IPv4 EXHAUSTION

IPv6オペレータ育成プログラム

iDCネットワーク編

株式会社IDCフロンティア
井上 一清

1st day Agenda

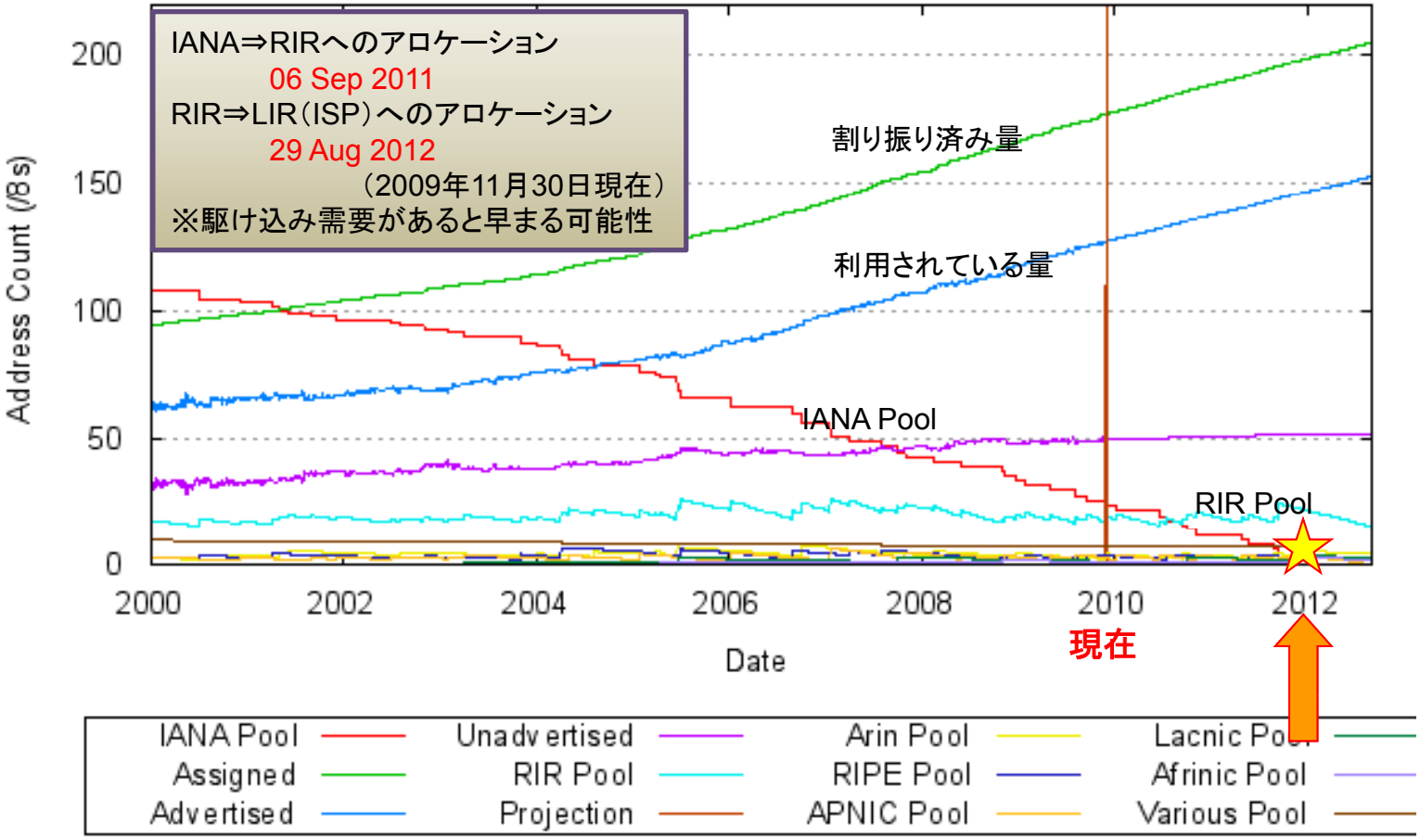
- 1スロット：IPv6の主な機能や特徴の説明
  - IPv6の機能、特徴
  - IPv6ヘッダ、拡張ヘッダフォーマット
  - IPv6アドレスの種類
  - IPv6アドレッシング
- 2スロット：ICMPv6の特徴、IPv6アドレス解決の仕組み
  - ICMPv6
  - NS/NA、RS/RA
  - Path MTU Discovery
  - セキュリティ
  - パケットフィルタ
  - DHCPv6、DNS
- 3スロット：実習
  - IPv6移行方法の説明
  - IPv6アドレス設定
  - NDP、RAの動作確認
  - パケットフィルタの設定

2nd day Agenda

- 1スロット（座学）
  - OSPFv3
  - BGP4+
  - Edge機能関連（HSRPv2/VRRPv3、uRPF）
  - 運用、監視関連（SNMP、Syslog、Flow）
- 2スロット（実習）
  - OSPFv3設定
  - BGP4+設定
  - 経路制御設定
- 3スロット（実習）
  - HSRPv2設定
  - 冗長試験
  - SNMP Trap、Syslog確認

IPv6の機能、特徴

IPv4アドレスの使用状況、枯渇予測



IANA（国際的在庫）在庫切れ

◆ Geoff Huston氏の最新予測より　http://www.potaroo.net/tools/ipv4/

IPv4アドレスの使用状況

World Regions	Population (2009 Est.)	Internet Users	Penetration	Users Grows 2000-2009
Africa	991,002,342	67,371,700	6.8 %	1,392.4 %
Asia	3,808,070,503	738,257,230	19.4 %	545.9 %
Europe	803,850,858	418,029,796	52.0 %	297.8 %
Middle East	202,687,005	57,425,046	28.3 %	1,648.2 %
North America	340,831,831	252,908,000	74.2 %	134.0 %
Latin America/Caribbean	586,662,468	179,031,479	30.5 %	890.8 %
Oceania/Australia	34,700,201	20,970,490	60.4 %	175.2 %
WORLD TOTAL	6,767,805,208	1,733,993,741	25.6 %	380.3 %

http://internetworldstats.com/stats.htm

- 世界の26%程度の人口（17億人）しかインターネットを利用していない
  - 2012年には19億人（3割程度）に増加するという予測もある
- 特にアジアやアフリカでの新興国のインターネット利用数の増加が予想される
  - ちなみに日本は9000万人程度が利用
- IPv4アドレスの約60%はアメリカ（3.1億人）で利用
  - US内でのIPv4アドレス枯渇は考えづらいが、2003年に国防総省がIPv6化を発表し、IPv6化に本格移行、IT製品のIPv6化対応も義務付け

iDCの課題

- Internet Connectivityを提供すること
  - IPv6対応
    - IPv6ネットワーク構築、デュアルスタック
    - 6to4、Teredo、6rd、トランスレータ、etc・・
  - IPv4の継続提供

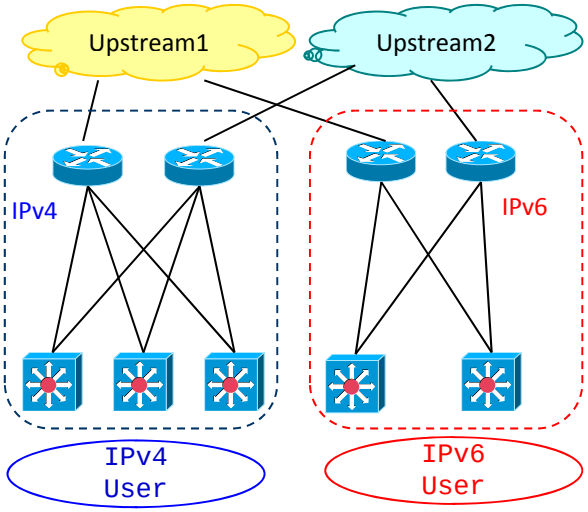
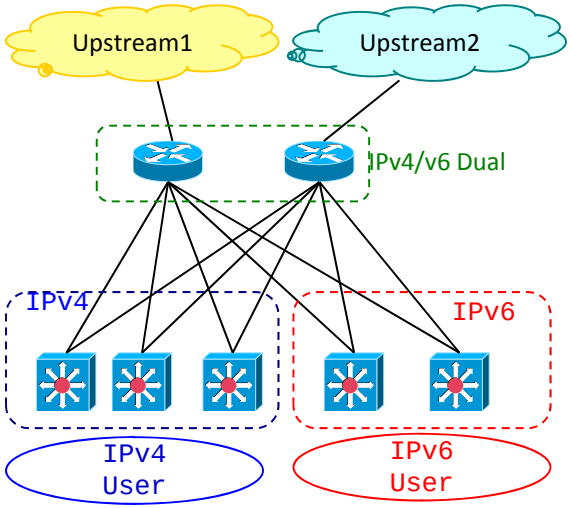
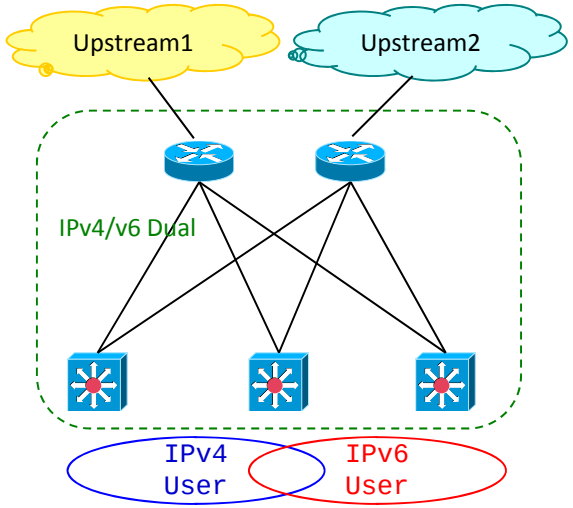
IPv6移行のリスクとチャンス

- 潜在的な顧客や新規市場への参入機会を逃す
- 最新のIPv6アプリケーションを活用できない
- 新規顧客開拓のためのサービスの差別化

IPv6移行への問題点・課題

- 既存IPv4インフラへの悪影響
  - 通信影響が大きい部分はIPv4/v6を物理的に分けるなどの工夫を行う
- コスト
  - HW/SWアップグレード時にIPv6化を意識しておくことでコストを抑える
  - 理想は機器リプレース時にIPv6も併せて導入
- 技術・スキル不足、情報不足、運用不足
  - 所詮は新プロトコルの追加
  - アドレス空間が膨大に増えるため、効率的な管理方法が重要
  - 十分な教育とIPv6を利用できる環境が必要

IPv6への移行パターン

IPv4/v6完全別ネットワーク構成	一部別ネットワーク構成	完全デュアルスタック構成
		
メリット　:IPv6の影響を完全に切り離せる トラブル時の切り分けが容易 デメリット:機器コストがかかる 管理機器数が倍増 上位キャリアの接続時に回線の 引き回しが必要	メリット　:顧客影響が最も大きい機器を切り離せる 上位キャリアの接続が容易 デメリット:一部機器のコストが増える 管理機器数が一部増える デュアルとシングル機器が分かれる	メリット　:機器コストを最も抑えられる 管理機器数が現状と同等 ユーザ側のデュアルスタック化要望に 容易に対応可能 デメリット:IPv6の影響がIPv4にも生じうる トラブル発生時の切り分けが困難

IPv6の特徴

広大なアドレス空間

●128ビットのアドレス
IPv4：IPv6 = バケツの体積：太陽の体積
約340澗個 （澗 = 10^{36}）
340,282,366,920,938,463,463,374,607,431,768,211,456個

●全てのノードにグローバルアドレスを付与可能：エンドツーエンド原理への回帰
本来のインターネットの姿　⇒　NATによる通信阻害がなくなる

追加された標準機能

●アドレス自動設定機能（プラグアンドプレイ）
管理者やエンドユーザの利便性が向上
●セキュリティ機能（IPsec）やマルチキャストの標準サポート
IPv4では追加機能だったものを標準装備
●QoSやモビリティの向上
QoS用のフィールドを準備（ただし利用方法は未定）
拡張ヘッダを利用したモビリティ通信における経路最適化

IPv6の広大なアドレス空間

- IPv4/IPv6でアドレス個数を比較することは無意味だが、十分に広いと言える。
- 構築可能なセグメント数は？(※)
  - IPv4 : 1073741824
  - IPv6 : 18446744073709551616

17,179,869,184倍（約170億倍）

(※)IPv4は、全アドレス帯を/30で分割した場合。IPv6は、/64で分割した場合。すべてがグローバルアドレスとして利用できるわけではないので、あくまでも目安

IPv6ヘッダ、拡張ヘッダフォーマット

IPv6ヘッダ

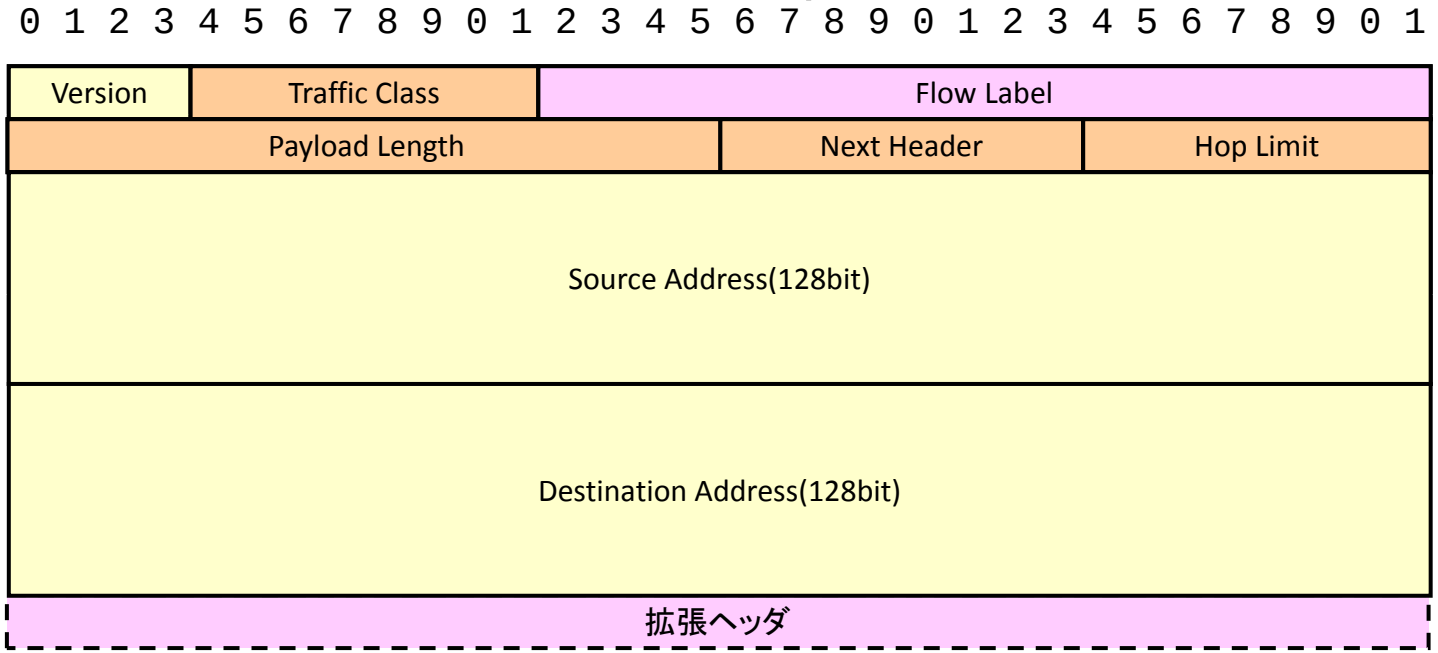
◆削除・追加されたヘッダ

- Internet Header Length（IHL）
  - IPv6ではヘッダ長固定（40byte）
- Identification、Flag、Fragment Offset
  - ルータ等の中継ノードはフラグメントしない
- Header Checksum
  - 処理速度向上のためIP層ではチェックサム計算、更新をしない
- Flow Labelが追加

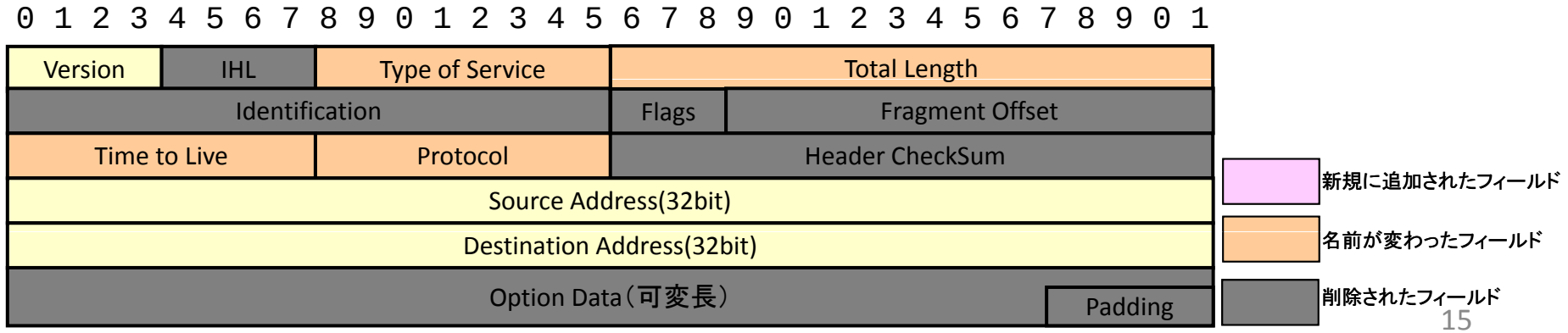
◆名称が変更されたヘッダ

- Type of Service ⇒ Traffic Class
- Total Length ⇒ Payload Length
- Protocol ⇒ Next Header
- Time to Live ⇒ Hop Limit

IPv6ヘッダ構造



IPv4ヘッダ構造



IPv6ヘッダ（1）

- Version（4ビット）
  - IPv6は”6”、IPv4は”4”
- Traffic Class（1バイト）
  - Differentiated Service（差別化サービス）と呼ばれる
- Flow Label（20ビット）
  - リアルタイム系のトラフィック処理に使用
  - 同フローを効率的に処理
  - 発信元にて設定するフローを識別する値
  - RFC3697で利用用途を想定

 # Ethertypeは0x86DD（IPv4は0x0800）

IPv6ヘッダ（2）

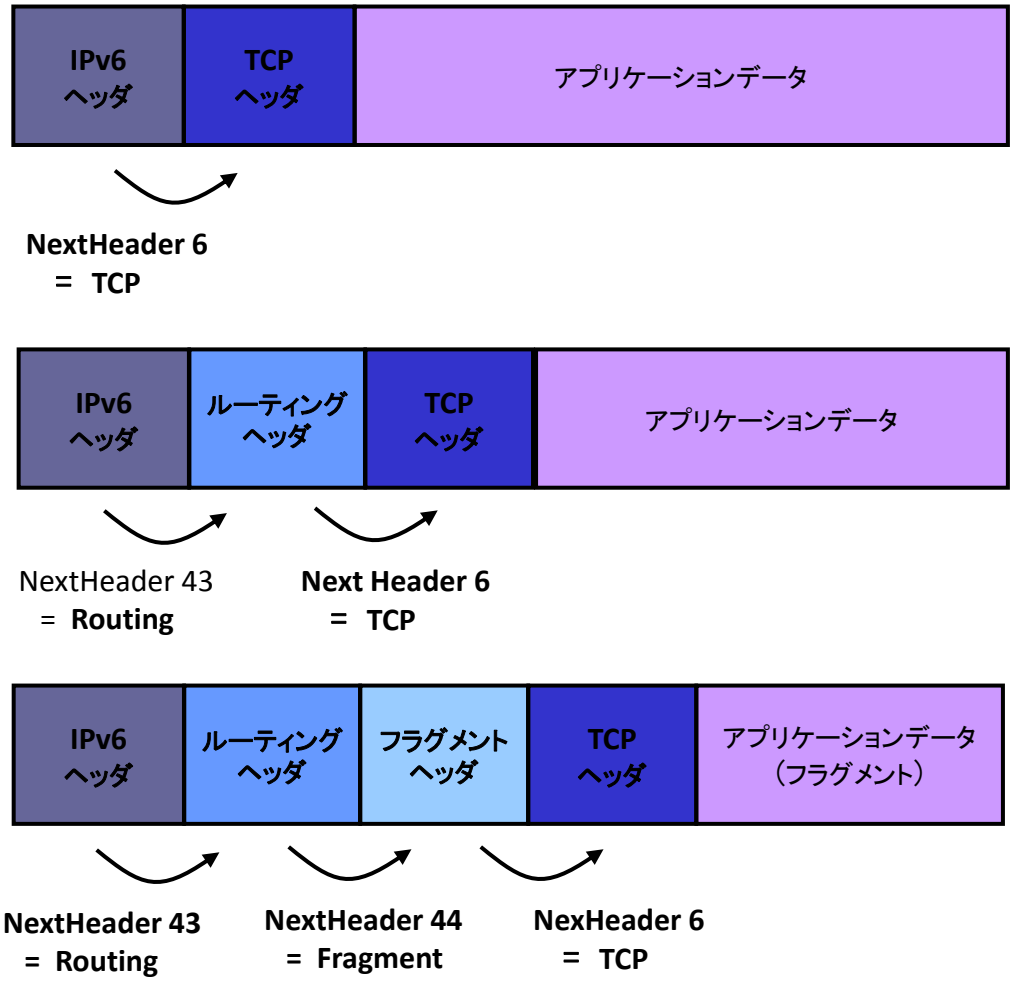
- Payload Length（2バイト）
  - 最大65535バイト
    - それ以上はJumbogram Extension Headerを使用（PLは0となる）
- **Next Header（1バイト）**
  - IPv4でのProtocol番号相当
    - 1:ICMPv4 , 58：ICMPv6 , 6:TCP , 17:UDP , 89：OSPF , etc・・
  - 拡張ヘッダの種別もここに記述される
    - 0：Hop-by-Hop , 43：Routing Header , 44：Fragment Header、etc・・
- Hop Limit（1バイト）
  - TTLと同様
    - 0になったらhop limit exceeded in transitのICMPv6(type3)を返す

拡張ヘッダ

- Hop-by-Hop Options Header（NH0）
  - RSVP、MLDのRouter Alert等で使用される
  - Jumbogram Extension Headerもこれを使用
- Routing Header（NH43）
  - 中継ノードを1つ以上指定（**RH0は禁止：RFC5095**）
  - RH2はモバイルIPv6で使用
- Fragment Header（NH44）
  - Don’t Fragment bitはIPv6では不要のためなし
  - 全て同じ送信元/送信先、識別子を持っていなければならない
- Authentication Header（NH51）
- Encapsulating Security Payload Header（NH50）
- Destination Options Header（NH60）
  - 終点アドレスノードにて実行する内容を記述
  - モバイルIPv6で使用される

Hop-by-Hopを除き、拡張ヘッダは終点アドレスノードのみが処理する

拡張ヘッダのイメージ



推奨される拡張ヘッダの順序

IPv6アドレスの種類

IPv6アドレス表記法

◆IPv4のアドレス表記法

2進数表記（32ビット）

11000000 10101000 00000000 00000001

・8ビットに区切り10進数で表現　区切り文字はピリオド「.」

192.168.0.1

◆IPv6のアドレス表記法

2進数表記（128ビット）

0010000000000001 0000110110111000 1011111011101111 1100101011111110
0000000000000000 0000000000000000 0000000000000000 0001001000110100

・**16ビットに区切り16進数で表現　区切り文字はコロン「:」**

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

・省略表記①：各ブロックの先頭の連続する「0」は省略可能

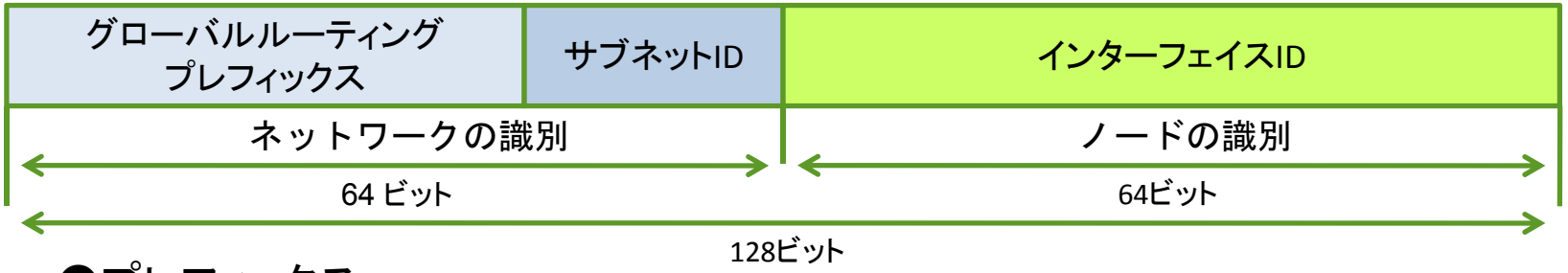
2001:db8:beef:cafe:0:0:0:1234

・省略表記②：連続した「0」は1回に限り「::」に省略可能

2001:db8:beef:cafe::1234

IPv6アドレスの種類

◆IPv6アドレスの構造



●プレフィックス
グローバルルーティングプレフィックスとサブネットIDを合わせた
上位64ビット（64ビットでない構成も可能）

◆IPv6アドレスの種類

●ユニキャストアドレス　　１対１　通信
ネットワークインターフェイス毎に設定されるアドレス
グローバルアドレス，リンクローカルアドレス，ULA

●マルチキャストアドレス　　１対多　通信
グループを識別するアドレスで複数のノードを識別
IPv6ではIPv4のブロードキャストの置き換えとしても利用

●エニーキャストアドレス　　１対１of 多　通信
複数のノードに指定可能な「機能」に対して設定されるアドレス

IPv6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

・いわゆるグローバルアドレス　（例）2001:db8::1

◆リンクローカルユニキャストアドレス

・同一リンク（セグメント）内にて一意なアドレス（fe80::/10）
　プラグアンドプレイなどのリンク内通信で利用される

◆ユニークローカルユニキャストアドレス（ULA）　[RFC4193]

Lビット：0 未定義　1 ランダム生成による独自割り当て

・自由に利用可能なローカルアドレス（fd00::/8）
・廃止されたサイトローカルアドレスの代用

特殊なユニキャストIPv6アドレス

◆未指定アドレス

●アドレスが未割り当てのときに始点アドレスとして利用
すべて0のアドレス　0:0:0:0:0:0:0:0 = ::

◆ループバックアドレス

●自分自身を表すアドレス（IPv4における127.0.0.1）
最下位ビットのみ1　　0:0:0:0:0:0:0:1 = ::1

◆移行技術用アドレス

●IPv4ネットワークを利用してIPv6通信を実現するトンネル接続に利用されるアドレス
●IPv4互換アドレス（IPv4-compatible IPv6 address）(既に廃止)
上位96ビットが0で残り32ビットがIPv4アドレス
表記方法　　::192.168.0.1
●その他の自動トンネルアドレス
6to4アドレス，Teredoアドレス，ISATAPアドレス

IPv6マルチキャストアドレス（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

◆マルチキャストアドレス

フラグ	意味
Tフラグ	0：恒久的な割り当て（IANAにより定義済み）アドレス　1：一時的な割り当てアドレス
Pフラグ	1：Unicast-Prefix-basedマルチキャストアドレス（RFC3306）※P=1の場合にはT=1
Rフラグ	1：PIM-SMにおけるRendezvous Point (RP)マッピング用（RFC3956）※R=1の場合P=1 T=1

スコープ：マルチキャストの有効範囲を指定			
0000（0）	予約	0101（5）	site-local scope
0001（1）	interface-local scope	1000（8）	organizational-local scope
0010（2）	link-local scope	1110（E）	global scope
0100（4）	admin-local scope	1111（F）	予約

IPv6マルチキャストアドレス（2）

◆定義済みのマルチキャストアドレス

FF02:0:0:0:0:0:0:1	All nodes（IPv4ブロードキャストの代用）
FF02:0:0:0:0:0:0:2	All routers
FF02:0:0:0:0:0:0:5	All OSPF routers
FF02:0:0:0:0:0:0:6	All OSPF Designated Routers
FF02:0:0:0:0:0:0:9	All RIP routers
FF02:0:0:0:0:0:1:2	All DHCP Agents (Relay Agents & Servers)
FF02:0:0:0:0:0:1:3	LLMNR (Link-Local Multicast Name Resolution)
FF02:0:0:0:0:1:FFxx:xxxx	要請ノードマルチキャストアドレス （xxxxxxは該当IPv6アドレスの下位24ビット）

EtherヘッダのDestination Addressは 33:33:xx:xx:xx:xx となる

最新の割り当て状況は以下で確認可能

http://www.iana.org/assignments/ipv6-multicast-addresses/

IPv6エニーキャストアドレス

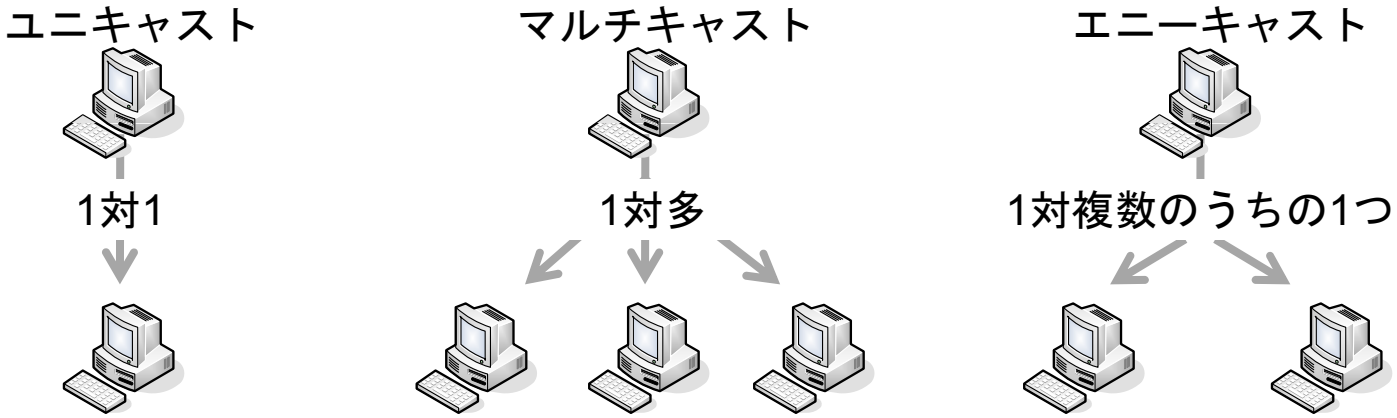
◆エニーキャストアドレス

- 複数の機器に付与され最も近い（経路情報的に）ものに転送
- アドレスの見た目はユニキャストアドレスと同じ
- ルートDNSなどで利用されている

◆サブネットルータエニーキャストアドレス

- 特定のプレフィックスを持つサブネット上のルータを表す

◆通信形態の比較



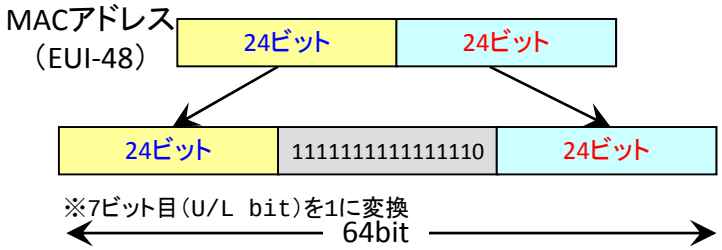
ノードに付与されるアドレス

- ノードが持つアドレス　　一般的な設定
  - リンクローカルアドレス（fe80::/10）・・・・・ 自動／手動
  - ユニキャストアドレス（2000::/3）・・・・・ 自動／手動
  - ループバックアドレス（::1/128）・・・・・ 自動
  - 全ノードマルチキャストアドレス（ff02::1）・・・・・ 自動
  - 要請ノードマルチキャストアドレス（ff02::1:ff/104）・・・・・ 自動
  - 所属するグループのマルチキャストアドレス・・・・・ （自動）
- ルータの場合はさらに下記アドレスを持つ
  - サブネットルータエニーキャストアドレス・・・・・ 実装依存
  - 全ルータマルチキャストアドレス（ff02::2）・・・・・ 自動

IPv6アドレッシング

インタフェースID

- 手動設定
- modified EUI-64形式
  - MACアドレスから生成



例）
MACアドレス　0016.9c43.cc00
インタフェースID　FE80::216:9CFF:FE43:CC00

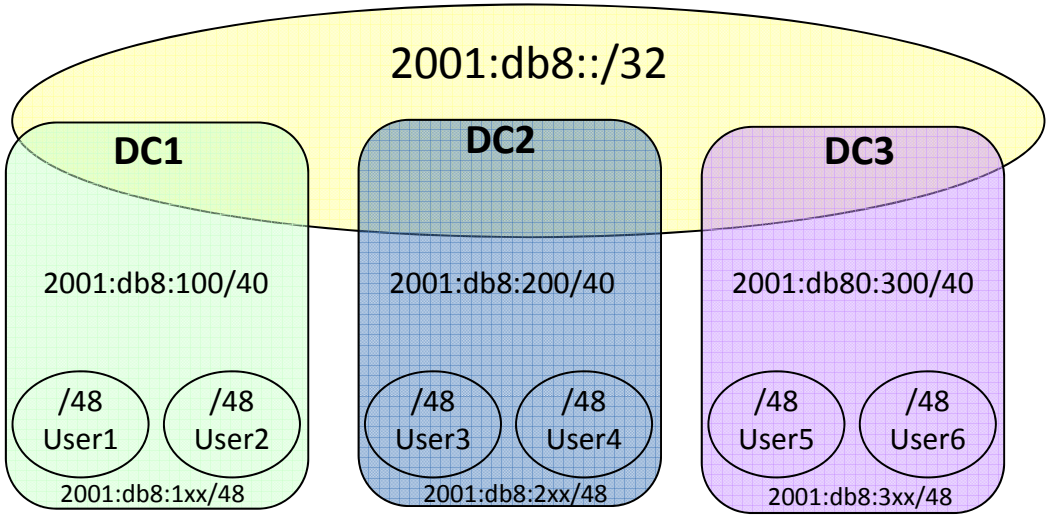
- Temporary Address（一時アドレス：RFC4941）
  - インタフェースIDにランダムな値を用いる一時アドレスを使用
  - 一定時間（最大7日間）で更新し、ノードの特定を困難にする
  - Windows Vistaではさらに独自の生成アルゴリズムを実装

- DAD（Duplicate Address Detection）
  - 重複アドレス検出
    - 自らのアドレスをもとにした要請ノードマルチキャスト（NS）を送信

IPv6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には/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
- ただ1つのデバイスが接続する場合には/128

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アドレス設計の工夫

- 経路集約を考えたアドレス設計が重要
  - 経路集約は4bit刻みが分かり易い
- 管理・運用性の高いアドレス設計
  - 主要なNW機器に対してはリンクローカルアドレスも手動で設定しておいた方がよい
- サブネットプレフィックス設定の工夫（参考）
  - 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

セキュリティ

- DAD機能の悪用
  - 全てのNSに応えるような設定
  - 特に無線LANが危険
- RAの悪用
  - デフォルトルートの変更
    - ルータを接続するポートからのみRAを許可するような設定をL2SWで実装することが望ましい
- IPsecのAHやSENDがあるが実用的ではない
- 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
  - セキュリティと管理・運用性はトレードオフ

ICMPv6

ICMPv6

- **ICMP Error Message（type 0～127）**
  - Destination Unreachable（type 1）
  - Packet Too Big（type 2）
  - 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）

NS/NA、RS/RA

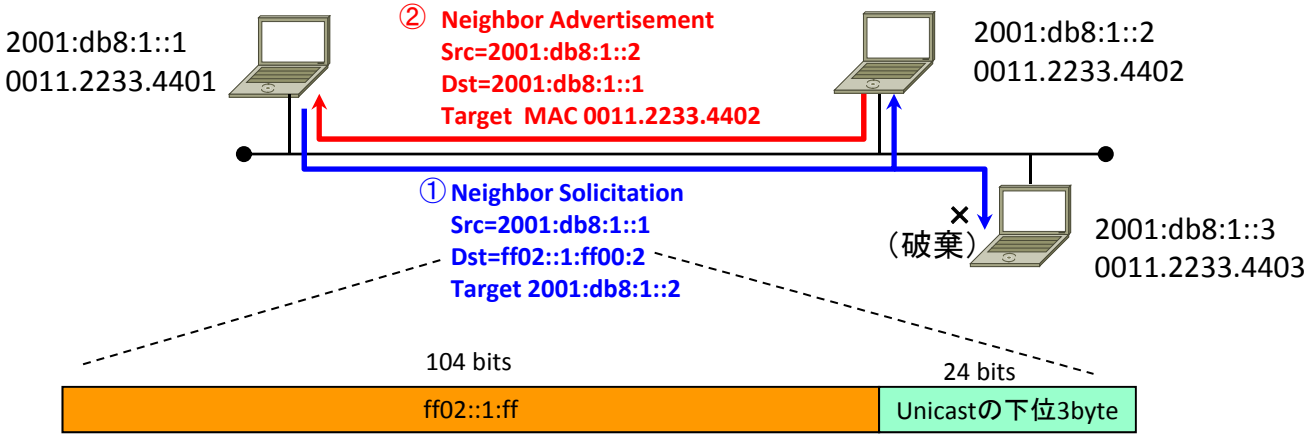
NDP（近隣探索プロトコル）

■ 5つのメッセージタイプ

- 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）

Neighbor Solicitation/Neighbor Advertisement

- リンク層アドレス解決とNUD
- 255未満のHop Limitは無視
- ARPと異なり双方向で行われる必要がある
- 要請ノードマルチキャストアドレスはFF02::1:FF00:0000～FF02::1:FFFF:FFFF



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::1:ff00:2)

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

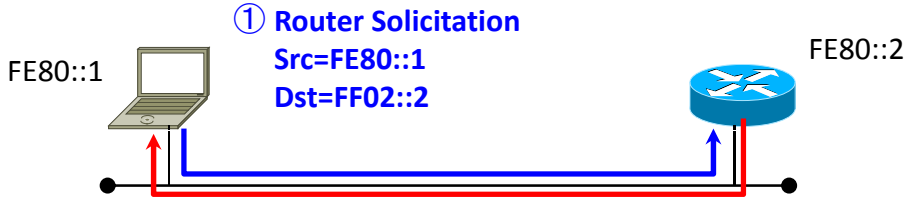
※”33:33”にMulticastの下位4byteを連結

近隣キャッシュの状態

INCOMPLETE	アドレス解決が未完了　NSを送信してNAを待っている状態
REACHABLE	指定したアドレスに対してNAを受け取るとReachableに変化
STALE	Reachable timer（デフォルト30秒）が経過
DELAY	Stale状態のアドレスに対してパケットが送信されるとDelayに変わる 送信されたパケットに対して応答が返ってきた場合はReachableに戻る
PROBE	Delay状態から応答がないまま5秒経過するとProbeに変化する Retrans timer経過後NSを3回送信（解決されなればINCOMPLETE）

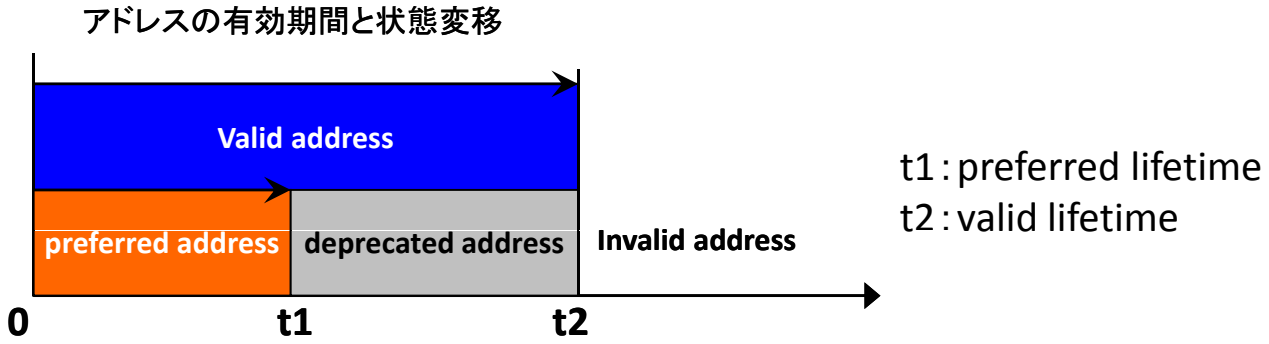
Router Solicitation/Router Advertisement

- RSの宛先アドレスはFF02::2、Hop Limitは255
- RAの宛先アドレスはFF02::1かRS内の始点アドレス、Hop Limitは255
- RA内のCurrent Hop Limitフィールドでノードが用いるホップ制限を設定
- M-flagが0ならステートレスアドレス自動設定、1ならDHCPv6によるアドレス設定
- O-flagが1ならアドレス以外の情報をDHCPv6により取得
- Router Lifetimeはデフォルトルータのみが1以上（65535以下）を指定
- 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

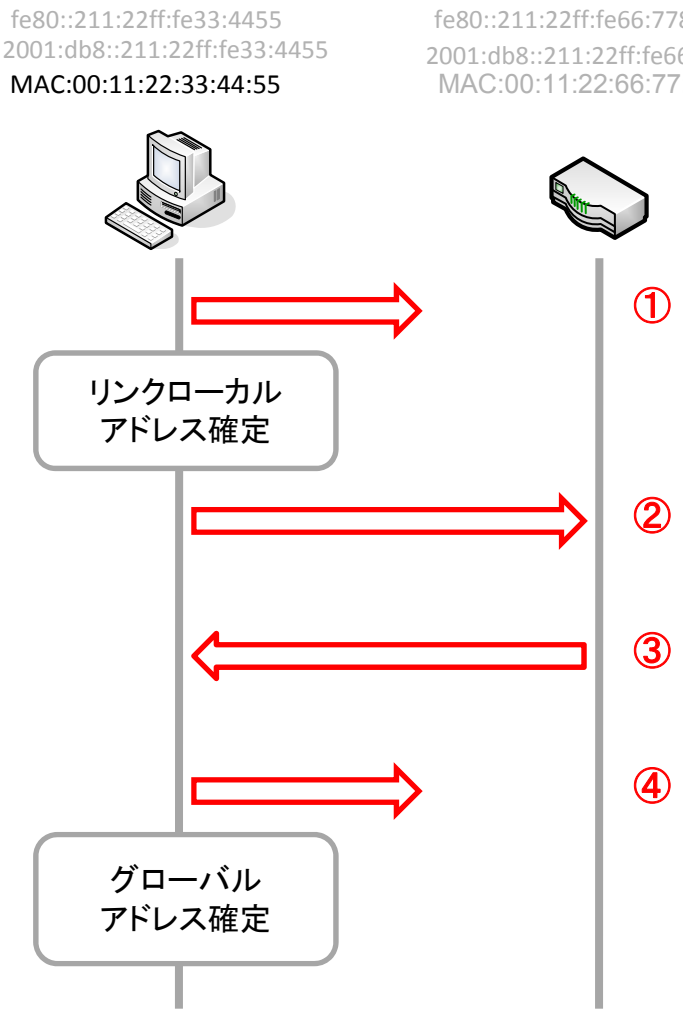


IPv6アドレスの状態、アドレスのlifetime

- tentative address
  - インタフェースに付与されていないアドレスでNDメッセージにしか使用できない。この時点でアドレスの一意性をDADで確認する。
- preferred address
  - インタフェースに付与されたアドレス。アドレスが一意で通信可能な状態
- deprecated address
  - 有効ではあるが、新規通信への使用をしないことが望まれる
- valid address
  - Preferredとdeprecatedのアドレスの双方を指す
- Invalid address
  - 有効アドレスの有効期間が過ぎるとこの無効アドレスになる



ステートレス自動アドレス設定の流れ



①近隣要請（NS）
近隣広告がなければ
ターゲットアドレス
の利用が可能
＜重複アドレス検出＞
要請ノードマルチキャスト

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

②ルータ要請（RS）
全ルータマルチキャスト
（ff02::2）宛に送信

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

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

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

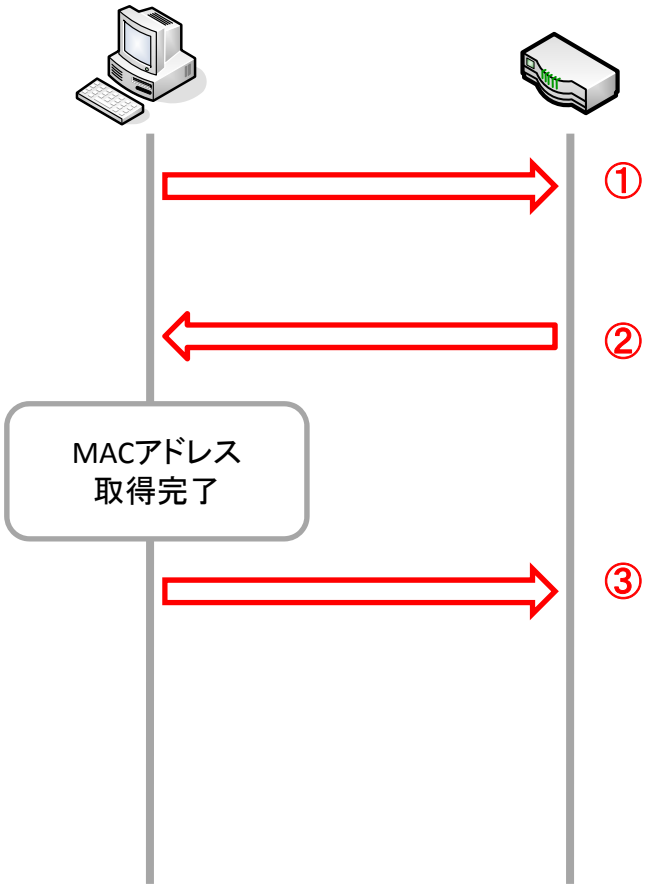
④近隣要請
近隣広告がなければ
ターゲットアドレス
の利用が可能
応答があるとアドレス
を再構成する必要あり
＜重複アドレス検出＞

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

リンクレイヤアドレスの解決の流れ

fe80::211:22ff:fe33:4455
2001:db8::211:22ff:fe33:4455
MAC:00:11:22:33:44:55

fe80::211:22ff:fe66:7788
2001:db8::211:22ff:fe66:7788
MAC:00:11:22:66:77:88



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

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

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

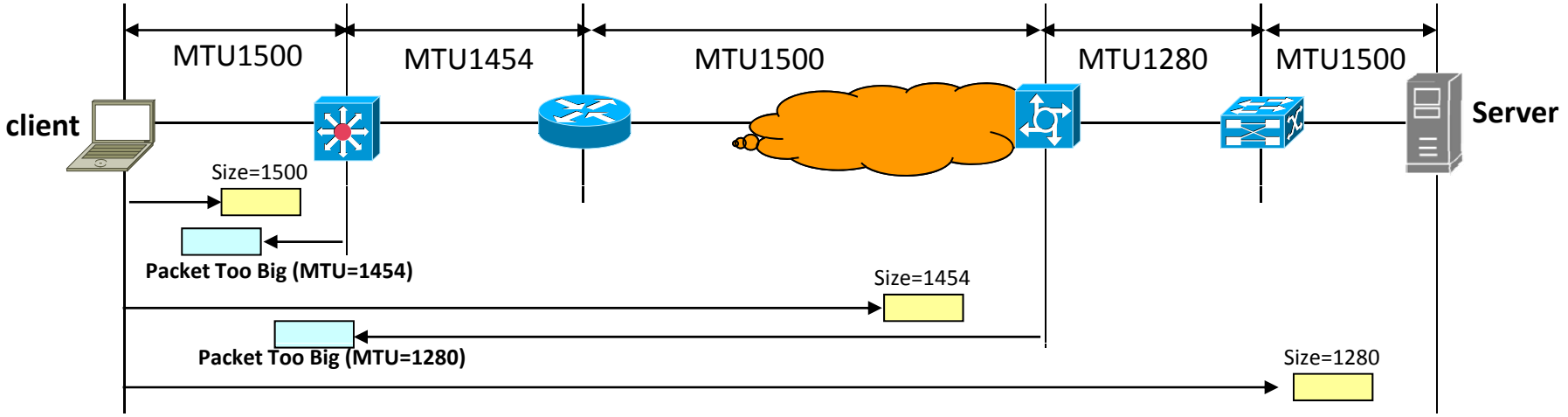
Src MAC 00:11:22:66:77:88
Dst MAC 00:11:22:33:44:55
Src IPv6 fe80::211:22ff:fe66:7788
Dst IPv6 fe80::211:22ff:fe33:4455
ICMPv6 Type 136 Target 2001:db8::211:22ff:fe66:7788 Target MAC 00:11:22:66:77:88

③通信開始

Path MTU Discovery

Path MTU Discovery

- 送信元ホストは送出先リンクのMTUをパスMTUと仮定
- 経由するルータ上でパケットを転送できない場合、ルータはそのパケットを破棄してPacket Too Big（ICMPv6 type2）を送信元に返信する（次ホップへのリンクのMTU情報を盛り込む）
- IPv6の最小MTUは1280バイト
- マルチキャストでも同様
  - 宛先全体の最小MTUとなる
- L2SWのMTUに引っかかった場合には破棄される



セキュリティ

パケットフィルタの基本

- 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
- IPv6での注意点
  - ICMPv6はとめない
    - 特にtype2(Packet Too Big)
  - 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ほぼ必須
- 拡張ヘッダへの対応
  - 単純なパケットフィルタでは対応が難しいものもある
    - RH0、フラグメントヘッダ等
  - ファイアウォールでの検討も必要

パケットフィルタ１（参考）

	Ingress	Egress
必須	[1]全ICMPv6をaccept [2]以下がSourceアドレスとなっているパケットをreject ・予約済みアドレス ::/8 ・元サイトローカルアドレス fec0::/10 ・ユニークローカルアドレス fc00::/7 ・マルチキャストアドレス ff00::/8 ・ドキュメントアドレス 2001:db8::/32 [3]自ASで持っているprefixがSourceアドレスに なっているパケットをreject（トランジット接続）	特になし
オプション	[1]境界インタフェース宛となっているICMPv6パケットの制限をする - 前提条件 1. Neighbor Discovery で使われる ICMPv6 TYPEはaccept をする 2. Path MTU Discovery で使われる ICMPv6 TYPE =2 (Packet Too Big) は accept をする 3.速やかな IPv6/IPv4 フォールバック の為に、ICMPv6 TYPE = 1 (Destination Unreachable)は accept をする [2]境界インタフェース宛となっている上記以外のICMPv6をreject ※traceroute, pingの確認ができなくなる [3]6bone用アドレス（廃止）をreject 3FFE::/16	[1]全てのICMPv6をacceptする [2]以下がSourceアドレスになっているパケットをreject ・予約済みアドレス ::/8 ・元サイトローカルアドレス fec0::/10 ・ユニークローカルアドレス fc00::/7 ・マルチキャストアドレス ff00::/8 ・ドキュメントアドレス 2001:db8::/32 ・ 6bone用アドレス 3FFE::/16

参考：http://www.janog.gr.jp/doc/janog-comment/jc1006.txt

パケットフィルタ２．１（参考）

Recommendations for ICMPv6 Transit Traffic

Traffic that Must Not be Dropped	Destination Unreachable (Type 1) - All codes Packet Too Big (Type 2) Time Exceeded (Type 3) - Code 0 only Parameter Problem (Type 4) - Codes 1 and 2 only Echo Request (Type 128) Echo Response (Type 129)
Traffic that Normally Should Not be Dropped	Time Exceeded (Type 3) - Code 1 Parameter Problem (Type 4) - Code 0 Home Agent Address Discovery Request (Type 144) Home Agent Address Discovery Reply (Type 145) Mobile Prefix Solicitation (Type 146) Mobile Prefix Advertisement (Type 147)
Traffic That Will Be Dropped Anyway (All these messages should never be propagated beyond the link which they were initially transmitted)	Router Solicitation (Type 133) Router Advertisement (Type 134) Neighbor Solicitation (Type 135) Neighbor Advertisement (Type 136) Redirect (Type 137) Inverse Neighbor Discovery Solicitation (Type 141) Inverse Neighbor Discovery Advertisement (Type 142) Listener Query (Type 130) Listener Report (Type 131) Listener Done (Type 132) Listener Report v2 (Type 143) Certificate Path Solicitation (Type 148) Certificate Path Advertisement (Type 149) Multicast Router Advertisement (Type 151) Multicast Router Solicitation (Type 152) Multicast Router Termination (Type 153)
Traffic for Which a Policy Should Be Defined	Seamoby Experimental (Type 150) Unallocated Error messages (Types 5-99 inclusive and 102-126 inclusive) Unallocated Informational messages (Types 154-199 inclusive and 202-254 inclusive)

参考：http://www.ietf.org/rfc/rfc4890.txt?number=4890

パケットフィルタ２．２（参考）

Recommendations for ICMPv6 Local Configuration Traffic

Traffic that Must Not be Dropped	Destination Unreachable (Type 1) - All codes Packet Too Big (Type 2) Time Exceeded (Type 3) - Code 0 only Parameter Problem (Type 4) - Codes 1 and 2 only Echo Request (Type 128) Echo Response (Type 129) Router Solicitation (Type 133) Router Advertisement (Type 134) Neighbor Solicitation (Type 135) Neighbor Advertisement (Type 136) Inverse Neighbor Discovery Solicitation (Type 141) Inverse Neighbor Discovery Advertisement (Type 142) Listener Query (Type 130) Listener Report (Type 131) Listener Done (Type 132) Listener Report v2 (Type 143) Certificate Path Solicitation (Type 148) Certificate Path Advertisement (Type 149) Multicast Router Advertisement (Type 151) Multicast Router Solicitation (Type 152) Multicast Router Termination (Type 153)
Traffic that Normally Should Not be Dropped	Time Exceeded (Type 3) - Code 1 Parameter Problem (Type 4) - Code 0
	Router Renumbering (Type 138)
Traffic That Will Be Dropped Anyway (if the service is not implemented)	Home Agent Address Discovery Request (Type 144) Home Agent Address Discovery Reply (Type 145) Mobile Prefix Solicitation (Type 146) Mobile Prefix Advertisement (Type 147) Seamoby Experimental (Type 150)
	Redirect (Type 137)
Traffic for Which a Policy Should Be Defined	Node Information Query (Type 139) Node Information Response (Type 140) Unallocated Error messages (Types 5-99 inclusive and 102-126 inclusive)

参考：http://www.ietf.org/rfc/rfc4890.txt?number=4890

DHCPv6、DNS

DHCPv6の変更点

- 1つのI/Fに複数のアドレスをアサイン可
- Prefix Delegationを実行する
- BroadcastではなくIPv6マルチキャストを使用
  - All_DHCP_Relay_Agents_and_Servers（FF02::1:2）
    - クライアントからサーバ又はRelay Agentへ向けて
  - All_DHCP_Servers（FF05::1:3）
    - Relay Agentからサーバへ向けて（Unicast Addressを知らないときに使用）
  - ClientはUDP546、サーバ/Relay AgentはUDP547
- メッセージタイプが増えている
  - 特にRenewの明示的なメッセージの実装（IPv4ではRequest）

DHCPv6詳細

- IPv6アドレスはステートレス自動設定、その他情報はDHCPv6で取得、といった使い方も可能
- DHCPv6ではDHCPの利用はRAオプション（M-flag,O-flag）で通知
  - DHCPv4ではホスト依存
- DHCP-PD（RFC3633）
  - 委譲ルータ（delegation router）またはDHCPv6サーバから要求元ルータにプレフィックス情報を送付
  - DHCP-PDとDHCPv6アドレス割り当ては混在可能
- インタフェースIDまでの管理が可能
- DHCPv4と同様のセキュリティ対策が必要
- DHCPv6クライアントはDUID（DHCP Unique Identifier）により識別
  - 1つのクライアントにつき1つの永続的なDUID（IPv4ではMAC）
- DHCPv6はデフォルトルート、プレフィックスを渡せない

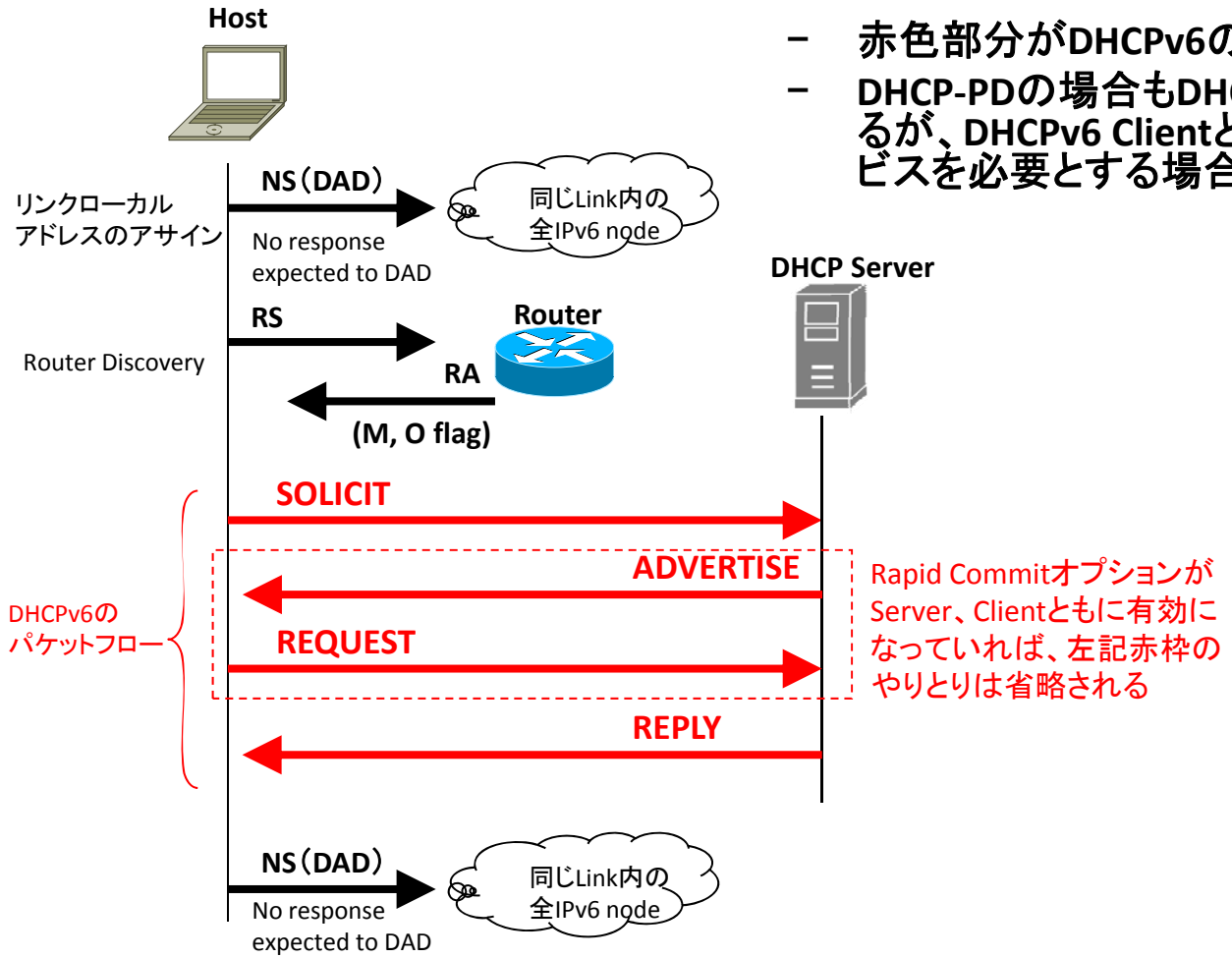
DHCPv6の通信(DHCPv4とほぼ同様)

- クライアントはマルチキャストSOLICIT（要請）メッセージを送信
  - Dst：FF02::1:2（ALL_DHCP_Relay_Agents_and_Servers）
  - Src：interface link-local source
- DHCPサーバ（複数可）からADVERTISEメッセージを応答
  - Dst：client link-local
  - Src：server link-local
- クライアントが選択したDHCPサーバにREQUESTメッセージを送信
  - IAオプション、DUID、要求オプションを記載
- DHCPサーバは要求されたオプションを含んだREPLYメッセージをクライアントに返す

- クライアントはDADを実施

アドレスが既に付与され他の情報を取得したい場合にはINFORMATION REQUESTメッセージを使用（ステートレスDHCP）
  - RAでアドレスを付与されているがOフラグがついているような場合
  - DNS、NTP、SIP・・

DHCPv6パケットフロー



- 赤色部分がDHCPv6のパケットフローを示す
- DHCP-PDの場合もDHCPv6のパケットフローとなるが、DHCPv6 ClientとDHCPv6 PD Clientのサービスを必要とする場合は、別々に要求する

DHCPv6メッセージタイプ

メッセージ種別	番号	発出側	内容	V4相当
Solicit	**1**	**Client**	**DHCPサービスを探す**	**DISCOVER**
Advertise	**2**	**Server**	**Solicitに対してDHCPサービスが有効であることを示す**	**OFFER**
Request	**3**	**Client**	**IPアドレス、オプションの入手を要求**	**REQUEST**
Confirm	4	Client	アサインされたIPアドレスがまだ有効であることを通知	
Renew	5	Client	リース時間延長を要求	REQUEST
Rebind	6	Client	Renewに応答がない場合にこのメッセージを送出してリース時間を要求	
Reply	**7**	**Server**	**Solicit, Request, Renew, Rebind に対するサーバの応答**	**ACK/NACK**
Release	8	Client	アサインされたアドレスが不要である旨の通知	RELEASE
Decline	9	Client	サーバによってアサインされたアドレスがすでに使用中である旨の通知	DECLINE
Reconfigure	10	Server	パラメータの更新があったことを通知	

DNS（IPv6）

- AAAA（クアッドA）を使用（RFC3596）
  - 逆引きのドメインはIPv6.ARPA
    - 圧縮表記なし・・
  - NS、PTRは変更なし
  - BIND8.4以上またはBIND9で実装
- 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OSの対応

- DNSリゾルバの改良（IPv4通信の品質を保つため）
  - Aレコード解決を優先する（FreeBSD、Windows Vista）
    - IPv6が優勢になった時に問題になる可能性あり
  - Aレコード解決時にNXDOMAINならAAAAレコード解決をしない（Windows Vista）
  - Aレコードのレスポンス時間によりAAAAレコードの処理待ち時間を決定（FreeBSD、Windows Vista）
    - AAAAレコードがない場合のタイムアウト時間を小さくするため
- AAAAレコード解決の抑制
  - グローバルIPv6アドレスが付与されない限りAAAAクエリによる名前解決は実施しない（Windows Vista）

DNSクエリの順序

- クエリ順序はOSで異なる
  - FreeBSD-5.5R
    - IPv4の名前解決とIPv6の名前解決を交互に繰り返し名前解決ができた時点で終了
  - Windows XP SP2
    - まずIPv6の名前解決を全て実施し次にIPv4の名前解決を全て実施
  - Windows Vista
    - まずIPv4の名前解決を全て実施し次にNXDOMAINが返されたもの以外の全てに関してIPv6の名前解決を実施

OSPFv3

OSPFv3の特徴

- リンクごとで処理
  - OSPFv3ではネットワーク、サブネット、という用語はリンクに置き換えられている
- OSPFパケットヘッダからアドレス情報を削除
  - IPv6アドレスはOSPFv3パケットのペイロード部分に書き込まれる
- フラッディングスコープの明示
  - リンクローカル、エリア、ASの3種類を定義
- リンクごとのインスタンスを明示的にサポート
  - 同一I/Fに複数のOSPFプロセスを動かすことが可能
- リンクローカルアドレスを使用
  - OSPFパケットの始点アドレスはリンクローカルアドレス
  - リンクローカルアドレスがネクストホップ
- 認証フィールドの削除
  - IPv6プロトコルスタック上でIPSecを利用

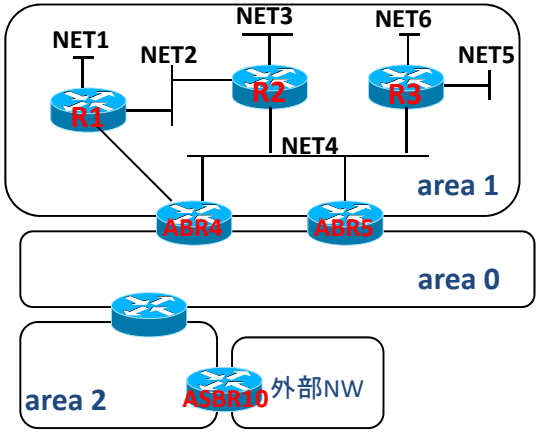
Flooding scope

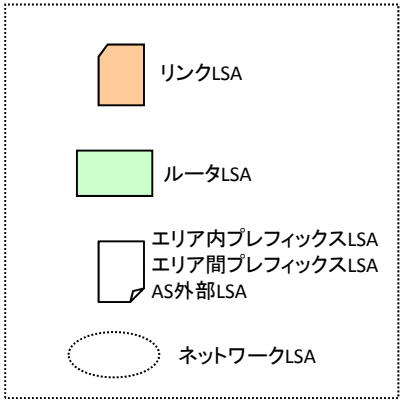
Scope	Link scope	Area scope	AS scope
Flooding area	リンク内でのみflooding	エリア内でのみflooding	全OSPFルータにflooding
LS Type	リンクLSA	ルータLSA ネットワークLSA エリア間プレフィックスLSA エリア間ルータLSA エリア内プレフィックスLSA	AS外部LSA
LSDB Type	Link LSDB	Area LSDB	AS LSDB

LSタイプ

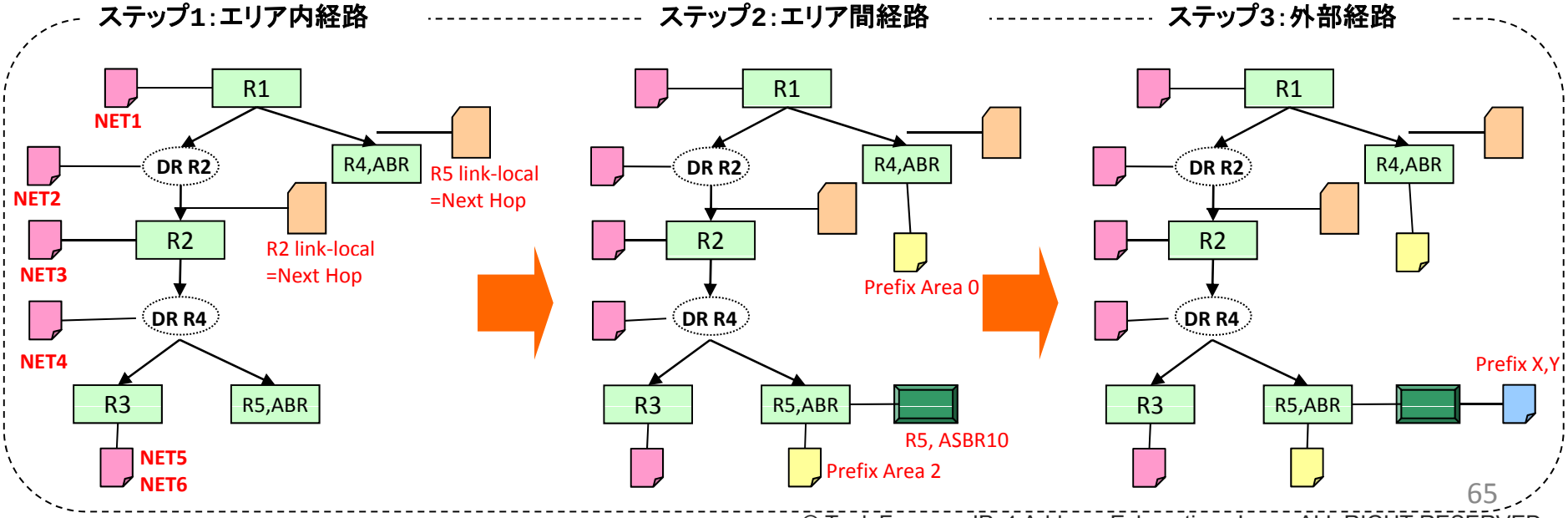
LSタイプ	名称	Flooding scope	広告元	記述内容	備考
0x2001	Router-LSA	エリア	各ルータ	インタフェース情報	prefix情報はなし
0x2002	Network-LSA	エリア	DR	DR管轄のルータ情報	prefix情報はなし
0x2003	Inter-Area-Prefix-LSA	エリア	ABR	他エリアのprefix	旧Summary link Prefixを搬送
0x2004	Inter-Area-Router-LSA	エリア	ABR	ASBRへの経路情報	旧AS Summary link Prefixを搬送
0x4005	AS-External-LSA	AS	ASBR	外部IPv6 prefix	再配送関連のprefixを搬送
0x2006	Group-Membership-LSA	エリア	RFC1584参照		
0x2007	Type 7 LSA	エリア	RFC3101参照		
0x0008	Link-LSA	リンク	各リンク上の各ルータ	Link local address IPv6 prefixリスト	Link区間のaddressを搬送
0x2009	Intra-Area-Prefix-LSA	エリア	各ルータ	Area内のprefix	ルータ、ネットワークリンクのIPv6プレフィックスを搬送

OSPFv3のルーティングテーブル計算





[R1を起点としたSPFツリー]



OSPFv3設定時の留意事項

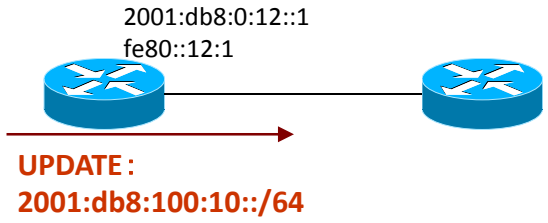
- ルータID
  - ルータID（32bit）の設定が必要
- リンクローカルアドレス
  - ネクストホップがリンクローカルアドレスになる
  - Neighborのリンクローカルアドレスを全てFE80::1などとやるとルーティングテーブルの確認が困難になる可能性も
    - ただ出力I/Fも当然表示されるのでそれほど問題ではないかも
- リンクローカルマルチキャストアドレス
  - ff02::5 AllSPFRouters（全てのOSPFルータ）
  - ff02::6 ALLDRouters（全てのOSPF DR/BDR）
- 認証がIPSec
  - 機器によってはサポートしていない場合も
  - 異機種の相互接続時には確認必要

BGP4+

BGP4+（IPv6）

- 基本的にはIPv4とほぼ同様
  - 元々マルチプロトコル用途のため。RFCも共通（RFC4760）
- BGP経路配送
  - IPv4ではNLRIとPath Attributeからなる
  - IPv6ではNLRIは使用不可
    - IPv6ではMP_REACH_NLRI、MP_UNREACH_NLRIを使用
- BGPメッセージタイプ（変更なし）
  - OPEN・・・パラメータの交換
  - UPDATE・・利用可能経路や取り消された経路を交換
  - NOTIFICATION・・エラーの報告、コネクションの切断
  - KEEPALIVE・・・対向の生死確認

BGP4+のパケット内容



BGP Update

Border Gateway Protocol
UPDATE Message
Marker: 16 bytes
Length: 98 bytes
Type: UPDATE Message (2)
Unfeasible routes length: 0 bytes
Total path attribute length: 75 bytes
Path attributes

IPv4で使われていたNEXT_HOP、NLRIはなし
ORIGINやAS_PATHなど他のものは共通

ORIGIN: IGP (4 bytes)
AS_PATH: 65535 (7 bytes)
MULTI_EXIT_DISC: 0 (7 bytes)

削除の場合はMP_UNREACH_NLRI
（IPv4でのWithdrawn相当）

MP_REACH_NLRI (57 bytes)
Flags: 0x80 (Optional, Non-transitive, Complete)
Type code: MP_REACH_NLRI (14)
Length: 54 bytes

IPv6のAFIは2
SAFIはは1

Address family: IPv6 (2)
Subsequent address family identifier: Unicast (1)

IPv6のNextHopアドレスを記述

Next hop network address (32 bytes)
Next hop: 2001:db8:0:12::1 (16)
Next hop: fe80::12:1 (16)
Subnetwork points of attachment: 0

IPv6のprefix情報を記述

Network layer reachability information (17 bytes)
2001:db8:100:10::/64

BGP4+設定時の留意事項

- ルータID
  - 32bitのルータIDが必要
- ピアアドレス
  - グローバルアドレス、リンクローカルアドレスどちらも使用可能だが、グローバルでpeerを張るべき
    - リンクローカルでpeerを張る場合にはNextHopSelfが必要
- ASの区別
  - 自AS番号をIPv4/v6で別に定義できる機器も

BGPでのIPv6経路制御

	Ingress	Egress
必須	[1] 以下の Special-Use Prefix を reject する - デフォルト ::/0 exact - 予約済み Prefix ::/8 or longer - リンクローカルアドレス fe80::/10 or longer - 元サイトローカルアドレス fec0::/10 or longer - ユニークローカルアドレス fc00::/7 or longer - マルチキャストアドレス ff00::/8 or longer - ドキュメントアドレス 2001:db8::/32 or longer [2] 自 AS で持っている Prefix を reject する	[1] 自 AS で持っている Prefix を aggregate して accept をする [2] 以下の Special-Use Prefix を reject する - デフォルト ::/0 exact - 予約済み Prefix ::/8 or longer - リンクローカルアドレス fe80::/10 or longer - 元サイトローカルアドレス fec0::/10 or longer - ユニークローカルアドレス fc00::/7 or longer - マルチキャストアドレス ff00::/8 or longer - ドキュメントアドレス 2001:db8::/32 or longer [3] プライベート AS 番号を外部に広告しないようにする
オプション	[1] 細かい Prefix (Long Prefix) を reject する [2] 各 RIR から各組織に割り振り済みの Prefix のみを accept する ※ RIR の IP アドレス割り振りリストが更新される度に、 フィルタの設定の更新を行う必要があります [3] 一定値以上の長い AS-PATH 長の経路を reject する	特になし

参考：http://www.janog.gr.jp/doc/janog-comment/jc1006.txt

Edge機能関連（HSRPv2/VRRPv3、uRPF）

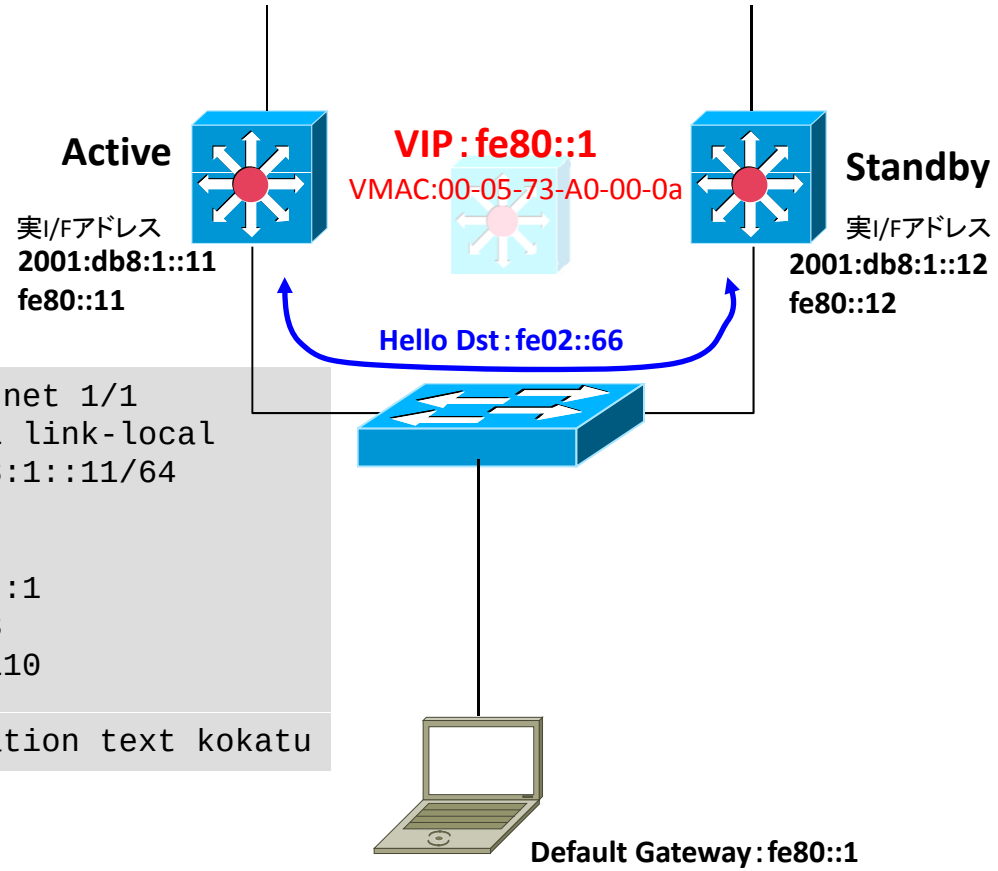
HSRPv2（IPv6）の主な特徴

- VIPがリンクローカルアドレスとなる
  - 例：fe80::1
  - 配下のホストのデフォルトルートもリンクローカルアドレスにする
- VMACの変更
  - 00-05-73-a0-0x-xx（HSRPv1は00-00-0c-07-ac-xx ）
    - Group番号が0-4095に拡張（HSRPv1では0-255）
- Helloパケットの宛先
  - ff02::66（33:33:00:00:00:66）（HSRPv1では224.0.0.2）
- ポート番号
  - UDP：2029（HSRPv1では1985）
- ActiveルータがRAを送信し、Backup側はsuppressする
- StateはHSPRv1と同じ
  - Init、Learn、Listen、Speak、Standby、Active
- 認証は平文 or MD5

参考：HSRPv2（IPv4）

- VMAC
  - 00-00-0C-9f-fx-xx（HSRPv1は00-00-0c-07-ac-xx ）
- Helloパケットの宛先
  - 224.0.0.102（01-00-5e-00-00-66 ）（HSRPv1では224.0.0.2）
- ポート番号
  - 1985（HSRPv1と同様）
- IOS 12.3Tからサポート

HSRPv2（IPv6）動作イメージ




```
Interface GigabitEthernet 1/1
 ipv6 address FE80::11 link-local
 ipv6 address 2001:db8:1::11/64
 ipv6 enable
 standby version 2
 standby 10 ipv6 FE80::1
 standby 10 timers 1 3
 standby 10 priority 110
 standby 10 preempt
 standby 10 authentication text kokatu
```

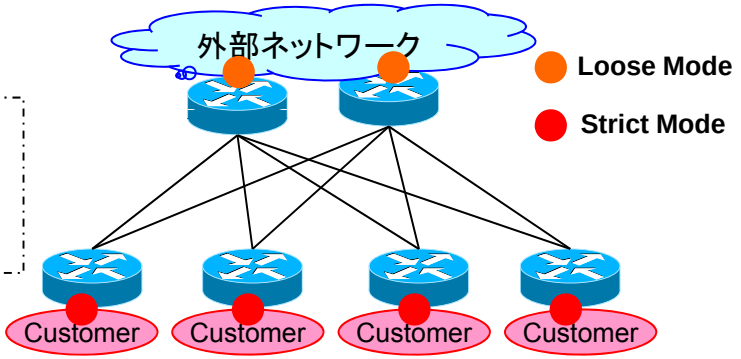
VRRPv3

- まだRFC化はされていない
  - 最新（23-Oct-2009）は”draft-ietf-vrrp-unified-spec-04”
- VIPはリンクローカルアドレス
- VMACは00-00-5e-00-02-xx（IPv4では00-00-5e-00-01-xx ）
  - VRIDは1-255
- Helloの始点アドレスはI/Fのリンクローカルアドレス
- Helloのdstはff02::12（IPv4では224.0.0.18）
- Hop Limitは255
- Next Headerは112
- MasterがRAを送信し、BackupはRAを送信しない
- StateはVRRPv2と同様（Initialize、Master、Backup）
- 認証フィールドはなし

uRPF（復習）

- uRPF（Unicast Reverse Path Forwarding）
  - パケットの始点アドレスが経路情報に存在するかどうかを確認し、存在しなければ破棄
  - ACLを手動で設定する必要がないため作業負荷が軽減
  - Loose Mode：始点アドレスが経路情報に存在すれば転送
  - Strict Mode：始点アドレスが経路情報に存在し、且つそのパケットを受信したI/Fが送信先となっていれば転送

外部ネットワークとの接続I/Fに対してはLoose Mode
ユーザとの接続I/Fに対してはStrict Mode
というような使い方がIPv4では使われています



IPv6 uRPFの注意事項

- 学習されていない経路からPacket Too BigのICMPv6が返ってきた場合にはuRPFで破棄されてしまう
  - 議論中ではあるがuRPFの前にICMPv6（特にPacket Too Big）は必ず通すような実装が必要
    - 各ベンダーに確認が必要
    - HW処理されるかどうかも確認必要

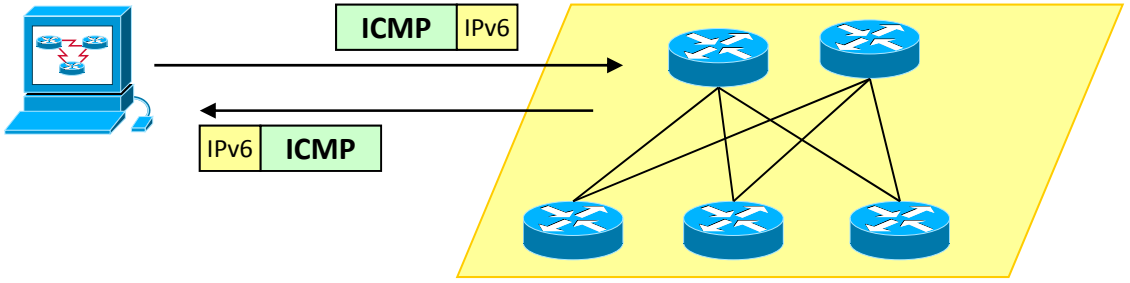
運用、監視

監視の分類

- インバンド監視
  - サービス死活監視：**ping**、http、smtp、ftp・・
  - サービス品質計測：RTT、Jitter、SLA・・
- アウトバンド監視
  - 機器情報の取得：**SNMP、Syslog**
  - トラフィック監視：MRTG、**flow**

インバンド監視

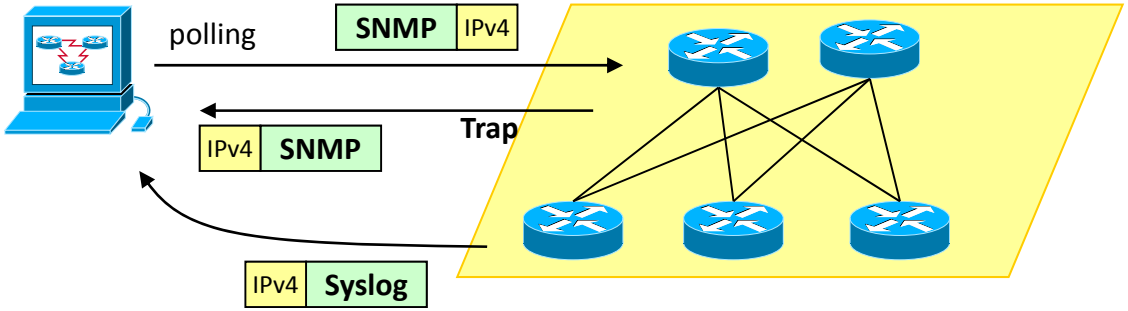
- サービス死活監視
  - ICMPv6などを利用した監視ツールが必要
  - 場合によってはアプリケーション側でのIPv6対応も必要
- サービス品質計測
  - ICMPv6などによるSLA計測



アウトバンド監視（SNMP・Syslog）

- SNMP
  - ノードの情報・状態を取得するためのプロトコル
    - トランスポートがIPv4であってもIPv6の情報が取得できれば問題はない
    - トランスポートまでもIPv6化するのはさらに次のステップ
      - SNMP側はプロトコル非依存なので問題ないはずだが、対応製品が少ない
    - IPv4/v6共に障害が発生した場合には複数IP（複数機器）で障害が発生したように見えるため、ノードの対応付けが重要

- Syslog
  - ノードのログ情報をエクスポートするためのプロトコル
    - トランスポートがIPv4であってもIPv6のログ情報は取得できるので問題はない
    - トランスポートまでもIPv6化するのはさらに次のステップ



IPv6 MIB

- IPv4/v6ごとのトラフィックを採取することはできない
  - IPv4/v6で物理I/F、vlanを分ける
  - xFlowを使う
    - 流量が異なりすぎる場合には注意が必要

IPv6基本MIB	RFC4293	IPv6,ICMPv6含むIP全般のMIB
その他IPv6関連MIB	RFC4668～4671	IPv6 Radius関連MIB
	RFC4295	Mobile IPv6 MIB
	RFC3595	IPv6 Flow Label MIB
	RFC3019	MLD MIB
アドレス表現	RFC4001	InetAddress MIB

IPv6アドレスMIB

ipAddressPrefixTableで指定したI/FのIPv6アドレスを取得

オブジェクト	内容
ipAddressPrefixIfindex	InterfaceIndex（IfIndex）
ipAddressPrefixType	InetAddressType（IPv4/v6を識別）
ipAddressPrefixPrefix	InetAddress（IPアドレス）
ipAddressPrefixLength	InetAddressPrefixLength（プレフィックス長）

Routing MIB

- ~~OSPFv3~~、BGP4+ともにRFC標準化はされていない
  - ベンダーMIBでのサポートが必要
  - ベンダーMIBがない場合には、IPv6でのみOSPF、BGPがdownした場合には障害に気付くことが困難

内容	RFC/ID	Date	Status
OSPFv3 MIB	RFC5643 ~~draft-ietf-ospf-ospfv3-mib-16~~	2009-08	PROPOSED STANDARD
BGP4 MIB	draft-ietf-idr-bgp4-mibv2-09	2009-02-18	Active
VRRPv3 MIB	draft-ietf-vrrp-unified-mib-06	2006-12-15	Expired
TCP MIB	RFC4022	2005-03	PROPOSED STANDARD
UDP MIB	RFC4113	2005-05	PROPOSED STANDARD

OSPFv3 SNMP Trap

RFC5643

NOTIFICATIONS	意味	Trapの内容
ospfv3NbrStateChange	change in the state of a OSPFv3 neighbor	ospfv3RouterId ospfv3NbrState
ospfv3IfConfigError	configuration parameters conflict	ospfv3RouterId
ospfv3ifRxBadPacket	OSPFv3 packet that cannot be parsed has been received	ospfv3IfState ospfv3PacketSrc ospfv3PacketType
ospfv3IfStateChange	change in the state of a OSPFv3 interface	ospfv3RouterId ospfv3IfState

BGP SNMP Trap

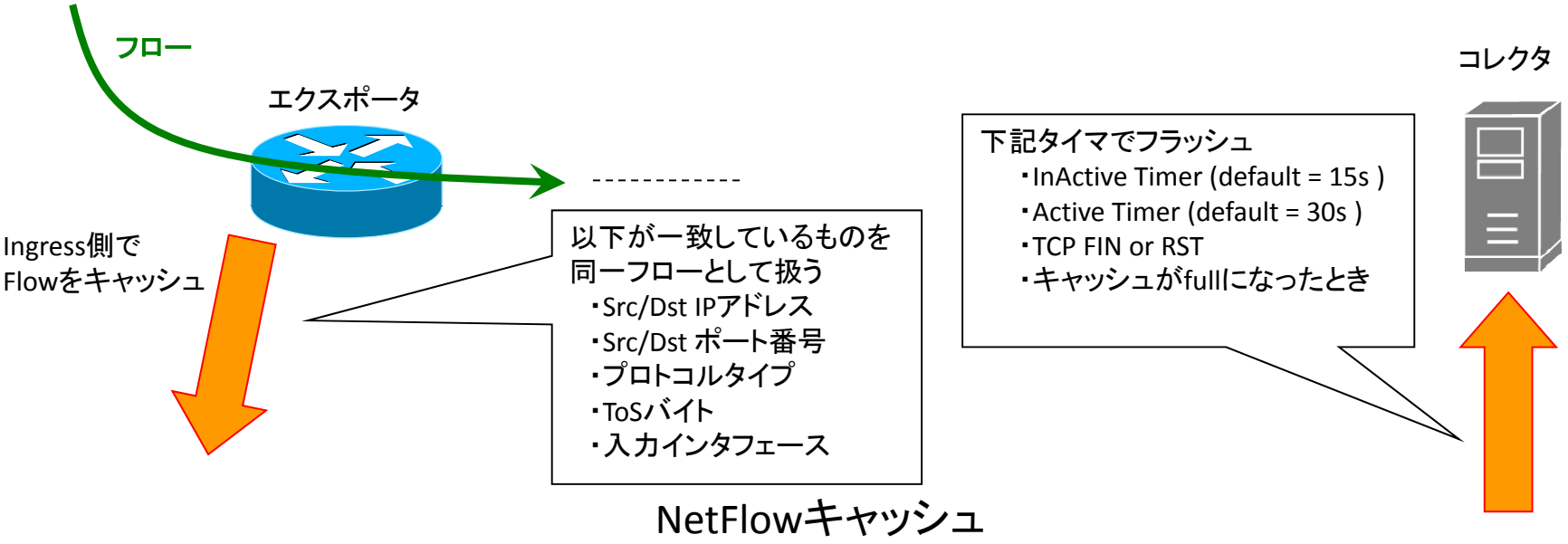
http://www.ietf.org/internet-drafts/draft-ietf-idr-bgp4-mibv2-09.txt

NOTIFICATIONS	意味	Trapの内容
bgp4V2EstablishedNotification	Established state	bgp4V2PeerState bgp4V2PeerLocalPort bgp4V2PeerRemotePort
bgp4V2BackwardTransitionNotification	out of the Established state	bgp4V2PeerState bgp4V2PeerLocalPort bgp4V2PeerRemotePort bgp4V2PeerLastErrorCodeReceived bgp4V2PeerLastErrorSubCodeReceived bgp4V2PeerLastErrorReceivedText

Flow（IPv6）

- NetFlow
  - Cisco systems社が開発
  - Version9（RFC3954）にてIPv6フロー対応
    - テンプレート機能によりフォーマットが拡張可能に
    - IPFIX（IP Flow Information Export）のベース
- sflow
  - InMon社が中心となって開発
    - Brocade,Extreme,HP,AlaxalA,Force10,NECなどが実装
  - sFlowV4（RFC3176）でIPv6をサポート
    - sFlowV5はsFlow.orgに仕様公開

NetFlowの動作



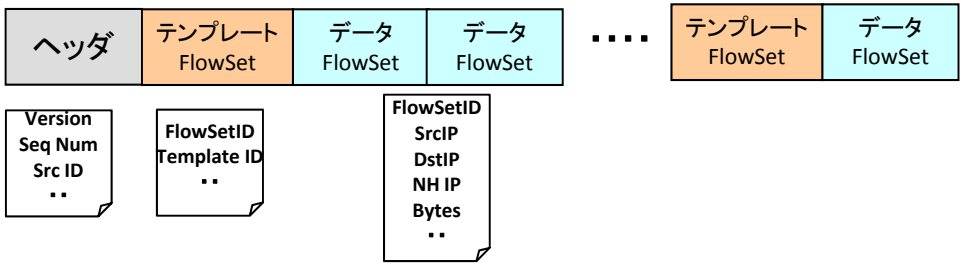
NetFlowキャッシュ

Src IF	Src IP	Dst IF	Dst IP	Protocol	Bytes	Packets	・・・	Active	Idle
3	a.a.a.a	5	x.x.x.x	6	3126	8		305	3
5	b.b.b.b	8	y.y.y.y	17	2094	15		1850	21
12	c.c.c.c	10	z.z.z.z	1	5076	22		56	10

NetFlowV9パケット形式

NetFlowヘッダに続き1つ以上のテンプレートFlowSetとデータFlowSetから構成される

Export Packet



テンプレートFlowSetでのIPv6用フィールド

Field Type	Value	Length	Description
IPv6_SRC_ADDR	27	16	IPv6 source address
IPV6_DST_ADDR	28	16	IPv6 destination address
IPV6_SRC_MASK	29	1	Length of the IPv6 source mask in contiguous bits
IPV6_DST_MASK	30	1	Length of the IPv6 destination mask in contiguous bits
IPV6_FLOW_LABEL	31	3	IPv6 flow label as per Length of the IPv6 destination mask in contiguous bits
IP_PROTOCOL_VERSION	32	1	Internet Protocol Version Set to 4 for IPv4, set to 6 for IPv6
IPV6_NEXT_HOP	60	16	next-hop router
BGP_IPV6_NEXT_HOP	62	16	Next-hop router in the BGP domain
IPV6_OPTION_HEADERS	63	4	Bit-encoded field identifying IPv6 option headers found in the flow

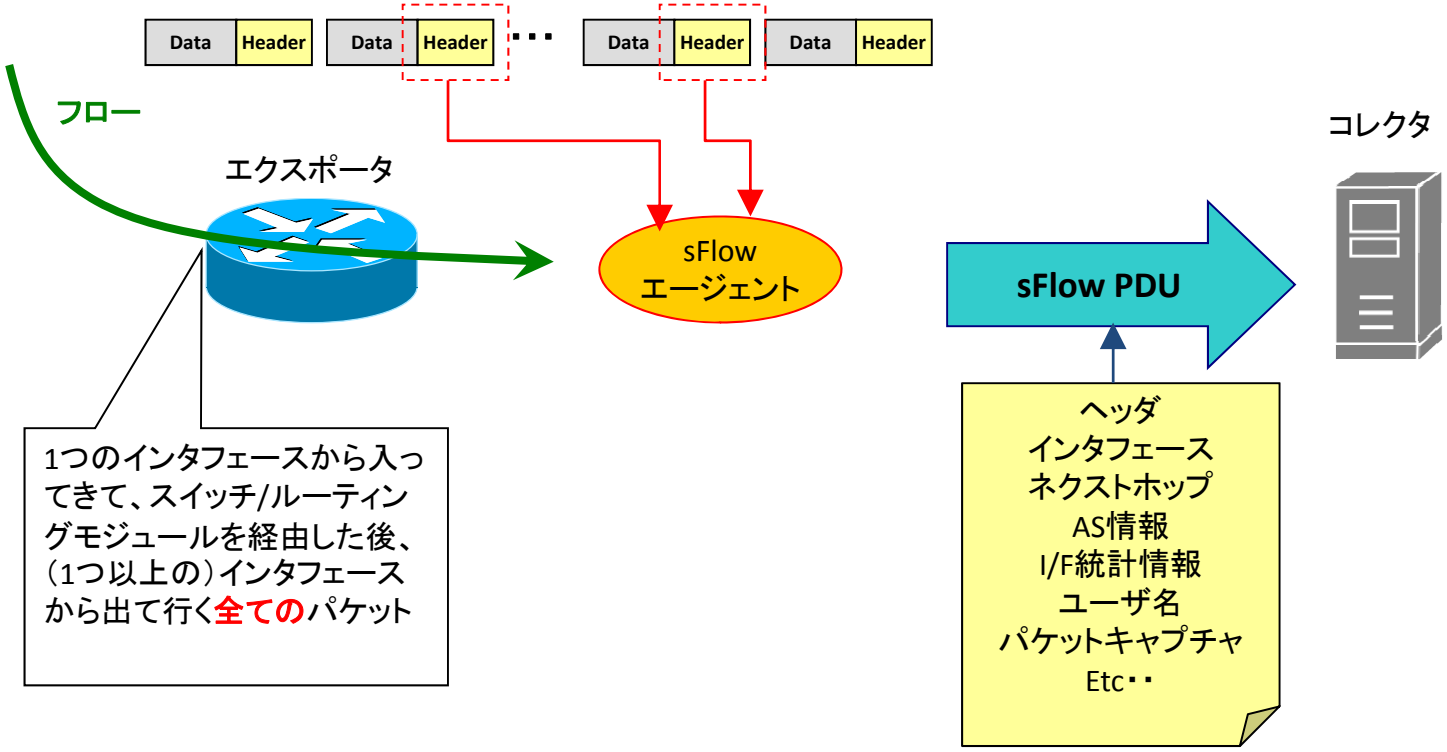
（参考）NetflowV5フローレコード

フィールドが決められているため、128bitのIPv6アドレスは埋め込むことができない

<table>
<tr><td colspan="4">Src IP</td></tr>
<tr><td colspan="4">Dst IP</td></tr>
<tr><td colspan="4">next hop</td></tr>
<tr><td colspan="2">Input Interface Number</td><td colspan="2">Output Interface Number</td></tr>
<tr><td colspan="4">Packet数</td></tr>
<tr><td colspan="4">Octet数</td></tr>
<tr><td colspan="4">最初にフローが観測されたsysuptime</td></tr>
<tr><td colspan="4">最後にフローが観測されたsysuptime</td></tr>
<tr><td colspan="2">Src port</td><td colspan="2">Dst port</td></tr>
<tr><td>Padding</td><td>TCP flag</td><td>Protocol</td><td>ToS</td></tr>
<tr><td colspan="2">送信元AS番号</td><td colspan="2">送信先AS番号</td></tr>
<tr><td>送信元ネットマスク</td><td>送信先ネットマスク</td><td colspan="2">Padding</td></tr>
</table>

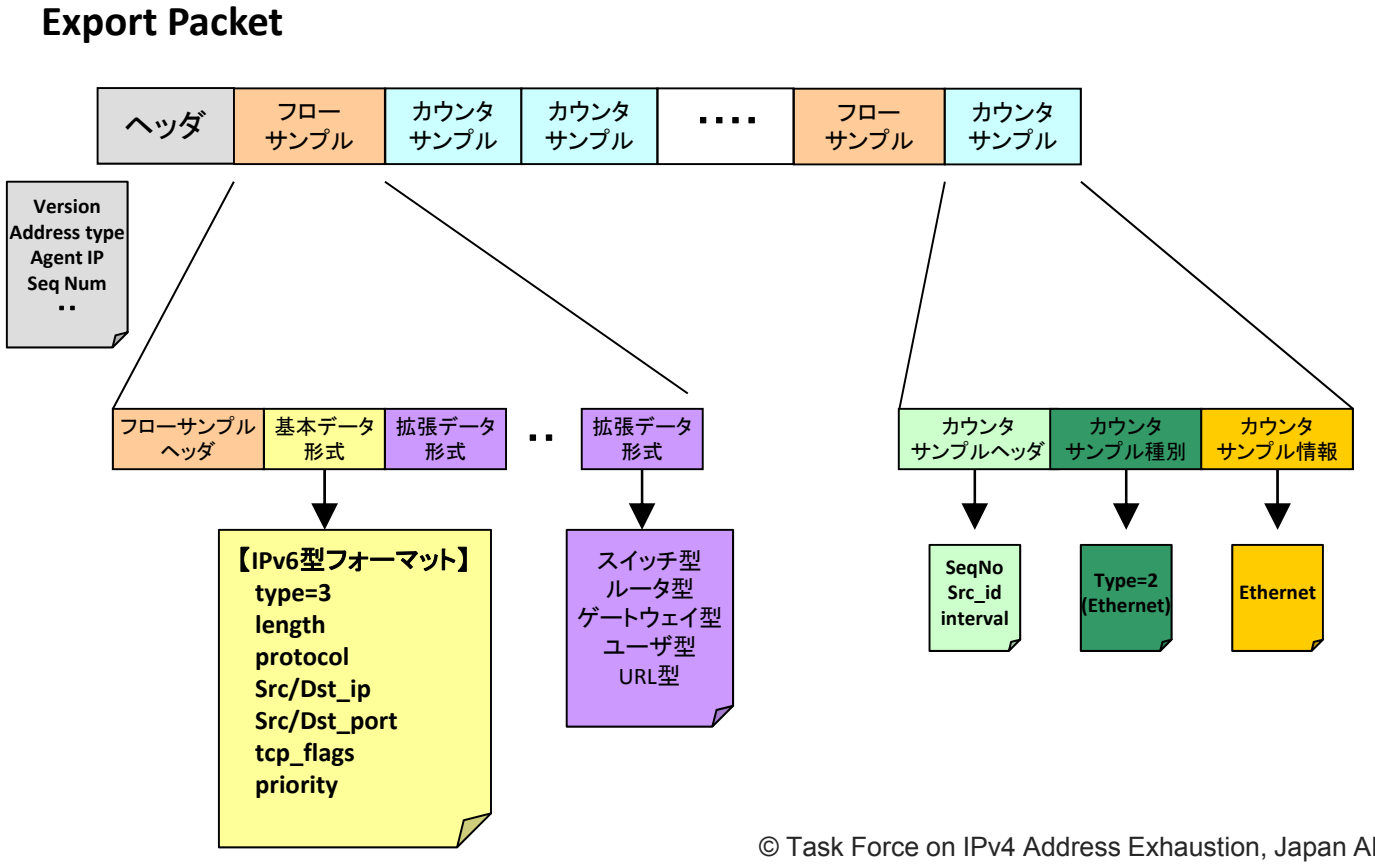
sFlowの動作

- sFlowは”サンプルベース”のテクノロジー
  - NetFlowのようなフローキャッシュは持たない



sFlowパケット形式

sFlowヘッダに続く1つ以上のフローサンプルとカウンタサンプルから構成される



IPv6 Flowの問題点

- IPv6トラフィックはIPv4トラフィックに比べ圧倒的に量が少ない
- sampling-rateはノード単位で設定する機器が多いため、IPv6個別のsampling-rateを設定することが困難
  - IPv4/v6 DualStackの場合にはsampling-rateの設定に注意が必要