IPv6の最前線から
–開発/運用現場からの報告–

鈴木伸介

suz@crl.hitachi.co.jp, suz@kame.net
http://www.kame.net/~suz/ciaj/

目次

- IPv4で現在何が困っているか?
- IPv6だとそれがどう救われるか?
- IPv6プロトコル概略
- IPv6の現状 (ベンダ,サービス)
- IPv6の課題

IPv4インターネットでの悩み...

□家庭の悩み
- ○Windows Messenger等のアプリがNATを通れない
- ○外からVirus攻撃を受けてしまう

□企業の悩み
- ○サブネット内でアドレスが足りなくなる度にアドレス振り直し
- ○Virusを会社に持ち込む人

□ISPの悩み
- ○経路エントリ増大によるルータ負荷
- ○顧客数変動によるアドレッシング変化
- ○アドレス・ポートスキャン攻撃

多くの問題の根源はアドレス不足

□アドレス振り直し

□NAT
- ○アドレスの使い回しを効率化する代わりに　動くアプリに制約

□Virus攻撃
- ○スキャン攻撃は　アドレス数が少ないからできる

□経路エントリ増大によるルータ負荷
- ○アドレス幅が少ないために経路集約しにくい

IPv4アドレス空間の狭さ

- 1サブネットにつき　2アドレスは必ず消費される
  - network address
  - broadcast address
- 更に最低1アドレスは消費される
  - ルータやサーバの分

ネットマスク長	アドレスを割り振れる端末数
/30	1
/29	5
/28	13
/27	29
/26	61
/25	125

IPv6はIPv4の再設計

- IPv4は1970年前半に生まれた技術
  - 当時32bitは膨大だったが　今はそうでもない
  - 必要な技術を後付けしたために　仕様拡張に無理が出てきた
- IPv6=IPv4の再設計によりIPv4の抱える問題を解決
  - アドレス空間の拡大
    - 32bit -> 128bit (髪の毛の幅 -> 銀河系の直径)
  - IPv4に後から追加された機能を標準盛込
    - Plug & Play, Multicast, IPsec, QoS etc

アドレス空間が広いと嬉しいこと

□NATの諸々の制約から解放される

=> ネットワーク設計の自由度向上・単純化

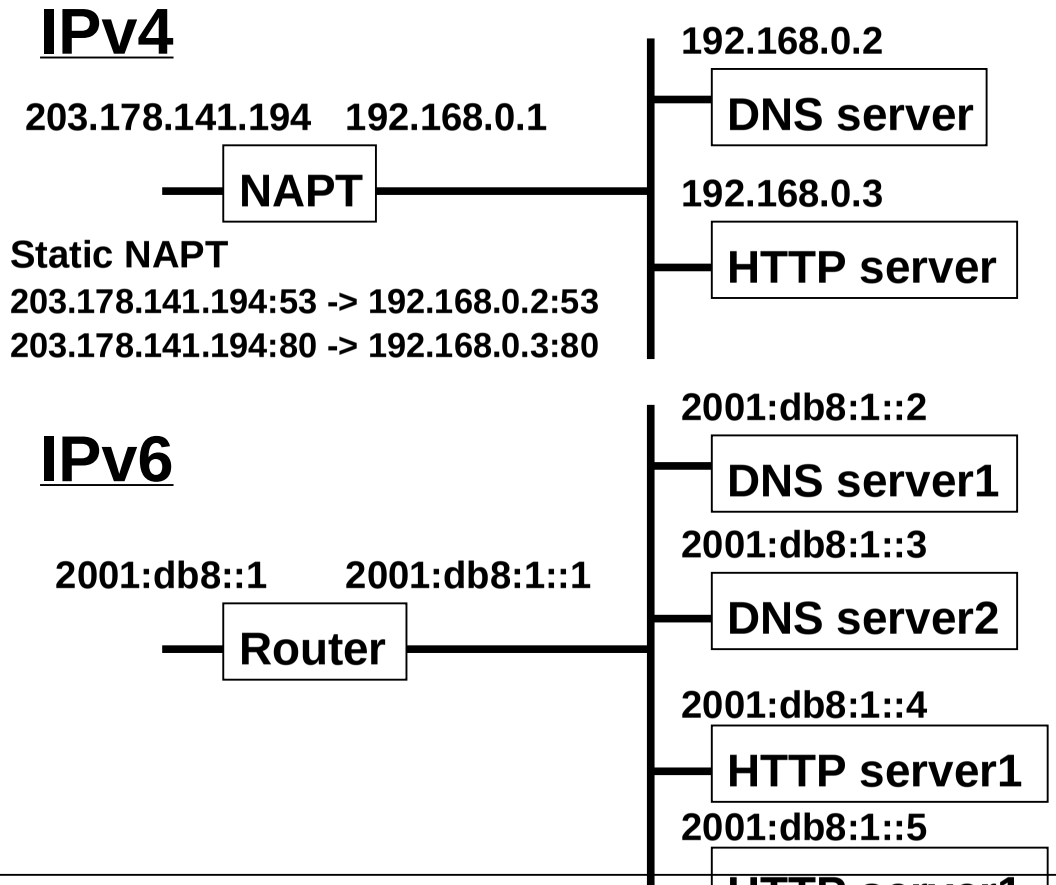
○サブネットの切り直し不要, IPsec, peer to peer application, netgame, 自宅webサーバ, multicast, 経路集約の容易化

□パソコン以外の物にもIPアドレスを振れる

=> 新規サービスの創生

○家電, センサ, 車, ペット, 弁当箱

NATの制約



アドレス空間が広いと嫌なこと

- 今までNATで守られていた人がthe Internetにさらされる
  - 運用で回避可能
- アドレスが覚えられない
  - URLをクリックするだけなら覚える必要がない

IPv6でもまだ救われない部分

- Virusを会社に持ち込む人
  - Virus付きメール を投げることまでは防御不能
  - アドレスポート・スキャン攻撃はIPv6だと困難
- Multicast, IPsec, QoS
  - 機能は標準で盛り込まれた
  - これらの技術自体、IPv4/v6に拘らず難しい

IPv6懐疑論者からの反論

- □NATがないからセキュリティが低い?
- □固定グロー バルアドレスを持つと危険?
- □IPv4アドレス枯渇は嘘?
- □とはいってもIPv4がないと困る
- □私は今のIPv4で満足している...

NATがないからセキュリティが低い?

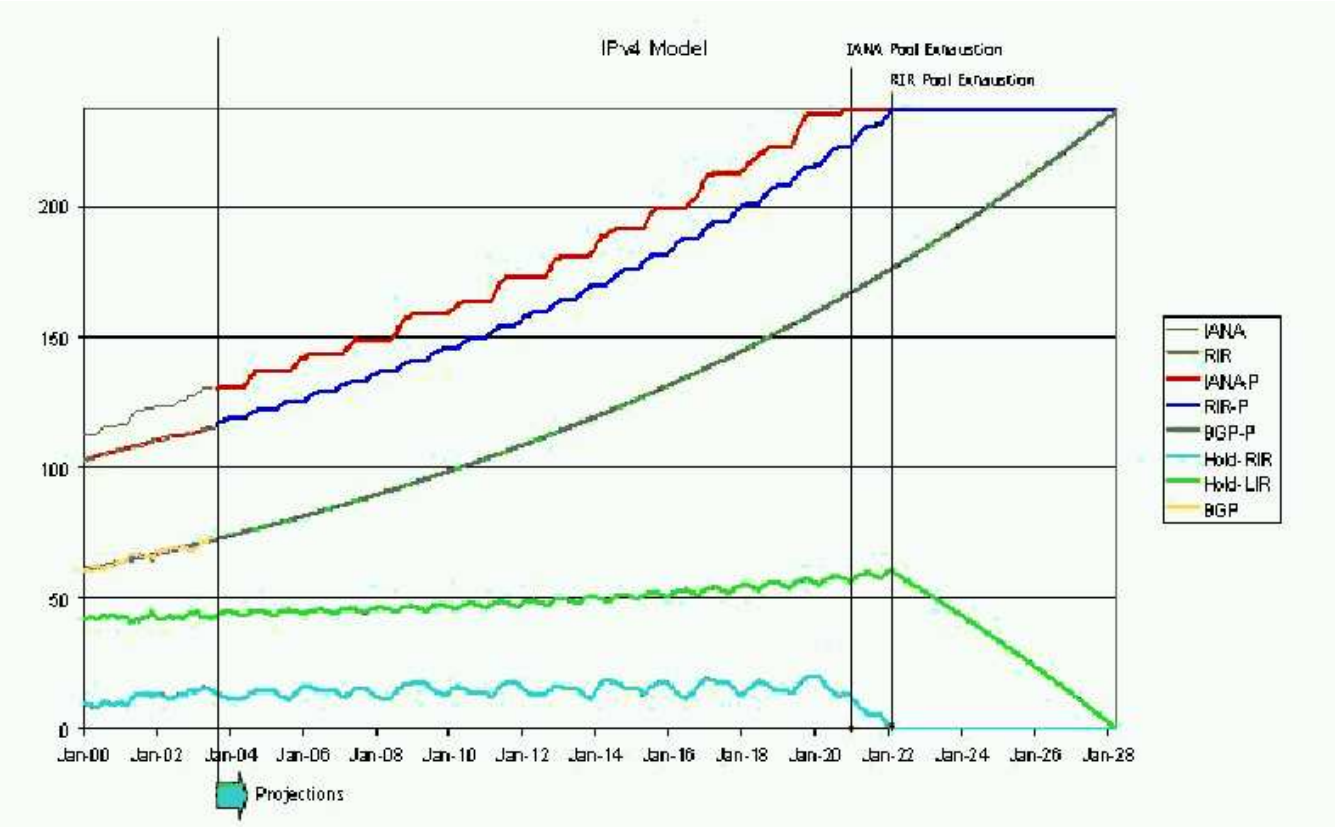
- □NATは所詮アドレス変換デバイス
  - ○外からの直接通信を防ぎやすくするだけ
- □IPv6でも外からの直接通信を防げる
  - ○パケットフィルタやファイアウォール
  - ○ネットワー ク用途の都合次第で　防ぐも防がないも自由
- □NATがあるとセキュリティ向上、というのはそもそも勘違い
  - ○Nimda, MS-Blaster, W32SoBig?

固定グローバルアドレスを持つと危険?

- 固定グローバルアドレス ≠ 外部通信
  - 必要ならproxyを介して通信してもいい
  - パケットフィルタやファイアウォールで通信遮断するのは容易
- グローバルアドレスの下64ビットを付け替えながら通信する技術もある

```
c:\> ipconfig
 Windows IP Configuration
 Ethernet adapter ローカル エリア接続:
  Connection-specific DNS Suffix :
  IP Address . . . . : 2001:db8:1:2:200:e2ff:fe16:81d4
  IP Address . . . . : 2001:db8:1:2:854e:aac6:636e:eca1
```

IPv4アドレス不足は嘘?



IPv4アドレス不足は嘘? (cont.)

- 2015~20年位までは大丈夫
  - 現状のアドレス消費トレンドからの解析結果
- 大前提
  - 近未来の環境変化は予測の対象外
    - 中国, インド, 携帯 etc
  - 各国NICのアドレス出し渋り
    - 我々がIPv4アドレスを簡単にもらえるようになるわけではない...

とはいってもIPv4がないと困る

- IPv6->IPv4への変換技術はいろいろある
  - 逆は難しい
- IPv4とIPv6とは共存可能
  - IPv4とIPXが共存していたのと同じ
- 選択肢は2つある
  - IPv4, IPv6共存
  - IPv6 + IPv6->IPv4変換
- どちらを使うかはケースバイケース

私は今のIPv4で満足している...

- 外部ASPに全部必要なデータやサーバは置いているから　社内はPrivate Addressで十分
- 今日現在のインターネット/イントラネットのままでいい?
  - IPv6を導入しなくてもOKでしょう
- 将来拡張を考える?
  - IPv6にしておいた方がなにかと便利

IPv6プロトコル概要

- IPv6アドレス
  - 書式
- IPv6での通信手順
  - Plug & Play
  - Neighbor Discovery
  - Multicast
  - Path MTU Discovery
  - Routing
- IPv6への移行
  - トンネリング
  - Dual Stack
  - トランスレータ

IPv6アドレスの表記方法

- 16bit毎に":"で分断した16進表記
  - 2001:0db8:1111:0000:0200:87ff:fe80:9850
- 先頭の0は省略可能
  - 2001:db8:1111:0:200:87ff:fe80:9850
- ":0:0:..."は1回だけ"::"に省略可能
  - 2001:db8:1111::200:87ff:fe80:9850
- プレフィックス長は"/(数字)"と書く
  - 2001:db8:1111::200:87ff:fe80:9850/64
- URLにIPv6アドレスを書くときは[]で括る

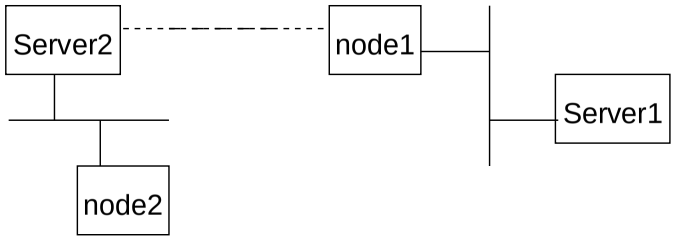
http://[2001:db8:1111::200:87ff:fe80:9850]:8080/

IPv6アドレスの種類

- 通信相手数による分類
  - unicast, multicast, anycast
- 通信可能範囲(=スコープ)による分類
  - linklocal, sitelocal, global
- 特殊アドレス
  - loopback(::1), unspecified(::),
  - ipv4-mapped(::ffff::/96), ipv4-compatible(::/96)

通信相手数による分類

- unicast
  - 相手が単数
- multicast
  - 相手が複数
  - ブロードキャストを吸収
- anycast
  - サービスを抽象化
  - 「あるサービスを提供する端末のうち、最も近くのもの」

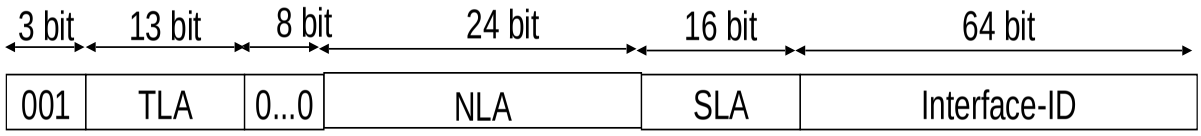


IPv6アドレスのスコープ

- linklocal
  - リンクの中でのみ一意なアドレス
  - 複数リンク間での重複可
- site local
  - 「サイト」内でのみ一意なアドレス
  - 複数サイト間での重複可 -> 廃止の方向
- global
  - 世界で一意なアドレス

IPv6アドレスのフォーマット

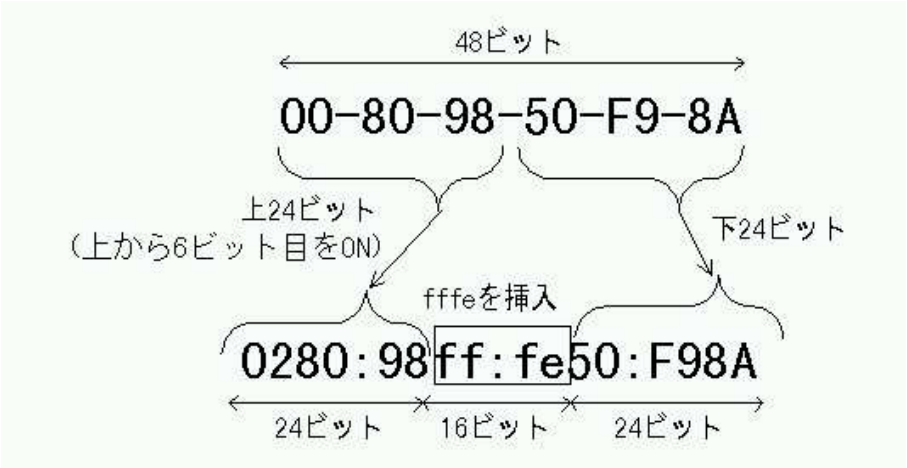
□(プレフィックス):(インターフェースID)
- ○プレフィックスは階層構造
- ○アドレス集約が簡単->経路表エントリ数削減



□但し、
- ○linklocal="fe80::(インターフェースID)"
- ○multicast="ff0X::(適当なID)"
  - ▹X=2(linklocal), 5(sitelocal), e(global)

インターフェースID

□同一ネットワー ク内でダブらないホストID
- ○IEEE EUI-64に従う
- ○大抵は　EthernetのMACアドレスを元に生成



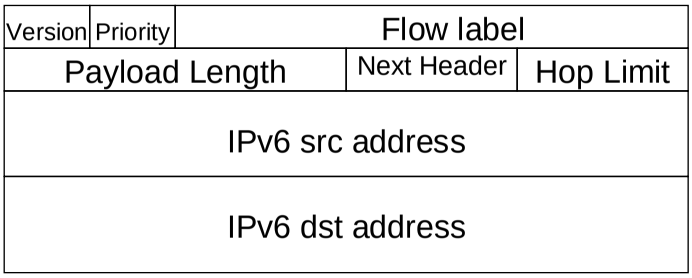
□MACアドレスを元にする必要はない
- ○重複がないことさえ保証できれば十分

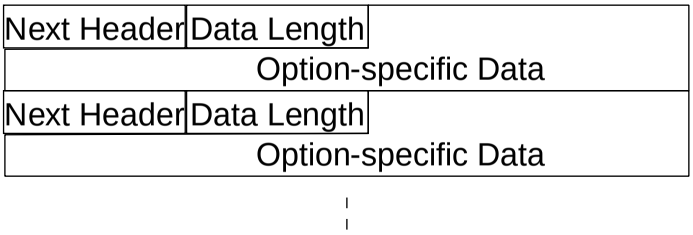
□常に同じアドレスで通信?
- ○インターフェースIDを切替えて通信するのもOK

パケットヘッダの構造化

- □標準ヘッダ
  - ○中継に最低限必要な情報のみ含む
  - ○固定長
- □拡張ヘッダ
  - ○標準ヘッダにないその他の情報を含む
  - ○数珠繋ぎ構造

    IPv4ヘッダ, IPv6ヘッダ, TCPヘッダ, UDPヘッダ,
    ICMPv6ヘッダ, 経路制御ヘッダ, フラグメントヘッダ,
    認証ヘッダ, 暗号ペイロード,
    オプションヘッダ(Hop-by-Hop, Destination)





IPv6での通信手順

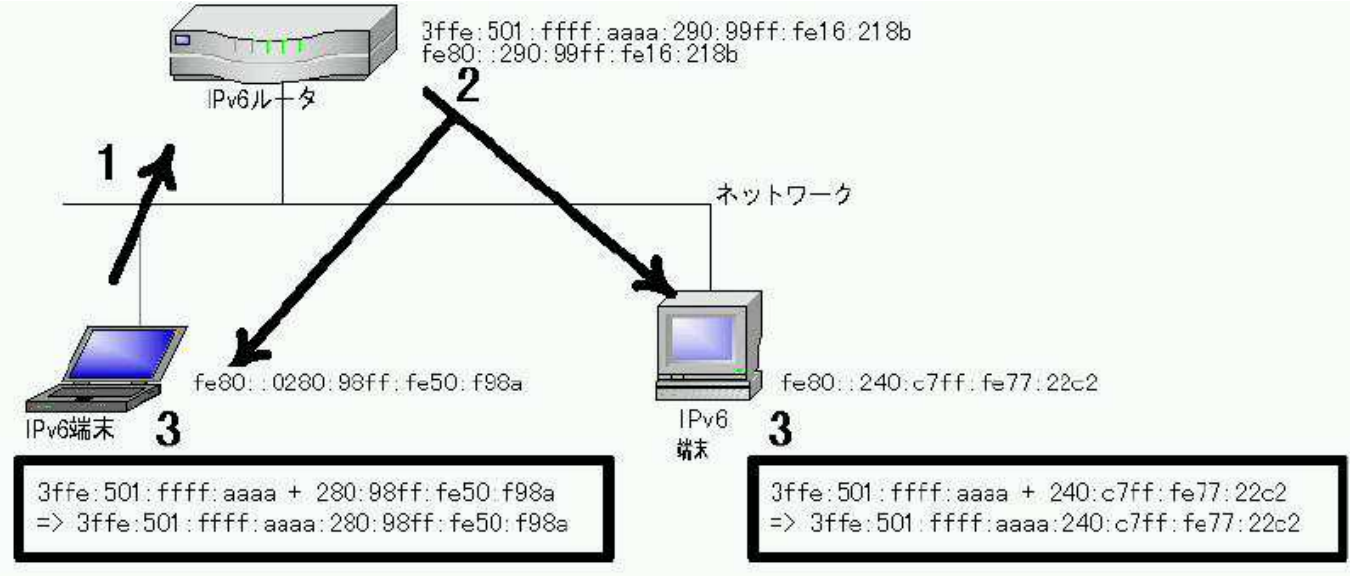
- □Router Advertisement
- □Multicast
- □NDP
- □Routing
- □Path MTU Discovery

IPv6でのEnd to End通信

- IPv4と同じく　宛先IPアドレスに基づいた経路制御
  - Plug & Play
    - Router Advertisement
  - ブロードキャストなし
    - Multicast
  - ARPなし
    - Neighbor Discovery
  - 中間ルータでFragmentしない
    - Path MTU Discovery

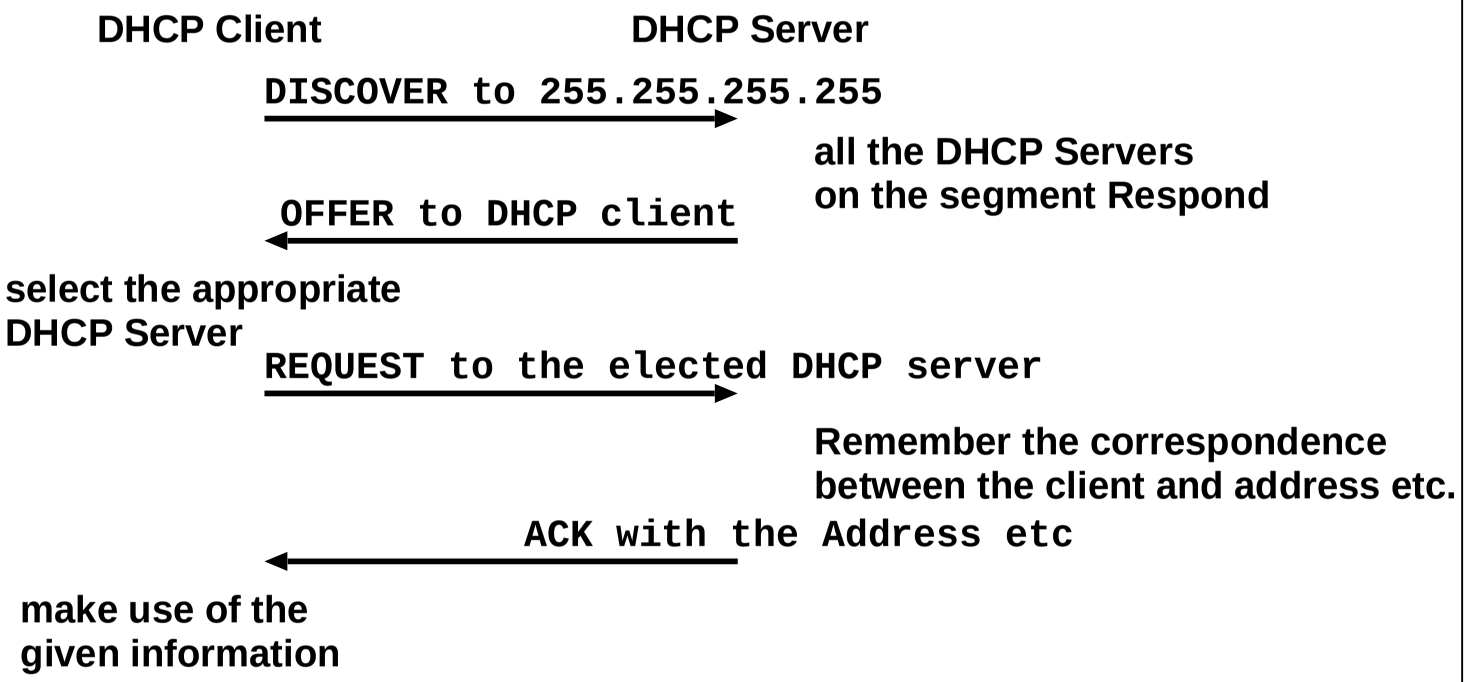
Router Advertisement

- ルータが端末へプレフィックスを定期的に広告
  - linklocal multicastで実現
  - プレフィックス + インターフェースID
    => グローバルアドレス
  - 端末は　デフォルトルートも同時に設定



c.f. DHCP

□端末とDHCPサーバの間でネゴ



DHCPと比べたRAの特徴

□ルータ側の作りが単純: 知るべき情報は2つ
- ○広告するプレフィックス
- ○その広告先インタフェース

□複数のアドレス配布サーバがあってもOK
- ○冗長性

□DNSサーバの情報を流せない
- ○stateless-DHCPv6が有力候補
  - ▹IPv6版DHCPからアドレス設定機能を排除して　単純化したもの

□ルータから端末へ一方的にプレフィックスを広告
- ○「アドレスを割当てない端末」はありえない

DHCPがあれば大丈夫?

- DHCPサーバの設定変更は実は結構手間
  - 「DHCPサーバの設定を変更したので　全員一度端末をリブートしてください」
- DHCPサーバには通常冗長性がない
  - DHCPサーバが落ちると...
- DHCPサーバは全てのアドレス設定を管理できない
  - DHCPサーバの管理外でアドレス設定することは可能

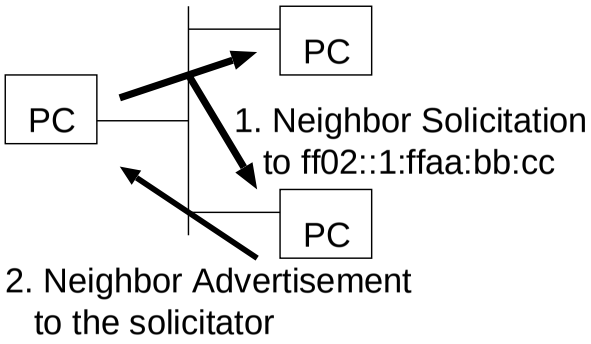
Multicast

- 端末がGroupへJoin, Leaveすることにより、マルチキャストパケットを受信
- IGMPではなく　ICMPv6の一部として実現
- いくつかのマルチキャストアドレスには　最初からJoin済
  - ff02::1 (あるリンクの全IPv6ノード)
  - ff02::2 (あるリンクの全IPv6ルータ)
  - ff02::1:ffXX:XXXX (要請マルチキャスト)

Neighbor Discovery

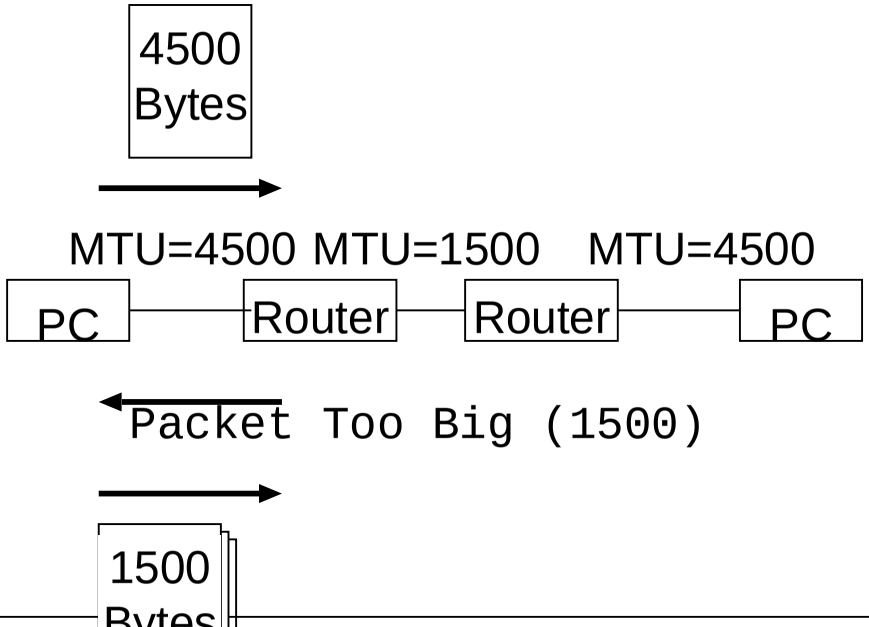
- 同じネットワーク内から　あるアドレスを持つ端末を探索
- ICMPv6の一部
- linklocal multicastで実現

要請マルチキャストアドレス= ff02::1:ffXX:XXXX
XX:XXXX=通信したい相手のv6アドレスの下24bit



Path MTU Discovery

- IPv4 TCPのPath MTU Discoveryと同様
- ICMPv6の一部
- パケット送信元が送信先までのMTUを検出
  - その大きさに最初から分割送信



Routing

- IPv4にあるものはIPv6にも大抵ある
  - BGP, RIP, OSPF, PIM
- IPv4のプロトコルをIPv6用に拡張しただけ
  - ルーティングオペレーションはIPv4と同様

IPv6への移行

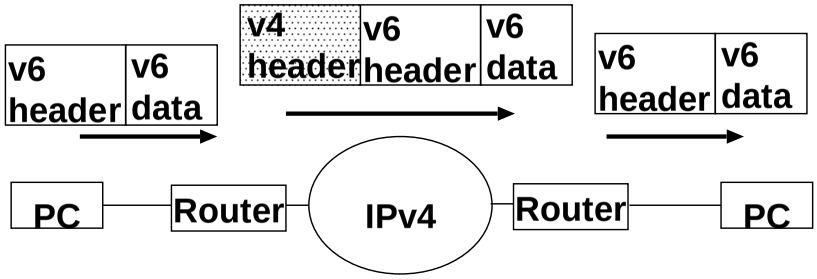
- 考えるべきケース
- トンネリング
- Dual Stack
- トランスレータ

考えるべきケース

- 一気に全ネットワークをIPv6化することはできない
  - 移行手順を考える必要あり
  - 1. IPv6---(IPv4)---IPv6
  - 2. IPv6---IPv4 only node
  - 3. IPv4---IPv6 only node
  - 4. IPv4---(IPv6)---IPv4
- 当面は1, 2のみ
- そのうち　3, 4も問題になってくる?

トンネリング

- 対処できるケース
  - 1. IPv6---(IPv4)---IPv6
  - 4. IPv4---(IPv6)---IPv4
- IPv4/v6でIPv6/v4パケットをカプセル化

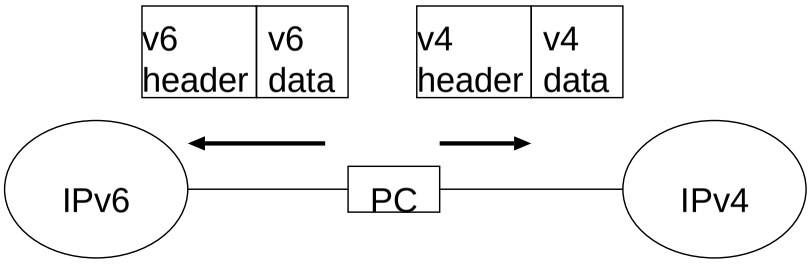


- カプセル化するアドレスの計算方法は様々
  - static, tunnel-broker (e.g. feel6)
  - 6to4, Teredo, ISATAP

Dual Stack

□対処できるケース
- ○2. IPv6(+IPv4)---IPv4 only node
- ○3. IPv4(+IPv6)---IPv6 only node

□IPv4, IPv6両方対応したOSを使う
- ○必要に応じてIPv4, IPv6を使い分ける



□特徴
- ○◯ IPv4空間とIPv6空間が分かれていれば　簡単
- ○△ Dual Stack同士は　どう通信すべき?
- ○× IPv4アドレス枯渇には対応できない

トランスレータ

□対処できるケース
- ○2. IPv6---IPv4 only node
- ○3. IPv4---IPv6 only node

□IPv4-IPv6の仲介サーバを介して通信
- ○IPパケットヘッダの変換 (Layer 3)
- ○TCPセッション接続 (Layer 4)
- ○アプリケーション毎のProxy (Layer 7)

□どれを使うべきか?
- ○どんなトラフィックを変換したいかに依存
  - ▹telnetだけ変換すればいいなら　Layer 4~でOK
  - ▹外にいくのがwebだけなら　Web ProxyでOK

IPv6の現状

- □OS
- □アプリ
- □ルータベンダ
- □ISP
- □情報家電
- □企業内ネットワーク
- □海外

OS

- □BSD　: KAME
  - ○2001年位からは　どのBSDも最初からKAME入り
- □Linux : USAGI
  - ○2.6以降は　最初からUSAGI入り
- □MS　: Windows XP~
- □Mac　: MacOS X~
- □Sun　: Solaris 8~
- □HP　: HP-UX 11~

アプリ

- メジャー なサービスのFree実装はほとんどIPv6対応済
  - Web, POP, SMTP, SSH, telnet, FTP, firewall, DNS, SNMP, LDAP
- 商用品となると少なくなるが　IPv6対応するのも時間の問題
  - Internet-Explorer, Personal Firewall (Microsoft)
  - Windows Media Player/Server (Microsoft)
  - Winbiff (Orangesoft),
  - JP1(Hitachi), OpenView(HP), LMAT(Yokogawa)
  - Checkpoint, Nokia, Netscreen, ...

ルー タベンダ

- core routerはIPv6-readyが当り前
  - Hitachi, NEC, Cisco, Juniper, Fujitsu, Furukawa ...
- Layer3 switchもIPv6-readyになりつつある
  - Foundry, Extreme Network, ...
- access routerも段々IPv6-readyに
  - YAMAHA, Panasonic, NEC, Fujitsu, Cisco ...
- Firewall/IDSのIPv6対応も始まった
  - Checkpoint, Nokia, Netscreen, ...

- この1~2年でIPv4並に安定してきた

ISP

- tunnel serviceは当り前
  - IPv4ネットワーク を介してIPv6パケットをカプセル化
    e.g.) Feel6 (http://www.feel6.jp/)
- native serviceも出始めた
  - 物理回線上で直接IPv6通信
- DSL回線のIPv6化も段々始まっている
  - ACCA, e-Access ...

情報家電

- 家電向けの小型IPv6 Stackはある
- 家電の激しいコスト競争の中、IPv6を取り込むのは risky
  - コストアップに見合った付加価値が必要
    (e.g. ビデオ/エアコンのお手軽な遠隔操作)
- 結論
  - コマは揃ってる
  - サービスモデルさえ明確になれば　爆発的に流行する
    - サービス自動検索方法
    - サービス公開ポリシー

企業内ネットワーク

- 現状
  - 実験ユース
  - 生活インフラになっているケースは少ない
- 考えられる背景
  - IPv6は従来の運用ポリシーにそぐわない
    - IPアドレスに基づいた端末管理
  - IPv6オペレーション経験不足による知識不足
  - 現状以上のことをしたくない
    - でもIPv4で四苦八苦しているのもまた然り...
  - 導入メリットが不明確
    - 何となくは分かるが　いくら儲かるの?
- 結論
  - 正しい導入ガイドライン/メリットを示せば　IPv6導入は進む

IPアドレスに基づいた端末管理 (cont.)

- IPアドレスをPlug & Playで渡すと　思わぬ人がIP通信できてしまう
  - 権利のない人がPlugできてしまうのがそもそも変
- 悪いことをしている端末をすぐにネットワークから外したい
  - IPアドレスが分かっただけでは場所は分からない。 (e.g. IPアドレスを詐称する攻撃)
  - Layer 2の情報を管理することが重要　(e.g. 802.1x, 認証VLAN)
- これらの問題はIPv6とIPv4の両方に存在

海外・日本政府

- US
  - Internet2
  - 国防総省調達仕様にIPv6が入った
  - この1年で急に力を入れ始めた

    http://www.dod.gov/releases/2003/nr20030613-0097.html
- ヨーロッパは産学共同で推進
  - 山程Projectが出来てる
    - Eurov6, Euro6IX, 6NET, GEANT, ...
  - 特に携帯, GRIDに注力
- アジアは産官学で後押し
  - 日本: e-Japan計画, IPv6高度・普及化推進協議会
  - 台湾: e-Taiwan
  - 中国: CERNET, 6TNet, CNGI
  - 韓国: e-Korea

IPv6の課題

- 問題は3種類ある
  - IPv6固有な問題
  - IPv6でより顕在化する問題
  - IPv4/IPv6で共通な問題
- ここでは前2つを中心に議論
  - 「3すくみ」状態の完全解消
  - 本当のPlug & Play
  - ファイアウォールアーキテクチャの見直し

3すくみ状態の完全解消

- 3すくみ状態
  - IPv6を使わないから　IPv6運用経験が不足
  - killer-applicationがないから　ユーザ数が増えない
  - ユーザ数が足りないから　IPv6を使う気になれない

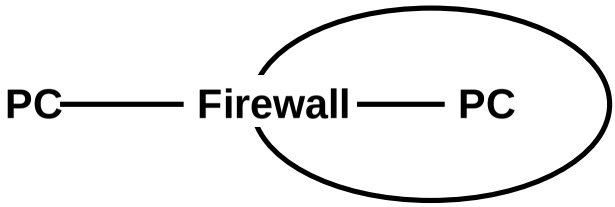
- まずは使おう!
  - アドレス不足に追い込まれたときがいい機会
    - 自動トンネルなど低コストでIPv6導入することは可能
    - (e.g. 6to4, Teredo, トンネルブローカ)
  - 最初はIPv4を全部IPv6に置き換えなくてもいい
    - 特定の新規実験サービスはIPv6でないと使えない

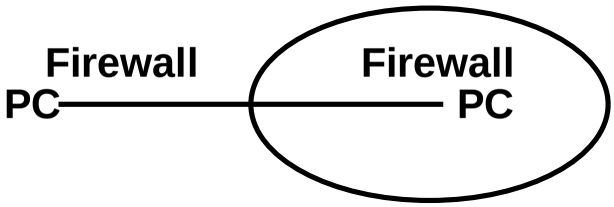
本当のPlug & Play

- IPv6の"Plug & Play"は　あくまで端末アドレスのPlug & Play
- 他の設定もPlug & Playできないと　真の"Plug & Play"ではない
- サービス~アドレス/ホスト名との対応付けの自動化が必須
  - DNSサーバ指定 -> stateless-DHCPv6
  - SOHOルータ設定 -> Prefix-Delegation
  - Web Proxy設定 -> ???
  - エアコン検索 -> Home-Gateway?

ファイアウォールアー キテクチャ見直し

- □IPv6とファイアウォールの不仲
  - ○End-to-End通信を志向するIPv6は　現在の「玄関モデル」　ファイアウォールとの相性が悪い
  - ○端末にファイアウォールを導入する「金庫モデル」　との協調が必要





- □IPv4でも「玄関モデル」　には限界がある
  - ○最近は　VirusはfirewallのWで広まることが多い

結論

- □広大なアドレス空間により
  - ○ネットワー ク設計の自由度を高める
- □IPv6プロトコル概略
  - ○基本的にはIPv4と同じ
  - ○Plug & Play
- □IPv6ベンダ,サービスの現状
  - ○ほぼインフラやアプリは整いつつある
  - ○あとはノウハウとコストメリット
- □IPv6の課題
  - ○本当のPlug & Play
  - ○ファイアウォールアー キテクチャの見直し