

IPv6 Operations Working Group  
Internet-Draft  
Intended status: Informational  
Expires: August 28, 2008

A. Matsumoto  
T. Fujisaki  
NTT  
R. Hiromi  
K. Kanayama  
Intec Netcore  
February 25, 2008

**Problem Statement of Default Address Selection in Multi-prefix  
Environment: Operational Issues of [RFC3484](#) Default Rules  
draft-ietf-v6ops-addr-select-ps-04.txt**

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on August 28, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2008).

Abstract

One physical link can carry multiple subnets. Moreover, we can use multiple physical networks at the same time in a host. In that environment, end hosts might have multiple IP addresses and be required to use them selectively. Without an appropriate source/

destination address selection mechanism, the host will experience some trouble in communication. [RFC 3484](#) defines default source and destination address selection algorithms, but the multi-prefix environment considered here needs additional rules beyond those of the default operation. This document describes the possible problems that end hosts could encounter in an environment with multiple subnets.

## Table of Contents

<a href="#">1.</a>	<a href="#">Introduction</a>	<a href="#">3</a>
<a href="#">1.1.</a>	<a href="#">Scope of this document</a>	<a href="#">3</a>
<a href="#">2.</a>	<a href="#">Problem Statement</a>	<a href="#">3</a>
<a href="#">2.1.</a>	<a href="#">Source Address Selection</a>	<a href="#">3</a>
<a href="#">2.1.1.</a>	<a href="#">Multiple Routers on Single Interface</a>	<a href="#">4</a>
<a href="#">2.1.2.</a>	<a href="#">Ingress Filtering Problem</a>	<a href="#">5</a>
<a href="#">2.1.3.</a>	<a href="#">Half-Closed Network Problem</a>	<a href="#">5</a>
<a href="#">2.1.4.</a>	<a href="#">Combined Use of Global and ULA</a>	<a href="#">7</a>
<a href="#">2.1.5.</a>	<a href="#">Site Renumbering</a>	<a href="#">8</a>
<a href="#">2.1.6.</a>	<a href="#">Multicast Source Address Selection</a>	<a href="#">8</a>
<a href="#">2.1.7.</a>	<a href="#">Temporary Address Selection</a>	<a href="#">8</a>
<a href="#">2.2.</a>	<a href="#">Destination Address Selection</a>	<a href="#">9</a>
<a href="#">2.2.1.</a>	<a href="#">IPv4 or IPv6 prioritization</a>	<a href="#">9</a>
<a href="#">2.2.2.</a>	<a href="#">ULA and IPv4 dual-stack environment</a>	<a href="#">10</a>
<a href="#">2.2.3.</a>	<a href="#">ULA or Global Prioritization</a>	<a href="#">10</a>
<a href="#">3.</a>	<a href="#">Conclusion</a>	<a href="#">11</a>
<a href="#">4.</a>	<a href="#">Security Considerations</a>	<a href="#">12</a>
<a href="#">5.</a>	<a href="#">IANA Considerations</a>	<a href="#">12</a>
<a href="#">6.</a>	<a href="#">References</a>	<a href="#">12</a>
<a href="#">6.1.</a>	<a href="#">Normative References</a>	<a href="#">12</a>
<a href="#">6.2.</a>	<a href="#">Informative References</a>	<a href="#">13</a>
<a href="#">Appendix A.</a>	<a href="#">Appendix. Revision History</a>	<a href="#">13</a>
	<a href="#">Authors' Addresses</a>	<a href="#">13</a>
	<a href="#">Intellectual Property and Copyright Statements</a>	<a href="#">15</a>



## **1. Introduction**

One physical link can carry multiple subnets. In that case, an end-host has multiple IP addresses. In the IPv4-IPv6 dual stack environment or in a site connected to both a ULA [[RFC4193](#)] and Global scope networks, an end-host has multiple IP addresses. These are examples of networks that we focus on in this document. In such an environment, an end-host will encounter some communication troubles.

Inappropriate source address selection at the end-host causes unexpected asymmetric routing, filtering by a router or discarding of packets because there is no route to the host.

Considering a multi-prefix environment, destination address selection is also important for correct or better communication establishment.

[RFC 3484](#) [[RFC3484](#)] defines default source and destination address selection algorithms. In most cases, the host will be able to communicate with the targeted host using the algorithms. However, there are still problematic cases. This document describes such possibilities of incorrect address selection, which leads to dropping packets and communication failure.

### **1.1. Scope of this document**

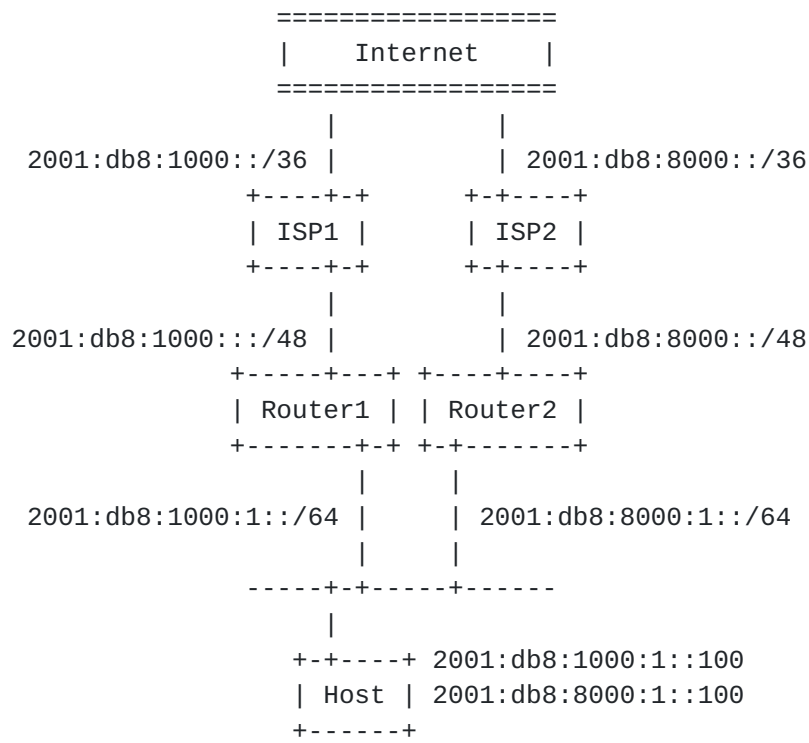
There has been a lot of discussion about "multiple addresses/prefixes". As other mechanisms already exists, the multi-homing techniques for achieving redundancy are out of our scope.

We focus on an end-site network environment. The scope of this document is to sort out problematic cases related to address selection. It includes problems that cannot always be solved by changing the host's address selection algorithm, such as an address selection mechanism that depends on the IPv6 address types. For example, a global address isn't always globally routable and ULA's routable domain is dependent on the network policy. This document includes these kind of network policy related address selection problems, as long as these problems are serious enough and worth solving.

## **2. Problem Statement**

### **2.1. Source Address Selection**



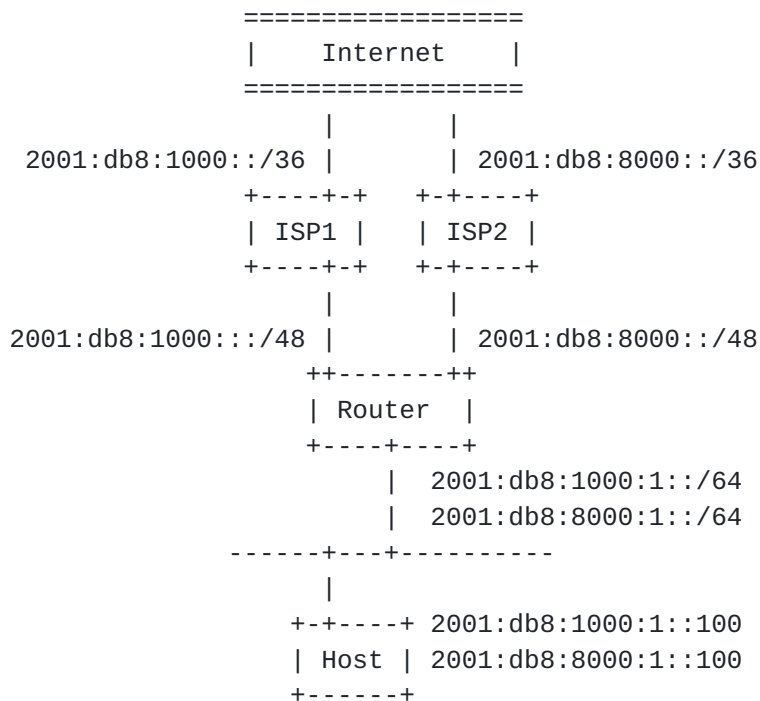
**2.1.1. Multiple Routers on Single Interface**

[Fig. 1]

Generally speaking, there is no interaction between next-hop determination and address selection. In this example, when a host sends a packet via Router1, the host does not necessarily choose address 2001:db8:1000:1::100 given by Router1 as the source address. This causes the same problem as described in the next section 'Ingress Filtering Problem'.



### 2.1.2. Ingress Filtering Problem



[Fig. 2]

When a relatively small site, which we call a "customer network", is attached to two upstream ISPs, each ISP delegates a network address block, which is usually /48, and a host has multiple IPv6 addresses.

When the source address of an outgoing packet is not the one that is delegated by an upstream ISP, there is a possibility that the packet will be dropped at the ISP by its Ingress Filter. Ingress filtering(uRPF: unicast Reverse Path Forwarding) is becoming more popular among ISPs to mitigate the damage of DoS attacks.

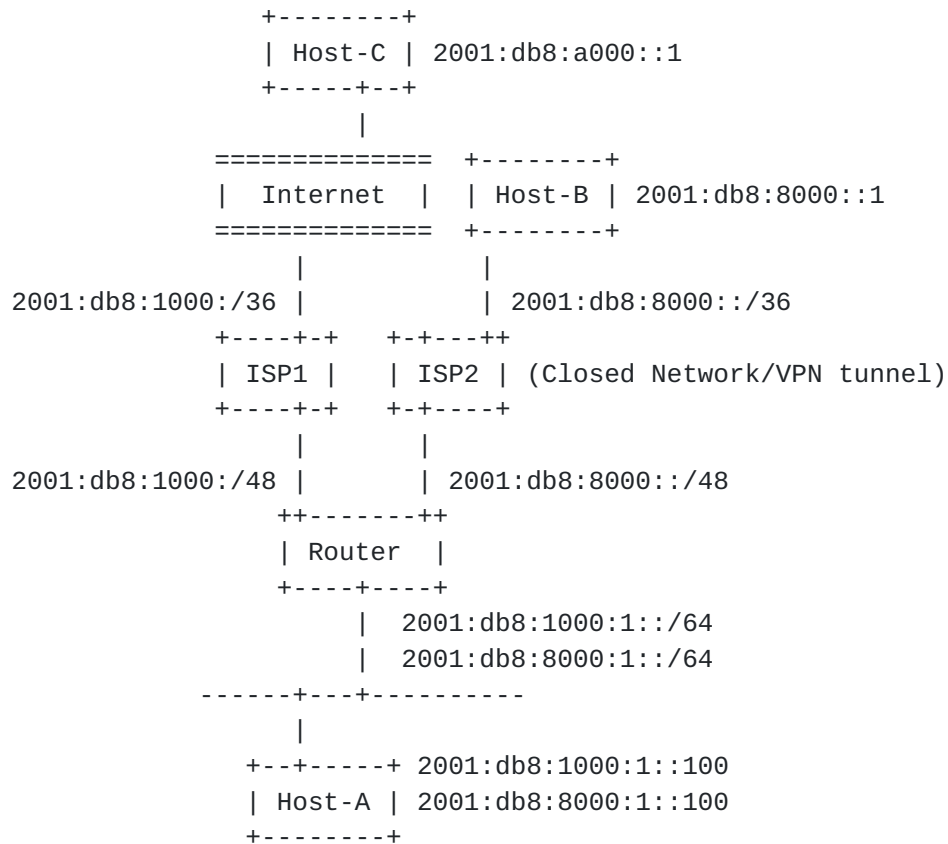
In this example, when the Router chooses the default route to ISP2 and the Host chooses 2001:db8:1000:1::100 as the source address for packets sent to a host (2001:db8:2000::1) somewhere on the Internet, the packets may be dropped at ISP2 because of Ingress Filtering.

### 2.1.3. Half-Closed Network Problem

You can see a second typical source address selection problem in a multihomed site with global-closed mixed connectivity like in the figure below. In this case, Host-A is in a multihomed network and has two IPv6 addresses, one delegated from each of the upstream ISPs. Note that ISP2 is a closed network and does not have connectivity to the Internet.







[Fig. 3]

You do not need two physical network connections here. The connection from the Router to ISP2 can be a logical link over ISP1 and the Internet.

When Host-A starts the connection to Host-B in ISP2, the source address of a packet that has been sent will be the one delegated from ISP2, that is 2001:db8:8000:1::100, because of rule 8 (longest matching prefix) in [RFC 3484](#).

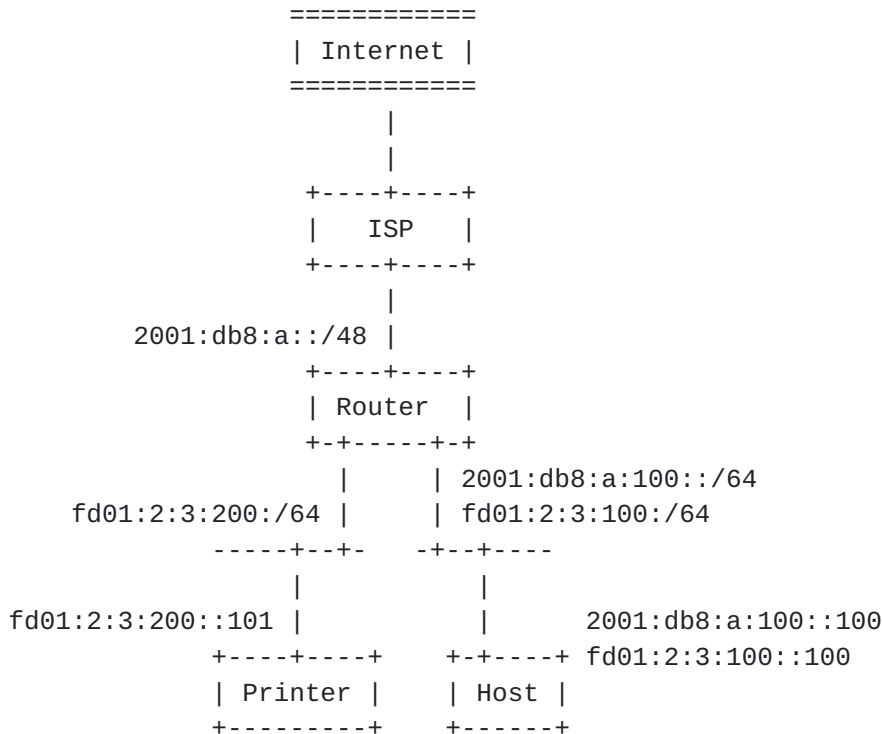
Host-C is located somewhere on the Internet and has IPv6 address 2001:db8:a000::1. When Host-A sends a packet to Host-C, the longest matching algorithm chooses 2001:db8:8000:1::100 for the source address. In this case, the packet goes through ISP1 and may be filtered by ISP1's ingress filter. Even if the packet is not filtered by ISP1, a return packet from Host-C cannot possibly be delivered to Host-A because the return packet is destined for 2001:db8:8000:1::100, which is closed from the Internet.

The important point is that each host chooses a correct source address for a given destination address as long as NAT does not exist in the IPv6 world. To solve this kind of network policy based



address selection problems, it is likely that delivering additional information to a node fits better than algorithmic solutions that are local to the node.

#### [2.1.4.](#) Combined Use of Global and ULA



[Fig. 4]

As NAP [[I-D.ietf-v6ops-nap](#)] describes, using a ULA may be beneficial in some scenarios. If the ULA is used for internal communication, packets with ULA need to be filtered at the Router.

There is no serious problem related to address selection in this case, because of the dissimilarity between the ULA and the Global Unicast Address. The longest matching rule of [RFC 3484](#) chooses the correct address for both intra-site and extra-site communication.

In the future, however, there is a possibility that the longest matching rule will not be able to choose the correct address anymore. That is the moment when the assignment of those Global Unicast Addresses starts, where the first bit is 1. In [RFC 4291](#) [[RFC4291](#)], almost all address spaces of IPv6, including those whose first bit is 1, are assigned as Global Unicast Addresses.

Namely, when we start to assign a part of the address block 8000::/1 as the global unicast address and that part is used somewhere in the



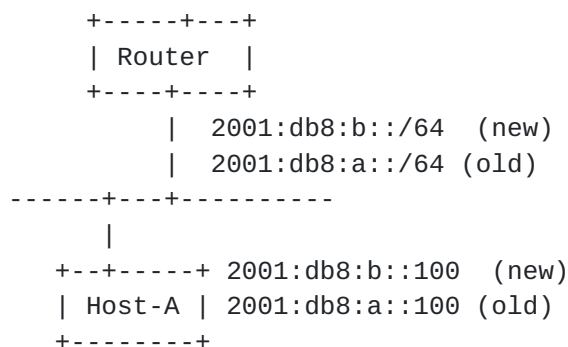
Internet, the longest matching rule ceases to function properly for the people trying to connect to the servers with those addresses.

#### 2.1.5. Site Renumbering

[RFC 4192](#) [[RFC4192](#)] describes a recommended procedure for renumbering a network from one prefix to another. An autoconfigured address has a lifetime, so by stopping advertisement of the old prefix, the autoconfigured address is eventually invalidated.

However, invalidating the old prefix takes a long time. You cannot stop routing to the old prefix as long as the old prefix is not removed from the host. This can be a tough issue for ISP network administrators.

There is a technique of advertising the prefix with the preferred lifetime zero, however, [RFC 4862](#) [[RFC4862](#)] 5.5.4 allows the use of a deprecated address for a new outgoing connection. So, this technique isn't always perfect.



[Fig. 5]

#### 2.1.6. Multicast Source Address Selection

This case is an example of Site-local or Global prioritization. When you send a multicast packet across site-borders, the source address of the multicast packet should be a globally routable address. The longest matching algorithm, however, selects a ULA if the sending host has both a ULA and a global address.

#### 2.1.7. Temporary Address Selection

[RFC 3041](#) [[RFC3041](#)] defines a Temporary Address. The usage of a Temporary Address has both pros and cons. That is good for viewing web pages or communicating with the general public, but that is bad for a service that uses address-based authentication and for logging purposes.



In the figure above, a site has native IPv4 and tunneled-IPv6 connectivity. Therefore, the administrator may want to set a higher

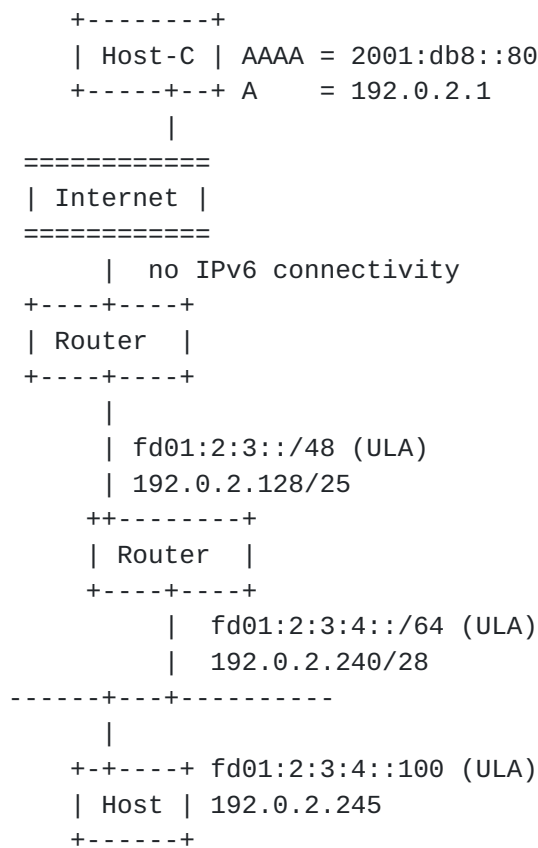




priority for using IPv4 than using IPv6 because the quality of the tunnel network seems to be worse than that of the native transport.

### **2.2.2. ULA and IPv4 dual-stack environment**

This is a special form of IPv4 and IPv6 prioritization. When an enterprise has IPv4 Internet connectivity but does not yet have IPv6 Internet connectivity, and the enterprise wants to provide site-local IPv6 connectivity, a ULA is the best choice for site-local IPv6 connectivity. Each employee host will have both an IPv4 global or private address and a ULA. Here, when this host tries to connect to Host-C that has registered both A and AAAA records in the DNS, the host will choose AAAA as the destination address and the ULA for the source address. This will clearly result in a connection failure.



[Fig. 7]

### **2.2.3. ULA or Global Prioritization**

Differentiating services by the client's source address is very common. IP-address-based authentication is an typical example of this. Another typical example is a web service that has pages for the public and internal pages for employees or involved parties. Yet







#### **4. Security Considerations**

When an intermediate router performs policy routing (e.g. source address based routing), inappropriate address selection causes unexpected routing. For example, in the network described in 2.1.3, when Host-A uses a default address selection policy and chooses an inappropriate address, a packet sent to VPN can be delivered to a location via the Internet. This issue can lead to packet eavesdropping or session hijack. However, sending the packet back to the correct path from the attacker to the node is not easy, so these two risk are not serious.

As documented in the security consideration section in [RFC 3484](#), address selection algorithms expose a potential privacy concern. When a malicious host can make a target host perform address selection, for example by sending a anycast or a multicast packet, the malicious host can know multiple addresses attached to the target host. In a case like 2.1.4, if an attacker can make Host to send a multicast packet and Host performs the default address selection algorithm, the attacker may be able to determine the ULAs attached to the Host.

These security risks have roots in inappropriate address selection. Therefore, if a countermeasure is taken, and hosts always select an appropriate address that is suitable to a site's network structure and routing, these risks can be avoided.

#### **5. IANA Considerations**

This document has no actions for IANA.

#### **6. References**

##### **6.1. Normative References**

- [I-D.ietf-v6ops-nap]  
Velde, G., "Local Network Protection for IPv6",  
[draft-ietf-v6ops-nap-06](#) (work in progress), January 2007.
- [RFC3041] Narten, T. and R. Draves, "Privacy Extensions for  
Stateless Address Autoconfiguration in IPv6", [RFC 3041](#),  
January 2001.
- [RFC3484] Draves, R., "Default Address Selection for Internet  
Protocol version 6 (IPv6)", [RFC 3484](#), February 2003.



- [RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", [RFC 3775](#), June 2004.
- [RFC4192] Baker, F., Lear, E., and R. Droms, "Procedures for Renumbering an IPv6 Network without a Flag Day", [RFC 4192](#), September 2005.
- [RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", [RFC 4193](#), October 2005.
- [RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", [RFC 4291](#), February 2006.
- [RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", [RFC 4862](#), September 2007.

## **[6.2.](#) Informative References**

## **[Appendix A.](#) Appendix. Revision History**

- 01:  
IP addresse notations changed to documentation address.  
Descriptoin of solutions deleted.
- 02:  
Security considerations section rewritten according to comments from SECDIR.
- 03:  
Intended status changed to Informational.
- 04:  
This version reflects comments from IESG members.

## Authors' Addresses

Arifumi Matsumoto  
NTT PF Lab  
Midori-Cho 3-9-11  
Musashino-shi, Tokyo 180-8585  
Japan

Phone: +81 422 59 3334  
Email: arifumi@nttv6.net





Tomohiro Fujisaki  
NTT PF Lab  
Midori-Cho 3-9-11  
Musashino-shi, Tokyo 180-8585  
Japan

Phone: +81 422 59 7351  
Email: fujisaki@nttv6.net

Ruri Hiromi  
Intec Netcore, Inc.  
Shinsuna 1-3-3  
Koto-ku, Tokyo 136-0075  
Japan

Phone: +81 3 5665 5069  
Email: hiromi@inetcore.com

Ken-ichi Kanayama  
Intec Netcore, Inc.  
Shinsuna 1-3-3  
Koto-ku, Tokyo 136-0075  
Japan

Phone: +81 3 5665 5069  
Email: kanayama@inetcore.com



## Full Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

## Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at [ietf-ipr@ietf.org](mailto:ietf-ipr@ietf.org).

## Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).

