

# IPv6 Fix

An activity to fix flaws of IPv6

23 Feb 2005, 17:40-19:00

Kazu Yamamoto  
The WIDE project  
`contact@v6fix.net`  
`http://v6fix.net/`

## Motivation

---

- IPv6 has minor flaws
  - But they are enough to give bad impressions to users
- An incident of a hotel
  - A man connected his Windows XP in a hotel room
  - An IPv4 address was obtained but his browser did not work
  - When he asked, the hotel answered "Type ipv6 uninstall"
  - (This is due to the system used in the hotel)
- BIND9
  - An ISP installed BIND9 to one of their services
  - Users complained web browsing got slower
  - (This is due to BIND9 implementation)
- Mozilla on Linux
  - When you use Mozilla 1.7 on Fedora core 2, browsing kept waiting for a long time
  - The release note of Mozilla 1.7 recommends to disable IPv6 functionality of OSes
  - (This is due to IPv6 spec called "onlink assumption")

# Instruction of "ipv6 uninstall"


**トラブルシューティング**

ブラウザがループ(検索)状態になり何も画面が表示されない。

↓

IPv6モジュールを使用可能に  
していませんか？


ココの表示が「検索して  
います」や「表示されまし  
た」等ループ状態になる。



**■確認方法**

1) 「スタートボタン」→「プログラム」→「アクセサリ」→「コマンドプロンプト」を選択すると右図が表示されますので「ipconfig」と入力し、キーボードのEnterを押します。

「ipconfig」と  
入力します。



IPv6のIPアドレスが表示されている場合は、IPv6モジュールを削除する必要があります。

IPv4のIPアドレス: 172.31.0.1 192.168.1.1 等全て数字  
IPv6のIPアドレス: fe80:206:56ff:fe02:e82054 等文字を含む

IPv6のIPアドレス

※OSによって「MS-DOSプロンプト」となっている場合があります。

●Windows XPでは「Microsoft IPv6 Developer Edition」というモジュールが標準で入っており、PCの種類によってはもともとインストールされている場合があります。

## Purposes of IPv6 Fix

---

- Fixing flaws of IPv6
  - To prevent users stepping back to IPv4
- The IPv6 specification
  - Fixing flaws if exist
- Implementations
  - Fixing mis-implementations if possible
  - Reporting mis-implementations to vendors
- Operations
  - Reporting mis-operations to operators

## Schedule

---

- Using events as trigger
- 2004.11.10 IETF
  - A presentation in English
  - Web site was opened
- 2004.12.1 Internet Week
  - A BOF in Japanese
  - Some researches
- 2005.1.2 JANOG
  - A presentation in Japanese
  - Japanese document was published
- 2005.2.25 APRICOT
  - A BOF in English
  - English document should be published
- 2005.3.9 IETF
  - A presentation in English
  - Product flaw database should be open

## Fall-back

---

- Smooth fall-back from IPv6 to IPv4 is a key for comfortable communication
  - in the dual-stack environment

### Communication process:

- 1) Looking up to DNS with a given name
  - Obtaining a list of destination addresses
- 2) Making a connection
  - Finding a pair of dest addr and src addr
- 3) Exchanging data
  - Negotiating of path MTU, etc

# 1) Looking up to DNS

---

- Resolving A RR and AAAA RR
  - if both IPv4 and IPv6 are available

## Problems

- Resolver problems
  - Resolving AAAA RR even when IPv6 is NOT available
- DNS server problems
  - 1) Returning a broken answer for an AAAA RR query
  - 2) Trying to look up DNS servers with unavailable IPv6
    - The cause of the BIND9 incident
    - It will be fixed in Bind version 9.2.5 and 9.3.1
- EDNS0 does NOT work
  - Some firewalls drop large DNS packets with EDNS0

## 2) Making a connection

---

- Finding a pair of dst addr and src addr
  - Finding a proper src addr for a dst addr
  - If a connection can be made, break. Otherwise, loop

### Problems

- Onlink assumption (Section 5.2, RFC 2461)
  - A dst is assumed to be on the same link
    - The dst addr is a global IPv6 addr
    - A default route does not exist
    - Only link-local addresses are available as src addr
  - Kept waiting for TCP timeout
    - The cause of the Mozilla 1.7 incident
- Mis-operation
  - A server does not accept IPv6 connections
    - eg) AAAA RR is registered and reachable with IPv6  
The server provides a mail service with IPv6, not a web service
  - Kept waiting for TCP RST (minor problem)
  - Cannot gain access to the server through an IPv6 => IPv4 translator

## 3) Exchanging data

---

- For smooth communication
  - Using an appropriate route
  - ICMPv6 must be exchangeable
    - Destination unreachable
    - Packet too big
    - Time exceeded

### Problems

- IPv6 connectivity quality
  - Some operations are still experimental
    - Since they do not use it in daily life, they cannot notice problems
  - Using improper tunnels
    - even though there are faster routes
- ICMPv6 is not exchangeable
  - Some firewalls drop ICMPv6 packets

## Summary of Activities

---

- IPv6 specification
  - Deleting onlink assumption
- Operation #
- DNS
  - Servers #
  - Resolvers #
- Quality
  - IPv6 connectivity #
  - TCP
  - ICMPv6 (Firewall) #
  - EDNS0 (Firewall) #
- Product information
  - BIND 9, the hotel system, etc

# items will be discussed in detail

## Operation

---

- Mail is IPv6 ready but web is not  
eg) If you change FreeBSD to OpenBSD,  
Apache 1.3 is not IPv6 ready

### Bad)

```
server.example.com. IN A      192.0.2.1
                   IN AAAA  2001:DB8::1
www.example.com.   IN CNAME server.example.com.
mail.example.com.  IN CNAME server.example.com.
```

### Good)

```
www.example.com.  IN A      192.0.2.1
mail.example.com. IN A      192.0.2.1
                   IN AAAA  2001:DB8::1
```

## DNS servers

---

- Right answer for "A RR exists but AAAA RR not"
  - RCODE 0 (no error) + answer section is empty

### Problems

- Ignoring AAAA RR
  - A RR query after timeout of AAAA RR query
- Returning RCODE 3 ("Name Error"="NXDOMAIN")
  - A RR query is not sent
- Returning RCODE other than "Name Error"
  - Negative cache does not work (minor problem)
- Auth servers return broken answer
  - Two kinds of actions of caching servers
    - Cache it as is
    - Throw away it and return RCODE 2 ("Server Failure")
  - In the latter case, AAAA RR query is repeatedly sent
- Lame delegation
  - A RR => auth, AAAA RR => inauth
  - Some caching servers cannot resolve A RR

## Investigating DNS servers

---

- Obtaining a list of domain under ".jp"
  - As collaborative research with JPRS
  - example.jp
- Identifying DNS auth servers
  - ns.example.jp, ns.wide.ad.jp
- A RR query to one of them with guessed name
  - A RR of www.example.jp => ns.example.jp
- If the name exists, AAAA RR query to them
  - AAAA RR of www.example.jp => ns.example.jp
  - AAAA RR of www.example.jp => ns.wide.ad.jp
- Measures
  - Domain: example.jp
  - DNS servers: ns.example.jp, ns.wide.ad.jp

## Result of the Investigation

---

- 2004.11.22

	domain	DNS server
no problem	82.16%	84.39%
problem	0.04%	0.11%
unknown	17.80%	15.50%

- Breakdown of the problematic DNS server case

- Ignoring AAAA RR (4.7%)
- Returning RCODE 3 (4.7%)
- Returning RCODE other than "Name Error" (8.5%)
- Auth servers return broken answer (0.0%)
- Lame delegation (82.1%)

- Product information is welcome!

# Workarounds of DNS resolvers

---

- Problem 1
  - getaddrinfo() resolves both A RR and AAAA RR always if AF\_UNSPEC is specified
- Workaround 1
  - getaddrinfo() resolves AAAA RR only when the host has global IPv6 addresses
    - Even AF\_UNSPEC is specified
    - This is a conformant behavior to the spec (RFC 3493)
- Problem 2
  - Sending AAAA RR query
  - If resolved or timeout, then sending A RR query
- Workaround 2
  - Sending A RR and AAAA RR query at the same time
  - If A RR is resolved, shrink the timeout of AAAA RR query
- Available in KAME snapshot

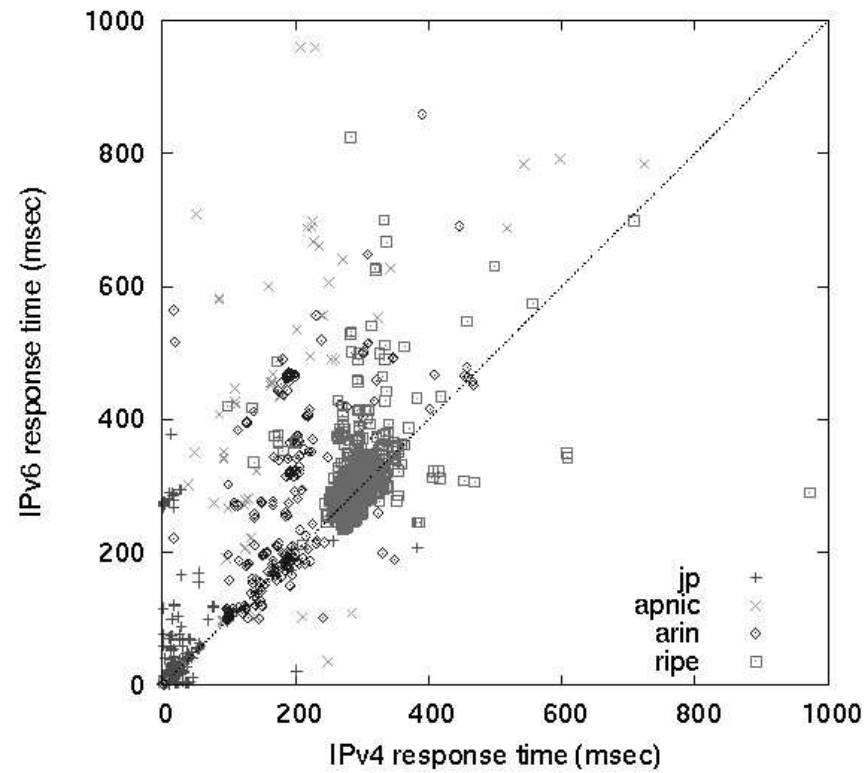
## Research on IPv6 quality

---

- Problems
  - Bad quality because of some experimental operations
  - Old unnecessary tunnels are still used
- Measurement of RTT with "ping"
  - Comparing IPv4 and IPv6
- Measurement of routes with "traceroute"
  - Finding suboptimal tunnels against physical topology
- Continuing the research
  - To watch the quality will get better

# Result of Ping

2004.8.23



SIGCOMM'04: "Identifying IPv6 Network Problems in the Dual-Stack World"

# Firewalls

---

- The problems
  - Dropping ICMPv6 packets
  - Dropping large DNS packets (with EDNS0)
- Making a tool
  - Generating an IPv6 packet which triggers ICMPv6 packets
  - Generating a DNS query which triggers large responses
  - Watching whether or not packets are returned
- Releasing the tool in the near future
  - People can test their firewalls by themselves

# Requests

---

- Proofreading of documents is welcome
  - English is not our native tongue
- Give us product information
  - Improper firewalls
  - Improper DNS servers
- DNS check
  - You can check with Malone's tool
    - [http://www.cnri.dit.ie/cgi-bin/check\\_aaaa.pl](http://www.cnri.dit.ie/cgi-bin/check_aaaa.pl)
- IPv6 quality
  - Please stop experimental operations
  - Please delete old tunnels (at the time of 6bone)
- Contact point
  - [contact@v6fix.net](mailto:contact@v6fix.net)
  - <http://v6fix.net/>