



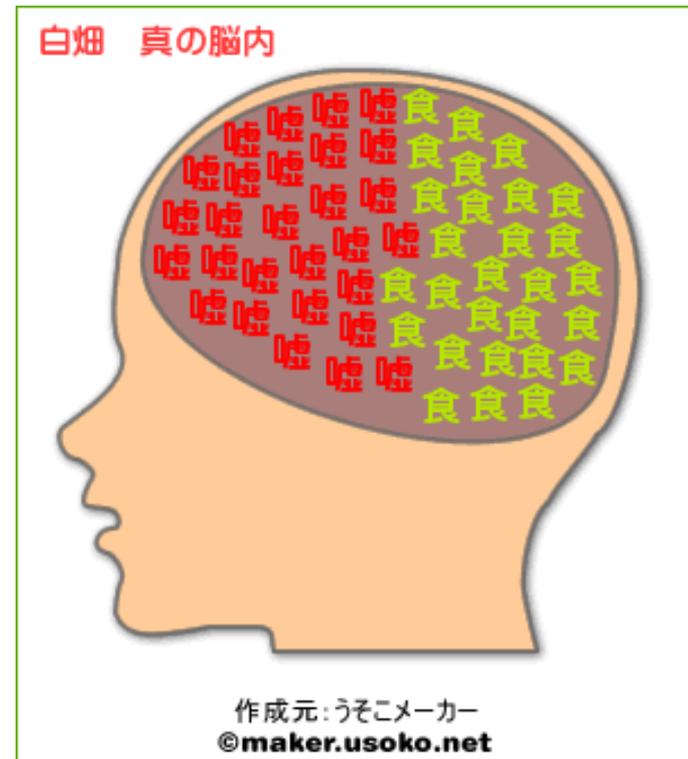
# IPv6自動トンネル技術とその展開

Tokyo6to4プロジェクト

白畑 真

# 自己紹介

- 仕事: 2000年より(株)クララオンライン
- ホスティング事業者
  - CTOという雑用係
    - 最近ではサービス企画、バックボーンネットワークの設計、運用など
- 2008年10月にTokyo6to4プロジェクトを設立
- 趣味: ドライブ (日帰り温泉 :-)

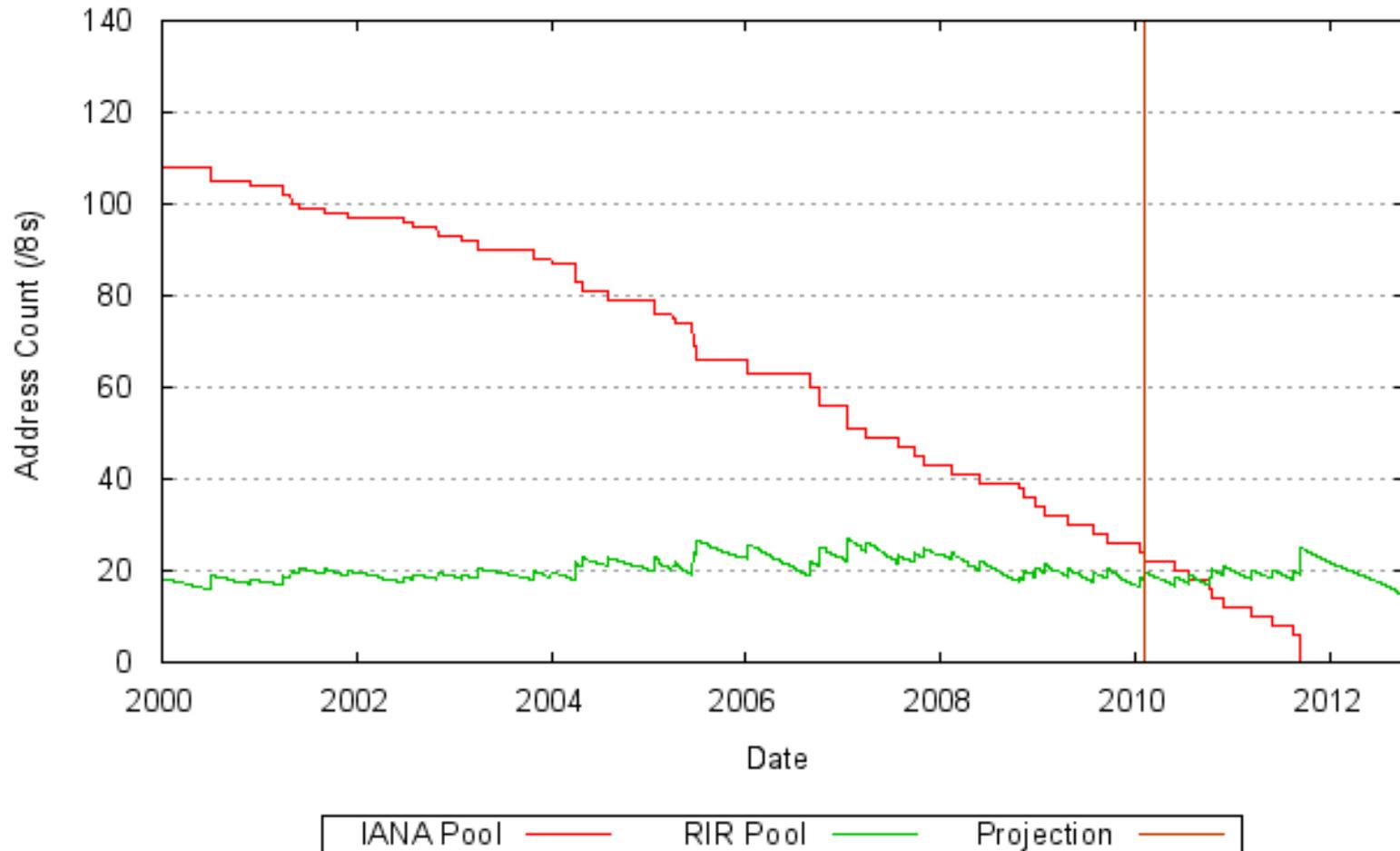




すでにご存じだと思いますが...

# IPv4アドレス在庫の枯渇

## 2011年末にJPNIC在庫が枯渇



# IPv4在庫枯渇問題への対応策

JPNIC「IPv4アドレス在庫枯渇問題に関する  
検討報告書（第一次）」より

(0) 未利用アドレスの  
回収・再在庫化  
および再分配

(1) IPv4アドレスの  
確保(自網での  
やりくりなど)

(2) IPv4 プライベート  
アドレス  
+ NATの利用

(3) IPv6の導入

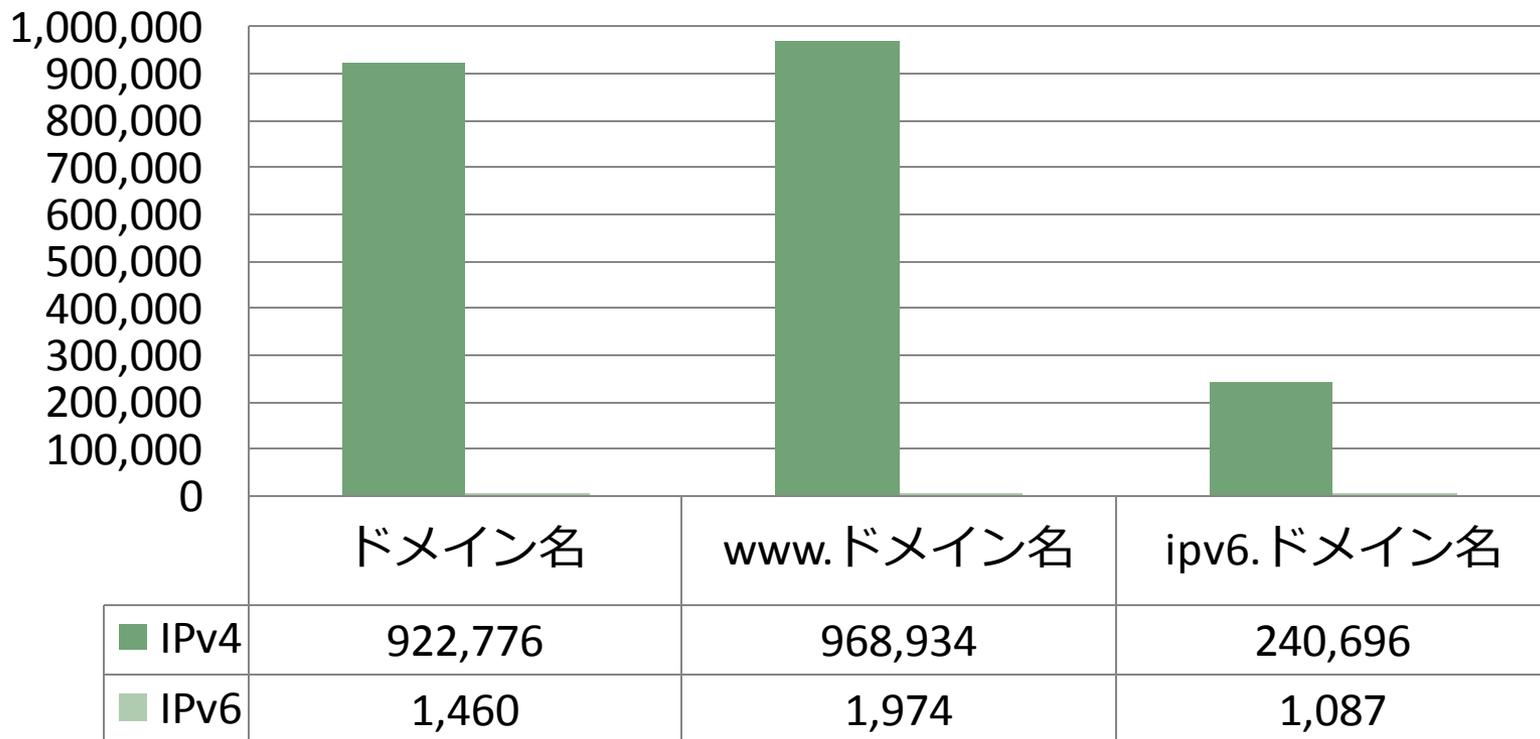


# IPV6の現実



## トップ100万ドメイン名の状況

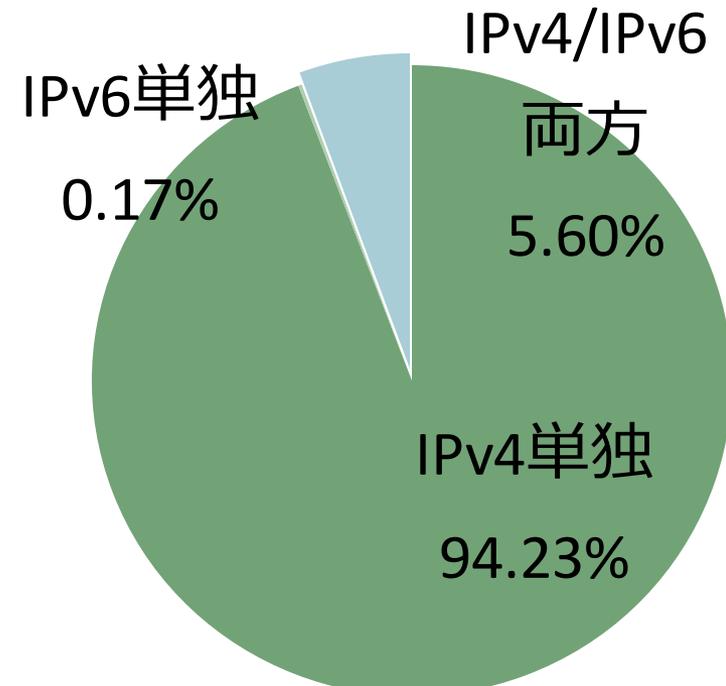
- Aレコード/AAAAレコードが設定されているドメイン数は?





# IPv6の普及状況: Autonomous System

- インターネットに広報されているAS数  
2010/2/6現在 (括弧内は2007/11/24)
  - IPv4単独: 31780 (26158)
  - IPv6単独: 58 (34)
  - IPv4/IPv6両方: 1888(684)
  - IPv4/IPv6合計: 33726 (26876)
- 徐々に増えてきてはいるが...

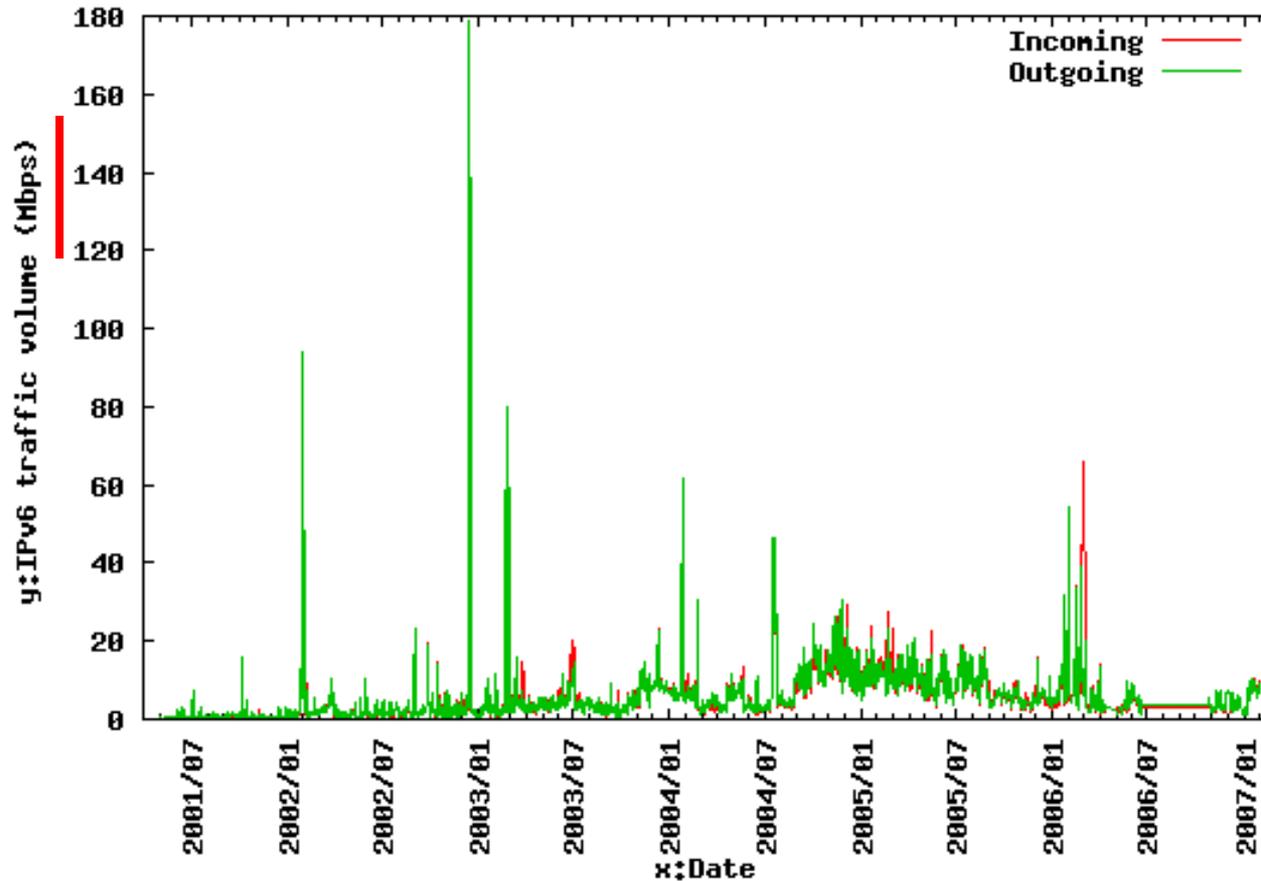




# IXにおけるトラフィック動向：IPv6

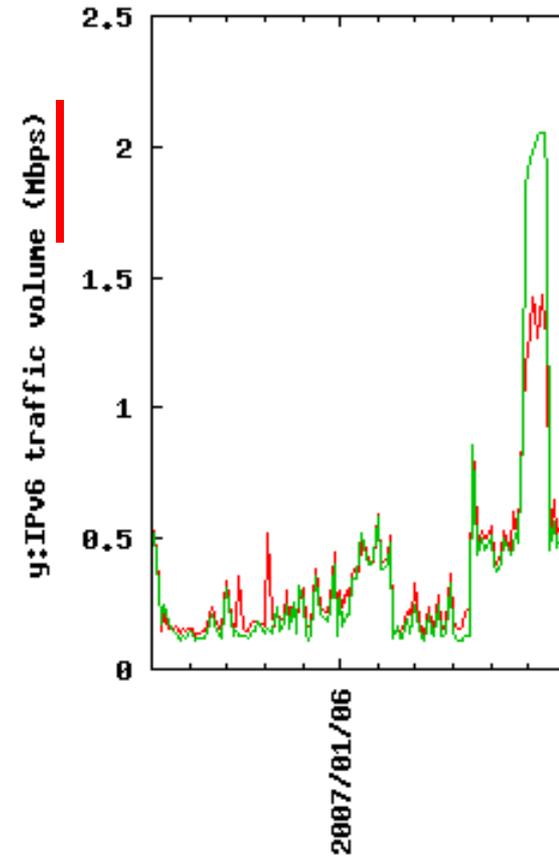


IPv6 traffic volume at an IX



Copyright (c) Internet Association Japan

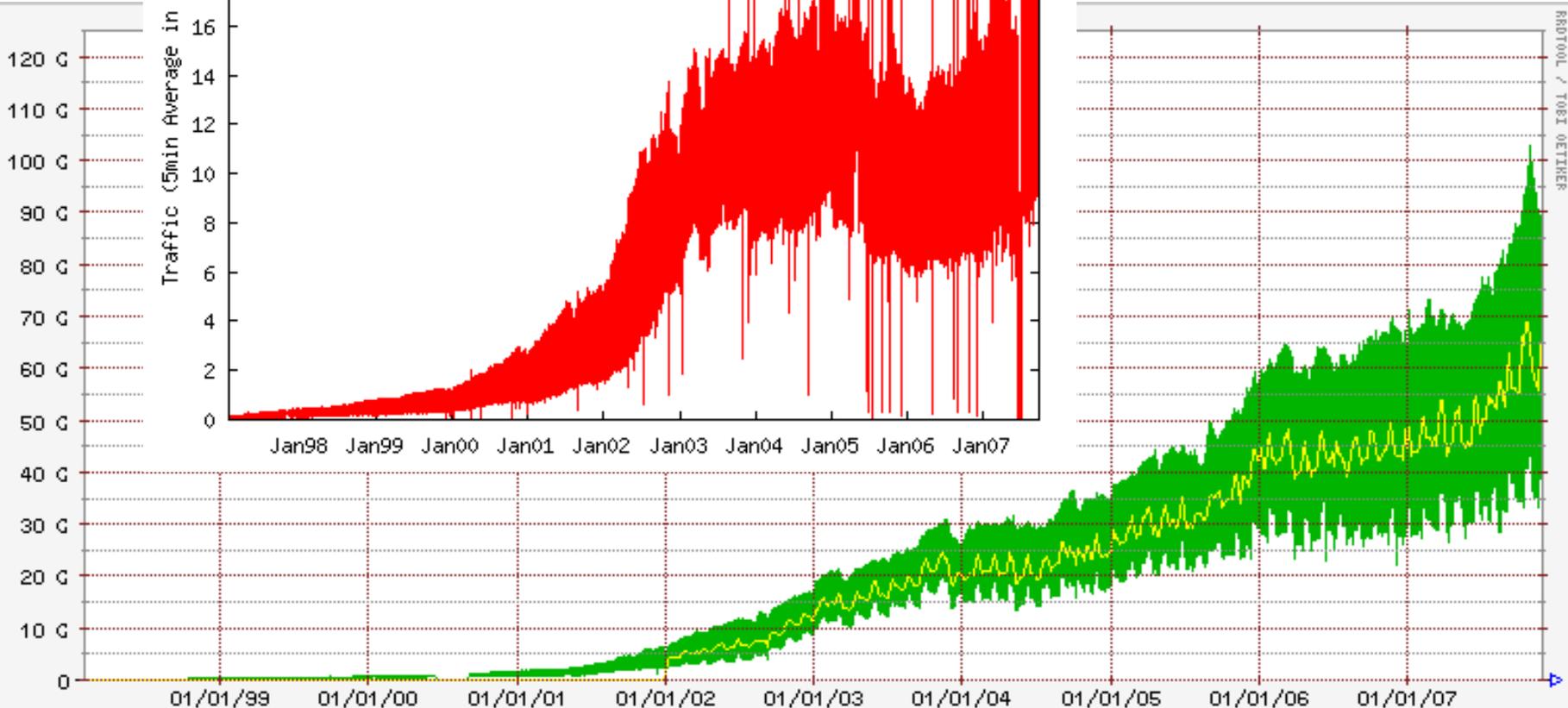
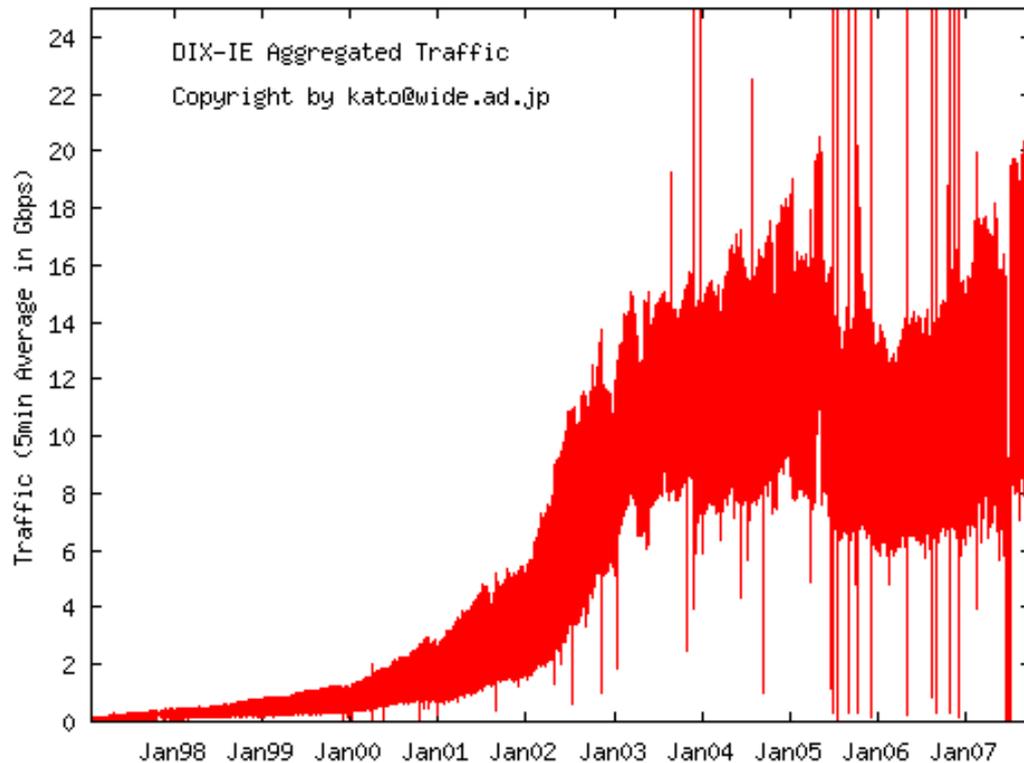
IPv6



Copyright (c)



# IXにおけるトラフィック動向：IPv4



■ 最大 □ 最小 ▲ 平均

Sun Nov 25 09:10:03 JST 2007

Copyright(c)2002-2006 JPIX All Rights Reserved.

Source: JaPan Internet eXchange <http://www.jpix.ad.jp/jp/technical/traffic.html>

(上) NSPIX-2 Traffic <http://nspix.wide.ad.jp/2/>



# IPV6自動トンネル技術と6TO4

# なぜIPv6自動トンネルなのか

- 商用IPv6接続サービス
  - 企業向けサービスが主であり、個人向けは少ない
    - オプションサービスであるケースが多い
  - サービスプロバイダの視点からは、需要がないとビジネスとして成立しにくい
- IPv6自動トンネル技術
  - ISPとの契約不要、(多くの場合)設定不要
  - とりあえず個人が簡単にIPv6を利用できる環境として適している



# 6to4とは

- IPv4ネットワーク上でIPv6パケットを転送できるようにする自動トンネル技術の一種
  - IPv4インターネットしかない環境からでもIPv6インターネットに到達可能
  - IPv6移行メカニズムとして設計、明示的なトンネル設定不要
- 6to4とトランスレータとの違い
  - 6to4はIPv4のみのホストとIPv6のみのホストの通信を可能にするわけではない



# IPv6自動トンネリング技術

	6to4	ISATAP	6rd	Teredo
IPv4アドレス	Anycast	Unicast	Unicast	Unicast
IPv6アドレス	Anycast	Unicast	Unicast	Anycast
NAT越え	未対応	未対応	未対応	一部対応 (UDP/IPv4)

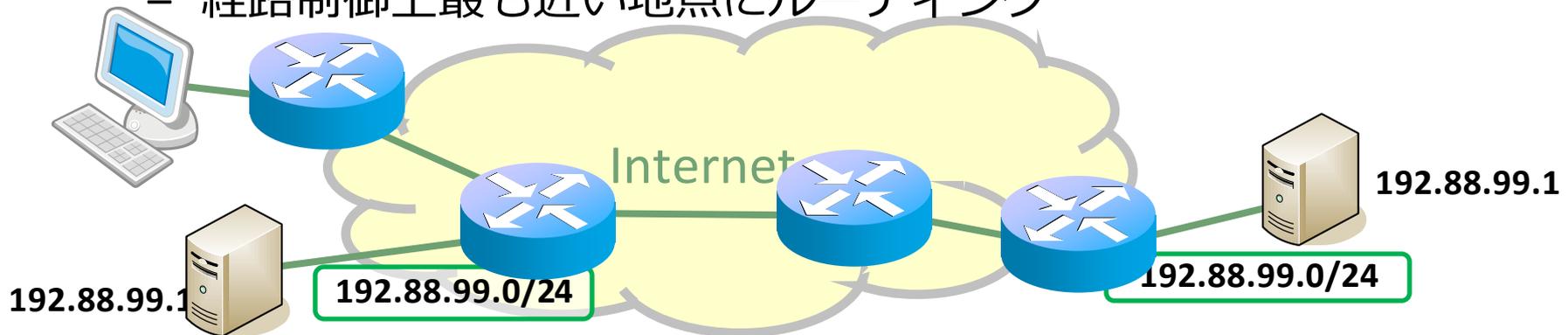
Tokyo6to4で、

↑運用中

↑準備中

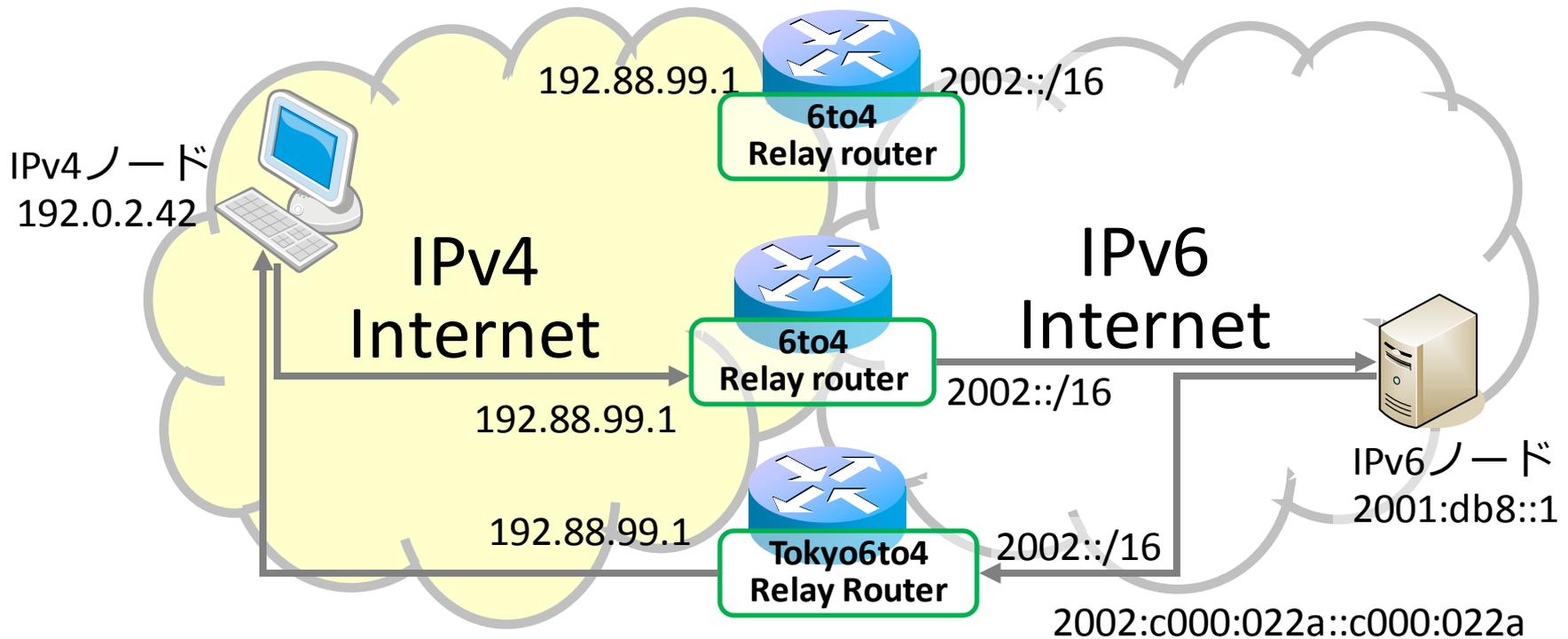
# IP Anycast

- Unicast: グローバルIPアドレスはユニーク(唯一無二)
- 同じIPアドレスを持つノードを複数設置
  - 経路制御上最も近い地点にルーティング



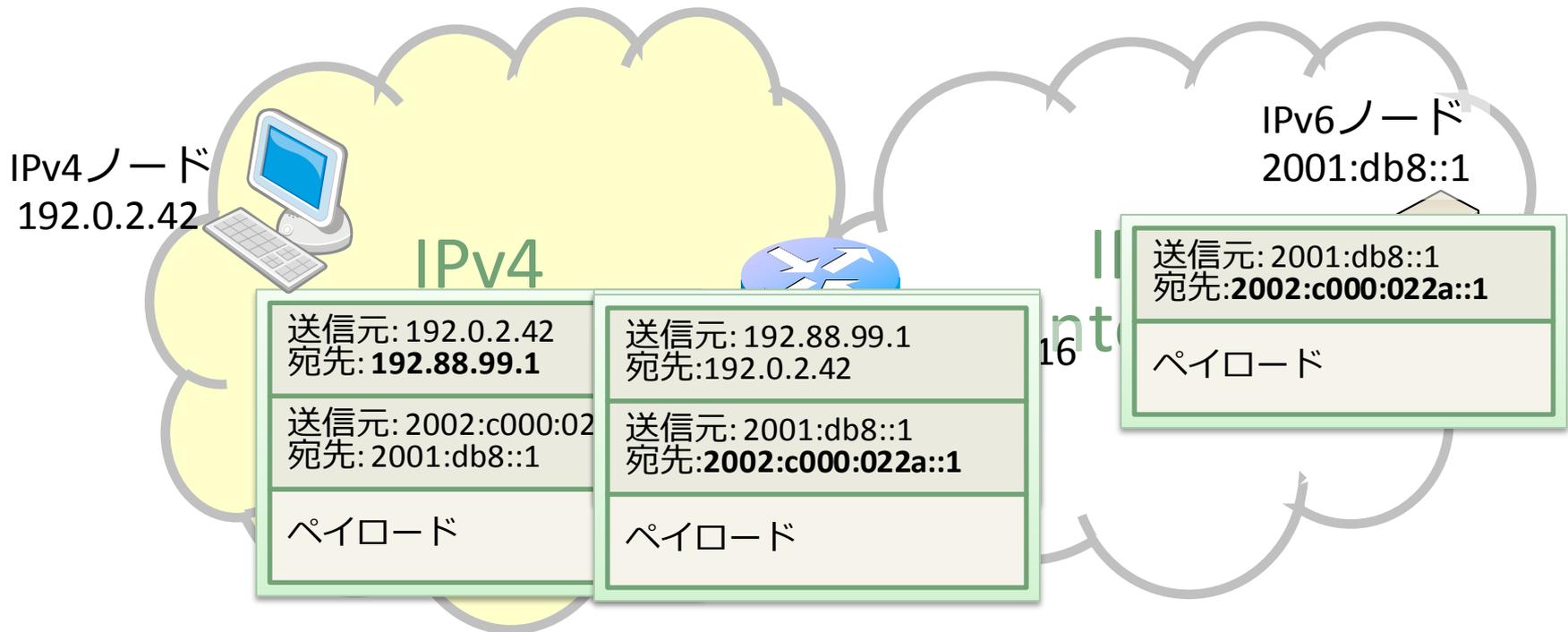
- Anycast技術の利用例:
  - Root DNS/ccTLD DNS(.jpなど)
  - 一部のCDN(Contents Delivery Network)
  - 6to4/TeredoなどIPv6自動トンネル

# 6to4リレールータとは



- IPv4インターネット上の6to4ノードとIPv6インターネット間の通信を相互に中継するルータ
  - リレールータは世界各地に設置され、同じアドレスを共有

# 6to4の動作





# 6to4アドレスの仕組み

- 2002::/16
  - 特別なアドレスプレフィックス [RFC3056]
- グローバルIPv4アドレス毎に/48が利用可能
  - /64のサブネットを複数利用できる
- IPv4アドレスをIPv6アドレスにマッピング

例: 192.0.2.42の場合

0~15	16-47	48-63	64-127
16bits	32bits	16bits	64bits
6TO4プレフィックス	IPv4アドレス	SLA ID	インタフェースID
2002	c000:022a	::c000:022a	

192 0 2 42

下位80bitについては実装依存。

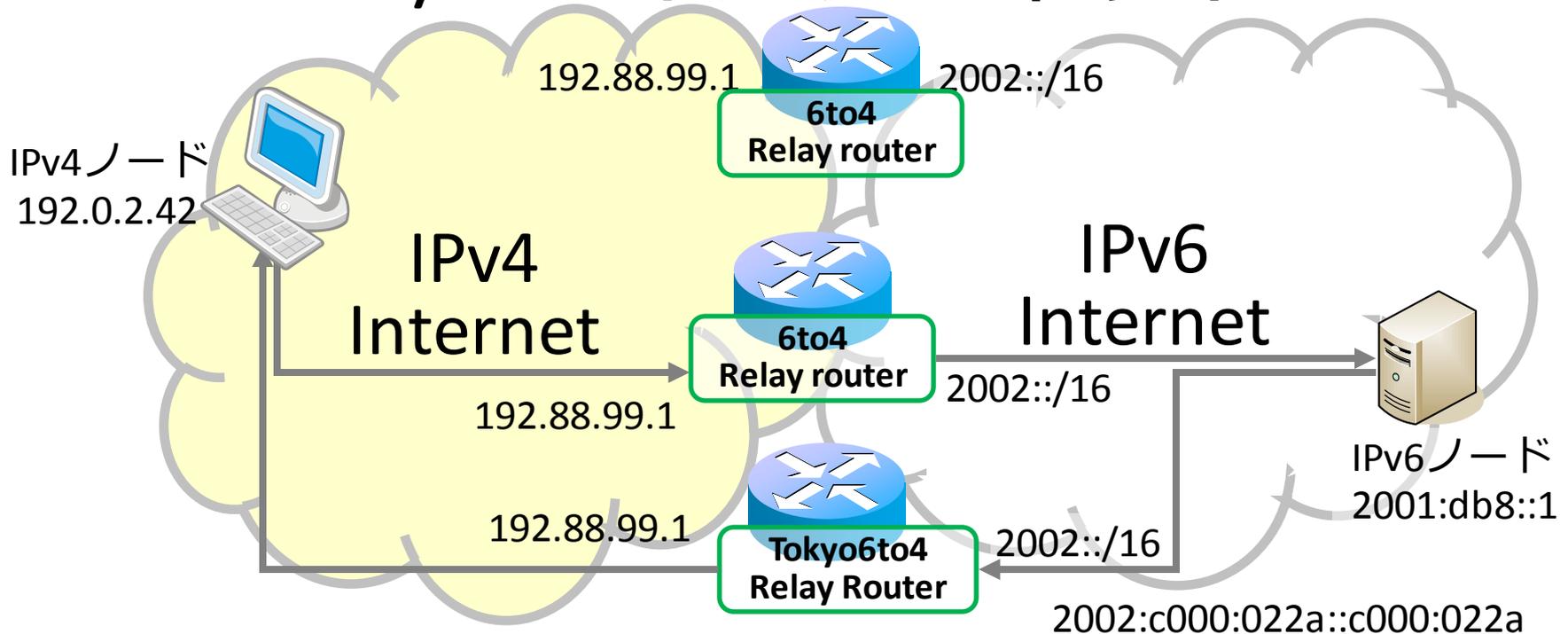
- Windowsの場合”::16進数のIPv4アドレス”
- Linuxでは”::1”



# 6to4の packets ヘッダ フォーマット

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Version				IHL			Type of Service					Total Length																			
Identification												Flags			Fragment Offset																
Time to Live					Protocol 41					Header Checksum																					
Source Address																															
Destination Address (192.88.99.1)																															
Options																								Padding							
IPv6 header and payload ...																															

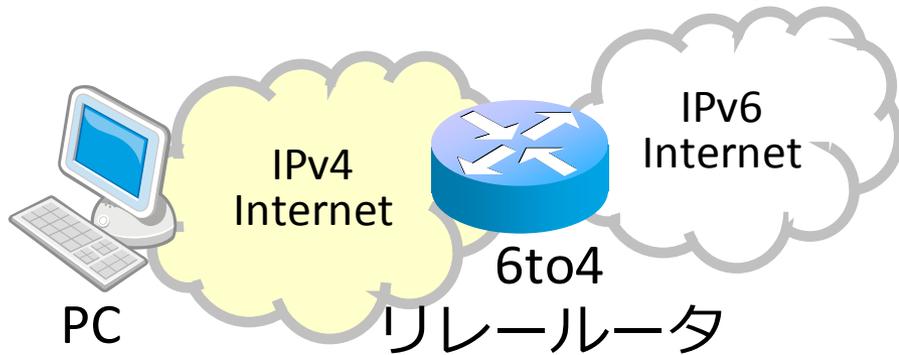
# 6to4リレールータと IPv4/IPv6インターネット



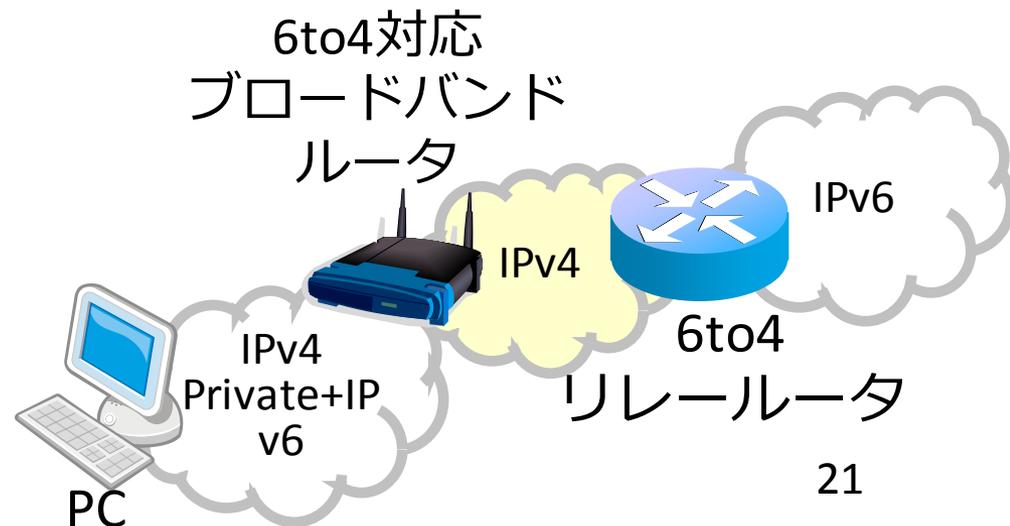
192.88.99.0/24と2002::/16がそれぞれAnycastされている  
行きと帰りの経路が非対称となる場合も。

# 接続方法

- **直接接続**
- PCにグローバルIPv4アドレスが割り当てられている場合

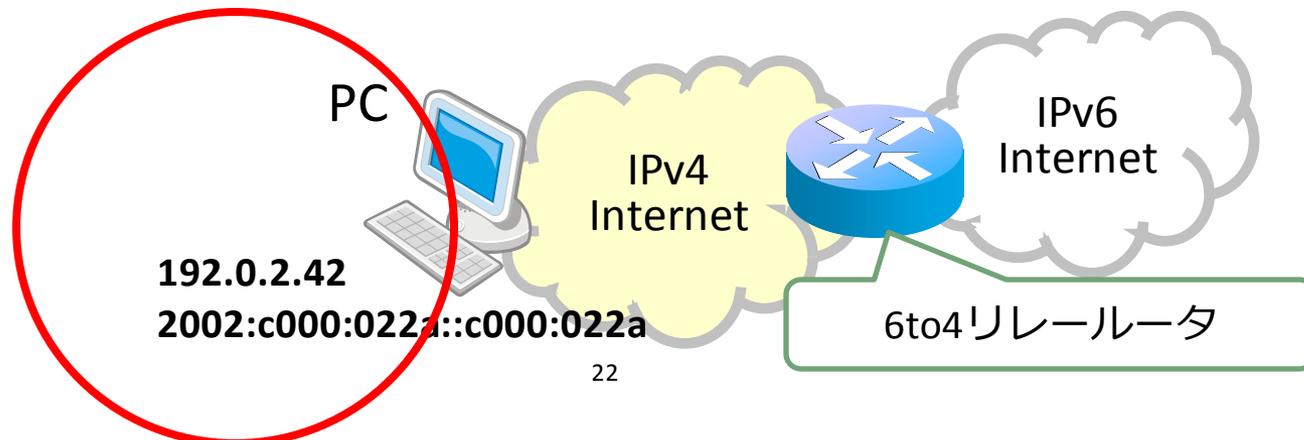


- **ブロードバンドルータ経由**
- ブロードバンドルータにグローバルIPv4アドレスが割り当てられている場合
- 6to4対応ブロードバンドルータが必要



# 直接接続による6to4接続

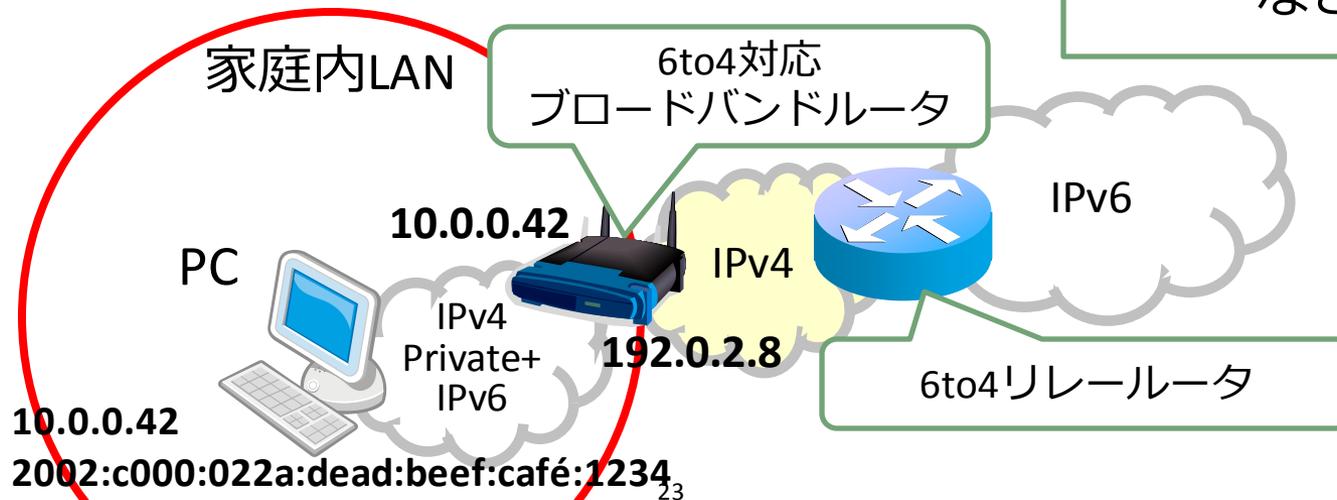
- PCにグローバルIPv4アドレスが割り当てられている環境で6to4を利用する方法
    - PCで6to4を終端
    - ダイヤルアップ接続、モバイル接続、ブロードバンドルータを使わない接続など
- ※IPプロトコル番号41がフィルタされていないこと



# ブロードバンドルータによる6to4接続

- 6to4ブロードバンドルータを利用しており、グローバルIPv4アドレスがルータに割り当てられている場合
- 6to4対応ブロードバンドルータが必要
  - ブロードバンドルータが6to4を終端
  - PCとブロードバンドルータ間はNative IPv6
    - ブロードバンドルータがRAを広報

Apple社 AirMac  
Extreme, TimeCapsule  
BUFFALO社  
WZR-AMPG300NH  
など...





# 6to4接続が利用される状況について

サーバ側	標準で利用されるプロトコル
IPv4	IPv4 接続
IPv4/IPv6	
IPv6	6to4によるIPv6接続

例:

- <http://www.kame.net/> (IPv4/IPv6デュアルスタック)  
6to4が有効な場合でもIPv4接続が利用される。
  - <http://IPv6.google.com/> (IPv6 シングルスタック)  
名前解決ができる場合、6to4が利用される。
- クライアントのポリシーテーブルの設定を変更することで、IPv4/IPv6デュアルスタック接続時に6to4の利用を強制できる  
詳細: <http://www.tokyo6to4.net/index.php/6to4の利用方法>



**TEREDO**



# Teredoとは

- IPv4自動トンネリング技術の一種
  - IPv6をIPv4のUDPパケット内にカプセル化
  - クライアントには/128が割り当て
- 多くの種類のNATを越えられる
  - Cone NAT, Restricted NAT に対応
- Microsoft社により開発
  - Windows XP以降で利用可能
  - オープンソース実装(Miredoなど)も存在。Mac OS X, Linux, \*BSDなどで利用できる



# Teredoの動作の概略 (Restricted NATの場合)

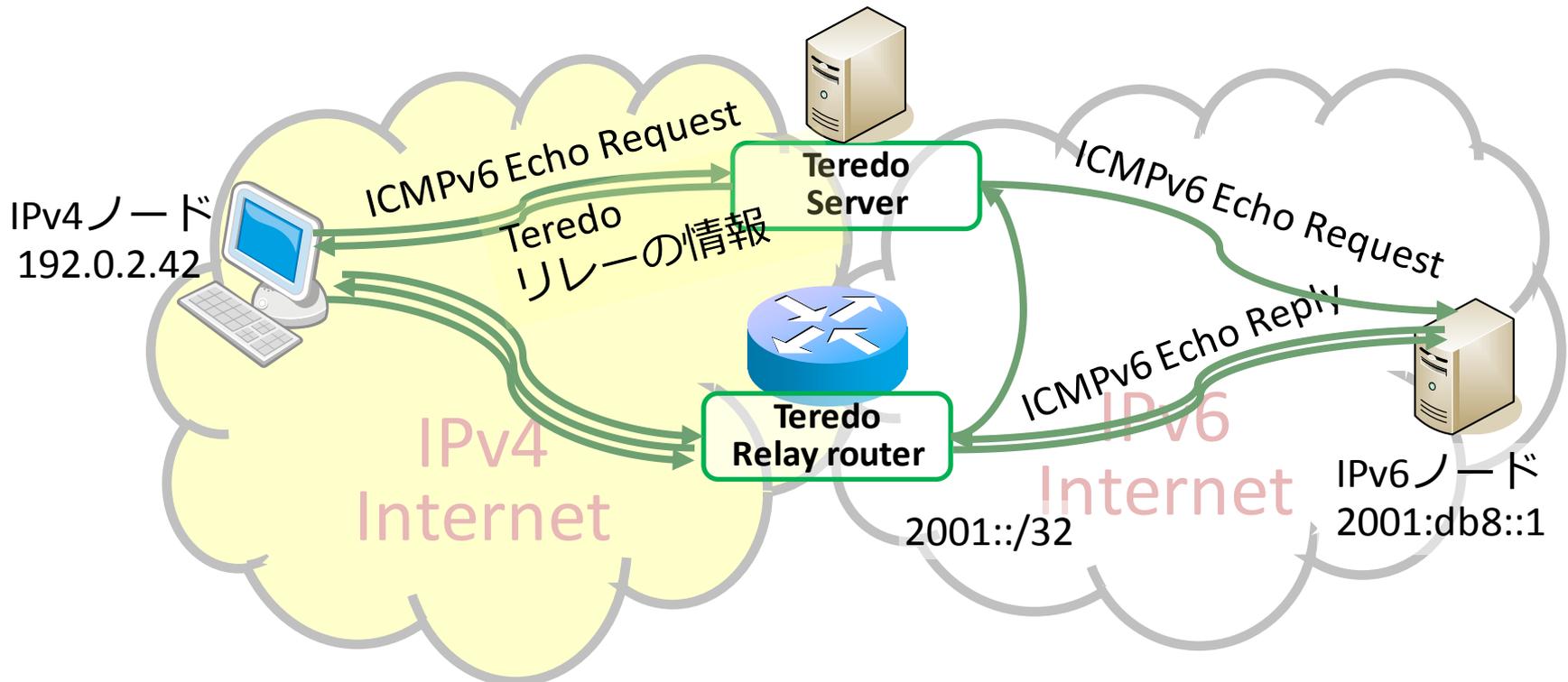
## 準備

1. NATのタイプを判別
  - TeredoクライアントがNAT内部からTeredoサーバにパケット送信
2. TeredoクライアントがTeredoサーバ経由でIPv6ホストにパケットを送信
3. IPv6ホストがTeredoリレーにパケットを送信。TeredoリレーからTeredoサーバを経由してクライアントにパケットが届く。
  - この際、クライアントはTeredoリレーの情報を得る
4. TeredoクライアントがTeredoリレーと通信開始

## TeredoによるIPv6通信

5. Teredoリレーとクライアントの通信開始

# Teredoの通信の概略 (Restricted NATの場合)



TeredoでNAT越えに利用する packets を「バブル」と呼ぶ  
通信が確立されるまで数秒程度かかる

# Teredoのアドレス形式

- 2001::/32
  - Teredo専用のプレフィックス [RFC4380]
- Teredoサーバのアドレス
- NAT実装の種類(cone NATとそれ以外)
- UDPポート番号とNAT箱のIPv4アドレス
  - XORにより難読化  
例: 3ffffdd2 xor ffffffff = c000022d. 10進数では 192.0.2.45

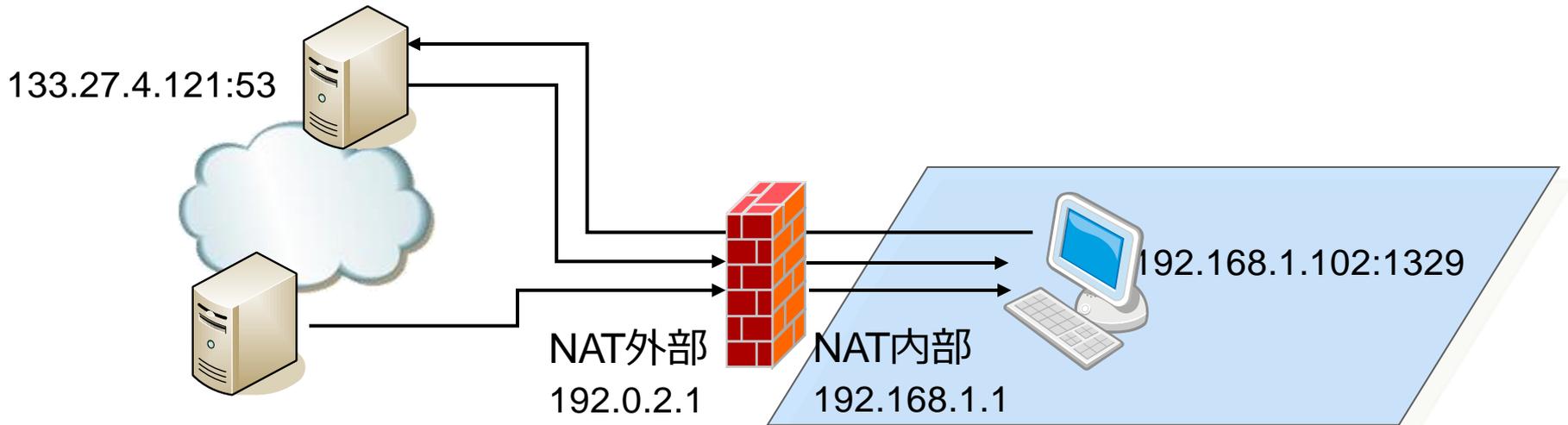
	0~31	32~63	64~79	80~95	96~127
長さ	32bits	32bits	16bits	16bits	32bits
説明	Teredo プレフィックス	Teredoサーバ IPv4アドレス	フラグ	UDP ポート	クライアント パブリック IPv4アドレス
部分 復元	<b>2001:0000</b>	<b>4136:e378</b>  65.54.227.120	<b>8000</b>  cone NAT	<b>63bf</b>  40000	<b>3fff:fdd2</b>  192.0.2.45



# さまざまなNAT

- さまざまなNAT実装
  - RFC3489で主要な実装が整理されている
    - いわゆるNAT越え技術の中での議論
  - NATは必ずしもFirewallの代わりにならない
- Full Cone NAT
- Restricted Cone NAT
- Port Restricted Cone NAT
- Symmetric NAT
  - これらのNAT実装に対するUDPの処理を説明
  - 必ずしもこれらの分類に当てはまらない実装も

# Full Cone NAT

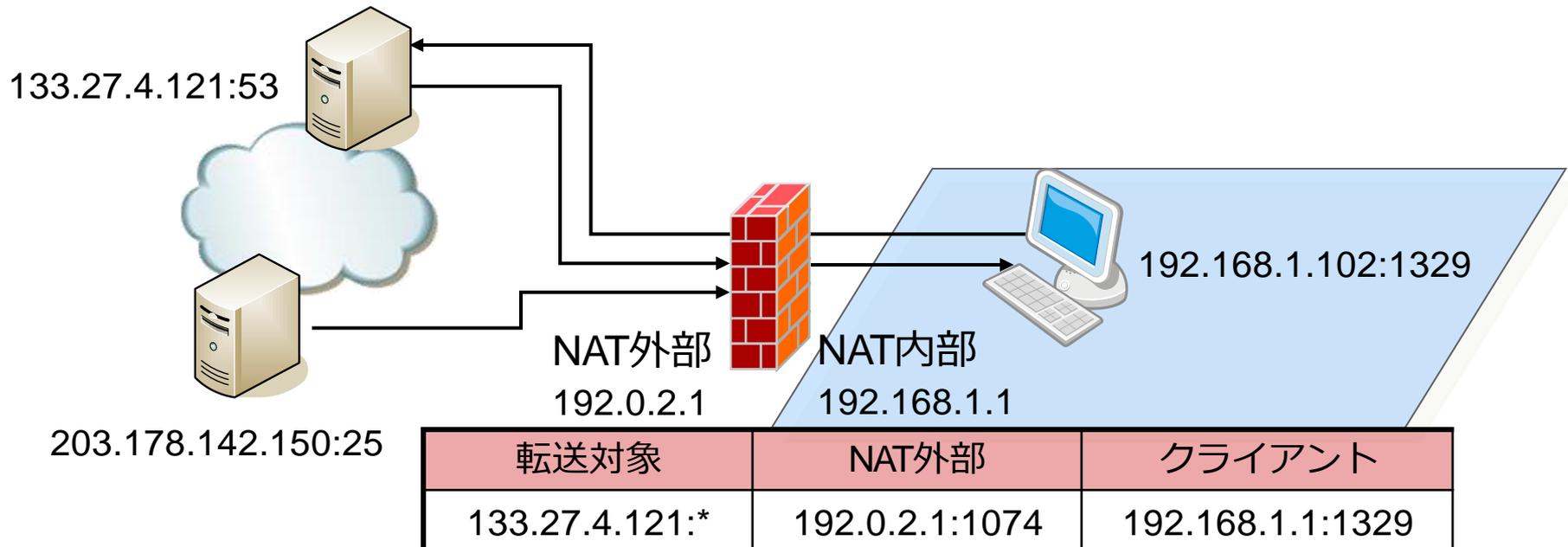


転送対象	NAT外部	クライアント
*.*	192.0.2.1:1074	192.168.1.1:1329

## • Full Cone NATの動作

- NAT内部のクライアントがパケットを最初に送信した際に、NATルータの外部のインタフェースのポート番号とクライアントのポート番号が1:1で割り当てられる
- NAT外部に割り当てられたIPアドレス/ポート番号がパケットを受信した場合、**任意のIPアドレス/ポート番号からのパケット**をNAT内部に転送

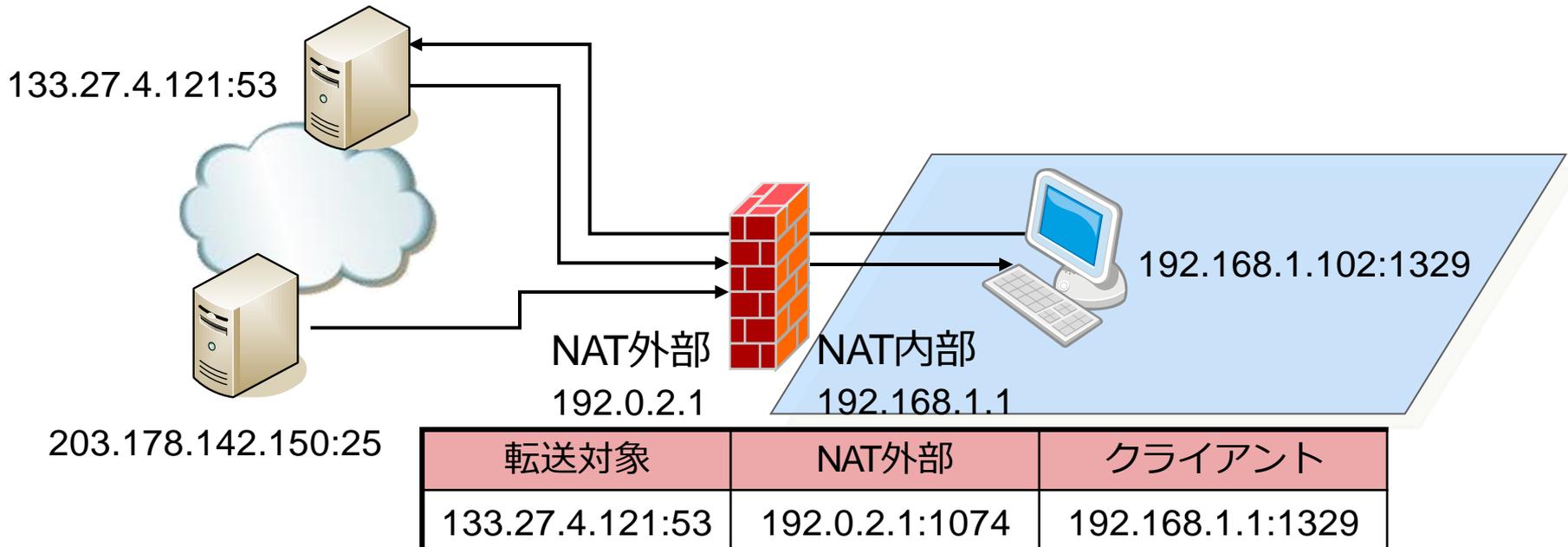
# Restricted Cone NAT



## • Restricted Cone NATの動作

- NAT内部のクライアントのポートとNATルータの外部のインタフェースのポート番号が1:1で割り当てられる
- NAT外部に割り当てられたIPアドレス/ポート番号がパケットを受信した場合、**NATのエントリの相手先IPアドレス(クライアントが接続した相手先IPアドレス)**からのパケットをポート番号にかかわらずNAT内部のクライアントに転送

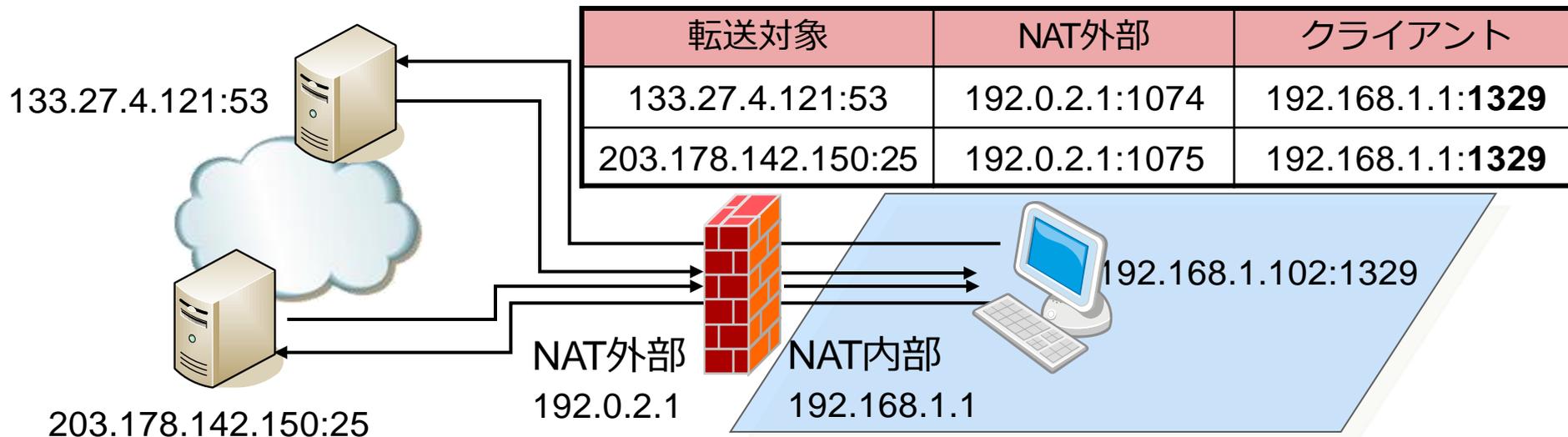
# Port Restricted Cone NAT



## □ Port Restricted Cone NATの動作

- NAT内部のクライアントのポートとNATルータの外部のインタフェースのポート番号が1:1で割り当てられる
- NAT外部に割り当てられたIPアドレス/ポート番号がパケットを受信した場合、**NATのエントリの相手先IPアドレスとポート番号**(クライアントが接続した相手先IPアドレス)からのパケットをNAT内部のクライアントに転送
- 同じ送信元ポート番号を使って異なる宛先IPアドレスに送った場合、NATルータの外部ポート番号は同じになる

# Symmetric NAT



## □ Symmetric NATの動作

- これまで説明した以外のNAT
- NAT内部のクライアントのポートと、NATルータの外部のインターフェースのポート番号はセッション毎に割り当てられる
- NAT外部に割り当てられたIPアドレス/ポート番号がパケットを受信した場合、NATのエントリの相手先IPアドレスとポート番号(クライアントが接続した相手先IPアドレス)からのパケットをNAT内部のクライアントに転送



**TOKYO6TO4**



# Tokyo6to4プロジェクトについて

- 目的: 自動トンネリング技術によるIPv6インターネット接続性の提供を通じたIPv6利用環境整備
  - 商用IPv6接続サービスが広く普及するまでの「つなぎ」
- 若手技術者を中心としたボランティアによる任意団体
  - 既存の組織に対して中立
  - メンバーの資材持ち寄りと各社様の協賛により運営
- 機材
  - 現在、DIX-IEおよびJPIXに接続
  - IPv4/IPv6 ピアリングパートナー様募集中
- Webサイト: <http://www.tokyo6to4.net/>



# プロジェクトのモチベーション

- IPv4ユーザ向けの**お試し**IPv6環境づくり
  - 手始めに実装が普及している**6to4**に着目
    - Windows, Mac OS X, Linux, \*BSD, Solaris, Cisco IOS..
  - 次のステップとしてTeredoを検討
- IPv4/IPv6共存技術の普及
  - 設定・運用ノウハウの共有
  - 設定や負荷状況などの情報公開



# モチベーション for Users

- IPv6を簡単に試せる環境づくり
  - **6to4, Teredo, ISATAP等の自動トンネル技術で、多くのIPv4インターネットユーザに、IPv6に触れていただける環境をつくりたい**
    - Windows XP, Vistaや一部のルータ(AirMac Extreme等)では6to4を利用可能
    - 6to4はあくまでIPv6導入初期のお試し環境
  - プロジェクト開始時点では6to4リレールータは海外にしかなかった
    - KDDI研究所の6to4リレールータ(<http://www.6to4.jp/>)の運用は2006年3月で終了



# モチベーション for Network Operators

- IPv4/IPv6共存技術としての自動トンネリング技術の導入
  - 多くのネットワークで6to4リレールータが運用されるように、ひいてはネイティブIPv6が導入されるようになってほしい
    - 今回はPCルータ(DELL PowerEdge 1950 + Quagga)を利用
- ノウハウの共有
  - 構築・運用を行ううえで必要な情報共有
  - ハードウェア構成、ソフトウェア設定例、トラブルフィックス、パフォーマンス情報 etc..
    - パスワード等を除き積極的に公開予定



# 2008年当時に考えていた運用

- 期間限定での運用(1~2年程度を予定)
  - スケーラビリティ等のノウハウ蓄積と公開
  - ISPの商用IPv6サービスとのすみわけ
  - 6to4はあくまでパブリックサービスであり、  
ビジネスモデルを構築しにくい
- KDDI研究所の6to4.jpとの違い
  - IPv4 Anycast アドレスでの運用  
(192.88.99.0/24)



## プロジェクトのあらまし: 2008年の活動

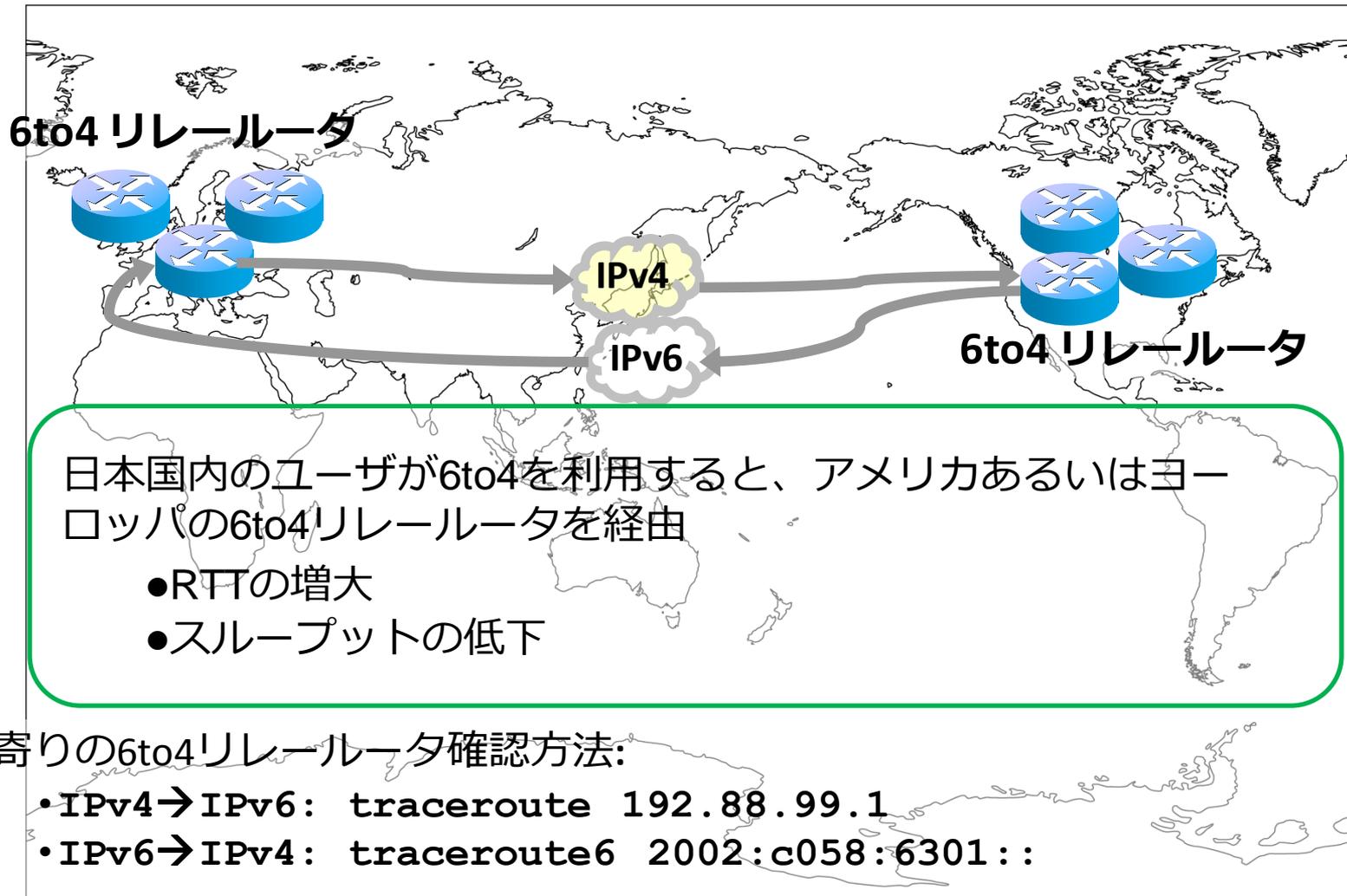
- 9月終盤: プロジェクトを構想、設立
- 10月21日: キックオフテレコン
- 10月25日～26日未明: 慶応大学湘南藤沢キャンパスにてインストール大会
- 10月31日: NSPIXPミーティングで6to4リレーの運用をアナウンス
- 11月: さくらインターネットさんで性能試験
- 11月6日: AS番号(AS38646)取得
- 12月2日: KDDI大手町ビル内のラックにマウント
- 12月6日: WIDEインターネットに対してIPv6の6to4プレフィックス(2002::/16)を広報開始
- 12月26日: 公式にリレールータの運用を開始



## プロジェクトのあらまし: 2009年の活動

- 1月20日: DIX-IE上でISP様とピアリング開始、192.88.99.0/24を広報
- 6月29日: Cisco 3825をCiscoさんよりお借りする
- 7月16日: 慶応大学三田キャンパスでCisco箱のセットアップとテストを行う
- 7月31日: JPIXに接続
- 8月7日: JPIX上でISP様とピアリング開始
- 12月24日: IPv4のプロバイダ独立アドレスを取得

# 6to4利用時の課題





# 6to4 relay anycast address Origin ASN list (1/2)

## Europe:

- Denmark:
  - 1835 FSK Net
- Estonia:
  - 3327 Linxtelecom
- Finland:
  - 1741 FUNET
- Germany:
  - 286 kpn.de
  - 5430 Freenet
  - 8767 m-net.de
  - 12816 mwn
  - 15598 IP Exchange
  - 20640 Titan
  - 29259 IABG Teleport
  - 35244 kms.de
- Italy:
  - 12779 itgate.net
- Netherlands:
  - 1101 SURFNet
  - 8954 InTouch
  - 26943 Your.Org
  - 31383 Computel
- Portugal:
  - 1930 FCCN
- Spain:
  - 16206 Abared
- Sweden:
  - 1257 Tele2
  - 16150 GlobalTransit
- Switzerland:
  - 559 switch.ch
- United Kingdom:
  - 5400 BT



# 6to4 relay anycast address Origin ASN list (2/2)

## Oceania/Asia:

- Australia:
  - 1221 Telstra
- Korea:
  - 17832 NISA

日本国内に無かった

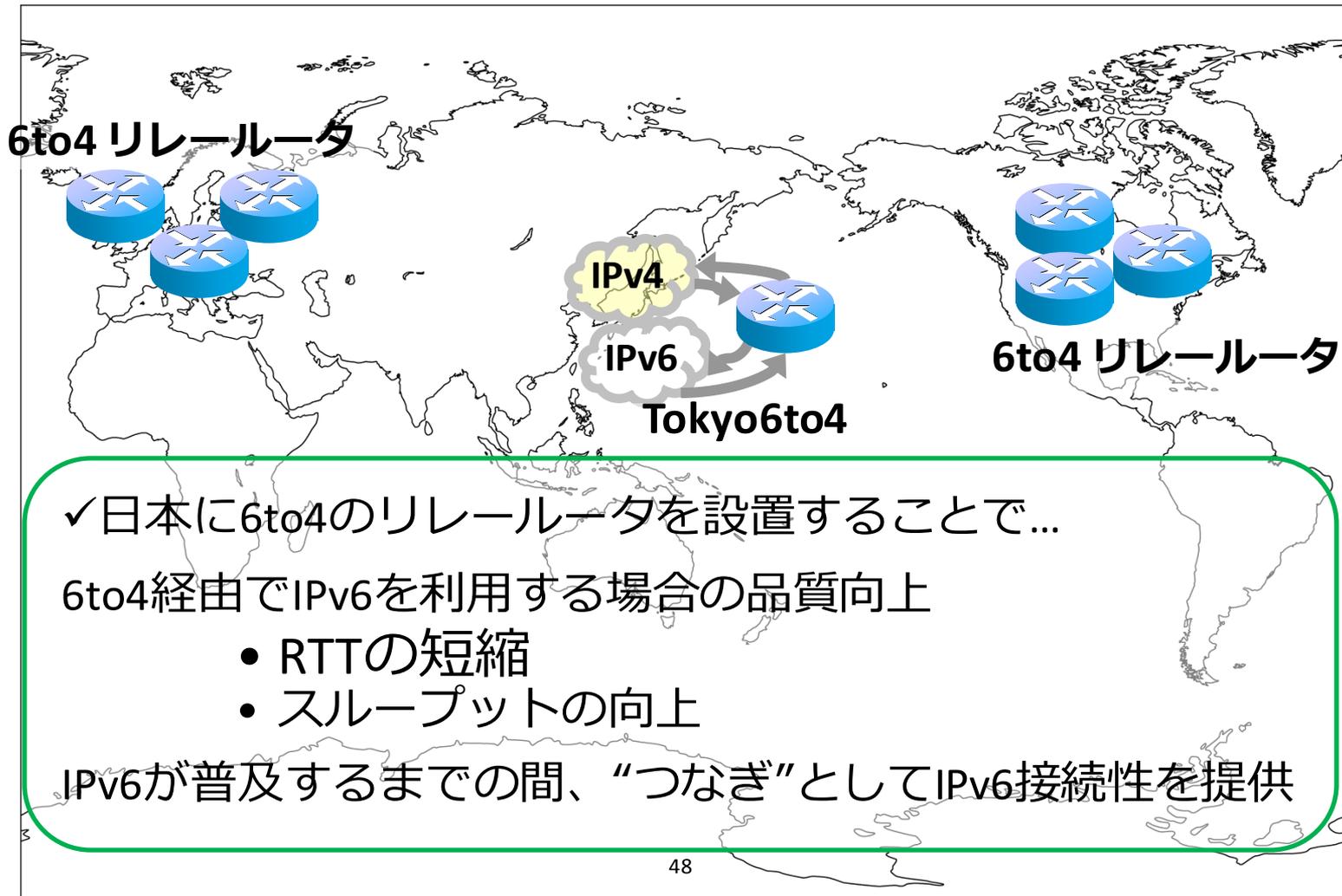


Tokyo6to4プロジェクトで  
日本国内にリレールータを！

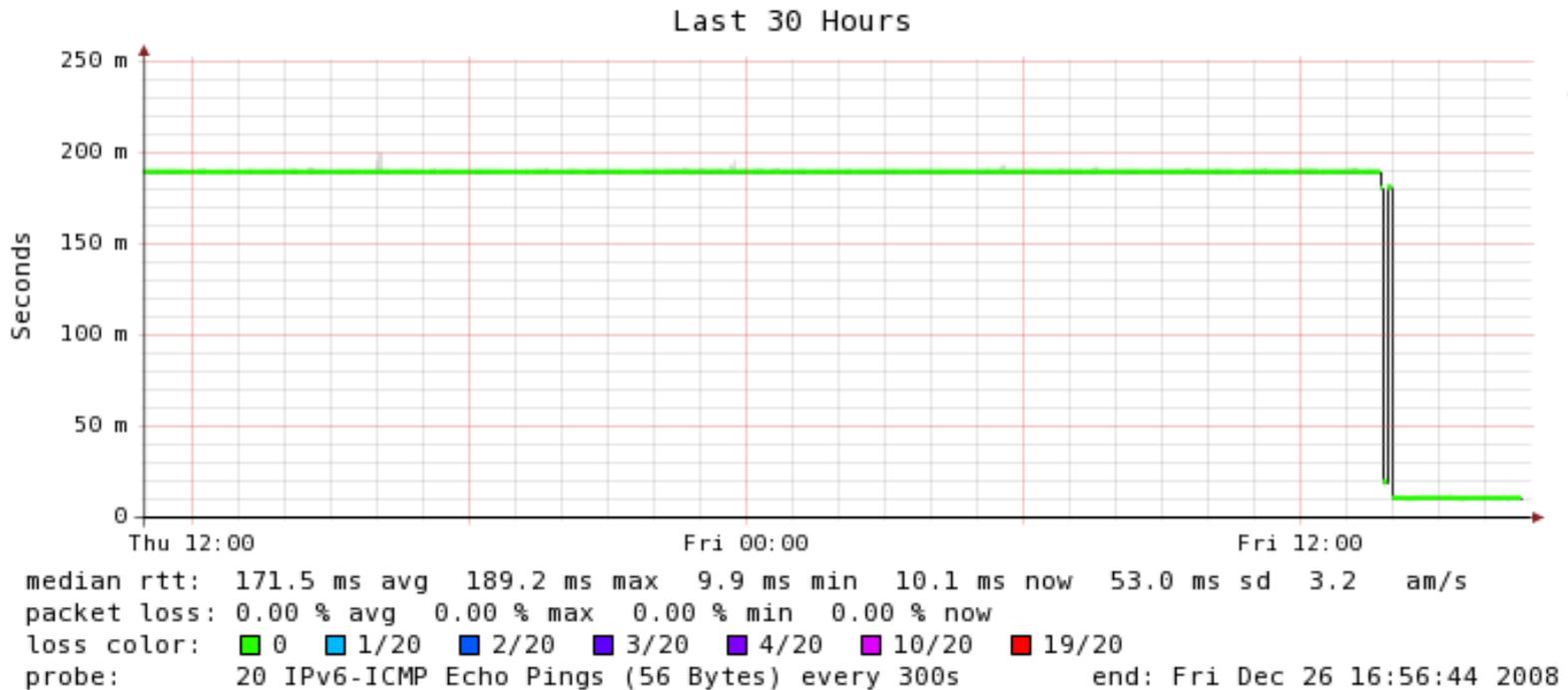
## North America:

- US:
  - 59 University of Wisconsin
  - 109 Cisco
  - 1239 Sprint
  - 3344 Kewlio
  - 5050 Pittsburgh Supercomputing Center
  - 6175 Sprint
  - 7019 NTT
  - 10533 Ottawa Internet Exchange
  - 19255 Your.Org
  - 19782 Indiana University
  - 25795 ARP Networks

# Tokyo6to4 プロジェクト使用後



# わかりやすい効果



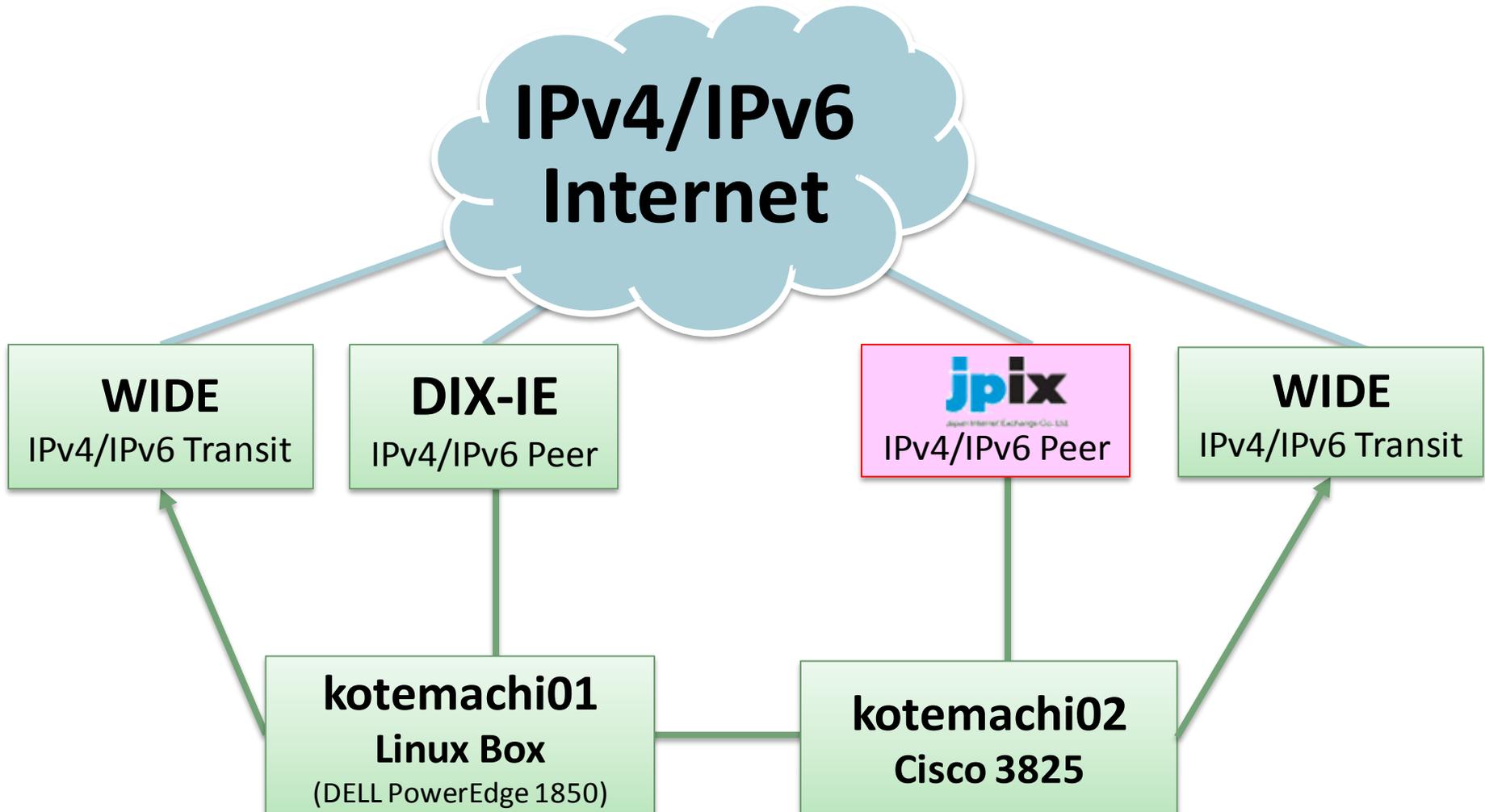
6to4を経由したwww.kame.netへのRTT  
- 約190msから10ms以下に



# リレールータの確認方法

- Tokyo6to4のリレールータを利用しているかを確認する方法は?
- 6to4ノードでtracert6を実行する
  - 1stホップが“2001:200:0:b000:192:88:99:1”だった場合、トラフィックはTokyo6to4のリレールータを経由している。
  - 異なるIPv6アドレスの場合、他の6to4リレールータを経由している。

# ネットワーク構成





# 6to4リレールータの設定: Linux (抜粋)

- Debian系
- /etc/network/interfaces

```
auto tun6to4
iface tun6to4 inet6 v4tunnel
    endpoint any local
    192.88.99.1
up ip -6 route add
2002::/16 dev tun6to4
    mtu 1472
    ttl 128
```
- コマンドで書くと...

```
/sbin/ip tunnel add tun6to4
    mode sit ttl 128 remote any
    local 192.88.99.1
/sbin/ip link set dev tun6to4 up
/sbin/ip -4 addr add
    192.88.99.1/32 dev tun6to4
/sbin/ip -6 route add 2002::/16
    dev tun6to4
```

※別途、この箱に192.88.99.0/24と2002::/16が来るようにルーティングの設定が必要



# 6to4リレータの設定: Cisco IOS (抜粋)

interface Loopback0

```
ip address 192.88.99.1  
255.255.255.255 secondary
```

```
ip address 203.178.148.4  
255.255.255.255 secondary
```

※通常のIOSの6to4リレーの設定ではSecondary IPアドレスは1つで良いため、本来この行は不要。Tokyo6to4の特殊事情(次スライド)で設定

```
ip address 192.88.99.2  
255.255.255.255
```

```
no ip redirects
```

```
no ip proxy-arp
```

```
ipv6 address 2002:CBB2:9404::1/128
```

```
ipv6 mtu 1480
```

```
no ipv6 redirects
```

interface Tunnel0

```
description 6to4 relay
```

```
no ip address
```

```
no ip redirects
```

```
no ip proxy-arp
```

```
ipv6 address 2002:C058:6301::/128  
anycast
```

```
ipv6 unnumbered Loopback0
```

```
no ipv6 redirects
```

```
tunnel source Loopback0
```

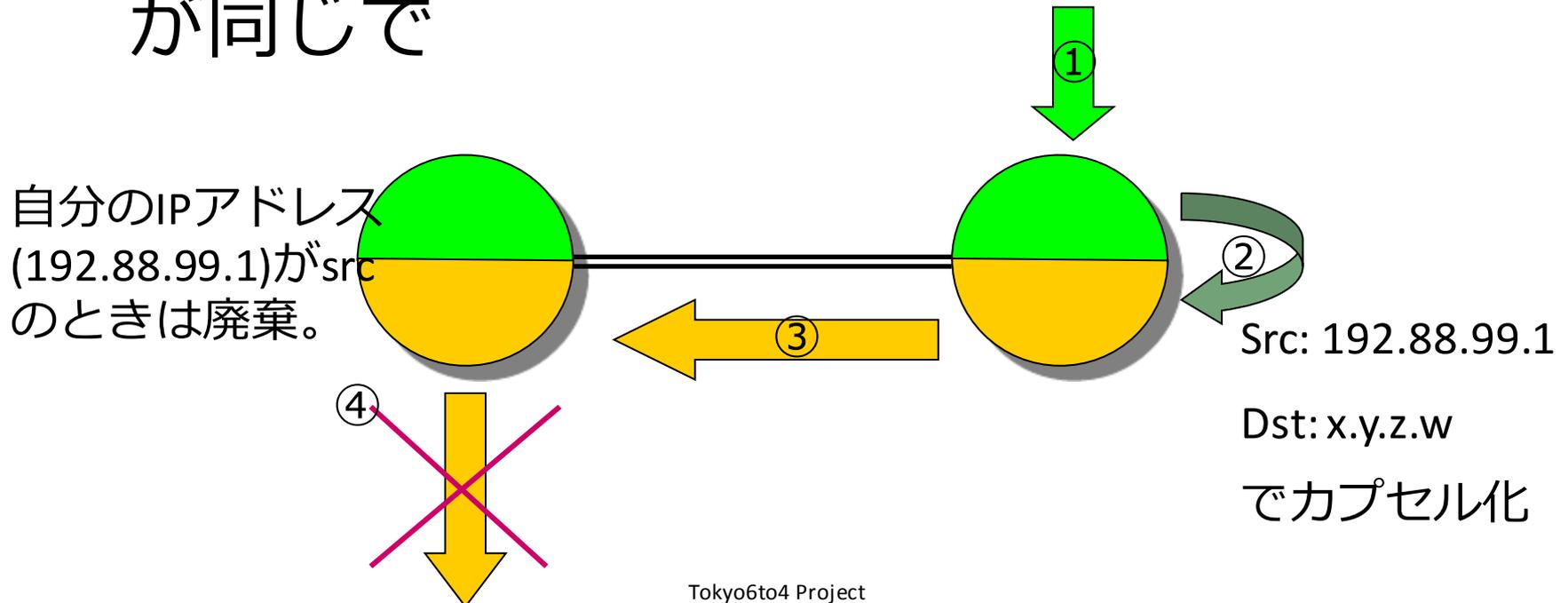
```
tunnel mode ipv6ip 6to4
```

```
tunnel path-mtu-discovery
```

※別途、この箱に192.88.99.0/24と2002::/16が来るようにルーティングの設定が必要

# 実際にやってみて

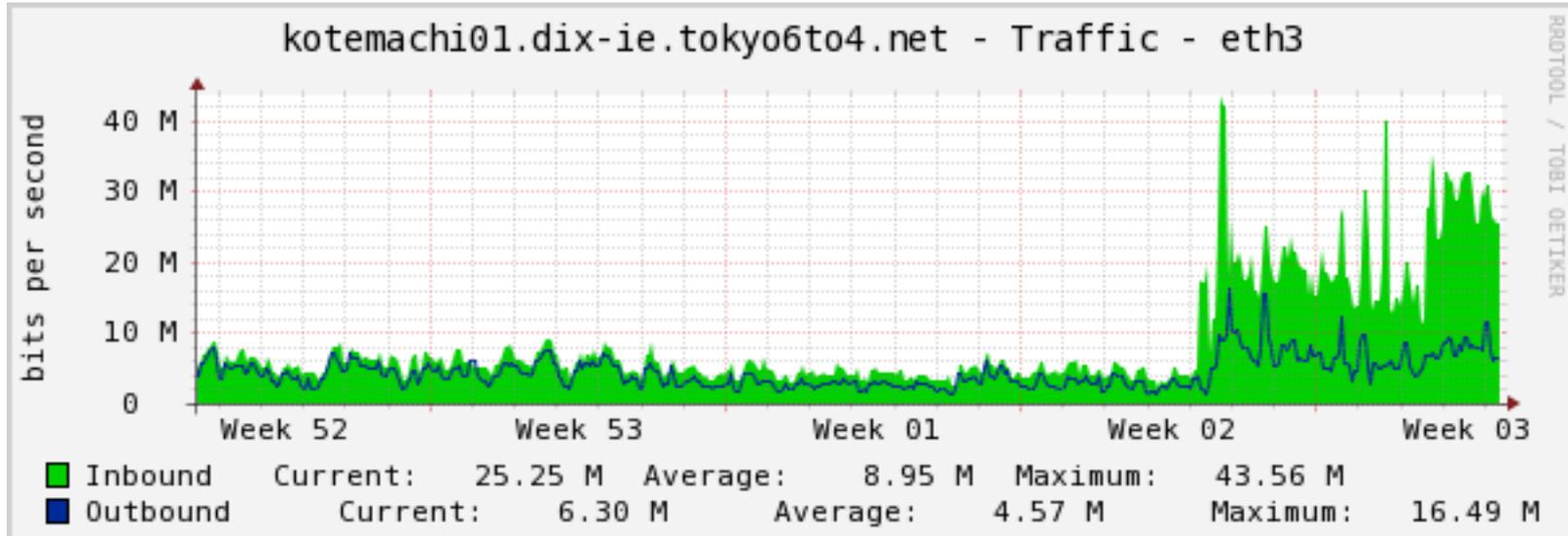
- Quagga MD5問題
- 2台の6to4 relayの、source IPv4アドレスが同じで



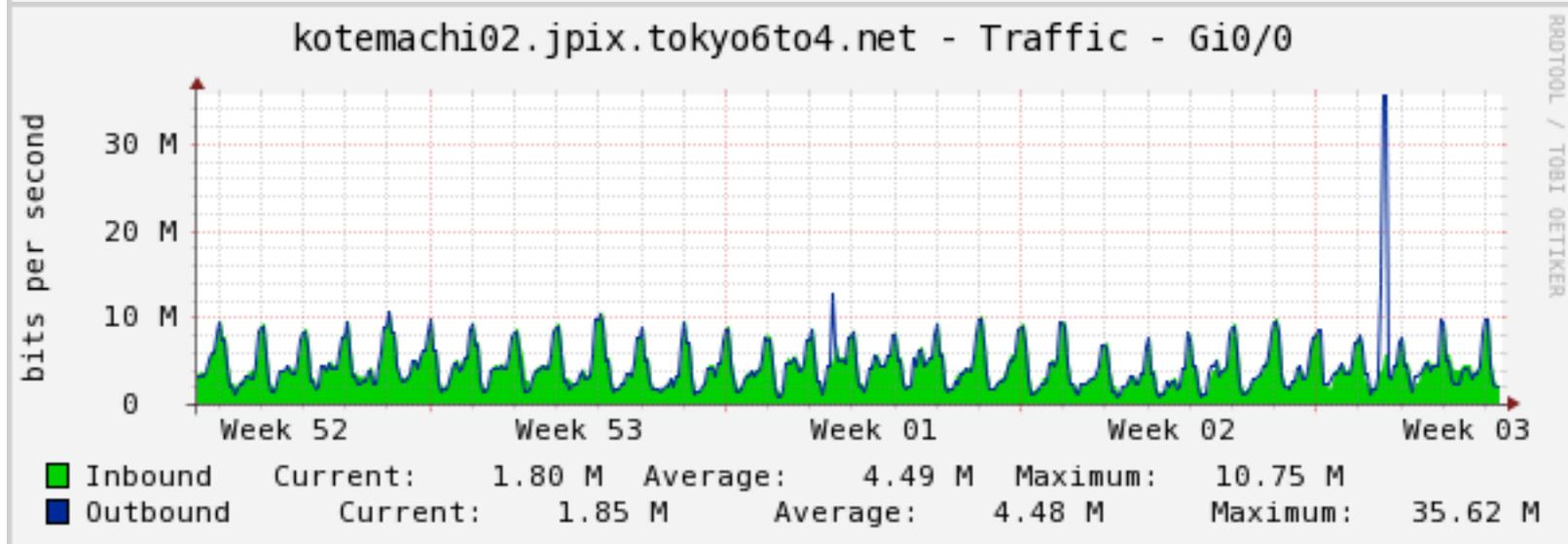


# トラフィック

DIX-IE



JPIX



# 今後の活動予定

## JPNAPでTeredoリレー はじめます！ (2010年3月予定)

- JPNAPユーザのISPさん、ピアしましょう
  - 現在検証・試験運用中
- インターネットマルチフィードさん、NTT PF研さんありがとうございます!

Teredoとは: Microsoft社が開発したIPv6自動トンネリング技術の一種。NATを越えて接続できるのが特徴。





# IPv6自動トンネルの意義と課題

- IPv6普及期におけるIPv6自動トンネル技術
  - 既存の設備を大幅に改修せずIPv6サービスを提供可能
  - ネイティブに比べた場合のオーバーヘッドは存在
- パブリックサービス (Tokyo6to4の領域): 6to4, Teredo
  - 不特定多数を対象としたボランティアなサービス
    - IPトランジットのコスト負担に課題
    - Anycastのため品質保証が難しい: 特に6to4は双方向でAnycast
  - 世界中で最低一社がサービスを提供していれば、(一応は)利用できる
- 商用 (ISP, 企業): 6rd, ISATAP
  - 顧客を対象
  - 利用できる範囲を制限できるためコスト負担も明確

# 今後の予定

- 非商用の実験的サービスから商用サービスへ
  - Tokyo6to4を含む6to4/Teredoリレールータの運営はIPトランジットサービスや他の資源を寄付に依存
  - 持続可能なIPv6接続モデルが必要—商用サービスこそが持続可能なサービスモデル
  - 商用サービス(特に消費者向け)が広く普及した段階で、Tokyo6to4プロジェクトはサービス終了へ
- プロジェクトの運用期間
  - プロジェクト開始時には完了を2010年末に設定
  - NGNサービス上で商用IPv6接続サービスの開始の遅れ(2011年4月予定)から、2011年夏～秋ごろまで期間の延長を検討
- **ノウハウは共有させていただきますので、お気軽にお声かけください!**



ご静聴ありがとうございました