞﾙ/ﾌﾟﾗｲﾍﾞｰﾄ） DHCP・固定含む
ケース 3 IPv6 トンネル方式	途中経路も含めて全て IPv6 化	宅内端末や GW 等で IPv6 にカプセル化する（途中経路は IPv6）

(1)ケース 1：dual-stack 方式

加入者宅内機器から IPv6 バックボーンまで dual-stack であり、目指すべき最終構成である。全ての機器を dual-stack 対応とする必要があるため IPv6 対応を完了するまでの期間も長くなり機器交換コストも必要となるが、運用性や拡張性の点で優れている。

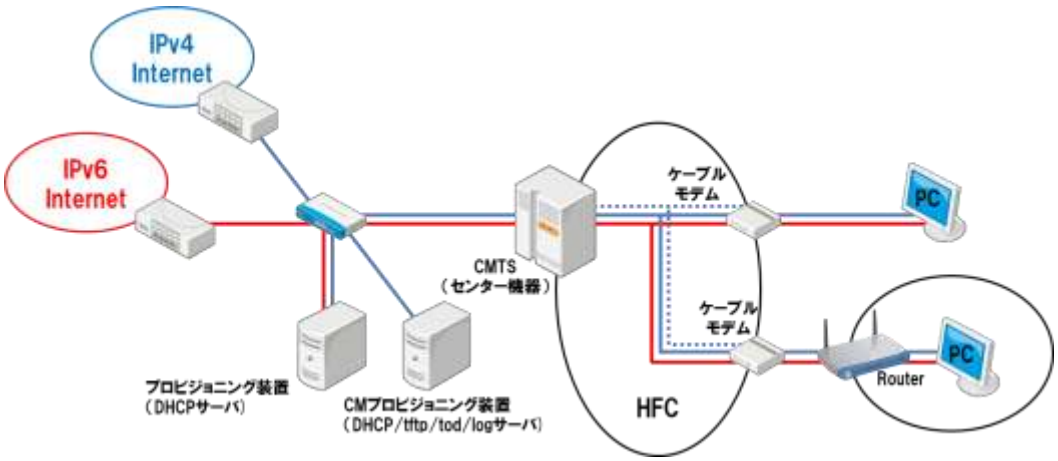


図 3-1 dual-stack 方式

(2)ケース 2：IPv4 トンネル方式

IPv6 パケットを IPv4 でカプセル化して、トンネルリレールータまで IPv4 にて転送、カプセルを解除した後、IPv6 ネットワークに転送する方式。加入者宅内及びセンターにトンネルルータが必要であるが、途中の経路は IPv4 のみで加入者宅内を dual-stack にすることができるため、宅内を早期に IPv6 対応させることが可能となルータだ、センターのトンネルルータに障害等が発生した場合、IPv6 サービスが停止するため冗長性の確保が課題である。また、トンネルを使用するため、運用性や拡張性の観点で優れていない。なお、この方式の採用は、急遽 IPv6 のネットワークが必要になった場合などの一時的な措置であることを十分に理解した上で構築を行い、最終形とならないようにすることが望ましい。

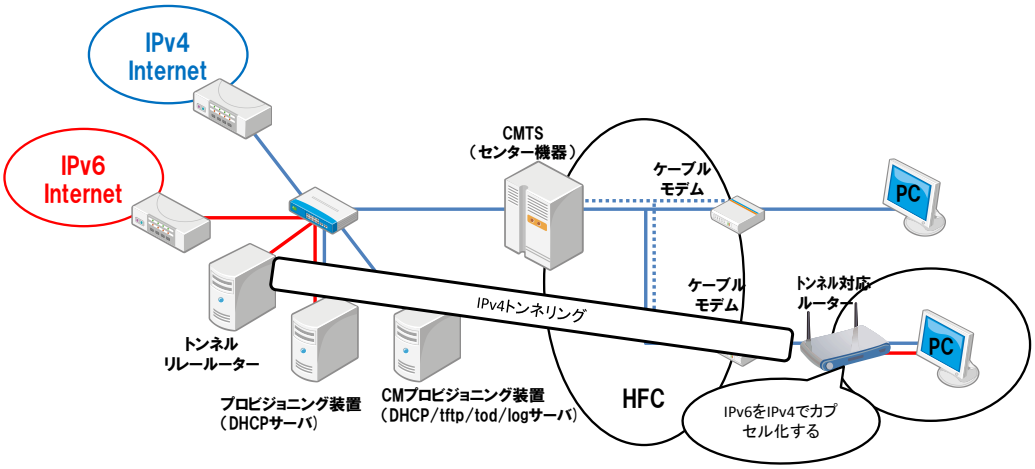


図 3-2 IPv4 トンネル方式

(3)ケース 3：IPv6 トンネル方式

IPv4 パケットを IPv6 でカプセル化して、トンネルリレールータまで IPv6 にて転送、カプセル化を解除した後、IPv4 ネットワークに転送する方式。加入者宅内及びセンターにトンネルルータが必要であるが、途中の経路は IPv6 のみで加入者宅内を dual-stack にすることができる。センターのトンネルルータに障害等が発生した場合、IPv4 サービスが停止するため冗長性の確保が課題である。またトンネルを使用するため、運用性や拡張性の観点で優れていない。なお、途中の経路が IPv6 に対応していることが前提となるため、dual-stack 方式によるネットワーク構築を行った後となる。また、IPv4 アドレス枯渇対策としては加えて LSN を利用することもできるため、どちらの方式を採用するかは検討が必要である。

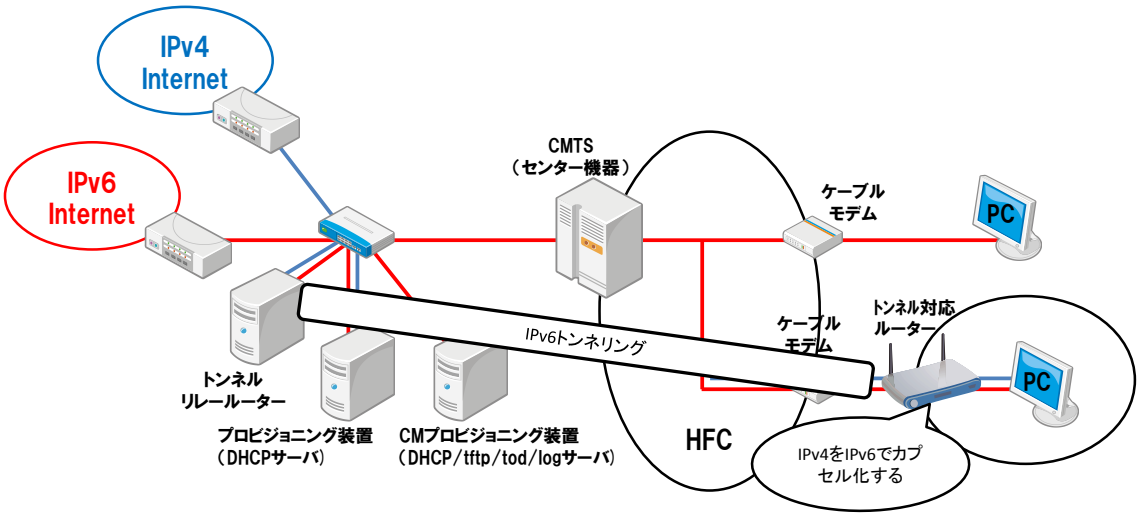


図 3-3 IPv6 トンネル方式

3.1.3. IPv6 サービス提供開始順序

IPv6 サービスを提供開始する際には、サービスに差分なく提供できることが理想であるが、設備対応状況や加入者周知、カスタマ部門の教育など、一度にサービスを開始することが困難であるケースが多いと想定されるために、加入者に対する混乱を招かない方法で提供開始することが重要である。

以下にサービス提供開始順序例を示す。所要期間は 1 年程度と想定されるが、関係各所への教育やトライアル等も必要となるため、早期に着手することが望ましい。

＜提供順序例＞

・DOCSIS を利用したケーブルインターネット接続サービスの場合

・IPv4/v6 アドレス割り当て方式は、ケース 1 の dual-stack 方式にて記述

(1)基本ポリシーを決定する

- 高速サービス（チャネルボンディング）からサービス提供を開始
  ※DOCSIS システムの IPv6 対応は、DOCSIS3.0 である事が必須
- その他サービスについては、設備対応が準備できた時点で開始
  ※FTTH の場合
  ・新規導入のケースが多いため、当初設計から IPv6 対応を考慮し設備構築する
  ・サービス提供時期はケーブル事業者の判断に委ねる

(2)CMTS より上位部分を全て dual-stack 化

- CMTS に接続されるルータや L3-SW 等の機器を全て dual-stack 化

(3)CM の Config で、IPv6 のパケットをフィルタ

- LLC フィルタを用いて IPv4 と ARP のみ透過を許可

(4)CMTS を DOCSIS3.0 対応にして IPv6 を有効化

- この時点で CPE 用の DHCPv6 サーバの構築を完了している必要がある。
  なお、CM 用のプロビジョニングシステムは、IPv6 対応を実施しない。
  ※CM のマネージメントは IPv4 のみのため

(5) 上記(3)で設定したパケットフィルタの解除

- サービス提供が可能と判断されたエリアの高速サービス用 CM の Confiig を変更
  （IPv4/ARP に加えて IPv6 の Ethernet タイプ番号 0x86DD を透過）

3.2 IPv6 サービス提供開始における広報・契約面の課題

3.2.1. IPv6 サービス提供に関する広報について

IPv6 サービスを提供開始することについては ISP としてのケーブル事業者には必然であり、既存加入者や新規顧客に対しても広報すべきである。ここでは以下のような広報手法を推奨する。

(1)自社のホームページによる対応状況の広報

2010 年 4 月に総務省から公開されている『ISP の IPv4 アドレス在庫枯渇対応に関する情報開示ガイドライン』に基づき、各ケーブル事業者としての基本方針などを公開するとよい。
http://www.soumu.go.jp/menu_news/s-news/02kiban04_000022.html　参照

また、可能であれば関係団体などのホームページへのリンクも行い、メールマガジンなどを用いた広報を行うこともよい。

図 3-4　IPv6 対応についての掲載例

※株式会社コミュニティネットワークセンターのホームページから抜粋

(2) 自社のホームページの IPv6 対応

自社加入者への IPv6 サービスを提供するよりも前か同時期までには自社のホームページは IPv6 対応していることが望ましい。

3.2.2. IPv6 サービスによる料金追加について

IPv6 サービスによる加入者からの追加課金について、同業他社を見る限りでは IPv6 サービスを提供することによる追加課金はないようなので、競争力の面も勘案して慎重に検討する必要がある。

表 3-3 同業他社の IPv6 サービス状況※1

提供事業者	サービス名	IPv6 アドレス割り当て方式	追徴の有無
KDDI	au ひかり※2	加入者宅設置の GW にて DHCPv6-PD で Prefix 割当、宅内は SLAAC	無し
コミュファ	コミュファ光※3	加入者宅設置の GW にて DHCPv6-PD で Prefix 割当、宅内は SLAAC（Wi-Fi 付 HGW）	無し

※1：表の情報は平成 24 年 8 月 31 日現在

※2：引用 HP　http://www.kddi.com/corporate/news_release/2012/0124/besshi.html

※3：引用 HP　http://www.ctc.co.jp/news/2012/120808_1.html

第 4 章 IPv6 ネットワーク概要

4.1 定義

4.1.1. アクセス網

(1) DOCSIS におけるアクセス網の定義範囲を図 4-1 に示す。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。

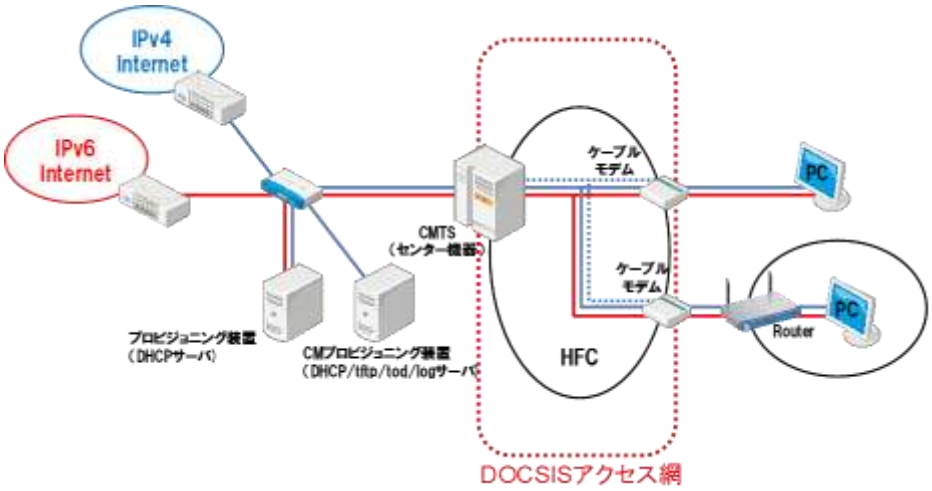


図 4-1 DOCSIS アクセス網の定義

(2) FTTH におけるアクセス網の定義範囲を図 4-2 に示す。OLT が L3 終端しないため、上位の L3 装置までがアクセス網となる。CMTS-CM の役割を L3 装置-OLT/ONU の組み合わせで実現するため、L3 装置に要求される 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 L3 装置と OLT/ONU のどちらで持たせるのかなどの考慮が必要である。L3 装置は FTTH ベンダと相談して選定することが望ましい。

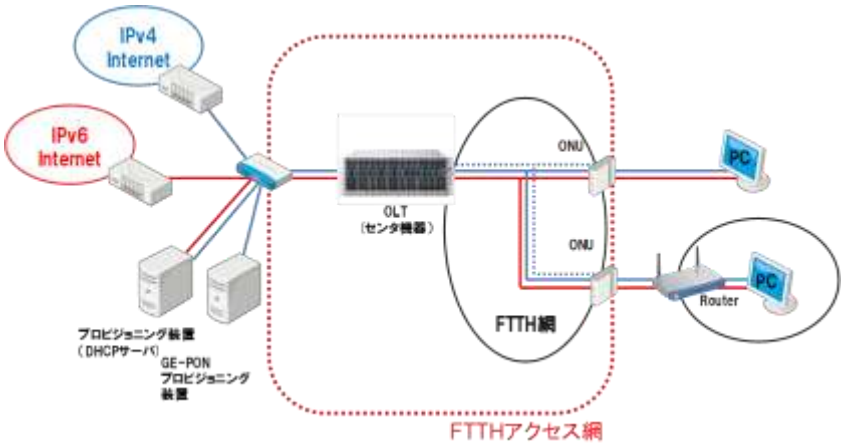


図 4-2 FTTH アクセス網の定義

4.1.2 上位ネットワーク

上位ネットワークの定義範囲を図 4-3 に示す。

(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 の場合は GE-PON 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。

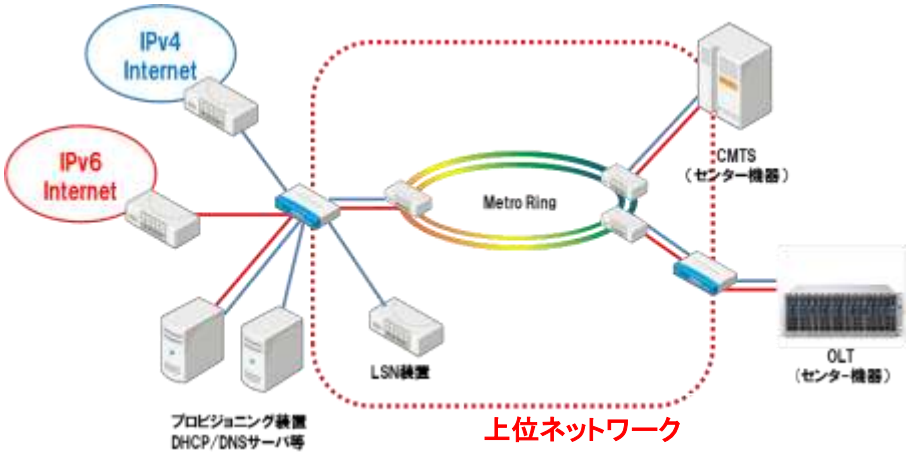


図 4-3 上位ネットワーク構成図

4.1.3 プロビジョニングシステム

プロビジョニングシステムの定義範囲を図 4-4 に示す。障害の場合、影響が大きいため通常はコンポーネント毎に 2 台以上での筐体冗長を図る。DHCP/DNS/TFTP などの影響度が特に高いコンポーネントについてはセグメント分離、拠点分離などできる限り耐障害性向上を図ること。また Firewall を適切に配したセキュリティ、DoS 対策などを行う必要がある。入り口には Firewall による NAT を行うことが望ましい。

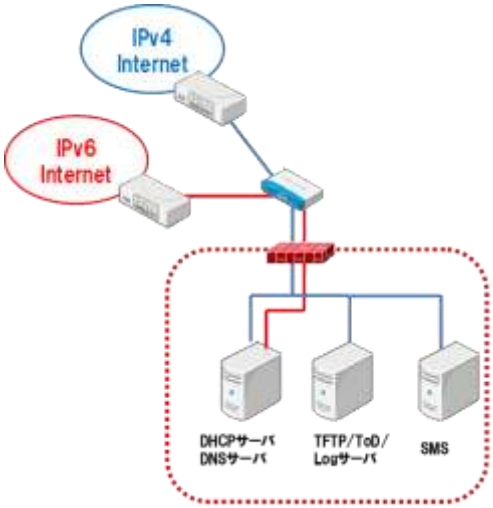


図 4-4 プロビジョニング構成図

4.1.4 サーバ

サーバは dual-stack でサービスすることにより、End-to-End での通信が可能になりサーバロードバランサ等のプロトコル変換装置を導入せずにシンプルな構成が実現できる。また、新規アプリケーションへの対応が容易になる。監視の面でもアクセス元の IP アドレスを確実に把握でき、アクセス制御や監視等がシンプルに対応可能である。しかし、IPv4/v6 の分解点が設定できないためサービスの全面的な dual-stack 化が必要なる。

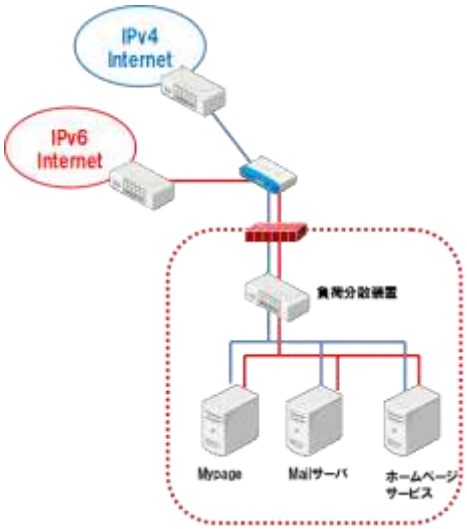


図 4-5 サーバ構成図

4.2 移行ネットワーク図

基本的な IPv4 ネットワーク（図 4-6）から dual-stack（図 4-7）への想定される移行モデルを以下に示す。

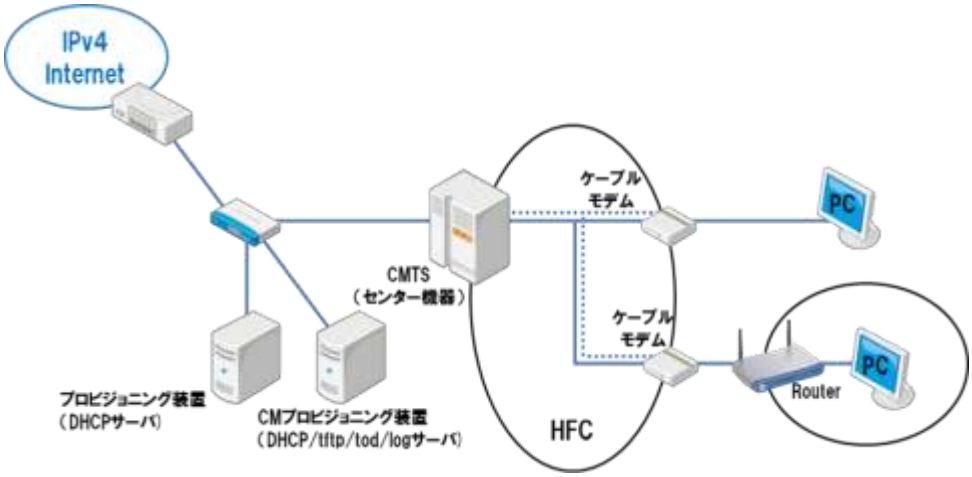


図 4-6 IPv4 のケーブルネットワーク構成例

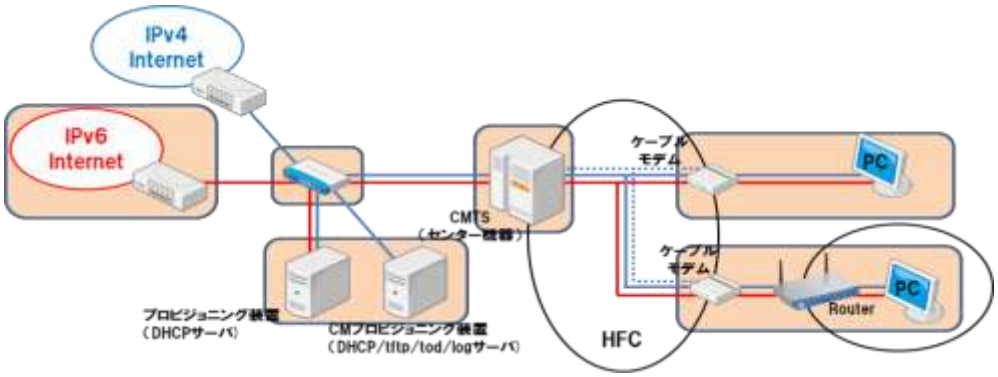


図 4-7 IPv4/v6 dual-stack のケーブルネットワーク構成例

4.3　IPv4 を IPv6 ネットワークへ移行する場合の考慮すべき事項

図 4-7 の構成略図内の枠色つき個所を変更する。

(1) IPv4/v6 へ対応の ISP との接続。

(2) ルータ、CMTS 及びプロビジョニングサーバ(DHCP など) を IPv6 対応製品へソフトウェアのバージョンアップもしくは入れ替え。

(3) CM を IPv6 対応へファームウェアのバージョンアップ、もしくは DOCSIS3.0 対応 CM へ入れ替え。

(4) PC は　IPv6 プロトコルに対応した製品にする。

(5) IPv6 の場合、HE・コアネットワーク内、ルータないし NAT 追加もしくは LSN を経由し IPv4　ISP へ繋ぐ。（本書では言及しない）

＜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、性能インパクトの検証。
- IPv6 化移行に関する、段取り。

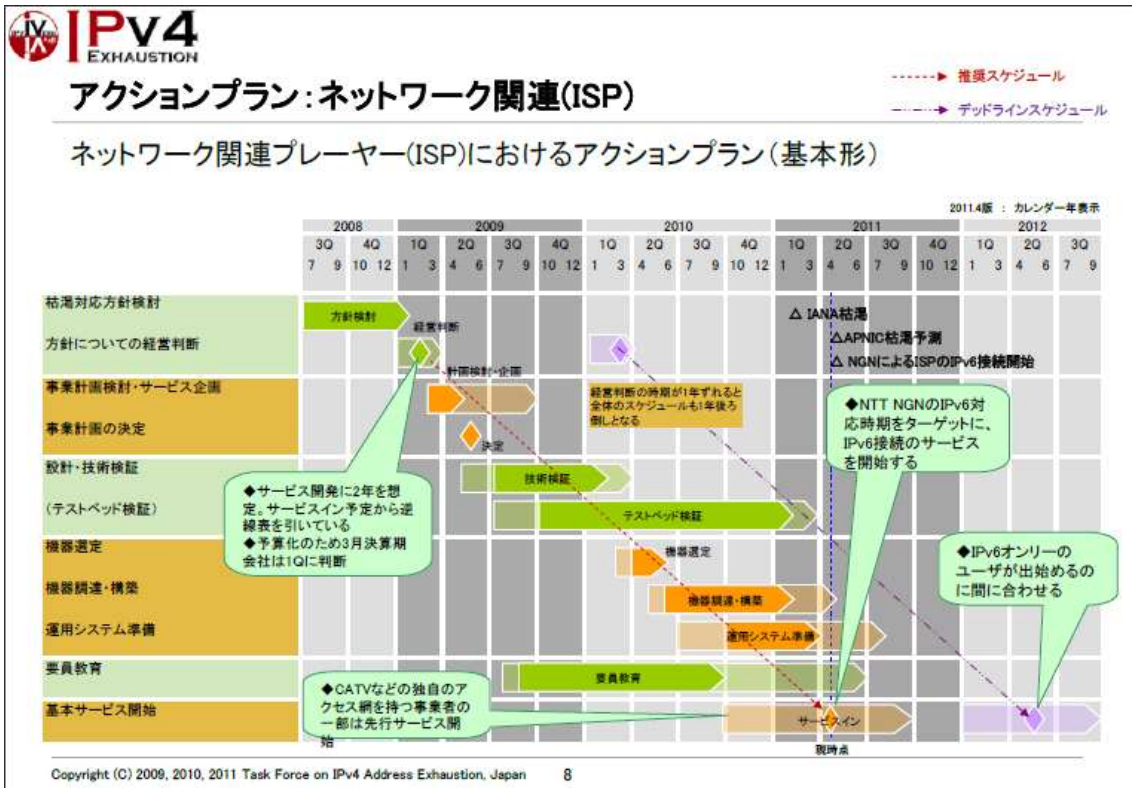
① CMTS のみを IPv6 対応（バージョンアップ、または新規導入）にする。

② CM のファームウェア・バージョンアップ。

③ CM の DOCSIS3.0 へ入れ替え。

上記①、②、③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。

4.4 移行プラン



IPv4 アドレス枯渇対応アクションプラン 2011.04 版より

● システム移行のシナリオ

現状の IPv4 から IPv6 ネットワークへの移行シナリオを表 4-1 に示す。導入期と共存期が長期に渡ると考えられる。この期間は設備規模や投資計画などの要因で変動する。対応性の良いサーバや上位ネットワークから対応し、CMTS/CM/CPE のリプレイスに合わせて対応していくのがスムーズである。

表 4-1 IPv4 から IPv6 への移行シナリオ

ﾌｪｰｽﾞ	現在	導入期	共存期	完了期
		IPv6 移行開始	本格的 IPv6 移行	完全 IPv6
状態 ｱｸｼｮﾝ 注意点 など	IPv4 のみ	・試験導入 ・ｱﾌﾟﾘｹｰｼｮﾝ試験		IPv6 のみ 一部に IPv4 が残る可能性あり。
		・端末の Dual-Stack ・サーバの Dual-Stack と ｱﾌﾟﾘｹｰｼｮﾝ IPv6 対応	更改に合わせたｽﾑｰｽﾞな Dual-Stack 化	
		・トンネル、v4/v6 ﾄﾗﾝｽﾚｰﾄ、GW ・対応できない機器、ｱﾌﾟﾘｹｰｼｮﾝの洗い出し。 ・IPv4/v6 混在時の誤動作機器の洗い出し。 ・Multicast の IPv6 化検討 ・Mobile 機器の IPv6 化検討	・Dual-Stack による併行稼働状態 ・IPv4 だけのｾｸﾞﾒﾝﾄが残る可能性あり ・Internet 接続 IPv6 化	

4.5 ルーティング

static 運用は経路数が多くなり config も増大して、管理コストも大きくなるので、動的プロトコルでのルーティングを推奨する。対応プロトコルは、OSPF、IS-IS、OSPF+PrivateAS での BGP、RIP 等が考えられるので、上位機器等の config など考慮して検討する必要がある。

第 5 章 DOCSIS ネットワークの IPv6 対応

5.1 既存の IPv4 サービス仕様

DOCSIS ネットワークは図 5-1 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。

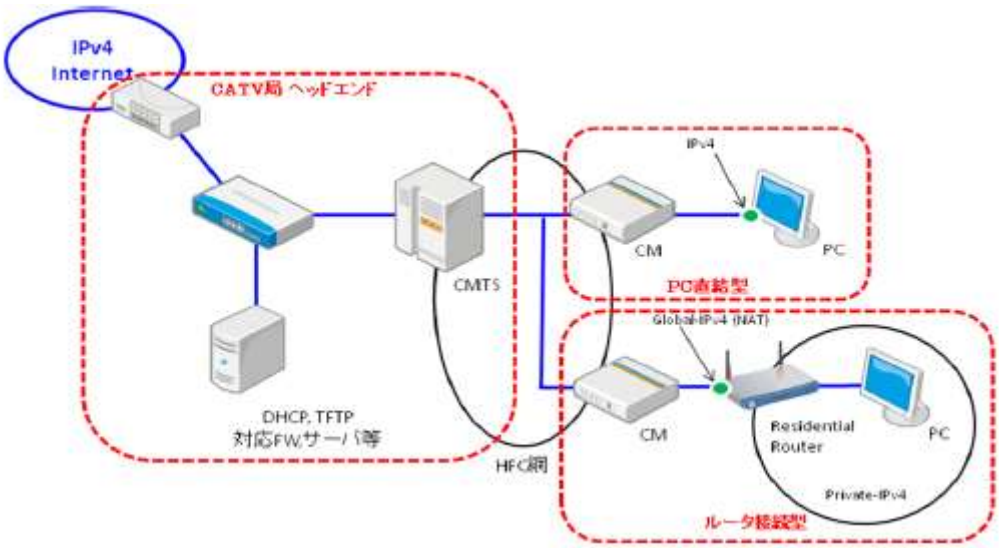


図 5-1 一般的な DOCSIS IPv4 サービス設備構成例

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例が多い。
- 不正 DHCP server 対策
- NetBIOS / Direct Hosting of SMB
- ウイルス対策（option,1434,4444,5000,etc）

5.2 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 2.0+IPv6 仕様を用いて、CM に対して管理用に IPv4 または IPv6 または dual-stack でその両方を割り当て、さらに CM の先の加入者端末に dual-stack 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 により行われる。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 5-2 に示す。

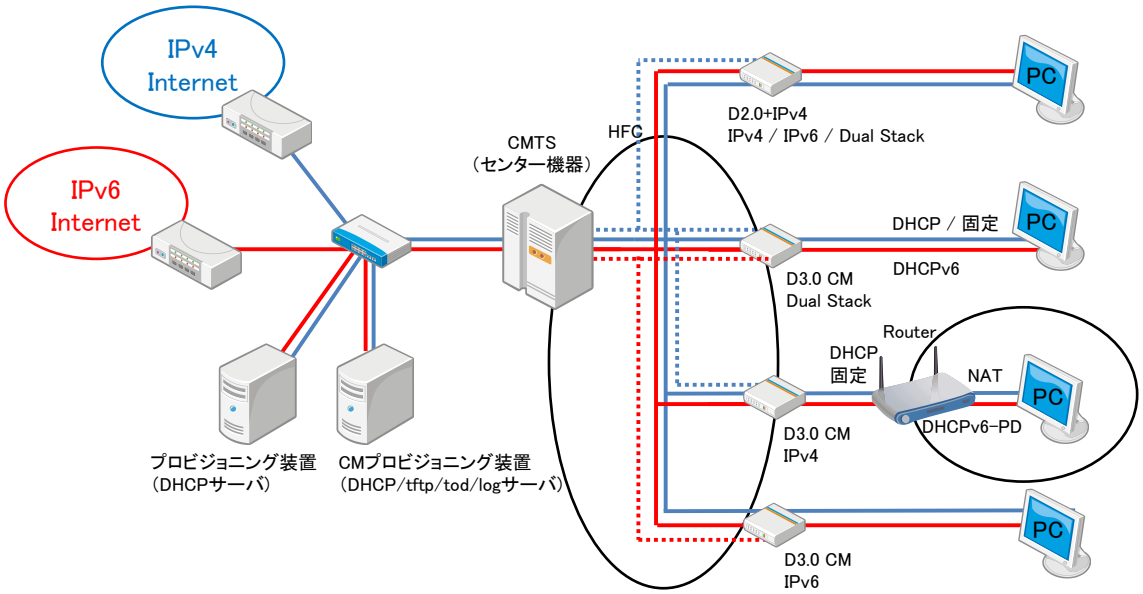


図 5-2 想定する IPv6 サービス形態

IPv6 サービスには DOCSIS 3.0 と 2.0+IPv6 準拠の CM を用いる。ガイドライン 1.0 版では IPv6 未対応の DOCSIS 2.0 CM に対して static multicast MAC アドレス機能を用い、透過したい multicast アドレスの MAC アドレスを設定することで RA を受信するという対応方法を述べたが、その後の検討で運用面を含めた管理が不十分と判断されたため本版からは除外した。その理由は 5.5 項に述べている。

5.3 ネットワーク構成

基本的な構成を図 5-3 に示す。CMTS は上位のルータ/L3-SW に接続される。上位接続のリンクを dual-stack 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 インタフェイスには 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としては CPE の dual-stack 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。

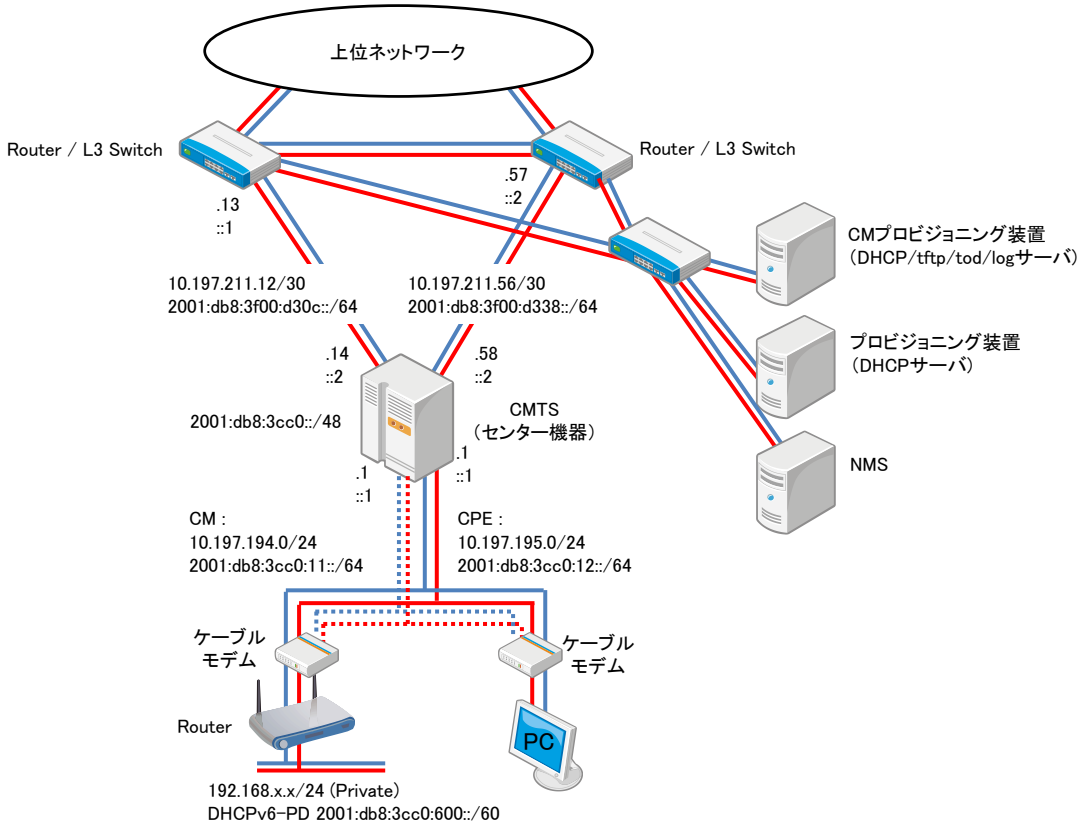


図 5-3 基本的なネットワーク構成

5.4 DOCSIS システムでの IPv6 サービス構築上の検討ポイント

加入者に dual-stack 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 5-1 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 アクセスは従来通り 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 5-1 IPv6 サービスのために必要な機能

目的	機能	IPv4	IPv6
ユーザーにDual Stackサービスを提供する	Dual Stack	○	○
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	○	○
ユーザーの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	○	△

5.5 DOCSIS システムにおける 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 5-2 に示す。これらの個々の機能の解説を(1)～(9)にて説明する。

表 5-2 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 dual-Stack	Multicast DSID Forwarding	GMAC Promiscuous
		GMAC Explicit
	RA Off-Link	
	DAD Proxy	
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 のインタフェイスでの IPv6 アドレス割り当て

インタフェイスは dual-stack にし、IPv6 側では/64 のアドレスを割り当てることを設定。CPE へのアドレス割り当てポリシーは Cable インタフェイスでの 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 を立てる設定を入れる。

(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 毎となり、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フィックに 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。

尚、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、dual-stack 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 dual-stack 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 dual-stack を提供することはできない。CPE に dual-stack を許可する場合には LLC フィルタに Ether Type = 34525 を追加する。また逆にこの LLC フィルタを用いて dual-stack を許可する加入者と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させることが可能である。

(5)DHCPv6-PD と Route Injection

IPv6 ルータへの 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ルータが必要とする Prefix を割り当てる。ルータからの Solicit に対して DHCPv6 サーバは例えば 2001:db8:3cc0:1ff0::/60 などの Prefix を割り当て、ルータは LAN インタフェイ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。ルータの LAN 側に接続された CPE はルータ LAN インタフェイスからの 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 Prefix と CPE が生成するアドレスの関係を図 5-4 に示す。

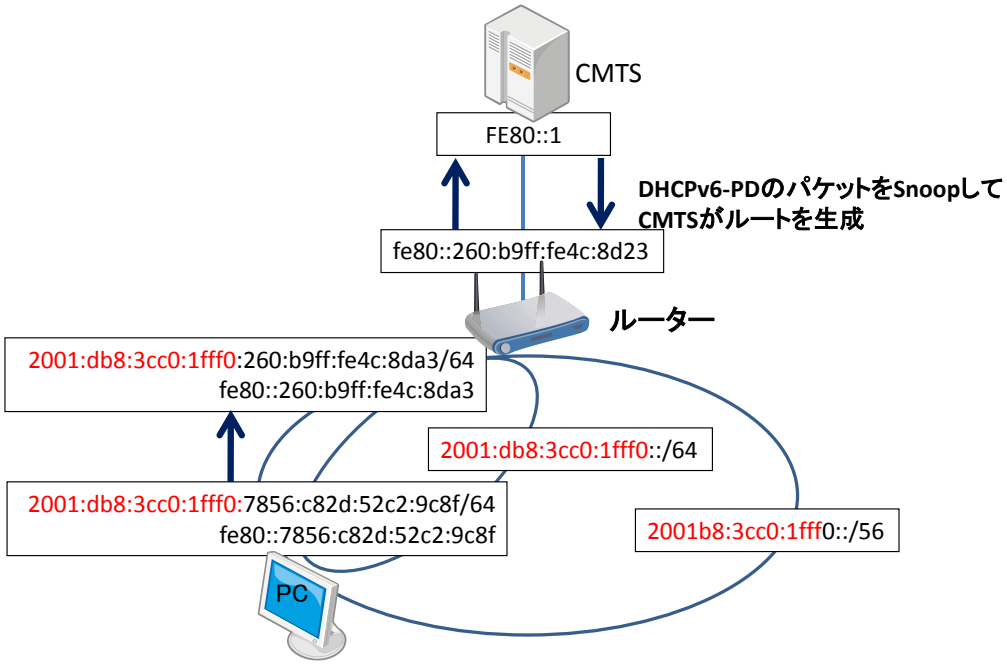


図 5-4 DHCPv6-PD で割り当てたアドレスの CPE での使用

CPE から見た default route はルータの LAN インタフェイスからの RA で CPE に与えらる。またルータの default route は CMTS の Cable インタフェイスからの RA で与えらる。逆に DHCPv6-PD で割り当てた Prefix がどのルータ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 し動的に Route Table を生成する必要があり、これを DHCPv6-PD Route Injection と言う。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無いため、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 Multicast が多く使用される。DOCSIS 3.0 または 2.0+IPv6 仕様では Multicast 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 Multicast がフォワードされる。

表 5-3 DOCSIS 3.0/2.0+IPv6 で規定された MDF の Mode

CM / CMTS	DOCSIS2.0+IPv6		DOCSIS3.0
	MDF-incapable CM	MDF-capable CM	
REG-REQ / REG-RSP	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 Multicast を対応する仕様で default では IPv6 で必要な Multicast を通さない。CM が Multicast 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。

① RA が CM を通過せず、CPE が IPv6 Default Gateway を受け取れない。

② 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。

③ 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①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 Malticast 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 Multicast 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 トラフィ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 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

方法としてインタフェイスに 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フィルタリングの方法がある。

① IP Filtering (docsDevFilterEntry)

② Subscriber Management Filter (CM Config File : TLV37)

③ 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、dual-stack には利用できない。よって dual-stack 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をは 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。

5.6 DOCSIS システムでの 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、場合によっては、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の必要がある。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 dual-stack 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 5-5 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。

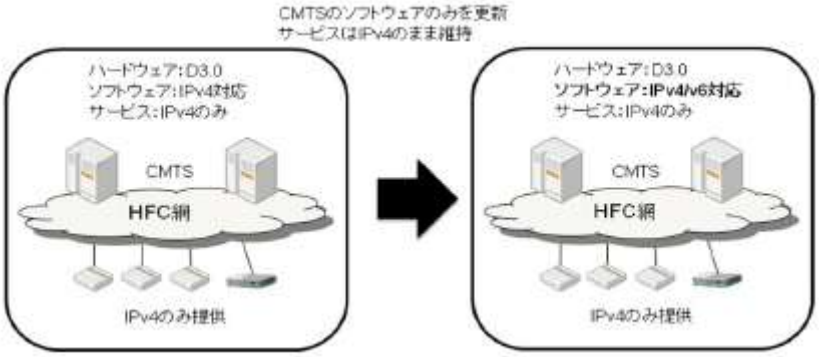


図 5-5 CMTS のみバージョンアップしサービスは IPv4 のまま維持

(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 dual-stack 化する場合、各インタフェイスの 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。

- 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。
- 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 など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。

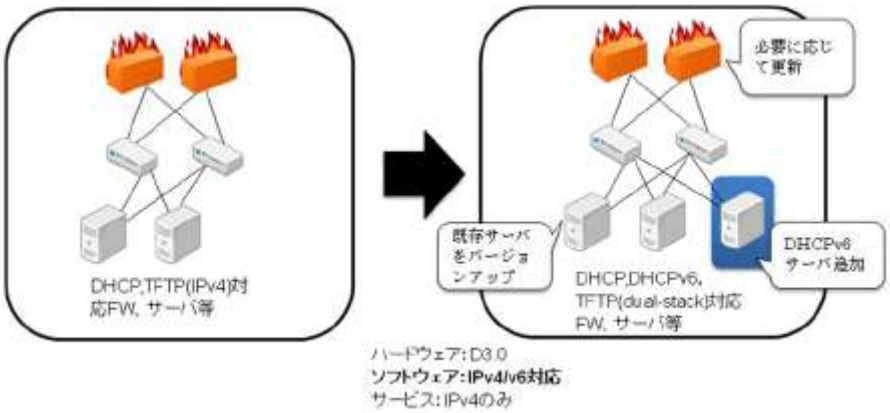


図 5-6 DHCP サーバを準備

(4)CM プロビジョニンング方法の変更

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 2.0+IPv6 CM が必要である。しかし、DOCSIS3.0 および 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。

※2010 年 6 月時点の実装状況にて記述

(a) DOCSIS3.0、2.0+IPv6CM に使用する管理用 IP アドレスを IPv4 のまま維持する。

(b) DOCSIS3.0、2.0+IPv6CM に管理用 IP アドレスとして IPv6 を割り当てる。
または dual-stack とする。

- CM は IPv4 アドレスのまま運用する場合、
  上記(a)の方法を選択する場合、CMTS の MDF を有効化することにより Multicast 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 Multicast が透過される。
- CM に IPv6 アドレスを割り当てる。
  上記(b)の方法を選択する場合、CMTS の MDF を有効化することにより Multicast 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 Multicast 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イスに CM 用の IPv6 アドレスを設定する。そして、stateful 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)dual-stack 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。Dual-stack 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

dual-stack 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 6 章 FTTH ネットワークの IPv6 対応

6.1 既存の IPv4 サービス仕様

現在、FTTH では GE-PON が用いられる事が多く、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。

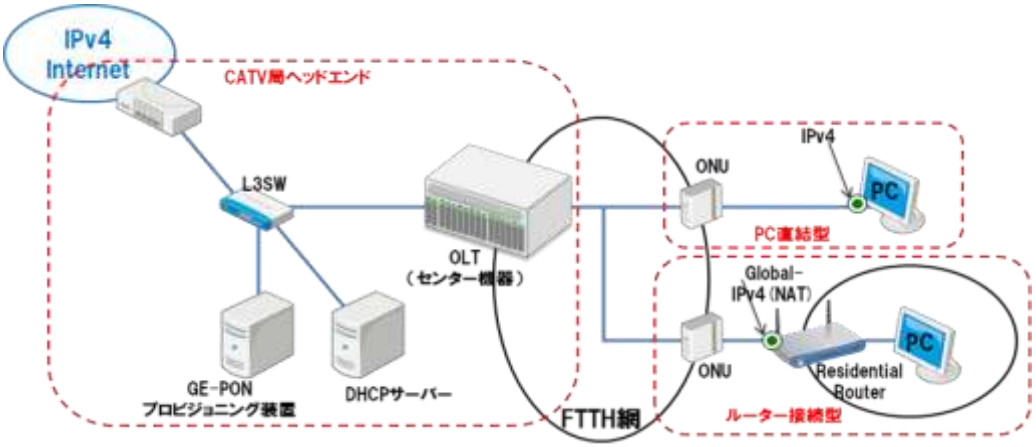


図 6-1 一般的な FTTH インターネット接続サービス設備構成例

(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無く、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 等）

6.2 FTTH ネットワークへの IPv6 適用

6.2.1. IPv6 対応の GE-PON の導入

FTTH ネットワークを IPv6 対応にする場合、第 3 章で説明のあった 3 つの方式のうち dual-stack 及び IPv6 トンネルの場合は使用する GE-PON で IPv6 のストリームが流れることが必要となる。また dual-stack 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 の Snooping を行える機能が必要となる。

6.2.2. IPv6 対応後の想定するサービス仕様とネットワーク構成

第 3 章の 3 つの方式について FTTH の場合の注意点も含めて以下に述べる。

(1)ケース 1：dual-stack 方式

FTTH 網も含めて dual-stack 化されている構成。IPv4 のストリームも IPv6 のストリームも 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 GE-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。

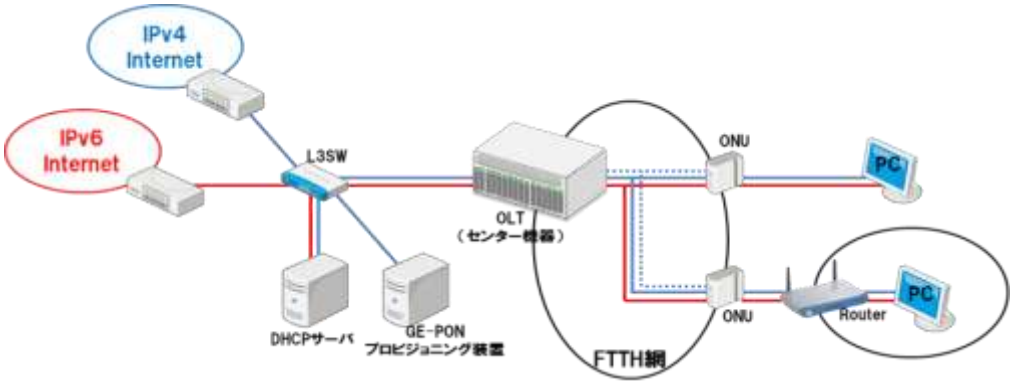


図 6-2 dual-stack 方式の設備構成例

(2)ケース 2：IPv4 トンネル方式

OLT から加入者側の経路が IPv4 の方式。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。尚、本方式は納期等の問題により 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。

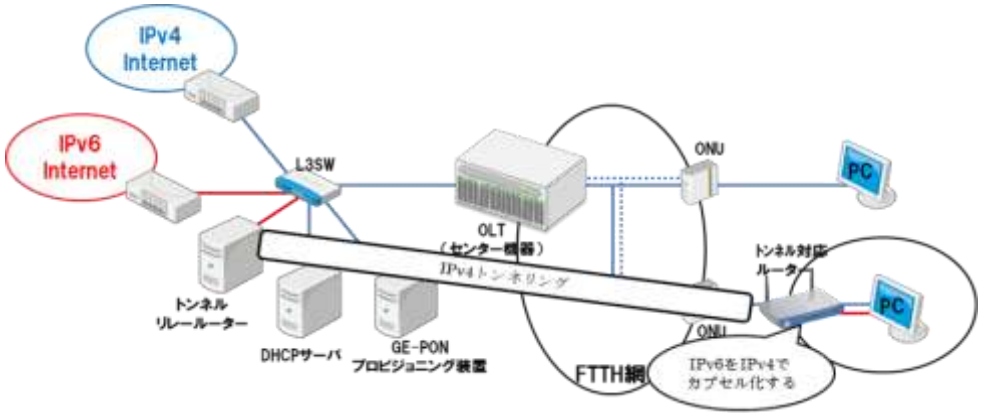


図 6-3 IPv4 トンネル方式の設備構成例

(3)ケース 3：IPv6 トンネル方式

OLT から加入者側の全ての経路が IPv6 である方式。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等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 dual-stack 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。

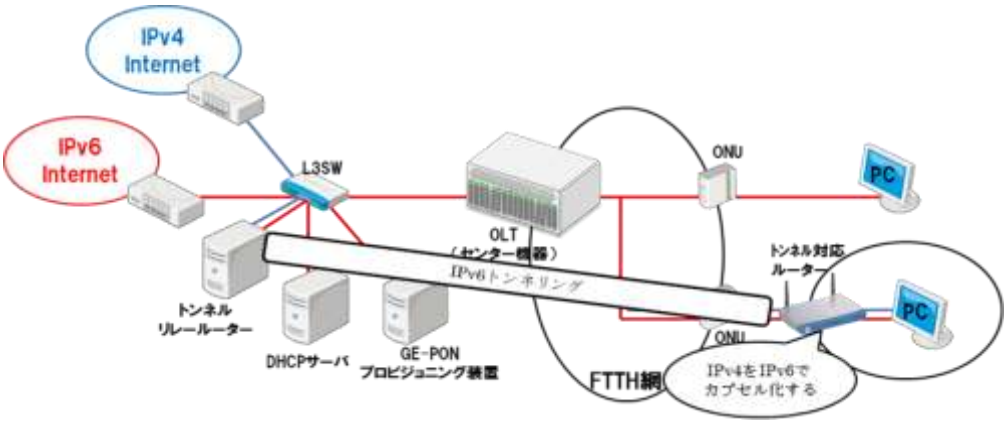


図6-4　IPv6トンネル方式の設備構成例

6.2.3. FTTH ネットワークにおける v4/v6 の CPE プロビジョニングの違い

FTTH ネットワーク上で CPE プロビジョニングをする場合、CPE が要求するアドレスが IPv4 か IPv6 であるかによってプロビジョニング方法に大きな違いが発生する。また L3-SW の機能も備えている CMTS とも異なり、OLT にはその機能がないので L3-SW を組み合わせて IPv6 プロビジョニングを行う必要がある。以下にその例を示す。

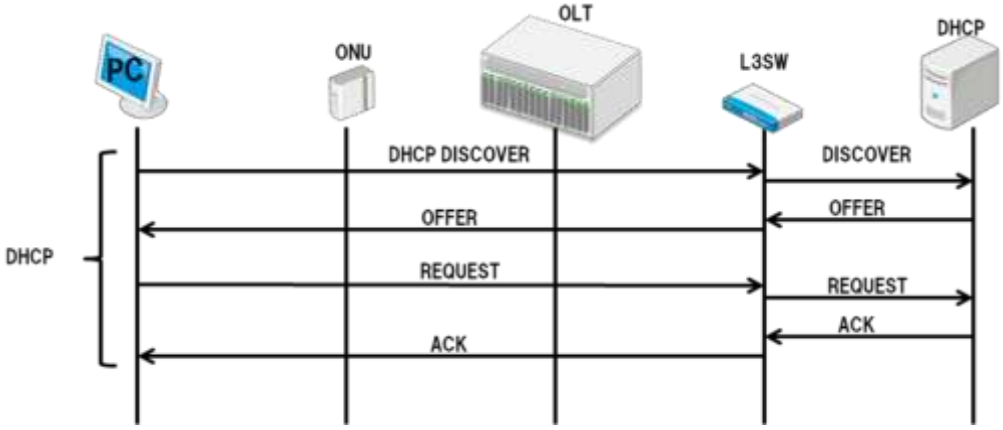


図6-5 IPv4構成時のCPEプロビジョニング例

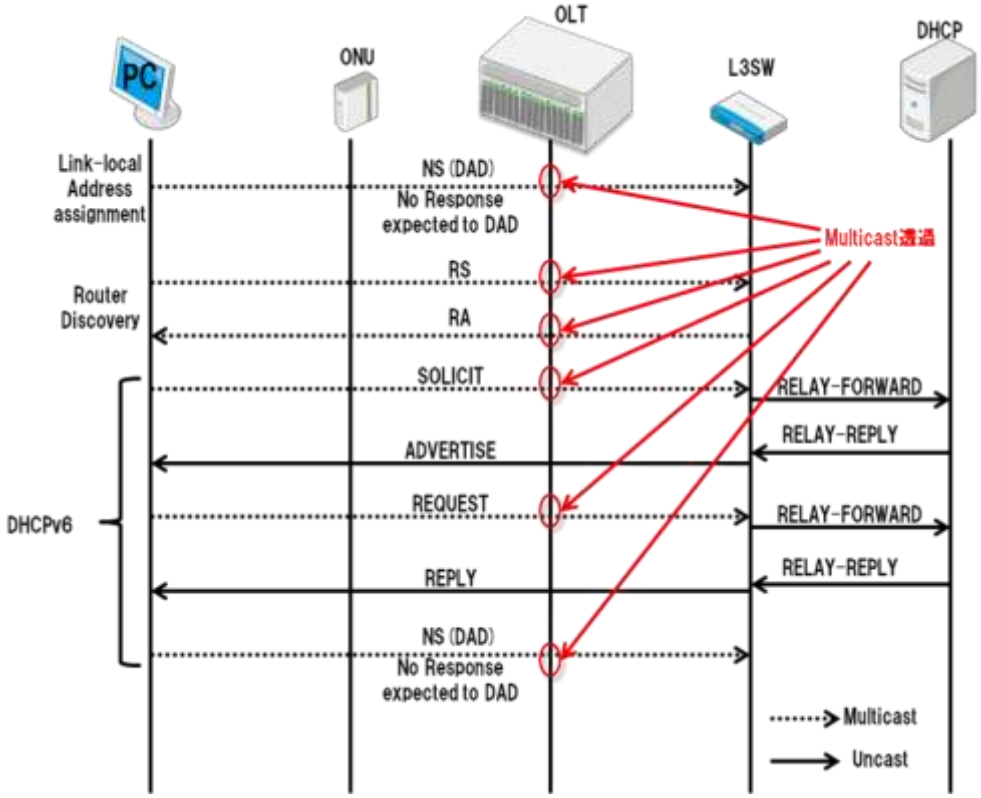


図6-6 IPv6構成時のCPEプロビジョニング例（DHCPv6利用時）

IPv4 構成時には CPE からの Broadcast を含めた DHCP パケットを透過できることを意識するのみでプロビジョニングを動作させることができる。一方、IPv6 構成時においてはその仕様上、IPv4 で利用していた Broadcast は Maluticast に置き換えられているため OLT あるいは ONU で当該 Maluticast を透過する事が必須となりフィルタ設定に注意が必要になる。CMTS は L3-SW と同等の機能を持つものもあり、CPE と CMTS の間で IPv6 のアドレス取得の処理を行うこともあるが、OLT には L3-SW の機能を持つものは少ないため、ネットワーク構成時には L3-SW を利用する事が重要となってくる。

6.2.4. DHCPv6-PD 利用時の注意点

DHCPv6-PD を用いて IPv6 の CPE プロビジョニングする場合、OLT のリレーエージェント機能では CPE から受信した DHCPv6 の Solicit を Relay-Forward で送信するため注意が必要となる。

まず IPv4 構成時にプロビジョニングをする場合、ユーザトレースのため DHCP Snooping 機能を利用することがある。これは SW 等のネットワークを構成する機器によって DHCP クライアントと DHCP サーバのやりとりを snooping し、そこで得られる DHCP クライアントの MAC アドレス、IP アドレス等からテーブルを構成することによりユーザトレースを実現するものである。このとき DHCP option82 を SW で有効にすると、その SW は自身の MAC アドレスやポート番号などを DHCP discover メッセージに付加するので DHCP サーバで SW の情報を確認できるようになり、更に高度なユーザトレースが可能となる。この機能は IPv4 構成時には一般的によく用いられる。また、IPv6 構成時においては SW 等の機器のリレーエージェント機能を有効にすることにより DHCP option18 が有効になり、IPv4 構成時と同様に機器の情報に基づいたユーザトレースが可能となる。しかし、このリレーエージェント機能を OLT で使用する場合は注意が必要である。具体例を挙げると、OLT の情報を利用して CPE のユーザトレースを行いたい場合、L3-SW ではなく OLT でリレーエージェント機能を利用する事が考えられる。しかし OLT によっては受信した DHCPv6 の Solicit を L3-SW には送信せず、OLT から Relay-Forward を送信するため、L3-SW で CPE への経路の自動ルート挿入機能が動作しなくなることがある。この場合 CPE プロビジョニングが完了しても L3-SW に CPE への経路が入らないため、上位から CPE への通信が出来なくなる。よって OLT でリレーエージェント機能を利用したときに CPE から受信した DHCPv6 の Solicit を Relay-Forward で送信する場合は実際の運用には使用出来ない。

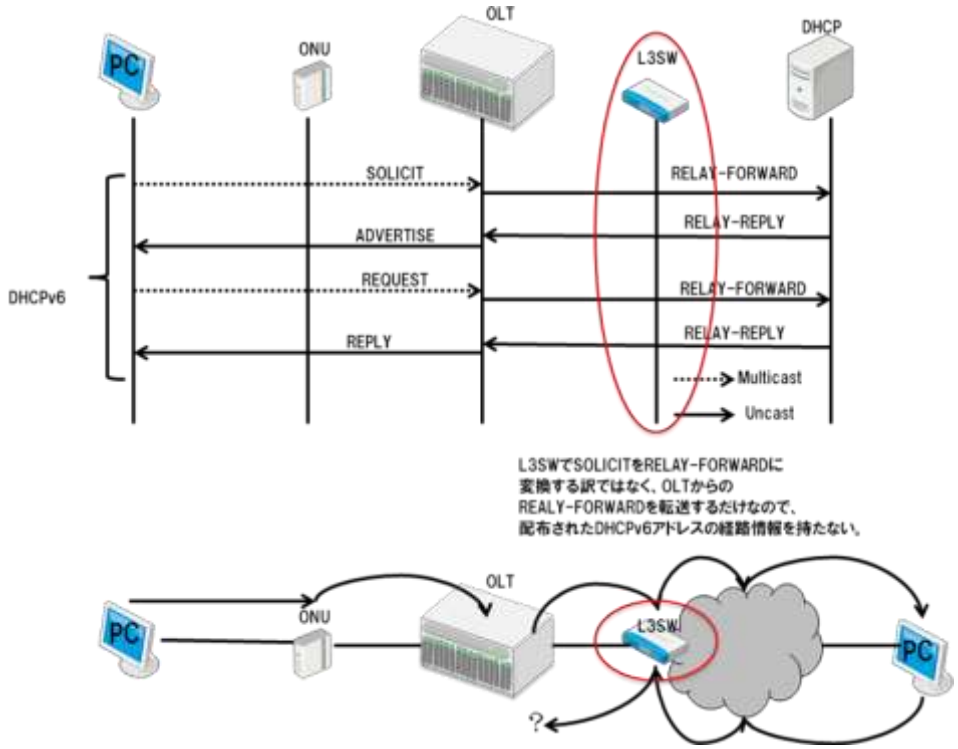


図6-7 IPv6構成時のOLTリレーエージェント設定時の注意点

このような OLT で DHCPv6-PD 機能を利用するには OLT だけでなく、その上位の L3-SW でも DHCPv6 の solicit や Relay-Forward を受けた時の挙動を十分に確認する必要がある。解決方法は OLT でリレーエージェント機能を使用せず OLT の IPv6 DHCP Snooping 機能か DHCPv6-PD Snooping 機能を有効にして OLT から送信される Syslog 等の利用でユーザトレースを行う方法もある。また、DHCPv6-PD 利用時に配布された経路を L3-SW から上位ネットワークにそのまま広報すると経路数が膨大になる可能性があるため、L3-SW で経路の Prefix をサマライズした上で上位ネットワークに広報することを考慮する必要がある。いずれにしても、使用する OLT、L3-SW の動きを十分に検証する必要がある。

6.2.5. FTTH ネットワークでの IPv6 対応のための検討

FTTH ネットワークを IPv6 対応させるためには GE-PON などの FTTH の装置だけでなく、上位のネットワークに関しても必要である。上述したように L3-SW 機能を持つ CMTS と異なり FTTH では L3-SW の IPv6 機能を上手く利用する事が重要なる。以下に検討項目について述べる。

(1) dual-stack 及び IPv6 トンネルの際に使用する L3-SW

L3-SW 機能がない OLT に代わり L3 での IPv4/v6 通信の制御や IPv6 の Router Discovery の応答ができる必要がある。上位ネットワークの L3 の終端になる場合は IPv6 リレー機能が必要となる。特に DHCP のリレーエージェント機能が必須でこのように L3-SW が IPv6 に対応していることが大前提となる。

(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 L3-SW の配下に DHCPv6 に対応したサーバの設置が必要である。

(3)GE-PON の dual-stack 対応

GE-PON 装置は通信を透過させる土管的なものと捉え、ストリームを透過させるだけの最低限の機能であっても dual-stack を実現する事は可能である。ONU 配下の PC の台数制限で IPv4 端末 n 台、IPv6 端末 m 台、といった制御をする場合、GE-PON で IPv4/v6 を区別して制御する機能が必要となる。また IPv6 の Multicast を透過させられることも必要である。

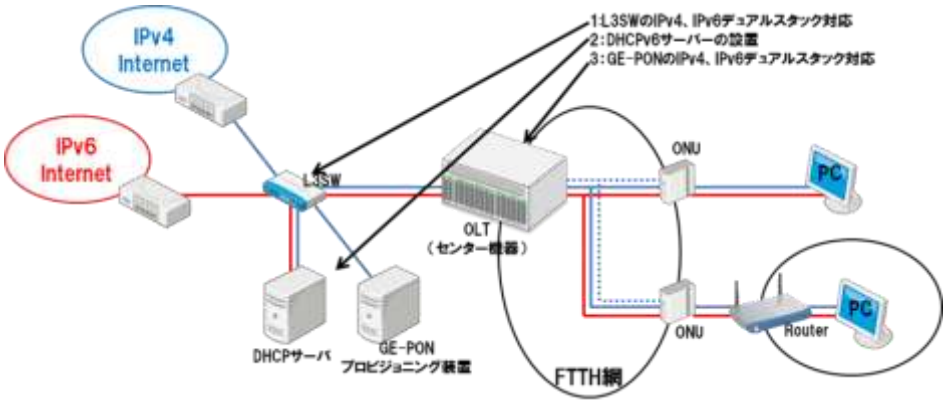


図6-8 dual-stack方式の設備構成時の注意点

6.2.6. FTTH ネットワークにおける CPE プロビジョニング使用時の注意点

CPE プロビジョニングにおいて IPv4、IPv6 に関わらず通信の制御において GE-PON と L3-SW の保持する情報にズレが発生し、これにより障害が発生する可能性があることに注意すべきである。例えば OLT において CPE の MAC アドレスを登録したテーブルによって通信を制御しているとする。このとき MAC テーブルに記憶している時間と L3-SW の ARP を記憶している時間が異なると MAC アドレスについて装置間で情報のズレが生じてしまい、通信ができなくなることがある。具体的には OLT で保持する時間が L3-SW で ARP を保持する時間より短い場合、OLT の MAC テーブルから消えた段階で ONU への通信ができなくなる。

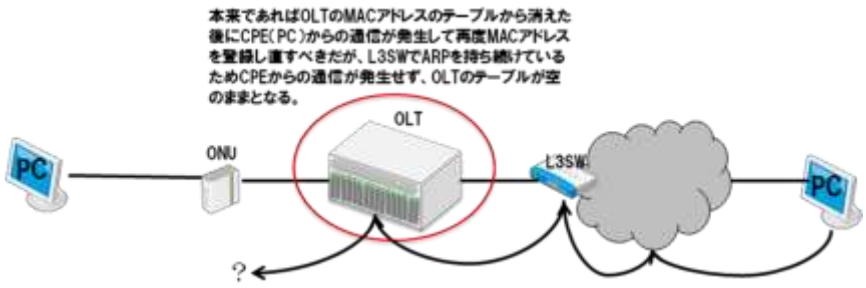


図6-9 プロビジョニング時の注意例

この場合の解決策は OLT の MAC テーブルに固定の情報として登録しておくか、一度登録した MAC アドレスを消さない設定にしておく方法が考えられる。また、CPE は加入者の所有物なので実際には不可能だが、可能であれば CPE から上位のネットワークのいずれかの端末に対して定期的に通信を行う事で OLT の MAC テーブルから消えないようにすることができる。このように FTTH ネットワークで OLT の MAC テーブルを使用して通信の管理を行う場合には、実際の環境で十分に検証する必要がある。

第 7 章 ケーブル Wi-Fi の IPv6 対応

7.1 概要

ケーブル Wi-Fi は、DOCSIS ネットワークや FTTH ネットワークと同様な新たなアクセスネットワークなので IPv6 対応が必要である。ケーブル Wi-Fi のサービス提供方法によっては設備構成が異なる。本書ではケーブル事業者自らが AP および APC を所有して IP アドレスを割り当てる図 7-1 のケースついて述べる。

DOCSIS CM などを内蔵した AP は、AP と APC との間に IPv4 を使用した L2 の論理トンネルを形成して DOCSIS の MAX-CPE に抵触しない方式が一般的である。これは第 3 章に記載した IPv6 アドレス割り当て方式の中の「ケース 2 ：IPv4 トンネル」相当である。したがって、AP と APC 間は IPv6 対応である必要性はないが次のような注意点がある。それは、加入者 Wi-Fi 端末の L3 終端は APC ではなく上位の L3 装置であることが多いが、上述したように AP と APC 間は「L2 の論理トンネル」ということである。この点でケーブル Wi-Fi は FTTH ネットワークと同様の特徴を持つと言える。

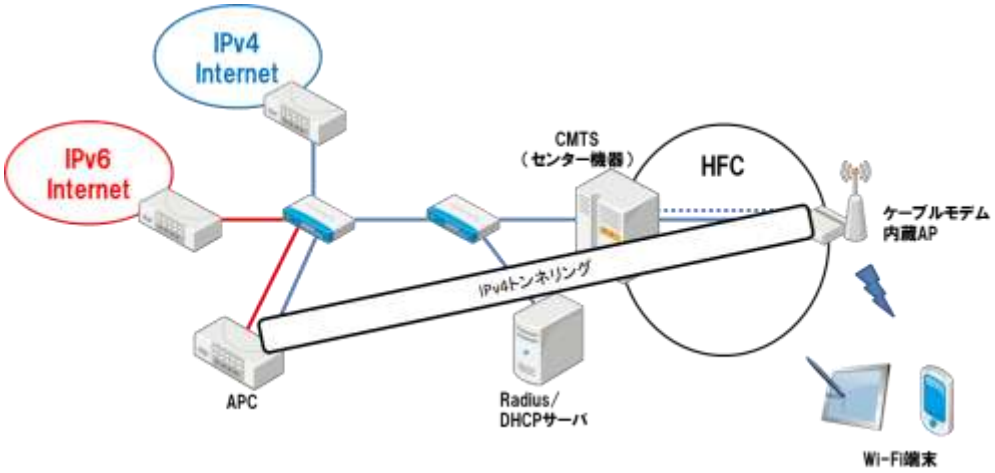


図 7-1 ケーブル Wi-Fi の設備構成例

7.2 サービス仕様

加入者 Wi-Fi 端末への IPv6 アドレスの割り当て方法については、「第 5 章 DOCSIS ネットワーク」及び「第 6 章 FTTH ネットワーク」と同様のため割愛する。

加入者 Wi-Fi 端末が dual-stack の場合、仕様によっては IPv6 を優先して使用する場合があるが、Web サーバや認証用サーバ等の関連機器が dual-stack でない場合、フォールバックなどの不具合が発生する可能性が考えられる。

したがって、ケーブル Wi-Fi を dual-stack 化する際は、加入者 Wi-Fi 端末のインターネット接続性だけでなく、IPv4/v6 のユーザトレーサビリティについても十分考慮し、機器仕様を確認した上で認証用サーバ等の dual-stack 化について検討する必要がある。

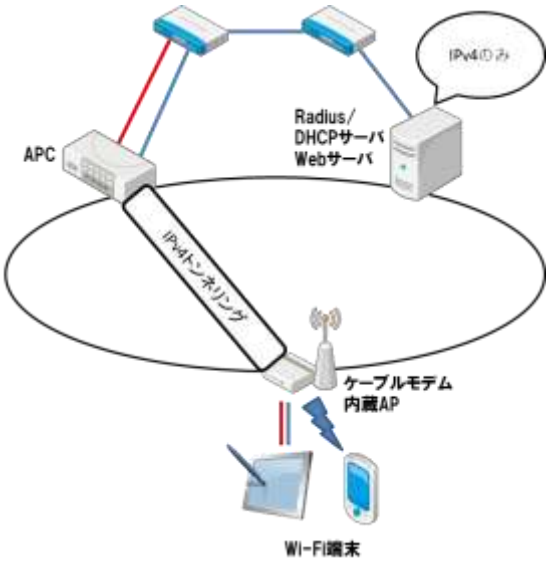


図 7-2　ケーブル Wi-Fi の dual-stack に関する課題

なお、セキュリティフィルタに関しては、DOCSIS ネットワークならびに FTTH ネットワークと同様とするのが基本であるが、ケーブル Wi-Fi の性質上、加入者端末は「常時接続ではなく、一時的な接続」、「PC よりも、スマートフォン／タブレットが中心」となることが一般的なので、セキュリティフィルタについては実利用も考慮した構成とすることが望ましい。

第 8 章 CPE の接続形態

8.1 DOCSIS システムのインターネットサービスでの CPE の接続形態

8.1.1. 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/v6 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 8-1 にまとめた。

表 8-1 CPE 接続形態と運用について

接続形態	端末 1 台接続	複数端末接続	ルータ接続型	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 BB ルータ 1 台接続。 BB ルータ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 BB ルータを接続することもある。	DHCPv6-PD クライアントを実装するルータのみを接続。	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 BB ルータでフィルタ、CM に流れない動きを想定。 IPv6 はパススルーにより CPE から直接 CM に到達。 IPv6 接続の場合は MAC 数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。 BB ルータ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	BB ルータの WAN-IF に 1 つ付与。 CPE は BB ルータの NAT 機能で複数 CPE を接続できる。	PC もしくは BB ルータの WAN-IF に 1 つずつ付与。 BB ルータ配下の 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。	

IPv6	CPE は HUB を介して CM に接続。 CPE への IPv6 アドレス付与は DHCPv6。 接続可能 CPE 数は付与する Global IPv6 アドレス数もしくは BB ルータの WAN 側 MAC も含めた MAC アドレス数で設定する。	ルータの LAN-IF に/64 以上の Prefix を付与する。 WAN-IF では Link Local か Global を付与するかルータの実装によるが SLAAC は利用しない。

※上表での BB ルータとは IPv4 は NAT し、IPv6 はブリッジでパススルーするものを指し、ルータとは IPv4 は NAT し、IPv6 は DHCPv6-PD をサポートして LAN 側のセグメントと WAN 側のセグメントを L3 でルーティングするものを指す。

8.1.2. 端末 1 台接続

(1) BB ルータ接続型の概要

PC を 1 台のみ接続するか、もしくは BB ルータ 1 台を接続する。BB ルータ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 BB ルータを利用するか 1 台の CPE を接続するか管理しない。

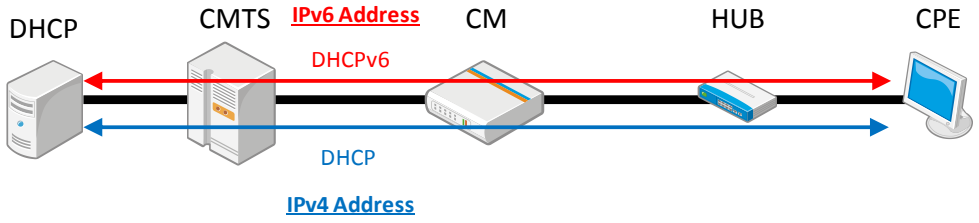


図 8-1 端末 1 台接続型

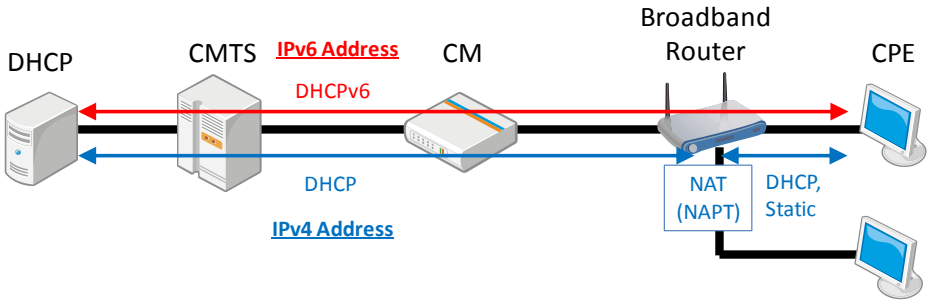


図 8-2 端末 1 台接続（BB ルータを接続した場合）

(2) IPv4 アドレス割り当て方法

PC もしくは BB ルータの WAN インタフェイスへの 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 Stateful 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。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 に割り当てる等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 などの 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。dual-stack において CPE 数を制限する場合も IPv4/v6 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 BB ルータを利用しており、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 BB ルータ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言える。

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 BB ルータ 1 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 BB ルータをスルーして IPv6 通信を行うことができる CPE 数を制限する。

尚、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言える。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。

8.1.3 複数端末接続

(1) 複数端末接続の概要

HUB を介して複数台の PC を接続する。PC の代わりに BB ルータ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 BB ルータを利用するかは事業者としては管理しない。

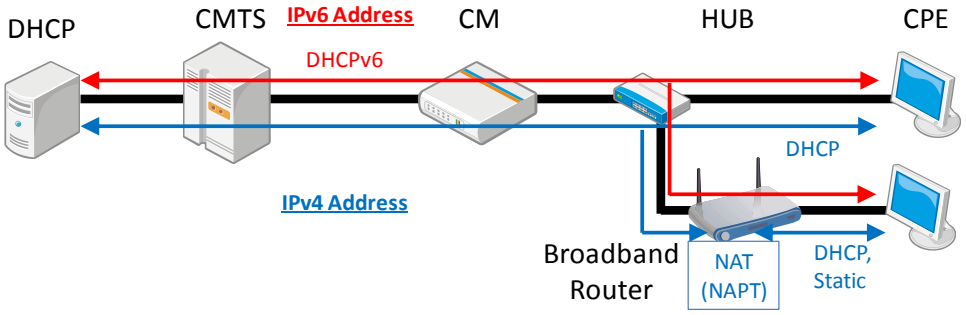


図 8-3 複数端末接続

(2) IPv4 アドレス割り当て方法

PC もしくは BB ルータの WAN インタフェイスへの 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 Stateful 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 Stateful 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 を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、例えば特定の Prefix に属するアドレスを CPE に割り当てる等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等で可能である。

(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。dual-stack において CPE 数を制限する場合も IPv4/v6 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 BB ルータを利用しており、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 BB ルータ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 BB ルータを考慮した 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言える。

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

但し m≦n

ここでは CM に直接 CPE が m 台接続され、その内には BB ルータ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 BB ルータをスルーして IPv6 通信を行うことができる CPE 数を制限する。BB ルータの接続を考慮しなければ m=n で良いが IPv6 をブリッジする BB ルータ配下の 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、可能であれば n は CMTS でサポートできる最大数に設定するのが望ましい。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。

8.1.4　ルータ接続型

(1)　ルータ接続型の概要

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。

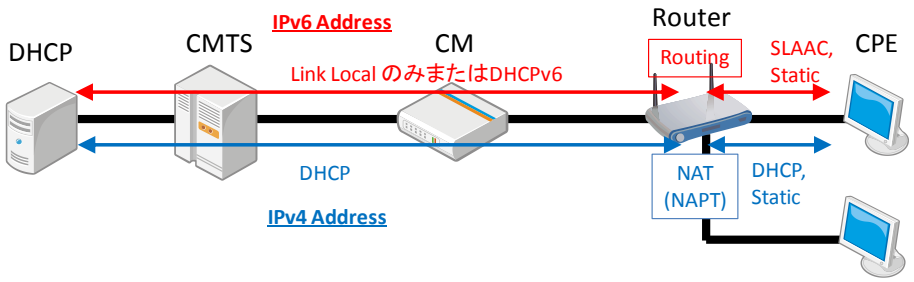


図 8-4 ルータ接続型

(2)　IPv4 アドレス割り当て方法

ルータの WAN インタフェイスへの 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 DHCP は用いない。

(3)　IPv6 アドレス割り当て方法

ルータの LAN インタフェイ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 LAN インタフェイスからの 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。ルータの WAN 側インタフェイスは 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 CM に接続された CPE が SLAAC でアドレスを生成しないようルータにおいても SLAAC を利用することは望ましくなく、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 RFC6106 で規定されている。ルータの 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。

ルータが 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、ルータが接続される 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、例えば固定の Prefix を割り当てる等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。ルータ接続型においては加入者毎に Prefix を DHCPv6 サーバから割り当てるので、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 のアドレスまでを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

接続される端末はルータに限られるため 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 アドレスはルータの WAN インタフェイスへ付与されるアドレスに限られ、複数 CPE においてはルータ LAN 側の Private アドレス領域を用いる。IPv6 は割り当てられた Prefix の内のアドレスをルータ 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、ルータの WAN インタフェイスへの 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 でルータへの 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が、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ルータ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 の範囲を設定する。

(b) DHCPv6 サーバに Relay Address Option を用いる等の方法で 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 にルーティングする Static Route を設定する。

(d) 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、ルータへのルートが確保されるようにする。

※具体的な CMTS での設定例は Appendix I にて解説する。

(7) 割り当てサイズ

1 台のルータに DHCPv6-PD で割り当てる Prefix 長は DHCPv6 サーバ側で設定される。ルータの LAN 側には/64 の Prefix を生成する。DHCPv6 サーバでの Prefix では/64～/56 を割り当てる。

8.1.5 eRouter タイプの CM を用いる場合

eRouter と 8.1.4 項で記載したルータは同等なので運用の指針についても 8.1.4 項と同じ。

8.2 FTTH システムのインターネットサービスでの CPE の接続形態

8.2.1. 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/v6 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 8-5 にまとめた。

表 8-5 CPE 接続形態と運用について

接続形態	端末 1 台接続	複数端末接続	ルータ接続型
接続対象端末 接続許可台数	PC を 1 台のみ接続するか BB ルータ 1 台接続。 BB ルータ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 BB ルータを接続することもある。	DHCPv6-PD クライアントを実装するルータのみを接続。
MAC	IPv4 のみサービスでは IPv6 は BB ルータでフィルタ、ONU に流れない動きを想定。 IPv6 はパススルーにより CPE から ONU に到達。IPv6 接続の場合は MAC 数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 又は ONU で接続許可台数を設定。 BB ルータ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 は 1。
IPv4	BB ルータの WAN-IF に 1 つ付与。 CPE は BB ルータの NAT 機能で複数 CPE を接続できる。	PC もしくは BB ルータの WAN-IF に 1 つずつ付与。 BB ルータ配下の 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 BB ルータの 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 BB ルータの WAN 側 MAC も含めた MAC アドレス数で設定する。	ルータの LAN-IF に /64 以上の Prefix を付与。 WAN-IF では Link Local のみか Global を付与するかはルータの実装によるが SLAAC は利用しない。

※上表での BB ルータとは IPv4 は NAT し、IPv6 はブリッジでパススルーするものを指し、

ルータとは IPv4 は NAT し、IPv6 はそのルータの LAN 側のセグメントと WAN 側のセグメントを L3 で Static ルーティングするものを指す。

8.2.2. 端末 1 台接続

(1) BB ルータ接続型の概要

PC を 1 台のみ接続するか、もしくは BB ルータ 1 台を接続する。BB ルータ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 BB ルータを利用するか 1 台の CPE を接続するかは管理しない。

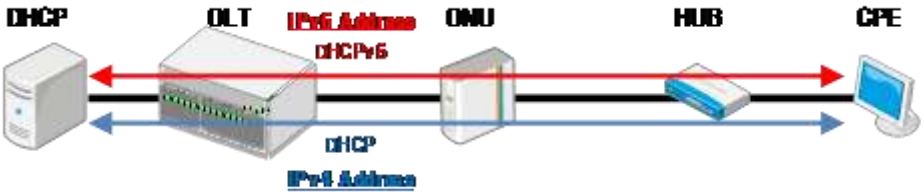


図 8-6 端末 1 台接続型

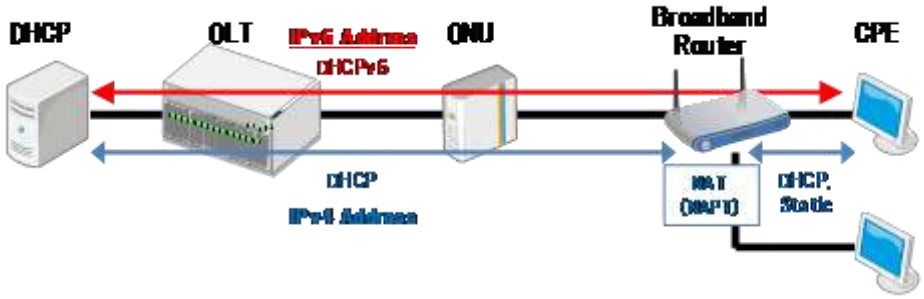


図 8-7 端末 1 台接続（BB ルータを接続した場合）

(2) IPv4 アドレス割り当て方法

PC もしくは BB ルータの WAN インタフェイスへの 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

PC への IPv6 アドレス割り当ては Stateful 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。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。

(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。dual-Stack において CPE 数を制限する場合も IPv4/v6 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 BB ルータを利用しており、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 BB ルータ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。

8.2.3. 複数端末接続

(1) 複数端末接続の概要

HUB を介して複数台の PC を接続する。PC の代わりに BB ルータ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 BB ルータを利用するかは事業者として管理しない。

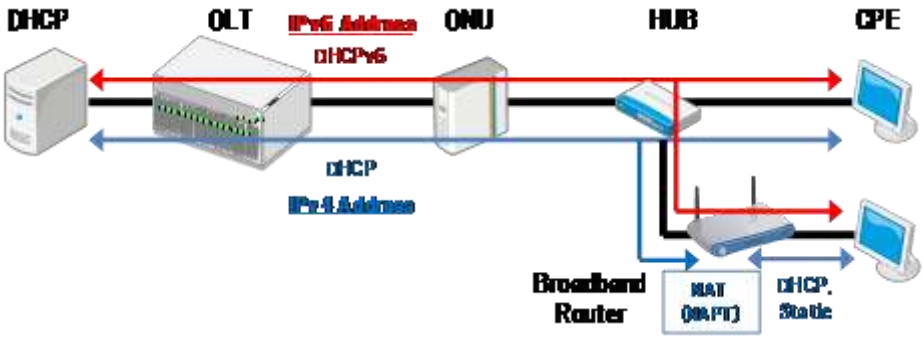


図 8-8 複数端末接続

(2) IPv4 アドレス割り当て方法

PC もしくは BB ルータの WAN インタフェイスへの 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

PC への IPv6 アドレス割り当ては Stateful DHCPv6 にて、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 を含める。CPE の OS においては Stateful 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 利用を検討すべきである。

(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

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。dual-Stack において CPE 数を制限する場合も IPv4/v6 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 BB ルータを利用しており、このうち IPv4 は NAT(NAPT)で IPv6 はブリッジするタイプがあるた。ブリッジ型接続でもその仕様の BB ルータ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。

8.2.4. ルータ接続型

(1) ルータ接続型の概要

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。

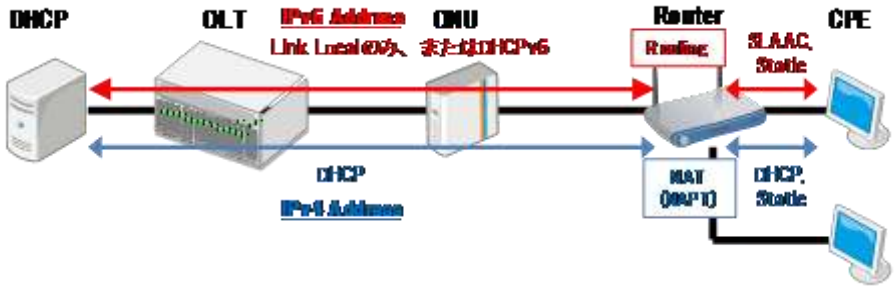


図 8-9 ルータ接続型

(2) IPv4 アドレス割り当て方法

ルータの WAN インタフェイスへの 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 DHCP は用いない。

(3) IPv6 アドレス割り当て方法

ルータの LAN インタフェイ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 インタフェイスからの 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。ルータの WAN 側インタフェイスは 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ルータにおいても SLAAC を利用することは望ましくなく、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 RFC6106 で規定されている。ルータの 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。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

接続される端末はルータに限られるため 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 アドレスはルータの WAN インタフェイスへ付与されるアドレスに限られ、複数 CPE においてはルータ LAN 側の Private アドレス領域を用いる。IPv6 は割り当てられた Prefix の内のアドレスをルータ 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 でルータへの Prefix が割り当てられた際、どのルータ配下にあるかは 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 の領域を上位ルータに 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 台のルータに DHCPv6-PDn で割り当てる Prefix 長は DHCPv6 サーバ側で設定される。ルータの LAN 側には/64 の Prefix を生成する。DHCPv6 サーバでは/64～/56 の Prefix を割り当てる。

第 9 章 運用・マネージメントについて

9.1 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,etc)
(4) OP25B(Outbound Port 25 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。

(5) 不正 RA(Router Advertisement) 対策
(6) 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。

(7) ICMPv6
(8) IPv6 の Multicast

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。

9.1.1. 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てメーカまたはベンダに確認することが必要である。

9.1.2. CM によるパケットフィルタ

CM で IPv6 のパケットフィルタする方法は以下のとおり。

(1) IP Filtering(docDevFilterEntry)
(2) Subscriber Management Filter(TLV37)
(3) Upstream Drop Classifier(TLV60)

dual-stack においては個別のトラフィ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。

9.1.3. FTTH におけるパケットフィルタ

FTTH は GE-PON が用いられることが多い。GE-PON の OLT では CMTS とは異なり L3-SW 機能を持つものが少ないため、ONU や OLT と OLT の上位に接続する L3-SW を組み合わせてフィルタを適用することになるが、実装は GE-PON メーカの機器仕様に依存する。導入時には上述したフィルタ要件（不正 RA 対策、不正 DHCPv6 対策、Windows 共有対策、ウイルス対策、OP25B）を整理し、設定方法を含め OLT および L3-SW のメーカまたはベンダへの確認が必要である。

9.1.4. 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。（次頁図 9-1 参照）

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。

	受信側(Ingress)	送信側(Egress)
必須	[1] Neighbor Discovery、Path MTU Discovery などの為に、全てのICMPv6 を accept する。 [2] 以下の Special-Use Prefix が Source アドレスになっている packet は reject する。 - 予約済みアドレス: ::/8,fec0::/10 - ユニークローカルアドレス: fc00::/7 - マルチキャストアドレス: ff00::/8 - ドキュメントアドレス:2001:db8::/32 [3] 自 AS で持っている Prefix が Source アドレスになっている packet を reject する。 ※顧客の場合トランジット接続でのみ必要。	特になし
オプション	[1] 境界インタフェイス宛となっているICMPv6 パケットの制限をする、 - 前提条件： 1. Neighbor Discovery で使われる ICMPv6 TYPE は accept する。 2. Path MTU Discovery で使われる ICMPv6 TYPE=2(Packet Too Big)は accept する。 3. 速やかな IPv6/IPv4 フォールバックの為に、ICMPv6 TYPE =1(Destination Unreachable)は accept する。 [2] 境界インタフェイス宛となっている上記以外の ICMPv6 を reject する。 ※ traceroute の確認ができなくなる。	[1] Neighbor Discovery、Path MTU Discovery などの為に、全てのICMP v6 を accept する。 [2] 以下の Special-Use Prefix が Source アドレスになっている packet を reject する。 - 予約済みアドレス: ::/8,fec0::/10 - ユニークローカルアドレス: fc00::/7 - マルチキャストアドレス: ff00::/8 - ドキュメントアドレス ：2001:db8::/32

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

図 9-1 xSP のルータにおいて設定を推奨するフィルタの項目について(IPv6 版)

9.2 マネージメントおよび監視

9.2.1. ユーザプロビジョニング

(1) プロビジョニングサーバ

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を委ねられるが、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。

(2)CM での CPE の台数制限

IPv4 では CM に接続される CPE 台数は CM の config file の MAX CPE で制御がされることが多い。dual-stack においても CPE 台数を MAC アドレスベースに制限する場合は、MAX CPE で MAC アドレス数を制限することも可能ではあるが、IPv4 と IPv6 アドレス数を区別して制御することが望ましい。IPv4 と IPv6 アドレス数制御方法を下表に示す。

表 9-2 IPv4/v6 アドレス数制限方法

サービス	設定数	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 docsDevCpeIpMax を設定
IPv6 アドレス許可数	n	CM Config File で TLV 18 = n を設定

MAX CPE のサポート状況はケーブルモデムシステムのバージョンなどにより異なる場合があるため、導入時にはメーカまたはベンダに確認することが必要である。

また、DOCS-CABLE-DEVICE-MIB(RFC4639)内の docsDevCpeIpMax の実装についてはベンダに委ねられているため docsDevCpeIpMax で設定を行う場合は CM メーカおよびベンダに実装状況を確認することが必要である。

(3) FTTH での CPE の台数制限

FTTH でも ONU に接続される CPE の台数は MAC アドレスをベースに制御することが多い。dual-stack でも同様に MAC アドレスをベースに制御することになるが、 CM での CPE 台数制限と同様に IPv4 および IPv6 アドレスそれぞれを区別し制限することが想定される。IPv4 および IPv6 アドレスそれぞれを制御する実装はメーカの機器仕様に依存するため、設定方法について GE-PON メーカまたはベンダに確認することが必要である。

9.2.2. ユーザトレーサビリティ

前述の通り abuse への対応を行う場合、IPv6 アドレスとその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り、IPv4 アドレスと同様にユーザトレーサビリティを確保する必要がある。したがって、ケーブル事業者では PC への IPv6 アドレス割り当てには SLAAC により 設定するのではなく、Stateful な割り当てができる DHCPv6 を使用し、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必要となる。

また、同一リンク内であれば IPv6 Link local Address での通信も可能となるがこれらの通信はその利用者の特定が困難であることから許可しないことが望ましい。

9.3 監視

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既に 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。CMTS 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。

Appendix I 技術情報（CMTS 設定）

Appendix I - I　C4 CMTS CLI 設定例

図 A-1 に示すネットワーク構成図を実現する C4 CMTS での CLI 設定を以下に示す。

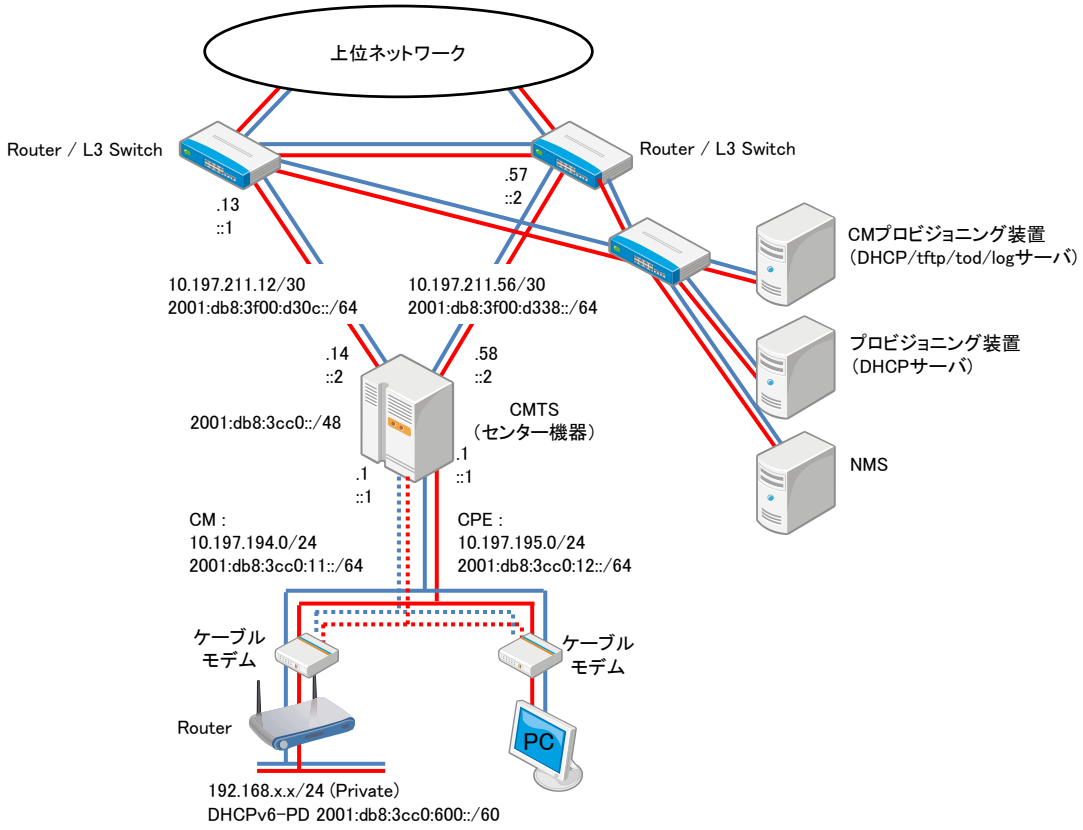


図 A-1 基本ネットワーク構成図

(1) Gigabit Interface

上位ルータに接続される RCM の Gigabit Ethernet Interface に IPv6 アドレスを割り当てる。Link Local アドレスはデフォルトでは EUI64 形式のアドレスが自動で割り当てられるが、後述する OSPFv3 では Next Hop に Link Local Address が使用されルートテーブルを見た際に EUI64 形式のアドレスでは Next Hop が判別しにくいため Global Address に基づきなんらかの規則で固定で Link Local Address を割り当てることを推奨する。また Gigabit Ethernet Interface では RA を出す必要は無いため ipv6 nd ra suppress コマンドで RA を抑制する。

```
configure interface gigabitEthernet 17/3 no shutdown
configure interface gigabitEthernet 17/3.0 ip address 10.197.211.14 255.255.255.252
configure interface gigabitEthernet 17/3.0 ipv6 enable
configure interface gigabitEthernet 17/3.0 ipv6 address fe80::d30c:2/64    link-local
configure interface gigabitEthernet 17/3.0 ipv6 address 2001:db8:3f00:d30c::2/64
configure interface gigabitEthernet 17/3.0 ipv6 nd ra suppress
configure interface gigabitEthernet 18/3 no shutdown
configure interface gigabitEthernet 18/3.0 ip address 10.197.211.58 255.255.255.252
configure interface gigabitEthernet 18/3.0 ipv6 enable
configure interface gigabitEthernet 18/3.0 ipv6 address fe80::d338:2/64    link-local
configure interface gigabitEthernet 18/3.0 ipv6 address 2001:db8:3f00:d338::2/64
configure interface gigabitEthernet 18/3.0 ipv6 nd ra suppress
```

(2) Loopback Interface

Loopback Interface も IPv4 と IPv6 の両方を設定する。

```
configure interface loopback 0 ip address 10.197.213.192 255.255.255.255
configure interface loopback 0 ipv6 enable
configure interface loopback 0 no shutdown
configure interface loopback 0 ipv6 address 2001:db8:3f00:d500::c0/128
```

(3) Cable Interface

IPv4 設定部分は従来と同様。

```
configure interface cable-mac 1.0 ip address 10.197.194.1 255.255.255.192
configure interface cable-mac 1.0 ip address 10.197.195.1 255.255.255.192 secondary dhcp-giaddr
configure interface cable-mac 1.0 cable helper-address 10.197.210.33    cable-modem
configure interface cable-mac 1.0 cable helper-address 10.197.210.35    host
configure interface cable-mac 1.0 cable dhcp-giaddr policy
```

IPv6 設定では Gigabit Ethernet Interface と同様に Link Local Address と Global Unicast Address を割り当てる。Global Unicast Address は CM 用 Prefix (CM を IPv6 で Provisioning する場合)のものと CPE Prefix のものと最低限２つが必要である。Global Unicast Address の割り当て設定の後ろには dhcp-link-address オプションを付けることが可能で、これは CM もしくは CPE が DHCPv6 Solicit を投げた際に C4 がリレーする Relay Forward メッセージに含める Link Address を CM からの Solicit と CPE からの Solicit で使い分けに用いられる。これは IPv4 の DHCP のリレーの際の giaddr を policy 設定で CM では Primary Address、CPE は Secondary Address と使い分けることと同じ働きをするものである。これにより DHCPv6

Server では Shared Network もしくは Link の Bundle を用いなくても Solicit の Link Address をもって設定された Scope からアドレスを払いだすことが可能となる。dhcp-link-address オプションを用いない場合は CM、CPE とも Solicit に含まれる Link Address は設定された Global Unicast Address のうち最も若い番号のアドレスとなる。
Cable Interface では DHCPv6 サーバを dhcp relay destination コマンドで設定する。IPv4 での DHCP Server を CM と CPE で別にするように DHCPv6 でも dhcp relay destination コマンドの後ろに cable-modem オプション、host オプションをつけサーバを使い分けることが可能である。dhcp relay destination を複数設定した場合はその両方のアドレスに向けて Relay Forward を出す動きになる。
nd managed-config-flag, nd other-config-flag は CPE が DHCPv6 でアドレスを取得するために RA に M-Flag、O-Flag を設定するためのコマンドでデフォルトで ON となっている。
nd ra interval コマンドで RA の最大、最小送信間隔を設定する。デフォルトは 600, 200 となっている。Cable Interface では CM、CPE が RA によってデフォルトルートを得るため、RA を抑制してはいけない。

```
configure interface cable-mac 1.0 ipv6 enable
configure interface cable-mac 1.0 ipv6 address fe80::1:1/64    link-local
configure interface cable-mac 1.0 ipv6 address 2001:db8:3cc0:11::1/64    dhcp-link-address cable-modem
configure interface cable-mac 1.0 ipv6 nd prefix 2001:db8:3cc0:11::/64 off-link
configure interface cable-mac 1.0 ipv6 address 2001:db8:3cc0:12::1/64    dhcp-link-address host
configure interface cable-mac 1.0 ipv6 nd prefix 2001:db8:3cc0:12::/64 off-link
configure interface cable-mac 1.0 ipv6 dhcp relay destination 2001:db8:3f00:d200::33 cable-modem
configure interface cable-mac 1.0 ipv6 dhcp relay destination 2001:db8:3f00:d200::35 host
configure interface cable-mac 1.0 ipv6 nd managed-config-flag
configure interface cable-mac 1.0 ipv6 nd other-config-flag
configure interface cable-mac 1.0 ipv6 nd ra interval 600 200
configure interface cable-mac 1.0 ipv6 no nd ra suppress
```

デフォルトの設定では Cable Interface で発生される RA には Prefix 情報は含まれない。この場合 CPE は Prefix 長を取得できず DHCP で取得したアドレスは/128 になってしまうため、Prefix 長を/64 で指定する設定 ipv6 nd prefix を入れる。この際、autoconfig オプションを入れないことで CPE が SLAAC でアドレスを自動生成するのを抑制できる。
本ガイドラインでは CMTS の Cable Interface の RA から CPE が直接 SLAAC でアドレスを生成する方法は推奨していないが、CMTS の設定として SLAAC でのアドレス生成を有効にするには以下の設定を追加する。DHCPv6 用いる Prefix と SLAAC でアドレスを生成させる Prefix を分けるためには Cable Interface に３番目の Global Unicast Address の設定を行ない、その３番目の Prefix を nd prefix コマンドで指定する方法をとる。ipv6 nd prefix コマンドで autoconfig

オプションを入れ、RA での Autoconfig Flag を立てる。これにより CPE はここで設定された Prefix においてアドレスを自動生成する。この場合、Windows 7 のような DHCPv6 Client が実装されている OS の場合、DHCPv6 で取得したアドレスに加えて SLAAC でのアドレスも持つことになる。

```
configure interface cable-mac 1.0 ipv6 address 2001:fa0:3cc0:11::1/64    dhcp-link-address cable-modem
configure interface cable-mac 1.0 ipv6 address 2001:fa0:3cc0:12::1/64    dhcp-link-address host
configure interface cable-mac 1.0 ipv6 address 2001:fa0:3cc0:13::1/64
configure interface cable-mac 1.0 ipv6 nd prefix 2001:fa0:3cc0:13::/64 off-link autoconfig
```

(4) OSPFv3

IPv4 OSPF の設定は従来通り。

```
configure router ospf vrf default router-id 10.197.213.192
configure router ospf vrf default no shutdown
configure router ospf vrf default network 10.197.211.12 0.0.0.3 area 0.0.0.0
configure router ospf vrf default network 10.197.211.56 0.0.0.3 area 0.0.0.0
configure router ospf vrf default redistribute connected metric 1
configure interface gigabitEthernet 17/3.0 ip ospf network point-to-point
configure interface gigabitEthernet 18/3.0 ip ospf network point-to-point
```

OSPFv3 の基本設定は以下の内容となる。Neighbor との接続形態は C4 CMTS では Point-to-Point および Broadcast がサポートされている。

```
configure ipv6 pd-route-injection
configure ipv6 router ospf router-id 10.197.213.192
configure ipv6 router ospf no shutdown
configure ipv6 router ospf redistribute connected metric 1
configure interface gigabitEthernet 17/3.0 ipv6 ospf network point-to-point
configure interface gigabitEthernet 17/3.0 ipv6 ospf area 0.0.0.0
configure interface gigabitEthernet 18/3.0 ipv6 ospf network point-to-point
configure interface gigabitEthernet 18/3.0 ipv6 ospf area 0.0.0.0
```

redistribute connected で Cable Interface の Prefix を広報する。
ipv6 pd-route-injection によっておよび redistribute pd で DHCPv6 Prefix Delegation で CM の先のルータに割り当てた Prefix に対するルートを C4 が生成する。
ここで、さらに以下の redistribute pd を用いると、PD Route Injection で生成したルートを OSPFv3 で広報する。

```
configure ipv6 router ospf redistribute pd metric 1
```

しかしながら、複数の Prefix Delegation によるルートテーブルが生成された場合、C4 は個々のルートをサマリせず、個別に広報する。よって仮に 1000 の Prefix Delegation によるルートが生成されると 1000 の Entry を広報し、上位ルータでのルートテーブルに負担を与えることが考えられる。
よって、アリスでは redistribute pd を用いず、以下の方法であらかじめ Prefix Delegation でその C4 CMTS に割り当てる範囲の Prefix を Static で広報する方法を推奨している。
まず、DHCPv6 サーバの設定から該当する C4 の先のルータに割り当てられる Prefix のレンジを確認する。

```
ISC dhcpd の例
# Prefix range for delegation to sub-routers
prefix6 2001:fa0:3cc0:1000:: 2001:fa0:3cc0:1fff:: /64;
#  これで 2001:fa0:3cc0:1000::/52 がそのレンジとなる。
```

Null Interface を C4 に設定し、DHCPv6 サーバに設定された Prefix へのルートを Null Interface へ割り当てる。さらに redistrobute static でこのルートを OSPFv3 で広報する。

```
configure interface null 0
configure interface null 0 ip unreachables
configure interface null 0 ipv6 icmp unreachables
configure ipv6 route 2001:fa0:3cc0:1000/52 null 0
configure ipv6 router ospf redistribute static
```

上記の設定により、PD Route は上位のルータへは 1 Entry のみ広報され、上位ルータから見て、この例では 2001:db0:3cc0:1000/52 のルートはその C4 宛になる。その Prefix 中のホスト宛のパケットは Prefix Delegation で実際にルートが生成されていない場合には Null で破棄される。PD Route Injection で C4 がルートを生成している場合には、当該のルータへ送らる。

(5) Filtering (Network Side ACL)
C4 CMTS では IPv6 に対する Network Side ACL としては Source Address のみを規定してフィルタリングする標準 ACL のみがサポートされる。

```
configure ipv6 access-list ACL1    deny    2001:fa0:3f00:24::/64
```

(6) Filtering (Subscriber Management Filter)
Subscriber Management Filter は Port 番号でフィルタリングするルールでは IP Version の指

定ができるように拡張され、ip-version = IPv4, IPv6, Unknown が指定できる。Unknown を指定すると IPv4、IPv6 の両方に同一の Port によるフィルタルールが適用される。
アドレスでフィルタリングをかける方法において IPv6 Source Address/Prefix、IPv6 Destination Address/Prefix の指定できるようになっている。

```
C4 # configure cable filter group 3 index 1 ?
  dest-ip                    - IP destination address
  dest-mask                  - IP source address mask
  dest-port                  - UDP destination port
  ip-proto                   - IP protocol
  ip-tos                     - IP TOS byte settings
  ip-version                 - IP version of the filter entry (ipv4, ipv6 or unknown)
  log                        - Capture a packet that matches the filter
  match-action               - Filter Match action processing
  src-ip                     - IP source address
  src-mask                   - IP source address mask
  src-port                   - UDP source port
  v6-dest-address            - IPv6 destination address
  v6-dest-pfxlen             - IPv6 destination address prefix length
  v6-flow-label              - IPv6 flow label
  v6-src-address             - IPv6 source address
  v6-src-pfxlen              - IPv6 source address prefix length
```

フィルタのかけ方は一連のフィルタリングルールを設定した Cable Filter Group を設定し、CM Config File の TLV37 による指定が無い CM 全てに適用される Default Filter Group として割り当てるか、CM Config File の TLV37 で Filter Group 番号を指定し CM 個々のフィルタルールを適用する。以下に Windows のファイル共有フィルタの一部として下り、上りとも Dst Port 135、TCP+UDP をフィルタする設定を示す。

Default Filter Group を設定する場合には以下のコマンドで Default Filter Group を Active にする。

```
configure cable submgmt default active
```

さらに Default で使用する Filter Group ID を下り、上りで選択する。

```
configure cable submgmt default filter-group host downstream 1
configure cable submgmt default filter-group host upstream 2
```

フィルタリングルール自身は以下の configure cable filter group コマンドで設定する。

```
onfigure cable filter group 1 index 1 ip-version unknown
configure cable filter group 1 index 1 src-port 0
configure cable filter group 1 index 1 dest-port 135
configure cable filter group 1 index 1 ip-proto 257
configure cable filter group 1 index 1 match-action drop
configure cable filter group 1 index 1 ip-tos 0x0 0x0
configure cable filter group 2 index 1 ip-version unknown
configure cable filter group 2 index 1 src-port 0
configure cable filter group 2 index 1 dest-port 135
configure cable filter group 2 index 1 ip-proto 257
configure cable filter group 2 index 1 match-action drop
configure cable filter group 2 index 1 ip-tos 0x0 0x0
```

CM Config File の TLV37 でモデム毎に別のフィルタリングルールを設定する場合には Default Group で用いたのと別の Filter Group ID で追加でフィルタリングルールを設定する。

```
configure cable filter group 11 index 1 ip-version unknown
configure cable filter group 11 index 1 src-port 0
configure cable filter group 11 index 1 dest-port 135
configure cable filter group 11 index 1 ip-proto 257
configure cable filter group 11 index 1 match-action drop
configure cable filter group 11 index 1 ip-tos 0x0 0x0
configure cable filter group 21 index 1 ip-version unknown
configure cable filter group 21 index 1 src-port 0
configure cable filter group 21 index 1 dest-port 135
configure cable filter group 21 index 1 ip-proto 257
configure cable filter group 21 index 1 match-action drop
configure cable filter group 21 index 1 ip-tos 0x0 0x0
```

さらに CM Config File 側で Filter Group ID を指定します。TLV37 (SubscriberManagementFilter)は CPE 用下りフィルタ、CPE 用上りフィルタ、CM 用下りフィルタ、CM 用上りフィルタの４つの ID を連続して記載するフォーマットになっている。上位から 2 Byte づつ CPE 用 DS、CPE 用 US、CM 用 DS、CM 用 US となっているため、上のフィルタリングルール、DS Filter Group ID=11 (0x00.0b)、US Filter Group ID = 21(0x00.15)を設定するには以下のような記載とする。

```
SubscriberManagementFilter = hexstr: 00.0b.00.15.00.00.00.00
```

(7) CPE 数制御

これまで IPv4 のサービスでは CM 配下に接続できる CPE 数の制限は許可される MAC Address 数で制限をかける CM Config File TLV18 (Max Cpe)を一般的に用いてきた。現実的にはユーザーはブロードバンドルータを接続し、IPv4 通信で NAT を用いることで、そのブロードバンドルータ配下には複数端末を接続することが可能となっており、ユーザーは接続可能な端末台数を意識することは無い。市販の多くのブロードバントルータでは IPv4 は NAT し、IPv6 は Bridge 接続となる仕様となっています。これの場合には MAC Address 数のみで制限をかけることができない。これは上記の場合に CM 配下の IPv4 アドレス数は 1 となるものの、IPv6 が Bridge されるため、IPv6 Packet によって CM には複数の MAC Address が認識されるためである。よってデュアルスタックサービスでは MAC Address 数に加えて、IPv4 Address、IPv6 Address 数を組み合わせて制限をかける必要があります。

IPv4 Address 数、IPv6 Address 数の制限は C4 上の Default Subscriber Management で全 CM に対して共通のルールを適用させる方法と、CM Config のパラメータ(IPv4=TLV35, IPv6=TLV63)によって行う方法がある。

C4 の Default Subscriber Management を適用させる C4 CLI コマンドを以下に示す。ここで max-cpe は CM の先で通信可能な IPv4 アドレスの数を規定し、v6-max-cpe は同じく通信可能は IPv6 アドレスの数を規定します。MAC アドレス数での台数制限は C4 Default Subscriber Management では行われず CM Config File TLV18 (Max Cpe)で行ないます。

```
configure cable submgmt default max-cpe 1
configure cable submgmt default v6-max-cpe 4
configure cable submgmt default active
```

Default Subscriber Management を configure cable submgmt default active no で無効にした場合は IPv4 Address は最高 32、IPv6 Address は最高 64 となります。Default Subscriber Management を有効にし、max-cpe、v6-max-cpe を C4 CLI 上で設定しない場合には IPv4 Address、IPv6 Address とも最高 16 となる。

これらの値は CM Config File に TLV35、TLV63 の設定がある場合には CM Config File の設定が優先します。これにより Default 以外のアドレス数制限が必要な CM には CM Config File で設定を行うことで複数のアドレス数制限ポリシーを適用させることができる。

尚、TLV63、v6-max-cpe で IPv6 アドレス数を制限する方法は本ガイドラインの 8.1 項で記載がある通り、1 台の CPE が複数 IPv6 アドレスを使用することがあることから望ましくなく IPv6 数自体は管理せず TLV18 での MAC アドレス数で全体の CPE 台数を制限する方法が望ましい。

(8) Cable Source Verify

Cable Source Verify の設定は IPv4、IPv6 ともに同一の設定となる。

```
configure interface cable-mac <WORD> cable source-verify
configure interface cable-mac <WORD> cable source-verify dhcp
configure interface cable-mac <WORD> cable source-verify dhcp authoritative
```

以下に設定全体を示す。

Gigabit Interface 設定

```
configure interface gigabitEthernet 17/3.0 ip address 10.197.211.14 255.255.255.252
configure interface gigabitEthernet 17/3.0 ipv6 enable
configure interface gigabitEthernet 17/3.0 ipv6 address fe80::d30c:2/64  link-local
configure interface gigabitEthernet 17/3.0 ipv6 address 2001:db8:3f00:d30c::2/64
configure interface gigabitEthernet 17/3.0 ipv6 nd ra suppress
configure interface gigabitEthernet 17/3 ip scm access-group 1

configure interface gigabitEthernet 18/3.0 ip address 10.197.211.58 255.255.255.252
configure interface gigabitEthernet 18/3.0 ipv6 enable
configure interface gigabitEthernet 18/3.0 ipv6 address fe80::d338:2/64  link-local
configure interface gigabitEthernet 18/3.0 ipv6 address 2001:db8:3f00:d338::2/64
configure interface gigabitEthernet 18/3.0 ipv6 nd ra suppress
configure interface gigabitEthernet 18/3 ip scm access-group 1
```

Cable Interface 設定

```
configure interface cable-mac 1.0 ip address 10.197.194.1 255.255.255.192
configure interface cable-mac 1.0 ipv6 enable
configure interface cable-mac 1.0 ipv6 address fe80::1:1/64  link-local
configure interface cable-mac 1.0 ip address 10.197.195.1 255.255.255.192 secondary dhcp-giaddr
# Cable Modem を IPv6 で Provision する場合の Prefix 設定
configure interface cable-mac 1.0 ipv6 address 2001:db8:3cc0:11::1/64 dhcp-link-address cable-modem
# CPE 用 Prefix (DHCPv6 にて Address 割り当て)
configure interface cable-mac 1.0 ipv6 address 2001:db8:3cc0:12::1/64  dhcp-link-address host
# CPE 用 Prefix (SLAAC 用の Prefix を作る場合)
configure interface cable-mac 1.0 ipv6 address 2001:db8:3cc0:13::1/64
configure interface cable-mac 1.0 cable helper-address 10.197.210.33
configure interface cable-mac 1.0 cable dhcp-giaddr policy
configure interface cable-mac 1.0 ipv6 dhcp relay destination 2001:db8:3f00:d200::33 cable-modem
configure interface cable-mac 1.0 ipv6 dhcp relay destination 2001:db8:3f00:d200::35 host
configure interface cable-mac 1.0 ipv6 nd managed-config-flag
configure interface cable-mac 1.0 ipv6 nd other-config-flag
configure interface cable-mac 1.0 ipv6 nd ra interval 600 200
configure interface cable-mac 1.0 ipv6 no nd ra suppress
configure interface cable-mac 1.0 ipv6 nd prefix 2001:db8:3cc0:13::/64 off-link autoconfig (SLAAC 用の Prefix を作る場合)
```

Routing 設定

```
configure ipv6 pd-route-injection
configure router ospf vrf default router-id 10.197.213.192
configure router ospf vrf default no shutdown
configure router ospf vrf default network 10.197.211.12 0.0.0.3 area 0.0.0.0
configure router ospf vrf default network 10.197.211.56 0.0.0.3 area 0.0.0.0
configure router ospf vrf default redistribute connected metric 1
configure ipv6 router ospf router-id 10.197.213.192
configure ipv6 router ospf no shutdown
configure ipv6 router ospf redistribute connected metric 1
configure interface gigabitEthernet 17/3.0 ip ospf network point-to-point
configure interface gigabitEthernet 17/3.0 ipv6 ospf network point-to-point
configure interface gigabitEthernet 17/3.0 ipv6 ospf area 0.0.0.0
configure interface gigabitEthernet 18/3.0 ip ospf network point-to-point
configure interface gigabitEthernet 18/3.0 ipv6 ospf network point-to-point
configure interface gigabitEthernet 18/3.0 ipv6 ospf area 0.0.0.0

#以下の設定で Prefix Delegation で生成する Prefix Range を上位ルータへ広報。
configure interface null 0
configure interface null 0 ip unreachables
configure interface null 0 ipv6 icmp unreachables
configure ipv6 route 2001:fa0:3cc0:1000/52 null 0
configure ipv6 router ospf redistribute static
```

CPE 数制限

```
configure cable submgmt default max-cpe 1
configure cable submgmt default v6-max-cpe 4
configure cable submgmt default active
```

Cable Source Verify

```
configure interface cable-mac 1 cable source-verify dhcp
```

Filtering 設定

例として Microsoft Windows のファイル共有を禁止する設定を以下に示します。

ここでは Filter Group 1、2 を作成し、1 を下りの Default ルールに 2 を上りの Default ルールに設定しています。3 番以降の Filter Group を作成し、それらを CM Config File TLV37 (SubscriberManagementFilter) で個々の CM に割り当てることも可能です。

```
configure cable submgmt default active
configure cable submgmt default filter-group host downstream 1
configure cable submgmt default filter-group host upstream 2
configure cable filter group 1 index 1 ip-version unknown
configure cable filter group 1 index 1 src-port 0
configure cable filter group 1 index 1 dest-port 135
configure cable filter group 1 index 1 ip-proto 257
configure cable filter group 1 index 1 match-action drop
configure cable filter group 1 index 1 ip-tos 0x0 0x0
configure cable filter group 1 index 2 ip-version unknown
configure cable filter group 1 index 2 src-port 0
configure cable filter group 1 index 2 dest-port 137
configure cable filter group 1 index 2 ip-proto 257
configure cable filter group 1 index 2 match-action drop
```

```
configure cable filter group 1 index 2 ip-tos 0x0 0x0
configure cable filter group 1 index 3 ip-version unknown
configure cable filter group 1 index 3 src-port 0
configure cable filter group 1 index 3 dest-port 138
configure cable filter group 1 index 3 ip-proto 257
configure cable filter group 1 index 3 match-action drop
configure cable filter group 1 index 3 ip-tos 0x0 0x0
configure cable filter group 1 index 4 ip-version unknown
configure cable filter group 1 index 4 src-port 0
configure cable filter group 1 index 4 dest-port 139
configure cable filter group 1 index 4 ip-proto 257
configure cable filter group 1 index 4 match-action drop
configure cable filter group 1 index 4 ip-tos 0x0 0x0
configure cable filter group 1 index 5 ip-version unknown
configure cable filter group 1 index 5 src-port 0
configure cable filter group 1 index 5 dest-port 445
configure cable filter group 1 index 5 ip-proto 257
configure cable filter group 1 index 5 match-action drop
configure cable filter group 1 index 5 ip-tos 0x0 0x0
configure cable filter group 1 index 6 ip-version unknown
configure cable filter group 1 index 6 src-port 0
configure cable filter group 1 index 6 dest-port 67
configure cable filter group 1 index 6 ip-proto 17
configure cable filter group 1 index 6 match-action drop
configure cable filter group 1 index 6 ip-tos 0x0 0x0
configure cable filter group 2 index 1 ip-version unknown
configure cable filter group 2 index 1 src-port 0
configure cable filter group 2 index 1 dest-port 135
configure cable filter group 2 index 1 ip-proto 257
configure cable filter group 2 index 1 match-action drop
configure cable filter group 2 index 1 ip-tos 0x0 0x0
configure cable filter group 2 index 2 ip-version unknown
configure cable filter group 2 index 2 src-port 0
configure cable filter group 2 index 2 dest-port 137
configure cable filter group 2 index 2 ip-proto 257
configure cable filter group 2 index 2 match-action drop
configure cable filter group 2 index 2 ip-tos 0x0 0x0
configure cable filter group 2 index 3 ip-version unknown
configure cable filter group 2 index 3 src-port 0
configure cable filter group 2 index 3 dest-port 138
configure cable filter group 2 index 3 ip-proto 257
configure cable filter group 2 index 3 match-action drop
configure cable filter group 2 index 3 ip-tos 0x0 0x0
configure cable filter group 2 index 4 ip-version unknown
configure cable filter group 2 index 4 src-port 0
configure cable filter group 2 index 4 dest-port 139
configure cable filter group 2 index 4 ip-proto 257
configure cable filter group 2 index 4 match-action drop
configure cable filter group 2 index 4 ip-tos 0x0 0x0
configure cable filter group 2 index 5 ip-version unknown
configure cable filter group 2 index 5 src-port 0
configure cable filter group 2 index 5 dest-port 206
configure cable filter group 2 index 5 ip-proto 17
configure cable filter group 2 index 5 match-action drop
```

```
configure cable filter group 2 index 5 ip-tos 0x0 0x0
configure cable filter group 2 index 6 ip-version unknown
configure cable filter group 2 index 6 src-port 0
configure cable filter group 2 index 6 dest-port 445
configure cable filter group 2 index 6 ip-proto 257
configure cable filter group 2 index 6 match-action drop
configure cable filter group 2 index 6 ip-tos 0x0 0x0
```

Appendix Ⅰ-Ⅱ　Cisco uBR CMTS CLI 設定例

図 B-1 に示すネットワーク構成図を実現する uBR CMTS での CLI 設定を以下に示す。

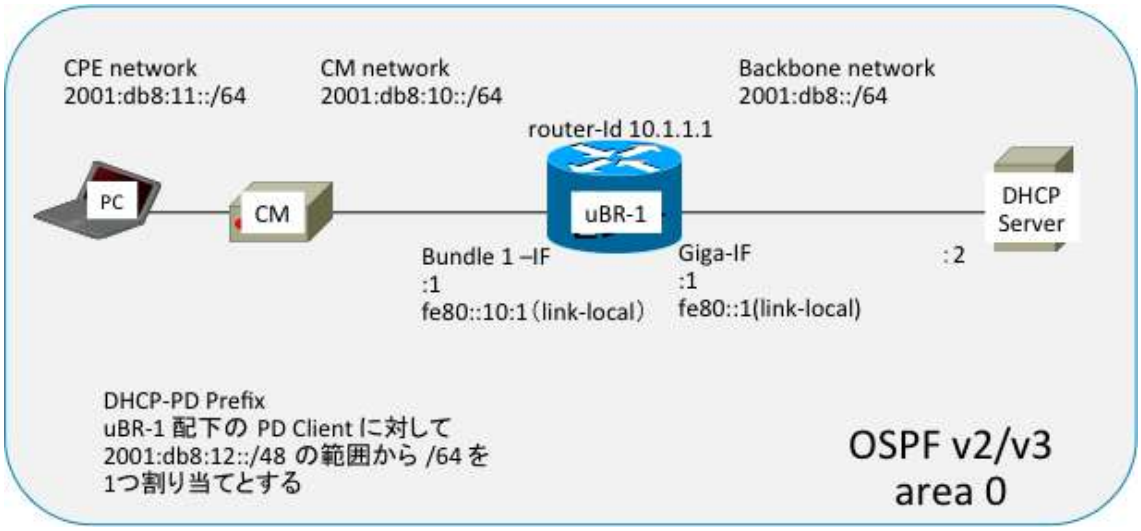


図 B-1 基本ネットワーク構成図

(1) Uplink Interface (Gigabit Interface/10GE interface)

Global Config モードで ipv6 を有効にするために”ipv6 unicast-routing”を設定する。

CMTS の上位ネットッワークに接続する Uplink Interface(Gigabit Interface/10GE interface) にグローバルユニキャスト IPv6 アドレスを割り当てる。

Link Local アドレスはデフォルトでは EUI64 形式のアドレスが自動で割り当てられるが、EUI64 形式のアドレスでは Next Hop が判別しにくいため Global Address に基づきなんらかの規則で固定で Link Local Address を割り当てることを推奨すルータだし、ルーティングプロトコルに OSPFv3 を使用する場合、上位ルータに接続される他のルータ等に CMTS と同じ Link Local アドレスが設定されている場合、上位ルータでアドレスの重複が発生していると判断し、OSPFv3 が正しく動作しないため、設定する Link Local アドレスには注意が必要である。また Uplink Interface では RA を出す必要は無いため ipv6 nd ra suppress コマンドで RA を抑制する。

図 B-2 に IPv 6 の有効化及び Giga-IF に IPv6 アドレスの設定例を示す。

Giga-IF にアドレスを設定する例

```
(config)# ipv6 unicast-routing(1)
(config)#
(config)# interface GigabitEthernet0/3
(config-if)# ipv6 address FE80::1 link-local   (2)
(config-if)# ipv6 address 2001:DB8::1/64
(config-if)# ipv6 nd ra suppress  (3)
```

(1) IPv6サービスを有効化

コマンドを入力しないと、ルーティング以外の機能も有効にならない（例えば ipv6 ping に応答しない、RA を送出しないなど。）ので必ず入力すること。

(2) link-local を static で設定

(3) RA を送信しないように設定

 3

図 B-2　Giga-IF へのアドレス設定例

(9) Cable Interface

RF 関連のパラメータは IPv6/IPv6 に関わらず同じ。CM 起動時にどのプロビジョンングモードで起動するかを指定するために、“cable ip-init xxxx” コマンドを設定する。

図 B-3 に Cable Interrface でのプロビジョニングモードの設定例を示す。

Cable-IF で Provisioning mode を設定する例

```
(config)# interface Cable 1/0
(config-if)# cable ip-init dual-stack (1)
```

(1) CM を dual-stack mode で動作するように設定。オプションは、ipv4(デフォルト), ipv6, apm, dual-stack を選択可能

 2

図 B-3　Cable-IF へプロビジョニングモード設定例

(10)Bundle　Interface

L3 関連の設定は必要な Bundle Interface に設定を行う。

IPv4 の設定に加え、以下の IPv6 の設定を Bundle Interface に対して実施する。

①Link Local アドレス

Gigabit Ethernet Interface と同様に Link Local Address の割当を行う。デフォルトでは EUI-64 で生成された Link Local アドレスが自動的に設定されるが、運用上判別が困難になるので、Static で設定を行うことを推奨する。

②、③Global Unicast アドレス

CM を IPv6 で管理する場合は、CM 管理用と CPE 用の Global Unicast アドレスの設定を行う。（CM を IPv4 のみで管理する場合は IPv4 のみで可）

④、⑤RA M/O フラグの設定

CPE を DHCPv6 でアドレスの取得を実施させるために、RA 内の M フラグと O フラグを Enable にする必要があるため、これらを Enable にするために" ipv6 nd managed-config-flag"と"ipv6 nd other-config-flag"の設定を行う。

⑥、⑦RA Prrefix 情報 no-autoconfig 設定

デフォルトの設定では Bundle Interface で生成される RA の Prefix 情報において、A-flag が enable となっており、CPE が SLAAC でアドレスを自動生成してしまう。no-autoconfig オプションを設定し、A-flag disable とすることで本ガイドラインにおいて推奨していない SLAAC での CPE のアドレスを自動生成することを制限出来る。

⑦DHCPv6 Relay 設定

CM、CPE からの DHCPv6 パケットを転送する DHCPv6 サーバの IPv6 アドレスを設定する。

図 B-3 に Bundle Interface での IPv6 設定例を示す。

Bundle-IF を設定する例

```
(config)# interface Bundle1
(config-if)# ipv6 address FE80::10:1 link-local  (1)
(config-if)# ipv6 address 2001:DB8:10::1/64  (2)
(config-if)# ipv6 address 2001:DB8:11::1/64  (3)
(config-if)# ipv6 nd managed-config-flag  (4)
(config-if)# ipv6 nd other-config-flag  (5)
(config-if)# ipv6 nd prefix 2001:DB8:10::/64 300 300 no-autoconfig (6)
(config-if)# ipv6 nd prefix 2001:DB8:11::/64 300 300 no-autoconfig (7)
(config-if)# ipv6 dhcp relay destination 2001:DB8::2  (8)
```

(1) link-local を static で設定
(2) CM 用の IPv6 グローバルユニキャストアドレス
(3) CPE 用の IPv6 グローバルユニキャストアドレス
(4) 送信する RAメッセージの M Flag を enable
(5) 送信する RAメッセージの O Flag を enable
(6) 送信する RA メッセージの CM用 Prefix の A Flag を disable
(7) 送信する RAメッセージの CPE用 Prefix の A Flag を disable
(8) DHCPv6パケットの転送先アドレス（DHCPサーバ）を設定

Presentation_ID © 2012 Cisco Systems, Inc. All rights reserved. 4

図 B−3　Bundle-IF の IPv6 設定

(11)OSPFv3

IPv6 での OSPF 設定は、IPv6 を動作させる IF 毎に OSPFv3 の有効化を行う必要がある。図 2-1 の構成においては、Giga-IF、Bundle-IF において有効化を行う必要がある。（Cable-IF は L3 を取り扱わないため設定不要）

OSPFv3 設定の手順としては、

①Global Config モードで OSPFv3 の有効化と router-id の設定

②Giga-IF での OSPFv3 有効化

③Bundle-IF での OSPFv3 有効化

④Global Config モードでの各種 OSPFv3 設定

・Bundle-IF 配下に OSPFv3 ルート情報を広報する必要がないため、passive-interface 設定

・CPE に対して DHCPv6-PD を使用する場合、Prefix 数が膨大になるため、ルートを Summrize して配信するように設定

図 B-4 に OSPFv3 の設定例を示す。

OSPFv3を設定する例

```
(config)# ipv6 router ospf 1      (1)
(config-rtr)# router-id 10.1.1.1

(config)# interface GigabitEthernet0/3
(config-if)# ipv6 ospf 1 area 0   (2)

(config)# interface Bundle1
(config-if)# ipv6 ospf 1 area 0   (3)

(config)# ipv6 router ospf 1
(config-rtr)# passive-interface Bundle1   (4)
(config-rtr)# summary-prefix 2001:db8:12::/48     (5)
(config-rtr)# redistribute static metric-type 1
```

(1) OSPFv3 を有効化し、router-id を設定

(2) Gig-IF で OSPFv3 を有効化

(3) Bundle-IF で OSPFv3 を有効化

(4) Bundle-IF を passive-interface に設定

(5) DHCP-PD の Static route を Summary で配信するように設定

Presentation_ID © 2012 Cisco Systems, Inc. All rights reserved. 5

図 B-4　OSPFv3 の設定例

(12)IPv6 ACL

図 B-5 に IPv6 ACL の設定例（IPv6 での TELNET アクセスを特定の Prefix のみに許可）を示す。

IPv6 ACL 設定例

```
(config)#ipv6 access-list V6_VTY
(config-ipv6-acl)#permit 2001:db8:20::/64 any      (1)

(config)#line vty 0 4
(config-line)#ipv6 access-class V6_VTY in          (2)
```

(1) 送信元IPv6アドレス 2001:db8:20::/64 のみ許可するACLを設定

(2) Vty に ACL を適用

ipv6 unicast-routing コマンドと IF へのipv6 アドレス設定を行うと、そのIPv6アドレス宛て（link-localも含む）に vty アクセスが可能になるため、ACL は必ず設定すること。

 6

図 B-5　IPv6 ACL 設定例

Appendix Ⅰ-Ⅲ　BSR64000 CMTS CLI 設定例

図 C-1 に示すネットワーク構成図を実現する BSR64000 CMTS での CLI 設定を以下に示す。

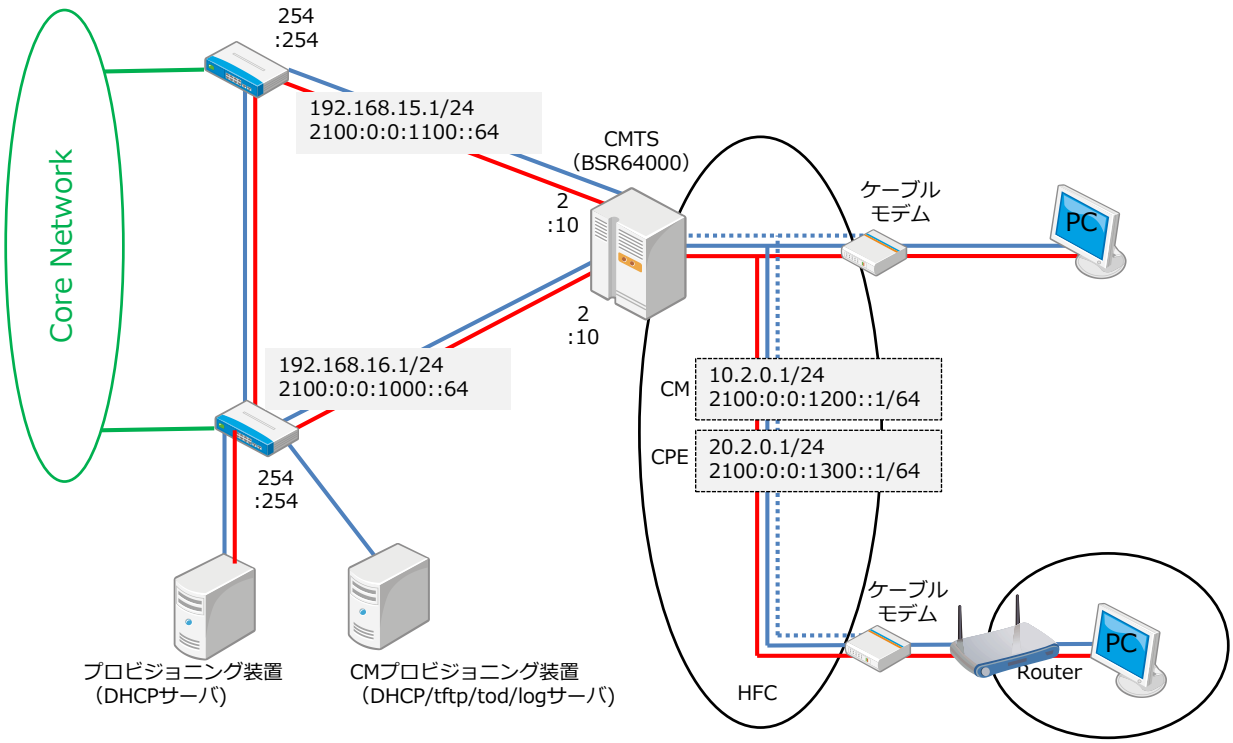


図 C-1 基本ネットワーク構成図

(1) Gigabit Interface

上位ルータに接続される HSIM4 の Gigabit Ethernet Interface に IPv6 アドレスを割り当てる。Link Local アドレスはデフォルトでは EUI64 形式のアドレスが自動で割り当てられる。固定での Link Local アドレス指定も可能である為、運用形態に合せて設定する事が可能である。また Gigabit Ethernet Interface では RA を出す必要は無いため ipv6 nd ra suppress コマンドで RA を抑制する。

```
bsr2_lab:7A#configure
bsr2_lab:7A(config)#interface gigaether 14/0
bsr2_lab:7A(config-if)#ip address 192.168.16.2 255.255.255.0
bsr2_lab:7A(config-if)#ipv6 address 2100:0:0:1000::10/64
bsr2_lab:7A(config-if)#ipv6 address fe80::192:168:16:2 link-local
bsr2_lab:7A(config-if)#ipv6 nd ra suppress
```

Loopback Interface には、CM 用、CPE 用 Address を設定する。IPv4 設定部分は、従来通りの設定方法となる。IPv6 設定部分は、Global Unicast Address は、CM 用 Prefix（CM を IPv6 で Provisioning する場合）と CPE Prefix を設定する。IPv4 Address 設定と同様に Global Unicast Address 設定の後段に secondary オプションを設定する事により CM/CPE Prefix が設定された場合に CPE からの DHCPv6 Solicit を BSR64000 が Relay Agent する際に DHCPv6 Solicit メッセージ内に含まれる Link Address を CPE Global Unicast Address として Forward します。

また、DHCPv6 Server の設定も IPv4 DHCP Server と同様に ipv6 helper-address コマンドにて Loopback Interface に設定します。この ipv6 helper-address 設定も後段に cable-modem 又は host を設定する事で IPv6 用 CM/CPE DHCPv6 Server を個々に設定する事が可能である。ipv6 helper-address を複数設定した場合は、設定したアドレス全てに対して Relay Agent をして DHCPv6 Solicit を Forward する。

```
bsr2_lab:7A#configure
bsr2_lab:7A(config)#interface loopback 2
bsr2_lab:7A(config-if)#ip address 10.2.0.1 255.255.255.0
bsr2_lab:7A(config-if)#ip address 20.2.0.1 255.255.255.0 secondary
bsr2_lab:7A(config-if)#cable helper-address 172.10.1.254 cable-modem global
bsr2_lab:7A(config-if)#cable helper-address 172.10.1.254 host global
bsr2_lab:7A(config-if)#ipv6 address 2100:0:0:1200::1/64
bsr2_lab:7A(config-if)#ipv6 address 2100:0:0:1300::1/64 secondary
bsr2_lab:7A(config-if)#cable ipv6 helper-address 2001:0:0:10::153 cable-modem
bsr2_lab:7A(config-if)#cable ipv6 helper-address 2001:0:0:10::153 host
```

(3) Cable Interface(Mac Domain)

IPv4、IPv6 Address 共に IPv4/IPv6 Address を設定した Loopback Interface を Bundle 設定する事で各 Cable Interface に IPv4/IPv6 Address を割り当てる事になる。

Nd managed-config-flag, nd other-config-flag は CPE が DHCPv6 でアドレスを取得するために RA 内の M-Flag、O-Flag はデフォルトで ON(1)となっている。

nd reachable-time コマンドで CPE からの ND 送信間隔を設定する。ND 送信回数を極力最小にする為、3600000ms を設定する。

nd ra interval コマンドで RA の送信間隔を設定する。CM、CPE が RA よりデフォルトルートを設定する為、30 秒間隔で RA を送信する事を推奨する。

BSR64000 のデフォルトの設定では Cable Interface で発生される RA には Prefix 情報は含まれていない。この場合 CPE は Prefix 長を取得できず DHCP で取得したアドレスは/128 になる。CPE の Prefix 長を/64 で指定する場合、ipv6 nd prefix に no-autoconfig オプションを入れることで CPE は Prefix 長/64 を RA より取得できる。また、no-autoconfig オプションにより CPE が SLAAC(Stateless address autoconfiguration)でアドレスを自動生成するのを抑制できる。

BSR64000 内にて CPE の IPv6 通信を実現する為に multicast dsid-forwarding を各 Interface Cable(MacDomain)に設定する。

各 Cable Interface にて個別に Link Local Address を設定できます。設定を投入しなかった場合は、BSR64000 シャーシ MAC Address をベースに各 Cable Interface の Link Local Address が自動生成されます。

```
bsr2_lab:7A#configure
bsr2_lab:7A(config)#interface cable 1/0
bsr2_lab:7A(config-if)#ipv6 nd reachable-time 3600000
bsr2_lab:7A(config-if)#ipv6 nd ra-interval msec 30000
bsr2_lab:7A(config-if)#ipv6 nd prefix 2100:0:0:1300::/64 no-autoconfig
bsr2_lab:7A(config-if)#cable multicast dsid-forwarding
bsr2_lab:7A(config-if)#cable ip prov-mode dpm
```

(4) Routing プロトコル（OSPF）

IPv4 OSPF の設定は従来通り。

```
bsr2_lab:7A#configure
bsr2_lab:7A(config)#router ospf
bsr2_lab:7A(config-ospf)#router-id 172.25.100.3
bsr2_lab:7A(config-ospf)#passive-interface loopback 2
bsr2_lab:7A(config-ospf)# network 192.168.16.0 0.0.0.255 area 1.2.3.4
bsr2_lab:7A(config-ospf)# network 192.168.15.0 0.0.0.255 area 1.2.3.4
bsr2_lab:7A(config-ospf)# network 20.2.0.0 0.0.0.255 area 1.2.3.4
bsr2_lab:7A(config-ospf)# network 10.2.0.0 0.0.0.255 area 1.2.3.4
bsr2_lab:7A(config-ospf)# redistribute connected
```

現時点の BSR64000 の Farmware では、OSPFv3 の Routing プロトコルをサポートしていない。これにより IPv6 の Routing には、Dynamic Routing ではなく、Static Routing を設定する。（BSR64000 の OSPFv3 は、2012 年 10 月にサポートする。）

```
bsr2_lab:7A#configure
bsr2_lab:7A(config)#ipv6 route ::/0 fe80::192:168:16:254 interface gigaether 14/0
bsr2_lab:7A(config)#ipv6 route ::/0 fe80::192:168:15:254 interface gigaether 15/0
```

(5) Filtering (Network Side ACL)

IPv6 ACL は、IPv4 ACL と同様に Access-List グループを定義し、設定条件に一致した IPv6 パケットで許可（Permit）、拒否（Deny）する事が可能です。指定するプロトコルには、ahp、esp、icmp6、ipv6、tcp、udp その他に個別 0-255 までのプロトコル番号が設定可能です。Source、Distination アドレスは、IPv6/Prefix、any 又は Host の設定をします。Port 番号に関しては、Filter を実行したい Port 番号を適応します。

定義した IPv6 ACL は、各 Gigabit 及び Cable Interface に ipv6 traffic-filter コマンドにて設定します。

```
bsr2_lab:7A#configure
bsr2_lab:7A(config)#ipv6 access-list mot-in
bsr2_lab:7A(config-ipv6-acl)#deny udp any any eq 521
bsr2_lab:7A(config-ipv6-acl)#deny udp any any eq 3702
bsr2_lab:7A(config-ipv6-acl)#deny tcp any any eq 3702
bsr2_lab:7A(config-ipv6-acl)#permit ipv6 any any
bsr2_lab:7A(config-ipv6-acl)#permit udp any any
bsr2_lab:7A(config-ipv6-acl)#permit tcp any any
bsr2_lab:7A(config-ipv6-acl)#permit icmp6 any any

bsr2_lab:7A(config)#ipv6 access-list mot-out
bsr2_lab:7A(config-ipv6-acl)#deny deny udp any any eq 521
bsr2_lab:7A(config-ipv6-acl)#deny permit udp any any
bsr2_lab:7A(config-ipv6-acl)#deny permit ipv6 any any
bsr2_lab:7A(config-ipv6-acl)#deny permit icmp6 any any

bsr2_lab:7A(config)#interface cable 1/0
bsr2_lab:7A(config-if)#ipv6 traffic-filter mot-in in
bsr2_lab:7A(config-if)#ipv6 traffic-filter mot-out out
```

(6) Filtering (Subscriber Management Filter)

BSR64000 に Subscriber Management Filter を設定する事により BSR64000 配下 CM 全てに対して IPv4 パケットの Flitering を実施します。

Filtering 方法は、上りパケット、下りパケットにユニークな Index ID を設定し、その Index ID に個々のフィルタリングルールを Index ID と共に定義します。

```
bsr2_lab:7A#configure
bsr2_lab:7A(config)#cable submgmt default filter-group downstream 1
bsr2_lab:7A(config)#cable submgmt default filter-group upstream 2

bsr2_lab:7A(config)#cable filter group 1 index 1 action drop
bsr2_lab:7A(config)#cable filter group 1 index 1 enable
bsr2_lab:7A(config)#cable tcpudp-filter group 1 index 1 dst-port 135
bsr2_lab:7A(config)#cable tcpudp-filter group 1 index 1 enable

bsr2_lab:7A(config)#cable filter group 2 index 1 action drop
bsr2_lab:7A(config)#cable filter group 2 index 1 enable
bsr2_lab:7A(config)#cable tcpudp-filter group 2 index 1 dst-port 135
bsr2_lab:7A(config)#cable tcpudp-filter group 2 index 1 enable
```

また、CM 単体でフィルタリングルールを設定する場合は、CM Config に TLV37 を設定し、個々の CM へ適応する事により可能となる。

(7) CPE 数制御

BSR64000 にて CM 配下 CPE 数を制限する方法としては、CM Config TLV18 による制限と BSR64000 の設定による cable submgmt default で制限が可能となります。TLV18 を設定した場合は、CM 配下の CPE MAC Address 数にて制限がかけられます。また、cable submgmt

default を設定した場合は、mac-cpe で指定した IPv4 Address 数のみ CM 配下で制限をかけられます。IPv6 Address 数に対しては、制限はかけられません。
尚、本ガイドライン 8.1 項で一台の CPE が複数の IPv6 Address を取得する事を望ましい設定と定義している事から TLV18 と cable submgmt default を併用する事を推奨する。
尚、BSR64000 では TLV35、63 を今後の Farmware リリースにてサポートする。

```
bsr2_lab:7A#configure
bsr2_lab:7A(config)#cable submgmt default cpe-control max-cpe 4
bsr2_lab:7A(config)#cable submgmt default cpe-control active true
```

(8) DHCP leasequery

BSR64000 では、故意の Static IP Address の制限として DHCP leasequery の設定があります。本設定により DHCP より Dynamic の取得した IP Address のみ通信を許可する事ができます。DHCP leasequery の設定は IPv4、IPv6 ともに同一の設定となり、各 Interface Cable に設定します。

```
bsr2_lab:7A#configure
bsr2_lab:7A(config)#interface cable 1/0
bsr2_lab:7A(config-if)#host authorization on
bsr2_lab:7A(config-if)# dhcp leasequery authorization on
bsr2_lab:7A(config-if)# dhcp leasequery default lease-time 0
```

下記に設定全体を示す。

<u>Gigabit Interface 設定</u>

```
interface gigaether 14/0
 ip address 192.168.16.2 255.255.255.0
 ipv6 address fe80::192:168:16:2 link-local
 ipv6 address 2100:0:0:1000::10/64
 no shutdown
 ipv6 nd ra-interval msec 600000
 ipv6 nd ra suppress
 ip ospf cost 10
 ip ospf dead-interval 40
 ip ospf hello-interval 10
 ip ospf priority 0

interface gigaether 15/0
 ip address 192.168.15.2 255.255.255.0
 ipv6 address fe80::192:168:15:2 link-local
 ipv6 address 2100:0:0:1100::10/64
 no shutdown
 ipv6 nd ra-interval msec 600000
 ipv6 nd ra suppress
 ip ospf cost 110
 ip ospf dead-interval 40
 ip ospf hello-interval 10
 ip ospf priority 0
```

loopback Interface 設定

```
interface loopback 2
 cable bundle 1 master
 ip address 10.2.0.1 255.255.255.0
 ip address 20.2.0.1 255.255.255.0 secondary
 ipv6 address 2100:0:0:1200::1/64
 ipv6 address 2100:0:0:1300::1/64 secondary
 cable helper-address 172.10.1.254 cable-modem global
 cable helper-address 172.10.1.254 host global
 cable ipv6 helper-address 2001:0:0:10::153 cable-modem
 cable ipv6 helper-address 2001:0:0:10::153 host
 no shutdown
```

Cable Interface 設定

```
interface cable 1/0
 cable bundle 1
 no ip address
 mdrc enable
 no shutdown
 ipv6 traffic-filter mot-in in
 ipv6 traffic-filter mot-out out
 arp timeout 120
 cable bind downstream 11/2/0,11/2/1,11/2/2,11/2/3
 cable downstream bonding-group 11 11/2/0 11/2/1 11/2/2 11/2/3
 cable bind upstream 0,1,2,3
 cable upstream 0/0 channel-type atdma
 cable upstream 0 frequency 30000000
 cable upstream 0/0 range-backoff 2 8
 cable upstream 0 power-level 10
 cable upstream 0/0 modulation-profile 224
 no cable upstream 0 shutdown
 no cable upstream 0/0 shutdown
 cable upstream 0/1 shutdown
 cable upstream 0/2 shutdown
 cable upstream 0/3 shutdown
 cable upstream 1/0 channel-type atdma
 cable upstream 1 frequency 30000000
 cable upstream 1/0 range-backoff 2 8
 cable upstream 1 power-level 10
 cable upstream 1/0 modulation-profile 231
 no cable upstream 1 shutdown
 no cable upstream 1/0 shutdown
 cable upstream 1/1 shutdown
 cable upstream 1/2 shutdown
 cable upstream 1/3 shutdown
 cable upstream 2/0 channel-type atdma
 cable upstream 2 frequency 30000000
 cable upstream 2/0 range-backoff 2 8
 cable upstream 2 power-level 10
 cable upstream 2/0 modulation-profile 231
 no cable upstream 2 shutdown
 no cable upstream 2/0 shutdown
 cable upstream 2/1 shutdown
```

```
 cable upstream 2/2 shutdown
 cable upstream 2/3 shutdown
 cable upstream 3/0 channel-type atdma
 cable upstream 3 frequency 30000000
 cable upstream 3/0 range-backoff 2 8
 cable upstream 3 power-level 10
 cable upstream 3/0 modulation-profile 231
 no cable upstream 3 shutdown
 no cable upstream 3/0 shutdown
 cable upstream 3/1 shutdown
 cable upstream 3/2 shutdown
 cable upstream 3/3 shutdown
 cable mdd-interval 500
 cable ip prov-mode dpm
 cable multicast dsid-forwarding
 ipv6 nd dad attempts 1
 ipv6 nd reachable-time 3600000
 ipv6 nd ra-interval msec 30000
 ipv6 nd prefix 2100:0:0:1300::/64 no-autoconfig
 cable dynamic-service authorization-mode disable
 ip dhcp relay information option
 host authorization on
 dhcp leasequery authorization on
 dhcp leasequery default lease-time 0
```

Routing 設定

```
router ospf
 router-id 172.25.100.3
 passive-interface loopback 2
 network 192.168.16.0 0.0.0.255 area 1.2.3.4
 network 192.168.15.0 0.0.0.255 area 1.2.3.4
 network 20.2.0.0 0.0.0.255 area 1.2.3.4
 network 10.2.0.0 0.0.0.255 area 1.2.3.4
 redistribute connected

ipv6 route ::/0 fe80::192:168:16:254 interface gigaether 14/0
ipv6 route ::/0 fe80::192:168:15:254 interface gigaether 15/0
```

CPE 数制限

```
cable submgmt default cpe-control max-cpe 4
cable submgmt default cpe-control active true
```

DHCP leasequery

```
host authorization on
dhcp leasequery authorization on
dhcp leasequery default lease-time 0
```

Filtering 設定(IPv6 ACL)

```
ipv6 access-list mot-in
   deny udp any any eq 521
   deny udp any any eq 3702
   deny tcp any any eq 3702
   permit ipv6 any any
```

```
  permit udp any any
  permit tcp any any
  permit icmp6 any any

ipv6 access-list mot-out
  deny udp any any eq 521
  permit udp any any
  permit ipv6 any any
  permit icmp6 any any
```

Filtering 設定(Subscriber Management Filter)

```
cable filter group 1 index 1 action drop
cable filter group 1 index 1 enable
cable filter group 1 index 2 action drop
cable filter group 1 index 2 enable
cable filter group 1 index 3 action drop
cable filter group 1 index 3 enable
cable filter group 1 index 4 action drop
cable filter group 1 index 4 enable
cable filter group 1 index 5 action drop
cable filter group 1 index 5 enable
cable filter group 1 index 6 ulp 17
cable filter group 1 index 6 action drop
cable filter group 1 index 6 enable
cable filter group 1 index 7 ulp 17
cable filter group 1 index 7 action drop
cable filter group 1 index 7 enable
cable filter group 2 index 1 action drop
cable filter group 2 index 1 enable
cable filter group 2 index 2 action drop
cable filter group 2 index 2 enable
cable filter group 2 index 3 action drop
cable filter group 2 index 3 enable
cable filter group 2 index 4 action drop
cable filter group 2 index 4 enable
cable filter group 2 index 5 action drop
cable filter group 2 index 5 enable
cable filter group 2 index 6 ulp 17
cable filter group 2 index 6 action drop
cable filter group 2 index 6 enable
cable filter group 2 index 7 ulp 17
cable filter group 2 index 7 action drop
cable filter group 2 index 7 enable
cable filter group 2 index 8 ulp 17
cable filter group 2 index 8 action drop
cable filter group 2 index 8 enable
cable filter group 2 index 9 action drop
cable filter group 2 index 9 enable
!
cable submgmt default filter-group downstream 1
cable submgmt default filter-group upstream 2
!
cable tcpudp-filter group 1 index 1 dst-port 135
cable tcpudp-filter group 1 index 1 enable
```

```
cable tcpudp-filter group 1 index 2 dst-port 137
cable tcpudp-filter group 1 index 2 enable
cable tcpudp-filter group 1 index 3 dst-port 138
cable tcpudp-filter group 1 index 3 enable
cable tcpudp-filter group 1 index 4 dst-port 139
cable tcpudp-filter group 1 index 4 enable
cable tcpudp-filter group 1 index 5 dst-port 445
cable tcpudp-filter group 1 index 5 enable
cable tcpudp-filter group 1 index 6 dst-port 520
cable tcpudp-filter group 1 index 6 enable
cable tcpudp-filter group 1 index 7 dst-port 521
cable tcpudp-filter group 1 index 7 enable
cable tcpudp-filter group 2 index 1 dst-port 135
cable tcpudp-filter group 2 index 1 enable
cable tcpudp-filter group 2 index 2 dst-port 137
cable tcpudp-filter group 2 index 2 enable
cable tcpudp-filter group 2 index 3 dst-port 138
cable tcpudp-filter group 2 index 3 enable
cable tcpudp-filter group 2 index 4 dst-port 139
cable tcpudp-filter group 2 index 4 enable
cable tcpudp-filter group 2 index 5 dst-port 445
cable tcpudp-filter group 2 index 5 enable
cable tcpudp-filter group 2 index 6 dst-port 520
cable tcpudp-filter group 2 index 6 enable
cable tcpudp-filter group 2 index 7 dst-port 521
cable tcpudp-filter group 2 index 7 enable
cable tcpudp-filter group 2 index 8 dst-port 68
cable tcpudp-filter group 2 index 8 enable
cable tcpudp-filter group 2 index 9 dst-port 3702
cable tcpudp-filter group 2 index 9 enable
```

Appendix II 執筆者一覧

IPv4 アドレス枯渇対応プロジェクト
IPv6 対応ガイドラインドラフティンググループ　※活動期間：2012/1/30～9/13

網干　勝也	古河電気工業
荒井　康祐	ＮＥＣマグナスコミュニケーションズ
伊藤　太郎	伊藤忠テクノソリューションズ
上田　健太郎	古河電気工業
小川　貴正	倉敷ケーブルテレビ
奥山　清雄	ネットワンシステムズ
川島　誠一	シスコシステムズ
小木曽　哲哉	コミュニティネットワークセンター
小山　海平	倉敷ケーブルテレビ　<プロジェクト&ドラフティンググループ主任>
澤崎　栄治	コミュニティネットワークセンター
鷹野　要介	テクノロジーネットワークス
友松　和彦	アリス・グループ・ジャパン
平松　史昭	ジャパンケーブルネット
守屋　篤	ブロードネットマックス

（五十音順）

あとがき

「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）」が策定されて既に２年以上が経過している。Version1.0 の策定にもある程度関わったのだが、改めてこの２年で IPv6 対応について、まわりの環境や取組み方が変わってきていることを実感している。

元々IPv6 対応の普及に関しての予測をどのようにしていたかにもよるが、私自身は２年前の想定よりは普及の速度は上がっていると感じている。

World IPv6 Day、World IPv6 Launch を通じて、Hyper Giant がかなり本気で IPv6 化を進めているのが、やはり大きいと思える。彼らには、IPv4 アドレスが枯渇した状況では、IPv4 は何らかのアドレスシェアリングをされている Simple では無いネットワークで、品質もシェアリングされていないよりデグレードされているに違いなく、IPv6 の方が Simple で品質も高くなる可能性があるという思想（正義？）があるのではなかろうか。

確かに、自分の立場や環境を離れて客観的に考えれば、その通りと思うところもある。

今回の Version2.0 ではドキュメントの量としても倍以上となり、昨今ケーブル事業者でも取り組んでいる FTTH に関しても適用範囲としている。

今すぐには動かなくてもクリティカルでは無いが、数年後かにドラスティックな事が起きないとも限らない。我々ケーブルインターネット事業者は、速度には差こそあれ、粛々と IPv6 対応を進めていかなければならないし、またその時に本ドキュメントが役に立つことを切に願っている。

最後に、本書の作成にあたり、本来の業務と並行して忙しい中対応いただいたドラフティングメンバーには、改めて感謝の意を評したいと思う。

2012 年 9 月

IPv4 アドレス枯渇対応プロジェクト主任　小山海平

（空　白）

日本ケーブルラボ仕様ガイドライン

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 2.0 版

2010 年 6 月 30 日　1.0 版
2012 年 9 月 14 日　2.0 版

発行　一般社団法人　日本ケーブルラボ
〒108-0071 東京都港区白金台 3-19-1
興和白金台ビル 5 階
電話　03-6450-4311　FAX　03-6450-4310