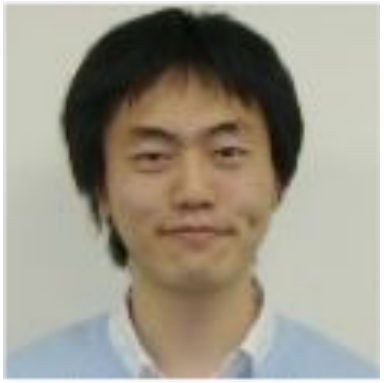
IPv6チュートリアル
～IPv6化ことはじめ～

Internet Weekショーケース in 仙台
西塚要 @__kaname__
(NTTコミュニケーションズ株式会社
/JPNIC IPv6教育専門家チーム)

自己紹介

- 2006年 NTTコミュニケーションズ入社
  - OCNアクセス系ネットワークの設計に従事した後、大規模ISP向けのトータル保守運用サービスを担当
- メインフィールド
  - トラフィック分析
  - DDoS対策ソリューション
  - IPv4枯渇対策関連技術
- IETF提案活動
  - DOTS WG (DDoS対策)
- JPNIC「IPv6教育専門家チーム」



本日のコンテンツについて

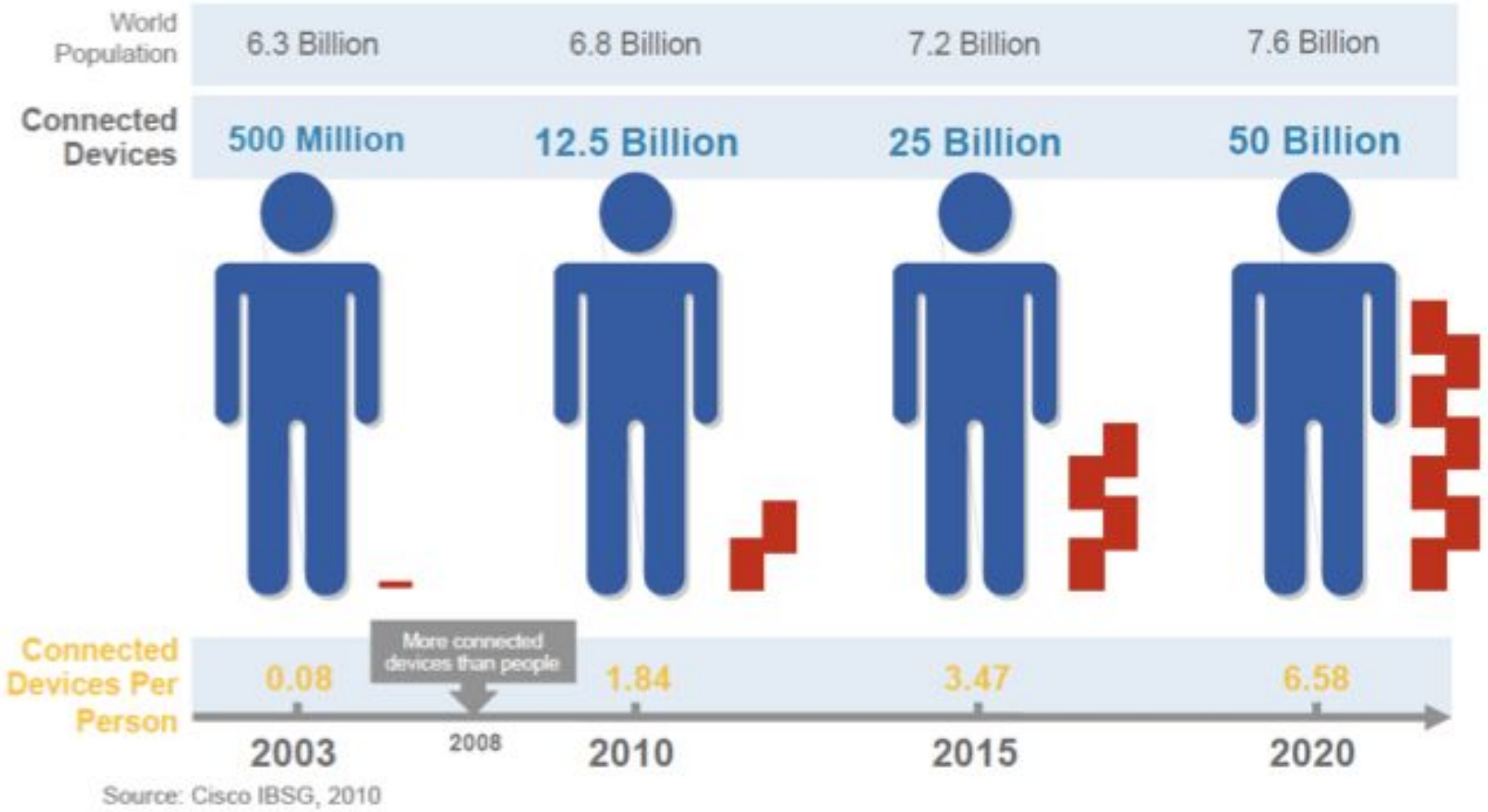
- JPNIC技術セミナー
  - エンジニア向けIPv6技術解説
  - https://www.nic.ad.jp/ja/tech/seminar/
  - 座学および実機演習を組み合わせて2日間

- 本日のコンテンツ
  - 50分の座学に凝縮してエッセンスをお伝えします。

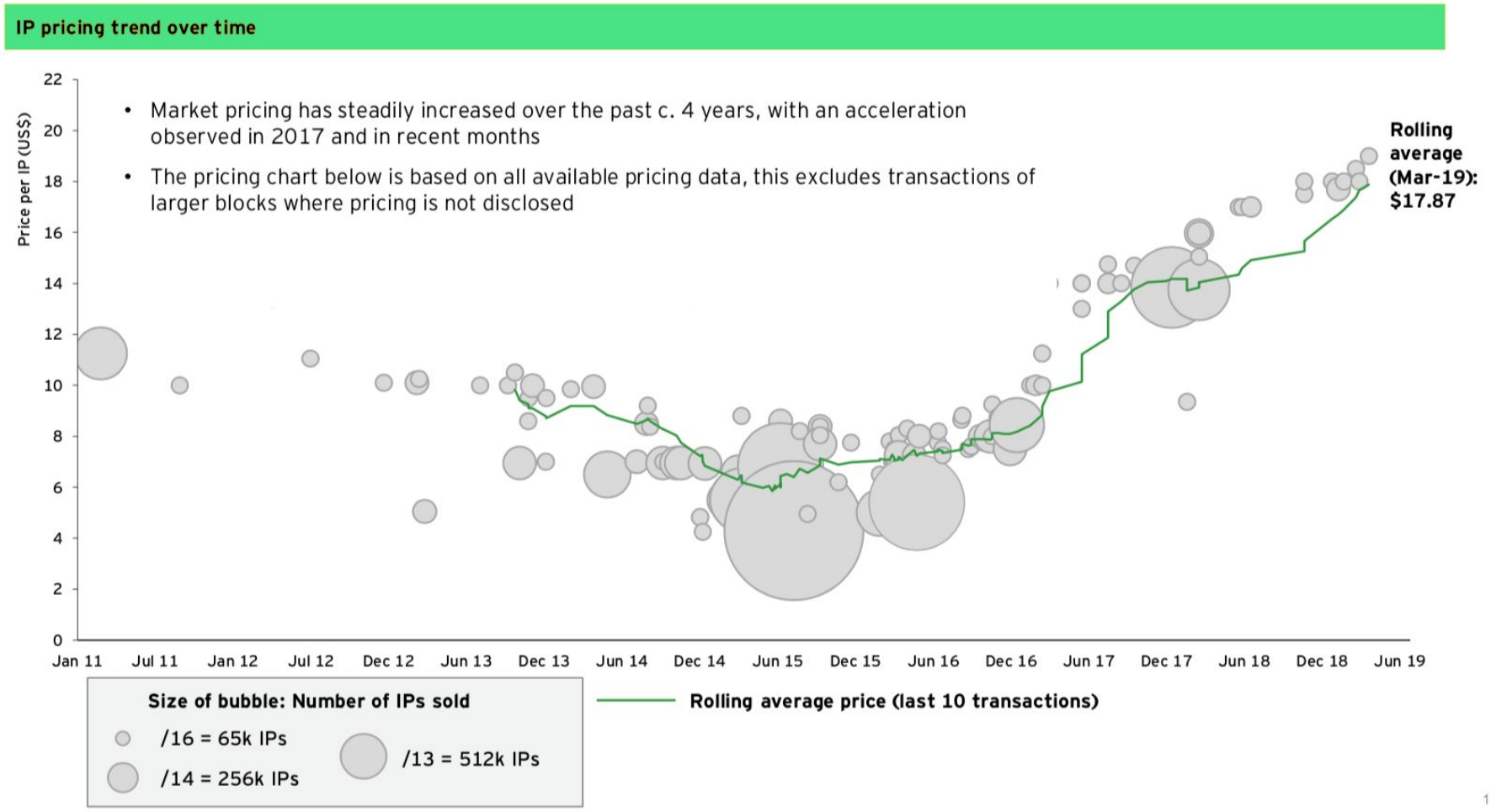
IPv4 Head-to-Head IPv6

IPv4 (Deployed 1989)		IPv6 (Deployed 1999)
32-bit number	ADDRESS SIZE	128-bit number
Dotted Decimal Notation 192.0.2.76	ADDRESS FORMAT	**Hexadecimal Notation** 2001:0DB8:0234:AB00:0123:4567:8901:ABCD
192.0.2.0/24	PREFIX NOTATION	2001:0DB8:0234::/48
DEPLETED IN 2015 2^{32} ~ 4,294,967,296	NUMBER OF ADDRESSES	2^{128} ~340,282,366,920,938,463,463,374,607,431,768,211,456

インターネットの急成長



IPv4アドレス1個 = 約2000円



1

http://ipv4marketgroup.com/ipv4-price-trends/

諸外国のIPv6対応と日本の現状

GoogleへのIPv6によるアクセス割合（世界）

（出典）https://www.google.com/intl/ja/ipv6/statistics.html

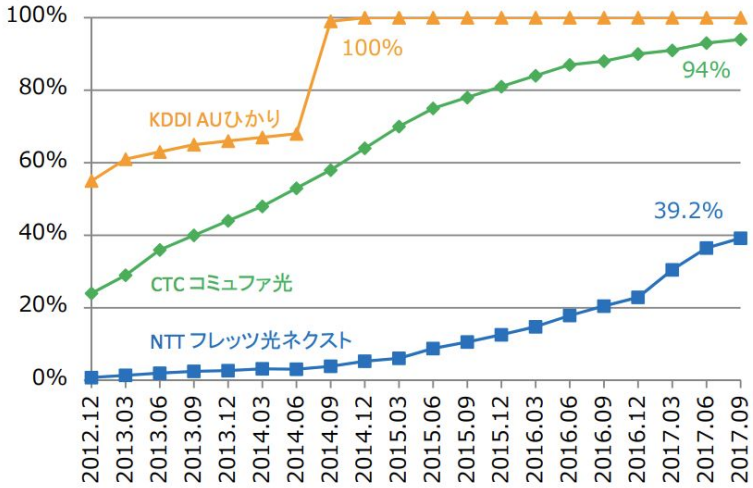
GoogleへのIPv6によるアクセス割合（国別）

	国名	IPv6利用率
1	ベルギー	54.94%
2	アメリカ	38.78%
3	ドイツ	37.57%
4	ギリシャ	36.75%
5	スイス	31.5%
6	ルクセンブルク	29.94%

	国名	IPv6利用率
7	ウルグアイ	29.54%
8	インド	24.86%
9	日本	22.37%
10	フランス	22.3%
11	ブラジル	22.28%
12	イギリス	21.95%

（出典）https://www.google.com/intl/ja/ipv6/statistics.html をもとに総務省作成（2018年1月1日時点）

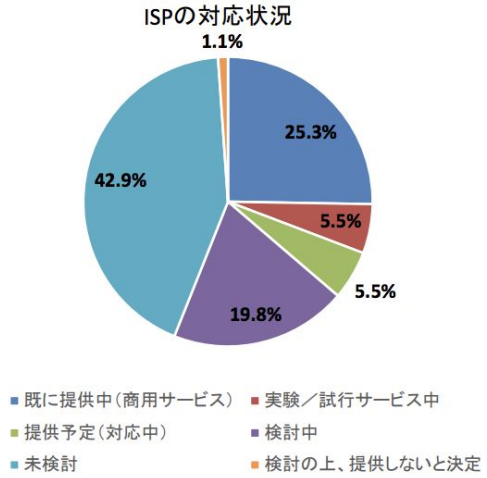
我が国のIPv6対応の現状（アクセス網）



（出典）http://v6pc.jp/jp/spread/ipv6spread_03.phtml をもとに総務省作成

我が国のIPv6対応の現状（ISP）

・ IPv6インターネット接続サービスを提供中のISPは、25.3%



http://www.soumu.go.jp/main_content/000531614.pdf

IPv6仕様の現状

1. IPv6仕様の再整理
    - RFC8200 (2017/7)
2. 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
3. IPv4からの移行
    - IPv4 as a Service 技術の普及
4. 新技術への期待
    - SRv6(IPv6 Segment Routing)

Agenda

1. IPv6アドレス表記とアドレス帯
2. ICMPv6とその機能
    a. PathMTUDiscovery
    b. NDP(近隣探索プロトコル)
3. RA v.s. DHCPv6
4. まとめ

IPv6アドレスの構造

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、
:: を用いて省略する。

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

→2001:db8::206:29ff:fe1e:482e

IPv6アドレス推奨表記

前述の表記ルールでは表記が一意に定まらないので、RFC5952(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。
　　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。

QUIZ: 推奨表記にしてみよう

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

- ○ 2001:db8::fff0:0:0:f
- ×　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アドレス帯

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(2000::/3)
- リンクローカルアドレス(fe80::/10)
- ユニークローカルアドレス(fc00::/7 (実質的fd00::/8))
- その他特殊用途のアドレス

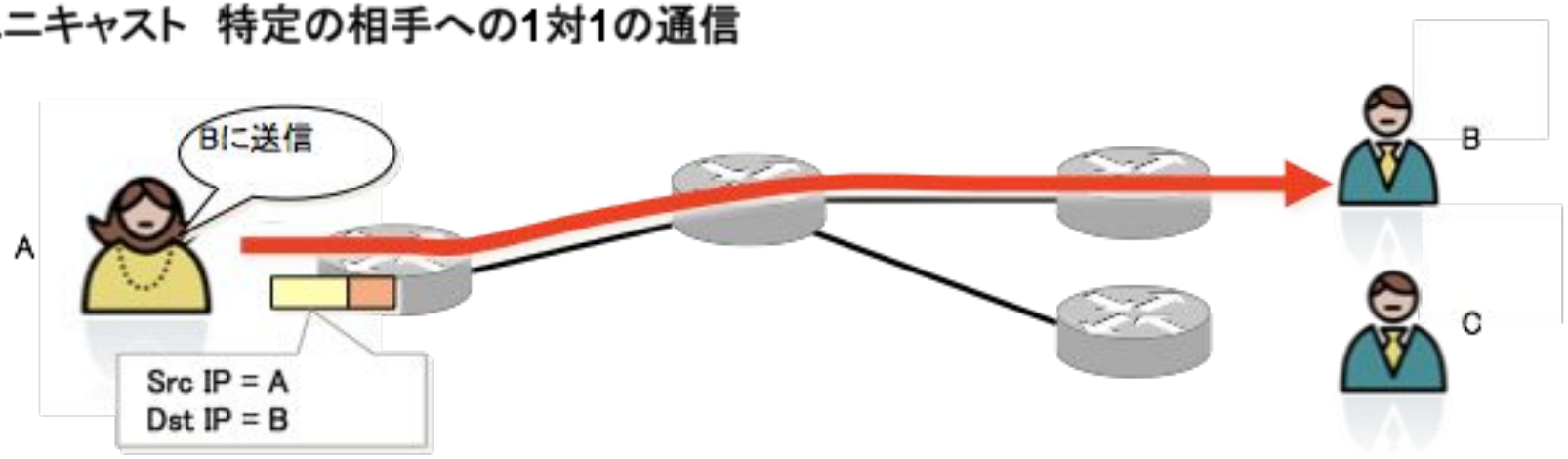
※昔は、サイトローカルアドレスというのがあったが廃止された(RFC3879)

マルチキャストアドレス(ff00::/8)

- グローバルスコープ(ff0e::/16)
- ローカルスコープ(ff02::/16)

ユニキャスト通信

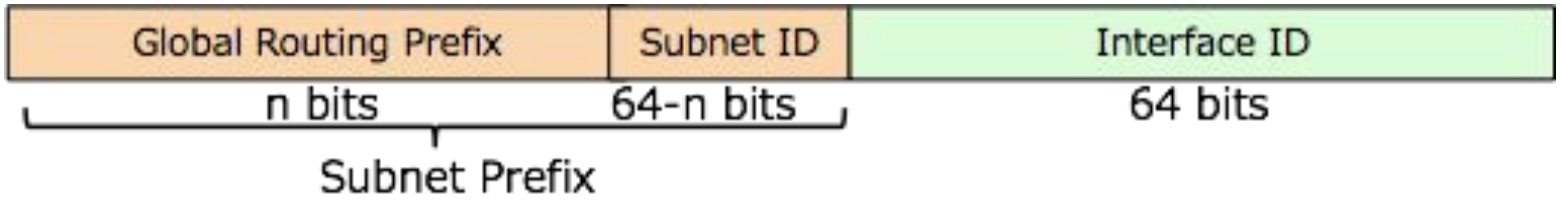
◆ユニキャスト　特定の相手への1対1の通信



グローバルユニキャストアドレス

Global Unicast Address(GUA)
IPv4におけるグローバルアドレスに相当

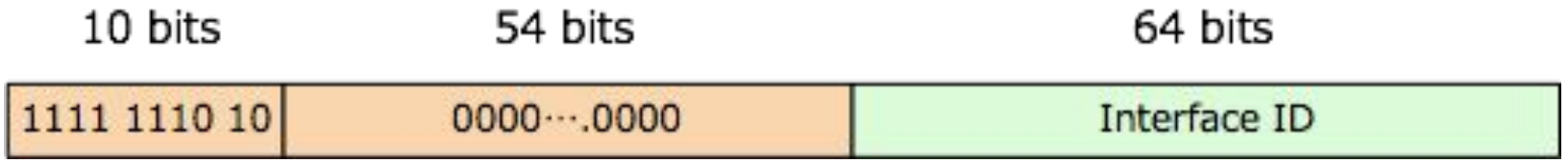
- 現在は 2000::/3 のアドレス空間を使用中
  - [RFC3587]（IPv6 Global Unicast Address Format）
- インターネット上でグローバルにルーティング可能
  - インターネットレジストリにより割り当てられる
- 割り当てられたプレフィックスからSubnet IDで切り出す
  - Subnet ID：サブネットの識別に使用
  - Interface ID(IID)：サブネット内のインタフェース識別に使用



リンクローカルアドレス

Link Local Address(LLA)
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）

- fe80::/10
- NDP: 近隣探索プロトコル(Neighbor Discovery Protocol)などで使用される
- 同じプレフィックスが別のリンクにも使われる



つまづきやすいIPv4 との違い ~その1~

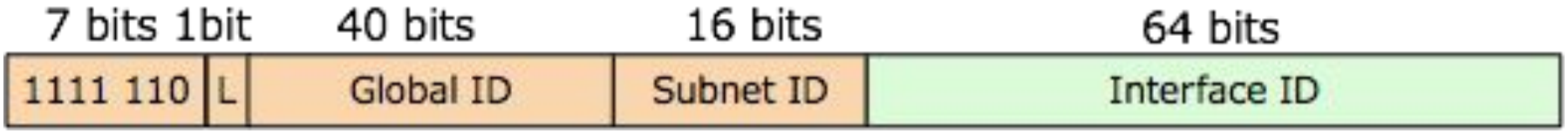
Link Local Address(LLA)の扱い

- IPv4
  - Link Local Addressはほとんど利用されない
  - WindowsやMacOS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
  - 必ずLink Local Addressが割り当てられる
    - sshで接続することも可能
  - GUAと合わせて複数持つことができる
  - LLAだけのネットワークなどIPv6独自の使い方が可能
    - RFC 7404 Using Only Link-Local Addressing inside an IPv6 Network

ユニークローカルアドレス

Unique Local Address(ULA)
IPv4のプライベートアドレスに相当

- サイト内通信用途で利用可能
  - ULAを送信元/送信先とするパケットをインターネットへ送信することは禁止されている
- fc00::/7
  - L bit
    - L=1 (fd00::/8) ローカル管理による割当て→こちらを使う
    - L=0 (fc00::/8) 将来の為に予約（管理組織による割当を想定）
- Global IDはランダム生成
  - アドレスの重複が避けられるデザイン



特殊なアドレス

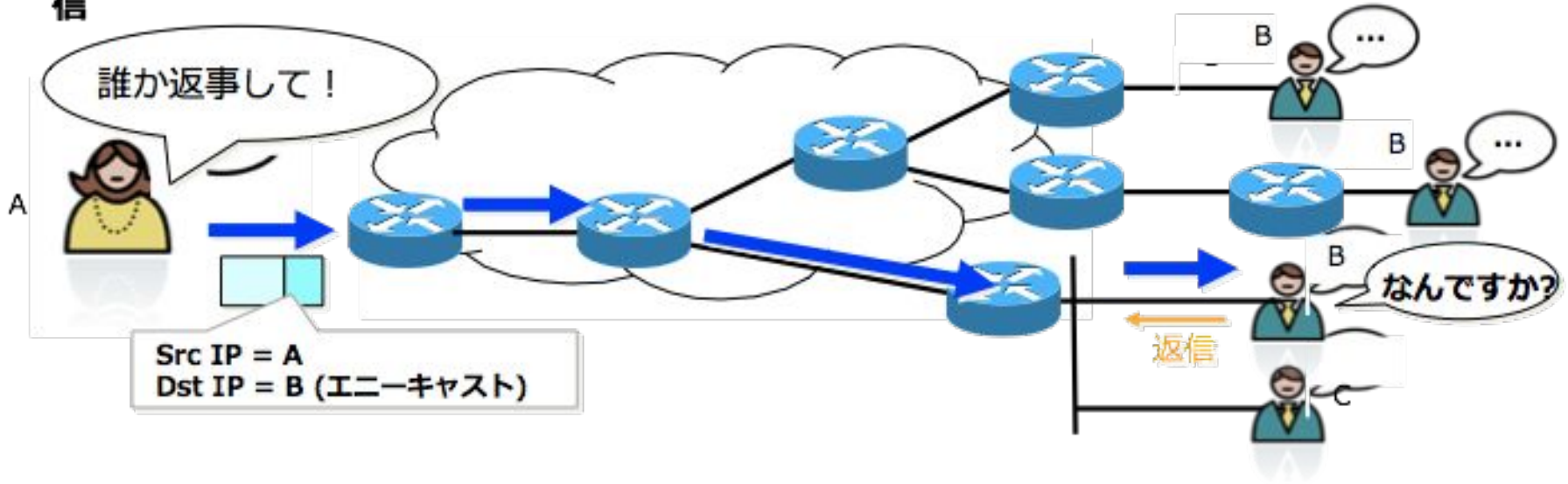
- ループバックアドレス（::1）
  - IPv4 の 127.0.0.1 に相当
- デフォルトルート(::/0)
  - 0.0.0.0/0に相当
- 文書用アドレス（ IPv6 Documentation Address ）
  - 2001:db8::/32
  - 技術文書、記事、資料においてIPv6アドレスを利用した例を提示しなければいけない場合に用いられる
  - グローバルインターネットに広報してはいけない
  - (参考) IPv4の文章用アドレス: 192.0.2.0/24, 198.51.100.0/24, 203.0.113.0/24

IPv4-IPv6 変換アドレス

- IPv4-IPv6 Translation Address
  - 64:ff9b::/96
  - 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変換技術で用いられる
  - グローバルインターネットに広報してはいけない
- アドレスを埋め込んだ例: 64:ff9b::192.0.2.33
  - IPv4アドレスを含むIPv6アドレスを表記するとき、最後の32ビット部分をドットで区切ったIPv4アドレス表記で記載することもできる

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



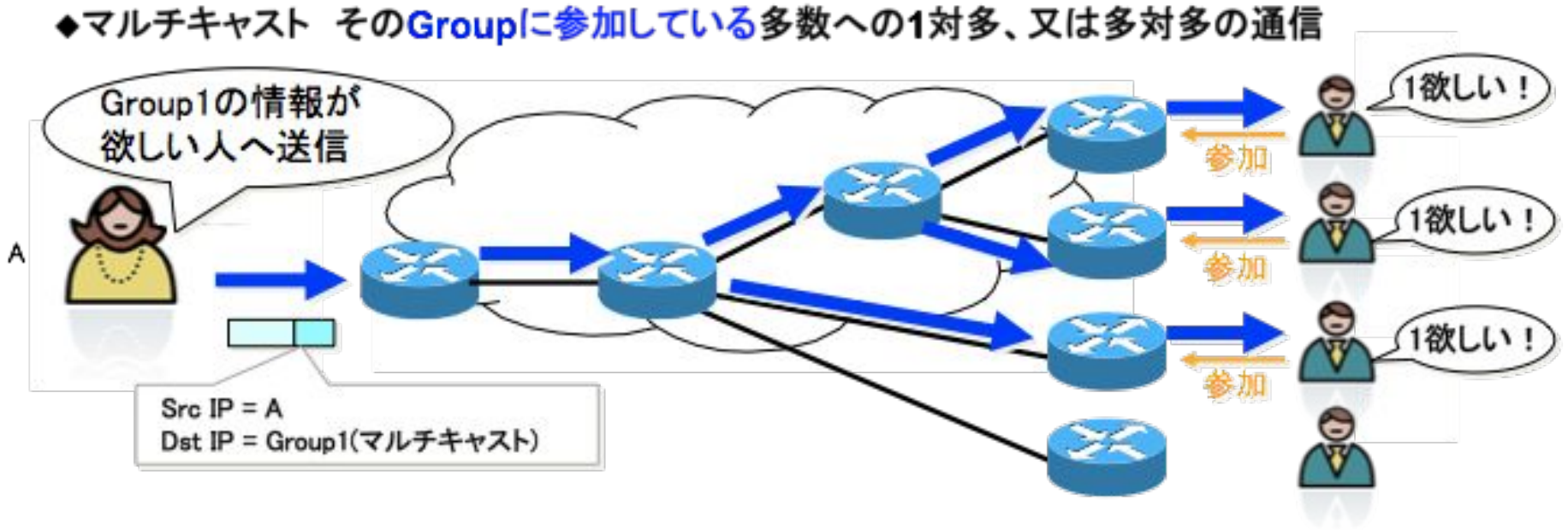
エニーキャストアドレス

アドレス自体は、ユニキャストアドレスの範囲

- 異なるサーバやルータ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ため、対障害性やDDoS攻撃対策などの目的で、地理的に分散配置されたサーバで主に使用される
- 利用例
  - Public DNS (Google: 8.8.8.8)
  - Root Server (L-root serverなど)

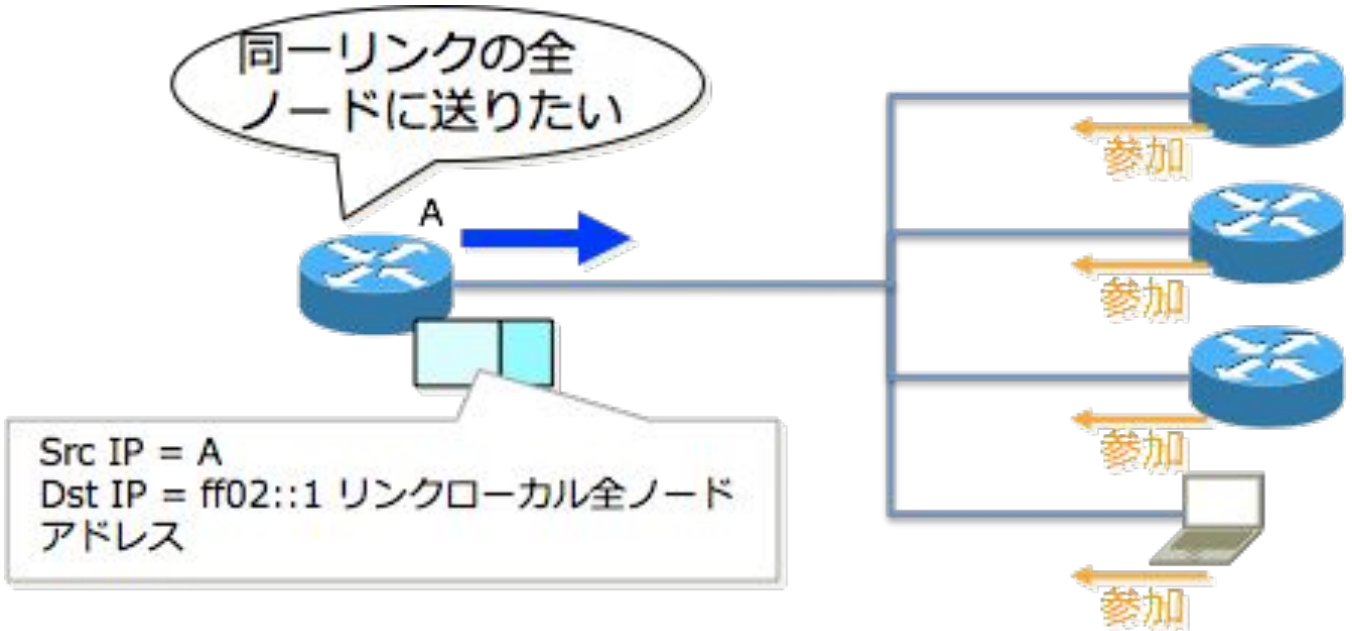
マルチキャスト通信
(グローバルスコープ)

- グローバルスコープ
  - ルータを超えて通信ができる
  - 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(送信元の負荷を軽減)



マルチキャスト通信
(リンクローカルスコープ)

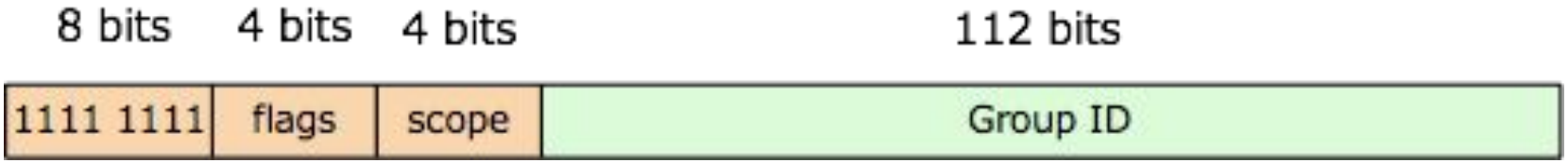
- リンクローカルスコープ
  - パケットが到達する範囲が同一サブネット上のみ
- 例: ff02::1 全ノードが参加するマルチキャストアドレス
  - IPv4におけるブロードキャストアドレスの代わりに使われる



マルチキャストアドレス

1対n 通信を行う場合に使用される

- ff00::/8
- スコープ
  - Scope = 1 : Interface-local
  - Scope = 2 : Link-local
  - Scope = 4 : Admin-local
  - Scope = 8 : Organization-local
  - Scope = e : Global scope
- グローバルスコープ(ff0e::/16)
  - ルータを超えて通信ができる
- リンクローカルスコープ(ff02::/16)
  - 同一サブネット内のみ



予約済み
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アドレスとインタフェース

- インタフェースに複数アドレスを付与することが可能
  - IPv4では基本的にNG
- IPv6 ではIPv4 よりも多くのアドレスが使用される
- 端末がパケットを受け取る IPv6アドレス
  - ループバックアドレス (::1/128)
  - インタフェースに付与された1つまたは複数のリンクローカルアドレス
  - インタフェースに付与された1つまたは複数のグローバルアドレス
  - 自分が所属するグループのマルチキャストアドレス
    - 例えば、全ノードマルチキャストアドレス (ff0e::1)

Happy eyeballs (RFC6555)

- IPv4とIPv6両方が利用可能な時の処理順序
  - アプリケーションやOSに依存
- Happy Eyeballs
  - フォールバックを緩和するための仕組み。
  - 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 v2
  - Appleが率先して実装
  - よりアグレッシブにIPv6を優先
  - 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。

Agenda

1. IPv6アドレス表記とアドレス帯
2. ICMPv6とその機能
    a. PathMTUDiscovery
    b. NDP(近隣探索プロトコル)
3. RA v.s. DHCPv6
4. まとめ

ICMPv6: IPv6で機能追加

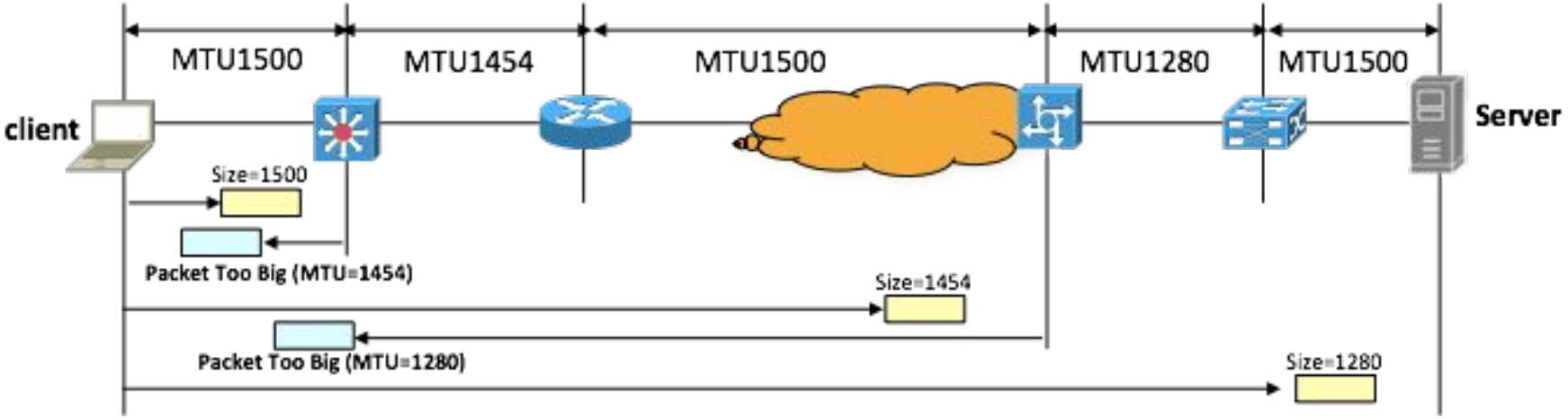
- ICMPv6 [RFC4443, RFC4884]
  - Internet Control Message Protocol for IPv6
- IPv6での用途(赤字が追加機能)
  - Ping6
  - Path MTU Discovery [RFC1981]
  - 近隣探索プロトコル(NDP) [RFC4861]
  - アドレス自動設定(SLAAC)

ICMPv6: 追加されたメッセージ

- ICMP Error Message（type 0～127）
  - Destination Unreachable（type 1）
  - **Packet Too Big（type 2）: Path MTU Discoveryに使われる**
  - 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）**
  - Redirect Message (type137)

近隣探索プロトコル(NDP)
アドレス自動設定(SLAAC)
で使われる

Path MTU Discovery



- IPv6：ルータ等の中継ノードでフラグメントしない
  - IPv4では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(Packet Too Big)を受信するとMTUを変更して、始点ノードでフラグメントして再送
  - 最初のリンクのMTU が初期値
  - IPv6最小MTUは1280byte
    - Path MTU Discovery の実装が難しいノードは 1280byte 固定
  - L2 SWのMTUにひっかかった場合は破棄される
- ICMPv6 Error を受け取れないと一部通信ができない(PMTU Blackhole)

近隣探索の機能とメッセージ(NS/NA)

Neighbor Solicitation（NS 近隣要請）
Neighbor Advertisement（NA 近隣広告）

- アドレス解決 (Address Resolution)
  - 宛先 IPアドレスだけを知っているときにリンク上の宛先のリンク層アドレス(MACアドレス)を決定する。
  - IPv4のARPに相当
- 近隣到達不能検出 (NUD, Neighbor Unreachability Detection)
  - リンク上の宛先に到達ができないことを検知する。
- 重複アドレス検出 (DAD, Duplicate Address Detection)
  - 使おうとしたアドレスを他のノードが使用していないかどうかを知る。

重複アドレス検出 (DAD)

- 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アドレス
    - ff02::1:ff/104 + 調べるアドレスの下位24bit
  - 送信元アドレス: 未指定アドレス（::）
  - 対象アドレス: 調べるアドレス
- 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
  - 重複していなければそのアドレスは使用可能となる
  - 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

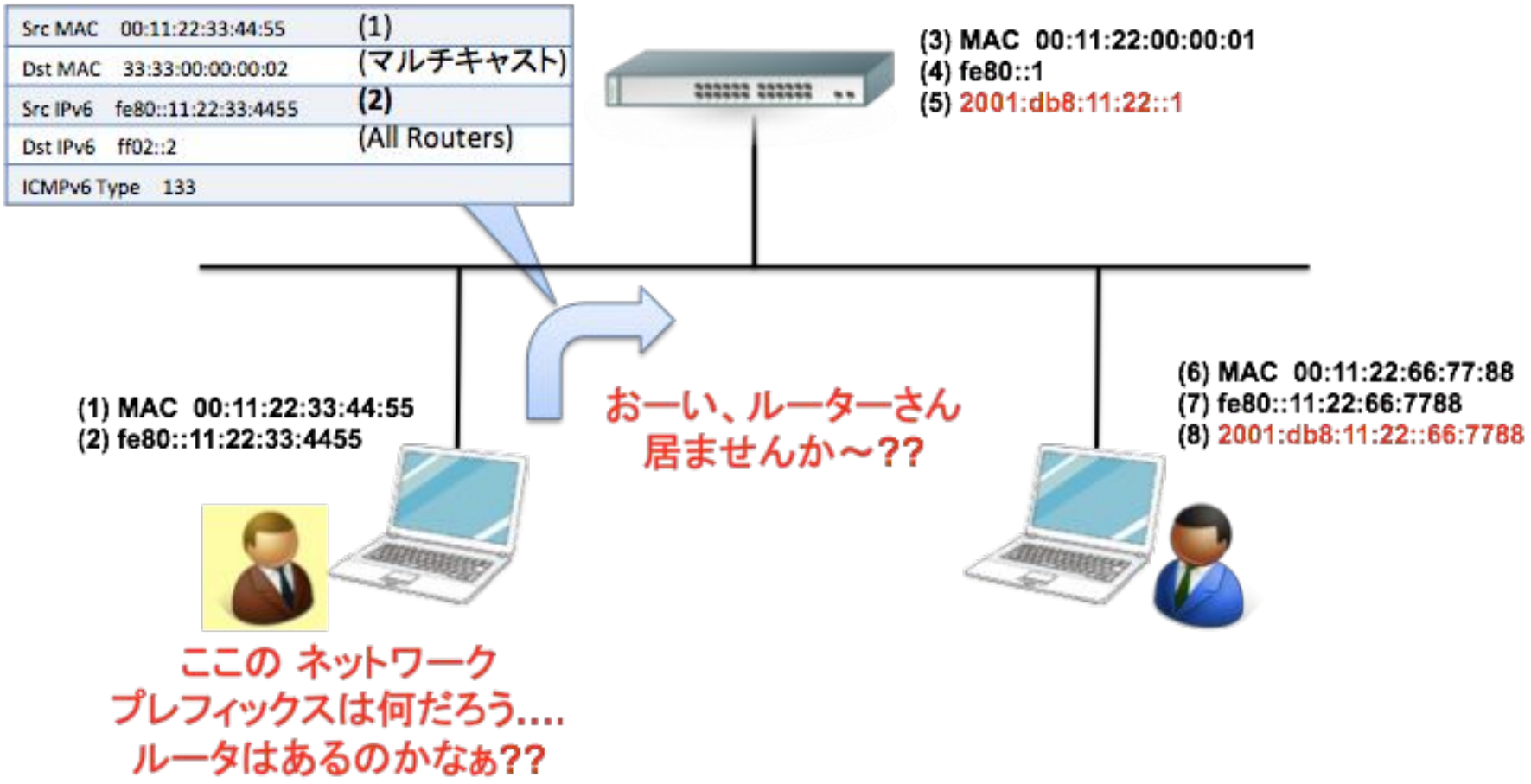
近隣探索の機能とメッセージ(RS/RA)

Router Solicitation（RS ルータ要請）
Router Advertisement（RA ルータ広告）

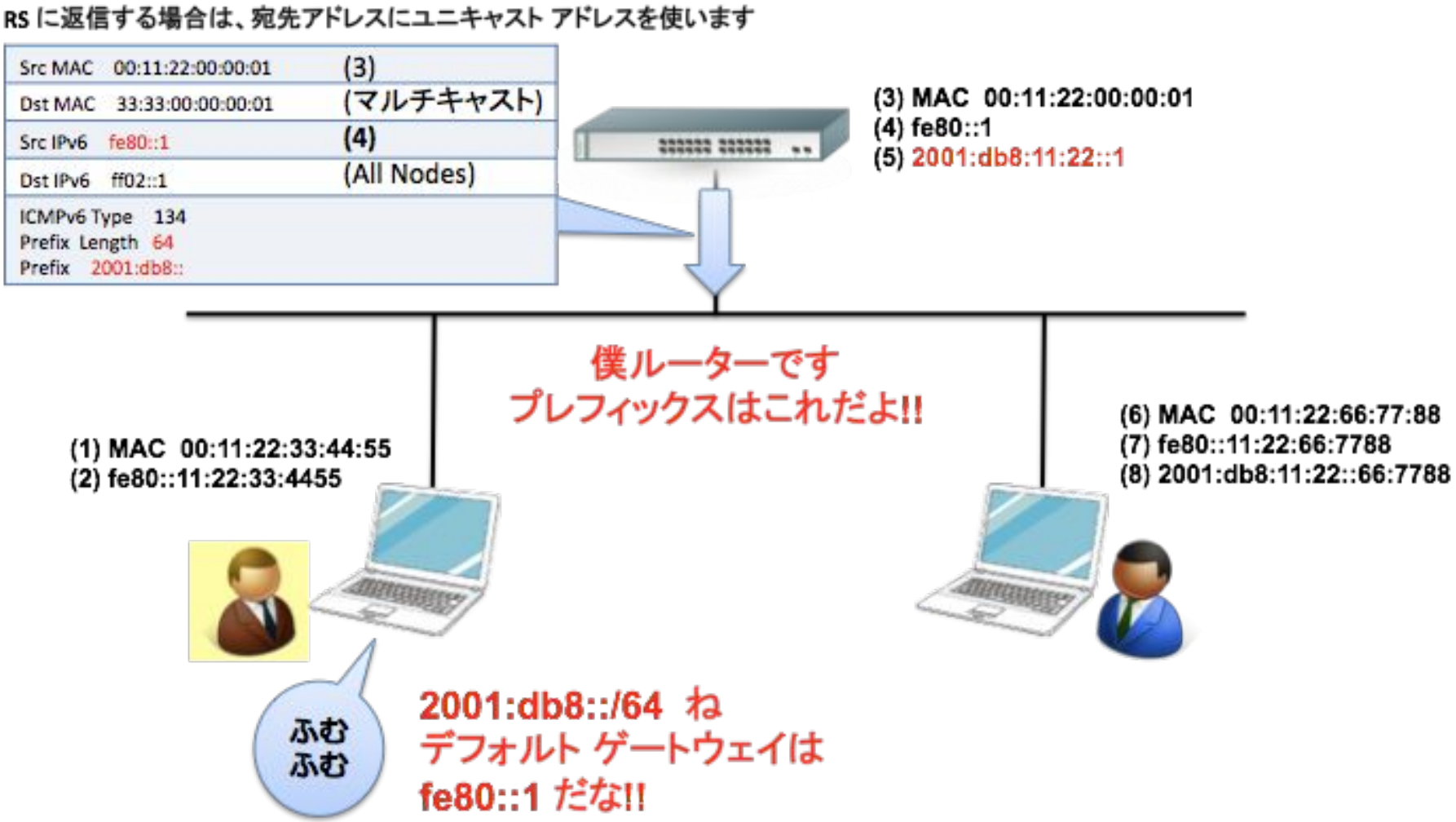
- ルータ発見 (Router Discovery)
  - ホスト・コンピュータが同一リンク上にあるルータを特定する
- プレフィックス発見 (Prefix Discovery)
  - ホスト・コンピュータが接続されたリンクのアドレス・プレフィックスをみつける。
- アドレス自動設定 (Address Autoconfiguration)
  - インタフェースに自動的にアドレスを設定する。

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によって通知できる主な情報

- デフォルトゲートウェイとなるルータの情報
  - リンクローカルアドレスである点に注意
  - 利用可能期間
- そのリンクで使用可能なプレフィックス情報
  - プレフィックス、プレフィックス長、寿命
- DHCPv6の使用に関する情報
  - M-flag:アドレス設定にDHCPv6を利用
  - O-flag:それ以外の情報の設定にDHCPv6を使用
- DNS情報(RFC6106:RDNSS) ※後述

つまづきやすいIPv4 との違い ~その2~

ファーストホップ

- 同一Link(Broadcast Domain)に存在するNodeと通信するための情報

- IPv4 AddressのMAC Address との対応表
  - ARP (Address Resolution Protocol)
  - IPv4 Broadcast/個別プロトコルを利用して実装
- IPv6 AddressのMAC Address との対応表
  - ND (Neighbor Discovery: 近隣探索)
  - NDはIPv6 Multicast/ICMPv6を利用して実装
- セキュリティ的には、ARP Spoofingと同様ND Spoofingが可能
- 不正RA対策が必要

Agenda

1. IPv6アドレス表記とアドレス帯
2. ICMPv6とその機能
    a. PathMTUDiscovery
    b. NDP(近隣探索プロトコル)
3. RA v.s. DHCPv6
4. まとめ

IPv6アドレスの自動設定

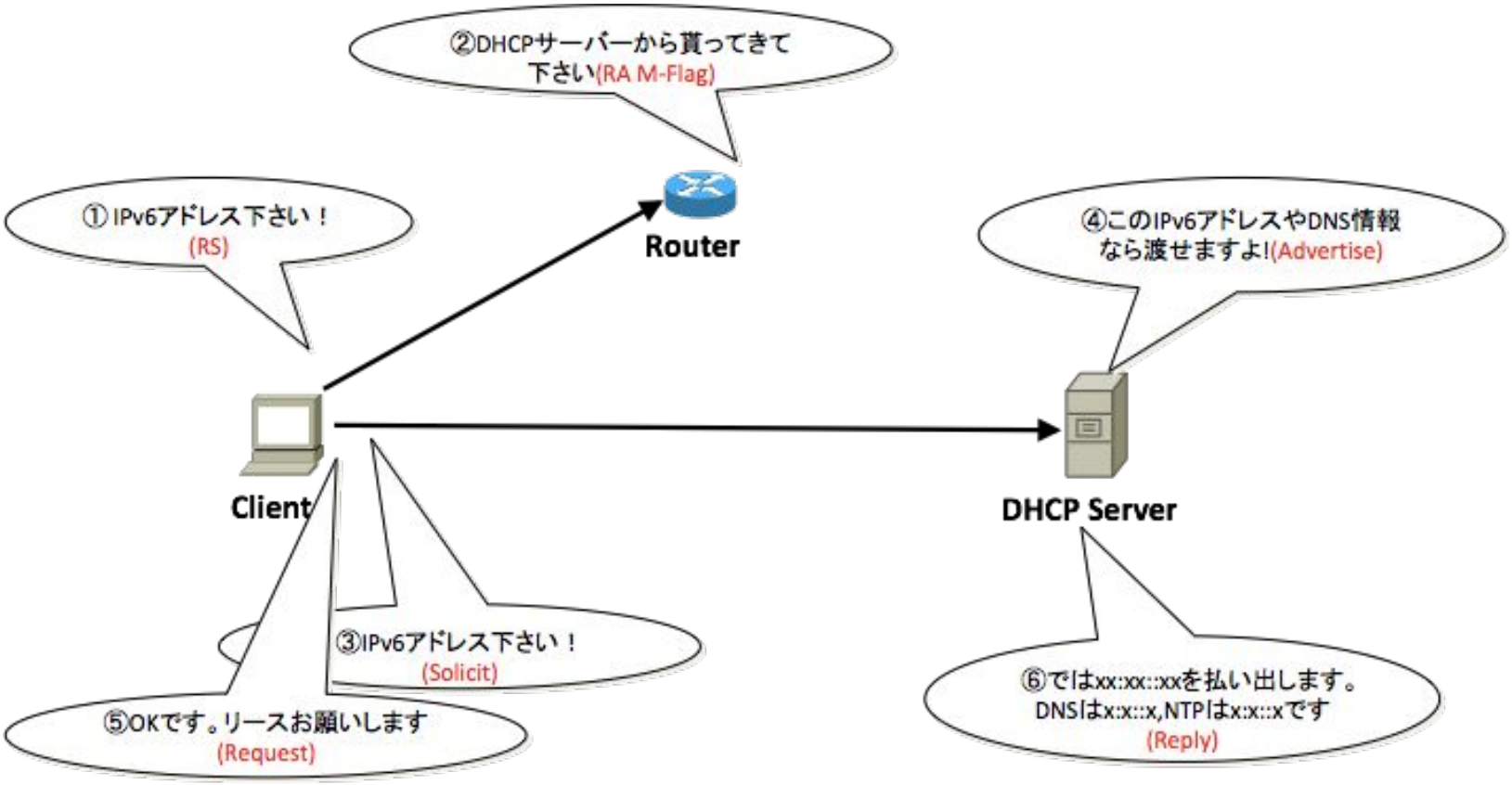
- SLAAC: StateLess Address Auto Configuration [RFC4862]
  - ステートレスなアドレスの自動設定
  - 端末はRAで受け取ったプレフィックス情報を使用して自動的にアドレスを生成する
  - アドレスを管理するサーバはない
- DHCPv6: Dynamic Host Configuration Protocol for IPv6 [RFC3315]
  - ステートフルなアドレスの自動設定
  - デフォルトゲートウェイが通知されない
    - RAと組み合わせて使う前提
  - その他の機能は IPv4 の DHCP とほぼ同じ

アドレス生成方法

- EUI-64：MACアドレスを元に世界中で一意なインターフェースIDを生成
  - 現在は非推奨
    - 毎回生成されるインターフェースIDが同じ
    - MACアドレスを簡単に知ることができてしまう
- プライバシー拡張：ランダムな値を元にインタフェースIDを生成し、一定時間内で使い捨てる方式
    - 一時アドレスや匿名アドレスと呼ばれる
    - 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
    - Windows などのOSで、デフォルトで有効化されている

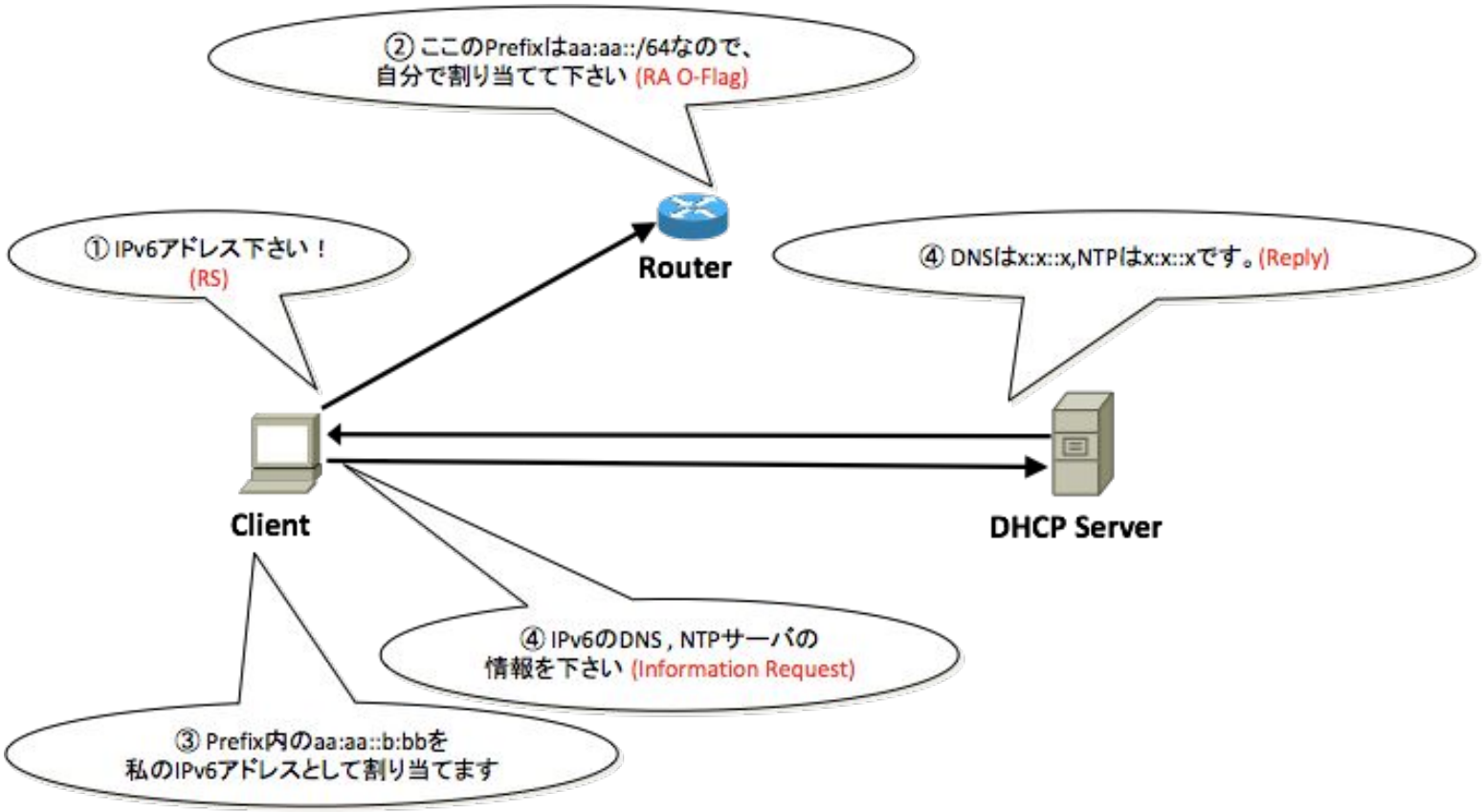
Stateful DHCPv6

- DHCP Server にてIPアドレス等の情報管理が可能
- 端末はRAのM-Flag受信によりDHCPv6 Client が動作する



Stateless DHCPv6(DHCPv6-lite)

- DHCP Server はIPアドレス等の情報管理をしない
- 端末はRAのO-Flag受信によりDHCPv6 Client が動作する
- RAだけでは得られないDNS/NTPなどのサーバ情報を取得



つまづきやすいIPv4 との違い　~その3~

アドレスの自動設定

- DHCPだけでは足りない。RAだけでも足りない。

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	○	–	–	○
Server Address (DNS , SIP , etc)	△ ※RDNSS	○	○	○

RDNSSオプション

Google(RA派) v.s. Microsoft(DHCPv6派)

- 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。
- その代わり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

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

Agenda

1. IPv6アドレス表記とアドレス帯
2. ICMPv6とその機能
    a. PathMTUDiscovery
    b. NDP(近隣探索プロトコル)
3. RA v.s. DHCPv6
4. まとめ

IPv4とIPv6 の違い

- 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
  - 機器や開発言語のIPv6対応状況やバグに注意
- IPv4とIPv6ではアドレスの長さや表記方法が違う
- パケット形式やプロトコルが備える機能が違う
  - 例: マルチキャストを利用した近隣探索
- IPv4とIPv6がある時は処理順序に注意
  - アプリケーションやOSに依存
  - HappyEyeball

IPv6 のセキュリティ

- IPv6のセキュリティ面の性質はIPv4と同等
  - RFC8200に明記
  - IPv6におけるIPSecの利用は、従来MUST（必須）とされてきたが、2011年のRFC6434によってSHOULD（推奨）に格下げされている。
  - 「IPv6はIPSecの利用が必須とされているからIPv4より安全である」というのはよくある誤解
- サービス毎にIPv4とIPv6でポリシーを整合させる
- IPv6独自に気をつけるべき点
  - ICMPv6の許可
  - 不正RA対策