



NTT Information Sharing Platform Laboratories
NTT 情報流通プラットフォーム研究所

IPv6 トラブルシューティング

ホームネットワーク／SOHO編

NTT情報流通プラットフォーム研究所

藤崎 智宏

fujisaki@nttv6.com

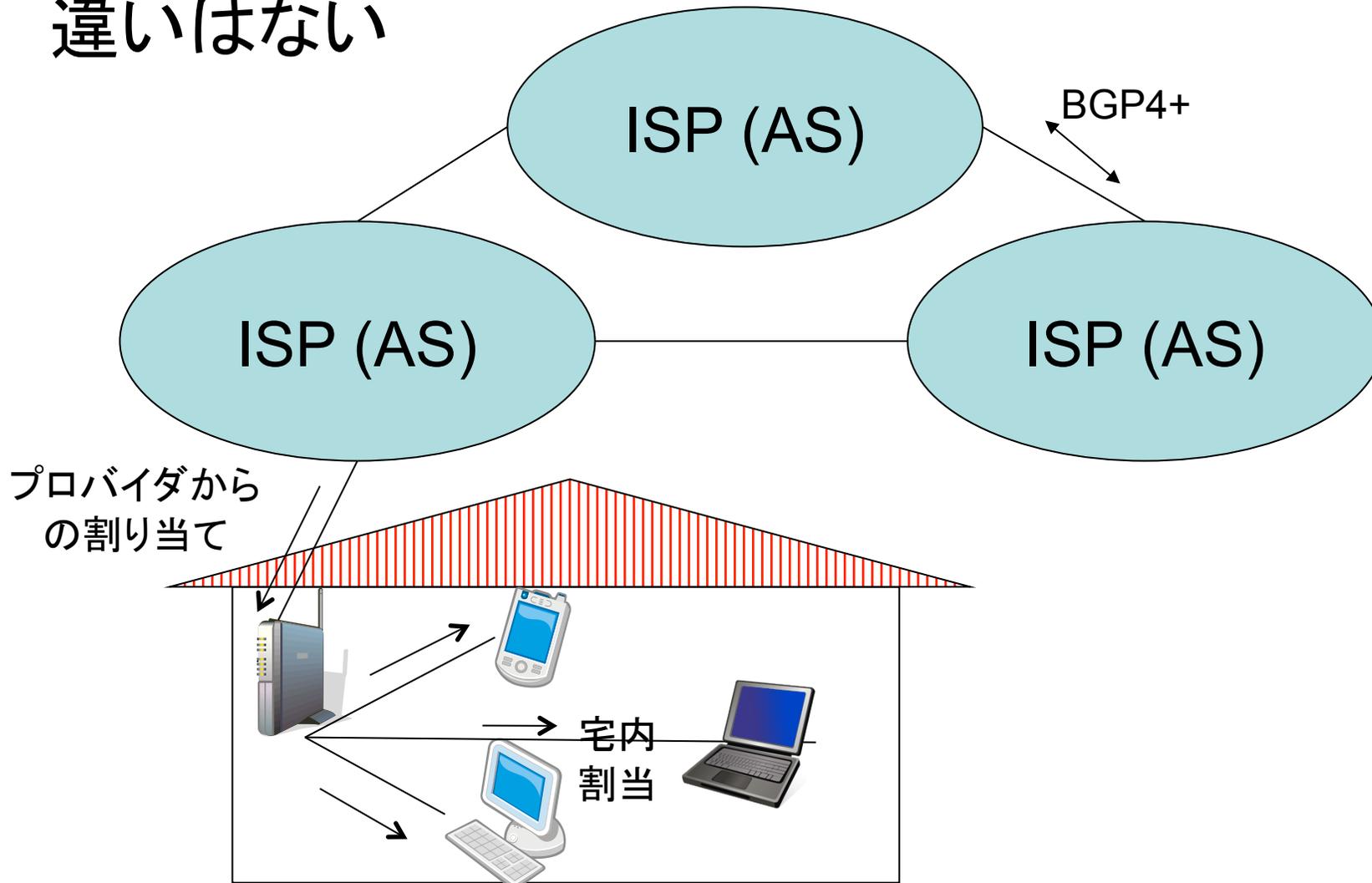
- IPv6の実利用が進み始めています。日本でも、来年春順次、コンシューマ向けIPv6サービスが開始される予定です。
- IPv6ネットワークの利用上、IPv4との共存、IPv6ならではの機能等により、実利用上、問題が発生する可能性があります。
 - IPv4/IPv6フォールバック問題、MTU問題等、対処が必要な問題が想定されます。
- 本セッションでは、IPv6網を運用する上で遭遇しやすいトラブルについて、その原因やトラブルシューティングの方法について解説します。

- IPv6トラブルシューティング ホームネットワーク／SOHO編
 - 藤崎 智宏(NTT情報流通プラットフォーム研究所/)
 - SOHO等のIPv6網で起こりやすいトラブルとその解決方法
- IPv6トラブルシューティング サーバ編
 - 白畑 真(株式会社クララオンライン)
 - サーバの運用管理で起こりやすいトラブルとその解決方法
- IPv6トラブルシューティング ISP編
 - 松崎 吉伸(株式会社インターネットイニシアティブ)
 - ISPで起こりやすいトラブルとその解決方法

IPv6トラブルシューティング

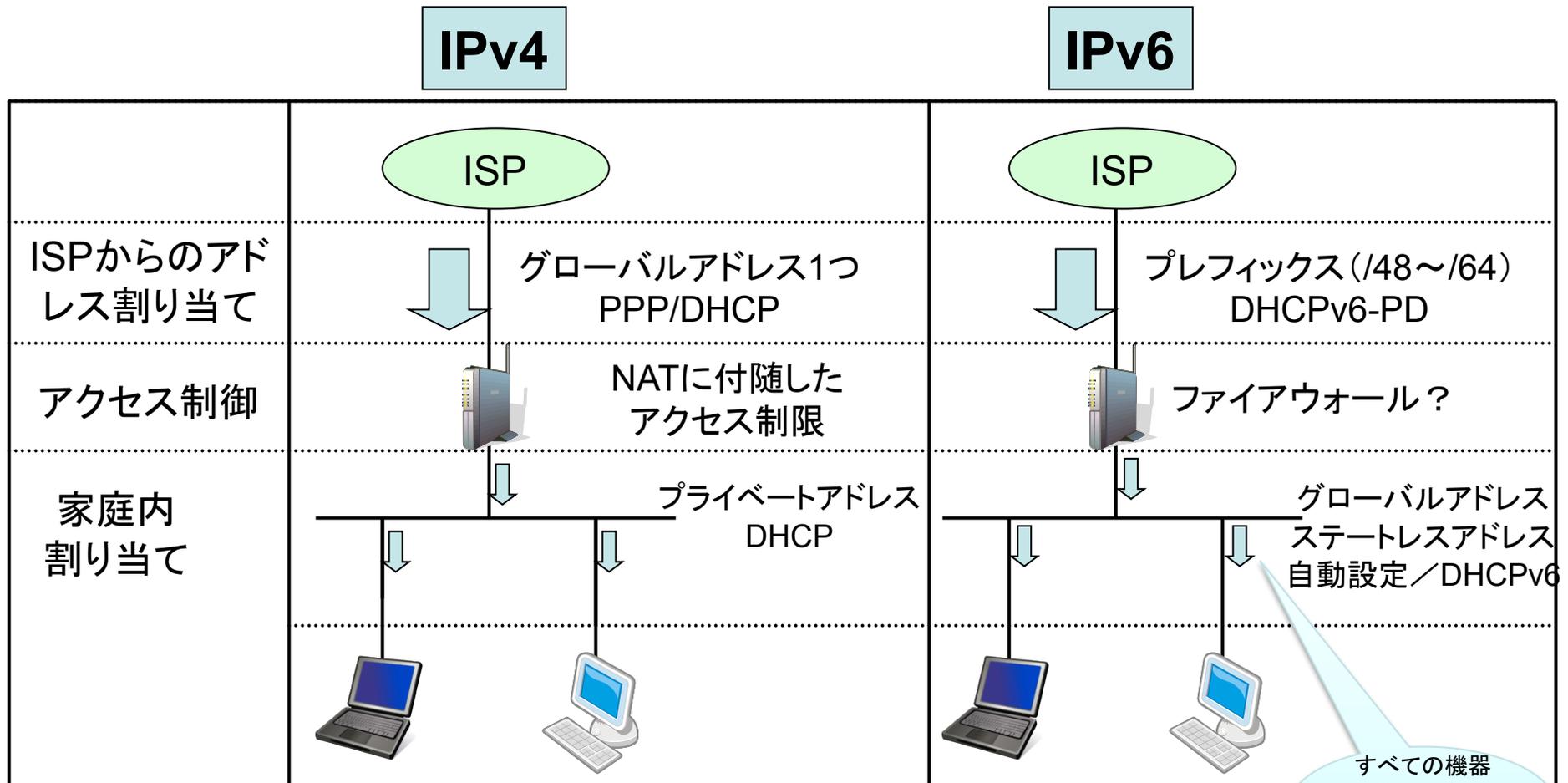
ホームネットワーク／SOHO編

- 機器や、構成に関しては、(今のところ)大きな違いはない



IPv4 と IPv6 の違い

- IPv4とIPv6のネットワーク構成の違いの概略



すべての機器にグローバルアドレスが付与される。

今後のネットワークは、IPv4/IPv6ネットワークが同時に利用される **デュアルスタックネットワーク** となる。

- PPPの仕様の違い

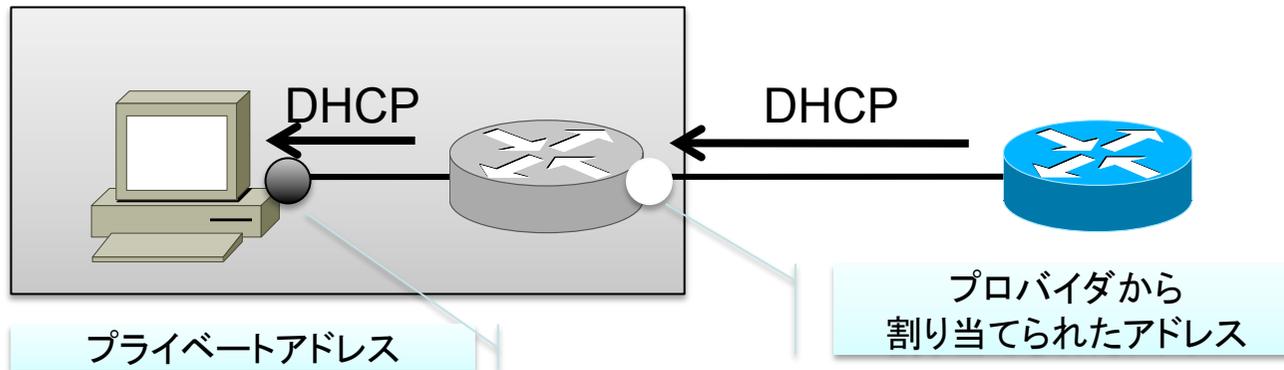
- IPv4では, PPPで, IPCPにてグローバルアドレスを割り当てる
- IPv6では, PPPで, IPV6CPにて, “リンクローカルアドレス”を割り当てる
 - 「リンクローカルアドレス」: 同一リンク内でのみ利用可能なアドレス
 - IPv6グローバルアドレスは, DHCP-PDを使用して割り当てられる.

- 割り当てるアドレスサイズの違い

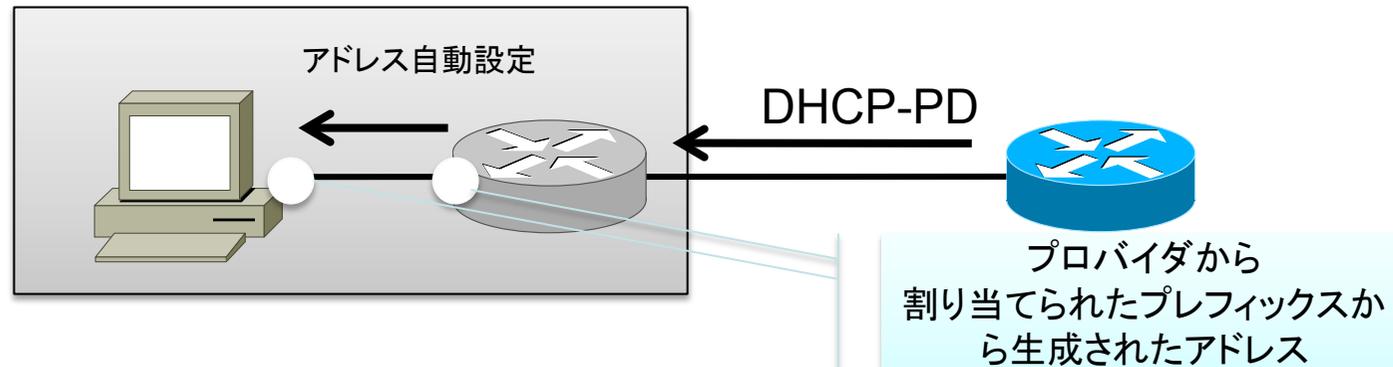
- IPv4では, DHCPにてアドレスを「一つ (/32)」割り当てる
- IPv6では, DHCP-PDにて「アドレスブロック (/64 ~ /48)」を割り当てる
 - 複数のプレフィックス

• アドレス付与位置の違い

-IPv4では、プロバイダとの境界のインタフェースにアドレスが付与される。

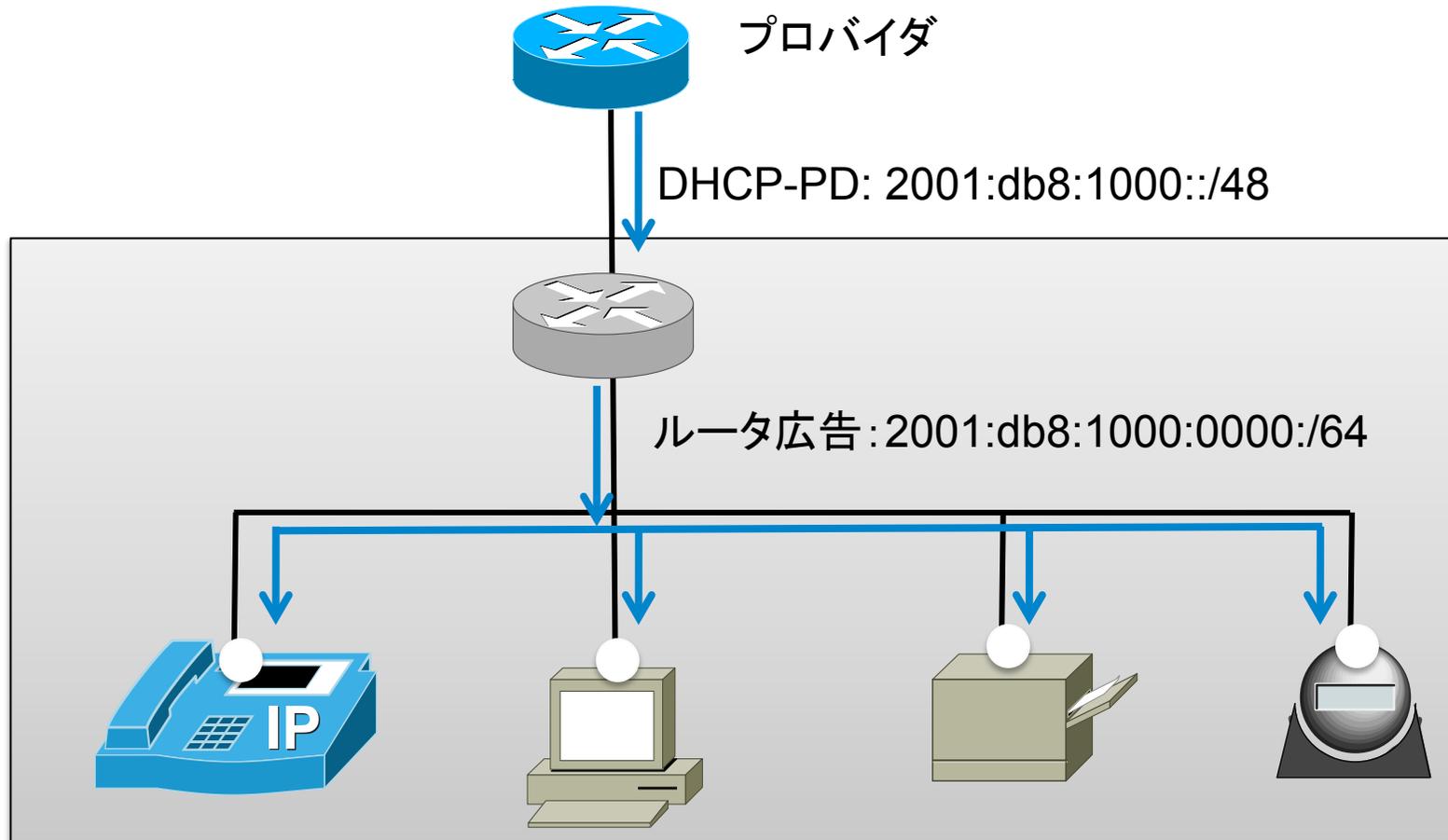


-IPv6では、宅内機器すべてにグローバルアドレスが付与される。





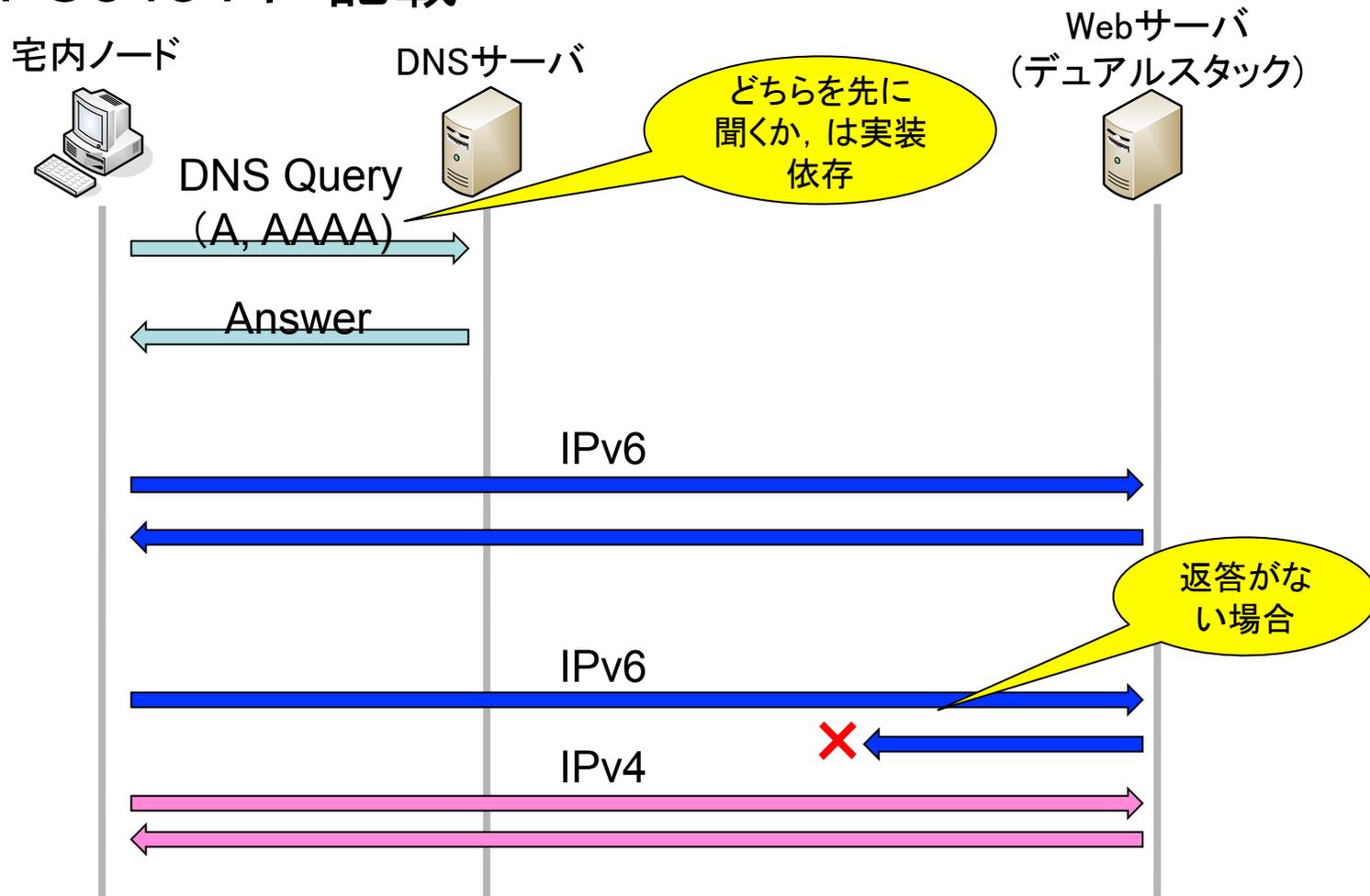
- 宅内でステートレスアドレス自動設定を利用する場合 (DHCPv6も利用可)



- ホームネットワーク/SOHOへのIPv6導入時のトラブルを,
 - IPv6とIPv4混在によるもの
 - IPv6特有の機能(や特徴)によるもの
 - IPv6移行技術の導入によるもの
- に大別し、以下で解説します。

IPv6とIPv4の混在によるトラブル

- 多くのノードは, IPv6を先に試す.
 -RFC3484 に記載



- IPv6で通信できているかどうかの確認
 - IPv6 と IPv4 で動作の違う Web サイトにアクセス
 - www.kame.net, www.apnic.net など
- IPv4/IPv6のどちらで通信しているかを見分けるのは困難
 - アプリケーションは一般的に、プロトコル種別を気にしない
 - Firefoxプラグイン, ShowIP
 - 接続アドレス情報を表示

• ShowIP

- 利用中のIPアドレスを表示
- フォールバックが発生すると、正しいアドレスを表示しない



The KAME project

1998.4 - 2006.3



Dancing kame by [atelier momonga](#)



The **KAME project** was a joint effort of six companies in Japan to provide a free stack of IPv6, IPsec, and Mobile IPv6 for BSD variants.

Our products are available in:

- [FreeBSD](#) 4.0 and beyond
- [OpenBSD](#) 2.7 and beyond
- [NetBSD](#) 1.5 and beyond
- BSD/OS 4.2 and beyond

The project officially concluded in March 2006 (see [press release](#) from the WIDE project). Almost all of our implemented code has been merged to FreeBSD and NetBSD. The snap releases ([FTP](#) or [cvsweb](#)), [anoncvs access](#), [git](#), and [Archives of the snap-users mailing-list](#) are still available.

[\[Top\]](#) [\[Old info\]](#)



完了

2001:200:dff:fff1:216:3eff:feb1:44d7 +1

2001:200:dff:fff1:216:3eff:feb1:44d7 +1



- 通信トラブルが発生した際、どちらのプロトコルが問題になっているかの区別が必要であるが、現状、見分けることは難しい。
 - Wireshark 等でパケットを眺める
 - 通信中の場合には、OSの通信状態を確認
 - netstat コマンドで確認可能 (Windows, Mac, UNIX)

Windows での例

```
C:\Users\fujisaki>netstat -an

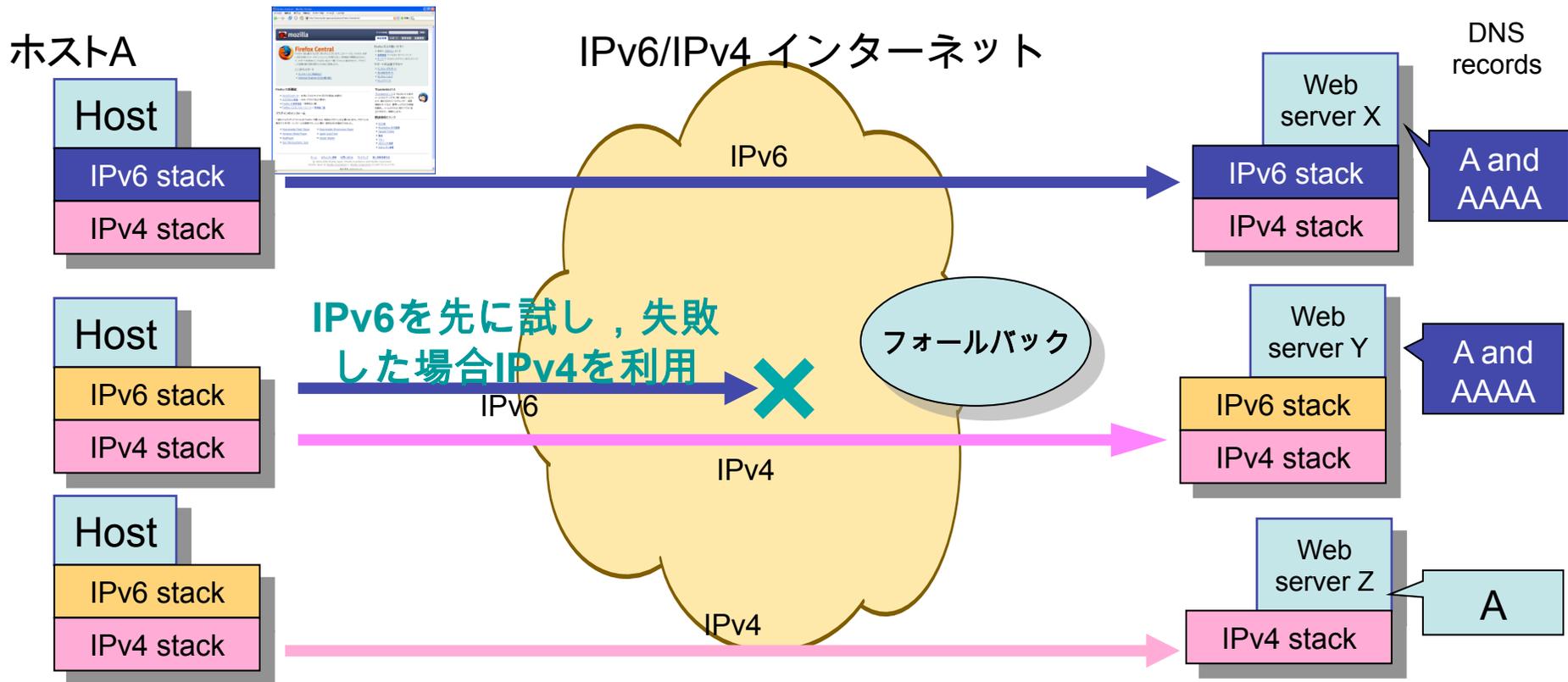
アクティブな接続

プロトコル ローカル アドレス      外部アドレス  状態
TCP      0.0.0.0:135      0.0.0.0:0      LISTENING
TCP      [::]:135        [::]:0         LISTENING
TCP      [2001:fa8:1000:0:6d8b:c02f:f8d5:7f06]:49285 [2001:fa8:ffe:1000::25]:22 ESTABLISHED
TCP      [fe80::fd12:5fb7:7168:1fff%11]:49284 [fe80::fc55:d725:7985:e3df%11]:2869 ESTABLISHED
```

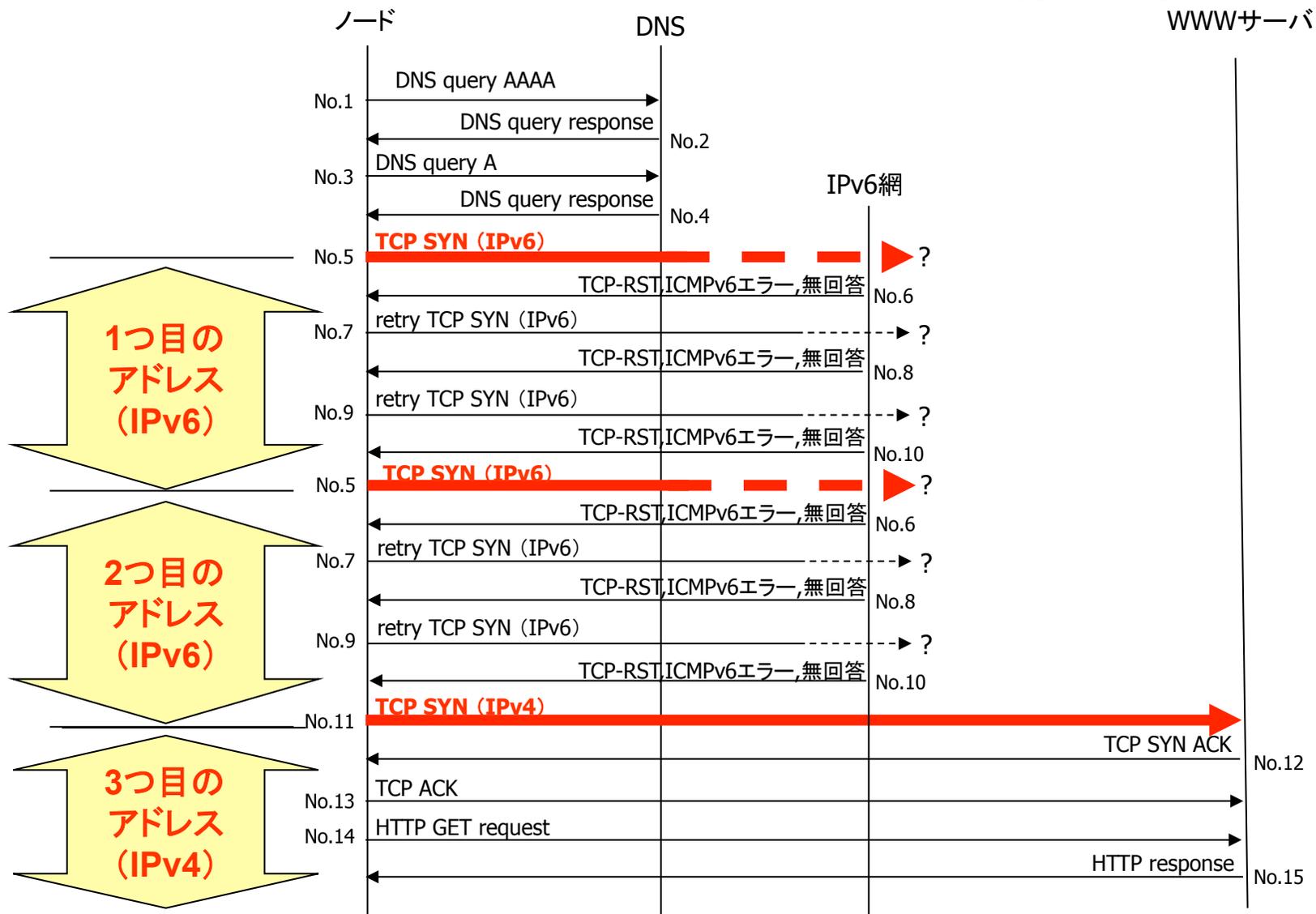


“IPv6/IPv4フォールバック問題”

- 現在、多くのIPv6/IPv4 デュアルスタック実装は、IPv6通信を優先する
 - 終点ノードがIPv6/IPv4の両方のアドレスを持っている場合 (DNSで両方のアドレスが引ける場合)、IPv6通信を先に試す。
 - IPv6通信が失敗 (タイムアウトなど) すると、IPv4通信を試す。

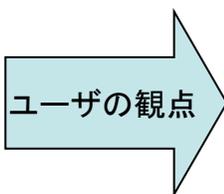


宛先ノードのIPv6アドレスが2つ、IPv4アドレスの場合の例

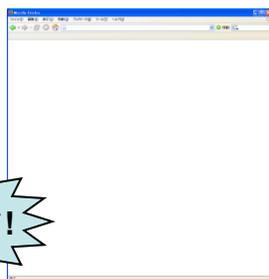


問題: フォールバックに非常に時間がかかることがある。

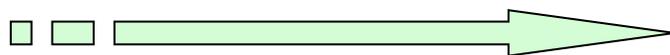
- TCPを利用したアプリケーションで問題が顕在化。
 - 通信前に、チャネルの確立処理が必要。
 - 標準的な実装手法では、通信相手のノードが複数のIPアドレスを持つ場合、アプリケーションは通信チャネルが確立するまですべてのアドレスに対し、順番に確立処理を実施



Webページが完全に表示されるまで、長い時間待たされる！



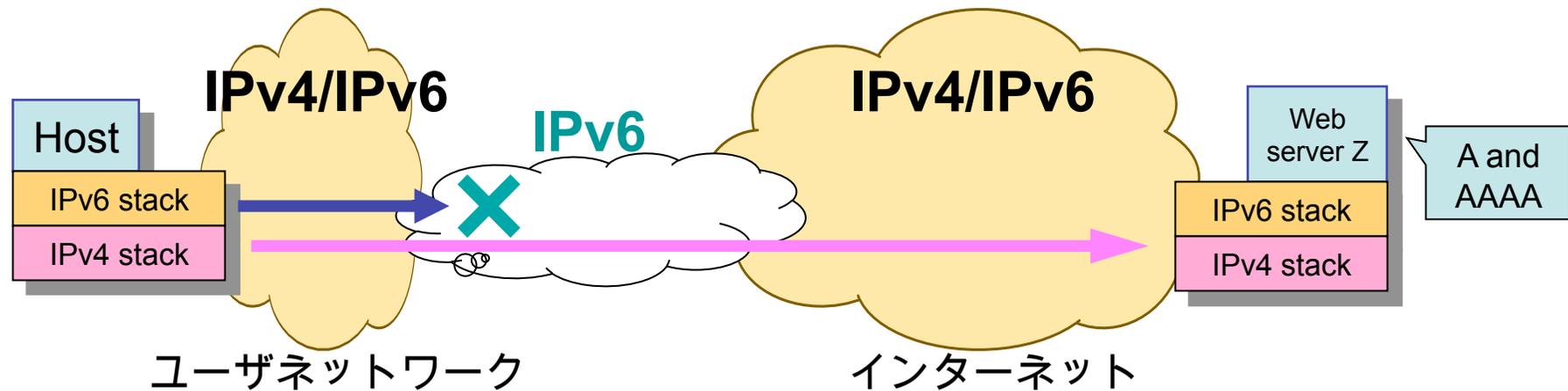
20秒以上...



フォールバック時間

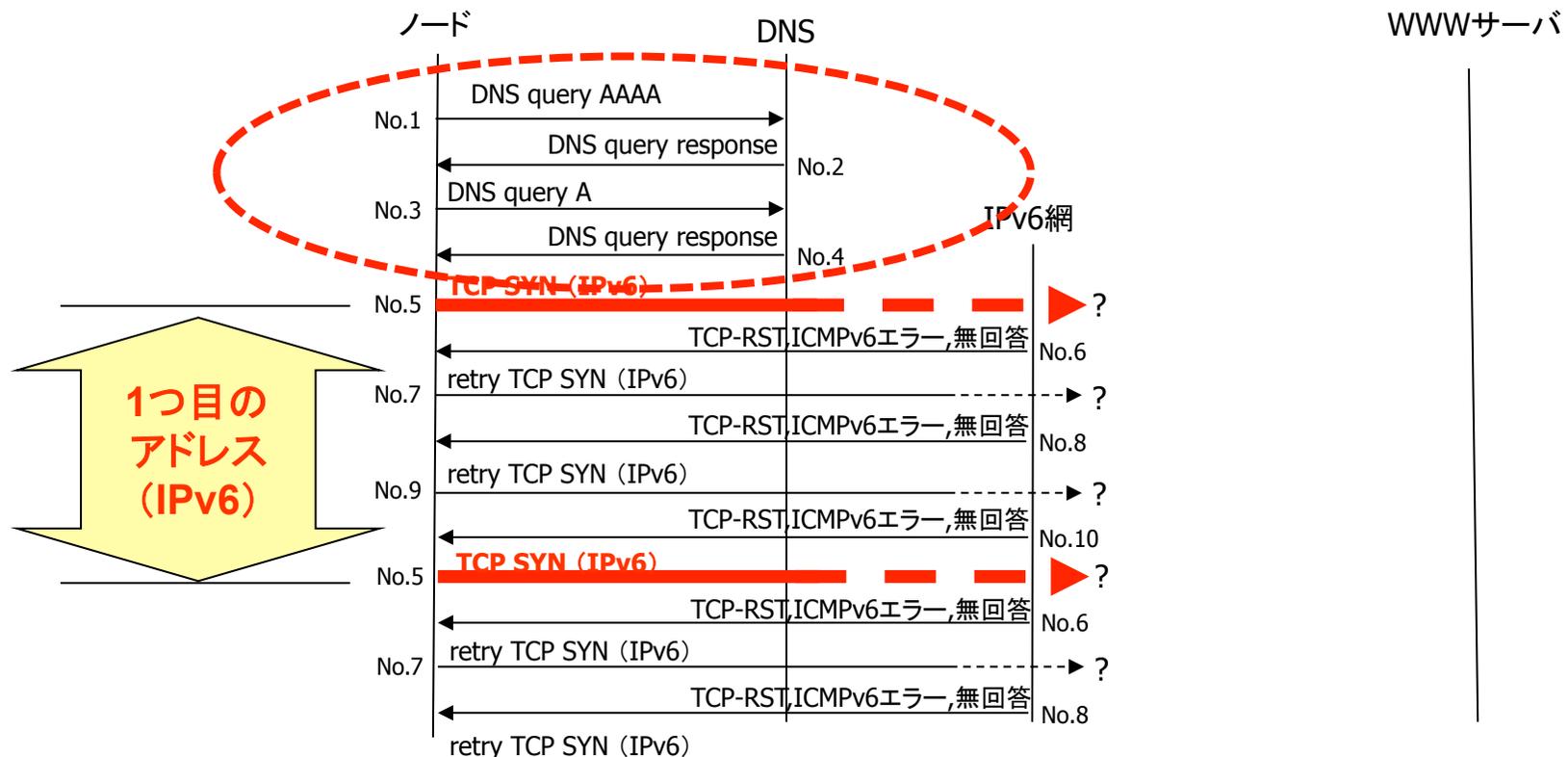
単位：秒

OS	ブラウザ	タイムアウトのみ	Type=1 (Destination Unreachable)							TCP reset
			Code=0	Code=1	Code=2	Code=3	Code=4	Code=5	Code=6	
Windows 7 Ultimate	IE	21.01	21.01	21.01	21.01	21.00	21.00	21.01	21.01	1.01
	FireFox	21.01	20.99	21.00	21.00	21.00	21.00	21.00	21.00	1.01
	Google chrome	21.00	21.01	21.01	21.01	21.01	21.00	21.00	21.00	1.01
WindowsXP	IE	22.91	22.90	22.93	22.91	22.92	22.90	22.93	22.92	1.06
	FireFox	22.94	22.93	22.95	22.93	22.90	No fallback	22.91	22.94	1.01
	Google chrome	21.05	21.10	21.07	21.08	21.10	No fallback	21.10	21.07	1.02
Windows Vista Home Premium	IE	21.00	21.01	21.02	20.99	21.02	21.00	21.00	21.01	1.00
	FireFox	21.00	21.01	21.00	20.99	21.01	21.00	20.99	21.00	1.00
	Google Chrome	21.00	21.00	21.00	21.00	20.99	20.99	21.00	21.00	1.00
MAC OS X バージョン 10.6.4	Safari	74.70	3.95	3.95	3.93	3.94	3.97	74.99	74.71	0.01
	FireFox	74.75	3.94	3.95	No Fallback	No fallback	3.95	74.78	74.75	0.01
	Google chrome	74.76	3.95	3.94	No Fallback	No fallback	3.95	74.73	74.78	0.01
Fedora 13	FireFox	21.01	0.01	0.01	0.01	0.01	0.01	No fallback	No Fallback	0.01
FreeBSD7.2	FireFox	75.01	12.64	12.64	No Fallback	No fallback	12.64	75.01	75.03	0.01



- IPv6の接続性に問題がある場合.
 - 管理されていない移行技術の利用
 - 通信先のAAAAレコード登録があるが, IPv6接続性ない場合
 - IPv6 インターネット接続性がない場合 (例: VPN, ULAアドレス等)

- DNSへのアクセスが原因の可能性も
 - DNSサーバがデュアルスタックで、クライアントがIPv4/IPv6DNSサーバアドレスを持つ場合
 - どちらかのDNSが落ちていれば、フォールバック発生

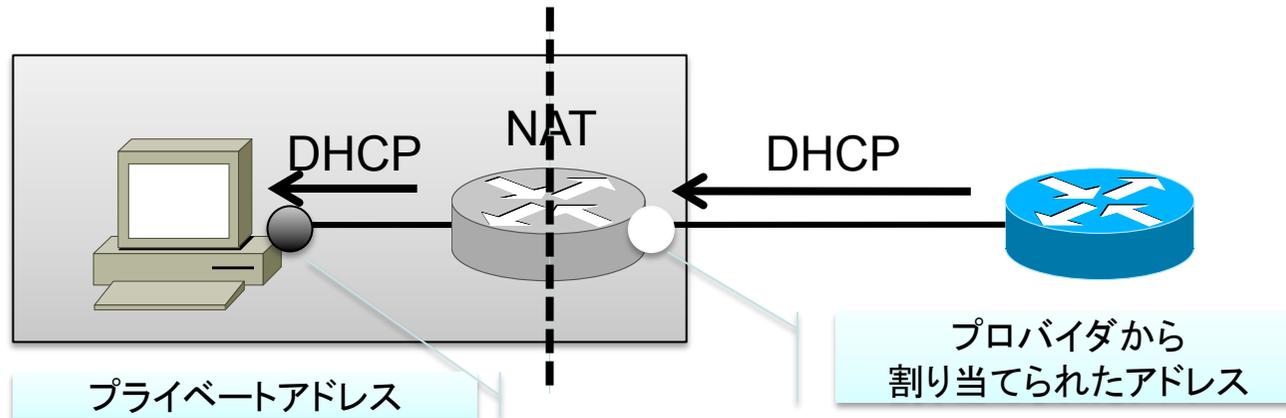


- 通信完了に時間がかかる (Webページの表示に時間がかかる) と思ったら、フォールバック問題も疑って下さい。
- 確認方法：
 - 通信相手のDNS登録状況 (AAAAレコードの有無, 数)
 - host, nslookup コマンド等の利用
 - 通信相手までの到達性の確認
 - ping6, traceroute/tracert コマンド等の利用
 - パケットダンプ
 - シーケンスを追う必要があり, 結構大変
 - DNSの原因が考えられる場合
 - ホームルータの持っているDNSサーバの正常性確認

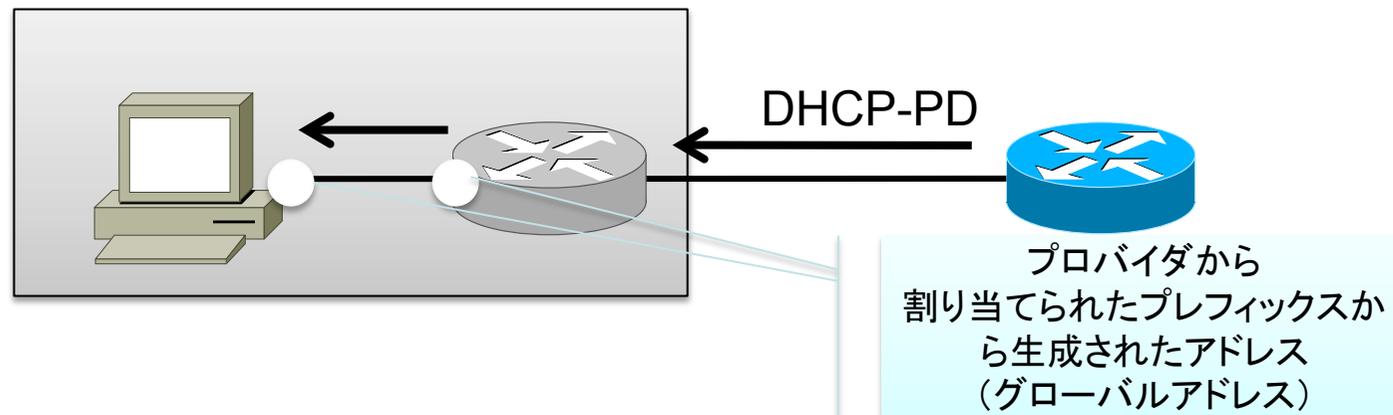


- IPv6の接続性チェック
 - 不安定な接続性(6to4等)の場合には, それを改善
- 特定の宛先のみIPv4を優先するように設定する
 - Windows 等で, ポリシーテーブル(参考資料参照)をいじる

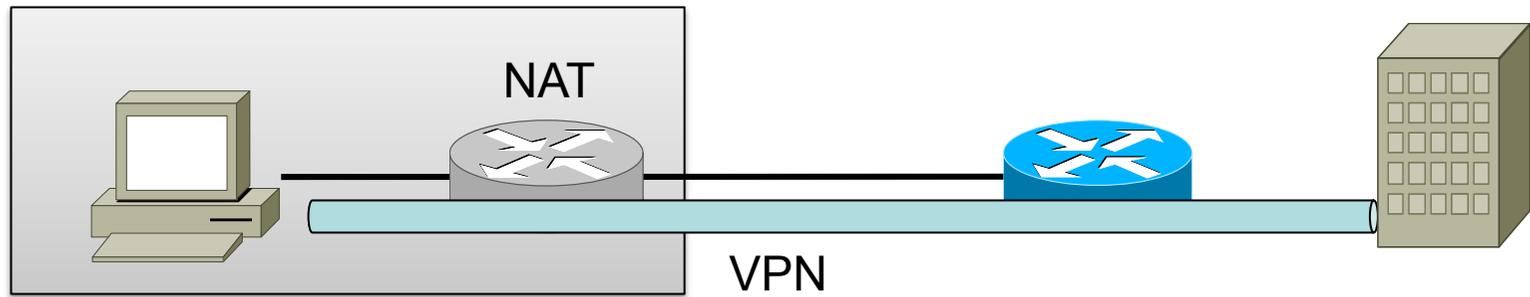
- 外部からの接続可能性の違いに注意
 - IPv4は, NATが存在する.



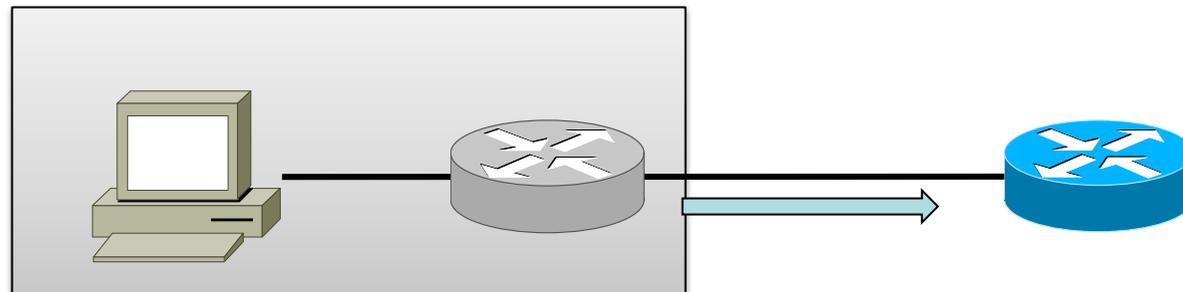
- IPv6では, グローバルアドレスが付与される.



- インターネットへの出口が“2つ”あることに注意
 - IPv4でVPN接続

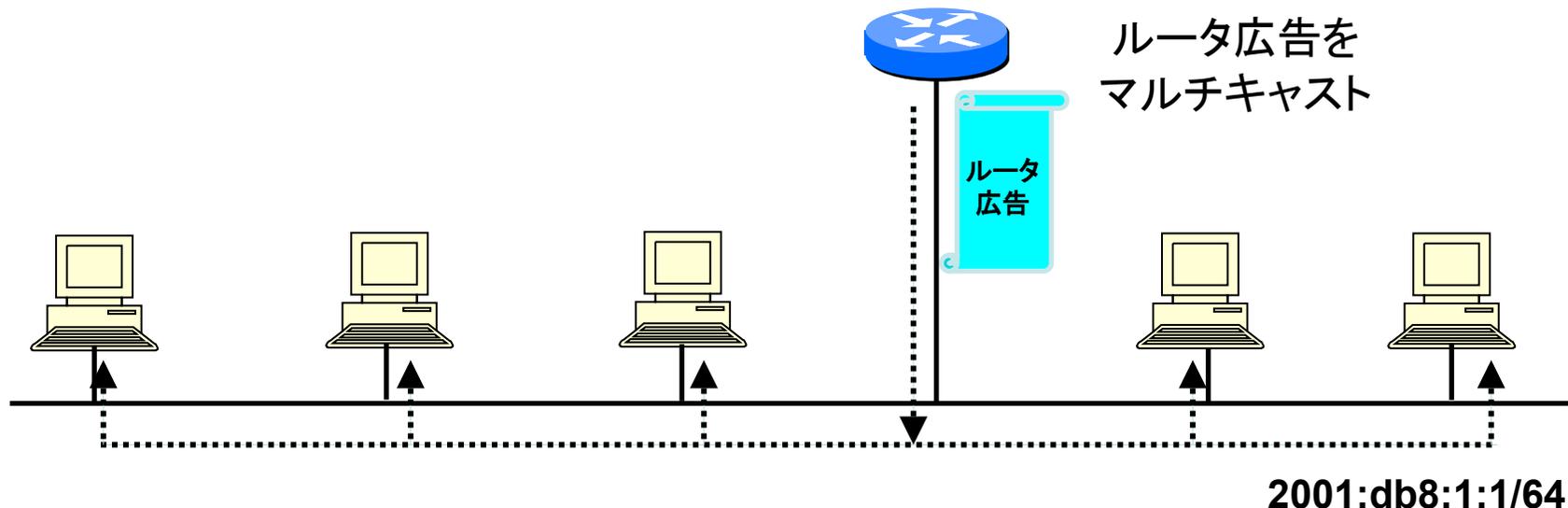


– IPv6では, そのままインターネットへ.



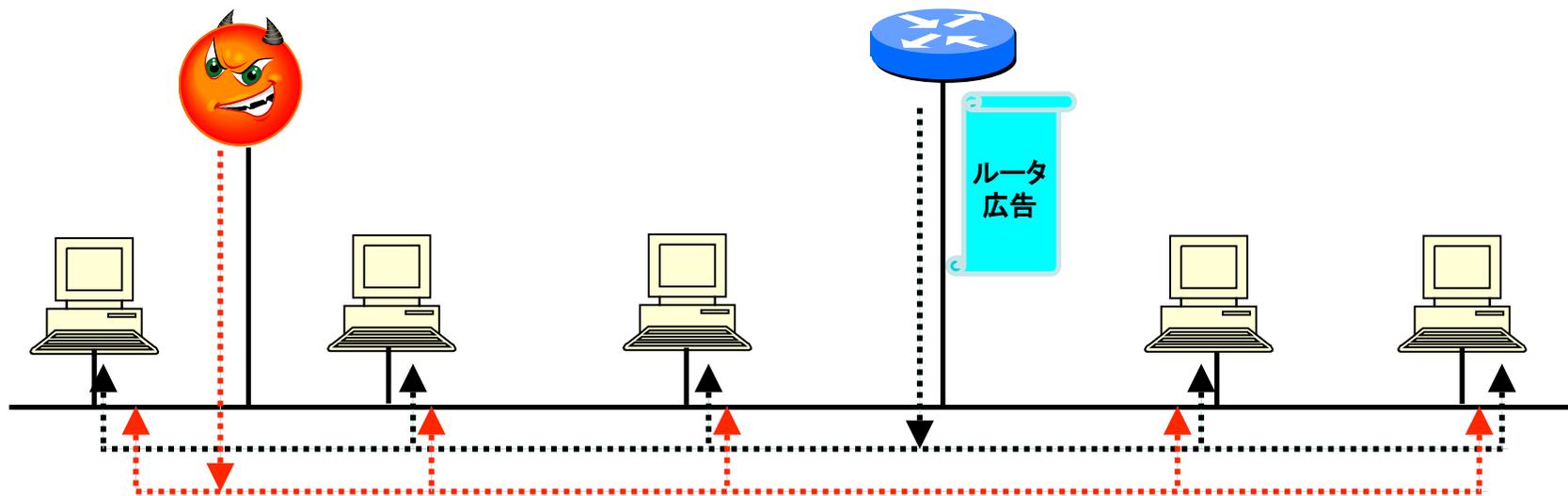
IPv6特有の機能に起因するトラブル

- 家庭内や小規模オフィスでは、ステートレスアドレス自動設定 (SLAAC) によるアドレス自動設定が多用されると考えられる。
 - ルータが、ルータ広告メッセージ (RA) により、デフォルトルータアドレスやリンクで利用するプレフィックス等の情報を通知



トラブル:

- 正規のルータ以外の機器が、ルータ広告を送出。
 - ネットワーク上の機器は、ルータ広告メッセージを受け取り、デフォルトルータ情報、アドレスプレフィックス情報を自身に追加設定。
 - 結果として、IPv6での通信が不能もしくは不安定になる。

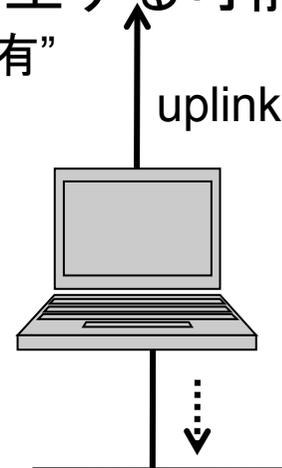


- Windows OS は、設定により、ルータ広告を送出可能

– “インターネット接続の共有” 機能を設定すると、ルータ広告を送出 (IPv4 のDHCPサーバにもなる).

- ノートPCを持ち出して、宅内ネットワーク等に再接続した場合に起こる可能性あり.
- 今後、6to4機能(後述)等を持ったホームルータ等の導入により、発生する可能性もある.

“インターネット接続の共有”



IPv4 NAT ルータ, IPv4 DHCP サーバ,
IPv6 デフォルトルータとなり, IPv6
ルータ広告送出手を実施

- クライアントのアドレス情報等から容易に発見できる
 - FreeBSD での例

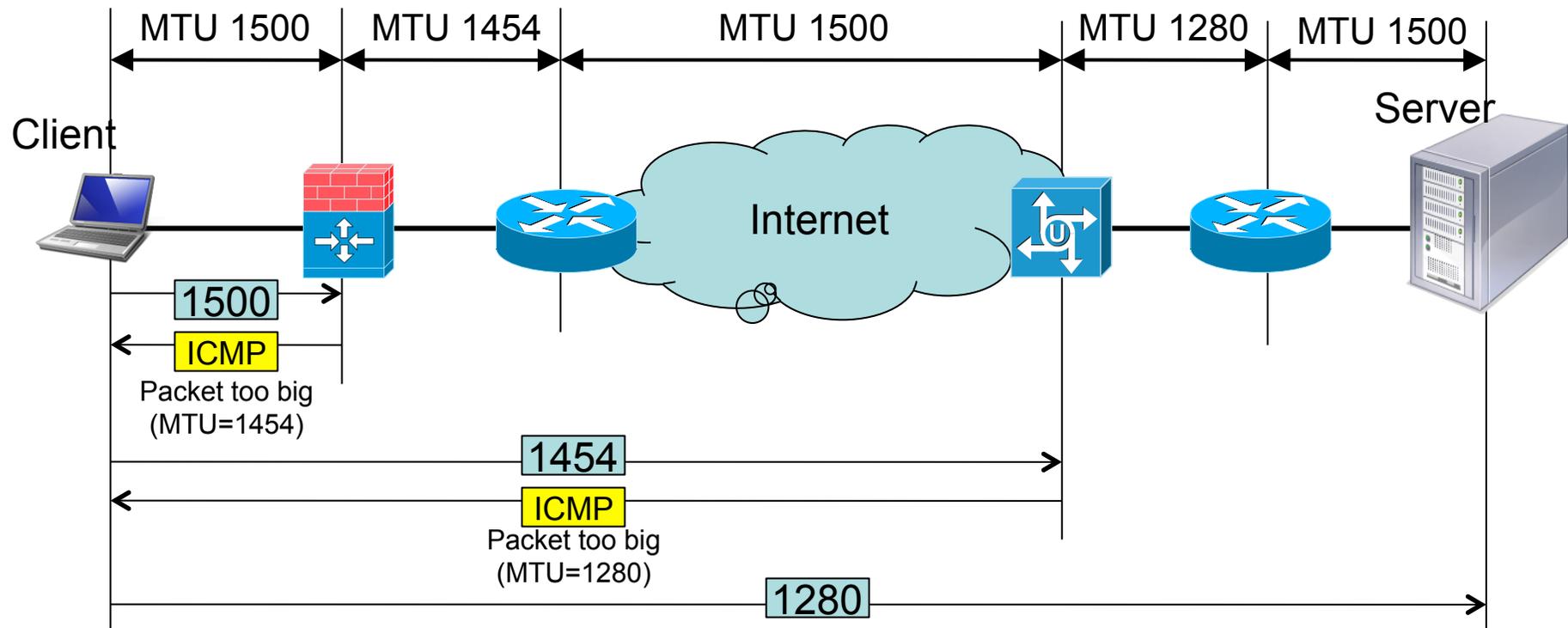
```
speedvm(2) ifconfig -a
Inc0:
flags=108843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST,NEEDSGIAN
T> mtu 1500
    inet6 fe80::20c:29ff:fea1:xxxx%Inc0 prefixlen 64 scopeid 0x1
    inet6 2001:xx8:1000:0:20c:29ff:fea1:xxxx prefixlen 64 detached autoconf
    inet6 2001:xx0:640:f152:20c:29ff:fea1:xxxx prefixlen 64 detached autoconf
    inet6 2002:72xx:27xx:1:20c:29ff:fea1:xxxx prefixlen 64 autoconf
    ether 00:0c:29:xx:xx:xx
```

デフォルトルータも複数登録されている。

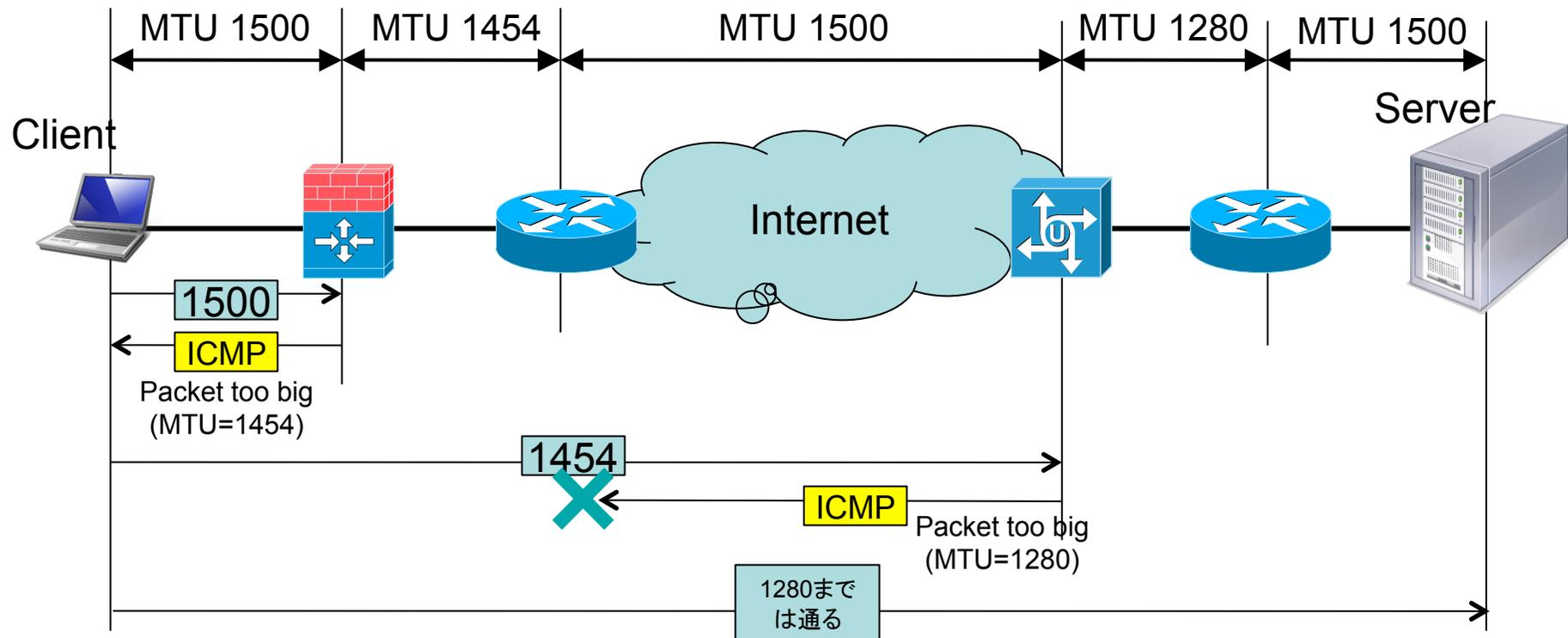
- RA送出装置の確認も可能
 - Windows: netsh interface ipv6 show neighbors 等
 - Mac/FreeBSD系: ndp -p 等

- ルータ広告送出機器の発見, 広告の停止
 - 小規模ネットワークでは発見, 対処は容易
 - 全クライアント機器での対応(再起動等)も必要
- (可能なら)L2レベルでのフィルタ
 - 不正RA対策の標準化は進んでいるので, 将来的には家庭内の機器も対応することを期待

- IPv6 は, 経路途中でパケットを断片化しない
 - 通信の両端で, 経路MTUの調整を実施(パスMTU検索)



- “ICMPv6 packet too big” がフィルタ等で届かない場合，パスMTU探索が動作しない。



•現象

- 簡単なWebページは見えるが、複雑なページが表示できない。
- 短いメールは届くが、長いメールが届かない

•確認方法

- ping6 による確認 (-s オプション等でサイズ指定)
- Linux: tracepath6 等の利用

Tracepath6 の出力

```
[shin@localhost ~]$ tracepath6 2001:a18:1:20::42
1?: [LOCALHOST] pmtu 1500
1: 2001:fa8:1000::1 3.803ms
1: 2001:fa8:1000::1 3.288ms
2: 2001:fa8:ffff:ffff::7:179 2.922ms
3: 2001:fa8:ffff:1::770:3 1.924ms asymm 4
4: 2001:218:2000:5000::35 3.113ms
5: 2001:218:0:6000::131 1.753ms asymm 6
6: 2001:218:0:2000::21 110.656ms asymm 7
7: 2001:418:0:2000::b6 101.572ms
8: 2001:418:0:5000::b6 120.589ms
9: 2001:1900:1b:1::4 234.129ms
10: 2001:1900:4:1::109 258.200ms asymm 13
11: 2001:1900:4:1::36 219.077ms
12: 2001:1900:4:1::1d 189.418ms asymm 13
13: 2001:1900:4:1::22 201.236ms asymm 12
14: 2001:1900:4:1::fd 183.251ms asymm 11
15: 2001:1900:4:1::ed 216.240ms asymm 11
16: 2001:1900:6:1::11 260.191ms asymm 10
17: 2001:1900:5:1::102 311.967ms asymm 10
18: 2001:1900:5:1::206 265.499ms asymm 9
19: 2001:1900:5:1::229 269.213ms asymm 7
20: 2001:1900:5:1::229 266.116ms pmtu 1450
20: 2001:1900:5:2::ea 287.139ms asymm 10
20: 2001:1900:5:2::ea 286.539ms asymm 10
21: 2001:a18:0:102::2 287.068ms asymm 11
22: 2001:a18:0:ff01::1 286.986ms asymm 12
23: 2001:a18:0:408::4 287.235ms reached
Resume: pmtu 1450 hops 23 back 52
```

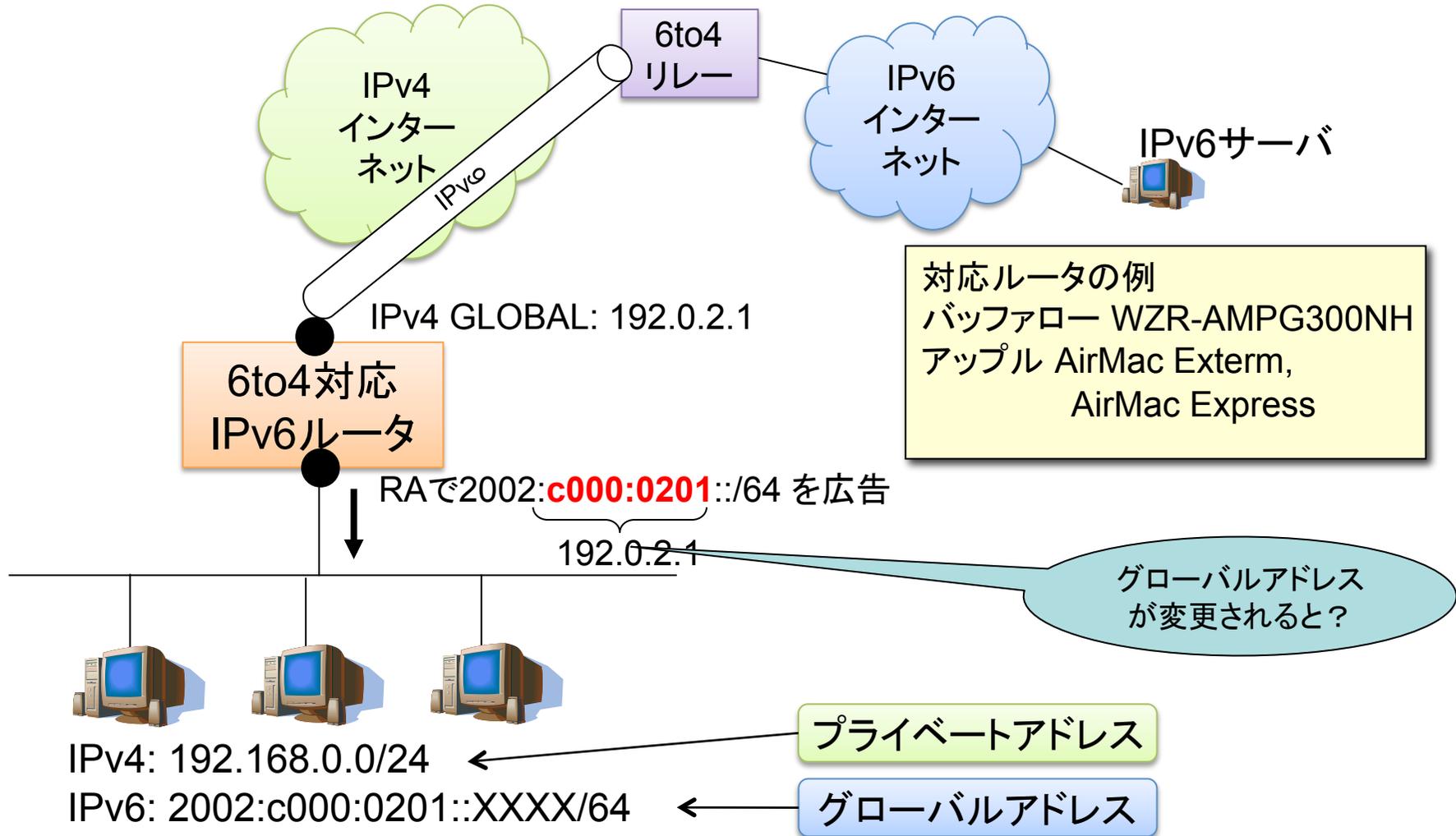
- ICMPv6 の返答がない
 - ファイアウォール等によるフィルタ
 - 経路途中のルータの過負荷
- ICMPv6のフィルタについて
 - IPv6では, ICMPv6に依存している部分多し
 - 以下のはフィルタ不可 ICMPv6 メッセージ:
 - Destination Unreachable (Type 1)
 - » All codes
 - Packet Too Big (Type 2)
 - Time Exceeded (Type 3)
 - » Code 0 only
 - Parameter Problem (Type 4)
 - » Codes 1 and 2 only
- RFC 4890 “Recommendations for Filtering ICMPv6 Messages in Firewalls” を参照.

- 自環境のMTUの調整
 - OSによっては、経路毎にMTUを設定可能
 - デフォルトのMTUを変更することも可能
 - ルータ広告のパラメータで指定可能
 - 小さくすると、通信効率は落ちる。
- 問題を発見した場合には、先方に対処を依頼する
- TCP通信に限っては、途中ルータや自ノードでのMSSの調整という解もある。

IPv6移行技術の導入によるもの

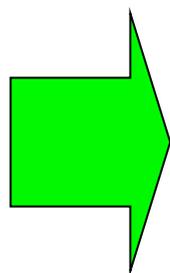
6to4とIPv6アドレス

6to4 により, 簡易にIPv6インターネットに接続できるが...

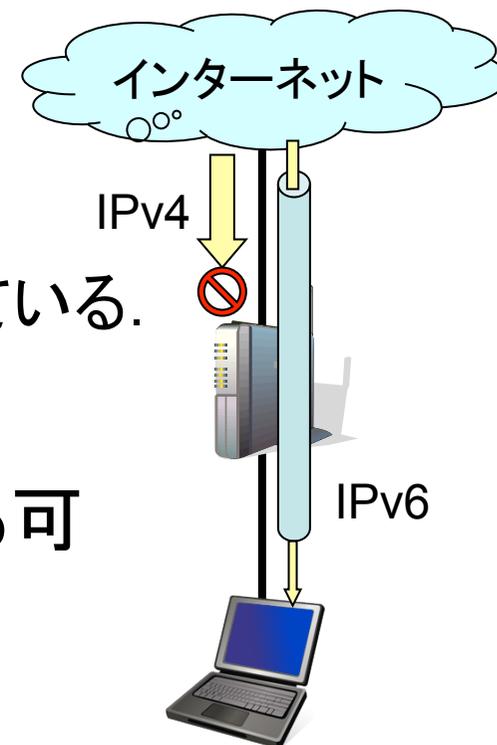


- 6to4 をまじめに使う場合には、固定IPv4アドレスの方がうれしい。
 - が、本末転倒？
- 今後、LSNが入ってくると、6to4 は動かなくなる。
 - グローバルアドレスが必要。

- 宅内機器（特に，PC）が，自動的にIPv4トンネルを利用したIPv6接続をする場合あり。
 - 6to4 (グローバルアドレスを持つ機器での利用を想定)
 - Windows OS, Airmac Extreme 等で実装されている
 - Teredo (NAT配下での利用を想定)
 - Windows OS 等に実装されている
- これらのトンネルが動作すると，ユーザは気がつかないうちにIPv6 reachable になっている。



フォールバック問題等にはまる可能性あり。



参考資料

RFC3484（アドレス選択ポリシー）は複数あるソースアドレスと宛先アドレスからどれを選択するかアルゴリズム。IPv6では実装はMUSTであり、WindowsではXP以降が実装。

RFC3484を使った対応策1の実現例

宛先アドレスとソースアドレスがそれぞれ2つずつある場合

宛先アドレス：A.[非優先IPv6アドレス], B.100.200.0.1

ソースアドレス：①[自IPv6アドレス], ②192.168.1.1

IPv6スタックに以下のテーブルを構成する
追加前の場合

IPv4優先のために
この行を追加する

Step1
宛先のラベルを求める

Step2
ソースアドレスを調べる

Step3
Step1とStep2で求めたラベルを比較して一致するアドレスを選択する→Aと①、Bと②

Step4
Step3の中から優先度の高いものを選択する→Aと①
宛先アドレス [自IPv6アドレス]
ソースアドレス [非優先IPv6アドレス]を選択

Prefix	優先順位	Label
[非優先IPv6アドレス]	60	6
::1/128	50	0
:::0	40	1
2002:::/16	30	2
:::/96	20	3
::ffff:0:0:/96 (IPv4アドレスの互換表記)	10	4

追加後の場合

Step1
宛先のラベルを求める

Step2
ソースアドレスを調べる

Step3
Step1とStep2で求めたラベルを比較して一致するアドレスを選択する→Bと②のみ
↓
宛先アドレス 100.200.0.1
ソースアドレス 192.168.1.1
を選択

← FallbackでIPv4通信