IPv6オペレータ育成プログラム

SOHO/一般ユーザ向けネットワーク編［講義資料］

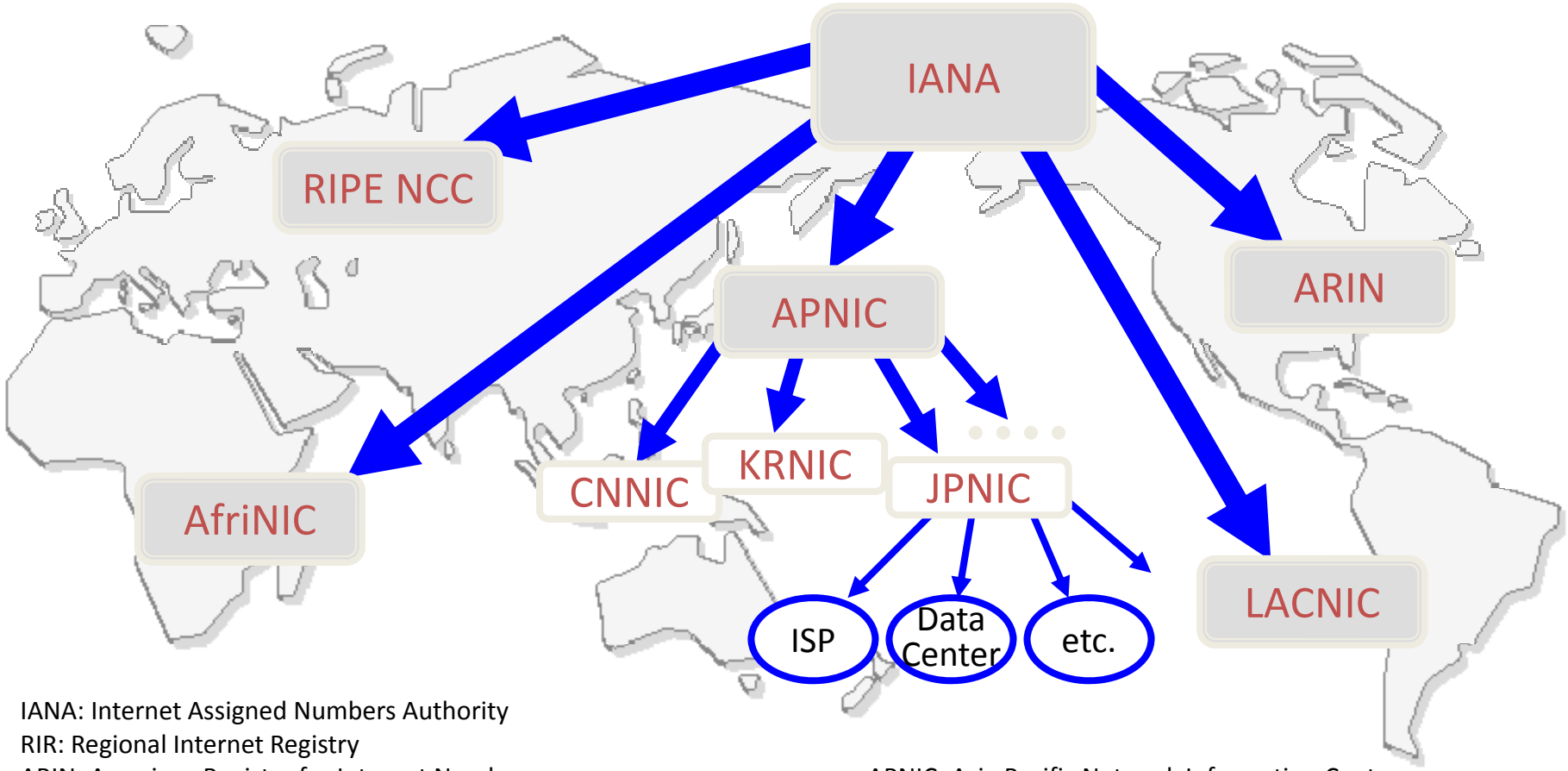
NECアクセステクニカ株式会社
川島　正伸

Contents

- IPv4アドレス枯渇状況と対策
- IPv6プロトコル基礎知識
- DHCPv6
- ルーティングプロトコル
- 移行技術
- DNS
- アドレス選択とマルチプレフィックス問題
- TCPフォールバック問題
- セキュリティ
- その他

IPv4アドレス枯渇状況と対策

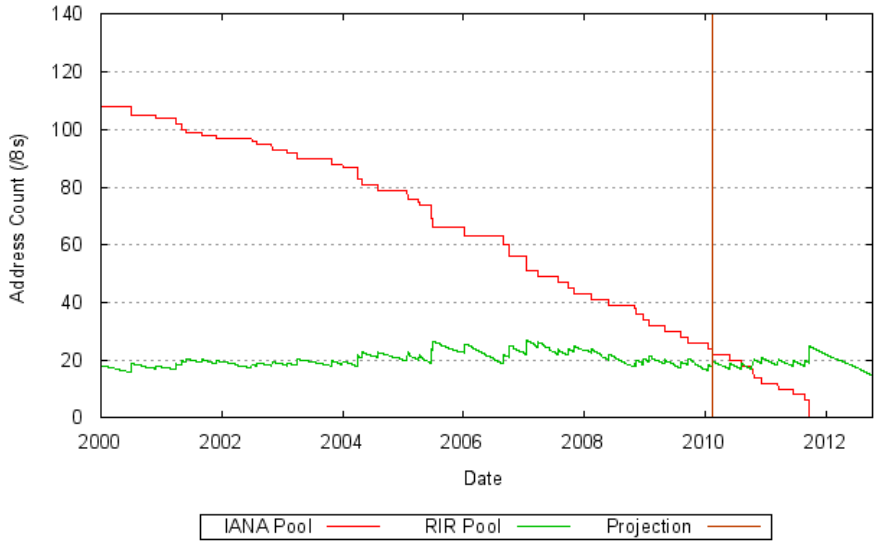
IPアドレス管理の階層構造

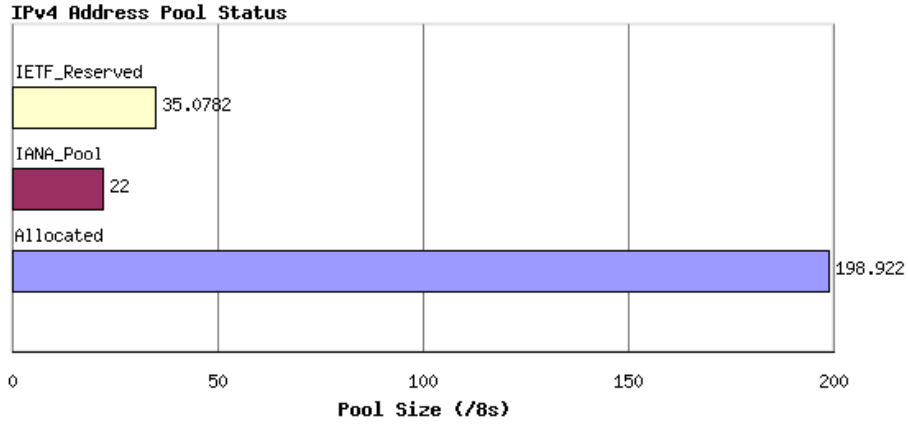


IANA: Internet Assigned Numbers Authority
RIR: Regional Internet Registry
ARIN: American Registry for Internet Numbers
RIPE NCC: Resource IP Europeans Network Coordination Centre
LACNIC: Latin American and Caribbean Internet Address Registry
AfriNIC: African Network Information Centre

APNIC: Asia Pacific Network Information Center
JPNIC: Japan Network Information Center
KRNIC: Korea Network Information Center
CNNIC: China Internet Network Information Center

IPv4アドレス枯渇予測と現状





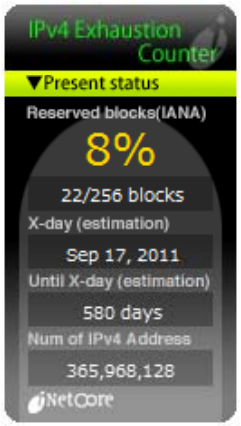
IPv4 Address Report (http://www.potaroo.net/tools/ipv4/)

APNIC Chief Scientist の Geoff Huston 氏による予測（2010/2/13 時点）

- IANA pool 枯渇は 2011年9月
- RIR pool 枯渇は 2012年10月

残り 22 ブロック（ 1 ブロックは /8 ）
22 / 256 ブロック ＝ 8 %
最後の5ブロックは各RIRに分配され、トランスレータなどのIPv6 移行用途に使用される予定

過去のアドレス割当て
2005年　13 ブロック
2006年　10 ブロック
2007年　13 ブロック
2008年　 9 ブロック
2009年　 8 ブロック
2010年　 4 ブロック（2010/2/13時点）



http://枯渇時計.com

IPv4アドレス枯渇対策（1）

- IPv4アドレスの移転 IPv4延命策
  - 遊休アドレス再利用によりグローバルアドレス を有効活用
  - ARIN（2件処理済）、RIPE NCC は施行中。
  - APNIC でも 2010年2月より施行開始。
    - JPNIC（国内）は、2009年11月のJPNIC Open Policy Meeting にて、コンセンサスが得られ、施行に向けて準備中。
- IPv4アドレス延命技術 IPv4延命策
  - 大規模NAT を用いる LSN、DS-Lite など複数の方式が IETF で議論されている。いずれもグローバルアドレスの消費を抑制することが狙い。
  - その他に behave WG にてトランスレータ技術に関する検討も行われている。

IPv4アドレス枯渇対策（2）

- IPv6の導入 **恒久対策**
  - IPv4アドレス枯渇が現実味を帯びてきて、IPv6 への期待が高まっている
  - ネットワーク機器や主要なサーバOS、ホストOS における IPv6 対応は概ね完了しているが、アプリケーション開発や運用面でのIPv6 対応が遅れているのが実状。
  - 国内では、NTT-NGN におけるマルチプレフィクス問題の動向が注目されていたが、兆しが見えてきた。
    - NTT東西は 2009年5月にIPv6 インターネット接続機能を提供するための接続約款変更の認可申請を行った。2011年4月 以降にはIPv6インターネット接続サービスが開始される見込み。
    - 国内の各ISP、CATV、iDC 事業者におけるサービス検討も始まっている。

IPv6プロトコル基礎知識

IPv6の特徴（1）

- アドレス空間の拡張
  - IPv4 (32bit) ＝ 約43億個
  - IPv6 (128bit) ＝ 約340澗個
    - 億＜兆＜京＜垓＜杼＜穣＜溝＜澗
  - 全世界の人口を100億人とした場合、
    1人当たり 3.4 × 10^28個のアドレスを割当て可能
    - 携帯電話、カーナビ、インターネット家電、センサ等にも
      割当て可能な膨大なアドレス空間

- 階層化アドレス構造
  - 効率的なネットワーク管理、ルータ等の処理負荷軽減

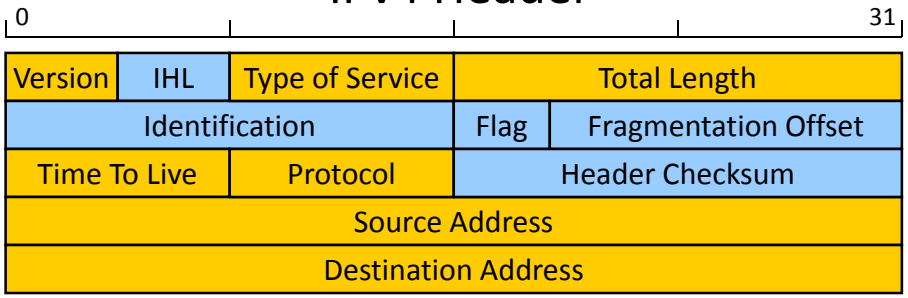
IPv6の特徴（2）

- Plug & Play による容易なアドレス設定
  - 情報家電の普及
- Multicast の標準実装
  - 放送と通信の融合
- 移動体通信への考慮
  - Mobile IP による固定網と移動網のシームレス化

IPv6基本ヘッダ（1）

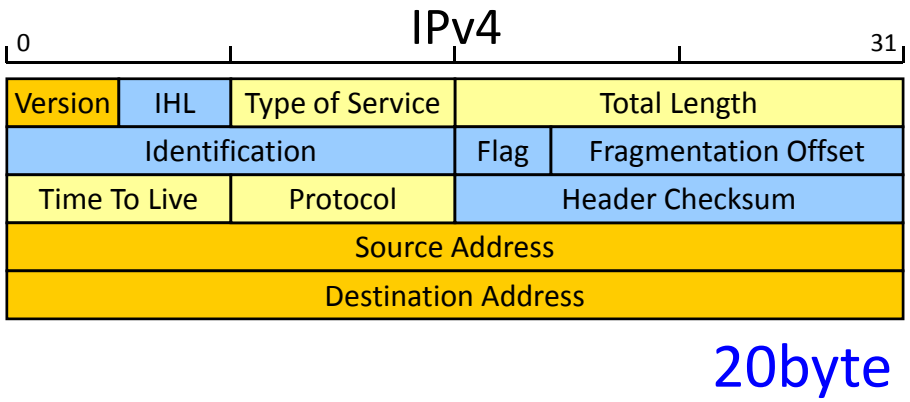
- IPv6 では使用されないフィールド（ の部分）
  - IPv6 ではヘッダ長固定（40byte）
    - IHL (Internet Header Length) 不要
  - IPv6 ではルータ等の中継ノードはフラグメントしない
    - Identification、Flag、Fragmentation Offset 不要
    - エンドノードのフラグメントは拡張ヘッダで対応
  - IPv6 では IP層ではチェックサム計算、更新をしない
    - Header Checksum 不要

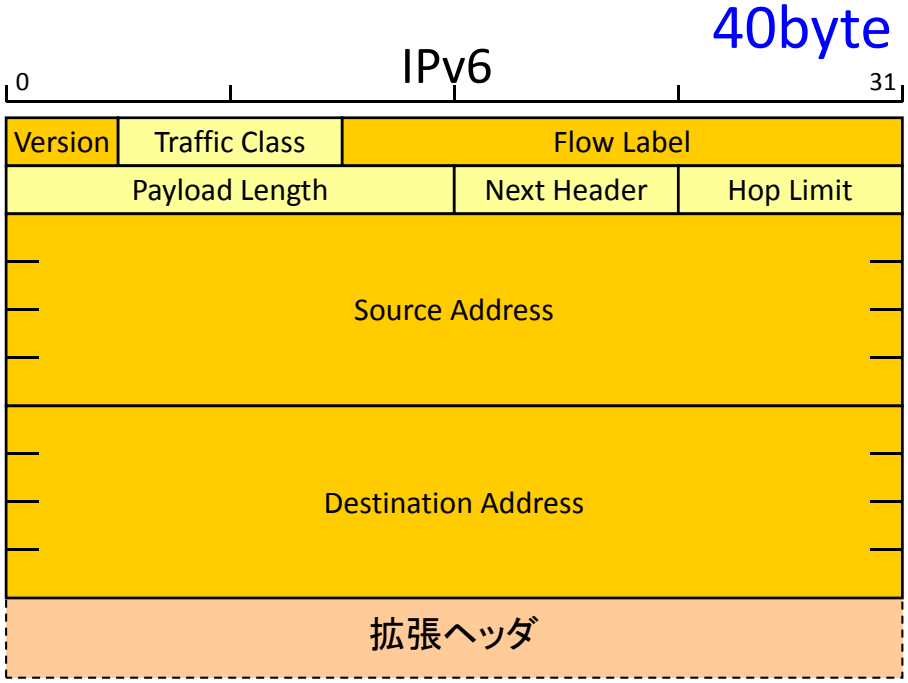
IPv4 Header



IPv6基本ヘッダ（2）

- フィールド名称の変更など（ の部分）
  - Type of Service → Traffic Class
  - Total Length → Payload Length
  - Time To Live → Hop Limit
  - Protocol → Next Header

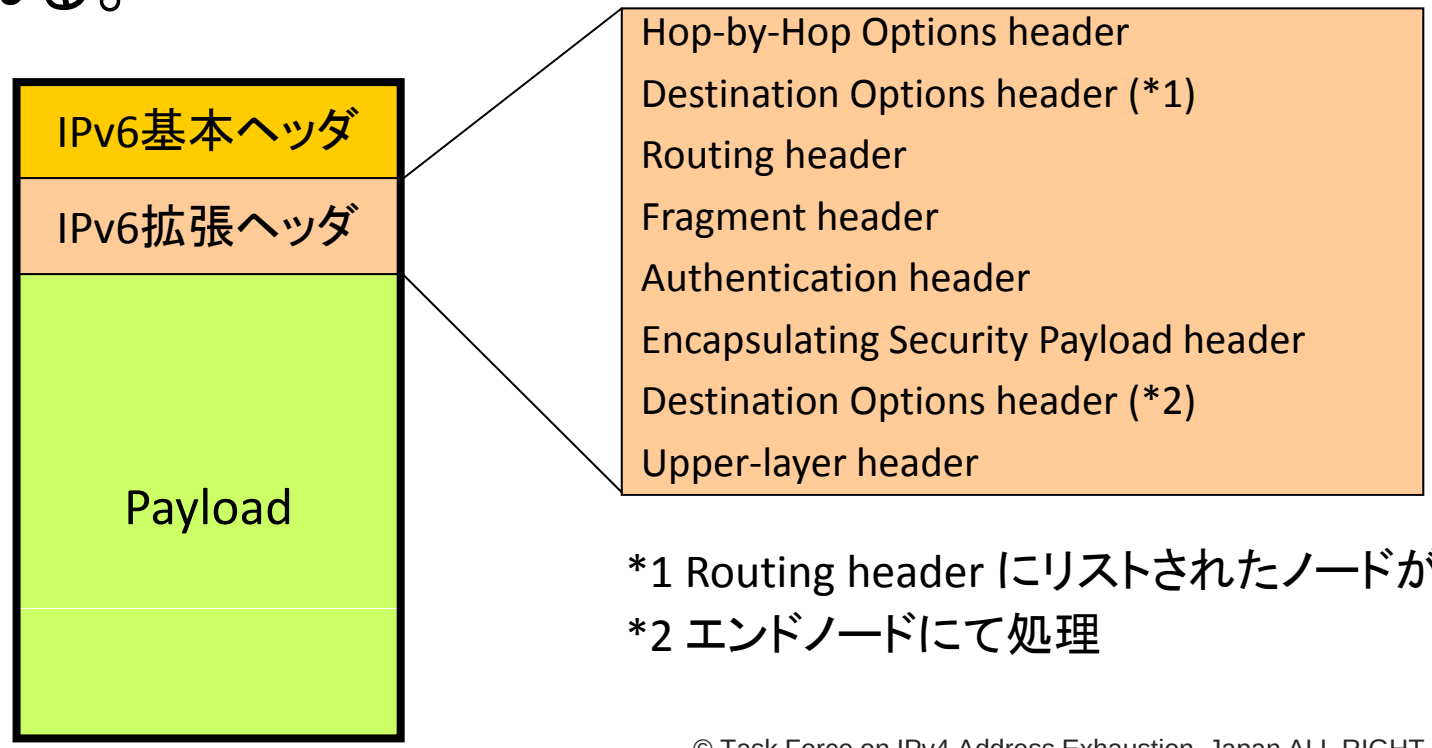




- オプション的な機能は拡張ヘッダで対応

IPv6拡張ヘッダ

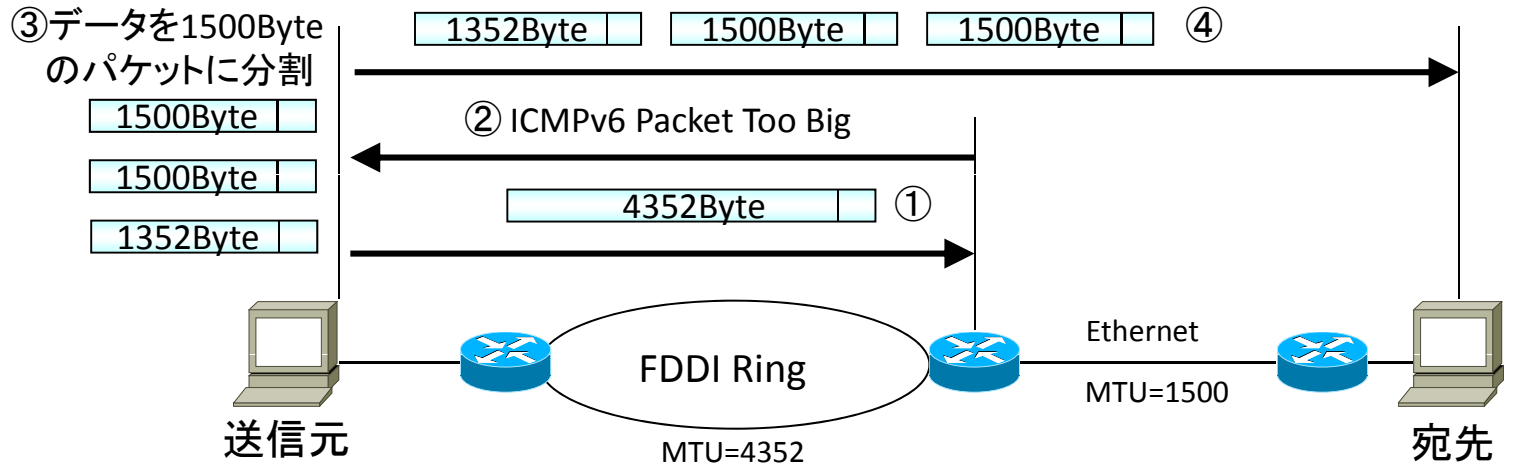
- 全てのノードで処理すべきものと、エンドノードで処理するものを分離。
- 拡張ヘッダの推奨順序は決まっている。出現順で処理される。



*1 Routing header にリストされたノードが処理
*2 エンドノードにて処理

Path MTU Discovery

- IPv6 では中継ノードでフラグメントしない（始点ノードが実施）
  - IPv4 ではルータ等の中継ノードがフラグメントを実施
  - 送信パケットに対する ICMPv6 Error Message を受信時、MTU を変更
    - 最初のリンクのMTU が初期値
    - ICMPv6 Packet Too Big Message 受信時、始点ノードでフラグメントして再送
  - IPv6最小MTU は、1280byte
    - Path MTU Discovery の実装が難しいノードは 1280byte 固定



IPv6アドレス表記

- 128bit を 16bit 毎に 8分割後、各フィールドを 16進数表記にして、“ : ”(コロン)で区切る。

  00100000000000010000110110111000000000000000000000000000000000000000000010000001100010100111111111111111100001111001001000001011 10

  ↓

  2001:0db8:0000:0000:0206:29ff:fe1e:482e

- 先行する 0 は省略可能。但し、各フィールドには少なくとも 1つの数値を含むこと。

  2001:0db8:0000:0000:0206:29ff:fe1e:482e

  ↓

  2001:db8:0:0:206:29ff:fe1e:482e

- 16bit の 0 または、16bit の 0 が複数連続するフィールドを 1箇所のみ、”::”を用いて省略可能。

  2001:db8:0:0:206:29ff:fe1e:482e

  ↓

  2001:db8::206:29ff:fe1e:482e

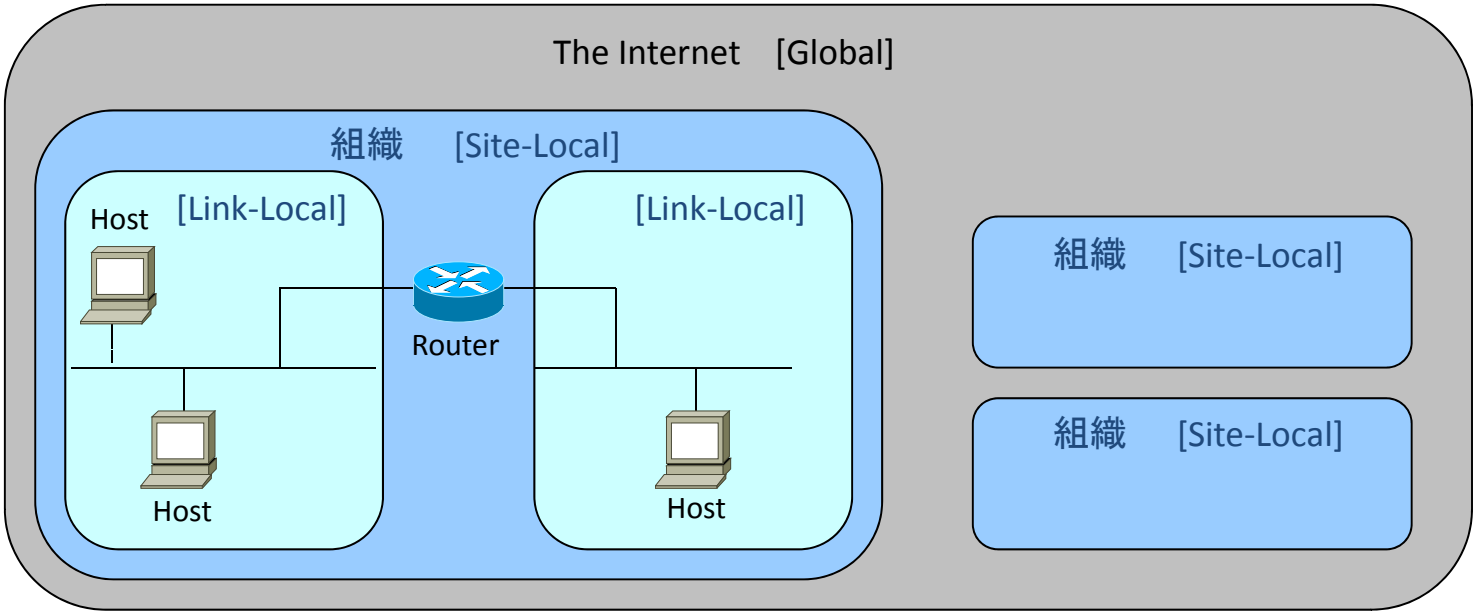
（参考）IPv6アドレス表記の柔軟性

- IPv6アドレスの省略表記は必須ではない為、省略してもよいし、省略しなくてもよい。
  - RFC4291（IP Version 6 Addressing Architecture）
  - 製品やシステム毎に様々なIPv6アドレス表記 が存在。
    - IPv6アドレス検索、ログ分析、設定情報の監査、ユーザからの問合せ時など、多くの場面で問題となりそう。
- 問題の発生を減らすために代表的な表記方法がIETF の 6man WG で議論されている。
  - A Recommendation for IPv6 Address Text Representation [draft-ietf-6man-text-addr-representation-04] (work in progress)
    - IETF Last Call が終了、IESG によるレビュー中。

IPv6アドレスタイプとスコープ

Address type	Binary prefix	IPv6 notation
Link-Local unicast	1111 1110 10	fe80::/10
Site-Local unicast	1111 1110 11	fec0::/10
Global unicast	(everything else)	

[RFC3879]
Deprecating
Site Local Addresses



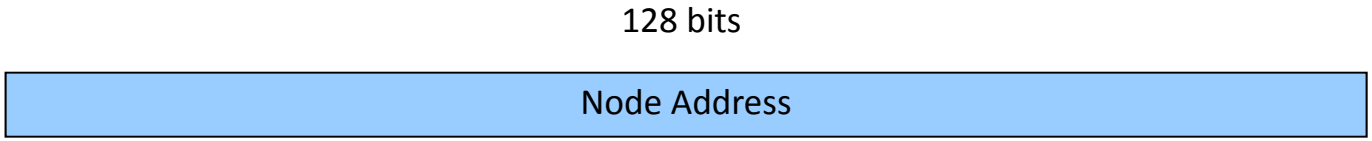
IPv6アドレスタイプと通信形態

アドレスタイプ	付与対象	通信形態
Unicast	Interface	1 : 1
Anycast	Service	1 : 1 ※
Multicast	Group	1 : n

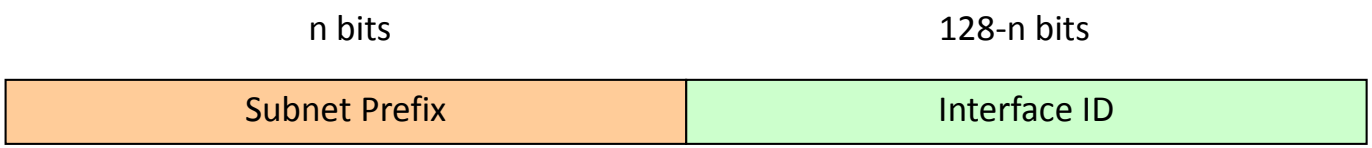
※ネットワーク的に最も近い1つを選択

Unicast Address（1）

- ノードのアドレス

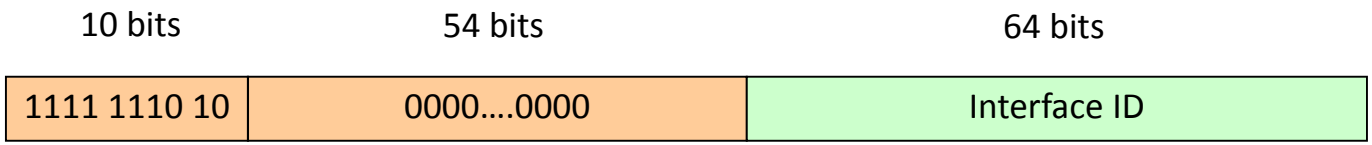


- サブネットプレフィックスとインタフェースID

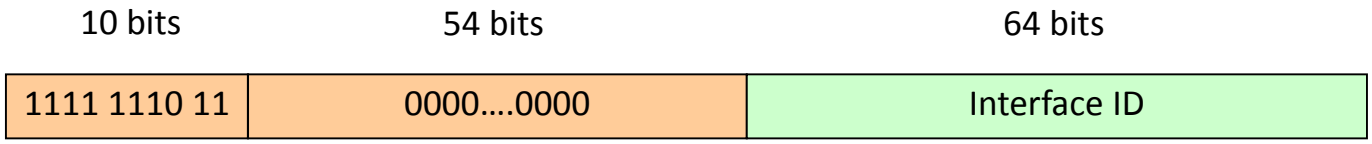


Unicast Address（2）

- リンクローカルアドレス（fe80::/10）
  - 同一リンク上でのみ通信可能（ルータを越える通信はできない）
  - NDPなどの管理トラフィックで使用される

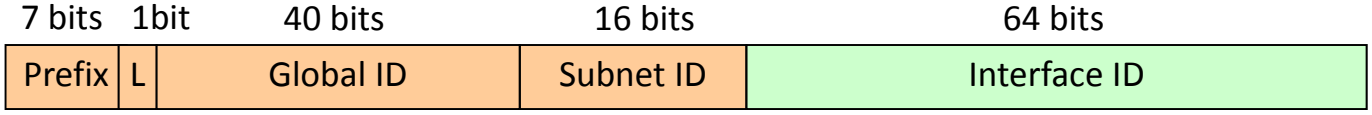


- サイトローカルアドレス（fec0::/10）
  - 同一サイト内でのみ通信可能（ルータを越えて通信できる）
  - サイトの定義困難、NAT 助長などの問題により廃止された。
    - Deprecating Site Local Addresses [RFC3879]



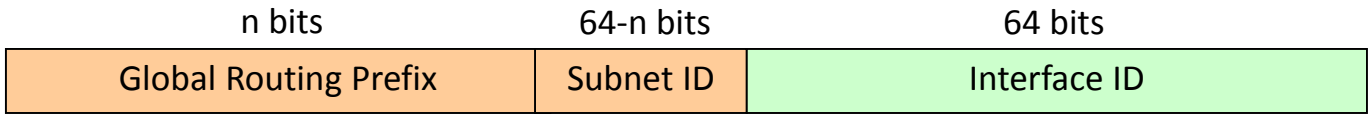
Unicast Address（3）

- ユニークローカルアドレス［ULA］（fc00::/7）
  - サイトローカルアドレスの代替アドレスとして標準化された
    - Unique Local IPv6 Unicast Addresses [RFC4193]
  - アドレスフォーマット
    - Prefix　：　fc00::/7
    - L = 1　：　ローカル管理による割当て
      - L = 0 は、将来の為に予約。（RIR/LIR による管理を想定。）
    - Global ID　：　ランダム生成（L = 1 が前提）
      - trunc(SHA1(NTP current time + EUI-64) , 40bit)
      - ULA Generator http://www.kame.net/~suz/gen-ula.html
  - インターネット接続がなくてもサイト内通信用途で利用可能
    - グローバルスコープかつ ISP非依存なアドレスとなっているが インターネットへ送信することは禁止されている



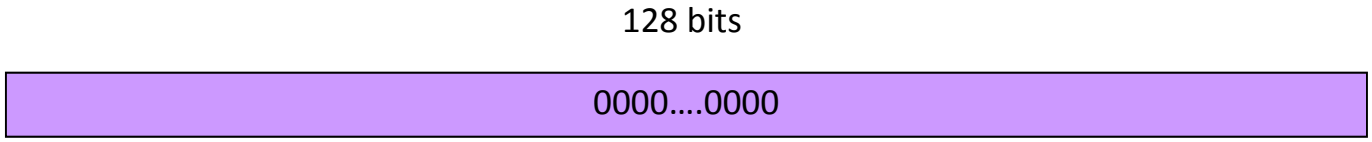
Unicast Address（4）

- グローバルユニキャストアドレス
  - 歴史的経緯により、現在は 2000::/3 のアドレス空間を使用中
    - RFC3587（IPv6 Global Unicast Address Format）
  - Global Routing Prefix
    - RIR もしくは NIR、LIR より割り当てられる
  - Subnet ID
    - サイト内のリンク識別に使用
  - Interface ID
    - サブネット内のインタフェース識別に使用
  - 割り当て状況は、以下で確認可能
    - [IANA→RIR] http://www.iana.org/assignments/ipv6-unicast-address-assignments
    - [IPv6 DFP visibility] http://www.sixxs.net/tools/grh/dfp/

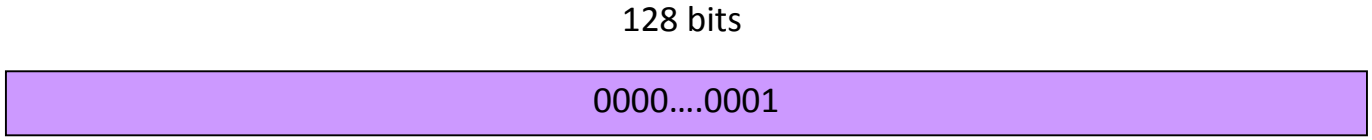


Unicast Address（5）

- 未指定アドレス（::）
  - IPv4 の 0.0.0.0 に相当

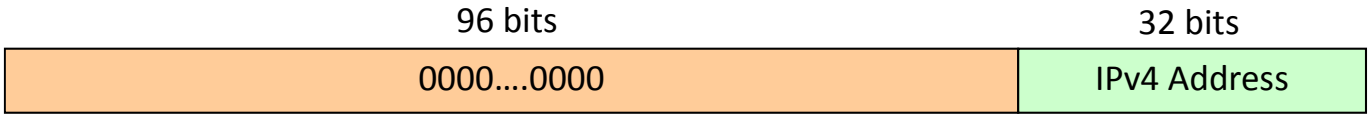


- ループバックアドレス（::1）
  - IPv4 の 127.0.0.1 に相当



Unicast Address（6）

- IPv4互換 IPv6アドレス（ IPv4-Compatible IPv6 Address ）
  - Automatic Tunneling 用途。現在は非推奨アドレス。
  - 例 ::192.168.1.1



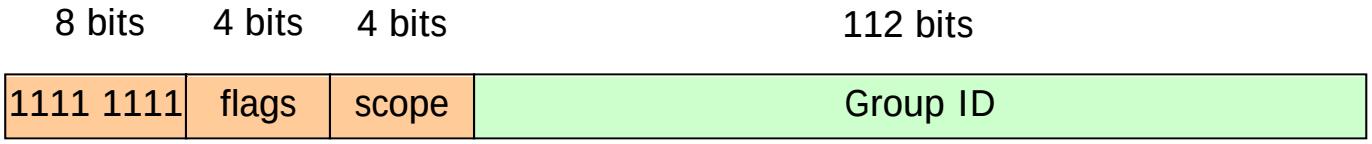
- IPv4射影 IPv6アドレス（ IPv4-Mapped IPv6 Address ）
  - IPv4アドレスのみ有するノードを IPv6アドレスで表現したアドレス。
    IPv6のみに対応したアプリケーションの内部通信などで用いられる。
    - セキュリティホールにならないよう適切なアクセス制御が必要。
  - 例 ::ffff:192.168.1.1

Anycast Address

- アドレス自体は、Unicast Address の範囲
- 複数のインタフェースに同一の Unicast Address を割当てるとAnycast Address になる
- ルーティング上、最も近いインタフェースに転送される
- 具体例
  - Subnet Router Anycast Address [RFC4291]
  - Mobile IPv6 Home-Agents anycast [RFC2526]
  - 6to4 Relay Router [RFC3068]
  - Root Server や JP DNS（a.dns.jp , d.dns.jp , e.dns.jp）
    - 対障害性やDDoS攻撃の影響分散などの目的で、分散配置されたサーバで使用されている

Multicast Address（1）

- 1対n 通信を行う場合に使用される
  - 映像のライブ配信など、特定のグループに向けて送信される
  - IPv6 では NDP（Neighbor Discovery Protocol ）においても積極的に使用されている
- Scope
  - Scope = 1 ： Interface-local
  - Scope = 2 ： Link-local
  - Scope = 4 ： Admin-local
  - Scope = 5 ： Site-local
  - Scope = 8 ： Organization-local
  - Scope = e ： Global scope



Multicast Address（2）

- 予約済みのMulticast Address
  - ff02::1 : All nodes
  - ff02::2 : All routers
  - ff02::5 : All OSPF routers
  - ff02::6 : All OSPF Designated Routers
  - ff02::9 : All RIP routers
  - ff02::1:2 : All DHCP Agents（Relay Agents & Servers）
  - ff02::1:3 : LLMNR（Link-Local Multicast Name Resolution）
  - ff02::1:ff : Solicited-Node address

  - 最新の割当て状況は以下で確認可能
    - http://www.iana.org/assignments/ipv6-multicast-addresses

Multicast Address（3）

- Solicited Node Multicast Address（ff02::1:ff/104）
  - 要請ノードマルチキャストアドレス
  - Link Layer Address 解決時に使用（IPv4 のARP相当）
  - ブロードキャストドメインよりも小さい特定のグループ宛

fe80::240:26ff:fe18:19b1

↓

ff02::1:ff18:19b1

(Multicast Address と Ethernet Addressの関係）

ff02::1:ff18:19b1

↓

(MAC Address) 33:33:ff:18:19:b1

※“33:33”にMulticast の下位4byteを連結

ノードやルータが使うIPv6アドレス

- IPv6 では、IPv4 よりも多くのアドレスが使用される

- ノードが使う IPv6アドレス
  - ループバックアドレス (::1/128)
  - 全ノードマルチキャストアドレス (ff0x::1)
  - 要請ノードマルチキャストアドレス (ff02::1:ff/104)
  - インタフェース毎に1つのリンクローカルアドレス (fe80::/10)
  - インタフェース毎に1つまたは複数のユニキャストアドレス
  - 自分が所属するグループのマルチキャストアドレス

- ルータが使う IPv6アドレス
  - ノードが使う IPv6アドレス
  - 全ルータマルチキャストアドレス (ff0x::2)
  - サブネットルータエニィキャストアドレス (Subnet Prefix 以外All 0)

ICMPv6（1）

- Internet Control Message Protocol for IPv6 [RFC4443]
- ネットワーク状態に関するメッセージ群
- IPv4 の ICMP ＋ α の機能
  - 近隣探索（Neighbor Discovery）
  - マルチキャストグループ管理
    - IPv4 の IGMP（Internet Group Management Protocol）相当
  - Mobile IPv6 サポート
    - Home Agentアドレス探索など

ICMPv6（2）

- ICMPv6エラーメッセージ
  - 終点到達不能　Destination Unreachable Message　（Type = 1）
  - パケット過大　Packet Too Big Message　（Type = 2）
  - 有効時間超過　Time Exceeded Message　（Type = 3）
  - パラメータ異常　Parameter Problem Message（Type = 4）
- エコー要求・応答メッセージ
  - エコー要求　Echo Request Message　（Type = 128）
  - エコー応答　Echo Reply Message　（Type = 129）
- マルチキャスト関連メッセージ（MLDv1、MLDv2で使用）
  - マルチキャストリスナー照会　Multicast Listener Query　（Type = 130）
  - マルチキャストリスナー報告　Multicast Listener Report　（Type = 131）
  - マルチキャストリスナー終了　Multicast Listener Done　（Type = 132）
  - マルチキャストリスナー報告　Version 2 Multicast Listener Report　（Type = 143）
    Version 2

ICMPv6（3）

- 近隣探索メッセージ（NDPで使用）
  - ルータ要請（RS）　Router Solicitation Massage　（Type = 133）
    - ノードからルータへ問合せ。
  - ルータ広告（RA）　Router Advertisement Message（Type = 134）
    - ルータからノードへ通知
  - 近隣要請（NS）　Neighbor Solicitation Message（Type = 135）
    - 近隣ノードから近隣ノードへ問合せ
  - 近隣通知（NA）　Neighbor Advertisement Message（Type = 136）
    - 近隣ノードから近隣ノードへ通知
  - リダイレクト　Redirect Message　（Type = 137）
    - 適切な経路の指示

NDP

- Neighbor Discovery Protocol [RFC4861]
  - 近隣探索
    - IPアドレスの重複検出
      - DAD : Duplicate Address Detection
    - リンクレイヤアドレスの解決
      - Ethernet であれば、MACアドレスの解決（IPv4 の ARP相当）
    - ルータ発見
    - ネクストホップ発見
    - プレフィックス発見
    - パラメータ発見
      - リンクMTU や Hop Limit など
    - 近隣ノードの到達不能検出
      - NUD : Neighbor Unreachability Detection
    - リダイレクト
      - 最適経路の通知

アドレス自動設定（1）

- SLAAC（Stateless Address Autoconfiguration）[RFC4862]
  - アドレスを管理するサーバはない
    - RAにて取得するPrefix情報、ノード自身のMACアドレス等を使用して アドレスの自動生成を行なう。

- DHCPv6（Dynamic Host Configuration Protocol for Pv6）[RFC3315]
  - Stateful Address Autoconfiguration
  - IPv4 の DHCP と 基本的には同じ
    - Default Gateway が通知されないなどの違いがあることに注意

アドレス自動設定（2）

- IPv4 と IPv6 で異なる自動設定

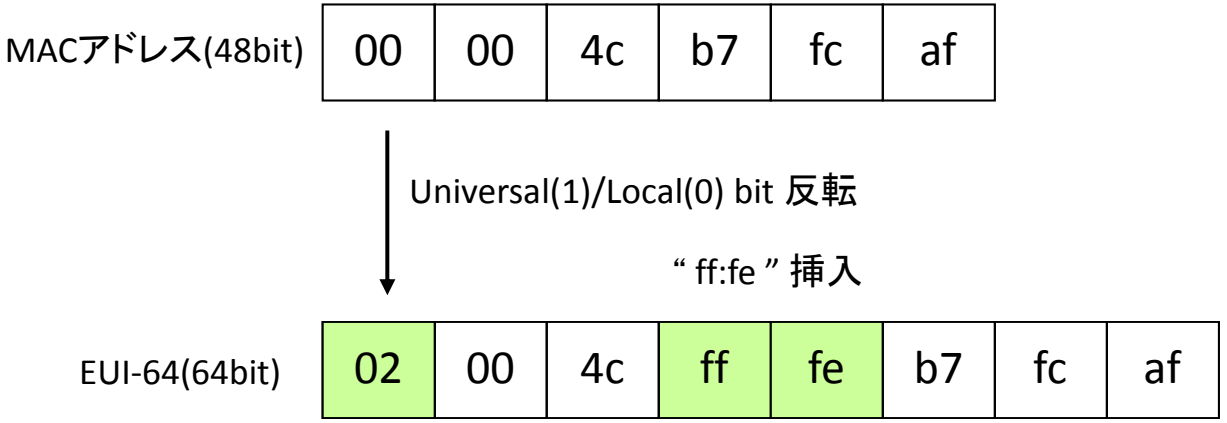
	IPv4	IPv6	
	DHCPv4	RA	DHCPv6
IP Address	○ /32を通知	○ Prefix情報を通知	○
Default Gateway	○	○	― ※1
Server Address (DNS , SIP , etc)	○	△ ※2	○

※1　標準化されていない

※2　RFC5006 で標準化されているが Experimental の位置づけ

SLAAC（1）

- EUI-64 Format
  - IEEE によって標準化された 64bit 長の ID
    - GUIDELINES FOR 64-BIT GLOBAL IDENTIFIER (EUI-64) REGISTRATION AUTHORITY
      http://standards.ieee.org/regauth/oui/tutorials/EUI64.html
- IPv6 の Interface-ID は、Modified EUI-64 を使用 [RFC4291]
  - 世界中で一意な識別子を生成可能



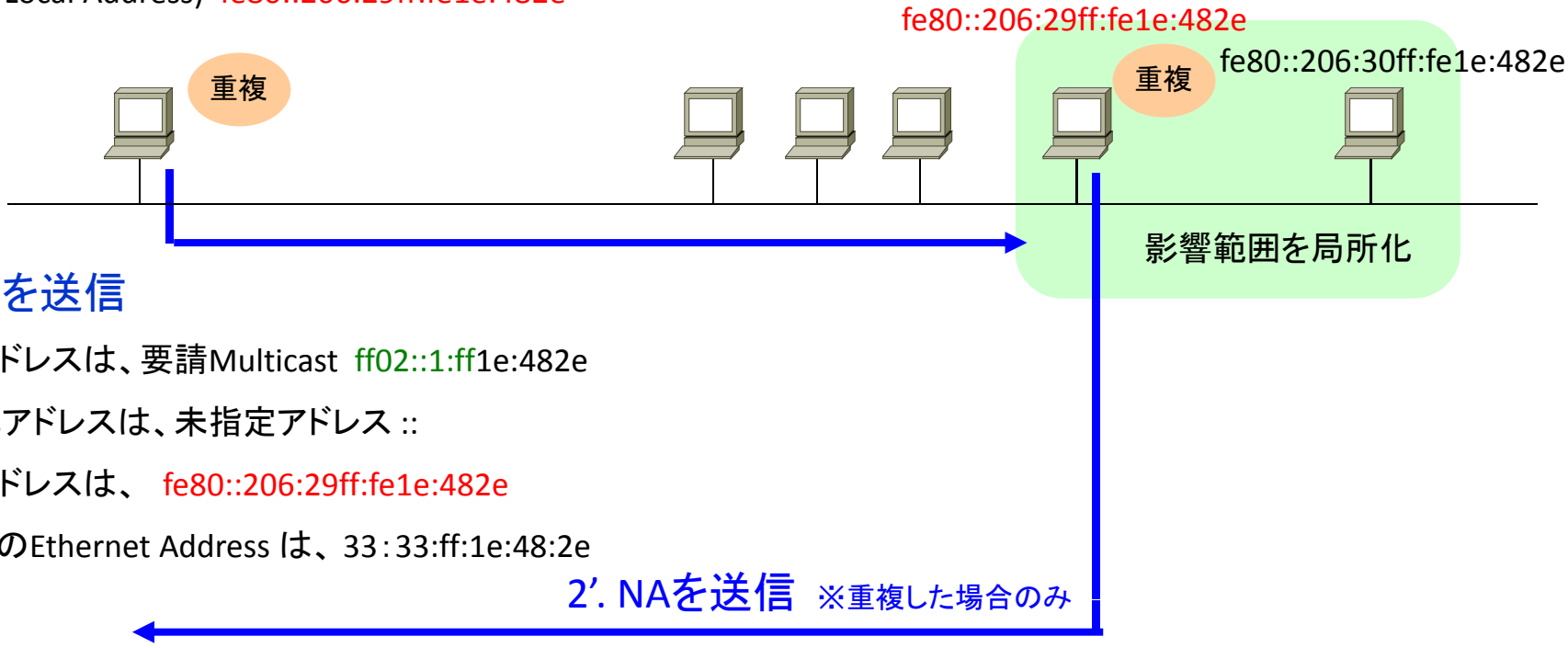
SLAAC（2）

- DAD（Duplicate Address Detection）
  - 実際にIPv6アドレスを使用する前に重複検知を行う
  - NS（Neighbor Solicitation）をリンク上に送信
    - 宛先アドレス　＝　要請ノードマルチキャスト（ff02::1:ff/104）
    - 送信元アドレス　＝　未指定アドレス（::）
      - 生成したアドレスはまだ重複していないことが確認されていないので、送信元アドレスに使うことができない
    - 対象アドレス　＝　生成した仮のアドレス
  - 重複していなければそのアドレスは使用可能となる
    - 対象アドレスが重複していた場合、アドレスを保有しているノードはNA（Neighbor Advertisement）により重複を知らせる
      - 重複していた場合、一般的には手動による再設定が必要となる

SLAAC（3）

1. EUI-64にて、Link Local Address(仮)を生成

(MAC Address)　0006.291e.482e
(Link-Local Address)　fe80::206:29ff:fe1e:482e



2. NS を送信

宛先アドレスは、要請Multicast　ff02::1:ff1e:482e

送信元アドレスは、未指定アドレス ::

対象アドレスは、　fe80::206:29ff:fe1e:482e

この時のEthernet Address は、33：33:ff:1e:48:2e

2’. NAを送信　※重複した場合のみ

SLAAC（4）

(MAC Address) 0006.291e.482e

(Link-Local Address) fe80::206:29ff:fe1e:482e

(Global Address) 2001:db8::206:29ff:fe1e:482e

(Link-Local Address) fe80::200:4cff:feb7:fcaf

(Global Address) 2001:db8::200:4cff:feb7:fcaf

3. RS を送信

fe80::206:29ff:fe1e:482e	ff02::2
Source Address	Destination Address

4. RA を送信

fe80::206:29ff:fe1e:482e	fe80::200:4cff:feb7:fcaf	2001:db8::/64
Destination Address	Source Address	prefix

Privacy Extensions for SLAAC（1）

- SLAAC（Stateless Address Autoconfiguration）の
  プライバシー拡張 [RFC4941]
  - EUI-64 で生成したインタフェースID では MACアドレスを
    簡単に知ることができてしまう問題の解決策
  - Temporary Address や Anonymous Address と呼ばれる
- ランダムな初期値を MD5 でハッシュして、インタフェースID
  を生成し、一定時間内で使い捨てる方式
  - 一定時間でアドレスが変わるため、サーバでの利用には適さない
- IPv6 Node Requirements [RFC4294] では、
  “SHOULD” の扱いとなっている
  - Windows XP/Vista/7 では、デフォルトで有効化されている
  - Windows Vista/7 では上記以外に独自のアドレスが生成される

Privacy Extensions for SLAAC（2）

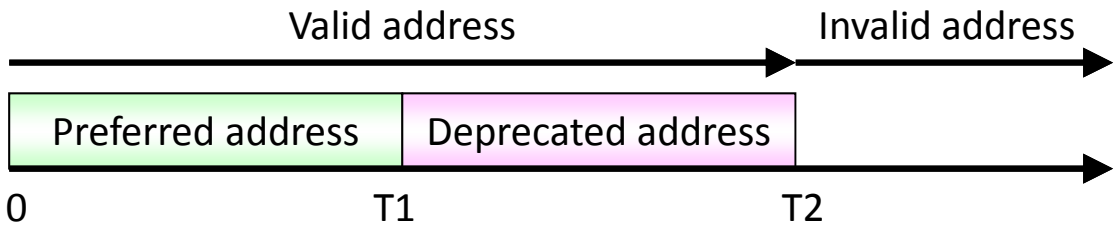
- Privacy Extensions for SLAAC [RFC4941]
  - 推奨有効期限　：　24 時間
  - 最大有効期限　：　7 日間（期限延長不可）

- EUI-64 で生成したアドレス
  - 推奨有効期限　：　7 日間
  - 最大有効期限　：　30 日間（期限延長可）

- Windows Vista/7 が生成する独自のアドレス
  - 推奨有効期限　：　7 日間
  - 最大有効期限　：　30 日間（期限延長可）
  - 再起動後でもアドレスは変わらない

IPv6アドレスの State と Lifetime

- Tentative address
  - インタフェースに付与されていない仮（DAD前）のアドレス。
- Preferred address
  - インタフェースに付与され、アドレスが一意で通信可能なアドレス。
- Deprecated address
  - 有効なアドレスだが、新規通信への使用が推奨されないアドレス。
- Valid address
  - 有効なアドレス。Preferred address と Deprecated address を示す。
- Invalid address
  - Valid Lifetime が超過した無効なアドレス。



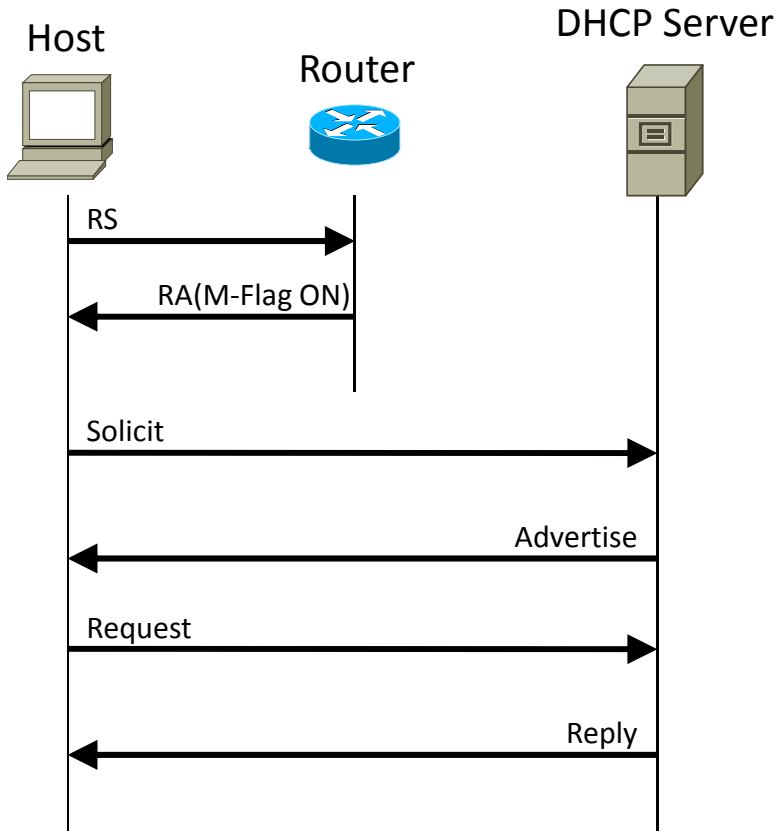
T1 : Preferred Lifetime（推奨有効期限）
T2 : Valid Lifetime（最大有効期限）

DHCPv6

DHCPv6

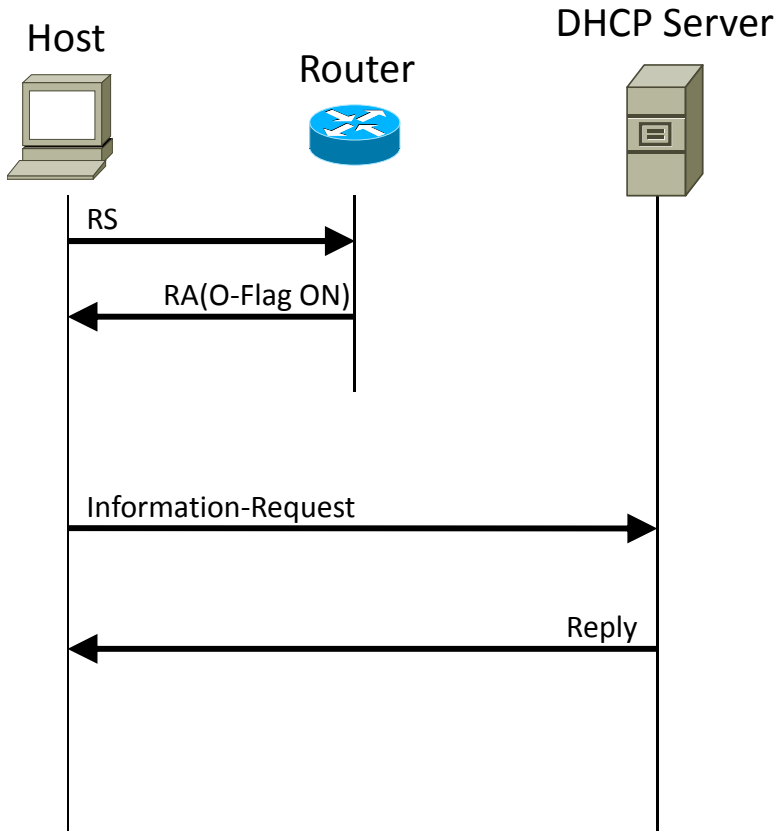
- Stateful DHCPv6
  - DHCP for IPv6 [RFC3315]
  - DHCPv4 と基本的に同じ
    - Default Gateway 情報は通知されないので RA にて取得
- Stateless DHCPv6
  - Stateless DHCP Service for IPv6 [RFC3736]
  - DNSサーバ情報などのIPv6アドレス以外の情報を通知
    - DHCPv6サーバはノードの状態を管理しない
- DHCPv6-PD
  - IPv6 Prefix Options for DHCPv6 [RFC3633]
  - 主に HGW の LAN側で使用する Prefix を通知する目的で使用
    - Prefix を取得した HGW は、RA または DHCPv6 を使用して再配布

Stateful DHCPv6



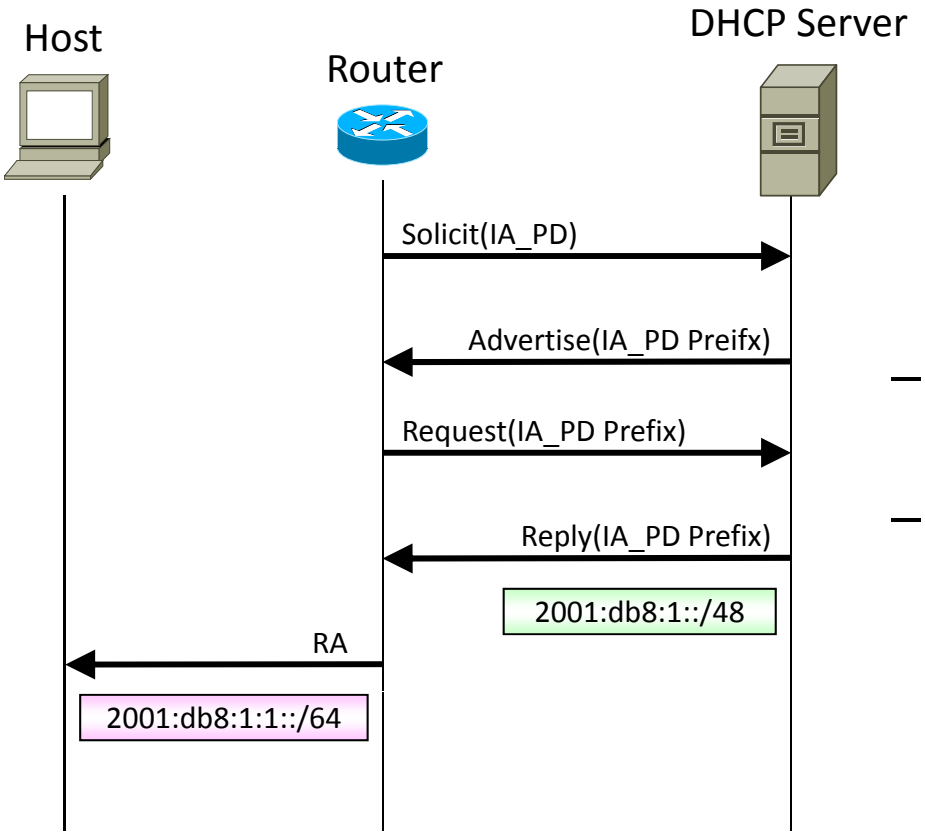
- DHCP Server にてIPアドレス等の Host情報管理が可能
- Host は、RA の M-Flag 受信により、DHCPv6 Client が動作
- Rapid Commit Option が有効な場合、Advertise、Request は省略される

Stateless DHCPv6



- DHCP Server はHost情報を管理しない（IPアドレス情報、リース管理など）
- Host は、RA の O-Flag 受信により、DHCPv6 Client が動作
- DNSサーバ、SIPサーバ、NTPサーバ等の設定情報を通知

DHCPv6-PD



- 単一のアドレスではなく、Prefix を付与
- Prefix を取得した HGW等のRouter (DHCPv6-PD Client) は、RA や DHCP を使用して再配布

  例. /48を取得、先頭の/64をRAで通知

ルーティングプロトコル

Default Router

- RA の Router Lifetime を 0 以外の値で通知すれば ホストの Default Router List に追加される
- 複数の RA を受信したホストは通知された内容から 最適な Router を選択することが可能
  - Default Router Preferences and More-Specific Routes [RFC4191]
    - Default Router Preference は、 High / Medium(Default) / Low を通知可能である
    - Route Information Option により、より詳細な経路を 通知可能である

RIPng

- RIPng（next generation）[RFC2080]
- RIPv2 との比較
  - 送信元アドレスは、リンクローカルアドレス（特定要求などは除く）
  - UDP 521番ポートを使用
    - RIPv1/RIPv2 では、UDP 520番ポートを使用
  - 認証用のパケットフォーマットを廃止
    - IPv6 では、AH やESP で代替え可能
  - Next Hop Field の廃止
    - 専用のRTE（Routing Table Entry）を使用
      - Metric Field = 0xff が Next Hop を示す
      - Next Hop RTE の後に続く RTE が対象となる
      - Next Hop RTE が無い場合、送信元アドレスが Next Hop となる

OSPFv3

- OSPF version 3 [RFC5340]
- OSPFv2 との比較
  - 送信元アドレスは、リンクローカルアドレス（Virtual Link は除く）
  - 認証用のパケットフォーマットを廃止
    - IPv6 では、AH やESP で代替え可能
  - 同一リンク上に複数のルーティングドメインを設定可能
    - 各インタフェースに Instance ID を付与する
  - Router ID、Area ID は、32bit のまま
    - IPアドレスと紐付けて設計する手法はやりにくくなった
    - DR（Designated Router）、BDR（Backup Designated Router）の選出時に IP Address から Router ID を得ることができないので明示的に指定する必要がある

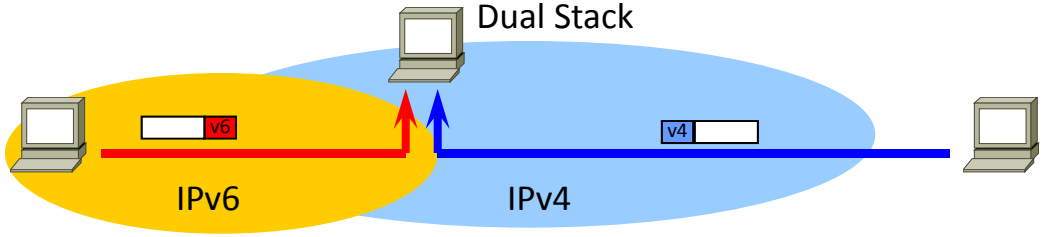
BGP4+

- Multiprotocol Extensions for BGP-4 [RFC4760]
  - Open Message の Option Parameter にて、Multiprotocol 拡張（BGP Capability）を通知
    - AFI（Address Family Identifier）に 0x0002 を指定することで IPv6 をサポート
      - http://www.iana.org/assignments/address-family-numbers/
  - IPv6 経路情報は、Path Attribute を使用して通知
    - MP_REACH_NLRI
      - 有効経路の通知
    - MP_UNREACH_NLRI
      - 無効経路の通知
  - BGP セッション自体は、IPv4 / IPv6 のどちらで確立してもよい
    - 到達性を保証するには、IPv6 で確立するのが望ましい

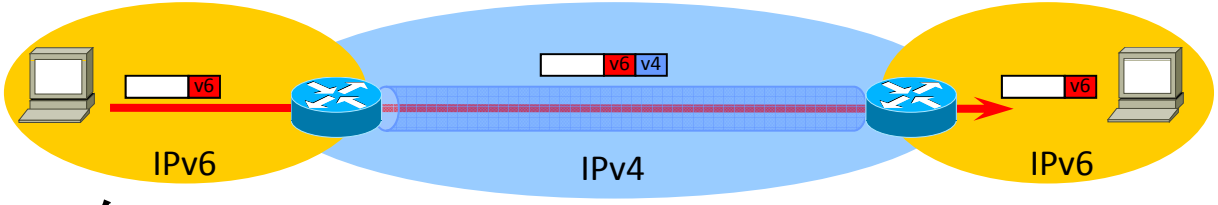
移行技術

移行技術

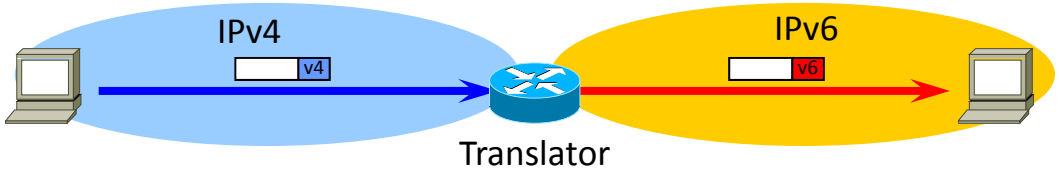
- デュアルスタック
  - IPv6 ノード、IPv4 ノードの両方と通信可能



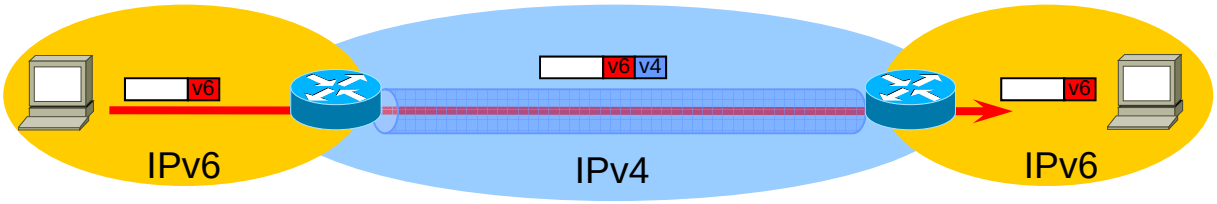
- トンネリング
  - IPv6 ノードまたはサイト間でIPv4 ネットワークを経由して通信

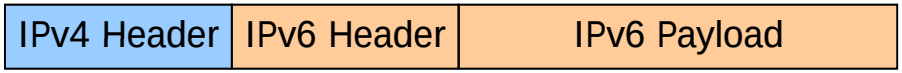


- トランスレータ
  - IPv4 ノードと IPv6 ノード間の通信におけるプロトコル変換



Configured Tunnel

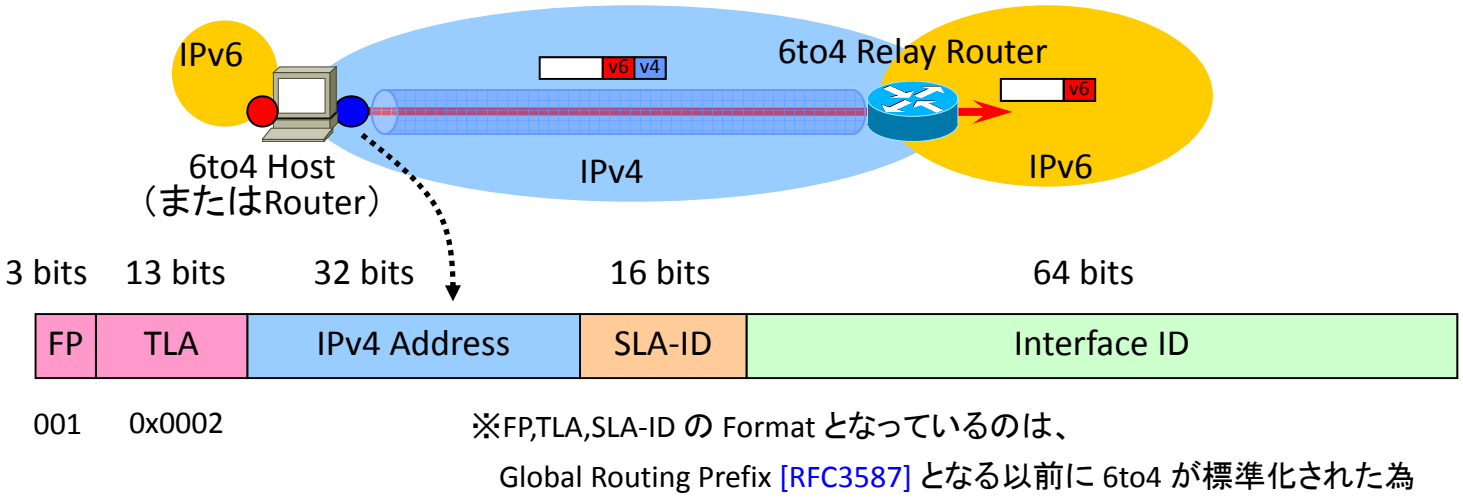




Protocol = 41

- IPv6 パケットを IPv4 ヘッダでカプセル化
  - IPv4 ヘッダの Protocol Field は、41（IPv6）となる
    - 6to4 や ISATAP も同じ
- トンネルの両端の IPv4アドレスを手動で設定する
- トンネル数が増加すると管理負担が大きくなる

6to4（1）



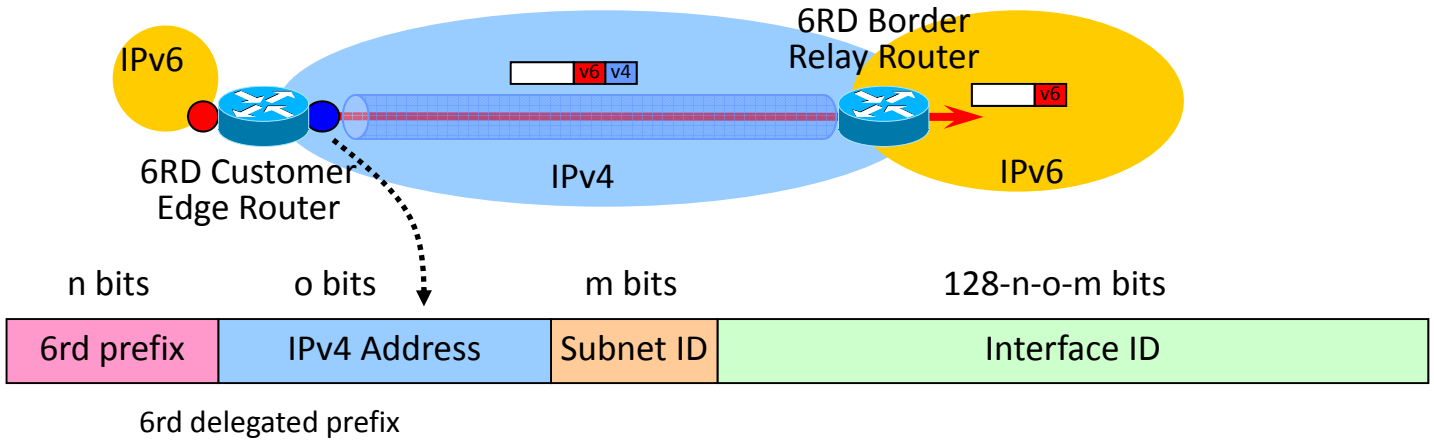
- Connection of IPv6 Domains via IPv4 Clouds [RFC3056]
- 6to4 の Prefix は、2002:[IPv4 Address]::/48
- IPv4 Anycast Address の利用
  - 6to4 ホスト（またはルータ）が 6to4 リレールータを手動設定しなくてよいように、192.88.99.1 が定義されている [RFC3068]
  - 国内の6to4リレールータ（http://www.tokyo6to4.net/）

6to4（2）

- 6to4 ホスト（またはルータ）
  - グローバル IPv4 アドレスを Prefix 内に埋め込み、IPv4 でカプセル化を行い、6to4 リレールータに転送する
  - グローバル IPv4 アドレスを有している必要がある
  - 6to4 ルータの場合、配下の IPv6 ホスト等には 6to4 は不要

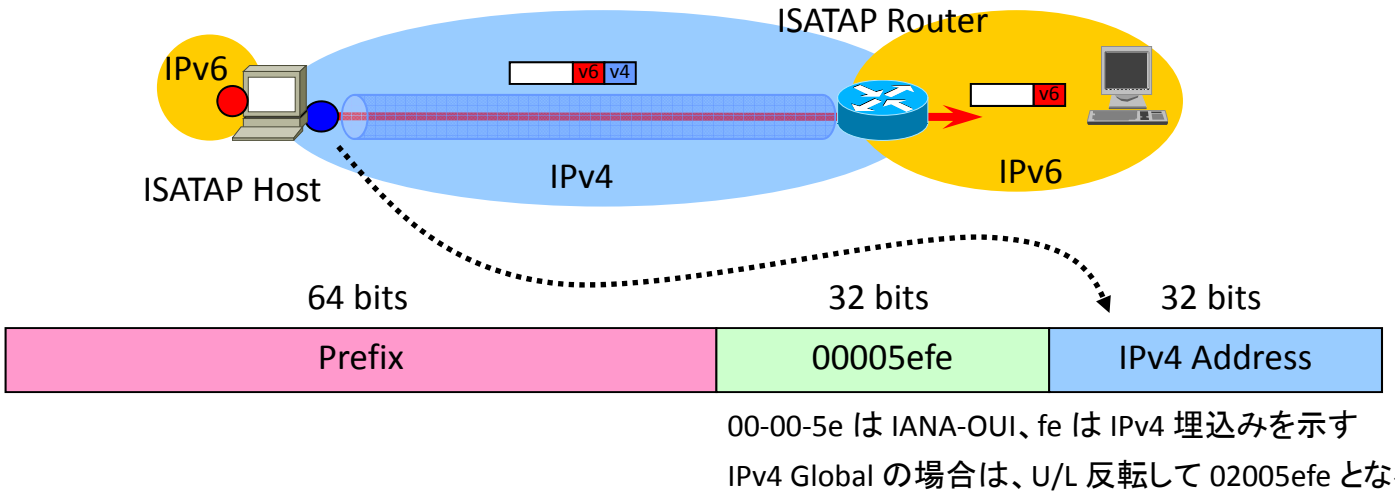
- 6to4 リレールータ
  - Native IPv6 ネットワークへの接続を提供する
  - 全ての 6to4 リレールータは、IPv6 ネットワークに対して、2002::/16 を広告する
    - IPv6 ネットワークからは Anycast Address となるので最も近い 6to4 リレールータに転送される
  - 6to4 ホスト（またはルータ）宛の グローバル IPv4 アドレスは、宛先となる IPv6 Prefix 内から知ることができる

6RD



- IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) [RFC5569]
- draft-ietf-softwire-ipv6-6rd-04 (work in progress)
  - より一般的な環境で使うための考慮
- 6to4 技術をベースにISP等でより使い易く改善
  - ISP の保有する IPv6 Prefix が使用可能、Private Address 考慮など
  - Free Telecom で実績あり
  - Comcast は 2010年に 6rd のトライアルを実施

ISATAP（1）



- Intra-Site Automatic Tunnel Addressing Protocol [RFC5214]
- ISATAP の Prefix には Global Unicast、6to4 などを付与可能であり、Prefixに関する制限はない
- ISATAP ルーターISATAP ホスト間は Link Layer のように扱われる
  - RS / RA により Prefix を取得

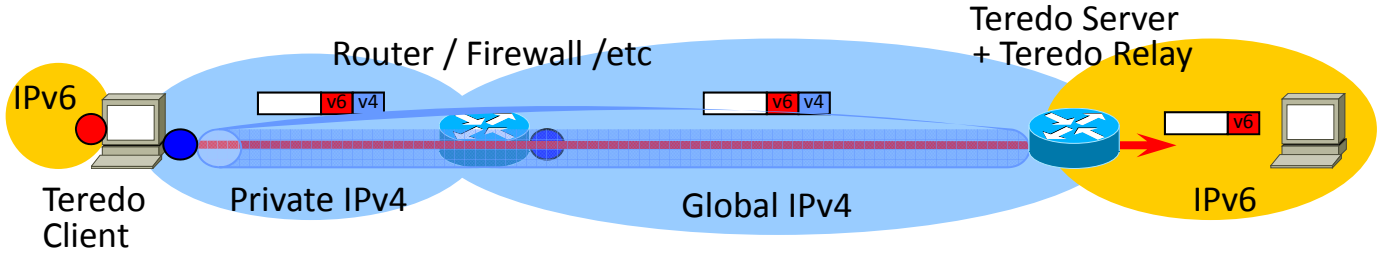
ISATAP（2）

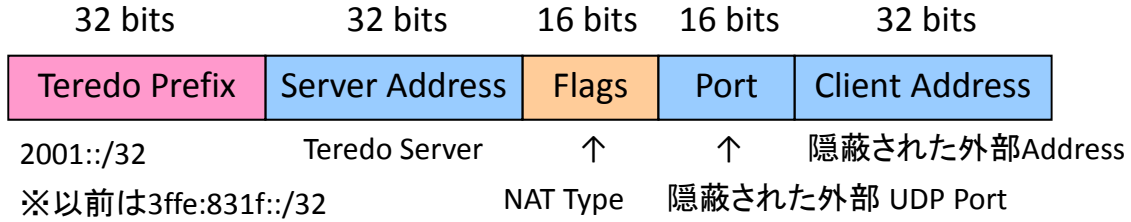
- 通信先が同一 Prefix の場合、ISATAP ルータを経由せずに直接の通信となる

- IPv4 Address は、Global / Private のどちらでもよい
  - イントラネット内に孤立した IPv6 ホストが IPv6 を利用可能

- ISATAP ルータの IPv4 アドレスは、
  手動、DHCP（vendor-specific option）、FQDN等で知ることができる
  - 例．isatap.example.com を引いて ISATAP ルータのIPv4 アドレスを得るなど

Teredo（1）





- Teredo: Tunneling IPv6 over UDP through NATs [RFC4380]
- Teredo クライアント
  - IPv6 パケットを UDP でカプセル化する（UDP Port 3544）
- Teredo サーバ
  - Teredo クライアントの NAT タイプ判定支援や、Teredo Prefix の通知を行う

Teredo（2）

- Teredo リレー
  - Teredo クライアントに Native IPv6 ネットワークへの接続を提供する
  - IPv6 ネットワークに対して 2001::/32 を広告する
- NAT 配下の IPv4 プライベートアドレスから利用可能
  - ブロードバンドルータやファイアウォール配下の IPv6 ホストが利用可能
- Windows Vista における接続性の改善
  - Windows XP で対応できなかった Symmetric NAT に対応
    - NAT タイプ判定の為に 複数の Teredo サーバを利用

トンネル接続サービス

提供会社	サービス名称	技術	付与Prefix
FreeBit	FB Feel6	DTCP	/48
HEXAGO	Freenet6	TSP	/48
Hurricane Electric	Free IPv6 Tunnel Broker	IP in IP	/64
NTT Communications	OCN IPv6	L2TP	/64
IIJ	IPv6仮想アクセス	PPTP	/64

- List of IPv6 tunnel brokers
  - http://en.wikipedia.org/wiki/List_of_IPv6_tunnel_brokers
- OCN、IIJ、KDDI等から法人向けトンネル接続サービスあり
  - IP in IP 方式

トランスレータ

- NAT-PT 方式
  - IP レイヤで IPv4/IPv6 アドレスおよびヘッダを変換
  - ペイロードに埋め込まれたアドレスの処理はできない
  - RFC2766 で標準化されたが、RFC4966 で Historic Status になっている
  - IETF behave WG にて、フレームワークや各機能毎の再検討が行われている
- Transport Relay 方式
  - An IPv6-to-IPv4 Transport Relay Translator [RFC3142]
  - Transport Layer で TCP/UDP を終端し、新たな session を生成
- Proxy 方式（ALG : Application Level Gateway）
  - HTTP や FTP などのアプリケーション単位で変換を行う
  - 標準的なアプリケーション以外の使用は困難

DNS

DNSのIPv6対応

- RR（Resource Record）のIPv6対応
  - DNS Extensions to Support IP Version 6 [RFC3596]
    - 正引きは、AAAA（クアッドA）を使用する
    - 逆引きドメインは、ip6.arpa を使用する
      - 2001:db8::1 の PTR RR は、
        1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa.

- トランスポートのIPv6対応
  - DNSパケットの転送プロトコルとしてIPv6を使用

DNSリゾルバの挙動（1）

- DNSクエリ順序
  - AAAA クエリが先
    - Windows XP、Linux
  - A クエリが先
    - Windows Vista、Windows 7、FreeBSD、Mac OS X
      - A の応答時間からAAAAのタイムアウト時間を決定する。[Windows Vista、Windows 7、FreeBSDなど]
      - NXDOMAIN（RCODE=3）が返ったら、AAAAクエリは行わない。[Windows Vista、Windows 7]
      - IPv6グローバルアドレス（Teredoを除く）が付与されている場合のみAAAAクエリを行う。[Windows Vista、Windows 7]

DNSリゾルバの挙動（2）

- トランスポートの優先順序
  - IPv6 を優先
    - Windows Vista、Windows7
  - 設定（/etc/resolv.conf）に依存
    - FreeBSD、Linux
  - IPv4 のみに対応
    - Windows XP

アドレス選択とマルチプレフィックス問題

Default Address Selection

- IPv6 ではインタフェースに複数のアドレスが付与できる
  - 複数の送信元アドレスの中からどのアドレスを通信に使用するか選択するための基準が必要
  - 複数の宛先アドレスの中からどのアドレス宛に送信するか選択するための基準が必要
    - DNS から 複数の宛先アドレスを得た場合など
- Default Address Selection for IPv6 [RFC3484]
  - ホストにおけるデフォルトのアドレス選択ルールを定義
    - 宛先アドレス選択アルゴリズムでは、デュアルスタック環境における IPv4 / IPv6 選択についても考慮
  - IPv6 Node Requirements [RFC4294] では、“MUST” の扱い
  - 実装状況
    - Windows XP、Windows Vista、Windows 7
    - BSD系UNIX、Linux

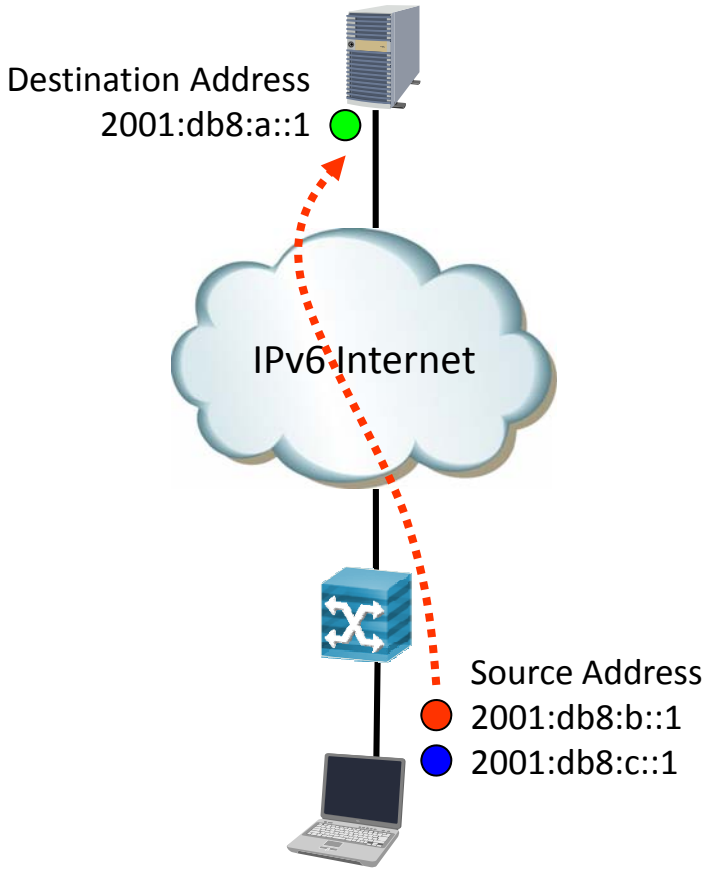
宛先アドレス選択ルール

- Rule 1： 到達不能など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が優先
- Rule 3： Deprecated Address（非推奨アドレス）を避ける
- Rule 4： Home Address が優先（モバイルIP）
- Rule 5： Policy Table において送信元アドレスと Label が同じアドレスが優先
- Rule 6： Policy Table において Precedence が高いアドレス優先
- Rule 7： Native Transport が優先
- Rule 8： より小さいスコープが優先
- Rule 9： 送信元アドレスに対して、Longest Match Prefix が優先
- Rule 10： リストの順序を入れ替えず先にあるアドレスが優先

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が優先
- 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： Deprecated Address（非推奨アドレス）を避ける
- Rule 4： Home Address が優先（モバイルIP）
- Rule 5： 送信先インタフェースに付与されたアドレスが優先
- Rule 6： Policy Table において宛先アドレスと Label が同じアドレスが優先
- Rule 7： Temporary Address よりも Public Address が優先
- Rule 8： 宛先アドレスに対して、Longest Match Prefix が優先

Longest Match Prefix（Rule8）における送信元アドレス選択例



Destination Address
- 2001:db8:a(hex) → 1010(bin)

Source Address
- 2001:db8:b(hex) → 1011(bin)
- 2001:db8:c(hex) → 1100(bin)

→ Source Address として
- 2001:db8:2000:b::1 を選択

Default Policy Table（1）

Prefix	Precedence	Label	
::1/128	50	0	loopback 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）

- 宛先アドレス
  - 送信元アドレスとラベルが同じアドレスが優先（Rule 5）
  - Precedence の高いアドレスが優先（Rule 6）
- 送信元アドレス
  - 宛先アドレスとラベルが同じアドレスが優先（Rule 6）

Default Policy Table（2）

- Windows XP SP3 の Policy Table

```
Precedence  Label  Prefix
----------  -----  --------------
         5      5  2001::/32
        10      4  ::ffff:0:0/96
        20      3  ::/96
        30      2  2002::/16
        40      1  ::/0
        50      0  ::1/128
```

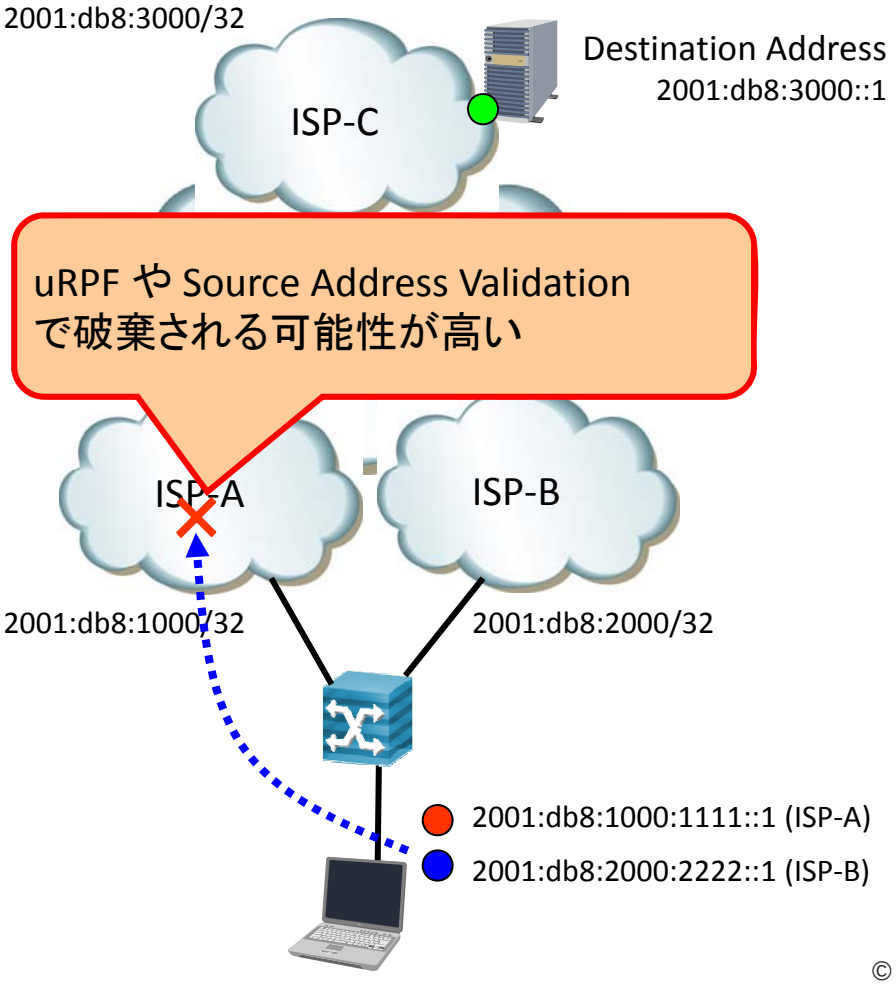
← Teredo Address [RFC4380]

- Windows Vista SP2、Windows 7 の Policy Table

```
優先順位    ラベル  プレフィックス
----------  -----  ----------------
        50      0  ::1/128
        40      1  ::/0
        30      2  2002::/16
        20      3  ::/96
        10      4  ::ffff:0:0/96
         5      5  2001::/32
```

← Teredo Address [RFC4380]

送信元アドレスの制御例
（不適切なアドレス選択の是正）（1）



Destination Address
- 2001:db8:3(hex) → 0011(bin)

Source Address
- 2001:db8:1(hex) → 0001(bin)
- 2001:db8:2(hex) → 0010(bin)

→ Longest Match Prefix により、
Source Address として
- 2001:db8:2000:2222::1 を選択

送信元アドレスの制御例
（不適切なアドレス選択の是正）（2）

Prefix	Precedence	Label		
::1/128	50	0		loopback 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）
2001:db8:1000::/32	45	10	●	ISP-A Address
2001:db8:3000::/32	45	10	●	ISP-C Address

- 通信させたい送信元／宛先 Prefix を同じLabel にすることで適切なアドレス選択を実現

マルチプレフィックス問題の解決策
（技術的観点からみた根本解決）

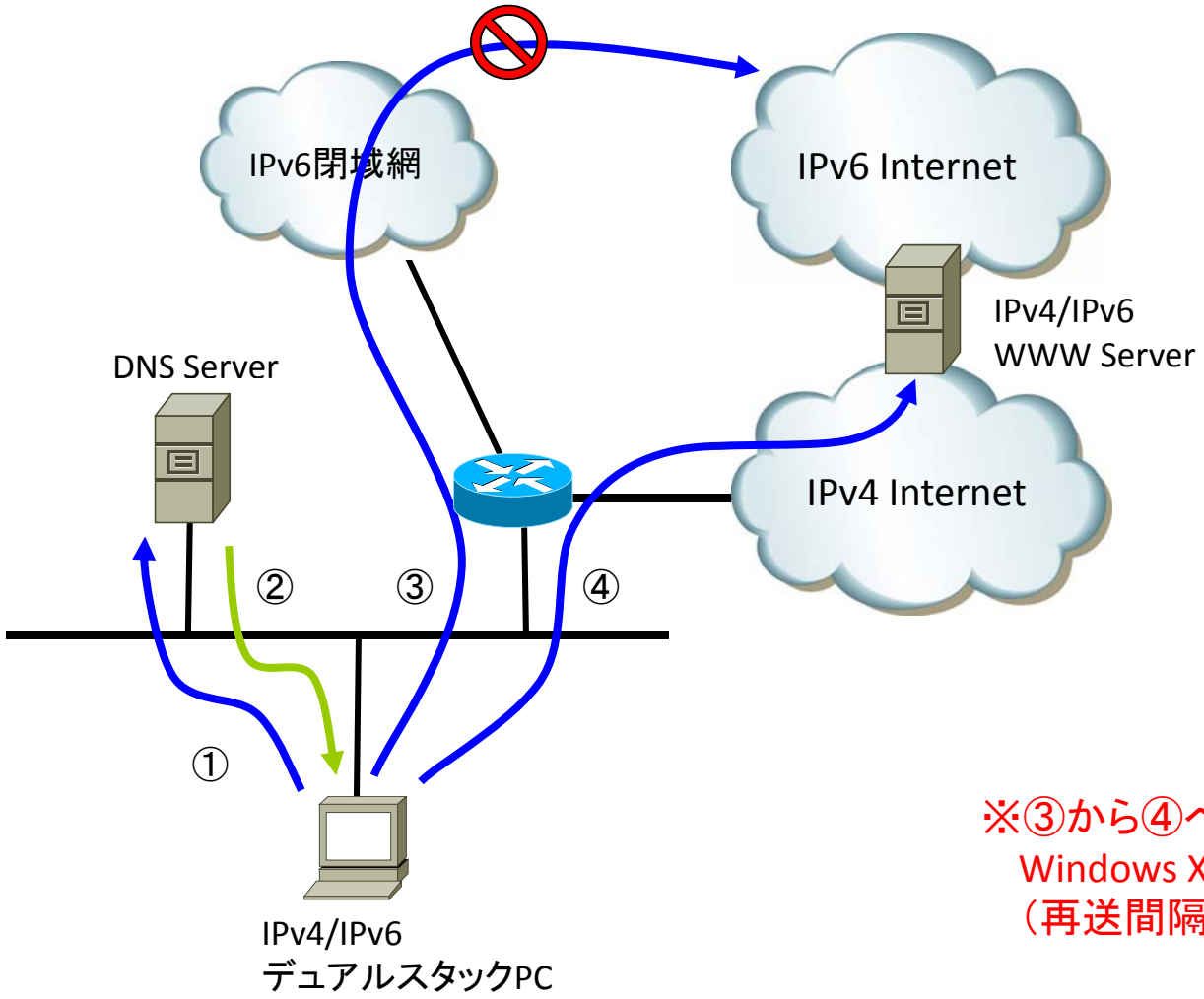
- 宛先経路選択の問題
  - Default Router Preferences and More-Specific Routes [RFC4191] の使用
- Default Address Selection for IPv6 [RFC3484] の再検討
  - Host や Router に適切なアドレス選択機構が必要
    - RFC3484 における問題点と追加要件の整理
      - » Problem Statement for Default Address Selection in Multi-Prefix Environments: Operational Issues of RFC 3484 Default Rules [RFC5220]
      - » Requirements for Address Selection Mechanisms [RFC5221]
    - RFC3484 における問題点の解決について議論中
      - » Solution approaches for address-selection problems [draft-ietf-6man-addr-select-sol-02] (work in progress)
      - » Considerations for IPv6 Address Selection Policy Changes [draft-ietf-6man-addr-select-considerations-00] (work in progress)

TCPフォールバック問題

TCPフォールバック問題（1）

- IPv6 Internet への到達性がない IPv6閉域網の環境から IPv6対応サーバへのアクセスに時間がかかってしまう問題
  - フレッツドットネット等のIPv6閉域網、企業内での ULA 使用など
  - IPv6閉域網に接続されている IPv6端末から Internet上に存在する IPv6 対応WWWサーバ等にアクセスした場合に発生
    - www.kame.net
    - www.kokatsu.jp
    - www.v6pc.jp
    - www.ocnipv6.jp
    - www.iij.ad.jp
    - etc

TCPフォールバック問題（2）



①WWWサーバのDNS解決

②A RRとAAAA RRが返信される

③IPv6によるTCP接続
※IPv6 Internetへの到達性はない

④IPv4によるTCP接続にフォールバック

※③から④へのフォールバック時間は、
Windows XP / Vista の場合、約21秒かかる
（再送間隔 3秒＋6秒＋12秒＝21秒）

TCPフォールバック問題解決策（1）

- ICMPv6 Type1（Destination Unreachable）
  Code 0（no route to destination）もしくは
  Code 3（address unreachable）を返す
  - OS標準の Firewall機能によって破棄されてしまう場合あり
  - 破棄されなかった場合でも ICMPエラーハンドリング上、
    soft error として扱われ、セッションは中止されない
    - Requirements for Internet Hosts -- Communication Layers [RFC1122]
      にて定義されている（IPv4前提）
    - 迅速にフォールバックする為の仕様
      TCP‘s Reaction to Soft Errors [RFC5461]

TCPフォールバック問題解決策（2）

- IPv4通信を優先する
  - Default Address Selection for IPv6 [RFC3484] の Policy Table を使用する
    - IPv4（::ffff:0:0/96）の Precedence を高くする
    - エンドユーザに設定させるのは困難
- IPv6 Default Route を通知しない
  - Default Router Preferences and More-Specific Routes [RFC4191] を使用する
    - RA では閉域網内の経路のみアナウンスし、Default Route をアナウンスしない
    - Windows Vista、Windows 7 では More-Specific Routes に対応しているが、Windows XP は未対応
    - Router における実装も多くない

TCPフォールバック問題解決策（3）

- その他のアプローチ
  - 閉域網内で TCP RST を応答する
  - 専用ツールのインストール

セキュリティ

セキュリティ

- NDPは脆弱である（ただし、IPv4と同質）
  - 不正RAやDADを悪用した攻撃への対策
    - SEND（SEcure Neighbor Discover）[RFC3971] は普及していない
    - IPv6 RA-Guard [draft-ietf-v6ops-ra-guard-04] (work in progress)
      - L2SW 等の L2 Device にて 不正 RA を破棄
- Router、FireWall でのフィルタリング
  - 基本的な考え方はIPv4 と同じで必要な通信だけを許可
    - 但し、ICMPv6 は破棄しないこと
      - Path MTU Discovery が機能しなくなる
    - EDNS0 や TCP Port 53 も破棄しないこと
      - IPv6 や DNSSEC の普及でDNS応答は大きくなる
    - RH0（Type 0 Routing Header）は破棄すること
      - Deprecation of Type 0 Routing Headers in IPv6 [RFC5096]

その他

Special-Use IPv6 Addresses

- Special-Use IPv6 Addresses [RFC5156]
  - Special-Use IPv4 Addresses [RFC5735] の IPv6版
    - Node-scoped Unicast (::1/128 , ::/128)
    - IPv4-Mapped Addresses (::FFFF:ipv4-address/96)
    - IPv4-compatible Addresses (::ipv4-address/96)
    - Link-scoped Unicast (fe80::/10)
    - Unique-Local (fc00::/7)
    - Documentation Prefix (2001:db8::/32)
    - 6to4 (2002::/16)
    - Teredo (2001::/32)
    - 6bone (5f00::/8 , 3ffe::/16)
    - etc

Documentation Prefix

- IPv6 Address Prefix Reserved for Documentation [RFC3849]
- 文書作成用途の IPv6 Prefix
- マニュアルやコンフィグサンプル等での使用を想定
- Prefix は、2001:db8::/32
- 申請手続きなどは不要
- 実際の通信に使用してはならない