

今からはじめるIPv6 ~プロトコル基礎編~

金沢大学総合メディア基盤センター
北口善明

「プロトコル基礎編」の内容

- IPv6誕生の背景とIPv4枯渇問題
- IPv6の基礎知識
- IPv6アドレス
- 自動アドレス設定
- 移行技術
- その他の機能

IPv6誕生の背景とIPv4枯渇問題

IPv6誕生の背景

IPv4アドレス枯渇問題

IPv4アドレスは32ビット＝約43億個のアドレス数
インターネットの指数的な成長によるアドレス数の消費が加速

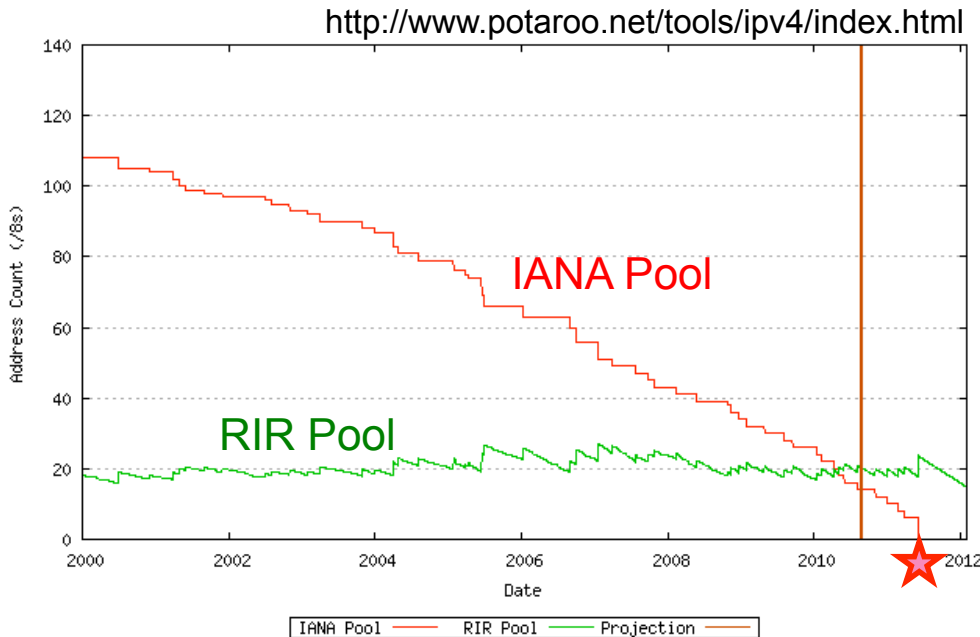
2011年には使い切るとの予想



延命技術	メリット	デメリット
CIDR(Classless Inter-Domain Routing) クラス概念をなくしVLSMによる柔軟性のあるサブネットを構成可能にする技術	IPアドレスを効率的にセグメントに割り当てることが可能	特になし
プライベートアドレス ローカルネットワーク内で自由に利用可能なアドレス	ローカルで利用する端末でグローバルに一意的なアドレスを消費しない	VPN接続時にアドレス重複が発生する可能性がある
NAT(Network Address Translation) プライベートアドレスとグローバルアドレスの変換を行う技術	ポート番号変換を併用（IPマスカレード/NAPT）することでグローバルアドレスを共有利用できる	IPアドレスをデータ部に含むアプリケーションが利用できない E2E通信ができない

IPv4アドレス枯渇予測

● Geoff Huston 氏による枯渇予測



IANA poolの枯渇 (IANA⇒RIR)

2011年3月11日

RIR poolの枯渇 (RIR⇒LIR/ISP)

2011年12月13日 (APNICの枯渇)

(2010年11月16日時点)

IANA (Internet Assigned Numbers Authority)

インターネット上で利用されるアドレス資源の
管理・調整を行なうICANNの機能

RIR (Regional Internet Registry)

世界を5つの地域に分けそれぞれの地域で資源
割り当てを行なう組織

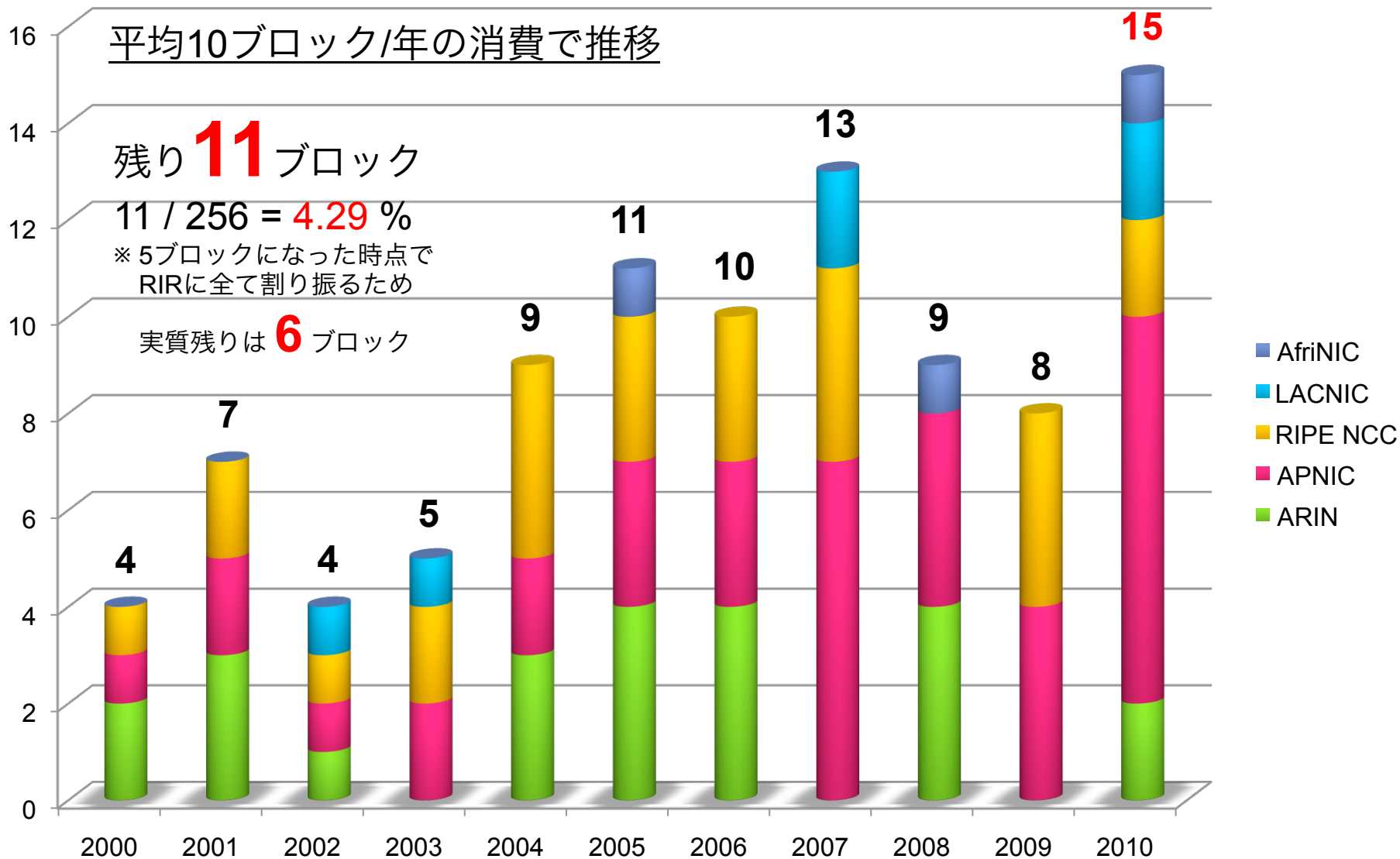
ここから各国地域レジストリやISPにアドレス
資源が割り振られる



※ 日本が含まれるAPNICにおけるアドレス消費ペースが最も早く、真っ先にアドレスが枯渇するRIRと予測されている

近年のアドレス消費量の推移

18 アドレスブロックのRIRへの割り振り推移



※ 2010年11月現在 <http://www.iana.org/assignments/ipv4-address-space/>

IPv4アドレス枯渇への一般的な対策

IPv4アドレスの入手

利用されていないIPv4アドレスを外部組織から入手する

利点：現行システムのまま運用可

欠点：アドレス市場が存在しない
対策としての寿命が一番短い

IPv4アドレスの節約

外部到達性が不要な個所のグローバルIPv4アドレスを使い回す

利点：既存システムの改変が小さい

欠点：リナンバリングが発生
プライベートIPv4を利用することによる制限の発生

IPv6への対応

新規サービスにIPv6アドレスの割り当てを行う

利点：根本的な解決と拡張性

欠点：サーバ側だけの対応では解決が不可能
ISP側の対応が不可欠

IPv6の基礎知識

IPv6の特徴

- 広大なアドレス空間

- 128ビットのアドレス

- IPv4 : IPv6 = バケツの体積 : 太陽の体積

- 約340澗個 (澗 = 1036)

- 340,282,366,920,938,463,463,374,607,431,768,211,456個



- エンドツーエンド原理への回帰

- 本来のインターネットの姿 ⇒ NATによる通信障害がなくなる

- 追加された標準機能

- アドレス自動設定機能 (プラグアンドプレイ)

- 管理者やエンドユーザの利便性が向上

- セキュリティ機能やマルチキャストの標準サポート

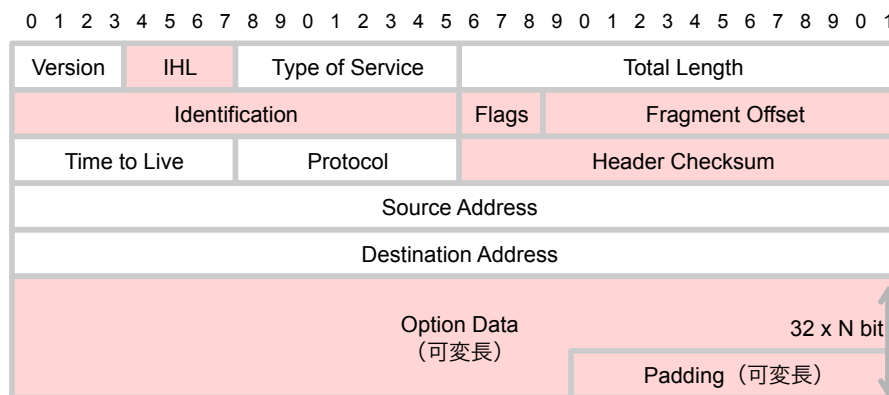
- QoSやモビリティの向上

- 拡張ヘッダを利用したモビリティ通信における経路最適化

IPv6ヘッダの特徴

- IPv4のヘッダとの相違点
 - IPv6のヘッダは固定長（40 Byte）
 - IHL（Internet Header Length）が不要
 - オプション機能は拡張ヘッダとして用意
 - IPv6ではエンドノードでのみフラグメントを実施
 - Identification, Flags, Fragment Offsetが不要
 - IPv6ではチェックサム機構をIPレイヤで実施しない
 - Header Checksumが不要

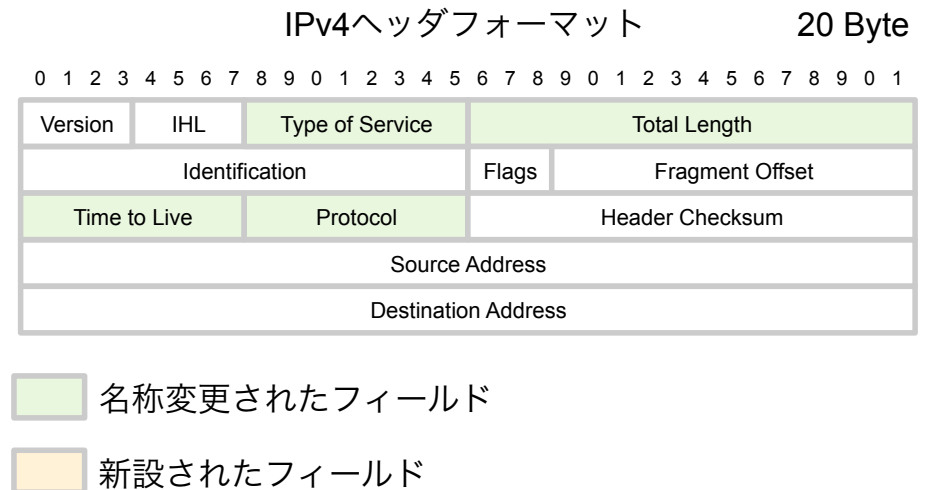
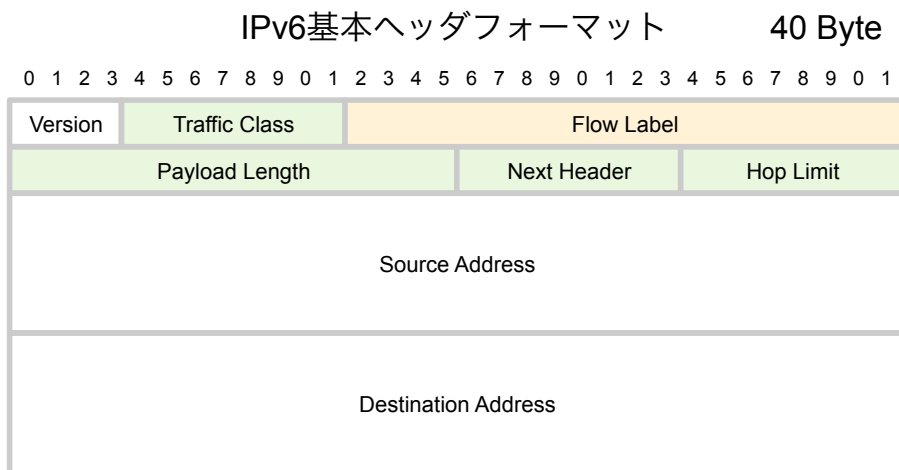
IPv4ヘッダフォーマット



削除されたフィールド

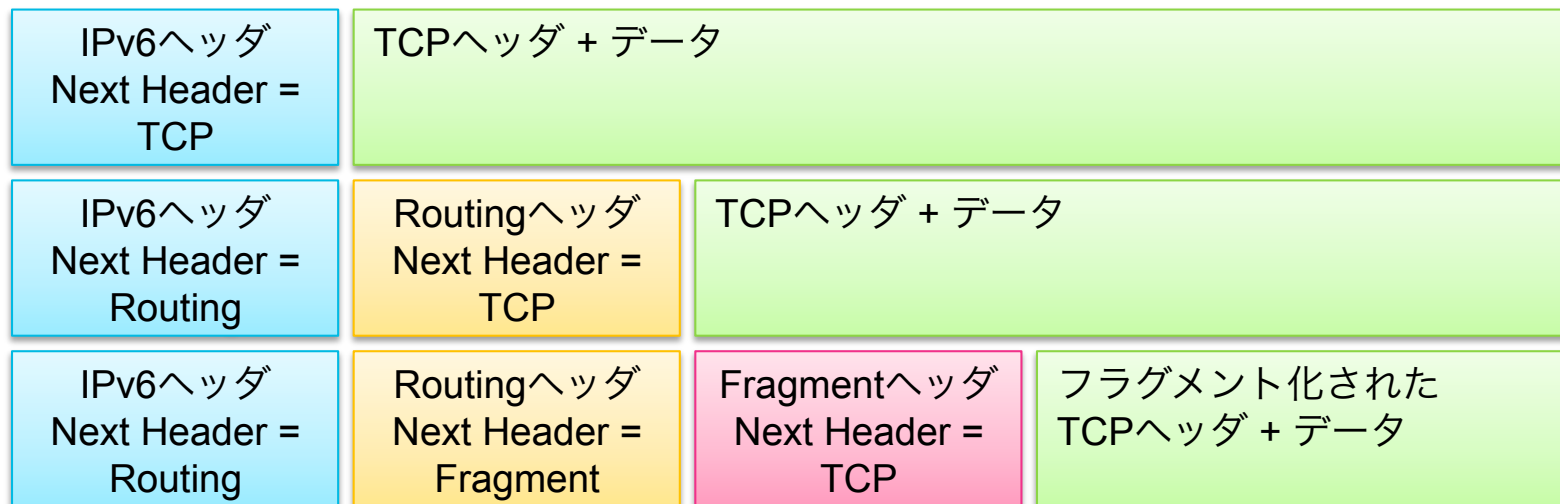
IPv6基本ヘッダ

- 利用に則した名称への変更
 - Type of Service ⇒ Traffic Class
 - Total Length ⇒ Payload Length
 - Protocol ⇒ Next Header
 - Time to Live ⇒ Hop Limit
- 新規に追加されたフィールド
 - Flow Label : QoSなどへの利用



IPv6拡張ヘッダ

● 数珠つなぎで拡張機能を付加

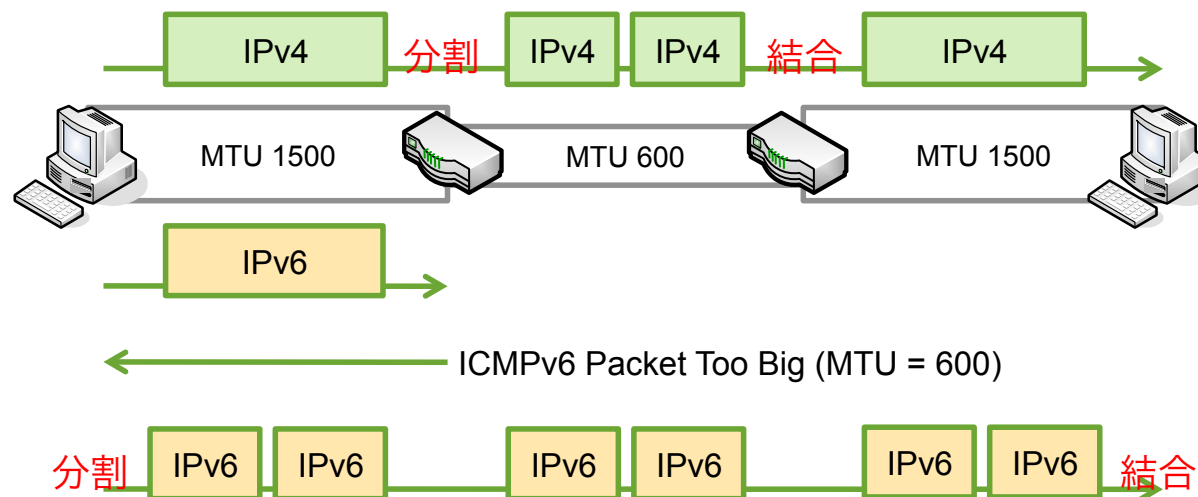


● 拡張ヘッダの種類

Protocol番号	拡張ヘッダ名称	説明
0	Hop-by-Hop Options header	中継ノードの処理を記述する
43	Routing header	送信元がルーティング経路を指定する Type 0は利用禁止に (RFC5095)
44	Fragment header	パケット分割時に利用する
60	Destination Options header	エンドノードにて実行する内容を記述する
51	Authentication header	エンドツーエンドにて完全性と認証を提供する
50	Encapsrational Security Payload header	IPsecにてペイロードを暗号化する際に利用する

Path MTU Discovery

- 通信経路の最小MTUサイズを求める手順
 - 中継ノードでのフラグメントをしないIPv6では必須
 - IPv4では中継ノードで適宜フラグメントしている
 - ICMPv6を利用して調整
 - 転送先リンクのMTUサイズを超えるパケットが来た場合ルータは送信元にICMPv6 Packet Too Bigを送信
 - 送信元はメッセージ内のMTUサイズにフラグメントして再送信



IPv6アドレス表記法

● IPv4のアドレス表記法

2進数表記 (32ビット)

```
11000000 10101000 00000000 00000001
```

・ 8ビットに区切り10進数で表現 区切り文字はピリオド「.」

```
192.168.0.1
```

● IPv6のアドレス表記法

2進数表記 (128ビット)

```
0010000000000001 0000110110111000 1011111011101111 1100101011111110  
0000000000000000 0000000000000000 0000000000000000 0001001000110100
```

・ **16ビット**に区切り**16進数**で表現 区切り文字は**コロン**「:」

```
2001:0db8:beef:cafe:0000:0000:0000:1234
```

・ 省略表記①：各ブロックの先頭の連続する「0」は省略可能

```
2001:db8:beef:cafe:0:0:0:1234
```

・ 省略表記②：連続した「0」は1回に限り「::」に省略可能

```
2001:db8:beef:cafe::1234
```

IPv6アドレス表記での注意点

● 柔軟な表記が可能なIPv6アドレス

- ◆ 省略形やアルファベットの大文字/小文字など複数の表記が可能
＜同じアドレスの例＞
 - ① 2001:db8:0:0:1:0:0:1 ::による省略がなくてもよい
 - ② 2001:0db8:0:0:1:0:0:1 頭の0の省略があってもなくてもよい
 - ③ 2001:db8::1:0:0:1 同じ長さの0なのでどちらの表記も可
2001:db8:0:0:1::1
 - ④ 2001:db8::0:1:0:0:1 1ブロックだけを::に省略してもよい
 - ⑤ 2001:DB8:0:0:1::1 アルファベットは大文字/小文字が可
- ◆ IPv4アドレス埋め込みIPv6アドレス表記の扱い (IPv4射影アドレス)
::ffff:10.10.1.1 vs ::ffff:a0a:101
- ◆ 文字列で扱う際には正規化を
アプリケーションの実装によってログ出力時などの表記が異なる

RFC5952にて代表的な表記ルールが明確になった
②と④はNG、③は前半省略、⑤は小文字利用

IPv6アドレス

IPv6アドレスの種類

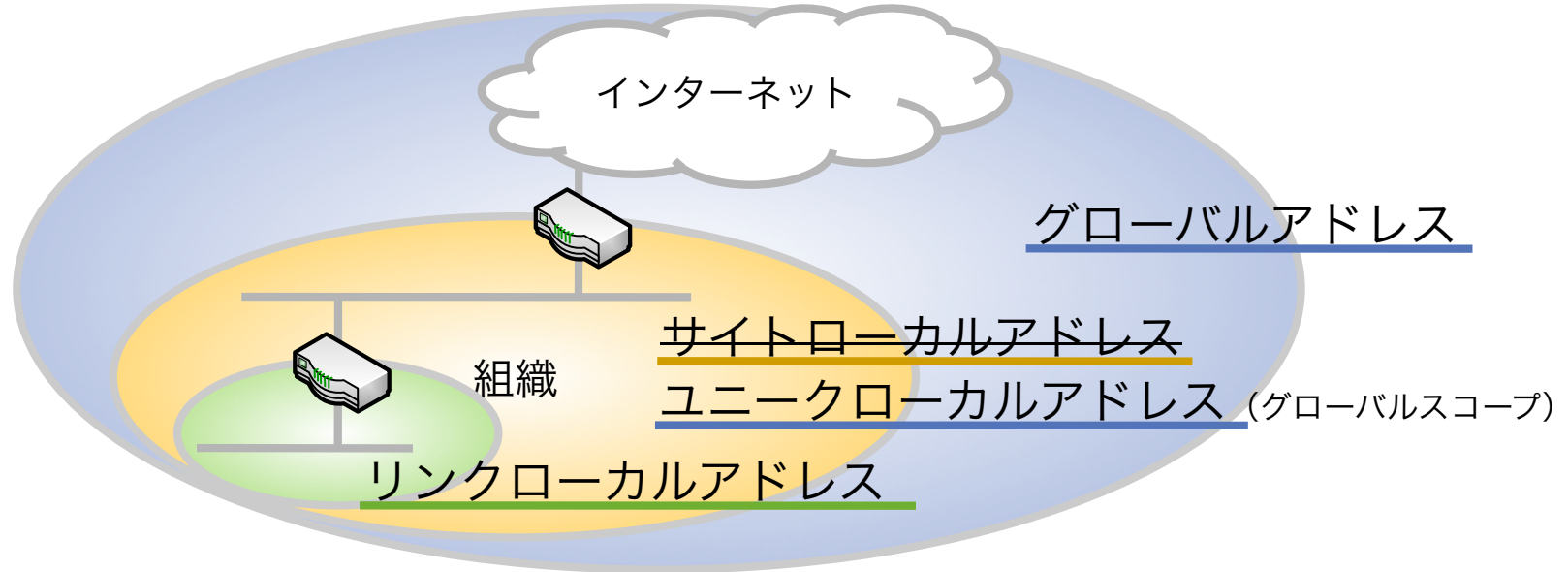
- ユニキャストアドレス 1対1 通信
 - ネットワークインターフェース毎に設定されるアドレス

アドレス種別	アドレス範囲	説明
グローバルアドレス	2000::/3	IPv4のグローバルアドレスと同じ
リンクローカルアドレス	fe80::/10	リンク内の通信に利用される
サイトローカルアドレス	fec0::/10	IPv4のプライベートアドレスと同じ (ただしRFC3879で廃止に)
ユニークローカルアドレス[ULA]	fc00::/7	IPv4のプライベートアドレス相当

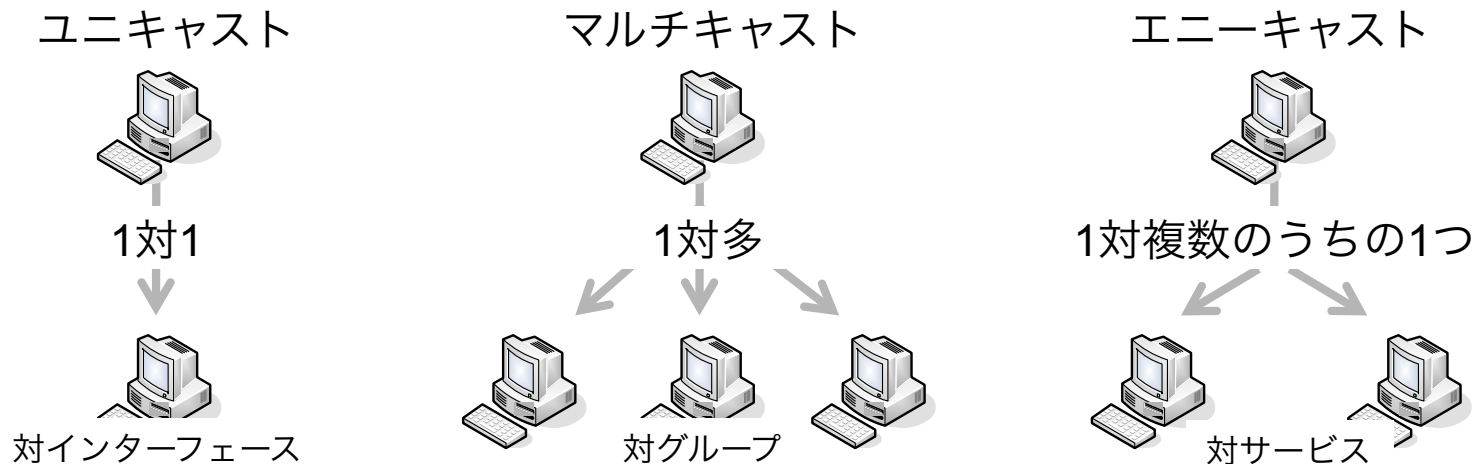
- マルチキャストアドレス 1対多 通信
 - グループを識別するアドレスで複数のノードを識別
 - IPv6ではIPv4のブロードキャストの置き換えとして利用
- エニーキャストアドレス 1対1 of 多 通信
 - 複数のノードに指定可能な「機能」に対して設定される

IPv6アドレスの利用比較

● 通信範囲（スコープ）の違い



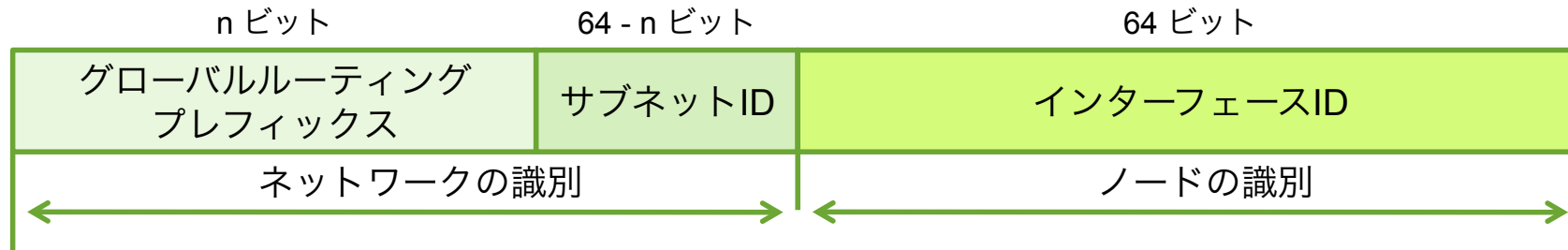
● 通信形態の違い



ユニキャストアドレス (1)

● グローバルアドレス

[RFC3587]



● プレフィックス

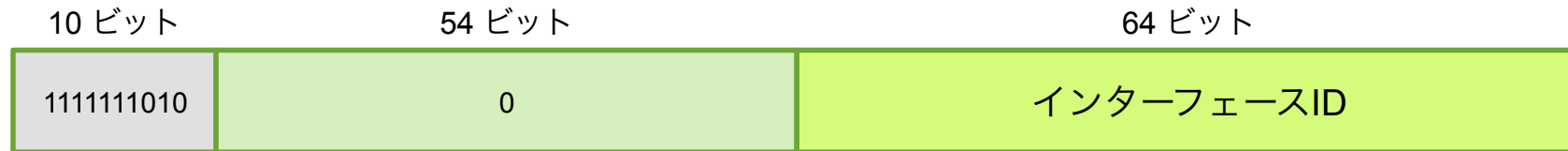
- グローバルルーティングプレフィックスとサブネットIDを合わせた上位64ビット

● ネットワークの表現方法

- 2001:2f8:1000:1::/64
 - プレフィックスが「2001:2f8:1000:1」のセグメントを表す
- 2002::/16
 - 上位16ビットが「2002」で始まるアドレスの塊を意味する

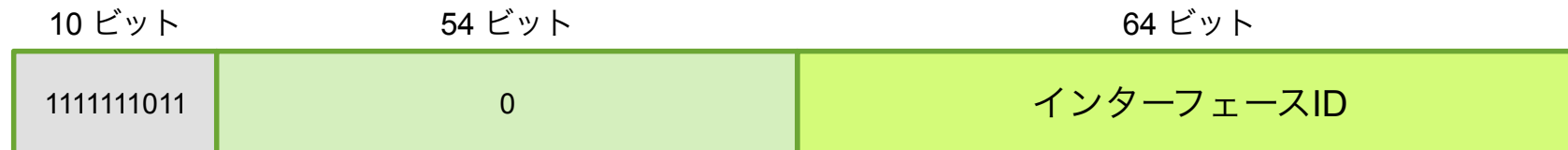
ユニキャストアドレス (2)

● リンクローカルアドレス (fe80::/10)



- 同一リンク (セグメント) 内で一意なアドレス
 - ルータを越えた通信は不可
 - NDPなどの通信で利用されるアドレス

● ~~サイトローカルアドレス (fec0::/10)~~

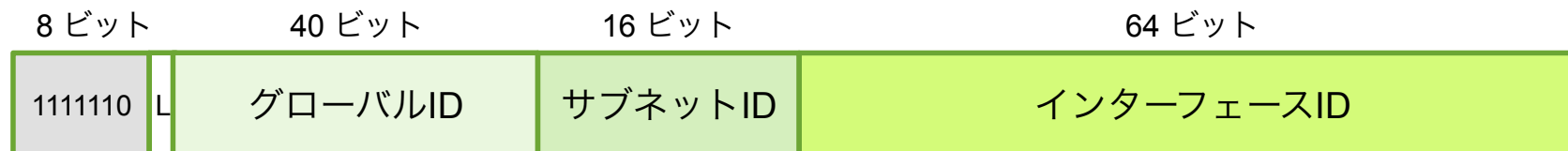


- 同一サイト内で一意なアドレス
 - サイト定義の困難さやNAT助長などの問題で**廃止** (RFC3879)

ユニキャストアドレス (3)

● ユニークローカルアドレス (fc00::/7)

[RFC4193]



- 廃止されたサイトローカルアドレスの代用として標準化
 - インターネットへ送信することは禁止
- サイトローカルアドレスと異なりスコープはグローバル
- アドレスフォーマット
 - L = 1 : 自由に利用可能なローカルアドレス (fd00::/8)
 - L = 0 : 登録制 (将来利用)
 - グローバルIDのランダム生成方法
 - trunc(SHA1(NTP current time + EUI-64), 40 bit)
 - ULA Generator : <http://www.kame.net/~suz/gen-ula.html>

ユニキャストアドレス (4)

● 未指定アドレス (::)

128 ビット

00000000 00000000

- アドレスが未割り当ての時に送信元アドレスとして利用
- IPv4における0.0.0.0に相当

● ループバックアドレス (:::1)

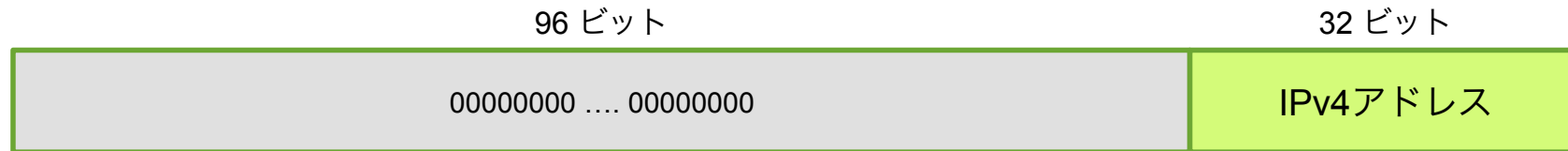
128 ビット

00000000 00000001

- 自分自身を表すアドレス
- IPv4における127.0.0.1に相当

ユニキャストアドレス (5)

- ~~IPv4互換アドレス (::/96)~~ IPv4-compatible IPv6 address



- 自動トンネリング用アドレス (RFC4291にて非推奨)
- 表記例 ::192.168.1.1

- IPv4射影アドレス (::ffff:/96) IPv4-mapped IPv6 address



- IPv4アドレスをIPv6アドレスで表現したアドレス
 - IPv6アプリケーション内での内部通信に利用
- 表記例 ::ffff:192.168.1.1

エニーキャストアドレス

● エニーキャストアドレス

- IPv6で登場した概念でサービスにアドレスを設定
- アドレス自体はユニキャストアドレスの範囲
- 複数の機器（インターフェース）に付与して利用
- 経路的に一番近いものに転送される
- 具体的な利用アドレス

- Subnet Router Anycast Address

[RFC4291]

64 ビット

64 ビット



- 対象プレフィックスを持つサブネット上のルータを表す
- Mobile IPv6 Home-Agents anycast [RFC2526]
- 6to4リレールータやTeredoリレー
- DNSルートサーバやJPドメインDNSサーバ
 - 分散配置されたサーバで利用されている

マルチキャストアドレス (1)

● マルチキャストアドレス



● グループに対して設定されるアドレス

- 複数のノードにデータを送る放送型の通信で利用
- IPv6ではNDPなどで積極的に利用される

● スコープ

- マルチキャスト通信の有効範囲を指定

スコープ	意味	スコープ	意味
0001 (1)	Interface-local scope	0101 (5)	Site-local scope
0010 (2)	Link-local scope ※	1000 (8)	Organizational-local scope
0100 (4)	Admin-local scope	1110 (e)	Global scope ※

※ 一般的に利用されるもの

マルチキャストアドレス (2)

● 予約済みのマルチキャストアドレス例

アドレス	説明
ff02:0:0:0:0:0:0:1	全ノードアドレス
ff02:0:0:0:0:0:0:2	全ルータアドレス
ff02:0:0:0:0:0:0:5	OSPFルータ
ff02:0:0:0:0:0:0:6	OSPF DR (Designated Router)
ff02:0:0:0:0:0:0:9	RIPルータ
ff02:0:0:0:0:0:0:16	MLDv2対応ルータ
ff02:0:0:0:0:0:0:fb	mDNSv6
ff02:0:0:0:0:0:1:2	DHCPサーバ/リレーエージェント
ff02:0:0:0:0:0:1:3	LLMNR (Link-Local Multicast Name Resolution)
ff02:0:0:0:0:1:ff00:0/104	要請ノードマルチキャストアドレス 下位24ビットはユニキャストアドレスの下位24ビット

● 最新の割り当て情報

- <http://www.iana.org/assignments/ipv6-multicast-address/>

マルチキャストアドレス (3)

● 要請ノードマルチキャストアドレス



● リンクレイヤのアドレス解決時に利用

- 下位3バイトが同じユニキャストアドレスを持つノードが応答するアドレス
- アドレス解決に送信する範囲を小さくする効果

● 利用例

【リンクローカルアドレス fe80::2a0:f8ff:fe01:6ab8 のアドレス解決の場合】

宛先のIPv6アドレスとMACアドレス

要請ノードマルチキャストアドレス

ff02:1:ff01:6ab8

MACアドレス

33:33:FF:01:6A:B8

※ “33:33”で始まるMACアドレスはマルチキャスト用

IPv6アドレスの下位4バイトを利用する

ノードやルータが持つIPv6アドレス

- ノードが持つアドレス
 - インターフェース毎のリンクローカルアドレス
 - インターフェース毎のユニキャストアドレス
 - ループバックアドレス
 - 全ノードマルチキャストアドレス
 - 要請ノードマルチキャストアドレス
 - 所属するマルチキャストアドレス
- ルータが持つアドレス
 - ノードが持つアドレス
 - サブネットルータエニーキャストアドレス
 - 全ルータマルチキャストアドレス

自動アドレス設定

ICMPv6 (1)

- Internet Control Message Protocol for IPv6
 - ネットワーク状態通知を行なうメッセージ群
 - IPv4のICMPに追加された機能
 - 近隣探索機能
 - プラグアンドプレイを実現する機能
 - マルチキャストグループ管理
 - IPv4におけるIGMP相当
 - モバイルIPv6関連機能
 - ホームエージェント探索など
 - IPv6ではより重要な位置づけに

ICMPv6 (2)

● 代表的なメッセージタイプ

タイプ	種別	説明
1	エラーメッセージ	終点到達不能 (Destination Unreachable Message)
2		パケット過大 (Packet Too Big Message)
3		有効時間超過 (Time Exceeded Message)
4		パラメータ異常 (Parameter Problem Message)
128	エコー要求・応答	エコー要求 (Echo Request Message)
129		エコー応答 (Echo Reply Message)
130	マルチキャスト関連 (MLDv1/v2で利用)	マルチキャストリスナー照会 (Multicast Listener Query)
131		マルチキャストリスナー報告 (Multicast Listener Report)
132		マルチキャストリスナー終了 (Multicast Listener Done)
143		マルチキャストリスナー報告 (version 2 Multicast Listener Report)
133	近隣探索 (NDPで利用)	ルータ要請 [RS] (Router Solicitation Message)
134		ルータ広告 [RA] (Router Advertisement Message)
135		近隣要請 [NS] (Neighbor Solicitation Message)
136		近隣広告 [NA] (Neighbor Advertisement Message)
137		リダイレクト (Redirect Message)

近隣探索プロトコル：NDP（1）

● Neighbor Discovery Protocol

[RFC4861]

- リンクレイヤアドレスの解決（IPv4のARP機能に相当）
 - 近隣キャッシュ
 - アドレスとリンクレイヤアドレス対応を保持
 - 不到達検出機能
 - 近隣キャッシュ内のリストを最新に保つ
- ステートレス自動アドレス設定（SLAAC）
 - 重複アドレス検出機能（DAD）
 - 設定アドレスの重複がないか検出
 - ※ RFC5227にてIPv4の仕様に逆輸入された
 - デフォルトルート設定
 - ルータ広告を送信しているアドレスを採用
 - グローバルアドレス生成
 - ルータ広告に含まれるプレフィックスオプション情報を利用することで実現

近隣探索プロトコル：NDP（2）

- 5つのメッセージタイプ
 - 近隣要請：Neighbor Solicitation（NS）
 - 重複アドレス検出や到達性／不到達性の確認
 - リンクレイヤアドレスの解決（IPv4のARPと同様）
 - 近隣広告：Neighbor Advertisement（NA）
 - 近隣要請に対する応答、自身のアドレス変更通知
 - ルータ要請：Router Solicitation（RS）
 - セグメント内のルータ発見に利用
 - ルータ広告を即座に取得する場合に送出
 - ルータ広告：Router Advertisement（RA）
 - ルータによるデフォルト経路の通知
 - プレフィックス情報配布で自動アドレス設定が可能になる
 - リダイレクト
 - 最適なデフォルト経路を通知（IPv4のリダイレクトと同様）

自動アドレス設定 (1)

- ステートレス自動アドレス設定 (SLAAC) [\[RFC4862\]](#)
 - アドレスを管理するサーバが存在しない
 - NDPのRAを用いてアドレスの自動生成を実施
 - DNSサーバなどのアドレス通知はExperimental
- DHCPv6 [\[RFC3315\]](#)
 - ステートフル自動アドレス設定
 - IPv4におけるDHCPと基本的に同じ
 - DNSサーバ情報の通知やアドレス管理が可能
 - デフォルトルートの配布はできない点がIPv4との違い
 - ステートレスDHCPv6
 - アドレス設定は実施せずネットワーク構成情報のみ配布

自動アドレス設定 (2)

- 設定項目の違い

- 二種類の方式で設定できる項目に違いがある

	RA	DHCPv6
デフォルト経路	○	— ※1
アドレス/プレフィックス	プレフィックス割り当て	アドレス割り当て
プレフィックス長	○	RAから学習
サーバ情報 (DNSなど)	△ ※2	○

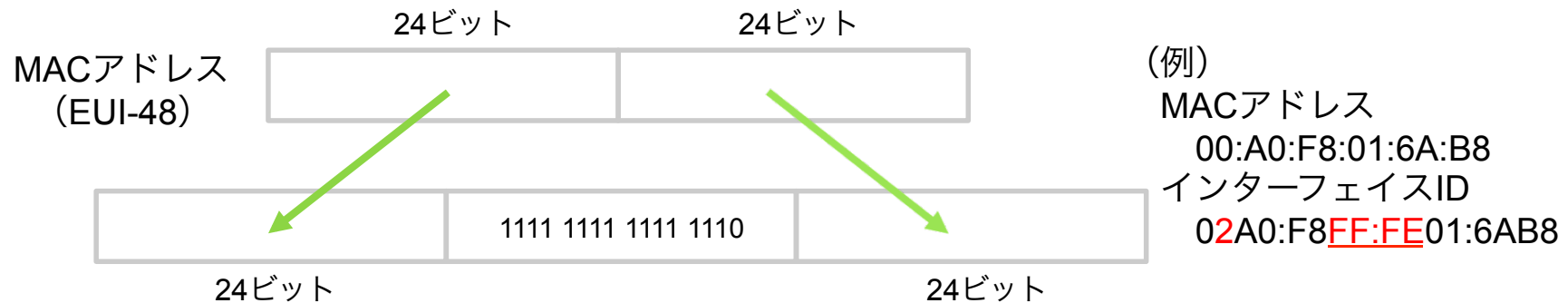
※1 標準化されておらずIETFにて議論中のステータス

※2 [RFC5006](#)にて標準化されているがStandardステータスには至っていない
現状はステートレスDHCPv6との組み合わせが一般的

SLAAC (1)

● インターフェースIDの生成

● MACアドレスから生成する場合 (EUI-64形式)



※7ビット目：MAC addressのLocal Addressビットを1に設定

● プライバシ拡張アドレス

[RFC3041]

- インターフェースIDにランダムな値を用いる
- 一定時間 (最大7日間) で更新しノードの特定を困難にする

● その他の実装

- Windows Vista/7ではMACアドレスを基に独自の生成アルゴリズムを実装している

SLAAC (2)

- リンクローカルアドレスの生成
 - リンクローカルプレフィックスとインターフェイスID

リンクローカルプレフィックス fe80::	インターフェイスID 2a0:f8ff:fe01:6ab8
--------------------------	----------------------------------

fe80::2a0:f8ff:fe01:6ab8

- グローバルアドレスの生成
 - ルータに対してルータ広告を要請 (ルータ要請)
 - ルータ広告中のプレフィックス情報を利用

ルータ広告に含まれるプレフィックス 2001:db8:beef:1	インターフェイスID 2a0:f8ff:fe01:6ab8
--------------------------------------	----------------------------------

2001:db8:beef:1:2a0:f8ff:fe01:6ab8

- 重複アドレス検出 (DAD)
 - 要請ノードマルチキャスト宛てに近隣要請を送信
 - 検出対象のアドレスから近隣広告による応答がなければ重複なしと判断してアドレス利用を開始

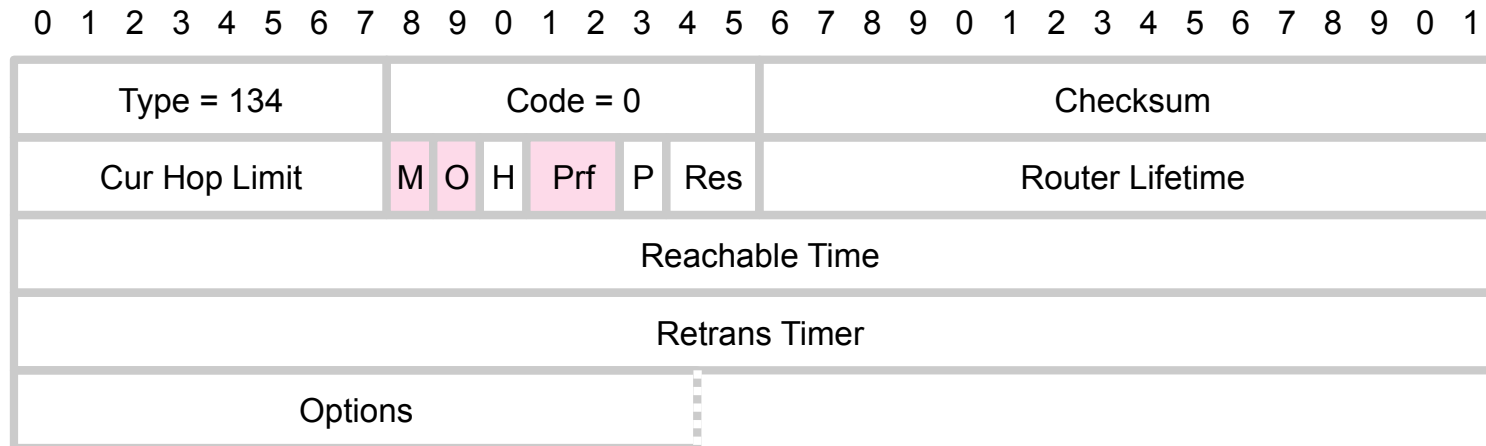
SLAAC (3)

● デフォルト経路の設定

- ルータ広告で通知されたルータをデフォルト経路とする
 - ルータ広告の送信元アドレス（リンクローカル）が選ばれる
- デフォルト経路が無効となる場合
 - ルータ広告の「Router Lifetime」が0の場合には利用されない
- ルータの優先度
 - RFC4191にてデフォルト経路の優先度を設定可能な仕様が追加

SLAAC (4)

● ルータ広告のメッセージフォーマット



● Mフラグ

- ステートフルアドレス自動設定をノードに促す (DHCPv6)

● Oフラグ

- 他の設定情報取得をノードに促す (ステートレスDHCPv6)

● Prfフラグ

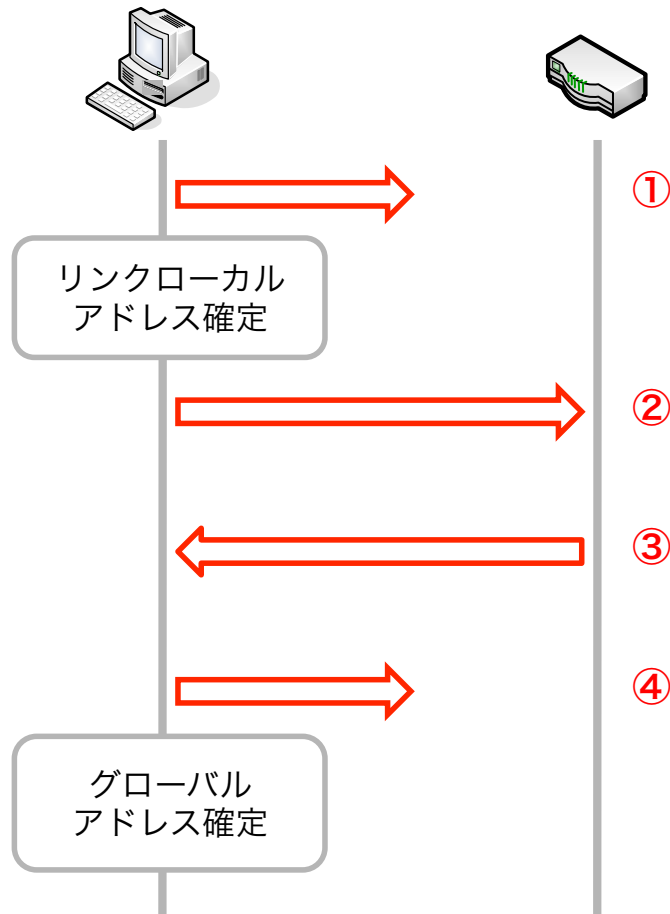
- デフォルト経路になりえるルータの優先度を指定

00 : Medium 01 : High 11 : Low

SLAACの流れ

MAC:00:11:22:33:44:55

MAC:00:11:22:66:77:88



- ①近隣要請 (NS)
 近隣広告がなければ
 ターゲットアドレス
 の利用が可能
 <重複アドレス検出>

要請ノードマルチキャスト

Src MAC	00:11:22:33:44:55
Dst MAC	33:33:FF:33:44:55
Src IPv6	:: (未定義アドレス)
Dst IPv6	ff02::1:ff33:4455
ICMPv6 Type	135
Target	fe80::211:22ff:fe33:4455

- ②ルータ要請 (RS)
 全ルータマルチキャスト
 (ff02::2) 宛に送信

Src MAC	00:11:22:33:44:55
Dst MAC	33:33:00:00:00:02
Src IPv6	fe80::211:22ff:fe33:4455
Dst IPv6	ff02::2
ICMPv6 Type	133

- ③ルータ広告 (RA)
 全ノードマルチキャスト
 (ff02::1) 宛に送信
 取得プレフィックス
 を用いてグローバル
 アドレスを生成

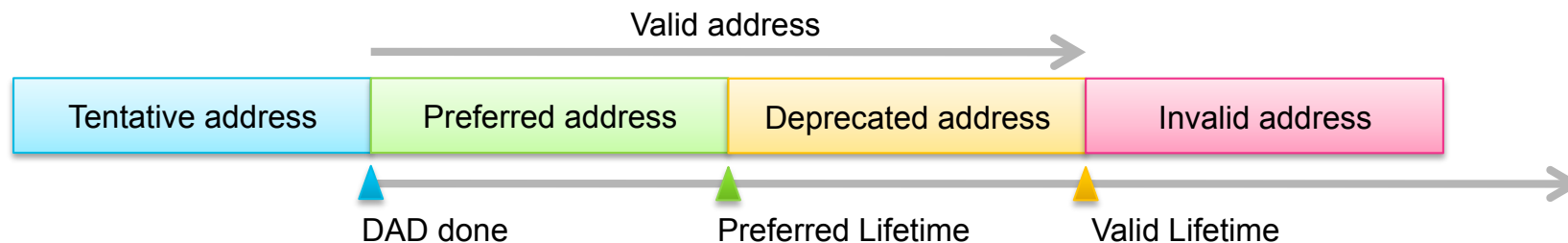
Src MAC	00:11:22:66:77:88
Dst MAC	33:33:00:00:00:01
Src IPv6	fe80::211:22ff:fe66:7788
Dst IPv6	ff02::1
ICMPv6 Type	134
Prefix	2001:db8::

- ④近隣要請
 近隣広告がなければ
 ターゲットアドレス
 の利用が可能
 応答があるとアドレス
 を再構成する必要あり
 <重複アドレス検出>

Src MAC	00:11:22:33:44:55
Dst MAC	33:33:FF:33:44:55
Src IPv6	:: (未定義アドレス)
Dst IPv6	ff02::1:ff33:4455
ICMPv6 Type	135
Target	2001:db8::211:22ff:fe33:4455

IPv6アドレスの状態

- 有効期限 (Lifetime) により状態が変化する
 - 仮アドレス (Tentative address)
 - インターフェースに付与されていない仮のアドレス (DAD前)
 - 有効アドレス (Valid address)
 - 推奨アドレス (Preferred address)
 - インターフェースに付与された利用可能なアドレス
 - 非推奨アドレス (Deprecated address)
 - 推奨有効期間 (Preferred Lifetime) が超過したアドレス
 - 新規通信に用いることは推奨されない
 - Invalid address
 - 最大有効期間 (Valid Lifetime) が超過したアドレス

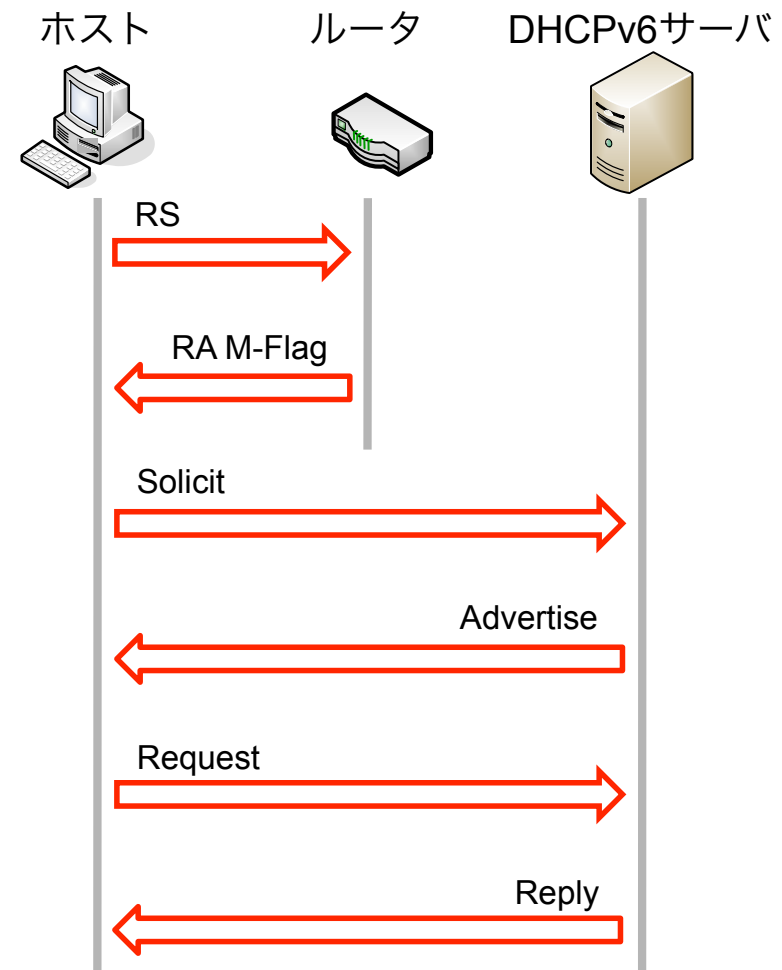


DHCPv6 (1)

- 管理サーバによりアドレスを付与する技術
- ステートフルDHCPv6 [\[RFC3315\]](#)
 - DHCPサーバによりネットワークの構成情報を配布
 - DNSサーバ情報の通知やアドレス管理が可能
 - ルータ広告のMフラグにより利用を促すことが可能
- ステートレスDHCPv6 [\[RFC3736\]](#)
 - アドレス設定は実施せずネットワーク構成情報のみ配布
 - ノードの管理しない (ステートを持たない)
- DHCPv6-PD (Prefix Delegation) [\[RFC3633\]](#)
 - ISPから割り当てるプレフィックスサイズを通知
 - 割り当てられるプレフィックスをRAなどでLAN側に再配布

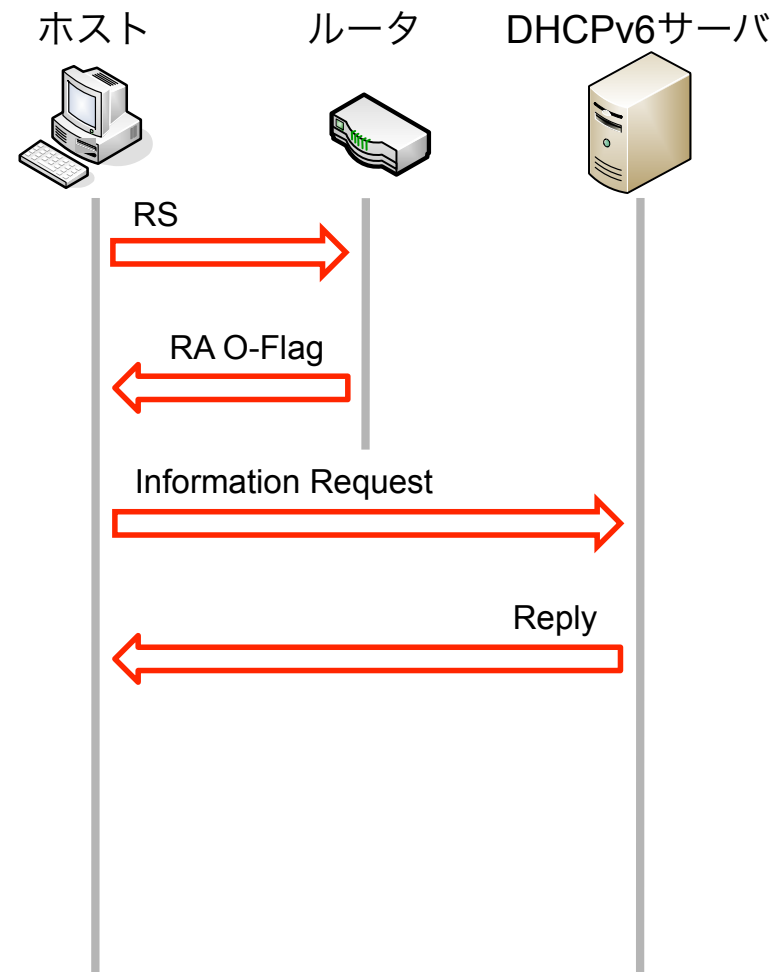
DHCPv6 (2)

- ステートフルDHCPv6
 - DHCPv6サーバにてホストのアドレス管理が可能
 - RAのMフラグを受信するとステートフルDHCPv6の動作にホストは入る
 - Rapid Commitオプションが指定された場合にはAdvertise/Requestを省略
 - /128のIPv6アドレスと各種ネットワークサーバ情報を配布



DHCPv6 (3)

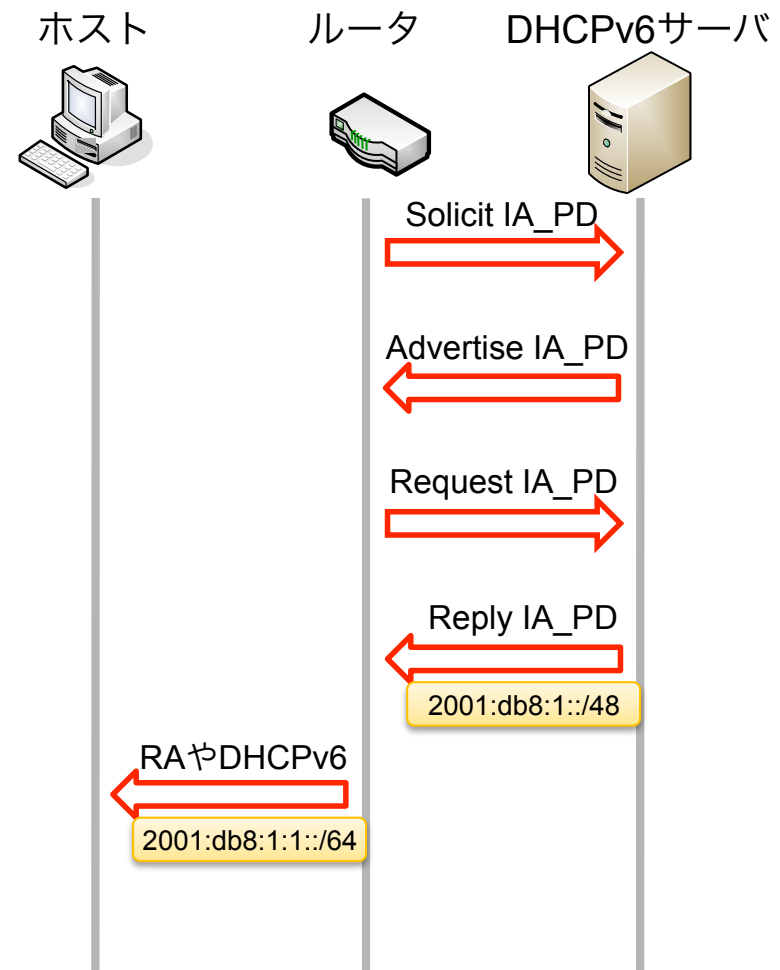
- ステートレスDHCPv6
 - DHCPv6サーバではホストの状態を管理しない
 - RAのOフラグを受信するとステートレスDHCPv6の動作にホストは入る
 - アドレス設定をRAで実施する際にネットワークサーバ情報の配布用に利用される



DHCPv6 (4)

● DHCPv6-PD

- クライアント（ルータ）に対してプレフィックスを配布（ステートフルな動作）
- 割り当てプレフィックスは /48～/64の範囲が一般的
- プレフィックスを取得したルータはRAやDHCPv6を利用してホストに再配布

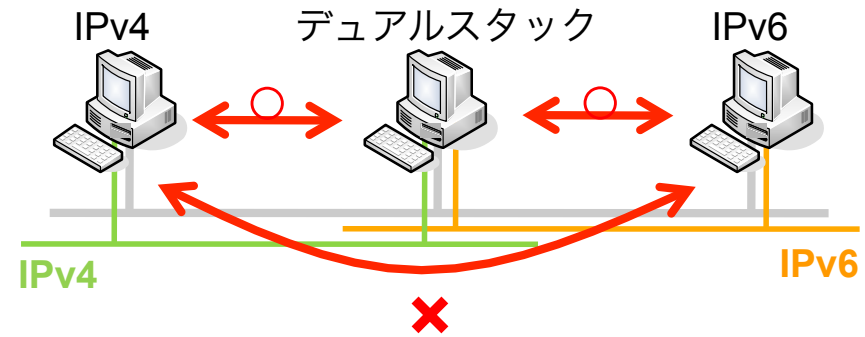


移行技術

IPv6への移行技術

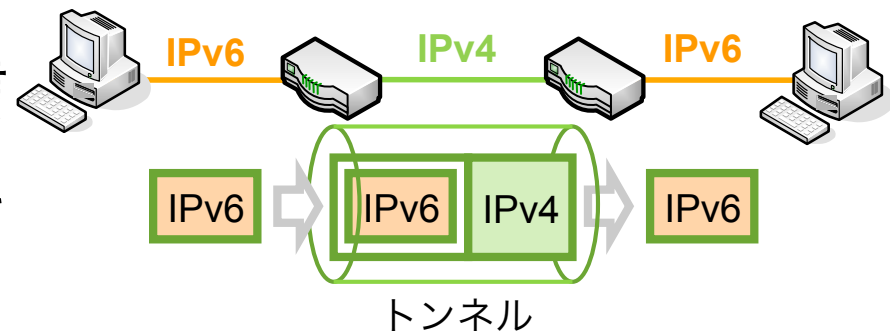
● デュアルスタック

- IPv4とIPv6双方をサポート
- 現在のIPv6対応製品はほとんどがこの形態



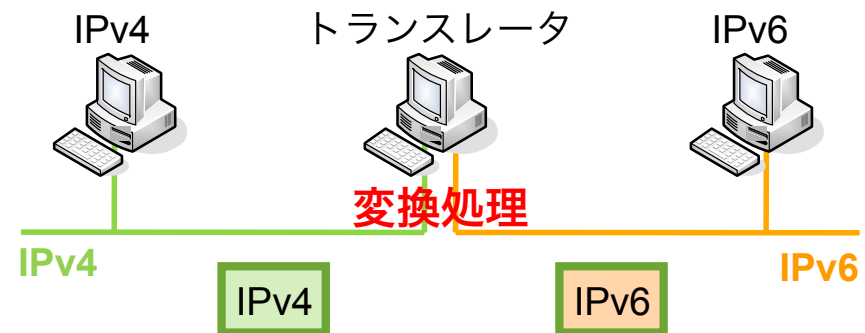
● トンネリング

- IPv4でカプセル化して通信
- ネットワークのIPv6化時に最初に導入される形態



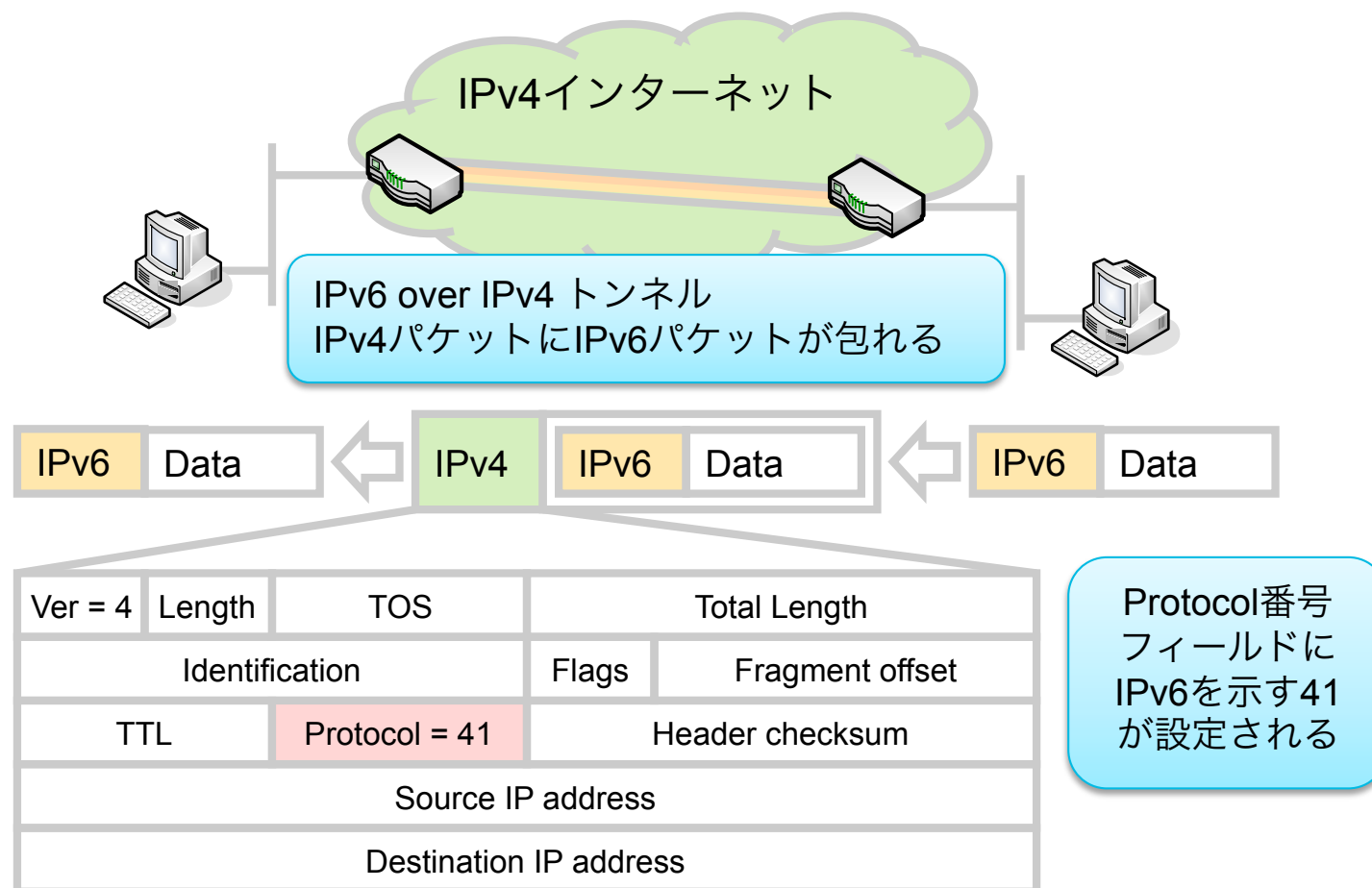
● トランスレータ

- 通信を仲介する翻訳機
- NATと同様の課題を持っている



トンネリング (1)

- 手動設定トンネリング
 - トンネルの両端にて設定を実施
 - 拡張性が乏しいが利用するIPv6アドレスに制限なし



トンネリング (2)

● 自動設定トンネリング

● 6to4

[RFC3056]

- トンネル接続とIPv6アドレス割り当てを同時に実現
- IPv4グローバルアドレスを利用したIPv6アドレス

● 6rd (IPv6 Rapid Deployment)

[RFC5569]

- 6to4技術を利用したISP等でのトンネル接続
- ISPが持つIPv6プレフィックスを利用可能

● ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)

[RFC5214]

- イントラネット内でのトンネリング技術
- プレフィックスに制限はない

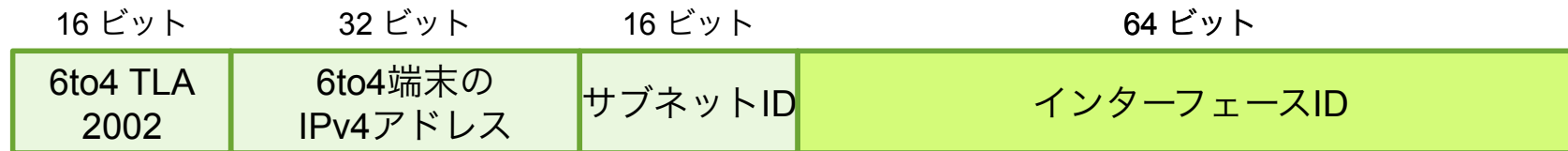
● Teredo

[RFC4380]

- NATトラバーサルをIPv6で実現する技術
- NATの内側からIPv6トンネル接続が可能

6to4 (1)

● 6to4のアドレス形式



● 6to4の構成要素

● 6to4リレールータ

- IPv6ネットワークへの接続を提供
- IPv6ネットワークに2002::/16を広告
 - 経路的に近い6to4リレールータが選ばれる
- IPv4ネットワークに192.88.99.0/24を広告
 - 192.88.99.1がIPv4のエニーキャストアドレス
- 国内のリレールータ：<http://www.tokyo6to4.net/>

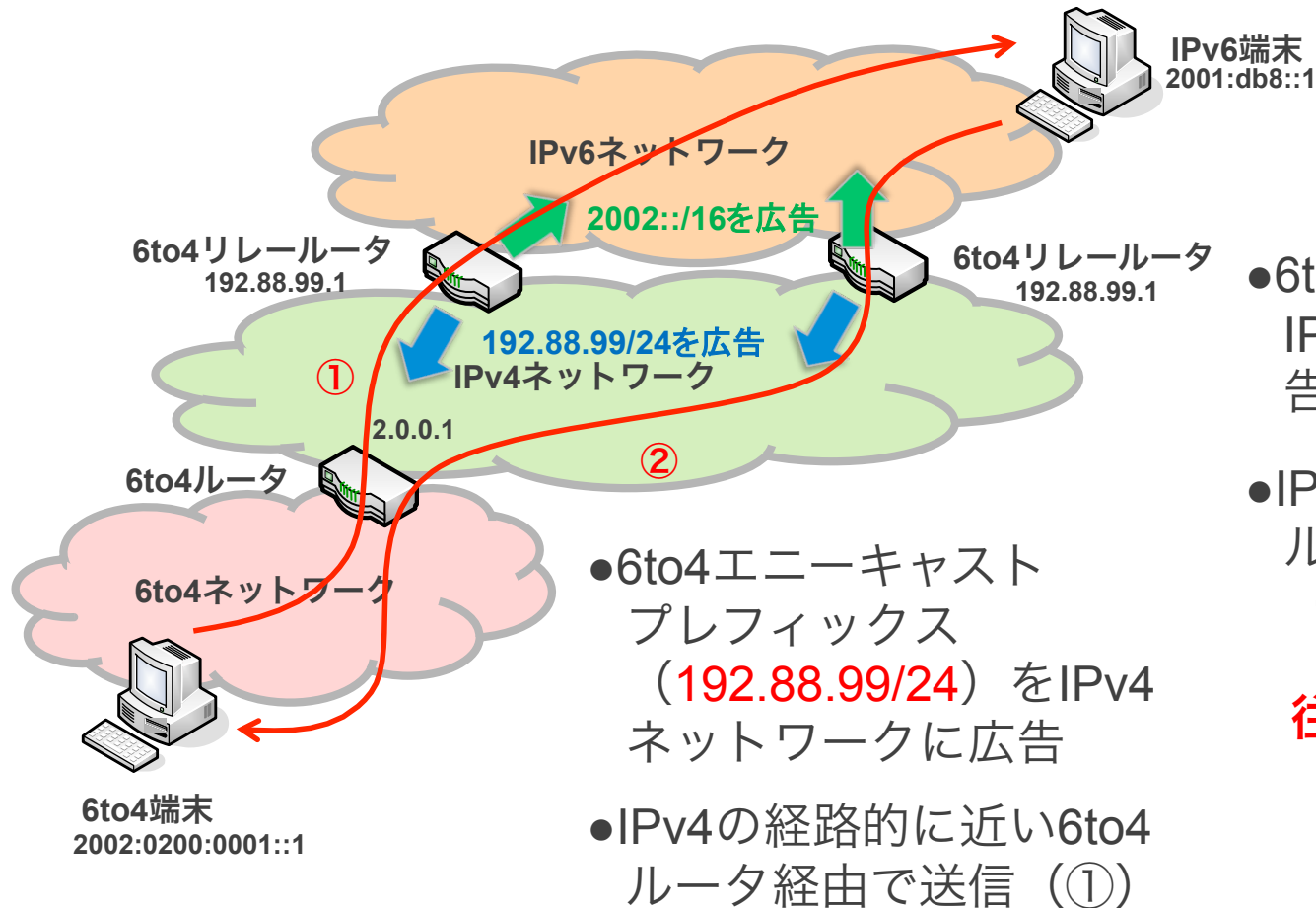
[RFC3068]

● 6to4ホスト/ルータ

- IPv4でカプセル化して6to4リレールータに転送
- IPv4グローバルアドレスが必要

6to4 (2)

● 6to4端末とIPv6端末の通信



- 6to4空間 (2002::/16) を IPv6ネットワークに広告
- IPv6の経路的に近い6to4ルータ経由で返信 (②)

往復の経路は基本的に異なる

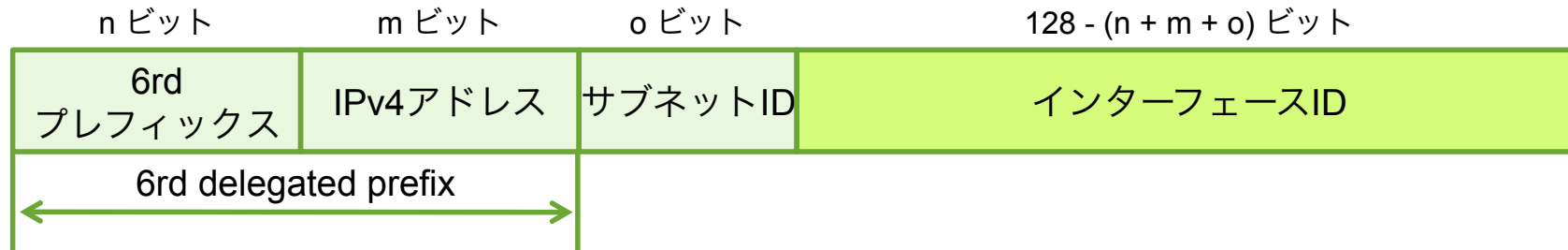


トラブルシュー트가困難

※6to4リレールータはボランティア運用が一般的

6rd

● 6rdのアドレス形式



● 6rd delegated prefixの生成例

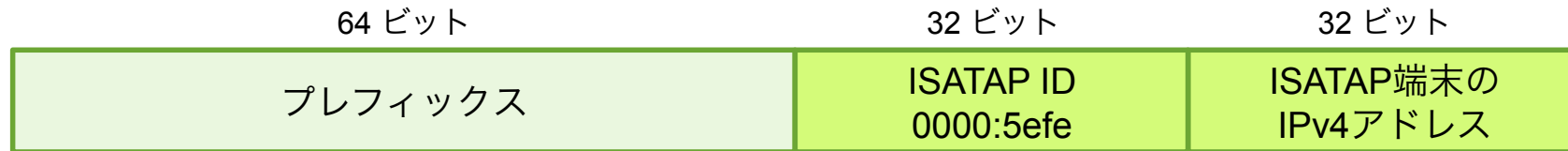
- ISPのIPv6プレフィックス 2001:db8::
- 6rdプレフィックス長 32
- IPv4マスク長 8
- ユーザCPEのIPv4アドレス 10.100.100.100

2001:db8::の32ビット分 10.100.100.100の後半24ビット分（先頭8ビットを除外）

2001:db8:6464:6400::/56 がユーザに割り当てられる

ISATAP

● ISATAPのアドレス形式



- プレフィックスには任意のものが利用可能

● ISATAP ID

- 00-00-5EはIANA-OUI
- FEはIPv4埋込みを示す
- IPv4グローバルアドレス利用の場合0200:5efeとなる

● ISATAPの特徴

- ISATAPルータとISATAPホスト間はリンクレイヤのように扱われる
- DHCPオプションでISATAPルータを配布可能

Teredo (1)

● Teredoのアドレス形式

32 ビット	32 ビット	16 ビット	16 ビット	32 ビット
Teredoプレフィックス 2001:0000	Teredoサーバの IPv4アドレス	フラグ	隠蔽した 外部ポート	隠蔽したNATルータの 外部IPv4アドレス

- 隠蔽方法はall 1とのXOR
- フラグには判別されたNATタイプが入る

● Teredoの構成要素

● Teredoサーバ

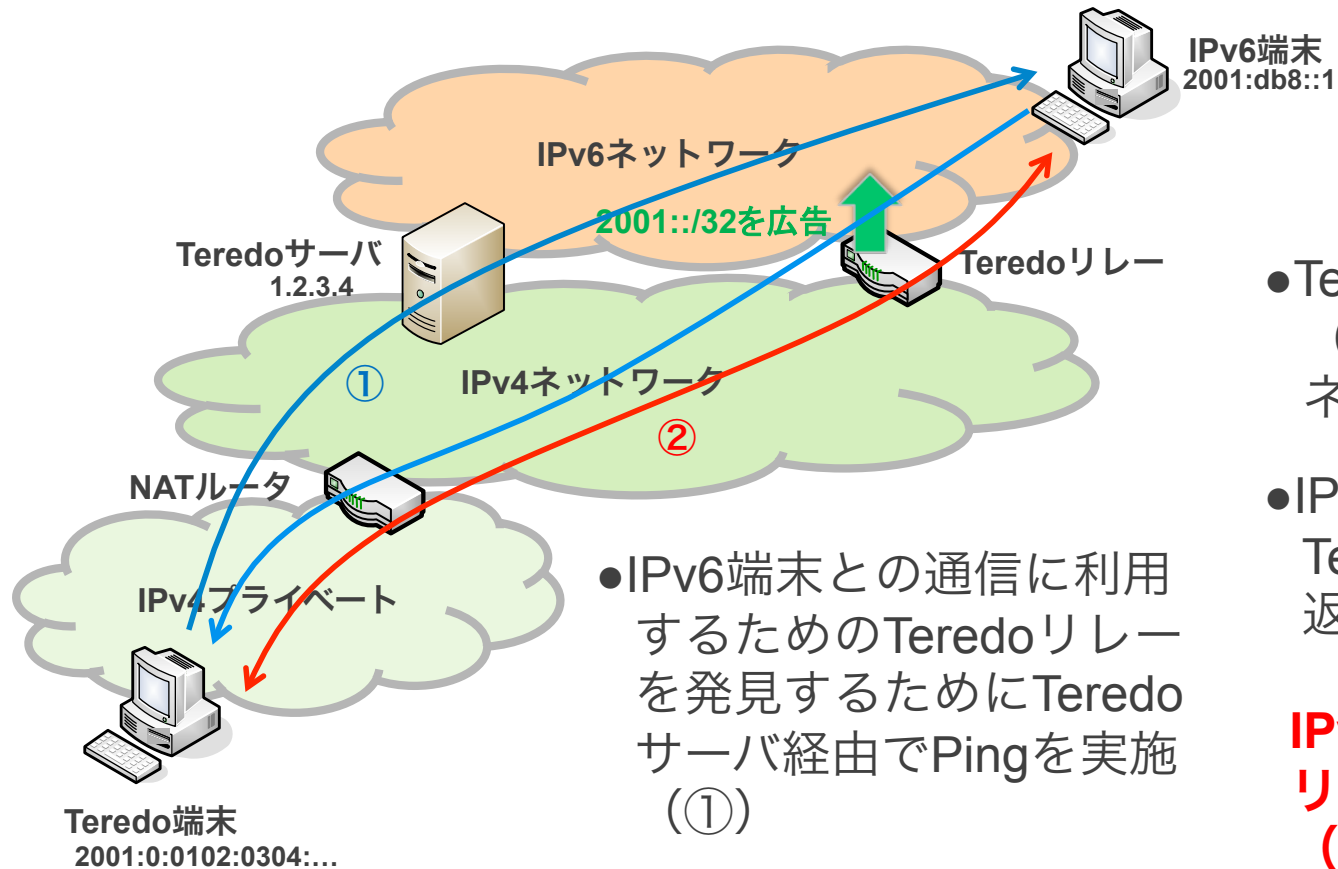
- TeredoクライアントのNATタイプ判定
- Teredoプレフィックス通知

● Teredoリレー

- IPv6ネットワークへの接続を提供
- IPv6ネットワークに2001::/32を広告
 - 経路的に近いTeredoリレーが選ばれる

Teredo (2)

● Teredo端末とIPv6端末の通信



- Teredo空間 (2001::/32) をIPv6ネットワークに広告

- IPv6の経路的に近いTeredoリレー経由で返信

IPv6端末に近いTeredoリレーを経由して通信 (②)

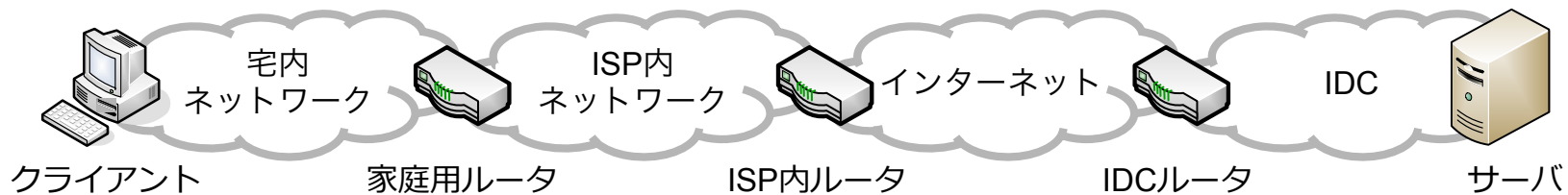
※TeredoサーバやTeredoリレーはボランティア運用が一般的

トランスレータの種別

- ヘッダ変換方式
 - IPv4ヘッダとIPv6ヘッダの相互変換を実現
 - IPv4でのNATに似た技術
 - NAT-PT ([RFC2766](#)で標準化されたが[RFC4966](#)でHistoricalに)
 - 処理のオーバヘッドは比較的小さいが制約がある
- TCPリレー方式
 - トランスポート層 (TCPセッション) での中継方式
 - TRT ([RFC3142](#)) など
 - ヘッダ変換方式よりも処理が大きいが制約は少ない
- アプリケーションレベルゲートウェイ方式
 - アプリケーションによる中継方式 (ALG方式)
 - 処理のオーバヘッドが一番大きくアプリケーション毎の対応が必要になるが相互接続性を完全に確立できる

万能ではないトランスレータ

● 変換アドレス空間からみた実現性と利用価値



	46NAT (IPv4⇒IPv6変換)	64NAT (IPv6⇒IPv4変換)	備考
家庭用ルータ	宅内ネットワークでプライベートIPv4アドレスが利用できるため空間の広いIPv6アドレスの対応付けが比較的容易	IPv6アドレスプレフィックスによるIPv4アドレス対応は容易 IPv4のNAT(NAPT)よりもプロトコル変換による制限があるのでデュアルスタック環境では利用価値は低い	IPv6非対応端末からIPv6サービスを利用するためには家庭用ルータにおけるアドレス変換が現実的
ISP内ルータ	IPv6ネットワーク空間用のIPv4アドレスプレフィックスを確保し顧客に伝える必要がある 変換時に利用するポート数に制限があるため利用顧客数により設備投資が必要	変換時に利用するポート数に制限があるため利用顧客数により設備投資が必要 IPv4のNAT(NAPT)よりも制限があるのでデュアルスタック環境では利用価値は低い	ネットワークの途中でのアドレス変換ではリソース管理が課題となる (CGNと同様の課題)
IDCルータ	内部のIPv6アドレスに対応づけるためにグローバルIPv4アドレスを同数確保する必要があり困難	内部のIPv4アドレスに対応させるIPv6アドレスは潤沢に用意できるため容易 サーバサイトのIPv6対応のために利用される可能性が高い	IDCにおいてIPv6のみのサービスに対してIPv4からの到達性を確保することは困難

その他の機能

セキュリティ機能とQoS機能

● IPv6のセキュリティ機能

● IPsecを考慮した設計

- IPv4では後付け機能のIPsecを標準実装（拡張ヘッダの一部）
- 認証ヘッダ（AH）：認証，完全性を提供
- 暗号ペイロード（ESP）：認証，完全性，機密性を保証

● 鍵管理（IKE）

- IPv6の範囲外で定義し柔軟な暗号化技術の利用が可能

● IPv6のQoS機能

● IPv6で登場したフローラベル（Flow Label）

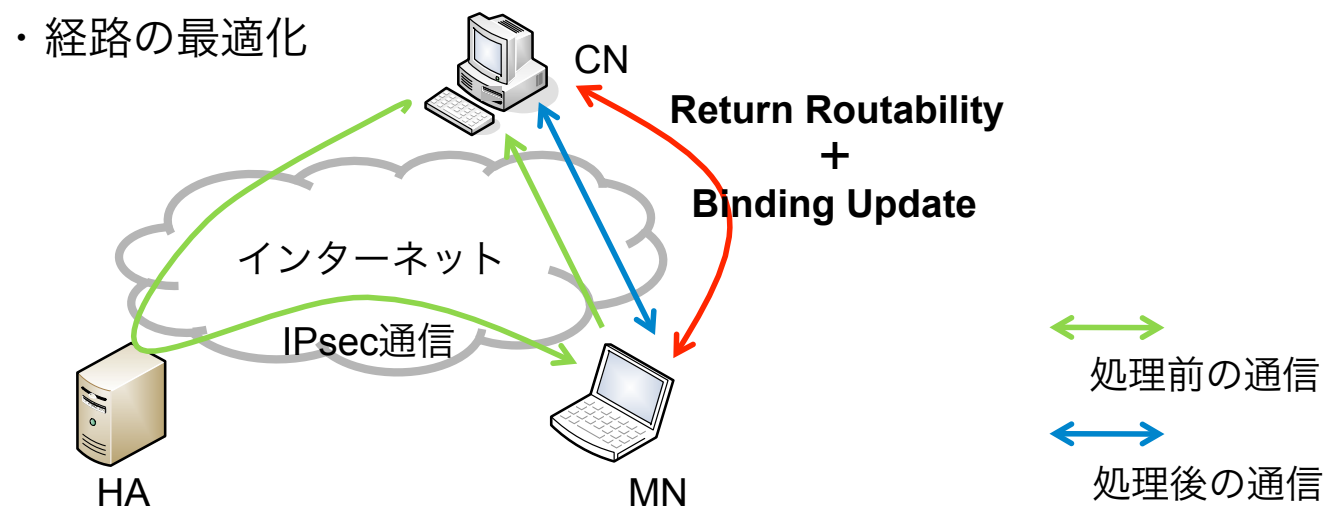
- IPv6ヘッダに定義されているが利用方法は明確になっていない

モビリティ機能

● IPv6のモビリティ機能

● モバイルIPv6 (MIPv6)

- 経路最適化のために用意された拡張ヘッダ
- ルーティングヘッダ (Type 2) : 経由ルータを1つだけ指定可能
- 宛先オプションヘッダ (Home Address Option) : HoAを指定



● NEMO (Network Mobility)

- IPv6におけるネットワークの移動性を提供する

IPv6における動的経路制御

- IGP : Interior Gateway Protocol
 - AS内における経路制御方式
 - 距離ベクトル型 (Distance Vector) : RIP, IGRP
 - リンクステート型 (Link State) : OSPF, IS-IS
- EGP : Exterior Gateway Protocol
 - AS間の経路制御方式
 - パスベクトル型 (Path Vector) : BGP

	IPv4	IPv6
IGP	RIPv2	RIPng
	OSPFv2	OSPFv3
	ISIS	ISIS for IPv6
EGP	BGP4	MP-BGP4
Multicast (Group Mgmt.)	PIM (IGMPv2/v3)	PIM (MLDv1/v2)

AAAAグルーレコードの登録

- AAAAグルーレコードが登録できないと
 - IPv6オンリーサイトからDNSの名前解決ができない
- DNSレジストラの対応が芳しくない現状
 - JPドメインでは6社のみ可能（2010年11月現在）
21-Domain.com, インターネットサービス, STCN, avis,
ドメインネーム・フォー・ユー, @ドメイン （提供会社50音順）
- 登録可能なレジストラ情報
 - JPRSによるJPドメインにおける対応レジストラ情報
 - 汎用JPドメイン：http://jpshop.jp/list/gjp_list/gjp_pl1_01.html
 - 属性型JPドメイン：http://jpshop.jp/list/ojp_list/ojp_pl1_01.html
 - SixXSによる他のTLDにおける対応レジストラ情報
 - <http://www.sixxs.net/faq/dns/?faq=ipv6glue>

OS毎のDNSリゾルバ実装

- クエリ順序はOSで異なる
 - AAAAクエリを先に実施するOS
 - Windows XP、Linux
 - Aクエリを先に実施するOS
 - Windows Vista、Windows 7、FreeBSD、Mac OS X
- 利用プロトコルの優先順位
 - IPv6を優先的に利用するOS
 - Windows Vista、Windows 7
 - IPv4しか利用できないOS
 - Windows XP
 - 設定ファイルに依存するOS (/etc/resolv.confの順序)
 - FreeBSD、Linux

アドレス選択機構

- IPv6では複数のアドレスを使い分ける必要がある
 - リンクローカルアドレスとグローバルアドレス
 - IPv4アドレスとIPv6アドレス など
- Default Address Selection for IPv6 [RFC3484]
 - 複数のアドレスを選択するための基準
 - 宛先アドレス選択と送信元アドレス選択のルール
 - ポリシーテーブルの定義
- 実装状況
 - RFC3484の実装はほぼすべてのOSで完了
 - Mac OS Xは未実装
 - ポリシーテーブル操作が不可のものもある
 - Linuxはkernel 2.6.25（要iproute2-2.6.25以上）から送信元アドレスのためのラベル操作が可能

アドレス選択のルール

● 宛先アドレス選択ルール

- Rule 1 : 到達不能などの使用できないアドレスを避ける
- Rule 2 : スコープが同じアドレスを優先
- Rule 3 : 非推奨アドレスを避ける
- Rule 4 : ホームアドレス（モバイルIP用）を優先
- Rule 5 : ポリシーテーブルにて送信元アドレスとラベルが同じアドレスを優先
- Rule 6 : ポリシーテーブルにて優先度が高いアドレスを優先
- Rule 7 : トランスポートがネイティブなものを優先
- Rule 8 : スコープが小さいものを優先
- Rule 9 : 送信元アドレスとLongest prefix matchとなるアドレスを優先
- Rule 10 : 与えられたアドレスリストの順番を利用

● 送信元アドレス選択ルール

- Rule 1 : 宛先アドレスと同じアドレスを優先
- Rule 2 : 宛先アドレスに対する適切なスコープのアドレスが優先
- Rule 3 : 非推奨アドレスを避ける
- Rule 4 : ホームアドレス（モバイルIP用）を優先
- Rule 5 : 送信先インターフェースに付与されたアドレスを優先
- Rule 6 : ポリシーテーブルにて宛先アドレスとラベルが同じアドレスを優先
- Rule 7 : 一時アドレス（Temporary）よりも公共アドレス（Public）を優先
- Rule 8 : 宛先アドレスとLongest prefix matchとなるアドレスを優先

Longest prefix match

- プレフィックスの最長一致
 - プレフィックスの先頭ビットから最も長く一致するものを選択するルール

	16進数表記	2進数表記
宛先アドレス	2001:db8:1:1::1	0010 0000 0000 0001 1100 ...
候補アドレス1 ○	2001:db8:1:100::1	<u>0010 0000 0000 0001 1100 ...</u>
候補アドレス2	2002:a00:1:1::1	<u>0010 0000 0000 0010 1010 ...</u>

※ 先頭からのビットパターンが長く一致する候補アドレス1が送信元アドレスに選ばれる

- アドレス選択ルールの最終手段として用いられる

ポリシーテーブルのデフォルト定義

● ポリシーテーブル

- アドレス選択時に利用するラベルや優先度を定義

- 優先度 (Precedence)

 - 宛先アドレス選択時に利用され値が大きいものが優先

- ラベル (Label) を定義

 - 宛先と送信元アドレス選択時に利用され一致するものが優先

● デフォルト定義

Prefix	Precedence	Label	

::1/128	50	0	loopbak address
::/0	40	1	IPv6 address
2002::/16	30	2	6to4 address
::/96	20	3	IPv4 compatible address
::ffff:0:0/96	10	4	IPv4 mapped address (IPv4 address)

ポリシーテーブルの実装 (1)

- Windows 7/Vistaのデフォルト設定

- **netsh interface ipv6 show prefixpolicies** で確認

```
C:>netsh interface ipv6 show prefixpolicies
アクティブ状態を照会しています...
```

優先順位	ラベル	プレフィックス		
50	0	::1/128		
40	1	::/0	IPv6アドレス	
30	2	2002::/16		6to4アドレス
20	3	::/96		
10	4	::ffff:0:0/96	IPv4アドレス	
5	5	2001::/32		Teredoアドレス

```
C:¥Windows¥system32>
```

- RFC3484における標準設定 + Teredoプレフィックス

ポリシーテーブルの実装 (2)

- Linux (kernel 2.6.25以上)

- ip addrlabel show で確認可能 (iproute2-2.6.25以上)

```
$ ip addrlabel show
prefix ::1/128 label 0
prefix ::/96 label 3
prefix ::ffff:0.0.0.0/96 label 4
prefix 2001::/32 label 6
prefix 2002::/16 label 2
prefix fc00::/7 label 5
prefix ::/0 label 1
```

ULA

- LinuxではULAのラベルも独自追加されている
- 優先度は/etc/gai.confで設定

```
$ cat /etc/gai.conf
...
#precedence ::1/128 50
#precedence ::/0 40
#precedence 2002::/16 30
#precedence ::/96 20
#precedence ::ffff:0:0/96 10
...
```

※デフォルトは/usr/share/doc/glibc-common-2.*/gai.conf