NTT

NTT Information Sharing Platform Laboratories
NTT 情報流通プラットフォーム研究所

いまからはじめるIPv6
IPv6ネットワーク構築基礎

NTT情報流通プラットフォーム研究所
ネットワークセキュリティプロジェクト
岡田　真悟

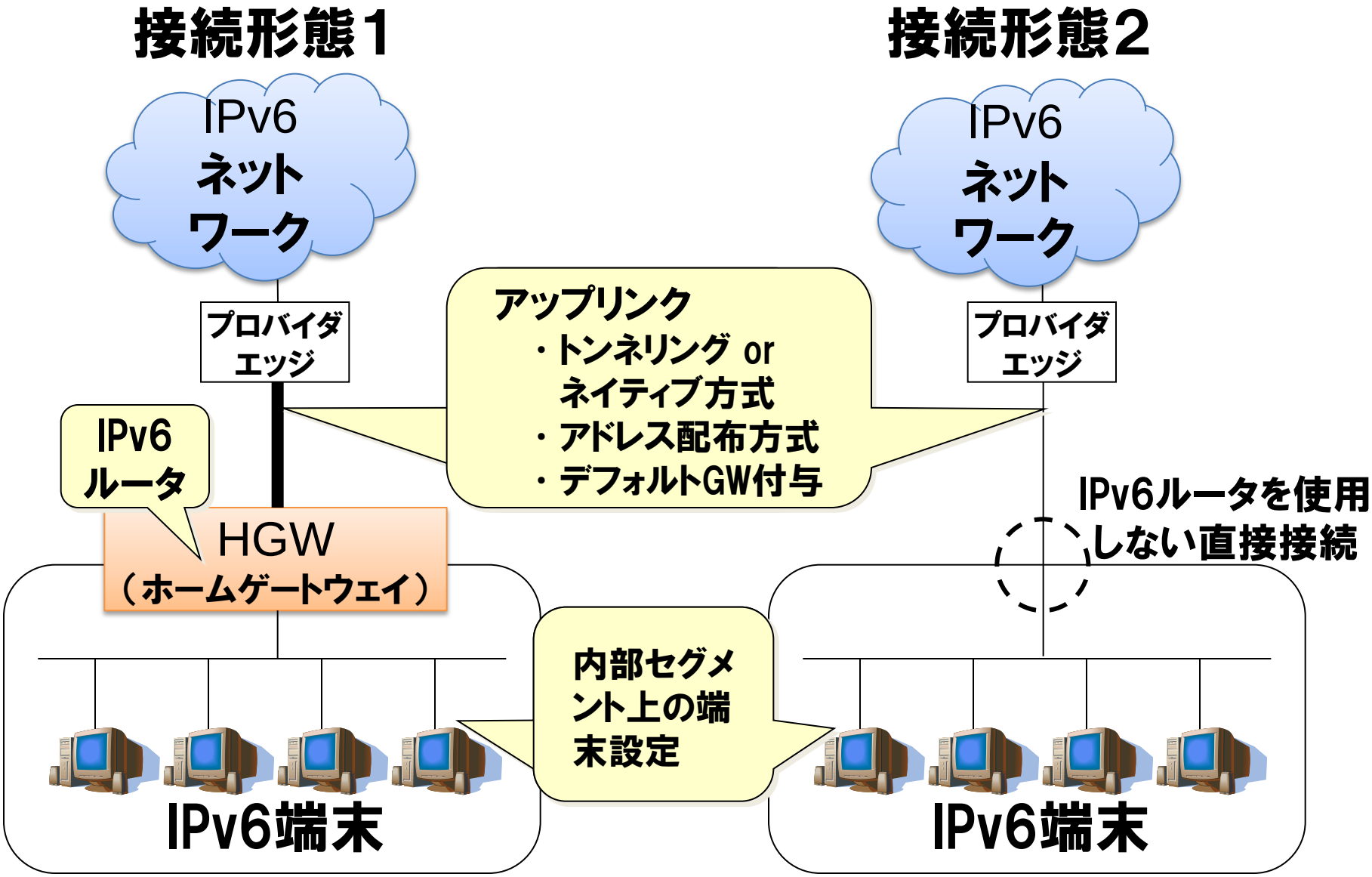
本セッションの目的とアウトライン

- 目的
  - 家庭・SOHO環境を対象としたIPv6ネットワーク構築法の解説

- 主なトピック
  - IPv6インターネットへの対外接続の確保
  - IPv6アドレス割り当てとデフォルトルータの配布方式
  - LAN内部での端末設定のアドレス設定
  - デュアルスタックネットワーク
  - 家庭・SOHO環境でのセキュリティ

  [付録]
    - ヤマハ製ブロードバンドルータRT58iにおける設定例
    - ステートレスDHCPv6サーバの設定例
    - 家庭・SOHO向けIPv6ルータの現状

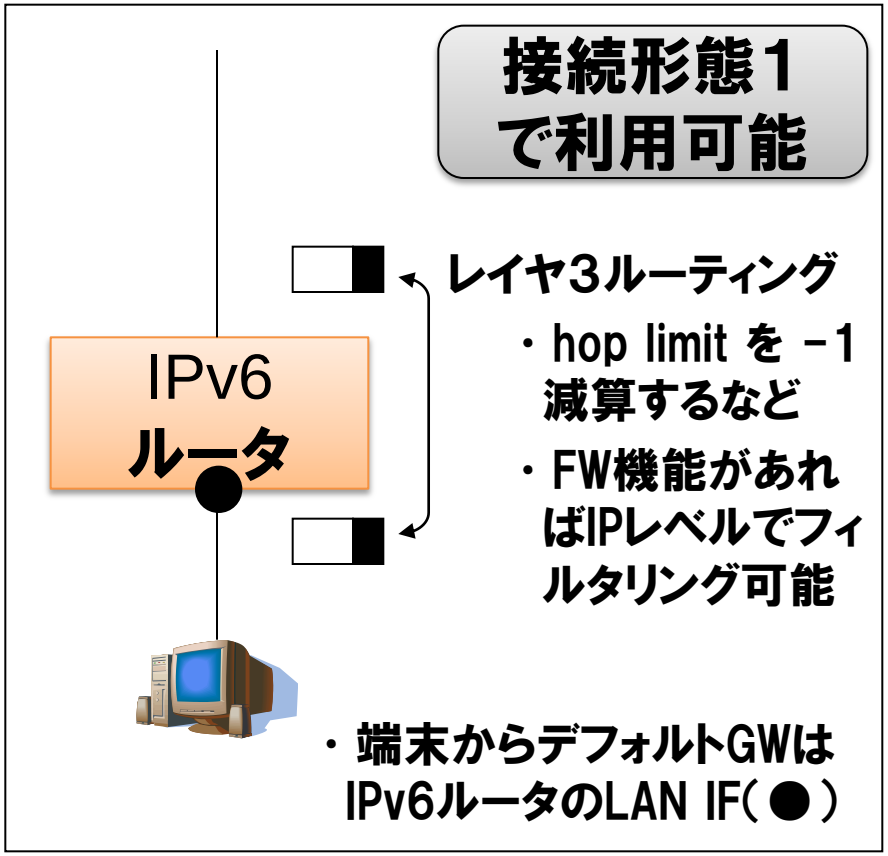
本セッションの想定ネットワーク

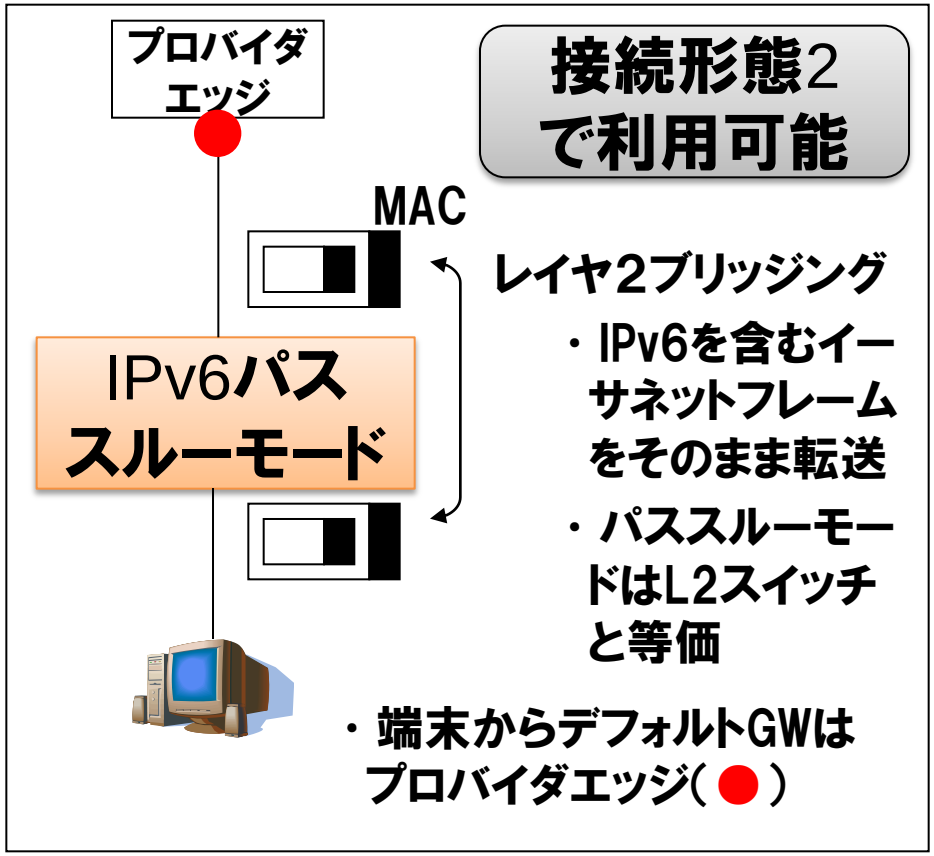


ルータの「IPv6対応」表記の注意点

ルータのパッケージに「IPv6対応」表記は2通りの機能の場合がある
- IPv6ルータ　　：接続形態1で利用
- IPv6パススルーモード　：接続形態2で利用

用途にあった製品を選ぶ必要がある





本日のセッションについて

- 目的
  - 家庭・SOHO環境を対象としたIPv6ネットワーク構築法の解説
- 主なトピック
  - IPv6インターネットへの対外接続の確保
  - IPv6アドレス割り当てとデフォルトルータの配布方式
  - LAN内部での端末設定のアドレス設定
  - デュアルスタックネットワーク
  - 家庭・SOHO環境でのセキュリティ

  [付録]
    - ヤマハ製ブロードバンドルータRT58iにおける設定例
    - ステートレスDHCPv6サーバの設定例
    - 家庭・SOHO向けIPv6ルータの現状

接続形態1，2の両形態を対象とした説明

接続形態1（HGW有り）を対象とした説明

IPv6インターネットへの対外接続の確保

現在または近い将来に利用できる
対外接続サービスや技術の紹介

IPv6接続サービスの現状

個人向け・法人向けともに提供ISPが増えてきており選択肢が広がりつつある

- IPv4アドレス枯渇対応タスクフォースで取りまとめられている
  - 2010年11月15日時点で13社64サービス

IPv4 EXHAUSTION IPv4アドレス枯渇対応タスクフォース

お問い合わせ RSS | Google™カスタム検索 検索 | 日本語 ENGLISH

概要 ABOUT TF | ニュース NEWS | セミナー&イベント SEMINAR&EVENT | 活動報告等 ACHIEVEMENTS | 参加団体 MEMBER | よくある質問 FAQ

IPv6サービスリスト

2010年11月15日時点で13社64サービスを掲載しています。
掲載されたサービスの品質、記述内容の信憑性に関しては、タスクフォースでは関知しておりません。
掲載をご希望の場合は応募要領をご覧ください。

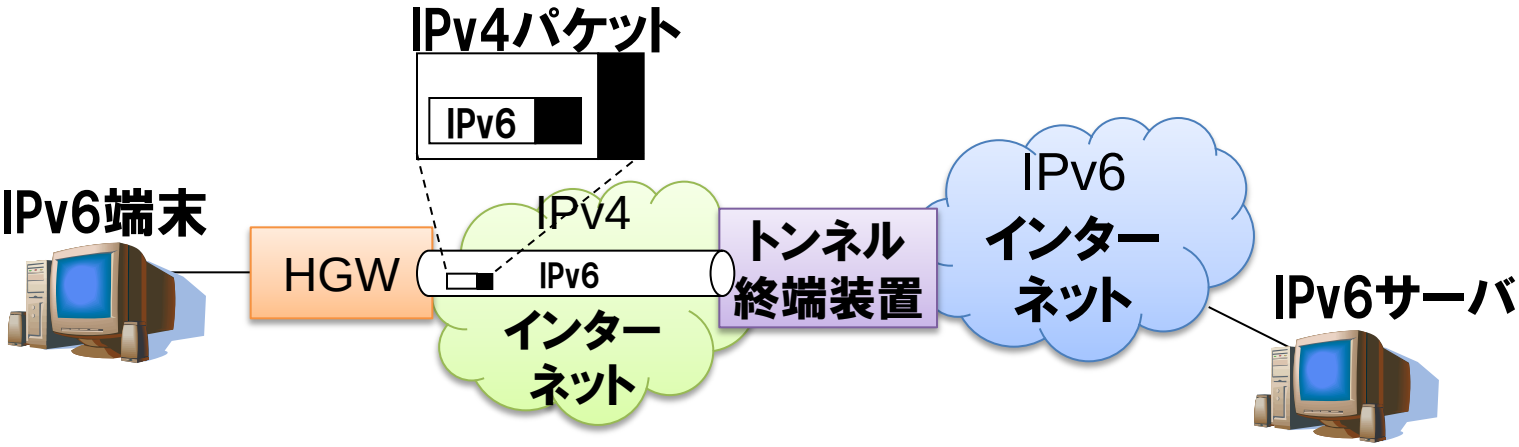
- あ行 株式会社インターネットイニシアティブ、NTTコミュニケーションズ株式会社
- か行 株式会社グローバルネットコア
- さ行 GMOホスティング & セキュリティ株式会社、ソフトバンクテレコム株式会社、ソフトバンクテレコム株式会社/日本インターネットエクスチェンジ株式会社
- た行 株式会社電算、株式会社ドリーム・トレイン・インターネット
- な行 有限会社ナインレイヤーズ、日本インターネットエクスチェンジ株式会社
- は行 株式会社ビーコンエヌシー、フリービット株式会社、Verio,Inc.(NTTコミュニケーションズグループ)

事業者名	サービス名称	サービスカテゴリ	サービス内容	URL
株式会社電算	avis	アクセス	IPv6トンネル接続サービス	http://www.avis.ne.jp/service/ipv6.htm
		アクセス	イーサネット専用線接続サービス	http://www.avis.ne.jp/service/lease-line.htm
		アクセス	構内(データセンター内)専用線接続サービス	http://www.avis.ne.jp/service/premises.htm

（出典）http://www.kokatsu.jp/blog/ipv4/data/ipv6service-list.html

スタティック（IPv6 over IPv4）トンネル

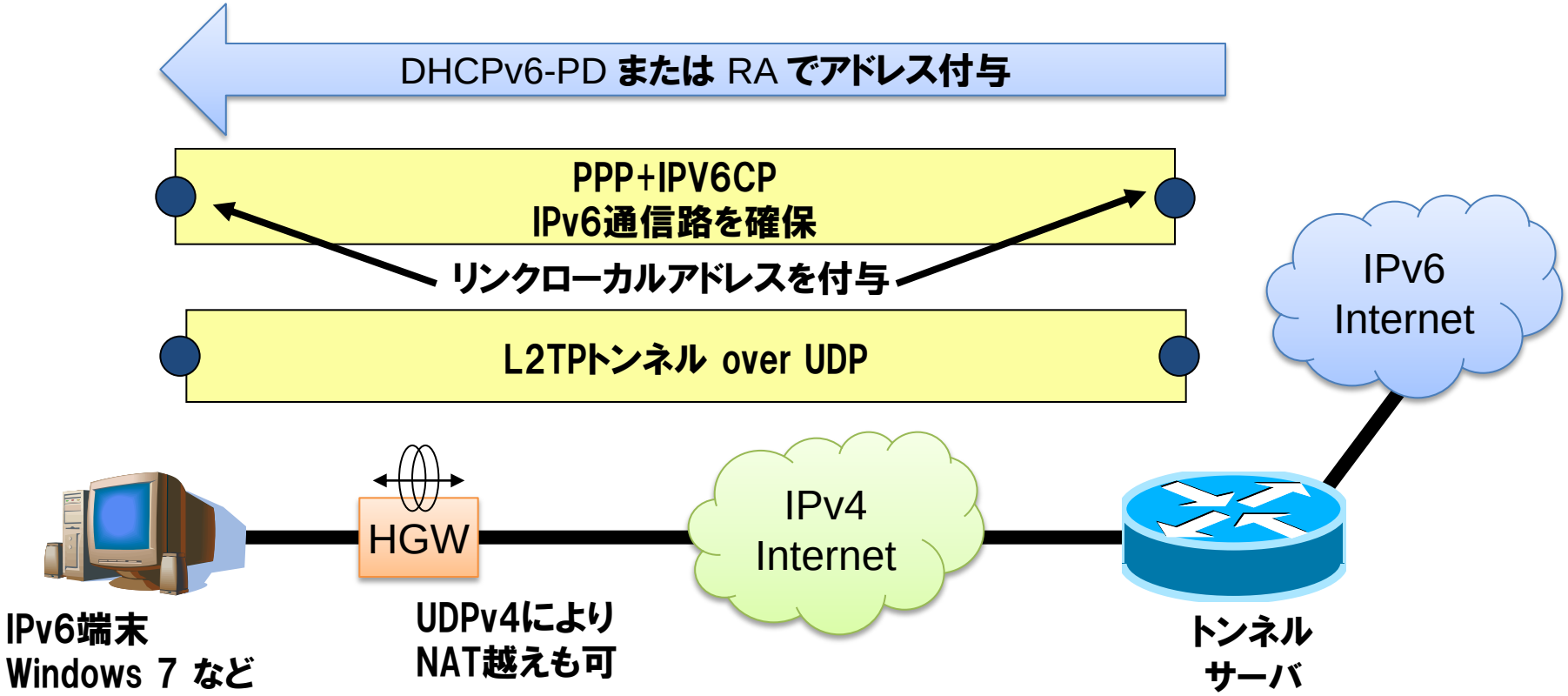
・IPv4インターネット上で IPv6パケットをカプセル化して転送する方式



・いくつかの主要ISPが固定IPv4アドレスユーザ向けに提供
  ・代表例
    ・OCN ： OCN IPv6トンネル接続サービス
    ・IIJ　 ： IPv6トンネリングサービス
    ・Yahoo!BB ： IPv6インターネットサービス
・HGW, 終端装置の双方にIPv4アドレスを指定する設定が必要
・IPv6端末から直接トンネルを張る場合、HGWを通す設定が必要

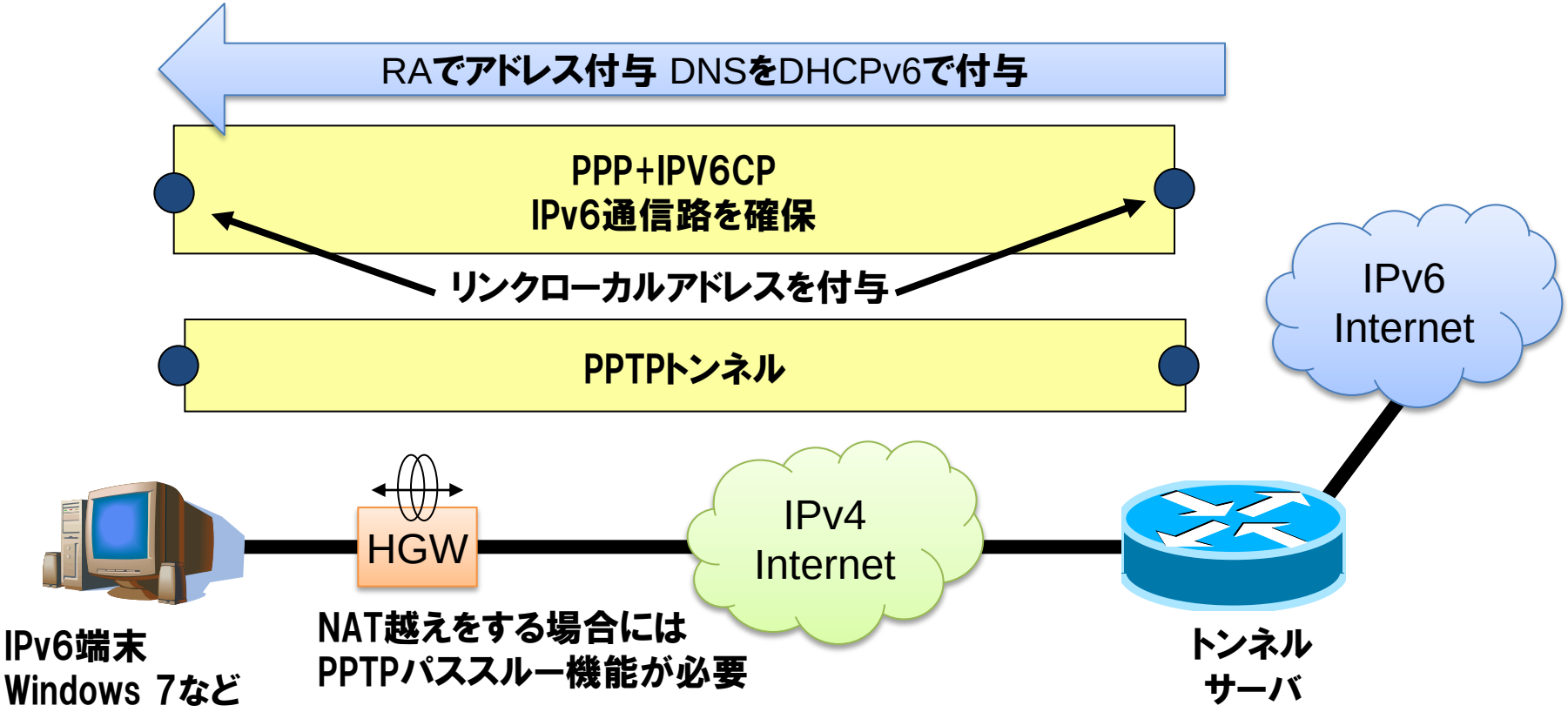
NTT OCNによる個人向けIPv6インターネット接続サービス

- OCNが有償で提供するオプションサービス
- 固定IPv4アドレスは不要
- プライバシーに配慮し 二つのプレフィックスを選択可
  - 固定プレフィックス（/64ひとつ）
  - 動的プレフィックス（接続のたびに値が変わる /64をひとつ）両者を使用可能
- Windows XP, Vista, 7端末のサポートの他、コレガ社から対応ルータが発売されていた



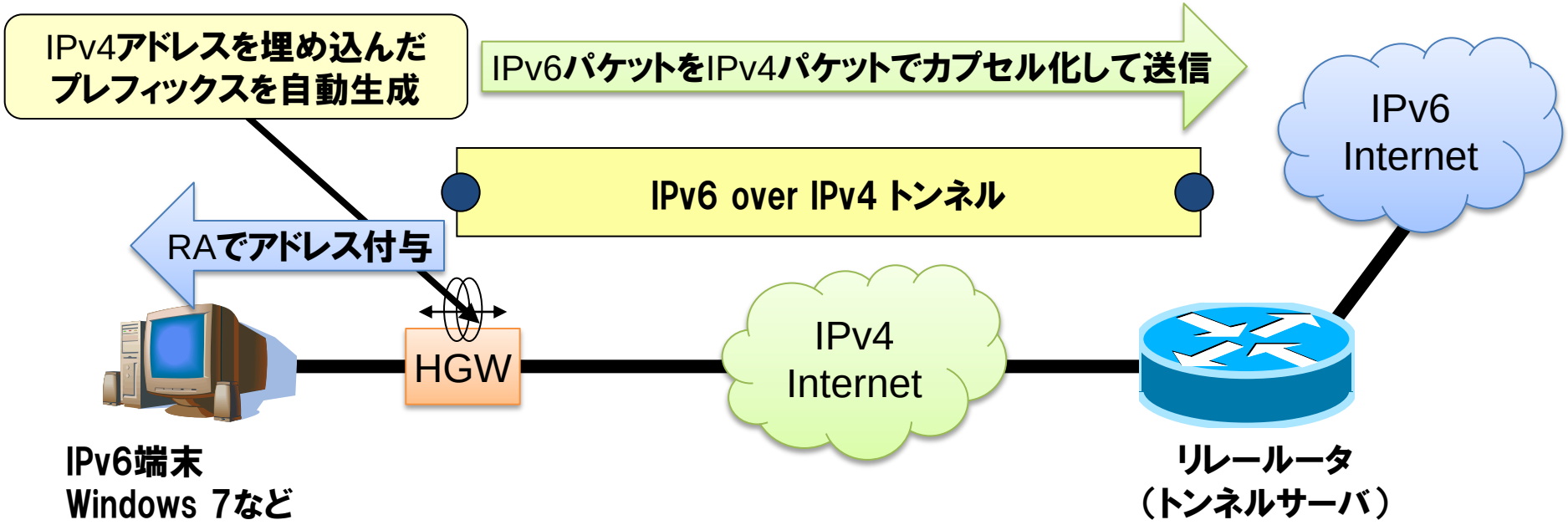
IIJによる個人向けIPv6インターネット接続サービス

- IIJが自社の顧客向けに無償で提供するオプションサービス
- 固定IPv4アドレスは不要
- /64 サイズのプレフィックスが付与される



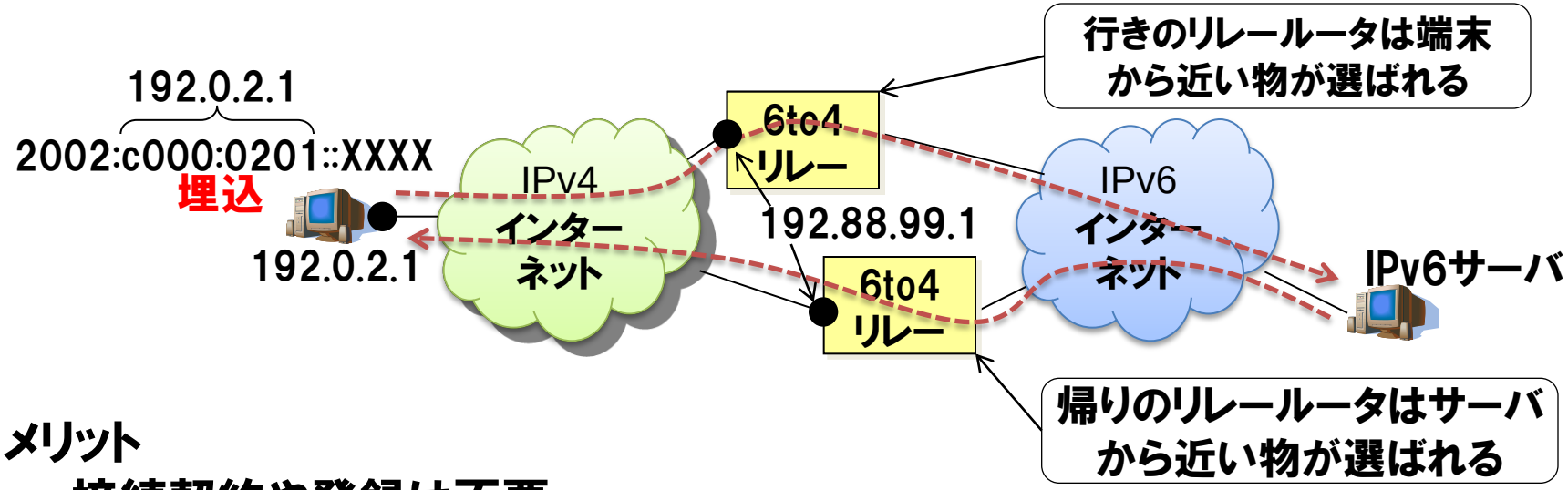
NTT Yahoo!BBによる個人向けIPv6インターネット接続サービス

- Yahoo!BBが自社の顧客向けに無償で提供するオプションサービス
- 6rdという IPv6 over IPv4 トンネル技術を利用
  - 6to4と類似の技術。リレールーターはISPのものを利用する。
- HGWからトンネルを張るので、HGWの設定変更で利用可能
- IPv4アドレスをベースとしたプレフィックスをHGWが自動生成する



自動トンネル接続技術 6to4

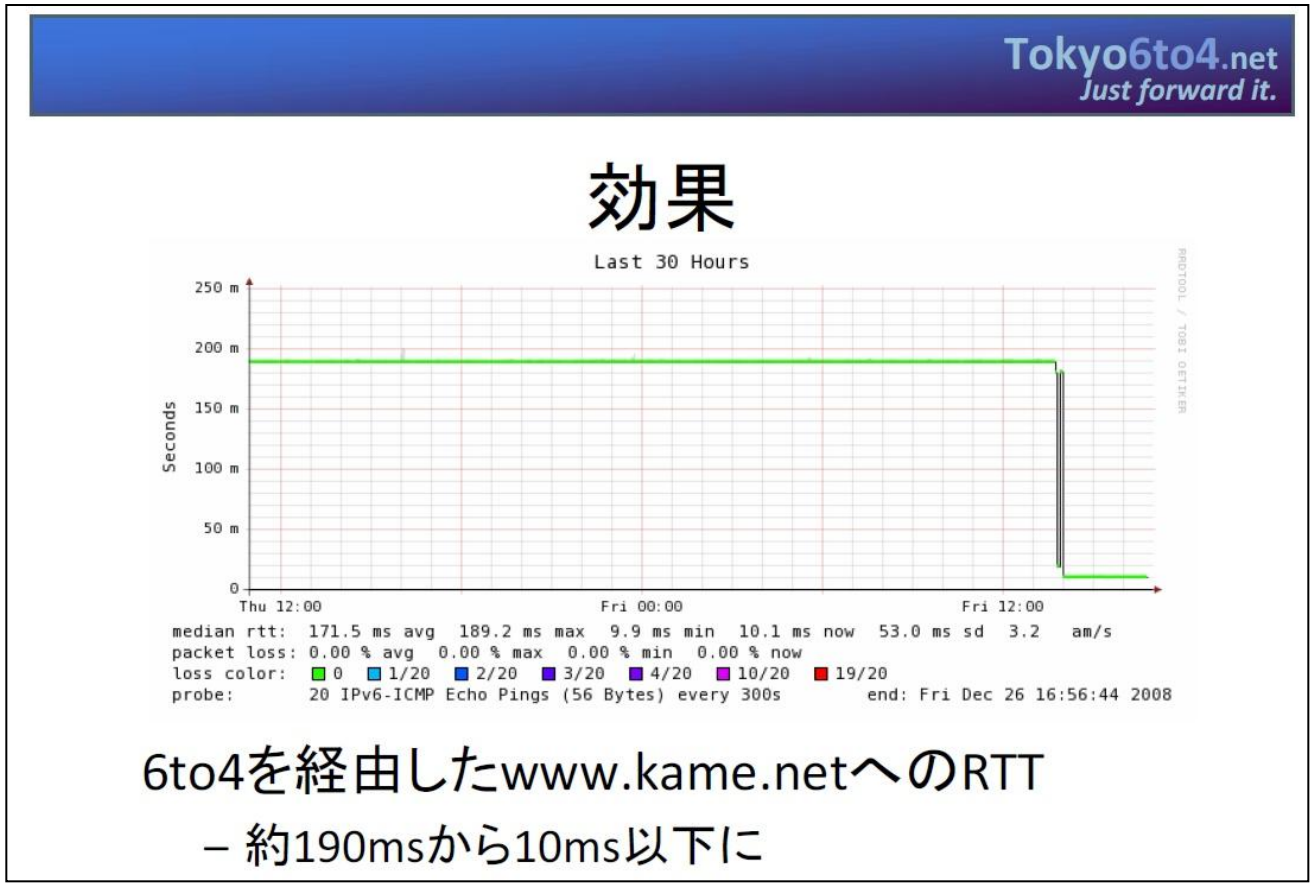
トンネル設定が不要なIPv6インターネット接続性確保技術



- メリット
  - 接続契約や登録は不要
  - IPv4アドレスをベースとしたプレフィックスを自動生成する
  - RFC3056にて仕様が規定されており、実装が豊富（Win, Mac, UNIX, ブロードバンドルータも存在）
    - Windows Vista, 7 では標準機能として提供される
- デメリット
  - 経路制御が難しい（行きと帰りが非対称）
  - IPv4グローバルアドレスを必要とする
  - リレールータの信頼性に課題(どこのリレールータを通るかわからない)

Tokyo6to4 プロジェクト

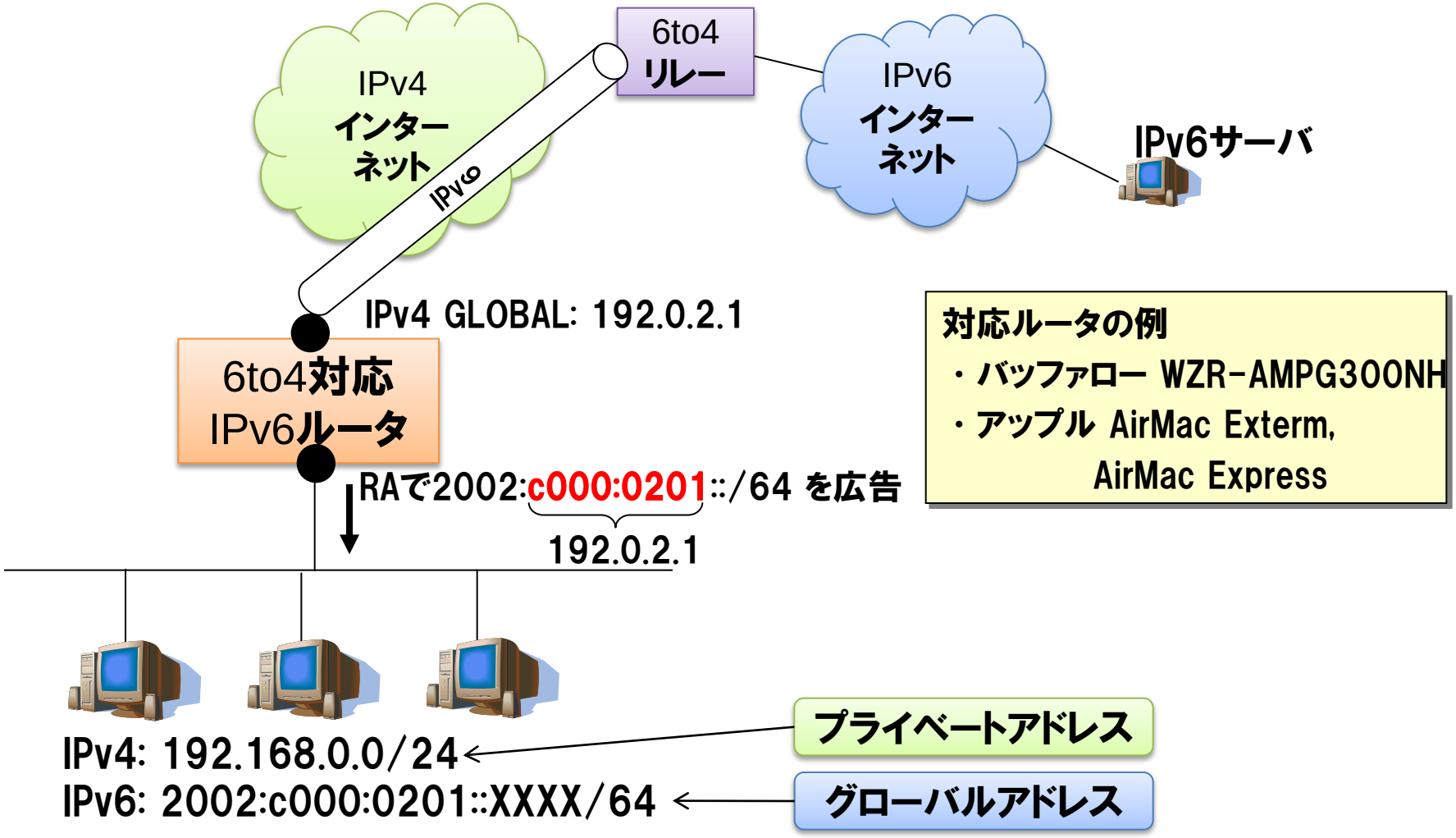
- 日本国内(JPIX)で、6to4リレールータが実験運用されている
- IPv6インターネットへの接続性が改善



(出典) http://www.tokyo6to4.net/

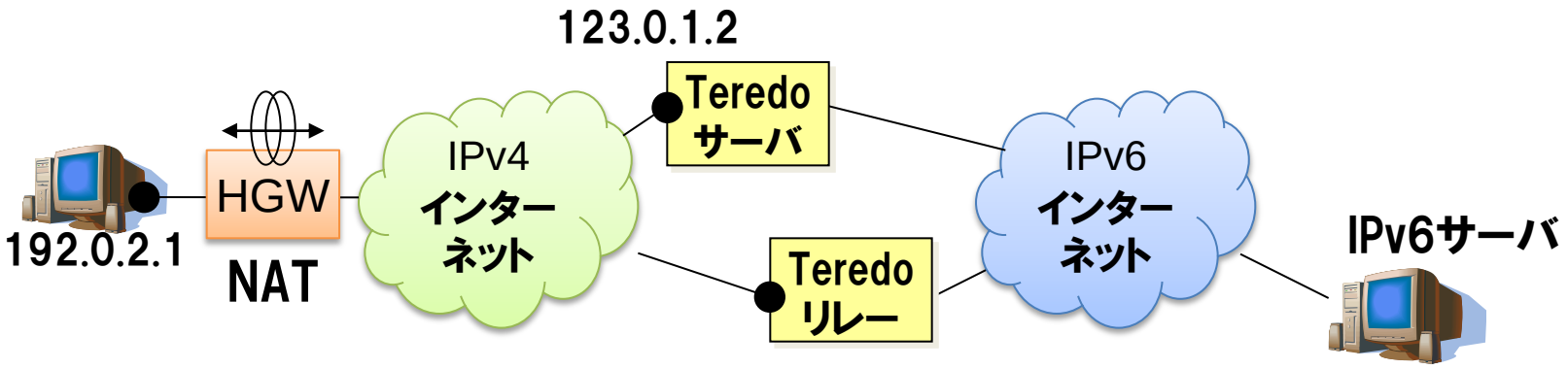
NTT 6to4対応ブロードバンドルータを使った外部接続

プライベートIPv4アドレスをもつデュアルスタック端末でもIPv6外部接続が可能



NTT NAT越えが可能な自動トンネル接続技術 Teredo（1）

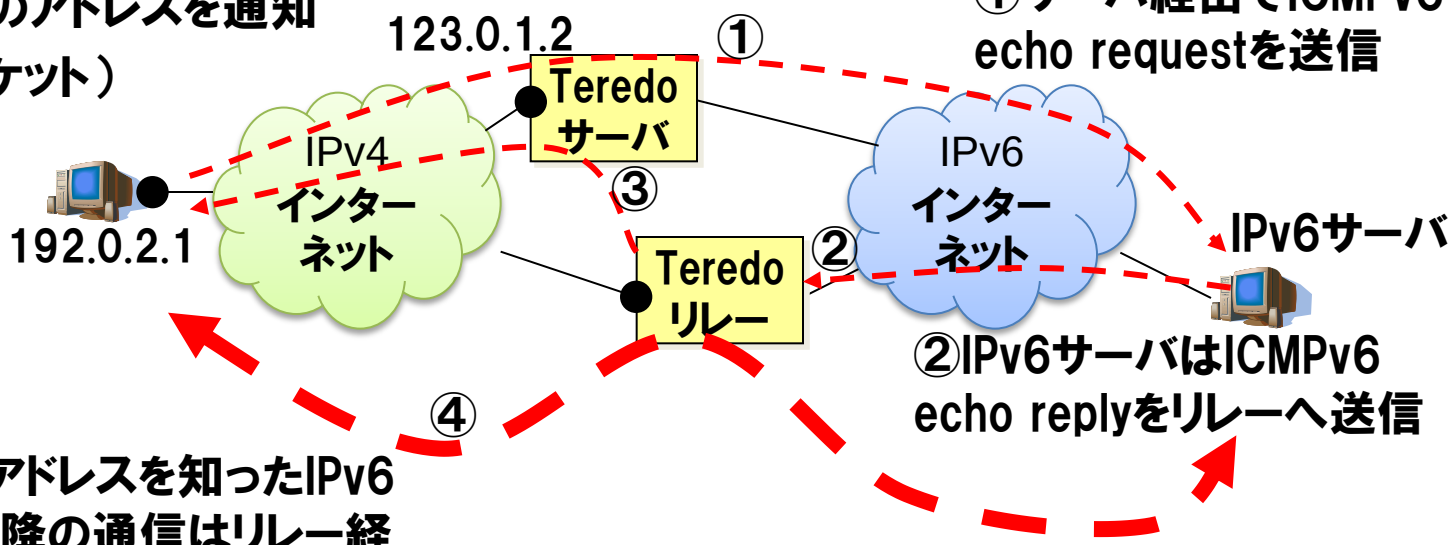
トンネル設定が不要なIPv6インターネット接続性確保技術



- メリット
  - 6to4と同様に接続契約や登録は不要
    - IPv6アドレスをIPv4アドレスから自動生成する
  - NATに対応。プライベートIPv4アドレスの端末でも使用可能
    - Symmetric NAT は対応が難しい
  - Windows Vista, 7 では標準機能として提供される
- デメリット
  - パブリックに利用可能なサーバー・リレールータが少ない
  - IPv6アドレスが端末情報を多く含む セキュリティ面の懸念
    - 待受（開放済み）ポートなどの情報が含まれるため

Teredoの動作例

③リレーはサーバ経由で、端末へリレーのアドレスを通知（バブルパケット）



①サーバ経由でICMPv6 echo requestを送信

②IPv6サーバはICMPv6 echo replyをリレーへ送信

④リレーのアドレスを知ったIPv6端末は、以降の通信はリレー経由で通信を行う（対称経路）

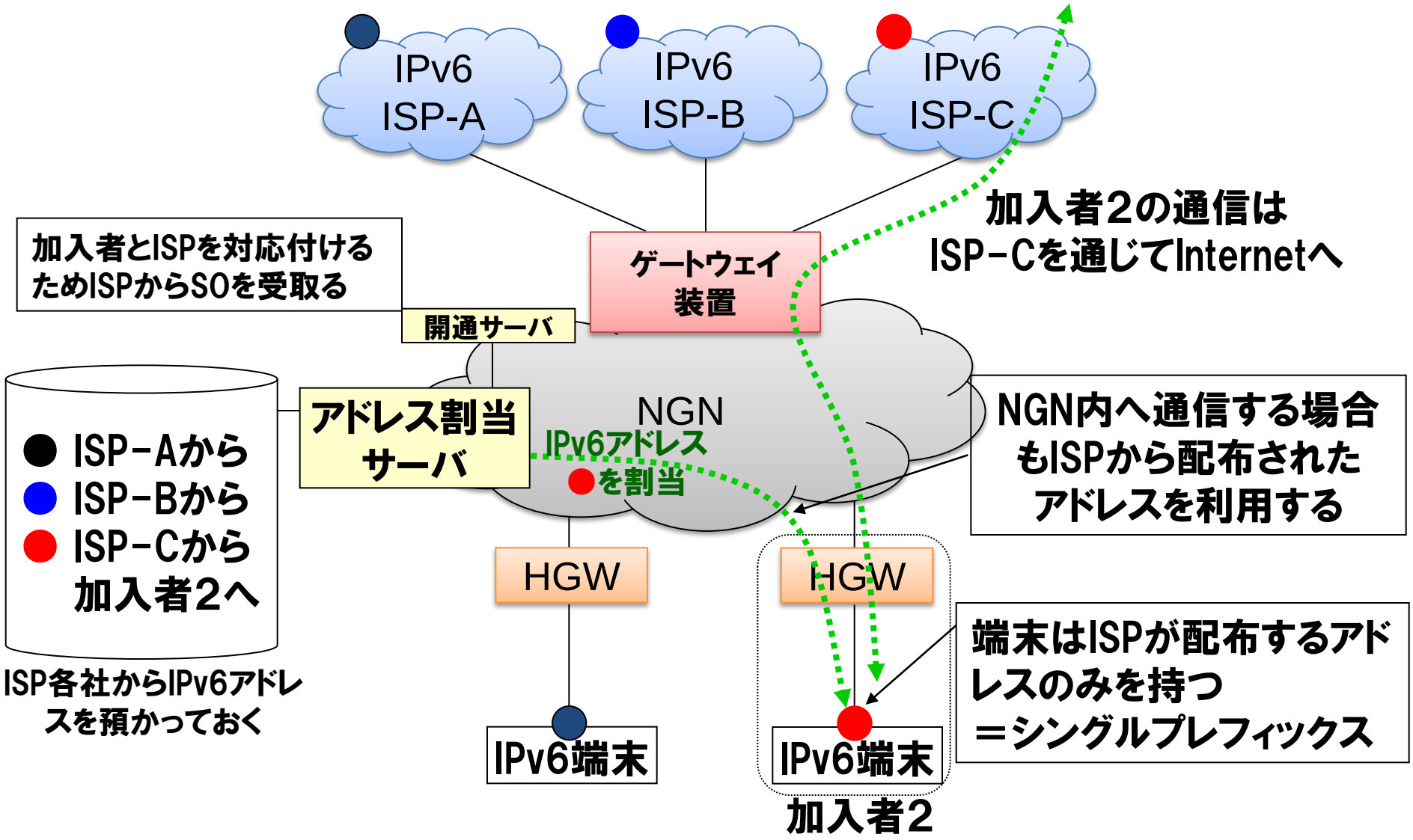
32ビット		16ビット	16ビット	32ビット
2001:0000:	[サーバのIPv4アドレス] :	[フラグ] :	[ポート] :	[端末のIPv4アドレス]
	123.0.1.2	NATタイプ判定	端末の待受ポート	192.0.2.1

その他のトンネルブローカー

- フリービット feel6（DTCP） - http://start.feel6.jp/
  - /48サイズのプレフィックスを委譲（サイト内で再委譲が可能）
  - 固定/48 が無料で使用可能
  - Windows, Mac OS, Linux など広範なOSのサポート
  - ヤマハ製のブロードバンドルータ（RTシリーズ）がサポート
  - NAT越えには工夫（プロトコル番号41のマッピング）が必要

- Hexago freenet6（TSP） – http://www.gogo6.com/
  - 無料で利用可能
  - ソフトウェアGPLで公開されており、多くの機種で動作可能
  - NAT越えに対応している
  - トンネル終端サーバが北米にあるため国内からの接続はやや不利

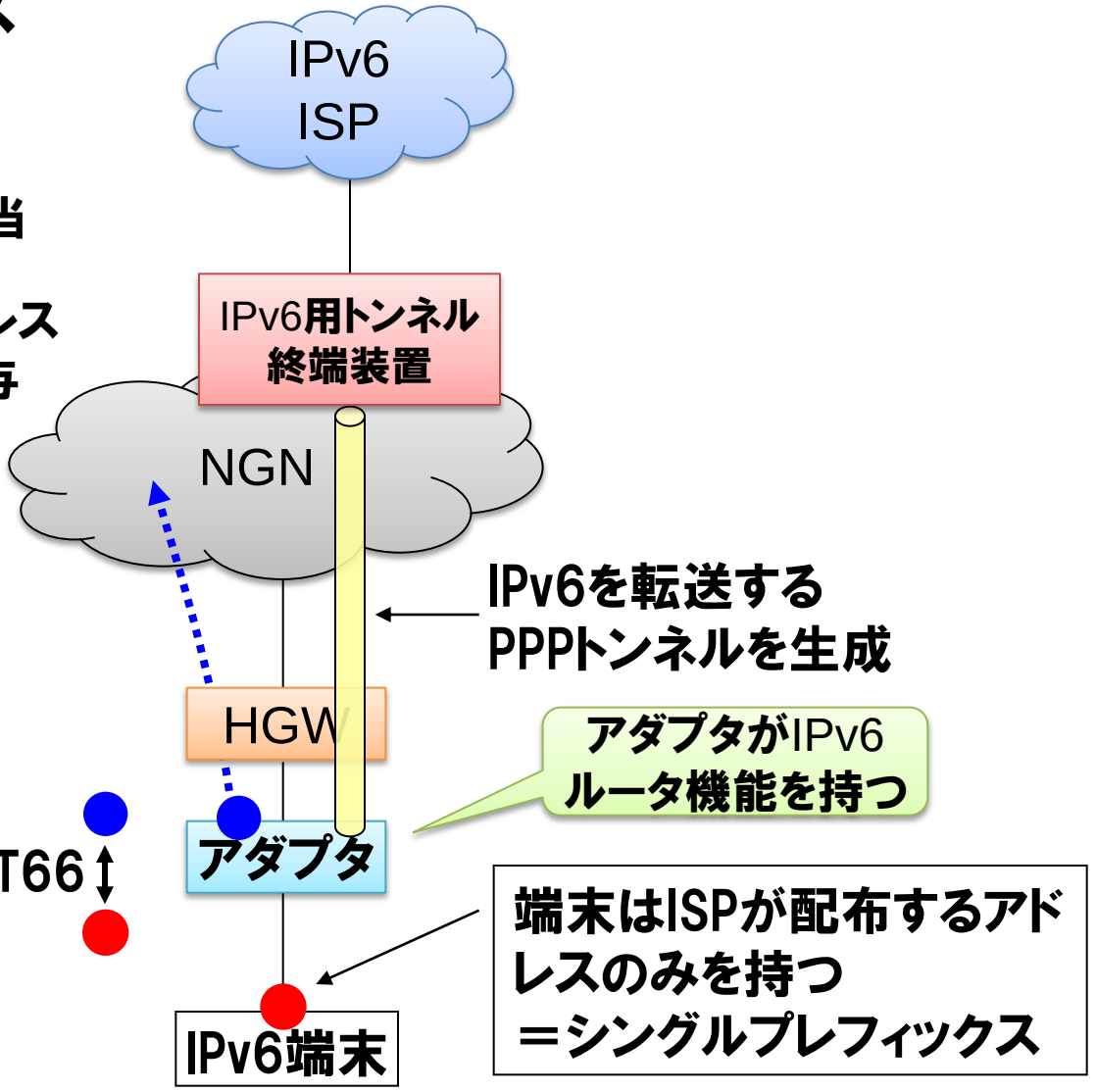
NTT NGNが提供予定のIPv6インターネットアクセス（ネイティブ方式）



NGNが提供予定のIPv6インターネットアクセス（トンネル方式）

■2種類のIPv6アドレス

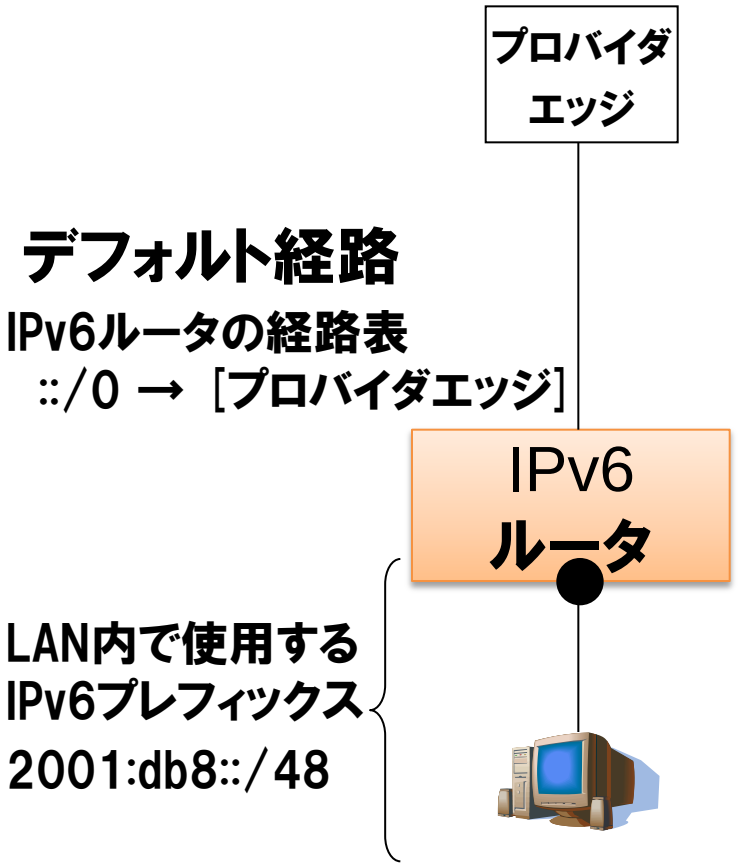
- ISP事業者が割り当てる IPv6アドレス トンネルを通じて端末へ割当
- NGNが割り当てるIPv6アドレス アダプタのWAN側I/Fに付与



IPv6アドレス割り当てと
デフォルトルータの配布方式

ISPなどから家庭・SOHOネットワークへの
IPv6アドレス割り当て及びデフォルトルータ
の配布方式について

IPv6アドレスの配布とデフォルト経路の設定



IPv6アドレスの割り当て方法

(1) 手動割り当て

- IPv6ルータにアドレス情報をあらかじめ手動設定しておく方法
- IPv6アドレス情報は書面等で通知
- 外部接続がスタティックトンネルの形態で使われることが多い

(2) 自動割り当て

- ISPからRA, DHCPv6などの自動設定プロトコルを使ってアドレスを通知する
- 固定アドレス割り当てが一般的だが動的な割り当て行う運用も可能

IPv6アドレスの自動割り当て方式

ステートレスアドレス生成

RA

プロバイダ
エッジ

64ビットのIPv6プレフィックスを通知
2001:db8:a::/64

MACなどから下位64ビットを生成しIPv6アドレス生成（下位64ビットをランダムに生成する端末もある）

I/F

2001:db8:a:: [mEUI64]

ステートフルアドレス割り当て

DHCPv6

プロバイダ
エッジ

128ビットのIPv6アドレスを割り当て
2001:db8:a::1234

I/F

2001:db8:a::1234

DHCPv6-PD
Prefix Delegation

プロバイダ
エッジ

プリフィリックスを委譲（delegation）する
2001:db8:a::/48

WAN

IPv6ルータ

LAN 2001:db8:a::1

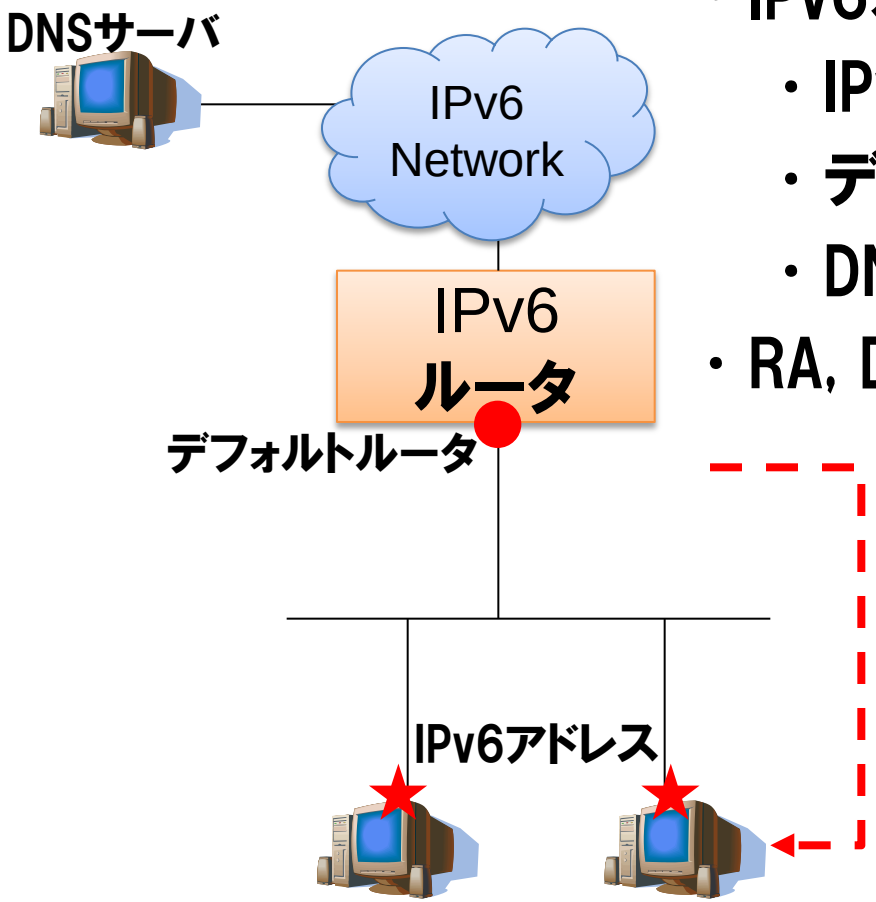
2001:db8:a::/64

IPv6ルータは端末へIPv6アドレスを再配布する

LAN内部の端末設定

接続形態1（HGW有り）の時、つまり
IPv6ルータを管理する際のLAN内部
の端末設定について

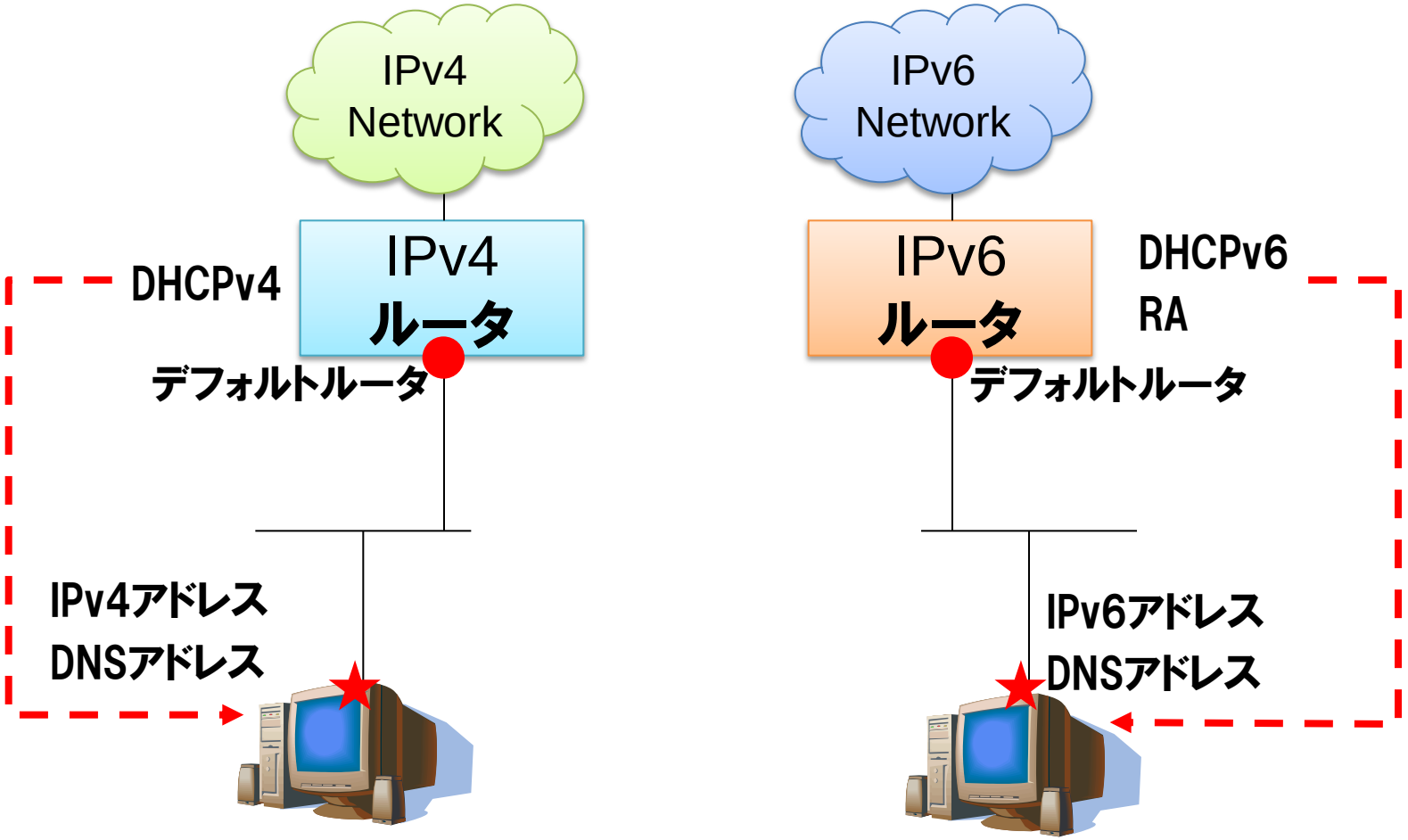
家庭・SOHOのLAN内部の端末設定



- IPv6ルータから端末へ付与する情報
  - IPv6アドレス
  - デフォルトルータアドレス
  - DNSサーバアドレス
- RA, DHCPv6の利用が一般的

端末OSは Windows Vista, 7 などを想定

IPv4ネットワークとIPv6ネットワーク



一見大きな違いがないように見えるが・・・

DHCPv4とDHCPv6の違い

DHCPv4	DHCPv6
・IPv4アドレス	・IPv6アドレス
・サブネットマスク	・サブネットマスク　なし！
・デフォルトゲートウェイ	・デフォルトゲートウェイ　なし！
・DNS情報	・DNS情報
・その他付加的情報（NTP, SIP など）	・その他付加的情報（NTP, SIP など）
・端末識別はMACアドレス	・端末識別はDUID

DHCPv6はデフォルトゲートウェイ付与不可
Router Advertisement（RA）の併用が必要

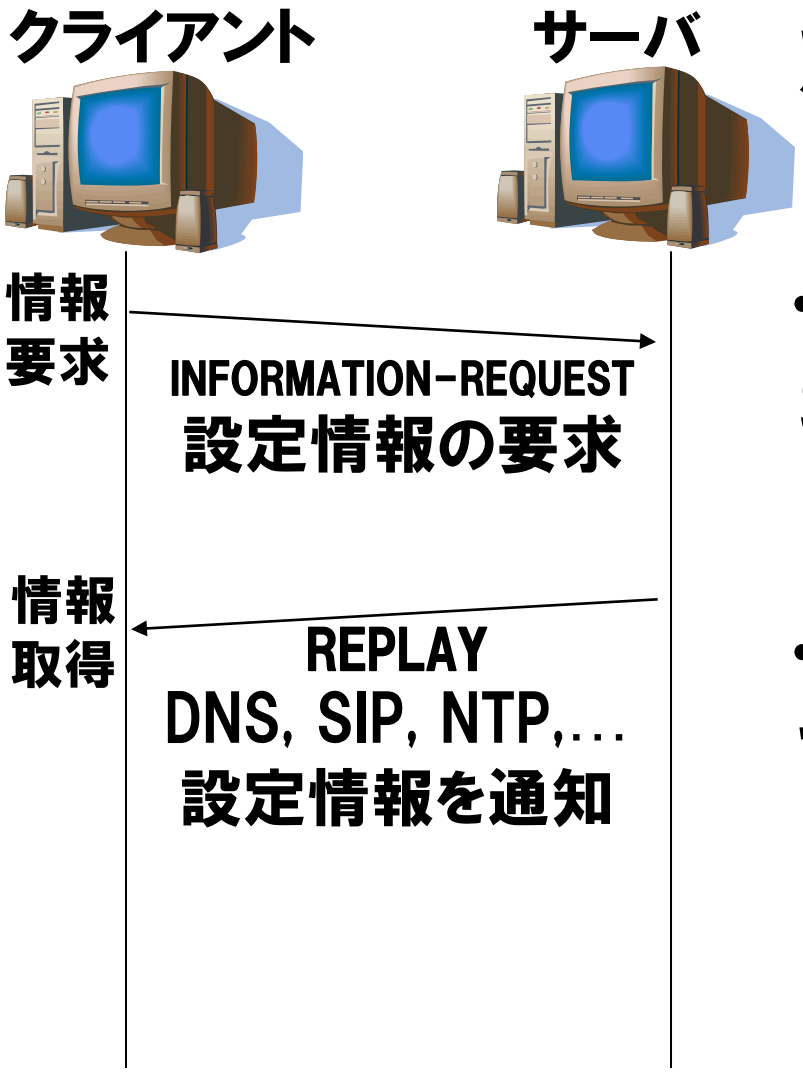
DHCPv6とRAの連携によるアドレス付与

- Router Advertisement（RA）
  - 本来の役目は「ルータの存在」を「広告」するもの
    - ⇒ 端末はRAの送信元をデフォルトゲートウェイに設定
  - アドレス情報（prefix information option）はオプション
    - ⇒ アドレス情報なしのRAもありえる
  - DNSアドレス情報はRAでは通知不可（**オプションがない**）
    - ⇒ **DHCPv6との併用が必要！**

RAがもつ2つのフラグ：M/O flags（Managed/Other）

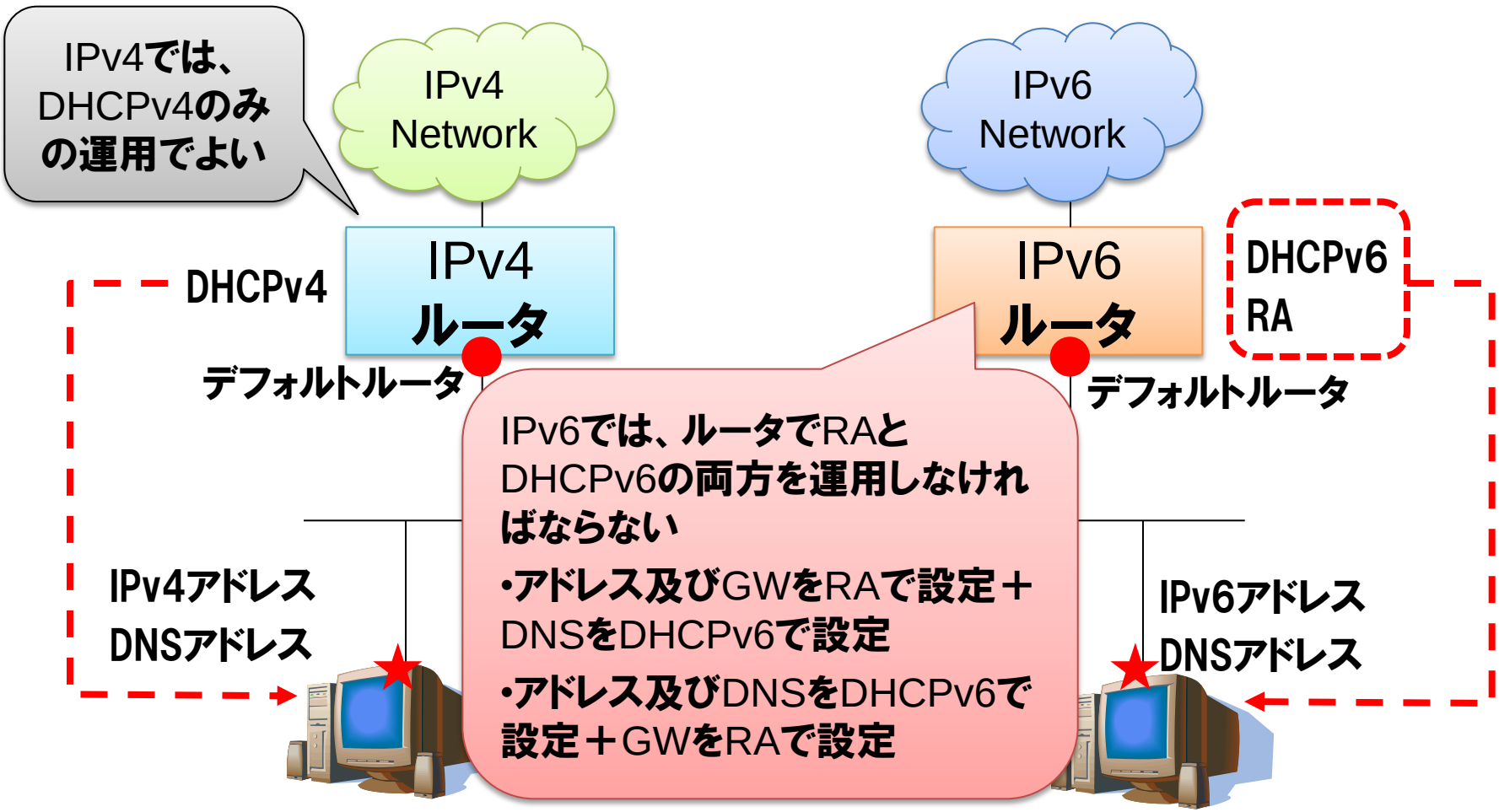
Mフラグ	Oフラグ	端末の動作
OFF（0）	OFF（0）	アドレスはRA，それ以外の情報（DNS等）は手動等の別手段で構成
OFF（0）	ON（1）	アドレスはRA，それ以外の情報はDHCPv6で構成
ON（1）	OFF（0）	アドレスはDHCPv6，それ以外の情報は手動等の別手段で構成
ON（1）	ON（1）	アドレス及びそれ以外の情報をDHCPv6で構成

stateless-DHCPv6（RFC3736）



- サーバがクライアントの状態を管理しない
- 端末の設定情報（DNS, SIP, NTP）のみを渡す
- １往復（２メッセージ）だけで情報を取得

IPv4ネットワークとIPv6ネットワークの違い



※RAのDNS Option及びDHCPv6のGW Optionが現在標準化中のため将来的には片方のみでよくなる可能性有り

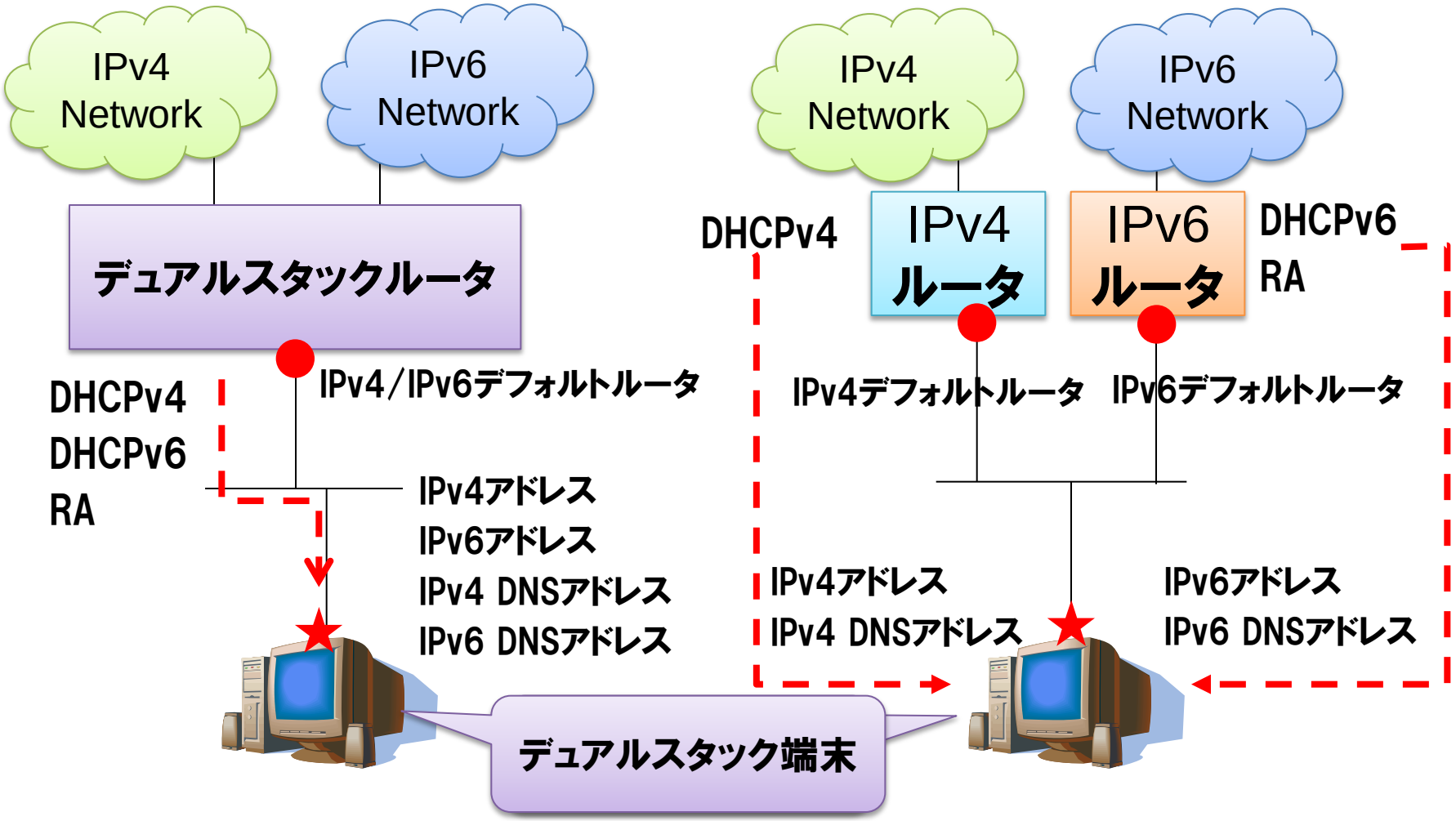
デュアルスタックネットワーク

現状ではIPv6ネットワークのみではできることが
少なく、IPv4インターネットのほうが遙かに巨大
そこで必要になるのがデュアルスタックネットワーク

デュアルスタックとは

- デュアルスタックネットワーク
  - IPv4とIPv6の両方の端末を同時に利用できるネットワーク
    - メリット
      - IPv4のみの端末もIPv6のみの端末も両方利用することが可能
    - デメリット
      - IPv4とIPv6は互換性がないため、IPv4とIPv6の二つのネットワークを同時に管理することになる
- デュアルスタック端末
  - IPv4とIPv6を同時に利用できる端末
    - IPv4ネットワーク、IPv6ネットワーク、デュアルスタックネットワークの全てで利用できる
    - IPv6対応のOS・端末はIPv4とIPv6を同時に利用できるデュアルスタック端末になっていることが多い
      - Windows, Mac, Linux, UNIXなど

デュアルスタックネットワークの構成



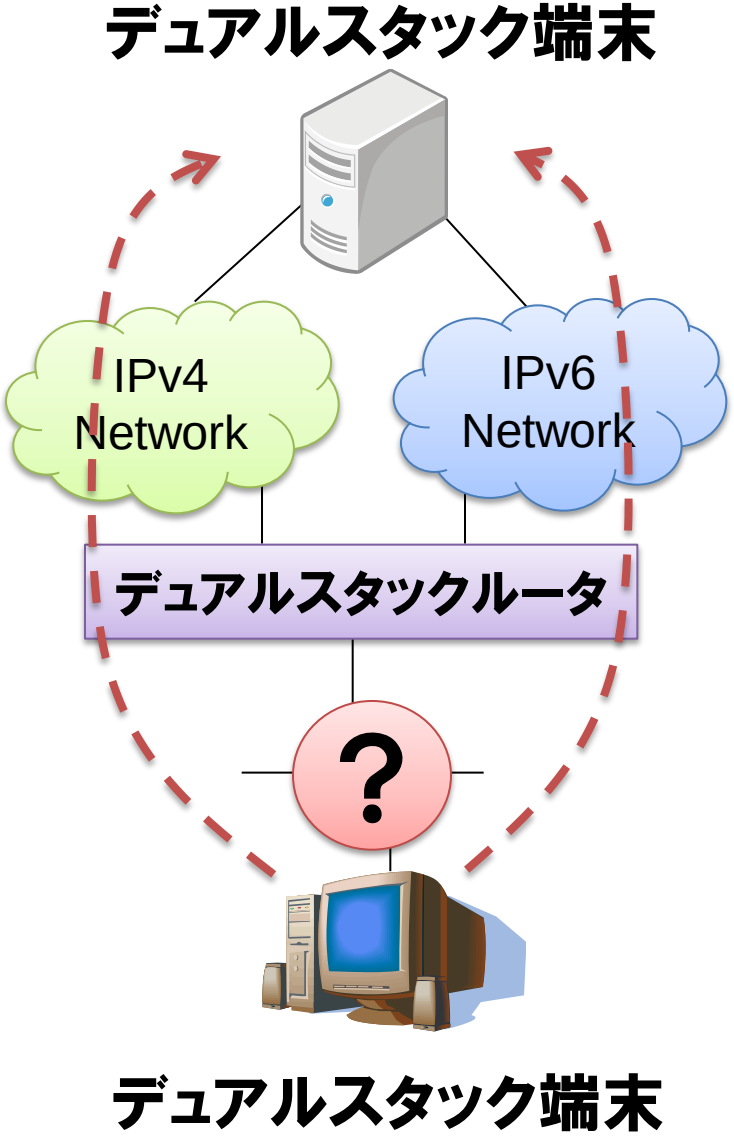
1台のルータでIPv4/IPv6の両機能を運用する、もしくは
2台のルータでIPv4/IPv6の機能をそれぞれ運用する

デュアルスタックネットワークの注意点

- デュアルスタック端末はIPv4とIPv6両方のネットワークに繋がる
  - 通信先もデュアルスタック端末の場合、IPv6を利用することが多いがIPv4を優先する時もある
    - 通信先や環境により変わる

    ※端末が宛先アドレス及び送信元アドレスを複数持つ場合の選択ルールは規定されている(RFC3484)

- 障害に気づきづらい
  - IPv6で障害が起きていても、IPv4で通信可能だとなかなか気づけない
    - デュアルスタック端末の場合、IPv6が不通でもIPv4へ通信を切り替えるなどうまく動いてしまう



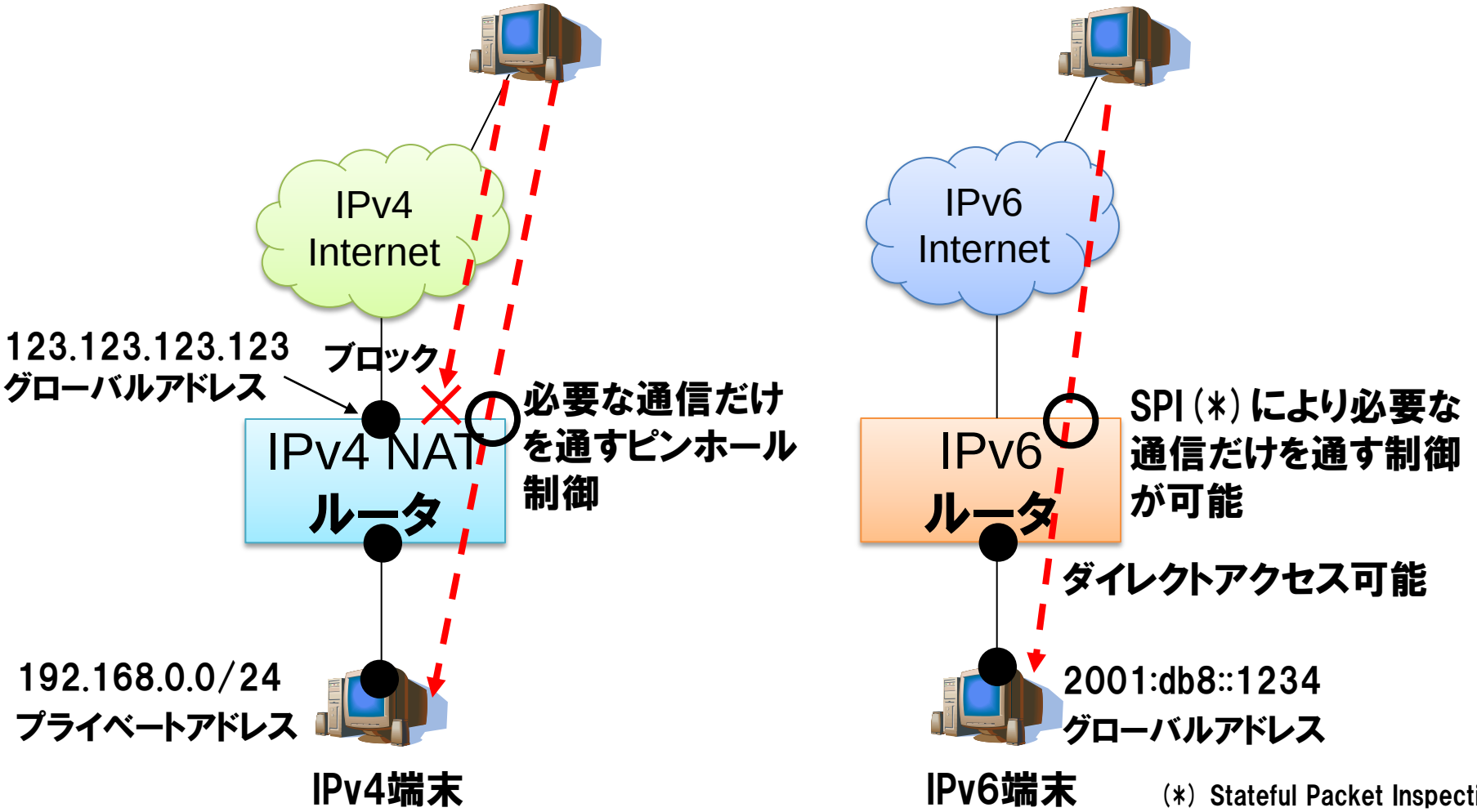
家庭・SOHO環境でのセキュリティ

デュアルスタックネットワークにおける
セキュリティのポイント

IPv4プライベートアドレス＋NAT と IPv6の比較

適切なパケットフィルタリングでIPv4 NATと同等なセキュリティを確保

RFC4864（Local Network Protection for IPv6）は安全性担保の方法を記述



（*）Stateful Packet Inspection

NTTデュアルスタックネットワークでのセキュリティ上の注意点

- ファイヤウォールポリシの不整合に注意
  - IPv4は適切なポリシーが設定されていてもIPv6は一切の制御なし、全通信が許可では意味がない
    - 基本的にIPv4/IPv6同一ポリシで運用するのが望ましい

      ⇒IPv4のポリシーによってはIPv6で同一の運用ができないことに注意！（IPv6では外部との一部のICMP通信が必須）
      - ICMPv6 Type2:PMTUDで必須
- 自動トンネルによる意図しない外部接続
  - 6to4, Teredo
    - Windows Vista/7 では端末にIPv6アドレスが設定されない時に自動起動する

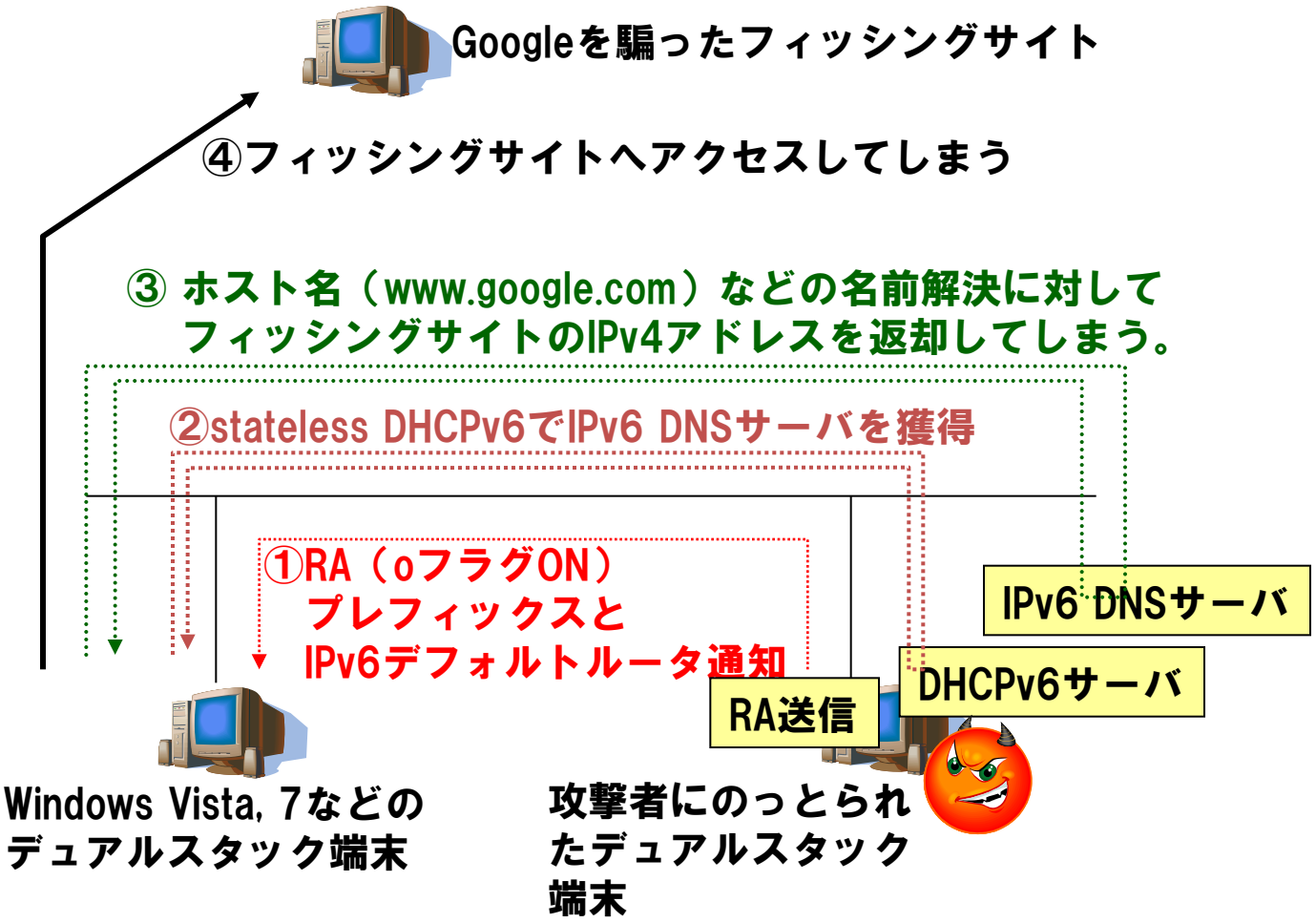
      ⇒ 意図しない外部接続性を放置しないこと

  [対処法] LAN内部からのIPv4パケットを遮断する
  - プロトコル番号41（IPv6 over IPv4トンネル, 6to4）
  - UDP ポート 3544（Teredo）

NTTデュアルスタックネットワークに対する攻撃例

デュアルスタック環境ではIPv4, IPv6が相互に影響しあう場面がある

■ DHCPv6とDNSを使った攻撃例 – 多くのIPv6/IPv4デュアル端末はIPv6を優先して使用

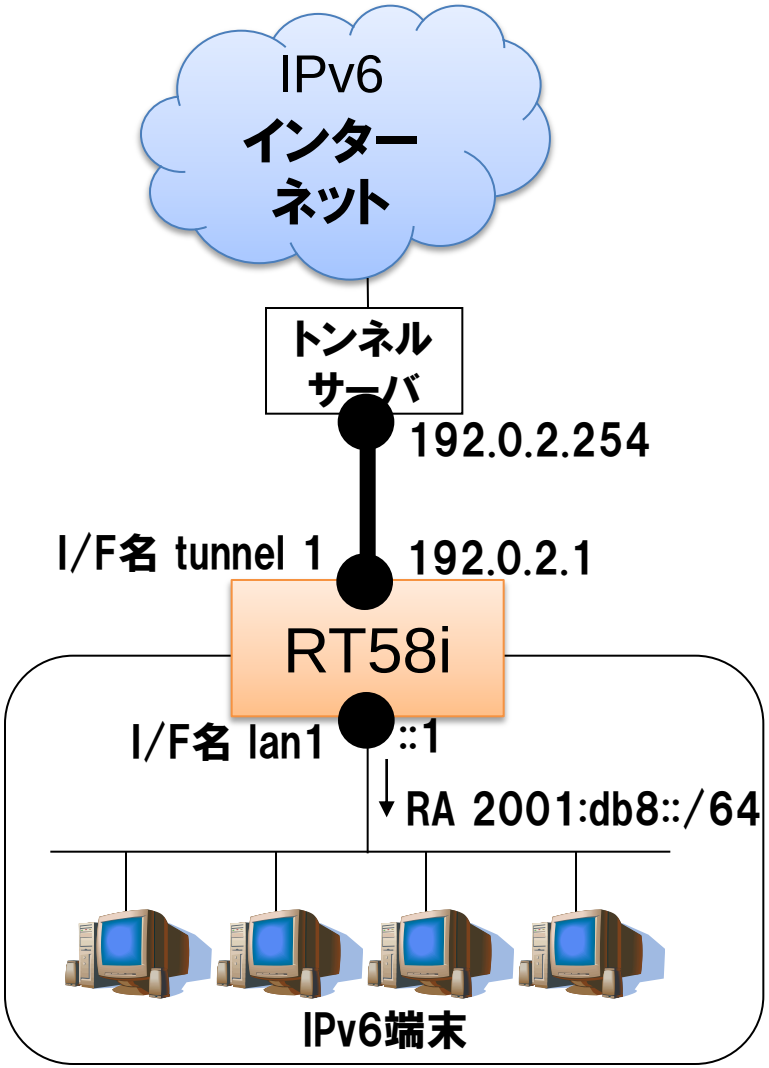


付録

ヤマハ製ブロードバンドルータ
RT58iでの設定例

ヤマハRT58iによる設定例(１)

IPv6 over IPv4 トンネルによる接続

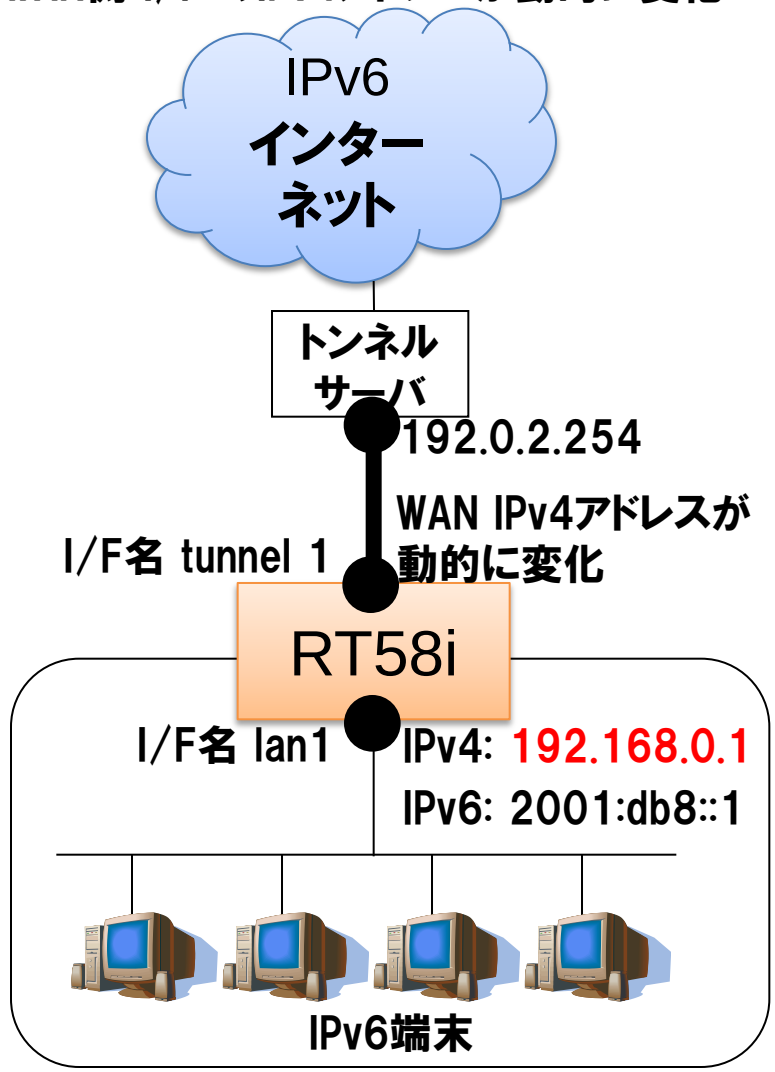


- 外部接続
  - 接続方式 IPv6 over IPv4 スタティックトンネル
    - 192.0.2.1 ⇔ 192.0.2.254
  - プレフィックス 2001:db8::/48 を通知されている
- 内部設定
  - プレフィックス 2001:db8::/64 を端末へ割当て

```
# IPv6ルーティングをON
ipv6 routing on

# トンネルデバイスを作成
tunnel select 1
  encapsulation ipip
  endpoint address 192.0.2.1 192.0.2.254
  tunnel enable 1

# デフォルトゲートウェイをトンネルに向ける
ipv6 route default gateway tunnel 1

# LAN内の設定
ipv6 lan1 address 2001:db8::1/64
ipv6 prefix 1 2001:db8::/64
ipv6 lan1 rtadv send 1 o_flag=on
```

ヤマハRT58iによる設定例(２)

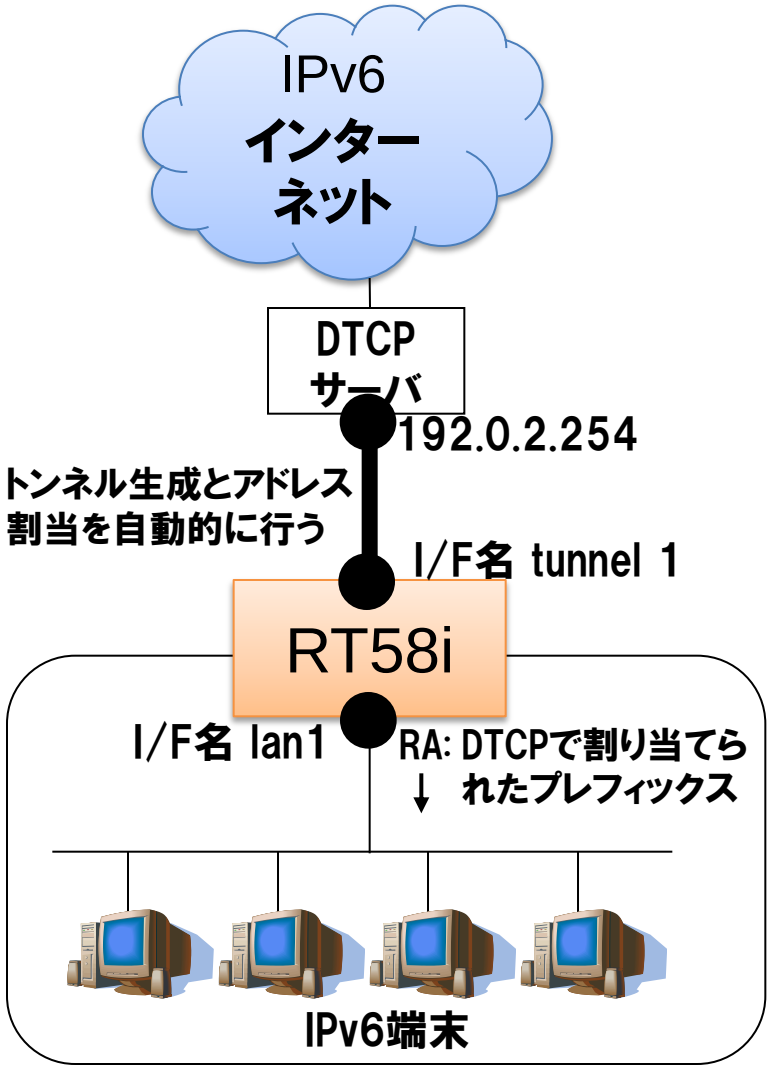
IPv6 over IPv4 トンネルによる接続
WAN側 I/F のIPv4アドレスが動的に変化




```
# IPv6ルーティングをON
ipv6 routing on

# トンネルデバイスを作成
# エンドポイントを（LANプライベートアドレス）-（トンネルサーバ）
tunnel select 1
  encapsulation ipip
  endpoint address 192.168.0.1 192.0.2.254
  tunnel enable 1

# デフォルトゲートウェイをトンネルに向ける
ipv6 route default gateway tunnel 1

# LAN内の設定
ipv6 lan1 address 2001:db8::1/64
ipv6 prefix 1 2001:db8::/64
ipv6 lan1 rtadv send 1 o_flag=on

# NAT設定
nat descriptor type 1 masquerade
nat descriptor masquerade static 1 1
                              192.168.0.1 ipv6 *
pp select 1
  ip pp nat descriptor 1
```

ヤマハRT58iによる設定例(３)

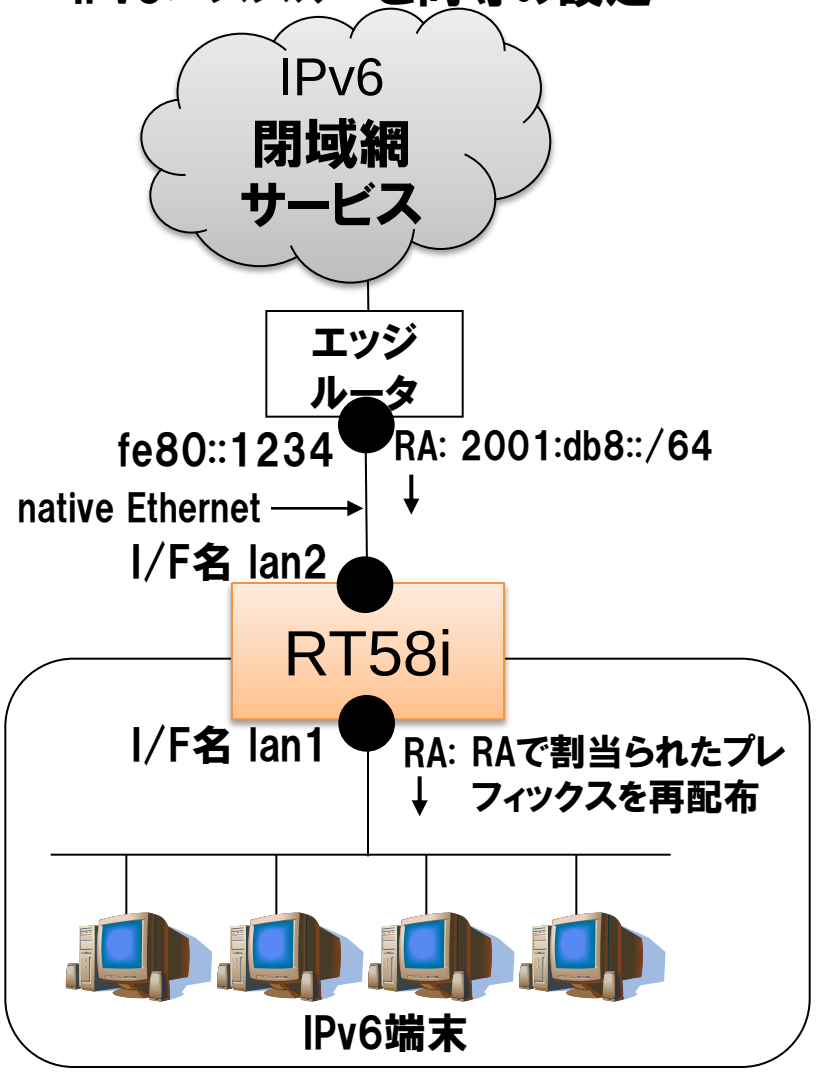
DTCPによるトンネル接続




```
# IPv6ルーティングをON
ipv6 routing on

#  DTCPトンネルを作成 – feel6サービスへの接続例
tunnel select 1
   tunnel dtcp dtcp.feel6.jp
                myname USERID PASSWORD
   tunnel enable 1

#  デフォルトゲートウェイをトンネルに向ける
ipv6 route default gateway tunnel 1

# LAN内の設定
ipv6 lan1 address dtcp-prefix@tunnel1::1/64
ipv6 prefix 1 dtcp-prefix@tunnel1::/64
ipv6 lan1 rtadv send 1 o_flag=on

#  必要に応じてフィルタリング設定も可
ipv6 filter 1 reject
       dtcp-prefix@tunnel1::/64 *
ipv6 filter 2 pass
       * dtcp-prefix@tunnel1::1 * tcp * www
```

ヤマハRT58iによる設定例(４)

RA-proxy による接続例
IPv6パススルーと同等の設定

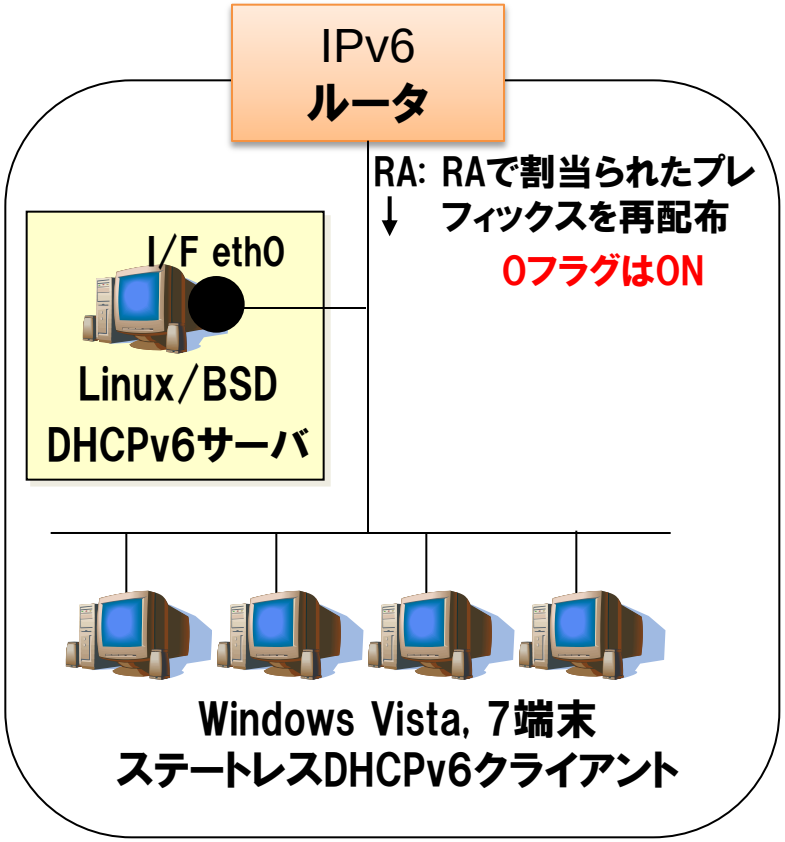



```
# IPv6ルーティングをON
ipv6 routing on

# デフォルトゲートウェイをトンネルに向ける
ipv6 route default gateway tunnel 1

# LAN内の設定
ipv6 lan1 address ra-prefix@lan2::1/64
ipv6 prefix 1 ra-prefix@lan2::/64
ipv6 lan1 rtadv send 1

# RA-Proxyでも必要に応じてフィルタリング設定も可
# IPv6パススルーに対応したルータでも、フィルタリングは
# ほとんど実装されていない
ipv6 filter 1 reject
            ra-prefix@lan2::/64 *
ipv6 filter 2 pass
            * ra-prefix@lan2::1 * tcp * www
```

ステートレスDHCPv6サーバの設定例

ステートレスDHCPv6サーバの設定例

WIDE-DHCPv6サーバによる設定例



■ステートレスDHCPv6サーバの設定と起動

dhcp6s.conf への記述内容

```
option domain-name-servers 2001:db8::53;
option domain-name "example.jp";
```

ステートレスDHCPv6サーバの起動

```
# dhcp6s -c dhcp6s.conf eth0
```

■Windows Vista 端末での情報取得の様子

```
C:¥> ipconfig /renew6
C:¥> ipconfig /all
イーサネット アダプタ ローカル エリア接続:
   接続固有の DNS サフィックス. : example.jp
   DHCP 有効 ..... : はい
   自動構成有効 ..... : はい
   IPv6 アドレス ..... : 2001:db8::XXXX(優先)
   デフォルト ゲートウェイ ..... : fe80::XXXX%1
   DHCPv6 IAID ..... : 268869872
   DHCPv6 クライアント DUID . : 00-01-00-01-11-62-4C
                                -59-00-1C-25-9F-8C-39
   DNS サーバー ..... : 2001:db8::53
```

http://sourceforge.jp/projects/sfnet_wide-dhcpv6/

家庭・SOHO向けIPv6ルータの現状

家庭・SOHO向け市販IPv6ルータのラインナップ

家庭・SOHO向けのIPv6ルータ製品群も選択肢が広がりつつある

メーカ 機種名	主な特徴	参考 価格
NEC UNIVERGE IX2005 	IPv6ルーティングのほか、IPsec, VRRP, QoSなど高度な機能に対応した企業向け	6万円 程度
アライドテレシス CentreCOM AR415S 	IPsec, VRRP, IEEE802.1x など、高度な機能に対応した企業向けVPNアクセスルータ	6万円 程度
ヤマハ NetVolante RT58i 	IPv6ルーティング, SPIファイヤウォールを搭載 DTCP, RA proxy（NTTフレッツ向け機能）	3万円 程度
バッファロー WZR-AMPG300NH 	Win Vista Premiumロゴ取得。6to4でのIPv6インターネットアクセスをサポートしている	1～2万 円程度
アップル AirMac Extreme, AirMac Express  TimeCapsule	6to4によるIPv6インターネットアクセスをサポート。Extremeはファイヤウォール機能を装備	16,800円 9,800円 29,800円
コレガ CG-BARPRO6 	OCN IPv6への接続機能をサポート 現在は販売終了	1万円 未満