長崎県立大学
UNIVERSITY OF NAGASAKI

IPv6基礎解説

IPv6対応セミナー（山梨）

2023年2月9日

長崎県立大学
UNIVERSITY OF NAGASAKI

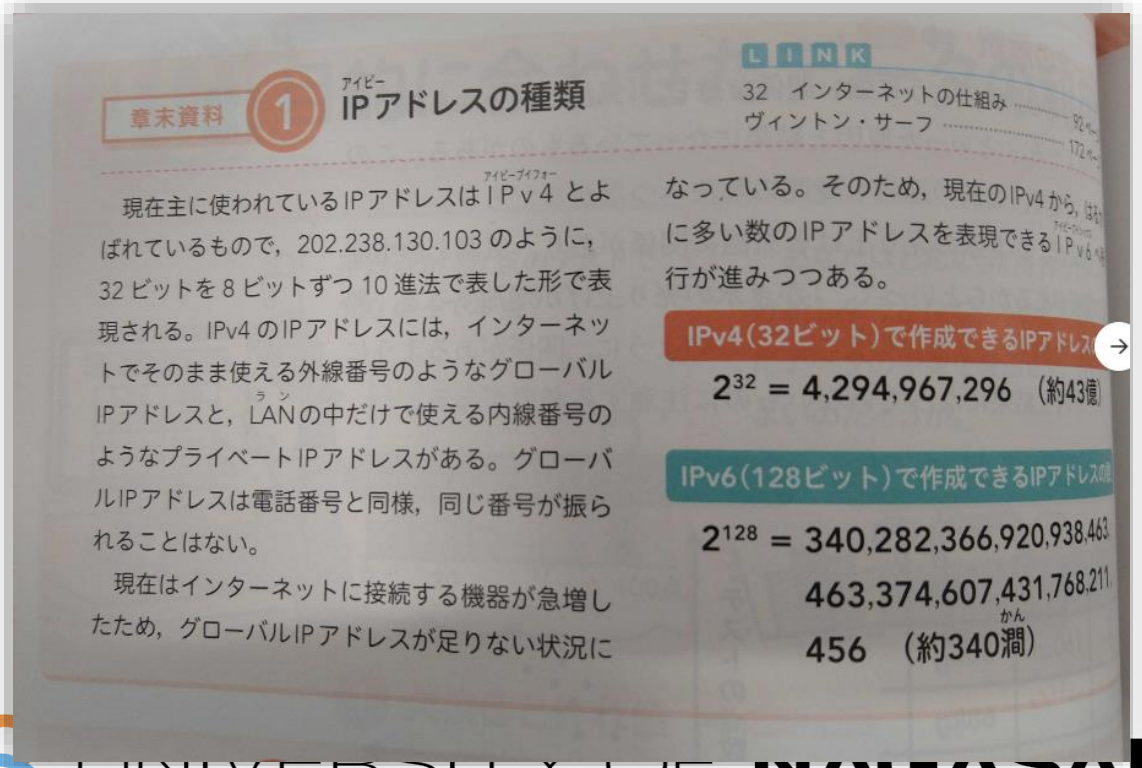
はじめに

このセミナーは、JPNICもメンバーとして協力する、
旧IPv4アドレス枯渇対応タスクフォース
https://kokatsu.jp/blog/ipv4/
(現：IPv6社会実装推進タスクフォース)で作成した教材を、
執筆者の同意を得て利用して実施するものです。

目次

IPv6と高校 情報Ⅰ

- **令和７年大学入学共通テスト 情報Iが導入**
  - ◆令和4年より高校 必修化
- **一部の教科書にもIPv6の記載が存在**



章末資料 1 IPアドレスの種類

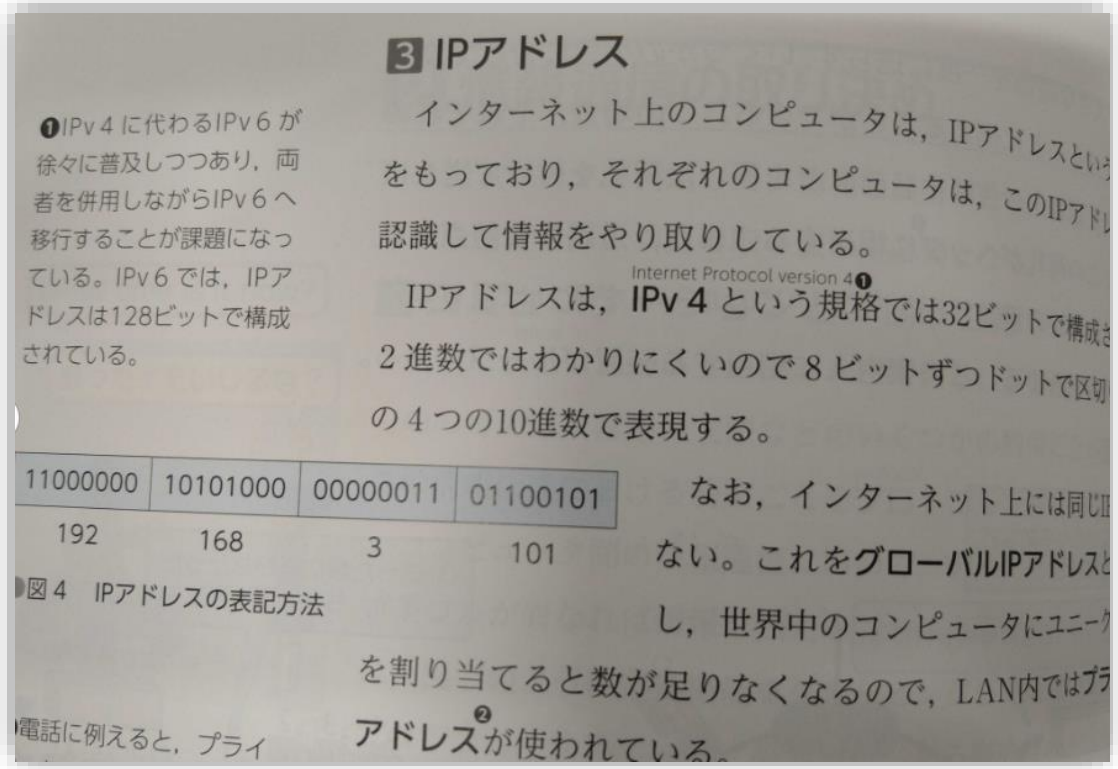
現在主に使われているIPアドレスはIPv4とよばれているもので，202.238.130.103のように，32ビットを8ビットずつ10進法で表した形で表現される。IPv4のIPアドレスには，インターネットでそのまま使える外線番号のようなグローバルIPアドレスと，LANの中だけで使える内線番号のようなプライベートIPアドレスがある。グローバルIPアドレスは電話番号と同様，同じ番号が振られることはない。

現在はインターネットに接続する機器が急増したため，グローバルIPアドレスが足りない状況になっている。そのため，現在のIPv4から，はるかに多い数のIPアドレスを表現できるIPv6への移行が進みつつある。

LINK
32 インターネットの仕組み
ヴィントン・サーフ

IPv4(32ビット)で作成できるIPアドレス
2^{32} = 4,294,967,296 (約43億)

IPv6(128ビット)で作成できるIPアドレス
2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456 (約340澗)



3 IPアドレス

❶IPv4に代わるIPv6が徐々に普及しつつあり，両者を併用しながらIPv6へ移行することが課題になっている。IPv6では，IPアドレスは128ビットで構成されている。

インターネット上のコンピュータは，IPアドレスというをもっており，それぞれのコンピュータは，このIPアドレス認識して情報をやり取りしている。

IPアドレスは，IPv4という規格では32ビットで構成され2進数ではわかりにくいので8ビットずつドットで区切りの4つの10進数で表現する。

11000000	10101000	00000011	01100101
192	168	3	101

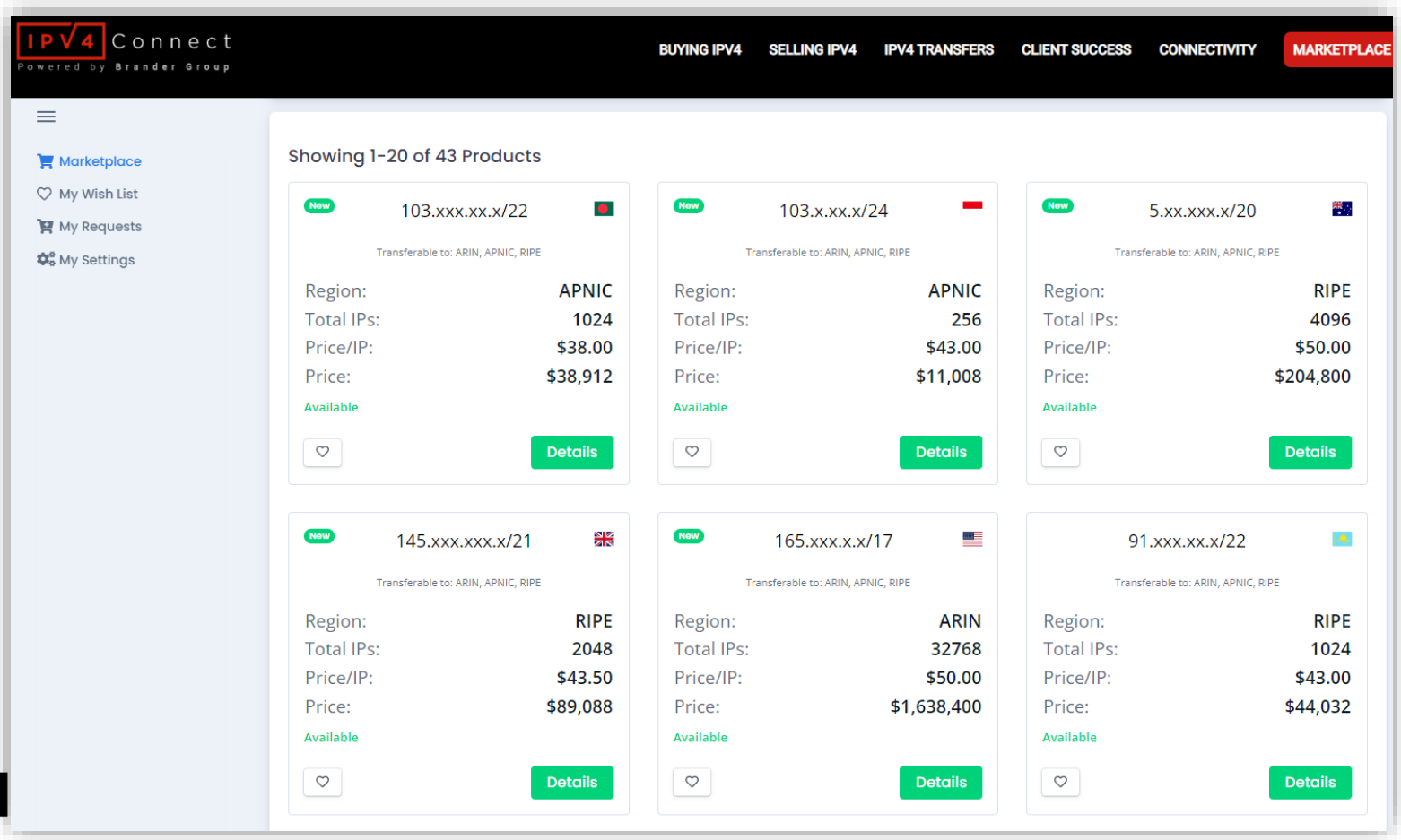
図4 IPアドレスの表記方法

なお，インターネット上には同じIPアドレスはない。これをグローバルIPアドレスと，世界中のコンピュータにユニークを割り当てると数が足りなくなるので，LAN内ではプライベートアドレス❷が使われている。

電話に例えると，プライ

最近のIPv4の確保の状況

- 国内での流動性はかなり厳しい
- APNICブローカーとの取引も日本の商習慣に合わない
  - ◆かつ、高額
- IPv4の補充は困難



長崎県立大学
UNIVERSITY OF NAGASAKI

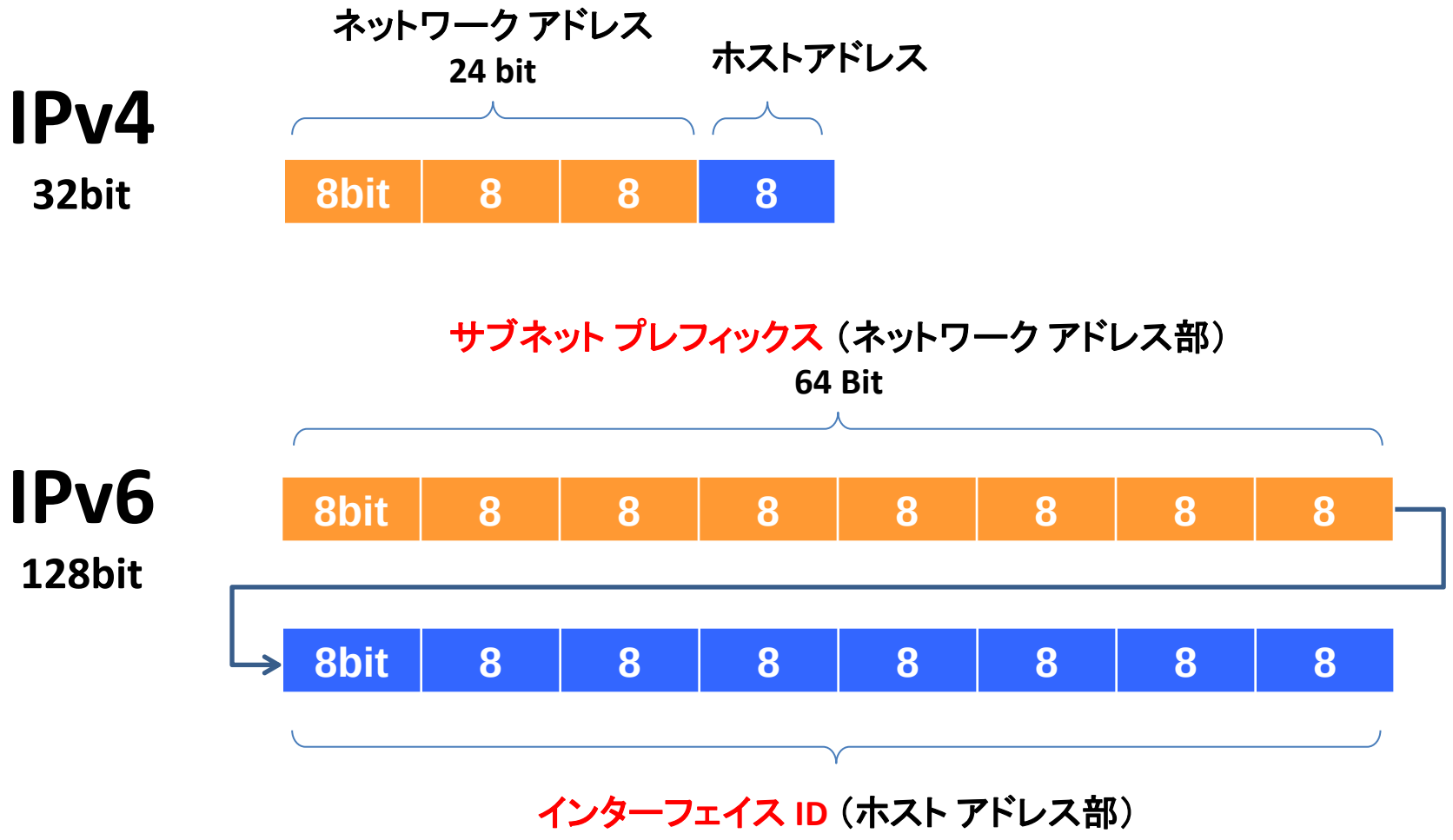
IPv6アドレスの主な特徴や機能

Agenda

1.IPv6の主な機能や特徴
2.ICMPとアドレス自動設定

長崎県立大学
UNIVERSITY OF NAGASAKI

IPv4　vs　IPv6 Address



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。

  0010000000000001000011011011100000000000000000000000000000000000000000000000000100000011000101001111111111111111000011110010010000010111 0

  ↓

  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、:: を用いて省略する。

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

  ↓

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

推奨表記[RFC5952]

- **前述の表記ルールでは表記が一意に定まらないので、RFC6952(A Recommendation for IPv6 Address Text Representation)にて、以下の省略記法を推奨**
  1. 16-Bit Field 内の先頭の“0”は省略すること。
     ※“0000”の場合は、“0”にします。
  2. “::”を使用して可能な限り省略すること。
  3. 16-Bit 0 Field（＝“0000”）が一つだけの場合、“::”を使用して省略してはならない。
  4. “::”を使用して省略可能なFieldが複数ある場合、最も多くの16-Bit 0 Fieldが省略できるFieldを省略すること。また、省略できるフィールド数が同じ場合は前方を省略すること。
  5. “a”～“f”は小文字を使用すること。

省略記法について、詳細は [RFC5952]
(A Recommendation for IPv6 Address Text Representation)を参照

https://www.nic.ad.jp/ja/newsletter/No46/0800.html

では以下の場合は？

- 2001:0db8:0000:0000:fff0:0000:0000:000f

○ 2001:db8::fff0:0:0:f

・ダメな例

× 2001:db8::fff0::f

△ 2001:db8:0:0:fff0::f

IPv6アドレスを取得する方法

1．IPアドレス指定事業者から分配を受ける

- 詳細は各IPアドレス管理指定事業者に確認
- 「IPアドレス管理指定事業者リスト」
  https://www.nic.ad.jp/ja/ip/member/cidr-block-list.txt

2．JPNICから直接分配を受ける（その1）

- マルチホーム接続を目的とし、下記要件をすべて満たす場合、
  JPNICから/48の割り当てを受けることができる

> **a） 現在割り当てられたアドレスでマルチホーム接続をしている。または、今後3ヶ月以内にマルチホーム接続をする予定がある。**
> **b) エンドサイトである(割り当てられたアドレスは自組織のみで使用し、割り当てを行わない)。**

- 詳細は「特殊用途用プロバイダ非依存アドレス割り当て申請」を参照
  https://www.nic.ad.jp/ja/ip/pi-application.html

IPv6アドレスを取得する方法

3. JPNICから直接分配を受ける（その2）

a. 既にIP指定事業者であり、IPv4の割り振りがある場合は、
割り当て予定などの確認なしに、/32の割り振りを行なう
https://www.nic.ad.jp/ja/ip/application-procedure/about-alloc-application.html

b. 要件を満たすことでIPアドレス管理指定事業者となって分配を受けることが出来る

> a）LIRであること
> b) エンドサイトでないこと
> c)割り当て先組織やエンドユーザに対し、2年以内に、IPv6の接続性を提供する計画があること

c. https://www.nic.ad.jp/ja/ip/member/

4. 通信事業者・ISP等から半固定・固定のIPv6アドレスの割り当てを受ける

IPv6の特徴と利用上の注意

IPv4とIPv6は互換性がない

・IPv4前提で作ったプログラムはIPv6の処理ができない
・開発言語のIPv6対応状況やバグに注意

IPv4　192.168.0.1
IPv6　2001:db8:fa0:4000::1

IPv4とIPv6ではアドレスの長さや表記方法が違う

・IPv4を前提としているとIPv6ではエラーになる

パケット形式やプロトコルが備える機能が違う

・セキュリティ対策などに注意

IPv4とIPv6がある時は処理順序に注意（アプリケーションに依存）

・IPv6を優先、だめだったらIPv4へ
・サーバ側ではパラレルスタックにして、独立して待受けする等もアリ

IPv6 アドレスと移転

- **IPv6アドレスの移転はできません。**
  - ◆どんな時に困るの？
- **例えば：会社分割**
  - ◆IPv6アドレスを分割したい
  - ◆できません。
- **分割会社の一方は新規で取得・リナンバーの必要性**
- **蛇足**
  - ◆IPv6移転ポリシーを成立させるのは短期的には困難

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	Group	1 : 1 ※1
Multicast ※2	Group	1 : n

Group: インターフェースの集合

※1 グループの中からネットワーク的に最も近い1つを選択

※2 IPv6ではブロードキャストは廃止され、マルチキャストが利用されている

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	Group	1 : 1 ※1
Multicast ※2	Group	1 : n

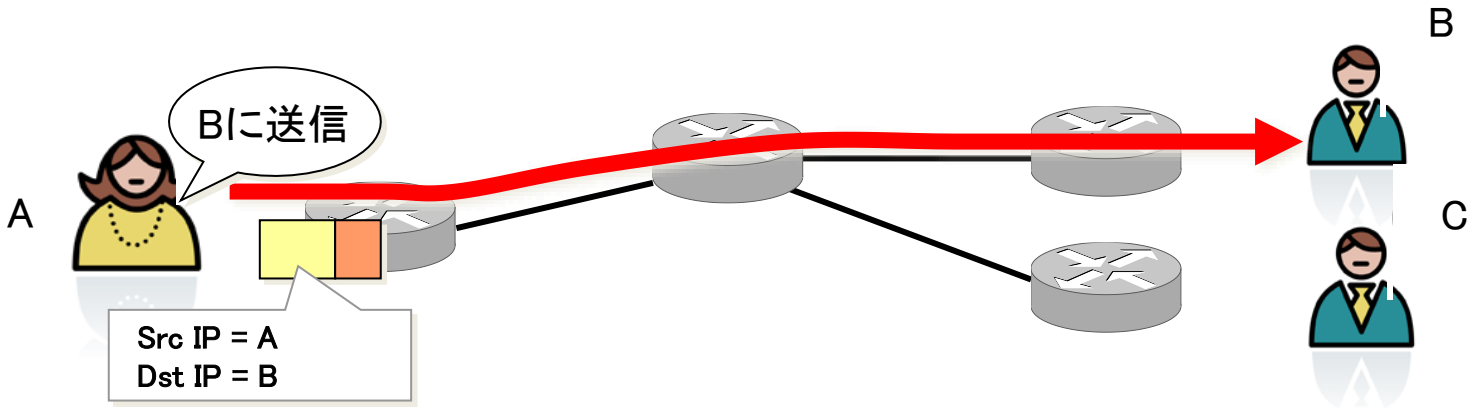
Group: インターフェースの集合

※1 グループの中からネットワーク的に最も近い1つを選択

※2 IPv6ではブロードキャストは廃止され、マルチキャストが利用されている

ユニキャスト通信

◆ユニキャスト　特定の相手への1対1の通信

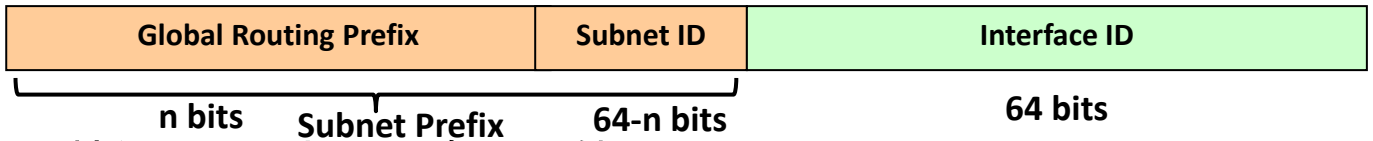


ユニキャストアドレス

- **リンクローカルアドレス fe80::/10**
  - 同一リンク内でのみ使われる
  - ルータを超えた通信はできない
- **ユニークローカルアドレス fc00::/7 （実質的に fd00::/8）**
  - IPv4におけるプライベートアドレスに相当
  - ルータを超えた通信は可能だが、インターネットに向けた通信はできない
- **グローバルユニキャストアドレス 上記以外**
  (現在は2000:: /3を利用）
  - IPv4におけるグローバルアドレスに相当
- **その他、特定用途のアドレス**

ユニキャストアドレス (1)

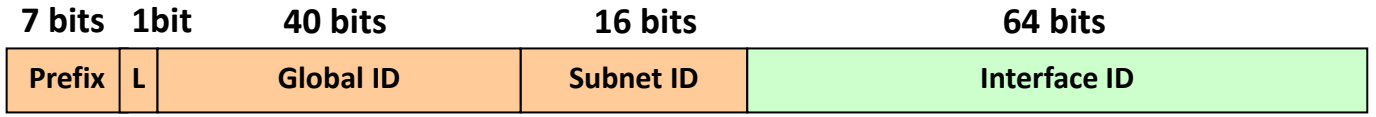
- **グローバルユニキャストアドレス**
  - 現在は **2000::/3** のアドレス空間を使用中
    - [RFC3587]（IPv6 Global Unicast Address Format）
  - Global Routing Prefix
    - RIR もしくは NIR、LIR より割り当てられる
  - Subnet ID
    - サイト内でサブネットの識別に使用
  - Interface ID
    - サブネット内のインタフェース識別に使用



  - 割り振り状況は、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/ (concluded)

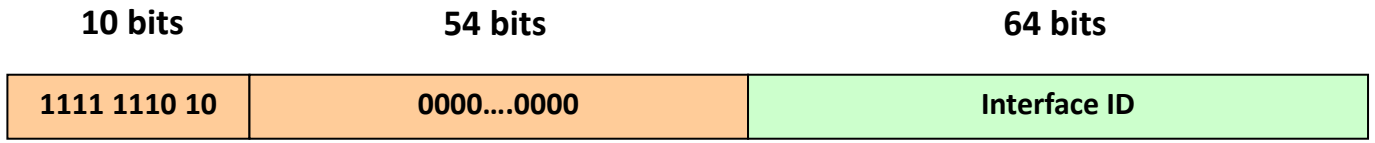
ユニキャストアドレス (2)

- **ユニークローカルアドレス［ULA］（fc00::/7 … 実質 fd00::/8）**
  - 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、*fc00::/8* 将来の為に予約。（管理組織による割当を想定）
      - *L = 1* は、*fd00::/8*
    - Global ID　：　ランダム生成（L = 1 が前提）
      - *trunc (SHA1(NTP current time + EUI-64) , 40bit)*
      - 【参考】 *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



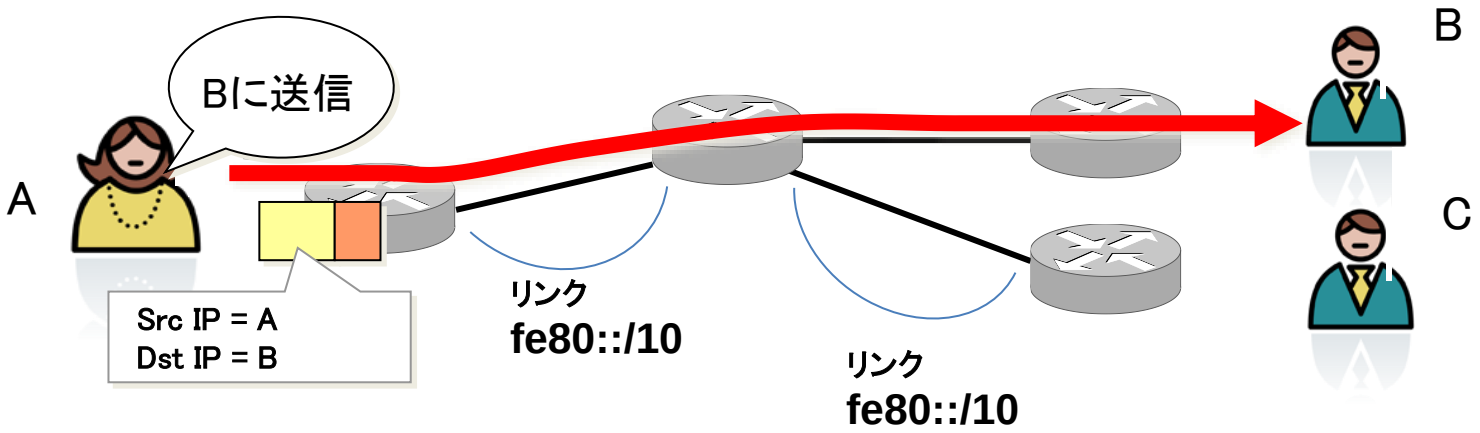
ユニキャストアドレス (3)

- **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(近隣探索プロトコル)などで使用される



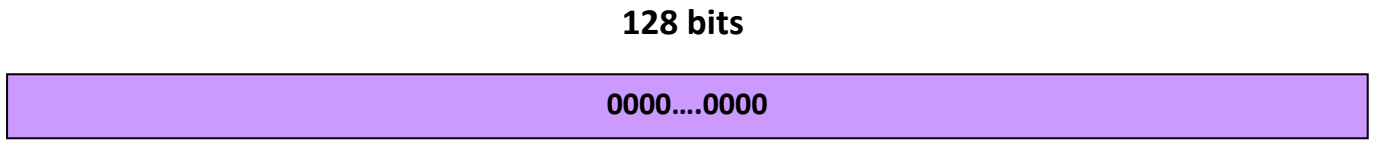
ユニキャスト通信

◆ユニキャスト　特定の相手への1対1の通信

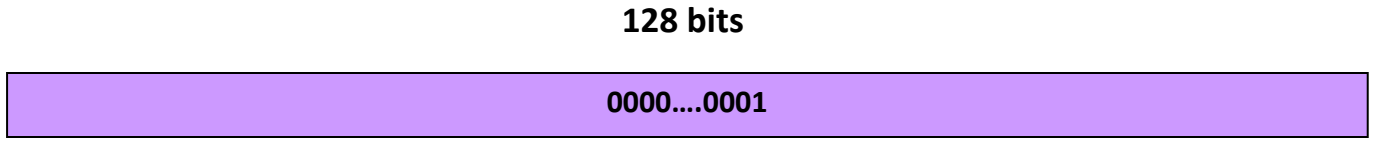


ユニキャストアドレス (4)

- **未指定アドレス（::/128）**
  - IPv4 の 0.0.0.0/32に相当

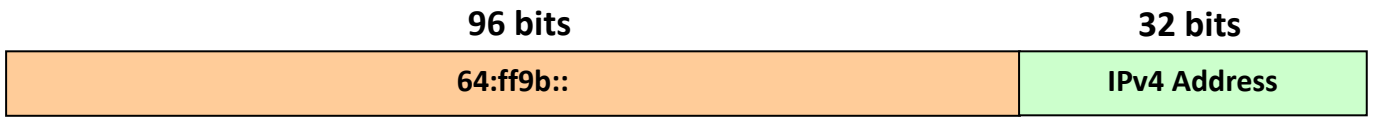


- **ループバックアドレス（::1）**
  - IPv4 の 127.0.0.1 に相当



ユニキャストアドレス (5)

- **IPv4-IPv6 変換アドレス（ IPv4-IPv6 Translation Address ）**
  - IPv4とIPv6をアルゴリズム的に相互変換するアドレス
  - NAT64などのIPv4/IPv6トランスレーションで用いられる
  - グローバルインターネットに広報してはいけない
  - 範囲: 64:ff9b::/96
  - アドレスを埋め込んだ例: 64:ff9b::192.0.2.33=64:ff9b::c000:0221



ユニキャストアドレス (6)

- **文書用アドレス（ IPv6 Documentation Address ）**
  - 技術文書、記事、資料においてIPアドレスを利用した例を提示しなければいけない場合に用いられるアドレス
  - グローバルインターネットに広報してはいけない
  - 範囲: 2001:db8::/32
  - (参考) IPv4の文章用アドレス: 192.0.2.0/24, 198.51.100.0/24, 203.0.113.0/24
- **ベンチマーク用アドレス（ IPv6 Benchmarking Address ）**
  - 検証環境用に利用可能なアドレス
  - グローバルインターネットに広報してはいけない
  - 範囲: 2001:2::/48

その他、特定用途のアドレスについて：

IPv4 http://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml

IPv6 http://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml

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	Group	1 : 1 ※1
Multicast ※2	Group	1 : n

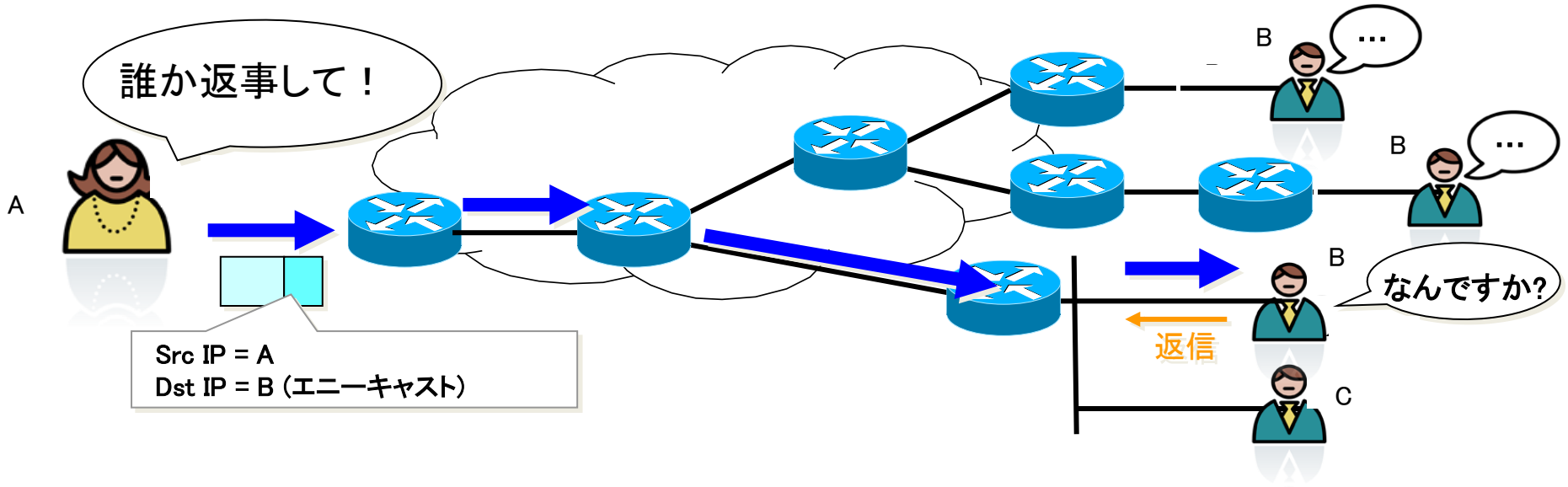
Group: インターフェースの集合

※1 グループの中からネットワーク的に最も近い1つを選択

※2 IPv6ではブロードキャストは廃止され、マルチキャストが利用されている

エニーキャスト通信

◆エニーキャスト　対象のアドレスを所有するルーティング的に近い1つのホストへの通信



エニーキャストアドレス

- **アドレス自体は、ユニキャストアドレスの範囲**
- **複数のインタフェースに同一の ユニキャストアドレスを割当てると エニーキャストアドレスになる**
- **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]
  - Root Server や JP DNS（a.dns.jp , d.dns.jp , e.dns.jp など）
    - 対障害性やDDoS攻撃対策などの目的で、分散配置されたサーバで使用されている

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	Group	1 : 1 ※1
Multicast ※2	Group	1 : n

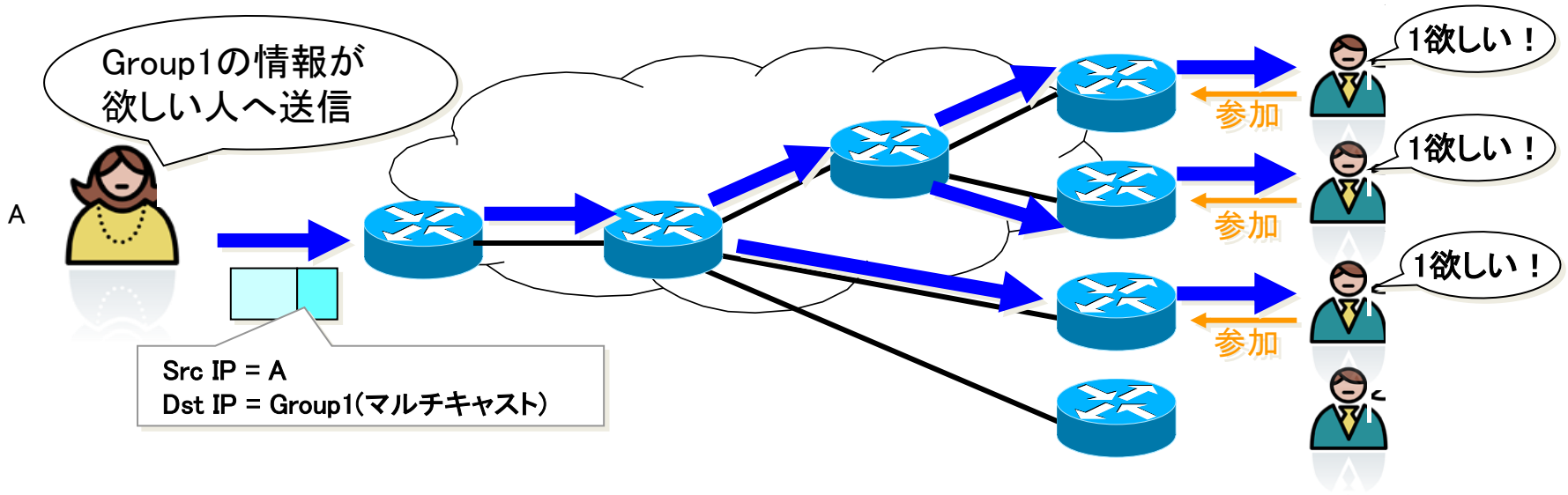
Group: インターフェースの集合

※1 グループの中からネットワーク的に最も近い1つを選択

※2 IPv6ではブロードキャストは廃止され、マルチキャストが利用されている

マルチキャスト通信

◆マルチキャスト　そのGroupに参加している多数への1対多、又は多対多の通信

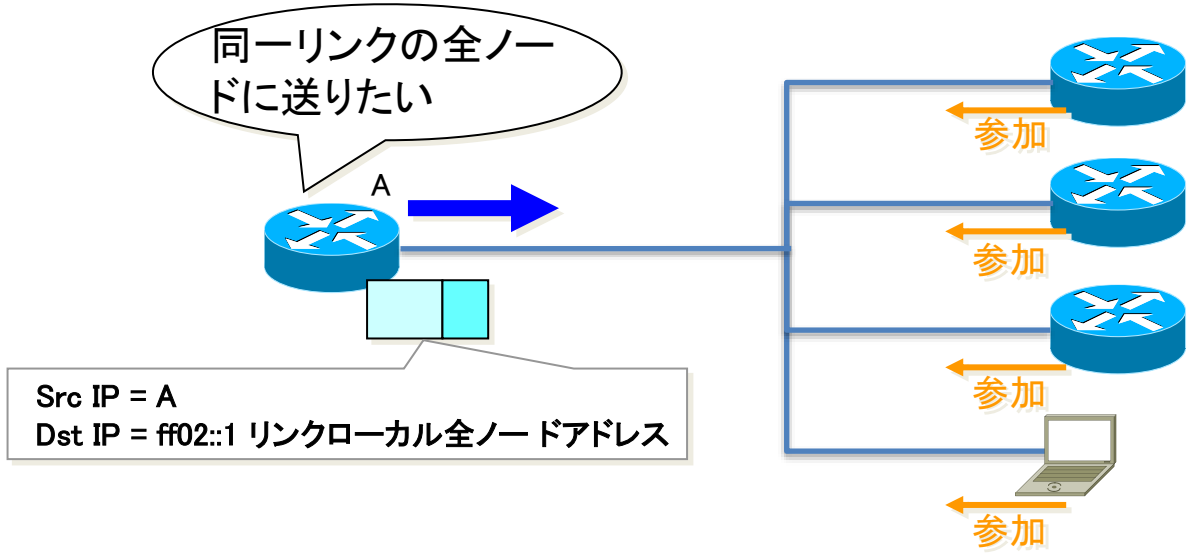


マルチキャスト通信 (リンクローカル・スコープ)

◆**リンクローカルスコープ：パケットが到達する範囲が同一サブネット上のみ**

例: ff02::1 全ノードが参加するマルチキャスト・アドレス

→IPv4におけるブロードキャストアドレスの代わりに使われる



マルチキャストアドレス (2)

- **予約済みのリンクローカルマルチキャストアドレス**
  - **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:ff00:0/104　：　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

IPv6アドレスのまとめ

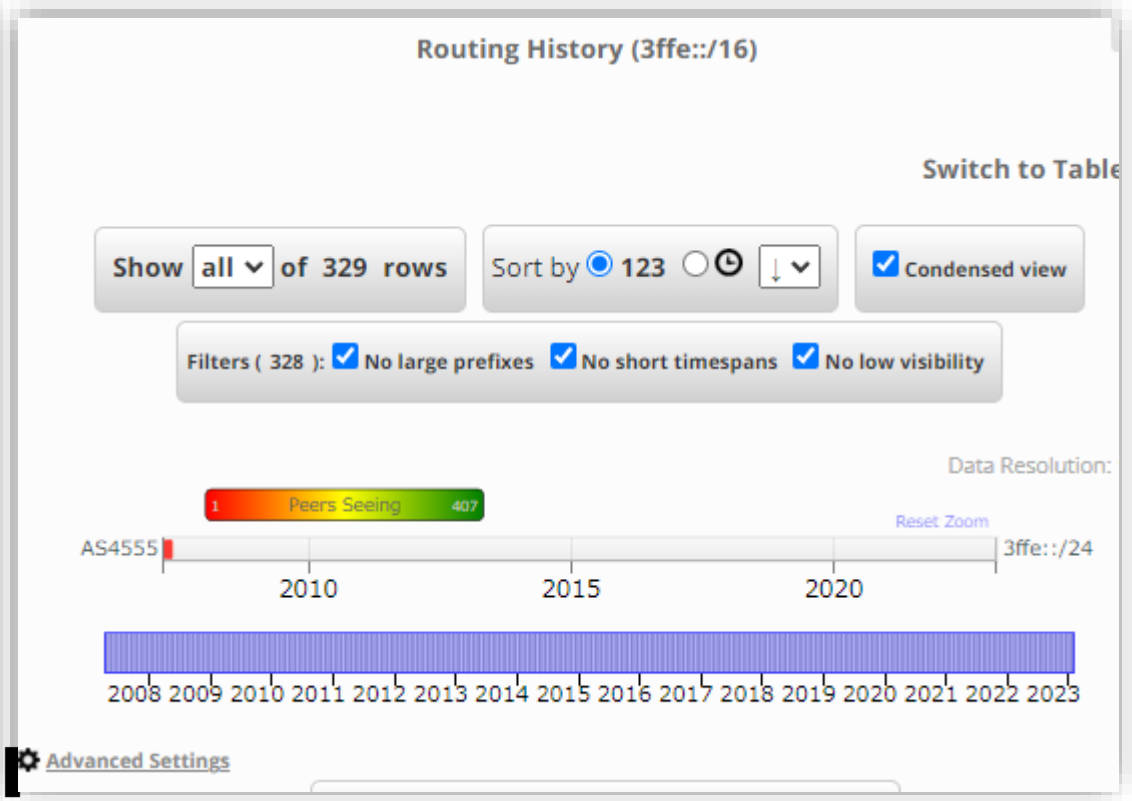
- **IPv6 では、IPv4 よりも多くのアドレスが使用される**
  - 同一インターフェースに複数アドレスが付与される

- **ノードが使う IPv6アドレス**
  - ループバックアドレス (::1/128)
  - 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
    - 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:ff00:0/104)

- **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ーキャストアドレス (Subnet Prefix 以外All 0)

過去の亡霊 3ffe::/16 6bone

- 2000::/3の範囲
  - ◆2000::/64～3fff:ffff:ffff:ffff::/64まで
  - ◆3ffe::/16　　6bone



長崎県立大学
UNIVERSITY OF NAGASAKI

ICMPとアドレス自動設定

Agenda

1.IPv6の主な機能や特徴
2.ICMPとアドレス自動設定

長崎県立大学
UNIVERSITY OF NAGASAKI

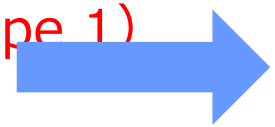
ICMPv6とは

- **ICMPv6 [RFC4443, RFC4884]**
  - ◆Internet Control Message Protocol for IPv6

- **IPv6で利用される用途**
  - ◆Ping6
  - ◆Path MTU Discovery [RFC8201]
  - ◆NDP(近隣探索プロトコル) [RFC4861]
  - ◆アドレス自動設定

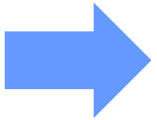
基本のICMPv6メッセージ

- **ICMP Error Message（type 0～127）**
  - Destination Unreachable（type 1）
  - **Packet Too Big（type 2）**
  - Time Exceeded（type 3）
  - Parameter Problem（type 4）



Path MTU Discovery

- **ICMP Informational Message（type 128～255）**
  - Echo Request（type 128）
  - Echo Reply（type 129）
  - **Router Solicitation（type 133）**
  - **Router Advertisement（type 134）**
  - **Neighbor Solicitation（type 135）**
  - **Neighbor Advertisement（type 136）**
  - Redirect Message (type137)



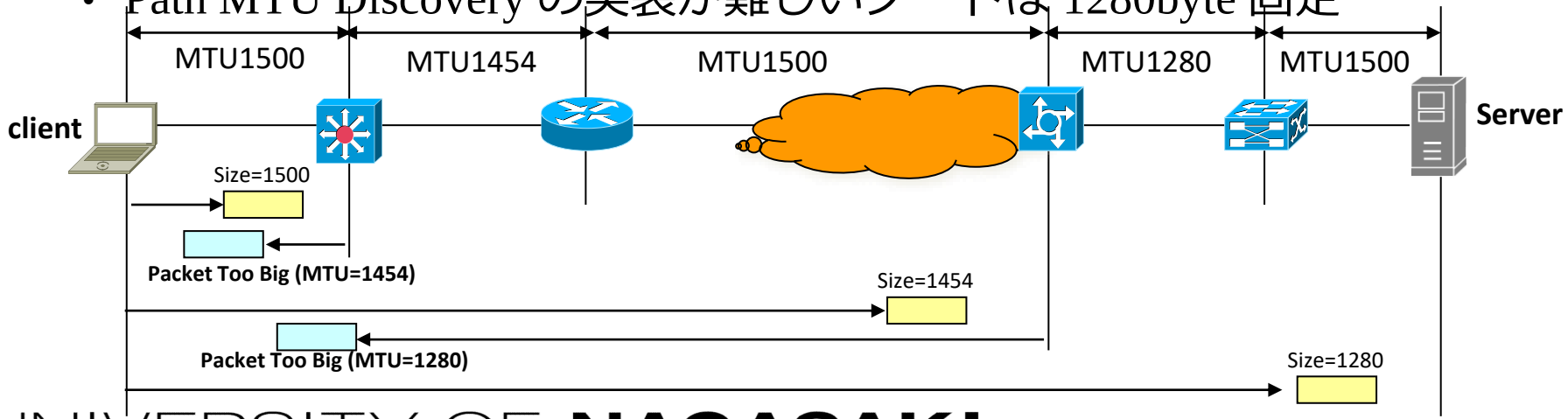
Neighbor Discovery(近隣探索)
アドレス自動設定

Deny icmp any any

ダメ、ゼッタイ！

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
    - L2 SWのMTUにひっかかった場合は破棄される
    - Path MTU Discovery の実装が難しいノードは 1280byte 固定



NDP (近隣探索) プロトコル（IPv4のARP）

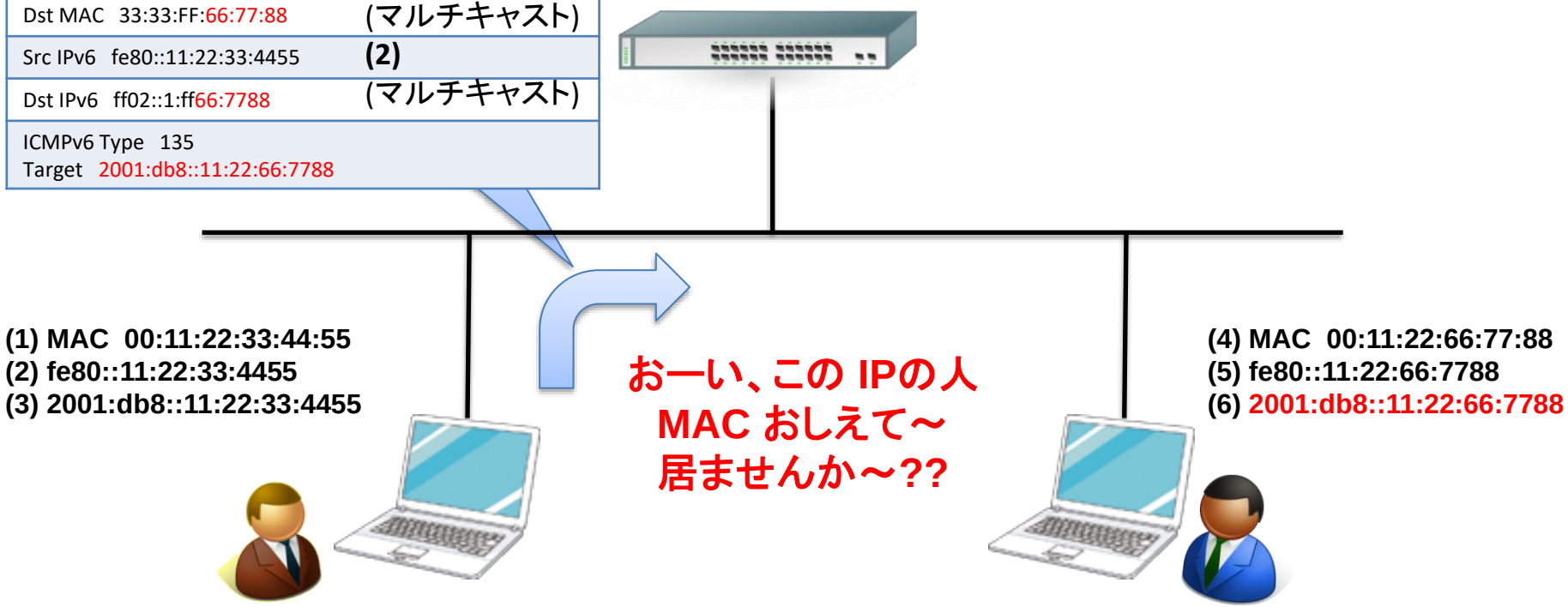
■ 5つのメッセージタイプ （ICMPv6機能の一部）

- Neighbor Solicitation（NS 近隣要請）
  - リンクレイヤアドレスの解決（ARP相当）
  - 重複アドレス検出（DAD）、近隣到達不能検出（NUD）
- Neighbor Advertisement（NA 近隣広告）
  - NSに対する応答
- Router Solicitation（RS ルータ要請）
  - ルータ発見に利用
  - RAを即座に取得したい場合に送出
- Router Advertisement（RA ルータ広告）
  - ノードにプレフィックス情報等を配布
  - ルータによるデフォルト経路の通知
- リダイレクト
  - 最適な経路を通知（IPv4と同様）

NS 近隣要請

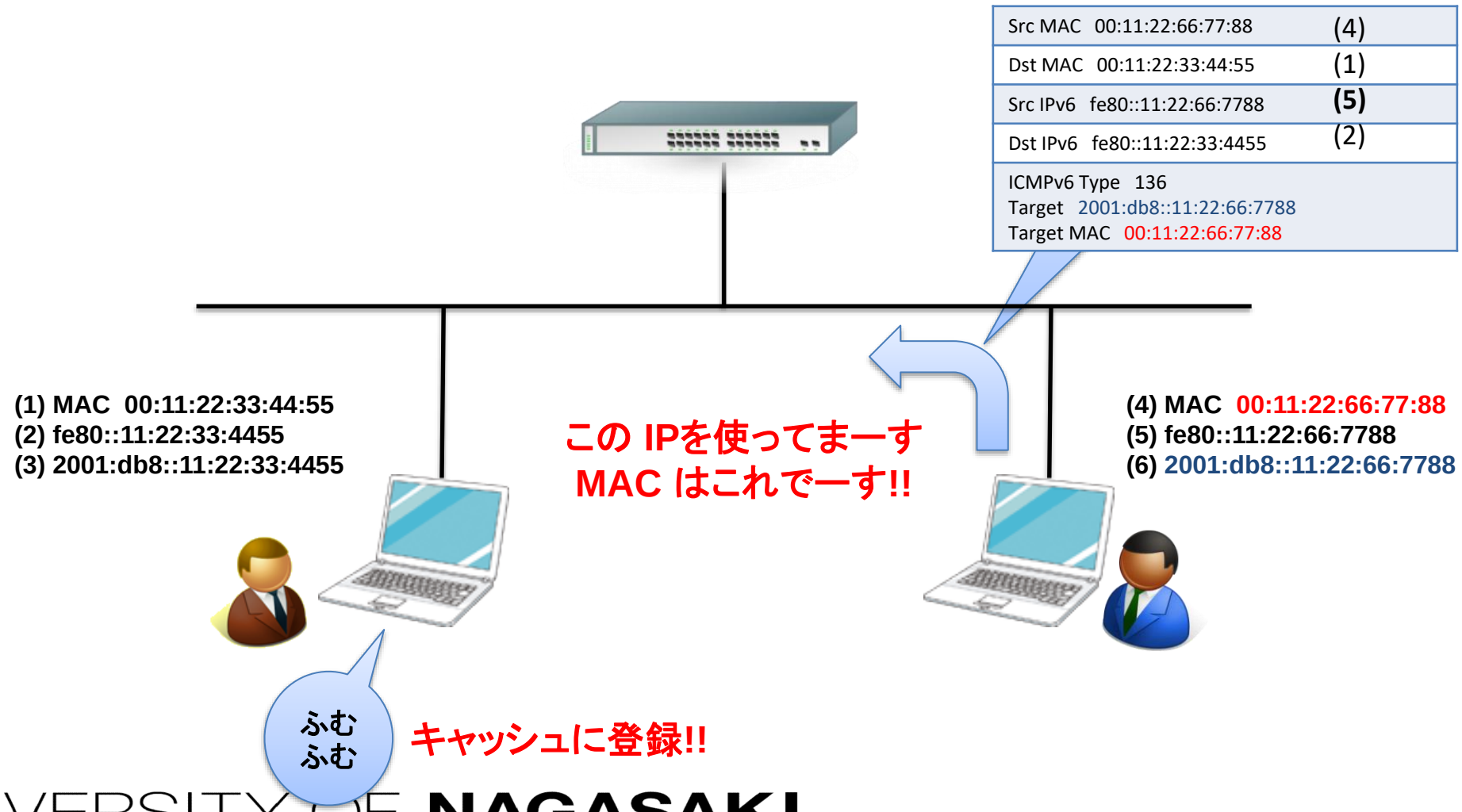
宛先アドレスには、要請ノードアドレス（マルチキャスト）を使います

Src MAC 00:11:22:33:44:55	(1)
Dst MAC 33:33:FF:66:77:88	(マルチキャスト)
Src IPv6 fe80::11:22:33:4455	(2)
Dst IPv6 ff02::1:ff66:7788	(マルチキャスト)
ICMPv6 Type 135 Target 2001:db8::11:22:66:7788	

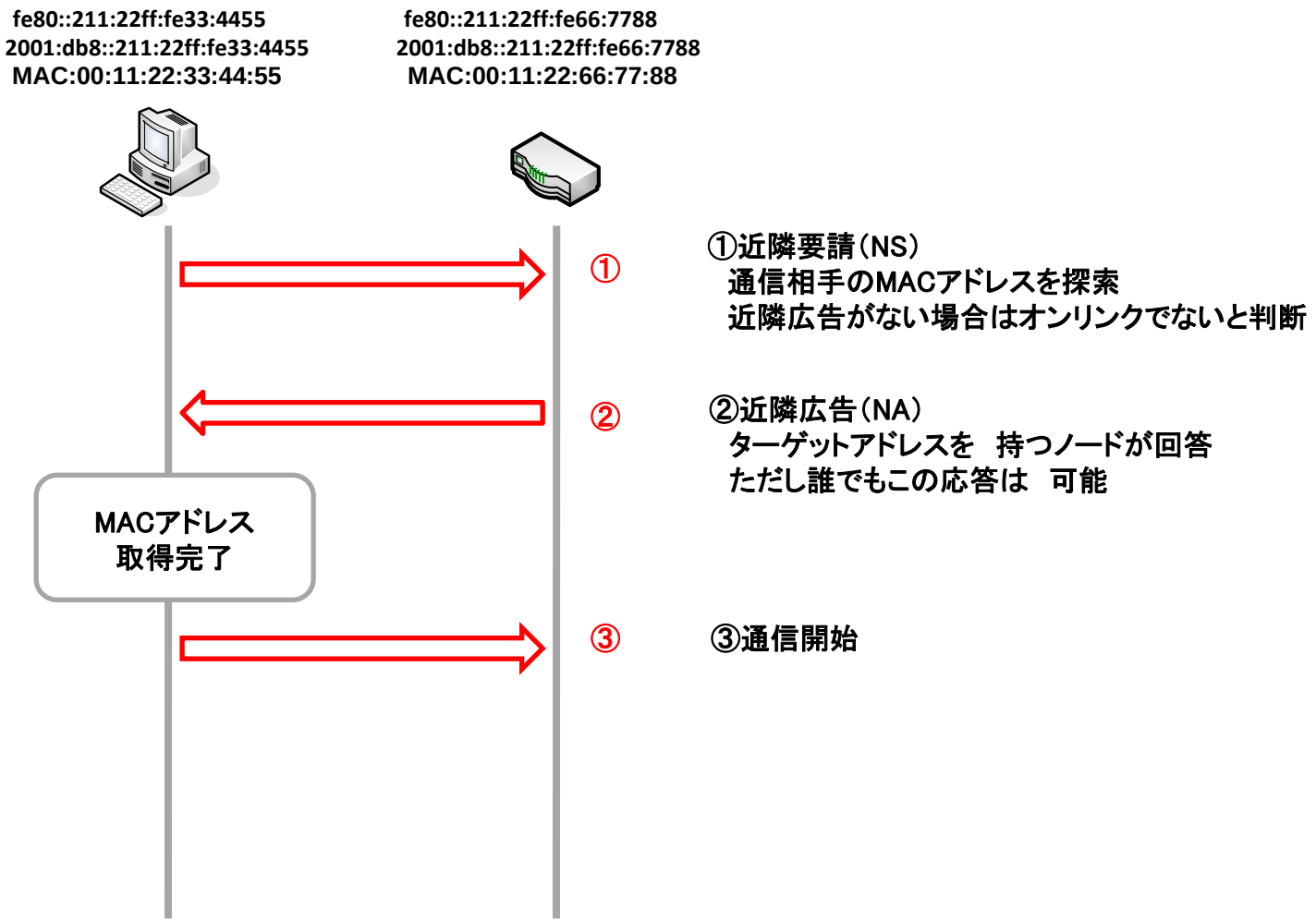


相手先 2001:db8::11:22:66:7788
と通信したい…..
けど相手の MAC アドレスを知らない
（存在しないかもしれない…）

NA 近隣広告


Src MAC 00:11:22:66:77:88 (4)
Dst MAC 00:11:22:33:44:55 (1)
Src IPv6 fe80::11:22:66:7788 (5)
Dst IPv6 fe80::11:22:33:4455 (2)
ICMPv6 Type 136
Target 2001:db8::11:22:66:7788
Target MAC 00:11:22:66:77:88
(1) MAC 00:11:22:33:44:55
(2) fe80::11:22:33:4455
(3) 2001:db8::11:22:33:4455
この IPを使ってまーす
MAC はこれでーす!!
(4) MAC 00:11:22:66:77:88
(5) fe80::11:22:66:7788
(6) 2001:db8::11:22:66:7788
ふむ
ふむ
キャッシュに登録!!

リンクレイヤアドレス解決の流れ



①近隣要請（NS）
通信相手のMACアドレスを探索
近隣広告がない場合はオンリンクでないと判断

②近隣広告（NA）
ターゲットアドレスを　持つノードが回答
ただし誰でもこの応答は　可能

③通信開始

Src MAC　00:11:22:33:44:55
Dst MAC　33:33:FF:66:77:88
Src IPv6　fe80::211:22ff:fe33:4455
Dst IPv6　ff02::1:ff66:7788
ICMPv6 Type　135 Target　2001:db8::211:22ff:fe66:7788

Src MAC　00:11:22:66:77:88
Dst MAC　00:11:22:33:44:55
Src IPv6　fe80::211:22ff:fe66:7788
Dst IPv6　fe80::211:22ff:fe33:4455
ICMPv6 Type　136 Target　2001:db8::211:22ff:fe66:7788 Target MAC　00:11:22:66:77:88

NS / NA まとめ

- **リンク層アドレス解決とNUD (Neighbor Unreachability Detection)**
  - IPv4のARP Request/Replyに似ている
- **宛先に要請ノードマルチキャストアドレスを使用**
  - 効率化 - リンクの全てのノードが受け取る必要が無い
- **ソースアドレスは、自分のインターフェイスのアドレスを使用**
  - 使用できるアドレスがない場合はUnspecified (::)を使用
- **255未満のHop Limitは無視**
  - (Hop Limitは255が上限 ＝ 同一リンク上から以外のパケットを廃棄)
- **ARPと異なり双方向で行われる必要がある**
  - NSをもってL2アドレス解決とすることができない。
- **アドレス解決後 NCE(Neighbor Cache Entry)を作成**

アドレスの自動設定 IPv6

- **RA：SLAAC（StateLess Address Auto Configuration）[RFC4862]**
  - アドレスを管理するサーバはない
    - ノードは、RAで受け取ったPrefix情報や、ノード自身のMACアドレス等を使用して自動的にアドレスを生成する

- **DHCPv6（Dynamic Host Configuration Protocol for IPv6）[RFC8415]**
  - ステートフルなアドレスの自動設定
  - Default Gateway が通知されない
    - RAと組み合わせて使う前提
  - その他の機能は IPv4 の DHCP とほぼ同じ

アドレスの自動設定 IPv4 との違い

IPv4 と IPv6 で異なる自動設定

	IPv6			IPv4
	RA (SLAAC)	DHCPv6	DHCPv6-lite	DHCPv4
IP Address	○ Prefix情報を通知	○ アドレスを通知	–	○ アドレスを通知
Default Gateway	○	– ※1	–	○
Server Address (DNS , SIP , etc)	△ ※2	○	○	○

※1　経路情報の配布として標準化が試みられた
※2　DNSサーバアドレスの配布は [RFC8106] で標準化

RA / DHCPv6

- **RA**
  - ◆Default Routeの冗長化がIPv4と比べて容易
  - ◆DNSアドレスが配れないことがある
    (現在は全ての端末が一般的に対応している状況とはいえない。)
  - ◆不正なRAに対する対処が必要

- **DHCPv6/DHCPv6-lite**
  - ◆DNSやNTPサーバの情報を配布可能
  - ◆Default Gatewayのアドレスを配れない
  - ◆端末が対応していないことがある。
  - ◆RAとの併用が前提
  - ◆不正なDHCPv6サーバの対処が必要

RDNSSオプション [RFC8106]

- 現在Androidなどの一部のデバイスやOSバージョンでは、DHCPv6に対応していないものが存在する。

- DHCPv6に対応していない機器の場合、殆どがRAによってDNSアドレスを配布するRDNSS(Recursive DNS Server)オプションに対応しているため、その場合はIPv6 DNSアドレスの配布にRAを利用する。

IPアドレス	DNS	Windows10 Creators update以前	Windows10 Creators update後	MacOS X	iPhone	Android
RA	RA	NG	OK	OK	OK	OK
RA	DHCPv6	OK	OK	OK	OK	**NG**
DHCPv6	DHCPv6	OK	OK	OK	OK	**NG**

Android Open Source Project - issue Tracker https://code.google.com/p/android/issues/detail?id=32621
https://ja.wikipedia.org/wiki/%E3%82%AA%E3%83%9A%E3%83%AC%E3%83%BC%E3%83%86%E3%82%A3%E3%83%B3%E3%82%B0%E3%82%B7%E3%82%B9%E3%83%86%E3%83%A0%E3%81%AEIPv6%E5%AF%BE%E5%BF%9C%E3%81%AE%E6%AF%94%E8%BC%83

SLAACによるアドレス自動設定

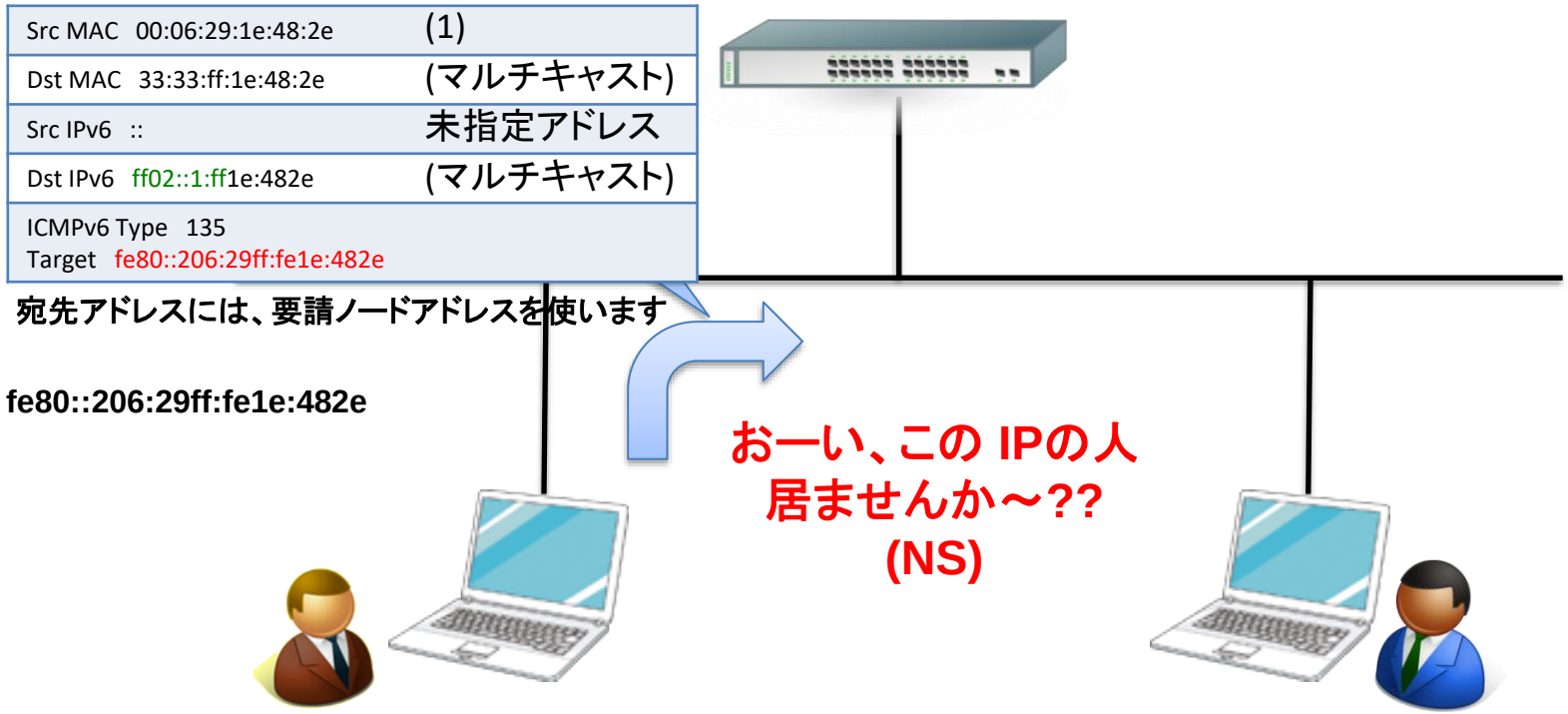
- 1. クライアントは、自分自身のMACアドレスを基に、EUI-64にて、Link Local Address(仮)を生成

(MAC Address) 00:06:29:1e:48:2e

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

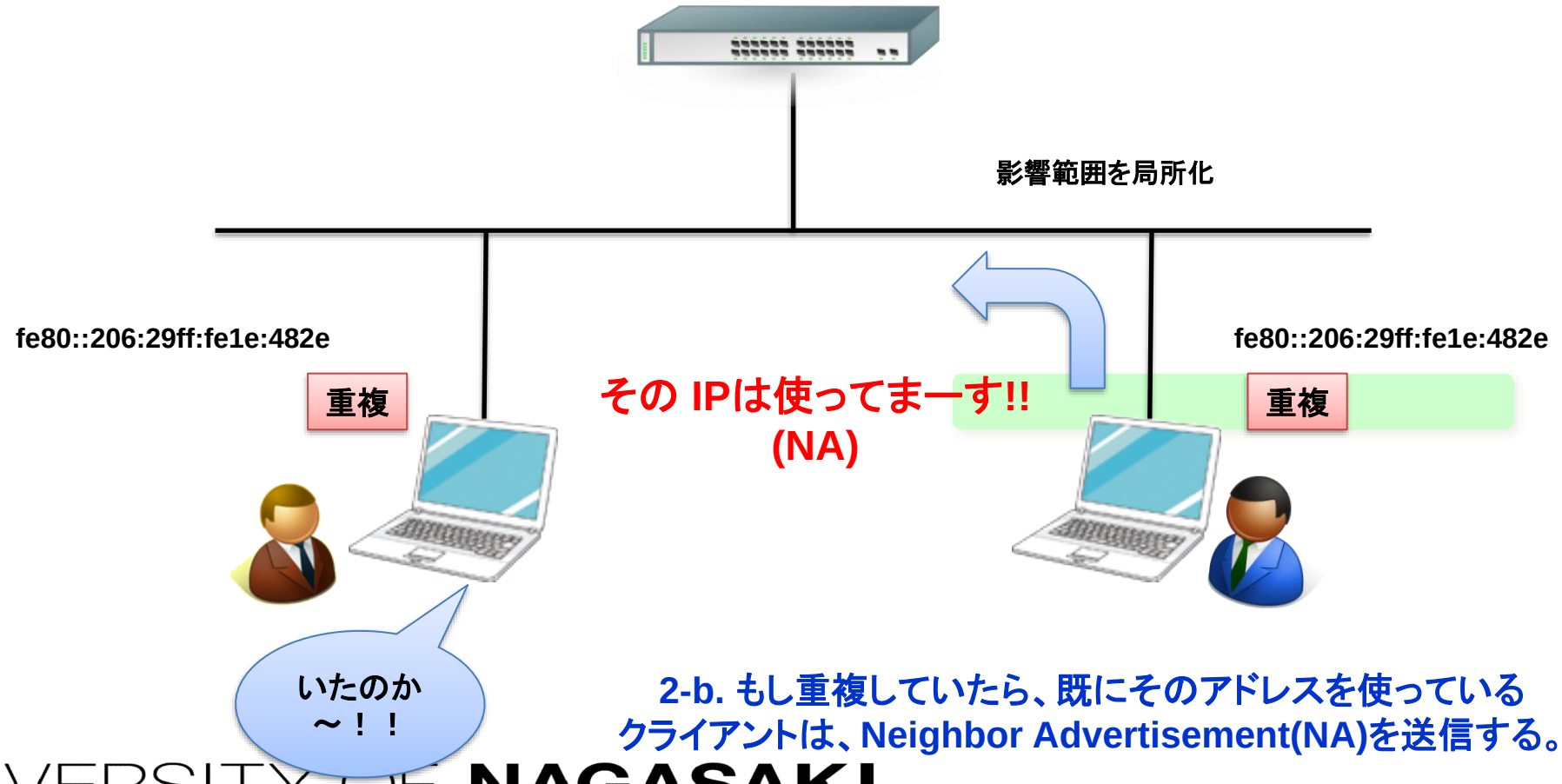
SLAACによるアドレス自動設定

2. クライアントは、Neighbor Solicitation(NS)を送信し、生成したリンクローカルアドレスが他のノードで使用されていないか確認



2-a. 返事がなければ、重複していない
= リンクローカルアドレスが確定

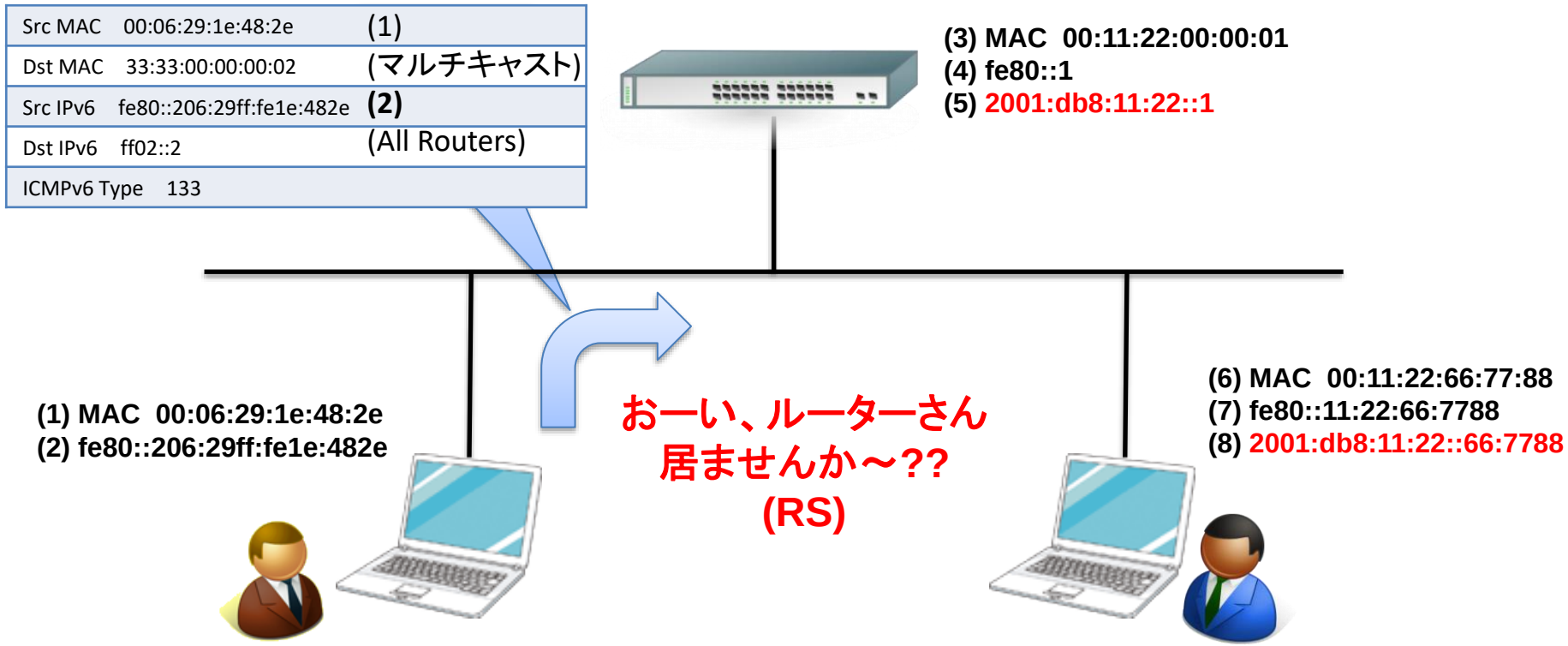
SLAACによるアドレス自動設定



2-b. もし重複していたら、既にそのアドレスを使っている
クライアントは、Neighbor Advertisement(NA)を送信する。

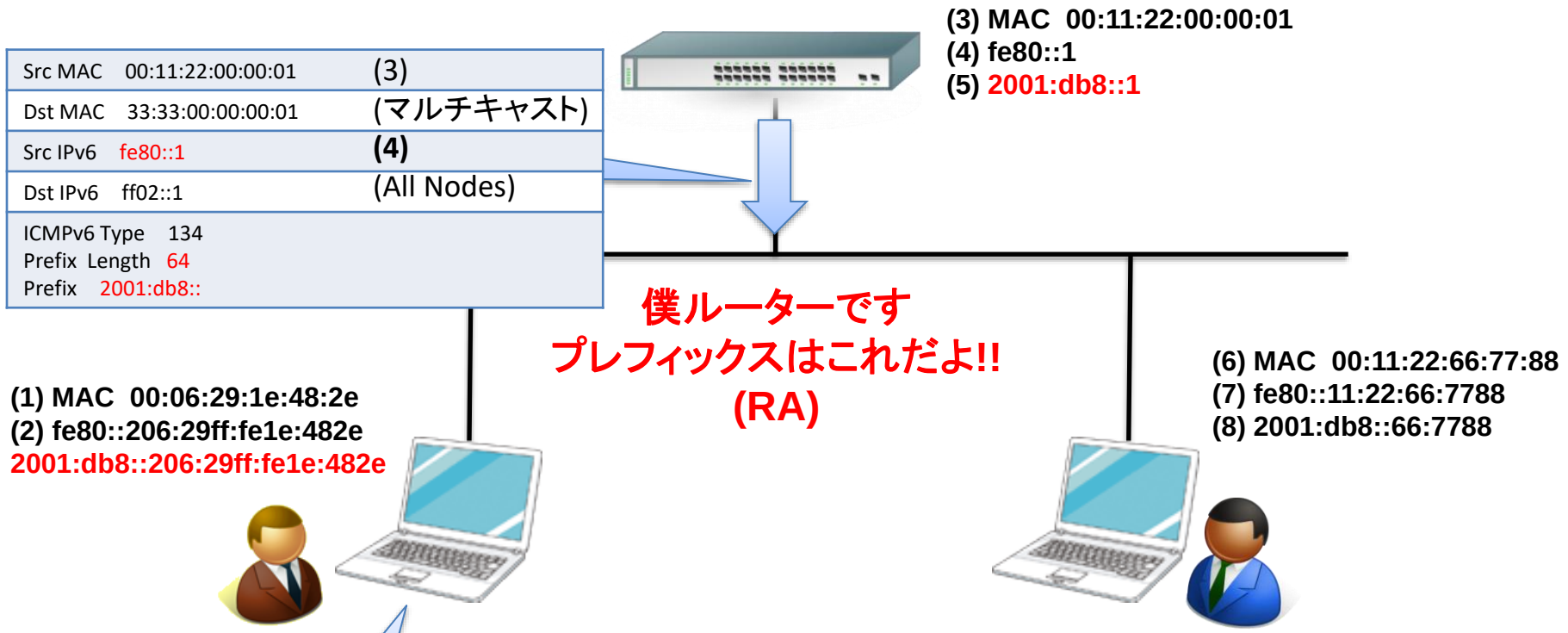
SLAACによるアドレス自動設定

3. クライアントは、Router Solicitation(RS)を送信し、ルータを探索する



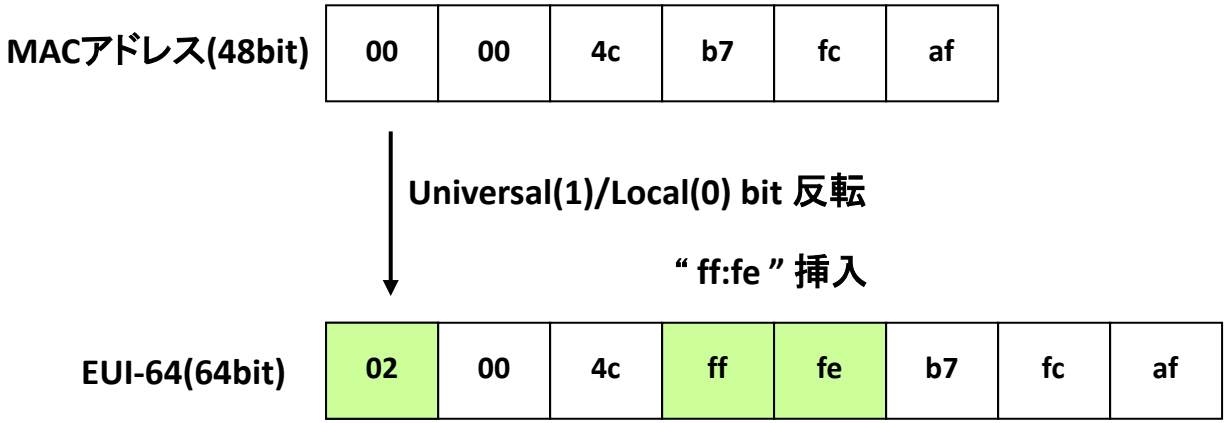
SLAACによるアドレス自動設定

4. 返ってきたRouter Advertisement(RA)に含まれるプレフィックス情報から、
自分のグローバルアドレスとデフォルトゲートウェイを設定する



アドレスの生成方法

- **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



- **Windows などの多くのOSでMACアドレスベースではなく、この独自のインターフェイスIDを生成利用**

Default Gateway Availability

- **IPv4でのHSRP/VRRP**
- **IPv6**
  - ◆HSRP/VRRP
    - ■もちろん普通に動作
      - ロただし、ライセンスが追加必要な場合も
  - ◆IPv6 Router Adviter

アドレスの自動設定

- **IPv4 と IPv6 で異なる自動設定**

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

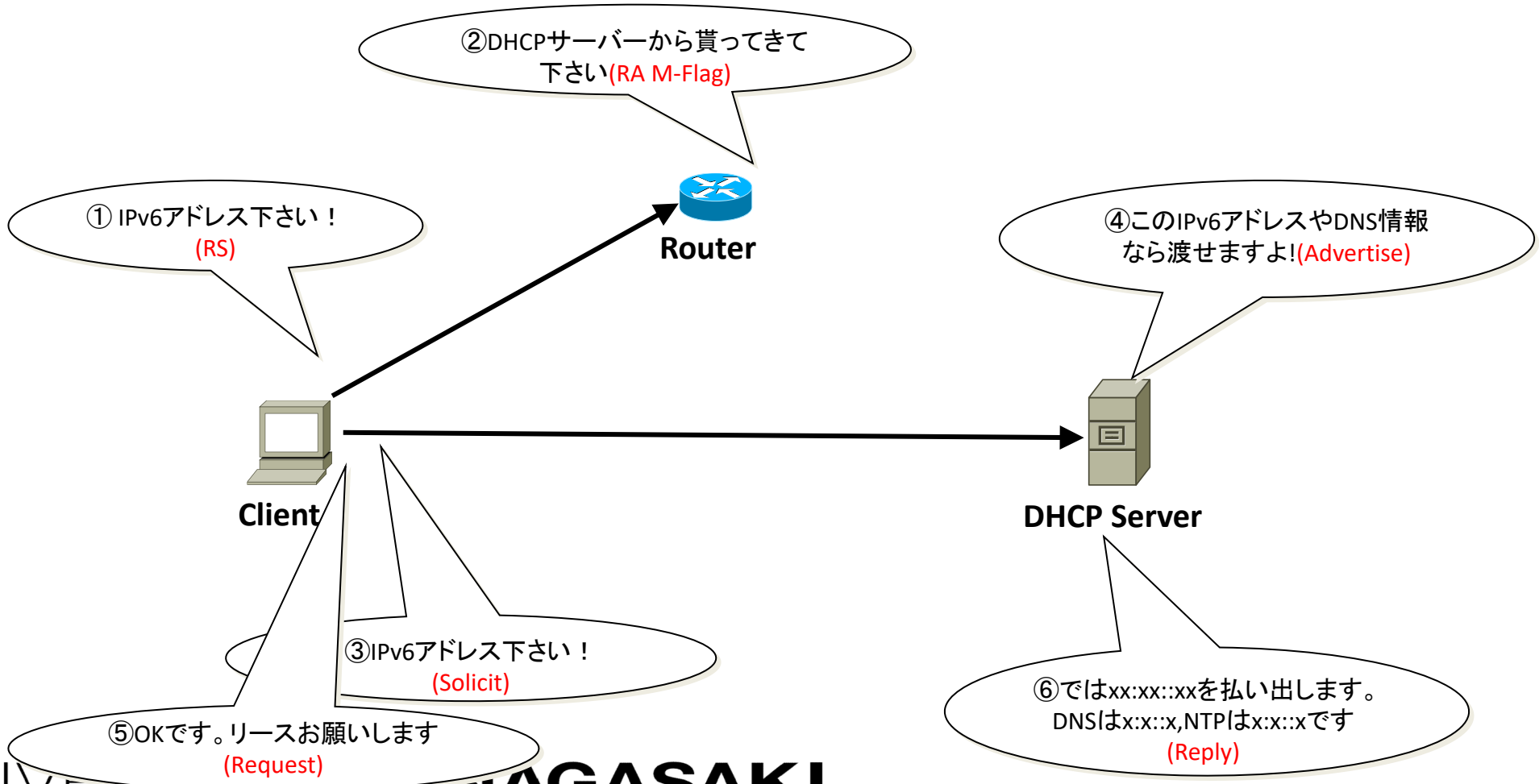
※1　経路情報の配布として標準化が試みられた
※2　DNSサーバアドレスの配布は [RFC8106] で標準化

DHCPv6

- **Stateful DHCPv6**
  - DHCP for IPv6 [RFC8415]
    - 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
  - DHCPv6-PD [RFC8415]
    - 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 (Home GateWay) は、RA または DHCPv6 を使用して再配布

- **Stateless DHCPv6 (DHCPv6-lite)** [RFC8415]
  - 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

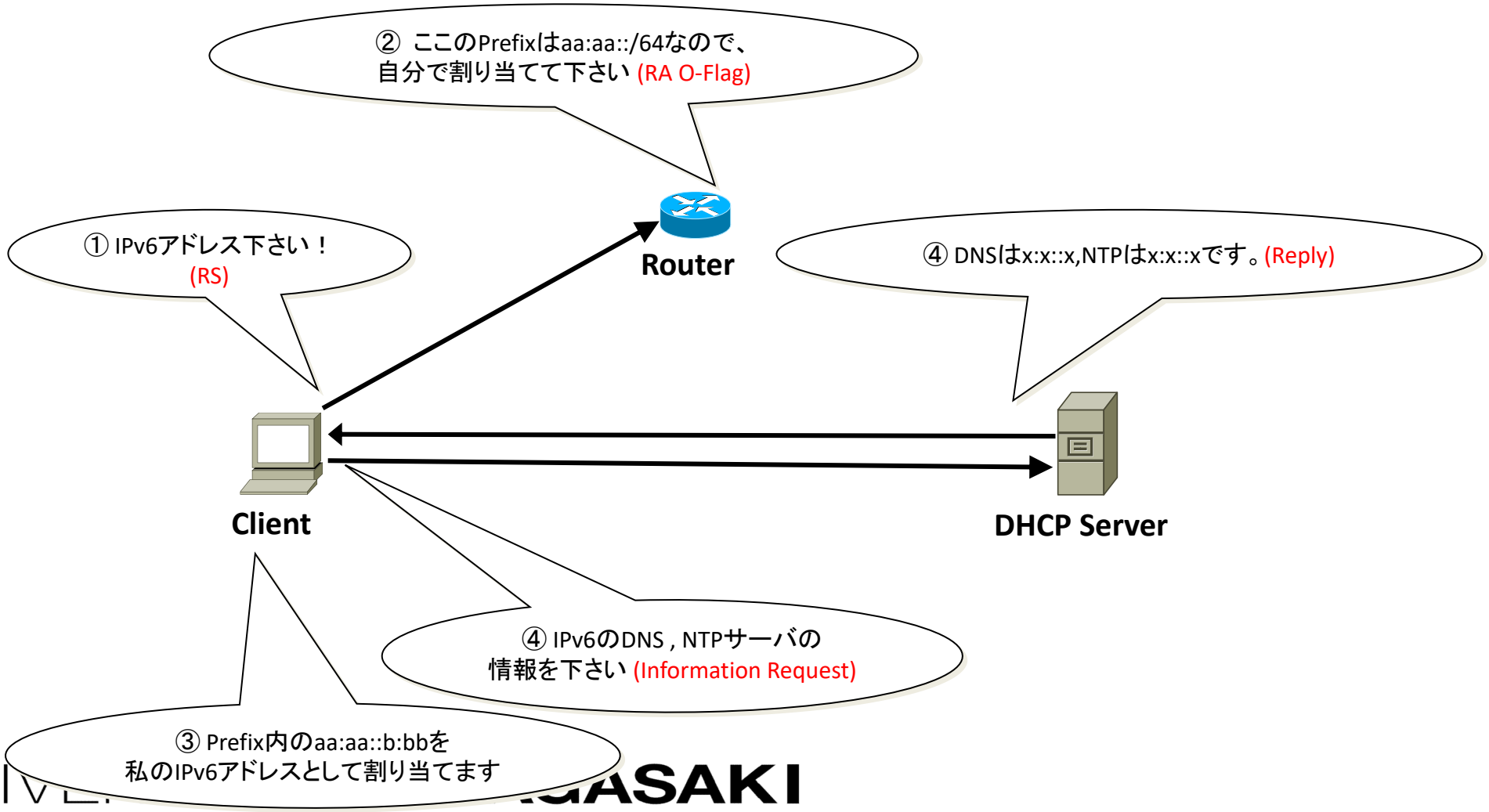
Stateful DHCPv6



Stateful DHCPv6の特徴

- 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 が動作する
- Rapid Commit Option が有効な場合、Advertise/Request は省略される
- アドレスの要求にはIA_NAオプションか、IA_TAオプションを使用

Stateless DHCPv6 (DHCPv6-lite)



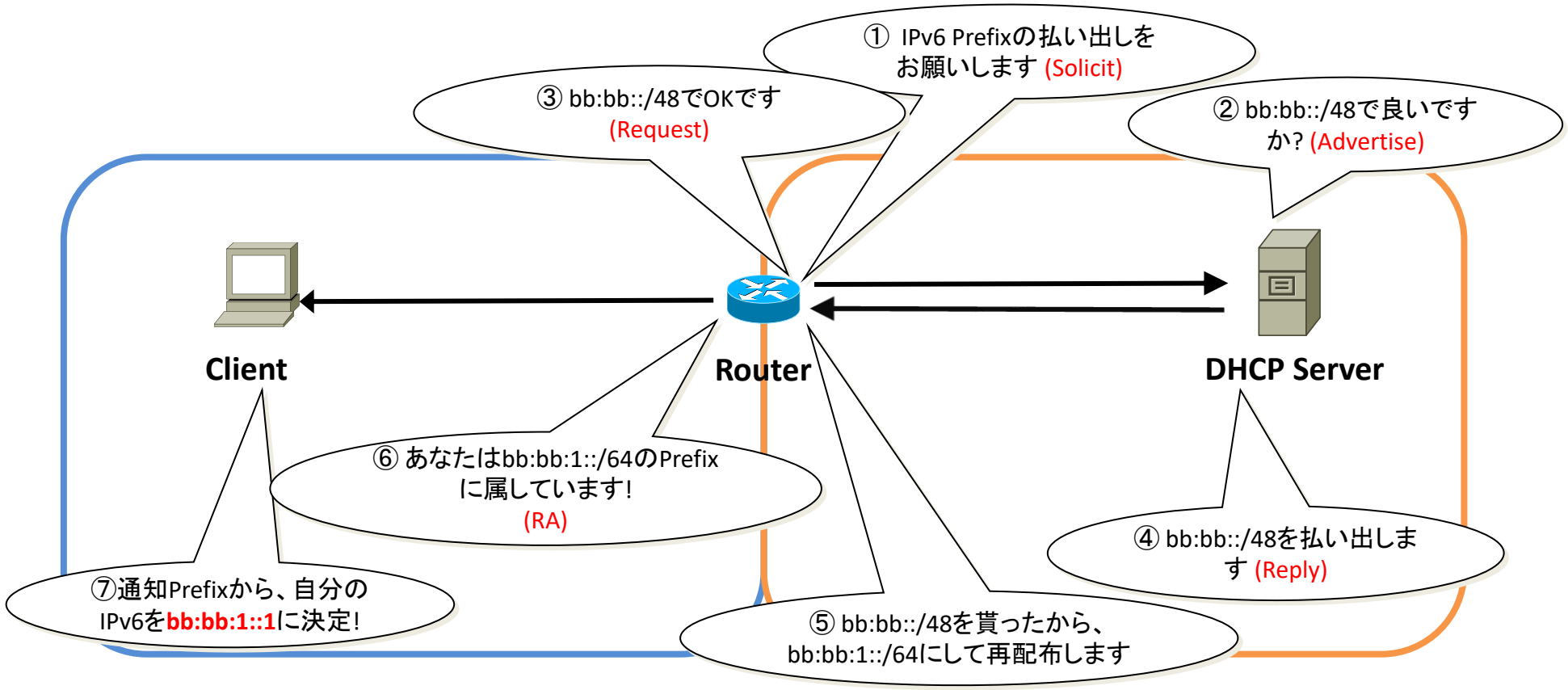
Stateless DHCPv6の特徴

- DHCP Server はHost情報を管理しない
  （IPアドレス情報/リース管理等）

- Host は、RA の O-Flag 受信により、DHCPv6 Client が動作

- RAだけではDNS/NTPなどの必要なサーバ情報の通知に不足があるケースあり
  - 利用端末の仕様によって、DHCPサーバによって追加でNTPやDNSなどの通知が必要な場合がある。

DHCPv6-PD


① IPv6 Prefixの払い出しを
お願いします (Solicit)
③ bb:bb::/48でOKです
(Request)
② bb:bb::/48で良いです
か? (Advertise)
Client
Router
DHCP Server
⑥ あなたはbb:bb:1::/64のPrefix
に属しています!
(RA)
④ bb:bb::/48を払い出しま
す (Reply)
⑦通知Prefixから、自分の
IPv6をbb:bb:1::1に決定!
⑤ bb:bb::/48を貰ったから、
bb:bb:1::/64にして再配布します

DHCPv6-PDの特徴

- ノードアドレスではなく、Prefix を付与
- Prefixの要求にはIA_PDオプションを使用
- Prefix を取得した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

- 主にISPとユーザネットワークの間で利用されている

長崎県立大学
UNIVERSITY OF NAGASAKI

セッション2
v6導入のための設計・構築・運用

- 移行技術
- アドレッシングとDNS
- 運用監視
- ルーティングと冗長
- パケットフィルタリング

長崎県立大学
UNIVERSITY OF NAGASAKI

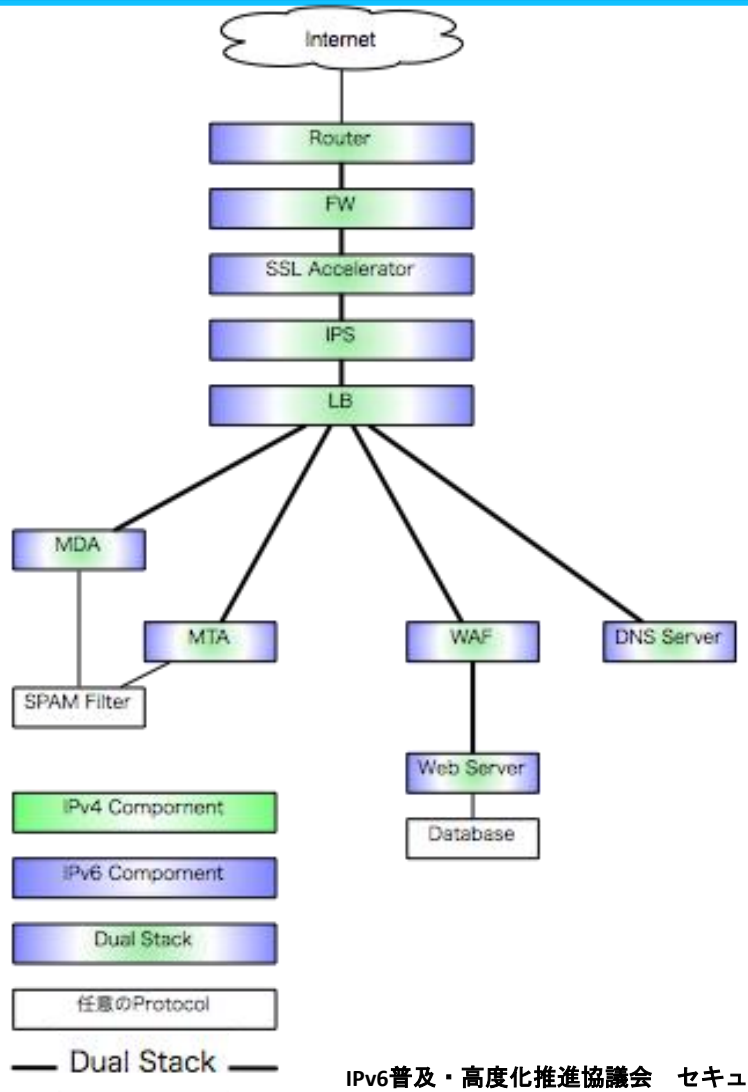
IPv6対応へのシナリオ

- **IPv4からIPv4/v6対応ネットワークへの移行時の検討が重要**

➢ **対応モデルとして考えられるのは以下の３つ**

- IPv4/IPv6 Dual Stack Model
- IPv4 Network と別に IPv6 Networkを構築する Parallel Stack Model
- 一部をDual Stackに、一部をIPv4/IPv6それぞれに独立させる Hybrid Model

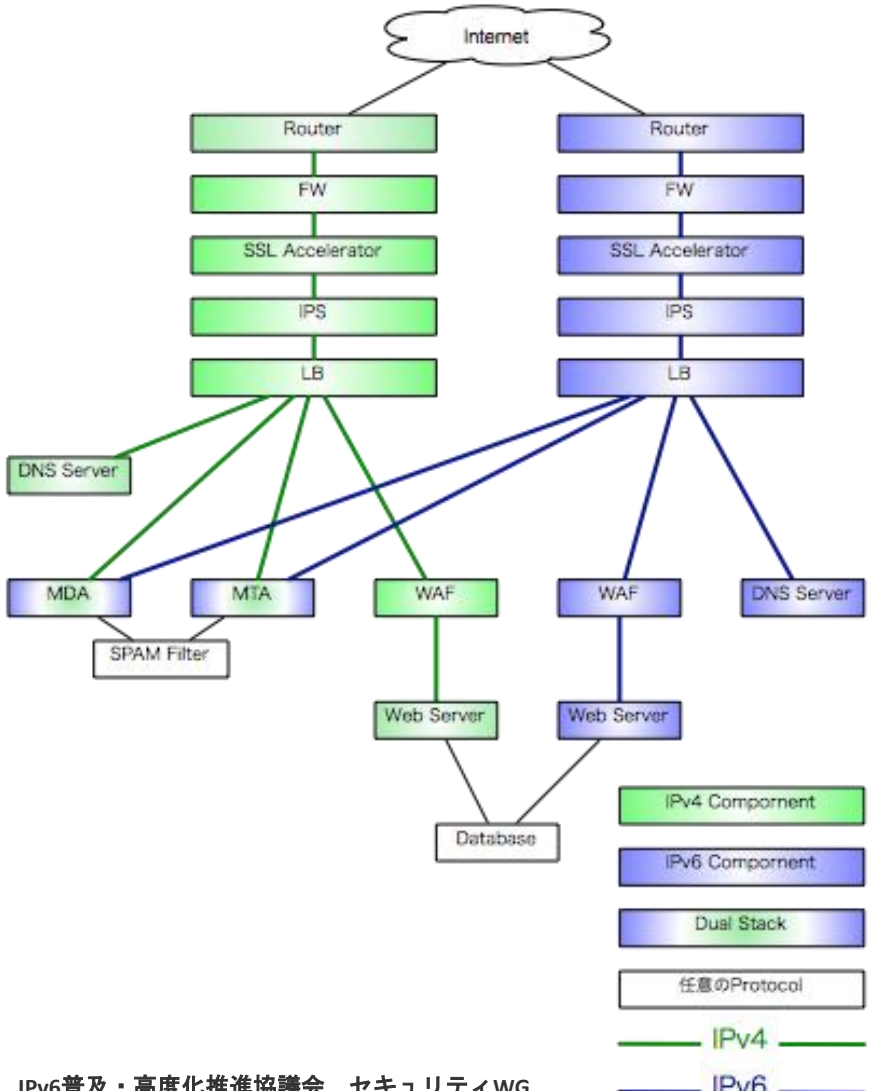
Dual Stack Network



- **Merit**
  - 構造が単純、機器が少ない
  - IPv4で構築した構造をそのままにIPv6に対応できる
- **Demerit**
  - v4 Networkの構造に縛られる
  - 機器毎の管理が複雑になる
  - 障害が全域に影響する
  - v4通信とv6通信のlogが混ざるため、分析が面倒になる

IPv6普及・高度化推進協議会　セキュリティWG
IPv6対応セキュリティガイドライン（第2.0版）より

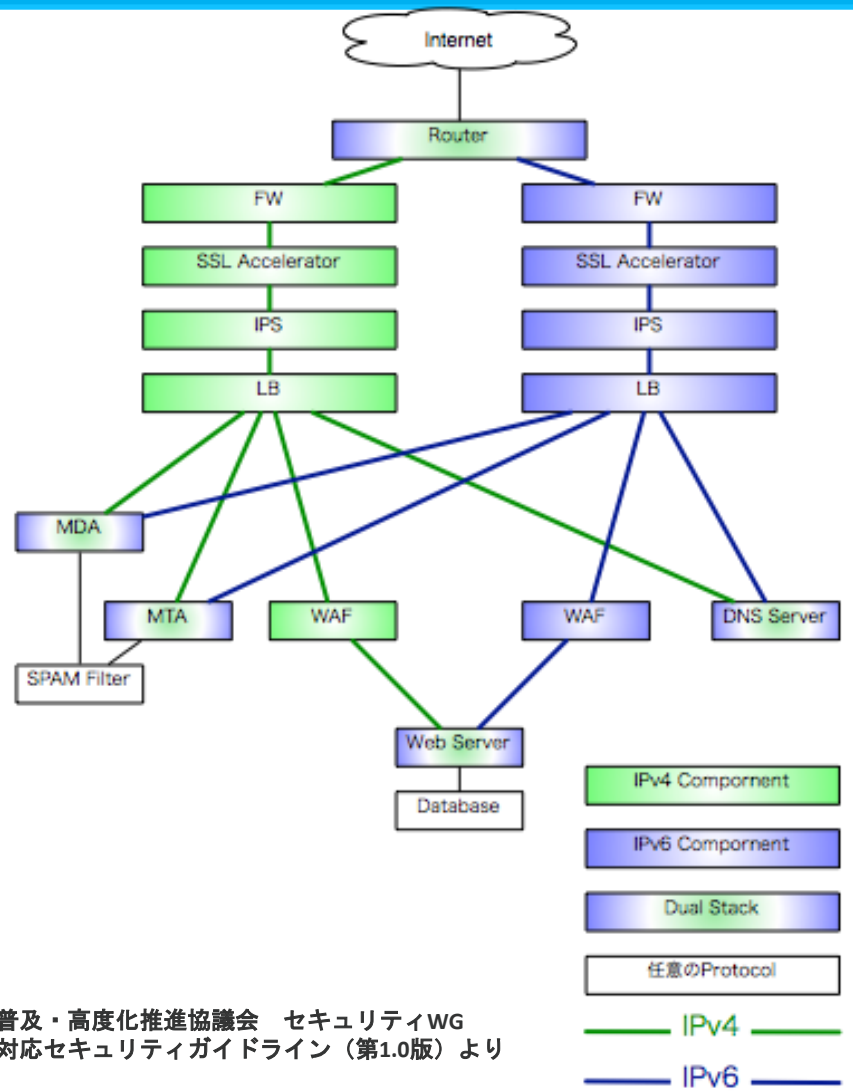
Parallel Stack Network



- **Merit**
  - 構造は簡単
  - ネットワークの再設計が可能
    - Protocol毎に管理すればよい
  - 片系の障害が逆系に波及しない
  - IPv4の障害とIPv6の障害を切り分けやすい

- **Demerit**
  - 機器が多く、故障率が上がる
  - 管理が大変になる

Hybrid Network



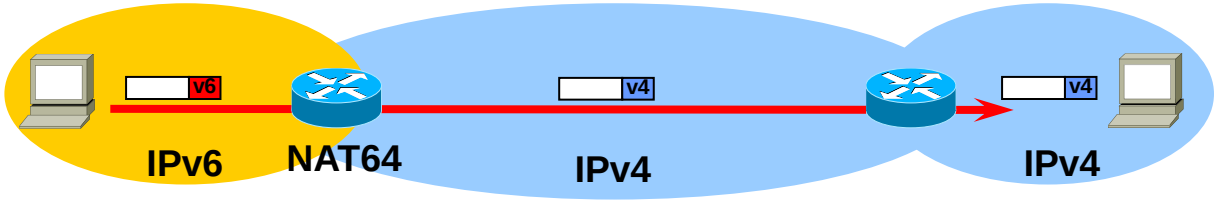
IPv6普及・高度化推進協議会　セキュリティWG
IPv6対応セキュリティガイドライン（第1.0版）より

- **Dual Stack ModelとParallel Stack Model のちょうど中間**
- **Merit**
  - ある程度の実績はある
  - 障害の分離がしやすくなる
- **Demerit**
  - 機器が多くなり、故障率があがる
  - 管理が面倒

IPv4/v6共存まとめ

- **構成の検討**
  - ◆全てデュアルスタックできるか確認していく、もしくはv6対応させるサービス、システムに新しくv6用のシステムを別建することから検討を始めていくと考えやすいかもしれない
  - ◆既存機器がIPv6に対応していない場合、ハイブリッドのようにv6ネットワーク用機器を追加する形で対応可能
- **注意点**
  - ◆ネットワーク側でIPv4 NAT/NAPTを維持し続ける必要がある
  - ◆IPv4/IPv6両方の不具合を確認する管理コストが増加

NAT64/DNS64



- **NAT64 と DNS64 を組み合わせて利用**
- **NAT64で、宛先が設定されたIPv4-IPv6 変換アドレスとなっているIPv6 パケットのIPv6 ヘッダを、 IPv4 ヘッダへ変換。応答パケットもNAT64でIPv4からIPv6ヘッダへ変換する。**
- **端末が利用するIP アドレス の変換には DNS64 を利用**
  - 端末は、アドレス解決時にDNS64 によって提供される IPv4 アドレスが合成されたIPv6アドレスを利用。
  - IPv4-IPv6 変換アドレスのWell-Known Prefixは64:ff9b::/96 [RFC6052] Well-known Prefix以外も利用可能。

長崎県立大学
UNIVERSITY OF NAGASAKI

アドレッシングとDNS

Agenda

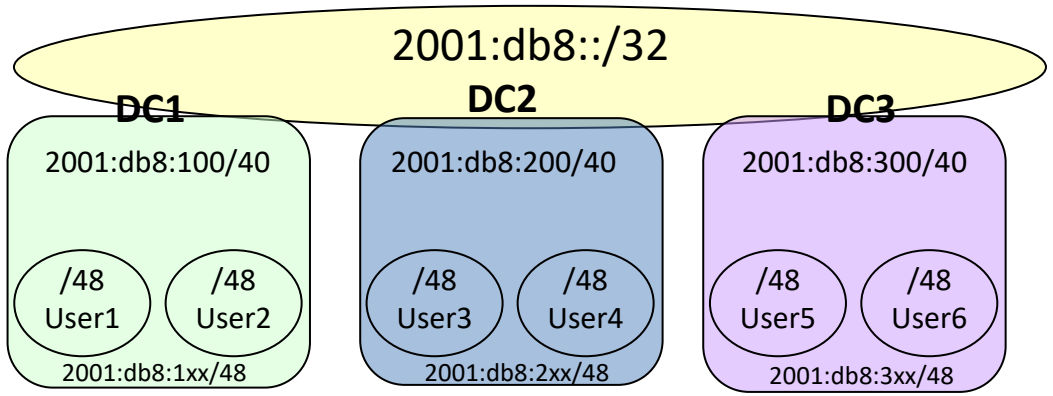
1.移行技術
2.アドレッシングとDNS
3.運用監視
4.ルーティングと冗長
5.パケットフィルタリング

長崎県立大学
UNIVERSITY OF NAGASAKI

IPv6アドレス設計

- **一般的なセグメントに対しては/64を割り当て**
  - Point-to-Pointリンクも/64でOK
    - 一部実装によっては空きアドレス宛のパケットがピンポンする場合があるので、その際にはフィルターが必要
  - Point-to-Point リンクで/64より長い Prefix を利用する提案もある [RFC6164]
- **Loopbackアドレスには/128を割り当て**
- **ISPでは、一般的な加入者に対して/64～/48を割り当て**

IPv6アドレッシング例



◆アドレスの分類方法

DCの他にもフロア、サービス、バックボーン、社内、‥といった分類も考えられる

ユーザのアドレスリナンバを許可するか否かといったポリシーも事前に決めておく

IPv6アドレス設計の基本的な考え方

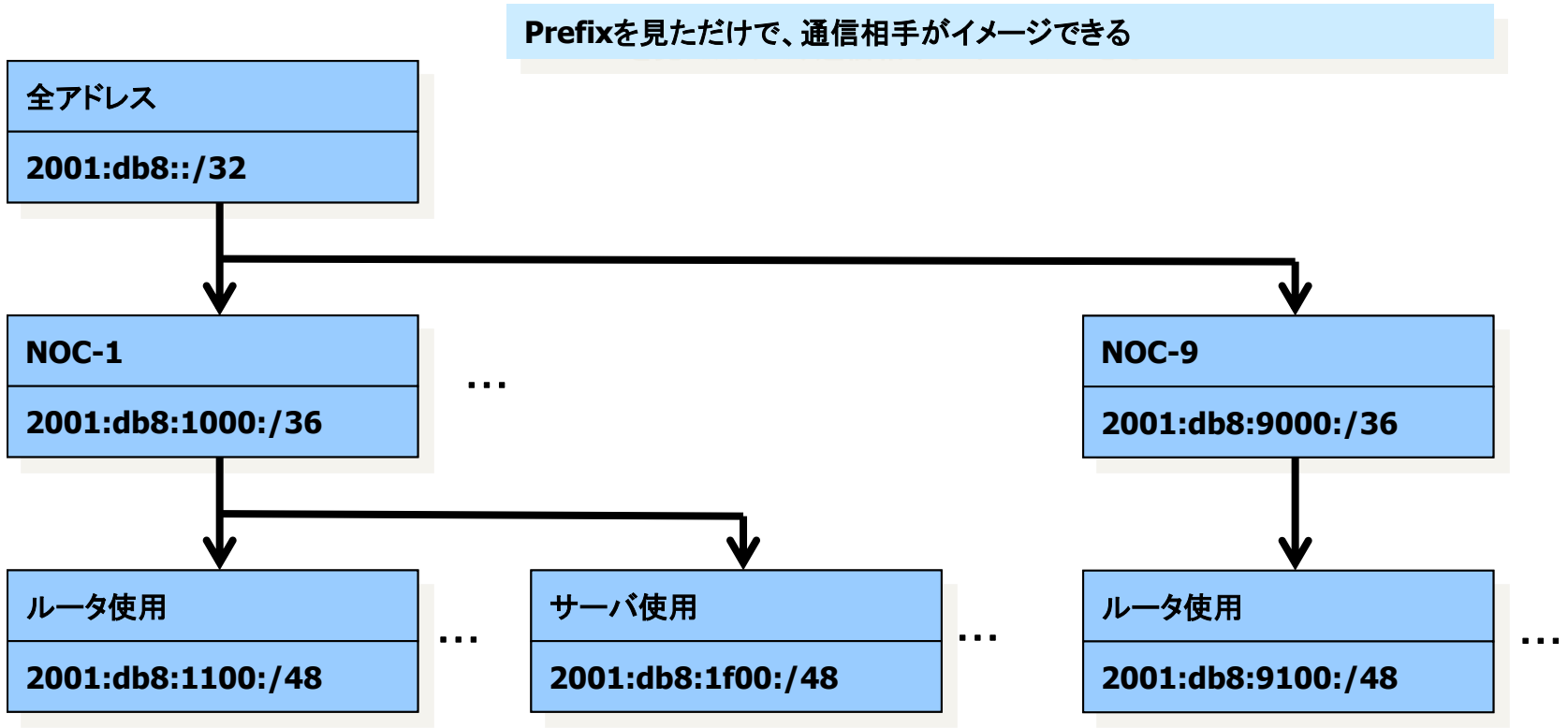
- **基本的にはIPv4と同様**
  - ◆経路集約可能であること
    - ■HWリソース(ルーティングテーブルを保持するメモリ、検索にかかるCPU処理)を最小限に
  - ◆体系化されていること
    - ■設備/端末用、ルータ間/拠点間用、組織毎等の種類により分別することで、アドレス表やACL管理負荷軽減
  - ◆拡張性があること
    - ■スペースに余裕を持たせ、将来の拡張に備える

IPv6アドレス設計の基本的な考え方

- **IPv6ではこんなことも**

  - ◆アプリやサービス毎に複数のアドレスを付与
    - ■IPv6では、端末に複数のアドレスが付与可能
    - ■アプリケーション単位でのアクセス制御、QoS制御も
      - ロ*IP*電話はこのブロック、など
  - ◆視覚判別しやすく
    - ■既存の情報(部署コードや、IPv4アドレス等)と視覚的に近づける方法も

IPv6アドレスの視覚判別



IPv6アドレスの視覚判別

- **アドレスブロックの分割は4bit毎がわかりやすい**
  - ◆ 2 0 0 1 : 0 d b 8 : 0 1 0 0 : 0 0 0 0::/40
  - ◆ 2 0 0 1 : 0 d b 8 : 0 1 1 0 : 0 0 0 0::/44

- **サブネットプレフィックス設定の工夫**
  - ◆ グローバルとリンクローカルのアドレスを見易い形で同期させる2001:db8:0:100::1 ⇒ fe80::100:1
  - ◆ OSPFエリアと合わせる
    - ■ Area 0 ⇒ 2001:db8:0::/40 , Area 3 ⇒ 2001:db8:300::/40
  - ◆ BGPのcommunityに合わせる
    - ■ community 10 ⇒ 2001:db8:1000::/40

各機器へのアドレス付与

- わかりやすいアドレスを静的に設定
  - サーバのアドレス設定例
    - <prefix>::<サービスのポート番号>
    - 2001:db8::53　(DNSサーバ)
    - 2001:db8::25　(SMTPサーバ)
    - 2001:db8::80　(WWWサーバ)
  - ルータのアドレス設定例
    - <prefix>::<上流に近い順番>
    - 2001:db8::1　(上位ルータのIF)
    - 2001:db8::5　(そのセグメントの5番目のルータのIF)
    - 2001:db8::0000:0000:0000:0001/64 (ISP側)
    - 2001:db8::0000:0000:0000:0002/64 (お客様側)

複数アドレスの付与

- **IPv6では、端末のIFに複数のアドレスを付与できるため、複数のサービスを提供する機器には複数のアドレスをつけることも可能**
  - 異なるFQDNで同じIPアドレスを参照したり、エイリアスを利用したりするのと結果は同等

```
% ifconfig -a
fxp0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1280
        inet6 fe80::206:5bff:fe3b:XXXX%fxp0 prefixlen 64 scopeid 0x1
        inet6 2001:db8:4fd::25 prefixlen 64
        inet6 2001:db8:4fd::110 prefixlen 64
        ether 00:06:5b:3b:XX:XX
        media: Ethernet autoselect (100baseTX <full-duplex>)
        status: active
```

各リンクへのアドレス設計

- **IPv4ではセグメント毎にマスク長を変更**
  - ルータ間などP2Pリンクでは/30
  - 収容NWでは端末台数に応じて/26～/28など

⇓

- **IPv6ではセグメントは/64で統一**
  - P2Pの場合でもアドレスは/64でOK
  - /127を利用することも可能
    - 但し、Subnet-Router-anycastアドレスの無効化等、幾つかの制約がある。[RFC6164 Recommendation参照]

各リンクへのアドレス設計

- **一般的なユーザに対しては/64～/48をアサイン**
- **ただ1つのサブネットが必要な場合も /64**
  - Point-to-Point リンクも /64 でOK
    - 一部実装によっては空きアドレス宛のパケットがピンポンする場合があるので、その際にはフィルターが必要
    - 別ネットワークとの境界には、/64のアドレス切り出し、設定上だけ/126にする場合もあり、それもOK
- **1つのデバイスが接続する場合には/128**
  - LoopBackアドレス等
- **安易なインタフェースアドレスを付与しない（参考）**
  - 64ビットの膨大な空間を活かす
  - ウィルスやワームの伝播を抑制する

各機器へのアドレス付与

- **クライアント端末**
  - ◆RA(Router Advertisement)で動的設定が可能

- **ルータ機器やサーバ機器**
  - ◆RAから自動生成してしまうと管理しづらい
    - ■長く複雑
    - ■NICや装置を交換するとアドレスが変わる
  - ◆わかりやすいアドレスを静的に設定
    - ■::1
    - ■::53
    - ■::443

楽しいIPv6 アドレス

```
> set type=AAAA
> www.facebook.com
サーバー:  dns-nagasaki.sun.ac.jp
Address:  10.30.5.117

権限のない回答:
名前:    star-mini.c10r.facebook.com
Address:  2a03:2880:f10f:83:face:b00c:0:25de
Aliases:  www.facebook.com

> www.netflix.com
```

Network information

IP address	2620:52:3:1:dead:beef:cafe:fed7
PTR record	no PTR record
ASN number	17314
ASN name (ISP)	Red Hat, Inc.
IP-range/subnet	2620:52:3::/48 2620:52:3:: - 2620:52:3:ffff:ffff:ffff:ffff:ffff
Network tools	Ping 2620:52:3:1:dead:beef:cafe:fed7 Tracert 2620:52:3:1:dead:beef:cafe:fed7

ノードに対するアドレス割当方式

- **ルータ**
  - リンクローカルアドレスは手動で設定する
    - 経路選択的にnexthopになることがあるため
- **サーバ**
  - スタティックで設定
- **ユーザ端末**
  - ユーザノードの管理をスタティックで行なう場合もある
  - 自動割当(RA, DHCP)

DNS（IPv6）

- **IPv6アドレスのレコードタイプはAAAA(quad A) [RFC3596]**
  - 逆引きのドメインは ip6.arpa.
    - 圧縮表記なし・・
  - NS、PTRは変更なし
- **一つのFQDNにIPv4とIPv6の両方のアドレスが設定されている場合がある**
  - リゾルバは双方のアドレスをアプリケーションに渡すか、どちらかを選択することも可能
- **DNSのデュアルスタック化とは**
  - DNSサーバがAAAAをサポートしている
  - トランスポート層にIPv6を用いることができる

DNSクエリに関する端末の挙動(2022年時点)

- **クエリ順序はOSやアプリケーションで異なる**
  - AAAAクエリを先に実施するOS
    - Windows11,Windows10、Windows XP、Linux
  - Aクエリを先に実施するOS
    - Windows Vista、Windows 7、FreeBSD、Mac OS X
- **トランスポートプロトコルの優先順位**
  - IPv6を優先的に利用するOS
    - Windows11, Windows10, 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

長崎県立大学
UNIVERSITY OF NAGASAKI

参考：フィルタリング

Agenda

1.移行技術
2.アドレッシングとDNS
3.運用監視
4.ルーティングと冗長
5.パケットフィルタリング

長崎県立大学
UNIVERSITY OF NAGASAKI

IPv6のセキュリティ

IPv6にするとセキュリティが高まる？
IPsecがあるからファイヤーウォールは要らない？

- **あらゆる端末がグローバルアドレスを持つIPv6ではファイヤーウォールは、より一層重要性は高まる**
- **一方で、ローカルアドレスをどうしても持たせたいという声のため、IPv6 ULA(Unique Local Address)というものが用意されている(fc00::/7) [RFC4864]**
  - IPv4 NAPT(IPマスカレード)と同等のセキュリティを確保可能
- **ULAをグローバルアドレス等に変換するため、IPv4のNATに相当する、NPTv6の標準化が進んでいる [RFC6296 Experimental]**

フィルタリングの基本的な考え方

- **end-to-endの通信を想定しているため端末側でしっかり守る必要がある**
- **フィルタリングの役割**
  - ◆外部からの不正なパケットの侵入を防ぐ
  - ◆基本はパケットのヘッダに記載されているアドレス・ポート番号情報で振り分けているに過ぎない
  - ◆パケットを通過/破棄するかを、何らかの基準で判断する
- **実装方法**
  - ◆ファイヤーウォール装置（SPI対応）
  - ◆ルータ機器でのパケットフィルタリング
  - ◆端末でのパーソナルファイヤーウォール

フィルタリングポリシーの例

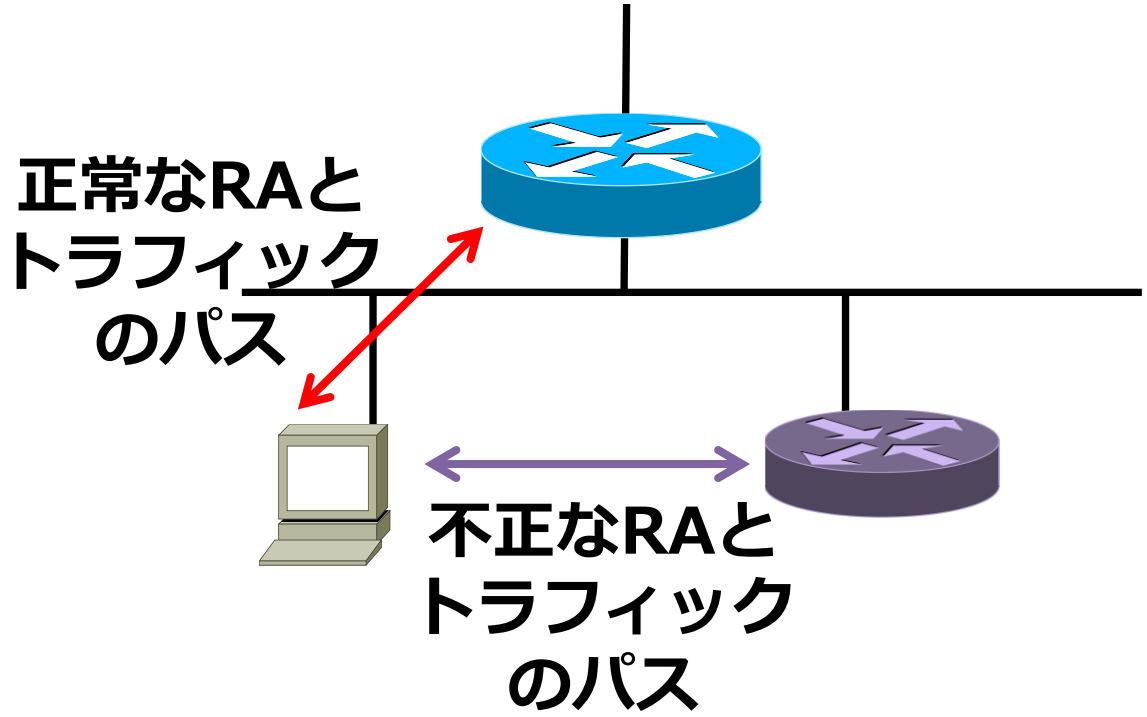
- **サービス毎にIPv4とIPv6でポリシーを整合させる**
  - 内部→外部
    - ■サーバ/端末から外部へ向けた通信は許可
  - 外部→内部
    - ■確立済みTCPコネクションは通過
    - ■サービス用通信は通過(DNS/WEB/MAIL/NTP など)
- **ICMPv6 type 1,2,3を通過**

Type 1: Destination Unreachable
Type 2: Packet Too big
Type 3: Time Exceeded

- **同一リンク内**
  - NDPなどの通信に不可欠なリンクローカルアドレス同士の通信を許可する
  - 不正RAをフィルタする

不正RAのフィルタ

- 不正なRAが送信されてしまうとトラフィックが誘導されて盗聴が可能となってしまう為、フィルタを行う。



ICMPとICMPv6

- **IPv4では**
  - ◆セキュリティ上の理由からICMPを通らないようにしている場合もある
- **IPv6では**
  - ◆ ICMPv6は通信上重要な役割を果たすため、特定のICMPv6パケットを通過させることが重要
    - ■ 終点到達不能（Destination Unreachable）　（Type = 1）
    - ■ パケット過大（Packet Too Big）　（Type = 2）
    - ■ 有効期間超過（Time Exceeded）　（Type = 3）

- **Recommendations for Filtering ICMPv6 Messages in Firewalls [RFC4890]**

ICMP6を「対外通信・内部通信」と「必須・オプション」に分けて考える

Message	対外：必須	対外：Option	対外：不要	LL：必須	LL：Option	LL：不要
Destination Unreachable	◎			◎		
Packet too Big	◎			◎		
Time Exceed	◎			◎		
Parameter Problem	◎			◎		
Echo Request		◎			◎	
Echo Reply		◎			◎	
Router Solicitation			◎	◎		
Router Advertisement			◎	◎		
Neighbor Solicitation			◎	◎		
Neighbor Advertisement			◎	◎		
Node Information Query		◎			◎	
Node Information Reply		◎			◎	
Inverse Neighbor Discovery Solicitation			◎	◎		
Inverse Neighbor Discovery Advertisement			◎	◎		

ip6tablesの例

- **Serverであることが想定されるので、LinkLocalの表を元に作成**
  - Mobile IPv6のHome Agentではない事を想定

```
# Approve certain ICMPv6 types and all outgoing ICMPv6
-A INPUT -p icmpv6 -j ICMPv6
-A ICMPv6 -p icmpv6 --icmpv6-type destination-unreachable -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type packet-too-big -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type time-exceeded -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type parameter-problem -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type echo-request -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type echo-reply -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type 130 -s fe80::/10 -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type 131 -s fe80::/10 -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type 132 -s fe80::/10 -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type router-solicitation -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type router-advertisement -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type neighbour-solicitation -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type neighbour-advertisement -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type redirect -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type 139 -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type 140 -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type 141 -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type 142 -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type 143 -s fe80::/10 -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type 151 -s fe80::/10 -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type 152 -s fe80::/10 -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type 153 -s fe80::/10 -j ACCEPT
-A ICMPv6 -j RETURN
-A OUTPUT -p icmpv6 -j ACCEPT
```

Router Access-listの例

- いわゆるNetwork FWであることが想定されるので「対外」を利用

```
!
flow detection out mode layer3-3-out
# IPv6 & ICMP の ACL を設定するには H/W リソースの設定が必要
(egress用)
flow detection mode layer3-5
# IPv6 & ICMP の ACL を設定するには H/W リソースの設定が必要
(ingress用)
!
ipv6 access-list FILTERv6
 10 permit ipv6 any fe80::/10
 20 deny ipv6 ::/8 any
 30 deny ipv6 fec::/10 any
 40 deny ipv6 fc00::/7 any
 50 deny ipv6 2001:db8::/32 any
 60 deny ipv6 ff00::/8 any
 101 permit icmp any any unreachable
 102 permit icmp any any packet-too-big
 103 permit icmp any any time-exceeded
 104 permit icmp any any parameter-problem
 105 permit icmp any any echo-request
 106 permit icmp any any echo-reply
 107 permit icmp any any router-solicitation
 108 permit icmp any any router-advertisement
 109 permit icmp any any nd-ns
 110 permit icmp any any nd-na
 111 permit icmp any any 137
 112 permit icmp any any 139
 113 permit icmp any any 140
 114 permit icmp any any 141
 115 permit icmp any any 142
 130 permit icmp fe80::/10 any mld-query
 131 permit icmp fe80::/10 any mld-report
 132 permit icmp fe80::/10 any mld-reduction
 143 permit icmp fe80::/10 any 143
 151 permit icmp fe80::/10 any 151
 152 permit icmp fe80::/10 any 152
 153 permit icmp fe80::/10 any 153
 1000 deny ipv6 any any
!
interface range gigabitethernet 0/1-2
 ipv6 traffic-filter FILTERv6 in
!
# 上記フィルターを GbE Port 0/1〜2 の Ingress に適用
```

フィルタリングポリシーの例

- **サービス毎にIPv4とIPv6でポリシーを整合させるべき**
  - 内部→外部
    - サーバ/端末から外部へ向けた通信は原則許可
  - 外部→内部
    - 確立済みTCPコネクションは通過
    - サービス用通信は通過(DNS/WEB/MAIL/NTP など)
  - サービスネットワークの保護ならば Default を Deny にしておくべき

- **EDNS0やTCP53も通す**
  - IPv6ではDNS回答パケットが大きくなりがちなため

- **ICMPに関しては、IPv4 と IPv6 でポリシーが異なる**

- **同一リンク（各サーバーに設定する）**
  - できる限り不要な通信は通さない

IPv4 との違い

- **ARPとND**
  - ◆ 同一Link(Broadcast Domain)に存在するNodeと通信するための情報
    - IPv4 Address ←→ MAC Address の対応表　：　ARP (Address Resolution Protocol)
    - IPv6 Address ←→ MAC Address の対応表　：　ND (Neighbor Discovery)
  - ◆ ARPはIPv4 Broadcast/個別プロトコルを利用して実装されている
  - ◆ NDはIPv6 Multicast/ICMPを利用して実装されている
  - ◆ Security的には、ARP Spoofingと同様ND Spoofingが可能
    - arpwatchと同様にNDMonを用いて監視するのが良い

- **LinkLocal Addressの扱い**
  - ◆ IPv4では、Linklocal Addressはほとんど利用されない
    - WindowsやMacOS-Xで「DHCP等でアドレスが解決されない時に割り当てられることがある」
  - ◆ IPv6では、必ずLinkLocal Addressが割り当てられる
    - LLAddrを利用して、ssh等で接続することも可能
    - Global Addressを持つ必要がないNetworkにはLL Addrを割り付けるだけで良い
    - Hop-by-Hopで接続することで、運用の工数を軽減することが可能
    - ICMP6 Neighbor DiscoveryのOptionにNeighbor whoisがあるので、これを利用すれば近隣のノード名を特定することが可能（しかし、Linuxなどでは、この機能は使えなくなっている）

IPv4との違い その他

- **ジオロケーション**
  - ◆IPv4とことなり、地域vsIPアドレスのデータベースの整備が若干弱い
- **フィルタリングデータベース等**
  - ◆SPAMHause,他、データベースの精度に難点
  - ◆そもともIPv6を対象としていない場合も
  - ◆商用サービスは概ねOK

まとめ

セッション1　IPv6概要

- IPv6の主な機能や特徴
  - IPv6アドレスの表記方法
  - IPv6アドレスタイプと通信形態（Unicast, Anycast, Multicast）
- ICMPとアドレス自動設定
  - Path MTU Discovery
  - NDP（近隣探索）プロトコル：NS/NAとRS/RA
  - RA/SLAACとDHCPv6

セッション2　v6導入のための設計・構築・運用

- 移行技術
- アドレッシングとDNS
- パケットフィルタリング

IPv4アドレス枯渇対応タスクフォース
IPv6セミナー教材執筆者一覧

（2016年8月更新）

高津　智明	三井情報株式会社
佐藤　秀樹	一般社団法人日本ネットワークインフォメーションセンター
清水　一貴	ジュニパーネットワークス株式会社
西塚　要	NTTコミュニケーションズ株式会社
馬渕　俊弥	ビッグローブ株式会社

（前版までの履歴）

芦田　宏之	BBIX株式会社
井上　一清	株式会社IDCフロンティア
鹿志村　康生	日本アルカテル・ルーセント株式会社
川島　誠一	シスコシステムズ合同会社
川島　正伸	NECアクセステクニカ株式会社
北口　善明	金沢大学
國武　功一	株式会社ブロードバンドタワー
高津　智明	三井情報株式会社
佐藤　晋	一般社団法人日本ネットワークインフォメーションセンター
土本　康生	東京大学
友松　和彦	アリス・グループ・ジャパン株式会社
仲西　亮子	三井情報株式会社
服部　亜紀子	シスコシステムズ合同会社
廣海　緑里	株式会社インテック
藤崎　智宏	日本電信電話株式会社
許　先明	株式会社ブロードバンドタワー
三川　荘子	NTTコミュニケーションズ株式会社
安田　歩	NTTコミュニケーションズ株式会社