

IPv6 家庭用ルータ ガイドライン

【第 1.0 版】

2009 年 6 月 22 日

IPv6 普及・高度化推進協議会

IPv4/IPv6 共存 WG IPv6 家庭用ルーターSWG

変更履歴

版	改版日	摘要
0.9	2009 年 5 月 22 日	パブリックコメント版
1.0	2009 年 6 月 22 日	第 1 版 若干の修正，未検討項目の作成

目次

1	はじめに	1
1.1	当該文書の背景と目的	1
1.2	本ガイドラインの想定環境と対象とする読者	2
1.3	記述用語と表記方法に関して	3
1.4	ガイドライン作成にあたり	4
1.4.1	ISP が提供する基本機能	4
1.4.2	宅内ネットワークの概略	5
1.4.3	家庭用ルータに求められる機能	6
2	ISP への接続機能	8
2.1	ネイティブ接続	8
2.1.1	接続形態	8
2.2	PPPoE/PPPoA	8
2.2.1	接続形態	8
2.3	IP ベースのトンネル (IPv6 over IPv4・IPv6 over IPv6 など)	9
2.3.1	接続形態	9
3	アドレス割り当て手法	10
3.1	プレフィックス割り当て	10
3.1.1	宅内ネットワークへ配布するプレフィックス情報	10
3.1.2	宅内ネットワークへの割り当てプレフィックスサイズ	10
3.1.3	プレフィックスの割り当て	11
3.2	WAN 側アドレス	12
3.2.1	グローバルアドレスの付与	12
3.3	LAN 側アドレス	14
3.3.1	プレフィックスの再配布	14
3.3.2	複数プレフィックスの受信	14
3.3.3	配布プレフィックスの変化	15
4	外部からのアクセス制御機能	16
4.1	外部からのアクセス制御機能	16
4.1.1	外部からのアクセスを制限する	16
4.1.2	外部からのアクセスを制限する条件設定	17
4.2	装置自身に対するアクセス制限	18

5	DNS プロキシ／リゾルバ機能	19
5.1	前提条件	19
5.2	トランスポート	20
5.2.1	利用可能なトランスポート	20
5.2.2	優先するトランスポート	20
5.3	DNS プロキシとして待ち受けるアドレスの種類	21
5.3.1	DNS プロキシとして待ち受けるアドレスの種類	21
5.4	DNS サーバが複数存在する場合の選択方法	22
5.4.1	順次サーチ方式による選択	22
5.4.2	任意選択機能	22
	キャッシュ	23
5.5		23
5.5.1	キャッシュ機能	23
5.6	リゾルバ機能	24
5.6.1	対応リソースレコード	24
5.6.2	EDNS0	24
5.6.3	TCP 53 番ポート対応	24
5.6.4	DNSSEC (参考)	25
6	宅内ネットワークへの情報配布機能	26
6.1	アドレス／プレフィックス情報の配布	26
6.1.1	RA による配布	26
6.1.2	DHCPv6 による配布	27
6.2	サーバ情報の配布	28
6.2.1	RA による配布	28
6.2.2	DHCPv6 による配布	28
6.2.3	DHCPv6 リレー機能	29
7	ルーティング／マルチキャスト機能	30
7.1	使用していないアドレス／ネットワークへの通信の扱い	30
7.2	経路情報・拡張ヘッダ	31
7.2.1	WAN 側における経路制御	31
7.2.2	LAN 側への経路制御	32
7.2.3	拡張ヘッダ	33
7.3	IPv6 マルチキャスト	34
7.3.1	IPv6 マルチキャスト接続形態ごとの機能	34

7.3.2	PIM による接続.....	34
7.3.3	MLD プロキシによる接続.....	35
7.3.4	MLD スヌーピング.....	35
8	サービス側の設定手法.....	37
8.1	設定方式.....	37
8.1.1	自動設定.....	37
8.1.2	手動設定.....	39
8.2	設定項目.....	40
8.2.1	アドレス設定.....	40
8.2.2	セキュリティ関連設定.....	40
8.2.3	DNS 設定.....	40
8.2.4	宅内ネットワーク設定.....	41
8.2.5	ルーティング・マルチキャスト設定.....	41
9	おわりに.....	42
9.1	IPv6 家庭用ルータが必要とする機能のまとめ.....	42
9.2	次版に向けた検討項目.....	46
9.2.1	見直し/詳細検討が必要な項目.....	46
9.2.2	未検討項目.....	46
9.3	検討メンバー.....	47
9.4	リファレンス一覧.....	48

1 はじめに

1.1 当該文書の背景と目的

近年、IPv4 アドレスの在庫枯渇問題が取り沙汰され、早急なネットワーク事業者の IPv6 対応が求められている。

このような状況下において、2008 年 9 月に、IPv6 普及・高度化推進協議会¹の IPv4/IPv6 共存ワーキンググループ (WG) は、「IPv6 家庭用ルーターサブワーキンググループ (SWG)」²を設置した。この SWG では、インターネット利用者がスムーズに IPv6 環境の利用が可能になるように、ISP による IPv6 接続サービスの提供に必要な「家庭用ルータ」における最小限の共通機能をまとめることを目的としている。ここで言う「最小限の共通機能」に関しては、インターネット利用者の視点をはじめ、家庭用ルータ開発ベンダーおよび IPv6 接続サービス提供者の視点にて議論を行った。

本文章は、「IPv6 家庭用ルーターSWG」にて検討を進めてきた内容を、具体的なアウトプット「IPv6 家庭用ルータガイドライン」としてまとめたものである。またこの内容は、家庭用ルータの実装および ISP における IPv6 接続サービスの仕様に対して強制力を持つものではない。

¹ IPv6 普及・高度化推進協議会: <http://www.v6pc.jp/>

² IPv6 家庭用ルーターSWG: <http://www.v6pc.jp/jp/wg/coexistenceWG/v6hgw-swg.phtml>

1.2 本ガイドラインの想定環境と対象とする読者

本ガイドラインで扱うインターネット接続形態は、家庭用ルータ（ユーザ宅内に設置される小型ルータ）を介して家庭内ネットワークを ISP に接続する環境を想定している。また、IPv6 接続サービスはデュアルスタック環境を想定しており、IPv4 機器の通信は IPv4 で行うことを前提として検討する。さらに、IPv4 アドレス枯渇により LSN（Large Scale NAT）などの IPv4 環境の変化に伴い必要となる機能に関しても対象外としている。

下記に、対象外としたネットワーク例を列挙する。

<対象外のネットワーク環境>

- ・企業ネットワーク
- ・ホットスポット等の公共のネットワーク
- ・クライアント端末が直接接続するネットワーク
- ・多段 NAT 等のミドルボックスを併用したネットワーク

また、想定する IPv6 家庭用ルータとしては、拡張性を十分に考慮した上で、最低限必要とされる機能を有するものとなる。

本ガイドラインは、特に、下記の方々に読まれることを旨として記述している。

- ・ 家庭用ルータを設計・開発する方々
- ・ ISP など、インターネット接続性を提供するサービスを提供されている方々

1.3 記述用語と表記方法に関して

本ガイドラインにて記述されている用語は、IAJapan (財団法人日本インターネット協会) においてまとめている、「IPv6 関連用語集」³に従っている。各用語に関する解説は用語集を参照して頂きたい。また、上記に記述されていない用語に関して以下に解説する。

表 1-1 本ガイドラインで扱う用語解説

用語	説明
ULA (RFC 4193)	Unique Local IPv6 Unicast Addresses。サイト内など、ローカル通信で利用するために制定された IPv6 ユニキャストアドレス。IPv4 のプライベートアドレス (RFC 1918) に相当するが、プレフィックスの一部をランダムに生成することが規定されており、アドレスの一意性を高めている。
TR-069	Technical Report 069。BroadBand Forum の定める技術仕様の 1 つであり、いわゆる CPE 機器を遠隔管理するためのアプリケーション層のプロトコルを定義している。具体的には、SOAP/HTTP により CPE と自動設定サーバ (ACS : Auto Configuration Server) との間の通信を定義している[44]。
UPnP	Universal Plug and Play。UPnP Forum の定める技術仕様の総称であり、機器を接続しただけでネットワークに参加することを可能とすることを目的としている。具体的には、機器の持つ機能の記述や動作の制御などの情報を XML で記述し、それを SOAP/HTTP 等の既存プロトコルにより通信する[45]。

IPv4 アドレスと IPv6 アドレス双方を持つ表現として、「IPv4/IPv6」という表現方法を用いている。また、IPv6 アドレスのプレフィックスサイズを比較する表現には「(プレフィックス長が) 短い／長い」を用いており、その定義を以下に明示する。

- ・ /35 より短い : プレフィックス長が 35 ビットより短いことを意味する 例) /32
プレフィックスサイズとしてはその空間が広いことを示す
- ・ /35 より長い : プレフィックス長が 35 ビットより長いことを意味する 例) /64
プレフィックスサイズとしてはその空間が狭いことを示す

³ IPv6 関連用語集 (IAJapan) : http://www.iajapan.org/ipv6/v6term/glossary_01.html

1.4 ガイドライン作成にあたり

本節では、本ガイドラインにて取り上げる家庭用ルータの機能に関する概要をまとめ、本ガイドラインの構成を解説する。

1.4.1 ISP が提供する基本機能

本ガイドラインが想定する ISP による IPv6 接続サービスの形態は、図 1-1 に示すように大きく 4 つの機能に分けることができる。

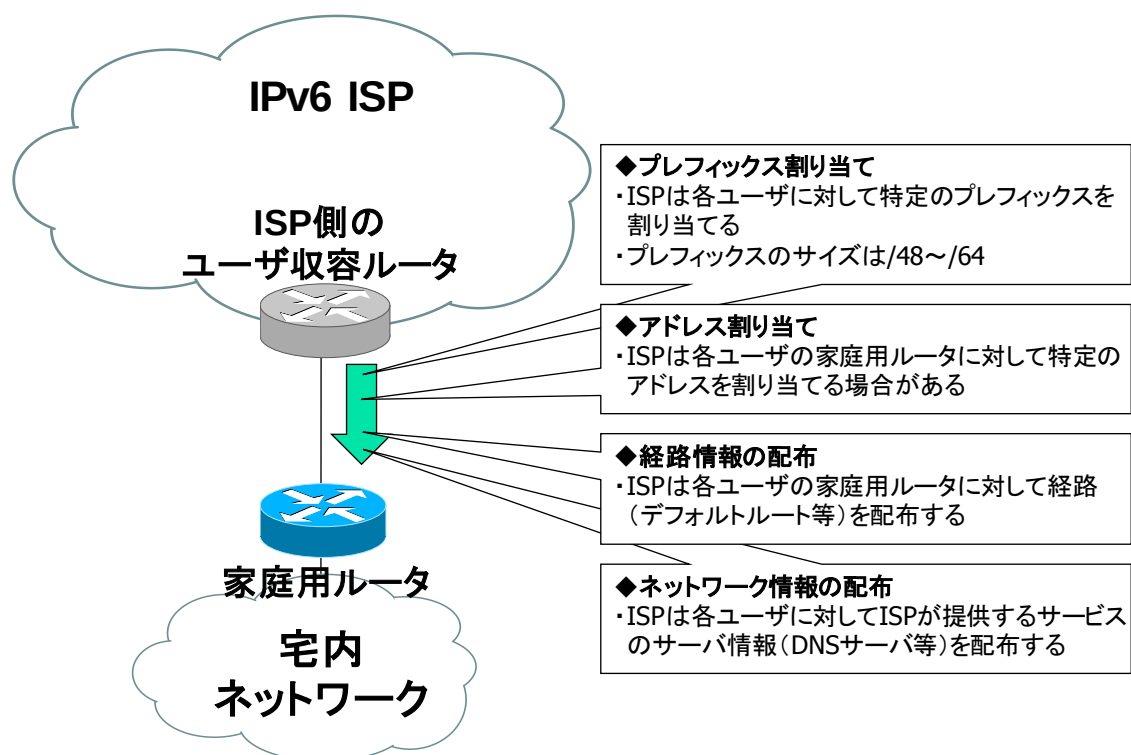


図 1-1 ISP のサービス形態概略

・プレフィックス割り当て

IPv6 では、IPv4 における接続サービスと異なり、プレフィックス単位でのアドレス割り当てが必要となる。割り当てプレフィックスサイズはサービスにより異なるが、概ねプレフィックス長が/64 から/48 の間と想定される[8]。

・アドレス割り当て

IPv6 の家庭用ルータの WAN 側インターフェースに対して、ISP 側から回線の死活監視などの目的でアドレスを付与する場合は考えられる。

・経路情報の配布

基本的に IPv4 の場合と同様に、ISP からはデフォルトルートがユーザ側に設定される。

- ・ネットワーク情報の配布

ISP がユーザに対して提供するサーバ情報は、静的な文字情報として伝えられるだけでなく、DHCP などによって配布されることが一般的である。

上記のような仕組みが想定される環境を前提に、家庭用ルータが実装する必要がある機能の整理に努めた。

1.4.2 宅内ネットワークの概略

家庭用ルータでは、前述した ISP 側から付与される各ネットワーク情報を宅内ネットワークに再配布および割り当てる必要がある。本ガイドラインでは、宅内ネットワークへのネットワーク設定に関して次のルータ機能を取り上げている。

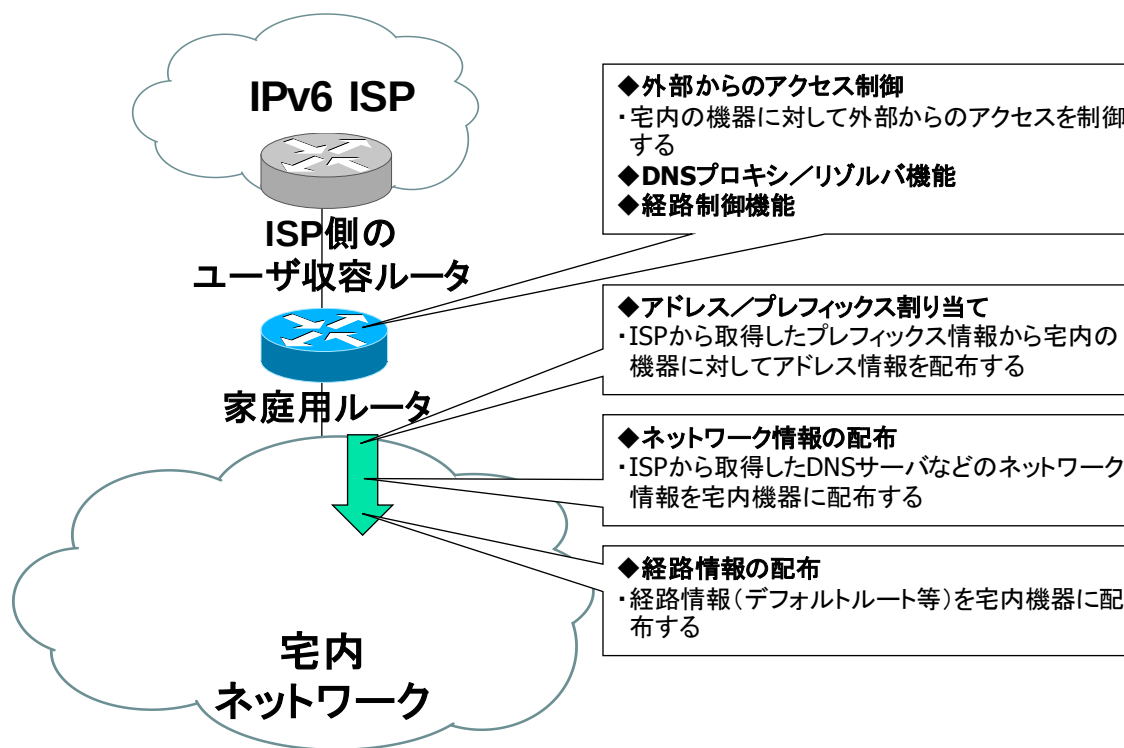


図 1-2 宅内ネットワークの設定概要

- ・アドレス/プレフィックスの割り当て

ISP 側から割り当てられたアドレス空間を用い、宅内の LAN に対してプレフィックスやアドレスをクライアント端末に割り当てる機能。動的・静的など様々な手法が考えられる。

- ・ネットワーク情報の配布

DNS サーバなどの情報をクライアント端末に配布する機能。標準化されているいくつかの手法が存在する。

- ・経路情報の配布

クライアント端末に対する経路情報としてはデフォルトルートのみを配布する形が一般的と考えられる。

- ・外部からのアクセス制御

IPv6 でも、IPv4 の場合と同様に宅内への通信制御が必要とされる。特に、IPv6 ではグローバルアドレスで宅内ネットワークが構成される可能性が高いため、外部からのアクセス制御は重要と考えられる。

- ・DNS プロキシ／リゾルバ機能

クライアント端末から直接 ISP の提供する DNS サーバを利用することも可能であるが、IPv4 の場合と同じように DNS 機能を有する場合が想定される。

- ・経路制御

IPv4 の場合と異なり、割り当てアドレス空間が広く、未使用空間が出現することへの正しい実装が求められる。また、提供サービスに依存するが、マルチキャストに対する実装が必要になるケースも想定される。

1.4.3 家庭用ルータに求められる機能

1.4.1 節および 1.4.2 節で挙げた各サービス・機能を前提として、本ガイドラインで取り上げる家庭用ルータに求められる機能を表 1-2 のように整理した。

表 1-2 家庭用ルータに求められる機能概要と掲載章番号一覧

大項目	中項目	章番号
アドレス／プレフィックス設定機能	プレフィックス情報の受信	3.1
	アドレス／プレフィックス情報の配布	3.3, 5.3, 6.1
	WAN 側アドレス設定	3.2, 8.1.1
経路制御機能	経路設定	7.2
	不到達アドレス／プレフィックス制御	7.1
	マルチキャスト機能	7.3
アクセス制御機能	ルータ自身へのアクセス制御	4.2
	宅内ネットワークへのアクセス制御	4.1, 7.2.3
	制御ルール設定	4.1(4.1.2)
サーバ機能	DNS プロキシ機能	5.2, 5.3, 5.4, 5.5
	DNS リゾルバ機能	5.6
	ネットワーク情報の取得と配布	6.2, 8.2.4.2, 8.2.4.3
	ルータ自身の設定機能	8.1, 8.2

本ガイドラインでは、これらの機能を以下の章立てでまとめている。

第2章では、IPv6 接続サービスを提供する ISP に対して接続する際に必要となる機能の整理を行う。ただし、2008 年度時点において、ISP が提供する IPv6 接続サービスの形態が不明確であることから、この版では、IPv6 接続サービス形態の整理のみとしている。

第3章では、ISP から割り当てられるアドレス空間の利用に焦点を当てて機能を整理する。具体的に利用するプロトコルに関しては第6章および第8章にて記載する。

第4章では、外部からのアクセス制御に関して必要となる機能をまとめる。IPv6 ではエンドツーエンド接続が可能になるため、本機能の重要性も増すと考えられる。

第5章では、DNS サービス関連の機能をまとめる。IPv4 の場合と同様に DNS プロキシ等を実装する際に注意が必要な点などを整理する。

第6章では、宅内ネットワーク設定の視点から整理を行う。

第7章では、経路制御に関する機能をまとめており、マルチキャスト利用についても触れる。

第8章では、IPv6 接続サービスを提供する ISP 側から必要となる機能としての整理を行う。大半の機能がここまでにまとめた機能となるためポイントを記載している。

以上のように家庭用ルータに求められる機能を整理し、詳細機能を表 1-3 に挙げる項目に整理して必要性をまとめている。

表 1-3 詳細機能（小項目）の記載項目説明

項目	意味
前提：	本要件に対する前提条件を記載
要件：	家庭用ルータに必要な詳細機能の概要を記載
必要度：	取りあげた要件の必要性を"必須/推奨/オプション"で表現 必須（MUST）：必ず必要とされる機能 推奨（SHOULD）：実装されていることが推奨される機能 オプション（MAY）：実装はルータとしての付加価値的なもの（サービス依存な機能など）であるため任意でよい機能
理由：	要件として挙げた機能の必要度を導き出した事由を記載
備考：	必要度を決める際に議論された経過情報などを記載

2 ISP への接続機能

この章では、ルータが ISP のサービスを利用する際に必要となる接続機能に関してまとめることを目的としている。ただし、本ガイドライン検討時点において、ISP による IPv6 ネットワークのリーチャビリティの提供手法が不明確であることから、どのような接続形態が存在するのかについての整理のみとしている。したがって、この章では、ルータに必要とされる機能定義は行っていない。また、各接続形態における認証技術に関しても今回は対象外としている。

2.1 ネイティブ接続

2.1.1 接続形態

要件：家庭用ルータでトンネル等を終端しないネイティブ接続で IPv6 ネットワークのリーチャビリティを提供する。

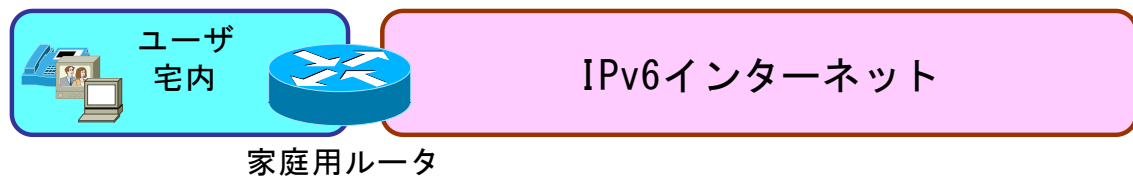


図 2-1 ネイティブ接続

2.2 PPPoE/PPPoA

2.2.1 接続形態

要件:PPP 上でユーザ宅内へ IPv6 ネットワークのリーチャビリティを提供する[1][2][3]。

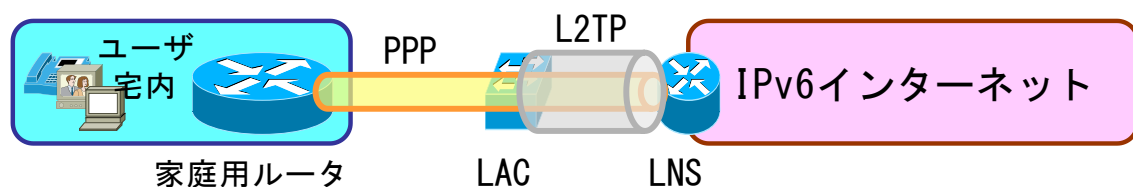


図 2-2 PPPoE/PPPoA 接続

2.3 IP ベースのトンネル (IPv6 over IPv4・IPv6 over IPv6 など)

2.3.1 接続形態

要件: IP でカプセリングし、ユーザ宅内へ IPv6 ネットワークのリーチャビリティを提供する[4][5][6][7]。

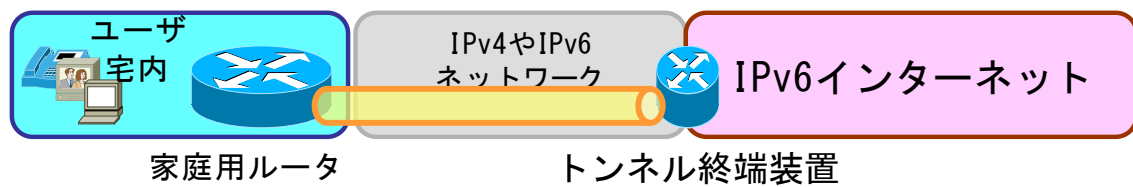


図 2-3 IP ベースのトンネル接続

3 アドレス割り当て手法

この章では、ルータの WAN 側、LAN 側および LAN 側セグメントに接続される端末への各種アドレスの割り当て手法について述べる。

3.1 プレフィックス割り当て

本節では、サービス提供者がユーザにプレフィックスを割り当てる際に、ルータに求められる要求条件について記述する。

3.1.1 宅内ネットワークへ配布するプレフィックス情報

要件：接続先 ISP から DHCPv6-PD にて取得できること。

必要度：必須 (MUST)

理由：DHCPv6-PD は、IPv6 プレフィックス割り当てを自動的に実施するための標準プロトコルである。ユーザ手入力による設定ミスをなくすためにも、実装は必須とする。

要件：手動設定できること。

必要度：必須 (MUST)

理由：接続先 ISP が DHCPv6-PD によるプレフィックス配布に対応していない場合の対処のために、必須とする。

3.1.2 宅内ネットワークへの割り当てプレフィックスサイズ

要件：/48～/64 の幅でサービス提供者が割り当てたプレフィックスを受信できること。

必要度：必須 (MUST)

理由：「JPNIC における IPv6 アドレス割り振りおよび割り当てポリシー」[8]において、エンドサイトには基本的に/48～/64 の割り当てを実施することが求められているためこの範囲のプレフィックスを扱えることを必須とする。

備考：

- 無線セグメント／有線セグメントの分離や、DMZ の設置などを考慮した場合には、複数セグメント（/64 より短いプレフィックス長）の分配が望ましいと考えるが、割り当てプレフィックスサイズはサービス提供者が決定する部分である。
- SOHO 等を考えた場合、/48 より短いプレフィックス長が割り当てられる可能性もある。

3.1.3 プレフィックスの割り当て

サービス提供者がユーザに配布するプレフィックスについては、固定的に割り当てるか、時間経過により変更するかが考えられる。

要件：ユーザに配布するプレフィックスを固定とすること。

必要度：推奨（SHOULD）

理由：可変なプレフィックス割り当てを実現するためには、ノードの要件等多くの制限事項がある（プレフィックス変更時のリナンバリング、変更時に継続している通信維持をどこまで担保するか等）。現状では、ユーザネットワークの安定動作性を考慮した場合、固定プレフィックス割り当ての方が可変より望ましいため、固定割り当てを推奨とする。

備考：基本固定とした場合でも、プライバシー隠蔽等を考慮し、ユーザ側からのプレフィックス変更要求には答えられるようにすべきである。

要件：ユーザに配布するプレフィックスが時間の経過により変更すること。

必要度：オプション（MAY）

理由：ユーザの通信プライバシーを担保するために必要という意見がある。また、現状、IPv4 では非固定割り当てが主流であり、同等の機能をユーザから求められる可能性がある。しかしながら、動作中のユーザ宅内機器がプレフィックス変更に従従できるかという問題や、プレフィックス切り替え時に家庭用ルータの動作が複雑になることから、現状、オプション扱いとする。

備考：

- プレフィックスを非固定とした場合には、ルータがプレフィックス変更を検知できること（以前割り当てられたプレフィックスを記憶しておき、変更があった場合には適切に動作すること）や、通信中のセッションの扱い、変更時にユーザ宅内機器のリナンバリングに対する対応の考慮が必要となる（3.3.3 節も参照）。
- アドレスを固定にするか、時間の経過により変更するかはサービス提供者のサービス次第であるが、それぞれに利点・考慮点が存在する（表 3-1 参照）。

表 3-1 割り当てアドレス固定／非固定による影響

	カテゴリ	具体的なイメージ	対象	セキュリティ/プライバシー
固定 ↑	ISP との契約を解除する都度アドレスが変わる	ユーザが ISP-A から ISP-B に契約を変更する場合	運用管理が容易	攻撃の対象になっていない ユーザは固定アドレスのメリットを享受 プライバシー問題あり
	場所が変わる都度アドレスが変わる	ユーザが引っ越しをする場合		
	オペレーション都合の都度アドレスが変わる	ISP バックボーン的设计変更等数年に一回程度		
非固定 ↓	ユーザの申告の都度アドレスが変わる	DoS 攻撃を受けたのでアドレスを変更したい場合	宅内すべてのアドレスが変わってしまう可能性がある ・リンクダウン時 ・家庭用ルータ交換時	攻撃の対象になっているユーザは攻撃を回避できる
	接続の都度アドレスが変わる	家庭用ルータもしくは PC を起動する度にアドレスが変わる (ユーザは気付かない程度)		

3.2 WAN 側アドレス

本節では、家庭用ルータの WAN 側（サービス提供者との間のリンク）に対するアドレス付与について述べる。

3.2.1 グローバルアドレスの付与

要件：家庭用ルータの WAN 側にも、グローバルアドレスを付与できること。付与するアドレスは、ユーザに割り当てたアドレス空間からではなく、サービス提供者が保有する別空間からとする。

必要度：推奨（SHOULD）

理由：サービス提供者の、ユーザ宅の死活管理を実施できるようにしたいという要望、および、サービス提供者がルータ上にサービスを実装しやすくするために家庭用ルータの WAN 側にアドレスを付与できるようにする。

備考：

- グローバルアドレスを付与せずに、リンクローカルアドレスだけでの運用も考えられる。
- サービス提供者が利用することを想定しているため、ユーザ割り当て空間からではなく、サービス提供者が別空間から割り当てることが望ましい。しかしながら、

サービス提供者が管理するアドレスを付与した場合、ユーザの管理外（認識外）となることが想定される。このアドレスが適切に管理されない場合、ユーザの想定していないアドレスに対する不正なアクセスを許す等のセキュリティ上の問題が発生する可能性がある。

3.2.1.1 グローバルアドレスの付与方法（自動）

前提：WAN 側にグローバルアドレスを付与する場合。

要件：WAN 側インターフェースへのグローバルアドレスを自動的に付与できること。

必要度：必須（MUST）

理由：ユーザの手を介さない自動設定を実現するために、必須とする。

下記のうちいずれかの方式を必須とする。

[a] SLAAC（Stateless Address Auto Configuration）

[b] DHCPv6

備考：

- SLAAC を利用する際には、別途、設定されたアドレスを通知する仕組み（DDNS 等）と併用しないと、サービス提供者が付与されたアドレスを知ることができない。
- 方式選択にあたっては、技術動向（2009 年 4 月現在、DHCPv6 ではプレフィックス長配布に別途ルータ広告／プレフィックスオプションとの併用が必要であることなど）、IPv6 のグローバルユニキャストアドレスにおいては、インターフェース識別子が 64 ビット長であると規定されていること[46]、および他要件（WAN 側に割り当てるアドレスプレフィックスサイズと、発生しうる問題（7.1 節））との兼ね合いも考慮が必要。

3.2.1.2 グローバルアドレスの付与方法（手動）

前提：WAN 側にグローバルアドレスを付与する場合。

要件：WAN 側インターフェースへのグローバルアドレスを手動で付与できること。

必要度：必須（MUST）

理由：自動設定が前提であるが、手動設定も必要であるため。

3.3 LAN 側アドレス

本節では、家庭用ルータの LAN 側（ユーザ宅内ネットワークとの間のリンク）に対するアドレス付与について述べる。

3.3.1 プレフィックスの再配布

要件:ISP から DHCPv6-PD で受け取ったプレフィックスを基に/64 のプレフィックスを生成しそれを LAN 側に再配布できること。

必要度：必須（MUST）

理由：ISP がユーザ宅に配布したプレフィックスを、自動的に宅内の機器に再配布する手段が必須であるため。

備考：

- 再配布するプロトコルは 6.1 節を参照。
- /64 より広いプレフィックスを DHCPv6-PD で受け取った場合に/64 プレフィックスの決定方法は規定しない。例えば DHCPv6-PD で/48 のプレフィックスを受け取った場合、LAN 側に再配布する際は 49～64 ビットの範囲で値を決める必要がある。その決め方は実装依存とし、本文書では規定しない。

3.3.2 複数プレフィックスの受信

要件：ひとつのもしくは複数の ISP から複数のプレフィックスを DHCPv6-PD で受け取った場合、どのプレフィックスを LAN 側に再配布するか選択できること。

必要度：オプション（MAY）

理由：上流 ISP が複数存在する環境や、ISP が複数の別々のプレフィックスを配布する環境に対応するための機能であるが、複数の上流がある環境は家庭用ルータとしては特殊であると考えられるため、オプション扱いとする。

備考：

- 固定プレフィックスと動的プレフィックスをそれぞれ 1 つずつ配布するような接続サービスが考えられる。
- 固定プレフィックスと動的プレフィックスにはそれぞれの利点があり、ユーザが選択できることが望ましい。
- 片方のプレフィックスを選択した場合に特定のネットワークにアクセスできなくなるようなケースも考えられるが、そのようなプレフィックスについては本文書では規定しない。

3.3.3 配布プレフィックスの変化

前提：ユーザ割り当てプレフィックスが時間の経過により変化するサービスの場合。

要件：WAN 側回線の再接続により、ISP が DHCPv6-PD にて配布するプレフィックスが変化した場合に、LAN 側に配布するプレフィックスをを適切に変更できること。

必要度：推奨（SHOULD）

理由：ユーザ割り当てプレフィックスを時間の経過により変化させるサービスを選択した場合、サービス提供者都合によるプレフィックスの変更が、ユーザネットワークにおける通信に与える影響を最小限に抑える必要があるが、プレフィックスの切り替えについて、家庭内機器の対応状況も不明であるため、推奨機能とする。

備考：具体的な方式は規定しない（3.1.3 節および 6.1.2 節も参照）。

4 外部からのアクセス制御機能

本章では、ユーザ宅内ネットワークを保護するために最低限必要と考えるアクセス制御機構について述べる。前提条件として、IPv6 の家庭用ルータにおいても、IPv4 の場合にとられていたセキュリティ機能（NAT/NAPT により外部ネットワークから直接宅内ネットワークへの到達性が失われていた点も含む）は必要とする。

4.1 外部からのアクセス制御機能

4.1.1 外部からのアクセスを制限する

4.1.1.1 アクセス制限の基本設定

要件：内部（LAN 側）から外部（WAN 側）への通信は通過させ、外部から内部への通信は遮断するアクセス制限が行えること。

必要度：必須（MUST）

理由：現在の IPv4 家庭用ルータの初期動作と同等のアクセス制御は必須と考えるため。

備考：デフォルトの挙動では外部から内部への通信を遮断としているが、設定により通信可能にできることも同時に必要である（4.1.2 節も参照のこと）。

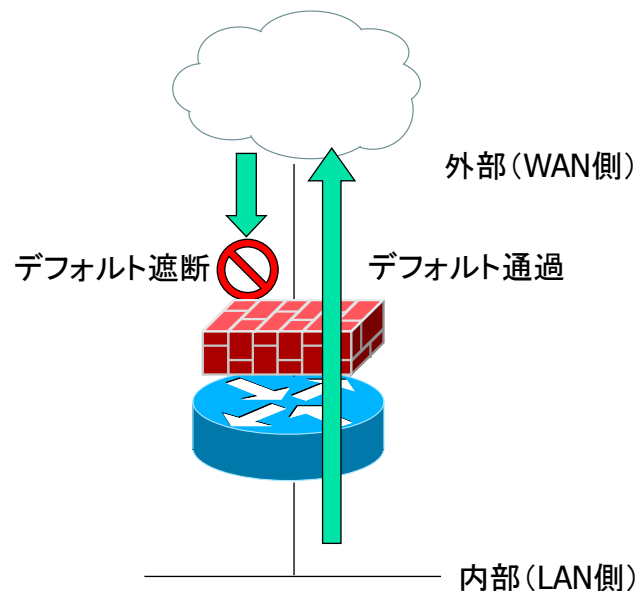


図 4-1 外部からのアクセス制御機能

4.1.1.2 アクセス制限の詳細設定

要件：静的フィルタによりアクセスを制限できること。

- 内部から外部へは、デフォルトで通過させる。
- TCP は外部から内部への SYN をデフォルトで遮断する。
- UDP は外部から内部への特定プロトコルのみ通過させ、その他のプロトコルはデフォルトで遮断する。

特定プロトコル：DNS、その他サービス依存で必須となるプロトコル（TV、電話など）。

- ICMPv6 は外部から内部へ必須なメッセージ[9]のみ通過させ、その他はデフォルトで遮断する。

必要度：必須（MUST）

理由：最低限必要だと思われるネットワークセキュリティレベルを IPv6 でも維持することは必須であるため。

備考：

- 内側からのトラフィックに対してセキュリティの観点などから制御が必要な場合もある。例えば、サービス提供者が割り当てたアドレス以外を始点アドレスにもつ通信を遮断する場合などが挙げられる。
- アクセス制御を実施する際には、フラグメントされたパケットの再構成を考慮して実装する必要がある。

4.1.1.3 アクセス制限の拡張機能

要件：動的フィルタ（SPI）によりアクセスを制限できること。

- 内部から外部へは、デフォルトで通過させる。
- 内部から外部への通信があったコネクションを記憶し、このコネクションについては外部から内部へ通過させる。

必要度：推奨（SHOULD）

理由：

- 現行の IPv4 NAT 相当のセキュリティレベルを IPv6 でも維持するために重要な機能であるため、推奨とする。
- SPI に関しては、RFC 4787 の記述も参照のこと[47]。

4.1.2 外部からのアクセスを制限する条件設定

要件：通過、遮断する条件を設定できること。

必要度：必須（MUST）

機能	必要度
IPv6 始点/終点アドレスでアクセスを制限できること	必須 (MUST)
次ヘッダ (プロトコル) を認識できること (7.2.3 節の参照)	必須 (MUST)
プロトコル種別 (拡張ヘッダ種別等) でアクセスを制限できること	推奨 (SHOULD)
次ヘッダチェーンを辿ること	必須 (MUST)
ICMP の Type と Code でアクセスを制限できること[9]	推奨 (SHOULD)
TCP/UDP の始点/終点ポート番号でアクセスを制限できること	必須 (MUST)

理由：現行の IPv4 ネットワークのセキュリティレベルを IPv6 でも維持するため[10]。

備考：次ヘッダチェーンを辿る際に、どの程度の深さまで辿る必要があるかは、実装に依存する（現状、明確な規定はない）。

4.2 装置自身に対するアクセス制限

要件：装置自身への通信に対するアクセス制御が可能であること。

必要度：必須 (MUST)

理由：装置自身が IPv6 ホストとして提供するサービス機能について、セキュリティ確保が必要なため。

5 DNS プロキシ／リゾルバ機能

本節では、既存 IPv4 対応家庭用ルータの多くに具備されている DNS プロキシ機能及び、リゾルバ機能等その他の DNS 関連機能について述べる。[14]も参照のこと。

5.1 前提条件

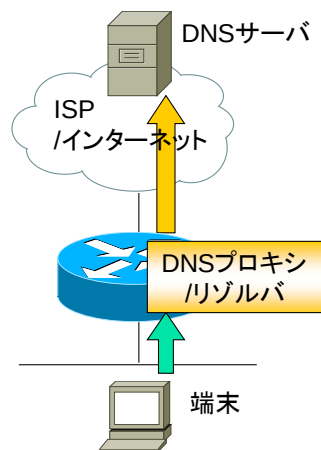


図 5-1 DNS プロキシ／リゾルバ機能の概念図

DNS プロキシ／リゾルバが必要な理由

実装した場合のメリット

DNS サーバの負荷軽減（キャッシュを使用した場合）

上位接続がない環境において、クライアントに対して DNS サーバの設定が可能。

ローカルの名前解決ができる。

実装しなかった場合のデメリット

端末側における DNS サーバの誤選択により、遅延や通信不可等の問題が発生する可能性がある。

Web-GUI へのアクセスに FQDN ではなく、IP アドレスを直接入力する必要がある（ユーザの利便性低下）。※IPv6 アドレスの入力は困難

`http://web.setup/` → `http://[2001:db8::1]/`

DNS プロキシ／リゾルバ機能を実装する場合の前提条件

原則は端末からの要求を透過的に扱うこと。

トランスレータや ALG 等の変換処理が入る場合、この機能はトランスレータや ALG の機能領域となる為、今回は検討対象外とした。

DNS 側の実装により、上記の変換処理が入る場合、端末が意図しない問い合わせ結果を得ることになるリスクがある為、個別検討が必要である。

DNS リゾルバ部分は IPv4 および IPv6 に関わらず考慮すべき事項として記述している。

5.2 トランスポート

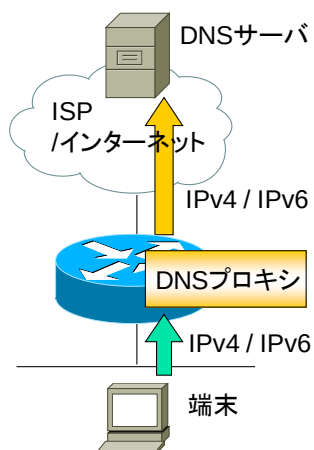


図 5-2 利用トランスポートの選択

5.2.1 利用可能なトランスポート

要件：DNS プロキシの上位側（ISP の DNS サーバ側）は、IPv6 トランスポートと IPv4 トランスポートの両方が利用可能であること。

必要度：必須（MUST）

理由：ISP などから指定される DNS サーバアドレスが IPv4・IPv6 いずれの場合であっても対応可能とするため。

5.2.2 優先するトランスポート

要件：端末からの DNS 要求と同一のトランスポートでプロキシ動作を行うこと。

必要度：オプション（MAY）

理由：トランスポートを変更することで、要求端末にて期待する結果が得られない可能性があるため[15]。

備考：同一トランスポートでのプロキシ動作が MUST/SHOULD ではなく MAY である理由は、家庭用ルータ（DNS プロキシ）から先にキャッシュサーバがある場合にはトランスポートを変える必要がある場合があるため。例えば、端末から DNS プロキシへの問い合わせが IPv6 トランスポートであるにもかかわらず、キャッシュサーバが IPv4 トランスポートのみの対応である場合には、DNS プロキシにはトランスポート変更機能が必要である。

同一トランスポートでのプロキシ動作を行う場合、DNS プロキシには端末から要求されたトランスポートを記憶しておく機能が必要である。

IPv4 インターネットでも問い合わせ始点アドレスによって DNS からの回答が異なる運用があるので、トランスポートを合わせても同じ回答を必ずしも得られるわけではないが、確率の面ではトランスポートを合わせておくことを推奨する。

5.3 DNS プロキシとして待ち受けるアドレスの種類

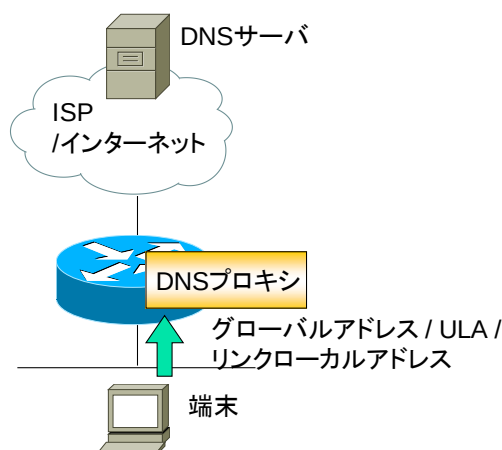


図 5-8 待ち受けるアドレスの種類

5.3.1 DNS プロキシとして待ち受けるアドレスの種類

要件：ユニキャストアドレス（グローバルアドレス、ULA、リンクローカルアドレスの内いずれか）で待ち受け可能であること。

必要度：必須（MUST）

理由：最低限ユニキャストアドレスで待ち受けることができる必要がある。

備考：ULA で待ち受ける場合、DNS プロキシにはあらかじめ使用する ULA を定義しておく必要がある。尚、ULA が LAN 上で既に使用されていた場合は衝突しない別の ULA を生成する仕組みが必要である。

- DNS プロキシが ULA でクエリーを待ち受ける場合、外部に対してはインターフェースとして見せず、内部側からのみに応答できる実装になっていてもよい。
- DNS プロキシがグローバルアドレスでクエリーを待ち受ける場合、上位回線の切断時あるいはセットアップ未完了時など、DNS プロキシにグローバルアドレスが付与されていない状態が存在することが考えられる。この時、DNS プロキシにはクエリーのパケットが届かなくなるため注意が必要である。
また、DNS の増幅攻撃の要因となる DNS オープンリゾルバとならないように、WAN 側からのクエリーを受け付けないなどの配慮が必要となる。
- DNS プロキシがリンクローカルアドレスでクエリーを待ち受ける場合、他のセグメントからのクエリーが DNS プロキシに届かなくなる。また、端末リゾルバでリ

ンクローカルアドレスが指定できないなどの問題がある可能性があるため注意が必要である。

なお、mDNS (RFC 4795) [53]の実装をすることも考えられる。

5.4 DNS サーバが複数存在する場合の選択方法

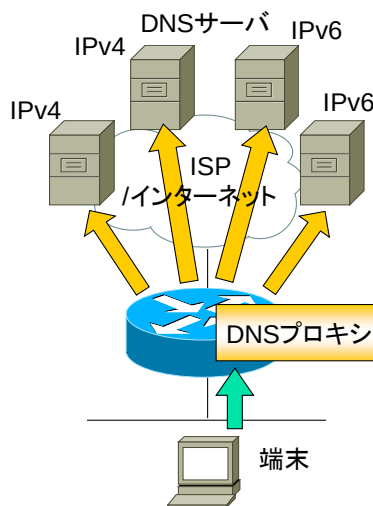


図 5-4 DNS サーバの選択

5.4.1 順次サーチ方式による選択

要件：複数の DNS サーバを利用することができ、順次サーチ方式により DNS の選択を行うこと。

必要度：必須 (MUST)

理由：通信先への到達可能性を高めるため。

5.4.2 任意選択機能

要件：特定のポリシーに応じて DNS サーバを任意に選択するドメイン識別方式などの機能がある場合はその機能で設定されたルールに従うこと。

必要度：オプション (MAY)

理由：ユーザもしくは ISP の意図を優先するため。

備考：

- 順次サーチ方式とドメイン識別方式のいずれも、マルチプレフィックス環境におけるサービスネットワーク毎の DNS サーバ選択問題の解決策にもなり得るが、万能ではない為、その得失を考慮した上で実装すべきである[16][17]。
- IPv6 トランスポートと IPv4 トランスポートの DNS サーバがそれぞれある場合の優先順位に関する規定はない。

- 現状では IPv6 の DNS サーバに不安があるので IPv4 にしたいという意見や、近い将来の IPv6 への移行を考慮するのであれば IPv6 にすべきという意見もあり、意見の分かれるところであり、今後の検討課題である。
- 各種 OS のリゾルバでは IPv6 を優先しているものが多い。
- DNS では、トランスポートに関わらず、同じ回答が返ってくることが前提となっている。

5.5 キャッシュ

5.5.1 キャッシュ機能

要件：端末からの DNS 要求により得られた結果をキャッシュしておき、以降同様の DNS 要求があった場合は、キャッシュ情報を応答すること。

必要度：オプション（MAY）

理由：ISP の DNS サーバの負荷軽減(要求/応答パケットの抑制)が可能であるため。

備考：カミンスキー攻撃[18]など DNS に関する脆弱性が見つかった場合は、迅速な対応が求められることからその得失を判断した上で実装する必要がある。

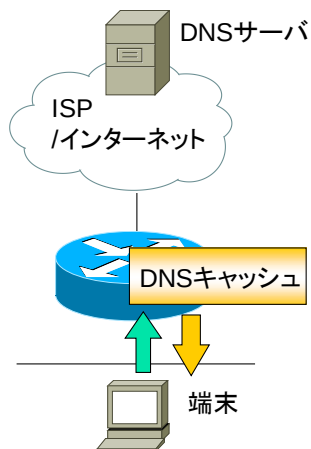


図 5-5 DNS キャッシュ機能

5.6 リゾルバ機能

リゾルバに必要な以下の機能は必ずしも IPv6 特有のものではないが、IPv4 よりも密接に関係している為、家庭用ルータへ実装するスペックとして考慮しておくことを推奨する。

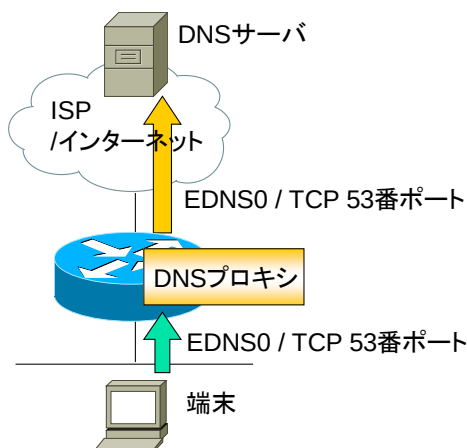


図 5-6 DNS リゾルバ機能

5.6.1 対応リソースレコード

要件：端末からの DNS 要求に対して、リソースレコード（RR）の種別に関わらず全て透過的に処理すること。

必要度：必須（MUST）

理由：RR 種別を限定すると、要求端末にて期待する結果が得られないため。

5.6.2 EDNS0

要件：EDNS0[19]に対応した要求（OPT RR を含む）パケットを透過的に処理し、512byte を超える応答を端末に送信可能なこと。

必要度：必須（MUST）

理由：AAAA や PTR、SPF、SRV、TXT、DNSSEC 等の使用により、DNS 応答パケットが 512byte を超える状況が発生しているため。

5.6.3 TCP 53 番ポート対応

要件：端末が（DNS Header TC=1 受信により[20][21]）TCP 接続にフォールバックして DNS 要求を行った場合においても透過的に処理を行うこと。

UDP 53 番ポートだけでなく、TCP 53 番ポートにおいても待ち受けること。

必要度：必須（MUST）

理由：端末の DNS 要求に関する振る舞いに影響を与えないため。

5.6.4 DNSSEC (参考)

要件：DNSSEC に対応した以下のパケットを透過的もしくは適切に処理可能なこと [22][23][24]。

EDNS0 (OPT RR) DO bit がセットされている。

RRSIG、DNSKEY、DS、NSEC、NSEC3、NSEC3PARAM の RR が使用される。

DNS Header Bit に CD (checking disabled) や AD (authentic data) が使用される。

必要度：オプション (MAY)

理由：端末の DNS 要求に関する振る舞いに影響を与えないため。

備考：現状、Windows XP や Windows Vista には実装されていないため、緊急性は高くないと考えられる。Windows 7 では DNSSEC 実装が予定されており IPsec との併用が想定されているため、IPsec 対応を検討する必要がある可能性がある [25]。家庭用ルータの DNS プロキシ/リゾルバ機能として、署名検証を含む再帰処理を実装するか、あるいは IP アドレスの変換のみの単機能プロキシとして動作するかは実装依存である。

6 宅内ネットワークへの情報配布機能

本章では、家庭用ルータが宅内端末に対して配布するアドレス／プレフィックス情報およびサーバ情報の配布方式について述べる。

6.1 アドレス／プレフィックス情報の配布

6.1.1 RA による配布

要件：宅内ネットワークの端末に割り当てるプレフィックスを RA で通知する機能を持つこと。

必要度：必須（MUST）

理由：IPv6 ルータに必須の機能であるため[28]。

備考：複数プレフィックスを ISP から取得した場合の LAN 内への配布ポリシー等については、3.3.2 節を参照。

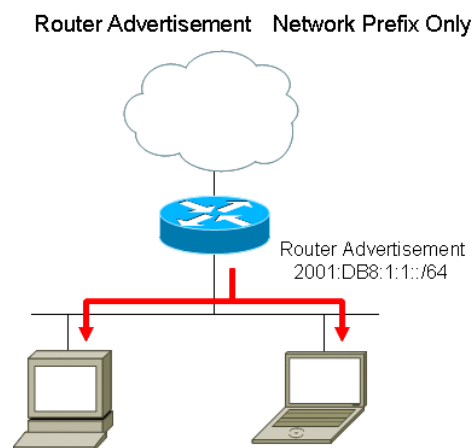


図 6-1 RA によるプレフィックス情報の配布

要件：RA で通知するプレフィックス長は、デフォルトを/64 とすること。

必要度：必須（MUST）

理由：端末におけるステートレスアドレス自動設定では、多くの実装がアドレスの下位 64 ビットをインターフェース ID とするため。

備考：/64 以外のプレフィックス長で配布した場合、LAN 内機器にアドレスが正しく設定されない場合がある点に留意すること。例えば、Windows Vista SP1 では/64 以外のプレフィックスからアドレス生成できない。

SLAAC（RFC 4862）の仕様では、RA の Prefix Information Option 中の prefix length と、ノード自身の持つ interface ID の長さの合計が 128 で無い場合には、

その Prefix Information Option を無視 (MUST) となっている[29][48]。

6.1.2 DHCPv6 による配布

要件：宅内の端末にアドレスを DHCPv6[27]で通知する機能を持つこと。

必要度：オプション (MAY)

理由：宅内ネットワークの端末に特定のアドレスを割り当てたい場合に有効であるため。

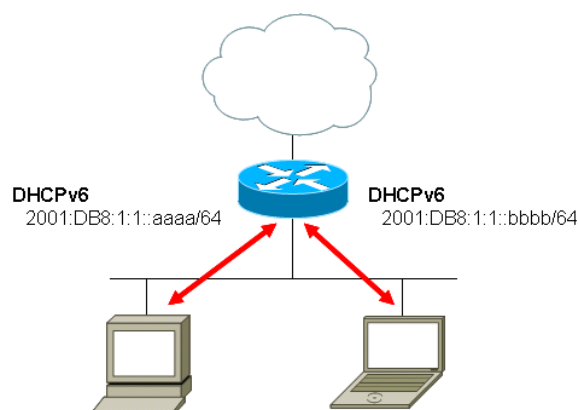


図 6-2 DHCPv6 によるアドレス情報の配布

要件：DHCPv6-PD[30]により宅内機器（ルータ）にプレフィックスを配布する機能を持つこと。機器毎に配布するプレフィックスを指定できる機能を持つこと。

必要度：オプション (MAY)

理由：宅内に複数のルータが存在する場合、当該ルータに接続された端末に割り当てるプレフィックスを配布するため。

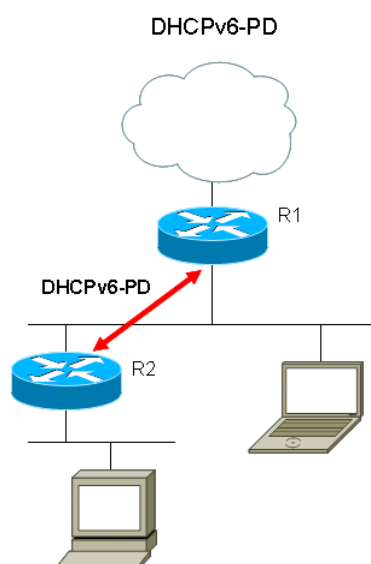


図 6-3 DHCPv6-PD によるプレフィックス情報の配布

6.2 サーバ情報の配布

6.2.1 RA による配布

要件：LAN セグメントに対して、DNS サーバアドレスを配布する機能を持つこと。

必要度：オプション（MAY）

理由：端末において、RA から DNS サーバ情報を取得する実装[31]が想定されるため。

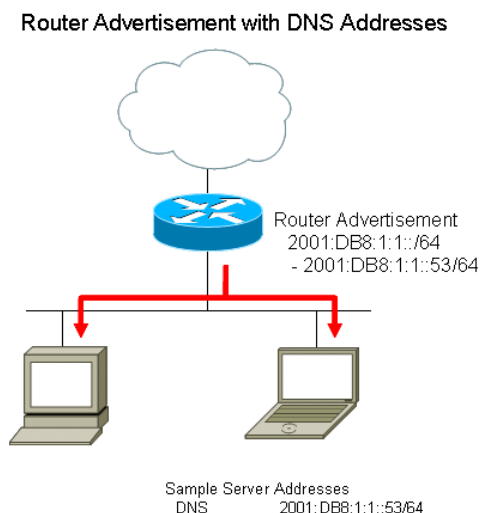


図 6-4 RA によるサーバ情報の配布

6.2.2 DHCPv6 による配布

要件：LAN セグメントに対して、DHCPv6 にて DNS サーバアドレスを配布する機能を持つこと。

必要度：必須（MUST）

理由：端末側の実装として、DHCPv6 により DNS サーバ情報を取得する方法が一般的であるため。

備考：標準化としては、DHCPv6 が Standard Track (RFC 3646) であるのに対し、RA の方は Experimental (RFC 5006) である[32]。

要件：LAN セグメントに対して、DHCPv6 にてその他のサーバアドレス（SIP、NTP など）を配布する機能を持つこと。

必要度：オプション（MAY）

理由：ユーザが各種サービスを利用するためのサーバ情報を、端末に自動設定するため。

備考：どのサーバアドレスを配布するかは ISP のサービス仕様に依存する。

DHCPv6 で配布可能なサーバアドレス：

SIP サーバ[49]、DNS サーバ[50]、NIS サーバ[51]、SNTP サーバ[52]など

DHCPv6 のパラメーター一覧：

<http://www.iana.org/assignments/dhcpv6-parameters/>

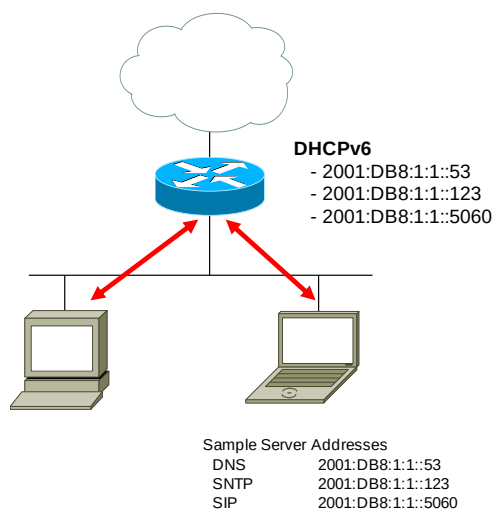


図 6-5 DHCPv6 によるサーバ情報の配布

6.2.3 DHCPv6 リレー機能

要件：DHCPv6 リレー機能を持つこと。

必要度：オプション（MAY）

理由：ISP が宅内ネットワーク設定を管理する場合が想定されるため。

備考：一つの機器にて DHCPv6 サーバ機能と DHCPv6 リレー機能を同時利用しない。

- DHCPv6 リレー機能を有効とした場合、DHCPv6 サーバ機能は無効とする（DHCPv6 サーバ機能を実装した場合）。
- DHCPv6 サーバ機能が有効となっている場合は、DHCPv6 リレー機能は無効とする。

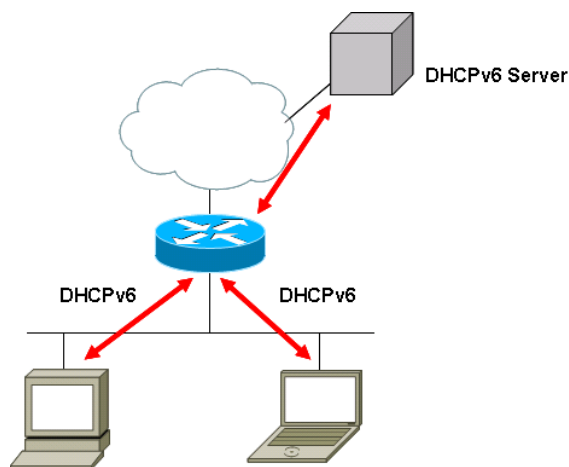


図 6-6 DHCPv6 リレー機能

7 ルーティング／マルチキャスト機能

本章では家庭用ルータに IPv6 をサービスに接続する為に最低限必要なルーティング機能／マルチキャスト機能に関して記述する

7.1 使用していないアドレス／ネットワークへの通信の扱い

前提：DHCPv6-PD によるアドレス割り当てを行うサービス。

要件：割り当てられたプレフィックス宛でのトラフィックを上流にフォワードしない機能を持つこと。

必要度：必須 (MUST)

理由：利用されていないアドレス空間宛でのパケットをデフォルトルートにフォワードすると、TTL が 0 になるまでパケットが家庭用ルータと ISP ルータ間でピンポンしてしまう。このピンポン現象を防ぐため。

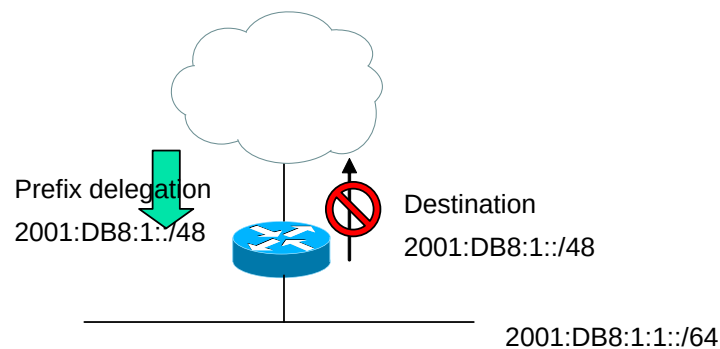


図 7-1 DHCPv6-PD によるアドレス割り当てを行うサービス

前提：WAN 側を Point-to-Point リンクとして接続を行うサービス。

要件：Point-to-Point リンクのルータにて、自インターフェース以外のアドレス宛のパケットを受け取った際には ICMPv6 Destination Unreachable messages, Code 3 (Address unreachable) を送出し、パケットを転送しないこと[33]。

必要度：必須 (MUST)

理由：TTL が 0 になるまでパケットが家庭用ルータと ISP ルータ間でピンポンすることを防ぐため。

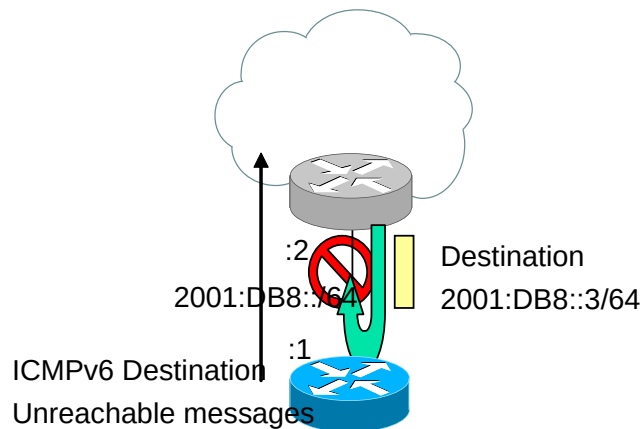


図 7-2 WAN 側を Point-to-point リンクとして接続するサービス

7.2 経路情報・拡張ヘッダ

7.2.1 WAN 側における経路制御

要件：WAN 向けのスタティックルートが設定できること。

必要度：必須 (MUST)

理由：デフォルトルートなどルータにて明示的に設定をする機能が最低限必要なため。

備考：ネクストホップアドレスにリンクローカルアドレスを指定できないと ICMPv6 のリダイレクト機能が有効に働かなくなるため、リンクローカルアドレスも指定できる必要がある。

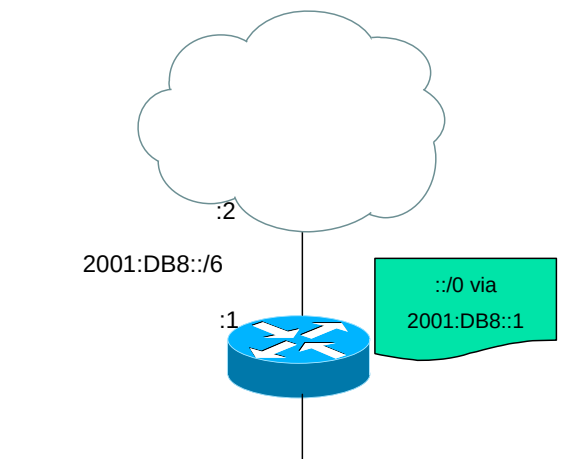


図 7-3 WAN 向けのスタティック経路設定

要件：RA を利用してのデフォルトルートが自動設定できること。

必要度：必須（MUST）

理由：RA による IPv6 アドレス設定を行うサービスへの考慮が必要であるため。

備考：ルータは一般的に RA による経路の自動設定をサポートしないが、家庭用ルータにおいては、ユーザの手を介さないサービス提供者への設定を実施することが重要である[48]。なお、複数の WAN インターフェースが存在し、複数の RA を受信する場合にはどちらのデフォルトルートを優先するか判断する必要があるため注意が必要である。今後検討が必要な項目としている（9.2 節参照）。

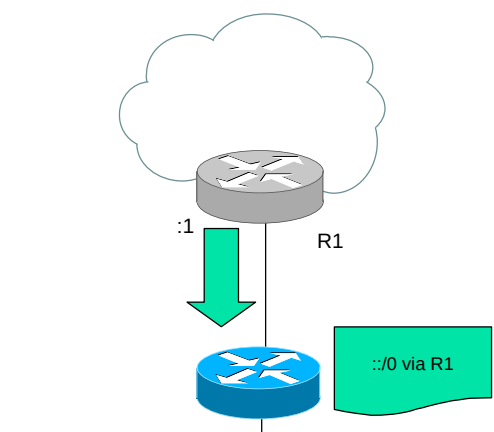


図 7-4 RA を利用したデフォルトルートの自動設定

7.2.2 LAN 側への経路制御

要件：RIPng[34]により LAN 側に経路配布ができること。

必要度：オプション（MAY）

理由：ルータの LAN 側に接続されたネットワークへの経路制御に対する使用が想定されるため。

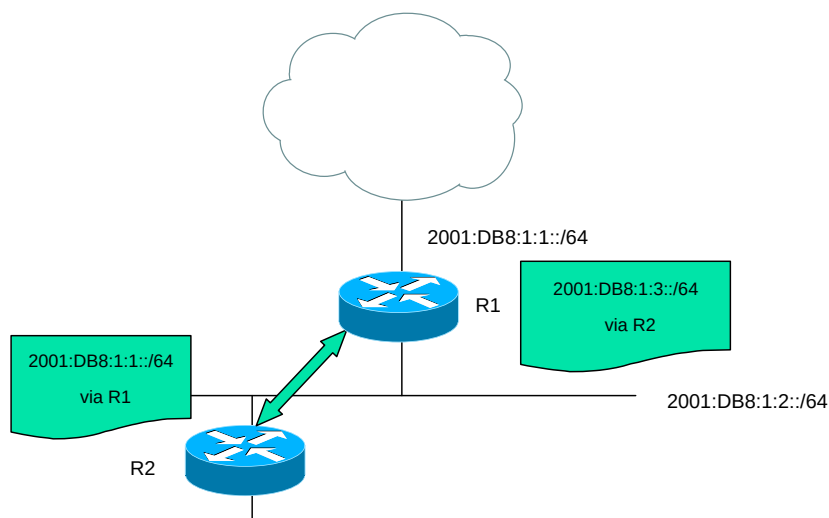


図 7-5 RIPng による経路制御

要件：More-Specific Routes[35]により LAN 側に経路を配布できること。

必要度：オプション（MAY）

理由：ルータの LAN 側に接続されたネットワークへの経路制御に対する使用が想定されるため。

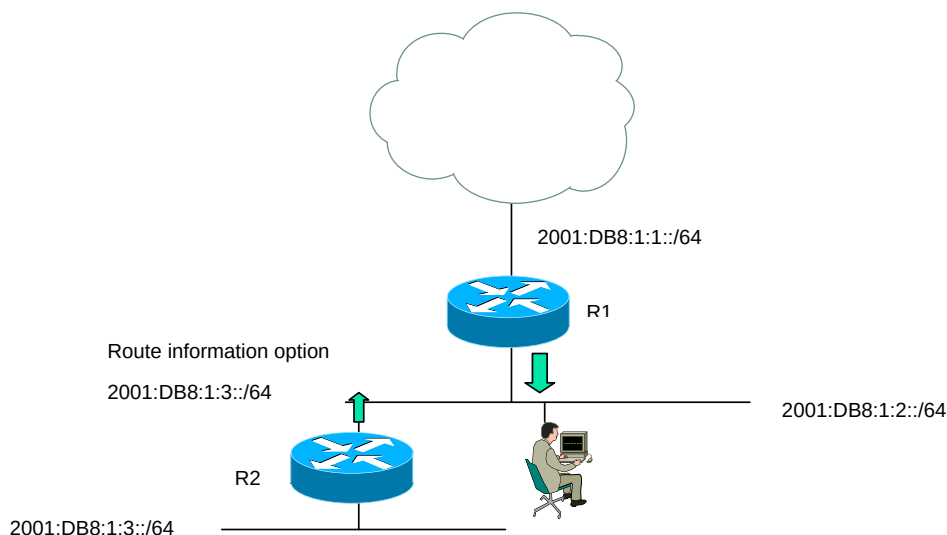


図 7-6 More-Specific Route の利用

7.2.3 拡張ヘッダ

要件：RH0（Type 0 ルーティングヘッダ）の packets 転送を禁止できること。

必要度：必須（MUST）

理由：IPv6 ソースルーティングによる DoS 攻撃への考慮[11]が必要であり、現仕様において利用が禁止されているため。

備考：ルーティングヘッダをすべて禁止する実装ではなく、タイプを正しく見て Type 0 のみ禁止できる必要がある。

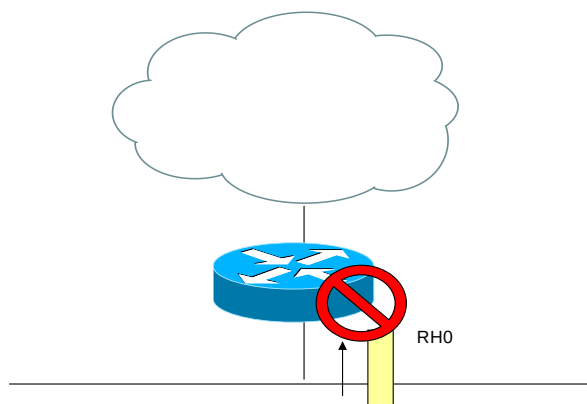


図 7-7 RH0 の packets 転送禁止

7.3 IPv6 マルチキャスト

家庭用ルータでの IPv6 マルチキャスト機能の対応は、ISP によるサービスに大きく依存する機能であるため、機能全体をオプション（MAY）とする。

7.3.1 IPv6 マルチキャスト接続形態ごとの機能

IPv6 マルチキャストサービスへの接続では、家庭用ルータから上位（WAN 側）で使用するプロトコルにより 2 つの接続パターンが考えられる。それぞれの接続形態ごとに必要となる機能を以下に示す。

7.3.2 PIM による接続

PIM を使用して ISP へマルチキャストグループへの参加／離脱を通知する。

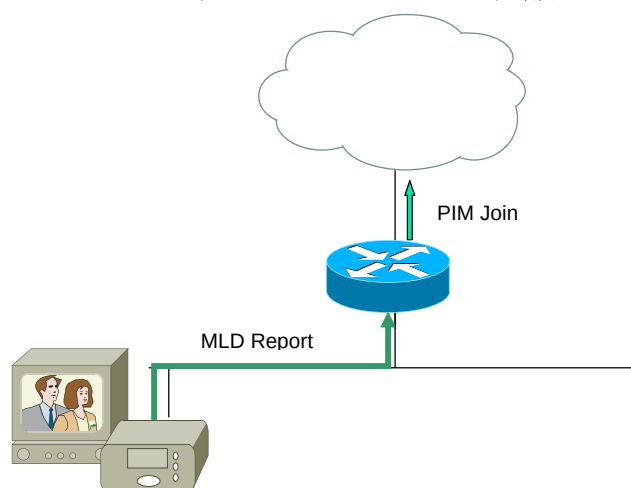


図 7-8 PIM を用いたマルチキャスト接続

前提：PIM を使用してマルチキャストサービスに接続する場合

要件：PIM[36][37][38]によるマルチキャストルーティング機能を持つこと。

必要度：必須（MUST）

理由：WAN 側のプロトコルとして PIM を使用するサービスへ対応するため。

備考：PIM-SM/SSM の仕様には多くのオプション機能が存在しており、機器の実装状況によっては、相互接続性に問題が発生する可能性がある。そのため実装における注意が必要である。今後検討が必要な項目としている（9.2 節参照）。

前提：PIM を使用してマルチキャストサービスに接続する場合

要件：MLD（v1/v2）ルータ機能[39][40][41]を有すること。

必要度：必須（MUST）

理由：PIM 接続の際に、端末がマルチキャストネットワークへ参加するためにはルータでの MLD ルータ機能のサポートが必要であるため。

7.3.3 MLD プロキシによる接続

MLD を使用して ISP へマルチキャストグループへの参加／離脱を通知する。

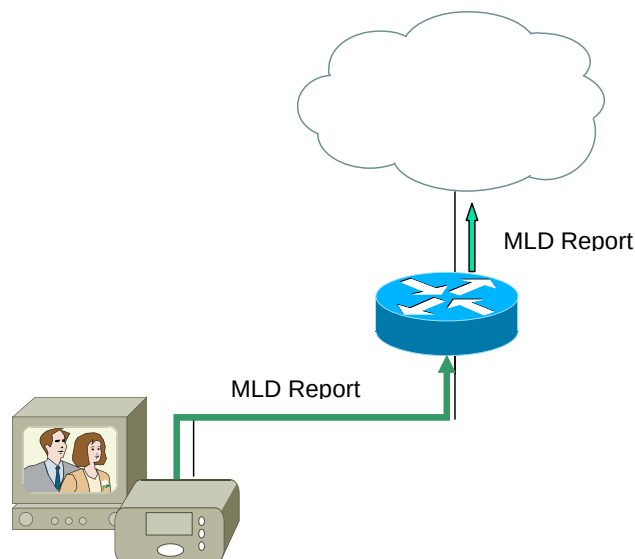


図 7-9 MLD プロキシを用いたマルチキャスト接続

前提：MLD プロキシを使用してマルチキャストサービスに接続する場合

要件：MLD (v1/v2) プロキシ[42]機能を有すること。

必要度：必須 (MUST)

理由：MLD で ISP 側へマルチキャストグループへの参加／離脱を通知するため。

7.3.4 MLD スヌーピング

7.3.1 節のいずれの接続形式においても、家庭用ルータがスイッチ機能を有する場合には下記の MLD スヌーピング[43]機能も実装する事が望ましい。なお、家庭用ルータが無線 LAN 機能を有する場合、無線 LAN 接続ノードに対しても不必要なマルチキャストトラフィックを流さないようにする MLD スヌーピング相当の機能を持つことが望ましい。

要件：MLD (v1/v2) スヌーピング[43]機能を有すること。

必要度：オプション (MAY)

理由：ルータがスイッチング機能を持つ際にのみ使用が想定されるため。

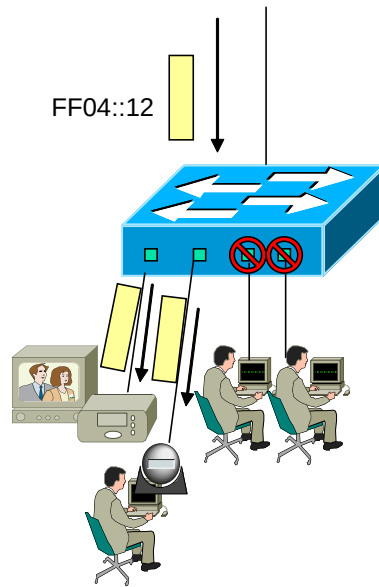


図 7-10 MLD スヌーピング機能

8 サービス側の設定手法

本章では、家庭用ルータに対する設定方式および設定項目について述べる。なお、設定主体はサービス提供者である。

8.1 設定方式

概要：サービス提供者から家庭用ルータに対して必要な設定の投入を行なうための機能を、家庭用ルータが具備すること。

必要度：必須（MUST）

理由：宅内機器がサービス提供者によるサービスを利用する上で必要となる情報を、家庭用ルータが何らかの手段により取得する必要があるため。管理者もしくはプラグアンドプレイによる設定が必要であるため。

備考：具体的な設定方式については、以下に例示列举する。

8.1.1 自動設定

本節では、サービス提供者から直接家庭用ルータを操作することなく、家庭用ルータが自律的に必要な設定情報を取得するための方式として、以下に例示列举する。

- SLAAC 機能を有すること。

DHCPv6 サーバを用いず RA によって IPv6 アドレスを設定する方法。

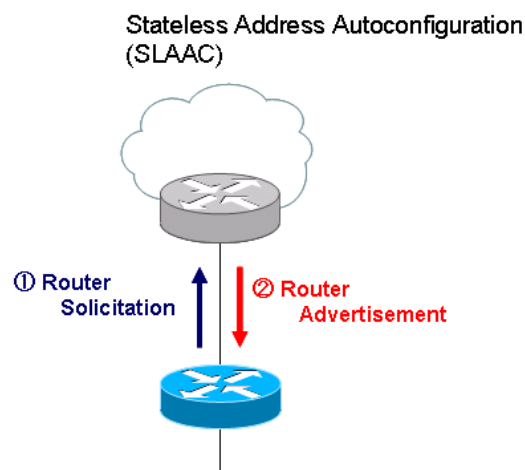


図 8-1 SLAAC による自動設定

- DHCPv6 クライアント機能を有すること。
DHCPv6 のクライアント機能とは IPv6 アドレス等の情報を DHCPv6 サーバに対して要求し、取得した情報をホスト自身に設定する機能を指す。

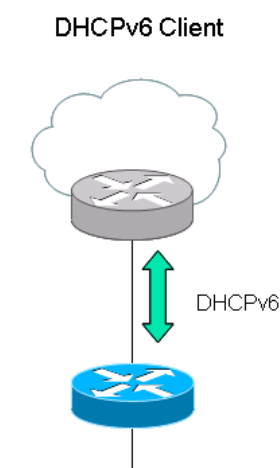


図 8-2 DHCPv6 によるアドレス設定

- TR-069 による設定ができること。
BroadBand Forum により定義された CPE 機器を遠隔管理するためのプロトコル : TR-069 を用いて設定する方法。

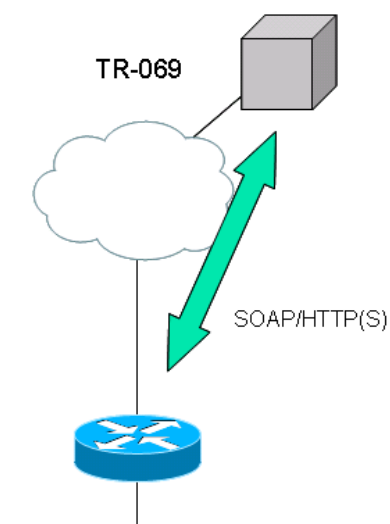


図 8-3 TR-069 によるアドレス設定

- UPnP による設定ができること。

UPnP Forum により定義された自動機器登録の仕組み：UPnP によりアドレスを設定する方法。

Universal Plug and Play (UPnP)

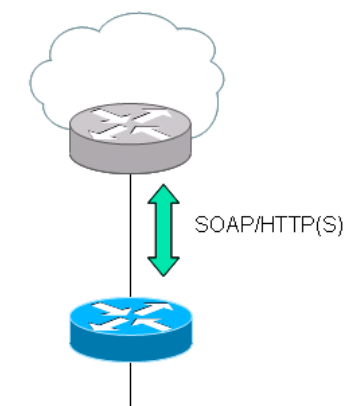


図 8-4 UPnP によるアドレス設定

8.1.2 手動設定

サービス提供者は家庭用ルータに対して手動で直接設定する場合も想定されるため、そのためのインターフェースを具備しておく必要がある。具体的には Web インターフェースや Telnet、SSH などが該当する。

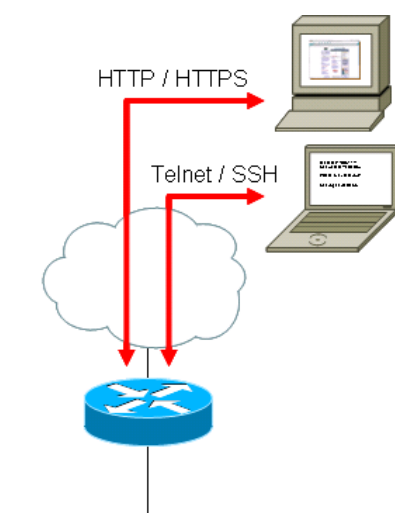


図 8-5 手動設定の概念図

8.2 設定項目

本節では、8.1 節にて述べた設定方式により家庭用ルータに設定される具体的な項目について述べる。

8.2.1 アドレス設定

3 章を参照のこと。

8.2.2 セキュリティ関連設定

要件：装置のアクセス制限機能に対して、ユーザが直接設定変更するほか、ISP など事業者側からも設定可能であること。

必要度：推奨（SHOULD）

理由：セキュリティ設定に不慣れなユーザでもサービスを受ける際に必要なセキュリティレベルを維持できるようなサービス提供を可能にするため。

備考：サービスに依存する機能であるため、利用しない場合などユーザの設定で機能を無効にできる必要がある。

要件：WAN インターフェース側にある ISP の管理セグメントから、家庭用ルータの管理用インターフェースへアクセスする手段を持つこと。

必要度：オプション（MAY）

理由：グローバルアドレスが付与されて監視する場合に、外部からの不正なアクセスから防御するため。

8.2.3 DNS 設定

本節では、家庭用ルータにて DNS プロキシ機能を使用する場合の、家庭用ルータへの DNS サーバアドレスの設定方式について述べる。その他の項目については 5 章参照のこと。

8.2.3.1 DNS プロキシ機能のための DNS サーバアドレス

要件：DHCPv6 などの手段にて取得した DNS サーバ情報を使用できること。

必要度：必須（MUST）

理由：自動化により設定ミスをなくするため。

要件：手動設定できること。

必要度：必須（MUST）

理由：ISP から自動取得できない場合も想定されるため。

8.2.4 宅内ネットワーク設定

本節では、家庭用ルータが宅内機器に対する設定を行なうにあたり必要となる情報の設定手法について述べる。

8.2.4.1 LAN 側へ配布するプレフィックス

3 章を参照のこと。

8.2.4.2 LAN 側へ配布する各種サーバアドレス

要件：接続先 ISP から DHCPv6 にて取得できること。

必要度：必須（MUST）

理由：ルータへ配布される各種サーバ情報は、提供するサービスに応じて異なることが一般的であり、必要な情報を選択的に配布できる方式が望ましいため。

要件：手動設定できること。

必要度：必須（MUST）

理由：ISP から自動取得できない場合も想定されるため。

8.2.4.3 DHCPv6 リレー機能のための DHCPv6 サーバアドレス

前提：DHCPv6 リレー機能を利用する場合

要件：手動設定できること。

必要度：必須（MUST）

理由：DHCPv6 サーバアドレスを自動で割当てする手法が必ずしも提供されていないため。

備考：DHCPv6 サーバと家庭用ルータ間で、マルチキャストルーティングを動作させることで、DHCPv6 サーバアドレスの明示的な設定を不要とすることも出来る。

8.2.5 ルーティング・マルチキャスト設定

7 章を参照のこと。

9 おわりに

9.1 IPv6 家庭用ルータが必要とする機能のまとめ

前章までにまとめた「IPv6 家庭用ルータにおける最小限の共通機能」を表 9-1 にまとめる。本ガイドラインでは、IPv6 家庭用ルータに対する機能をすべて網羅できていないが、ここに挙げた機能に関して最低限考慮した実装が IPv6 の家庭用ルータに求められる。なお今後議論が必要としている未検討項目は次節（0 節）にまとめる。

表 9-1 IPv6 家庭用ルータに必要とされる機能一覧

番号	小項目	必要度	節
1	宅内ネットワークへ配布するプレフィックス情報を接続先 ISP から DHCPv6-PD にて取得できること。	必須	3.1.1
2	宅内ネットワークへ配布するプレフィックス情報を手動設定できること。	必須	3.1.1
3	/48～/64 の幅でサービス提供者が割り当てたプレフィックスを受信できること。	必須	3.1.2
4	ユーザに配布するプレフィックスを固定とすること。	推奨	3.1.3
5	ユーザに配布するプレフィックスが時間の経過により変更すること。	オプション	3.1.3
6	家庭用ルータの WAN 側にもグローバルアドレスを付与できること。付与するアドレスは、ユーザに割り当てたアドレス空間からではなく、サービス提供者が保有する別空間からとする。	推奨	3.2.1
7	前提 6 WAN 側グローバルアドレスをダイナミックに付与できること。	必須	3.2.1.1
8	前提 6 WAN 側グローバルアドレスをマニュアルで付与できる。	必須	3.2.1.2
9	ISP から DHCPv6-PD で受け取ったプレフィックスを基に /64 のプレフィックスを生成しそれを LAN 側に再配布できること。	必須	3.3.1
10	ひとつのもしくは複数の ISP から複数のプレフィックスを DHCPv6-PD で受け取った場合、どのプレフィックスを LAN 側に再配布するか選択できること。	オプション	3.3.2

11	前提 5	WAN側回線の再接続により、ISPがDHCPv6-PDにて配布するプレフィックスが変化した場合に、LAN側に配布するプレフィックスを適切に変更できること。	推奨	3.3.3
12		内部（LAN側）から外部（WAN側）への通信は通過させ、外部から内部への通信はデフォルトで遮断するアクセス制限が行えること。	必須	4.1.1.1
13		静的フィルタによりアクセスを制限できること。	必須	4.1.1.2
14		動的フィルタ（SPI）によりアクセスを制限できること。	推奨	4.1.1.3
15		外部からのアクセスに対して通過、遮断する条件を設定できること。	必須	4.1.2
16		装置自身への通信に対するアクセスを制御するフィルタを設定可能であること。	必須	4.2
17		DNSプロキシの上位側（ISPのDNSサーバ側）は、IPv6トランスポートとIPv4トランスポートの両方が利用可能であること。	必須	5.2.1
18		端末からのDNS要求と同一のトランスポートでプロキシ動作を行うこと。	オプション	5.2.2
19		DNSプロキシとして、ユニキャストアドレス（グローバルアドレス、ULA、リンクローカルアドレスの内いずれか）で待ち受け可能であること。	必須	5.3.1
20		複数のDNSサーバを利用することができ、順次サーチ方式によりDNSの選択を行うこと。	必須	5.4.1
21		特定のポリシーに応じてDNSサーバを任意に選択するドメイン識別方式などの機能がある場合はその機能で設定されたルールに従うこと。	オプション	5.4.2
22		端末からのDNS要求により得られた結果をキャッシュしておき、以降同様のDNS要求があった場合は、キャッシュ情報を応答すること。	オプション	5.5
23		端末からのDNS要求に対して、リソースレコード（RR）の種別に関わらず全て透過的に処理すること。	必須	5.6.1
24		EDNS0に対応した要求（OPT RRを含む）パケットを透過的に処理し、512byteを超える応答を端末に送信可能なこと。	必須	5.6.2
25		端末が（DNS Header TC=1受信により）TCP接続にフォールバックしてDNS要求を行った場合においても透	必須	5.6.3

	過的に処理を行うこと。UDP 53 番ポートだけでなく、TCP 53 番ポートにおいても待ち受けること。			
26	DNSSEC に対応した以下のパケットを透過的もしくは適切に処理可能なこと。		オプション	5.6.4
27	宅内ネットワークの端末に割り当てるプレフィックスを RA で通知する機能を持つこと。		必須	6.1.1
28	RA で通知するプレフィックス長は、デフォルトを/64 とすること。		必須	6.1.1
29	宅内の端末にアドレスを DHCPv6 で通知する機能を持つこと。		オプション	6.1.2
30	DHCPv6-PD により宅内機器（ルータ）にプレフィックスを配布する機能を持つこと。機器毎に配布するプレフィックスを指定できる機能を持つこと。		オプション	6.1.2
31	LAN セグメントに対して、DNS サーバアドレスを配布する機能を持つこと。		オプション	6.2.1
32	LAN セグメントに対して、DHCPv6 にて DNS サーバアドレスを配布する機能を持つこと。		必須	6.2.2
33	LAN セグメントに対して、DHCPv6 にてその他のサーバアドレス（SIP、NTP など）を配布する機能を持つこと。		オプション	6.2.2
34	DHCPv6 リレー機能を持つこと。		オプション	6.2.3
35	前提 30	割り当てられたプレフィックス宛てのトラフィックを上流にフォワードしない機能を持つこと。	必須	7.1
36	Point-to-Point リンクのルータにて、自インターフェース以外のアドレス宛のパケットを受け取った際には ICMPv6 Destination Unreachable messages, Code 3 (Address unreachable) を送出し、パケットを転送しないこと		必須	7.1
37	WAN 向けのスタティックルートが設定できること。		必須	7.2.1
38	RA を利用しての WAN 側のデフォルトルートが自動設定できること。		必須	7.2.1
39	RIPng により LAN 側に経路広告ができること。		オプション	7.2.2
40	More-Specific Routes により LAN 側に経路を配布できること。		オプション	7.2.2
41	RH0 (Type 0 Routing Headers) のパケット転送を禁止できること。		必須	7.2.3

42		IPv6 マルチキャスト機能	オプション	7.3
43	前提 42	PIM を用いたマルチキャストが利用できること	オプション	7.3
44	前提 43	PIM によるマルチキャストルーティング機能を持つこと。	必須	7.3.2
45	前提 43	要件：MLD（v1/v2）ルータ機能を有すること	必須	7.3.2
46	前提 42	MLD プロキシを使用してマルチキャストサービスに接続できること。	オプション	7.3
47	前提 46	MLD（v1/v2）プロキシ機能を有すること。	必須	7.3.3
48	前提 42	MLD（v1/v2）スヌーピング機能を有すること。	オプション	7.3.4
49		サービス提供者から家庭用ルータに対して必要な設定の投入を行なうための機能を、家庭用ルータが具備すること。	必須	8.1.1
50		装置のアクセス制限機能に対して、ユーザが直接設定変更するほか、ISP など事業者側からも設定可能であること。	推奨	8.2.2
51		WAN インターフェース側にある ISP の管理セグメントから、家庭用ルータの管理用インターフェースへアクセスする手段を持つこと。	オプション	8.2.2
52		DHCPv6 などの手段にて取得した DNS サーバ情報を使用できること。	必須	8.2.3.1
53		DNS サーバアドレスを手動設定できること。	必須	8.2.3.1
54		各種サーバアドレスを接続先 ISP から DHCPv6 にて取得できること。	必須	8.2.4.2
55		各種サーバアドレスを手動設定できること。	必須	8.2.4.2
56	前提 34	DHCPv6 サーバアドレスを手動設定できること。	必須	8.2.4.3

9.2 次版に向けた検討項目

本ガイドラインでは、家庭用ルータにおける全ての機能を網羅して機能定義をできておらず、今後引き続き検討を重ねる必要がある。以下に今後検討が必要と考えている項目をまとめる。

9.2.1 見直し/詳細検討が必要な項目

- WAN 側グローバルアドレスの必要性
- フィルタリング時のフラグメント処理
- 拡張ヘッダチェーンの対応ヘッダ数
- TCP,UDP 以外のトランスポートプロトコルへの対応
- フィルタリングの推奨値
 - 利用可能アプリケーション一覧など
- DNS トランスポート議論の整理
- PIM 実装に関する再考

9.2.2 未検討項目

- DNS サービス時の課題
 - ソースポートランダム化マイゼーション, DNSSEC 対応など
- プロバイダ接続機能（プロバイダ毎のサービス対応）
 - Point-to-Multipoint 接続, ISP サービスの自動判別機能など
- マルチプレフィックス対応（複数の ISP 接続）
 - マルチセッション, デフォルトルートの扱い, 66NAT など
- サブネット・ルータ・エニーキャストの扱い
- トンネル接続機能
- IPv4/IPv6 相互変換機能
- 非固定プレフィックス対応機能
- uPnP
- ボンジュール
- ノードディスカバリ機能
- mDNS
- その他の未検討ルータ機能（参考）

QoS 機能, ダイナミック DNS 登録, 静的 NAT, ブリッジ機能, 機器のアクセス制御 (MAC アドレス認証等), ホームゲートウェイの個体認証 (個体識別), 802.1x 認証, 無線機能 (802.11, Bluetooth), セットアップに関する機能 (初期設定機能, Web での設定), 各種メディア対応 (無線, イーサ, USB, IEEE1394, 電話, ISDN) など

9.3 検討メンバー

下記に検討メンバーを示す。会務担当者以外のメンバーは、所属の 50 音順に従っている。

氏名	所属
荒野 高志 (WG 主査)	株式会社インテック・ネットコア
北口 善明 (chair)	株式会社インテック・ネットコア
藤崎 智宏 (co-chair)	日本電信電話株式会社
中川 あきら (co-chair)	KDDI 株式会社
印南 鉄也 (co-chair)	ソフトバンク BB 株式会社
新 善文	アラクサラネットワークス株式会社
鹿志村 康生	アルカテル・ルーセント
芦田 宏之	イツ・コミュニケーションズ株式会社
佐原 具幸	株式会社インターネットイニシアティブ
川島 正伸	NEC アクセステクニカ株式会社
鈴木 聡介	NTT コミュニケーションズ株式会社
植松 高史	西日本電信電話株式会社
柴田 巧	西日本電信電話株式会社
水越 一郎	東日本電信電話株式会社
岡田 真悟	日本電信電話株式会社
川島 倫央	KDDI 株式会社
屏 雄一郎	株式会社 KDDI 研究所
土屋 師子生	シスコシステムズ合同会社
河野 美也	Juniper Networks
上根 義昭	ソネットエンタテインメント株式会社
佐古田 寛司	ソネットエンタテインメント株式会社
山口 琢也	ソネットエンタテインメント株式会社
村上 誠	ソフトバンクテレコム株式会社
小林 丈記	ソフトバンク BB 株式会社
菅沼 真	株式会社 電算
花山 寛	ネットワンシステムズ株式会社
伊田 吉宏	パナソニックコミュニケーションズ株式会社
本橋 篤	富士通株式会社
小野田 充宏	ヤマハ株式会社

9.4 リファレンス一覧

- [1] RFC 5072: IP Version6 over PPP
- [2] RFC 5172: Negotiation for IPv6 Datagram Compression Using IPv6 Control Protocol
- [3] RFC 1994: PPP Challenge Handshake Authentication Protocol (CHAP)
- [4] RFC 3056: Connection of IPv6 Domains via IPv4 Clouds (6to4)
- [5] RFC 4380: Tunneling IPv6 over UDP through Network Address Translations (Teredo)
- [6] RFC 2784: Generic Routing Encapsulation (GRE)
- [7] Draft-kuwabara-softwire-ipv6-via-l2tpv2-00: A Model of IPv6 Internet Access Service via L2TPv2 Tunnel (softwire)
- [8] JPNIC における IPv6 アドレス割り振りおよび割り当てポリシー
<http://www.nic.ad.jp/doc/jpnic-01078.html>
- [9] RFC 4890: Recommendations for Filtering ICMPv6 Messages in Firewalls
- [10] RFC 4864: Local Network Protection for IPv6
- [11] RFC 5095 Deprecation of Type 0 Routing Headers in IPv6
- [12] NAT66 IPv6-to-IPv6 Network Address Translation
- [13] DOCSIS 3.0 specification <http://www.cablelabs.com/specifications/doc30.html>
- [14] DNS Proxy Implementation Guidelines (draft-ietf-dnsext-dnsproxy-03)[work in progress]
- [15] RFC 3484: Default Address Selection for Internet Protocol version 6 (IPv6)
- [16] RFC 4477: Dynamic Host Configuration Protocol (DHCP) : IPv4 and IPv6 Dual-Stack Issues
- [17] IPv6 マルチプレフィックス環境の構築に関する考察
<http://www.v6pc.jp/pdf/v6pc-mp-1.0.pdf>
- [18] Kaminsky Attack に関する情報
<http://jprs.jp/tech/security/multiple-dns-vuln-cache-poisoning.html>
- [19] RFC 2671: Extension Mechanisms for DNS (EDNS0)
- [20] RFC 1035: DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION
- [21] RFC 1123: Requirements for Internet Hosts -- Application and Support
- [22] RFC 4033: DNS Security Introduction and Requirements
- [23] RFC 4034: Resource Records for the DNS Security Extensions
- [24] RFC 4035: Protocol Modifications for the DNS Security Extensions
- [25] DNSSEC on Windows 7 DNS client
<http://blogs.technet.com/sseshad/archive/2008/11/11/dnssec-on-windows-7-dns-clien>

t.aspx

- [26] RFC 4294: IPv6 Node Requirements
- [27] RFC 3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- [28] RFC 4294: IPv6 Node Requirements
- [29] RFC 4861: Neighbor Discovery for IP version 6 (IPv6)
- [30] RFC 3633: IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6
- [31] RFC 5006: IPv6 Router Advertisement Option for DNS Configuration
- [32] RFC 4339: IPv6 Host Configuration of DNS Server Information Approaches
- [33] RFC 4443: Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
- [34] RFC 2080: RIPng for IPv6
- [35] RFC 4191: Default Router Preferences and More-Specific Routes
- [36] RFC 4601: Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)
- [37] RFC 2362: Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification
- [38] RFC 4607: Source-Specific Multicast for IP
- [39] RFC 2710: Multicast Listener Discovery (MLD) for IPv6
- [40] RFC 3810: Multicast Listener Discovery Version 2 (MLDv2) for IPv6
- [41] RFC 4604: Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast
- [42] RFC 4605: Internet Group Management Protocol (IGMP) / Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP/MLD Proxying")
- [43] RFC 4541: Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches
- [44] TR-069
<http://www.broadband-forum.org/technical/download/TR-069Amendment2.pdf>
- [45] UPnP <http://www.upnp.org/specs/arch/UPnP-arch-DeviceArchitecture-v1.1.pdf>
- [46] RFC 4291: IP Version 6 Addressing Architecture
- [47] RFC 4787: Network Address Translation (NAT) Behavioral Requirements for Unicast UDP
- [48] RFC 4862: IPv6 Stateless Address Autoconfiguration
- [49] RFC 3319: Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers

- [50] RFC 3646: DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- [51] RFC 3898: Network Information Service (NIS) Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- [52] RFC 4075: Simple Network Time Protocol (SNTP) Configuration Option for DHCPv6
- [53] RFC 4795: Link-Local Multicast Name Resolution (LLMNR)