

OCN IPv6
ユーザ網インタフェース仕様書

第 1.0 版

平成 17 年 12 月 5 日

NTT コミュニケーションズ株式会社

本仕様書の内容は、機能追加等により、予告なく追加・変更することがあります。

内容についてのお問い合わせ先は、次の通りです。

NTT コミュニケーションズ株式会社 コンシューマ&オフィス事業部

Email: ocnipv6-uni@ntt.com

1 章. はじめに.....	3
2 章. 『OCN IPv6』 サービス概要	4
3 章. ユーザ網インタフェース仕様	7
3.1. L2TP フェーズ.....	7
3.2. PPP フェーズ.....	8
3.3. プレフィックス付与フェーズ.....	9
3.4. 接続シーケンス例	11
3.5. 切断シーケンス例	13
4 章. クライアント機能仕様.....	15
4.1. はじめに.....	15
4.2. 必須機能.....	15
4.2.1. IPv6 通信機能.....	15
4.2.2. 『OCN IPv6』 接続機能.....	15
4.2.3. モードスイッチ機能.....	15
4.2.4. 各種パラメータ既定値及び設定機能.....	20
A. 付録.....	21
A.1. IPv6 に関する主な RFC 一覧.....	21
A.2. 改版履歴.....	22

1章. はじめに

本仕様書は、NTT コミュニケーションズ株式会社(以下、当社)が提供する、『OCN IPv6』サービスにクライアントが接続するためのユーザ網インタフェース仕様、ならびにクライアントに必要な機能仕様を規定したものである。2章に『OCN IPv6』サービス概要、3章にユーザ網インタフェース仕様、4章にクライアント機能仕様を示す。

なお、本仕様書は、端末設備を含めた通信システムの品質を保証するものではない。

また、本仕様書の内容は、今後の機能追加等により予告なく追加・変更されることがある。

2章. 『OCN IPv6』 サービス概要

『OCN IPv6』(以下、OCN IPv6)は、既存のIPv4 ネットワークにグローバルIPv6 ネットワークへの接続機能を付与するサービスである。

OCN IPv6 は、既存のIPv4 ネットワークを利用し、IPv4 ネットワーク上に設置されているOCN IPv6 接続サーバ(以下、接続サーバ)とOCN IPv6 接続クライアント(以下、接続クライアント)との間で、Layer Two Tunneling Protocol (RFC 2661) (以下、L2TP)により仮想的なパスをはり、そのパスの上でPoint-to-Point Protocol (RFC 1661) (以下、PPP)を用い、PPP リンク上でIPv6 通信の接続性を提供する。

OCN IPv6 の特徴を以下に示す。

IPv6 接続性の提供

- 1つの接続クライアントにつき、1つの/64のプレフィックスを付与する。
- アグリゲータブルグローバルユニキャストアドレスのIPv6プレフィックスを付与する。
- 接続サーバは接続クライアントに対して動的¹にIPv6プレフィックスを付与する。
- 接続サーバが接続クライアントに対して付与するIPv6プレフィックスは固定²または非固定とする。

NAT 透過性

- 接続サーバと接続クライアントの間にNAT装置が介在した場合においても、接続を確立し、IPv6での接続性を提供する。

IPv6 自動設定機能

- 接続サーバは接続クライアントに対してRFC 3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6) (以下、DHCPv6)のIPv6 Prefix Options for DHCPv6 (RFC 3633) (以下、DHCPv6 PD)を用いてIPv6プレフィックスを動的に付与する。

認証機能

- PPP Link Control Protocol (以下、LCP)のPPP Challenge Handshake Authentication Protocol (CHAP) (RFC1994)によって認証を行う。

以下にOCN IPv6での代表的な利用例を示し、各々について説明する。

¹ 「動的」とは何らかのネットワークプロトコルシーケンスを用いて接続クライアントにプレフィックスを付与する方法を示す。ユーザに付与するプレフィックスを事前に書面にて通知する方法を「静的」とする。

² 「固定」とはOCN IPv6 接続確立毎に、ユーザに常に同じ値のプレフィックスを付与することを示す。OCN IPv6 接続確立毎にユーザに付与するプレフィックスが変化する事を「非固定」とする。

利用例 1：ホスト型

図 1 のように、ブロードバンドルータ配下のプライベート IPv4 ネットワークに接続クライアントを接続する。接続クライアントは接続サーバより付与された IPv6 プレフィックスから任意の IPv6 アドレスを選び出し、そのアドレスを接続クライアント自身のネットワークインタフェースに付与する。この時接続クライアントは IPv4 的にも、IPv6 的にもホストとして動作する。

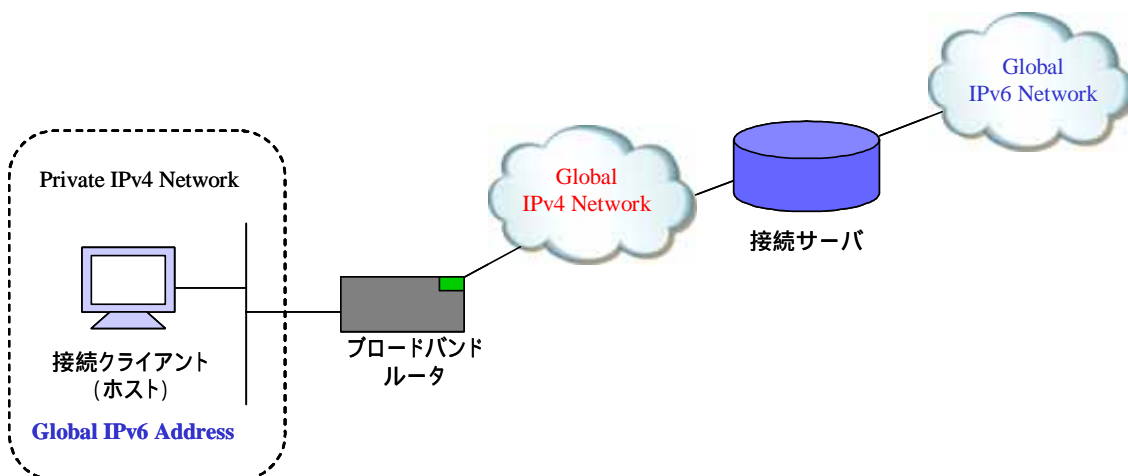


図 1. ホスト型利用例

利用例 2：ルータ型

図 2 のように、ブロードバンドルータ配下のプライベート IPv4 ネットワークに接続クライアントを接続し、ブロードバンドルータ配下のネットワークの一部、あるいはすべてにグローバル IPv6 ネットワークへの接続性を提供する。この時、接続クライアントは、IPv4 的にはホストとして動作し、IPv6 的にはルータとして動作する。

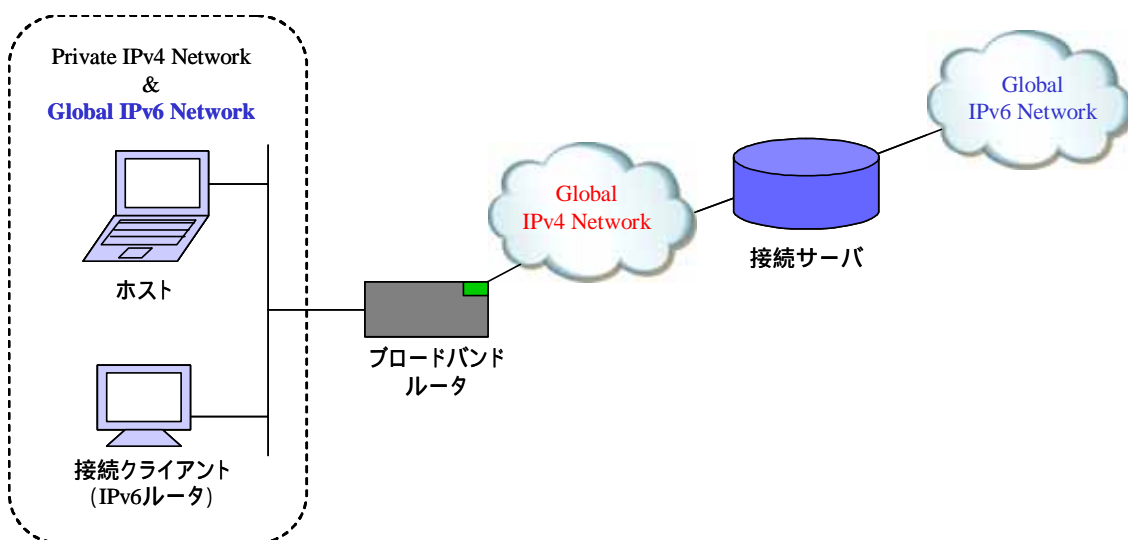


図 2. ルータ型利用例

利用例 3 : ブロードバンドルータ内蔵型

図 3 のように、接続クライアント機能をブロードバンドルータなど同一の機器に実装し、IPv6 ネットワーク接続性を機器配下のネットワークに提供する。このときブロードバンドルータ兼接続クライアントは IPv4 的にも、IPv6 的にもルータとして機能する。

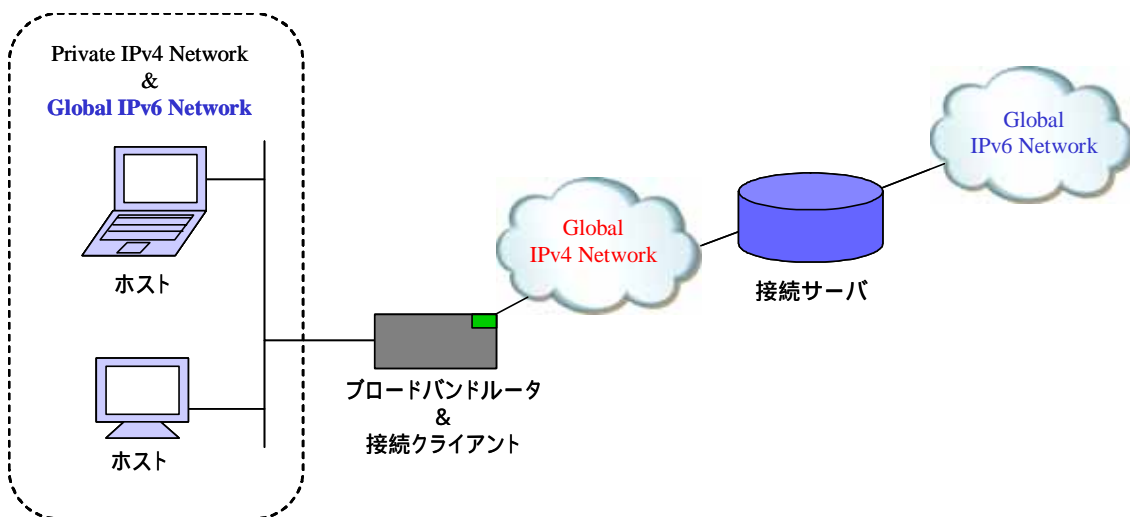


図 3. ブロードバンドルータ内蔵型利用例

3 章. ユーザ網インタフェース仕様

本章では、ユーザ網インタフェース仕様を規定する。

OCN IPv6 は IPv4 で接続サーバと接続クライアントが通信できることを前提にしていることから、本章で規定するレイヤは IPv4 layer 以上とし、IPv4 でのネットワーク接続確立方法は本仕様書の規定外とする。

本章で規定するインタフェースとプロトコルスタックを図 4 に示す。

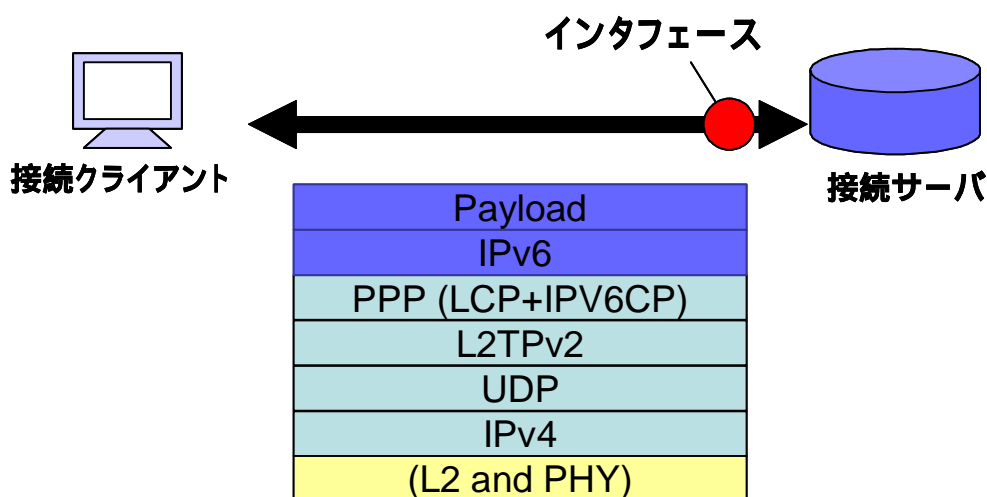


図 4. プロトコルスタック

上記のプロトコルスタックを実現するために、以下のステップを踏む。

1. L2TP フェーズ
 - RFC 2661 で定義されている L2TP を用いて接続サーバから接続クライアントへ仮想的なパスを張る。
2. PPP フェーズ
 - L2TP により確立した仮想的なパスの上で PPP 接続を行う。
3. プレフィックス付与フェーズ
 - DHCPv6 PD による接続クライアントへの IPv6 プレフィックス自動付与や接続サーバから接続クライアントのルーティング等を設定する。

3.1. L2TP フェーズ

RFC 2661 に準拠する。

接続クライアントから接続サーバへ L2TP の "Start Control Connection Request(以下、SCCRQ)" メッセージを送信する際、SCCRQ メッセージ中の "Host Name Attribute Value Pair(以下、Host Name AVP)" を付けることが必須となっている。RFC 2661 では、"Host Name AVP" として、Fully Qualified Domain Name(FQDN)が適当であると述べている。

しかし本仕様では、“Host Name AVP”として、後述する PPP フェーズでの PPP Challenge Handshake Authentication Protocol (以下、CHAP)における“name”フィールドに格納すべき値を“Host Name AVP”の値とすることが望ましい。CHAPにおける“name”フィールドに格納すべき値は、通常サービス提供者からサービス利用者に払い出されるアカウント名である。

RFC 2661 の通り L2TP パケットは UDP によりカプセリングされる。UDP に関しては RFC 768 で定義される“User Datagram Protocol”に準拠する。L2TP のパケットが UDP によりカプセリングされることにより、NAT を透過してのトンネル確立を可能とする。接続サーバは UDP port 1701 番で接続を待ち受ける。

なお、接続サーバ側から接続クライアントにセッション³の確立を要求する“Outgoing Call Establishment”は行わない。また、RFC 2661 にあるように、一つの接続クライアントが複数のセッション確立をサポートする必要はなく、単一のセッションのみをサポートできればよい。

3.2. PPP フェーズ

L2TP により張られた仮想的なパスの上で、PPP コネクションを確立する。PPP による接続は RFC 1661 で示される PPP と、IP version 6 over PPP (RFC 2472) に規定されている IPV6CP に準拠する。

PPP 認証で必須とするプロトコルは、

- CHAP

とする。なお RFC 1661 で定義されている Password Authentication Protocol (PAP) はサポートしない。

PPP Network Control Protocol (以下、NCP) で必須とする機能を以下に示す。

- NCP として、IPV6CP を利用可能

RFC 1661 で記載されている事柄ではあるが、接続クライアントは以下の機能を持たなければならない。

- LCP Opened の状態で LCP Echo-Request を受信した場合、LCP Echo-Reply で応答

IPV6CP は Interface-Identifier のネゴシエーション機能を持つが、グローバルスコープのプレフィックス付与機能は持たない。したがって、この時点では、L2TP で張られた仮想的なパス上で PPP インタフェースを通じて接続クライアントと接続サーバが IPv6 で通信する際は、IPv6 のリンクローカルアドレスを用いた通信のみが可能となる。

³ RFC 2661 で述べられている“Session”のことであり、end-to-endでPPP接続が確立した際にL2TP Network Server (LNS)とL2TP Access Client (LAC)との間で、そのPPP接続と1対1にマッピングされるセッションである。

3.3. プレフィックス付与フェーズ

PPP フェーズ終了後、つまり IPV6CP ネゴシエーション終了後、接続サーバは接続クライアントからの DHCPv6 PD による要求に対して、動的にグローバルスコープのプレフィックスを付与する。接続クライアントは接続サーバから付与された IPv6 プレフィックスの範囲で任意の IPv6 アドレスを選定しインタフェースに付与する。

この後、接続クライアントと接続サーバの間でグローバルアドレスを用いた通信が可能となる。

IPv6 アドレス設定

接続クライアントは接続サーバから委譲されたプレフィックス空間の中からプレフィックス長 64 のプレフィックスを自動生成し、任意のインタフェースに自動的に設定する。

ルーティング設定

接続クライアントは IPv6 デフォルトルートを PPP 仮想インタフェースに向けて自動設定する機能を持つ。

また、接続サーバと接続クライアントの間の IPv6 に関するルーティングはスタティックルーティングとする。

接続クライアントに付与されたプレフィックス空間内で、未使用のプレフィックス空間内のアドレスを Destination Address として持つ IPv6 パケットを接続クライアントが受信した場合、接続クライアントはそのパケットを接続サーバに転送してはならない。また、あわせて以下のいずれかの動作をとるべきである。

- ICMPv6 (RFC 2463) Destination Unreachable メッセージを返信する
- パケットを破棄する

プレフィックス付与機能

接続サーバから接続クライアントへのプレフィックスの付与は、RFC 3315 および、RFC 3633 で規定されている DHCPv6 PD に準拠する。

なお接続クライアントは、下記に示す DHCPv6 メッセージおよび DHCPv6 オプションを処理しなければならない。

- メッセージの送信
 - Solicit
 - Request
 - Renew
 - Rebind
 - Release
- メッセージの受信
 - Advertise
 - Reply

- オプションの処理
 - Client Identifier
 - Server Identifier
 - Option Request
 - Elapsed Time
 - Status Code
 - Domain Name Server
 - IA_PD
 - IA_PD Prefix

なお、DHCPv6 PD によるプレフィックス委譲の動作概要は以下の通りである。

1. 接続クライアントは IA_PD Option のついた Solicit メッセージを送信する。
2. 接続サーバは IA_PD Prefix Option を含む IA_PD Option のついた Advertise メッセージで応答する。
3. 接続クライアントは Advertise メッセージで得られたプレフィックス情報を反映した IA_PD Prefix Option を含む IA_PD Option を含めた Request メッセージを接続サーバへ送信する。
4. 接続サーバはメッセージの内容を確認し、問題がなければ Reply メッセージを返す。何らかの理由で IPV6CP の切断 - 再接続が行なわれた場合、接続クライアントは DHCPv6 PD を Renew から行う。ただし、LCP 切断後の再接続時には Solicit からやり直してもよい。

DNS サーバの通知機能

OCN IPv6 では ISP 側に存在する IPv6 DNS サーバは通知しない。しかし、将来 IPv6 DNS サーバの Global Unicast Address を、プレフィックス通知に用いる DHCPv6 Advertise Message ならびに DHCPv6 Reply Message において、RFC 3646 で規定される Domain Name Server Option を用いて通知する可能性がある。

その他

Simple Network Time Protocol Server Option (RFC4075)を用いて NTP Server の IPv6 アドレスを通知する可能性がある。

Keep-Alive 機能

接続クライアントは、トンネル接続の維持のため、L2TP の Control Message の一つである”Hello”メッセージと PPP LCP の”echo-request”メッセージを接続サーバに対して定期的に送信する。

また、この Keep-Alive の機能により接続クライアントがブロードバンドルータ等配下のプライベート IPv4 ネットワークに接続された際にも、ブロードバンドルータ等の NAT

テーブルを定期的に更新することが可能となる。同時にブロードバンドルータ等にも実装された Stateful Packet Inspection 機能をもったファイアウォールのテーブルも更新することが可能となる。

3.4. 接続シーケンス例

接続サーバと接続クライアントの間で IPv4 でのコネクティビティ確立後から、グローバルスコープアドレスでの IPv6 通信を開始するまでの正常起動シーケンス例を図 5 に示す。IPV6CP でのネゴシエーション後にリンクローカルアドレスでの通信、DHCPv6 PD でのネゴシエーション後にグローバル IPv6 アドレスでの通信が可能となる。

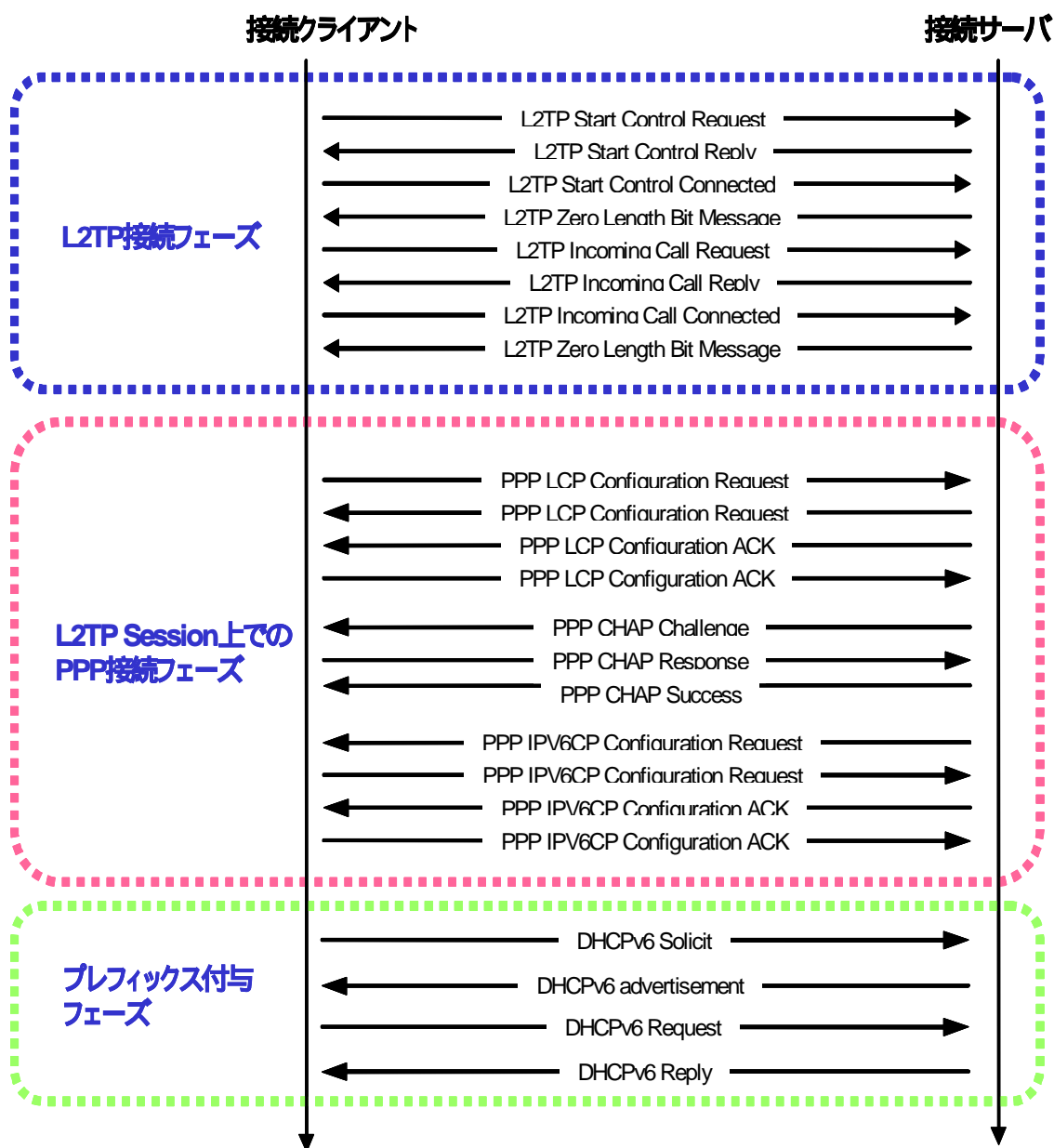


図 5. 正常接続シーケンス例

正常接続シーケンス中の L2TP メッセージの中で、最低限含めなければならない Attribute Value Pair を以下に示す。

- SCCRQ
 - Message Type
 - Protocol Version AVP
 - Host Name AVP
 - Framing Capabilities AVP
 - Assigned Tunnel ID AVP
- SCCRП
 - Message Type
 - Protocol Version AVP
 - Framing Capabilities AVP
 - Host Name AVP
 - Assigned Tunnel AVP
- SСССN
 - Message Type
- ZLB ACK
- ICRQ
 - Message Type
 - Assigned Session ID
 - Call Serial Number
- ICRP
 - Message Type
 - Assigned Session ID
- ICCN
 - Message Type
 - (TX) Connect Speed
 - Framing Type
- ZLB ACK

また正常接続シーケンスにおける DHCPv6 の各パケットのオプション構成例を以下に示す。

- Solicit
 - Client ID
 - Elapsed Time
 - IA_PD(IAID=0,T1=0,T2=0)
 - Option Request(IA_PD)

- Advertise
 - Client ID
 - Server ID
 - IA_PD
 - ◇ IA_PD Prefix
- Request
 - Client ID
 - Server ID
 - Elapsed Time
 - Option Request(IA_PD)
 - IA_PD
 - ◇ IA_PD Prefix
- Reply
 - Client ID
 - Server ID
 - IA_PD
 - ◇ IA_PD Prefix

3.5. 切断シーケンス例

接続クライアントが接続サーバとの接続を切る際のシーケンス例を示す。

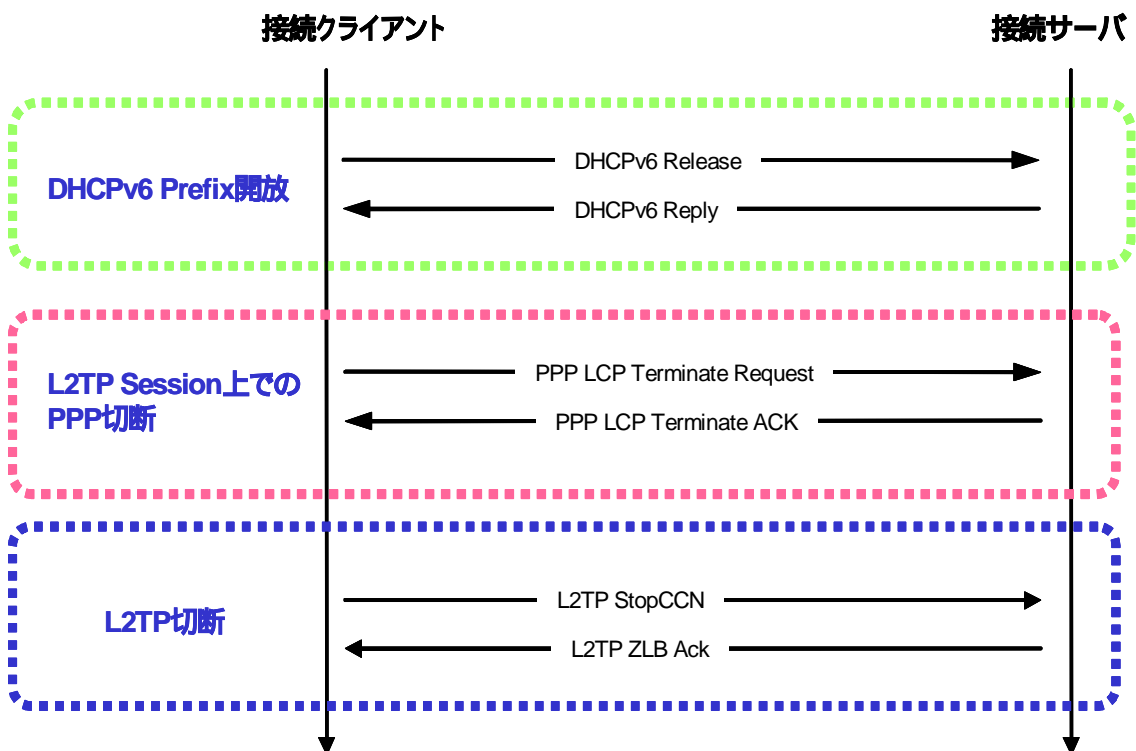


図 6. 正常切断シーケンス例

正常切断シーケンスにおける DHCPv6 の各パケットのオプション構成例を以下に示す。

- Release
 - Client ID
 - Server ID
 - IA_PD
 - ◇ IA_PD Prefix
- Reply
 - Server ID
 - Client ID
 - Status Code

また、正常切断シーケンス中の L2TP メッセージの中で、最低限含めなければならない Attribute Value Pair を以下に示す。

- StopCCN
 - Message Type
 - Assigned Tunnel ID AVP
 - Result Code AVP
- ZLB ACK

4 章. クライアント機能仕様

4.1. はじめに

接続クライアントが有すべき機能仕様を規定する。

4.2 項に接続クライアントが最低限有すべき機能を示す。

4.2. 必須機能

4.2.1. IPv6 通信機能

接続クライアントは IPv6 に関する RFC 仕様を満たし、IPv6 対応のネットワーク機器と通信可能であること。IPv6 に関する主な RFC は付録 A.1 を参照すること。

4.2.2. OCN IPv6 接続機能

3 章で述べたユーザ網インタフェース仕様に従い、IPv6 接続を確立できること。

また、以下に示す仕様を満たすとする。

1. L2TP フェーズ

- RFC 2661 で規定される "Tunnel Authentication" は行わないこととする。(ただし、将来にわたって "Tunnel Authentication" を行わないことを保証することではない。)
- RFC 2661 で規定される "Hiding of AVP Attribute Value" は行わない。(ただし、将来にわたって "Hiding of AVP Attribute Value" を行わないことを保証することではない。)

2. PPP フェーズ

- PPP Network Control Protocol (NCP) は、IPV6CP のみとする。

4.2.3. モードスイッチ機能

接続クライアントは、以下二つのモードいずれかで動作する。

1. 接続クライアントのみが IPv6 通信をする "ホストモード"
2. 接続クライアント以外の IPv6 Host が送信したパケットを転送する "ルータモード"

この 2 つのモードを設定ファイルの変更や GUI からの操作により切替えることを可能とし、この機能を "モードスイッチ機能" と呼ぶ。

モードスイッチ機能は、原則実装することを必須とするが、ブロードバンドルータ等のように、リッチな Man-Machine インタフェース (キーボード等) を持たない機器に接続クライアントを実装する際は、ホストモードを必須とせずルータモードのみで動作することを許容する。

接続クライアントはデフォルトではホストモードで起動し、ユーザの設定によりルータモードに切り替えられるものとする。

以下に各モードの特徴をまとめる。

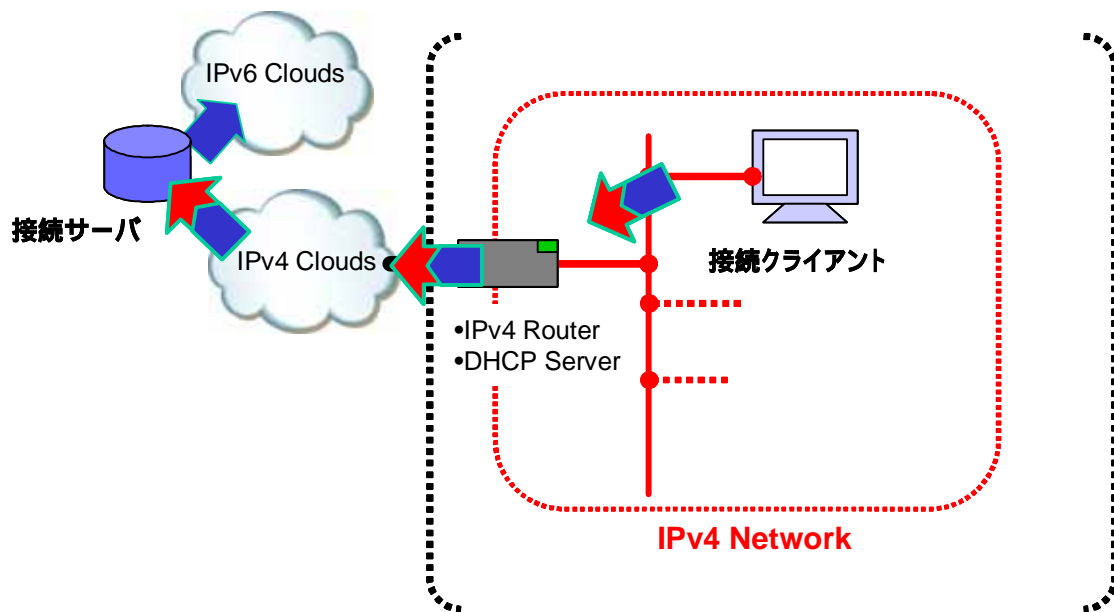


図 7. ホストモード動作イメージ

ホストモード

ホストモードの動作イメージは図 7 のとおりである。

ホストモードは以下のような特徴をもつ。

- DHCPv6 PD の後、トンネルサーバより付与されたグローバルスコープのプレフィックスから任意の IPv6 アドレスを選出し、そのアドレスを適当なネットワークインタフェース(自身の仮想インタフェースやループバックインタフェース等)に設定し、そのアドレスを用いて IPv6 通信を行う。
- IPv6 デフォルトルート PPP 仮想インタフェースに向けて設定する。
- RA を送信しない。
- IPv6 パケットの転送を行わない。

ホストモードでの接続サーバへの接続から、グローバル IPv6 アドレスを用いての通信が可能となるまでのシーケンスは図 8 の通りである。

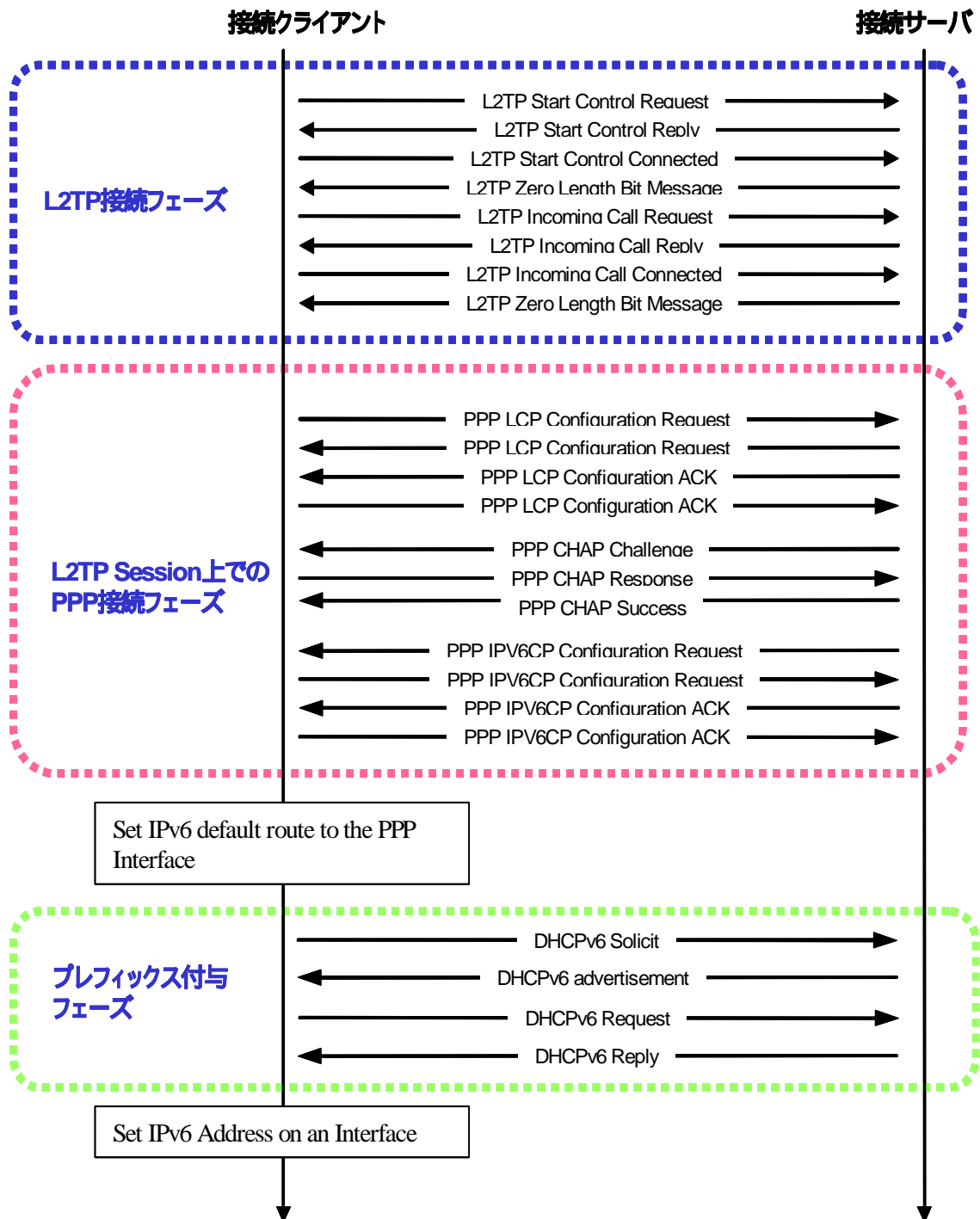


図 8. ホストモード起動シーケンス例(正常時)

ルータモード

ルータモードの動作イメージは図9のとおりである。

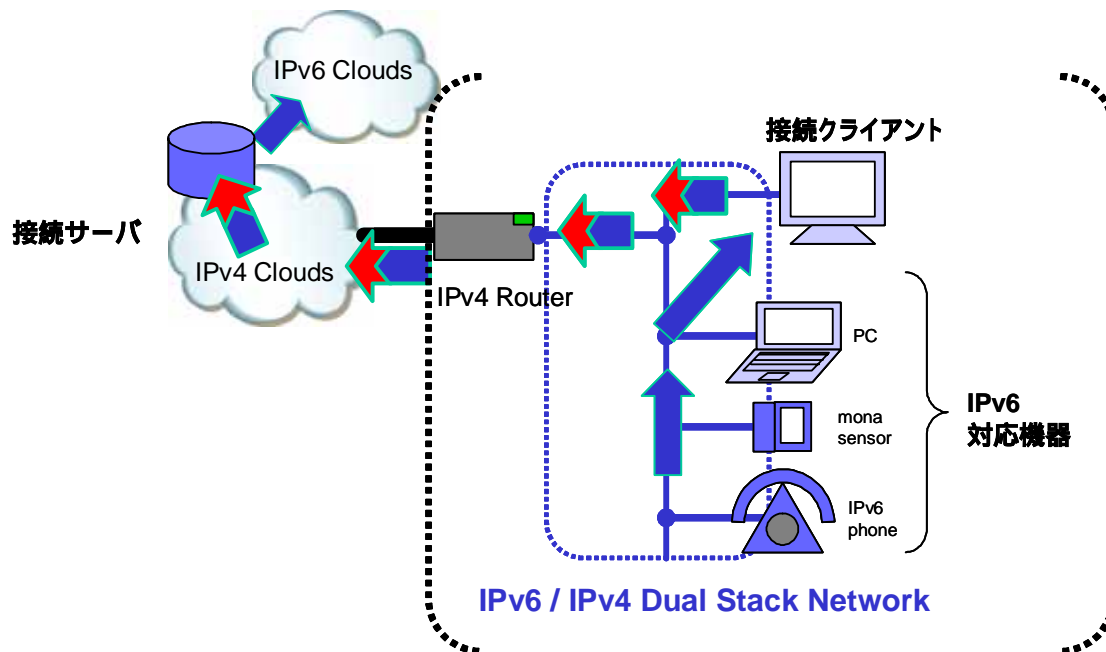


図9. ルータモード動作イメージ

ルータモードは以下のような特徴をもつ。

- PPP 仮想インタフェース以外のインタフェースに向けて RA を送信する。
- DHCPv6 PD の後、トンネルサーバより付与されたグローバルスコープの IPv6 プレフィックスから任意な IPv6 アドレスを選出し、そのアドレスを RA を送信する物理インタフェースに設定し、そのアドレスを用いて IPv6 通信を行なう。
- IPv6 パケットのフォワーディングを行なう。

接続クライアントがルータモードで動作し、IPv6 ルータとして動作するまでのシーケンスは図10の通りである。

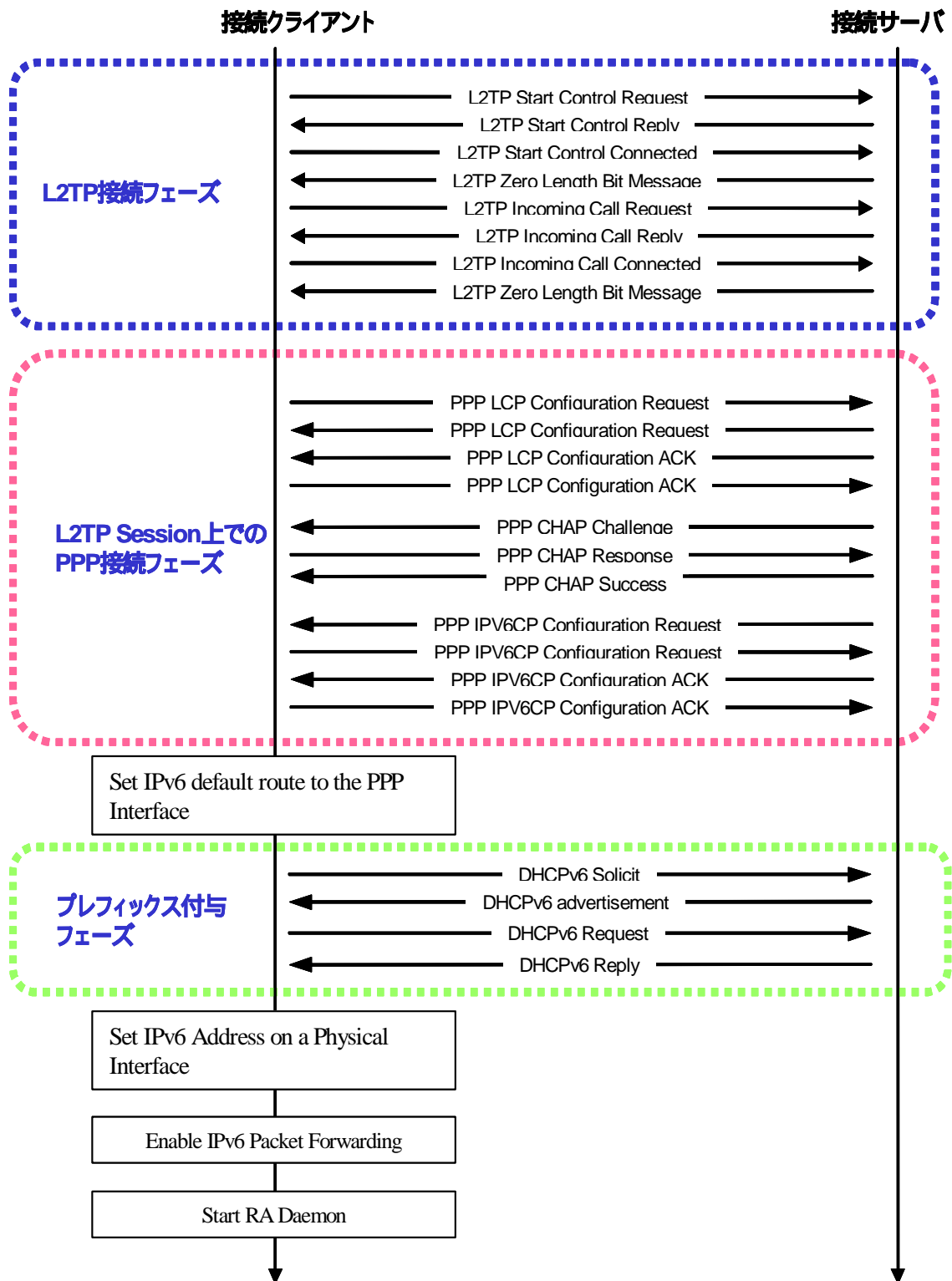


図 10. ルータモード起動シーケンス例(正常時)

4.2.4. 各種パラメータ既定値及び設定機能

以下に示すパラメータはコンフィグファイルの編集、もしくは GUI により設定可能とすること。

L2TP Hello のインターバル

- 60 秒とする。

PPP インタフェースの MTU

- RFC 2460 に記述されている IPv6 Minimum MTU の値である 1280 バイトから、Ethernet の MTU である 1500 バイトまでの間で調整可能とする。
- デフォルト値は 1390 バイトとする。

PPP Echo-Request のインターバル

- PPP LCP の”Echo-Request”メッセージのインターバルは 10 秒から 60 秒の間で可変とする。
- デフォルト値は 30 秒とする。

Router Advertisement (RA)の各種パラメータ (ルータモード時)

以下に、接続クライアント (ルータモード時) が RA を送信する際の Router Advertisement メッセージに関する各種パラメータのデフォルト値を定義する。

- 1 Max RA Interval
 - 30 秒
- 2 Valid Lifetime
 - 180 秒
- 3 Preferred Lifetime
 - 90 秒

上記 RA のパラメータは、接続クライアント (ルータモード時) と、その配下の IPv6 Hosts の間だけで有効なパラメータであるので任意に設定できるとする。

A. 付録

A.1. IPv6 に関する主な RFC 一覧

RFC 番号	RFC 名
1981	Path MTU Discovery for IP version 6
2375	IPv6 Multicast Address Assignments
2460	Internet Protocol, Version 6 (IPv6) Specification
2461	Neighbor Discovery for IP Version 6 (IPv6)
2462	IPv6 Stateless Address Autoconfiguration
2463	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6)
2464	Transmission of IPv6 Packets over Ethernet Networks
2472	IP Version 6 over PPP
3315	Dynamic Host Configuration Protocol for IPv6
3484	Default Address Selection for Internet Protocol version 6 (IPv6)
3513	IP Version 6 Addressing Architecture
3587	An IPv6 Aggregatable Global Unicast Address Format
3633	IPv6 Prefix Options for DHCPv6

A.2. 改版履歴

第 1.0 版 初版