IPv6チュートリアル
～IPv6化ことはじめ～
ネットワーク編

Internet Week 2018 S4

西塚要
NTTコミュニケーションズ株式会社

JPNIC技術セミナー

- https://www.nic.ad.jp/ja/tech/seminar/
  - 座学 エンジニア向けIPv6技術解説

本来であれば座学および実機演習を組み合わせて2日間を使いたい内容を凝縮し、 2.5時間の座学で効率良く学ぶことができるセッションです。

IPv6の現状

IPv6仕様の再整理
- RFC8200 (2017/7)

仕様の変更のきっかけとなる外部環境の変化
- 有線から無線へ。メディア/端末の変化への対応
  - IoTデバイスへの対応も含まれる
- IPv4からの移行
  - IPv4 as a Service の技術・運用

新技術への期待
- SRv6(IPv6 Segment Routing)

目次

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
3.アドレッシング

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

Happy eyeballs (RFC6555)

- フォールバックを緩和するための仕組み。
- IPv4とIPv6のうち、通信状態の良いほうを優先。
- 通信開始当初からIPv6とIPv4両方のプロトコルを使って接続を行い、先に成功したほうを利用。
- これにより、一方が失敗してから他方を開始するより切替時間短縮される。

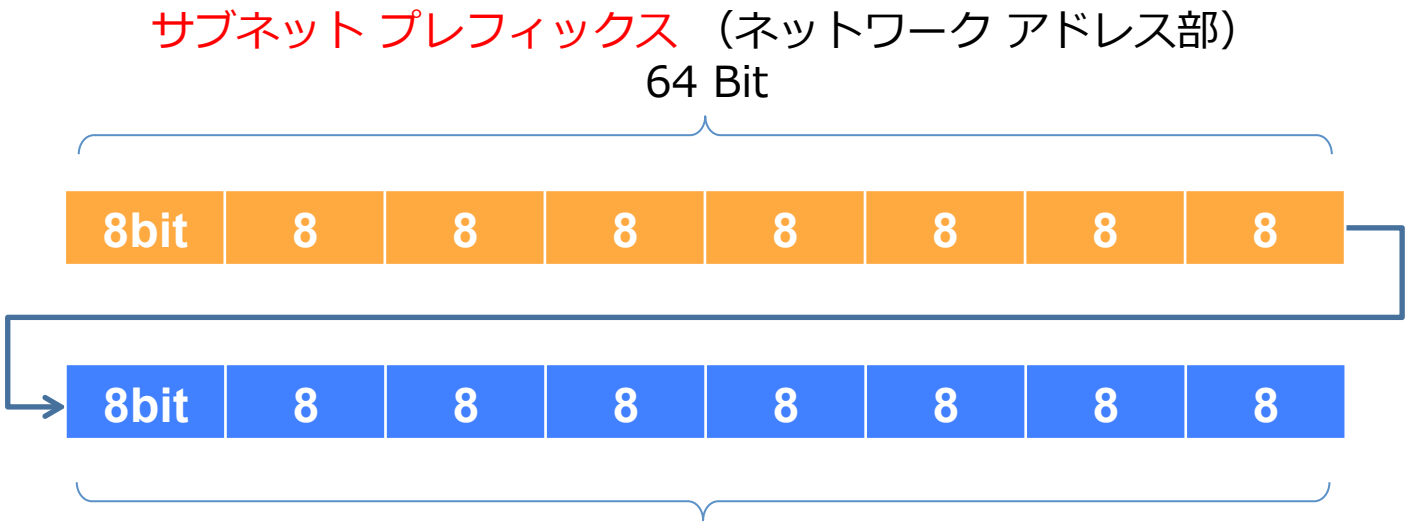
Happy eyeballs v2 (RFC8305)

- Happy Eyeballs version2では、AとAAAAのクエリを実行してから、コネクションの確立を行うまでに、他方のDNSクエリに対して待ち時間を持たないことを推奨。
- AAAAレコード（IPv6）の応答が先にあった場合は、即座にコネクションを確立し、Aレコード(IPv4)の応答が先にあった場合は、AAAAの応答の待ち時間を50msもつ事を推奨。

IPv4　vs　IPv6 Address

IPv4
32bit

IPv6
128bit



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。

  0010000000000001000011011011100000000000000000000000000000000000000000000000000010000001100010100111111111111111100001111001001000001011 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

例題

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

○ 2001:db8::fff0:0:0:f

・ダメな例

X 2001:db8::fff0::f →元のアドレスに再現不可能

△ 2001:db8:0:0:fff0::f→推奨表記ではない

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

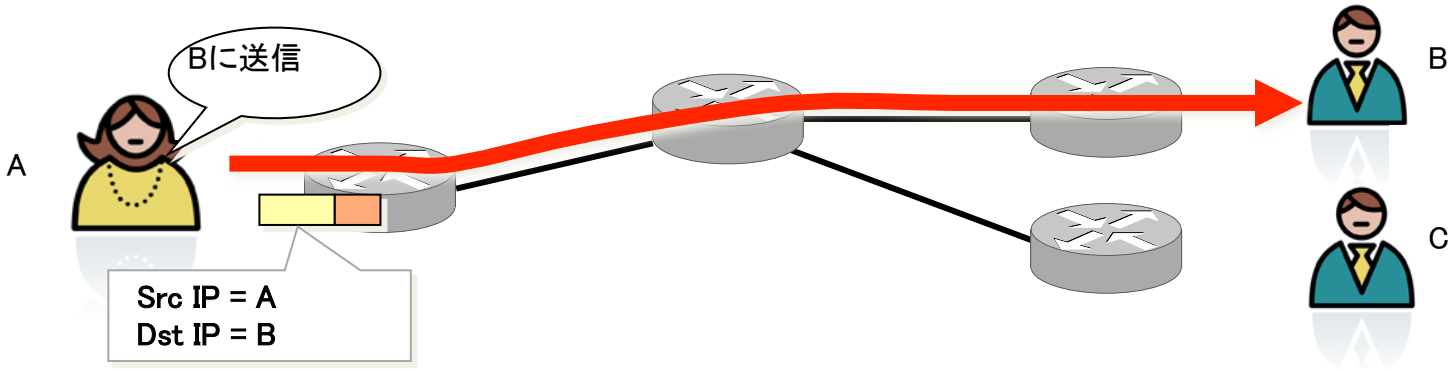
Group: インターフェースの集合

※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

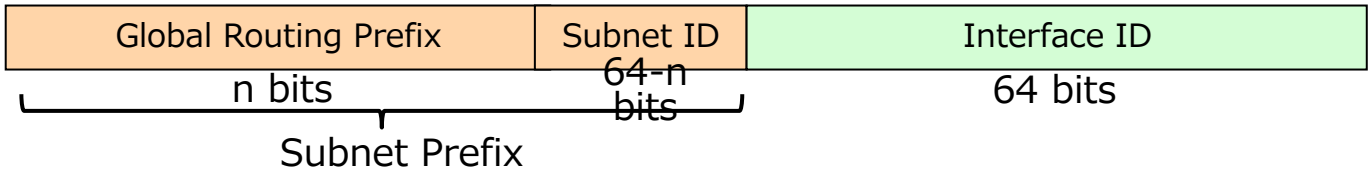


ユニキャストアドレス

- グローバルユニキャストアドレス 下記以外
  (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
- 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
- その他、特定用途のアドレス

ユニキャストアドレス (1)

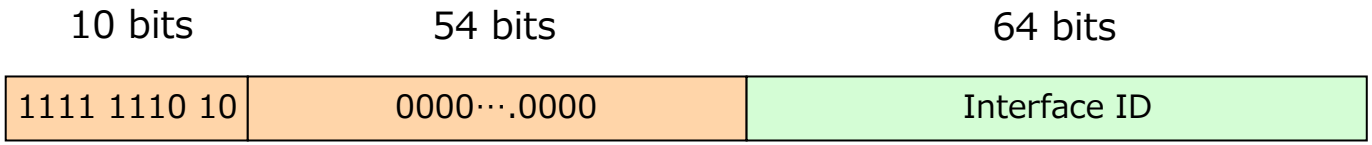
- グローバルユニキャストアドレス
  - 現在は 2000::/3 のアドレス空間を使用中
    - [RFC3587]（IPv6 Global Unicast Address Format）
  - Global Routing Prefix
    - RIR もしくは NIR、LIR より割り当てられる
  - Subnet ID
    - サイト内でサブネットの識別に使用
  - Interface ID
    - サブネット内のインタフェース識別に使用



  - 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)

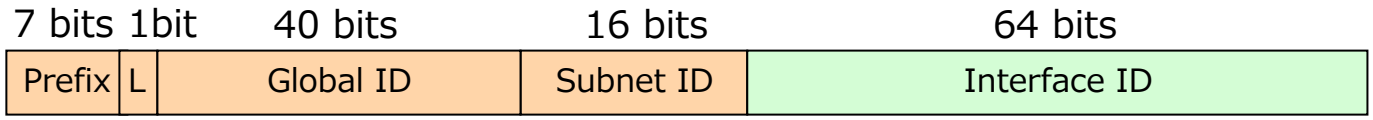
ユニキャストアドレス (2)

- 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



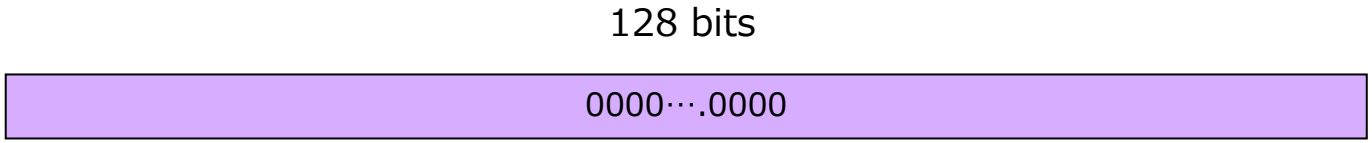
ユニキャストアドレス (3)

- 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



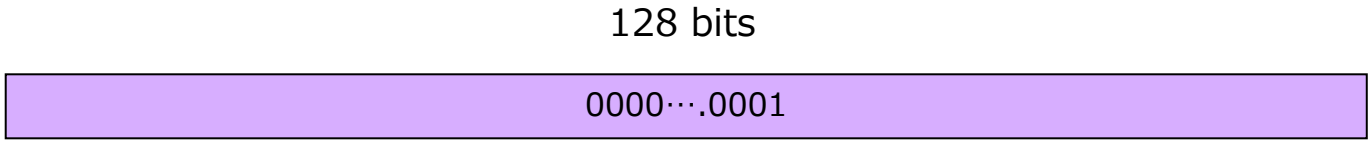
ユニキャストアドレス (4)

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



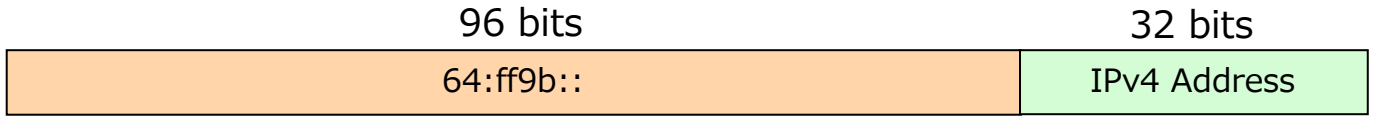
  - デフォルトルート(::/0) 0.0.0.0/0に相当

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



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



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

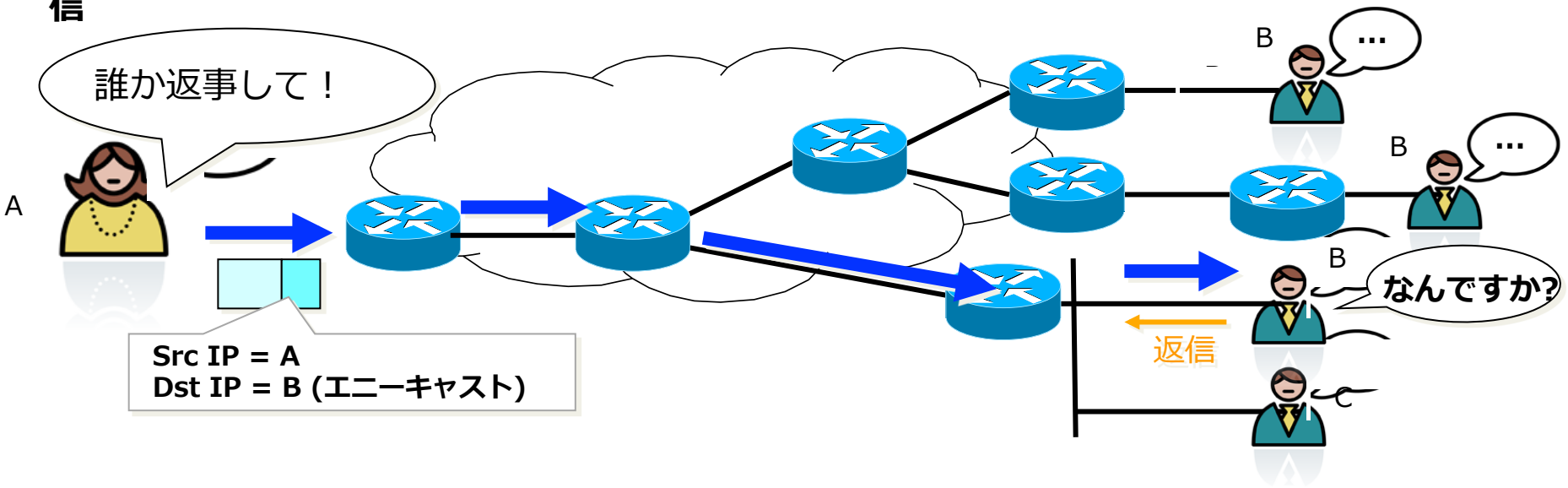
Group: インターフェースの集合

※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

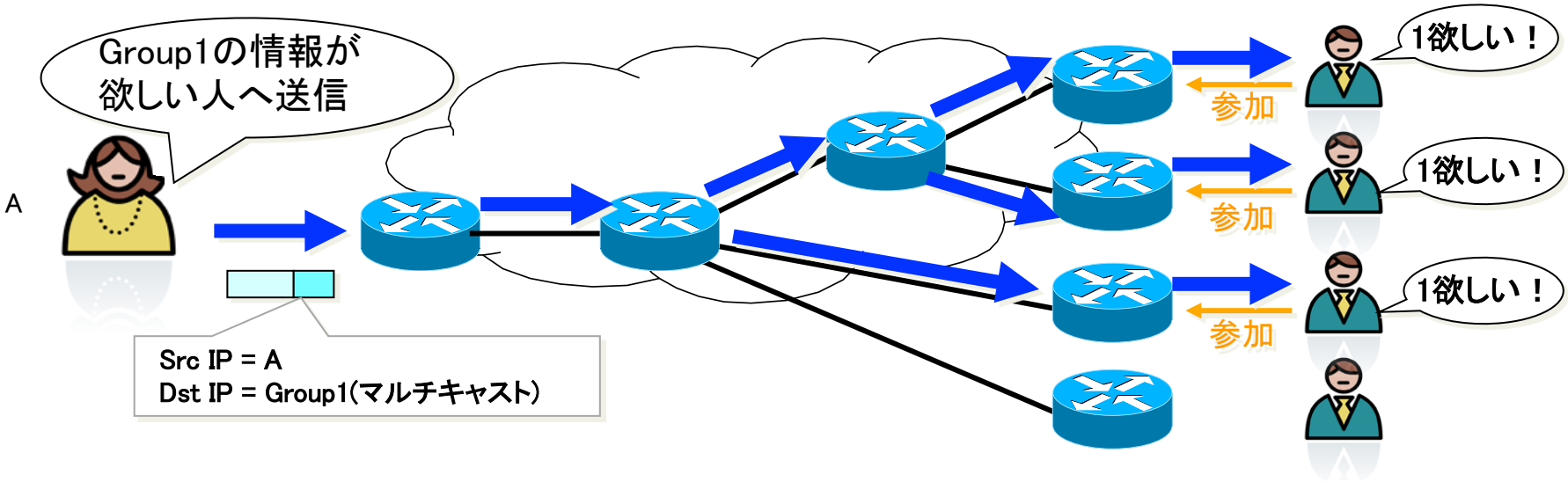
Group: インターフェースの集合

※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

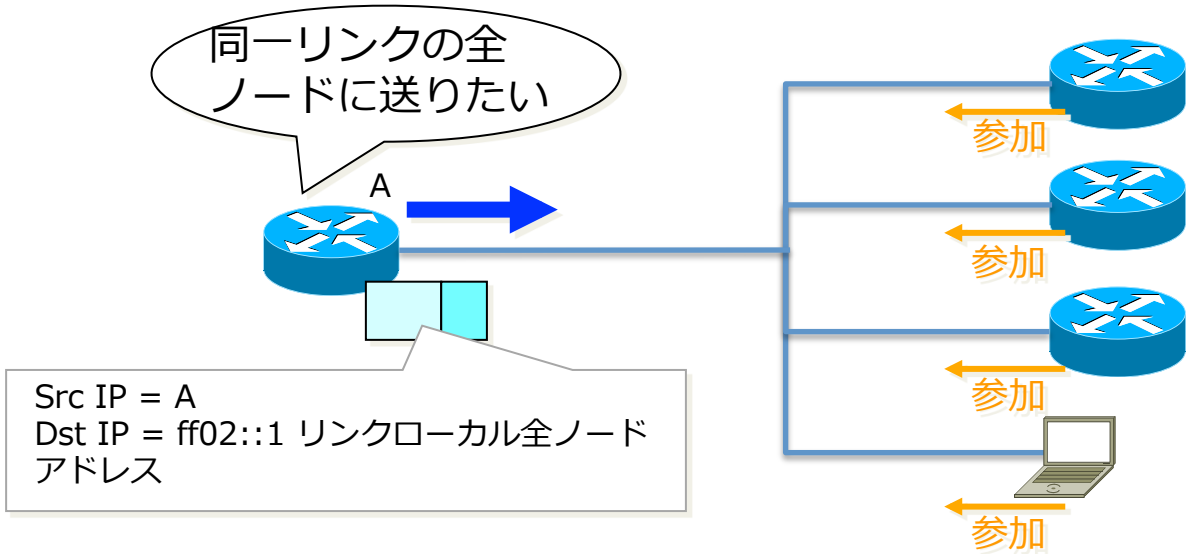
マルチキャスト通信

◆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



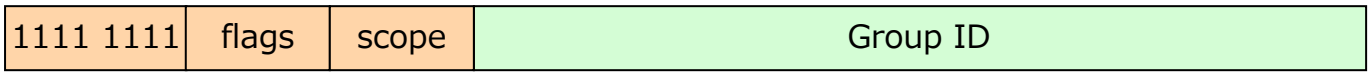
マルチキャスト通信
(リンクローカル・スコープ)

◆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 (1)

- ff00::/8
- 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 = 8 : Organization-local
  - Scope = e : Global scope

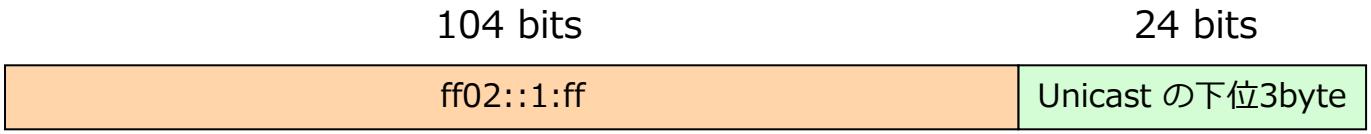


マルチキャストアドレス (2)

- 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

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（ff02::1:ff00:0/104）
  - Solicited Node Multicast Address
  - 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

IPv4 EXHAUSTION

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
3.アドレッシング

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 [RFC1981]
  - 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

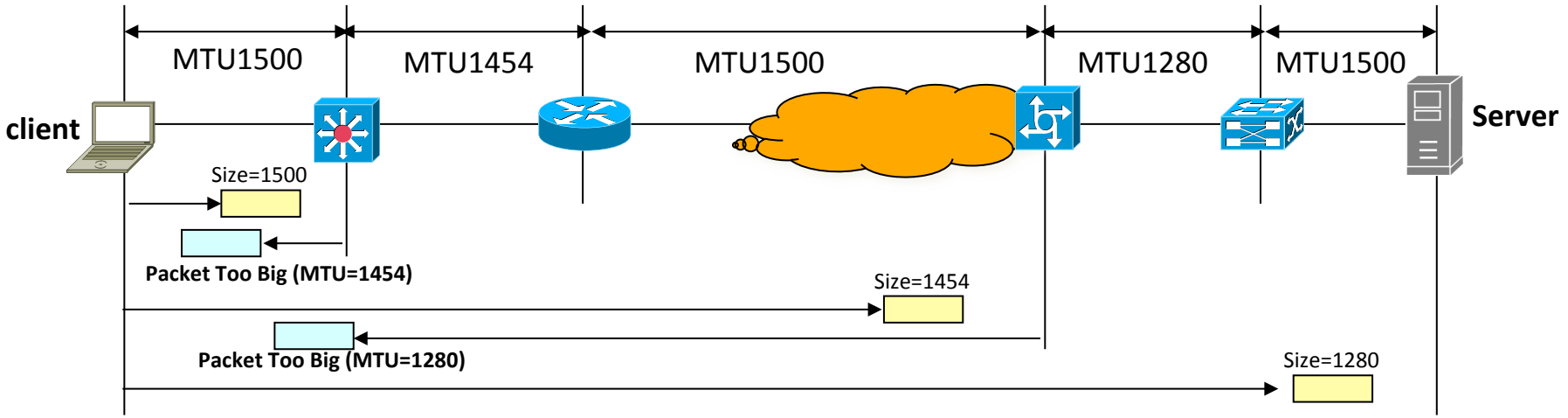
- **ICMP Error Message（type 0～127）**
  - Destination Unreachable（type 1）
  - **Packet Too Big（type 2）** → **Path MTU Discovery**
  - Time Exceeded（type 3）
  - Parameter Problem（type 4）

- **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）** → **Neighbor Discovery(近隣探索)**
    アドレス自動設定
  - Redirect Message (type137)

33

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



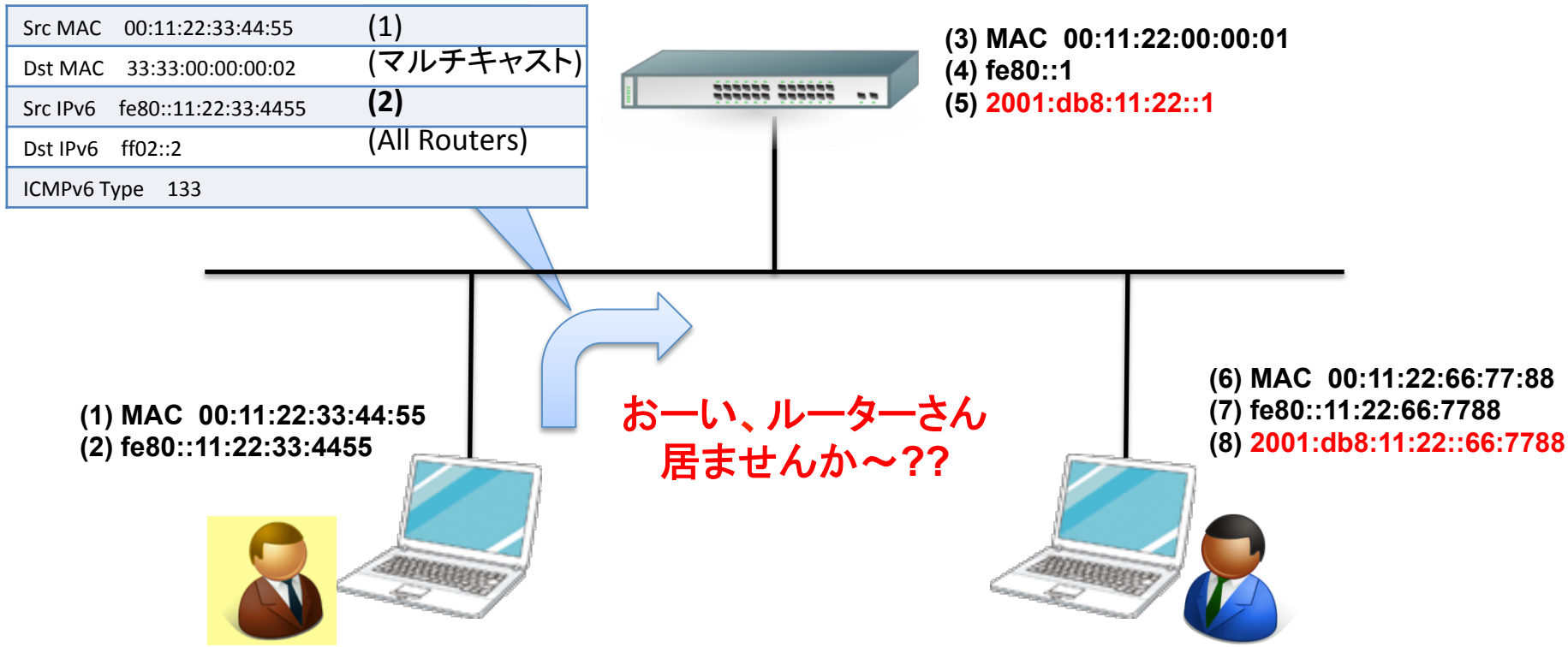
NDP (近隣探索)プロトコル

■ 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）

RS ルータ要請

宛先アドレスには、All Routersアドレス（マルチキャスト）を使います



RA ルータ広告

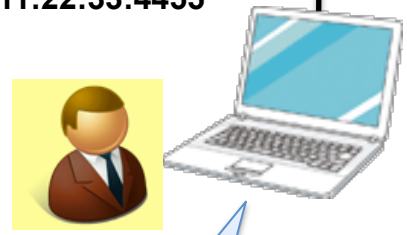
RS に返信する場合は、宛先アドレスにユニキャスト アドレスを使います

Src MAC 00:11:22:00:00:01	(3)
Dst MAC 33:33:00:00:00:01	(マルチキャスト)
Src IPv6 fe80::1	**(4)**
Dst IPv6 ff02::1	(All Nodes)
ICMPv6 Type 134 Prefix Length 64 Prefix 2001:db8::	

(3) MAC 00:11:22:00:00:01
(4) fe80::1
(5) 2001:db8:11:22::1

僕ルーターです
プレフィックスはこれだよ!!

(1) MAC 00:11:22:33:44:55
(2) fe80::11:22:33:4455



(6) MAC 00:11:22:66:77:88
(7) fe80::11:22:66:7788
(8) 2001:db8:11:22::66:7788

ふむ
ふむ

2001:db8::/64 ね
デフォルト ゲートウェイは
fe80::1 だな!!

RAの機能

- RAによって通知できる主な情報
  - Defaultルータの情報(link-local address, Link-layer address)
  - ノードが用いるHop limit
  - DHCPの使用　(M-flag:アドレス設定に使用 / O-flag:それ以外の情報の設定に使用)
  - RouterのLifetime (利用可能期間)
  - そのリンクで使用可能なPrefix情報(prefix,prefix length, lifetime)
  - DNS情報 [RFC6106]
- DRP（Default Router Preference[RFC4191]）によってデフォルトルータの優先度の通知が可能
  - High（01）、Medium（00）、Low（11）
  - ノード、ルータ双方がサポートしている必要がある

38

NDP (近隣探索)プロトコル

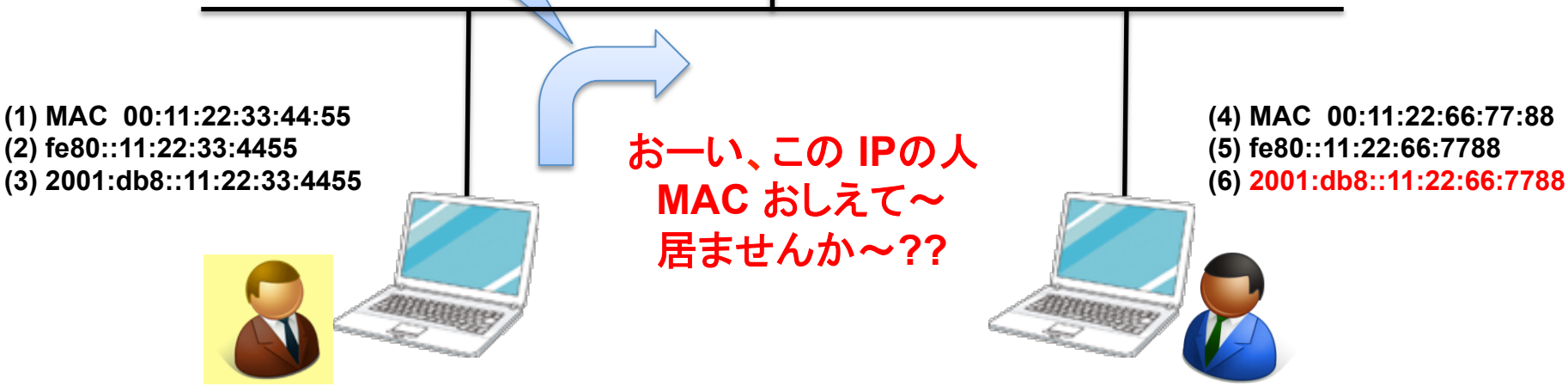
■ 5つのメッセージタイプ（ICMPv6機能の一部）

- 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

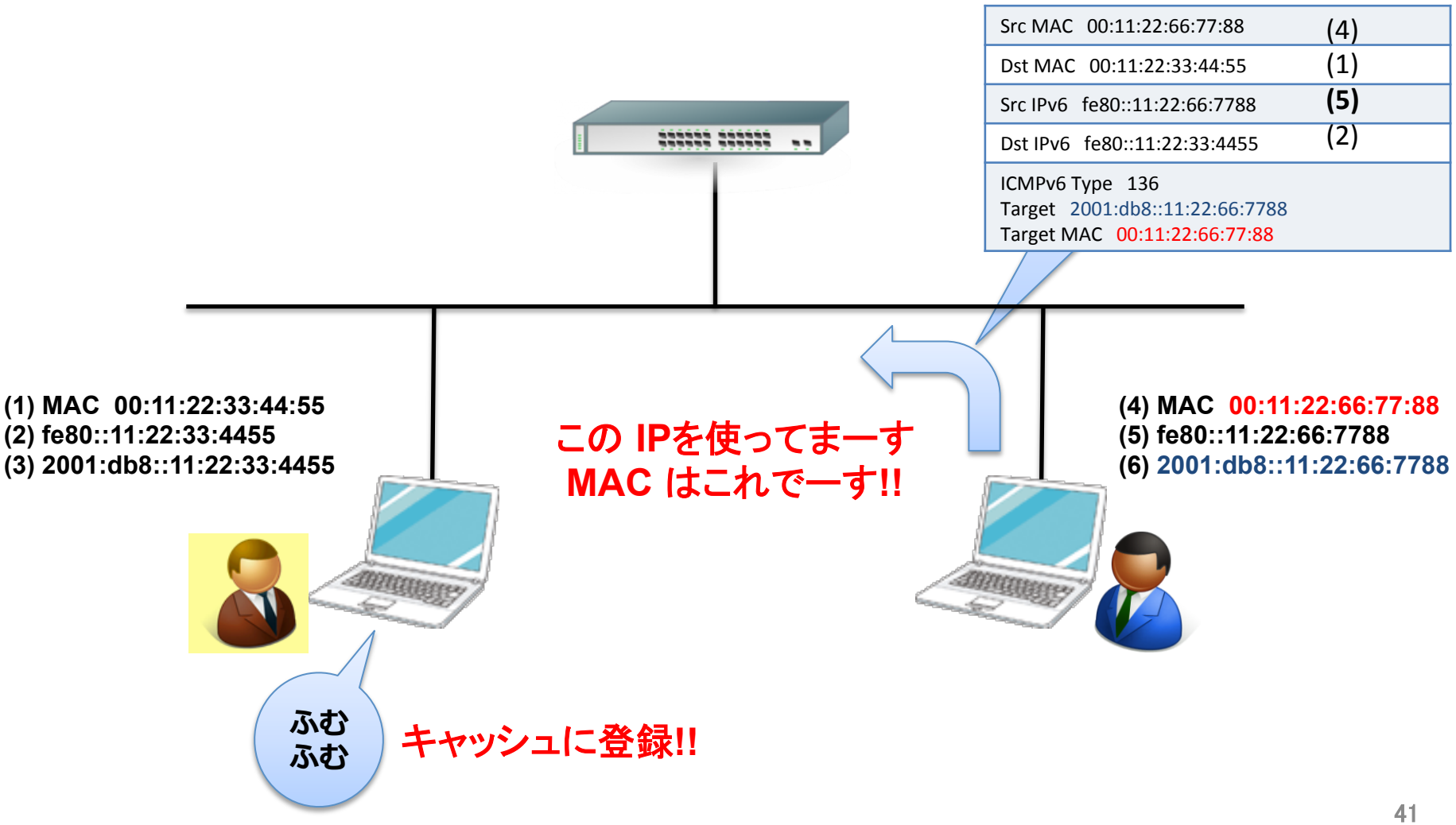
宛先アドレスには、要請ノードアドレス（マルチキャスト）を使います

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	

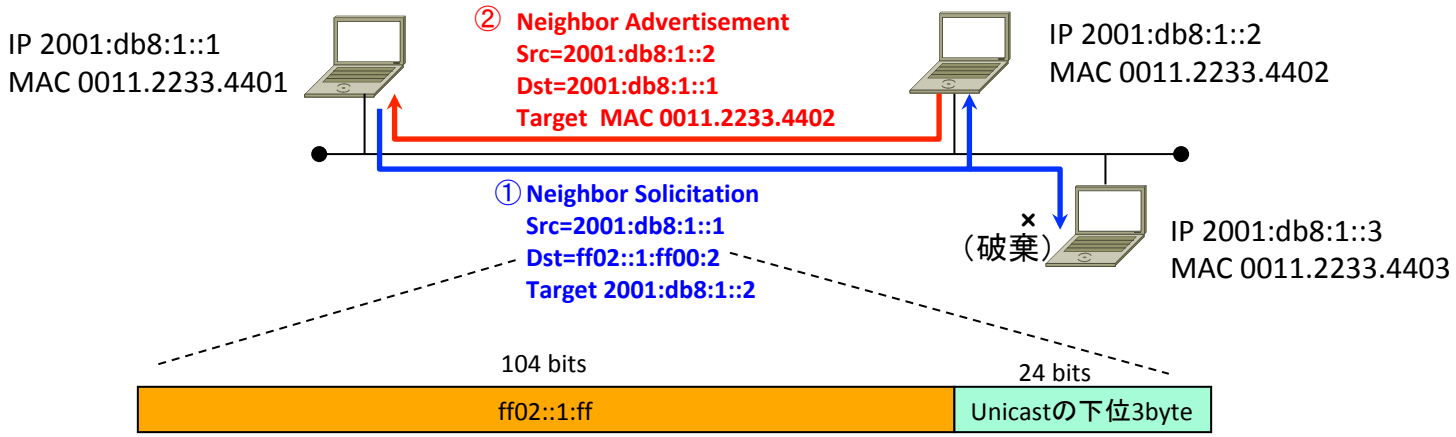


相手先 2001:db8::11:22:66:7788
と通信したい…..
けど相手の MAC アドレスを知らない
（存在しないかもしれない!?）

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!!

要請ノードマルチキャスト (NS / NA で使う)



2001:db8:1::0000:0002 (2001:db8:1::2)

↓

ff02::1:ff00:0002 (ff02:1::ff00:2)

要請ノードマルチキャストアドレス

Multicast AddressとEthernet Addressの関係

ff02::1:ff00:0002 (ff02::ff00:2)

(Dst Ethernet Address) 33:33:ff:00:00:02

※"33:33"にMulticastの下位4byteを連結

DAD

- 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

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

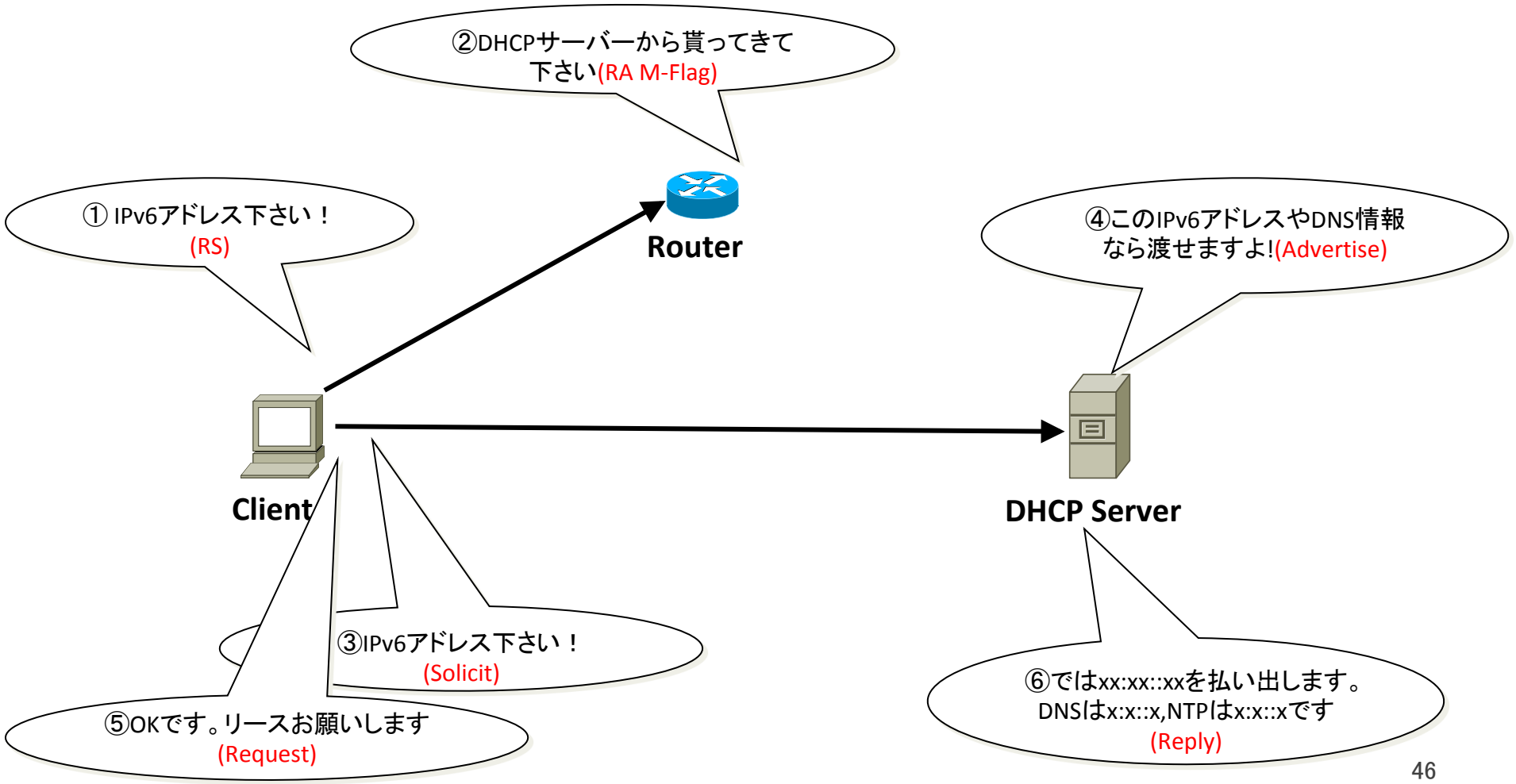
- DHCPv6（Dynamic Host Configuration Protocol for IPv6）[RFC3315]
  - ステートフルなアドレスの自動設定
  - Default Gateway が通知されない
    - RAと組み合わせて使う前提
  - その他の機能は IPv4 の DHCP とほぼ同じ

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
  - DHCPv6-PD [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 (Home GateWay) は、RA または DHCPv6 を使用して再配布

- Stateless DHCPv6 (DHCPv6-lite) [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

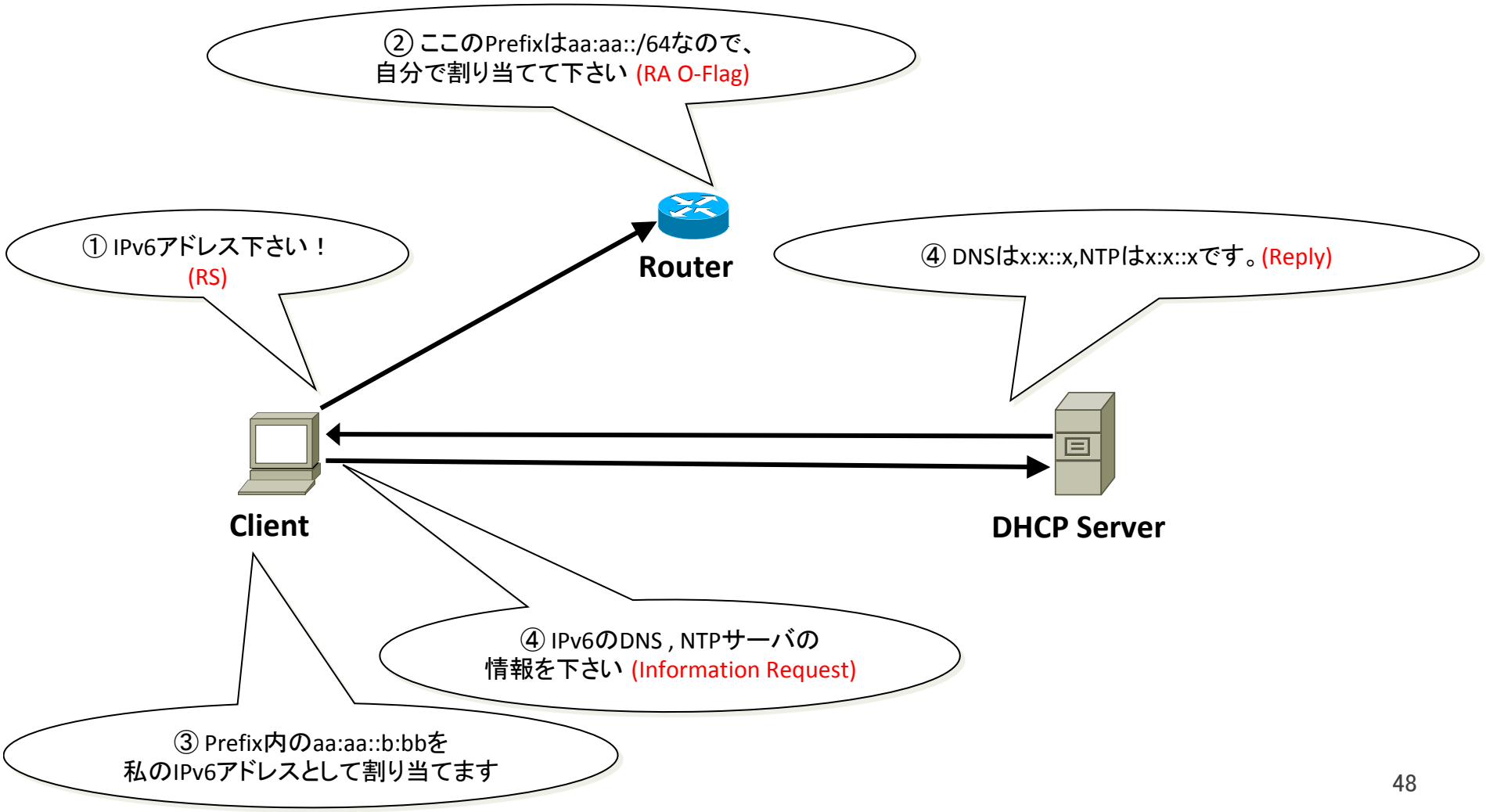
Stateful DHCPv6



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

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。

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 [RFC6106] で標準化された

RA v.s. 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 [RFC6106]

- 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

IPv4 EXHAUSTION

アドレッシング

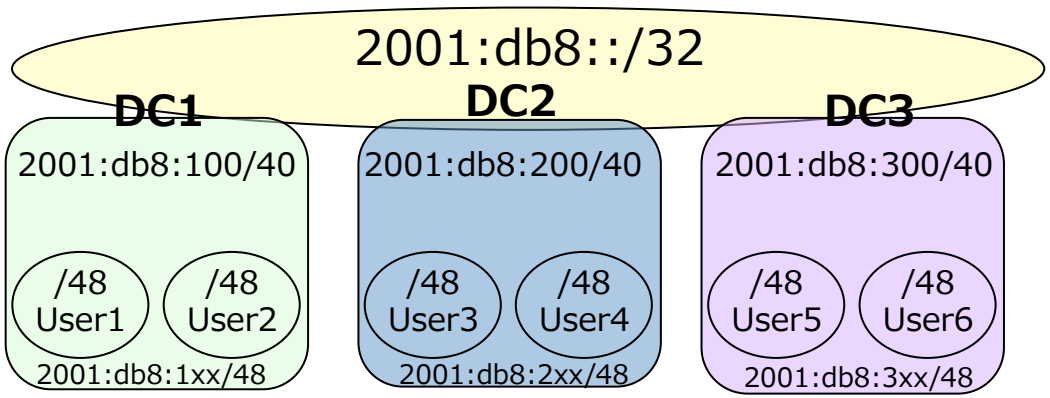
Agenda

1.IPv6の主な機能や特徴
2.ICMPとアドレス自動設定
3.アドレッシング

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

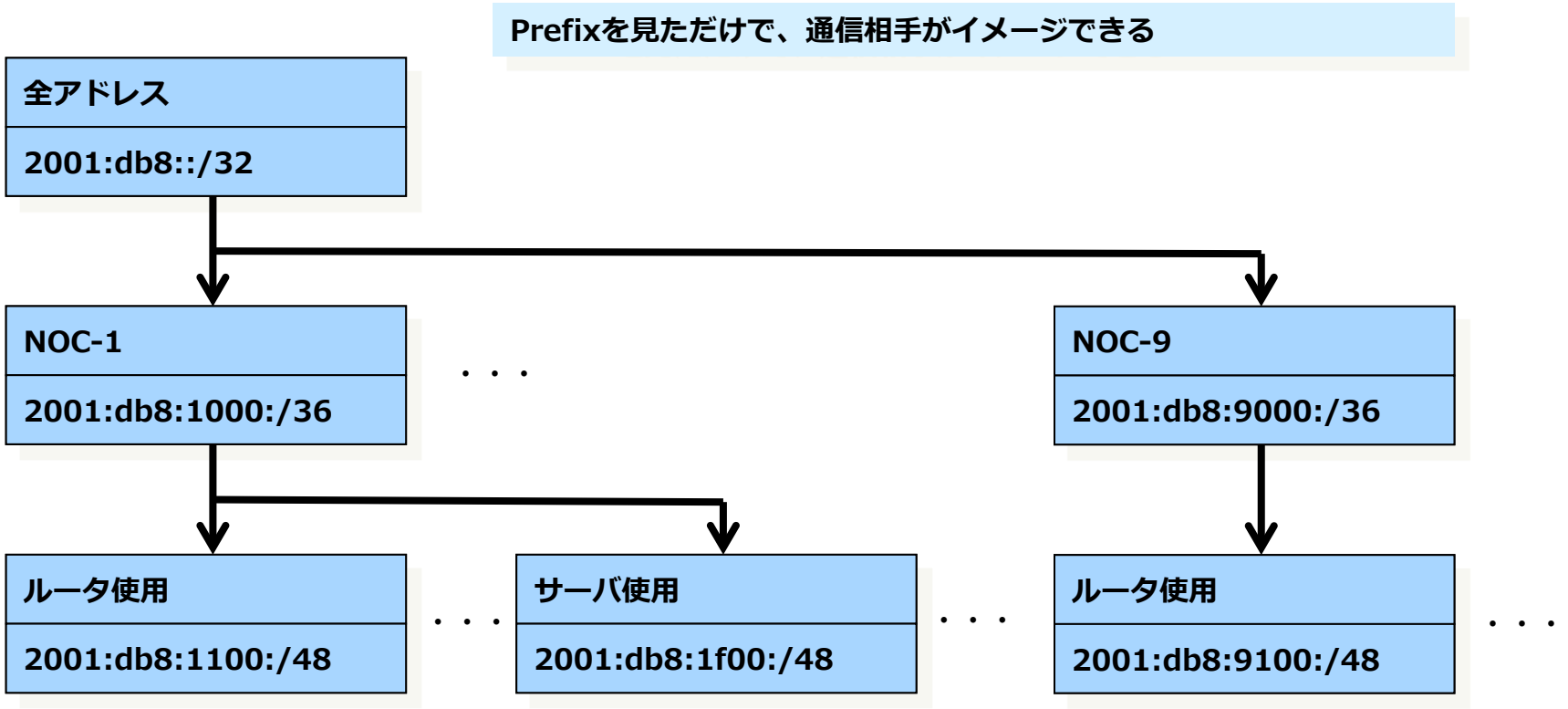
ユーザのアドレスリナンバを許可するか否かといったポリシーも事前に決めておく

54

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アドレスの階層化と視覚判別



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
      - IP電話はこのブロック、など
  - より視覚判別しやすく
    - 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

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

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)

つまづきやすい! 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)
- ARPはIPv4 Broadcast/個別プロトコルを利用して実装されている

- IPv6 Address ←→ MAC Address の対応表：ND (Neighbor Discovery)
- NDはIPv6 Multicast/ICMPv6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

つまづきやすい! IPv4 との違い

- Link Local 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
  - 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